

Microsoft Entra fundamentals documentation

Learn about Microsoft Entra concepts and processes, such as creating a basic environment, adding users, applying licenses, and managing groups.

About Microsoft Entra ID

OVERVIEW

[What is Microsoft Entra ID?](#)

[What's new in Microsoft Entra ID](#)

CONCEPT

[Microsoft Entra architecture](#)

Get started

QUICKSTART

[Access the portal and create a tenant](#)

[Create a group and add members](#)

[Add company branding](#)

Create a Microsoft Entra account

HOW-TO GUIDE

[Sign up for Microsoft Entra ID P1 or P2 editions](#)

[Sign up for Microsoft Entra ID as an organization](#)

[Add your custom domain name](#)

Manage groups in Microsoft Entra ID

CONCEPT

[Learn about groups](#)

HOW-TO GUIDE

[Manage groups and group membership](#)

Add users and assign roles and licenses

HOW-TO GUIDE

[Create or delete users](#)

[Assign roles to users](#)

[Assign licenses to users](#)

Microsoft Security Copilot + Microsoft Entra

HOW-TO GUIDE

[Respond to identity threads using risky user summarization](#)

[Investigate incidents using Microsoft Copilot for Security](#)

What is Microsoft Entra?

Article • 07/11/2024

Microsoft Entra is a family of identity and network access products. It enables organizations to implement a [Zero Trust](#) security strategy and create a [trust fabric](#) that verifies identities, validates access conditions, checks permissions, encrypts connection channels, and monitors for compromise.

Microsoft Entra product family

The Microsoft Entra product family covers four maturity stages of secure end-to-end access for any trustworthy identity. These stages include establishing Zero Trust access controls, and securing access for employees, customers, partners, and any cloud environment.



Establish Zero Trust access controls

Microsoft Entra ID

[Microsoft Entra ID](#) is the foundational product of Microsoft Entra. It provides the essential identity, authentication, policy, and protection to secure employees, devices, and enterprise apps and resources.

Microsoft Entra Domain Services

[Microsoft Entra Domain Services](#) provides managed domain services such as group policy, lightweight directory access protocol (LDAP), and Kerberos/NTLM authentication. It enables organizations to run legacy applications in the cloud that can't use modern authentication methods.

For example, organizations with services that require access to Kerberos authentication can create a managed domain where the core service components are deployed and maintained by Microsoft as a managed domain experience.

Secure access for employees

Microsoft Entra Private Access

[Microsoft Entra Private Access](#) secures access to all private apps and resources, including corporate networks and multicloud environments. It enables remote users to connect to internal resources from any device and network without a virtual private network (VPN).

For example, an employee can securely access a corporate network printer while working from home or even a cafe.

Microsoft Entra Internet Access

[Microsoft Entra Internet Access](#) secures access to all internet resources including software as a service (SaaS) apps, and Microsoft 365 apps and resources. It enables organizations to continuously monitor and adjust user access in real time if permissions or risk levels change.

For example, organizations can enable web content filtering to regulate access to websites based on content categories and domain names.

Microsoft Entra ID Governance

[Microsoft Entra ID Governance](#) makes identity and permissions easier to manage by automating access requests, assignments, and reviews. Additionally, it helps protect critical assets through identity lifecycle management.

For example, administrators can automatically assign user accounts and Microsoft 365 licenses to new employees, and remove those assignments from employees that are no longer with the company.

Microsoft Entra ID Protection

[Microsoft Entra ID Protection](#) detects and reports identity-based risks. It enables administrators to investigate and automatically remediate risks using tools like [Conditional Access](#).

For example, organizations can create risk-based Conditional Access policies that require multifactor authentication when the sign-in risk level is reported as medium or high.

Microsoft Entra Verified ID

In addition to identities that are used for authentication, there are decentralized identities (DIDs) used for information verification.

[Microsoft Entra Verified ID](#) is a credential verification service based on open [DID standards](#). It enables organizations to issue a verifiable credential (digital signature proving the validity of information) to a user who stores the credential on their personal device. After they receive the verifiable credential, the user can present it to a company or organization that wants to verify something about their identity.

For example, a recent college graduate can ask the university to issue a digital copy of their diploma to their DID. They can then choose to present the diploma to a potential employer who can independently verify the issuer of the diploma, the time of issuance, and its status.

Secure access for customers and partners

Microsoft Entra External ID

[Microsoft Entra External ID](#) enables external identities to safely access business resources and consumer apps. It offers secure methods for collaborating with business partners and guests on internal apps and resources, as well as managing customer identity and access management (CIAM) for your consumer-facing applications.

For example, organizations can set up self-service registration for customers to sign-in to a web application using methods such as one-time passcodes, or social accounts from Google or Facebook.

Secure access in any cloud

Microsoft Entra Permissions Management

[Microsoft Entra Permissions Management](#) provides comprehensive visibility into permissions assigned to all identities managed by Microsoft Entra ID and other identity providers. It enables organizations to detect, automatically right-size, and continuously monitor unused and excessive permissions across Microsoft Azure, Amazon Web Services (AWS), and Google Cloud Platform (GCP).

For example, administrators can see the users that have high-risk permissions but aren't using them, and automatically remove those unused permissions across authorization systems.

Microsoft Entra Workload ID

In addition to human and device identities, workload identities such as applications, services, and containers require authentication and authorization policies.

[Microsoft Entra Workload ID](#) is the identity and access management solution for workload identities. It enables organizations to secure access to resources using adaptive policies and custom security attributes for apps.

For example, GitHub Actions need a workload identity to access Azure subscriptions to automate, customize, and execute software development workflows.

Getting ready for Microsoft Entra

Before organizations deploy Microsoft Entra, they should configure their infrastructure and processes according to security best practices and standards. The following articles provide the architectural, deployment, and operational guidance to successfully integrate Microsoft Entra.

- [Architecture](#)
- [Deployment plans](#)
- [Operations reference](#)
- [Operations guide](#)

Working with Microsoft Entra

After organizations deploy Microsoft Entra, administrators can use the [Microsoft Entra admin center](#) and [Microsoft Graph API](#) to manage the identity and network access resources, and developers can use the [Microsoft identity platform](#) to build identity and access applications.

Microsoft Entra admin center

The [Microsoft Entra admin center](#) is a web-based portal for administrators to configure and manage Microsoft Entra products using a single user interface.

To learn more, see [Overview of Microsoft Entra admin center](#).

Microsoft Graph API

In addition to the Microsoft Entra admin center, the [Microsoft Graph API](#) can be used to automate administrative tasks, including license deployments, and user lifecycle management.

To learn more, see [Manage Microsoft Entra using Microsoft Graph](#).

Microsoft identity platform

The [Microsoft identity platform](#) enables developers to build authentication experiences for web, desktop, and mobile applications using open-source libraries and standard-compliant authentication services.

To start developing, see [Getting started](#).

Next steps

- [Licensing](#)
-

Feedback

Was this page helpful?



[Provide product feedback](#)

What is Microsoft Entra ID?

Article • 03/05/2025

Microsoft Entra ID is a cloud-based identity and access management service that your employees can use to access external resources. Example resources include Microsoft 365, the Azure portal, and thousands of other SaaS applications.

Microsoft Entra ID also helps them access internal resources like apps on your corporate intranet, and any cloud apps developed for your own organization. To learn how to create a tenant, see [Quickstart: Create a new tenant in Microsoft Entra ID](#).

To learn the differences between Active Directory and Microsoft Entra ID, see [Compare Active Directory to Microsoft Entra ID](#). You can also refer to [Microsoft Cloud for Enterprise Architects Series](#) posters to better understand the core identity services in Azure like Microsoft Entra ID and Microsoft-365.

Who uses Microsoft Entra ID?

Microsoft Entra ID provides different benefits to members of your organization based on their role:

- **IT admins** use Microsoft Entra ID to control access to apps and app resources, based on business requirements. For example, as an IT admin, you can use Microsoft Entra ID to require multifactor authentication when accessing important organizational resources. You could also use Microsoft Entra ID to automate user provisioning between your existing Windows Server AD and your cloud apps, including Microsoft 365. Finally, Microsoft Entra ID gives you powerful tools to automatically help protect user identities and credentials and to meet your access governance requirements. To get started, sign up for a [free 30-day Microsoft Entra ID P1 or P2 trial](#).
- **App developers** can use Microsoft Entra ID as a standards-based authentication provider that helps them add single sign-on (SSO) to apps that work with a user's existing credentials. Developers can also use Microsoft Entra APIs to build personalized experiences using organizational data. To get started, sign up for a [free 30-day Microsoft Entra ID P1 or P2 trial](#). For more information, you can also see [Microsoft Entra ID for developers](#).
- **Microsoft 365, Office 365, Azure, or Dynamics CRM Online subscribers** already use Microsoft Entra ID as every Microsoft 365, Office 365, Azure, and Dynamics

CRM Online tenant is automatically a Microsoft Entra tenant. You can immediately start managing access to your integrated cloud apps.

What are the Microsoft Entra ID licenses?

Microsoft Online business services, such as Microsoft 365 or Microsoft Azure, use Microsoft Entra ID for sign-in activities and to help protect your identities. If you subscribe to any Microsoft Online business service, you automatically get access to [Microsoft Entra ID Free](#).

To enhance your Microsoft Entra implementation, you can also add paid features by upgrading to Microsoft Entra ID P1 or P2 licenses, or adding on licenses for products such as Microsoft Entra ID Governance. You can also license Microsoft Entra paid licenses are built on top of your existing free directory. The licenses provide self-service, enhanced monitoring, security reporting, and secure access for your mobile users.

Note

For the pricing options of these licenses, see [Microsoft Entra pricing](#).

For more information about Microsoft Entra pricing, contact the [Microsoft Entra Forum](#).

- **Microsoft Entra ID Free.** Provides user and group management, on-premises directory synchronization, basic reports, self-service password change for cloud users, and single sign-on across Azure, Microsoft 365, and many popular SaaS apps.
- **Microsoft Entra ID P1.** In addition to the Free features, P1 also lets your hybrid users access both on-premises and cloud resources. It also supports advanced administration, such as dynamic membership groups, self-service group management, Microsoft Identity Manager, and cloud write-back capabilities, which allow self-service password reset for your on-premises users.
- **Microsoft Entra ID P2.** includes features in addition to the features included in Free and P1. P2 includes [Microsoft Entra ID Protection](#) to help provide risk-based Conditional Access to your apps and critical company data and [Privileged Identity Management](#) to help discover, restrict, monitor administrators, their access to resources and to provide just-in-time access when needed.

In addition to Microsoft Entra ID licenses, you can enable additional identity management capabilities with licenses for other Microsoft Entra products, including:

- **Microsoft Entra ID Governance.** [Microsoft Entra ID Governance](#) is an advanced set of [identity governance capabilities](#) for Microsoft Entra ID P1 and P2 customers.
- **Microsoft Entra Permissions Management.** [Microsoft Entra Permissions Management](#) is a cloud infrastructure entitlement management (CIEM) solution that provides comprehensive visibility into permissions assigned to all identities (users and workloads), actions, and resources across cloud infrastructures Microsoft Azure, Amazon Web Services (AWS), and Google Cloud Platform (GCP).
- **"Pay as you go" feature licenses.** You can also get licenses for features such as Microsoft Entra Domain Services, and Microsoft Entra Business-to-Customer (B2C). B2C can help you provide identity and access management solutions for your customer-facing apps. For more information, see [Azure Active Directory B2C documentation](#).

For more information on the Microsoft Entra product family, see [Microsoft Entra](#).

For more information about associating an Azure subscription to Microsoft Entra ID, see [Associate or add an Azure subscription to Microsoft Entra ID](#). For more information about assigning licenses to your users, see [How to: Assign or remove Microsoft Entra ID licenses](#).

Which features work in Microsoft Entra ID?

After you choose your Microsoft Entra ID license, you'll get access to some or all of the following features:

[] [Expand table](#)

Category	Description
Application management	Manage your cloud and on-premises apps using Application Proxy, single sign-on, the My Apps portal, and Software as a Service (SaaS) apps. For more information, see How to provide secure remote access to on-premises applications and Application Management documentation .
Authentication	Manage Microsoft Entra self-service password reset, Multifactor Authentication, custom banned password list, and smart lockout. For more information, see Microsoft Entra authentication documentation .
Microsoft Entra ID for developers	Build apps that sign in all Microsoft identities, get tokens to call Microsoft Graph, other Microsoft APIs, or custom APIs. For more information, see Microsoft identity platform (Microsoft Entra ID for developers) .

Category	Description
Business-to-Business (B2B)	Manage your guest users and external partners, while maintaining control over your own corporate data. For more information, see Microsoft Entra B2B documentation .
Business-to-Customer (B2C)	Customize and control how users sign up, sign in, and manage their profiles when using your apps. For more information, see Azure Active Directory B2C documentation .
Conditional Access	Manage access to your cloud apps. For more information, see Microsoft Entra Conditional Access documentation .
Device Management	Manage how your cloud or on-premises devices access your corporate data. For more information, see Microsoft Entra Device Management documentation .
Domain services	Join Azure virtual machines to a domain without using domain controllers. For more information, see Microsoft Entra Domain Services documentation .
Enterprise users	Manage license assignments, access to apps, and set up delegates using groups and administrator roles. For more information, see Microsoft Entra user management documentation .
Hybrid identity	Use Microsoft Entra Connect and Connect Health to provide a single user identity for authentication and authorization to all resources, regardless of location (cloud or on-premises). For more information, see Hybrid identity documentation .
Identity governance	Microsoft Entra ID P2 includes basic capabilities for privileged identity management (PIM), access reviews and entitlement management. Microsoft Entra ID Governance customers can manage their organization's identities and access through comprehensive employee, business partner, vendor, service, and app controls. For more information, see Microsoft Entra ID Governance documentation and features by license .
Microsoft Entra ID Protection	Detect potential vulnerabilities affecting your organization's identities, configure policies to respond to suspicious actions, and then take appropriate action to resolve them. For more information, see Microsoft Entra ID Protection .
Managed identities for Azure resources	Provide your Azure services with an automatically managed identity in Microsoft Entra ID that can authenticate any Microsoft Entra-supported authentication service, including Key Vault. For more information, see What is managed identities for Azure resources? .
Privileged identity management (PIM)	Manage, control, and monitor access within your organization. This feature includes access to resources in Microsoft Entra ID and Azure, and other Microsoft Online Services, like Microsoft 365 or Intune. For more information, see Microsoft Entra Privileged Identity Management .

Category	Description
Monitoring and health	Gain insights into the security and usage patterns in your environment. For more information, see Microsoft Entra monitoring and health .
Workload identities	Give an identity to your software workload (such as an application, service, script, or container) to authenticate and access other services and resources. For more information, see workload identities faqs .

Terminology

To better understand Microsoft Entra ID and its documentation, we recommend reviewing the following terms.

 [Expand table](#)

Term or concept	Description
Identity	A thing that can get authenticated. An identity can be a user with a username and password. Identities also include applications or other servers that might require authentication through secret keys or certificates.
Account	An identity that has data associated with it. You can't have an account without an identity.
Microsoft Entra account	An identity created through Microsoft Entra ID or another Microsoft cloud service, such as Microsoft 365. Identities are stored in Microsoft Entra ID and accessible to your organization's cloud service subscriptions. This account is also sometimes called a Work or school account.
Account Administrator	This classic subscription administrator role is conceptually the billing owner of a subscription. This role enables you to manage all subscriptions in an account. For more information, see Azure roles, Microsoft Entra roles, and classic subscription administrator roles .
Service Administrator	This classic subscription administrator role enables you to manage all Azure resources, including access. This role has the equivalent access of a user who is assigned the Owner role at the subscription scope. For more information, see Azure roles, Microsoft Entra roles, and classic subscription administrator roles .
Owner	This role helps you manage all Azure resources, including access. This role is built on a newer authorization system called Azure role-based access control (Azure RBAC) that provides fine-grained access management to Azure resources. For more information, see Azure roles, Microsoft Entra roles, and classic subscription administrator roles .

Term or concept	Description
Microsoft Entra Global Administrator	By default, the user who creates a Microsoft Entra tenant is automatically assigned the Global Administrator role. You can have multiple accounts with this role, but anyone with at least Privileged Role Administrator can assign administrator roles to users. For more information about the various administrator roles, see Administrator role permissions in Microsoft Entra ID .
Azure subscription	Used to pay for Azure cloud services. You can have many subscriptions and they're linked to a credit card.
Tenant	A dedicated and trusted instance of Microsoft Entra ID. The tenant is automatically created when your organization signs up for a Microsoft cloud service subscription. These subscriptions include Microsoft Azure, Microsoft Intune, or Microsoft 365. This tenant represents a single organization and is intended for managing your employees, business apps, and other internal resources. For this reason, it's considered a workforce tenant configuration. By contrast, you can create a tenant in an <i>external</i> configuration, which is used in customer identity and access management (CIAM) solutions for your consumer-facing apps (learn more about Microsoft Entra External ID).
Single tenant	Azure tenants that access other services in a dedicated environment are considered single tenant.
Multitenant	Azure tenants that access other services in a shared environment, across multiple organizations, are considered multitenant.
Microsoft Entra directory	Each Azure tenant has a dedicated and trusted Microsoft Entra directory. The Microsoft Entra directory includes the tenant's users, groups, and apps and is used to perform identity and access management functions for tenant resources.
Custom domain	Every new Microsoft Entra directory comes with an initial domain name, for example <code>domainname.onmicrosoft.com</code> . In addition to that initial name, you can also add your organization's domain names. Your organization's domain names include the names you use to do business and your users use to access your organization's resources, to the list. Adding custom domain names helps you to create user names that are familiar to your users, such as <code>alain@contoso.com</code> .
Microsoft account (also called, MSA)	Personal accounts that provide access to your consumer-oriented Microsoft products and cloud services. These products and services include Outlook, OneDrive, Xbox LIVE, or Microsoft 365. Your Microsoft account is created and stored in the Microsoft consumer identity account system that's run by Microsoft.

Next steps

- [Sign up for Microsoft Entra ID P1 or P2](#)

- Associate an Azure subscription to your Microsoft Entra ID
 - Microsoft Entra ID P2 feature deployment checklist
-

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback 

What is the Microsoft Entra admin center?

Article • 04/27/2025

The [Microsoft Entra admin center](#) is a web-based identity portal for Microsoft Entra products. It provides a unified administrative experience for organizations to configure and manage their Microsoft Entra solutions in a centralized location.

Explore the Microsoft Entra admin center

The Microsoft Entra admin center is organized by product. The products can be accessed through the search bar or left-hand menu.

Home includes at-a-glance information about your tenant, recent activities, and other helpful resources, including shortcuts and deployment guides.

The screenshot shows the Microsoft Entra admin center interface. The left sidebar contains a 'Favorites' section and links to various products: Home, Agents, Entra ID, ID Protection, ID Governance, Verified ID, Permissions Management, Global Secure Access, What's new, Billing, Diagnose & solve problems, and New support request. The main content area displays tenant information for 'MicrosoftLearnSecurityDocs', including Tenant ID, Primary domain, and counts for users, groups, devices, and apps. It also shows a user profile for 'Preben Bjerklund' and a section for 'Users at high risk' with a note about unauthorized access. The bottom right features sections for 'Microsoft Entra plan' (Entra Suite) and 'Standalone products' (Entra Workload ID). A red box highlights the top navigation bar, and another red box highlights the left sidebar.

The following sections provide a high-level overview of the product interfaces and links to learn more about the features.

Entra ID

Entra ID gives administrators and developers access to [Microsoft Entra ID](#) and [Microsoft Entra External ID](#) solutions, including tenants, users, groups, devices, applications, roles, and licensing.

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a sidebar with a 'Favorites' section containing items like Home, Agents, and Entra ID (which is highlighted with a red box). Below that is a list of other management options: Overview, Users, Groups, Devices, Enterprise apps, App registrations, and Roles & admins. The main content area is titled 'Microsoft' and has tabs for Overview, Monitoring, Properties, Recommendations, and Tutorials. It includes a search bar and a 'Basic information' section with tenant statistics:

Name	Users	63
Tenant ID	Groups	24
Primary domain	Applications	61
License	Devices	11

For more information about configuring and managing Microsoft Entra ID solutions, see the following documentation:

- [Users and groups](#)
- [Devices](#)
- [Enterprise applications](#)
- [App registrations](#)
- [Roles and admins](#)
- [External identities](#)
- [Conditional access](#)
- [Multifactor authentication](#)
- [Identity secure score](#)
- [Authentication methods](#)
- [Password reset](#)
- [Custom security attributes](#)

ID Protection

ID Protection gives administrators and developers access to [Microsoft Entra ID Protection](#) solutions, including the protection dashboard, risk-based access policies, risky users report, multifactor authentication, and password reset.

The screenshot shows the Microsoft Entra admin center interface. The left sidebar has a red box around the 'ID Protection' section. The main dashboard includes a large graphic of a padlock and clouds, and two data cards: one for blocked attacks and one for protected users.

For more information about configuring and managing Microsoft Entra ID Protection solutions, see the following documentation:

- [Identity Protection dashboard](#)
- [Risk-based access policies](#)
- [Risky users](#)
- [Risky workload identities](#)

Identity governance

Identity Governance gives administrators and developers access to [Microsoft Entra ID Governance](#) solutions, including entitlement management, access reviews, and lifecycle workflows.

Microsoft Entra admin center

Home > Identity Protection | Dashboard > Microsoft ...

Welcome to Identity Governance

Manage identity and access rights across multiple applications and services to meet security and regulatory compliance requirements. With Microsoft Entra ID Governance, balance security and productivity by ensuring that the right people have the right access to the right resources for the right amount of time.

Learn more ↗

ID Governance

Member user lifecycle governance

13,385 member user accounts recently...

Improve operational efficiency, increase new hire productivity and reduce security risks by automating your employee onboarding and offboarding tasks.

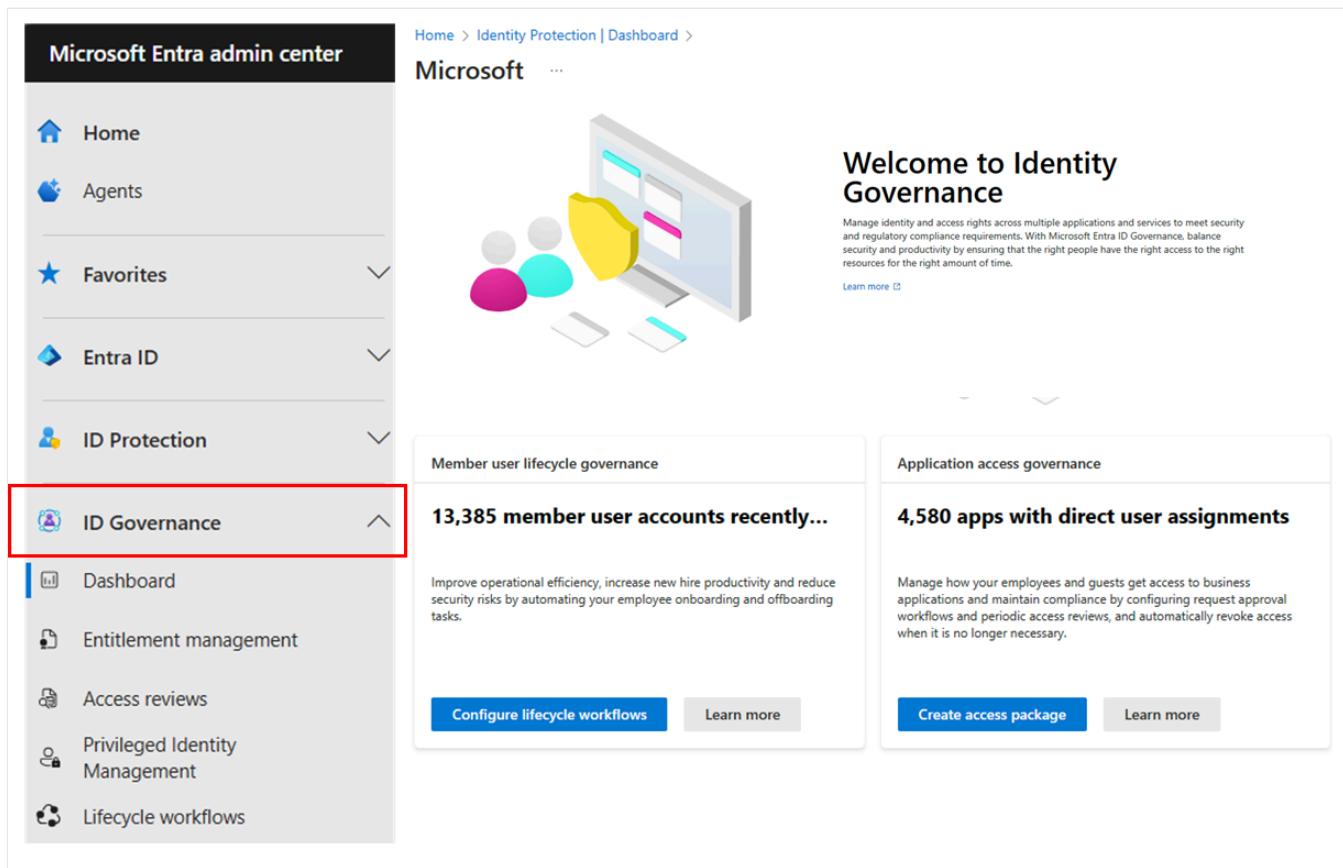
Configure lifecycle workflows **Learn more**

Application access governance

4,580 apps with direct user assignments

Manage how your employees and guests get access to business applications and maintain compliance by configuring request approval workflows and periodic access reviews, and automatically revoke access when it is no longer necessary.

Create access package **Learn more**



For more information about configuring and managing Microsoft Entra ID Governance solutions, see the following documentation:

- [Identity Governance dashboard](#)
- [Entitlement management](#)
- [Access reviews](#)
- [Privileged Identity Management](#)
- [Lifecycle workflows](#)

Verified ID

Verified ID gives administrators and developers access to [Microsoft Entra Verified ID](#) solutions, including credentials and organization settings.

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with links like Home, Agents, Favorites, Entra ID, ID Protection, ID Governance, and Verified ID. The 'Verified ID' link is highlighted with a red box. The main content area has a header 'Overview' and tabs for 'Setup' and 'Overview'. It features a central illustration of a computer monitor, a smartphone, and a tablet connected by lines, representing remote access. A section titled 'Welcome to Entra Verified ID' explains that it enables fast remote onboarding, secure access, and account recovery. Below this, a heading 'Unlock the power of Verified ID' is followed by three cards: 'Simplified workplace verification with LinkedIn', 'Faster application access approval', and 'Credentials tailored to your needs'. Each card includes a 'Learn more' button.

For more information about configuring and managing Microsoft Entra Verified ID solutions, see the following documentation:

- [Credentials](#)

Permissions Management

Permissions Management gives administrators and developers access to [Microsoft Entra Permissions Management](#) solutions, including user identities, actions, and resources across multicloud infrastructure environments.

Microsoft Entra admin center

Home > Microsoft ...

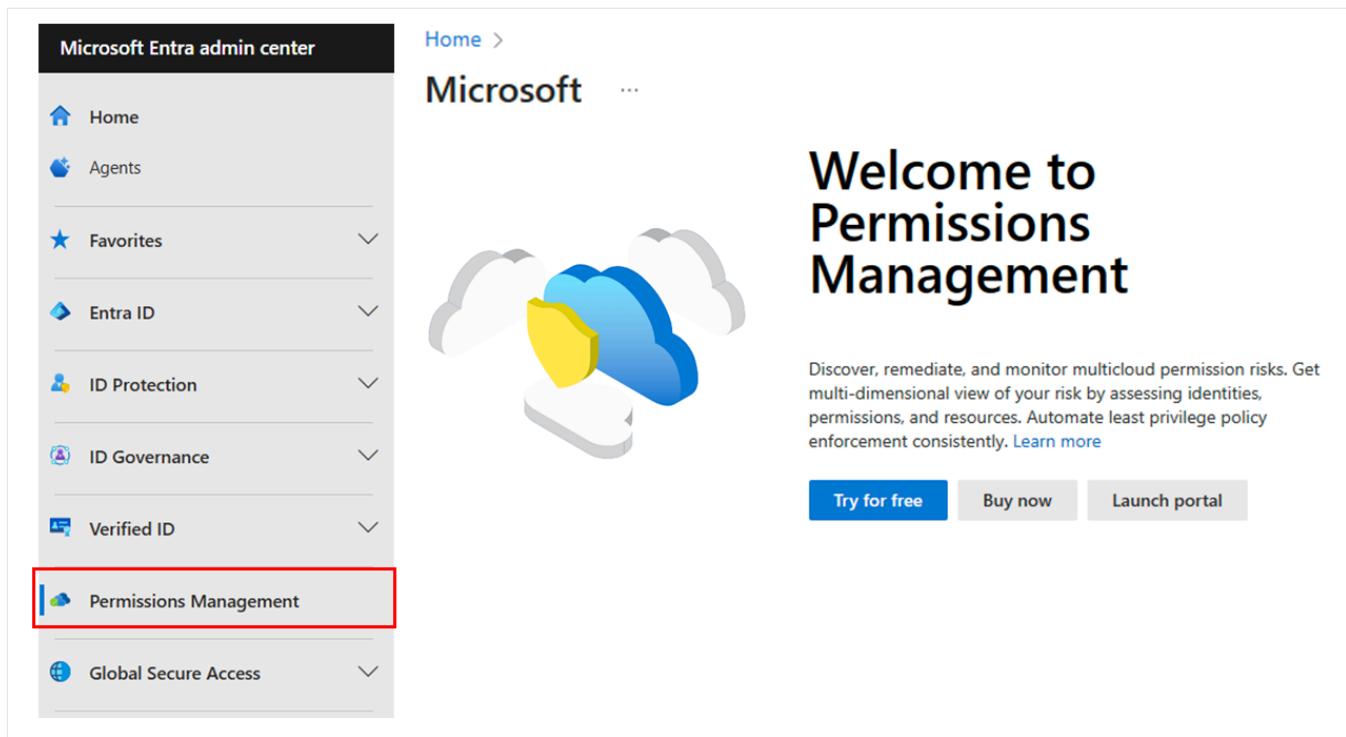
Home Agents Favorites

Entra ID ID Protection ID Governance Verified ID Permissions Management Global Secure Access

Welcome to Permissions Management

Discover, remediate, and monitor multicloud permission risks. Get multi-dimensional view of your risk by assessing identities, permissions, and resources. Automate least privilege policy enforcement consistently. [Learn more](#)

Try for free Buy now Launch portal



For more information about configuring and managing Microsoft Entra Permissions Management solutions, see the [Quickstart guide to Microsoft Entra Permissions Management](#).

Global Secure Access

Global Secure Access gives administrators and developers access to [Microsoft Entra Private Access](#) and [Microsoft Entra Internet Access](#) solutions, including the Global Secure Access dashboard, clients, connectors, and monitoring.

Microsoft Entra admin center

Home > Microsoft ...

Welcome to Global Secure Access

Secure access and improve visibility to the internet, Microsoft 365, SaaS, and private apps. [Learn more about Global Secure Access](#)

Entra ID

ID Protection

ID Governance

Verified ID

Permissions Management

Global Secure Access

Dashboard

Applications

Connect

Secure

Monitor

Settings

Get Started with the dashboard ...

The screenshot shows the Microsoft Entra admin center interface. The left sidebar has a red box around the 'Global Secure Access' section. The main area displays the 'Welcome to Global Secure Access' page with a diagram of a laptop, smartphone, and cloud connected by lines, with a shield icon.

For more information about configuring and managing Global Secure Access solutions, see the following documentation:

- [Global Secure Access dashboard](#)
- [Global Secure Access client](#)
- [Traffic forwarding](#)
- [Remote networks](#)
- [Logs and monitoring](#)

Need help?

Diagnose & solve problems provides troubleshooting resources to fix common problems, and the option to contact our support team by opening a **New support request**.

Microsoft Entra admin center

Home > **Diagnose and solve problems** ... X

Start Over New Support Request Got feedback?

How can we help you?

Briefly describe the issue

Your search query data will be processed by Bing and according to the Product Terms applicable to Microsoft Search in Bing. [Link to Bing Product Terms](#)

Troubleshooters

Select Troubleshoot for the problem you are attempting to resolve.

Diagnose SSO problems

Find out how to fix device and application related Single Sign-on problems

Troubleshoot

Diagnose & solve problems (highlighted with a red box)

New support request

Microsoft Entra admin center

Home > **New support request** ...

1. Problem description 2. Recommended solution 3. Additional details 4. Review + create

Tell us your issue, and we'll help you resolve it.

Provide information about your billing, subscription, quota management, or technical issue (including requests for technical advice).

Issue type *

Subscription *

Can't find your subscription? [Show more](#) ⓘ

Diagnose & solve problems (highlighted with a red box)

New support request

Related content

- [Find your tenant](#)
- [Create a new tenant](#)

Trial user guide: Microsoft Entra Suite

Article • 04/02/2025

Welcome to the Microsoft Entra Suite trial user guide. Make the most of your free trial by discovering the robust and comprehensive capabilities of [Microsoft Entra](#).

💡 Tip

Save this trial user guide to your browser favorites. When links in the trial user guide take you away from this location, it'll be easier to return to this guide to continue.

What is the Microsoft Entra Suite?

[Microsoft Entra Suite](#) is the solution to deliver unified Zero Trust user access, enabling your employees to securely access cloud and on-premises applications. The suite allows you to provide least privilege access across public and private networks, inside and outside of your corporate perimeter. By combining network access, ID Protection, governance, and identity verification solutions, the Microsoft Entra Suite extends Conditional Access across identities and network controls, filtering out malicious content, and ensuring least privilege access for a simple and consistent user experience, whether employees are in the office or remote.

Trial licensing prerequisites

- Microsoft Entra ID P1
- Any package that includes Microsoft Entra ID P1 or Microsoft Entra ID P2 (for example, ME3 or ME5)

When you start a trial or purchase Microsoft Entra Suite, your first step is to determine which licensing option is best suited for your organization. Special pricing is available for Microsoft Entra ID P2/E5 customers. For more information about pricing, see [Microsoft Entra plans & pricing](#).

What is included in the Microsoft Entra Suite trial?

The Microsoft Entra Suite includes these products:

Microsoft Entra Private Access: Removes the risk and operational complexity of legacy VPNs while boosting user productivity. Quickly and securely connects remote users from any device and any global network to private apps—on-premises, across clouds, and anywhere in between.

Microsoft Entra Internet Access: Secures global access to all internet, SaaS, and Microsoft 365 apps and resources while protecting organizations against internet threats, malicious network traffic, and unsafe or noncompliant content with an identity-centric Secure Web Gateway (SWG).

Microsoft Entra ID Governance: Manages user identities, access rights, and entitlements across IT environments to ensure proper access controls, mitigate risk, and maintain compliance with regulatory requirements.

Microsoft Entra ID Protection: Blocks identity takeover in real time by analyzing user and sign-in patterns based on integrated risk scores from various sources. Protects against identity-based attacks, such as phishing, infected devices, and leaked credentials.

Microsoft Entra Verified ID: Validate users with secure verification methods to ensure secure identity authentication scenarios like user onboarding, and secure access to sensitive resources and account recovery processes.

Microsoft Entra Suite product guides

To help you get the most out of your Microsoft Entra Suite trial, we recommend you review the following how-to guides to help ensure a more secure environment for your organization.

The following how-to guides are expanded upon in this section:

- [Step 1: Deploy ID Protection:](#) Deploy security controls to enhance identification and protection of risky users.
- [Step 2: Enact access reviews:](#) Conduct an access review to ensure appropriate system access within your enterprise.
- [Step 3: Secure access to the internet:](#) Protect internet traffic with secure web gateways.
- [Step 4: Enable private access gateways:](#) Depreciate costly VPN systems with Quick Access.
- [Step 5: Onboard customers with a workflow portal:](#) Automate employee onboarding with lifecycle workflows.

Your first 90 days

Accelerating your Zero Trust strategy with the Microsoft Entra Suite



The following sections include process steps to walk you through each product. Each of these steps is fully documented in a separate how-to guide that you can access by clicking the link at the end of each step.

Step 1: Deploy Microsoft Entra ID Protection

Microsoft Entra ID Protection detects identity-based risks and reports them, allowing administrators to investigate and remediate these risks to keep organizations safe and secure. Risk data can be further fed into tools like Conditional Access to make access decisions or fed to a security information and event management (SIEM) tool for further analysis and investigation.

1. Review existing reports
2. Plan for Conditional Access risk policies
3. Configure your policies
4. Monitoring and continuous operational needs

To view the complete how-to guide, see [Plan a Microsoft Entra ID Protection deployment](#).

Step 2: Enact access reviews

Microsoft Entra access reviews are a Microsoft Entra ID Governance capability that helps your organization keep the enterprise more secure by managing its resource access lifecycle. The other capabilities are entitlement management, Privileged Identity Management (PIM), lifecycle workflows, provisioning, and terms of use.

1. Plan access reviews for access packages, groups, and applications
2. Plan review of Microsoft Entra ID and Azure resource roles
3. Deploy access reviews
4. Use the Access Reviews API
5. Monitor access reviews

To view the complete how-to guide, see [Plan a Microsoft Entra access reviews deployment](#).

Step 3: Secure access to the internet

Microsoft Entra Internet Access protects enterprise users and managed devices from malicious internet traffic and malware infection concerns all companies. Using the Secure Web Gateway functionality enables you to block traffic based on web categories, and a fully qualified domain name (FQDN) by integrating with Microsoft Entra Conditional Access.

1. Deploy and test Microsoft Entra Internet Access
2. Create a baseline policy applying to all internet traffic routed through the service
3. Block a group from accessing websites based on category
4. Block a group from accessing websites based on FQDN
5. Allow a user to access a blocked website

To view the complete how-to guide, see [Deployment guide for Microsoft Entra Internet Access](#).

Step 4: Enable private access gateways

Microsoft Entra Private Access converges network and identity access controls so you can secure access to any app or resource from any location, device, or identity. It enables and orchestrates access policy management for employees, business partners, and digital workloads.

1. Deploy and test Microsoft Entra Private Access
2. Apply Microsoft Entra Conditional Access
3. Control access by multiple users to multiple apps

To view the complete how-to guide, see [Deployment guide for Microsoft Entra Private Access](#).

Step 5: Onboard customers with a workflow portal

The Microsoft Entra admin portal enables you to automate prehire tasks with Lifecycle workflows through an HR provisioning process. Provisioning creates an identity in a target system based on certain conditions. Deprovisioning removes the identity from the target system, when conditions are no longer met. These processes are part of identity lifecycle management.

1. Create a workflow using prehire template
2. Run the workflow
3. Check tasks and workflow status
4. Enable the workflow schedule

To view the complete how-to guide, see [Automate employee onboarding tasks with Microsoft Entra](#).

Customer scenarios for using the Microsoft Entra Suite trial

The following deployment scenarios provide detailed guidance on how to combine and test all five Microsoft Entra Suite products. Each scenario in this section includes separate step-by-step instructions that you can access by clicking the link at the end of each scenario.

To get the most out of your trial, get started by walking through the following user scenarios.

- [Scenario 1: Automate user onboarding and lifecycle with access to all apps](#)
- [Scenario 2: Modernize remote access to on-premises apps with MFA per app](#)
- [Scenario 3: Secure internet access based on business needs](#)

Take advantage of the better together security strategy during your Microsoft Entra Suite's trial period. Implement automated user onboarding and lifecycle management, modernize from traditional VPN to on-premises resources with multifactor authentication (MFA) down to the app level, and secure internet access based on your business rules.

The following table shows which of the five Microsoft Entra Suite products are covered in each scenario.

[] [Expand table](#)

Customer scenario	Microsoft Entra Private Access	Microsoft Entra Internet Access	Microsoft Entra ID Governance	Microsoft Entra ID Protection	Microsoft Entra Verified ID
1 – Automate user onboarding and lifecycle with access to all apps		Included	Included	Included	Included
2 – Modernize traditional VPN to on-premises resources with MFA per app		Included	Included	Included	
3 – Secure internet access based on business rules	Included		Included	Included	

Scenario 1: Automate user onboarding and lifecycle with access to all apps

The workforce and guest onboarding, identity, and access lifecycle governance scenario describes these goals:

- Provide remote employees with secure and seamless access to necessary apps and resources.
- Collaborate with external users by providing them with access to relevant apps and resources.

The step-by-step guidance focuses on Microsoft Entra Verified ID, Microsoft Entra ID Governance, Microsoft Entra ID Protection, and Microsoft Entra Conditional Access. For more information, see [Microsoft Entra deployment scenario - Workforce and guest lifecycle](#).

Scenario 2: Modernize remote access to on-premises apps with MFA per app

The modernized remote access to on-premises apps with MFA per app scenarios describe these goals:

- Upgrade existing VPN to a scalable cloud-based solution that helps to move towards Secure Access Service Microsoft Edge (SASE).

- Resolve issues where business application access relies on corporate network connectivity.

The step-by-step guidance focuses on Microsoft Entra Private Access, Microsoft Entra ID Protection, and Microsoft Entra ID Governance. For more information, see [Microsoft Entra deployment scenario - Modernize remote access](#).

Scenario 3: Secure internet access based on business needs

The secure internet access based on business needs scenario describes these goals:

- Augment existing strict default internet access policies with Microsoft Entra Internet Access control.
- Allow users to request access to prohibited sites in My Access. The approval process adds users to a group that grants them access. Examples include marketing department access to social networking sites and security department access to high-risk internet destinations while investigating incidents.

The step-by-step guidance focuses on Microsoft Entra Internet Access, Microsoft Entra ID Governance, Microsoft Entra Conditional Access, and Global Secure Access. For more information, see [Microsoft Entra deployment scenario - Secure internet access](#).

Related content

- [Microsoft Entra Suite now generally available - Microsoft Community Hub](#) ↗
- [Microsoft Entra plans & pricing](#) ↗
- [Learn how to simplify your Zero Trust strategy with the Microsoft Entra Suite](#) ↗
- [Simplified Zero Trust security with the Microsoft Entra Suite](#) ↗

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#) ↗

Identity and access management (IAM) fundamental concepts

Article • 03/13/2025

This article provides fundamental concepts and terminology to help you understand identity and access management (IAM).

What is identity and access management (IAM)?

Identity and access management ensures that the right people, machines, and software components get access to the right resources at the right time. First, the person, machine, or software component proves they're who or what they claim to be. Then, the person, machine, or software component is allowed or denied access to or use of certain resources.

Here are some fundamental concepts to help you understand identity and access management:

Identity

A digital identity is a collection of unique identifiers or attributes that represent a human, software component, machine, asset, or resource in a computer system. An identifier can be:

- An email address
- Sign-in credentials (username/password)
- Bank account number
- Government issued ID
- MAC address or IP address

Identities are used to authenticate and authorize access to resources, communicate with other humans, conduct transactions, and other purposes.

At a high level, there are three types of identities:

- **Human identities** represent people such as employees (internal workers and frontline workers) and external users (customers, consultants, vendors, and partners).

- **Workload identities** represent software workloads such as an application, service, script, or container.
- **Device identities** represent devices such as desktop computers, mobile phones, IoT sensors, and IoT managed devices. Device identities are distinct from human identities.

Authentication

Authentication is the process of challenging a person, software component, or hardware device for credentials in order to verify their identity, or prove they're who or what they claim to be. Authentication typically requires the use of credentials (like username and password, fingerprints, certificates, or one-time passcodes). Authentication is sometimes shortened to *AuthN*.

Multifactor authentication (MFA) is a security measure that requires users to provide more than one piece of evidence to verify their identities, such as:

- Something they know, for example a password.
- Something they have, like a badge or **security token**.
- Something they are, like a biometric (fingerprint or face).

Single sign-on (SSO) allows users to authenticate their identity once and then later silently authenticate when accessing various resources that rely on the same identity. Once authenticated, the IAM system acts as the source of identity truth for the other resources available to the user. It removes the need for signing on to multiple, separate target systems.

Authorization

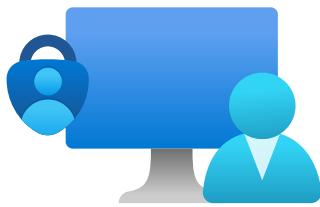
Authorization validates that the user, machine, or software component has been granted access to certain resources. Authorization is sometimes shortened to *AuthZ*.

Authentication vs. authorization

The terms authentication and authorization are sometimes used interchangeably, because they often seem like a single experience to users. They're actually two separate processes:

- Authentication proves the identity of a user, machine, or software component.
- Authorization grants or denies the user, machine, or software component access to certain resources.

Authentication



Confirms users are who they say they are

Authorization



Validates users have permission to complete the attempted action

Here's a quick overview of authentication and authorization:

[+] [Expand table](#)

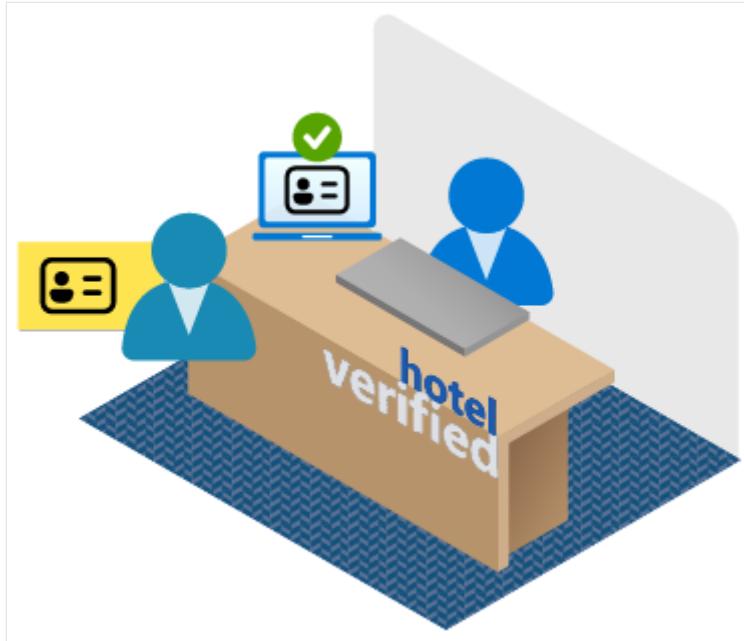
Authentication	Authorization
Can be thought of as a gatekeeper, allowing access only to those entities who provide valid credentials.	Can be thought of as a guard, ensuring that only those entities with the proper clearance can enter certain areas.
Verifies whether a user, machine, or software is who or what they claim to be.	Determines if the user, machine, or software is allowed to access a particular resource.
Challenges the user, machine, or software for verifiable credentials (for example, passwords, biometric identifiers, or certificates).	Determines what level of access a user, machine, or software has.
Done before authorization.	Done after successful authentication.
Information is transferred in an ID token.	Information is transferred in an access token.
Often uses the OpenID Connect (OIDC) (which is built on the OAuth 2.0 protocol) or SAML protocols.	Often uses the OAuth 2.0 protocol.

For more detailed information, read [Authentication vs. authorization](#).

Example

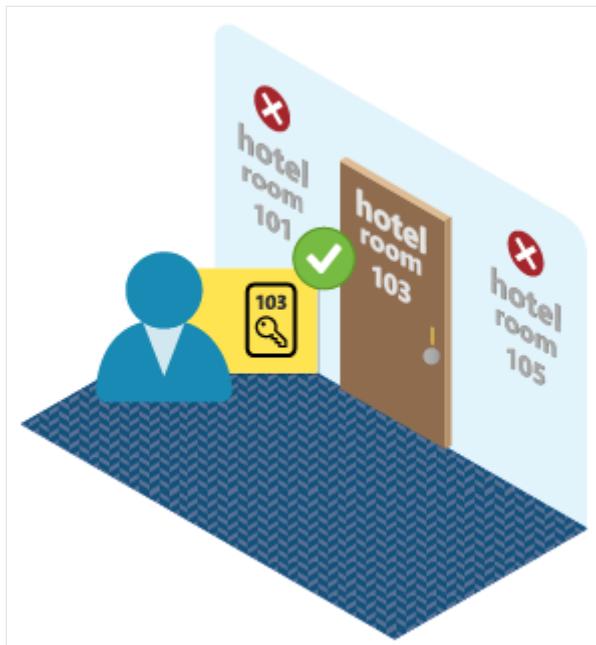
Suppose you want to spend the night in a hotel. You can think of authentication and authorization as the security system for the hotel building. Users are people who want to stay at the hotel, resources are the rooms or areas that people want to use. Hotel staff is another type of user.

If you're staying at the hotel, you first go to reception to start the "authentication process". You show an identification card and credit card and the receptionist matches your ID against the online reservation. After the receptionist has verified who you are, the receptionist grants you permission to access the room you've been assigned. You're given a keycard and can go now to your room.



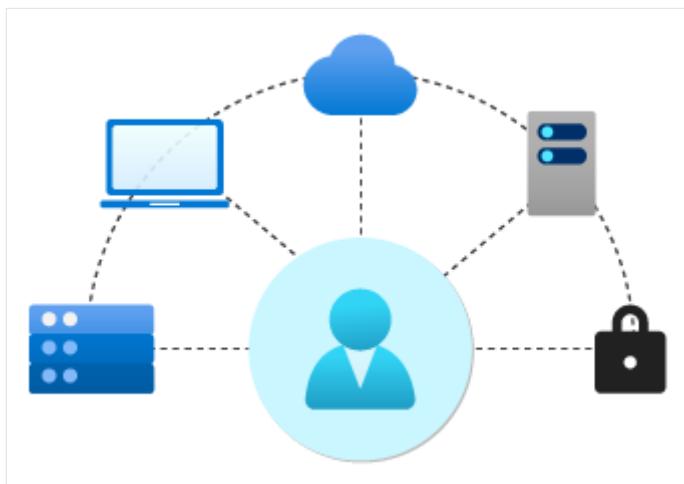
The doors to the hotel rooms and other areas have keycard sensors. Swiping the keycard in front of a sensor is the "authorization process". The keycard only lets you open the doors to rooms you're permitted to access, such as your hotel room and the hotel exercise room. If you swipe your keycard to enter any other hotel guest room, your access is denied.

Individual [permissions](#), such as accessing the exercise room and a specific guest room, are collected into [roles](#) which can be granted to individual users. When you're staying at the hotel, you're granted the Hotel Patron role. Hotel room service staff would be granted the Hotel Room Service role. This role permits access to all hotel guest rooms (but only between 11am and 4pm), the laundry room, and the supply closets on each floor.



Identity provider

An identity provider creates, maintains, and manages identity information while offering authentication, authorization, and auditing services.



With modern authentication, all services, including all authentication services, are supplied by a central identity provider. Information that's used to authenticate the user with the server is stored and managed centrally by the identity provider.

With a central identity provider, organizations can establish authentication and authorization policies, monitor user behavior, identify suspicious activities, and reduce malicious attacks.

[Microsoft Entra](#) is an example of a cloud-based identity provider. Other examples include X, Google, Amazon, LinkedIn, and GitHub.

Next steps

- Read [Introduction to identity and access management](#) to learn more.
 - Learn about [Single sign-on \(SSO\)](#).
 - Learn about [multifactor authentication \(MFA\)](#).
-

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

What is identity and access management (IAM)?

Article • 03/13/2025

In this article, you learn some of the fundamental concepts of Identity and Access Management (IAM), why it's important, and how it works.

Identity and access management ensures that the right people, machines, and software components get access to the right resources at the right time. First, the person, machine, or software component proves they're who or what they claim to be. Then, the person, machine, or software component is allowed or denied access to or use of certain resources.

To learn about the basic terms and concepts, see [Identity fundamentals](#).

What does IAM do?

IAM systems typically provide the following core functionality:

- **Identity management** - The process of creating, storing, and managing identity information. Identity providers (IdP) are software solutions that are used to track and manage user identities, as well as the permissions and access levels associated with those identities.
- **Identity federation** - You can allow users who already have passwords elsewhere (for example, in your enterprise network or with an internet or social identity provider) to get access to your system.
- **Provisioning and deprovisioning of users** - The process of creating and managing user accounts, which includes specifying which users have access to which resources, and assigning permissions and access levels.
- **Authentication of users** - Authenticate a user, machine, or software component by confirming that they're who or what they say they are. You can add multifactor authentication (MFA) for individual users for extra security or single sign-on (SSO) to allow users to authenticate their identity with one portal instead of many different resources.
- **Authorization of users** - Authorization ensures a user is granted the exact level and type of access to a tool that they're entitled to. Users can also be portioned into groups or roles so large cohorts of users can be granted the same privileges.

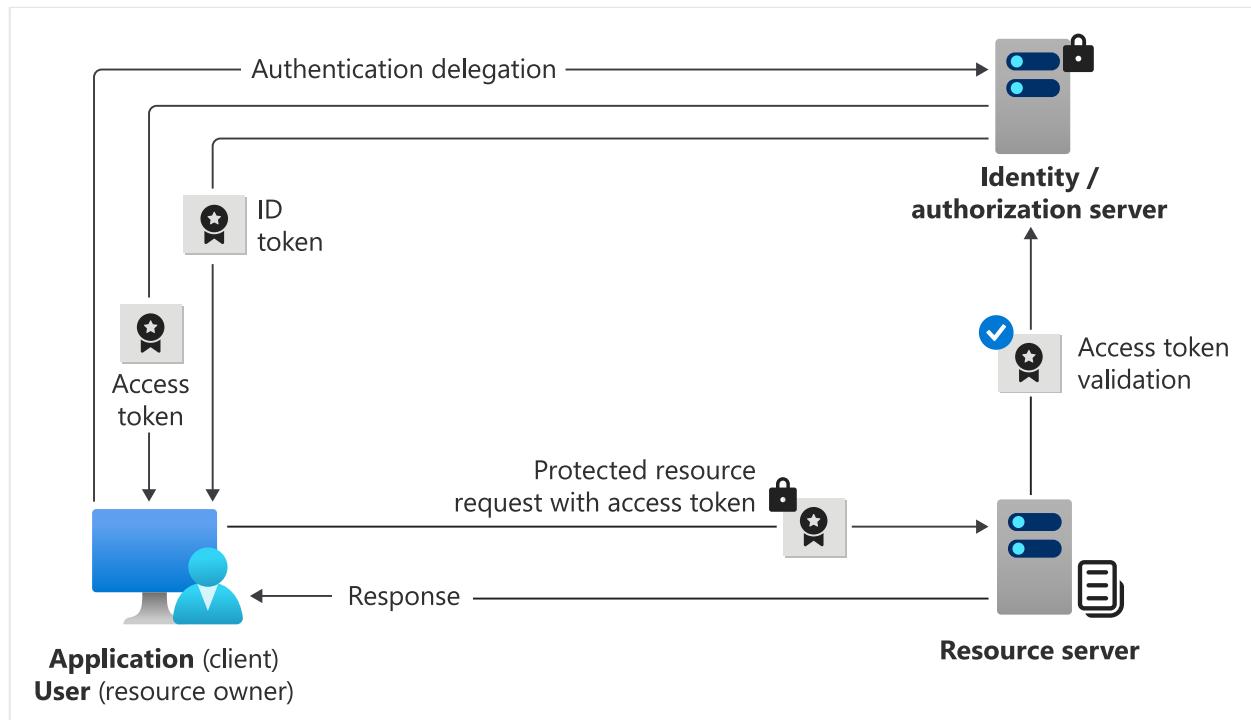
- **Access control** - The process of determining who or what has access to which resources. This includes defining user roles and permissions, as well as setting up authentication and authorization mechanisms. Access controls regulate access to systems and data.
- **Reports and monitoring** - Generate reports after actions taken on the platform (like sign-in time, systems accessed, and type of authentication) to ensure compliance and assess security risks. Gain insights into the security and usage patterns of your environment.

How IAM works

This section provides an overview of the authentication and authorization process and the more common standards.

Authenticating, authorizing, and accessing resources

Let's say you have an application that signs in a user and then accesses a protected resource.



1. The user (resource owner) initiates an authentication request with the identity provider/authorization server from the client application.
2. If the credentials are valid, the identity provider/authorization server first sends an ID token containing information about the user back to the client application.

3. The identity provider/authorization server also obtains end-user consent and grants the client application authorization to access the protected resource. Authorization is provided in an access token, which is also sent back to the client application.
4. The access token is attached to subsequent requests made to the protected resource server from the client application.
5. The identity provider/authorization server validates the access token. If successful the request for protected resources is granted, and a response is sent back to the client application.

For more information, read [Authentication and authorization](#).

Authentication and authorization standards

These are the most well-known and commonly used authentication and authorization standards:

OAuth 2.0

OAuth is an open-standards identity management protocol that provides secure access for websites, mobile apps, and Internet of Things and other devices. It uses tokens that are encrypted in transit and eliminates the need to share credentials. OAuth 2.0, the latest release of OAuth, is a popular framework used by major social media platforms and consumer services, from Facebook and LinkedIn to Google, PayPal, and Netflix. To learn more, read about [OAuth 2.0 protocol](#).

OpenID Connect (OIDC)

With the release of the OpenID Connect (which uses public-key encryption), OpenID became a widely adopted authentication layer for OAuth. Like SAML, OpenID Connect (OIDC) is widely used for single sign-on (SSO), but OIDC uses REST/JSON instead of XML. OIDC was designed to work with both native and mobile apps by using REST/JSON protocols. The primary use case for SAML, however, is web-based apps. To learn more, read about [OpenID Connect protocol](#).

JSON web tokens (JWTs)

JWTs are an open standard that defines a compact and self-contained way for securely transmitting information between parties as a JSON object. JWTs can be verified and

trusted because they're digitally signed. They can be used to pass the identity of authenticated users between the identity provider and the service requesting the authentication. They also can be authenticated and encrypted. To learn more, read [JSON Web Tokens](#).

Security Assertion Markup Language (SAML)

SAML is an open standard utilized for exchanging authentication and authorization information between, in this case, an IAM solution and another application. This method uses XML to transmit data and is typically the method used by identity and access management platforms to grant users the ability to sign in to applications that have been integrated with IAM solutions. To learn more, read [SAML protocol](#).

System for Cross-Domain Identity Management (SCIM)

Created to simplify the process of managing user identities, SCIM provisioning allows organizations to efficiently operate in the cloud and easily add or remove users, benefitting budgets, reducing risk, and streamlining workflows. SCIM also facilitates communication between cloud-based applications. To learn more, read [Develop and plan provisioning for a SCIM endpoint](#).

Web Services Federation (WS-Fed)

WS-Fed was developed by Microsoft and used extensively in their applications, this standard defines the way security tokens can be transported between different entities to exchange identity and authorization information. To learn more, read [Web Services Federation Protocol](#).

Next steps

To learn more, see:

- [Single sign-on \(SSO\)](#)
- [Multifactor authentication \(MFA\)](#)
- [Authentication vs authorization](#)
- [OAuth 2.0 and OpenID Connect](#)
- [App types and authentication flows](#)
- [Security tokens](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Quickstart: Create a new tenant in Microsoft Entra ID

Article • 03/05/2025

You can perform all of your administrative tasks using the Microsoft Entra admin center, including creating a new tenant for your organization.

In this quickstart article, you learn how to create a basic tenant for your organization.

ⓘ Note

Only paid customers can create a new Workforce tenant in Microsoft Entra ID.

Customers using a free tenant, or a trial subscription won't be able to create additional tenants from the Microsoft Entra admin center. Customers facing this scenario who need a new tenant can sign up for a [free account](#).

Create a new tenant for your organization

After you sign in to the [Azure portal](#), you can create a new tenant for your organization. Your new tenant represents your organization and helps you to manage a specific instance of Microsoft Cloud services for your internal and external users.

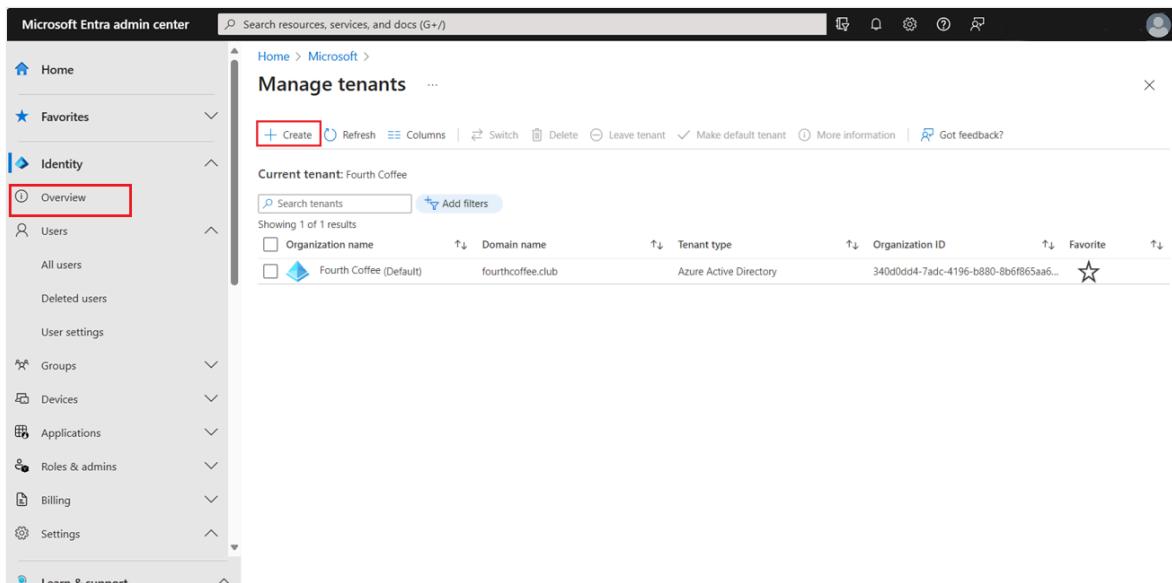
ⓘ Note

- If you're unable to create a Microsoft Entra ID or Azure AD B2C tenant, review your user settings page to ensure that tenant creation isn't switched off. If it is not enabled you must be assigned at least the [Tenant Creator](#) role.
- This article doesn't cover creating an *external* tenant configuration for consumer-facing apps; learn more about using [Microsoft Entra External ID](#) for your customer identity and access management (CIAM) scenarios.

To create a new tenant

1. Sign in to the [Azure portal](#).
2. From the Azure portal menu, select **Microsoft Entra ID**.
3. Navigate to **Identity > Overview > Manage tenants**.

4. Select Create.

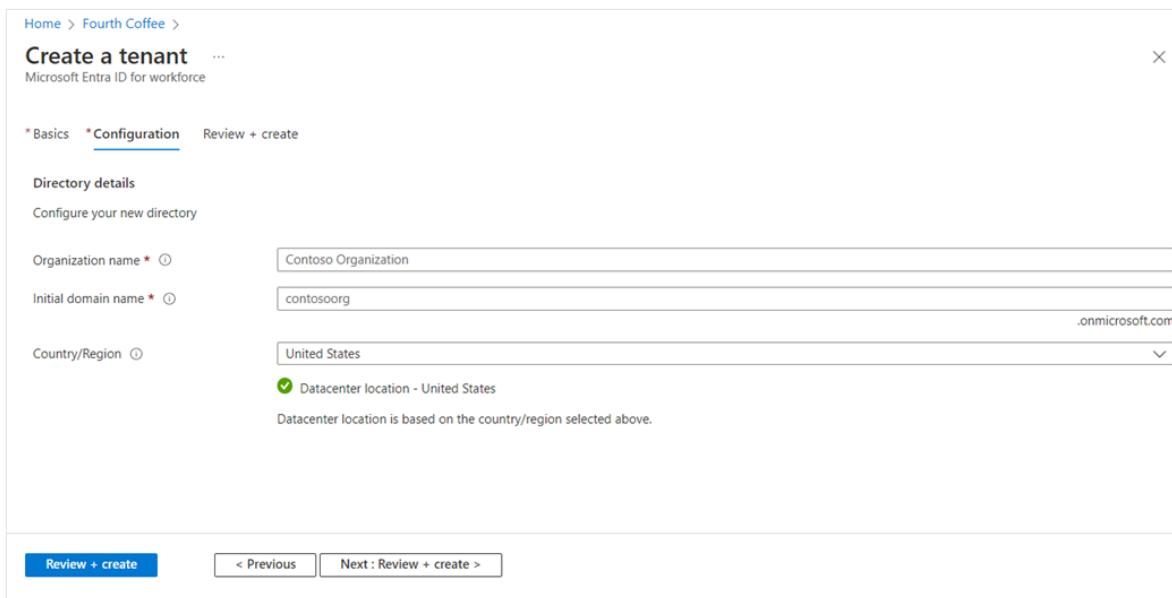


The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with sections like Home, Favorites, Identity (with Overview highlighted), Users, Groups, Devices, Applications, Roles & admins, Billing, and Settings. The main area is titled 'Manage tenants' and shows 'Current tenant: Fourth Coffee'. It includes a search bar, filter options, and a table with columns: Organization name, Domain name, Tenant type, Organization ID, Favorite, and a star icon. One row is visible: 'Fourth Coffee (Default)' with domain 'fourthcoffee.club', tenant type 'Azure Active Directory', and organization ID '340d0dd4-7adc-4196-b880-8b6f865aa6...'. There are also 'Create', 'Refresh', 'Columns', 'Switch', 'Delete', 'Leave tenant', 'Make default tenant', 'More information', and 'Got feedback?' buttons at the top.

5. On the Basics tab, select the type of tenant you want to create, either **Microsoft Entra ID** or **Microsoft Entra ID (B2C)**.

6. Select **Next: Configuration** to move to the Configuration tab.

7. On the Configuration tab, enter the following information:



The screenshot shows the 'Create a tenant' configuration page. At the top, it says 'Home > Fourth Coffee > Create a tenant ... Microsoft Entra ID for workforce'. Below that, there are tabs: * Basics, * Configuration (which is selected and underlined), and Review + create. Under 'Directory details', it says 'Configure your new directory'. There are three input fields: 'Organization name *' with 'Contoso Organization' typed in, 'Initial domain name *' with 'contosoorg' typed in followed by '.onmicrosoft.com', and 'Country/Region' with 'United States' selected. A note below says 'Datacenter location is based on the country/region selected above.' At the bottom, there are buttons for 'Review + create' (highlighted in blue), '< Previous', and 'Next : Review + create >'.

- Type your desired Organization name (for example *Contoso Organization*) into the **Organization name** box.
- Type your desired Initial domain name (for example *Contosoorg*) into the **Initial domain name** box.
- Select your desired Country/Region or leave the *United States* option in the **Country or region** box.

8. Select **Next: Review + Create**. Review the information you entered and if the information is correct, select **Create** in the lower left corner.

Your new tenant is created with the domain contoso.onmicrosoft.com.

Your user account in the new tenant

By default, the user who creates a Microsoft Entra tenant is automatically assigned the [Global Administrator](#) role.

By default, you're also listed as the [technical contact](#) for the tenant. Technical contact information is something you can change in [Properties](#).

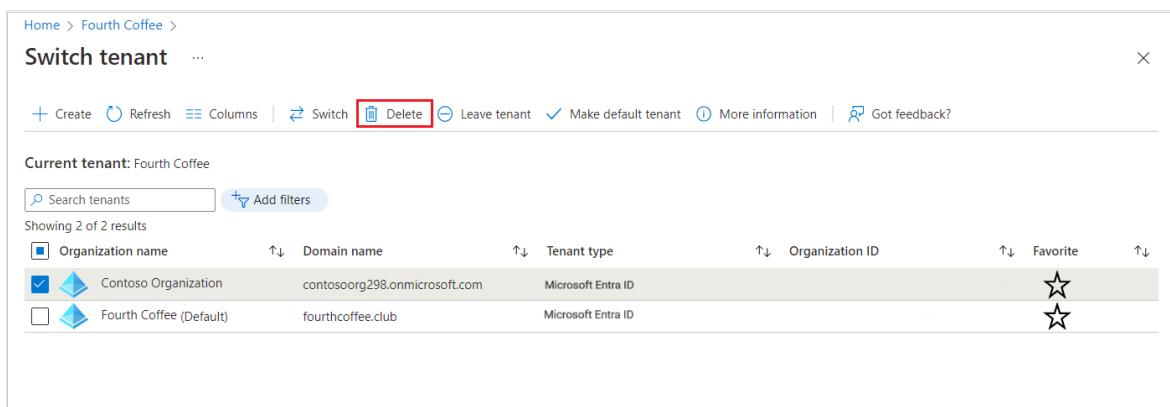
Microsoft recommends that organizations have two cloud-only emergency access accounts permanently assigned the [Global Administrator](#) role. These accounts are highly privileged and aren't assigned to specific individuals. The accounts are limited to emergency or "break glass" scenarios where normal accounts can't be used or all other administrators are accidentally locked out. These accounts should be created following the [emergency access account recommendations](#).

Clean up resources

If you're not going to continue to use this application, you can delete the tenant using the following steps:

- Ensure that you're signed in to the directory that you want to delete through the **Directory + subscription** filter in the Azure portal. Switch to the target directory if needed.
- Select **Microsoft Entra ID**, and then on the **Contoso - Overview** page, select **Delete directory**.

The tenant and its associated information are deleted.



The screenshot shows the 'Switch tenant' blade in the Microsoft Entra ID portal. At the top, there's a navigation bar with 'Home > Fourth Coffee >' and a 'Switch tenant' dropdown. Below the navigation is a toolbar with 'Create', 'Refresh', 'Columns', 'Switch', 'Delete' (which is highlighted with a red box), 'Leave tenant', 'Make default tenant', 'More information', and 'Got feedback?'. The main area is titled 'Current tenant: Fourth Coffee' and contains a search bar and a 'Add filters' button. It shows 'Showing 2 of 2 results' for 'Contoso Organization' and 'Fourth Coffee (Default)'. Each entry has columns for 'Organization name', 'Domain name', 'Tenant type', 'Organization ID', and 'Favorite'. There are star icons in the 'Favorite' column for both entries.

Organization name	Domain name	Tenant type	Organization ID	Favorite
Contoso Organization	contosoorg298.onmicrosoft.com	Microsoft Entra ID		★
Fourth Coffee (Default)	fourthcoffee.club	Microsoft Entra ID		★

Next steps

- Change or add other domain names, see [How to add a custom domain name to Microsoft Entra ID](#).
 - Add users, see [Add or delete a new user](#)
 - Add groups and members, see [Create a basic group and add members](#).
 - Learn about [Azure role-based access control \(RBAC\)](#) and [Conditional Access](#) to help manage your organization's application and resource access.
 - Learn about Microsoft Entra ID, including [basic licensing information](#), [terminology](#), and [associated features](#).
-

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

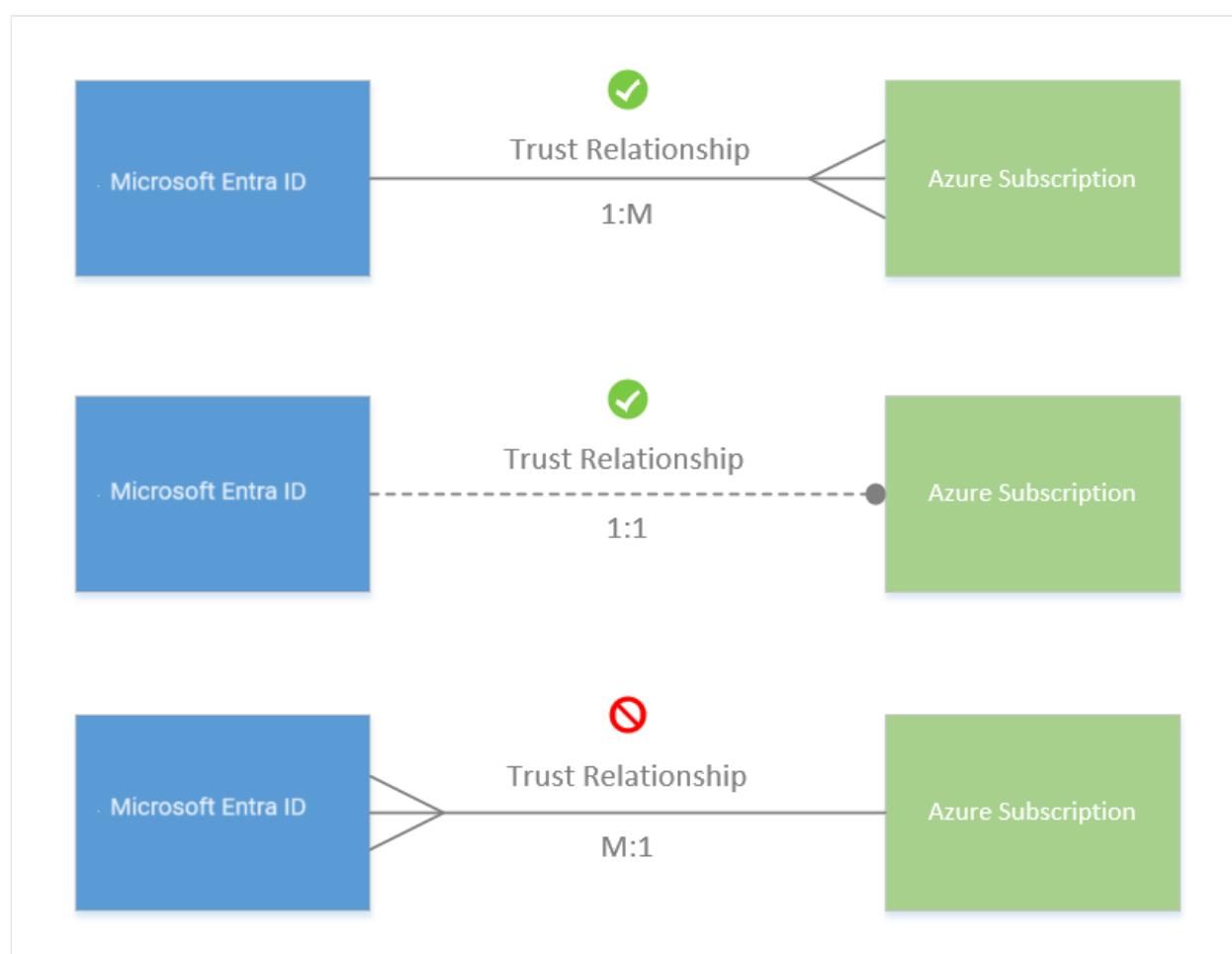
Associate or add an Azure subscription to your Microsoft Entra tenant

Article • 03/22/2024

All Azure subscriptions have a trust relationship with a Microsoft Entra tenant. Subscriptions rely on this tenant (directory) to authenticate and authorize security principals and devices. When a subscription expires, the trusted instance remains, but the security principals lose access to Azure resources. Subscriptions can only trust a single directory while one Microsoft Entra tenant might be trusted by multiple subscriptions.

When a user signs up for a Microsoft Cloud service, a new Microsoft Entra tenant is created and the user is made a Global Administrator. However, when an owner of a subscription joins their subscription to an existing tenant, the owner isn't assigned to the Global Administrator role.

While users may only have a single authentication *home* directory, users might participate as guests in multiple directories. You can see both the home and guest directories for each user in Microsoft Entra ID.



Important

When a subscription is associated with a different directory, users who have roles assigned using [Azure role-based access control \(RBAC\)](#) lose their access. Classic subscription administrators, including Service Administrator and Co-Administrators, also lose access.

Moving your Azure Kubernetes Service (AKS) cluster to a different subscription, or moving the cluster-owning subscription to a new tenant, causes the cluster to lose functionality due to lost role assignments and service principal's rights. For more information about AKS, see [Azure Kubernetes Service \(AKS\)](#).

Before you begin

Before you can associate or add your subscription, do the following steps:

- Review the following list of changes that will occur after you associate or add your subscription, and how you might be affected:
 - Users that have been assigned roles using Azure RBAC will lose their access.
 - Service Administrator and Co-Administrators will lose access.
 - If you have any key vaults, they'll be inaccessible, and you'll have to fix them after association.
 - If you have any managed identities for resources such as Virtual Machines or Logic Apps, you must reenable or re-create them after the association.
 - If you have a registered Azure Stack, you'll have to reregister it after association.

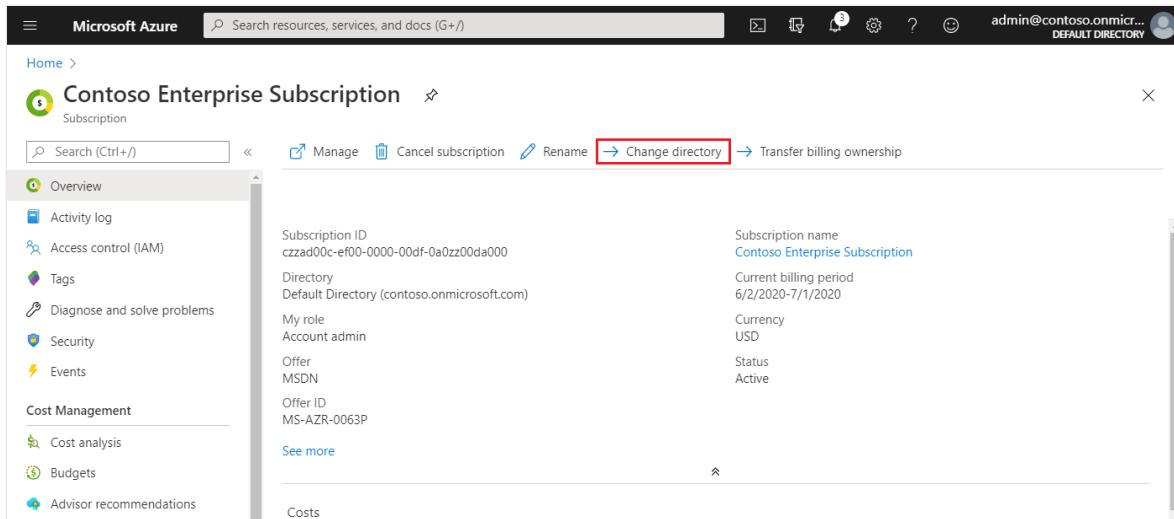
For more information, see [Transfer an Azure subscription to a different Microsoft Entra directory](#).

- Sign in using an account that:
 - Has an **Owner** role assignment for the subscription. For information about how to assign the Owner role, see [Assign Azure roles using the Azure portal](#).
 - Exists in both the current directory and in the new directory. The current directory is associated with the subscription. You'll associate the new directory with the subscription. For more information about getting access to another directory, see [Add Microsoft Entra B2B collaboration users in the Azure portal](#).
 - Make sure that you're not using an Azure Cloud Service Providers (CSP) subscription (MS-AZR-0145P, MS-AZR-0146P, MS-AZR-159P), a Microsoft Internal subscription (MS-AZR-0015P), or a Microsoft Azure for Students Starter subscription (MS-AZR-0144P).

Associate a subscription to a directory

To associate an existing subscription with your Microsoft Entra ID, follow these steps:

1. Sign to the [Azure portal](#) with the **Owner** role assignment for the subscription.
2. Browse to **Subscriptions**.
3. Select the name of the subscription you want to use.
4. Select **Change directory**.



The screenshot shows the Azure portal interface for managing subscriptions. The top navigation bar includes the Microsoft Azure logo, a search bar, and user information (admin@contoso.onmicrosoft.com, DEFAULT DIRECTORY). Below the header, the breadcrumb navigation shows 'Home > Contoso Enterprise Subscription'. The main content area displays the 'Contoso Enterprise Subscription' details. On the left, there's a sidebar with links like Overview, Activity log, Tags, Diagnose and solve problems, Security, Events, Cost Management, Cost analysis, Budgets, and Advisor recommendations. The main panel shows subscription details: Subscription ID (czzad00c-ef00-0000-00df-0a0zz00da000), Directory (Default Directory (contoso.onmicrosoft.com)), My role (Account admin), Offer (MSDN), Offer ID (MS-AZR-0063P), and various status metrics. At the top of this panel, there are buttons for Manage, Cancel subscription, Rename, Change directory (which is highlighted with a red box), and Transfer billing ownership. The 'Change directory' button is located at the top right of the main content area.

5. Review any warnings that appear, and then select **Change**.

Change the directory

X



Changing the directory removes access for all Role-Based Access Control users and other admins (including co-administrators). [See affected users](#)



Changing the directory doesn't change billing ownership for the subscription. You won't be able to delete the original directory until billing ownership is transferred to someone else. [Learn more](#)

From

Default Directory (contoso.onmicrosoft.com)

To

Contoso East Coast (000fb00a-0000-00fe-a00f-0d0ae0bcd0... ▾

Change

Cancel

After the directory is changed for the subscription, you'll get a success message.

6. Select **Switch directories** on the subscription page to go to your new directory.

The screenshot shows two side-by-side Azure portal pages. On the left, the 'Subscriptions' page lists 'Default Directory' and has a 'Switch directories' button highlighted with a red box. On the right, the 'Directory + subscription' page shows 'Contoso East Coast' as the current directory, with a 'Switch directory' section and a 'Sign in to your last visited directory' dropdown.

It can take several hours for everything to show up properly. If it seems to be taking too long, check the **Global subscription filter**. Make sure the moved subscription isn't hidden. You might need to sign out of the Azure portal and sign back in to see the new directory.

Changing the subscription directory is a service-level operation, so it doesn't affect subscription billing ownership. To delete the original directory, you must transfer the subscription billing ownership to a new Account Admin. To learn more about transferring billing ownership, see [Transfer ownership of an Azure subscription to another account](#).

Post-association steps

After you associate a subscription with a different directory, you might need to do the following tasks to resume operations:

- If you have any key vaults, you must change the Key Vault tenant ID. For more information, see [Change a Key Vault tenant ID after a subscription move](#).
- If you used system-assigned Managed Identities for resources, you must reenable these identities. If you used user-assigned Managed Identities, you must re-create these identities. After reenabling or re-creating the Managed Identities, you must reestablish the permissions assigned to those identities. For more information, see [What are managed identities for Azure resources?](#).
- If you've registered an Azure Stack using this subscription, you must reregister. For more information, see [Register Azure Stack Hub with Azure](#).
- For more information, see [Transfer an Azure subscription to a different Microsoft Entra directory](#).

Next steps

- To create a new Microsoft Entra tenant, see [Quickstart: Create a new tenant in Microsoft Entra ID](#).
- To learn more about how Microsoft Azure controls resource access, see [Azure roles, Microsoft Entra roles, and classic subscription administrator roles](#).
- To learn more about how to assign roles in Microsoft Entra ID, see [Assign administrator and non-administrator roles to users with Microsoft Entra ID](#).

Configure your company branding

Article • 03/25/2025

When users authenticate into your corporate intranet or web-based applications, Microsoft Entra ID provides the identity and access management (IAM) service. You can add company branding that applies to all these experiences to create a consistent sign-in experience for your users.

The default sign-in experience is the global look and feel that applies across all sign-ins to your tenant. Before you customize any settings, the default Microsoft branding appears in your sign-in pages. You can customize this default experience with a custom background image or color, favicon, layout, header, and footer. You can also upload a custom CSS file.

Prerequisites

Adding custom branding requires one of the following licenses:

- [Microsoft Entra ID P1 or P2](#)
- [Microsoft 365 Business Standard](#)
- [SharePoint \(Plan 1\)](#)

Microsoft Entra ID P1 or P2 editions are available for customers in China using the worldwide instance of Microsoft Entra ID. Microsoft Entra ID P1 or P2 editions aren't currently supported in the Azure service operated by 21Vianet in China.

The **Organizational Branding Administrator** role is the minimum role required to customize company branding.

Before you begin

All branding elements are optional. Default settings will remain, if left unchanged. For example, if you specify a banner logo but no background image, the sign-in page shows your logo with a default background image from the destination site such as Microsoft 365. Additionally, sign-in page branding doesn't carry over to personal Microsoft accounts. If your users or guests authenticate using a personal Microsoft account, the sign-in page doesn't reflect the branding of your organization.

Images have different image and file size requirements. We recommend you review the company branding process in the Microsoft Entra admin center to gather the image

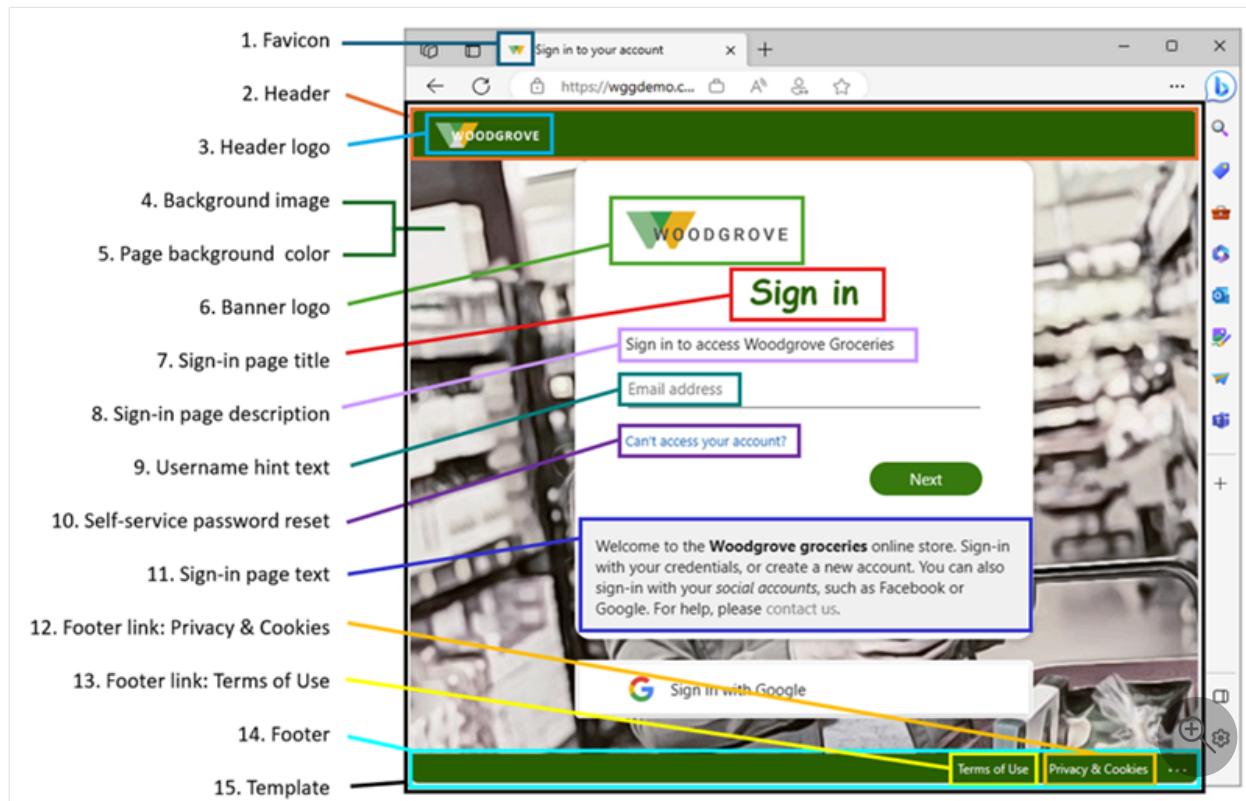
requirements you need. You might need to use a photo editor to create the right size images. The preferred image type for all images is PNG, but JPG is accepted.

External URLs aren't supported in the sign-in experience. For example, if you add an external URL for your internal help desk to the footer, that URL is displayed explicitly but isn't clickable. Users must copy the URL and navigate to it directly.

The Azure Active Directory B2C (Azure AD B2C) company branding options are different. Azure AD B2C branding is currently limited to background image, banner logo, and background color customization. For more information, see [Customize the UI](#) in the Azure AD B2C documentation.

Use Microsoft Graph with Microsoft Entra company branding. Company branding can be viewed and managed using Microsoft Graph on the `/beta` endpoint and the `organizationalBranding` resource type. For more information, see the [organizational branding API documentation](#).

The branding elements are called out in the following example. Text descriptions are provided following the image.



1. Favicon: Small icon that appears on the left side of the browser tab.
2. Header: Space across the top of the sign-in page, behind the header log.
3. Header logo: Logo that appears in the upper-left corner of the sign-in page.
4. Background image: The entire space behind the sign-in box.
5. Page background color: The entire space behind the sign-in box.
6. Banner logo: Logo that appears at the top of the sign-in box

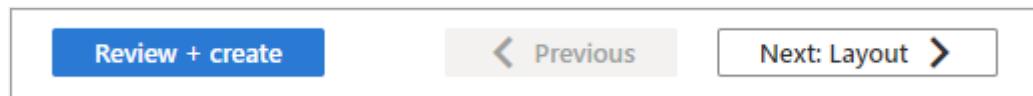
7. **Sign-in page title:** Larger text that appears below the banner logo.
8. **Sign-in page description:** Text to describe the sign-in page.
9. **Username hint and text:** The text that appears before a user enters their information.
10. **Self-service password reset:** A link you can add below the sign-in page text for password resets.
11. **Sign-in page text:** Text you can add below the username field.
12. **Footer link: Privacy & Cookies:** Link you can add to the lower-right corner for privacy information.
13. **Footer: Terms of Use:** Text in the lower-right corner of the page where you can add Terms of use information.
14. **Footer:** Space across the bottom of the page for privacy and Terms of Use information.
15. **Template:** The layout of the page and sign-in boxes.

How to navigate the company branding process

1. Sign in to the Microsoft Entra admin center [as a Organizational Branding Administrator](#).
2. Browse to **Identity > User experiences > Company branding**.
 - If you currently have a customized sign-in experience, the **Edit** button is available.

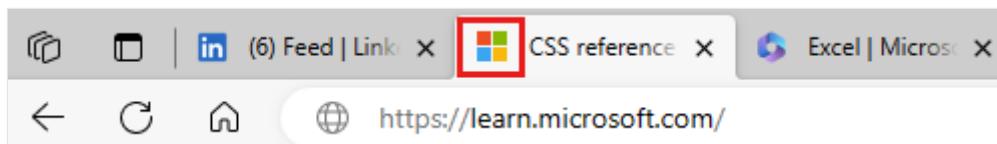
The screenshot shows the Microsoft Entra admin center interface. The left sidebar has a tree view with 'Identity' expanded, showing 'Overview', 'Users', 'Groups', 'Devices', 'Applications', 'Roles & admins', 'Billing', 'Settings', 'Protection', 'Identity governance', 'External Identities', 'User experiences' (which is selected and highlighted with a red box), 'Company branding' (which is also highlighted with a red box), 'Hybrid management', 'Monitoring & health', and 'Learn & support'. The main content area is titled 'Company Branding' and includes a 'Getting started' section, a 'Default sign-in' section with a 'Customize' button, and a 'Browser language customizations' section with a 'Customize' button. There is also a 'Customize your end user experiences' section with a 'Learn more' link.

The sign-in experience process is grouped into sections. At the end of each section, select the **Review + create** button to review what you selected and submit your changes or the **Next** button to move to the next section.



Basics

- **Favicon:** Select a PNG or JPG of your logo that appears in the web browser tab.
 - Image size: 32x32 px
 - Max file size: 5 KB



- **Background image:** Select a PNG or JPG to display as the main image on your sign-in page. This image scales and crops according to the window size, but the sign-in prompt might partially block it.
 - Image size: 1920x1080 px
 - Max file size: 300 KB
- **Page background color:** If the background image isn't able to load because of a slower connection, your selected background color appears instead.

Layout

- **Visual Templates:** Customize the layout of your sign-in page using templates or a custom CSS file.
 - Choose one of two **Templates:** Full-screen or partial-screen background. The full-screen background could obscure your background image, so choose the partial-screen background if your background image is important.
 - The details of the **Header** and **Footer** options are set on the next two sections of the process.

Customize default sign-in experience

X

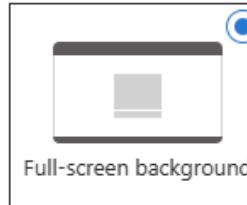
Basics Layout Header Footer Sign-in form Review

Configure layout by choosing a pre-defined template and setting up core web page elements such as the header, footer, and styling with CSS.

Visual templates

Choose menu behavior, your color theme, and whether to use a high-contrast theme.

Template ⓘ



Full-screen background

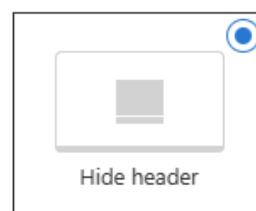


Partial-screen background

Header ⓘ

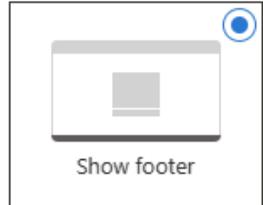


Show header



Hide header

Footer ⓘ



Show footer



Hide footer

- **Custom CSS:** Upload a custom CSS file to replace the Microsoft default style of the page.
 - [Download the CSS template ↗](#).
 - View the [CSS template reference guide](#).

Header

If you haven't enabled the header, go to the **Layout** section and select **Show header**.

Once enabled, select a PNG or JPG to display in the header of the sign-in page.

- Image size: 245x36 px
- Max file size: 10 KB



The header control has been disabled in the 'Layout' tab and will not appear on the sign-in screen. Enable it to make changes here.

Footer

If you haven't enabled the footer, go to the **Layout** section and select **Show footer**. Once enabled, adjust the following settings.

- **Show 'Privacy & Cookies'**: This option is selected by default and displays the [Microsoft 'Privacy & Cookies' ↗](#) link.
 - Uncheck this option to hide the default Microsoft link.
 - Optionally provide your own **Display text** and **URL**. The text and links don't have to be related to privacy and cookies.
 - Custom URLs are displayed as text and aren't clickable.
- **Show 'Terms of Use'**: This option is also selected by default and displays the [Microsoft 'Terms of Use' ↗](#) link.
 - Uncheck this option to hide the default Microsoft link. Optionally provide your own **Display text** and **URL**.
 - The text and links don't have to be related to your terms of use.

Important

The default Microsoft 'Terms of Use' link isn't the same as the Conditional Access Terms of Use. Seeing the terms here doesn't mean you accepted those terms and conditions.

Customize default sign-in experience

X

[Basics](#) [Layout](#) [Header](#) [Footer](#) [Sign-in form](#) [Errors and prompts](#) [Review](#)

Configure other elements such as images, text and hyperlinks inside of the footer.

Privacy & Cookies

Show 'Privacy & Cookies' [i](#)

Display text [i](#)

URL [i](#)

Terms of Use

Show 'Terms of Use' [i](#)

Display text [i](#)

URL [i](#)

[Review + create](#)[Previous](#)[Next: Sign-in form](#)

Sign-in form

- **Banner logo:** Select a PNG or JPG image file of a banner-sized logo (short and wide) to appear on the sign-in pages.
 - Image size: 245x36 px
 - Max file size: 50 KB
- **Square logo (light theme):** Select a square PNG or JPG image file of your logo to be used in browsers that are using a light color theme. This logo is used to represent your organization on the Microsoft Entra web interface and in Windows.
 - Image size: 240x240 px
 - Max file size: 50 KB
- **Square logo (dark theme)** Select a square PNG or JPG image file of your logo to be used in browsers that are using a dark color theme. This logo is used to represent your organization on the Microsoft Entra web interface and in Windows. If your logo looks good on light and dark backgrounds, there's no need to add a dark theme logo.
 - Image size: 240x240 px
 - Max file size: 50 KB

- **Username hint text:** Enter hint text for the username input field on the sign-in page. If guests use the same sign-in page, we don't recommend using hint text here.
- **Sign-in page text:** Enter text that appears on the bottom of the sign-in page. You can use this text to communicate additional information, such as the phone number to your help desk or a legal statement. This page is public, so don't provide sensitive information here. This text must be Unicode and can't exceed 1,024 characters.

To begin a new paragraph, press the Enter key twice. You can also change text formatting to include bold, italics, an underline, or clickable link. Use the following syntax to add formatting to text:

- Hyperlink: `[text](link)`
- Bold: `**text**` or `_text_`
- Italics: `*text*` or `_text_`
- Underline: `++text++`

 **Important**

Hyperlinks that are added to the sign-in page text render as text in native environments, such as desktop and mobile applications.

- **Self-service password reset:**
 - Show self-service password reset (SSPR): Select the checkbox to turn on SSPR.
 - Common URL: Enter the destination URL for where your users reset their passwords. This URL appears on the username and password collection screens as text and isn't clickable.
 - Username collection display text: Replace the default text with your own custom username collection text.
 - Password collection display text: Replace the default text with your own customer password collection text.

Review

All of the available options appear in one list so you can review everything you customized or left at the default setting. When you're done, select the **Create** button.

Once your default sign-in experience is created, select the **Edit** button to make any changes. You can't delete a default sign-in experience after it's created, but you can remove all custom settings.

The time it takes for changes to appear in the sign-in experience can vary based on the tenant's geographical location. Updates can take a few minutes or up to 2 hours. This time range is a target, not a guarantee.

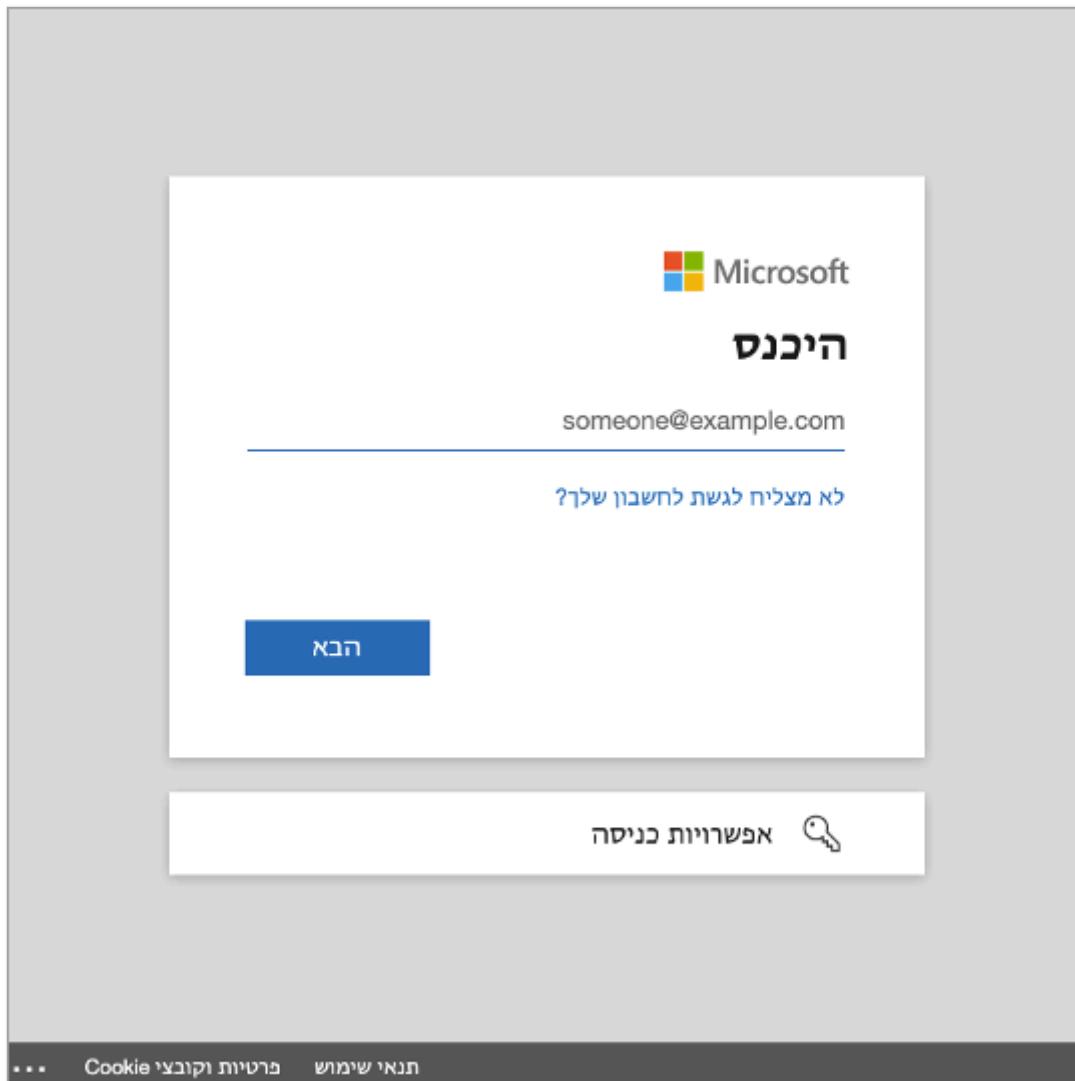
Customize the sign-in experience by browser language

You can create a personalized sign-in experience for users who sign in using a specific browser language by customizing the branding elements for that browser language. This customization overrides any configurations made to the default branding. If you don't make any changes to the elements, the default elements are displayed.

1. Sign in to the [Microsoft Entra admin center](#) as a [Organizational Branding Administrator](#).
2. Browse to **Identity > User experiences > Company branding**.
3. Select **Add browser language**.

The process for customizing the experience is the same as the [default sign-in experience](#) process, except you must select a language from the dropdown list in the **Basics** section. We recommend adding custom text in the same areas as your default sign-in experience.

Microsoft Entra ID supports right-to-left functionality for languages such as Arabic and Hebrew that are read right-to-left. The layout adjusts automatically, based on the user's browser settings.



User experience

There are some scenarios for you to consider when you customize the sign-in pages for your organization's tenant-specific applications.

Software as a Service (SaaS) and multitenant applications

For Microsoft, Software as a Service (SaaS), and multitenant applications such as <https://myapps.microsoft.com>, or <https://outlook.com>, the customized sign-in page appears only after the user types their **Email** or **Phone number** and selects the **Next** button.

Home Realm Discovery

Some Microsoft applications support [Home Realm Discovery](#) for authentication. In these scenarios, when a customer signs in to a Microsoft Entra common sign-in page, Microsoft Entra ID can use the customer's user name to determine where they should sign in.

For customers who access applications from a custom URL, the `whr` query string parameter, or a domain variable, can be used to apply company branding at the initial sign-in screen, not just after adding the email or phone number. For example, `whr=contoso.com` would appear in the custom URL for the app. With the Home Realm Discover and domain parameter included, the company branding appears immediately in the first sign-in step. Other domain hints can be included.

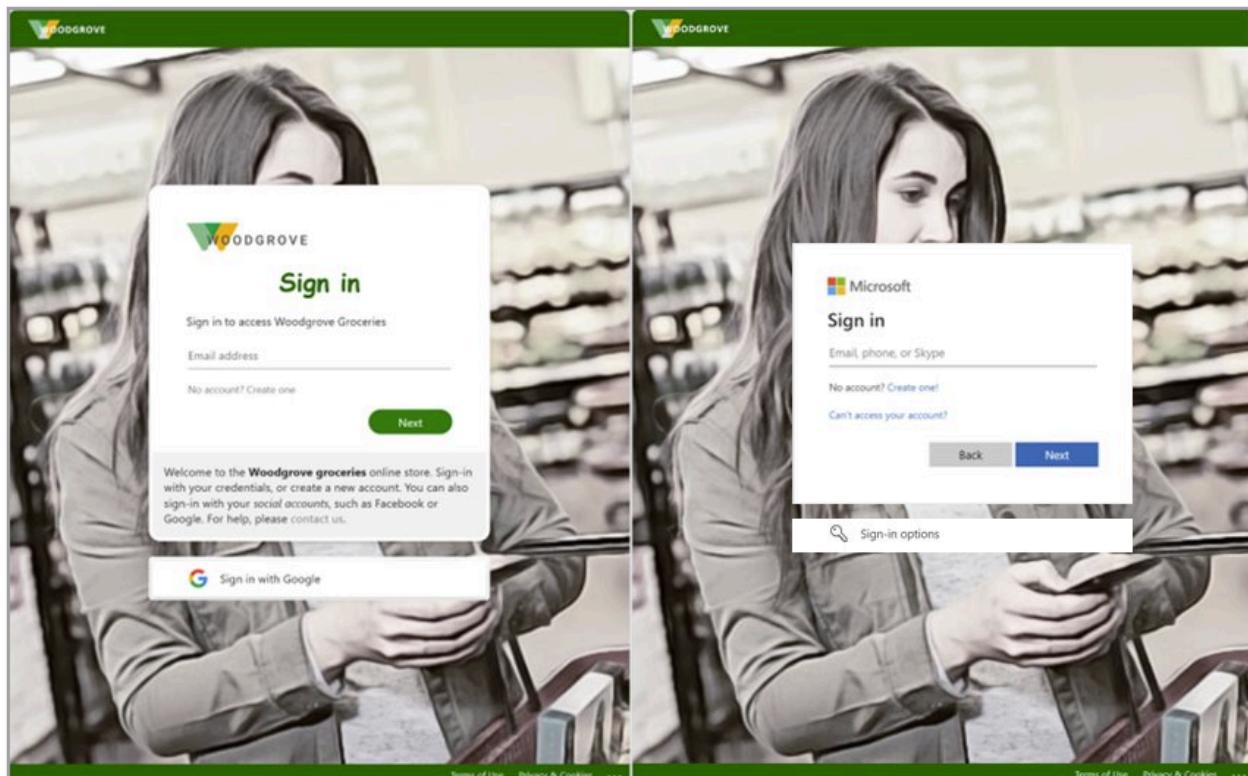
In the following examples, replace the contoso.com with your own tenant name, or verified domain name:

- For Microsoft Outlook <https://outlook.com/contoso.com>
- For SharePoint in Microsoft 365 <https://contoso.sharepoint.com>
- For My Apps portal <https://myapps.microsoft.com/?whr=contoso.com>
- Self-service password reset <https://passwordreset.microsoftonline.com/?whr=contoso.com>

B2B scenarios

For B2B collaboration end-users who perform cross-tenant sign-ins, their home tenant branding appears, even if there isn't custom branding specified.

In the following example, the company branding for Woodgrove Groceries appears on the left, with the Woodgrove logo, fonts, and custom text. The example on the right displays the default branding for the user's home tenant. The default branding displays the Microsoft logo, fonts, and text.



Next steps

- [View the CSS template reference guide](#)
 - [Learn more about default user permissions in Microsoft Entra ID](#)
 - [Manage the 'stay signed in' prompt](#)
-

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#) ↗

What are the default user permissions in Microsoft Entra ID?

Article • 03/05/2025

In Microsoft Entra ID, all users are granted a set of default permissions. A user's access consists of the type of user, their [role assignments](#), and their ownership of individual objects.

This article describes those default permissions and compares the member and guest user defaults. The default user permissions can be changed only in user settings in Microsoft Entra ID.

Member and guest users

The set of default permissions depends on whether the user is a native member of the tenant (member user) or is brought over from another directory, such as a business-to-business (B2B) collaboration guest (guest user). For more information about adding guest users, see [What is Microsoft Entra B2B collaboration?](#). Here are the capabilities of the default permissions:

- *Member users* can register applications, manage their own profile photo and mobile phone number, change their own password, and invite B2B guests. These users can also read all directory information (with a few exceptions).
- *Guest users* have restricted directory permissions. They can manage their own profile, change their own password, and retrieve some information about other users, groups, and apps. However, they can't read all directory information.

For example, guest users can't enumerate the list of all users, groups, and other directory objects. Guests can be added to administrator roles, which grant them full read and write permissions. Guests can also invite other guests.

Compare member and guest default permissions

 Expand table

Area	Member user permissions	Default guest user permissions	Restricted guest user permissions
Users and contacts	<ul style="list-style-type: none"> • Enumerate the list of all users and contacts • Read all public properties of users and contacts • Invite guests • Change their own password • Manage their own mobile phone number • Manage their own photo • Invalidate their own refresh tokens 	<ul style="list-style-type: none"> • Read their own properties • Read display name, email, sign-in name, photo, user principal name, and user type properties of other users and contacts • Change their own password • Search for another user by object ID (if allowed) • Read manager and direct report information of other users 	<ul style="list-style-type: none"> • Read their own properties • Change their own password • Manage their own mobile phone number
Groups	<ul style="list-style-type: none"> • Create security groups • Create Microsoft 365 groups • Enumerate the list of all groups • Read all properties of groups • Read nonhidden group membership • Read hidden Microsoft 365 group membership for joined groups • Manage properties, ownership, and membership of groups that the user owns • Add guests to owned groups • Manage group membership settings • Delete owned groups • Restore owned Microsoft 365 groups 	<ul style="list-style-type: none"> • Read properties of nonhidden groups, including membership and ownership (even nonjoined groups) • Read hidden Microsoft 365 group membership for joined groups • Search for groups by display name or object ID (if allowed) 	<ul style="list-style-type: none"> • Read object ID for joined groups • Read membership and ownership of joined groups in some Microsoft 365 apps (if allowed)
Applications	<ul style="list-style-type: none"> • Register (create) new applications 	<ul style="list-style-type: none"> • Read properties of registered and 	<ul style="list-style-type: none"> • Read properties of registered and

Area	Member user permissions	Default guest user permissions	Restricted guest user permissions
	<ul style="list-style-type: none"> • Enumerate the list of all applications • Read properties of registered and enterprise applications • Manage application properties, assignments, and credentials for owned applications • Create or delete application passwords for users • Delete owned applications • Restore owned applications • List permissions granted to applications 	<ul style="list-style-type: none"> enterprise applications • List permissions granted to applications 	<ul style="list-style-type: none"> enterprise applications • List permissions granted to applications
Devices	<ul style="list-style-type: none"> • Enumerate the list of all devices • Read all properties of devices • Manage all properties of owned devices 	No permissions	No permissions
Organization	<ul style="list-style-type: none"> • Read all company information • Read all domains • Read configuration of certificate-based authentication • Read all partner contracts • Read multitenant organization basic details and active tenants 	<ul style="list-style-type: none"> • Read company display name • Read all domains • Read configuration of certificate-based authentication 	<ul style="list-style-type: none"> • Read company display name • Read all domains
Roles and scopes	<ul style="list-style-type: none"> • Read all administrative roles and memberships • Read all properties and membership of 	No permissions	No permissions

Area	Member user permissions	Default guest user permissions	Restricted guest user permissions
administrative units			
Subscriptions	<ul style="list-style-type: none"> • Read all licensing subscriptions • Enable service plan memberships 	No permissions	No permissions
Policies	<ul style="list-style-type: none"> • Read all properties of policies • Manage all properties of owned policies 	No permissions	No permissions
Terms of use	Read terms of use a user has accepted.	Read terms of use a user has accepted.	Read terms of use a user has accepted.

Restrict member users' default permissions

It's possible to add restrictions to users' default permissions.

You can restrict default permissions for member users in the following ways:

 **Caution**

Using the **Restrict access to Microsoft Entra administration portal** switch is NOT a security measure. For more information on the functionality, see the following table.

 Expand table

Permission	Setting explanation
Register applications	Setting this option to No prevents users from creating application registrations. You can then grant the ability back to specific individuals, by adding them to the application developer role.
Allow users to connect work or school account with LinkedIn	Setting this option to No prevents users from connecting their work or school account with their LinkedIn account. For more information, see LinkedIn account connections data sharing and consent .
Create security groups	Setting this option to No prevents users from creating security groups. Those users assigned at least the User Administrators role can still create security groups. To learn how, see Microsoft Entra cmdlets for configuring group settings .

Permission	Setting explanation
Create Microsoft 365 groups	<p>Setting this option to No prevents users from creating Microsoft 365 groups. Setting this option to Some allows a set of users to create Microsoft 365 groups. Anyone assigned at least the User Administrator role can still create Microsoft 365 groups. To learn how, see Microsoft Entra cmdlets for configuring group settings.</p>
Restrict access to Microsoft Entra administration portal	<p>What does this switch do? No lets nonadministrators browse the Microsoft Entra administration portal. Yes Restricts nonadministrators from browsing the Microsoft Entra administration portal. Nonadministrators who are owners of groups or applications are unable to use the Azure portal to manage their owned resources.</p> <p>What does it not do? It doesn't restrict access to Microsoft Entra data using PowerShell, Microsoft GraphAPI, or other clients such as Visual Studio. It doesn't restrict access as long as a user is assigned a custom role (or any role).</p> <p>When should I use this switch? Use this option to prevent users from misconfiguring the resources that they own.</p> <p>When should I not use this switch? Don't use this switch as a security measure. Instead, create a Conditional Access policy that targets Windows Azure Service Management API that blocks nonadministrators access to Windows Azure Service Management API.</p> <p>How do I grant only a specific non-administrator users the ability to use the Microsoft Entra administration portal? Set this option to Yes, then assign them a role like global reader.</p> <p>Restrict access to the Microsoft Entra administration portal A Conditional Access policy that targets Windows Azure Service Management API targets access to all Azure management.</p>
Restrict non-admin users from creating tenants	<p>Users can create tenants in the Microsoft Entra ID and Microsoft Entra administration portal under Manage tenant. The creation of a tenant is recorded in the Audit log as category DirectoryManagement and activity Create Company. By default, the user who creates a Microsoft Entra tenant is automatically assigned the Global Administrator role. The newly created tenant doesn't inherit any settings or configurations.</p> <p>What does this switch do? Setting this option to Yes restricts creation of Microsoft Entra tenants to anyone assigned at least the Tenant Creator role. Setting this option to No allows nonadmin users to create Microsoft Entra tenants. Tenant create continues to be recorded in the Audit log.</p> <p>How do I grant only a specific non-administrator users the ability to create new tenants? Set this option to Yes, then assign them the Tenant Creator role.</p>

Permission	Setting explanation
Restrict users from recovering the BitLocker key(s) for their owned devices	This setting can be found in the Microsoft Entra admin center in the Device Settings. Setting this option to Yes restricts users from being able to self-service recover BitLocker key(s) for their owned devices. Users must contact their organization's helpdesk to retrieve their BitLocker keys. Setting this option to No allows users to recover their BitLocker keys.
Read other users	<p>This setting is available in Microsoft Graph and PowerShell only. Setting this flag to <code>\$false</code> prevents all nonadmins from reading user information from the directory. This flag might prevent reading user information in other Microsoft services like Microsoft Teams.</p> <p>This setting is meant for special circumstances, so we don't recommend setting the flag to <code>\$false</code>.</p>

The **Restricted non-admin users from creating tenants** option is shown in the following screenshot.

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with various options like Home, Favorites, Identity, Overview, Users, Groups, Devices, Applications, Roles & admins, Billing, and Settings. The main area is titled 'Users | User settings' and shows a list of users. Under 'Default user role permissions', there are several settings: 'Users can register applications' (Yes), 'Restrict non-admin users from creating tenants' (Yes, highlighted with a red box), and 'Users can create security groups' (Yes). Below this, under 'Guest user access', there are three radio button options for guest user access restrictions: 'Guest users have the same access as members (most inclusive)' (selected), 'Guest users have limited access to properties and memberships of directory objects', and 'Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)'. At the bottom, there's a note about restricting access to the Microsoft Entra admin center, which is set to 'No'.

Restrict guest users' default permissions

You can restrict default permissions for guest users in the following ways.

Note

The **Guest user access restrictions** setting replaced the **Guest users permissions are limited** setting. For guidance on using this feature, see [Restrict guest access permissions in Microsoft Entra ID](#).

[+] Expand table

Permission	Setting explanation
Guest user access restrictions	<p>Setting this option to Guest users have the same access as members grants all member user permissions to guest users by default.</p> <p>Setting this option to Guest user access is restricted to properties and memberships of their own directory objects restricts guest access to only their own user profile by default. Access to other users is no longer allowed, even when they're searching by user principal name, object ID, or display name. Access to group information, including groups memberships, is also no longer allowed.</p>
	<p>This setting doesn't prevent access to joined groups in some Microsoft 365 services like Microsoft Teams. To learn more, see Microsoft Teams guest access.</p>
	<p>Guest users can still be added to administrator roles regardless of this permission setting.</p>
Guests can invite	<p>Setting this option to Yes allows guests to invite other guests. To learn more, see Configure external collaboration settings.</p>

Object ownership

Application registration owner permissions

When a user registers an application, they're automatically added as an owner for the application. As an owner, they can manage the metadata of the application, such as the name and permissions that the app requests. They can also manage the tenant-specific configuration of the application, such as the single sign-on (SSO) configuration and user assignments.

An owner can also add or remove other owners. Unlike those users assigned at least the Application Administrator role, owners can manage only the applications that they own.

Enterprise application owner permissions

When a user adds a new enterprise application, they're automatically added as an owner. As an owner, they can manage the tenant-specific configuration of the application, such as the SSO configuration, provisioning, and user assignments.

An owner can also add or remove other owners. Unlike those users assigned at least the Application Administrator role, owners can manage only the applications that they own.

Group owner permissions

When a user creates a group, they're automatically added as an owner for that group. As an owner, they can manage properties of the group (such as the name) and manage group membership.

An owner can also add or remove other owners. Unlike those users assigned at least the [Groups Administrator](#) role, owners can manage only the groups that they own and they can add or remove group members only if the group's membership type is **Assigned**.

To assign a group owner, see [Managing owners for a group](#).

To use Privileged Access Management (PIM) to make a group eligible for a role assignment, see [Use Microsoft Entra groups to manage role assignments](#).

Ownership permissions

The following tables describe the specific permissions in Microsoft Entra ID that member users have over objects they own. Users have these permissions only on objects that they own.

Owned application registrations

Users can perform the following actions on owned application registrations:

[+] [Expand table](#)

Action	Description
<code>microsoft.directory/applications/audience/update</code>	Update the <code>applications.audience</code> property in Microsoft Entra ID.
<code>microsoft.directory/applications/authentication/update</code>	Update the <code>applications.authentication</code> property in Microsoft Entra ID.
<code>microsoft.directory/applications/basic/update</code>	Update basic properties on applications in Microsoft Entra ID.
<code>microsoft.directory/applications/credentials/update</code>	Update the <code>applications.credentials</code> property in Microsoft Entra ID.
<code>microsoft.directory/applications/delete</code>	Delete applications in Microsoft Entra ID.
<code>microsoft.directory/applications/owners/update</code>	Update the <code>applications.owners</code> property in Microsoft Entra ID.
<code>microsoft.directory/applications/permissions/update</code>	Update the <code>applications.permissions</code> property in Microsoft Entra ID.
<code>microsoft.directory/applications/policies/update</code>	Update the <code>applications.policies</code> property in Microsoft Entra ID.
<code>microsoft.directory/applications/restore</code>	Restore applications in Microsoft Entra ID.

Owned enterprise applications

Users can perform the following actions on owned enterprise applications. An enterprise application consists of a service principal, one or more application policies, and sometimes an application object in the same tenant as the service principal.

[Expand table](#)

Action	Description
microsoft.directory/auditLogs/allProperties/read	Read all properties (including privileged properties) on audit logs in Microsoft Entra ID.
microsoft.directory/policies/basic/update	Update basic properties on policies in Microsoft Entra ID.
microsoft.directory/policies/delete	Delete policies in Microsoft Entra ID.
microsoft.directory/policies/owners/update	Update the <code>policies.owners</code> property in Microsoft Entra ID.
microsoft.directory/servicePrincipals/appRoleAssignedTo/update	Update the <code>servicePrincipals.appRoleAssignedTo</code> property in Microsoft Entra ID.
microsoft.directory/servicePrincipals/appRoleAssignments/update	Update the <code>users.appRoleAssignments</code> property in Microsoft Entra ID.
microsoft.directory/servicePrincipals/audience/update	Update the <code>servicePrincipals.audience</code> property in Microsoft Entra ID.
microsoft.directory/servicePrincipals/authentication/update	Update the <code>servicePrincipals.authentication</code> property in Microsoft Entra ID.
microsoft.directory/servicePrincipals/basic/update	Update basic properties on service principals in Microsoft Entra ID.
microsoft.directory/servicePrincipals/credentials/update	Update the <code>servicePrincipals.credentials</code> property in Microsoft Entra ID.
microsoft.directory/servicePrincipals/delete	Delete service principals in Microsoft Entra ID.
microsoft.directory/servicePrincipals/owners/update	Update the <code>servicePrincipals.owners</code> property in Microsoft Entra ID.
microsoft.directory/servicePrincipals/permissions/update	Update the <code>servicePrincipals.permissions</code> property in Microsoft Entra ID.

Action	Description
microsoft.directory/servicePrincipals/policies/update	Update the <code>servicePrincipals.policies</code> property in Microsoft Entra ID.
microsoft.directory/signInReports/allProperties/read	Read all properties (including privileged properties) on sign-in reports in Microsoft Entra ID.
microsoft.directory/servicePrincipals/synchronizationCredentials/manage	Manage application provisioning secrets and credentials
microsoft.directory/servicePrincipals/synchronizationJobs/manage	Start, restart, and pause application provisioning synchronization jobs
microsoft.directory/servicePrincipals/synchronizationSchema/manage	Create and manage application provisioning synchronization jobs and schema
microsoft.directory/servicePrincipals/synchronization/standard/read	Read provisioning settings associated with your service principal

Owned devices

Users can perform the following actions on owned devices:

[Expand table](#)

Action	Description
microsoft.directory/devices/bitLockerRecoveryKeys/read	Read the <code>devices.bitLockerRecoveryKeys</code> property in Microsoft Entra ID.
microsoft.directory/devices/disable	Disable devices in Microsoft Entra ID.

Owned groups

Users can perform the following actions on owned groups.

① Note

Owners of dynamic membership groups must have the Groups Administrator, Intune Administrator, or User Administrator role to edit rules for dynamic membership groups. For more information, see [Create or update a dynamic membership group in Microsoft Entra ID](#).

Action	Description
microsoft.directory/groups/appRoleAssignments/update	Update the <code>groups.appRoleAssignments</code> property in Microsoft Entra ID.
microsoft.directory/groups/basic/update	Update basic properties on groups in Microsoft Entra ID.
microsoft.directory/groups/delete	Delete groups in Microsoft Entra ID.
microsoft.directory/groups/members/update	Update the <code>groups.members</code> property in Microsoft Entra ID.
microsoft.directory/groups/owners/update	Update the <code>groups.owners</code> property in Microsoft Entra ID.
microsoft.directory/groups/restore	Restore groups in Microsoft Entra ID.
microsoft.directory/groups/settings/update	Update the <code>groups.settings</code> property in Microsoft Entra ID.

Next steps

- To learn more about the **Guest user access restrictions** setting, see [Restrict guest access permissions in Microsoft Entra ID](#).
- To learn more about how to assign Microsoft Entra administrator roles, see [Assign a user to administrator roles in Microsoft Entra ID](#).
- To learn more about how resource access is controlled in Microsoft Azure, see [Understanding resource access in Azure](#).
- [Manage users](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Learn about group types, membership types, and access management

Article • 02/12/2025

Microsoft Entra ID provides several ways to manage access to resources, applications, and tasks. With Microsoft Entra groups, you can grant access and permissions to a group of users instead of to each individual user. Limiting access to Microsoft Entra resources to only those users who need access is one of the core security principles of [Zero Trust](#).

This article provides an overview of how groups and access rights can be used together to make managing your Microsoft Entra users easier, while also applying security best practices.

Note

Some groups can't be managed in the Azure portal or Microsoft Entra admin center.

- Groups synced from on-premises Active Directory can only be managed on-premises.
- Distribution lists and mail-enabled security groups can only be managed in the [Exchange admin center](#) or the [Microsoft 365 admin center](#). You must sign in and have the appropriate permissions for that admin center to manage those groups.

Microsoft Entra groups overview

Effective use of groups can reduce manual tasks, such as assigning roles and permissions to individual users. You can assign roles to a group and assign members to a group based on their job function or department. You can create a Conditional Access policy that applies to a group, and then assign the policy to the group. Because of the potential uses for groups, it's important to understand how they work and how they're managed.

Group types

You can manage two types of groups in the Microsoft Entra admin center:

- **Security groups:** Used to manage access to shared resources.
 - Members of a security group can include users, devices, [service principals](#).
 - Groups can be members of other groups, sometimes known as nested groups.
See note.
 - Users and service principals can be the owner of a security group.
- **Microsoft 365 groups:** Provide collaboration opportunities.
 - Members of a Microsoft 365 group can only include users.
 - Users and service principals can be the owner of a Microsoft 365 group.
 - People outside of your organization can be members of a group.
 - For more information, see [Learn about Microsoft 365 Groups](#).

 **Note**

When nesting an existing security group to another security group, only members in the parent group have access to shared resources and applications. For more info about managing nested groups, see [How to manage groups](#).

Membership types

- **Assigned groups:** Lets you add specific users as members of a group and have unique permissions.
- **Dynamic membership group for users:** Lets you use rules to automatically add and remove users as members. If a member's attributes change, the system looks at your rules for dynamic membership groups for the directory. The system checks to see whether the member meets the rule requirements (is added), or no longer meets the rules requirements (is removed).
- **Dynamic membership group for devices:** Lets you use rules to automatically add and remove devices as members. If a device's attributes change, the system looks at your rules for dynamic membership groups for the directory to see whether the device meets the rule requirements (is added) or no longer meets the rules requirements (is removed).

 **Important**

You can create a dynamic group for either devices or users, but not for both. You can't create a device group based on the device owners' attributes. Device membership rules can only reference device attributions. For more information, see [Create a dynamic group](#).

Access management

Microsoft Entra ID helps you give access to your organization's resources by providing access rights to a single user or a group. Using groups lets the resource owner or Microsoft Entra directory owner assign a set of access permissions to all members of the group. The resource or directory owner can also grant group management rights to someone such as a department manager or a help desk administrator, which allows that person to add and remove members. For more information about how to manage group owners, see the [Manage groups](#) article.

The resources that Microsoft Entra groups can manage access to can be:

- Part of your Microsoft Entra organization, such as permissions to manage users, applications, billing, and other objects.
- External to your organization, such as non-Microsoft Software as a Service (SaaS) apps.
- Azure services
- SharePoint sites
- On-premises resources

Each application, resource, and service that requires access permissions needs to be managed separately because the permissions for one might not be the same as another. Grant access using the [principle of least privilege](#) to help reduce the risk of attack or a security breach.

Assignment types

After creating a group, you need to decide how to manage its access.

- **Direct assignment.** The resource owner directly assigns the user to the resource.
- **Group assignment.** The resource owner assigns a Microsoft Entra group to the resource, which automatically gives all of the group members access to the resource. Both the group owner and the resource owner manage group membership, letting either owner add or remove members from the group. For more information about managing group membership, see the [Managed groups](#) article.
- **Rule-based assignment.** The resource owner creates a group and uses a rule to define which users are assigned to a specific resource. The rule is based on attributes that are assigned to individual users. The resource owner manages the rule, determining which attributes and values are required to allow access the resource. For more information, see [Create a dynamic group](#).

- **External authority assignment.** Access comes from an external source, such as an on-premises directory or a SaaS app. In this situation, the resource owner assigns a group to provide access to the resource and then the external source manages the group members.

Best practices for managing groups in the cloud

The following are best practices for managing groups in the cloud:

- **Enable self-service group management:** Allow users to search for and join groups or create and manage their own Microsoft 365 groups.
 - Empowers teams to organize themselves while reducing the administrative burden on IT.
 - Apply a **group naming policy** to block the use of restricted words and ensure consistency.
 - Prevent inactive groups from lingering by enabling group expiration policies, which automatically deletes unused groups after a specified period, unless renewed by a group owner.
 - Configure groups to automatically accept all users that join or require approval.
 - For more information, see [Set up self-service group management in Microsoft Entra ID](#).
- **Leverage sensitivity labels:** Use sensitivity labels to classify and govern Microsoft 365 groups based on their security and compliance needs.
 - Provides fine-grained access controls and ensures that sensitive resources are protected.
 - For more information, see [Assign sensitivity labels to Microsoft 365 groups in Microsoft Entra ID](#)
- **Automate membership with dynamic groups:** Implement dynamic membership rules to automatically add or remove users and devices from groups based on attributes like department, location, or job title.
 - Minimizes manual updates and reduces the risk of lingering access.
 - This feature applies to Microsoft 365 groups and Security Groups.
- **Conduct Periodic Access Reviews:** Use Microsoft Entra Identity Governance capabilities to schedule regular access reviews.
 - Ensures that membership in assigned groups remains accurate and relevant over time.
 - For more information, see [Create or update a dynamic membership group in Microsoft Entra ID](#)

- **Manage membership with access packages:** Create access packages with Microsoft Entra Identity Governance to streamline the management of multiple group memberships. Access packages can:
 - Include approval workflows for membership
 - Define criteria for access expiration
 - Provide a centralized way to grant, review, and revoke access across groups and applications
 - For more information, see [Create an access package in entitlement management](#)
- **Assign multiple group owners:** Assign at least two owners to a group to ensure continuity and reduce dependencies on a single individual.
 - For more information, see [Manage Microsoft Entra groups and group membership](#)
- **Use group-based licensing:** Group-based licensing simplifies user provisioning and ensures consistent license assignments.
 - Use dynamic membership groups to automatically manage licensing for users meeting specific criteria.
 - For more information, see [What is group-based licensing in Microsoft Entra ID?](#)
- **Enforce Role Based Access Controls (RBAC):** Assign roles to control who can manage groups.
 - RBAC reduces the risk of privilege misuse and simplifies group management.
 - For more information, see [Overview of role-based access control in Microsoft Entra ID](#)

Related content

- [Create and manage Microsoft Entra groups and group membership](#)
- [Manage access to SaaS apps using groups](#)
- [Manage rules for dynamic membership groups](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Quickstart: Create a group with members and view all groups and members

Article • 04/25/2025

In this quickstart, you set up a new group, assign members to the group, and review its membership. You can use the user and group you create here in other quickstarts and tutorials.

You can view your organization's existing groups and group members using the Microsoft Entra admin center. Groups are used to manage users that all need the same access and permissions for potentially restricted apps and services.

Prerequisites

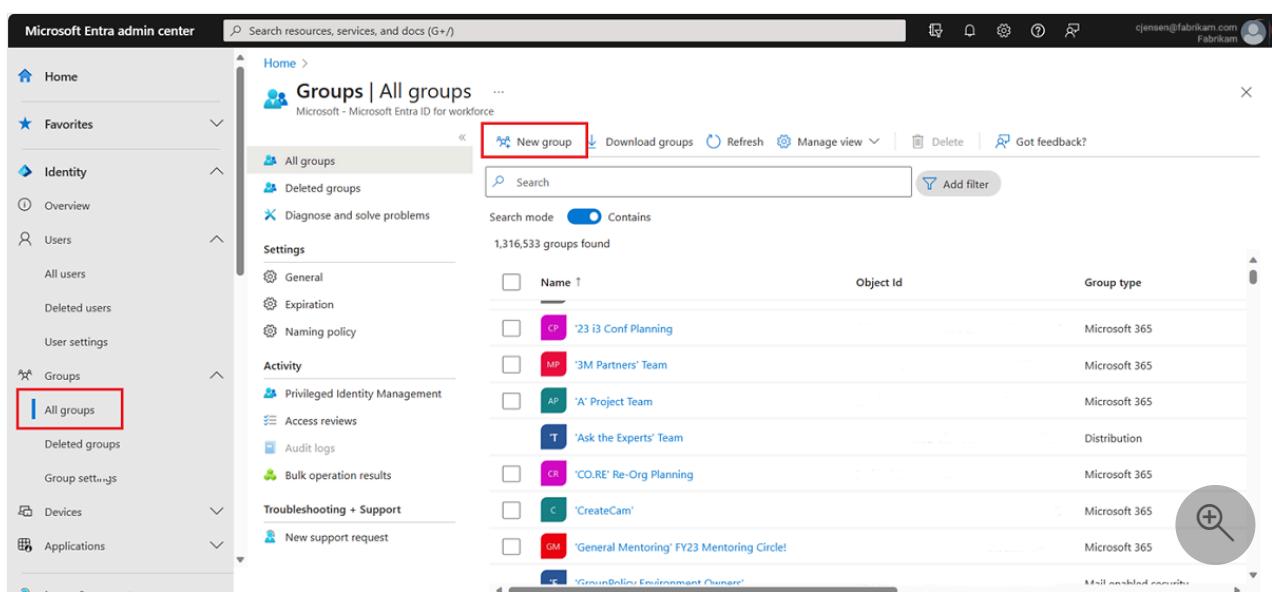
Before you begin, you need:

- An Azure subscription. If you don't have one, create a [free account](#).
- Access to a Microsoft Entra tenant. For more information, see [Create a new tenant](#).

Create a new group

Create a new group, named *MDM policy - West*. For more information about creating a group, see [How to create a basic group and add members](#).

1. Sign in to the [Microsoft Entra admin center](#) as at least a [User Administrator](#).
2. Browse to [Entra ID > Groups > All groups](#).



The screenshot shows the Microsoft Entra admin center interface. The left sidebar has a 'Groups' section with 'All groups' selected, indicated by a red box. The main content area is titled 'Groups | All groups' and shows a list of groups. At the top of this list, there is a 'New group' button, also highlighted with a red box. The list includes several groups such as '23 i3 Conf Planning', '3M Partners' Team', 'A Project Team', 'Ask the Experts' Team', 'CO.RE' Re-Org Planning', 'CreateCam', 'General Mentoring' FY23 Mentoring Circle!', and 'GroundOnline Environment Owners'. A search bar and filter options are visible at the top of the list.

3. Select **New group**.

4. Complete the options in the **Group** page:

- **Group name:** Type *MDM policy - West*
- **Membership type:** Select *Assigned*.

Home > Groups | All groups >

New Group

Got feedback?

Group type
Microsoft 365

Group name * ⓘ
MDM policy - West

Group email address * ⓘ
Enter the local part of the email address @microsoft.onmicrosoft.com

Group description ⓘ
Enter a description for the group

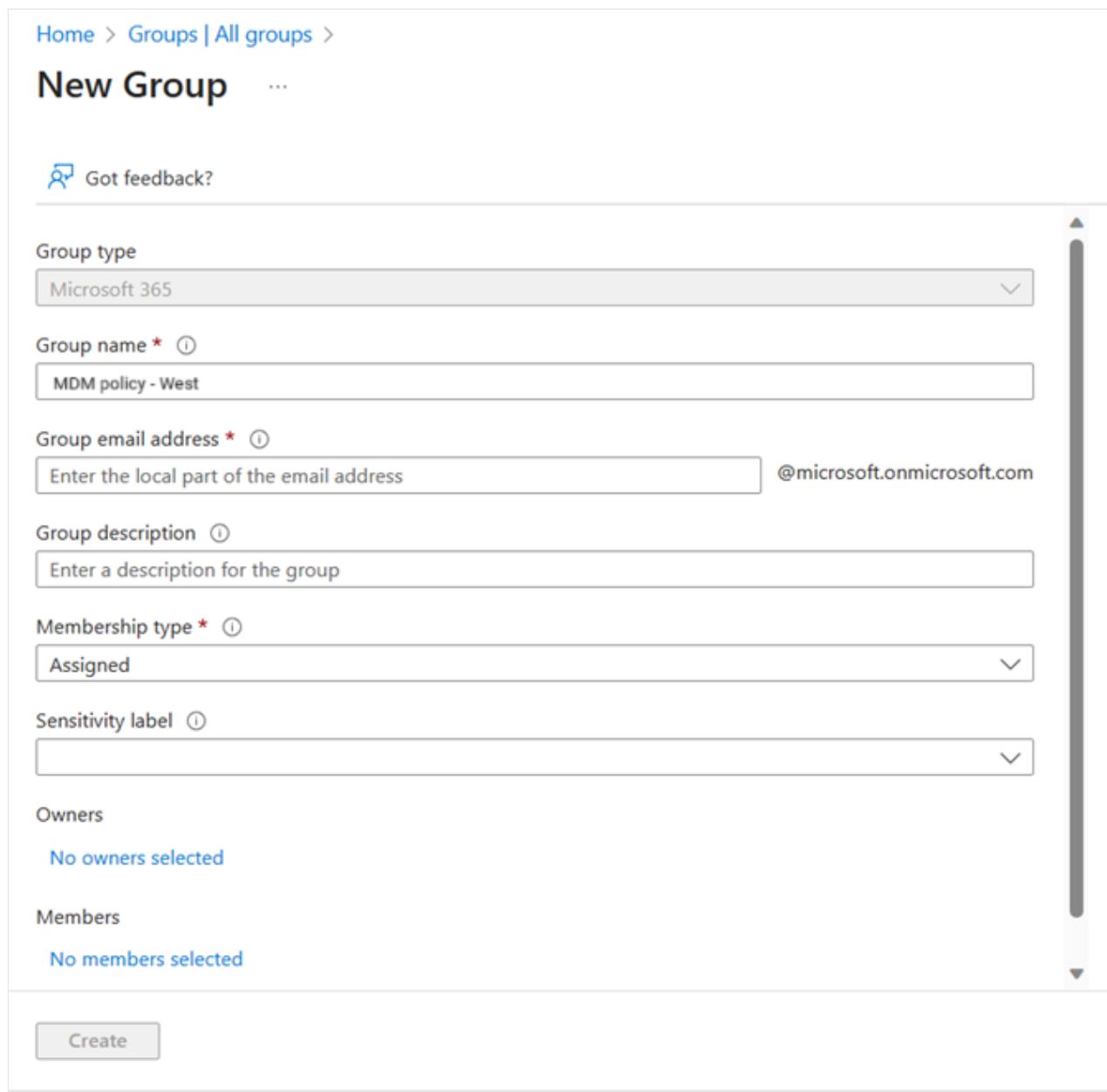
Membership type * ⓘ
Assigned

Sensitivity label ⓘ

Owners
No owners selected

Members
No members selected

Create



5. Select **Create**.

Create a new user

A user must exist before being added as a group member, so you need to create a new user. For this quickstart, we added a user named *Alain Charon*. Check the "Custom domain names" tab first to get the verified domain name in which to create users. For more information about creating a user, see [How to add or delete users](#).

1. Browse to Entra ID > Users.

2. Select New user > Create new user.

The screenshot shows the Microsoft Entra admin center interface. At the top, it says "Microsoft Entra admin center". Below that is a breadcrumb trail "Home > Users". On the left, there's a sidebar with icons for "All users", "Audit logs", "Sign-in logs", and "Diagnose and solve problems". In the main area, there's a search bar and a "New user" button with a dropdown arrow. A red box highlights the "Create new user" option under the "New user" dropdown, which is described as "Create a new internal user in your organization". Below this are other options: "Invite external user" (described as "Invite an external user to collaborate with your organization").

3. Complete the User page:

- **User principal name:** Type *alain@contoso.com*.
- **Display name:** Type *Alain Charon*.

4. Copy the autogenerated password provided in the **Password** box and select **Create**.

Add a group member

Now that you have a group and a user, you can add *Alain Charon* as a member to the *MDM policy - West* group. For more information about adding group members, see the [Manage groups](#) article.

1. Browse to Entra ID > Groups > All groups.
2. Select the MDM policy - West group created earlier.
3. From the MDM policy - West Overview page, select Members.
4. Select Add members, and then search and select Alain Charon.
5. Choose Select.

View all groups

You can see all the groups for your organization in the Groups - All groups page.

- Browse to Entra ID > Groups > All groups.

The All groups page appears, showing all your active groups.

The screenshot shows the 'Groups | All groups' page in Microsoft Entra ID. The left sidebar includes links for 'All groups', 'Deleted groups', 'Diagnose and solve problems', 'Settings' (General, Expiration, Naming policy), 'Activity' (Privileged Identity Management, Access reviews, Audit logs, Bulk operation results), and 'Troubleshooting + Support'. The main area has a search bar with 'Search mode' set to 'Contains' and a dropdown for 'Search mode'. A table lists 15 groups found, with columns for 'Name', 'Object Id', and 'Group type'. The groups listed are: All Company (AC), All Employees (AF), All Users (AU), Business Development, Contoso (C), and Executives (E). The 'All Company' group is selected.

Name	Object Id	Group type
All Company (AC)		Microsoft 365
All Employees (AF)		Distribution
All Users (AU)		Security
Business Development		Microsoft 365
Contoso (C)		Microsoft 365
Executives (E)		Distribution

Search for a group

Search the **All groups** page to find the **MDM policy – West** group.

1. Browse to **Entra ID > Groups > All groups**.
2. From the **All groups** page, type **MDM** into the **Search** box.

The search results appear under the **Search** box, including the **MDM policy - West** group.

The screenshot shows the 'Groups | All groups' page in Microsoft Entra ID. The search bar contains 'MDM'. One group, 'MDM policy – West', is listed in the results table. The table has columns for 'Name', 'Object Id', and 'Group type'. The 'MDM policy – West' group is highlighted with a red box.

Name	Object Id	Group type
MDM policy – West (MP)		Security

3. Select the group **MDM policy – West**.
4. View the group info on the **MDM policy - West Overview** page, including the number of members of that group.

MDM policy - West ...

Group

[Overview](#) [Delete](#) | [Got feedback?](#)

MDM policy - West

MP

Properties

Members **Owners** **Roles and administrators** **Administrative units** **Group memberships** **Applications** **Licenses** **Azure role assignments**

Activity

[Access reviews](#) [Audit logs](#) [Bulk operation results](#)

Troubleshooting + Support

[New support request](#)

Membership type: Assigned

Source: Cloud

Type: Security

Object Id:

Created at: 11/25/2020, 12:32:42 PM

Direct members: 40 Total 20 User(s) 0 Group(s) 20 Device(s) 0 Other(s)

Group memberships	Owners	Total members
User 0	User 2	User 0

View group members

Now that you found the group, you can view all the assigned members.

Select **Members** from the **Manage** area, and then review the complete list of member names assigned to that specific group, including *Alain Charon*.

The screenshot shows the 'MDM policy – West' group members page. The left sidebar has 'Overview' and 'Diagnose and solve problems' under 'Manage'. The 'Members' option is selected. The main area shows 'Direct members' and 'All members' tabs, with a search bar and filter button. A table lists three users:

	Name	Type	Email	User type
<input type="checkbox"/>	AC Alain Charon	User		Member
<input type="checkbox"/>	DM Danielle McKay	User		Member
<input type="checkbox"/>	ES Eggert Schafer	User		Member

Clean up resources

The group you just created is used in other articles in this documentation. If you'd rather not use this group, you can delete it and its assigned members using the following steps:

1. Browse to **Entra ID > Groups > All groups**.
2. On the **All groups** page, search for the **MDM policy - West** group.
3. Select the **MDM policy - West** group.

The **MDM policy - West Overview** page appears.

4. Select **Delete**.

The group and its associated members are deleted.

MDM policy - West

Delete Got feedback?

MDM policy - West

Membership type: Assigned

Source: Cloud

Type: Security

Object Id: [redacted]

Created at: 11/25/2020, 12:32:42 PM

Direct members: 40 Total (20 User(s), 0 Group(s), 20 Device(s), 0 Other(s))

Group memberships	Owners	Total members
0	2	0

Important

This doesn't delete the user Alain Charon, just his membership in the deleted group.

To delete your test user: Browse to **Entra ID > Users** select your test user and choose **Delete**.

Next steps

Advance to the next article to learn how to associate a subscription to your directory.

[Associate an Azure subscription](#)

What is group-based licensing in Microsoft Entra ID?

Article • 01/31/2025

ⓘ Note

Starting September 1, 2024, the Microsoft Entra ID Admin Center and the Microsoft Azure portal no longer supports license assignment through their user interfaces. To manage license assignments for users and groups, administrators must use the Microsoft 365 Admin Center. This update is designed to streamline the license management process within the Microsoft ecosystem. This change is limited to the user interface. API and PowerShell access remain unaffected. For detailed guidance on assigning licenses using the Microsoft 365 Admin Center, refer to the following resources:

- [Assign or Unassign Licenses for Users in the Microsoft 365 Admin Center](#)
- [Add Users and Assign Licenses in Microsoft 365](#)
- [Assign Licenses to a Group Using the Microsoft 365 Admin Center](#)

We encourage all administrators to familiarize themselves with the new procedures to ensure a smooth transition. For any further assistance or inquiries, contact our [support team](#).

Microsoft paid cloud services, such as Microsoft 365, Enterprise Mobility + Security, Dynamics 365, and other similar products, require licenses. These licenses are assigned to each user who needs access to these services. To manage licenses, administrators use one of the management portals (Office or Azure) and PowerShell cmdlets. Microsoft Entra ID is the underlying infrastructure that supports identity management for all Microsoft Cloud services. Microsoft Entra ID stores information about license assignment states for users.

Microsoft Entra ID includes group-based licensing, which allows you to assign one or more product licenses to a group. Microsoft Entra ID ensures that the licenses are assigned to all members of the group. Any new members who join the group are assigned the appropriate licenses. When they leave the group, those licenses are removed. This licensing management eliminates the need for automating license management via PowerShell to reflect changes in the organization and departmental structure on a per-user basis.

Licensing requirements

You must have one of the following licenses **for every user who benefits from group-based licensing**:

- Paid or trial subscription for Microsoft Entra ID P1 and higher.
- Paid or trial edition of Microsoft 365 Business Premium or Office 365 Enterprise E3 or Office 365 A3 or Office 365 GCC G3 or Office 365 E3 for GCCH or Office 365 E3 for DOD and higher.

Required number of licenses

For any groups assigned a license, you must also have a license for each unique member. While you don't have to assign each member of the group a license, you must have at least enough licenses to include all of the members. For example, if you have 1,000 unique members who are part of licensed groups in your tenant, you must have at least 1,000 licenses to meet the licensing agreement.

Features

Here are the main features of group-based licensing:

- Licenses can be assigned to any security group in Microsoft Entra ID. Security groups can be synced from on-premises, by using [Microsoft Entra Connect](#). You can also create security groups directly in Microsoft Entra ID (also called cloud-only groups), or automatically via the [Microsoft Entra dynamic group feature](#).
- When a product license is assigned to a group, the administrator can disable one or more service plans in the product. Typically, this assignment is done when the organization isn't yet ready to start using a service included in a product. For example, the administrator might assign Microsoft 365 to a department, but temporarily disable the Yammer service.
- All Microsoft Cloud services that require user-level licensing are supported. This support includes all Microsoft 365 products, Enterprise Mobility + Security, and Dynamics 365.
- Group-based licensing is currently available through the [Azure portal](#) and through the [Microsoft Admin center](#).
- Microsoft Entra ID automatically manages license modifications that result from group membership changes. Typically, license modifications are effective within

minutes of a membership change.

- A user can be a member of multiple groups with license policies specified. A user can also have some licenses that were directly assigned, outside of any groups. The resulting user state is a combination of all assigned product and service licenses. If a user is assigned the same license from multiple sources, the license is consumed only once.
- In some cases, licenses can't be assigned to a user. For example, there might not be enough available licenses in the tenant, or conflicting services might have been assigned at the same time. Administrators have access to information about users for whom Microsoft Entra ID couldn't fully process group licenses. They can then take corrective action based on that information.

Your feedback is welcome!

If you have feedback or feature requests, share them with us using the [Microsoft Entra admin forum](#).

Next steps

To learn more about other scenarios for license management through group-based licensing, see:

- [Assigning licenses to a group in Microsoft Entra ID](#)
- [Identifying and resolving license problems for a group in Microsoft Entra ID](#)
- [How to migrate individual licensed users to group-based licensing in Microsoft Entra ID](#)
- [How to migrate users between product licenses using group-based licensing in Microsoft Entra ID](#)
- [Microsoft Entra group-based licensing additional scenarios](#)
- [Licensing PowerShell examples](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)

Identify and resolve license assignment problems for a group in the Microsoft 365 Admin Portal

Article • 03/13/2025

Note

Starting September 1, 2024, the Microsoft Entra ID Admin Center and the Microsoft Azure portal no longer supports license assignment through their user interfaces.

To manage license assignments for users and groups, administrators must use the Microsoft 365 Admin Center. This update is designed to streamline the license management process within the Microsoft ecosystem. This change is limited to the user interface. API and PowerShell access remain unaffected. For detailed guidance on assigning licenses using the Microsoft 365 Admin Center, refer to the following resources:

- [Assign or Unassign Licenses for Users in the Microsoft 365 Admin Center](#)
- [Add Users and Assign Licenses in Microsoft 365](#)
- [Assign Licenses to a Group Using the Microsoft 365 Admin Center](#)

We encourage all administrators to familiarize themselves with the new procedures to ensure a smooth transition. For any further assistance or inquiries, contact our [support team](#).

Group-based licensing (GBL) in Microsoft 365 Admin Portal, introduces the concept of users in a licensing error state. This article explains the reasons why users might end up in this state.

When you assign licenses directly to individual users or using group-based licensing (or both), the assignment operation might fail for reasons that are related to business logic.

Some example issues include but aren't limited to:

- An insufficient number of licenses
- Conflict between two service plans that can't be assigned at the same time
- Service plans in one license depend on service plans from another license

Find license assignment errors on users members of a group when using group based licensing

When you're using group-based licensing, these errors happen in the background while the service is assigning licenses. For this reason, the errors can't be communicated to you immediately. Instead, they're recorded on the user object within the group. The original intent to license the user is never lost, but is recorded in an error state for future investigation and resolution. You can also [use audit logs to monitor group-based licensing activity](#).

To find Users in an error state within a group

1. Sign in to the [Microsoft 365 Admin Portal](#) as at least a [License Administrator](#).
2. Browse to **Billing > Licenses** to open a page where you can see and manage all license products in the organization.
3. Select the affected license and to view the status of each group assigned to the selected license navigate to the group selection option.

The screenshot shows the Microsoft 365 Admin Portal interface. At the top, there's a breadcrumb navigation: Home > Licenses > License details. Below that is a 'Back to Licenses' link. The main title is 'Microsoft 365 E5 (no Teams)'. A message indicates 'You own at least 1 subscription for this product.' with a link to 'Manage subscription details'. Under the title, there's a section for 'Licenses' showing 'Licenses assigned' (25 / 25) with a progress bar. Below this, there are tabs for 'Users' and 'Groups', with 'Groups' being the active tab. A note below the tabs says 'Assign and manage group licenses.' followed by a link to 'Learn how to assign licenses to groups.'. At the bottom, there are two buttons: '+ Assign licenses' and a 'Refresh' button with a circular arrow icon.

4. A notification appears if there are any users of the group in an error state. The status of license assignment for each group would be one of the following values:
 - All licenses Assigned – no issues

- **In progress** – pending assignment of licenses to users
- **Errors and issues** – need to investigate

Assign and manage group licenses. [Learn how to assign licenses to groups.](#)

+ Assign licenses Refresh

<input type="checkbox"/>	Name ↑	Status
<input type="checkbox"/>	Teams calling plan	Errors and issues
<input type="checkbox"/>	Test for Training	All licenses assigned

5. Select the **group name** to review errors for the affected users in the group.
6. You can also filter the errors using the **Filter** option on the top right if you have a large number of affected users.

Action needed Sucessfully assigned

Filter Search

Clear filter

- Not enough licenses
- Missing dependent service plans
- Conflicting service plans
- User usage location not specified
- Duplicate proxy address
- Other

<input type="checkbox"/>	User	Status
<input type="checkbox"/>	user5	Not enough licenses
<input type="checkbox"/>	user21	Conflicting service plans
<input type="checkbox"/>	User20	Not enough licenses
<input type="checkbox"/>	User19	Not enough licenses
<input type="checkbox"/>	user22	Conflicting service plans
<input type="checkbox"/>	User7	Not enough licenses

The following sections give a description of each potential problem and ways to try resolving it.

Note

Azure AD and MSOnline PowerShell modules are deprecated as of March 30, 2024.

To learn more, read the [deprecation update](#). After this date, support for these modules are limited to migration assistance to Microsoft Graph PowerShell SDK and security fixes. The deprecated modules will continue to function through March, 30 2025.

We recommend migrating to [Microsoft Graph PowerShell](#) to interact with Microsoft Entra ID (formerly Azure AD). For common migration questions, refer to the [Migration FAQ](#). Note: Versions 1.0.x of MSOnline may experience disruption after June 30, 2024.

Not enough licenses

Problem: There aren't enough available licenses for one of the products specified in the group. You need to either purchase more licenses for the product or free up unused licenses from other users or groups.

To see how many licenses are available, go to the [Entra Admin Portal](#) > **Billing** > **Licenses** > **All products**.

Name	Total	Assigned	Available	Expiring Soon
Microsoft Power Automate Free	10,000	6	9,994	0
Microsoft Fabric (Free)	1,000,000	4	999,996	0

To see which users and groups are consuming licenses, navigate to the [M365 Admin portal](#) under **Billing** > **Licenses** and select a product. Under **Users**, you see a list of all users who have licenses assigned directly or via one or more groups. Under **Groups**, you see all groups that have that product assigned.

Conflicting service plans

Problem: One of the products specified in the group contains a service plan that conflicts with another service plan already assigned to the user via a different product. Some service plans are configured in a way that they can't be assigned to the same user as another related service plan. The decision about how to resolve conflicting product licenses always belongs to the administrator. Microsoft Entra ID doesn't automatically resolve license conflicts. **PowerShell:** PowerShell cmdlets report this error as **MutuallyExclusiveViolation**. **Audit log Details:**

Licensing Error Message

License assignment failed because service plans
[xxxxxxxxxxxxxxxxxxxxxxxxxxxxx], [xxxxxxxxxxxxxxxxxxxxxxxxxxxxx] are
mutually exclusive.

Missing dependent service plans

Problem: One of the products specified in the group contains a service plan that must be enabled for another service plan, in another product, to function. This error occurs when Microsoft Entra ID attempts to remove the underlying service plan. For example, this problem can happen when you remove the user from the group. To solve this problem, you need to make sure that the required plan is still assigned to users through some other method or that the dependent services are disabled for those users. After doing that, you can properly remove the group license from those users.

PowerShell: PowerShell cmdlets report this error as DependencyViolation.

Audit log Details:

Licensing Error Message

License assignment failed because service plan
[xxxxxxxxxxxxxxxxxxxxxxxxxxxxx] depends on
the service plan(s) [xxxxxxxxxxxxxxxxxxxxxxxxxxxxx],
[xxxxxxxxxxxxxxxxxxxxxxxxxxxxx].

Usage location not specified

Problem: Some Microsoft services aren't available in all locations because of local laws and regulations. Before you can assign a license to a user, you must specify the Usage location property for the user. You can specify the location under the User > Profile > Edit section in the portal. When Microsoft Entra ID attempts to assign a group license to a user in an unsupported usage location, it fails. The system records an error on the user. To solve this problem, remove users from unsupported locations from the licensed group. If the current usage location values don't represent the actual user location, you can modify them so licenses are correctly assigned next time (if the new location is supported).

PowerShell: PowerShell cmdlets report this error as ProhibitedInUsageLocationViolation.

Note

When Microsoft Entra ID assigns group licenses, any users without a specified usage location inherit the location of the directory. Microsoft recommends that administrators set the correct usage location values on users before using group-based licensing to comply with local laws and regulations. - The attributes of First name, Last name, Other email address, and User type aren't mandatory for license assignment.

Duplicate proxy addresses

Problem: If you use Exchange Online, some users in your organization might be incorrectly configured with the same proxy address value. When group-based licensing tries to assign a license to such a user, it fails and shows "Proxy address is already being used".

Tip

To see if there's a duplicate proxy address, execute the following PowerShell cmdlet against Exchange Online:

PowerShell

```
Get-Recipient -Filter "EmailAddresses -eq 'user@contoso.onmicrosoft.com'" |  
fl DisplayName, RecipientType, Emailaddresses
```

For more information about this problem, see [Proxy address is already being used ↗](#) error message in Exchange Online.

Other

Other errors are typically the result of an error with another license assigned by the same group.

Error type

Other

Error details

Something went wrong when we tried to assign this license.

To identify the other licensing assigned to the affected user from the same group, you can review the user licenses from the Microsoft Entra Admin Portal.

In the **Entra Admin Portal**, navigate to **Users – All Users** – locate the affected user and then review their **Licenses**.

You can review the user's audit logs for more information about the error as long as the error occurred in the last 30 days in most cases (depending on the number of days Audit logs available in the tenant, some may have only seven days)

Audit log License Assignment Error Records can be identified using the following details:

Activity Type: Change user license

Status: failure

Initiated by (actor)

- **Type:** Application
- **Display Name:** Microsoft Entra ID Group-Based Licensing

Force user license processing to resolve errors

Problem: Depending on what steps you took to resolve the errors, it might be necessary to manually trigger the processing of a user to update the users state.

For example, after you resolve a dependency violation error for an affected user, you need to trigger the reprocessing of the user. To reprocess a user, navigate back to the **M365 Admin Portal > Billing > Licenses**. Select the license and navigate to the group where one or more affected users show in error, select the user(s) and then select the **Reprocess** button on the toolbar.

Alternately, you can use Graph for PowerShell [Invoke-MgLicenseUser](#) to reprocess users.

More than one product license assigned to a group

You can assign more than one product license to a group. For example, you can assign Office 365 Enterprise E3 and Enterprise Mobility + Security to a group to easily enable all included services for users.

Problem: Group based licensing processing attempts to assign all specified licenses in the group to each user within the group. However, if the processing of the licenses encounters issues such as insufficient licenses or conflicts with other services enabled, it doesn't assign other licenses in the group either. You need to check which users have license assignment failures and which products are affected. If a problem occurs during license assignment, the process may not complete. For example, issues like insufficient licenses or service plans that can't be assigned at the same time, would prevent the process from finishing.

When a licensed group is deleted

Problem: You must remove all licenses assigned to a group before you can delete the group. However, removing licenses from all the users in the group may take time. When an administrator removes license assignments from a group, there can be failures if user has a dependent license assigned or if there's a proxy address conflict issue that prevents the license removal. If a user has a license assigned dependent on a license being removed due to group deletion, all licenses assigned by the deleted group enter an error state on the affected user and it can't be removed until the dependency is resolved. Once the dependency is resolved, you need to reprocess the user licensing using Graph for PowerShell.

Manage licenses for products with prerequisites

Some Microsoft Online products you might own have prerequisites. These include add-ons and other service plans which may require a prerequisite service plan to be enabled on a user or a group before the dependent service plans can be added to the user or group. With group-based licensing, the system requires that both the prerequisite and add-on service plans or other dependent service plans be present in the same group. This requirement exists to ensure that any users who are added to the group can receive the fully working product. Let's consider the following example: Microsoft Workplace Analytics is an add-on product. It contains a single service plan with the same name. You

can only assign this service plan to a user, or group, when one of the following prerequisites is also assigned:

- Exchange Online (Plan 1)
- Exchange Online (Plan 2)

Problem: If you try to assign this product on its own to a group, the portal returns a notification message. To assign this add-on license to a group, you must ensure that the group contains the prerequisite service plan. It's also possible to create a standalone group that contains only the minimum required products to make the add-on work. It can be used to license only selected users for the add-on product. Based on the previous example, you would assign the following products to the same group:

- Office 365 Enterprise E3 with only the Exchange Online (Plan 2) service plan enabled
- Microsoft Workplace Analytics

From now on, any users added to this group consume one license of the E3 product and one license of the Workplace Analytics product. At the same time, those users can be members of another group that gives them the full E3 product, and they still consume only one license for that product.

Tip

You can create multiple groups for each prerequisite service plan. For example, if you use both Office 365 Enterprise E1 and Office 365 Enterprise E3 for your users, you can create two groups to license Microsoft Workplace Analytics: one that uses E1 as a prerequisite and the other that uses E3. This approach lets you distribute the add-on to E1 and E3 users without consuming other licenses.

License removal of dynamic membership groups with rules based on licenses with an initial static group

This error occurs because users are added and removed from another batch of dynamic membership groups. The cascading setup of dynamic membership groups, with rules based on licenses in an initial static group, creates this issue. This error can affect multiple dynamic membership groups and demands extensive reprocessing to restore access.

Warning

When you change an existing static group to a dynamic group, all existing members are removed from the group, and then the membership rule is processed to add new members. If the group is used to control access to apps or resources, the original members might lose access until the membership rule is fully processed.

We recommend that you test the new membership rule beforehand to make sure that the new membership in the group is as expected. If you encounter errors during your test, see [Use audit logs to monitor group-based licensing activity](#).

Microsoft Entra ID Mail and ProxyAddresses attribute change

Problem: While updating license assignment on a user or a group, you might see that the Mail and ProxyAddresses attribute of some users are changed. Updating license assignment on a user causes the proxy address calculation to be triggered, which can change user attributes. To understand the exact reason of the change and solve the problem, see [this article](#) on how the proxyAddresses attribute is populated in Microsoft Entra ID.

Next steps

To learn more about other scenarios for license management through groups, see:

- [What is group-based licensing in Microsoft Entra ID?](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Microsoft Entra ID preview program information

Article • 12/18/2024

Microsoft Entra ID may include preview, beta, or other prerelease features, services, software, or regions offered by Microsoft to obtain customer feedback ("Previews"). Previews are made available to you under the terms applicable to previews, which are outlined in the overall Microsoft product terms for [online services](#).

Microsoft may roll out previews in phases to give Microsoft and customers the opportunity to evaluate and understand potential new features.

Note

Not all features that are in preview become generally available. While it isn't the norm, it is possible that Microsoft might cancel features during preview.

The phases may include:

1. **Private preview** – during this phase we invite a few customers to take part in early access to new concepts and features. This phase doesn't include formal support.
2. **Public preview** – during this phase we allow any customer with the proper Microsoft Entra ID license to evaluate the new feature. Public previews may include limited customer support and normal service level agreements don't apply. For new features exposed in the Microsoft Entra admin center, customers can expect to see information banners in the user interface that draw attention to the new experience available during the preview. By clicking on the information banner customers then opt in to the preview experience.
3. **Generally available (GA)** – during this phase, the feature is open for any licensed customer to use and is supported via all Microsoft support channels. Be aware when a new feature impacts existing functionality, it might change the way you or your users use the functionality.

Each Microsoft Entra ID preview program may have different opt-in requirements and dependencies.

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback 

Microsoft Entra licensing

Article • 03/05/2025

This article discusses licensing options for the Microsoft Entra product family. It's intended for security decision makers, identity and network access administrators, and IT professionals who are considering Microsoft Entra solutions for their organizations.

Microsoft Entra licensing options

Microsoft Entra is available in several licensing options that allow you to choose the package best suited to your needs.

ⓘ Note

The licensing options on this page aren't comprehensive. You can get detailed information about the various options at the [Microsoft Entra pricing page](#) and at the [Compare Microsoft 365 Enterprise plans and pricing page](#).

Microsoft Entra ID Free - Included with Microsoft cloud subscriptions such as Microsoft Azure, Microsoft 365, and others.

Microsoft Entra ID P1 - Microsoft Entra ID P1 is available as a standalone product or included with Microsoft 365 E3 for enterprise customers and Microsoft 365 Business Premium for small to medium businesses.

Microsoft Entra ID P2 - Microsoft Entra ID P2 is available as a standalone product or included with Microsoft 365 E5 for enterprise customers.

Microsoft Entra Suite - The suite combines Microsoft Entra products to secure access for your employees. It allows administrators to provide secure access from anywhere to any app or resource whether cloud or on-premises, while ensuring least privilege access. A Microsoft Entra ID P1 subscription is required. The Microsoft Entra suite includes five products:

- Microsoft Entra Private Access
- Microsoft Entra Internet Access
- Microsoft Entra ID Governance
- Microsoft Entra ID Protection
- Microsoft Entra Verified ID (premium capabilities)

ⓘ Important

User and group license assignments are managed through the Microsoft 365 Admin Center. For more information on how to assign or unassign licenses to users and groups, see this article: - [Assign or unassign licenses for users in the Microsoft 365 admin center](#)

App provisioning

Microsoft Entra application proxy requires Microsoft Entra ID P1 or P2 licenses. For more information about licensing, see [Microsoft Entra pricing](#).

Authentication

The following table lists features that are available for authentication in the various versions of Microsoft Entra ID. Plan out your needs for securing user sign-in, then determine which approach meets those requirements. For example, although Microsoft Entra ID Free provides security defaults with multifactor authentication, only Microsoft Authenticator can be used for the authentication prompt, including text and voice calls. This approach might be a limitation if you can't make sure that Authenticator is installed on a user's personal device.

 Expand table

Feature	Microsoft Entra ID Free - Security defaults (enabled for all users)	Microsoft Entra ID Free - Global Administrators only	Office 365	Microsoft Entra ID P1	Microsoft Entra ID P2
Protect Microsoft Entra tenant admin accounts with MFA	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (Microsoft Entra Global Administrator accounts only)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Mobile app as a second factor	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Phone call as a second factor			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
SMS as a second factor		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Admin control over verification methods		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Fraud alert				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
MFA Reports				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Feature	Microsoft Entra ID Free - Security defaults (enabled for all users)	Microsoft Entra ID Free - Global Administrators only	Office 365	Microsoft Entra ID P1	Microsoft Entra ID P2
Custom greetings for phone calls			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Custom caller ID for phone calls			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Trusted IPs			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Remember MFA for trusted devices		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
MFA for on- premises applications			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Conditional Access			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Risk-based Conditional Access				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Self-service password reset (SSPR)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
SSPR with writeback			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Managed identities

There are no licensing requirements for using Managed identities for Azure resources. Managed identities for Azure resources provide an automatically managed identity for applications to use when connecting to resources that support Microsoft Entra authentication. One of the benefits of using managed identities is that you don't need to manage credentials, and they can be used at no extra cost. For more information, see [What is managed identities for Azure resources?](#).

Microsoft Entra ID Governance

The following table shows the licensing requirements for Microsoft Entra ID Governance features. Microsoft Entra Suite includes all features of Microsoft Entra ID Governance. Licensing

information and example license scenarios for Entitlement management, Access reviews, and Lifecycle Workflows are provided following the table.

Features by license

The following table shows what features are available with each license. Not all features are available in all clouds; see [Microsoft Entra feature availability](#) for Azure Government.

 Expand table

Feature	Free	Microsoft Entra ID P1	Microsoft Entra ID P2	Microsoft Entra ID Governance	Microsoft Entra Suite
API-driven provisioning					
HR-driven provisioning					
Automated user provisioning to SaaS apps					
Automated group provisioning to SaaS apps					
Automated provisioning to on-premises apps					
Conditional Access - Terms of use attestation					
Entitlement management - Capabilities previously generally available in Microsoft Entra ID P2					
Entitlement management - Conditional Access Scoping					
Entitlement management MyAccess Search					
Entitlement management with Verified ID					
Entitlement management - Custom Extensions (Logic Apps)					
Entitlement management - Auto Assignment Policies					
Entitlement management - Directly Assign Any User					

Feature	Free	Microsoft Entra ID P1	Microsoft Entra ID P2	Microsoft Entra ID Governance	Microsoft Entra Suite
(Preview)					
Entitlement management - Mark guest as governed				✓	✓
Entitlement management - Manage the lifecycle of external users			✓	✓	✓
My Access portal		✓		✓	✓
Entitlement management - Microsoft Entra Roles (Preview)				✓	✓
Entitlement management - Request access packages on-behalf-of (Preview)			✓		✓
Entitlement management - Sponsors Policy			✓		✓
Privileged Identity Management (PIM)		✓		✓	✓
PIM For Groups		✓		✓	✓
PIM Conditional Access Controls		✓		✓	✓
Access reviews - Capabilities previously generally available in Microsoft Entra ID P2		✓		✓	✓
Access reviews - PIM For Groups (Preview)			✓		✓
Access reviews - Inactive Users reviews			✓		✓
Access Reviews - Inactive Users recommendations		✓		✓	✓
Access reviews - Machine learning assisted access certifications and reviews			✓		✓
Lifecycle Workflows (LCW)			✓		✓
LCW + Custom Extensions (Logic Apps)			✓		✓

Feature	Free	Microsoft Entra ID P1	Microsoft Entra ID P2	Microsoft Entra ID Governance	Microsoft Entra Suite
Identity governance dashboard	<input checked="" type="checkbox"/>				
Insights and reporting - Inactive guest accounts				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Entitlement Management

Using this feature requires Microsoft Entra ID Governance subscriptions for your organization's users. Some capabilities within this feature can operate with a Microsoft Entra ID P2 subscription.

Example license scenarios

Here are some example license scenarios to help you determine the number of licenses you must have.

[+] Expand table

Scenario	Calculation	Number of licenses
An Identity Governance Administrator at Woodgrove Bank creates initial catalogs. One of the policies specifies that All employees (2,000 employees) can request a specific set of access packages. 150 employees request the access packages.	2,000 employees who can request the access packages	2,000
An Identity Governance Administrator at Woodgrove Bank creates initial catalogs. They create an auto-assignment policy that grants All members of the Sales department (350 employees) access to a specific set of access packages. 350 employees are auto-assigned to the access packages.	350 employees need licenses.	351

Access reviews

Using this feature requires Microsoft Entra ID Governance subscriptions for your organization's users, including for all employees who are reviewing access or having their access reviewed. Some capabilities within this feature might operate with a Microsoft Entra ID P2 subscription.

Example license scenarios

Here are some example license scenarios to help you determine the number of licenses you must have.

[+] [Expand table](#)

Scenario	Calculation	Number of licenses
An administrator creates an access review of Group A with 75 users and 1 group owner, and assigns the group owner as the reviewer.	1 license for the group owner as reviewer, and 75 licenses for the 75 users.	76
An administrator creates an access review of Group B with 500 users and 3 group owners, and assigns the 3 group owners as reviewers.	500 licenses for users, and 3 licenses for each group owner as reviewers.	503
An administrator creates an access review of Group B with 500 users. Makes it a self-review.	500 licenses for each user as self-reviewers	500
An administrator creates an access review of Group C with 50 member users. Makes it a self-review.	50 licenses for each user as self-reviewers.	50
An administrator creates an access review of Group D with 6 member users. Makes it a self-review.	6 licenses for each user as self-reviewers. No additional licenses are required.	6

Lifecycle Workflows

With Microsoft Entra ID Governance licenses for Lifecycle Workflows, you can:

- Create, manage, and delete workflows up to the total limit of 50 workflows.
- Trigger on-demand and scheduled workflow execution.
- Manage and configure existing tasks to create workflows that are specific to your needs.
- Create up to 100 custom task extensions to be used in your workflows.

Using this feature requires Microsoft Entra ID Governance subscriptions for your organization's users.

Example license scenarios

[+] [Expand table](#)

Scenario	Calculation	Number of licenses
A Lifecycle Workflows Administrator creates a workflow to add new hires in the Marketing department to the Marketing teams group. 250 new hires are assigned to the Marketing teams group via this workflow once. Other 150 new hires are assigned to the Marketing teams group via this workflow later the same year.	1 license for the Lifecycle Workflows Administrator, and 400 licenses for the users.	401
A Lifecycle Workflows Administrator creates a workflow to pre-offboard a group of employees before their last day of employment. The scope of users who will be pre-offboarded are 40 users once. We offboard 40 licensed users. Now, we can re-assign these 40 licenses and assign 10 more licenses later in the year to pre-offboard 50 more users.	50 licenses for users, and 1 license for the Lifecycle Workflows Administrator.	51

Microsoft Entra Connect

Using this feature is free and included in your Azure subscription.

Microsoft Entra Connect Health

Using this feature requires Microsoft Entra ID P1 licenses. To find the right license for your requirements, see [Compare generally available features of Microsoft Entra ID](#).

Microsoft Entra Conditional Access

Using this feature requires Microsoft Entra ID P1 licenses. To find the right license for your requirements, see [Compare generally available features of Microsoft Entra ID](#).

Customers with [Microsoft 365 Business Premium licenses](#) also have access to Conditional Access features.

Risk-based policies require access to [Microsoft Entra ID Protection](#), which is a Microsoft Entra ID P2 feature.

Microsoft Entra Suite includes all Microsoft Entra Conditional Access features.

Other products and features that could interact with Conditional Access policies require appropriate licensing for those products and features.

When licenses required for Conditional Access expire, policies aren't automatically disabled or deleted. This grants customers the ability to migrate away from Conditional Access policies.

without a sudden change in their security posture. Remaining policies can be viewed and deleted, but no longer updated.

Security defaults help protect against identity-related attacks and are available for all customers.

Microsoft Entra Domain services

Microsoft Entra Domain Services usage is charged per hour, based on the [SKU ↗](#) selected by the tenant owner.

Microsoft External ID

Microsoft Entra External ID core features are free for your first 50,000 monthly active users. More licensing information is available at the [External ID FAQ ↗](#)

Microsoft Entra ID Protection

Using this feature requires Microsoft Entra ID P2 licenses. To find the right license for your requirements, see [Compare generally available features of Microsoft Entra ID ↗](#).

[] Expand table

Capability	Details	Microsoft Entra ID Free / Microsoft 365 Apps	Microsoft Entra ID P1	Microsoft Entra ID P2	Microsoft Entra Suite
Risk policies	Sign-in and user risk policies (via Conditional Access)	No	No	Yes	Yes
Security reports	Overview	No	No	Yes	Yes
Security reports	Risky users	Limited Information. Only users with medium and high risk are shown. No details drawer or risk history.	Limited Information. Only users with medium and high risk are shown. No details drawer or risk history.	Full access	Yes

Capability	Details	Microsoft Entra ID Free / Microsoft 365 Apps	Microsoft Entra ID P1	Microsoft Entra ID P2	Microsoft Entra Suite
Security reports	Risky sign-ins	Limited Information. No risk detail or risk level is shown.	Limited Information. No risk detail or risk level is shown.	Full access	Yes
Security reports	Risk detections	No	Limited Information. No details drawer.	Full access	Yes
Notifications	Users at risk detected alerts	No	No	Yes	Yes
Notifications	Weekly digest	No	No	Yes	Yes
MFA registration policy		No	No	Yes	Yes

Microsoft Entra Internet Access

[Microsoft Entra Internet Access](#) is available on its own or as part of the Microsoft Entra Suite.

Microsoft Entra monitoring and health

The required licenses vary based on the monitoring and health capability.

[Expand table](#)

Capability	Microsoft Entra ID Free	Microsoft Entra ID P1 or P2 / Microsoft Entra Suite
Audit logs	Yes	Yes
Sign-in logs	Yes	Yes
Provisioning logs	No	Yes
Custom security attributes	Yes	Yes
Health	No	Yes
Microsoft Graph activity logs	No	Yes
Usage and insights	No	Yes

Microsoft Entra Permissions management

Permissions Management supports all resources across Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform but only requires licenses for [billable resources](#).

Microsoft Entra Private Access

[Microsoft Entra Private access](#) is available on its own or as part of the Microsoft Entra Suite.

Microsoft Entra Privileged Identity Management

To use Microsoft Entra Privileged Identity Management, a tenant must have a valid license. Licenses must also be assigned to the administrators and relevant users. This article describes the license requirements to use Privileged Identity Management. To use Privileged Identity Management, you must have one of the following licenses:

Valid licenses for PIM

You need either Microsoft Entra ID Governance licenses or Microsoft Entra ID P2 licenses to use PIM and all of its settings. Currently, you can scope an access review to service principals with access to Microsoft Entra ID, resource roles with a Microsoft Entra ID P2 or users with Microsoft Entra ID Governance edition active in your tenant.

Licenses you must have for PIM

Ensure that your directory has Microsoft Entra ID P2 or Microsoft Entra ID Governance licenses for the following categories of users:

- Users with eligible and/or time-bound assignments to Microsoft Entra ID or Azure roles managed using PIM
- Users with eligible and/or time-bound assignments as members or owners of PIM for Groups
- Users able to approve or reject activation requests in PIM
- Users assigned to an access review
- Users who perform access reviews

Example license scenarios for PIM

Here are some example license scenarios to help you determine the number of licenses you must have.

Scenario	Calculation	Number of licenses
Woodgrove Bank has 10 administrators for different departments and 2 Privileged Role Administrators that configure and manage PIM. They make five administrators eligible.	Five licenses for the administrators who are eligible	5
Graphic Design Institute has 25 administrators of which 14 are managed through PIM. Role activation requires approval and there are three different users in the organization who can approve activations.	14 licenses for the eligible roles + three approvers	17
Contoso has 50 administrators of which 42 are managed through PIM. Role activation requires approval and there are five different users in the organization who can approve activations. Contoso also does monthly reviews of users assigned to administrator roles and reviewers are the users' managers of which six aren't in administrator roles managed by PIM.	42 licenses for the eligible roles + five approvers + six reviewers	53

When a license expires for PIM

If a Microsoft Entra ID P2, Microsoft Entra ID Governance, or trial license expires, Privileged Identity Management features are no longer available in your directory:

- Permanent role assignments to Microsoft Entra roles are unaffected.
- The Privileged Identity Management service in the Microsoft Entra admin center, and the Graph API cmdlets and PowerShell interfaces of Privileged Identity Management, will no longer be available for users to activate privileged roles, manage privileged access, or perform access reviews of privileged roles.
- Eligible role assignments of Microsoft Entra roles are removed, as users no longer be able to activate privileged roles.
- Any ongoing access reviews of Microsoft Entra roles ends, and Privileged Identity Management configuration settings are removed.
- Privileged Identity Management no longer sends emails on role assignment changes.

Microsoft Entra Verified ID

Microsoft Entra Verified ID is included with any Microsoft Entra ID subscription, including Microsoft Entra ID free, at no extra cost. Core Verified ID functionality help organizations:

- Verify and issue organizational credentials for any unique identity attributes.

- Empower end-users with ownership of their digital credential and greater visibility
- Reduce organizational risk and simplify the audit process
- Create user-centric, serverless apps that use Verified ID credentials.

Microsoft Entra Verified ID also provides Face Check as a premium feature available as an add-on and included in the Microsoft Entra Suite (limited to 8 Face Checks per user per month).

Microsoft Entra Workload ID

Microsoft Entra [Workload ID](#) supports application identities and service principles in Azure, requiring licenses per workload identity per month.

Multitenant organizations

In the source tenant: Using this feature requires Microsoft Entra ID P1 licenses. Each user who is synchronized with cross-tenant synchronization must have a P1 license in their home/source tenant. To find the right license for your requirements, see [Microsoft Entra ID Plans & Pricing](#).

In the target tenant: Cross-tenant sync relies on the Microsoft Entra External ID billing model. To understand the external identities licensing model, see [MAU billing model for Microsoft Entra External ID](#). You also need at least one Microsoft Entra ID P1 license in the target tenant to enable autoredemption.

All multitenant organizations features are included as part of Microsoft Entra suite.

Role-based access control

Using built-in roles in Microsoft Entra ID is free. Using custom roles require a Microsoft Entra ID P1 license for every user with a custom role assignment. To find the right license for your requirements, see [Comparing generally available features of the Free and Premium editions](#).

Roles

Administrative units

Using administrative units requires a Microsoft Entra ID P1 license for each administrative unit administrator who is assigned directory roles over the scope of the administrative unit, and a Microsoft Entra ID Free license for each administrative unit member. Creating administrative units is available with a Microsoft Entra ID Free license. If you are using [rules for dynamic membership groups](#) for administrative units, each administrative unit member requires a

Microsoft Entra ID P1 license. To find the right license for your requirements, see [Comparing generally available features of the Free and Premium editions](#).

Restricted management administrative units

Restricted management administrative units require a Microsoft Entra ID P1 license for each administrative unit administrator, and Microsoft Entra ID Free licenses for administrative unit members. To find the right license for your requirements, see [Comparing generally available features of the Free and Premium editions](#).

Features in preview

Licensing information for any features currently in preview is included here when applicable. For more information about preview features, see [Microsoft Entra ID preview features](#).

Next steps

- [Microsoft Entra pricing](#)
- [Azure AD B2C pricing](#)

Sign up for Microsoft Entra ID P1 or P2 editions

Article • 03/05/2025

You can purchase and associate Microsoft Entra ID P1 or P2 editions with your Azure subscription. If you need to create a new Azure subscription, you also need to [activate your licensing plan](#) and your [Microsoft Entra ID service access](#). For information about obtaining a free trial, see [Microsoft Entra ID P2 Trial](#).

Before you sign up for Active Directory Premium 1 or Premium 2, you must first determine which of your existing subscription or plan to use:

- Through your existing Azure or Microsoft 365 subscription.
- Through your Enterprise Mobility + Security licensing plan.
- Through a Microsoft Volume Licensing plan.

Sign up options

When you sign up using your Azure subscription with previously purchased and activated Microsoft Entra ID licenses, automatically activates the licenses in the same directory. If that's not the case, you must still [activate your license plan](#) and your [Microsoft Entra ID service access](#).

Sign up using your existing Azure or Microsoft 365 subscription

As an Azure or Microsoft 365 subscriber, you can purchase the Microsoft Entra ID P1 or P2 editions online. For detailed steps, see [Buy or remove licenses](#).

Sign up using your Enterprise Mobility + Security licensing plan

Enterprise Mobility + Security is a suite, comprised of Microsoft Entra ID P1 or P2, Azure Information Protection, and Microsoft Intune. If you already have a Microsoft Enterprise Mobility + Security license, you can get started with Microsoft Entra ID, using one of these licensing options:

For more information about Microsoft Enterprise Mobility + Security, see [Enterprise Mobility + Security web site](#).

- Join the [Microsoft 365 Developer](#) program and if qualified get a free renewable Microsoft 365 E5 instant sandbox.
- Purchase [Enterprise Mobility + Security E5 licenses](#)
- Purchase [Enterprise Mobility + Security E3 licenses](#)

Sign up using your Microsoft Volume Licensing plan

Through your Microsoft Volume Licensing plan, you can sign up for Microsoft Entra ID P1 or P2 using one of these two programs, based on the number of licenses you want to get:

- For 250 or more licenses, see [Microsoft Enterprise Agreement](#).
- For 5 to 250 licenses, see [Open Volume License](#).
- For more information about volume licensing purchase options, see [How to purchase through Volume Licensing](#).

Activate your new license plan

If you signed up using a new Microsoft Entra ID license plan, you must activate it for your organization, using the confirmation email sent after purchase.

To activate your license plan

1. Open the confirmation email that you received from Microsoft after you signed up.

From: Microsoft Online Services Team [mailto:msonlineservicesteam@officeliveemail.com]
Sent: Friday, March 21, 2014 1:04 PM
To: Microsoft Online Services User
Subject: Action required: Complete your profile to set up your services

Microsoft

Please complete your profile to set up your Microsoft Online Services.

Dear User,

Thank you for purchasing Microsoft Online Services through Microsoft Volume Licensing.

To start using your subscription, please choose one of the following options:

1. USE AN EXISTING ACCOUNT

If you have an existing Microsoft Online Services trial or paid subscription, you already have a Microsoft Online Services ID that was created at the time of sign up.

To preserve your settings and data from this existing account and connect it to your Volume Licensing subscription, select "Sign In." This will connect your existing account to your Volume Licensing Agreement. Once associated, all future Volume Licensing purchases and provisioning must be done on this account.

IMPORTANT NOTE: Before you click "Sign In", please ensure you are not already signed into any other Microsoft Online Service Accounts.

Sign In

2. CREATE A NEW ACCOUNT

If you don't have an existing Microsoft Online Services trial or paid subscription or would not like to preserve your settings and data from a previous account, select "Sign Up" to create a new Microsoft Online Services ID.

Follow the steps to create an account profile. You'll be asked to provide a domain name which will help us create a new Microsoft Online Services ID for your organization. This account will be connected to your Volume Licensing agreement. Once associated, all future Volume Licensing purchases and provisioning must be done on this account.

Sign Up

Thanks again for purchasing Microsoft Online Services.

Sincerely,
The Microsoft Online Services Team

2. Select Sign in or Sign up.

- **Sign in.** Choose this option if you have an existing tenant, and then sign in using your existing administrator account. You must be a Global Administrator on the tenant where the licenses are being activated.
- **Sign up.** Choose this option if you want to open the **Create Account Profile** page and create a new Microsoft Entra tenant for your licensing plan.

When you're done, you'll receive confirmation of activating the license plan for your tenant.

Activate your Microsoft Entra ID access

If you're adding new Microsoft Entra ID P1 or P2 licenses to an existing subscription, your Microsoft Entra ID access should already be activated. Otherwise, you need to activate Microsoft Entra ID access after you receive the **Welcome email**.

After your purchased licenses are provisioned in your directory, you'll receive a **Welcome email**. This email confirms that you can start managing your Microsoft Entra ID P1 or P2 or Enterprise Mobility + Security licenses and features.

💡 Tip

You won't be able to access Microsoft Entra ID for your new tenant until you activate Microsoft Entra directory access from the welcome email.

To activate your Microsoft Entra ID access

1. Open the **Welcome email**, and then select **Sign In**.
2. After successfully signing in, you'll go through two-step verification using a mobile device.

The activation process typically takes only a few minutes and then you can use your Microsoft Entra tenant.

Next steps

Now that you have Microsoft Entra ID P1 or P2, you can [customize your domain](#), add your [corporate branding](#), [create a tenant](#), and [add groups](#) and [users](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Configure Microsoft Entra for increased security (Preview)

Article • 04/27/2025

In Microsoft Entra, we group our security recommendations into several main areas. This structure allows organizations to logically break up projects into related consumable chunks.

💡 Tip

Some organizations might take these recommendations exactly as written, while others might choose to make modifications based on their own business needs. In our initial release of this guidance, we focus on traditional [workforce tenants](#). These workforce tenants are for your employees, internal business apps, and other organizational resources.

We recommend that all of the following controls be implemented where licenses are available. This helps to provide a foundation for other resources built on top of this solution. More controls will be added to this document over time.

Privileged access

Privileged accounts are cloud native identities

If an on-premises account is compromised and is synchronized to Microsoft Entra, the attacker might gain access to the tenant as well. This risk increases because on-premises environments typically have more attack surfaces due to older infrastructure and limited security controls. Attackers might also target the infrastructure and tools used to enable connectivity between on-premises environments and Microsoft Entra. These targets might include tools like Microsoft Entra Connect or Active Directory Federation Services, where they could impersonate or otherwise manipulate other on-premises user accounts.

If privileged cloud accounts are synchronized with on-premises accounts, an attacker who acquires credentials for on-premises can use those same credentials to access cloud resources and move laterally to the cloud environment.

Remediation action

- [Protecting Microsoft 365 from on-premises attacks](#)

For each role with high privileges (assigned permanently or eligible through Microsoft Entra Privileged Identity Management), you should do the following actions:

- Review the users that have `onPremisesImmutableId` and `onPremisesSyncEnabled` set. See [Microsoft Graph API user resource type](#).
- Create cloud-only user accounts for those individuals and remove their hybrid identity from privileged roles.

Privileged accounts have phishing-resistant methods registered

Without phishing-resistant authentication methods, privileged users are more vulnerable to phishing attacks. These types of attacks trick users into revealing their credentials to grant unauthorized access to attackers. If non-phishing-resistant authentication methods are used, attackers might intercept credentials and tokens, through methods like adversary-in-the-middle attacks, undermining the security of the privileged account.

Once a privileged account or session is compromised due to weak authentication methods, attackers might manipulate the account to maintain long-term access, create other backdoors, or modify user permissions. Attackers can also use the compromised privileged account to escalate their access even further, potentially gaining control over more sensitive systems.

Remediation action

- [Get started with a phishing-resistant passwordless authentication deployment](#)
- [Ensure that privileged accounts register and use phishing resistant methods](#)
- [Deploy Conditional Access policy to target privileged accounts and require phishing resistant credentials using authentication strengths](#)
- [Monitor authentication method activity](#)

Privileged users sign in with phishing-resistant methods

Without phishing-resistant authentication methods, privileged users are more vulnerable to phishing attacks. These types of attacks trick users into revealing their credentials to grant unauthorized access to attackers. If non-phishing-resistant authentication methods are used, attackers might intercept credentials and tokens, through methods like adversary-in-the-middle attacks, undermining the security of the privileged account.

Once a privileged account or session is compromised due to weak authentication methods, attackers might manipulate the account to maintain long-term access, create other backdoors, or modify user permissions. Attackers can also use the compromised privileged account to escalate their access even further, potentially gaining control over more sensitive systems.

Remediation action

- Get started with a phishing-resistant passwordless authentication deployment
- Ensure that privileged accounts register and use phishing resistant methods
- Deploy Conditional Access policy to target privileged accounts and require phishing resistant credentials using authentication strengths
- Monitor authentication method activity

All privileged role assignments are activated just in time and not permanently active

Threat actors target privileged accounts because they have access to the data and resources they want. This might include more access to your Microsoft Entra tenant, data in Microsoft SharePoint, or the ability to establish long-term persistence. Without a just-in-time (JIT) activation model, administrative privileges remain continuously exposed, providing attackers with an extended window to operate undetected. Just-in-time access mitigates risk by enforcing time-limited privilege activation with extra controls such as approvals, justification, and Conditional Access policy, ensuring that high-risk permissions are granted only when needed and for a limited duration. This restriction minimizes the attack surface, disrupts lateral movement, and forces adversaries to trigger actions that can be specially monitored and denied when not expected. Without just-in-time access, compromised admin accounts grant indefinite control, letting attackers disable security controls, erase logs, and maintain stealth, amplifying the impact of a compromise.

Use Microsoft Entra Privileged Identity Management (PIM) to provide time-bound just-in-time access to privileged role assignments. Use access reviews in Microsoft Entra ID Governance to regularly review privileged access to ensure continued need.

Remediation action

- Start using Privileged Identity Management
- Create an access review of Azure resource and Microsoft Entra roles in PIM

Credential management

Users have strong authentication methods configured

Attackers might gain access if multifactor authentication (MFA) isn't universally enforced or if there are exceptions in place. Attackers might gain access by exploiting vulnerabilities of weaker MFA methods like SMS and phone calls through social engineering techniques. These techniques might include SIM swapping or phishing, to intercept authentication codes.

Attackers might use these accounts as entry points into the tenant. By using intercepted user sessions, attackers can disguise their activities as legitimate user actions, evade detection, and continue their attack without raising suspicion. From there, they might attempt to manipulate MFA settings to establish persistence, plan, and execute further attacks based on the privileges of compromised accounts.

Remediation action

- [Deploy multifactor authentication](#)
- [Get started with a phishing-resistant passwordless authentication deployment](#)
- [Deploy Conditional Access policies to enforce authentication strength](#)
- [Review authentication methods activity](#)

Access control

Block legacy authentication

Legacy authentication protocols such as basic authentication for SMTP and IMAP don't support modern security features like multifactor authentication (MFA), which is crucial for protecting against unauthorized access. This lack of protection makes accounts using these protocols vulnerable to password-based attacks, and provides attackers with a means to gain initial access using stolen or guessed credentials.

When an attacker successfully gains unauthorized access to credentials, they can use them to access linked services, using the weak authentication method as an entry point. Attackers who gain access through legacy authentication might make changes to Microsoft Exchange, such as configuring mail forwarding rules or changing other settings, allowing them to maintain continued access to sensitive communications.

Legacy authentication also provides attackers with a consistent method to reenter a system using compromised credentials without triggering security alerts or requiring reauthentication.

From there, attackers can use legacy protocols to access other systems that are accessible via the compromised account, facilitating lateral movement. Attackers using legacy protocols can blend in with legitimate user activities, making it difficult for security teams to distinguish between normal usage and malicious behavior.

Remediation action

Deploy the following Conditional Access policy:

- [Block legacy authentication](#)

Privileged Microsoft Entra built-in roles are targeted with Conditional Access policies to enforce phishing-resistant methods

Without phishing-resistant authentication methods, privileged users are more vulnerable to phishing attacks. These types of attacks trick users into revealing their credentials to grant unauthorized access to attackers. If non-phishing-resistant authentication methods are used, attackers might intercept credentials and tokens, through methods like adversary-in-the-middle attacks, undermining the security of the privileged account.

Once a privileged account or session is compromised due to weak authentication methods, attackers might manipulate the account to maintain long-term access, create other backdoors, or modify user permissions. Attackers can also use the compromised privileged account to escalate their access even further, potentially gaining control over more sensitive systems.

Remediation action

- Get started with a phishing-resistant passwordless authentication deployment
- Ensure that privileged accounts register and use phishing resistant methods
- Deploy Conditional Access policy to target privileged accounts and require phishing resistant credentials using authentication strengths
- Monitor authentication method activity

Restrict access to high risk users

Assume any users at high risk are compromised by threat actors. Without investigation and remediation, threat actors can execute scripts, deploy malicious applications, or manipulate API calls to establish persistence, based on the potentially compromised user's permissions. Threat actors can then exploit misconfigurations or abuse OAuth tokens to move laterally across workloads like documents, SaaS applications, or Azure resources. Threat actors can gain access to sensitive files, customer records, or proprietary code and exfiltrate it to external repositories while maintaining stealth through legitimate cloud services. Finally, threat actors might disrupt operations by modifying configurations, encrypting data for ransom, or using the stolen information for further attacks, resulting in financial, reputational, and regulatory consequences.

Remediation action

- Create a Conditional Access policy to [require a secure password change for elevated user risk](#).
- Use Microsoft Entra ID Protection to [further investigate risk](#).

Restrict device code flow

Device code flow is a cross-device authentication flow designed for input-constrained devices. It can be exploited in phishing attacks, where an attacker initiates the flow and tricks a user into completing it on their device, thereby sending the user's tokens to the attacker. Given the security risks and the infrequent legitimate use of device code flow, you should enable a Conditional Access policy to block this flow by default.

Remediation action

- Create a Conditional Access policy to [block device code flow](#).
- [Learn more about device code flow](#)

Require multifactor authentication for device join and device registration using user action

Threat actors can exploit the lack of multifactor authentication during new device registration. Once authenticated, they can register rogue devices, establish persistence, and circumvent security controls tied to trusted endpoints. This foothold enables attackers to exfiltrate sensitive data, deploy malicious applications, or move laterally, depending on the permissions of the accounts being used by the attacker. Without MFA enforcement, risk escalates as adversaries can continuously reauthenticate, evade detection, and execute objectives.

Remediation action

- Create a Conditional Access policy to [require multifactor authentication for device registration](#).

Use cloud authentication

An on-premises federation server introduces a critical attack surface by serving as a central authentication point for cloud applications. Threat actors often gain a foothold by compromising a privileged user such as a help desk representative or an operations engineer through attacks like phishing, credential stuffing, or exploiting weak passwords. They might also target unpatched vulnerabilities in infrastructure, use remote code execution exploits, attack the Kerberos protocol, or use pass-the-hash attacks to escalate privileges. Misconfigured remote access tools like remote desktop protocol (RDP), virtual private network (VPN), or jump servers provide other entry points, while supply chain compromises or malicious insiders further increase exposure. Once inside, threat actors can manipulate authentication flows, forge security tokens to impersonate any user, and pivot into cloud environments. Establishing persistence, they can disable security logs, evade detection, and exfiltrate sensitive data.

Remediation action

- Migrate from federation to cloud authentication like Microsoft Entra Password hash synchronization (PHS).

Application management

Inactive applications don't have highly privileged Microsoft Graph API permissions

Attackers might exploit valid but inactive applications that still have elevated privileges. These applications can be used to gain initial access without raising alarm because they're legitimate applications. From there, attackers can use the application privileges to plan or execute other attacks. Attackers might also maintain access by manipulating the inactive application, such as by adding credentials. This persistence ensures that even if their primary access method is detected, they can regain access later.

Remediation action

- Disable privileged service principals
- Investigate if the application has legitimate use cases
- If service principal doesn't have legitimate use cases, delete it

Inactive applications don't have highly privileged built-in roles

Attackers might exploit valid but inactive applications that still have elevated privileges. These applications can be used to gain initial access without raising alarm because they're legitimate applications. From there, attackers can use the application privileges to plan or execute other attacks. Attackers might also maintain access by manipulating the inactive application, such as by adding credentials. This persistence ensures that even if their primary access method is detected, they can regain access later.

Remediation action

- Disable inactive privileged service principals
- Investigate if the application has legitimate use cases. If so, [analyze if a OAuth2 permission is a better fit](#)
- If service principal doesn't have legitimate use cases, delete it

Applications don't have secrets configured

Applications that use client secrets might store them in configuration files, hardcode them in scripts, or risk their exposure in other ways. The complexities of secret management make client secrets susceptible to leaks and attractive to attackers. Client secrets, when exposed, provide attackers with the ability to blend their activities with legitimate operations, making it easier to bypass security controls. If an attacker compromises an application's client secret, they can escalate their privileges within the system, leading to broader access and control, depending on the permissions of the application.

Applications and service principals that have permissions for Microsoft Graph APIs or other APIs have a higher risk because an attacker can potentially exploit these additional permissions.

Remediation action

- Move applications away from shared secrets to managed identities and adopt more secure practices.
 - Use managed identities for Azure resources
 - Deploy Conditional Access policies for workload identities
 - Implement secret scanning
 - Deploy application authentication policies to enforce secure authentication practices
 - Create a least-privileged custom role to rotate application credentials
 - Ensure you have a process to triage and monitor applications

Applications don't have certificates with expiration longer than 180 days

Certificates, if not securely stored, can be extracted and exploited by attackers, leading to unauthorized access. Long-lived certificates are more likely to be exposed over time.

Credentials, when exposed, provide attackers with the ability to blend their activities with legitimate operations, making it easier to bypass security controls. If an attacker compromises an application's certificate, they can escalate their privileges within the system, leading to broader access and control, depending on the privileges of the application.

Remediation action

- Define certificate based application configuration ↗
- Define trusted certificate authorities for apps and service principals in the tenant
- Define application management policies
- Enforce secret and certificate standards
- Create a least-privileged custom role to rotate application credentials

Application Certificates need to be rotated on a regular basis

If certificates aren't rotated regularly, they can give threat actors an extended window to extract and exploit them, leading to unauthorized access. When credentials like these are exposed, attackers can blend their malicious activities with legitimate operations, making it easier to bypass security controls. If an attacker compromises an application's certificate, they can escalate their privileges within the system, leading to broader access and control, depending on the application's privileges.

Query all of your service principals and application registrations that have certificate credentials. Make sure the certificate start date is less than 180 days.

Remediation action

- [Define an application management policy to manage certificate lifetimes](#)
- [Define a trusted certificate chain of trust](#)
- [Create a least privileged custom role to rotate application credentials](#)
- [Learn more about app management policies to manage certificate based credentials ↗](#)

Creating new applications and service principals is restricted to privileged users

If nonprivileged users can create applications and service principals, these accounts might be misconfigured or be granted more permissions than necessary, creating new vectors for attackers to gain initial access. Attackers can exploit these accounts to establish valid credentials in the environment and bypass some security controls.

If these nonprivileged accounts are mistakenly granted elevated application owner permissions, attackers can use them to move from a lower level of access to a more privileged level of access. Attackers who compromise nonprivileged accounts might add their own credentials or change the permissions associated with the applications created by the nonprivileged users to ensure they can continue to access the environment undetected.

Attackers can use service principals to blend in with legitimate system processes and activities. Because service principals often perform automated tasks, malicious activities carried out under these accounts might not be flagged as suspicious.

Remediation action

- [Block nonprivileged users from creating apps](#)

App registrations use safe redirect URIs

OAuth applications configured with URLs that include wildcards, localhost, or URL shorteners increase the attack surface for threat actors. Insecure redirect URIs (reply URLs) might allow

adversaries to manipulate authentication requests, hijack authorization codes, and intercept tokens by directing users to attacker-controlled endpoints. Wildcard entries expand the risk by permitting unintended domains to process authentication responses, while localhost and shortener URLs might facilitate phishing and token theft in uncontrolled environments.

Without strict validation of redirect URLs, attackers can bypass security controls, impersonate legitimate applications, and escalate their privileges. This misconfiguration enables persistence, unauthorized access, and lateral movement, as adversaries exploit weak OAuth enforcement to infiltrate protected resources undetected.

Remediation action

- [Check the redirect URLs for your application registrations](#). Make sure the redirect URLs don't have localhost, *.azurewebsites.net, wildcards, or URL shorteners.

Service principals use safe redirect URLs

Non-Microsoft and multitenant applications configured with URLs that include wildcards, localhost, or URL shorteners increase the attack surface for threat actors. These insecure redirect URLs (reply URLs) might allow adversaries to manipulate authentication requests, hijack authorization codes, and intercept tokens by directing users to attacker-controlled endpoints. Wildcard entries expand the risk by permitting unintended domains to process authentication responses, while localhost and shortener URLs might facilitate phishing and token theft in uncontrolled environments.

Without strict validation of redirect URLs, attackers can bypass security controls, impersonate legitimate applications, and escalate their privileges. This misconfiguration enables persistence, unauthorized access, and lateral movement, as adversaries exploit weak OAuth enforcement to infiltrate protected resources undetected.

Remediation action

- [Check the redirect URLs for your application registrations](#). Make sure the redirect URLs don't have localhost, *.azurewebsites.net, wildcards, or URL shorteners.

External collaboration

Guests can't invite other guests

External user accounts are often used to provide access to business partners who belong to organizations that have a business relationship with your enterprise. If these accounts are

compromised in their organization, attackers can use the valid credentials to gain initial access to your environment, often bypassing traditional defenses due to their legitimacy.

Allowing external users to onboard other external users increases the risk of unauthorized access. If an attacker compromises an external user's account, they can use it to create more external accounts, multiplying their access points and making it harder to detect the intrusion.

Remediation action

- [Restrict who can invite guests to only users assigned to specific admin roles](#)

Guests have restricted access to directory objects

External user accounts are often used to provide access to business partners who belong to organizations that have a business relationship with your enterprise. If these accounts are compromised in their organization, attackers can use the valid credentials to gain initial access to your environment, often bypassing traditional defenses due to their legitimacy.

External accounts with permissions to read directory object permissions provide attackers with broader initial access if compromised. These accounts allow attackers to gather additional information from the directory for reconnaissance.

Remediation action

- [Restrict guest access to their own directory objects](#)

Guest access is protected by strong authentication methods

External user accounts are often used to provide access to business partners who belong to organizations that have a business relationship with your organization. If these accounts are compromised in their organization, attackers can use the valid credentials to gain initial access to your environment, often bypassing traditional defenses due to their legitimacy.

Attackers might gain access with external user accounts, if multifactor authentication (MFA) isn't universally enforced or if there are exceptions in place. They might also gain access by exploiting the vulnerabilities of weaker MFA methods like SMS and phone calls using social engineering techniques, such as SIM swapping or phishing, to intercept the authentication codes.

Once an attacker gains access to an account without MFA or a session with weak MFA methods, they might attempt to manipulate MFA settings (for example, registering attacker controlled methods) to establish persistence to plan and execute further attacks based on the privileges of the compromised accounts.

Remediation action

- [Deploy Conditional Access policies to enforce authentication strength for guests.](#)
- For organizations with a closer business relationship and vetting on their MFA practices, consider deploying cross-tenant access settings to accept the MFA claim.
 - [Configure B2B collaboration cross-tenant access settings](#)

Monitoring

Diagnostic settings are configured for all Microsoft Entra logs

The activity logs and reports in Microsoft Entra can help detect unauthorized access attempts or identify when tenant configuration changes. When logs are archived or integrated with Security Information and Event Management (SIEM) tools, security teams can implement powerful monitoring and detection security controls, proactive threat hunting, and incident response processes. The logs and monitoring features can be used to assess tenant health and provide evidence for compliance and audits.

If logs aren't regularly archived or sent to a SIEM tool for querying, it's challenging to investigate sign-in issues. The absence of historical logs means that security teams might miss patterns of failed sign-in attempts, unusual activity, and other indicators of compromise. This lack of visibility can prevent the timely detection of breaches, allowing attackers to maintain undetected access for extended periods.

Remediation action

- [Configure Microsoft Entra diagnostic settings](#)
- [Integrate Microsoft Entra logs with Azure Monitor logs](#)
- [Stream Microsoft Entra logs to an event hub](#)

No legacy authentication sign-in activity

Legacy authentication protocols such as basic authentication for SMTP and IMAP don't support modern security features like multifactor authentication (MFA), which is crucial for protecting against unauthorized access. This lack of protection makes accounts using these protocols vulnerable to password-based attacks, and provides attackers with a means to gain initial access using stolen or guessed credentials.

When an attacker successfully gains unauthorized access to credentials, they can use them to access linked services, using the weak authentication method as an entry point. Attackers who gain access through legacy authentication might make changes to Microsoft Exchange, such as

configuring mail forwarding rules or changing other settings, allowing them to maintain continued access to sensitive communications.

Legacy authentication also provides attackers with a consistent method to reenter a system using compromised credentials without triggering security alerts or requiring reauthentication.

From there, attackers can use legacy protocols to access other systems that are accessible via the compromised account, facilitating lateral movement. Attackers using legacy protocols can blend in with legitimate user activities, making it difficult for security teams to distinguish between normal usage and malicious behavior.

Remediation action

- Exchange protocols can be deactivated in Exchange
- Legacy authentication protocols can be blocked with Conditional Access
- Sign-ins using legacy authentication workbook to help determine whether it's safe to turn off legacy authentication

All user sign-in activity uses strong authentication methods

Attackers might gain access if multifactor authentication (MFA) isn't universally enforced or if there are exceptions in place. Attackers might gain access by exploiting vulnerabilities of weaker MFA methods like SMS and phone calls through social engineering techniques. These techniques might include SIM swapping or phishing, to intercept authentication codes.

Attackers might use these accounts as entry points into the tenant. By using intercepted user sessions, attackers can disguise their activities as legitimate user actions, evade detection, and continue their attack without raising suspicion. From there, they might attempt to manipulate MFA settings to establish persistence, plan, and execute further attacks based on the privileges of compromised accounts.

Remediation action

- Deploy multifactor authentication
- Get started with a phishing-resistant passwordless authentication deployment
- Deploy Conditional Access policies to enforce authentication strength
- Review authentication methods activity

All high-risk users are triaged

Users considered at high risk by Microsoft Entra ID Protection have a high probability of compromise by threat actors. Threat actors can gain initial access via compromised valid accounts, where their suspicious activities continue despite triggering risk indicators. This

oversight can enable persistence as threat actors perform activities that normally warrant investigation, such as unusual login patterns or suspicious inbox manipulation.

A lack of triage of these risky users allows for expanded reconnaissance activities and lateral movement, with anomalous behavior patterns continuing to generate uninvestigated alerts. Threat actors become emboldened as security teams show they aren't actively responding to risk indicators.

Remediation action

- [Investigate high risk users](#) in Microsoft Entra ID Protection
- [Remediate high risk users and unblock](#) in Microsoft Entra ID Protection

All high-risk sign-ins are triaged

Risky sign-ins flagged by Microsoft Entra ID Protection indicate a high probability of unauthorized access attempts. Threat actors use these sign-ins to gain an initial foothold. If these sign-ins remain uninvestigated, adversaries can establish persistence by repeatedly authenticating under the guise of legitimate users.

A lack of response lets attackers execute reconnaissance, attempt to escalate their access, and blend into normal patterns. When untriaged sign-ins continue to generate alerts and there's no intervention, security gaps widen, facilitating lateral movement and defense evasion, as adversaries recognize the absence of an active security response.

Remediation action

- [Investigate risky sign-ins](#)
- [Remediate risks and unblock users](#)

High priority Entra recommendations are addressed

Leaving high-priority Microsoft Entra recommendations unaddressed can create a gap in an organization's security posture, offering threat actors opportunities to exploit known weaknesses. Not acting on these items might result in an increased attack surface area, suboptimal operations, or poor user experience.

Remediation action

- [Address all high priority recommendations in the Microsoft Entra admin center](#)

All Microsoft Entra recommendations are addressed

Microsoft Entra recommendations give organizations opportunities to implement best practices and optimize their security posture. Not acting on these items might result in an increased attack surface area, suboptimal operations, or poor user experience.

Remediation action

- Address all active or postponed recommendations in the Microsoft Entra admin center

Free security features

Enable Microsoft Entra ID security defaults

Enabling security defaults in Microsoft Entra is essential for organizations with Microsoft Entra Free licenses to protect against identity-related attacks. These attacks can lead to unauthorized access, financial loss, and reputational damage. Security defaults require all users to register for multifactor authentication (MFA), ensure administrators use MFA, and block legacy authentication protocols. This significantly reduces the risk of successful attacks, as more than 99% of common identity-related attacks are stopped by using MFA and blocking legacy authentication. Security defaults offer baseline protection at no extra cost, making them accessible for all organizations.

Remediation action

- Enable security defaults in Microsoft Entra ID

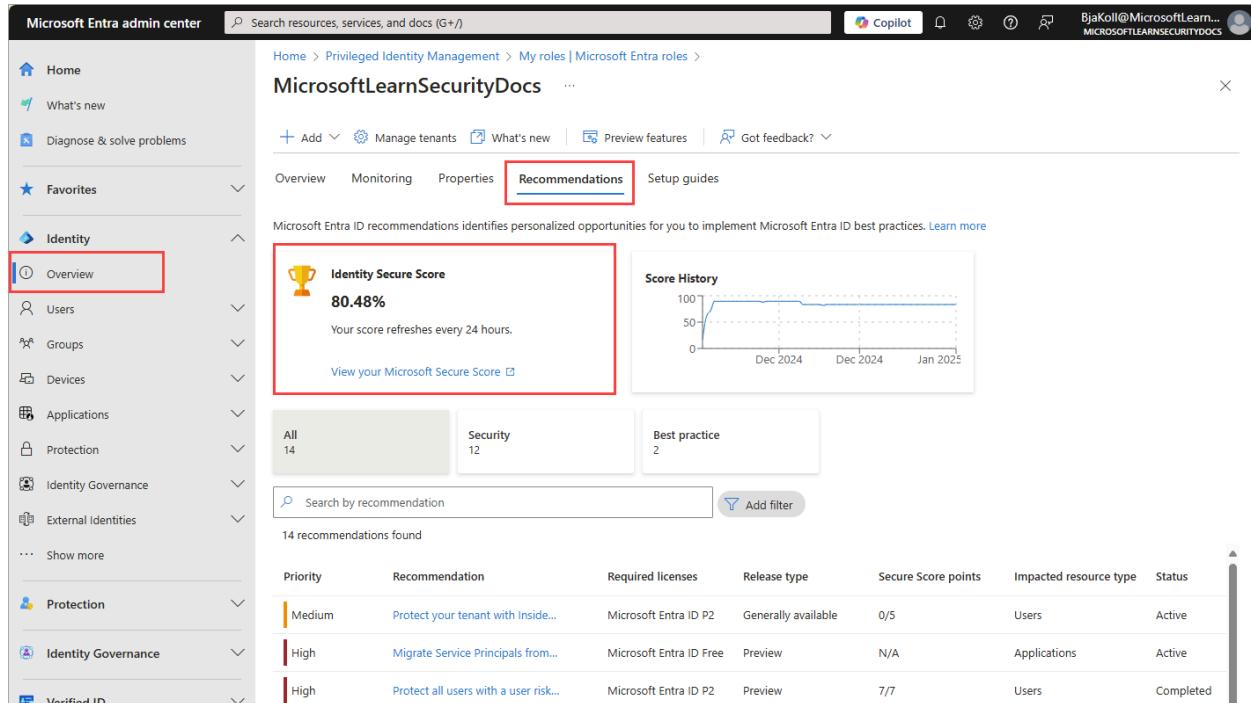
Related content

- [Microsoft Entra deployment plans](#)
- [Microsoft Entra operations reference guide](#)

What is Identity Secure Score?

Article • 01/26/2025

The Identity Secure Score is shown as a percentage that functions as an indicator for how aligned you are with Microsoft's recommendations for security. Each improvement action in Identity Secure Score is tailored to your configuration. You can access the score and view individual recommendations related to your score in Microsoft Entra recommendations. You can also see how your score has changed over time.



The screenshot shows the Microsoft Entra admin center interface. On the left, there is a navigation sidebar with categories like Home, What's new, Diagnose & solve problems, Favorites, Identity (which is selected and highlighted with a red box), Protection, Identity Governance, and Verified ID. Under Identity, 'Overview' is also highlighted with a red box. The main content area shows the 'Privileged Identity Management' section with 'My roles | Microsoft Entra roles'. Below this, the 'Recommendations' tab is selected and highlighted with a red box. A large box highlights the 'Identity Secure Score' section, which displays a score of 80.48% with a trophy icon. It also states that the score refreshes every 24 hours and provides a link to 'View your Microsoft Secure Score'. To the right of this is a 'Score History' chart showing a line graph from December 2024 to January 2025. Below the chart, there are three tabs: 'All' (14), 'Security' (12), and 'Best practice' (2). A search bar and a 'Add filter' button are located below these tabs. At the bottom, a table lists 14 recommendations with columns for Priority, Recommendation, Required licenses, Release type, Secure Score points, Impacted resource type, and Status. The recommendations include various security measures such as enabling MFA, protecting tenant with Inside... (Medium priority), migrating Service Principals (High priority), and protecting users with a user risk policy (High priority).

The following recommendations are included in the Identity Secure Score:

- Require multifactor authentication (MFA) for administrative roles
- Ensure all users can complete MFA
- Enable policy to block legacy authentication
- Do not expire passwords
- Protect all users with a user risk policy
- Protect all users with a sign-in risk policy
- Enable password hash sync if hybrid
- Do not allow users to grant consent to unreliable applications
- Use least privileged administrative roles
- Designate more than one Global Administrator
- Enable self-service password reset

How does the Identity Secure Score benefit me?

This score helps to:

- Objectively measure your identity security posture
- Plan identity security improvements
- Review the success of your improvements

By following the improvement actions in the Microsoft Entra recommendations, you can:

- Improve your security posture and your score
- Take advantage the features available to your organization as part of your identity investments

How does it work?

Every 24 hours, we look at your security configuration and compare your settings with the recommended best practices. Based on the outcome of this evaluation, a new score is calculated for your directory. It's possible that your security configuration isn't fully aligned with the best practice guidance and the improvement actions are only partially met. In these scenarios, you're awarded a portion of the max score available for the control.

Prerequisites

- Identity Secure Score is available to free and paid customers.
- Some recommendations require a paid license to view and act on. For more information, see [What are Microsoft Entra recommendations](#).
- To update the status of an improvement action, you need to have [Security Administrator](#), [Exchange Administrator](#), or [SharePoint Administrator](#) permissions.
- To view the improvement action but not update, you need to have [Helpdesk Administrator](#), [User Administrator](#), [Service Support Administrator](#), [Security Reader](#), [Security Operator](#), or [Global Reader](#) permissions.

How do I use the Identity Secure Score?

To access the Identity Secure Score:

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Global Reader](#).
2. Browse to **Protection > Identity Secure Score** to view the dashboard.

The score and related recommendations are also found at **Identity > Overview > Recommendations**.

Each recommendation is measured based on your configuration. If you're using non-Microsoft products to enable a best practice recommendation, you can indicate this configuration in the settings of an improvement action. You might set recommendations to be ignored if they don't apply to your environment. An ignored recommendation doesn't contribute to the calculation of your score.

Improvement action X

Use limited administrative roles

SCORE IMPACT ⓘ +1.79%

CURRENT SCORE ⓘ 1

MAX SCORE ⓘ 1

STATUS ⓘ

To address

To address

Risk accepted

Planned

Resolved through third party

Resolved through alternate mitigation

administrative privileged account being breached.

USER IMPACT ⓘ Low

IMPLEMENTATION COST ⓘ Low

WHAT AM I ABOUT TO CHANGE? ⓘ Reduce the number of persistent global administrator roles

Secure score updates can take up to 48 hours.

Save

- **To address** - You recognize that the improvement action is necessary and plan to address it at some point in the future. This state also applies to actions that are detected as partially, but not fully completed.
- **Risk accepted** - Security should always be balanced with usability, and not every recommendation works for everyone. When that is the case, you can choose to accept the risk, or the remaining risk, and not enact the improvement action. You aren't awarded any points, and the action isn't visible in the list of improvement actions. You can view this action in history or undo it at any time.
- **Planned** - There are concrete plans in place to complete the improvement action.
- **Resolved through third party** and **Resolved through alternate mitigation** - The improvement action was addressed by a non-Microsoft application or software, or an internal tool. You're awarded the points the action is worth, so your score better

reflects your overall security posture. If a non-Microsoft or internal tool no longer covers the control, you can choose another status. Keep in mind, Microsoft has no visibility into the completeness of implementation if the improvement action is marked as either of these statuses.

Frequently asked questions

Many factors can affect your score. Here are some frequently asked questions about the Identity Secure Score.

How are the recommendations scored?

Recommendations can be scored in two ways. Some are scored in a binary fashion, so you get 100% of the score if you have the feature or setting configured based on our recommendation. Other scores are calculated as a percentage of the total configuration. For example, the recommendation states there's a maximum of 10.71% increase if you protect all your users with MFA. You have 5 of 100 total users protected, so you're given a partial score around 0.53% ($5 \text{ protected} / 100 \text{ total} * 10.71\% \text{ maximum} = 0.53\% \text{ partial score}$).

What does [Not Scored] mean?

Actions labeled as [Not Scored] are ones you can perform in your organization but aren't scored. So, you can still improve your security, but you aren't given credit for those actions right now.

My score changed. How do I figure out why?

The [Microsoft 365 Defender portal](#) shows your complete Microsoft secure score. You can easily see all the changes to your secure score by reviewing the in-depth changes on the history tab.

Does the score measure my risk of getting breached?

No, score doesn't express an absolute measure of how likely you're to get breached. It expresses the extent to which you adopted features that can *offset* risk. No service can guarantee protection, and the score shouldn't be interpreted as a guarantee in any way.

How should I interpret my score?

Your score improves for configuring recommended security features or performing security-related tasks (like reading reports). Some actions are scored for partial completion, like enabling multifactor authentication (MFA) for your users. Your secure score is directly representative of the Microsoft security services you use. Remember that security must be balanced with usability. All security controls have a user impact component. Controls with low user impact should have little to no effect on your users' day-to-day operations.

How does the Identity Secure Score relate to the Microsoft 365 secure score?

The [Microsoft secure score](#) contains five distinct control and score categories:

- Identity
- Data
- Devices
- Infrastructure
- Apps

The Identity Secure Score represents the identity part of the Microsoft secure score. This overlap means that your recommendations for the Identity Secure Score and the identity score in Microsoft are the same.

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Secure your organization's identities with Microsoft Entra ID

Article • 05/31/2024

It can seem daunting trying to secure your workers in today's world, especially when you have to respond rapidly and provide access to many services quickly. This article helps provide a concise list of actions to take, helping you identify and prioritize features based on the license type you own.

Microsoft Entra ID offers many features and provides many layers of security for your Identities, navigating which feature is relevant can sometimes be overwhelming. This document is intended to help organizations deploy services quickly, with secure identities as the primary consideration.

Each table provides security recommendations to protect identities from common security attacks while minimizing user friction.

The guidance helps:

- Configure access to software as a service (SaaS) and on-premises applications in a secure and protected manner
- Both cloud and hybrid identities
- Users working remotely or in the office

Prerequisites

This guide assumes that your cloud-only or hybrid identities are established in Microsoft Entra ID already. For help with choosing your identity type see the article, [Choose the right authentication \(AuthN\) method for your Microsoft Entra hybrid identity solution](#).

Microsoft recommends that organizations have two cloud-only emergency access accounts permanently assigned the [Global Administrator](#) role. These accounts are highly privileged and aren't assigned to specific individuals. The accounts are limited to emergency or "break glass" scenarios where normal accounts can't be used or all other administrators are accidentally locked out. These accounts should be created following the [emergency access account recommendations](#).

Guided walkthrough

For a guided walkthrough of many of the recommendations in this article, see the [Set up Microsoft Entra ID](#) guide when signed in to the Microsoft 365 Admin Center. To review best

practices without signing in and activating automated setup features, go to the [Microsoft 365 Setup portal](#).

Guidance for Microsoft Entra ID Free, Office 365, or Microsoft 365 customers

There are many recommendations that Microsoft Entra ID Free, Office 365, or Microsoft 365 app customers should take to protect their user identities. The following table is intended to highlight key actions for the following license subscriptions:

- Office 365 (Office 365 E1, E3, E5, F1, A1, A3, A5)
- Microsoft 365 (Business Basic, Apps for Business, Business Standard, Business Premium, A1)
- Microsoft Entra ID Free (included with Azure, Dynamics 365, Intune, and Power Platform)

[] [Expand table](#)

Recommended action	Detail
Enable Security Defaults	Protect all user identities and applications by enabling multifactor authentication and blocking legacy authentication.
Enable Password Hash Sync (if using hybrid identities)	Provide redundancy for authentication and improve security (including Smart Lockout, IP Lockout, and the ability to discover leaked credentials).
Enable AD FS smart lock out (If applicable)	Protects your users from experiencing extranet account lockout from malicious activity.
Enable Microsoft Entra smart lockout (if using managed identities)	Smart lockout helps to lock out bad actors who are trying to guess your users' passwords or use brute-force methods to get in.
Disable end-user consent to applications	The admin consent workflow gives admins a secure way to grant access to applications that require admin approval so end users don't expose corporate data. Microsoft recommends disabling future user consent operations to help reduce your surface area and mitigate this risk.
Integrate supported SaaS applications from the gallery to Microsoft Entra ID and enable single sign-on (SSO)	Microsoft Entra ID has a gallery that contains thousands of preintegrated applications. Some of the applications your organization uses are probably in the gallery accessible directly from the Azure portal. Provide access to corporate SaaS applications remotely and securely with improved user experience (single sign-on (SSO)).

Recommended action	Detail
Automate user provisioning and deprovisioning from SaaS Applications (if applicable)	Automatically create user identities and roles in the cloud (SaaS) applications that users need access to. In addition to creating user identities, automatic provisioning includes the maintenance and removal of user identities as status or roles change, increasing your organization's security.
Enable Secure hybrid access: Secure legacy apps with existing app delivery controllers and networks (if applicable)	Publish and protect your on-premises and cloud legacy authentication applications by connecting them to Microsoft Entra ID with your existing application delivery controller or network.
Enable self-service password reset (applicable to cloud only accounts)	This ability reduces help desk calls and loss of productivity when a user can't sign in to their device or an application.
Use least privileged roles where possible	Give your administrators only the access they need to only the areas they need access to.
Enable Microsoft's password guidance ↴	Stop requiring users to change their password on a set schedule, disable complexity requirements, and your users are more apt to remember their passwords and keep them something that is secure.

Guidance for Microsoft Entra ID P1 customers

The following table is intended to highlight the key actions for the following license subscriptions:

- Microsoft Entra ID P1
- Microsoft Enterprise Mobility + Security E3
- Microsoft 365 (E3, A3, F1, F3)

 [Expand table](#)

Recommended action	Detail
Enable combined registration experience for Microsoft Entra multifactor authentication and SSPR to simplify user registration experience	Allow your users to register from one common experience for both Microsoft Entra multifactor authentication and self-service password reset.
Configure multifactor authentication settings for your organization	Ensure accounts are protected from being compromised with multifactor authentication.
Enable self-service password reset	This ability reduces help desk calls and loss of productivity when a

Recommended action	Detail
	user can't sign in to their device or an application.
Implement Password Writeback (if using hybrid identities)	Allow password changes in the cloud to be written back to an on-premises Windows Server Active Directory environment.
Create and enable Conditional Access policies	<p>Multifactor authentication for admins to protect accounts that are assigned administrative rights.</p> <p>Block legacy authentication protocols due to the increased risk associated with legacy authentication protocols.</p>
	<p>Multifactor authentication for all users and applications to create a balanced multifactor authentication policy for your environment, securing your users and applications.</p>
	<p>Require multifactor authentication for Azure Management to protect your privileged resources by requiring multifactor authentication for any user accessing Azure resources.</p>
Enable Password Hash Sync (if using hybrid identities)	Provide redundancy for authentication and improve security (including Smart Lockout, IP Lockout, and the ability to discover leaked credentials.)
Enable AD FS smart lock out (If applicable)	Protects your users from experiencing extranet account lockout from malicious activity.
Enable Microsoft Entra smart lockout (if using managed identities)	Smart lockout helps to lock out bad actors who are trying to guess your users' passwords or use brute-force methods to get in.
Disable end-user consent to applications	The admin consent workflow gives admins a secure way to grant access to applications that require admin approval so end users don't expose corporate data. Microsoft recommends disabling future user consent operations to help reduce your surface area and mitigate this risk.
Enable remote access to on-premises legacy applications with Application Proxy	Enable Microsoft Entra application proxy and integrate with legacy apps for users to securely access on-premises applications by signing in with their Microsoft Entra account.
Enable Secure hybrid access: Secure legacy apps with existing app delivery controllers and networks (if applicable).	Publish and protect your on-premises and cloud legacy authentication applications by connecting them to Microsoft Entra ID with your existing application delivery controller or network.
Integrate supported SaaS applications from the gallery to Microsoft Entra ID and enable single sign-on	Microsoft Entra ID has a gallery that contains thousands of preintegrated applications. Some of the applications your organization uses are probably in the gallery accessible directly from the Azure portal. Provide access to corporate SaaS

Recommended action	Detail
	applications remotely and securely with improved user experience (SSO).
Automate user provisioning and deprovisioning from SaaS Applications (if applicable)	Automatically create user identities and roles in the cloud (SaaS) applications that users need access to. In addition to creating user identities, automatic provisioning includes the maintenance and removal of user identities as status or roles change, increasing your organization's security.
Enable Conditional Access – Device-based	Improve security and user experiences with device-based Conditional Access. This step ensures users can only access from devices that meet your standards for security and compliance. These devices are also known as managed devices. Managed devices can be Intune compliant or Microsoft Entra hybrid joined devices.
Enable Password Protection	Protect users from using weak and easy to guess passwords.
Use least privileged roles where possible	Give your administrators only the access they need to only the areas they need access to.
Enable Microsoft's password guidance ↴	Stop requiring users to change their password on a set schedule, disable complexity requirements, and your users are more apt to remember their passwords and keep them something that is secure.
Create an organization specific custom banned password list	Prevent users from creating passwords that include common words or phrases from your organization or area.
Deploy passwordless authentication methods for your users	Provide your users with convenient passwordless authentication methods.
Create a plan for guest user access	Collaborate with guest users by letting them sign in to your apps and services with their own work, school, or social identities.

Guidance for Microsoft Entra ID P2 customers

The following table is intended to highlight the key actions for the following license subscriptions:

- Microsoft Entra ID P2
- Microsoft Enterprise Mobility + Security E5
- Microsoft 365 (E5, A5)

 [Expand table](#)

Recommended action	Detail
Enable combined registration experience for Microsoft Entra multifactor authentication and SSPR to simplify user registration experience	Allow your users to register from one common experience for both Microsoft Entra multifactor authentication and self-service password reset.
Configure multifactor authentication settings for your organization	Ensure accounts are protected from being compromised with multifactor authentication.
Enable self-service password reset	This ability reduces help desk calls and loss of productivity when a user can't sign in to their device or an application.
Implement Password Writeback (if using hybrid identities)	Allow password changes in the cloud to be written back to an on-premises Windows Server Active Directory environment.
Enable Microsoft Entra ID Protection policies to enforce multifactor authentication registration	Manage the roll-out of Microsoft Entra multifactor authentication.
Enable user and sign-in risk-based Conditional Access policies	The recommended sign-in policy is to target medium risk sign-ins and require multifactor authentication. For User policies, you should target high risk users requiring the password change action.
<p>Create and enable Conditional Access policies</p> <p>Block legacy authentication protocols due to the increased risk associated with legacy authentication protocols.</p> <p>Require multifactor authentication for Azure Management to protect your privileged resources by requiring multifactor authentication for any user accessing Azure resources.</p>	<p>Multifactor authentication for admins to protect accounts that are assigned administrative rights.</p> <p>Block legacy authentication protocols due to the increased risk associated with legacy authentication protocols.</p> <p>Require multifactor authentication for Azure Management to protect your privileged resources by requiring multifactor authentication for any user accessing Azure resources.</p>
Enable Password Hash Sync (if using hybrid identities)	Provide redundancy for authentication and improve security (including Smart Lockout, IP Lockout, and the ability to discover leaked credentials.)
Enable AD FS smart lock out (If applicable)	Protects your users from experiencing extranet account lockout from malicious activity.
Enable Microsoft Entra smart lockout (if using managed identities)	Smart lockout helps to lock out bad actors who are trying to guess your users' passwords or use brute-force methods to get in.
Disable end-user consent to applications	The admin consent workflow gives admins a secure way to grant access to applications that require admin approval so end users don't expose corporate data. Microsoft recommends disabling

Recommended action	Detail
	future user consent operations to help reduce your surface area and mitigate this risk.
Enable remote access to on-premises legacy applications with Application Proxy	Enable Microsoft Entra application proxy and integrate with legacy apps for users to securely access on-premises applications by signing in with their Microsoft Entra account.
Enable Secure hybrid access: Secure legacy apps with existing app delivery controllers and networks (if applicable)	Publish and protect your on-premises and cloud legacy authentication applications by connecting them to Microsoft Entra ID with your existing application delivery controller or network.
Integrate supported SaaS applications from the gallery to Microsoft Entra ID and enable single sign-on	Microsoft Entra ID has a gallery that contains thousands of preintegrated applications. Some of the applications your organization uses are probably in the gallery accessible directly from the Azure portal. Provide access to corporate SaaS applications remotely and securely with improved user experience (SSO).
Automate user provisioning and deprovisioning from SaaS Applications (if applicable)	Automatically create user identities and roles in the cloud (SaaS) applications that users need access to. In addition to creating user identities, automatic provisioning includes the maintenance and removal of user identities as status or roles change, increasing your organization's security.
Enable Conditional Access – Device-based	Improve security and user experiences with device-based Conditional Access. This step ensures users can only access from devices that meet your standards for security and compliance. These devices are also known as managed devices. Managed devices can be Intune compliant or Microsoft Entra hybrid joined devices.
Enable Password Protection	Protect users from using weak and easy to guess passwords.
Use least privileged roles where possible	Give your administrators only the access they need to only the areas they need access to.
Enable Microsoft's password guidance ↗	Stop requiring users to change their password on a set schedule, disable complexity requirements, and your users are more apt to remember their passwords and keep them something that is secure.
Create an organization specific custom banned password list	Prevent users from creating passwords that include common words or phrases from your organization or area.
Deploy passwordless authentication methods for your users	Provide your users with convenient passwordless authentication methods
Create a plan for guest user access	Collaborate with guest users by letting them sign in to your apps

Recommended action	Detail
	and services with their own work, school, or social identities.
Enable Privileged Identity Management (PIM)	Enables you to manage, control, and monitor access to important resources in your organization, ensuring admins have access only when needed and with approval.
Complete an access review for Microsoft Entra directory roles in PIM	Work with your security and leadership teams to create an access review policy to review administrative access based on your organization's policies.

Zero Trust

This feature helps organizations to align their [identities](#) with the three guiding principles of a Zero Trust architecture:

- Verify explicitly
- Use least privilege
- Assume breach

To find out more about Zero Trust and other ways to align your organization to the guiding principles, see the [Zero Trust Guidance Center](#).

Next steps

- For detailed deployment guidance for individual features of Microsoft Entra ID, review the [Microsoft Entra ID project deployment plans](#).
- Organizations can use [identity secure score](#) to track their progress against other Microsoft recommendations.

Five steps to integrate your apps with Microsoft Entra ID

Article • 10/23/2023

Learn to integrate your applications with Microsoft Entra ID, which is a cloud-based Identity and Access Management (IAM) service. Organizations use Microsoft Entra ID for secure authentication and authorization so customers, partners, and employees can access applications.

With Microsoft Entra ID, features such as Conditional Access, Microsoft Entra multifactor authentication, single sign-on (SSO), and application provisioning make Identity and Access Management easier to manage and more secure.

Learn more:

- [What is Conditional Access?](#)
- [How it works: Microsoft Entra multifactor authentication](#)
- [Microsoft Entra seamless single sign-on](#)
- [What is app provisioning in Microsoft Entra ID?](#)

If your company has a Microsoft 365 subscription, you likely use Microsoft Entra ID. However, you can use Microsoft Entra ID for applications. If you centralize application management, identity management features, tools, and policies for your app portfolio. The benefit is a unified solution that improves security, reduces costs, increases productivity, and enables compliance. In addition, there's remote access to on-premises apps.

Learn more:

- [Deploy your identity infrastructure for Microsoft 365](#)
- [What is application management in Microsoft Entra ID?](#)

Microsoft Entra ID for new applications

When your business acquires new applications, add them to the Microsoft Entra tenant. Establish a company policy of adding new apps to Microsoft Entra ID.

See: [Quickstart: Add an enterprise application](#)

Microsoft Entra ID has a gallery of integrated applications to make it easy to get started. Add a gallery app to your Microsoft Entra organization (see previous link) and learn

about integrating software as a service (SaaS) tutorials.

See: [Tutorials for integrating SaaS applications with Microsoft Entra ID](#)

Integration tutorials

Use the following tutorials to learn to integrate common tools with Microsoft Entra single sign-on (SSO).

- Tutorial: [Microsoft Entra SSO integration with ServiceNow](#)
- Tutorial: [Microsoft Entra SSO integration with Workday](#)
- Tutorial: [Microsoft Entra SSO integration with Salesforce](#)
- Tutorial: [Microsoft Entra SSO integration with AWS Single-Account Access](#)
- Tutorial: [Microsoft Entra SSO integration with Slack](#)

Apps not in the gallery

You can integrate applications that don't appear in the gallery, including applications in your organization, or third-party application from vendors. Submit a request to publish your app in the gallery. To learn about integrating apps you develop in-house, see [Integrate apps your developers build](#).

Learn more:

- Quickstart: [View enterprise applications](#)
- Submit a request to publish your application in [Microsoft Entra application gallery](#)

Determine application usage and prioritize integration

Discover the applications employees use, and prioritize integrating the apps with Microsoft Entra ID. Use the Microsoft Defender for Cloud Apps Cloud Discovery tools to discover and manage apps not managed by your IT team. Microsoft Defender for Endpoint (formerly known as Microsoft Defender for Endpoint) simplifies and extends the discovery process.

Learn more:

- [Set up Cloud Discovery](#)
- [Microsoft Defender for Endpoint](#)

In addition, use the Active Directory Federation Services (AD FS) in the Azure portal to discover AD FS apps in your organization. Discover unique users that signed in to the apps, and see information about integration compatibility.

See: [Review the application activity report](#)

Application migration

After you discover apps in your environment, prioritize the apps to migrate and integrate. Consider the following parameters:

- Apps used most frequently
- Riskiest apps
- Apps to be decommissioned, therefore not in migration
- Apps that stay on-premises

See: [Resources for migrating applications to Microsoft Entra ID](#)

Integrate apps and identity providers

During discovery, there might be applications not tracked by the IT team, which can create vulnerabilities. Some applications use alternative identity solutions, including AD FS, or other identity providers (IdPs). We recommend you consolidate Identity and Access Management. Benefits include:

- Reduce on-premises user set-up, authentication, and IdP licensing fees
- Lower administrative overhead with streamlined Identity and Access Management process
- Enable single sign-on (SSO) access to applications in the My Apps portal
 - See: [Create collections on the My Apps portal](#)
- Use Microsoft Entra ID Protection and Conditional Access to increase signals from app usage, and extend benefits to recently added apps
 - [What is ID Protection?](#)
 - [What is Conditional Access?](#)

App owner awareness

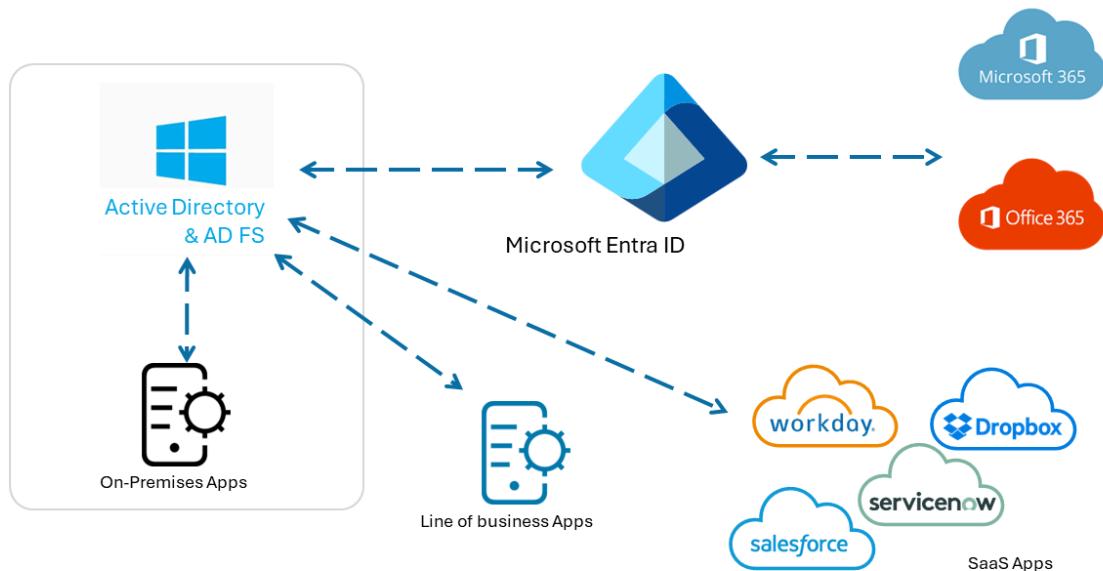
To help manage app integration with Microsoft Entra ID, use the following material for application owner awareness and interest. Modify the material with your branding.

You can download:

- Zip file: [Editable Microsoft Entra App Integration One-Pager](#)
- Microsoft PowerPoint presentation: [Microsoft Entra application integration guidelines](#)

Active Directory Federation Services

Evaluate use of AD FS for authentication with SaaS apps, line of business (LOB) apps, also Microsoft 365 and Microsoft Entra apps.

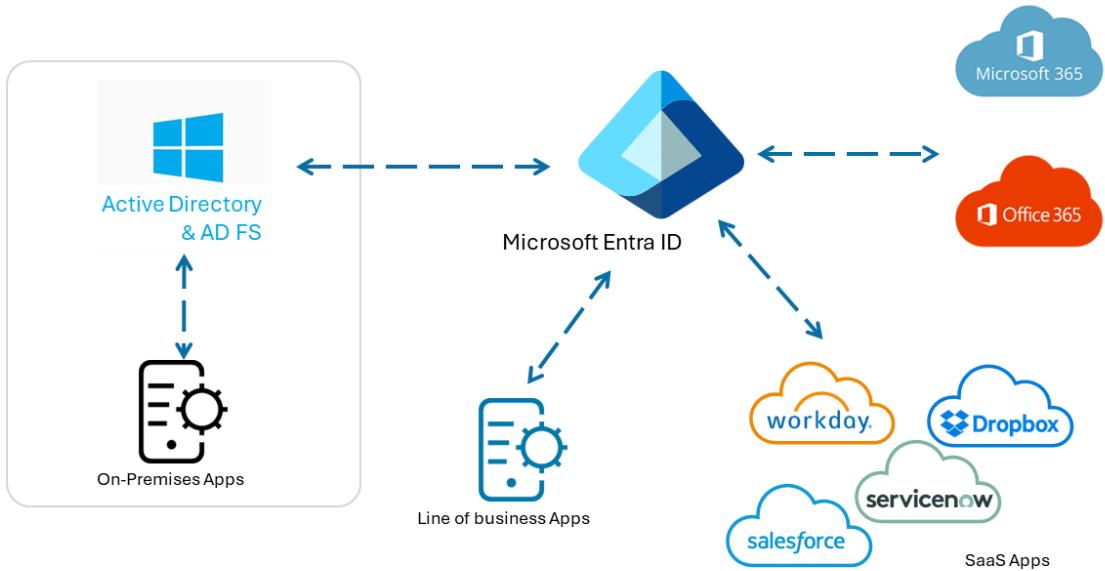


Improve the configuration illustrated in the previous diagram by moving application authentication to Microsoft Entra ID. Enable sign-on for apps and ease application discovery with the My Apps portal.

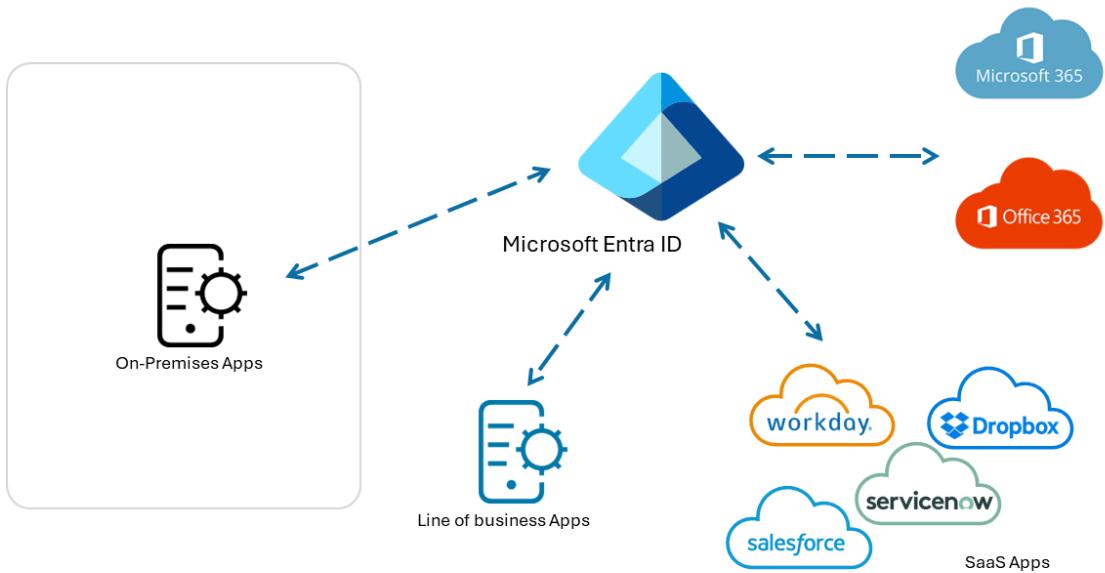
Learn more:

- [Move application authentication to Microsoft Entra ID](#)
- [Sign in and start apps from the My Apps portal](#)

See the following diagram of app authentication simplified by Microsoft Entra ID.



After Microsoft Entra ID is the central IdP, you might be able to discontinue AD FS.



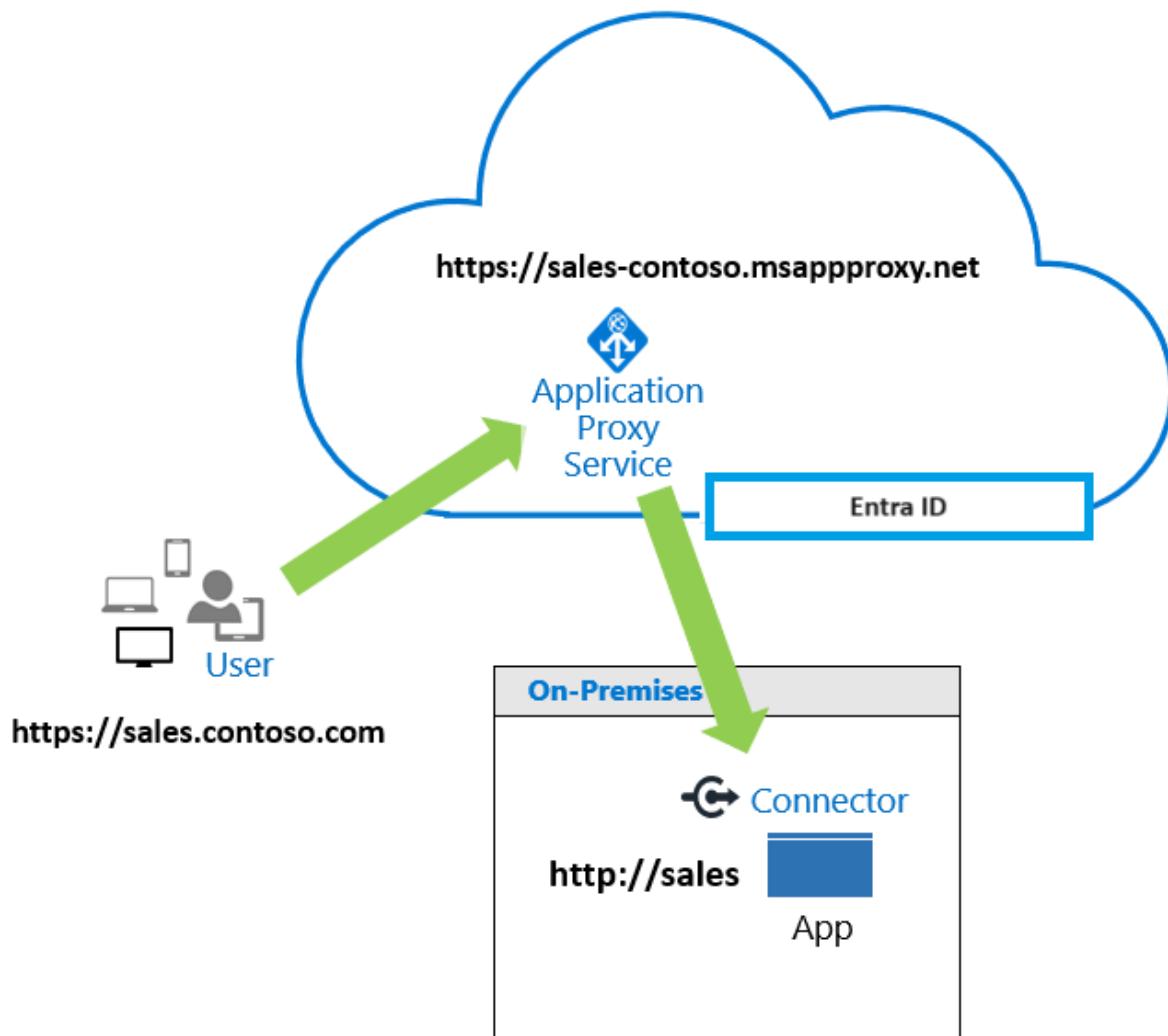
You can migrate apps that use a different cloud-based IdP. Your organization might have multiple Identity Access Management (IAM) solutions. Migrating to one Microsoft Entra infrastructure can reduce dependencies on IAM licenses and infrastructure costs. If you paid for Microsoft Entra ID with Microsoft 365 licenses, likely you don't have to purchase another IAM solution.

Integrate on-premises applications

Traditionally, application security enabled access during a connection to a corporate network. However, organization grant access to apps for customers, partners, and/or employees, regardless of location. Application Proxy Service in Microsoft Entra connects on-premises apps to Microsoft Entra ID and doesn't require edge servers or more infrastructure.

See: [Using Microsoft Entra application proxy to publish on-premises apps for remote users](#)

The following diagram illustrates Application Proxy Service processing a user request.



See: [Tutorial: Add an on-premises application for remote access through Application Proxy in Microsoft Entra ID](#)

In addition, integrate application delivery controllers like F5 BIG-IP APM, or Zscaler Private Access, with Microsoft Entra ID. Benefits are modern authentication and identity management, traffic management, and security features. We call this solution secure hybrid access.

See: [Secure hybrid access: Protect legacy apps with Microsoft Entra ID](#)

For the following services, there are Microsoft Entra integration tutorials.

- Tutorial: Microsoft Entra SSO integration with Akamai
- Tutorial: Microsoft Entra SSO integration with Citrix ADC Security Assertion Markup Language (SAML) Connector for Microsoft Entra ID (Kerberos-based authentication)
 - Formerly known as Citrix NetScaler
- Integrate F5 BIG-IP with Microsoft Entra ID
- Tutorial: Integrate Zscaler Private Access (ZPA) with Microsoft Entra ID

Integrate apps your developers build

For your developers' apps, use the Microsoft identity platform for authentication and authorization. Integrated applications are registered and managed like other apps in your portfolio.

Learn more:

- Microsoft identity platform documentation
- Quickstart: Register an application with the Microsoft identity platform

Developers can use the platform for internal and customer-facing apps. For instance, use Microsoft Authentication Libraries (MSAL) to enable multifactor authentication and security to access apps.

Learn more:

- Overview of the Microsoft Authentication Library (MSAL)
- Microsoft identity platform code samples
- Video: Overview of the Microsoft identity platform for developers ↗ (33:54)

Next step

Resources for migrating applications to Microsoft Entra ID

Feedback

Was this page helpful?



Provide product feedback ↗

Security defaults in Microsoft Entra ID

Article • 09/27/2024

Security defaults make it easier to help protect your organization from identity-related attacks like password spray, replay, and phishing common in today's environments.

Microsoft is making these preconfigured security settings available to everyone, because we know managing security can be difficult. Based on our learnings more than 99.9% of those common identity-related attacks are stopped by using multifactor authentication and blocking legacy authentication. Our goal is to ensure that all organizations have at least a basic level of security enabled at no extra cost.

These basic controls include:

- Requiring all users to register for multifactor authentication
- Requiring administrators to do multifactor authentication
- Requiring users to do multifactor authentication when necessary
- Blocking legacy authentication protocols
- Protecting privileged activities like access to the Azure portal

Who's it for?

- Organizations who want to increase their security posture, but don't know how or where to start.
- Organizations using the free tier of Microsoft Entra ID licensing.

Who should use Conditional Access?

- If you're an organization with Microsoft Entra ID P1 or P2 licenses, security defaults are probably not right for you.
- If your organization has complex security requirements, you should consider [Conditional Access](#).

Enabling security defaults

If your tenant was created on or after October 22, 2019, security defaults might be enabled in your tenant. To protect all of our users, security defaults are being rolled out to all new tenants at creation.

To help protect organizations, we're always working to improve the security of Microsoft account services. As part of this protection, customers are periodically notified for the automatic enablement of the security defaults if they:

- Don't have any Conditional Access policies
- Don't have premium licenses
- Aren't actively using legacy authentication clients

After this setting is enabled, all users in the organization will need to register for multifactor authentication. To avoid confusion, refer to the email you received and alternatively you can [disable security defaults](#) after it's enabled.

To configure security defaults in your directory, you must be assigned at least the [Conditional Access Administrator](#) role.

By default, the user who creates a Microsoft Entra tenant is automatically assigned the [Global Administrator](#) role.

To enable security defaults:

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Conditional Access Administrator](#).
2. Browse to **Identity > Overview > Properties**.
3. Select **Manage security defaults**.
4. Set **Security defaults** to **Enabled**.
5. Select **Save**.

The screenshot shows the Microsoft Entra admin center interface. On the left, the navigation menu includes sections like Home, Favorites, Identity, Overview, Users, Groups, Devices, Applications, Protection, Identity governance, External Identities, Show more, and Protection. The main content area displays the 'Contoso' tenant properties. The 'Properties' tab is selected. In the 'Security defaults' section, a dropdown menu shows 'Disabled (not recommended)' is selected. Below it, there are three options: 'Enabled' and 'Disabled'. A red box highlights this section. At the bottom of the 'Security defaults' section, a warning message is displayed: '⚠ Your organization is not protected by security defaults. Manage security defaults'. A red box highlights this message. The bottom right of the page has 'Save' and 'Discard' buttons.

Revoking active tokens

As part of enabling security defaults, administrators should revoke all existing tokens to require all users to register for multifactor authentication. This revocation event forces previously authenticated users to authenticate and register for multifactor authentication. This task can be accomplished using the [Revoke-AzureADUserAllRefreshToken](#) PowerShell cmdlet.

Enforced security policies

Require all users to register for Microsoft Entra multifactor authentication

ⓘ Note

Starting July 29, 2024, new tenants and existing tenants had the 14-day grace period for users to register for MFA removed. We are making this change to help reduce the risk of account compromise during the 14-day window, as MFA can block over 99.2% of identity-based attacks.

When users sign in and are prompted to perform multifactor authentication, they see a screen providing them with a number to enter in the Microsoft Authenticator app. This measure helps prevent users from falling for MFA fatigue attacks.



adelev@contoso.onmicrosoft.com

Approve sign in request



Open your Authenticator app, and enter the number shown to sign in.

88

No numbers in your app? Make sure to upgrade to the latest version.

[I can't use my Microsoft Authenticator app right now](#)

[More information](#)

Contoso

Require administrators to do multifactor authentication

Administrators have increased access to your environment. Because of the power these highly privileged accounts have, you should treat them with special care. One common method to improve the protection of privileged accounts is to require a stronger form of account verification for sign-in, like requiring multifactor authentication.

💡 Tip

Recommendations for your admins:

- Ensure all your admins sign in after enabling security defaults so that they can register for authentication methods.
- Have separate accounts for administration and standard productivity tasks to significantly reduce the number of times your admins are prompted for MFA.

After registration is finished, the following administrator roles will be required to do multifactor authentication every time they sign in:

- Global Administrator
- Application Administrator
- Authentication Administrator
- Billing Administrator
- Cloud Application Administrator
- Conditional Access Administrator
- Exchange Administrator
- Helpdesk Administrator
- Password Administrator
- Privileged Authentication Administrator
- Privileged Role Administrator
- Security Administrator
- SharePoint Administrator
- User Administrator
- Authentication Policy Administrator
- Identity Governance Administrator

Require users to do multifactor authentication when necessary

We tend to think that administrator accounts are the only accounts that need extra layers of authentication. Administrators have broad access to sensitive information and can make changes to subscription-wide settings. But attackers frequently target end users.

After these attackers gain access, they can request access to privileged information for the original account holder. They can even download the entire directory to do a phishing attack on your whole organization.

One common method to improve protection for all users is to require a stronger form of account verification, such as multifactor authentication, for everyone. After users complete registration, they'll be prompted for another authentication whenever necessary. Microsoft decides when a user is prompted for multifactor authentication, based on factors such as location, device, role, and task. This functionality protects all registered applications, including SaaS applications.

 **Note**

In case of [B2B direct connect](#) users, any multifactor authentication requirement from security defaults enabled in resource tenant will need to be satisfied, including multifactor authentication registration by the direct connect user in their home tenant.

Block legacy authentication protocols

To give your users easy access to your cloud apps, we support various authentication protocols, including legacy authentication. *Legacy authentication* is a term that refers to an authentication request made by:

- Clients that don't use modern authentication (for example, an Office 2010 client)
- Any client that uses older mail protocols such as IMAP, SMTP, or POP3

Today, most compromising sign-in attempts come from legacy authentication. Legacy authentication doesn't support multifactor authentication. Even if you have a multifactor authentication policy enabled on your directory, an attacker can authenticate by using an older protocol and bypass multifactor authentication.

After security defaults are enabled in your tenant, all authentication requests made by an older protocol will be blocked. Security defaults blocks Exchange Active Sync basic authentication.

 **Warning**

Before you enable security defaults, make sure your administrators aren't using older authentication protocols. For more information, see [How to move away from legacy authentication](#).

- How to set up a multifunction device or application to send email using Microsoft 365

Protect privileged activities like access to the Azure portal

Organizations use various Azure services managed through the Azure Resource Manager API, including:

- Azure portal
- Microsoft Entra admin center
- Azure PowerShell
- Azure CLI

Using Azure Resource Manager to manage your services is a highly privileged action. Azure Resource Manager can alter tenant-wide configurations, such as service settings and subscription billing. Single-factor authentication is vulnerable to various attacks like phishing and password spray.

It's important to verify the identity of users who want to access Azure Resource Manager and update configurations. You verify their identity by requiring more authentication before you allow access.

After you enable security defaults in your tenant, any user accessing the following services must complete multifactor authentication:

- Azure portal
- Microsoft Entra admin center
- Azure PowerShell
- Azure CLI

This policy applies to all users who are accessing Azure Resource Manager services, whether they're an administrator or a user. This policy applies to Azure Resource Manager APIs such as accessing your subscription, VMs, storage accounts, and so on. This policy doesn't include Microsoft Entra ID or Microsoft Graph.

ⓘ Note

Pre-2017 Exchange Online tenants have modern authentication disabled by default. In order to avoid the possibility of a login loop while authenticating through these tenants, you must [enable modern authentication](#).

ⓘ Note

The Microsoft Entra Connect / Microsoft Entra Cloud Sync synchronization accounts (or any security principal assigned to the "Directory Synchronization Accounts" role)

are excluded from security defaults and will not be prompted to register for or perform multifactor authentication. Organizations should not be using this account for other purposes.

Deployment considerations

Preparing your users

It's critical to inform users about upcoming changes, registration requirements, and any necessary user actions. We provide [communication templates](#) and [user documentation](#) to prepare your users for the new experience and help to ensure a successful rollout. Send users to <https://myprofile.microsoft.com> to register by selecting the **Security Info** link on that page.

Authentication methods

Security defaults users are required to register for and use multifactor authentication using the [Microsoft Authenticator app using notifications](#). Users might use verification codes from the Microsoft Authenticator app but can only register using the notification option. Users can also use any third party application using [OATH TOTP](#) to generate codes.

Warning

Do not disable methods for your organization if you are using security defaults.

Disabling methods may lead to locking yourself out of your tenant. Leave all

[Methods available to users enabled in the MFA service settings portal](#).

B2B users

Any [B2B guest](#) users or [B2B direct connect](#) users that access your directory are treated the same as your organization's users.

Disabled MFA status

If your organization is a previous user of per-user based multifactor authentication, don't be alarmed to not see users in an **Enabled** or **Enforced** status if you look at the

multipath authentication status page. **Disabled** is the appropriate status for users who are using security defaults or Conditional Access based multipath authentication.

Disabling security defaults

Organizations that choose to implement Conditional Access policies that replace security defaults must disable security defaults.

To disable security defaults in your directory:

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Conditional Access Administrator](#).
2. Browse to **Identity > Overview > Properties**.
3. Select **Manage security defaults**.
4. Set **Security defaults** to **Disabled (not recommended)**.
5. Select **Save**.

Move from security defaults to Conditional Access

While security defaults are a good baseline to start your security posture from, they don't allow for the customization that many organizations require. Conditional Access policies provide a full range of customization that more complex organizations require.

[] [Expand table](#)

	Security defaults	Conditional Access
Required licenses	None	At least Microsoft Entra ID P1
Customization	No customization (on or off)	Fully customizable
Enabled by	Microsoft or administrator	Administrator
Complexity	Simple to use	Fully customizable based on your requirements

Recommended steps when moving from security defaults

Organizations who would like to test out the features of Conditional Access can [sign up for a free trial](#) to get started.

After administrators disable security defaults, organizations should immediately enable Conditional Access policies to protect their organization. These policies should include

at least those policies in the [secure foundations category of Conditional Access templates](#). Organizations with Microsoft Entra ID P2 licenses that include Microsoft Entra ID Protection can expand on this list to include [user and sign in risk-based policies](#) to further strengthen their posture.

Microsoft recommends that organizations have two cloud-only emergency access accounts permanently assigned the [Global Administrator](#) role. These accounts are highly privileged and aren't assigned to specific individuals. The accounts are limited to emergency or "break glass" scenarios where normal accounts can't be used or all other administrators are accidentally locked out. These accounts should be created following the [emergency access account recommendations](#).

Next steps

- [Blog: Introducing security defaults ↗](#)
 - More information about licensing can be found on the [Microsoft Entra pricing page↗](#).
-

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Copilot in Microsoft Entra

Article • 12/10/2024

Applies to:

- Microsoft Entra

[Microsoft Security Copilot](#) is a platform that brings together the power of AI and human expertise to help administrators and security teams respond to attacks faster and more effectively. Security Copilot is embedded in Microsoft Entra so you can investigate and resolve identity risks, assess identities and access with AI-driven intelligence, and complete complex tasks quickly. Copilot in Microsoft Entra (Copilot) gets insights from your Microsoft Entra users, groups, sign-in logs, audit logs, and more.

You can explore sign-ins and risky users and get contextualized insights on how to resolve incidents and what to do to protect the accounts in natural language. Built on top of real-time machine learning, Copilot can help you find gaps in access policies, generate identity workflows, and troubleshoot faster. You can also unlock new skills that allow admins at all levels to complete complex tasks such as incident investigation, sign-in log analysis, and more, to gain savings in time and resources.

This article introduces you to Copilot in Microsoft Entra.

Know before you begin

If you're new to Security Copilot, you should familiarize yourself with it by reading these articles:

- [What is Microsoft Security Copilot?](#)
- [Microsoft Security Copilot experiences](#)
- [Get started with Microsoft Security Copilot](#)
- [Understand authentication in Microsoft Security Copilot](#)
- [Prompting in Microsoft Security Copilot](#)

Security Copilot integration in Microsoft Entra

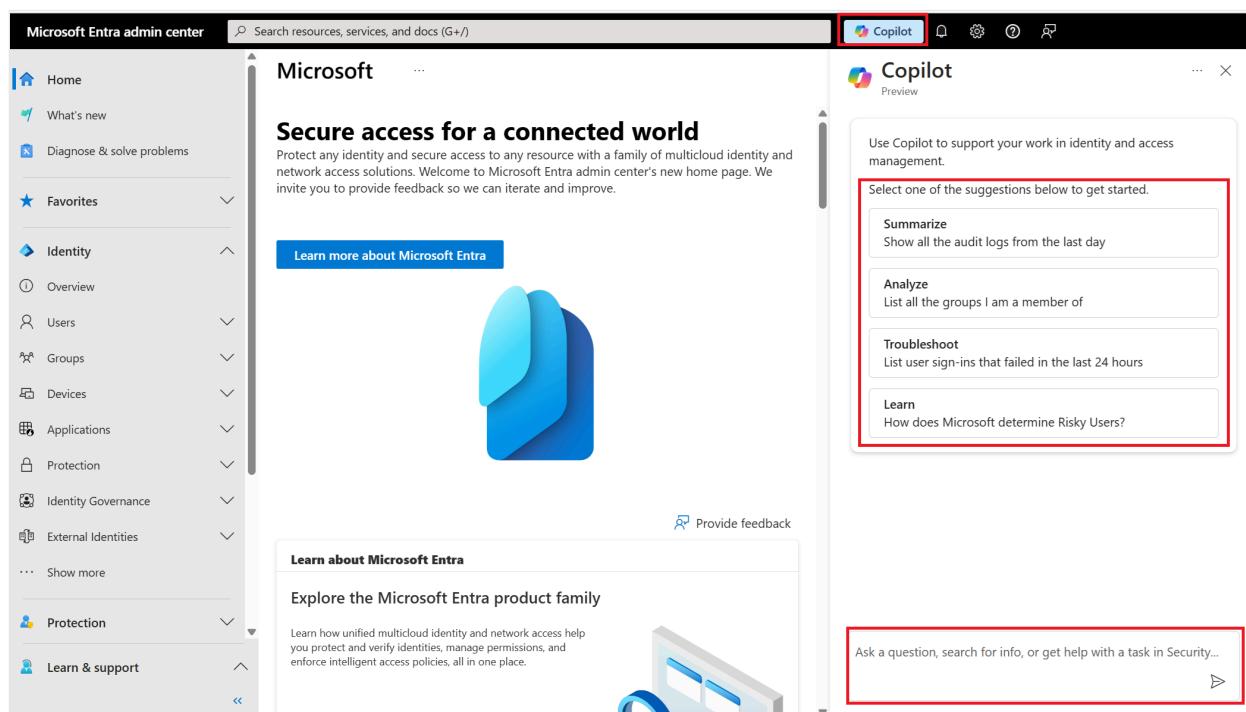
Microsoft Entra is one of the Microsoft plugins that enable the Security Copilot platform to generate accurate and relevant information. Through the Microsoft Entra plugin, the Security Copilot portal can provide more context to incidents and generate more accurate results. The key features mentioned in this article are capabilities that are also available in the Security Copilot portal.

Key features

Microsoft Entra brings the capabilities of Security Copilot to the Microsoft Entra admin center, enabling administrators and security teams to respond to identity threats quickly. Bringing AI to Microsoft Entra allows teams to understand risks immediately and determine remediation steps in a timely manner.

Create Security Copilot prompts in the Microsoft Entra admin center (preview)

Security Copilot is a part of the Microsoft Entra admin center, use it to create your own prompts. Launch Security Copilot from a globally available button in the menu bar. Choose from a set of starter prompts that appear at the top of the Security Copilot window or enter your own in the prompt bar to get started. Suggested prompts may also appear after a response, these are predefined prompts that Security Copilot selects based on the prior response.



Specific scenarios supported by Security Copilot embedded in Microsoft Entra skills:

- Troubleshoot a user's sign-in events.
- Find details about users and groups.
- Find and summarize changes made to users, roles, groups, and apps from Microsoft Entra audit log details.
- Improve your security posture and reduce application/workload identity risk.
- Learn more about Microsoft Entra and receive guidance on identity & access administration from relevant [Microsoft Entra documentation](#).

Summarize a user's risk level

Microsoft Entra ID Protection applies the capabilities of Security Copilot to [summarize a user's risk level](#), provide insights relevant to the incident at hand, and provide recommendations for rapid mitigation. Identity risk investigation is a crucial step to defend an organization. Copilot helps reduce the time to resolution by providing IT admins and security operations center (SOC) analysts the right context to investigate and remediate identity risk and identity-based incidents. Risky user summarization provides admins and responders quick access to the most critical information in context to aid their investigation.

Risky User Details

[Reset password](#) [Confirm user compromised](#) [Dismiss user risk](#) [Block user](#) [User's risk detections](#) [...](#)

[Summarize](#) [Basic info](#) [Recent risky sign-ins](#) [Detections not linked to a sign-in](#) [Risk history](#)

Summary by Copilot (Preview) [Download](#)
Generated by Copilot

- User Julieta Oliveiran has one recent risky activity with High risk.
- The risk detection type is Microsoft Entra threat intelligence.
- Microsoft Entra threat intelligence indicates user activity that is unusual for the user or consistent with known attack patterns. This detection is based on Microsoft's internal and external threat intelligence sources.
- Risky sign-in 1 (RequestId: 81e5c594-d704-497c-9e4a-[CorrelationId: aaaa0000-bb11-2222-33cd](#)) with High risk level occurred on 2024-03-26T22:59:48 UTC for Resource Azure Portal. The sign-in IP was [Redmond, Washington US](#). The IP, ASN, Location, Brower Id and Device Id were unfamiliar to the user. There was no MFA for this sign-in.

AI-generated content may be incorrect [Report](#)

What to do

Check to ensure this user is in scope of these risk-based Conditional Access policies which will shorten the time to mitigate the attack, automatically close the risk, and save you time and effort.

If you do not have those policies:

- [Create a sign-in risk based policy](#)
- [Create a user risk based policy](#)

For now, investigate this user for indicators of compromise and take action using the buttons above. Use our playbooks below for step-by-step guidance.

Help and documentation

[What is risk in ID Protection?](#) [Incident Response Playbooks](#) [Risk-based Access Policies](#)

Enable the Security Copilot integration in Microsoft Entra

You can learn more about plugins implemented in the Security Copilot portal in [Manage plugins in Security Copilot](#). Additionally, you can learn more about the embedded experiences in other Microsoft security products in [Security Copilot experiences](#).

Sample Microsoft Entra prompts

Once you're all set up in Security Copilot, you can start using natural language prompts to help remediate identity-based incidents:

- *Give me all user details for karita@woodgrovebank.com and extract the user Object ID.*
- *Does karita@woodgrovebank.com have any registered devices in Microsoft Entra?*
- *List the recent risky sign-ins for karita@woodgrovebank.com.*
- *Can you give me sign-in logs for karita@woodgrovebank.com for the past 48 hours? Put this information in a table format.*
- *Get Microsoft Entra audit logs for karita@woodgrovebank.com for the past 72 hours. Put information in table format.*

Provide feedback

Copilot in Microsoft Entra uses AI and machine learning to process data and generate responses for each of the key features. However, AI might misinterpret some data, which sometimes cause a mismatch in responses. Your feedback on the generated responses helps improve the accuracy of Copilot and Microsoft Entra over time.

All key features have an option for providing feedback. To provide feedback, perform the following steps:

1. Select the thumb up icon located at the bottom of any response card in the Copilot pane.
2. Answer the question **What did you like?**
3. Select **Yes, share samples** or **No, don't share samples**.
4. Select **Submit**.

Or

1. Select the thumb down icon located at the bottom of any response card in the Copilot pane.
2. Select **Inaccurate** if any detail is incorrect or incomplete based on your assessment. Select **Offensive or inappropriate** if it contains potentially harmful, questionable, or ambiguous information. Select **Other** for some other reason.
3. Whenever possible, write a few words explaining what can be done to improve the outcome in the **What went wrong?** text box.
4. Select **Yes, share samples** or **No, don't share samples**.
5. Select **Submit**.

Privacy and data security in Security Copilot

To understand how Security Copilot handles your prompts and the data that's retrieved from the service(prompt output), see [Privacy and data security in Microsoft Security Copilot](#).

Next steps

- Learn more about [risky user summarization](#).
- [Investigate security incidents](#) using the Microsoft Entra skills in Microsoft Security Copilot.
- [Investigate risky apps](#) using the Microsoft Entra skills in Microsoft Security Copilot.

See also

- [Get started with Microsoft Security Copilot](#)
- [What is Security Copilot?](#)
- [Privacy and data security in Security Copilot](#)
- [Responsible AI FAQs](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Microsoft Security Copilot agents in Microsoft Entra

Article • 04/27/2025

Microsoft Entra agents work seamlessly with [Microsoft Security Copilot](#). Microsoft Security Copilot agents automate repetitive tasks and reduce manual workloads. They enhance security and IT operations across cloud, data security and privacy, identity, and network security. These agents handle high-volume, time-consuming tasks by pairing data and code with an AI language model. They respond to user requests and system events, helping teams work more efficiently and focus on higher-impact tasks.

Agents fit naturally into existing workflows. You don't need special training or other licensing to use them. Agents utilize SCUs to operate just like other features in the product. They integrate seamlessly with Microsoft Security solutions and the broader supported partner ecosystem. Agents learn based on feedback and keep you in control on the actions it takes. They handle resource-intensive tasks like threat intelligence briefings, and Conditional Access optimization. With Microsoft Security Copilot agents, you can scale up your teams, people, and processes.

Microsoft Security Copilot agents offer significant benefits for security teams and IT operations by automating routine tasks and freeing up valuable time for teams to concentrate on strategic initiatives and complex problem-solving. This leads to improved operational efficiency, enhanced security and giving teams the ability to respond more swiftly to emerging threats. With Security Copilot agents, organizations can achieve greater scalability and resilience in their security and IT processes.

Available agents

Microsoft Entra Conditional Access optimization agent

The [Conditional Access optimization agent](#) ensures all users are protected by policy. It recommends policies and changes based on best practices aligned with [Zero Trust](#) and Microsoft's learnings. In preview, the agent evaluates policies requiring multifactor authentication (MFA), enforces device based controls (device compliance, app protection policies, and Domain Joined Devices), and blocks legacy authentication and device code flow.

Trigger

The agent runs every 24 hours but can also run manually.

Permissions

The agent reviews your policy configuration but acts only with your approval of the suggestions.

Identity

It runs in the context of the administrator who configured the agent.

Products

[Microsoft Entra Conditional Access](#) and [Security Copilot](#)

Plugins

[Microsoft Entra](#)

Role-based access

Administrators need the [Security Administrator](#) or [Global Administrator](#) role during the preview.

Respond to identity threats using risky user summarization

Article • 04/25/2025

Microsoft Entra ID Protection applies the capabilities of [Copilot in Microsoft Entra](#) to summarize a user's risk level, provide insights relevant to the incident at hand, and provide recommendations for rapid mitigation. Identity risk investigation is a crucial step to defend an organization. Copilot in Microsoft Entra helps reduce the time to resolution by providing IT admins and security operations center (SOC) analysts the right context to investigate and remediate identity risk and identity-based incidents. Risky user summarization provides admins and responders quick access to the most critical information in context to aid their investigation.

Respond to identity threats quickly:

- Risk summary: summarize in natural language why the user risk level was elevated.
- Recommendations: get guidance on how to mitigate and respond to these types of attacks, with quick links to help and documentation.

This article describes how to access the risky user summary capability of Microsoft Entra ID Protection and Copilot in Microsoft Entra. Using this feature requires [Microsoft Entra ID P2 licenses](#).

Investigate risky users

To view and investigate a risky user:

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Security Reader](#).
2. Navigate to **ID Protection** > [Risky users](#).
3. Select a user from the risky users report.

The screenshot shows the Microsoft Identity Protection interface. The left sidebar has a tree view with 'Identity' expanded, showing 'Overview', 'Users', 'Groups', 'Devices', 'Applications', 'Protection', 'Identity governance', 'External Identities', and 'Show more'. Under 'Protection', 'Identity Protection' is selected and highlighted with a red box. Below it are 'Conditional Access', 'Authentication methods', and 'Password reset'. The main content area is titled 'Identity Protection | Risky users'. It includes a search bar and navigation links like 'Learn more', 'Download', 'Select all', 'Confirm user(s) compromised', 'Dismiss user(s) risk', and 'Get help investigating a risky user with Copilot'. A message at the top says 'We recommend migrating Identity Protection policies to Conditional Access for more conditions and controls. Learn more'. The table lists three users: Giovanna Costa (At risk, last updated 3/26/2024, 4:06:02 PM), Ratih Winata (At risk, last updated 3/26/2024, 11:31:01 AM), and Sascha Lange (At risk, last updated 3/26/2024, 7:21:32 AM). The table has columns for 'User', 'Risk state', and 'Risk last updated'. Buttons for 'Auto refresh: Off', 'Show dates as: Local', 'Risk state: 2 selected', and 'Status: Active' are at the top of the table.

4. In the Risky User Details window, information appears in **Summarize**.

The screenshot shows the 'Risky User Details' window for user 'Giovanna Costa'. The top navigation bar includes 'Reset password', 'Confirm user compromised', 'Dismiss user risk', 'Block user', and 'User's risk detections'. Below the navigation bar, there are tabs: 'Summarize' (highlighted with a red box), 'Basic info', 'Recent risky sign-ins', 'Detections not linked to a sign-in', and 'Risk history'. The 'Summarize' tab displays a 'Summary by Copilot (Preview)' section with the sub-headline 'Generated by Copilot'. It lists several points about the user's recent activity:

- User Julieta Oliveiran has one recent risky activity with High risk.
- The risk detection type is Microsoft Entra threat intelligence.
- Microsoft Entra threat intelligence indicates user activity that is unusual for the user or consistent with known attack patterns. This detection is based on Microsoft's internal and external threat intelligence sources.
- Risky sign-in 1 (RequestId: 81e5c594-d704-497c-9e4a-, CorrelationId: aaaa0000-bb11-2222-33cd with High risk level occurred on 2024-03-26T22:59:48 UTC for Resource Azure Portal. The sign-in IP was and location was Redmond, Washington US. The IP, ASN, Location, Browser Id and Device Id were unfamiliar to the user. There was no MFA for this sign-in.

Below the summary, there is an 'AI-generated content may be incorrect' link with upvote and downvote buttons. The 'What to do' section advises checking Conditional Access policies. If no policies exist, it suggests creating a sign-in risk based policy or a user risk based policy. The 'Help and documentation' section links to 'What is risk in ID Protection?', 'Incident Response Playbooks', and 'Risk-based Access Policies'.

The risky user summary contains three sections:

- Summary by Copilot: summarizes in natural language why ID Protection flagged the user for risk.

- What to do: lists the next steps to investigate this incident and prevent future incidents.
- Help and documentation: lists resources for help and documentation.

In this example, suggested remediations are to:

- Create sign-in risk and user risk based [Conditional Access policies](#).

Suggested help and documentation are:

- [What is risk in ID Protection?](#)
- [Incident Response Playbooks](#)
- [Risk-based Access Policies](#)

Next steps

- Learn more about [risky users](#).

Manage employee lifecycle using Microsoft Security Copilot (Preview)

Article • 02/19/2025

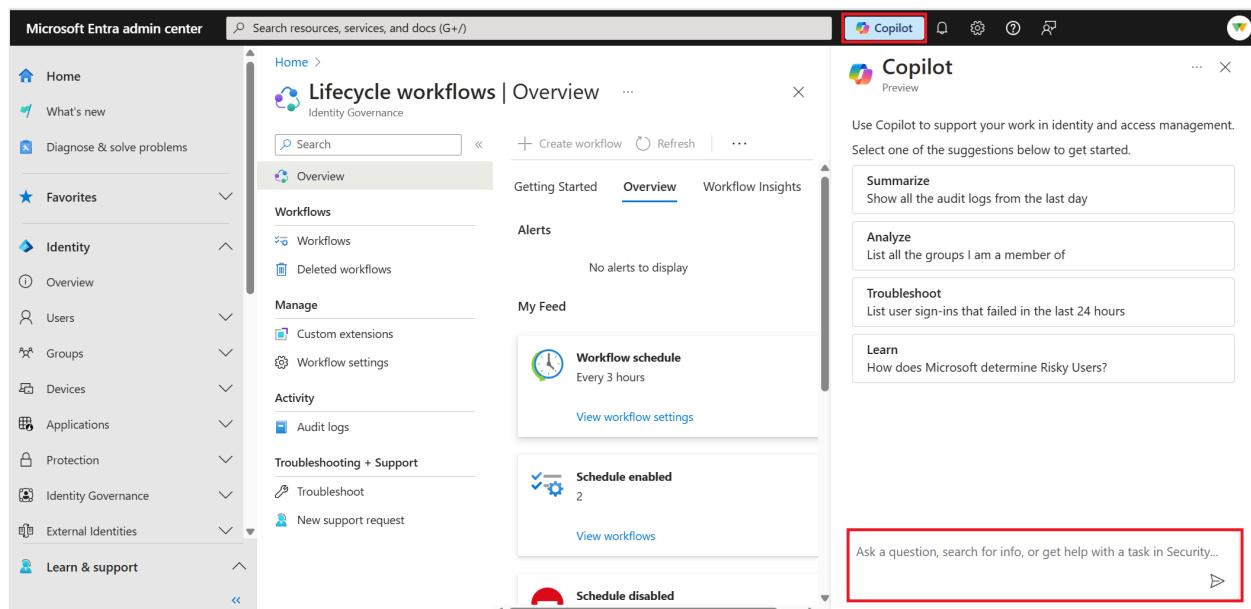
Microsoft Entra ID Governance applies the capabilities of [Microsoft Security Copilot](#) to save identity administrators time and effort when configuring custom workflows to manage the lifecycle of users across JML scenarios. It also helps you to customize workflows more efficiently using natural language to configure workflow information including custom tasks, execute workflows, and get workflow insights.

This article describes how to work with lifecycle workflows using Security Copilot in the Microsoft Entra admin center. Using this feature requires [Microsoft Entra ID Governance licenses](#).

Sign in to the [Microsoft Entra admin center](#) as at least a [Lifecycle Workflows Administrator](#). Navigate to **Identity Governance -> Lifecycle workflows overview**.

Launch Security Copilot from the **Copilot** button in the Microsoft Entra admin center. Use natural language questions or prompts to:

- Get step-by-step guidance for creating a lifecycle workflow
- Explore available workflow configurations
- Analyze the active workflow list
- Troubleshoot the processing results of workflows



Create step-by-step guidance for a new lifecycle workflow

Security Copilot can give you the steps to guide you in creating a new lifecycle workflow. Provide a prompt with actions to take when the workflow is triggered and conditions that define which users (scope) this workflow should run against, and when (trigger) the workflow should run. For example:

Create a lifecycle workflow for new hires in the Marketing department that sends a welcome email and a TAP and adds them to the "All Users in My Tenant" group. Also, provide the option to enable the schedule of the workflow.

Review the returned results to see what the workflow includes and then follow the steps to [create a new workflow](#) in the Microsoft Entra admin center. After the workflow is created, you can perform verification testing before enabling the schedule.

Explore available workflow configurations

Using Microsoft Security Copilot, you can efficiently manage various lifecycle workflows. Here are some common tasks you can accomplish with Security Copilot:

For example:

- *List all lifecycle workflows in my tenant*
- *List all the supported workflow templates for creating a new workflow*
- *What are my lifecycle workflow settings?*
- *Which leaver tasks can I automate with lifecycle workflows?*
- *What templates can be used for creating a mover workflow?*

Analyze active workflow list

With Microsoft Security Copilot, you can easily analyze and manage your active workflow list and retrieve specific workflow information.

For example:

- *Get my lifecycle workflows with the name {workflow name}*
- *List all mover workflows in my tenant*
- *List all the deleted lifecycle workflows in my tenant*
- *List all disabled lifecycle workflows in my tenant*
- *Show me the details of disabled workflow {workflow}*

Troubleshoot a Lifecycle Workflow run

You can use Security Copilot to help troubleshoot a workflow run. Security Copilot uses the information provided to generate and return a rich summary of the workflow history over the given time period for the specified workflow.

Explore workflow processing results of a specific workflow:

- *Summarize the runs for {workflow} in the last 7 days*
- *How many times did the workflow run in the last 24 hours*
- *Which users failed to be processed by this workflow in the last 7 days?*
- *Which tasks failed for {workflow} in the last 7 days?*
- *Show me the user processing results summary for {workflow} in the last 7 days*

Explore workflow processing results across workflows:

- *How many workflows were processed in the last 7 days?*
- *How many users were successfully processed by workflows in the last 14 days?*
- *Which workflows have been run the most in the last 7 days?*
- *Which tasks failed the most in the last 30 days?*
- *Which workflows failed the most in the last 7 days?*
- *How many mover workflows were executed in the last 30 days?*

Compare versions of a lifecycle workflow

You can use Security Copilot to compare workflow versions. Security Copilot uses the information provided to generate and return a rich summary of the content of two versions of the specified workflow as well as the core differences between the workflow versions including tasks and execution conditions.

For example:

- *List all workflow versions for {workflow}*
- *Show me who last modified {workflow} and when*
- *Show me the details of {version #} for this workflow*
- *What changed in the last version of this workflow?*
- *Compare the last two versions of this workflow*
- *Compare {version #} and {version #} of this workflow*

Next steps

- Learn more about [lifecycle workflows](#).

- Create a lifecycle workflow.
 - Run a workflow on demand.
-

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

Investigate security incidents using Microsoft Security Copilot

Article • 11/07/2024

[Microsoft Security Copilot](#) gets insights from your Microsoft Entra data through many different skills, such as Get Entra Risky Users and Get Audit Logs. IT admins and security operations center (SOC) analysts can use these skills and others to gain the right context to help investigate and remediate identity-based incidents using natural language prompts.

This article describes how a SOC analyst or IT admin could use the Microsoft Entra skills to investigate a potential security incident.

Scenario

Natasha, a security operations center (SOC) analyst at Woodgrove Bank, receives an alert about a potential identity-based security incident. The alert indicates suspicious activity from a user account that has been flagged as a risky user.

Investigate

Natasha starts her investigation and signs in to [Microsoft Security Copilot](#). In order to view user, group, risky user, sign-in logs, audit-logs, and diagnostic logs details, she signs in as at least a [Security Reader](#).

Get user details

Natasha starts by looking up details of the flagged user: karita@woodgrovebank.com. She reviews the user's profile information such as job title, department, manager, and contact information. She also checks the user's assigned roles, applications, and licenses to understand what applications and services the user has access to.

She uses the following prompts to get the information she needs:

- *Give me all user details for karita@woodgrovebank.com and extract the user Object ID.*
- *Is this user's account enabled?*
- *When was the password last changed or reset for karita@woodgrovebank.com?*
- *Does karita@woodgrovebank.com have any registered devices in Microsoft Entra?*

- *What are the authentication methods that are registered for karita@woodgrovebank.com if any?*

Get risky user details

To understand why karita@woodgrovebank.com was flagged as a risky user, Natasha starts looking at the risky user details. She reviews the risk level of the user (low, medium, high, or hidden), the risk detail (for example, sign-in from unfamiliar location), and the risk history (changes in risk level over time). She also checks the risk detections and the recent risky sign-ins, looking for suspicious sign-in activity or impossible travel activity.

She uses the following prompts to get the information she needs:

- *What is the risk level, state, and risk details for karita@woodgrovebank.com?*
- *What is the risk history for karita@woodgrovebank.com?*
- *List the recent risky sign-ins for karita@woodgrovebank.com.*
- *List the risk detections details for karita@woodgrovebank.com.*

Get sign-in logs details

Natasha then reviews the sign-in logs for the user and the sign-in status (success or failure), location (city, state, country), IP address, device information (device ID, operating system, browser), and sign-in risk level. She also checks the correlation ID for each sign-in event, which can be used for further investigation.

She uses the following prompts to get the information she needs:

- *Can you give me sign-in logs for karita@woodgrovebank.com for the past 48 hours? Put this information in a table format.*
- *Show me failed sign-ins for karita@woodgrovebank.com for the past 7 days and tell me what the IP addresses are.*

Get audit logs details

Natasha checks the audit logs, looking for any unusual or unauthorized actions performed by the user. She checks the date and time of each action, the status (success or failure), the target object (for example, file, user, group), and the client IP address. She also checks the correlation ID for each action, which can be used for further investigation.

She uses the following prompts to get the information she needs:

- *Get Microsoft Entra audit logs for karita@woodgrovebank.com for the past 72 hours. Put information in table format.*
- *Show me audit logs for this event type.*

Get group details

Natasha then reviews the groups that karita@woodgrovebank.com is a part of to see if Karita is a member of any unusual or sensitive groups. She reviews the group memberships and permissions associated with Karita's user ID. She checks the group type (security, distribution, or Office 365), membership type (assigned or dynamic), and the group's owners in the group details. She also reviews the group's roles to determine what permissions it has for managing resources.

She uses the following prompts to get the information she needs:

- *Get the Microsoft Entra user groups that karita@woodgrovebank.com is a member of. Put information in table format.*
- *Tell me more about the Finance Department group.*
- *Who are the owners of the Finance Department group?*
- *What roles does this group have?*

Get diagnostic logs details

Finally, Natasha reviews the diagnostic logs to get more detailed information about the system's operations during the times of the suspicious activities. He filters the logs by John's user ID and the times of the unusual sign-ins.

She uses the following prompts to get the information she needs:

- *What are the diagnostics log configuration for the tenant that is karita@woodgrovebank.com registered in?*
- *Which logs are being collected in this tenant?*

Remediate

By using Security Copilot, Natasha is able to gather comprehensive information about the user, sign-in activities, audit logs, risky user detections, group memberships, and system diagnostics. After completing her investigation, Natasha needs to take action to remediate the risky user or unblock them.

She reads about [risk remediation](#), [unblocking users](#), and [response playbooks](#) to determine possible actions to take next.

Next steps

Learn more about:

- Risky users
 - What is risk in ID Protection?
 - Risk-based Access Policies
-

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback 

Assess application risks using Microsoft Security Copilot in Microsoft Entra (Preview)

Article • 12/12/2024

[Microsoft Security Copilot](#) gets insights from your Microsoft Entra data through many different skills, such as Investigate identity risks with Entra ID Protection and Explore Microsoft Entra audit log details. App risk skills allow identity admins and security analysts who manage applications or workload identities in Microsoft Entra to identify and understand risks through natural language prompts. By using prompts like, "List risky app details for my tenant", the analyst gets a better picture of the risk from application identities and can discover other application details in Microsoft Entra - including permissions granted (especially those that might be considered high privileged), unused apps in their tenant, and apps from outside their tenant. Security Copilot then uses prompt context to respond, such as with a list of apps or permissions, then surface links to the Microsoft Entra admin center so that admins can see a full list and take the appropriate remediation actions for their risky apps. IT admins and security operations center (SOC) analysts can use these skills and others to gain the right context to help investigate and remediate identity-based incidents using natural language prompts.

This article describes how a SOC analyst or IT admin could use the Microsoft Entra skills to investigate a potential security incident.

Note

These app risk skills provide data on single tenant, third party SaaS, and multi-tenant apps that are applications or service principals in Microsoft Entra. Managed identities are not currently in scope.

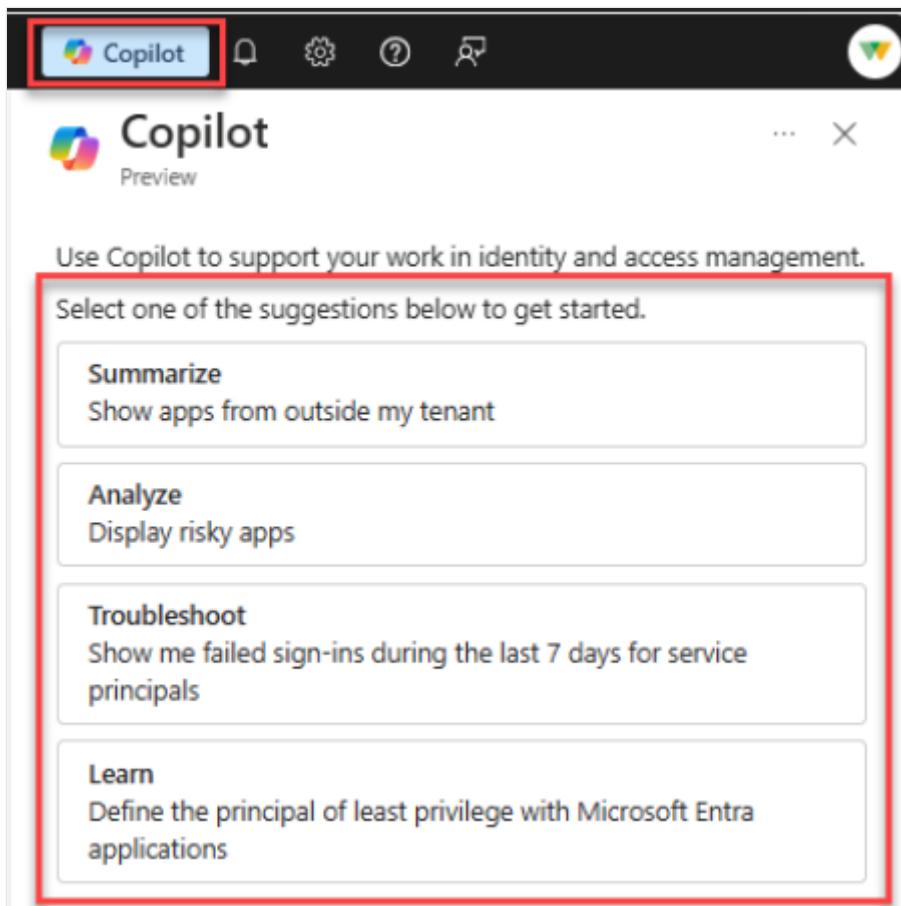
Scenario

Jason, an IT admin at Woodgrove Bank, is proactively trying to identify and understand any risky apps in their tenant.

Investigate

Jason starts his assessment and signs in to [Microsoft Security Copilot](#) or the Microsoft Entra admin center. In order to view application and service principal details, he signs in as at least a [Security Reader](#) and needs an [Microsoft Entra role assignment](#) of Application Administrator, Cloud Application Administrator, or similar Microsoft Entra administrator role that has permissions to manage application/workload identities in Microsoft Entra.

Identity admins using [Security Copilot as a part of the Microsoft Entra admin center](#) can choose from a set of app risk starter prompts that appear at the top of the Security Copilot window. Select from suggested prompts that may appear after a response. App risk starter prompts will appear in application-related admin center blades: **Enterprise applications**, **App Registrations**, and **Identity Protection Risky workload identities**.



Explore Microsoft Entra risky service principals

Jason begins by asking natural language questions to get a better picture of the risk "hot spots". This uses [ID Protection risky workload identity](#) data as an initial filter on the scale of apps in their tenant based on our Microsoft detections. These service principals carry an elevated risk of compromise.

He uses any of the following prompts to get the information he needs:

- *Show me risky apps*

- Are any apps at risk of being malicious or compromised?
- List 5 apps with High Risk Level. Format the table as follows: Display Name | ID | Risk State
- List the apps with Risk State "Confirmed compromise".
- Show me the details of risky app with ID {ServicePrincipalObjectId} (or App ID {ApplicationId})

 **Important**

You must use an account that is authorized to administer ID Protection for this skill to return risk information. Your tenant must also be licensed for [Workload Identities Premium](#).

Explore Microsoft Entra service principals

To get more information about these service principals identified as risky, Jason asks for more information from Microsoft Entra, including information like the owner.

He uses the following prompts to get the information he needs:

- Tell me more about these service principals (from previous response)
- Give me details about service principal with {DisplayName} (or {ServicePrincipalId})
- Give me a list of owners for these apps?

Explore Microsoft Entra applications

Jason also wants to understand more about the applications globally, such as details about the publisher and publisher verification status.

Jason uses the following prompts to retrieve selected application properties:

- Tell me more about the application {DisplayName} or {AppId}
- Tell me more about these apps (from previous response)

View the permissions granted on a Microsoft Entra service principal

Jason continues his assessment and wants to know what permissions have been granted to all or one of the apps to find the potential impact if compromised. This is normally difficult to evaluate across some of the different types of permissions ([API permissions](#) like User.Read.All + [Microsoft Entra administrator roles](#) like Application Administrator)

but Copilot simplifies it in a list in context of the investigation. This skill retrieves Delegated permissions, Application permissions, and Microsoft Entra administrator roles for a given Microsoft Entra service principal.

Jason can also identify high privilege permissions granted on a service principal, based on Microsoft's risk assessment. These are currently scoped to application permissions that generally enable tenant-wide access without user context and highly privileged Microsoft Entra administrator roles.

Important

This skill currently only looks at [API permissions](#) and [Entra administrator roles](#). It doesn't currently look at non-directory permissions granted in places like Azure RBAC or other authorization systems. High privileged permissions are limited to a static list of maintained by Microsoft that might evolve over time and it is not currently viewable or customizable by customers.

He uses the following prompts to get the permissions information he needs:

- *Which permissions are granted the app with ID {ServicePrincipalId} or app ID {AppId}?*
- *What permissions do the above risky apps have (from previous response)?*
- *Which permissions granted to this app are highly privileged?*

Explore unused Microsoft Entra applications

Jason realizes he has another "low hanging fruit" opportunity: to reduce risk by removing unused apps. These are quick wins because:

1. Removing an unused app addresses many other risks with a single remediation action.
2. You can often address unused apps aggressively through central action while keeping the risk of outage or business disruption low, since users aren't actually using the apps.

Using the Copilot skill integrated with the existing [Microsoft Entra recommendation for unused apps](#), Jason pulls the relevant data to investigate further or work with his team to improve their tenant security posture. The response includes links to specific apps for easier remediation. The analyst can also ask about a specific app's details directly in Security Copilot.

Note

The Copilot response returns a list of app registration or applications that are unused in past 90 days, which haven't been issued any tokens in that timeframe.

He uses the following prompts to get the information he needs:

- *Show me unused apps*
- *How many unused apps do I have?*

Explore Microsoft Entra Applications outside my tenant

Jason would also like to look into the risk factor of external apps or multitenant apps with a presence in his tenant that are registered in another organization's tenant. Since the security posture of these apps is impacted by the posture of the owning tenant, it's especially important to review these to identify risks and opportunities for surface area reduction. Copilot can return a list of service principals within the current tenant with a multitenant app registration outside of the user's tenant or details on if a particular service principal is registered outside the tenant.

Note

Jason can get a partial app list in Security Copilot and full list via a link to the [Microsoft Graph Explorer](#) query at the bottom of the response.

He uses the following prompts to get the information he needs:

- *Show me apps outside my tenant*
- *How many apps are from outside my tenant?*

Remediate

By using Security Copilot, Jason is able to gather comprehensive risk and basic information about the applications and service principals in their Microsoft Entra tenant. After completing his assessment, Jason takes action to remediate the risky applications. Security Copilot surfaces links to the Microsoft Entra admin center in responses for administrators to take the appropriate remediation actions.

He reads about [managing access and security for applications](#), [security workload identities](#), [protecting against consent phishing](#), and [response playbooks](#) to determine

possible actions to take next.

Next steps

Learn more about:

- [Manage application access and security](#)
 - [What is risk in ID Protection?](#)
 - [Securing workload identities with Microsoft Entra ID Protection](#)
 - [Protect against consent phishing - Microsoft Entra ID | Microsoft Learn](#)
 - [Compromised and malicious applications investigation](#)
 - [Respond to identity threats using risky user summarization](#)
-

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Responsible AI FAQ: Copilot in Microsoft Entra

Article • 11/19/2024

This FAQ provides answers to common questions about Responsible AI as it relates to Security Copilot in Microsoft Entra. Learn how this AI-powered security solution enhances the efficiency and capabilities of IT and security professionals to improve security outcomes.

What is Copilot in Microsoft Entra?

Microsoft Security Copilot is a natural language, generative AI-powered security solution that helps increase the efficiency and capabilities of IT and Security professionals to improve security outcomes at machine speed and scale. It draws context from plugins and data to answer prompts so that security professionals and IT admins can help keep their organizations secure.

What can Copilot in Microsoft Entra do?

Security Copilot embedded in Microsoft Entra helps answer questions in natural language so that you can receive actionable responses to common tasks related to identity and access management.

It helps in the following scenarios:

- Sign-in troubleshooting
- Inspect sign-in logs, uncover the cause of failed sign-ins including policies evaluated for MFA and Conditional Access.
- Identity Protection for users and workload identities
- Identify and mitigate risks of compromise for users, service principals, and workload identities
- Identity administration
- Find user account information, group ownership and membership details, and changes to users, apps, groups, and roles from Microsoft Entra audit logs.

What are Security Copilot in Microsoft Entra's intended uses?

Security Copilot embedded in Microsoft Entra is intended for use by identity and access administrators. Ask questions about Microsoft Entra data and documentation, find and summarize details about users, groups, apps, sign-ins, and changes to those objects.

How was Security Copilot in Microsoft Entra evaluated? What metrics are used to measure performance?

Security Copilot underwent substantial testing prior to being released. Testing included red teaming, which is the practice of rigorously testing the product to identify failure modes and scenarios that might cause Security Copilot to do or say things outside of its intended uses or that don't support the Microsoft AI Principles.

Now that it's released, user feedback is critical in helping Microsoft improve the system. You have the option of providing feedback whenever you receive output from Security Copilot embedded in Microsoft Entra. When a response is inaccurate, incomplete, or unclear, give it a thumbs down and indicate one or more categories to flag any objectionable output. You can also confirm when responses are useful and accurate by giving it a thumbs up. These buttons appear at the bottom of every Security Copilot response and your feedback goes directly to Microsoft to help us improve.

What are the limitations of Security Copilot embedded in Microsoft Entra? How can users minimize the impact of Security Copilot in Microsoft Entra's limitations when using the system?

Preview features aren't meant for production use and might have limited functionality.

Like any AI-powered technology, Security Copilot doesn't get everything right. However, you can help improve its responses by providing your observations using the feedback tool, which is built into the platform.

The system is designed to respond to prompts related to identity and access administration. Prompts outside the scope of Microsoft Entra might result in responses that lack accuracy and comprehensiveness.

The system might not be able to process long prompts, such as hundreds of thousands of characters.

Use of Security Copilot embedded in Microsoft Entra might be subject to usage limits or capacity throttling. Even short prompts can take time (up to several minutes) and require a high number of security consumption units.

What operational factors and settings allow for effective and responsible use of Security Copilot in Microsoft Entra?

You can use everyday words to describe what you'd like Security Copilot to do. For example: *Find this user* or *Who owns this group?*

You can also choose from a set of prompts provided in Security Copilot in Microsoft Entra and select from a set of suggested prompts to continue a conversation.

You can provide feedback about a response, including reporting anything unacceptable to Microsoft.

How do I provide feedback on Security Copilot embedded in Microsoft Entra?

You have the option of providing feedback whenever you receive output from Security Copilot embedded in Microsoft Entra. When a response is inaccurate, incomplete, or unclear, give it a thumbs down and indicate one or more categories to flag any objectionable output. You can also confirm when responses are useful and accurate by giving it a thumbs up. These buttons appear at the bottom of every Security Copilot response and your feedback goes directly to Microsoft to help us improve.

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Find help and get support for Microsoft Entra ID

Article • 03/18/2025

Microsoft documentation and learning content provide quality support and troubleshooting information, but if you have a problem not covered in our content, there are several options to get help and support for Microsoft Entra ID.

This article provides the options to find support from the Microsoft community and how to submit a support request with Microsoft.

Ask the Microsoft community

Start with our Microsoft community members who might have an answer to your question. These communities provide support, feedback, and general discussions on Microsoft products and services. Before creating a support request, check out the following resources for answers and information.

- Explore how-to information, quickstarts, and code samples for IT professionals and developers with our [technical documentation at learn.microsoft.com](#).
- Post a question to [Microsoft Q&A](#) to get answers to your identity and access questions directly from Microsoft engineers, Most Valuable Professionals (MVPs), and other members of our expert community.
- Collaborate, share, and learn from other customers and IT Pro partners in the [Microsoft Technical Community](#). Join the community to post questions and submit your ideas. Stay in the loop with announcements, blog posts, ask-me-anything (AMA) interactions with experts, and more.
- Be your own administrator and prototype apps and solutions on your fully pre-provisioned sandbox subscription with the [Azure Developer Program](#).

Microsoft Q&A best practices

[Microsoft Q&A](#) is Microsoft's recommended source for community support. From the Q&A home page, choose one of the following tabs:

- *Questions*: The main page for technical questions and answers at Microsoft.
- *Tags*: Use tags, which are keywords that categorize your question with other similar questions.
- *Help*: Get answers to frequently asked questions, troubleshoot common issues, and discover features related to Microsoft Q&A.

To ask a question, choose the **Ask a question** button at the top right of any Q&A page. You can also get your questions answered faster by using [AI Assist](#).

When asking a question, we recommend you follow these best practices:

- View the *Questions* and *Tags* pages first to search for product and service-related keywords, as you might find a previously posted solution. Use the filter to narrow the search results.
- Submit your questions in the language of the Q&A site you are on. This helps ensure that our community of experts can provide accurate and helpful answers to your question.
- Use tags when posting a question. You can select up to five tags to describe your question. Choose tags that relate most closely to your scenario to increase discoverability of your question among the community experts on Q&A.
- Include all the details of your issue in the **Question details** field. Start by asking *one* question in the body to ensure the highest quality answers. Next, include the following details in your request:
 - A summary of what you are attempting to accomplish
 - Any steps that you already took
 - Any relevant error messages
 - Unique aspects of your scenario or configuration
 - Any other pertinent information

For more information, see [Tips for writing quality questions](#).

Diagnose and solve problems

The Microsoft Entra admin center and Azure portal have built-in tools to help troubleshoot common problems. There are diagnostic tools for single-sign on, devices, and sign-ins. There's also guidance provided for many common problems.

Search for or select **Diagnose and solve problems** from the navigation menu.

The screenshot shows the Microsoft Entra admin center interface. The left sidebar has a red box around the 'Diagnose & solve problems' link. The main content area is titled 'Diagnose and solve problems'. It includes a search bar, a 'How can we help you?' section with a search input field, and a 'Troubleshooters' section with three cards: 'Diagnose SSO problems', 'Windows 10+ related issue?', and 'Sign-in Diagnostic'. Below these are 'Common problems' sections for '1603 error/Unable to install the synchronization service', 'App Registration', and 'Configuration and installation issues with Microsoft Entra Connect'. A magnifying glass icon is in the bottom right corner.

Some of the diagnostic tools require specific roles to use the tool. For example, you need to be at least a **Billing administrator** to use the sign-in diagnostic tool. Contact your local administrator for assistance or to get the necessary permissions.

Open a support request

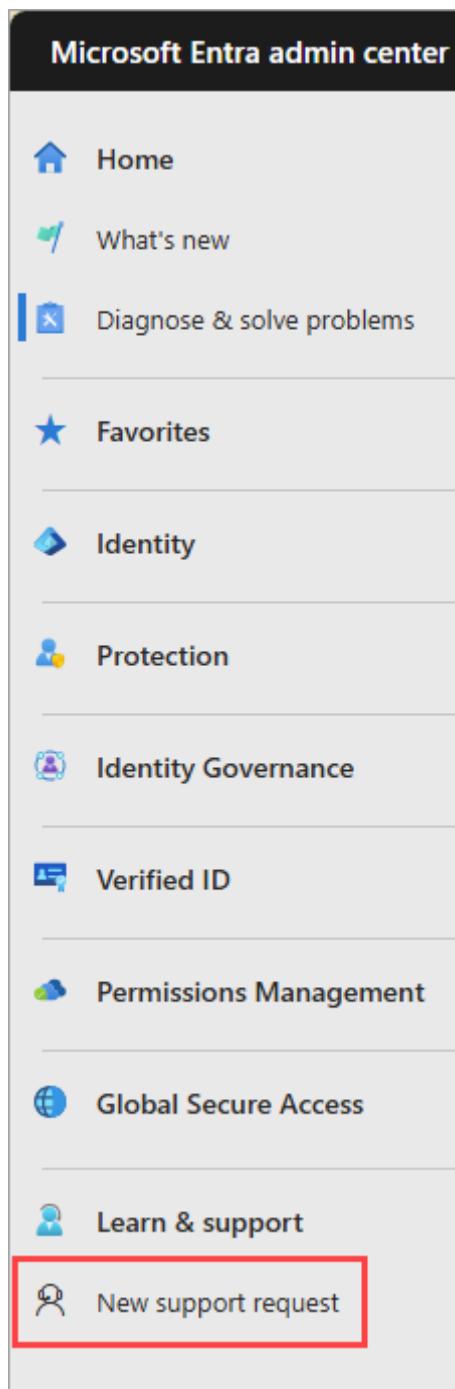
If you're unable to find answers by using the previously mentioned resources, you can open an online support request.

Online support requests can be created from several places in the admin center:

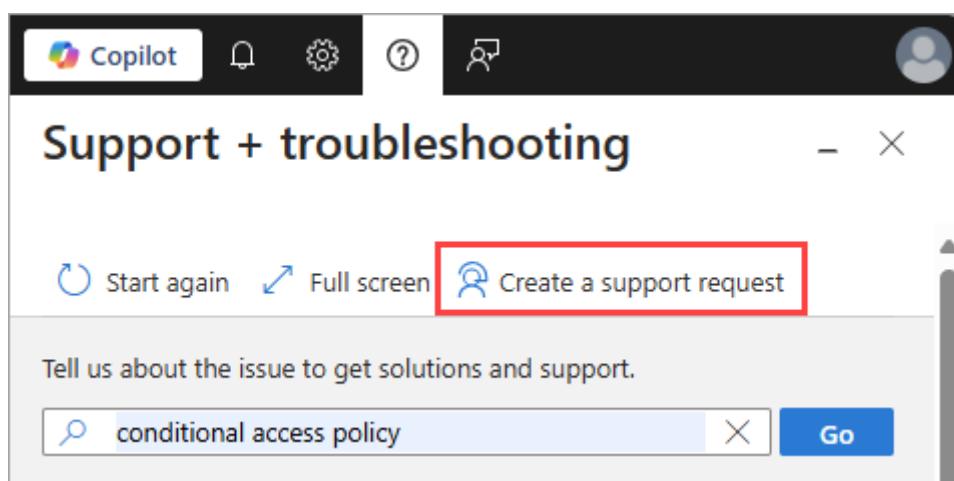
- From the **Diagnose and solve problems** page:

The screenshot shows the 'Diagnose and solve problems' page with a red box around the 'New Support Request' button in the top navigation bar.

- From the left-hand navigation menu:



- From the help icon, after following the help prompts:



Tips for creating online support requests

- Open a support request for only a single problem
 - We try to connect you to the support engineers who are subject matter experts for your problem.
 - Microsoft Entra engineering teams prioritize their work based on incidents that are generated from support, so you're often contributing to service improvements.
- Be as descriptive and specific as possible.
 - Self-help solutions might be presented to you based on the information you provide, which might help you resolve the issue without creating a support request.
 - The more details you provide, the faster we can help you.
- Diagnostic information might be collected as a part of the support request.
 - Selecting Yes allows support to gather [advanced diagnostic information](#) from the subscriptions associated with your request.
 - If you prefer not to share this information, select No. For more information about the types of files we might collect, see [Advanced diagnostic information logs](#).
- Support is available online and by phone for Microsoft paid and trial subscriptions
 - Support is provided for global technical, presales, billing, and subscription issues.
 - Phone support and online billing support are available in additional languages.
- Explore the [support options and choose the plan](#) that best fits your scenario.
- Microsoft customers can create and manage support requests in the Azure portal and the Microsoft Entra admin center.

ⓘ Note

- If you're using Microsoft Entra External ID in an external tenant, the support request feature is currently unavailable for external tenant technical issues. Instead, use the **Give Feedback** link on the **New support request** page. Or, switch to your Microsoft Entra workforce tenant and [open a support request](#).
- If you're using Azure AD B2C, open a support ticket by first switching to a Microsoft Entra tenant that has an Azure subscription associated with it. Typically, this is your employee tenant or the default tenant created for you

when you signed up for an Azure subscription. To learn more, see [how an Azure subscription is related to Microsoft Entra ID](#).

To open a support request in Microsoft Entra ID:

The steps to open a support request represent the high-level process. The actual steps vary based on your scenario and the values you select.

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Service Support Administrator**.
2. Open a new support request.
3. Follow the prompts to complete the **Problem description** section.
4. Based on the information you provided, review the information in the **Recommended solution** section for guidance or troubleshooting steps.
 - These solutions are written by Azure engineers and technical content developers and should resolve most common problems.
 - If you're still unable to resolve the issue, select **Next** to continue creating the support request.
5. Provide thorough and detailed information in the **Additional details** section to help us route your support request to the right team.
 - If possible, tell us when the problem started and any steps to reproduce it.
 - You can upload a file, such as a log file or output from diagnostics. For more information on file uploads, see [File upload guidelines](#).
6. Select **Next** when you've completed all of the necessary information.
7. Review all of the details you provided and select **Create**.

A support engineer will contact you using the method you indicated. For information about initial response times, see [Support scope and responsiveness](#).

Other options for creating a support request

If you already have an Azure Support plan, [open a support request here](#).

If you're not an Azure customer, you can open a support request with [Microsoft Support for business](#).

Microsoft Security Copilot

The Microsoft Security Copilot is a platform that brings together the power of AI and human expertise to help you and your teams respond to threats faster and more effectively. The capabilities of this powerful feature are under continuous development, with several features available today. These features can also be used for some troubleshooting and support scenarios. For more information, see [Copilot in Microsoft Entra](#)

Get Microsoft 365 admin center support

Support for Microsoft Entra ID in the [Microsoft 365 admin center](#) is offered for administrators through the admin center. Review the [support for Microsoft 365 for business article](#).

Stay informed

Things can change quickly. The following resources provide updates and information on the latest releases.

- [What's new in Microsoft Entra ID](#): Get to know what's new in Microsoft Entra ID including the latest release notes, known issues, bug fixes, deprecated functionality, and upcoming changes.
- [Microsoft Entra identity blog](#): Get news and information about Microsoft Entra ID.
- [Azure updates](#): Learn about important product updates, roadmap, and announcements.

Related content

- [Post a question to Microsoft Q&A](#)
- [Join the Microsoft Technical Community](#)
- Learn about the [diagnostic data Azure identity support can access](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)

Quarantine unsanctioned tenants

Article • 04/15/2025

Important

Refer to this article only after reviewing [the Microsoft Cloud Footprint FAQ](#) to discover your organization's inventory of tenants. This article outlines the specific existing Microsoft Entra capabilities administrators can leverage within their primary tenant to quarantine suspected unsanctioned tenants in their discovered list of tenants.

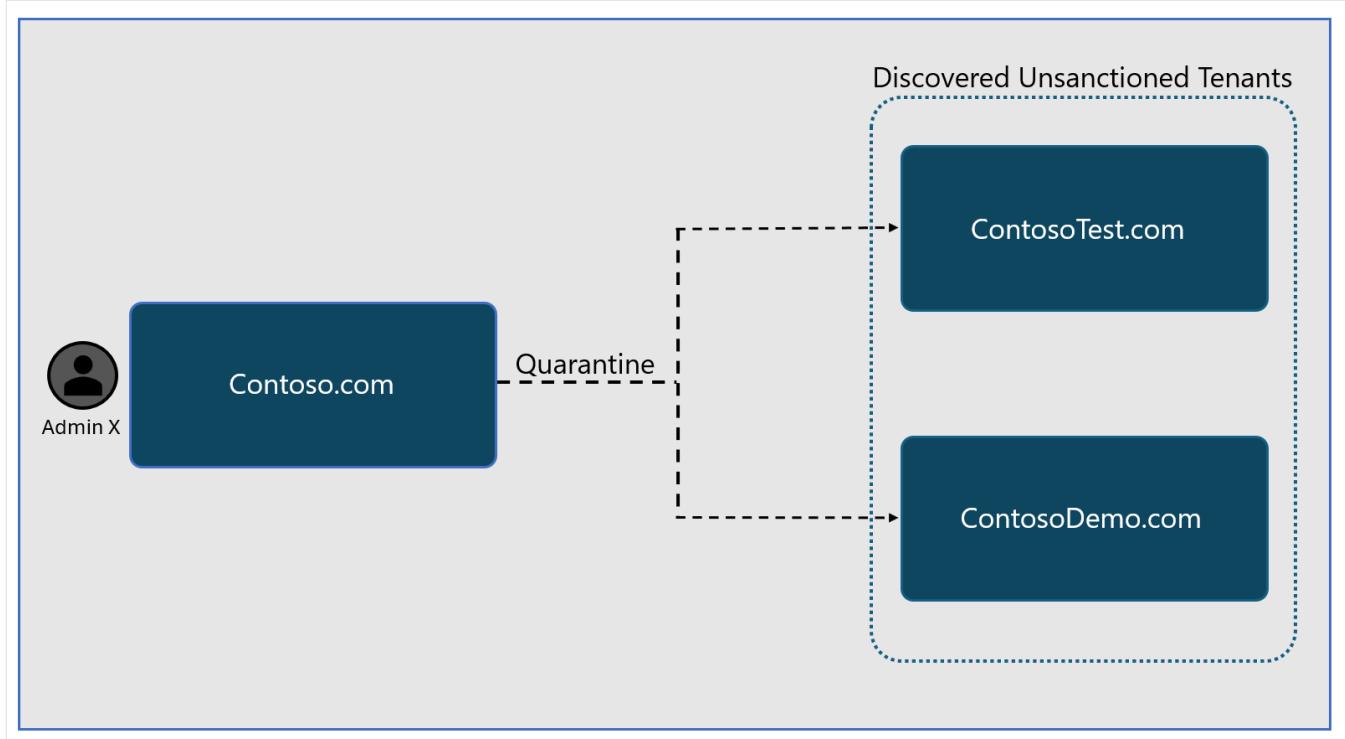
What does it mean to quarantine a tenant?

Quarantine involves isolating suspected unsanctioned tenants by using existing Microsoft Entra capabilities. This immediately reduces security risk that exists from exposure to such tenants that you do not have administrative control of within your environment. By isolating, you introduce friction between your tenant and theirs, which acts as a scream test. This friction prompts administrators of the suspected tenants to contact you in need of assistance, giving you the opportunity to verify the legitimacy of the relationships with these tenants and/or regain control over them. If no one is to contact you, then you can leave the tenants in the quarantined state indefinitely.

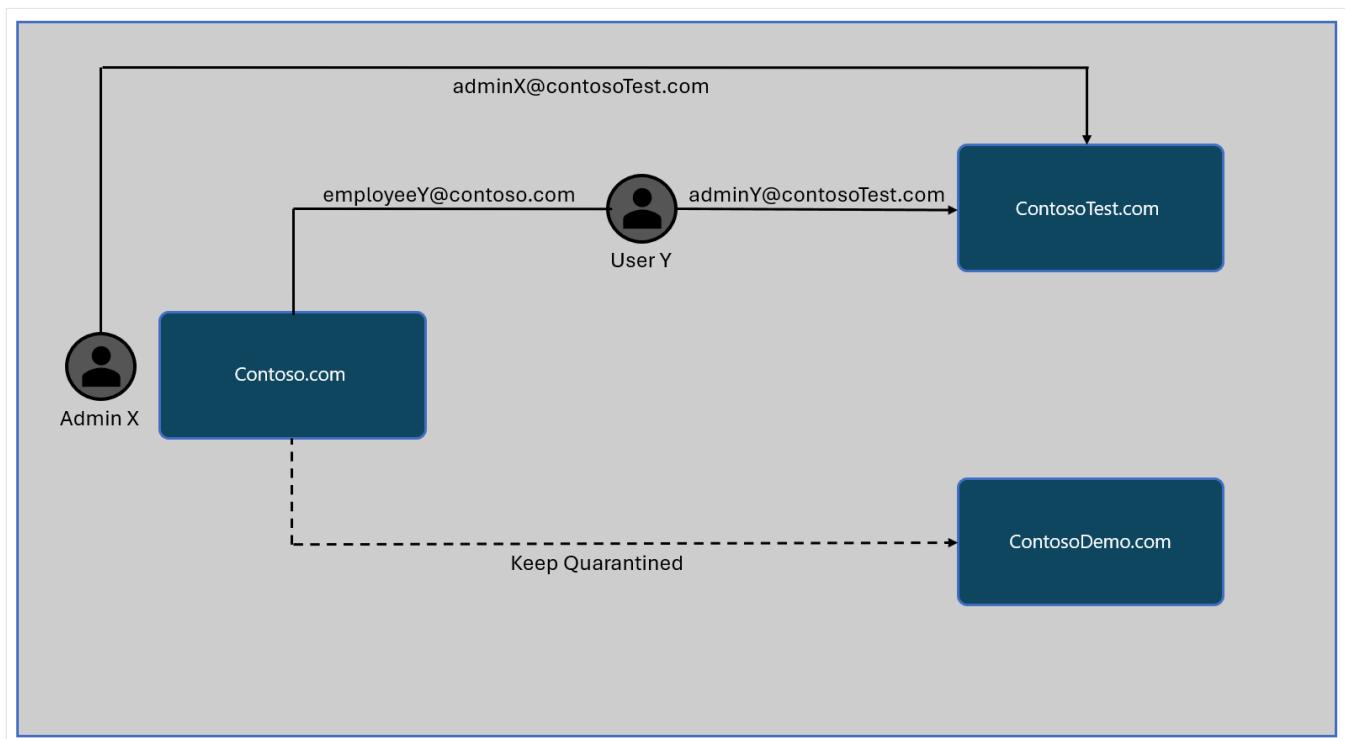
When should I quarantine a tenant?

You are an IT Admin for the company "Contoso" with the primary tenant of "Contoso.com." To secure data in the central Contoso tenant, you need to ensure users and applications with privileged access to your tenant are in tenants that properly secure these resources. Likewise, you want to ensure that external tenants in which your tenant has permissions into are known and following secure practices. To secure Contoso, you want to find all tenants that have inbound or outbound relationships with your primary tenant. After following the [Microsoft Cloud Footprint FAQ](#), you have identified a few potential tenants that may or may not belong to your company. Let's call these tenants ContosoTest.com and ContosoDemo.com for scenario purposes. Because you don't know who the global admins are for these tenants, you worry they are possibly employee-managed and do not comply with your organization's security policies. This poses a major security risk to your environment if they stay unmanaged. Since you don't have direct control over ContosoTest.com and ContosoDemo.com, you can only modify settings on the Contoso.com tenant. You want to quarantine them to minimize potential vulnerabilities that come from the exposure to these tenants. However, it's crucial that any changes you make are easily reversible, ensuring that no critical systems are unintentionally affected in the process. After quarantine, you introduced enough friction

between your tenant and the suspected tenants to encourage the administrators of the tenants to contact your helpdesk.



The administrator of the ContosoTest.com tenant contacts you. At this point, you determine that the tenant was employee-created and that you should be added as an administrator within the tenant to regain control. You no longer quarantine the ContosoTest.com tenant. However, no administrators from the ContosoDemo.com tenant contact you, so you leave the tenant in the quarantined state.



How can I use Microsoft Entra's capabilities to quarantine suspected tenants?

Using External ID Cross-tenant Access Settings to block user sign-in

License Required: Entra ID P1

Actions Against Suspected Tenant:

Microsoft Entra organizations can use Cross-tenant access with External ID to scope which users of other external Entra organizations have access to your resources and which users from your organization have access to other external Entra organizations. These policies let you restrict inbound or outbound login attempts with a suspect tenant without disrupting collaboration with other tenants. An administrator can [add an organization](#) and configure customized settings to block [inbound](#) and [outbound](#) user-sign for the suspected tenant.

Secure-by-default:

An administrator can [configure default settings](#) to block all inbound sign-in attempts from external users of a suspected tenant. Likewise, one can block all outbound user sign-in for users of your own tenant into a suspected tenant. Then, you can [add an organization](#) and configure customized settings to allow user sign-in only [inbound](#) from and [outbound](#) to specified tenants. These settings would enable you to secure your tenant by default and only allow B2B collaboration with trusted tenants.

For more information on managing Cross-tenant access settings, see:

- [Cross-tenant access overview](#).
- [Cross-tenant access settings](#).

Using Global Secure Access and Universal Tenant Restrictions to block user sign-in

License Required: Entra ID P1

Actions Against Suspected Tenant:

Tenant Restrictions v2 (TRv2) and Global Secure Access (GSA) effectively prevent authentication into unauthorized or suspect tenants across all managed devices and networks. As an administrator, you can create policies to [block users from signing into and accessing the specific suspected tenant using custom TRv2 configurations](#). You can then apply these created

policies using [Universal Tenant Restrictions v2](#) as part of GSA to provide both authentication plane and data plane protection without disrupting authentication for other existing tenants.

Secure-by-default:

As an administrator, you can [configure default restrictions](#) and then [allow users to sign into and access specific organizations](#), Microsoft Entra ID would prevent authentication on to all other tenants once applying policies using [Universal Tenant Restrictions v2](#) as part of GSA. Enabling TRv2 in audit mode and applying TRv2 policies with GSA shows all activity including attempts to access foreign tenants.

For more information on using TRv2 and GSA, see:

- [What is Global Secure Access?](#)
- [Global Secure Access and Universal Tenant Restrictions](#)
- [Configure tenant restrictions - Microsoft Entra ID](#)

Revoking permissions for multitenants Applications and Service Principals

License Required: Entra ID P1

Actions Against Suspected Tenant:

Microsoft Entra allows customers to restrict inbound application access for third-party multitenant apps where the tenant in which the app was registered is considered a suspect tenant. To restrict access, administrators must find the correct service principal, which corresponds to the application registered in the suspect tenant. The `appOwnerOrganizationId` property on the service principal object lists the `tenantId` in which the application was registered. Capturing these service principals can only be done programmatically via MSGraph API:

MSGraph: Request Headers: { `ConsistencyLevel: eventual` }

HTTP

```
GET https://graph.microsoft.com/v1.0/servicePrincipals?  
$count=true&$filter=appOwnerOrganizationId eq {tenantId}
```

After finding the correct service principal, you can either [review and revoke permissions granted to the application](#) or [delete the service principal](#) all together. Deleting a service principal is a [restorable action up to 30 days](#).

For more information on multitenant apps and service principals, see Apps & service principals in Microsoft Entra ID.

- [Apps & service principals in Microsoft Entra ID](#)

Canceling subscriptions provisioned in suspected tenants

License Required: None, available to all paying customers with a Microsoft billing account

Actions Against Suspected Tenant:

Use the following resources when you discover a tenant based on your billing account relationships but do not recognize the tenant which the subscription services are provisioned within. Canceled Azure and Microsoft 365 subscriptions can be reactivated during the grace period ([30 to 90 days after canceling](#)) before being permanently deleted. If needed, contact [support](#) for assistance on canceling and deleting subscriptions.

- For more information on quarantining by canceling Azure, see [Cancel and delete your Azure subscription](#).
- For more information on quarantining by canceling Microsoft 365, see [Cancel your Microsoft business subscription in the Microsoft 365 admin center](#).

Related content

- [Microsoft Cloud Footprint FAQ](#)

Tenant inaccessible due to inactivity

Article • 01/16/2025

Configured tenants no longer in use may still generate costs for your organization. Making a tenant inaccessible due to inactivity helps reduce unnecessary expenses. This article discusses how to handle an inaccessible tenant, reactivation, and guidance for both administrators and application developers.

If you try to access the tenant, you receive a message similar to the example shown.

Error message `Error message: AADSTS5000225: This tenant has been blocked due to inactivity. To learn more about ...` is expected for tenants' inaccessible due to inactivity.

Sign-in failed

Error code: AADSTS5000225

Error message: AADSTS5000225: This tenant has been blocked due to inactivity. To learn more about tenant lifecycle policies, see [https://aka.ms/TenantLifecycle Trace](https://aka.ms/TenantLifecycleTrace)
ID: 3c4c057b-36ef-4f3f-a0f0-9a7578e42f00 Correlation ID: 611e521a-bed9-43e4-98ff-33a8b980f055 Timestamp: 2024-01-18 17:59:38Z



[Learn more about the error >](#)

[Try again >](#)

[Perform self diagnostics >](#)

[Go to Azure status page >](#)

[Sign out >](#)

[Contact support >](#)

[Debugging information](#)

Browser ID: 611e521a-bed9-43e4-98ff-33a8b980f055



Administrators can request a tenant to be reactivated within 20 days of the tenant entering an inactive state. Tenants that remain in this state for longer than 20 days are deleted.

Take the appropriate steps depending on your goals for the tenant and your role in the environment.

Administrators

If you need to reactivate your tenant:

- The tenant administrator can reach out to Microsoft, see the [global support phone numbers](#).

- Refrain from submitting another assistance request while your existing case is in process and until you receive a response with a decision on this case.

If you don't plan to reactivate your tenant:

- The tenant is deleted after 20 days of being inaccessible due to inactivity and it isn't recoverable.
- Review Microsoft's data protection policies, [here](#).

Application owners/developers

- Minimize the number of authentication requests sent to this deactivated tenant until the tenant is reactivated.
- Refrain from submitting another assistance request. You are contacted once that a decision is made.
- Review Microsoft's [data protection policies](#).

Related content

- [Quickstart: Create a new tenant in Microsoft Entra ID](#)
- [Add your custom domain name to your tenant](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)

What's new (preview)

Article • 11/18/2024

Microsoft Entra is updated regularly to deliver new features, enhance existing functionality, fix defects, and address customer feedback. The best way to stay current with these developments is to visit **What's new (preview)** in the [Microsoft Entra admin center](#).

What's new is an information hub that provides a consolidated view of the Microsoft Entra roadmap and change announcements. It gives administrators a centralized location to track, learn, and plan for the releases and changes across the Microsoft Entra family of products.

The remaining sections describe the features and functionality of the **What's new** experience.

Explore What's new

Highlights

The **Highlights** tab summarizes important product releases and impactful changes. From the Highlights tab, you can select an announcement or release to view its details and access links to documentation for more information.

Top announcement

Microsoft Security Service
Edge now generally available

Secure access to any app or resource, from anywhere, with an identity-centric Security Service Edge (SSE) solution.

[View details](#)

New release highlight

Phishing resistant authentication with passkeys in Microsoft Authenticator

Public preview refresh: Device-bound passkey support in Microsoft Authenticator

[View details](#)

Change announcement highlight

Upcoming MFA Enforcement on Microsoft Entra admin center

Learn how multifactor authentication (MFA) can protect your data and identity and get ready for upcoming MFA requirement.

[View details](#)

Change announcement highlights

Change announcements

The following change announcements represent upcoming deprecations, breaking changes, feature changes, and UX changes.

Title	Target Date
Important Update: Azure ...	6/30/2025
Upcoming license enforce...	10/1/2024
Moving from a browse-ba...	10/30/2024

[View all](#)

New release highlights

New products and features

The following new releases from the last 30 days are available for your evaluation. Help us make them better!

Title	State
Native Authentication for ...	GA
Paskey authentication in ...	Public Preview
Suspicious API Traffic det...	GA

[View all](#)

Roadmap

The **Roadmap** tab lists the details of public preview and recent general availability releases in a sortable table. From the table, you can select a release to view the release **Details** which includes an overview and link to learn more.

What's new

Highlights **Roadmap** Change announcements

Find and try new identity and network access solutions for Microsoft Entra.

80 updates found

<input type="checkbox"/> Title ↑↓	Category ↑↓	Service ↑↓	Release Type ↑↓	Release Date ↑	State ↑↓
<input checked="" type="checkbox"/> Platform SSO for macOS...	User Authentication	Authentications (Logins)	Public Preview	5/10/2024	Available
<input type="checkbox"/> Workflow History Insigh...	Identity Governance	Lifecycle Workflows	Public Preview	5/15/2024	Available
<input type="checkbox"/> Configure Lifecycle Wor...	Identity Governance	Lifecycle Workflows	Public Preview	5/15/2024	Available

Details

Platform SSO for macOS with Entra ID

Overview

Here's what you will see in this release:

Platform SSO for macOS is now available in public preview with Microsoft Entra ID. Platform SSO is an enhancement to the Microsoft Enterprise SSO plug-in for Apple Devices that makes usage and management of Mac devices more seamless and secure than ever. At the start of public preview, Platform SSO will work with Microsoft Intune. Other Mobile Device Management (MDM) providers will be coming soon. Please contact your MDM provider for more information on support and availability.

Next steps

[Learn more](#)

To find a release, you can customize the table view using the following controls:

- Search:** Enter keywords to find a specific release.
- Add filter:** Filter by **Release Type** or by **State**.

- **Category:** Filter by product and/or feature category (for example, *User Authentication, Identity Governance*)
- **Release Date:** Filter by date range.
- **Manage view:** Remove or add columns.

Roadmap column descriptions

The following are the descriptions for the sortable columns in the roadmap table:

[\[+\] Expand table](#)

Column	Description
Title	Brief description of the product or feature.
Category	The identity and network access category of the product or feature (for example, <i>Identity Governance, Identity Security & Protection</i>).
Service	The Microsoft Entra service of the product or feature (for example, <i>Entitlement Management, Conditional Access</i>).
Release Type	The lifecycle phase of the release: <ul style="list-style-type: none"> • <i>Public Preview:</i> Available to all customers with the required license. The release might include limited customer support, and standard service level agreements don't apply. • <i>GA</i> (general availability): Available to all licensed customers. The release is supported via all Microsoft support channels.
Release Date	Date the release is made available.
State	Indicates whether the release is <i>Available</i> or <i>Coming Soon</i> .

Change announcements

The **Change announcements** tab lists the upcoming changes to existing products and features in a sortable table. From the table, you can select a change announcement to view the change **Details** which includes an overview of what's changing and link to learn more.

The screenshot shows the Microsoft Entra Change Announcements page. At the top, there's a navigation bar with 'Home > What's new' and a 'Change announcements' tab highlighted with a red box. Below the navigation, there are buttons for 'Refresh', 'Manage view', and 'Got feedback?'. A callout box labeled 'Details' provides information about enhancements to attribute collection in Entra External ID, mentioning improved accessibility and enhanced context. It also includes a 'Next steps' section with a 'Learn more' link. The main content area displays a table of 55 updates found, with columns for Title, Service, Change Type, Announcement Date, Target Date, and Action Required. One row is selected, showing 'Enhancements to Attribut...' under 'Service' and 'UX Change' under 'Change Type'. A red dashed box highlights the 'Action Required' column.

Title	Service	Change Type	Announcement Date	Target Date	Action Required
Enhancements to Attribut...	B2C - Consumer Identity Ma...	UX Change	11/2/2024	2/3/2025	No
Retirement of legacy user ...	Authentications (Logins)	Retirement	11/1/2024	10/31/2024	No
Encrypted Access Tokens f...	Enterprise Apps	Breaking Change	10/31/2024	10/31/2024	Yes

To find a change announcement, you can customize the table view using the following controls:

- Search:** Enter keywords to find a specific release.
- Add filter:** Filter by **Action Required** or by **Change Type**.
- Service:** Filter by the product or feature service (for example, *Entitlement Management, Conditional Access*)
- Release Date:** Filter by date range.
- Manage view:** Remove or add columns.

Roadmap column descriptions

The following are the descriptions for the sortable columns in the roadmap table:

[Expand table](#)

Column	Description
Title	Brief description of the product or feature.
Service	The Microsoft Entra service of the product or feature (for example, <i>Entitlement Management, Conditional Access</i>).
Change Type	The scope of the change: <ul style="list-style-type: none"> <i>UX Change:</i> A user experience change that doesn't require action. <i>Feature Change:</i> A change to existing functionality that might require action. <i>Breaking Change:</i> A change that is expected to break the user experience if no action is taken. <i>Deprecation:</i> The product or feature is no longer available to new customers and is scheduled for retirement. Deprecated products or features are still available and supported for existing customers.

Column	Description
	<ul style="list-style-type: none"> • <i>Retirement</i>: The product or feature is no longer available or supported. • End of Support: Product or feature is no longer supported for existing customers.
Announcement Date	Date of the announcement.
Target Date	The release date of the change.
Action Required	Indicates whether the change requires a user to take action.

What's new (preview) FAQ

Why do we need a What's new feature when we already have the Microsoft 365 and Azure roadmaps?

Not all Microsoft Entra products are part of Microsoft 365 and Azure (for example, Microsoft Entra Permissions Management, Microsoft Entra External ID). The What's new feature ensures transparency about new features and changes across all Microsoft Entra products in a centralized location.

Is What's new publicly accessible like the Microsoft 365 roadmap?

No, to access What's new you must sign in to the Microsoft Entra admin center. The sign in requirement enables us to provide a more personalized experience, tailored specifically to each tenant in future versions of What's new.

Can I consume Microsoft Entra updates programmatically and automate processes?

Yes, in the future you can use [Microsoft Graph](#) to retrieve updates (currently in beta) and automate processes. For example, you can automate responses to feature lifecycle events or integrate them with a product lifecycle management system.

Can I still use the existing RSS feeds and view the public release notes for What's new information?

Yes, the existing RSS feeds and [release notes](#) are still available.

Can I access What's new in the Microsoft 365 or Azure portal?

No, What's new is available only in the Microsoft Entra admin center.

How can I provide feedback about this feature?

To share feedback, go to the **Roadmap** tab or the **Change announcements** tab and select **Got feedback?**.

Do I need a specific Microsoft Entra role to access What's new?

No, all Microsoft Entra ID roles can access the What's new feature.

Are there any licensing requirements to access What's new?

No, What's new is available to all Microsoft Entra customers, including Microsoft Entra ID Free.

Can guest users in my tenant access What's new?

Yes, What's new is accessible to your business guests.

Is What's new available to government cloud customers?

Currently, What's new is only available to public cloud customers. But, there are plans to deliver the What's new experience to government clouds in the future.

Does What's new include all Microsoft Entra products?

Yes, What's new provides a consolidated view of the releases and change announcements across the Microsoft Entra product family.

Related content

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Microsoft Entra releases and announcements

Article • 04/30/2025

This article provides information about the latest releases and change announcements across the Microsoft Entra family of products over the last six months (updated monthly). If you're looking for information that's older than six months, see: [Archive for What's new in Microsoft Entra](#).

Get notified about when to revisit this page for updates by copying and pasting this URL:

`https://learn.microsoft.com/api/search/rss?search=%22Release+notes+-+Azure+Active+Directory%22&locale=en-us` into your  feed reader.

April 2025

Public Preview - Conditional Access Optimization Agent in Microsoft Entra

Type: New feature

Service category: Conditional Access

Product capability: Identity Security & Protection

[Conditional Access Optimization Agent in Microsoft Entra](#) monitors for new users or apps not covered by existing policies, identifies necessary updates to close security gaps, and recommends quick fixes for identity teams to apply with a single selection. For more information, see: [Microsoft Entra Conditional Access optimization agent](#).

Public Preview - Microsoft Entra ID Governance: Suggested access packages in My Access

Type: New feature

Service category: Entitlement Management

Product capability: Entitlement Management

In December 2024, we introduced a new feature in My Access: a curated list of suggested access packages. Users view the most relevant access packages, based on their peers' access packages and previous assignments, without scrolling through a long list. By May 2025, suggestions will be enabled by default and we'll introduce a new card in the Microsoft Entra

Admin Center Entitlement Management control configurations for admins to see My Access settings. We recommend admins turn on the peer-based insights for suggested access packages via this setting. For more information, see: [Suggested access packages in My Access \(Preview\)](#).

Public Preview - Conditional Access What If evaluation API

Type: New feature

Service category: Conditional Access

Product capability: Access Control

Conditional Access What If evaluation API – Leverage the What If tool using the Microsoft Graph API to programmatically evaluate the applicability of conditional access policies in your tenant on user and service principal sign-ins. For more information, see: [conditionalAccessRoot: evaluate](#).

Public Preview - Manage refresh tokens for mover and leaver scenarios with Lifecycle Workflows

Type: New feature

Service category: Lifecycle Workflows

Product capability: Identity Governance

Now customers can configure a Lifecycle workflows task to automatically revoke access tokens when employees move within, or leave, the organization. For more information, see: [Revoke all refresh tokens for user \(Preview\)](#).

General Availability - Use managed identities as credentials in Microsoft Entra apps

Type: New feature

Service category: Managed identities for Azure resources

Product capability: Identity Security & Protection

You can now use managed identities as federated credentials for Microsoft Entra apps, enabling secure, secret-less authentication in both single- and multi-tenant scenarios. This eliminates the need to store and manage client secrets or certificates when using Microsoft Entra app to access Azure resources across tenants. This capability aligns with Microsoft's

Secure Future Initiative [🔗](#) pillar of protecting identities and secrets across systems. Learn how to configure this capability in the [official documentation](#).

Plan for change - Roll out of Application Based Authentication on Microsoft Entra Connect Sync

Type: Plan for change

Service category: Microsoft Entra Connect

Product capability: Microsoft Entra Connect

What is changing

Microsoft Entra Connect creates and uses a [Microsoft Entra Connector account](#) to authenticate and sync identities from Active Directory to Microsoft Entra ID. The account uses a locally stored password to authenticate with Microsoft Entra ID. To enhance the security of the Microsoft Entra Connect application sync process, we will, in the coming week roll out support for "Application based Authentication" (ABA), which uses a Microsoft Entra ID application based identity and Oauth 2.0 client credential flow to authenticate with Microsoft Entra ID. To enable this, Microsoft Entra Connect will create a single tenant 3rd party application in customer's Microsoft Entra ID tenant, register a certificate as the credential for the application, and authorize the application to perform on-premises directory synchronization

The Microsoft Entra Connect Sync .msi installation file for this change will be exclusively available in the Microsoft Entra admin center within the [Microsoft Entra Connect pane](#) [🔗](#).

Check our [version history page](#) in the next week for more details of the change.

March 2025

Microsoft Entra Permissions Management end of sale and retirement

Type: Plan for change

Service category: Other

Product capability: Permissions Management

Effective April 1, 2025, Microsoft Entra Permissions Management (MEPM) will no longer be available for sale to new Enterprise Agreement or direct customers. Additionally, starting May

1, it will not be available for sale to new CSP customers. Effective October 1, 2025, we will retire Microsoft Entra Permissions Management and discontinue support of this product.

Existing customers will retain access to this product until September 30, 2025, with ongoing support for current functionalities. We have partnered with Delinea to provide an alternative solution, [Privilege Control for Cloud Entitlements \(PCCE\)](#), that offers similar capabilities to those provided by Microsoft Entra Permissions Management. The decision to phase out Microsoft Entra Permissions Management was done after deep consideration of our innovation portfolio and how we can focus on delivering the best innovations aligned to our differentiating areas and partner with the ecosystem on adjacencies. We remain committed to delivering top-tier solutions across the Microsoft Entra portfolio. For more information, see: [Important change announcement: Microsoft Entra Permissions Management end of sale and retirement](#).

Public Preview - Track and investigate identity activities with linkable identifiers in Microsoft Entra

Type: New feature

Service category: Authentications (Logins)

Product capability: User Authentication

Microsoft will standardize the linkable token identifiers, and expose them in both Microsoft Entra and workflow audit logs. This allows customers to join the logs to track, and investigate, any malicious activity. Currently linkable identifiers are available in Microsoft Entra sign in logs, Exchange Online audit logs, and MSGraph Activity logs.

For more information, see: [Track and investigate identity activities with linkable identifiers in Microsoft Entra \(preview\)](#).

General Availability- Conditional Access reauthentication policy

Type: New feature

Service category: Conditional Access

Product capability: Identity Security & Protection

Require reauthentication every time can be used for scenarios where you want to require a fresh authentication, every time a user performs specific actions like accessing sensitive

applications, securing resources behind VPN, or Securing privileged role elevation in PIM. For more information, see: [Require reauthentication every time](#).

General Availability- Custom Attributes support for Microsoft Entra Domain Services

Type: New feature

Service category: Microsoft Entra Domain Services

Product capability: Microsoft Entra Domain Services

Custom Attributes for Microsoft Entra Domain Services is now Generally Available. This capability allows customers to use Custom Attributes in their managed domains. Legacy applications often rely on custom attributes created in the past to store information, categorize objects, or enforce fine-grained access control over resources. For example, these applications might use custom attributes to store an employee ID in their directory and rely on these attributes in their application LDAP calls. Modifying legacy applications can be costly and risky, and customers might lack the necessary skills or knowledge to make these changes. Microsoft Entra Domain Services now supports custom attributes, enabling customers to migrate their legacy applications to the Azure cloud without modification. It also provides support to synchronize custom attributes from Microsoft Entra ID, allowing customers to benefit from Microsoft Entra ID services in the cloud. For more information, see: [Custom attributes for Microsoft Entra Domain Services](#).

Public Preview - Conditional Access Per-Policy Reporting

Type: New feature

Service category: Conditional Access

Product capability: Identity Security & Protection

Conditional Access Per-Policy Reporting enables admins to easily evaluate the impact of enabled and report-only Conditional Access policies on their organization, without using Log Analytics. This feature surfaces a graph for each policy in the Microsoft Entra Admin Center, visualizing the policy's impact on the tenant's past sign-ins. For more information, see: [Policy impact \(Preview\)](#).

Public Preview - Limit creation or promotion of multitenant apps

Type: New feature

Service category: Directory Management

Product capability: Developer Experience

A new feature has been added to the [App Management Policy Framework](#) that allows restriction on creation or promotion of multitenant applications, providing administrators with greater control over their app environments.

Administrators can now configure tenant default or custom app policy using the new 'audiences' restriction to block new app creation if the signInAudience value provided in the app isn't permitted by the policy. In addition, existing apps can be restricted from changing their signInAudience if the target value isn't permitted by the policy. These policy changes are applied during app creation or update operations, offering control over application deployment and usage. For more information, see: [audiencesConfiguration resource type](#).

General Availability - Download Microsoft Entra Connect Sync on the Microsoft Entra admin center

Type: Plan for change

Service category: Microsoft Entra Connect

Product capability: Identity Governance

The Microsoft Entra Connect Sync .msi installation files are also available on Microsoft Entra admin center within the [Microsoft Entra Connect pane](#). As part of this change, we'll stop uploading new installation files on the [Microsoft Download Center](#).

General Availability - New Microsoft-managed Conditional Access policies designed to limit device code flow and legacy authentication flows

Type: Changed feature

Service category: Conditional Access

Product capability: Access Control

As part of our ongoing commitment to enhance security and protect our customers from evolving cyber threats, we're rolling out two new Microsoft-managed Conditional Access policies designed to limit device code flow and legacy authentication flows. These policies are aligned to the secure by default principle of our broader [Secure Future Initiative](#), which aims to provide robust security measures to safeguard your organization by default.

Deprecated - Upgrade your Microsoft Entra Connect Sync version to avoid impact on the Sync Wizard

Type: Deprecated

Service category: Microsoft Entra Connect

Product capability: Microsoft Entra Connect

As announced in the Microsoft Entra What's New [Blog](#) and in Microsoft 365 Center communications, customers should upgrade their connect sync versions to at least [2.4.18.0](#) for commercial clouds and [2.4.21.0](#) for non-commercial clouds before April 7, 2025. A breaking change on the Connect Sync Wizard will affect all requests that require authentication such as schema refresh, configuration of staging mode, and user sign in changes. For more information, see: [Minimum versions](#).

February 2025

General Availability - Authentication methods migration wizard

Type: New feature

Service category: MFA

Product capability: User Authentication

The authentication methods migration guide in the Microsoft Entra Admin Center lets you automatically migrate method management from the [legacy MFA and SSPR policies](#) to the [converged authentication methods policy](#). In 2023, it was announced that the ability to manage authentication methods in the legacy MFA and SSPR policies would be retired in September 2025. Until now, organizations had to manually migrate methods themselves by using [the migration toggle](#) in the converged policy. Now, you can migrate in just a few selections by using the migration guide. The guide evaluates what your organization currently has enabled in both legacy policies, and generates a recommended converged policy configuration for you to review and edit as needed. From there, confirm the configuration, and we set it up for you and mark your migration as complete. For more information, see: [How to migrate MFA and SSPR policy settings to the Authentication methods policy for Microsoft Entra ID](#).

Public Preview - Enhanced user management in Admin Center UX

Type: New feature

Service category: User Management

Product capability: User Management

Admins are now able to multi-select and edit users at once through the Microsoft Entra Admin Center. With this new capability, admins can bulk edit user properties, add users to groups, edit account status, and more. This UX enhancement will significantly improve efficiency for user management tasks in the Microsoft Entra admin center. For more information, see: [Add or update a user's profile information and settings in the Microsoft Entra admin center.](#)

Public Preview – QR code authentication, a simple and fast authentication method for Frontline Workers

Type: New feature

Service category: Authentications (Logins)

Product capability: User Authentication

We're thrilled to announce public preview of QR code authentication in Microsoft Entra ID, providing an efficient and simple authentication method for frontline workers.

You see a new authentication method 'QR code' in Microsoft Entra ID Authentication method Policies. You can enable and add QR code for your frontline workers via Microsoft Entra ID, My Staff, or MS Graph APIs. All users in your tenant see a new link 'Sign in with QR code' on navigating to <https://login.microsoftonline.com> > 'Sign-in options' > 'Sign in to an organization' page. This new link is visible only on mobile devices (Android/iOS/iPadOS). Users can use this auth method only if you add and provide a QR code to them. QR code auth is also available in BlueFletch and Jamf. MHS QR code auth support is generally available by early March.

The feature has a 'preview' tag until it's generally available. For more information, see: [Authentication methods in Microsoft Entra ID - QR code authentication method \(Preview\).](#)

Public Preview - Custom SAML/WS-Fed External Identity Provider Support in Microsoft Entra External ID

Type: New feature

Service category: B2C - Consumer Identity Management

Product capability: B2B/B2C

By setting up federation with a custom-configured identity provider that supports the SAML 2.0 or WS-Fed protocol, you enable your users to sign up and sign in to your applications using their existing accounts from the federated external provider.

This feature also includes domain-based federation, so a user who enters an email address on the sign-in page that matches a predefined domain in any of the external identity providers will be redirected to authenticate with that identity provider.

For more information, see: [Custom SAML/WS-Fed identity providers \(preview\)](#).

Public Preview - External Auth Methods support for system preferred MFA

Type: New feature

Service category: MFA

Product capability: 3rd Party Integration

Support for external auth methods as a supported method begins rolling out at the beginning of March 2025. When this is live in a tenant where system preferred is enabled and users are in scope of an external auth methods policy, those users will be prompted for their external authentication method if their most secure registered method is Microsoft Authenticator notification. External Authentication Method will appear as third in the list of most secure methods. If the user has a Temporary Access Pass (TAP) or Passkey (FIDO2) device registered, they'll be prompted for those. In addition, users in the scope of an external auth methods policy will have the ability to delete all registered second factor methods from their account, even if the method being deleted is specified as the default sign in method or is system preferred. For more information, see: [System-preferred multifactor authentication - Authentication methods policy](#).

General Availability - Granular Microsoft Graph permissions for Lifecycle workflows

Type: New feature

Service category: Lifecycle Workflows

Product capability: Identity Governance

Now new, lesser privileged permissions can be used for managing specific read and write actions in Lifecycle workflows scenarios. The following granular permissions were introduced in Microsoft Graph:

- LifecycleWorkflows-Workflow.ReadBasic.All
- LifecycleWorkflows-Workflow.Read.All
- LifecycleWorkflows-Workflow.ReadWrite.All
- LifecycleWorkflows-Workflow.Activate
- LifecycleWorkflows-Reports.Read.All
- LifecycleWorkflows-CustomExt.Read.All
- LifecycleWorkflows-CustomExt.ReadWrite.All

For more information, see: [Microsoft Graph permissions reference](#).

January 2025

Public Preview - Manage Lifecycle Workflows with Microsoft Security CoPilot in Microsoft Entra

Type: New feature

Service category: Lifecycle Workflows

Product capability: Identity Governance

Customers can now manage, and customize, Lifecycle Workflows using natural language with Microsoft Security CoPilot. Our Lifecycle Workflows (LCW) Copilot solution provides step-by-step guidance to perform key workflow configuration and execution tasks using natural language. It allows customers to quickly get rich insights to help monitor, and troubleshoot, workflows for compliance. For more information, see: [Manage employee lifecycle using Microsoft Security Copilot \(Preview\)](#).

General Availability - Microsoft Entra PowerShell

Type: New feature

Service category: MS Graph

Product capability: Developer Experience

Manage and automate Microsoft Entra resources programmatically with the scenario-focused Microsoft Entra PowerShell module. For more information, see: [Microsoft Entra PowerShell module now generally available ↗](#).

General Availability - Improving visibility into downstream tenant sign-ins

Type: New feature

Service category: Reporting

Product capability: Monitoring & Reporting

Microsoft Security wants to ensure that all customers are aware of how to notice when a partner is accessing a downstream tenant's resources. Interactive sign-in logs currently provide a list of sign in events, but there's no clear indication of which logins are from partners accessing downstream tenant resources. For example, when reviewing the logs, you might see a series of events, but without any additional context, it's difficult to tell whether these logins are from a partner accessing another tenant's data.

Here's a list of steps that one can take to clarify which logins are associated with partner tenants:

1. Take note of the "ServiceProvider" value in the CrossTenantAccessType column:

- This filter can be applied to refine the log data. When activated, it immediately isolates events related to partner logins.

2. Utilize the "Home Tenant ID" and "Resource Tenant ID" Columns:

- These two columns identify logins coming from the partner's tenant to a downstream tenant.

After seeing a partner logging into a downstream tenant's resources, an important follow-up activity to perform is to validate the activities that might have occurred in the downstream environment. Some examples of logs to look at are Microsoft Entra Audit logs for Microsoft Entra ID events, Microsoft 365 Unified Audit Log (UAL) for Microsoft 365 and Microsoft Entra ID events, and/or the Azure Monitor activity log for Azure events. By following these steps, you're able to clearly identify when a partner is logging into a downstream tenant's resources and subsequent activity in the environment, enhancing your ability to manage and monitor cross-tenant access efficiently.

To increase visibility into the aforementioned columns, Microsoft Entra will begin enabling these columns to display by default when loading the sign-in logs UX starting on March 7, 2025.

Public Preview - Auditing administrator events in Microsoft Entra Connect

Type: New feature

Service category: Microsoft Entra Connect

Product capability: Microsoft Entra Connect

We have released a new version of Microsoft Entra Connect, version 2.4.129.0, that supports the logging of the changes an administrator makes on the Connect Sync Wizard and PowerShell. For more information, see: [Auditing administrator events in Microsoft Entra Connect Sync \(Public Preview\)](#).

Where supported, we'll also autoupgrade customers to this version of Microsoft Entra Connect in February 2025. For customers who wish to be autoupdated, [ensure that you have auto-upgrade configured](#).

For upgrade-related guidance, see [Microsoft Entra Connect: Upgrade from a previous version to the latest](#).

Public Preview - Flexible Federated Identity Credentials

Type: New feature

Service category: Authentications (Logins)

Product capability: Developer Experience

Flexible Federated Identity Credentials extend the existing Federated Identity Credential model by providing the ability to use wildcard matching against certain claims. Currently available for GitHub, GitLab, and Terraform Cloud scenarios, this functionality can be used to lower the total number of FICs required to manage similar scenarios. For more information, see: [Flexible federated identity credentials \(preview\)](#).

General Availability - Real-time Password Spray Detection in Microsoft Entra ID Protection

Type: New feature

Service category: Identity Protection

Product capability: Identity Security & Protection

Traditionally, password spray attacks are detected post breach or as part of hunting activity. Now, we've enhanced Microsoft Entra ID Protection to detect password spray attacks in real-

time before the attacker ever obtains a token. This reduces remediation from hours to seconds by interrupting attacks during the sign-in flow.

Risk-based Conditional Access can automatically respond to this new signal by raising session risk, immediately challenging the sign-in attempt, and stopping password spray attempts in their tracks. This cutting-edge detection, now Generally Available, works alongside existing detections for advanced attacks such as Adversary-in-the-Middle (AitM) phishing and token theft, to ensure comprehensive coverage against modern attacks. For more information, see: [What is Microsoft Entra ID Protection?](#)

General Availability - Protected actions for hard deletions

Type: New feature

Service category: Other

Product capability: Identity Security & Protection

Customers can now configure Conditional Access policies to protect against early hard deletions. Protected action for hard deletion protects hard deletion of users, Microsoft 365 groups, and applications. For more information, see: [What are protected actions in Microsoft Entra ID?](#).

Public Preview - Elevate Access events are now exportable via Microsoft Entra Audit Logs

Type: New feature

Service category: RBAC

Product capability: Monitoring & Reporting

This feature enables administrators to export and stream Elevate Access events to both first-party and third-party SIEM solutions via Microsoft Entra Audit logs. It enhances detection and improves logging capabilities, allowing visibility into who in their tenant has utilized Elevate Access. For more information on how to use the feature, see: [View elevate access log entries](#).

Deprecated - Action Required by February 1, 2025: Azure AD Graph retirement

Type: Deprecated

Service category: Azure AD Graph

Product capability: Developer Experience

The Azure AD Graph API service was [deprecated] in 2020. [Retirement of the Azure AD Graph API service](#) began in September 2024, and the next phase of this retirement starts February 1, 2025. This phase will impact new and existing applications unless action is taken. The latest updates on Azure AD Graph retirement can be found here: [Take action by February 1: Azure AD Graph is retiring](#).

Starting from February 1, both new and existing applications will be prevented from calling Azure AD Graph APIs, unless they're configured for an extension. You might not see impact right away, as we're rolling out this change in stages across tenants. We anticipate full deployment of this change around the end of February, and by the end of March for national cloud deployments.

If you haven't already, it's now urgent to review the applications on your tenant to see which ones depend on Azure AD Graph API access, and mitigate or migrate these before the February 1 cutoff date. For applications that haven't migrated to Microsoft Graph APIs, [an extension](#) can be set to allow the application access to Azure AD Graph through June 30, 2025.

Microsoft Entra Recommendations are the best tool to identify applications that are using Azure AD Graph APIs in your tenant and require action. Reference this blog post: Action required: [Azure AD Graph API retirement](#) for step by step guidance.

General Availability - Microsoft Entra Connect Version 2.4.129.0

Type: Changed feature

Service category: Microsoft Entra Connect

Product capability: Microsoft Entra Connect

On January 15, 2025, we released Microsoft Entra Connect Sync Version 2.4.129.0 which supports auditing administrator events. More details are available in the [release notes](#). We'll automatically upgrade eligible customers to this latest version of Microsoft Entra Connect in February 2025. For customers who wish to be auto-upgraded, [ensure that you have auto-upgrade configured](#).

Deprecated - Take action to avoid impact when legacy MSOnline and AzureAD PowerShell modules retire

Type: Deprecated

Service category: Legacy MSOnline and AzureAD PowerShell modules

Product capability: Developer Experience

As announced in Microsoft Entra [change announcements](#) and in the Microsoft Entra [Blog](#), the MSOnline, and Microsoft Azure AD PowerShell modules (for Microsoft Entra ID) retired on March 30, 2024.

The retirement for MSOnline PowerShell module starts in early April 2025, and ends in late May 2025. If you're using MSOnline PowerShell, you must take action by March 30, 2025 to avoid impact after the retirement by migrating any use of MSOnline to [Microsoft Graph PowerShell SDK](#) or [Microsoft Entra PowerShell](#).

Key points

- MSOnline PowerShell will retire, and stop working, between early April 2025 and late May 2025
- AzureAD PowerShell will no longer be supported after March 30, 2025, but its retirement will happen in early July 2025. This postponement is to allow you time to finish the MSOnline PowerShell migration
- To ensure customer readiness for MSOnline PowerShell retirement, a series of temporary outage tests will occur for all tenants between January 2025 and March 2025.

For more information, see: [Action required: MSOnline and AzureAD PowerShell retirement - 2025 info and resources](#).

December 2024

General Availability - What's new in Microsoft Entra

Type: New feature

Service category: Reporting

Product capability: Monitoring & Reporting

What's new in Microsoft Entra offers a comprehensive view of Microsoft Entra product updates including product roadmap (like Public Previews and recent GAs), and change announcements (like deprecations, breaking changes, feature changes and Microsoft-managed policies). It's a one stop shop for Microsoft Entra admins to discover the product updates.

Public Preview - Microsoft Entra ID Governance: Approvers can revoke access in MyAccess

Type: New feature

Service category: Entitlement Management

Product capability: Entitlement Management

For Microsoft Entra ID Governance users, approvers of access package requests can now revoke their decision in MyAccess. Only the person who took the approve action is able to revoke access. To opt into this feature, admins can go to the [Identity Governance settings page](#), and enable the feature. For more information, see: [What is the My Access portal?](#).

General Availability - Expansion of SSPR Policy Audit Logging

Type: New feature

Service category: Self Service Password Reset

Product capability: Monitoring & Reporting

Starting Mid-January, we are improving the audit logs for changes made to the SSPR Policy.

With this improvement, any change to the SSPR policy configuration, including enablement or disablement, will result in an audit log entry that includes details about the change made. Additionally, both the previous values and current values from the change will be recorded within the audit log. This additional information can be found by selecting an audit log entry and selecting the Modified Properties tab within the entry.

These changes are rolled out in phases:

- Phase 1 includes logging for the Authentication Methods, Registration, Notifications, and Customization configuration settings.
- Phase 2 includes logging for the On-premises integration configuration settings.

This change occurs automatically, so admins take no action. For more information and details regarding this change, see: [Microsoft Entra audit log categories and activities](#).

General Availability - Update Profile Photo in MyAccount

Type: New feature

Service category: My Profile/Account

Product capability: End User Experiences

Users can now update their profile photo directly from their MyAccount portal. This change exposes a new edit button on the profile photo section of the user's account.

In some environments, it's necessary to prevent users from making this change. Global Administrators can manage this using a tenant-wide policy with Microsoft Graph API, following the guidance in the [Manage user profile photo settings in Microsoft 365](#) document.

General Availability - Temporary Access Pass (TAP) support for internal guest users

Type: New feature

Service category: MFA

Product capability: Identity Security & Protection

Microsoft Entra ID now supports issuing Temporary Access Passes (TAP) to internal guest users. TAPs can be issued to internal guests just like normal members, through the Microsoft Entra ID Admin Center, or natively through Microsoft Graph. With this enhancement, internal guests can now seamlessly onboard, and recover, their accounts with time-bound temporary credentials.

For more information, see: [Configure Temporary Access Pass to register passwordless authentication methods](#).

Public Preview - Microsoft Entra ID Governance: access package request suggestions

Type: New feature

Service category: Entitlement Management

Product capability: Entitlement Management

Opt-In As communicated [earlier](#), we're excited to introduce a new feature in [My Access](#): a curated list of suggested access packages. This capability allows users to quickly view the most relevant access packages (based off their peers' access packages and previous requests) without scrolling through a long list. In December you can [enable the preview in the Opt-in Preview Features for Identity Governance](#). From January, this setting is enabled by default.

Public Preview - Security Copilot embedded in Microsoft Entra

Type: New feature

Service category: Other

Product capability: Identity Security & Protection

We've announced the public preview of Microsoft Security Copilot embedded in the Microsoft Entra admin Center. This integration brings all identity skills previously made generally available for the Security Copilot standalone experience in April 2024, along with new identity capabilities for admins and security analysts to use directly within the Microsoft Entra admin center. We've also added brand new skills to help improve identity-related risk investigation. In December, we broaden the scope even further to include a set of skills specifically for App Risk Management in both standalone and embedded experiences of Security Copilot and Microsoft Entra. These capabilities allow identity admins and security analysts to better identify, understand, and remediate the risks impacting applications and workload identities registered in Microsoft Entra.

With Security Copilot now embedded in Microsoft Entra, identity admins get AI-driven, natural-language summaries of identity context and insights tailored for handling security incidents, equipping them to better protect against identity compromise. The embedded experience also accelerates troubleshooting tasks like resolving identity-related risks and sign-in issues, without ever leaving the admin center.

Public Preview - Security Copilot in Microsoft Entra: App Risk skills

Type: New feature

Service category: Other

Product capability: Identity Security & Protection

Identity admins and security analysts managing Microsoft Entra ID registered apps can identify and understand risks through natural language prompts. Security Copilot has links to the Microsoft Entra Admin Center for admins to take needed remediation actions. For more information, see: [Assess application risks using Microsoft Security Copilot in Microsoft Entra](#).

Public Preview - Provision custom security attributes from HR sources

Type: New feature

Service category: Provisioning

Product capability: Inbound to Entra ID

With this feature, customers can automatically provision "*custom security attributes*" in Microsoft Entra ID from authoritative HR sources. Supported authoritative sources include: Workday, SAP SuccessFactors, and any HR system integrated using API-driven provisioning.

Public Preview - Sign in with Apple

Type: New feature

Service category: B2C - Consumer Identity Management

Product capability: Extensibility

This new feature adds Apple to our list of preconfigured social identity providers. As the first social identity provider implemented on the eSTS platform, it introduces a "*Sign in with Apple*" button to the sign-in options, allowing users to access applications with their Apple accounts. For more information, see: [Add Apple as an identity provider \(preview\)](#).

General Availability - Microsoft Entra External ID Custom URL Domains

Type: New feature

Service category: Authentications (Logins)

Product capability: Identity Lifecycle Management

This feature allows users to customize their Microsoft default sign in authentication endpoint with their own brand names. Custom URL Domains help users to change Ext ID endpoint < tenant-name >.ciamlogin.com to login.contoso.com.

General Availability - Privileged Identity Management integration in Azure Role Based Access Control

Type: New feature

Service category: RBAC

Product capability: Access Control

Privileged Identity Management (PIM) capabilities are now integrated into the Azure Role Based Access Control (Azure RBAC) UI. Before this integration, RBAC admins could only manage standing access (active permanent role assignments) from the Azure RBAC UI. With this integration, just-in-time access and timebound access, which are functionalities supported

by PIM, are now brought into the Azure RBAC UI for customers with either a P2, or Identity Governance, license.

RBAC admins can create assignments of type eligible and timebound duration from the Azure RBAC add role assignment flow, see the list of different states of role assignment in a single view, as well as convert the type and duration of their role assignments from the Azure RBAC UI. In addition, end users now see all their role assignments of different state straight from the Azure RBAC UI landing page, from where they can also activate their eligible role assignments. For more information, see: [List role assignments at a scope](#).

General Availability - Dedicated new 1st party resource application to enable Active Directory to Microsoft Entra ID sync using Microsoft Entra Connect Sync or Cloud Sync

Type: Changed feature

Service category: Provisioning

Product capability: Directory

As part of ongoing security hardening, Microsoft deployed Microsoft Entra AD Synchronization Service, a dedicated first-party application to enable the synchronization between Active Directory and Microsoft Entra ID. This new application, with Application ID `6bf85cfa-ac8a-4be5-b5de-425a0d0dc016`, was provisioned in customer tenants that use Microsoft Entra Connect Sync or the Microsoft Entra Cloud Sync service.

November 2024

Public Preview - Universal Continuous Access Evaluation

Type: New feature

Service category: Provisioning

Product capability: Network Access

Continuous Access Evaluation (CAE) revokes, and revalidates, network access in near real-time whenever Microsoft Entra ID detects changes to the identity. For more information, see: [Universal Continuous Access Evaluation \(Preview\)](#).

Public Preview - Microsoft Entra new store for certificate-based authentication

Type: New feature

Service category: Authentications (Logins)

Product capability: User Authentication

Microsoft Entra ID has a new scalable PKI (Public Key Infrastructure) based CA (Certificate Authorities) store with higher limits for the number of CAs and the size of each CA file. PKI based CA store allows CAs within each different PKI to be in its own container object allowing administrators to move away from one flat list of CAs to more efficient PKI container based CAs. PKI-based CA store now supports up to 250CAs, 8KB size for each CA and also supports issuers hints attribute for each CA. Administrators can also upload the entire PKI and all the CAs using the "Upload CBA PKI" feature or create a PKI container and upload CAs individually. For more information, see: [Step 1: Configure the certificate authorities with PKI-based trust store \(Preview\)](#).

Public Preview - Updating profile photo in MyAccount

Type: New feature

Service category: My Profile/Account

Product capability: End User Experiences

On November 13, 2024, users received the ability to update their profile photo directly from their [MyAccount](#) portal. This change exposes a new edit button on the profile photo section of the user's account.

In some environments, it's necessary to prevent users from making this change. Global Administrators can manage this using a tenant-wide policy with Microsoft Graph API, following the guidance in the [Manage user profile photo settings in Microsoft 365](#) document.

General Availability - Microsoft Entra Health Monitoring, Health Metrics Feature

Type: New feature

Service category: Reporting

Product capability: Monitoring & Reporting

Microsoft Entra health monitoring, available from the Health pane, includes a set of low-latency pre-computed health metrics that can be used to monitor the health of critical user scenarios

in your tenant. The first set of health scenarios includes MFA, CA-compliant devices, CA-managed devices, and SAML authentications. This set of monitor scenarios will grow over time. These health metrics are now released as general availability data streams with the public preview of an intelligent alerting capability. For more information, see: [What is Microsoft Entra Health?](#)

General Availability - Microsoft Entra Connect Sync Version 2.4.27.0

Type: Changed feature

Service category: Provisioning

Product capability: Identity Governance

On November 14, 2025, we released Microsoft Entra Connect Sync Version 2.4.27.0 that uses the OLE DB version 18.7.4 that further hardens our service. Upgrade to this latest version of connect sync to improve your security. More details are available in the [release notes](#).

Changed feature - expansion of WhatsApp as an MFA one-time passcode delivery channel for Microsoft Entra ID

Type: Changed feature

Service category: MFA

Product capability: User Authentication

In late 2023, Microsoft Entra ID started using WhatsApp as an alternate channel to deliver multifactor authentication (MFA) one-time passcodes to users in India and Indonesia. We saw improved deliverability, completion rates, and satisfaction when using the channel in both countries. The channel was temporarily disabled in India in early 2024. Starting early December 2024, we'll be re-enabling the channel in India, and expanding its use to more countries.

Starting December 2024, users in India, and other countries can start receiving MFA text messages via WhatsApp. Only users that are enabled to receive MFA text messages as an authentication method, and already have WhatsApp on their phone, get this experience. If a user with WhatsApp on their device is unreachable or doesn't have internet connectivity, we'll quickly fall back to the regular SMS channel. In addition, users receiving OTPs via WhatsApp for the first time will be notified of the change in behavior via SMS text message.

If you don't want your users to receive MFA text messages through WhatsApp, you can disable text messages as an authentication method in your organization or scope it down to only be

enabled for a subset of users. Note that we highly encourage organizations move to using more modern, secure methods like Microsoft Authenticator and passkeys in favor of telecom and messaging app methods. For more information, see: [Text message verification](#).

Retirement - MFA Fraud Alert will be retired on March 1st 2025

Type: Deprecated

Service category: MFA

Product capability: Identity Security & Protection

Microsoft Entra multifactor authentication (MFA) fraud alert allows end users to report MFA voice calls, and Microsoft Authenticator push requests, they didn't initiate as fraudulent.

Beginning March 1, 2025, MFA Fraud Alert will be retired in favor of the replacement feature

[Report Suspicious Activity](#) which allows end users to report fraudulent requests, and is also

integrated with [Identity Protection](#) for more comprehensive coverage and remediation.

To ensure users can continue reporting fraudulent MFA requests, organizations should migrate to using Report Suspicious Activity, and review how reported activity is remediated based on their Microsoft Entra licensing. For more information, see: [Configure Microsoft Entra multifactor authentication settings](#).

Public Preview - Microsoft Entra Health Monitoring, Alerts Feature

Type: Changed feature

Service category: Other

Product capability: Monitoring & Reporting

Intelligent alerts in Microsoft Entra health monitoring notify tenant admins, and security engineers, whenever a monitored scenario breaks from its typical pattern. Microsoft Entra's alerting capability watches the low-latency health signals of each scenario, and fires a notification if an anomaly is detected. The set of alert-ready health signals and scenarios will grow over time. This alerts feature is now available in Microsoft Entra Health as an API-only public preview release (UX release is scheduled for February 2025). For more information, see: [How to use Microsoft Entra Health monitoring alerts \(preview\)](#).

General Availability - Log analytics sign-in logs schema is in parity with MSGraph schema

Type: Plan for change

Service category: Authentications (Logins)

Product capability: Monitoring & Reporting

To maintain consistency in our core logging principles, we've addressed a legacy parity issue where the Azure Log Analytics sign-in logs schema didn't align with the MSGraph sign-in logs schema. The updates include fields such as ClientCredentialType, CreatedDateTime, ManagedServiceIdentity, NetworkLocationDetails, tokenProtectionStatus, SessionID, among others. These changes take effect in the first week of December 2024.

We believe this enhancement provides a more consistent logging experience. As always, you can perform pre-ingestion transformations to remove any unwanted data from your Azure Log Analytics storage workspaces. For guidance on how to perform these transformations, see:

[Data collection transformations in Azure Monitor](#).

Deprecated - MIM hybrid reporting agent

Type: Deprecated

Service category: Microsoft Identity Manager

Product capability: Monitoring & Reporting

The hybrid reporting agent, used to send a MIM Service event log to Microsoft Entra to surface in password reset and self-service group management reports, is deprecated. The recommended replacement is to use Azure Arc to send the event logs to Azure Monitor. For more information, see: [Microsoft Identity Manager 2016 reporting with Azure Monitor](#).

Archive for Microsoft Entra releases and announcements

Article • 03/25/2025

This article includes information about the releases and change announcements across the Microsoft Entra family of products that are older than six months (up to 18 months). If you're looking for more current information, see [Microsoft Entra releases and announcements](#).

For a more dynamic experience, you can now find the archive information in the Microsoft Entra admin center. To learn more, see [What's new \(preview\)](#).

September 2024

Public preview - New Conditional Access Template Requiring Device Compliance

Type: New feature

Service category: Conditional Access

Product capability: Identity Security & Protection

A new Conditional Access template requiring device compliance is now available in Public Preview. This template restricts access to company resources exclusively to devices enrolled in mobile device management (MDM) and compliant with company policy. Requiring device compliance improves data security, reducing risk of data breaches, malware infections, and unauthorized access. This is a recommended best practice for users and devices targeted by compliance policy through MDM. For more information, see: [Common policy: Create a Conditional Access policy requiring device compliance](#).

Public preview - Tenant admin can fail certificate based auth when the end user certificate issuer isn't configured with a certificate revocation list

Type: New feature

Service category: Authentications (Logins)

Product capability: User Authentication

With Certificate based authentication, a CA can be uploaded without a CRL endpoint, and certificate-based authentication won't fail if an issuing CA doesn't have a CRL specified.

To strengthen security and avoid misconfigurations, an Authentication Policy Administrator can require CBA authentication to fail if no CRL is configured for a CA that issues an end user certificate. For more information, see: [Understanding CRL validation \(Preview\)](#).

General Availability: Microsoft Authenticator on Android is FIPS 140 compliant for Microsoft Entra authentication

Type: New feature

Service category: Microsoft Authenticator App

Product capability: User Authentication

Beginning with version 6.2408.5807, Microsoft Authenticator for Android is compliant with Federal Information Processing Standard (FIPS 140-3) for all Microsoft Entra authentications, including phishing-resistant device-bound passkeys, push multifactor authentication (MFA), passwordless phone sign-in (PSI), and time-based one-time passcodes (TOTP). No changes in configuration are required in Microsoft Authenticator or Microsoft Entra ID Admin Portal to enable this capability. Microsoft Authenticator on iOS is already FIPS 140 compliant, as announced last year. For more information, see: [Authentication methods in Microsoft Entra ID - Microsoft Authenticator app](#).

General Availability - Microsoft Entra External ID extension for Visual Studio Code

Type: Changed feature

Service category: B2C - Consumer Identity Management

Product capability: B2B/B2C

[Microsoft Entra External ID Extension for VS Code](#) provides a streamlined, guided experience to help you kickstart identity integration for customer-facing apps. With this extension, you can create external tenants, set up a customized and branded sign-in experience for external users, and quickly bootstrap your projects with preconfigured External ID samples—all within Visual Studio Code. Additionally, you can view and

manage your external tenants, applications, user flows, and branding settings directly within the extension.

For more information, see: [Quickstart: Get started with the Microsoft Entra External ID extension for Visual Studio Code](#).

Public Preview - Custom Claims API for Claims Configuration of Enterprise Apps

Type: New feature

Service category: Enterprise Apps

Product capability: SSO

Custom Claims API allows admins to manage and update additional claims for their Enterprise Applications seamlessly through MS Graph. The Custom Claims API offers a simplified and user friendly API experience for claims management for our customers. With the introduction of Custom Claims API, we achieved UX and API interoperability. Admins can now use Microsoft Entra admin center and MS Graph API interchangeably to manage claims configurations for their Enterprise Applications. It facilitates admins to execute their automations using the API while allowing the flexibility to update claims on the Microsoft Entra admin center as required on the same policy object. For more information, see: [Customize claims using Microsoft Graph Custom Claims Policy \(preview\)](#).

General Availability - Cross-tenant manager synchronization

Type: New feature

Service category: Provisioning

Product capability: Identity Governance

Support for synchronizing the manager attribute using cross-tenant synchronization is now generally available. For more information, see: [Attributes](#).

Public Preview - Request on behalf of

Type: New feature

Service category: Entitlement Management

Product capability: Entitlement Management

Entitlement Management enables admins to create access packages to manage their organization's resources. Admins can either directly assign users to an access package, or configure an access package policy that allows users and group members to request access. This option to create self-service processes is useful, especially as organizations scale and hire more employees. However, new employees joining an organization might not always know what they need access to, or how they can request access. In this case, a new employee would likely rely on their manager to guide them through the access request process.

Instead of having new employees navigate the request process, managers can request access packages for their employees, making onboarding faster and more seamless. To enable this functionality for managers, admins can select an option when setting up an access package policy that allows managers to request access on their employees' behalf.

Expanding self-service request flows to allow requests on behalf of employees ensures that users have timely access to necessary resources, and increases productivity. For more information, see: [Request access package on-behalf-of other users \(Preview\)](#).

August 2024

Change announcement - Upcoming MFA Enforcement on Microsoft Entra admin center

Type: Plan for change

Service category: MFA

Product capability: Identity Security & Protection

As part of our commitment to providing our customers with the highest level of security, we previously [announced](#) that Microsoft requires multifactor authentication (MFA) for users signing into Azure.

We'd like to share an update that the scope of MFA enforcement includes [Microsoft Entra admin center](#) in addition to the Azure portal and Intune admin center. This change is rolled out in phases, allowing organizations time to plan their implementation:

Phase 1: Beginning in the second half of the calendar year 2024, MFA is required to sign in to the Microsoft Entra admin center, Azure portal, and Intune admin center. This enforcement is gradually rolled out to all tenants worldwide. This phase didn't affect

other Azure clients such as the Azure Command Line Interface, Azure PowerShell, Azure mobile app, and Infrastructure as Code (IaC) tools.

Phase 2: Beginning in early 2025, gradual enforcement of MFA at sign-in for the Azure CLI, Azure PowerShell, Azure mobile app, and Infrastructure as Code (IaC) tools commences.

Microsoft sends a 60-day advance notice to all Microsoft Entra Global Administrators by email, and through Azure Service Health Notifications, to notify them of the start date of enforcement and required actions. Extra notifications are sent through the Azure portal, Microsoft Entra admin center, and the Microsoft 365 message center.

We understand that some customers might need extra time to prepare for this MFA requirement. Therefore, Microsoft allows extended time for customers with complex environments or technical barriers. The notification from us also includes details about how customers can postpone specific changes. These changes include the start date of enforcement for their tenants, the duration of the postponement, and a link to apply changes. Visit [here](#) to learn more.

General Availability - restricted permissions on Directory Synchronization Accounts (DSA) role in Microsoft Entra Connect Sync and Microsoft Entra Cloud Sync

Type: Changed feature

Service category: Provisioning

Product capability: Microsoft Entra Connects

As part of ongoing security hardening, Microsoft removes unused permissions from the privileged *Directory Synchronization Accounts* role. This role is exclusively used by Microsoft Entra Connect Sync, and Microsoft Entra Cloud Sync, to synchronize Active Directory objects with Microsoft Entra ID. There's no action required by customers to benefit from this hardening, and the revised role permissions are documented here: [Directory Synchronization Accounts](#).

Plan for change - My Security-Info Add sign-in method picker UX update

Type: Plan for change

Service category: MFA

Product capability: End User Experiences

Starting Mid-October 2024, the *Add sign-in* method dialog on the My Security-Info page will be updated with a modern look and feel. With this change, new descriptors will be added under each method which provides detail to users on how the sign-in method is used (ex. *Microsoft Authenticator – Approve sign-in requests or use one-time codes*).

Early next year the *Add sign-in* method, dialog will be enhanced to show an initially recommended sign-in method instead of initially showing the full list of sign-in methods available to register. The recommended sign-in method will default to the strongest method available to the user based on the organization's authentication method policy. Users can select *Show more options* and choose from all available sign-in methods allowed by their policy.

This change will occur automatically, so admins take no action.

Public Preview - Provisioning UX Updates

Type: Plan for change

Service category: Provisioning

Product capability: Outbound to SaaS Applications

We'll start releasing user experience updates for application provisioning, HR provisioning, and cross-tenant synchronization next month. These updates include a new overview page, user experience to configure connectivity to your application, and new create provisioning experience. The new experiences include all functionality available to customers today, and no customer action is required.

Change Announcement - Deferred Changes to My Groups Admin Controls

Type: Plan for change

Service category: Group Management

Product capability: AuthZ/Access Delegation

In [October 2023 ↗](#), we shared that, starting June 2024, the existing Self Service Group Management setting in the Microsoft Entra Admin Center that states *restrict user ability to access groups features in My Groups* retires. These changes are under review, and might take place as originally planned. A new deprecation date will be announced in the future.

Public Preview - Microsoft Entra ID FIDO2 provisioning APIs

Type: New feature

Service category: MFA

Product capability: Identity Security & Protection

Microsoft Entra ID now supports FIDO2 provisioning via API, allowing organizations to pre-provision security keys (passkeys) for users. These new APIs can simplify user onboarding, and provide seamless phishing-resistant authentication on day one for employees. For more information on how to use this feature, see: [Provision FIDO2 security keys using Microsoft Graph API](#).

General Availability - Enable, Disable, and Delete synchronized users accounts with Lifecycle Workflows

Type: New feature

Service category: Lifecycle Workflows

Product capability: Identity Lifecycle Management

Lifecycle Workflows is now able to enable, disable, and delete user accounts that are synchronized from Active Directory Domain Services (AD DS) to Microsoft Entra. This capability allows you to complete the employee offboarding process by deleting the user account after a retention period.

To learn more, see: [Manage users synchronized from Active Directory Domain Services with workflows](#).

General Availability - Configure Lifecycle Workflow Scope Using Custom Security Attributes

Type: New feature

Service category: Lifecycle Workflows

Product capability: Identity Lifecycle Management

Customers can now use their confidential HR data stored in custom security attributes. They can do this addition to other attributes to define the scope of their workflows in Lifecycle Workflows for automating joiner, mover, and leaver scenarios.

To learn more, see: [Use custom security attributes to scope a workflow](#).

General Availability - Workflow History Insights in Lifecycle Workflows

Type: New feature

Service category: Lifecycle Workflows

Product capability: Identity Lifecycle Management

With this feature, customers can now monitor workflow health, and get insights for all their workflows in Lifecycle Workflows including viewing workflow processing data across workflows, tasks, and workflow categories.

To learn more, see: [Lifecycle workflow Insights](#).

General Availability - Configure custom workflows to run mover tasks when a user's job profile changes

Type: New feature

Service category: Lifecycle Workflows

Product capability: Identity Lifecycle Management

Lifecycle Workflows now supports the ability to trigger workflows based on job change events like changes to an employee's department, job role, or location, and see them executed on the workflow schedule. With this feature, customers can use new workflow triggers to create custom workflows for their executing tasks associated with employees moving within the organization including triggering:

- Workflows when a specified attribute changes
- Workflows when a user is added or removed from a group's membership
- Tasks to notify a user's manager about a move
- Tasks to assign licenses or remove selected licenses from a user

To learn more, see [Automated employee mover tasks when they change jobs using the Microsoft Entra admin center tutorial](#).

General Availability - Device based Conditional Access to M365/Azure resources on Red Hat Enterprise Linux

Type: New feature

Service category: Conditional Access

Product capability: SSO

Since October 2022, users on Ubuntu Desktop 20.04 LTS & Ubuntu 22.04 LTS with Microsoft Edge browser could register their devices with Microsoft Entra ID, enroll into Microsoft Intune management, and securely access corporate resources using device-based Conditional Access policies.

This release extends support to Red Hat Enterprise Linux 8.x and 9.x (LTS) which makes these capabilities possible:

- Microsoft Entra ID registration & enrollment of RedHat LTS (8/9) desktops.
- Conditional Access policies protecting web applications via Microsoft Edge. - Provides SSO for native & web applications (ex: Azure CLI, Microsoft Edge browser, Teams progressive web app (PWA), etc.) to access M365/Azure protected resources.
- Standard Intune compliance policies.
- Support for Bash scripts with custom compliance policies.
- Package Manager now supports RHEL *RPM* packages in addition to Debian *DEB* packages.

To learn more, see: [Microsoft Entra registered devices](#).

July 2024

General Availability - Insider Risk condition in Conditional Access is GA

Type: New feature

Service category: Conditional Access

Product capability: Identity Security & Protection

Insider Risk condition in Conditional Access is now GA

Insider Risk condition, in Conditional Access, is a new feature that uses signals from Microsoft Purview's Adaptive Protection capability to enhance the detection and automatic mitigation of Insider threats. This integration allows organizations to more effectively manage, and respond, to potential insider risks by using advanced analytics and real-time data.

For example, if Purview detects unusual activity from a user, Conditional Access can enforce extra security measures such as requiring multifactor authentication (MFA) or blocking access. This feature is a premium and requires a P2 license. For more information, see: [Common Conditional Access policy: Block access for users with insider risk](#).

General Availability - New SAML applications can't receive tokens through OAuth2/OIDC protocols

Type: Plan for change

Service category: Enterprise Apps

Product capability: Developer Experience

Starting late September 2024, applications indicated as *SAML* applications (via the `preferredSingleSignOnMode` property of the service principal) can't be issued JWT tokens. This change means they can't be the resource application in OIDC, OAuth2.0, or other protocols using JWTs. This change only affects SAML applications attempting to take a new dependency on JWT-based protocols; existing SAML applications already using these flows aren't affected. This update improves the security of apps.

For more information, see: [SAML authentication with Microsoft Entra ID](#).

General Availability - New Federated Apps available in Microsoft Entra Application gallery - July 2024

Type: New feature

Service category: Enterprise Apps

Product capability: Third Party Integration

In February 2024, we added the following 10 new applications in our App gallery with Federation support:

[Full story SAML, LSEG Workspace ↗](#)

You can also find the documentation of all the applications from here [https://aka.ms/AppsTutorial ↗](https://aka.ms/AppsTutorial).

For listing your application in the Microsoft Entra ID app gallery, read the details here [https://aka.ms/AzureADAppRequest ↗](https://aka.ms/AzureADAppRequest).

General Availability - Active Directory Federation Services (AD FS) Application Migration Wizard

Type: New feature

Service category: AD FS Application Migration

Product capability: Platform

The Active Directory Federation Services (AD FS) application migration wizard allows the user to quickly identify which AD FS relying party applications are compatible with being migrated to Microsoft Entra ID. This tool shows the migration readiness of each application and highlights issues with suggested actions to remediate. This tool also guides users through preparing an individual application for migration and configuring their new Microsoft Entra application. For more information on how to use this feature, see: [Use AD FS application migration to move AD FS apps to Microsoft Entra ID](#).

General Availability - Attacker in the Middle detection alert in Identity Protection

Type: New feature

Service category: Identity Protection

Product capability: Identity Security & Protection

The Attacker in the Middle detection is now Generally Available for users in Identity Protection.

This high precision detection is triggered on a user account compromised by an adversary that intercepted a user's credentials, including tokens issued. The risk is identified through Microsoft 365 Defender and raises the user with High risk to trigger the configured Conditional Access policy.

For more information on this feature, see: [What are risk detections?](#)

General Availability - Easy authentication with Azure App Service and Microsoft Entra External ID

Type: Changed feature

Service category: B2C - Consumer Identity Management

Product capability: B2B/B2C

An improved experience when using Microsoft Entra External ID as an identity provider for Azure App Service's built-in authentication, simplifying the process of configuring authentication and authorization for external-facing apps. You can complete initial configuration directly from the App Service authentication setup without switching into the external tenant. For more information, see: [Quickstart: Add app authentication to your web app running on Azure App Service](#).

June 2024

Plan for change - Passkey in Microsoft Authenticator (preview) registration experience is changing

Type: Plan for change

Service category: MFA

Product capability: End User Experiences

Starting late July 2024, through end of August 2024, we're rolling out changes to the registration experience for passkey in Microsoft Authenticator (preview) on the My Security-Info page. This registration experience change will go from a WebAuthn approach, to guide users to register by signing into the Microsoft Authenticator app. This change will occur automatically, and admins won't need to take any action. Here's more details:

- By default, we'll guide users to sign into the Authenticator app to set up passkeys.
 - If users are unable to sign in, they'll be able to fallback to an improved WebAuthn experience through a "*Having trouble?*" link on the page.
-

General Availability - Security Improvements to Microsoft Entra Connect Sync and Connect Health

Type: Changed feature

Service category: Provisioning

Product capability: Microsoft Entra Connect

Action Recommended: Security Improvements to Microsoft Entra Connect Sync and Connect Health

Since September 2023, we have been autoupgrading Microsoft Entra Connect Sync and Microsoft Entra Connect Health customers to an updated build as part of a

precautionary security-related service change. For customers who previously opted out of autoupgrade, or for whom autoupgrade failed, we strongly recommend that you upgrade to the latest versions by **September 23, 2024**.

When you upgrade to the latest versions, you ensure that when the service change takes effect, you avoid service disruptions for:

- Microsoft Entra Connect Sync
- Microsoft Entra Connect Health agent for Sync
- Microsoft Entra Connect Health agent for ADDS
- Microsoft Entra Connect Health agent for ADFS

See documentation here: [Security improvements to the autoupgrade process](#) for upgrade-related guidance, versioning information, and further details on the expected impacts of the service change.

Public Preview - MS Graph API support for per-user multifactor authentication

Type: New feature

Service category: MFA

Product capability: Identity Security & Protection

MS Graph API support for per-user multifactor authentication

Starting June 2024, we're releasing the capability to manage user status (Enforced, Enabled, Disabled) for per-user multifactor authentication through MS Graph API. This update replaces the legacy MSOnline PowerShell module that is being retired. The recommended approach to protect users with Microsoft Entra multifactor authentication is Conditional Access (for licensed organizations) and security defaults (for unlicensed organizations). For more information, see: [Enable per-user Microsoft Entra multifactor authentication to secure sign-in events](#).

Public Preview - Easy authentication with Azure App Service and Microsoft Entra External ID

Type: Changed feature

Service category: B2C - Consumer Identity Management

Product capability: B2B/B2C

We improved the experience when using Microsoft Entra External ID as an identity provider for Azure App Service's built-in authentication, simplifying the process of configuring authentication and authorization for external-facing apps. You can complete initial configuration directly from the App Service authentication setup without switching into the external tenant. For more information, see: [Quickstart: Add app authentication to your web app running on Azure App Service](#)

General Availability - Refactored account details screen in Microsoft Authenticator

Type: Plan for change

Service category: Microsoft Authenticator App

Product capability: User Authentication

In July, enhancements for the Microsoft Authenticator app UX roll-out. The account details page of a user account is reorganized to help users better understand, and interact with, the information and buttons on the screen. Key actions that a user can do today are available in the refactored page, but they're organized in three sections or categories that help better communicate to users:

- Credentials configured in the app
 - More sign in methods they can configure
 - Account management options in the app
-

General Availability - SLA Attainment Report at the Tenant Level

Type: New feature

Service category: Reporting

Product capability: Monitoring & Reporting

In addition to providing global SLA performance, Microsoft Entra ID reports tenant-level SLA performance for organizations with at least 5,000 monthly active users. This feature entered general availability in May 2024. The Service Level Agreement (SLA) sets a minimum bar of 99.99% for the availability of Microsoft Entra ID user authentication, reported on a monthly basis in the Microsoft Entra admin center. For more information, see: [What is Microsoft Entra Health?](#)

Preview – QR code sign-in, a new authentication method for Frontline Workers

Type: New feature

Service category: Authentications (Logins)

Product capability: User Authentication

We're introducing a new simple way for Frontline Workers to authenticate in Microsoft Entra ID with a QR code and PIN. This capability eliminates the need for users to enter and reenter long UPNs and alphanumeric passwords.

Beginning in August 2024, all users in your tenant now see a new link *Sign in with QR code* when navigating to <https://login.microsoftonline.com> > *Sign-in options* > *Sign in to an organization*. This new link, *Sign in with QR code*, is visible only on mobile devices (Android/iOS/iPadOS). If you aren't participating in the preview, users from your tenant can't sign in through this method while we're still in review. They receive an error message if they try to sign-in.

The feature has a *preview* tag until it's generally available. Your organization needs to be enabled to test this feature. Broad testing is available in public preview, to be announced later.

While the feature is in preview, no technical support is provided. Learn more about support during previews here: [Microsoft Entra ID preview program information](#).

May 2024

General Availability - Azure China 21Vianet now supports My sign-ins and MFA/SSPR Combined Registration

Type: Changed feature

Service category: MFA

Product capability: Identity Security & Protection

Beginning end of June 2024, all organizations utilizing Microsoft Azure China 21Vianet now has access to My Sign-ins activity reporting. They're required to use the combined security information registration end-user experience for MFA and SSPR. As a result of this enablement, users now see a unified SSPR and MFA registration experience when prompted to register for SSPR or MFA. For more information, see: [Combined security information registration for Microsoft Entra overview](#).

General Availability - \$select in signIn API

Type: New feature

Service category: MS Graph

Product capability: Monitoring & Reporting

The long-awaited `$select` property is now implemented into the `signIn` API. Utilize the `$select` to reduce the number of attributes that are returned for each log. This update should greatly help customers who deal with throttling issues, and allow every customer to run faster, more efficient queries.

General Availability - Multiple Passwordless Phone sign-ins for Android Devices

Type: New feature

Service category: Authentications (Logins)

Product capability: User Authentication

End users can now enable passwordless phone sign-in for multiple accounts in the Authenticator App on any supported Android device. Consultants, students, and others with multiple accounts in Microsoft Entra can add each account to Microsoft Authenticator and use passwordless phone sign-in for all of them from the same Android device. The Microsoft Entra accounts can be in the same tenant or different tenants. Guest accounts aren't supported for multiple account sign-ins from one device. For more information, see: [Enable passwordless sign-in with Microsoft Authenticator](#).

Public Preview - Bicep templates support for Microsoft Graph

Type: New feature

Service category: MS Graph

Product capability: Developer Experience

The Microsoft Graph Bicep extension brings declarative infrastructure-as-code (IaC) capabilities to Microsoft Graph resources. It allows you to author, deploy, and manage core Microsoft Entra ID resources using Bicep template files, alongside Azure resources.

- Existing Azure customers can now use familiar tools to deploy Azure resources and the Microsoft Entra resources they depend on, such as applications and service principals, IaC and DevOps practices.
- It also opens the door for existing Microsoft Entra customers to use Bicep templates and IaC practices to deploy and manage their tenant's Microsoft Entra resources.

For more information, see: [Bicep templates for Microsoft Graph resources](#)

Public Preview - Platform Single Sign-on for macOS with Microsoft Entra ID

Type: New feature

Service category: Authentications (Logins)

Product capability: User Authentication

Today we're announcing that Platform SSO for macOS is available in public preview with Microsoft Entra ID. Platform SSO is an enhancement to the Microsoft Enterprise SSO plug-in for Apple Devices that makes usage and management of Mac devices more seamless and secure than ever. At the start of public preview, Platform SSO works with Microsoft Intune. Other Mobile Device Management (MDM) providers are coming soon. Contact your MDM provider for more information on support and availability. For more information, see: [macOS Platform Single Sign-on overview \(preview\)](#).

Public Preview - Workflow History Insights in Lifecycle Workflows

Type: New feature

Service category: Lifecycle Workflows

Product capability: Identity Lifecycle Management

Customers can now monitor workflow health, and get insights throughout all their workflows in Lifecycle Workflows including viewing workflow processing data across workflows, tasks, and workflow categories. For more information, see: [Workflow Insights \(preview\)](#).

Public Preview - Configure Lifecycle Workflow Scope Using Custom Security Attributes

Type: New feature

Service category: Lifecycle Workflows

Product capability: Identity Lifecycle Management

Customers can now apply their confidential HR data stored in custom security attributes in addition to other attributes. This update enables customers to define the scope of their workflows in Lifecycle Workflows for automating joiner, mover, and leaver scenarios. For more information, see: [Use custom security attributes to scope a workflow](#).

Public Preview - Enable, Disable, and Delete synchronized users accounts with Lifecycle Workflows

Type: New feature

Service category: Lifecycle Workflows

Product capability: Identity Lifecycle Management

Lifecycle Workflows can now enable, disable, and delete user accounts that are synchronized from Active Directory Domain Services (AD DS) to Microsoft Entra. This feature allows you to ensure that the offboarding processes of your employees are completed by deleting the user account after a retention period.

For more information, see: [Managing synced on-premises users with Lifecycle Workflows](#).

Public Preview - External authentication methods for multifactor authentication

Type: New feature

Service category: MFA

Product capability: User Authentication

External authentication methods enable you to use your preferred multifactor authentication (MFA) solution with Microsoft Entra ID. For more information, see: [Manage an external authentication method in Microsoft Entra ID \(Preview\)](#).

General Availability - `LastSuccessfulSignIn`

Type: Changed feature

Service category: MS Graph

Product capability: Monitoring & Reporting

Due to popular demand and increased confidence in the stability of the properties, the update adds `LastSuccessfulSignIn` & `LastSuccessfulSigninDateTime` into V1. Feel free to take dependencies on these properties in your production environments now. For more information, see: [signInActivity resource type](#).

General Availability - Changing default accepted token version for new applications

Type: Plan for change

Service category: Other

Product capability: Developer Experience

Beginning in August 2024, new Microsoft Entra applications created using any interface (including the Microsoft Entra admin center, Azure portal, Powershell/CLI, or the Microsoft Graph application API) has the default value of the `requestedAccessTokenVersion` property in the app registration set to 2. This capability is a change from the previous default of null` (meaning 1). This means that new resource applications receive v2 access tokens instead of v1 by default. This update improves the security of apps. For more information on differences between token versions, see: [Access tokens in the Microsoft identity platform](#) and [Access token claims reference](#).

General Availability - Windows Account extension is now Microsoft Single Sign On

Type: Changed feature

Service category: Authentications (Logins)

Product capability: SSO

The Windows Account extension is now the [Microsoft Single Sign On](#) extension in docs and Chrome store. The Windows Account extension is updated to represent the new macOS compatibility. This capability is now known as the Microsoft Single Sign On (SSO) extension for Chrome, offering single sign-on and device identity features with the Enterprise SSO plug-in for Apple devices. This update is only a name change for the extension, there are no software changes to the extension itself.

General Availability - New provisioning connectors in the Microsoft Entra Application Gallery - May 2024

Type: New feature

Service category: App Provisioning

Product capability: Third Party Integration

Microsoft added the following new applications in our App gallery with Provisioning support. You can now automate creating, updating, and deleting of user accounts for these newly integrated apps:

- [ClearView Trade](#)

For more information about how to better secure your organization by using automated user account provisioning, see: [What is app provisioning in Microsoft Entra ID?](#).

April 2024

Public Preview - FIDO2 authentication in Android web browsers

Type: New feature

Service category: Authentications (Logins)

Product capability: User Authentication

Users can now sign in with a FIDO2 security key in both Chrome, and Microsoft Edge, on Android. This change is applicable to all users who are in scope for the FIDO2 authentication method. FIDO2 registration in Android web browsers isn't available yet.

For more information, see: [Support for FIDO2 authentication with Microsoft Entra ID](#).

General Availability - Security group provisioning to Active Directory using cloud sync

Type: New feature

Service category: Provisioning

Product capability: Microsoft Entra Cloud Sync

Security groups provisioning to Active Directory (also known as Group Writeback) is now generally available through Microsoft Entra Cloud Sync in Azure Global and Azure Government clouds. With this new capability, you can easily govern Active Directory based on-premises applications (Kerberos based apps) using Microsoft Entra Governance. For more information, see: [Provision groups to Active Directory using Microsoft Entra Cloud Sync](#).

Decommissioning of Group Writeback V2 (Public Preview) in Microsoft Entra Connect Sync

Type: Plan for change

Service category: Provisioning

Product capability: Microsoft Entra Connect Sync

The public preview of Group Writeback V2 (GWB) in Microsoft Entra Connect Sync will no longer be available after June 30, 2024. After this date, Connect Sync will no longer support provisioning cloud security groups to Active Directory.

Another similar functionality in Microsoft Entra Cloud Sync is *Group Provision to AD*. You can use this functionality instead of GWB V2 for provisioning cloud security groups to AD. Enhanced functionality in Cloud Sync, along with other new features, are being developed.

Customers who use this preview feature in Connect Sync should [switch their configuration from Connect Sync to Cloud Sync](#). Customers can choose to move all their hybrid sync to Cloud Sync, if it supports their needs. Customers can also choose to run Cloud Sync side-by-side and move only cloud security group provisioning to Azure AD onto Cloud Sync.

Customers who use Microsoft 365 groups to AD can continue using GWB V1 for this capability.

Customers can evaluate moving exclusively to Cloud Sync by using this wizard:
<https://aka.ms/EvaluateSyncOptions>

General availability - PIM approvals and activations on the Azure mobile app (iOS and Android) are available now

Type: New feature

Service category: Privileged Identity Management

Product capability: Privileged Identity Management

PIM is now available on the Azure mobile app in both iOS and Android. Customers can now approve or deny incoming PIM activation requests. Customers can also activate Microsoft Entra ID and Azure resource role assignments directly from an app on their devices. For more information, see: [Activate PIM roles using the Azure mobile app](#).

General Availability - On-premises password reset remediates user risk

Type: New feature

Service category: Identity Protection

Product capability: Identity Security & Protection

Organizations who enabled password hash synchronization can now allow password changes on-premises to remediate user risk. You can also use this capability to save hybrid users time and maintain their productivity with automatic self-service remediation in risk-based Conditional Access policies. For more information, see: [Remediate risks and unblock users](#).

General Availability - Custom Claims Providers enable token claim augmentation from external data sources

Type: New feature

Service category: Authentications (Logins)

Product capability: Extensibility

Custom authentication extensions allow you to customize the Microsoft Entra authentication experience by integrating with external systems. A custom claims provider is a type of custom authentication extension that calls a REST API to fetch claims from external systems. A custom claims provider maps claims from external systems into tokens and can be assigned to one or many applications in your directory. For more information, see: [Custom authentication extensions overview](#).

General Availability - Dynamic Groups quota increased to 15,000.

Type: Changed feature

Service category: Group Management

Product capability: Directory

Microsoft Entra organizations could previously have a maximum of 15,000 dynamic membership groups and dynamic administrative units combined.

This quota is increased to 15,000. For example, you can now have 15,000 dynamic membership groups and 10,000 dynamic AUs (or any other combination that adds up to 15k). You don't need to do anything to take advantage of this change - this update is available right now. For more information, see: [Microsoft Entra service limits and restrictions](#).

General Availability - Lifecycle Workflows: Export workflow history data to CSV files

Type: New feature

Service category: Lifecycle Workflows

Product capability: Identity Governance

In Lifecycle Workflows, IT admins can now export their workflow history data across users, runs, and tasks to CSV files for meeting their organization's reporting and auditing needs.

See [Download workflow history reports](#) to learn more.

Public preview - Native Authentication for Microsoft Entra External ID

Type: New feature

Service category: Authentications (Logins)

Product capability: User Authentication

Native authentication empowers developers to take complete control over the design of the sign-in experience of their mobile applications. It allows them to craft stunning, pixel-perfect authentication screens that are seamlessly integrated into their apps, rather than relying on browser-based solutions. For more information, see: [Native authentication \(preview\)](#).

Public Preview - Passkeys in Microsoft Authenticator

Type: New feature

Service category: Microsoft Authenticator App

Product capability: User Authentication

Users can now create device-bound passkeys in the Microsoft Authenticator to access Microsoft Entra ID resources. Passkeys in the Authenticator app provide cost-effective, phishing-resistant, and seamless authentications to users from their mobile devices. For more information, see <https://aka.ms/PasskeyInAuthenticator>.

General Availability - Maximum workflows limit in Lifecycle workflows is now 100

Type: Changed feature

Service category: Lifecycle Workflows

Product capability: Identity Governance

The maximum number of workflows that can be configured in Lifecycle workflows increased. Now IT admins can create up to 100 workflows in Lifecycle workflows. For more information, see: [Microsoft Entra ID Governance service limits](#).

Public Preview - Configure custom workflows to run mover tasks when a user's job profile changes

Type: New feature

Service category: Lifecycle Workflows

Product capability: Identity Governance

Lifecycle Workflows now supports the ability to trigger workflows based on job change events like changes to an employee's department, job role, or location and see them executed on the workflow schedule. With this feature, customers can use new workflow triggers to create custom workflows for executing tasks associated with employees moving within the organization including triggering:

- Workflows when a specified attribute changes
- Workflows when a user is added or removed from a group's membership
- Tasks to notify a user's manager about a move
- Tasks to assign licenses or remove selected licenses from a user

To learn more, see the [Automate employee mover tasks when they change jobs using the Microsoft Entra admin center](#) tutorial.

General Availability - Microsoft Graph activity logs

Type: New feature

Service category: Microsoft Graph

Product capability: Monitoring & Reporting

The Microsoft Graph activity logs is now generally available! Microsoft Graph activity logs give you visibility into HTTP requests made to the Microsoft Graph service in your tenant. With rapidly growing security threats, and an increasing number of attacks, this log data source allows you to perform security analysis, threat hunting, and monitor application activity in your tenant. For more information, see: [Access Microsoft Graph activity logs](#).

General Availability - New provisioning connectors in the Microsoft Entra Application Gallery - April 2024

Type: New feature

Service category: App Provisioning

Product capability: Third Party Integration

Microsoft added the following new applications in our App gallery with provisioning support. You can now automate creating, updating, and deleting of user accounts for these newly integrated apps:

[CultureHQ](#) [elia](#) [GoSkills](#) [Island](#) [Jellyfish](#)

For more information about how to better secure your organization by using automated user account provisioning, see [Automate user provisioning to SaaS applications with Microsoft Entra](#).

General Availability - Quick Microsoft Entra Verified ID setup

Type: New feature

Service category: Verified ID

Product capability: Decentralized Identities

Quick Microsoft Entra Verified ID setup, now generally available, removes several configuration steps an admin needs to complete with a single select on a Get started button. The quick setup takes care of signing keys, registering your decentralized ID, and verifying your domain ownership. It also creates a Verified Workplace Credential for you. For more information, see: [Quick Microsoft Entra Verified ID setup](#).

Public Preview - Assign Microsoft Entra roles using Entitlement Management

Type: New feature

Service category: Entitlement Management

Product capability: Entitlement Management

By assigning Microsoft Entra roles to employees, and guests, using Entitlement Management, you can look at a user's entitlements to quickly determine which roles are assigned to that user. When you include a Microsoft Entra role as a resource in an access package, you can also specify whether that role assignment is *eligible* or *active*.

Assigning Microsoft Entra roles through access packages helps to efficiently manage role assignments at scale and improves the role. For more information, see: [Assign Microsoft Entra roles \(Preview\)](#).

General Availability - Self-service password reset Admin policy expansion to include more roles

Type: Changed feature

Service category: Self Service Password Reset

Product capability: Identity Security & Protection

Self-service password reset (SSPR) policy for Admins expands to include three extra built-in admin roles. These extra roles include:

- Teams Administrator
- Teams Communications Administrator
- Teams Devices Administrator

For more information on Self-service password reset for admins, including the full list of in-scope admin roles, see [Administrator reset policy differences](#).

March 2024

Public Preview - Convert external users to internal

Type: New feature

Service category: User Management

Product capability: User Management

External user conversion enables customers to convert external users to internal members without needing to delete and create new user objects. Maintaining the same underlying object ensures the user's account, and access to resources, isn't disrupted and that their history of activities remains intact as their relationship with the host organization changes.

The external to internal user conversion feature includes the ability to convert on-premises synchronized users as well. For more information, see: [Convert external users to internal users \(Preview\)](#).

Public Preview - Alternate Email Notifications for Lockbox Requests

Type: New feature

Service category: Other

Product capability: Access Control

Customer Lockbox for Microsoft Azure is launching a new feature that enables customers to use alternate email IDs for getting lockbox notifications. This capability enables Lockbox customers to receive notifications in scenarios where their Azure account isn't email enabled, or if they have a service principal defined as the tenant admin or subscription owner.

Plan for change - Conditional Access location condition is moving up

Type: Plan for change

Service category: Conditional Access

Product capability: Identity Security & Protection

Beginning in mid-April 2024, the Conditional Access *Locations* condition is moving up. Locations become the *Network* assignment, with the new Global Secure Access assignment - *All compliant network locations*.

This change occurs automatically, so admins take no action. Here's more details:

- The familiar *Locations* condition is unchanged, updating the policy in the *Locations* condition are reflected in the *Network* assignment, and vice versa.
 - No functionality changes, existing policies continue to work without changes.
-

General Availability - Just-in-time application access with PIM for Groups

Type: New feature

Service category: Privileged Identity Management

Product capability: Privileged Identity Management

Provide just-in-time access to non-Microsoft applications such as AWS & GCP. This capability integrates PIM for groups. Application provisioning with PIM reduces the activation time from 40+ minutes to roughly 2 minutes when requesting just-in-time access to a role in non-Microsoft apps.

For more information, see:

- [AWS](#)
 - [GCP](#)
-

Public Preview - Azure Lockbox Approver Role for Subscription Scoped Requests

Type: New feature

Service category: Other

Product capability: Identity Governance

Customer Lockbox for Microsoft Azure is launching a new built-in Azure Role-based access control role that enables customers to use a lesser privileged role for users responsible for approving/rejecting Customer Lockbox requests. This feature is targeted to the customer admin workflow where a lockbox approver acts on the request from Microsoft Support engineer to access Azure resources in a customer subscription.

In this first phase, we're launching a new built-in Azure Role-based Access Control role. This role helps scope down the access possible for an individual with Azure Customer Lockbox approver rights on a subscription and its resources. A similar role for tenant-scoped requests is available in subsequent releases.

General Availability - New provisioning connectors in the Microsoft Entra Application Gallery - March 2024

Type: New feature

Service category: App Provisioning

Product capability: Third Party Integration

We added the following new applications in our App gallery with Provisioning support. You can now automate creating, updating, and deleting of user accounts for these newly integrated apps:

- [Astro](#)
- [Egnyte](#)
- [MobileIron](#)
- [SAS Viya SSO](#)

For more information about how to better secure your organization by using automated user account provisioning, see: [What is app provisioning in Microsoft Entra ID?](#).

General Availability - TLS 1.3 support for Microsoft Entra

Type: New feature

Service category: Other

Product capability: Platform

We're excited to announce that Microsoft Entra, is rolling out support for Transport Layer Security (TLS) 1.3 for its endpoints to align with security best practices ([NIST - SP 800-52 Rev. 2](#)). With this change, the Microsoft Entra ID related endpoints support both TLS 1.2 and TLS 1.3 protocols. For more information, see: [TLS 1.3 support for Microsoft Entra services](#).

General Availability - API driven inbound provisioning

Type: New feature

Service category: Provisioning

Product capability: Inbound to Microsoft Entra ID

With API-driven inbound provisioning, Microsoft Entra ID provisioning service now supports integration with any system of record. Customers and partners can choose any automation tool to retrieve workforce data from any system of record for provisioning to Microsoft Entra ID. This capability also applies to connected on-premises Active Directory domains. IT admins have full control on how the data is processed and transformed with attribute mappings. Once the workforce data is available in Microsoft Entra ID, IT admins can configure appropriate joiner-mover-leaver business processes using Microsoft Entra ID Governance Lifecycle Workflows. For more information, see: [API-driven inbound provisioning concepts](#).

General Availability - Changing Passwords in My Security Info

Type: New feature

Service category: My Security Info

Product capability: End User Experiences

Now Generally Available, My Sign Ins ([My sign-ins \(microsoft.com\)](#))  supports end users changing their passwords inline. When a user authenticates with a password and an MFA credential, they're able to change their password without entering their existing password. Beginning April 1, through a phased rollout, traffic from the [Change password \(windowsazure.com\)](#)  portal will redirect to the new My Sign Ins change experience. The [Change password \(windowsazure.com\)](#)  will no longer be available after June 2024, but will continue to redirect to the new experience.

For more information, see:

- [Combined security information registration for Microsoft Entra overview](#).
 - [Change work or school account settings in the My Account portal](#) 
-

February 2024

General Availability - Identity Protection and Risk Remediation on the Azure Mobile App

Type: New feature

Service category: Identity Protection

Product capability: Identity Security & Protection

Identity Protection, previously supported only on the portal, is a powerful tool that empowers administrators to proactively manage identity risks. Now available on the Azure Mobile app, administrators can respond to potential threats with ease and efficiency. This feature includes comprehensive reporting, offering insights into risky behaviors such as compromised user accounts and suspicious sign-ins.

With the Risky users report, administrators gain visibility into accounts flagged as compromised or vulnerable. Actions such as blocking/unblocking sign-ins, confirming the legitimacy of compromises, or resetting passwords are conveniently accessible, ensuring timely risk mitigation.

Additionally, the Risky sign-ins report provides a detailed overview of suspicious sign-in activities, aiding administrators in identifying potential security breaches. While capabilities on mobile are limited to viewing sign-in details, administrators can take necessary actions through the portal, such as blocking sign-ins. Alternatively, admins can choose to manage the corresponding risky user's account until all risks are mitigated.

Stay ahead of identity risks effortlessly with Identity Protection on the Azure Mobile app. These capabilities are intended to provide user with the tools to maintain a secure environment and peace of mind for their organization.

The mobile app can be downloaded at the following links:

- Android: <https://aka.ms/AzureAndroidWhatsNew>
 - IOS: <https://aka.ms/ReferAzureIOSWhatsNew>
-

Plan for change - Microsoft Entra ID Identity protection: Low risk age out

Type: Plan for change

Service category: Identity Protection

Product capability: Identity Security & Protection

Starting on March 31, 2024, all "low" risk detections and users in Microsoft Entra ID Identity Protection that are older than six months will be automatically aged out and dismissed. This change allows customers to focus on more relevant risk and provide a cleaner investigation environment. For more information, see: [What are risk detections?](#).

Public Preview - Expansion of the Conditional Access reauthentication policy for additional scenarios

Type: Changed feature

Service category: Conditional Access

Product capability: Identity Security & Protection

Reauthentication policy lets you require users to interactively provide their credentials again, typically before accessing critical applications and taking sensitive actions.

Combined with Conditional Access session control of Sign-in frequency, you can require reauthentication for users and sign-ins with risk, or for Intune enrollment. With this public preview, you can now require reauthentication on any resource protected by Conditional Access. For more information, see: [Require reauthentication every time](#).

General Availability - New premium user risk detection, Suspicious API Traffic, is available in Identity Protection

Type: New feature

Service category: Identity Protection

Product capability: Identity Security & Protection

We released a new premium user risk detection in Identity Protection called *Suspicious API Traffic*. This detection is reported when Identity Protection detects anomalous Graph traffic by a user. Suspicious API traffic might suggest that a user is compromised and conducting reconnaissance in their environment. For more information about Identity Protection detections including this one, visit our public documentation at the following link: [What are risks detections?](#).

General Availability - Granular filtering of Conditional Access policy list

Type: New feature

Service category: Conditional Access

Product capability: Access Control

Conditional Access policies can now be filtered on actor, target resources, conditions, grant control, and session control. The granular filtering experience can help admins

quickly discover policies containing specific configurations. For more information, see: [What is Conditional Access?](#).

End of support - Azure Active Directory Connector for Forefront Identity Manager (FIM WAAD Connector)

Type: Deprecated

Service category: Microsoft Identity Manager

Product capability: Inbound to Microsoft Entra ID

The Azure Active Directory Connector for Forefront Identity Manager (FIM WAAD Connector) from 2014 was deprecated in 2021. The standard support for this connector ended in April 2024. Customers must remove this connector from their MIM sync deployment, and instead use an alternative provisioning mechanism. For more information, see: [Migrate a Microsoft Entra provisioning scenario from the FIM Connector for Microsoft Entra ID](#).

General Availability - New provisioning connectors in the Microsoft Entra Application Gallery - February 2024

Type: New feature

Service category: App Provisioning

Product capability: Third Party Integration

We added the following new applications in our App gallery with Provisioning support. You can now automate creating, updating, and deleting of user accounts for these newly integrated apps:

- [Alohi](#)
- [Insightly SAML](#)
- [Starmind](#)

For more information about how to better secure your organization by using automated user account provisioning, see: [What is app provisioning in Microsoft Entra ID?](#).

General Availability - New Federated Apps available in Microsoft Entra Application gallery - February 2024

Type: New feature

Service category: Enterprise Apps

Product capability: Third Party Integration

In February 2024, we added the following 10 new applications in our App gallery with Federation support:

Crosswise, Stonebranch Universal Automation Center (SaaS Cloud), ProductPlan, Bigtincan for Outlook [↗](#), Blinktime [↗](#), Stargo [↗](#), Garage Hive BC v2 [↗](#), Avochato [↗](#), Luscii [↗](#), LEVR [↗](#), XM Discover, Sailsdock [↗](#), Mercado Electronic SAML, Moveworks, Silbo [↗](#), Alation Data Catalog, Papirfly SSO, Secure Cloud User Integration [↗](#), AlbertStudio [↗](#), Automatic Email Manager [↗](#), Streamboxy [↗](#), NewHotel PMS [↗](#), Ving Room [↗](#), Trevanna Tracks, Alteryx Server, RICOH Smart Integration [↗](#), Genius, Othership Workplace Scheduler, GitHub Enterprise Managed User - ghe.com, Thumb Technologies [↗](#), Freightender SSO for TRP (Tender Response Platform), BeWhere Portal (UPS Access) [↗](#), Flexiroute [↗](#), SEEDL [↗](#), Isolocity [↗](#), SpotDraft, Blinq, Cisco Phone OBTJ [↗](#), Applitools Eyes.

You can also find the documentation of all the applications from here

<https://aka.ms/AppsTutorial> [↗](#).

For listing your application in the Microsoft Entra ID app gallery, read the details here
<https://aka.ms/AzureADAppRequest> [↗](#).

January 2024

Generally Availability - New Microsoft Entra Home page

Type: Changed feature

Service category: N/A

Product capability: Directory

We redesigned the Microsoft Entra admin center's homepage to help you do the following tasks:

- Learn about the product suite
- Identify opportunities to maximize feature value
- Stay up to date with recent announcements, new features, and more!

See the new experience here: <https://entra.microsoft.com/> [↗](#)

Public Preview - Granular Certificate-Based Authentication Configuration in Conditional Access

Type: New feature

Service category: Conditional Access

Product capability: Identity Security & Protection

With the authentication strength capability in Conditional Access, you can now create a custom authentication strength policy, with advanced certificate-based authentication (CBA) options to allow access based on certificate issuer or policy OIDs. For external users whose MFA is trusted from partners' Microsoft Entra ID tenant, access can also be restricted based on these properties. For more information, see: [Custom Conditional Access authentication strengths](#).

Generally Availability - Conditional Access filters for apps

Type: New feature

Service category: Conditional Access

Product capability: Identity Security & Protection

Filters for apps in Conditional Access simplify policy management by allowing admins to tag applications with custom security, and target them in Conditional Access policies, instead of using direct assignments. With this feature, customers can scale up their policies, and protect any number of apps. For more information, see: [Conditional Access: Filter for applications](#)

Public preview - Cross-tenant manager synchronization

Type: New feature

Service category: Provisioning

Product capability: Identity Governance

Cross-tenant synchronization now supports synchronizing the manager attribute across tenants. For more information, see: [Attributes](#).

General Availability- Microsoft Defender for Office alerts in Identity Protection

Type: New feature

Service category: Identity Protection

Product capability: Identity Security & Protection

The *Suspicious sending patterns* risk detection type is discovered using information provided by Microsoft Defender for Office (MDO). This alert is generated when someone in your organization sent suspicious email. The alert is because the email is either at risk of being restricted from sending email, or has been restricted from sending email. This detection moves users to medium risk, and only fires in organizations that deployed MDO. For more information, see: [What are risk detections?](#).

Public preview - New Microsoft Entra recommendation to migrate off MFA Server

Type: New feature

Service category: MFA

Product capability: User Authentication

We've released a new recommendation in the Microsoft Entra admin center for customers to move off MFA Server to Microsoft Entra multifactor authentication. MFA Server will be retired on September 30, 2024. Any customers with MFA Server activity in the last seven days see the recommendation that includes details about their current usage, and steps on how to move to Microsoft Entra multifactor authentication. For more information, see: [Migrate from MFA Server to Microsoft Entra multifactor authentication](#).

Public Preview - New provisioning connectors in the Microsoft Entra Application Gallery - January 2024

Type: New feature

Service category: App Provisioning

Product capability: Third Party Integration

We added the following new applications in our App gallery with Provisioning support. You can now automate creating, updating, and deleting of user accounts for these newly integrated apps:

- [Personify Inc](#)
- [Screensteps](#)

- WiggleDesk

For more information about how to better secure your organization by using automated user account provisioning, see: [What is app provisioning in Microsoft Entra ID?](#).

General Availability - New Federated Apps available in Microsoft Entra Application gallery - January 2024

Type: New feature

Service category: Enterprise Apps

Product capability: Third Party Integration

In January 2024, we added the following new applications in our App gallery with Federation support:

[Boeing ToolBox](#), [Kloud Connect Practice Management](#), [トニチ・ネクスタ・メイシ](#) (Tonichi Nexta Meishi), [Vinkey](#), [Cognito Forms](#), [Ocurus](#), [Magister](#), [eFlok](#), [GoSkills](#), [FortifyData](#), Toolsfactory platform, [Briq](#), [Mailosaur](#), [Astro](#), [JobDiva / Teams VOIP Integration](#), [Colossyan SAML](#), [CallTower Connect](#), [Jellyfish](#), [MetLife Legal Plans Member App](#), [Navigo Cloud SAML](#), [Delivery Scheduling Tool](#), [Highspot for MS Teams](#), [Reach 360](#), [Fareharbor SAML SSO](#), [HPE Aruba Networking EdgeConnect Orchestrator](#), [Terranova Security Awareness Platform](#).

You can also find the documentation of all the applications from here <https://aka.ms/AppsTutorial>.

For listing your application in the Microsoft Entra ID app gallery, read the details here <https://aka.ms/AzureADAppRequest>.

December 2023

Public Preview - Configurable redemption order for B2B collaboration

Type: New feature

Service category: B2B

Product capability: B2B/B2C

With configurable redemption, you can customize the order of identity providers that your guest users can sign in with when they accept your invitation. This option lets your

override the default configuration order set by Microsoft and use your own. This option can be used to help with scenarios like prioritizing a SAML/WS-fed federation above a Microsoft Entra ID verified domain. This option disables certain identity providers during redemption, or even only using something like email one-time pass-code as a redemption option. For more information, see: [Configurable redemption \(Preview\)](#).

General Availability - Edits to Dynamic Group Rule Builder

Type: Changed feature

Service category: Group Management

Product capability: Directory

The dynamic group rule builder is updated to no longer include the '*contains*' and '*notContains*' operators, as they're less performant. If needed, you can still create rules for dynamic membership groups with those operators by typing directly into the text box. For more information, see: [Rule builder in the Azure portal](#).

November 2023

Decommissioning of Group Writeback V2 (Public Preview) in Microsoft Entra Connect Sync

Type: Plan for change

Service category: Provisioning

Product capability: Microsoft Entra Connect Sync

The public preview of Group Writeback V2 (GWB) in Microsoft Entra Connect Sync will no longer be available after June 30, 2024. After this date, Connect Sync will no longer support provisioning cloud security groups to Active Directory.

Another similar functionality is offered in Microsoft Entra Cloud Sync, called 'Group Provision to AD', that maybe used instead of GWB V2 for provisioning cloud security groups to AD. Enhanced functionality in Cloud Sync, along with other new features, are being developed.

Customers who use this preview feature in Connect Sync should [switch their configuration from Connect Sync to Cloud Sync](#). Customers can choose to move all their hybrid sync to Cloud Sync (if it supports their needs). They can also run Cloud Sync side-by-side and move only cloud security group provisioning to AD onto Cloud Sync.

Customers who provision Microsoft 365 groups to AD can continue using GWB V1 for this capability.

Customers can evaluate moving exclusively to Cloud Sync by using this wizard:
<https://aka.ms/EvaluateSyncOptions>

General Availability - Microsoft Entra Cloud Sync now supports ability to enable Exchange Hybrid configuration for Exchange customers

Type: New feature

Service category: Provisioning

Product capability: Microsoft Entra Connect

Exchange hybrid capability allows for the coexistence of Exchange mailboxes both on-premises and in Microsoft 365. Microsoft Entra Cloud Sync synchronizes a specific set of Exchange-related attributes from Microsoft Entra ID back into your on-premises directory. It also synchronizes any disconnected forests (no network trust needed between them). With this capability, existing customers who have this feature enabled in Microsoft Entra Connect sync can now migrate, and apply, this feature with Microsoft Entra cloud sync. For more information, see: [Exchange hybrid writeback with cloud sync](#).

General Availability - Guest Governance: Inactive Guest Insights

Type: New feature

Service category: Reporting

Product capability: Identity Governance

Monitor guest accounts at scale with intelligent insights into inactive guest users in your organization. Customize the inactivity threshold depending on your organization's needs, narrow down the scope of guest users you want to monitor, and identify the guest users that might be inactive. For more information, see: [Monitor and clean up stale guest accounts using access reviews](#).

Public Preview - lastSuccessfulSignIn property in signInActivity API

Type: New feature

Service category: MS Graph

Product capability: End User Experiences

An extra property is added to `signInActivity` API to display the last **successful** sign in time for a specific user, regardless if the sign in was interactive or non-interactive. The data won't be backfilled for this property, so you should expect to be returned only successful sign in data starting on December 8, 2023.

General Availability - Autorollout of Conditional Access policies

Type: New feature

Service category: Conditional Access

Product capability: Access Control

Starting in November 2023, Microsoft begins automatically protecting customers with Microsoft managed Conditional Access policies. Microsoft creates and enables these policies in external tenants. The following policies are rolled out to all eligible tenants, who are notified before policy creation:

1. Multifactor authentication for admin portals: This policy covers privileged admin roles and requires multifactor authentication when an admin signs into a Microsoft admin portal.
2. Multifactor authentication for per-user multifactor authentication users: This policy covers users with per-user multifactor authentication and requires multifactor authentication for all resources.
3. Multifactor authentication for high-risk sign-ins: This policy covers all users and requires multifactor authentication and reauthentication for high-risk sign-ins.

For more information, see:

- [Automatic Conditional Access policies in Microsoft Entra streamline identity protection](#)
 - [Microsoft-managed policies](#)
-

General Availability - Custom security attributes in Microsoft Entra ID

Type: New feature

Service category: Directory Management

Product capability: Directory

Custom security attributes in Microsoft Entra ID are business-specific attributes (key-value pairs) that you can define and assign to Microsoft Entra objects. These attributes can be used to store information, categorize objects, or enforce fine-grained access control over specific Azure resources. Custom security attributes can be used with [Azure attribute-based access control \(Azure ABAC\)](#). For more information, see: [What are custom security attributes in Microsoft Entra ID?](#).

Changes were made to custom security attribute audit logs for general availability that might affect your daily operations. If you have been using custom security attribute audit logs during the preview, there are the actions you must take before February 2024 to ensure your audit log operations aren't disrupted. For more information, see: [Custom security attribute audit logs](#).

Public Preview - New provisioning connectors in the Microsoft Entra Application Gallery - November 2023

Type: New feature

Service category: App Provisioning

Product capability: Third Party Integration

We added the following new applications in our App gallery with Provisioning support. You can now automate creating, updating, and deleting of user accounts for these newly integrated apps:

- [Colloquial](#)
- [Diffchecker](#)
- [M-Files](#)
- [XM Fax and XM SendSecure](#)
- [Rootly](#)
- [Simple In/Out](#)
- [Team Today](#)
- [YardiOne](#)

For more information about how to better secure your organization by using automated user account provisioning, see: [What is app provisioning in Microsoft Entra ID?](#)

General Availability - New Federated Apps available in Microsoft Entra Application gallery - November 2023

Type: New feature

Service category: Enterprise Apps

Product capability: Third Party Integration

In November 2023, we added the following 10 new applications in our App gallery with Federation support:

Citrix Cloud [↗](#), Freight Audit, Movement by project44, Alohi, AMCS Fleet Maintenance [↗](#), Real Links Campaign App [↗](#), Propely [↗](#), Contentstack, Jasper AI, IANS Client Portal, Avionic Interface Technologies LSMA [↗](#), CultureHQ, Hone, Collector Systems, NetSfere, Spendwise [↗](#), Stage and Screen

You can also find the documentation of all the applications from here

<https://aka.ms/AppsTutorial> [↗](#).

For listing your application in the Microsoft Entra ID app gallery, read the details here
<https://aka.ms/AzureADAppRequest> [↗](#).

ⓘ Note

In new updates from the previous version of the release notes: Microsoft Authenticator is not yet FIPS 140 compliant on Android. Microsoft Authenticator on Android is currently pending FIPS compliance certification to support our customers that may require FIPS validated cryptography.

October 2023

Public Preview - Managing and Changing Passwords in My Security Info

Type: New feature

Service category: My Profile/Account

Product capability: End User Experiences

My Sign Ins ([My Sign-Ins \(microsoft.com\)](https://my.microsoft.com/signin) [↗](#)) now supports end users managing and changing their passwords. Users are able to manage passwords in My Security Info and

change their password inline. If a user authenticates with a password and an MFA credential, they're able to change their password without entering their existing password.

For more information, see: [Combined security information registration for Microsoft Entra overview](#).

Public Preview - Govern AD on-premises applications (Kerberos based) using Microsoft Entra Governance

Type: New feature

Service category: Provisioning

Product capability: Microsoft Entra Cloud Sync

Security groups provisioning to AD (also known as Group Writeback) is now publicly available through Microsoft Entra Cloud Sync. With this new capability, you can easily govern AD based on-premises applications (Kerberos based apps) using Microsoft Entra Governance.

For more information, see: [Govern on-premises Active Directory based apps \(Kerberos\) using Microsoft Entra ID Governance](#)

Public Preview - Microsoft Entra Permissions Management: Permissions Analytics Report PDF for multiple authorization systems

Type: Changed feature

Service category:

Product capability: Permissions Management

The Permissions Analytics Report (PAR) lists findings relating to permissions risks across identities and resources in Permissions Management. The PAR is an integral part of the risk assessment process where customers discover areas of highest risk in their cloud infrastructure. This report can be directly viewed in the Permissions Management UI, downloaded in Excel (XSLX) format, and exported as a PDF. The report is available for all supported cloud environments: Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

The PAR PDF was redesigned to enhance usability, align with the product UX redesign effort, and address various customer feature requests. [You can download the PAR PDF](#)

for up to 10 authorization systems.

General Availability - Enhanced Devices List Management Experience

Type: Changed feature

Service category: Device Access Management

Product capability: End User Experiences

Several changes were made to the All Devices list since announcing public preview, including:

- Prioritized consistency and accessibility across the different components
- Modernized the list and addressed top customer feedback
 - Added infinite scrolling, column reordering, and the ability to select all devices
 - Added filters for OS Version and Autopilot devices
- Created more connections between Microsoft Entra and Intune
 - Added links to Intune in Compliant and MDM columns
 - Added Security Settings Management column

For more information, see: [View and filter your devices](#).

General Availability - Windows MAM

Type: New feature

Service category: Conditional Access

Product capability: Access Control

Windows MAM is the first step toward Microsoft management capabilities for unmanaged Windows devices. This functionality comes at a critical time when we need to ensure the Windows platform is on par with the simplicity and privacy promise we offer end users today on the mobile platforms. End users can access company resources without needing the whole device to be MDM managed.

For more information, see: [Require an app protection policy on Windows devices](#).

General Availability - Microsoft Security email update and Resources for Azure Active Directory rename to Microsoft

Entra ID

Type: Plan for change

Service category: Other

Product capability: End User Experiences

Microsoft Entra ID is the new name for Azure Active Directory (Azure AD). The rename and new product icon are now being deployed across experiences from Microsoft. Most updates are complete by mid-November of this year. As previously announced, it's a new name change, with no effect on deployments or daily work. There are no changes to capabilities, licensing, terms of service, or support.

From October 15 to November 15, Azure AD emails previously sent from azure-noreply@microsoft.com will start being sent from MSSecurity-noreply@microsoft.com. You might need to update your Outlook rules to match this change.

Additionally, we update email content to remove all references of Azure AD where relevant, and include an informational banner that announces this change.

Here are some resources to guide you rename your own product experiences or content where necessary:

- [How to: Rename Azure AD](#)
 - [New name for Azure Active Directory](#)
-

General Availability - End users will no longer be able to add password SSO apps in My Apps

Type: Deprecated

Service category: My Apps

Product capability: End User Experiences

Effective November 15, 2023, end users will no longer be able to add password SSO Apps to their gallery in My Apps. However, admins can still add password SSO apps following [these instructions](#). Password SSO apps previously added by end users remain available in My Apps.

For more information, see: [Discover applications](#).

General Availability - Restrict Microsoft Entra ID Tenant Creation To Only Paid Subscription

Type: Changed feature

Service category: Managed identities for Azure resources

Product capability: End User Experiences

The ability to create new tenants from the Microsoft Entra admin center allows users in your organization to create test and demo tenants from your Microsoft Entra ID tenant, [Learn more about creating tenants](#). When used incorrectly this feature can allow the creation of tenants that aren't managed or viewable by your organization. We recommend that you restrict this capability so that only trusted admins can use this feature, [Learn more about restricting member users' default permissions](#). We also recommend you use the Microsoft Entra audit log to monitor for the Directory Management: Create Company event that signals a new tenant created by a user in your organization.

To further protect your organization, Microsoft is now limiting this functionality to only paid customers. Customers on trial subscriptions are unable to create more tenants from the Microsoft Entra admin center. Customers in this situation who need a new trial tenant can sign up for a [Free Azure Account](#).

General Availability - Users can't modify GPS location when using location based access control

Type: Plan for change

Service category: Conditional Access

Product capability: User Authentication

In an ever-evolving security landscape, the Microsoft Authenticator is updating its security baseline for Location Based Access Control (LBAC) Conditional Access policies. Microsoft does this to disallow authentications where the user might be using a different location than the actual GPS location of the mobile device. Today, it's possible for users to modify the location reported by the device on iOS and Android devices. The Authenticator app starts to deny LBAC authentications where we detect that the user isn't using the actual location of the mobile device where the Authenticator is installed.

In the November 2023 release of the Authenticator app, users who are modifying the location of their device sees a denial message in the app when doing an LBAC authentication. Microsoft ensures that users aren't using older app versions to continue authenticating with a modified location. Beginning January 2024, any users that are on

Android Authenticator 6.2309.6329 version or prior and iOS Authenticator version 6.7.16 or prior are blocked from using LBAC. To determine which users are using older versions of the Authenticator app, you can use [our MSGraph APIs](#).

Public Preview - Overview page in My Access portal

Type: New feature

Service category: Entitlement Management

Product capability: Identity Governance

Today, when users navigate to myaccess.microsoft.com, they land on a list of available access packages in their organization. The new Overview page provides a more relevant place for users to land. The Overview page points them to the tasks they need to complete and helps familiarize users with how to complete tasks in My Access.

Admins can enable/disable the Overview page preview by signing into the Microsoft Entra admin center and navigating to Entitlement management > Settings > Opt-in Preview Features and locating My Access overview page in the table.

For more information, see: [My Access Overview page](#).

Public Preview - New provisioning connectors in the Microsoft Entra Application Gallery - October 2023

Type: New feature

Service category: App Provisioning

Product capability: Third Party Integration

We've added the following new applications in our App gallery with Provisioning support. You can now automate creating, updating, and deleting of user accounts for these newly integrated apps:

- [Amazon Business](#)
- [Bustle B2B Transport Systems](#)
- [Canva](#)
- [Cybozu](#)
- [Forcepoint Cloud Security Gateway - User Authentication](#)
- [Hypervault](#)
- [Oneflow](#)

For more information about how to better secure your organization by using automated user account provisioning, see: [What is app provisioning in Microsoft Entra ID?](#).

Public Preview - Microsoft Graph Activity Logs

Type: New feature

Service category: Microsoft Graph

Product capability: Monitoring & Reporting

The MicrosoftGraphActivityLogs provides administrators full visibility into all HTTP requests accessing your tenant's resources through the Microsoft Graph API. These logs can be used to find activity from compromised accounts, identify anomalous behavior, or investigate application activity. For more information, see: [Access Microsoft Graph activity logs \(preview\)](#).

Public Preview - Microsoft Entra Verified ID quick setup

Type: New feature

Service category: Other

Product capability: Identity Governance

Quick Microsoft Entra Verified ID setup, available in preview, removes several configuration steps an admin needs to complete with a single select on a Get started button. The quick setup takes care of signing keys, registering your decentralized ID, and verifying your domain ownership. It also creates a Verified Workplace Credential for you. For more information, see: [Quick Microsoft Entra Verified ID setup](#).

September 2023

Public Preview - Changes to FIDO2 authentication methods and Windows Hello for Business

Type: Changed feature

Service category: Authentications (Logins)

Product capability: User Authentication

Beginning January 2024, Microsoft Entra ID supports [device-bound passkeys](#) stored on computers and mobile devices as an authentication method in public preview, in

addition to the existing support for FIDO2 security keys. This update enables your users to perform phishing-resistant authentication using the devices that they already have.

We expand the existing FIDO2 authentication methods policy, and end user experiences, to support this preview release. For your organization to opt in to this preview, you need to enforce key restrictions to allow specified passkey providers in your FIDO2 policy.

Learn more about FIDO2 key restrictions [here](#).

In addition, the existing end user sign-in option for Windows Hello and FIDO2 security keys get indicated by "Face, fingerprint, PIN, or security key". The term "passkey" will be mentioned in the updated sign-in experience to be inclusive of passkey credentials presented from security keys, mobile devices, and platform authenticators like Windows Hello.

General Availability - Recovery of deleted application and service principals is now available

Type: New feature

Service category: Enterprise Apps

Product capability: Identity Lifecycle Management

With this release, you can now recover applications along with their original service principals, eliminating the need for extensive reconfiguration and code changes ([Learn more](#)). It significantly improves the application recovery story and addresses a long-standing customer need. This change is beneficial to you on:

- **Faster Recovery:** You can now recover their systems in a fraction of the time it used to take, reducing downtime and minimizing disruptions.
 - **Cost Savings:** With quicker recovery, you can save on operational costs associated with extended outages and labor-intensive recovery efforts.
 - **Preserved Data:** Previously lost data, such as SMAL configurations, is now retained, ensuring a smoother transition back to normal operations.
 - **Improved User Experience:** Faster recovery times translate to improved user experience and customer satisfaction, as applications are backed up and running swiftly.
-

Public Preview - New provisioning connectors in the Microsoft Entra Application Gallery - September 2023

Type: New feature

Service category: App Provisioning

Product capability: Third Party Integration

We've added the following new applications in our App gallery with Provisioning support. You can now automate creating, updating, and deleting of user accounts for these newly integrated apps:

- [Datadog](#)
- [Litmos](#)
- [Postman](#)
- [Recnice](#)

For more information about how to better secure your organization by using automated user account provisioning, see: [What is app provisioning in Microsoft Entra ID?](#).

General Availability - Web Sign-In for Windows

Type: Changed feature

Service category: Authentications (Logins)

Product capability: User Authentication

We're thrilled to announce that as part of the Windows 11 September moment, we're releasing a new Web Sign-In experience that will expand the number of supported scenarios and greatly improve security, reliability, performance, and overall end-to-end experience for our users.

Web Sign-In (WSI) is a credential provider on the Windows lock/sign-in screen for AADJ joined devices that provide a web experience used for authentication and returns an auth token back to the operating system to allow the user to unlock/sign-in to the machine.

Web Sign-In was initially intended to be used for a wide range of auth credential scenarios; however, it was only previously released for limited scenarios such as:

[Simplified EDU Web Sign-In](#) and recovery flows via [Temporary Access Password \(TAP\)](#).

The underlying provider for Web Sign-In is rewritten from the ground up with security and improved performance in mind. This release moves the Web Sign-in infrastructure from the Cloud Host Experience (CHX) WebApp to a newly written sign in Web Host (LWH) for the September moment. This release provides better security and reliability to support previous EDU & TAP experiences and new workflows enabling using various Auth Methods to unlock/sig in to the desktop.

General Availability - Support for Microsoft admin portals in Conditional Access

Type: New feature

Service category: Conditional Access

Product capability: Identity Security & Protection

When a Conditional Access policy targets the Microsoft Admin Portals cloud app, the policy is enforced for tokens issued to application IDs of the following Microsoft administrative portals:

- Azure portal
- Exchange admin center
- Microsoft 365 admin center
- Microsoft 365 Defender portal
- Microsoft Entra admin center
- Microsoft Intune admin center
- Microsoft Purview compliance portal

For more information, see: [Microsoft Admin Portals](#).

August 2023

General Availability - Tenant Restrictions V2

Type: New feature

Service category: Authentications (Logins)

Product capability: Identity Security & Protection

Tenant Restrictions V2 (TRv2) is now generally available for authentication plane via proxy.

TRv2 allows organizations to enable safe and productive cross-company collaboration while containing data exfiltration risk. With TRv2, you can control what external tenants your users can access from your devices or network using externally issued identities and provide granular access control on a per org, user, group, and application basis.

TRv2 uses the cross-tenant access policy, and offers both authentication and data plane protection. It enforces policies during user authentication, and on data plane access with Exchange Online, SharePoint Online, Teams, and MSGraph. While the data plane support

with Windows GPO and Global Secure Access is still in public preview, authentication plane support with proxy is now generally available.

Visit <https://aka.ms/tenant-restrictions-enforcement> for more information on tenant restriction V2 and Global Secure Access client side tagging for TRv2 at [Universal tenant restrictions](#).

Public Preview - Cross-tenant access settings supports custom Role-Based Access Controls roles and protected actions

Type: New feature

Service category: B2B

Product capability: B2B/B2C

Cross-tenant access settings can be managed with custom roles defined by your organization. This capability enables you to define your own finely scoped roles to manage cross-tenant access settings instead of using one of the built-in roles for management. [Learn more about creating your own custom roles](#).

You can also now protect privileged actions inside of cross-tenant access settings using Conditional Access. For example, you can require MFA before allowing changes to default settings for B2B collaboration. Learn more about [Protected actions](#).

General Availability - Additional settings in Entitlement Management autoassignment policy

Type: Changed feature

Service category: Entitlement Management

Product capability: Entitlement Management

In the Microsoft Entra ID Governance entitlement management autoassignment policy, there are three new settings. This capability allows a customer to select to not have the policy create assignments, not remove assignments, and to delay assignment removal.

Public Preview - Setting for guest losing access

Type: Changed feature

Service category: Entitlement Management

Product capability: Entitlement Management

An administrator can configure that when a guest brought in through entitlement management has lost their last access package assignment, they're deleted after a specified number of days. For more information, see: [Govern access for external users in entitlement management](#).

Public Preview - Real-Time Strict Location Enforcement

Type: New feature

Service category: Continuous Access Evaluation

Product capability: Access Control

Strictly enforce Conditional Access policies in real-time using Continuous Access Evaluation. Enable services like Microsoft Graph, Exchange Online, and SharePoint Online to block access requests from disallowed locations as part of a layered defense against token replay and other unauthorized access. For more information, see blog: [Public Preview: Strictly Enforce Location Policies with Continuous Access Evaluation](#) ↗ and documentation: [Strictly enforce location policies using continuous access evaluation \(preview\)](#).

Public Preview - New provisioning connectors in the Microsoft Entra Application Gallery - August 2023

Type: New feature

Service category: App Provisioning

Product capability: Third Party Integration

We've added the following new applications in our App gallery with Provisioning support. You can now automate creating, updating, and deleting of user accounts for these newly integrated apps:

- [Airbase](#)
- [Airtable](#)
- [Cleanmail Swiss](#)
- [Informacast](#)
- [Kintone](#)
- [O'reilly learning platform](#)

- Tailscale
- Tanium SSO
- Vbrick Rev Cloud
- Xledger

For more information about how to better secure your organization by using automated user account provisioning, see: [What is app provisioning in Microsoft Entra ID?](#).

General Availability - Continuous Access Evaluation for Workload Identities available in Public and Gov clouds

Type: New feature

Service category: Continuous Access Evaluation

Product capability: Identity Security & Protection

Real-time enforcement of risk events, revocation events, and Conditional Access location policies is now generally available for workload identities. Service principals on line of business (LOB) applications are now protected on access requests to Microsoft Graph.

For more information, see: [Continuous access evaluation for workload identities \(preview\)](#).

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Frequently asked questions about Microsoft Entra ID

FAQ

Microsoft Entra ID is a cloud-based identity and access management solution. It's a directory and identity management service that operates in the cloud and offers authentication and authorization services to various Microsoft services, such as Microsoft 365, Dynamics 365, and Microsoft Azure.

For more information, see [What is Microsoft Entra ID?](#)

Help with accessing Microsoft Entra ID and Azure

Why do I get "No subscriptions found" when I try to access the Microsoft Entra admin center or the Azure portal?

To access the Microsoft Entra admin center or the Azure portal, each user needs permissions with a valid subscription. If you don't have a paid Microsoft 365 or Microsoft Entra subscription, you need to activate a free [Microsoft Entra Account](#) or establish a paid subscription. All Azure subscriptions, whether paid or free, have a trust relationship with a Microsoft Entra tenant. All subscriptions rely on the Microsoft Entra tenant (directory) to authenticate and authorize security principals and devices.

For more information, see [How Azure subscriptions are associated with Microsoft Entra ID](#).

What's the relationship between Microsoft Entra ID, Microsoft Azure, and other Microsoft services, such as Microsoft 365?

Microsoft Entra ID provides you with common identity and access capabilities to all web services. Whether you're using Microsoft services, such as Microsoft 365, Power Platform, Dynamics 365, or other Microsoft products, you're already using Microsoft Entra ID to help turn on sign-on and access management for all cloud services.

All users who are set up to use Microsoft services are defined as user accounts in one or more Microsoft Entra instances, providing these accounts access to Microsoft Entra ID.

For more information, see [Microsoft Entra ID Plans & Pricing](#)

Microsoft Entra paid services, such as Enterprise Mobility + Security (Microsoft Enterprise Mobility + Security) complement other Microsoft services like Microsoft 365, with comprehensive enterprise-scale development, management, and security solutions.

For more information, see [The Microsoft Cloud](#).

What are the differences between Owner and Global Administrator?

By default, the person who signs up for a Microsoft Entra or Azure subscription is assigned the Owner role for Azure resources. An Owner can use either a Microsoft account or a work or school account from the directory that the Microsoft Entra or Azure subscription is associated with. This role is also authorized to manage services in the Azure portal.

If others need to sign in and access services by using the same subscription, you can assign them the appropriate [built-in role](#). For more information, see [Assign Azure roles using the Azure portal](#).

By default, the user who creates a Microsoft Entra tenant is automatically assigned the [Global Administrator](#) role. This user has access to all Microsoft Entra directory features. Microsoft Entra ID has a different set of administrator roles to manage the directory and identity-related features. These administrators have access to various features in the Azure portal. The administrator's role determines what they can do, like create or edit users, assign administrative roles to others, reset user passwords, manage user licenses, or manage domains.

For more information, see [Assign a user to administrator roles in Microsoft Entra ID](#) and [Assigning administrator roles in Microsoft Entra ID](#).

Is there a report that shows when my Microsoft Entra user licenses expire?

No. This isn't currently available.

How can I allow Microsoft Entra admin center URLs on my firewall or proxy server?

To optimize connectivity between your network and the Microsoft Entra admin center and its services, you might want to add specific Microsoft Entra admin center URLs to your allowlist. Doing so can improve performance and connectivity between your local- or wide area network.

Network administrators often deploy proxy servers, firewalls, or other devices, which can help secure and give control over how users access the internet. Rules designed to protect users can sometimes block or slow down legitimate business-related internet traffic. This traffic includes communications between you and Microsoft Entra admin center over the following URLs:

- *.entra.microsoft.com
- *.entra.microsoft.us
- *.microsoftonline.cn

For more information, see [Using Microsoft Entra application proxy to publish on-premises apps for remote users](#). Additional URLs that you should include are listed in the article [Allow the Azure portal URLs on your firewall or proxy server](#).

Help with hybrid Microsoft Entra ID

How do I leave a tenant when I'm added as a collaborator?

You can usually leave an organization on your own without having to contact an administrator. However, in some cases this option isn't available and you need to contact your tenant admin, who can delete your account in the external organization.

For more information, see [Leave an organization as an external user](#).

How can I connect my on-premises directory to Microsoft Entra ID?

You can connect your on-premises directory to Microsoft Entra ID by using Microsoft Entra Connect.

For more information, see [Integrating your on-premises identities with Microsoft Entra ID](#).

How do I set up SSO between my on-premises directory and my cloud applications?

You only need to set up single sign-on (SSO) between your on-premises directory and Microsoft Entra ID. As long as you access your cloud applications through Microsoft Entra ID, the service automatically drives your users to correctly authenticate with their on-premises credentials.

Implementing SSO from on-premises can be easily achieved with federation solutions such as Active Directory Federation Services (AD FS), or by configuring password hash sync. You can easily deploy both options by using the Microsoft Entra Connect configuration wizard.

For more information, see [Integrating your on-premises identities with Microsoft Entra ID](#).

Does Microsoft Entra ID provide a self-service portal for users in my organization?

Yes, Microsoft Entra ID provides you with the [Microsoft Entra ID Access Panel](#) for user self-service and application access. If you're a Microsoft 365 customer, you can find many of the same capabilities in the [Office 365 portal](#).

For more information, see [Introduction to the Access Panel](#).

Does Microsoft Entra ID help me manage my on-premises infrastructure?

Yes. The Microsoft Entra ID P1 or P2 edition provides you with Microsoft Entra Connect Health. Microsoft Entra Connect Health helps you monitor and gain insight into your on-premises identity infrastructure and the synchronization services.

For more information, see [Monitor your on-premises identity infrastructure and synchronization services in the cloud](#).

Help with password management

Can I use Microsoft Entra password write-back without password sync?

(For example, is it possible to use Microsoft Entra self-service password reset (SSPR) with password write-back and not store passwords in the cloud?)

This example scenario doesn't require the on-premises password to be tracked in Microsoft Entra. This is because you don't need to synchronize your Active Directory passwords to Microsoft Entra ID to enable write-back. In a federated environment, Microsoft Entra single sign-on (SSO) relies on the on-premises directory to authenticate the user.

How long does it take for a password to be written back to Active Directory on-premises?

Password write-back operates in real time.

For more information, see [Getting started with password management](#).

Can I use password write-back with passwords that are managed by an admin?

Yes, if you have password write-back enabled, the password operations performed by an admin are written back to your on-premises environment.

For more answers to password-related questions, see [Password management frequently asked questions](#).

What can I do if I can't remember my existing Microsoft 365 / Microsoft Entra password while trying to change my password?

There are a couple of options. You can use the self-service password reset (SSPR) if it's available. Whether SSPR works depends on how it's configured. For more information about resetting Microsoft Entra passwords, see [How does the password reset portal work](#).

For Microsoft 365 users, your admin can reset the password by using the steps outlined in [Reset user passwords](#).

For Microsoft Entra accounts, admins can reset passwords by using one of the following:

- [Reset a user's password using Microsoft Entra ID](#)
- [Reset a password using PowerShell](#)

Help with security

Are accounts locked after a specific number of failed attempts or is there a more sophisticated strategy used?

Microsoft Entra ID uses a more sophisticated strategy to lock accounts. This is based on the IP of the request and the passwords entered. The duration of the lockout also increases based on the likelihood that it's an attack.

For certain (common) passwords that get rejected, does this apply to passwords used only in the current directory?

Rejected passwords return the message 'This password has been used too many times'. This refers to passwords that are globally common, such as any variants of "Password" and "123456".

Will sign-in requests from dubious sources (botnets, for example) be blocked in a B2C tenant or does this require a Basic or Premium edition tenant?

We do have a gateway that filters requests and provides some protection from botnets, and is applied for all B2C tenants.

Help with application access

Where can I find a list of applications that are pre-integrated with Microsoft Entra ID and their capabilities?

Microsoft Entra ID has more than 2,600 pre-integrated applications from Microsoft, application service providers, and partners. All pre-integrated applications support single sign-on (SSO). SSO lets you use your organizational credentials to access your apps. Some of the applications also support automated provisioning and de-provisioning.

For a complete list of the pre-integrated applications, see the [Azure Marketplace](#).

What if the application I need is not in the Microsoft Entra marketplace?

With Microsoft Entra ID P1 or P2, you can add and configure any application that you want. Depending on your application's capabilities and your preferences, you can configure SSO and

automated provisioning.

For more information, see [Single sign-on SAML protocol](#) and [Develop and plan provisioning for a SCIM endpoint](#).

How do users sign in to applications using Microsoft Entra ID?

Microsoft Entra ID provides several ways for users to view and access their applications, such as:

- The [Microsoft Entra access panel](#)
- The Microsoft 365 application launcher
- Direct sign-in to federated apps
- Deep links to federated, password-based, or existing apps

For more information, see [End user experiences for applications](#).

What are the different ways Microsoft Entra ID enables authentication and single sign-on to applications?

Microsoft Entra ID supports many standardized protocols for authentication and authorization, such as SAML 2.0, OpenID Connect, OAuth 2.0, and WS-Federation. Microsoft Entra ID also supports password vaulting and automated sign-in capabilities for apps that only support forms-based authentication.

For more information, see [Identity fundamentals](#) and [Single sign-on for applications in Microsoft Entra ID](#).

Can I add applications that I'm running on-premises?

[Microsoft Entra application proxy](#) provides you with easy and secure access to on-premises web applications that you choose. You can access these applications in the same way that you access your software as a service (SaaS) apps in Microsoft Entra ID. There's no need for a VPN or to change your network infrastructure.

For more information, see [How to provide secure remote access to on-premises applications](#).

How do I require multifactor authentication for users who access a particular application?

With [Microsoft Entra Conditional Access](#), you can assign a unique access policy for each application. In your policy, you can require multifactor authentication always, or when users aren't connected to the local network.

For more information, see [Securing access to Microsoft 365 and other apps connected to Microsoft Entra ID](#).

What is automated user provisioning for SaaS apps?

Use Microsoft Entra ID to automate the creation, maintenance, and removal of user identities in many popular cloud SaaS apps.

For more information, see [What is app provisioning in Microsoft Entra ID?](#).

Can I set up a secure LDAP connection with Microsoft Entra ID?

No. Microsoft Entra ID doesn't support the Lightweight Directory Access Protocol (LDAP) protocol or Secure LDAP directly. However, it's possible to enable Microsoft Entra Domain Services instance on your Microsoft Entra tenant with properly configured network security groups through Azure Networking to achieve LDAP connectivity.

For more information, see [Configure secure LDAP for a Microsoft Entra Domain Services managed domain](#).

CSS template reference guide

Article • 12/01/2023

Configuring your company branding for the user sign-in process provides a seamless experience in your applications that use Microsoft Entra ID as the identity and access management service. Use this CSS reference guide if you're using the [CSS template](#) as part of the [customize company branding](#) process.

HTML selectors

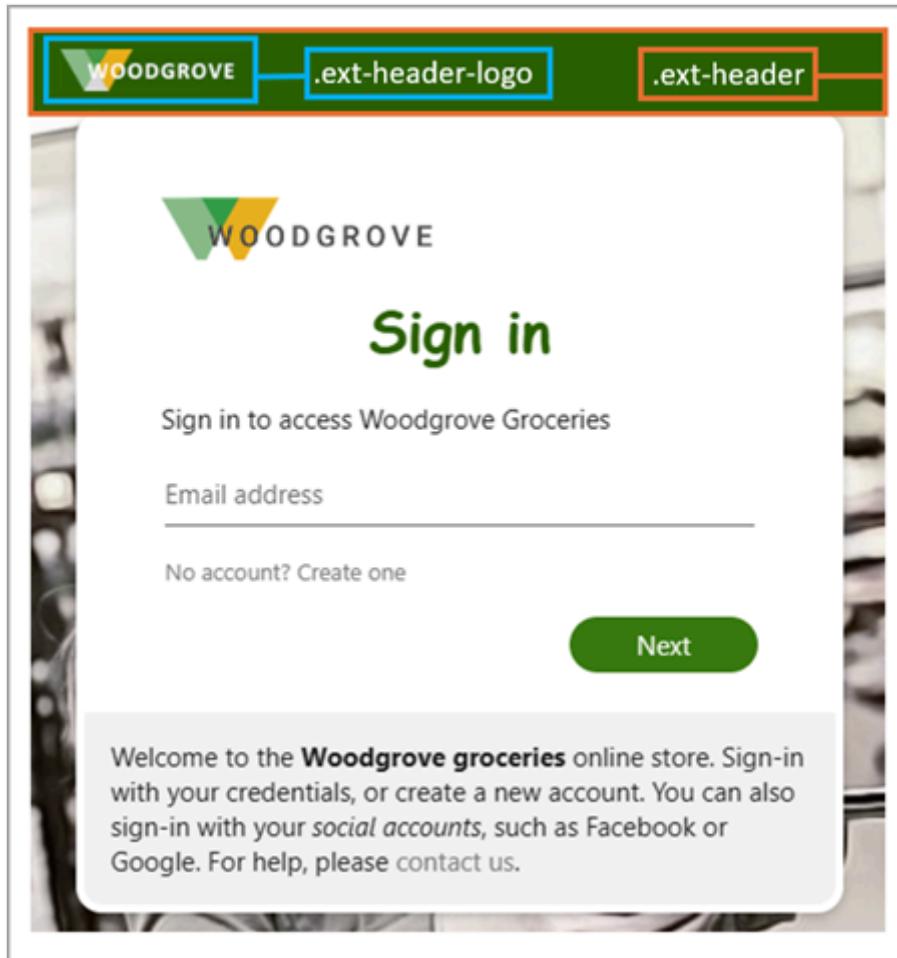
The following CSS styles become the default body and link styles for the whole page. Applying styles for other links or text override CSS selectors.

- `body` - Styles for the whole page
- Styles for links:
 - `a, a:link` - All links
 - `a:hover` - When the mouse is over the link
 - `a:focus` - When the link has focus
 - `a:focus:hover` - When the link has focus *and* the mouse is over the link
 - `a:active` - When the link is being clicked

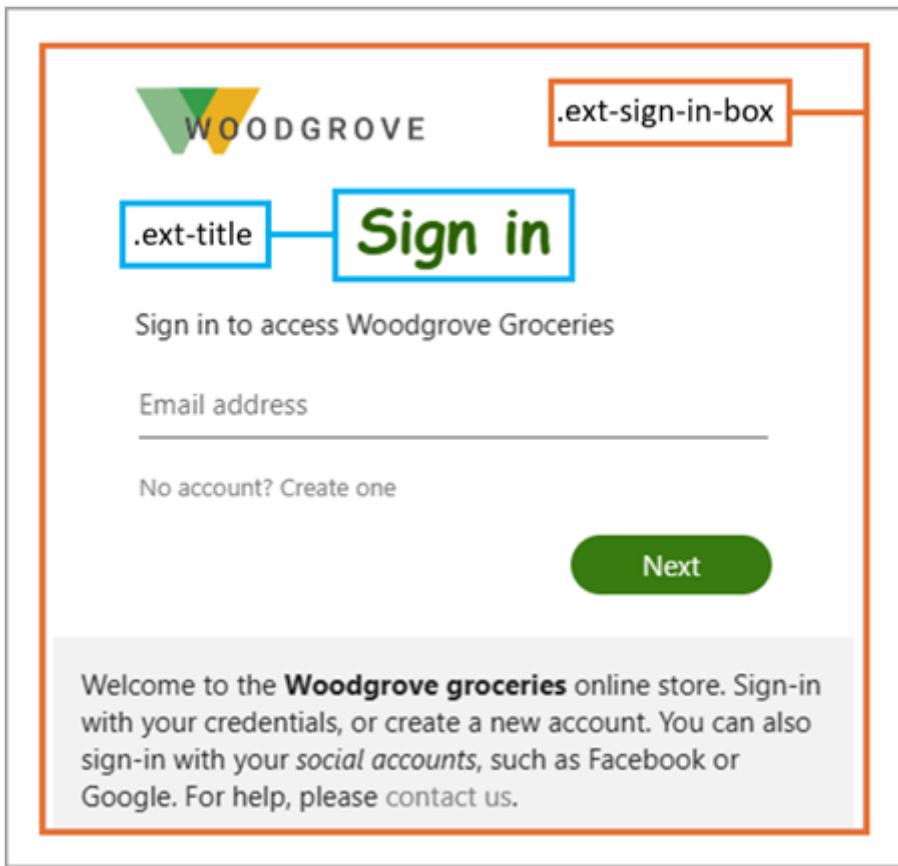
Microsoft Entra CSS selectors

Use the following CSS selectors to configure the details of the sign-in experience.

- `.ext-background-image` - Container that includes the background image in the default lightbox template
- `.ext-header` - Header at the top of the container
- `.ext-header-logo` - Header logo at the top of the container



- `.ext-middle` - Style for the full-screen background that aligns the sign-in box vertically to the middle and horizontally to the center
- `.ext-vertical-split-main-section` - Style for the container of the partial-screen background in the vertical split template that contains both a sign-in box and a background (This style is also known as the Active Directory Federation Services (ADFS) template.)
- `.ext-vertical-split-background-image-container` - Sign-in box background in the vertical split/ADFS template
- `.ext-sign-in-box` - Sign-in box container
- `.ext-title` - Title text



The image shows a sign-in form for Woodgrove Groceries. At the top left is the Woodgrove logo. To its right is a blue rectangular box labeled ".ext-sign-in-box". Below the logo is a blue button labeled ".ext-title" which contains the text "Sign in". A red line connects ".ext-sign-in-box" to the "Sign in" button. Below the "Sign in" button is the text "Sign in to access Woodgrove Groceries". Underneath this is a horizontal line labeled "Email address". Below the email input field is the text "No account? Create one". To the right of the "Email address" input is a green rounded rectangular button labeled "Next". At the bottom of the form is a gray box containing the text: "Welcome to the **Woodgrove groceries** online store. Sign-in with your credentials, or create a new account. You can also sign-in with your *social accounts*, such as Facebook or Google. For help, please contact us." A red line surrounds the entire sign-in form.

WOODGROVE

.ext-sign-in-box

.ext-title

Sign in

Sign in to access Woodgrove Groceries

Email address

No account? Create one

Next

Welcome to the **Woodgrove groceries** online store. Sign-in with your credentials, or create a new account. You can also sign-in with your *social accounts*, such as Facebook or Google. For help, please contact us.

- `.ext-subtitle` - Subtitle text
- Styles for primary buttons:
 - `.ext-button.ext-primary` - Primary button default style
 - `.ext-button.ext-primary:hover` - When the mouse is over the button
 - `.ext-button.ext-primary:focus` - When the button has focus
 - `.ext-button.ext-primary:focus:hover` - When the button has focus *and* the mouse is over the button
 - `.ext-button.ext-primary:active` - When the button is being clicked



Sign in

Sign in to access Woodgrove Groceries

Email address

No account? Create one

Next

Welcome to the **Woodgrove groceries** online store. Sign-in with your credentials, or create a new account. You can also sign-in with your *social accounts*, such as Facebook or Google. For help, please contact us.

- Styles for secondary buttons:
 - `.ext-button.ext-secondary` - Secondary buttons
 - `.ext-button.ext-secondary:hover` - When the mouse is over the button
 - `.ext-button.ext-secondary:focus` When the button has focus
 - `.ext-button.ext-secondary:focus:hover` - When the button has focus *and* the mouse is over the button
 - `.ext-button.ext-secondary:active` - When the button is being clicked



Create account

Sign up to access Woodgrove Groceries

Email

Have an account? Sign in instead

[Back](#)

[Next](#)

Welcome to the **Woodgrove groceries** online store. Sign-in with your credentials, or create a new account. You can also sign-in with your *social accounts*, such as Facebook or Google. For help, please contact us.

- `.ext-error` - Error text



Sign in

Sign in to access Woodgrove Groceries

We couldn't find an account with this email address.

`someone@example.com`

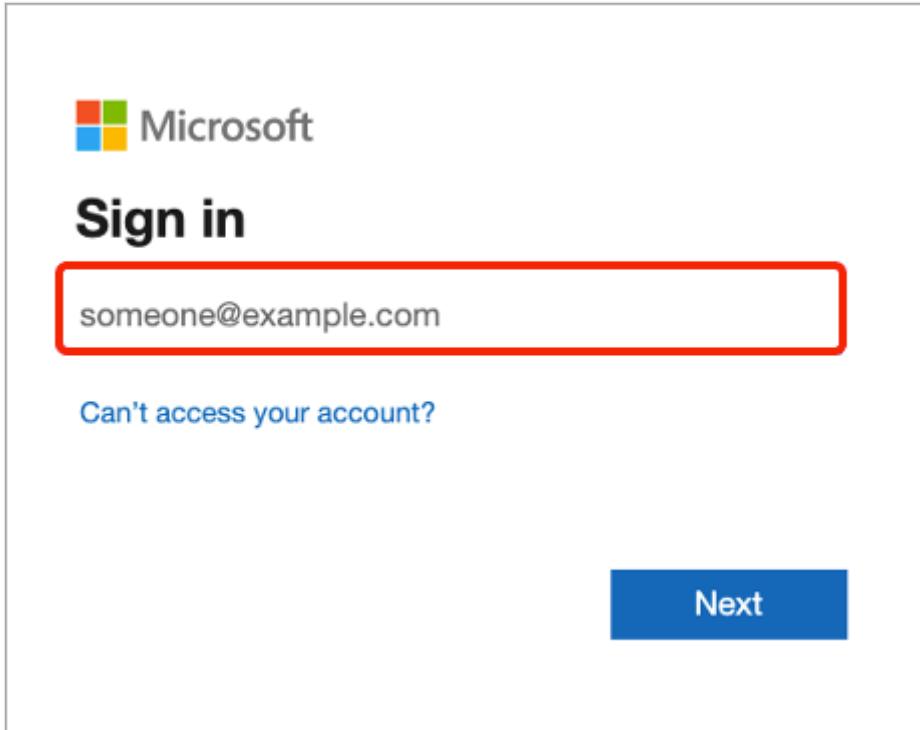
No account? Create one

[Next](#)

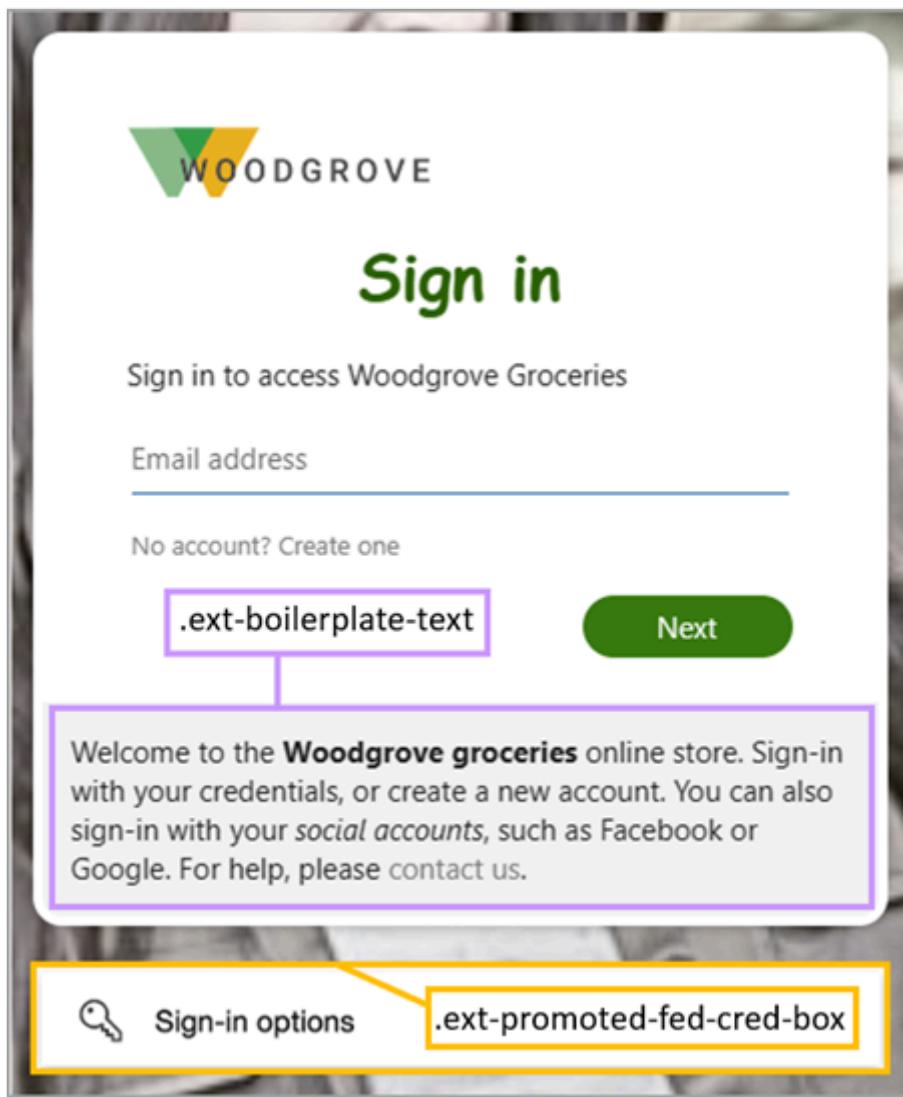
Welcome to the **Woodgrove groceries** online store. Sign-in with your credentials, or create a new account. You can also sign-in with your *social accounts*, such as Facebook or Google. For help, please contact us.

- Styles for text boxes:

- `.ext-input.ext-text-box` - Text boxes
- `.ext-input.ext-text-box.ext-has-error` - When there's a validation error associated with the text box
- `.ext-input.ext-text-box:hover` - When the mouse is over the text box
- `.ext-input.ext-text-box:focus` - When the text box has focus
- `.ext-input.ext-text-box:focus:hover` - When the text box has focus *and* the mouse is over the text box



- `.ext-boilerplate-text` - Custom message text at the bottom of the sign-in box
- `.ext-promoted-fed-cred-box` - Sign-in options text box



- Styles for the footer:
 - `.ext-footer` - Footer area at the bottom of the page
 - `.ext-footer-links` - Links area in the footer at the bottom of the page
 - `.ext-footer-item` - Link items (such as "Terms of use" or "Privacy & cookies") in the footer at the bottom of the page
 - `.ext-debug-item` - Debug details ellipsis in the footer at the bottom of the page

Feedback

Was this page helpful?

Yes

No

[Provide product feedback ↗](#)

Bulk operations

Article • 03/05/2025

Bulk operations in Microsoft Entra ID enable you to perform actions on multiple entities, such as users, groups, and devices, at once. These actions can include creating, deleting, or updating multiple records in a single operation. Bulk operations can greatly streamline administrative tasks and improve efficiency.

Bulk operations in the Microsoft Entra admin portal could time out and fail on large tenants. This limitation is a known issue due to scaling limitations.

ⓘ Note

When performing bulk operations, such as import or create, you may encounter a problem if the bulk operation doesn't complete within the hour. To work around this issue, we recommend splitting the number of records processed per batch. For example, before starting an export you could limit the result set by filtering on a group type or user name to reduce the size of the results. By refining your filters, essentially you are limiting the data returned by the bulk operation.

Bulk operations workaround

A workaround for this issue is to use PowerShell to make direct Microsoft Graph API calls. For bulk download users and groups failure, we recommend using the PowerShell cmdlets `GET-MgGroup -All` and `GET-MgUser -All`.

The following PowerShell code examples are for bulk operations related to:

- [Users](#)
- [Groups](#)
- [Devices](#)

Users

Download all users

Azure PowerShell

```

# Import the Microsoft Graph module
Import-Module Microsoft.Graph

# Authenticate to Microsoft Graph (you may need to provide your credentials)
Connect-MgGraph -Scopes "User.Read.All"

# Get all users using Get-MgUser
$users = Get-MgUser -All -ConsistencyLevel eventual -Property Id,
DisplayName,
UserPrincipalName,UserType,OnPremisesSyncEnabled,CompanyName,CreationType

# Specify the output CSV file path
$outputCsvPath = "C:\\\\Users\\\\YourUsername\\\\Documents\\\\Users.csv"

# Create a custom object to store user data
$userData = @()

# Loop through each user and collect relevant data
foreach ($user in $users) {
    $userObject = [PSCustomObject]@{
        Id = $user.Id
        DisplayName = $user.DisplayName
        UserPrincipalName = $user.UserPrincipalName
        UserType = $user.UserType
        OnPremisesSyncEnabled = $user.OnPremisesSyncEnabled
        CompanyName = $user.CompanyName
        CreationType = $user.CreationType
    }
    $userData += $userObject
}

# Export user data to a CSV file
$userData | Export-Csv -Path $outputCsvPath -NoTypeInformation

# Disconnect from Microsoft Graph
Disconnect-MgGraph

Write-Host "User data exported to $outputCsvPath"

```

Create users

Azure PowerShell

```

# Import the Microsoft Graph module
Import-Module Microsoft.Graph

# Authenticate to Microsoft Graph (you may need to provide your credentials)
Connect-MgGraph -Scopes "User.ReadWrite.All"

# Specify the path to the CSV file containing user data
$csvFilePath = "C:\\\\Path\\\\To\\\\Your\\\\Users.csv"

```

```

# Read the CSV file (adjust the column names as needed)
$usersData = Import-Csv -Path $csvFilePath

# Loop through each row in the CSV and create users \
foreach ($userRow in $usersData) {
    $userParams = @{
        DisplayName = $userRow.'Name [displayName] Required'
        UserPrincipalName = $userRow.'User name [userPrincipalName]
Required'
        PasswordProfile = @{
            Password = $userRow.'Initial password [passwordProfile]
Required'
        }
        AccountEnabled = $true
        MailNickName = $userRow.mailNickName
    }
    try {
        New-MgUser @userParams
        Write-Host "User $($userRow.UserPrincipalName) created
successfully."
    } catch {
        Write-Host "Error creating user $($userRow.UserPrincipalName):
$($_.Exception.Message)"
    }
}

# Disconnect from Microsoft Graph
Disconnect-MgGraph

Write-Host "Bulk user creation completed."

```

① Note

Make sure your CSV file contains the necessary columns (for example; `DisplayName`, `UserPrincipalName`, and so on). Also, adjust the script to match the actual column names in your CSV file.

Delete users

Azure PowerShell

```

# Import the Microsoft Graph module
Import-Module Microsoft.Graph

# Authenticate to Microsoft Graph (you may need to provide your credentials)
Connect-MgGraph -Scopes "User.ReadWrite.All"

# Specify the path to the CSV file containing user data

```

```

$csvFilePath = "C:\\Path\\To\\Your\\Users.csv"

# Read the CSV file (adjust the column names as needed)
$usersData = Import-Csv -Path $csvFilePath

# Loop through each row in the CSV and delete users
foreach ($userRow in $usersData) {
    try {
        Remove-MgUser -UserId $userRow.UserPrincipalName -Confirm:$false
        Write-Host "User $($userRow.UserPrincipalName) deleted
successfully."
    } catch {
        Write-Host "Error deleting user $($userRow.UserPrincipalName):
$($_.Exception.Message)"
    }
}

# Disconnect from Microsoft Graph
Disconnect-MgGraph

Write-Host "Bulk user deletion completed."

```

① Note

Make sure your CSV file contains the necessary columns (for example, `UserPrincipalName`). Also, adjust the script to match the actual column names in your CSV file.

Groups

Bulk download all groups

Azure PowerShell

```

Import-Module Microsoft.Graph.Groups

# Authenticate to Microsoft Graph (you may need to provide your
credentials)
Connect-MgGraph -Scopes "Group.Read.All"

# Get the group members
$groups = Get-MgGroup -All | Select displayName, Id, groupTypes,mail

# Create a custom object to store group data
$groupData = @()

# Loop through each group and collect relevant data

```

```

foreach ($group in $groups) {
    if ($group.groupTypes -contains "Unified"){$groupType = "Microsoft 365"}
    else {$groupType = "Security"}
    if ($group.groupTypes -contains "DynamicMembership"){$membershipType =
"Dynamic"}
    else {$membershipType = "Assigned"}
    $groupObject = [PSCustomObject]@{
        Id = $group.Id
        DisplayName = $group.displayName
        Mail = $group.mail
        GroupType = $groupType
        MembershipType = $membershipType
    }
    $groupData += $groupObject
}

# Specify the output CSV file path
$outputCsvPath = "C:\\\\Users\\\\<YourUsername>\\\\Documents\\\\Groups.csv"

$groupData | Export-Csv -Path $outputCsvPath -NoTypeInformation

Write-Host "Group members exported to $outputCsvPath"

```

Bulk download members of a group

Azure PowerShell

```

Import-Module Microsoft.Graph.Groups

# Authenticate to Microsoft Graph (you may need to provide your
credentials)
Connect-MgGraph -Scopes "Group.Read.All,GroupMember.Read.All"

# Set the group ID of the group whose members you want to download
$groupId = "your_group_id"

# Get the group members
$members = Get-MgGroupMember -GroupId $groupId -All | select * -
ExpandProperty additionalProperties | Select-Object @(
    'id'
    @{
        Name      = 'userPrincipalName'
        Expression = {
            $_.AdditionalProperties["userPrincipalName"] }
    }
    @{
        Name = 'displayName'
        Expression = { $_.AdditionalProperties["displayName"] }
    }
)

# Specify the output CSV file path
$outputCsvPath = "C:\\\\Users\\\\YourUserName\\\\Documents\\\\GroupMembers.csv"

```

```
$members | Export-Csv -Path $outputCsvPath -NoTypeInformation

# Disconnect from Microsoft Graph
Disconnect-MgGraph

Write-Host "Group members exported to $outputCsvPath"
```

Add members in bulk

Azure PowerShell

```
Import-Module Microsoft.Graph.Groups

# Authenticate to Microsoft Graph (you may need to provide your
credentials)
Connect-MgGraph -Scopes "GroupMember.ReadWrite.All"

# Import the CSV file
$members = Import-Csv -Path "C:\path\to\your\file.csv"

# Define the Group ID
$groupId = "your-group-id"

# Iterate over each member and add them to the group
foreach ($member in $members) {
    try{
        New-MgGroupMember -GroupId $groupId -DirectoryObjectId
$member.memberObjectId
        Write-Host "Added $($member.memberObjectId) to the group."
    }
    Catch{
        Write-Host "Error adding member
 $($member.memberObjectId):$($_.Exception.Message)"
    }
}

# Disconnect from Microsoft Graph
Disconnect-MgGraph
```

Remove members in bulk

Azure PowerShell

```
Import-Module Microsoft.Graph.Groups

# Authenticate to Microsoft Graph (you may need to provide your
credentials)
Connect-MgGraph -Scopes "GroupMember.ReadWrite.All"
```

```

# Import the CSV file
$members = Import-Csv -Path "C:\path\to\your\file.csv"

# Define the Group ID
$groupId = "your-group-id"

# Iterate over each member and add them to the group
foreach ($member in $members) {
    try{
        Remove-MgGroupMemberByRef -GroupId $groupId -DirectoryObjectId
$member.memberObjectId \
        Write-Host "Removed $($member.memberObjectId) from the group."
    }
    Catch{
        Write-Host "Error removing member
 $($member.memberObjectId):$($_.Exception.Message)"
    }
}

# Disconnect from Microsoft Graph
Disconnect-MgGraph

```

Devices

Bulk download all devices

Azure PowerShell

```

Import-Module Microsoft.Graph

# Authenticate to Microsoft Graph (you may need to provide your
credentials)
Connect-MgGraph -Scopes "Device.Read.All"

# Get all devices
$devices = Get-MgDevice -All |select
displayName,deviceId,operatingSystem,operatingSystemVersion,isManaged,isComp
liant,mdmAppId,registeredOwners,TrustType

# Specify the output CSV file path
$outputCsvPath = "C:\\\\Users\\\\YourUserName\\\\Documents\\\\Devices.csv"

$devices| Export-Csv -Path $outputCsvPath -NoTypeInformation

Write-Host "Devices exported to $outputCsvPath"

```

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback 

New name for Azure Active Directory

Article • 05/07/2025

Microsoft renamed Azure Active Directory (Azure AD) to Microsoft Entra ID to communicate the multicloud, multiplatform functionality of the products, alleviate confusion with Windows Server Active Directory, and unify the [Microsoft Entra](#) product family.

No interruptions to usage or service

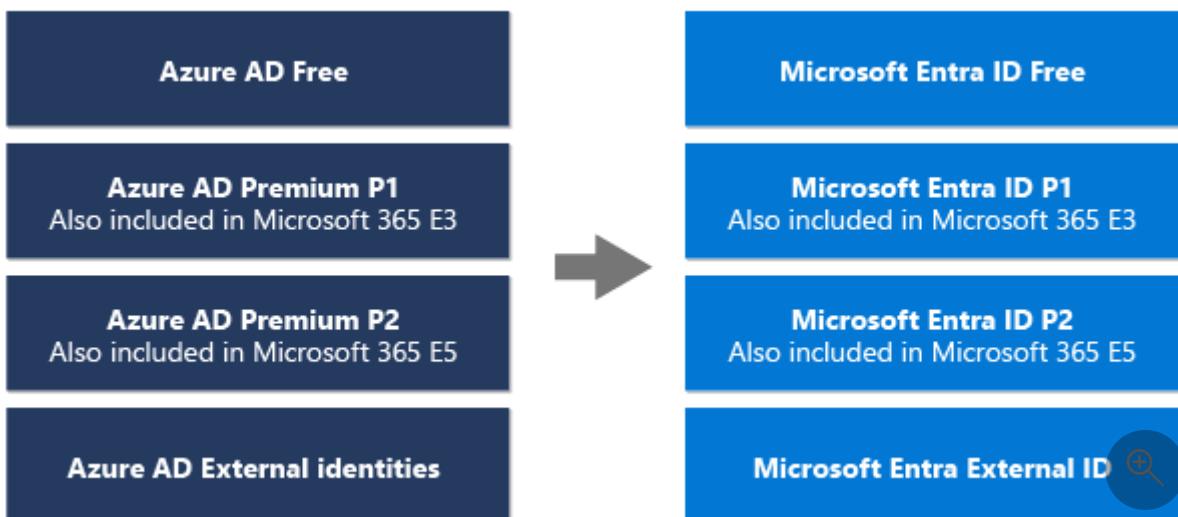
If you're currently using Azure AD today or previously deployed Azure AD in your organizations, you can continue to use the service without interruption. All existing deployments, configurations, and integrations continue to function as they do today without any action from you.

You can continue to use familiar Azure AD capabilities that you can access through the Azure portal, Microsoft 365 admin center, and the [Microsoft Entra admin center](#).

All features and capabilities are still available in the product. Licensing, terms, service-level agreements, product certifications, support and pricing remain the same.

To make the transition seamless, all existing login URLs, APIs, PowerShell cmdlets, and Microsoft Authentication Libraries (MSAL) stay the same, as do developer experiences and tooling.

Service plan display names changed on October 1, 2023. Microsoft Entra ID Free, Microsoft Entra ID P1, and Microsoft Entra ID P2 are the new names of standalone offers, and all capabilities included in the current Azure AD plans remain the same. Microsoft Entra ID – previously known as Azure AD – continues to be included in Microsoft 365 licensing plans, including Microsoft 365 E3 and Microsoft 365 E5. Details on pricing and what's included are available on the [pricing and free trials page](#).



For self-service support, look for the topic path of Microsoft Entra or Azure Active Directory/Microsoft Entra ID.

The product name and icons are changing, and features are now branded as Microsoft Entra instead of Azure AD. If you're updating the name to Microsoft Entra ID in your own content or experiences, see [How to: Rename Azure AD](#).

Naming changes and exceptions

Product name

Microsoft Entra ID is the new name for Azure AD. The names Azure Active Directory, Azure AD, and AAD are replaced with Microsoft Entra ID.

- Microsoft Entra is the name for the product family of identity and network access solutions.
- Microsoft Entra ID is one of the products within that family.
- Acronym usage isn't encouraged, but if you must replace AAD with an acronym due to space limitations, use ME-ID.

Logo/icon

Azure AD product icons are replaced with the Microsoft Entra ID product icon.

 Expand table

Azure AD product icons	Microsoft Entra ID product icon
	

You can download the Microsoft Entra ID icon here: [Microsoft Entra architecture icons](#)

Feature names

Capabilities or services formerly known as "Azure Active Directory <feature name>" or "Azure AD <feature name>" are branded as Microsoft Entra product family features. This change is done across our portfolio to avoid naming length and complexity, and because many features work across all the products. For example:

- "Azure AD Conditional Access" is now "Microsoft Entra Conditional Access"

- "Azure AD single sign-on" is now "Microsoft Entra single sign-on"

For a detailed list, see the [Glossary of updated terminology](#).

What names aren't changing?

The following table lists terminology that's not impacted by the rename. Names aren't changing for Active Directory, developer tools, Azure AD B2C, nor deprecated or retired functionality, features, or services.

 [Expand table](#)

Correct terminology	Details
Active Directory • Windows Server	Windows Server Active Directory, commonly known as Active Directory, and related features and services associated with Active Directory aren't branded with Microsoft Entra.
Active Directory • Active Directory	
Federation Services (AD FS) • Active Directory	
Domain Services (AD DS) • Active Directory • Any Active Directory feature(s)	
Authentication library • Azure AD Authentication Library (ADAL)	Azure Active Directory Authentication Library (ADAL) is deprecated. While existing apps that use ADAL continue to work, Microsoft no longer releases security fixes on ADAL. Migrate applications to the Microsoft Authentication Library (MSAL) to avoid putting your app's security at risk.
Authentication library • Microsoft Authentication Library (MSAL)	Microsoft Authentication Library (MSAL) - Provides security tokens from the Microsoft identity platform to authenticate users and access secured web APIs to provide secure access to Microsoft Graph, other Microsoft APIs, third-party web APIs, or your own web API.
B2C • Azure Active Directory B2C • Azure AD B2C	Azure Active Directory B2C isn't being renamed. We're continuing to invest in security, availability, and reliability in Azure AD B2C and our next-generation solution for external identities, Microsoft Entra External ID .
Graph • Azure Active Directory Graph	Azure Active Directory (Azure AD) Graph is deprecated. There are no further investments in Azure AD Graph and Azure AD Graph APIs have no SLA or maintenance commitment beyond security-related fixes. Investments in new features and functionalities will only be made in Microsoft Graph.

Correct terminology	Details
• Azure AD Graph • Microsoft Graph	Microsoft Graph - Grants programmatic access to organization, user, and application data stored in Microsoft Entra ID.
PowerShell • Azure Active Directory PowerShell • Azure AD PowerShell • Microsoft Graph PowerShell	Azure AD PowerShell for Graph is planned for deprecation on March 30, 2024. For more info on the deprecation plans, see the deprecation update. We encourage you to migrate to Microsoft Graph PowerShell, which is the recommended module for interacting with Azure AD. Microsoft Graph PowerShell - Acts as an API wrapper for the Microsoft Graph APIs and helps administer every Microsoft Entra ID feature that has an API in Microsoft Graph.
Accounts • Microsoft account • Work or school account	For end user sign-ins and account experiences, follow guidance for work and school accounts in Sign in with Microsoft branding guidelines .
Microsoft identity platform	The Microsoft identity platform encompasses all our identity and access developer assets. It continues to provide the resources to help you build applications that your users and customers can sign in to using their Microsoft identities or social accounts.
• Azure AD Sync • DirSync	DirSync and Azure AD Sync aren't supported and no longer work. If you're still using DirSync or Azure AD Sync, you must upgrade to Microsoft Entra Connect to resume your sync process. For more info, see Microsoft Entra Connect .

Frequently asked questions

When is the name change happening?

The name change across Microsoft experiences started on August 15, 2023. Display names for SKUs and service plans changed on October 1, 2023. Most naming text string changes in Microsoft experiences and partner experiences were completed at the end of 2023.

Why is the name being changed?

As part of our ongoing commitment to simplify secure access experiences for everyone, the renaming of Azure AD to Microsoft Entra ID is designed to make it easier to use and navigate the unified and expanded Microsoft Entra product family.

The Microsoft Entra ID name more accurately represents the multicloud and multiplatform functionality of the product, alleviates confusion with the on-premises identity solution (Active

Directory), and creates a path to deliver a simpler way to protect every identity and secure every access point as we expand the Microsoft Entra identity and network access portfolio.

What is Microsoft Entra?

The Microsoft Entra product family helps you protect all identities and secure network access everywhere. The expanded product family includes:

[+] [Expand table](#)

Identity and access management	New identity categories	Network access
Microsoft Entra ID (previously known as Azure AD)	Microsoft Entra Verified ID	Microsoft Entra Internet Access ↗
Microsoft Entra ID Governance		Microsoft Entra Private Access ↗
Microsoft Entra External ID	Microsoft Entra Workload ID	

Where can I manage Microsoft Entra ID?

You can manage Microsoft Entra ID and all other Microsoft Entra solutions in the [Microsoft Entra admin center](#) ↗ or the [Azure portal](#) ↗.

What are the display names for service plans and SKUs?

Licensing, pricing, and functionality aren't changing. Display names were updated October 1, 2023 as follows.

[+] [Expand table](#)

Old display name for service plan	New display name for service plan
Azure Active Directory Free	Microsoft Entra ID Free
Azure Active Directory Premium P1	Microsoft Entra ID P1
Azure Active Directory Premium P2	Microsoft Entra ID P2
Azure Active Directory for education	Microsoft Entra ID for education
Old display name for product SKU	New display name for product SKU

Old display name for service plan	New display name for service plan
Azure Active Directory Premium P1	Microsoft Entra ID P1
Azure Active Directory Premium P1 for students	Microsoft Entra ID P1 for students
Azure Active Directory Premium P1 for faculty	Microsoft Entra ID P1 for faculty
Azure Active Directory Premium P1 for government	Microsoft Entra ID P1 for government
Azure Active Directory Premium P2	Microsoft Entra ID P2
Azure Active Directory Premium P2 for students	Microsoft Entra ID P2 for students
Azure Active Directory Premium P2 for faculty	Microsoft Entra ID P2 for faculty
Azure Active Directory Premium P2 for government	Microsoft Entra ID P2 for government
Azure Active Directory F2	Microsoft Entra ID F2

Is Azure AD going away?

No, only the name Azure AD is going away. Capabilities remain the same.

Does Microsoft still support on-premises identity management?

We continue to support and enhance Windows Server Active Directory for on-premises identity and access management and the connection to Azure and other clouds, as many organizations continue to rely on this solution.

The name for Active Directory remains unchanged. Based on extensive feedback we received about Microsoft Entra ID as the new name for Azure Active Directory, for many customers the rename helps to better differentiate between the on-premises (Active Directory) and multicloud identity (Microsoft Entra ID) solutions.

What happens to the Azure AD capabilities and features like App Gallery or Conditional Access?

All features and capabilities remain unchanged aside from the name. Customers can continue to use all features without any interruption.

The naming of features changes to Microsoft Entra. For example:

- Azure AD tenant -> Microsoft Entra tenant

- Azure AD account -> Microsoft Entra account

For more examples, see the [glossary of updated terminology](#).

Are licenses changing? Are there any changes to pricing?

No. Prices, terms and service level agreements (SLAs) remain the same.

Is Microsoft Entra ID available as a free service with an Azure subscription?

Customers using Azure AD Free as part of their Azure, Microsoft 365, Dynamics 365, Teams, or Intune subscription continue to have access to the same capabilities. This is now called Microsoft Entra ID Free. Get the free version at <https://www.microsoft.com/security/business/microsoft-entra-pricing>.

What's changing for Microsoft 365 or Azure AD for Office 365?

Microsoft Entra ID – previously known as Azure AD – continues to be available within Microsoft 365 enterprise and business premium offers. Office 365 was renamed Microsoft 365 in 2022. Unique capabilities in the Azure AD for Office 365 apps (such as company branding and self-service sign-in activity search) are now available to all Microsoft customers in Microsoft Entra ID Free.

What's changing for Microsoft 365 E3?

There are no changes to the identity features and functionality available in Microsoft 365 E3. Microsoft 365 E3 includes Microsoft Entra ID P1, previously known as Azure AD Premium P1.

What's changing for Microsoft 365 E5?

In addition to the capabilities they already have, Microsoft 365 E5 customers also get access to new identity protection capabilities like token protection, Conditional Access based on GPS-based location and step-up authentication for the most sensitive actions. Microsoft 365 E5 includes Microsoft Entra ID P2, previously known as Azure AD Premium P2.

What's changing for identity developer and devops experiences?

Identity developer and devops experiences aren't being renamed. To make the transition seamless, all existing login URLs, APIs, PowerShell cmdlets, and Microsoft Authentication Libraries (MSAL) stay the same, as do developer experiences and tooling.

Many technical components either have low visibility to customers (for example, sign-in URLs), or usually aren't branded, like APIs.

Microsoft identity platform encompasses all our identity and access developer assets. It continues to provide the resources to help you build applications that your users and customers can sign in to using their Microsoft identities or social accounts.

For a detailed list of names that aren't changing, see [What names aren't changing?](#).

Are PowerShell cmdlets being renamed?

No. Today, we offer two PowerShell modules for administering identity tasks: the Azure AD PowerShell module, which is planned for deprecation in March 2024, and the Microsoft Graph PowerShell module.

In the Azure AD PowerShell for Graph module, `AzureAD` is in the name of almost all the cmdlets. These won't change, and you can continue to use these same cmdlets now that the official product name is Microsoft Entra ID.

Microsoft Graph PowerShell cmdlets aren't branded with Azure AD. We encourage you to plan your migration from Azure AD PowerShell to Microsoft Graph PowerShell, which is the recommended module for interacting with Microsoft Entra ID in the future.

How and when are customers being notified?

The name changes were publicly announced on July 11, 2023.

Banners, alerts, and message center posts notified users of the name change. The change was also displayed on the tenant overview page in the portals including Azure, Microsoft 365, and Microsoft Entra admin center, and Microsoft Learn.

What if I use the Azure AD name in my content or app?

We'd like your help spreading the word about the name change and implementing it in your own experiences. If you're a content creator, author of internal documentation for IT or identity security admins, developer of Azure AD–enabled apps, independent software vendor, or Microsoft partner, you can use the naming guidance outlined in [How to: Rename Azure AD](#) to make the name change in your content and product experiences.

Glossary of updated terminology

Features of the identity and network access products are attributed to Microsoft Entra—the product family, not the individual product name.

You're not required to use the Microsoft Entra attribution with features. Only use if needed to clarify whether you're talking about a concept versus the feature in a specific product, or when comparing a Microsoft Entra feature with a competing feature.

Only official product names are capitalized, plus Conditional Access and My * apps.

 Expand table

Category	Old terminology	Correct name as of July 2023
Microsoft Entra product family	Microsoft Azure Active Directory Azure Active Directory Azure Active Directory (Azure AD) Azure AD AAD	Microsoft Entra ID (Second use: Microsoft Entra ID is preferred, Entra ID should be used sparingly and only when space is truly limited) Acronym usage isn't encouraged, but if you must replace AAD with an acronym due to space limitations, use ME-ID.
	Azure Active Directory External Identities Azure AD External Identities	Microsoft Entra External ID (Second use: External ID)
	Azure Active Directory Identity Governance Azure AD Identity Governance Microsoft Entra Identity Governance	Microsoft Entra ID Governance (Second use: ID Governance)
	New	Microsoft Entra Internet Access (Second use: Internet Access)
	New	Microsoft Entra Private Access (Second use: Private Access)
	Azure Active Directory Verifiable Credentials Azure AD Verifiable Credentials	Microsoft Entra Verified ID (Second use: Verified ID)
	Azure Active Directory Workload Identities	Microsoft Entra Workload ID (Second use: Workload ID)

Category	Old terminology	Correct name as of July 2023
	Azure AD Workload Identities	
	Azure Active Directory Domain Services Azure AD Domain Services	Microsoft Entra Domain Services (Second use: Domain Services)
Microsoft Entra ID SKUs	Azure Active Directory Premium P1	Microsoft Entra ID P1
	Azure Active Directory Premium P1 for faculty	Microsoft Entra ID P1 for faculty
	Azure Active Directory Premium P1 for students	Microsoft Entra ID P1 for students
	Azure Active Directory Premium P1 for government	Microsoft Entra ID P1 for government
	Azure Active Directory Premium P2	Microsoft Entra ID P2
	Azure Active Directory Premium P2 for faculty	Microsoft Entra ID P2 for faculty
	Azure Active Directory Premium P2 for students	Microsoft Entra ID P2 for students
	Azure Active Directory Premium P2 for government	Microsoft Entra ID P2 for government
	Azure Active Directory Premium F2	Microsoft Entra ID F2
Microsoft Entra ID service plans	Azure Active Directory Free	Microsoft Entra ID Free
	Azure Active Directory Premium P1	Microsoft Entra ID P1
	Azure Active Directory Premium P2	Microsoft Entra ID P2
	Azure Active Directory for education	Microsoft Entra ID for education
Features and functionality	Azure AD access token authentication Azure Active Directory access token authentication	Microsoft Entra access token authentication

Category	Old terminology	Correct name as of July 2023
	Azure AD account Azure Active Directory account	Microsoft Entra account This terminology is only used with IT admins and developers. End users authenticate with a work or school account.
	Azure AD activity logs	Microsoft Entra activity logs
	Azure AD admin Azure Active Directory admin	Microsoft Entra admin
	Azure AD admin center Azure Active Directory admin center	Replace with Microsoft Entra admin center and update link to entra.microsoft.com
	Azure AD application proxy Azure Active Directory application proxy	Microsoft Entra application proxy
	Azure AD audit log	Microsoft Entra audit log
	Azure AD authentication authenticate with an Azure AD identity authenticate with Azure AD authentication to Azure AD	Microsoft Entra authentication authenticate with a Microsoft Entra identity authenticate with Microsoft Entra authentication to Microsoft Entra
	This terminology is only used with administrators. End users authenticate with a work or school account.	
	Azure AD B2B Azure Active Directory B2B	Microsoft Entra B2B
	Azure AD built-in roles Azure Active Directory built-in roles	Microsoft Entra built-in roles
	Azure AD Conditional Access Azure Active Directory Conditional Access	Microsoft Entra Conditional Access (Second use: Conditional Access)
	Azure AD cloud-only identities Azure Active Directory cloud-only identities	Microsoft Entra cloud-only identities
	Azure AD Connect Azure Active Directory Connect	Microsoft Entra Connect

Category	Old terminology	Correct name as of July 2023
	Azure AD Connect Sync Azure Active Directory Connect Sync	Microsoft Entra Connect Sync
	Azure AD connector Azure Active Directory connector	Microsoft Entra connector
	Azure AD domain Azure Active Directory domain	Microsoft Entra domain
	Azure AD Domain Services Azure Active Directory Domain Services	Microsoft Entra Domain Services
	Azure AD enterprise application Azure Active Directory enterprise application	Microsoft Entra enterprise application
	Azure AD federation services Azure Active Directory federation services	Active Directory Federation Services
	Azure AD groups Azure Active Directory groups	Microsoft Entra groups
	Azure AD hybrid identities Azure Active Directory hybrid identities	Microsoft Entra hybrid identities
	Azure AD identities Azure Active Directory identities	Microsoft Entra identities
	Azure AD identity protection Azure Active Directory identity protection	Microsoft Entra ID Protection
	Azure AD integrated authentication Azure Active Directory integrated authentication	Microsoft Entra integrated authentication
	Azure AD join Azure AD joined	Microsoft Entra join Microsoft Entra joined

Category	Old terminology	Correct name as of July 2023
	Azure Active Directory join Azure Active Directory joined	
	Azure AD license Azure Active Directory license	Microsoft Entra ID license or license for Microsoft Entra ID
	Azure AD login Azure Active Directory login	Microsoft Entra login
	Azure AD managed identities Azure Active Directory managed identities	Managed identities for Azure resources
	Azure AD multifactor authentication (MFA) Azure Active Directory multifactor authentication (MFA)	Microsoft Entra multifactor authentication (MFA) (Second use: MFA)
	Azure AD OAuth and OpenID Connect Azure Active Directory OAuth and OpenID Connect	Microsoft Entra ID OAuth and OpenID Connect
	Azure AD object Azure Active Directory object	Microsoft Entra object
	Azure Active Directory-only authentication Azure AD-only authentication	Microsoft Entra-only authentication
	Azure AD pass-through authentication (PTA) Azure Active Directory pass-through authentication (PTA)	Microsoft Entra pass-through authentication
	Azure AD password authentication Azure Active Directory password authentication	Microsoft Entra password authentication
	Azure AD password hash synchronization (PHS) Azure Active Directory password hash synchronization (PHS)	Microsoft Entra password hash synchronization

Category	Old terminology	Correct name as of July 2023
	Azure AD password protection Azure Active Directory password protection	Microsoft Entra password protection
	Azure AD Premium Azure Active Directory Premium	Microsoft Entra ID P1 or P2
	Azure AD principal ID Azure Active Directory principal ID	Microsoft Entra principal ID
	Azure AD Privileged Identity Management (PIM) Azure Active Directory Privileged Identity Management (PIM)	Microsoft Entra Privileged Identity Management (PIM)
	Azure AD registered Azure Active Directory registered	Microsoft Entra registered
	Azure AD reporting and monitoring Azure Active Directory reporting and monitoring	Microsoft Entra reporting and monitoring
	Azure AD role Azure Active Directory role	Microsoft Entra role
	Azure AD schema Azure Active Directory schema	Microsoft Entra schema
	Azure AD Seamless single sign-on (SSO) Azure Active Directory Seamless single sign-on (SSO)	Microsoft Entra seamless single sign-on (SSO) (Second use: SSO)
	Azure AD self-service password reset (SSPR) Azure Active Directory self-service password reset (SSPR)	Microsoft Entra self-service password reset (SSPR)
	Azure AD service principal Azure Active Directory	Microsoft Entra service principal

Category	Old terminology	Correct name as of July 2023
	service principal	
	Azure AD tenant Azure Active Directory tenant	Microsoft Entra tenant
	Create a user in Azure AD Create a user in Azure Active Directory	Create a user in Microsoft Entra
	Federated with Azure AD Federated with Azure Active Directory	Federated with Microsoft Entra
	Hybrid Azure AD Join Hybrid Azure AD Joined	Microsoft Entra hybrid join Microsoft Entra hybrid joined
	Managed identities in Azure AD for Azure SQL	Managed identities in Microsoft Entra for Azure SQL
Acronym usage	AAD	ME-ID Note that this isn't an official abbreviation for the product but may be used in code or when absolute shortest form is required.

Revision history

 Expand table

Date	Change description
March 5, 2024	Minor updates to statements that contained dates.
October 12, 2023	<ul style="list-style-type: none"> Updated statement about availability of license plans. Added three other terms in the glossary: "Azure AD connector", "Azure AD license", and "Azure AD Premium"
September 15, 2023	Added a link to the how-to article on renaming Azure AD, updated the description for Azure AD B2C, and added more info about why the name Azure AD is changing.
August 29, 2023	<ul style="list-style-type: none"> In the glossary, corrected the entry for "Azure AD activity logs" to separate "Azure AD audit log", which is a distinct type of activity log. Added Azure AD Sync and DirSync to the "What names aren't changing" section.

Date	Change description
August 18, 2023	<ul style="list-style-type: none">Updated the article to include a new section, "Glossary of updated terminology", which includes the old and new terminology.Updated info and added link to usage of the Microsoft Entra ID icon, and updates to verbiage in some sections.
July 11, 2023	Published the original guidance as part of the Microsoft Entra moment and related announcement .

Next steps

- [How to: Rename Azure AD](#)
- [Get started using Microsoft Entra ID at the Microsoft Entra admin center](#)
- [Learn more about the Microsoft Entra family with content from Microsoft Learn](#)

Microsoft Entra ID and data residency

Article • 01/09/2025

Microsoft Entra ID is an Identity as a Service (IDaaS) solution that stores and manages identity and access data in the cloud. You can use the data to enable and manage access to cloud services, achieve mobility scenarios, and secure your organization. An instance of the Microsoft Entra ID service, called a [tenant](#), is an isolated set of directory object data that the customer provisions and owns.

Note

Microsoft Entra External ID is a customer identity and access management (CIAM) solution that stores and manages data in a separate tenant created for your customer-facing apps and customer directory data. This tenant is called the external tenant. When you create an external tenant, you have the option to select the geographic location for data storage. It's important to note that the data locations and region availability may differ from those of Microsoft Entra ID, as indicated in this article.

Core Store

The Core Store is made up of tenants stored in scale units, each of which contains multiple tenants. Update or retrieval data operations in the Microsoft Entra Core Store relate to a single tenant, based on the user's security token, which achieves tenant isolation. Scale units are assigned to a geo-location. Each geo-location uses two or more Azure regions to store the data. In each Azure region, a scale unit data is replicated in the physical datacenters for resiliency and performance, as described in [the Microsoft Entra architecture](#).

For more information on the Core Store, see [Microsoft Entra Core Store Scale Units](#).
For more information on Azure regions, see [Azure geographies](#).

Microsoft Entra ID is available in the following clouds:

- Public
- China*
- US government*

* Not currently available for external tenants.

In the public cloud, you're prompted to select a location at the time of tenant creation (for example, signing up for Office 365 or Azure, or creating more Microsoft Entra instances through the Azure portal). Microsoft Entra ID maps the selection to a geo-location and a single scale unit in it. Tenant location can't be changed after it's set.

The location selected during tenant creation will map to one of the following geo-locations:

- Australia*
- Asia/Pacific
- Europe, Middle East, and Africa (EMEA)
- Japan*
- North America
- Worldwide

* Not currently available for external tenants.

Microsoft Entra ID handles Core Store data based on usability, performance, residency or other requirements based on geo-location. Microsoft Entra ID replicates each tenant through its scale unit, across datacenters, based on the following criteria:

- Microsoft Entra Core Store data, stored in datacenters closest to the tenant-residency location, to reduce latency and provide fast user sign-in times
- Microsoft Entra Core Store data stored in geographically isolated datacenters to assure availability during unforeseen single-datacenter, catastrophic events
- Compliance with data residency, or other requirements, for specific customers and geo-locations

Microsoft Entra cloud solution models

Use the following table to see Microsoft Entra cloud solution models based on infrastructure, data location, and operational sovereignty.

[+] Expand table

Model	Locations	Data location	Operations personnel	Put a tenant in this model
Public geo located	Australia (1), North America, EMEA, Japan (1), Asia/Pacific	At rest, in the target location. Exceptions by component service or feature, listed in the next section	Operated by Microsoft. Microsoft datacenter personnel must pass a background check.	Create the tenant in the sign-up experience. Choose the location for data residency.

Model	Locations	Data location	Operations personnel	Put a tenant in this model
Public worldwide	Worldwide	All locations	Operated by Microsoft. Microsoft datacenter personnel must pass a background check.	Tenant creation available via official support channel and subject to Microsoft discretion.
Sovereign or national clouds	US government (1), China (1)	At rest, in the target location. No exceptions.	Operated by a data custodian (2). Personnel are screened according to requirements.	Each national cloud instance has a sign-up experience.

Table references:

(1) These locations aren't currently available for external tenants. (2) **Data custodians:** datacenters in the US government cloud are operated by Microsoft. In China, Microsoft Entra ID is operated through a partnership with [21Vianet](#).

Learn more:

- Customer data storage and processing for European customers in Microsoft Entra ID
- Customer data storage for Australian and New Zealand customers in Microsoft Entra ID and Identity data storage for Australian and New Zealand customers in Microsoft Entra ID
- Customer data storage for Japan customers in Microsoft Entra ID
- Microsoft Trust Center - Where your data is located ↗

Data residency across Microsoft Entra components

Learn more: [Microsoft Entra product overview ↗](#)

ⓘ Note

To understand service data location for other services beyond Microsoft Entra ID, such as Exchange Online, or Skype for Business, refer to the corresponding service documentation and the [Trust Center](#) ↗.

Microsoft Entra components and data storage location

[+] Expand table

Microsoft Entra component	Description	Data storage location
Microsoft Entra authentication Service	<p>This service is stateless. The data for authentication is in the Microsoft Entra Core Store. It has no directory data. Microsoft Entra authentication Service generates log data in Azure Storage, and in the datacenter where the service instance runs. When users attempt to authenticate using Microsoft Entra ID, they're routed to an instance in the geographically nearest datacenter that is part of its Microsoft Entra logical region.</p>	In geo location
Microsoft Entra identity and Access Management (IAM) Services	<p>User and management experiences: The Microsoft Entra management experience is stateless and has no directory data. It generates log and usage data stored in Azure Tables storage. The user experience is like the Azure portal.</p> <p>Identity management business logic and reporting services: These services have locally cached data storage for groups and users. The services generate log and usage data that goes to Azure Tables storage, Azure SQL, and in Microsoft Elastic Search reporting services.</p>	In geo location
Microsoft Entra multifactor authentication	<p>For details about multifactor authentication-operations data storage and retention, see Data residency and customer data for Microsoft Entra multifactor authentication. Microsoft Entra multifactor authentication logs the User Principal Name (UPN), voice-call telephone numbers, and SMS challenges. For challenges to mobile app modes, the service logs the UPN and a unique device token.</p>	North America and/or in geo location
Microsoft Entra Domain Services	<p>See regions where Microsoft Entra Domain Services is published on Products available by region. The service holds system metadata globally in Azure Tables, and it contains no personal data.</p>	In geo location
Microsoft Entra Connect Health	<p>Microsoft Entra Connect Health generates alerts and reports in Azure Tables storage and blob storage.</p>	In geo location
Microsoft Entra dynamic membership groups, Microsoft Entra self-service group management	<p>Azure Tables storage holds rule definitions for dynamic membership groups.</p>	In geo location

Microsoft Entra component	Description	Data storage location
Microsoft Entra application proxy	Microsoft Entra application proxy stores metadata about the tenant, connector machines, and configuration data in Azure SQL.	In geo location
Microsoft Entra password writeback in Microsoft Entra Connect	<p>During initial configuration, Microsoft Entra Connect generates an asymmetric keypair, using the Rivest–Shamir–Adleman (RSA) cryptosystem. It then sends the public key to the self-service password reset (SSPR) cloud service, which performs two operations:</p> <ol style="list-style-type: none"> 1. Creates two Azure Service Bus relays for the Microsoft Entra Connect on-premises service to communicate securely with the SSPR service 2. Generates an Advanced Encryption Standard (AES) key, K1 <p>The Azure Service Bus relay locations, corresponding listener keys, and a copy of the AES key (K1) goes to Microsoft Entra Connect in the response. Future communications between SSPR and Microsoft Entra Connect occur over the new ServiceBus channel and are encrypted using SSL.</p> <p>New password resets, submitted during operation, are encrypted with the RSA public key generated by the client during onboarding. The private key on the Microsoft Entra Connect machine decrypts them, which prevents pipeline subsystems from accessing the plaintext password.</p> <p>The AES key encrypts the message payload (encrypted passwords, more data, and metadata), which prevents malicious ServiceBus attackers from tampering with the payload, even with full access to the internal ServiceBus channel.</p> <p>For password writeback, Microsoft Entra Connect need keys and data:</p> <ul style="list-style-type: none"> - The AES key (K1) that encrypts the reset payload, or change requests from the SSPR service to Microsoft Entra Connect, via the ServiceBus pipeline - The private key, from the asymmetric key pair that decrypts the passwords, in reset or change request payloads - The ServiceBus listener keys <p>The AES key (K1) and the asymmetric keypair rotate a minimum of every 180 days, a duration you can change during certain onboarding or offboarding configuration events. An example is a customer disables and reenables password writeback, which might occur during component upgrade during service and</p>	In geo location

Microsoft Entra component	Description	Data storage location
	<p>maintenance.</p> <p>The writeback keys and data stored in the Microsoft Entra Connect database are encrypted by data protection application programming interfaces (DPAPI) (CALG_AES_256). The result is the master ADSync encryption key stored in the Windows Credential Vault in the context of the ADSync on-premises service account. The Windows Credential Vault supplies automatic secret reencryption as the password for the service account changes. To reset the service account password invalidates secrets in the Windows Credential Vault for the service account. Manual changes to a new service account might invalidate the stored secrets.</p> <p>By default, the ADSync service runs in the context of a virtual service account. The account might be customized during installation to a least-privileged domain service account, a managed service account (Microsoft account), or a group managed service account (gMSA). While virtual and managed service accounts have automatic password rotation, customers manage password rotation for a custom provisioned domain account. As noted, to reset the password causes loss of stored secrets.</p>	
Microsoft Entra Device Registration Service	Microsoft Entra Device Registration Service has computer and device lifecycle management in the directory, which enable scenarios such as device-state Conditional Access, and mobile device management.	In geo location
Microsoft Entra provisioning	Microsoft Entra provisioning creates, removes, and updates users in systems, such as software as service (software as a service (SaaS)) applications. It manages user creation in Microsoft Entra ID and on-premises Microsoft Windows Server Active Directory from cloud HR sources, like Workday. The service stores its configuration in an Azure Cosmos DB instance, which stores the group membership data for the user directory it keeps. Azure Cosmos DB replicates the database to multiple datacenters in the same region as the tenant, which isolates the data, according to the Microsoft Entra cloud solution model. Replication creates high availability and multiple reading and writing endpoints. Azure Cosmos DB has encryption on the database information, and the encryption keys are stored in the secrets storage for Microsoft.	In geo location
Microsoft Entra business-to-business (B2B) collaboration	Microsoft Entra B2B collaboration has no directory data. Users and other directory objects in a B2B relationship, with another tenant, result in user data copied in other tenants, which might have data residency implications.	In geo location

Microsoft Entra component	Description	Data storage location
Microsoft Entra ID Protection	<p>Microsoft Entra ID Protection uses real-time user log-in data, with multiple signals from company and industry sources, to feed its machine-learning systems that detect anomalous logins. Personal data is scrubbed from real-time log-in data before it's passed to the machine learning system. The remaining log-in data identifies potentially risky usernames and logins. After analysis, the data goes to Microsoft reporting systems. Risky logins and usernames appear in reporting for Administrators.</p>	In geo location
Managed identities for Azure resources	<p>Managed identities for Azure resources with managed identities systems can authenticate to Azure services, without storing credentials. Rather than use username and password, managed identities authenticate to Azure services with certificates. The service writes certificates it issues in Azure Cosmos DB in the East US region, which fail over to another region, as needed. Azure Cosmos DB geo-redundancy occurs by global data replication. Database replication puts a read-only copy in each region that Microsoft Entra managed identities runs. To learn more, see Azure services that can use managed identities to access other services. Microsoft isolates each Azure Cosmos DB instance in a Microsoft Entra cloud solution model.</p> <p>The resource provider, such as the virtual machine (VM) host, stores the certificate for authentication, and identity flows, with other Azure services. The service stores its master key to access Azure Cosmos DB in a datacenter secrets management service. Azure Key Vault stores the master encryption keys.</p>	In geo location

Related resources

For more information on data residency in Microsoft Cloud offerings, see the following articles:

- [Data Residency in Azure | Microsoft Azure](#)
- [Microsoft 365 data locations - Microsoft 365 Enterprise](#)
- [Microsoft Privacy - Where is Your Data Located?](#)
- Download PDF: [Privacy considerations in the cloud](#)

Next steps

- [Microsoft Entra ID and data residency \(You're here\)](#)

- Data operational considerations
 - Data protection considerations
-

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

Data operational considerations

Article • 10/23/2023

In this article, learn about data operational considerations for your configuration. There's information about how log files and other features work in relation to Microsoft Entra ID, such as usage data and operator security. You'll learn about physical security considerations in addition to guidance on how the Microsoft Entra team defines deployments and change.

Log files

Microsoft Entra ID generates log files for auditing, investigation, and debugging for actions and events in the service. Log files might contain data about users, devices, and Microsoft Entra configuration, for instance policies, apps, and groups. Log files are created and stored in Azure Storage in the datacenter where the Microsoft Entra service runs.

Log files are used for local debugging, security, usage analysis, system-health monitoring, and service-wide analysis. These logs are copied over a Transport Layer Security (TLS) connection to Microsoft reporting machine learning systems, which are in Microsoft-owned datacenters in the continental United States.

Usage data

Usage data is metadata generated by the Microsoft Entra service that indicates how the service is being used. This metadata is used to generate administrator- and user-facing reports. The Microsoft Entra engineering team uses the metadata to evaluate system usage and identify opportunities to improve the service. Generally, this data is written to log files, but in some cases, is collected by our service monitoring and reporting systems.

Operator security

Access to Microsoft Entra ID by Microsoft personnel, contractors, and vendors (system admins) is highly restricted. Wherever possible, human intervention is replaced by an automated, tool-based process, including routine functions such as deployment, debugging, diagnostic collection, and restarting services.

Administrator access is limited to a subset of qualified engineers and requires completion of an authentication challenge with phishing-resistant credentials. System access and update functions are assigned to roles managed by the Microsoft just-in-time (JIT) privileged-access management system. System administrators request elevation using the JIT system, which routes the request for manual or automated approval. Upon approval, JIT elevates the account. Requests for elevation, approval, elevation into roles, and removal from roles are logged for future debugging or investigations.

Microsoft personnel can execute operations only from a secure access workstation, which uses an internal isolated strong authentication identity platform. Access to other Microsoft identity systems doesn't grant access to the security access workstation. The identity platform runs separately from other Microsoft identity systems.

Physical security

Physical access to servers that comprise the Microsoft Entra service, and access to Microsoft Entra back-end systems, is restricted by Azure facility, premises, and physical security. Microsoft Entra customers have no access to physical assets or locations, therefore they can't bypass the logical role-based access control (RBAC) policy checks. Personnel with operator access are authorized to run approved workflows for maintenance.

Learn more: [Azure facilities, premises, and physical security](#)

Change control process

To roll out changes to the service across datacenters, the Microsoft Entra team defines the layers of a deployment environment. Applying the change layers is constrained by strict exit criteria. The amount of time to roll a change across layers is defined by the operations team and is based on potential effects. Typically a rollout takes between 1 to 2 weeks. Critical changes, such as security fixes or hot fixes, can be deployed faster. If a change doesn't meet the exit criteria when applied to a deployment layer, it's rolled back to the prior, stable state.

Resources

- [Microsoft Service Trust Documents](#) ↗
- [Microsoft Azure Trusted Cloud](#) ↗
- [Office 365 datacenters](#) ↗

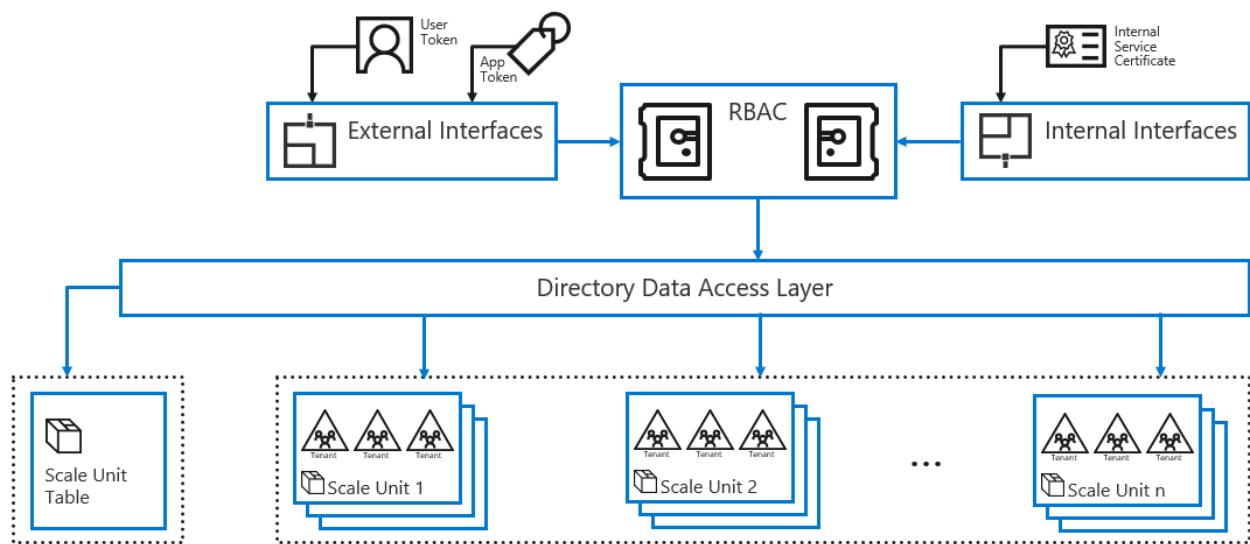
Next steps

- Microsoft Entra ID and data residency
- Data operational considerations (You're here)
- Data protection considerations

Data protection considerations

Article • 10/23/2023

The following diagram illustrates how services store and retrieve Microsoft Entra object data through a role-based access control (RBAC) authorization layer. This layer calls the internal directory data access layer, ensuring the user's data request is permitted:



Microsoft Entra Internal Interfaces Access: Service-to-service communication with other Microsoft services, such as Microsoft 365 use Microsoft Entra ID interfaces, which authorize the service's callers using client certificates.

Microsoft Entra External Interfaces Access: Microsoft Entra external interface helps prevent data leakage by using RBAC. When a security principal, such as a user, makes an access request to read information through Microsoft Entra ID interfaces, a security token must accompany the request. The token contains claims about the principal making the request.

The security tokens are issued by the Microsoft Entra authentication Services. Information about the user's existence, enabled state, and role is used by the authorization system to decide whether the requested access to the target tenant is authorized for this user in this session.

Application Access: Because applications can access the Application Programming Interfaces (APIs) without user context, the access check includes information about the user's application and the scope of access requested, for example read only, read/write, and so on. Many applications use OpenID Connect or Open Authorization (OAuth) to obtain tokens to access the directory on behalf of the user. These applications must be explicitly granted access to the directory or they won't receive a token from Microsoft Entra authentication Service, and they access data from the granted scope.

Auditing: Access is audited. For example, authorized actions such as create user and password reset create an audit trail that can be used by a tenant administrator to manage compliance efforts or investigations. Tenant administrators can generate audit reports by using the Microsoft Entra audit API.

Learn more: [Audit logs in Microsoft Entra ID](#)

Tenant Isolation: Enforcement of security in Microsoft Entra multitenant environment helps achieve two primary goals:

- Prevent data leakage and access across tenants: Data belonging to Tenant 1 can't be obtained by users in Tenant 2 without explicit authorization by Tenant 1.
- Resource access isolation across tenants: Operations performed by Tenant 1 can't affect access to resources for Tenant 2.

Tenant isolation

The following information outlines tenant isolation.

- The service secures tenants using RBAC policy to ensure data isolation.
- To enable access to a tenant, a principal, for example a user or application, needs to be able to authenticate against Microsoft Entra ID to obtain context and has explicit permissions defined in the tenant. If a principal isn't authorized in the tenant, the resulting token won't carry permissions, and the RBAC system rejects requests in this context.
- RBAC ensures access to a tenant is performed by a security principal authorized in the tenant. Access across tenants is possible when a tenant administrator creates a security principal representation in the same tenant (for example, provisioning a guest user account using B2B collaboration), or when a tenant administrator creates a policy to enable a trust relationship with another tenant. For example, a cross-tenant access policy to enable B2B Direct Connect. Each tenant is an isolation boundary; existence in one tenant doesn't equate existence in another tenant unless the administrator allows it.
- Microsoft Entra data for multiple tenants is stored in the same physical server and drive for a given partition. Isolation is ensured because access to the data is protected by the RBAC authorization system.
- A customer application can't access Microsoft Entra ID without needed authentication. The request is rejected if not accompanied by credentials as part of the initial connection negotiation process. This dynamic prevents unauthorized access to a tenant by neighboring tenants. Only user credential's token, or Security Assertion Markup Language (SAML) token, is brokered with a federated trust.

Therefore, it's validated by Microsoft Entra ID, based on the shared keys configured by the application owner.

- Because there's no application component that can execute from the Core Store, it's not possible for one tenant to forcibly breach the integrity of a neighboring tenant.

Data security

Encryption in Transit: To assure data security, directory data in Microsoft Entra ID is signed and encrypted while in transit between datacenters in a scale unit. The data is encrypted and unencrypted by the Microsoft Entra Core Store tier, which resides in secured server hosting areas of the associated Microsoft datacenters.

Customer-facing web services are secured with the Transport Layer Security (TLS) protocol.

Secret Storage: Microsoft Entra service back-end uses encryption to store sensitive material for service use, such as certificates, keys, credentials, and hashes using Microsoft proprietary technology. The store used depends on the service, the operation, the scope of the secret (user-wide or tenant-wide), and other requirements.

These stores are operated by a security-focused group via established automation and workflows, including certificate request, renewal, revocation, and destruction.

There's activity auditing related to these stores/workflows/processes, and there is no standing access. Access is request- and approval-based, and for a limited amount of time.

For more information about Secret encryption at rest, see the following table.

Algorithms: The following table lists the minimum cryptography algorithms used by Microsoft Entra components. As a cloud service, Microsoft reassesses and improves the cryptography, based on security research findings, internal security reviews, key strength against hardware evolution, and so on.

[Expand table](#)

Data/scenario	Cryptography algorithm
Password hash sync	Hash: Password Key Derivation Function 2 (PBKDF2), using hash-based message authentication code (HMAC)-SHA256 @ 1,000 iterations
Cloud account passwords	Hash: Password Key Derivation Function 2 (PBKDF2), using hash-based message authentication code (HMAC)-SHA256 @ 1,000 iterations

Data/scenario	Cryptography algorithm
Directory in transit between datacenters	AES-256-CTS-HMAC-SHA1-96 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
Pass-through authentication user credential flow	RSA 2048-Public/Private key pair Learn more: Microsoft Entra pass-through authentication security deep dive
Self-service password reset password writeback with Microsoft Entra Connect: Cloud to on-premises communication	RSA 2048 Private/Public key pair AES_GCM (256-bits key, 96-bits IV size)
Self-service password reset: Answers to security questions	SHA256
SSL certificates for Microsoft Entra application Proxy published applications	AES-GCM 256-bit
Disk-level encryption	XTS-AES 128
Seamless single sign-on (SSO) service account password software as a service (SaaS) application provisioning credentials	AES-CBC 128-bit
Managed identities for Azure resources	AES-GCM 256-bit
Microsoft Authenticator app: Passwordless sign-in to Microsoft Entra ID	Asymmetric RSA Key 2048-bit
Microsoft Authenticator app: Backup and restore of enterprise account metadata	AES-256

Resources

- [Microsoft Service Trust Documents ↗](#)
- [Microsoft Azure Trust Center ↗](#)
- [Recover from deletions in Microsoft Entra ID](#)

Next steps

- Microsoft Entra ID and data residency
- Data operational considerations
- Data protection considerations (You're here)

Customer data storage and processing for European customers in Microsoft Entra ID

Article • 01/07/2025

Microsoft Entra ID stores customer data in a geographic location based on how a tenant was created and provisioned. The following list provides information about how the location is defined:

- **Microsoft Entra admin center or Microsoft Entra API** - A customer selects a location from the predefined list.
- **Dynamics 365 and Power Platform** - A customer provisions their tenant in a predefined location.
- **EU Data Residency** - For customers who provided a location in Europe, Microsoft Entra ID stores most of the customer data in Europe, except where noted later in this article.
- **EU Data Boundary** - For customers who provided a location that is within the [EU Data Boundary](#) (members of the EU and EFTA), Microsoft Entra ID stores and processes most of the customer data in the EU Data Boundary, except where noted later in this article.
- **Microsoft 365** - The location is based on a customer provided billing address.

The following sections provide information about customer data that doesn't meet the EU Data Residency or EU Data Boundary commitments.

Services that will temporarily transfer a subset of customer data out of the EU Data Residency and EU Data Boundary

For some components of a service, work is in progress to be included in the EU Data Residency and EU Data Boundary, but completion of this work is delayed. The following sections in this article explain the customer data that these services currently transfer out of Europe as part of their service operations.

EU Data Residency:

- **Reason for customer data egress** - A few of the tenants are stored outside of the EU location due one of the following reasons:

- The tenants were initially created with a country code that is NOT in Europe and later the tenant country code was changed to the one in Europe. The Microsoft Entra directory data location is decided during the tenant creation time and not changed when the country code for the tenant is updated. Starting March 2019, Microsoft has blocked updating the country code on a tenant to avoid such confusion.
 - There are 13 country codes (Countries include: Azerbaijan, Bahrain, Israel, Jordan, Kazakhstan, Kuwait, Lebanon, Oman, Pakistan, Qatar, Saudi Arabia, Türkiye, UAE) that were mapped to Asia region until 2013 and later mapped to Europe. Tenants that were created before July 2013 from this country code are provisioned in Asia instead of Europe.
 - There are seven country codes (Countries include: Armenia, Georgia, Iraq, Kyrgyzstan, Tajikistan, Turkmenistan, Uzbekistan) that were mapped to Asia region until 2017 and later mapped to Europe. Tenants that were created before February 2017 from this country code are provisioned in Asia instead of Europe.
- **Types of customer data being egressed** - User and device account data, and service configuration (application, policy, and group).
 - **Customer data location at rest** - US and Asia/Pacific.
 - **Customer data processing** - The same as the location at rest.
 - **Services** - Directory Core Store

EU Data Boundary:

See more information on Microsoft Entra temporary partial customer data transfers from the EU Data Boundary [Services that temporarily transfer a subset of customer data out of the EU Data Boundary](#).

Services that will permanently transfer a subset of customer data out of the EU Data Residency and EU Data Boundary

Some components of a service will continue to transfer a limited amount of customer data out of the EU Data Residency and EU Data Boundary because this transfer is by design to facilitate the function of the services.

EU Data Residency:

Microsoft Entra ID: When an IP Address or phone number is determined to be used in fraudulent activities, they're published globally to block access from any workloads using them.

EU Data Boundary:

See more information on Microsoft Entra permanent partial customer data transfers from the [EU Data Boundary Services that will permanently transfer a subset of customer data out of the EU Data Boundary](#).

Other considerations

Optional service capabilities that transfer data out of the EU Data Residency and EU Data Boundary

EU Data Residency:

Some services offer optional features. In some cases, you need a subscription to use them. As a customer administrator, you can choose to turn these features on or off for your service accounts. If made available and used by a customer's users, these capabilities will result in data transfers out of Europe as described in the following sections in this article.

- **Multitenant administration:** An organization might choose to create a multitenant organization within Microsoft Entra ID. For example, a customer can invite users to their tenant in a B2B context. A customer can create a multitenant software as a service (SaaS) application that allows other third-party tenants to provision the application in the third-party tenant. A customer can link two or more tenants to work together as one in certain situations. These include forming a multitenant organization (MTO), syncing tenants, and sharing an email domain. Administrator configuration and use of multitenant collaboration might occur with tenants outside of the EU Data Residency and EU Data Boundary resulting in some customer data, such as user and device account data, usage data, and service configuration (application, policy, and group) being stored and processed in the location of the collaborating tenant.
- **Application Proxy:** Application proxy allows customers to access both cloud and on-premises applications through an external URL or an internal application portal. Customers might choose advanced routing configurations that would cause Customer Data to egress outside of the EU Data Residency and EU Data Boundary, including user account data, usage data, and application configuration data.

EU Data Boundary:

See more information on optional service capabilities that transfer customer data out of the EU Data Boundary [Optional service capabilities that transfer customer data out of the EU Data Boundary](#).

Other EU Data Boundary online services

Services and applications that integrate with Microsoft Entra ID have access to customer data. Review how each service and application stores and processes customer data, and verify that they meet your company's data handling requirements.

Next steps

For more information about Microsoft services' data residency, see the **Where your data is located** section of the [Microsoft Trust Center](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)

Identity data storage for Australian and New Zealand customers in Microsoft Entra ID

Article • 03/05/2025

Microsoft Entra ID stores identity data in a location chosen based on the address provided by your organization when subscribing to a Microsoft service like Microsoft 365 or Azure. For information on where your Identity Customer Data is stored, you can review the Microsoft Trust center section titled [Where is your data located?](#).

ⓘ Note

Services and applications that integrate with Microsoft Entra ID have access to Identity Customer Data. Evaluate each service and application you use. Determine how that specific service and application process identity data, and whether they meet your company's data storage requirements.

For customers who provided an address in Australia or New Zealand, Microsoft Entra ID keeps identity data for these services within Australian datacenters:

- Microsoft Entra Directory Management
- Authentication

All other Microsoft Entra services store customer data in global datacenters.

Microsoft Entra multifactor authentication

Multifactor authentication stores Identity Customer Data in global datacenters. To learn more about the user information collected and stored by cloud-based Microsoft Entra multifactor authentication and Azure multifactor authentication Server, see [Microsoft Entra multifactor authentication user data collection](#).

Next steps

For more information about Multifactor authentication, see these articles:

- [What is multifactor authentication?](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Customer Data storage for Australian and New Zealand customers in Microsoft Entra ID

Article • 03/05/2025

Microsoft Entra ID stores identity data in a location chosen based on the address provided by your organization when subscribing to a Microsoft service like Microsoft 365 or Azure. Microsoft Online services include Microsoft 365 and Azure.

For information about where Microsoft Entra ID and other Microsoft services' data is located, see the [Where your data is located](#) section of the Microsoft Trust Center.

From February 26, 2020, Microsoft began storing Microsoft Entra ID's Customer Data for new tenants with an Australian or New Zealand billing address within the Australian datacenters.

Additionally, certain Microsoft Entra features don't yet support storage of Customer Data in Australia. Go to the [Microsoft global datacenters map](#) for information specific to your region. For example, Microsoft Entra multifactor authentication stores Customer Data in the US and processes it globally. For more information, see [Data residency and customer data for Microsoft Entra multifactor authentication](#).

Note

Microsoft products, services, and third-party applications that integrate with Microsoft Entra ID have access to Customer Data. Evaluate each product, service, and application you use to determine how Customer Data is processed by that specific product, service, and application, and whether they meet your company's data storage requirements. For more information about Microsoft services' data residency, see the [Where your data is located](#) section of the Microsoft Trust Center.

Azure role-based access control (Azure RBAC)

Role definitions, role assignments, and deny assignments are stored globally to ensure that you have access to your resources regardless of the region you created the resource. For more information, see [What is Azure role-based access control \(RBAC\)?](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Customer data storage for Japan customers in Microsoft Entra ID

Article • 11/25/2024

Microsoft Entra ID stores its Customer Data in a geographical location based on the country/region you provided when you signed up for a Microsoft Online service. Microsoft Online services include Microsoft 365 and Azure.

For information about where Microsoft Entra ID and other Microsoft services' data is located, see the [Where your data is located](#) section of the Microsoft Trust Center.

Additionally, certain Microsoft Entra features do not yet support storage of Customer Data in Japan. For example, Microsoft Entra multifactor authentication stores Customer Data in the US and processes it globally. For more information, see [Data residency and customer data for Microsoft Entra multifactor authentication](#).

ⓘ Note

Microsoft products, services, and third-party applications that integrate with Microsoft Entra ID have access to Customer Data. Evaluate each product, service, and application you use to determine how Customer Data is processed by that specific product, service, and application, and whether they meet your company's data storage requirements. For more information about Microsoft services' data residency, see the [Where your data is located](#) section of the Microsoft Trust Center.

Azure role-based access control (Azure RBAC)

Role definitions, role assignments, and deny assignments are stored globally to ensure that you have access to your resources regardless of the region you created the resource. For more information, see [What is Azure role-based access control \(RBAC\) \(Azure RBAC\)?](#).

Feedback

Was this page helpful?



Yes



No

Provide product feedback ↗

Compare Active Directory to Microsoft Entra ID

Article • 03/08/2024

Microsoft Entra ID is the next evolution of identity and access management solutions for the cloud. Microsoft introduced Active Directory Domain Services in Windows 2000 to give organizations the ability to manage multiple on-premises infrastructure components and systems using a single identity per user.

Microsoft Entra ID takes this approach to the next level by providing organizations with an Identity as a Service (IDaaS) solution for all their apps across cloud and on-premises.

Most IT administrators are familiar with Active Directory Domain Services concepts. The following table outlines the differences and similarities between Active Directory concepts and Microsoft Entra ID.

[+] Expand table

Concept	Windows Server Active Directory	Microsoft Entra ID
Users		
Provisioning: users	Organizations create internal users manually or use an in-house or automated provisioning system, such as the Microsoft Identity Manager, to integrate with an HR system.	Existing Microsoft Windows Server Active Directory organizations use Microsoft Entra Connect to sync identities to the cloud. Microsoft Entra ID adds support to automatically create users from cloud HR systems . Microsoft Entra ID can provision identities in System for Cross-Domain Identity Management (SCIM) enabled software as a service (SaaS) apps to automatically provide apps with the necessary details to allow access for users.
Provisioning: external identities	Organizations create external users manually as regular users in a dedicated external Microsoft Windows Server Active Directory forest, resulting in administration overhead to manage the lifecycle of external identities (guest users)	Microsoft Entra ID provides a special class of identity to support external identities. Microsoft Entra B2B will manage the link to the external user identity to make sure they are valid.

Concept	Windows Server Active Directory	Microsoft Entra ID
Entitlement management and groups	Administrators make users members of groups. App and resource owners then give groups access to apps or resources.	<p>Groups are also available in Microsoft Entra ID and administrators can also use groups to grant permissions to resources. In Microsoft Entra ID, administrators can assign membership to groups manually or use a query to dynamically include users to a group.</p> <p>Administrators can use Entitlement management in Microsoft Entra ID to give users access to a collection of apps and resources using workflows and, if necessary, time-based criteria.</p>
Admin management	Organizations will use a combination of domains, organizational units, and groups in Microsoft Windows Server Active Directory to delegate administrative rights to manage the directory and resources it controls.	<p>Microsoft Entra ID provides built-in roles with its Microsoft Entra role-based access control (RBAC) system, with limited support for creating custom roles to delegate privileged access to the identity system, the apps, and resources it controls.</p> <p>Managing roles can be enhanced with Privileged Identity Management (PIM) to provide just-in-time, time-restricted, or workflow-based access to privileged roles.</p>
Credential management	<p>Credentials in Active Directory are based on passwords, certificate authentication, and smart card authentication.</p> <p>Passwords are managed using password policies that are based on password length, expiry, and complexity.</p>	<p>Microsoft Entra ID uses intelligent password protection for cloud and on-premises. Protection includes smart lockout plus blocking common and custom password phrases and substitutions.</p> <p>Microsoft Entra ID significantly boosts security through multifactor authentication and passwordless technologies, like FIDO2.</p> <p>Microsoft Entra ID reduces support costs by providing users a self-service password reset system.</p>
Apps		
Infrastructure apps	Active Directory forms the basis for many infrastructure on-premises components, for example, DNS, Dynamic Host Configuration Protocol (DHCP), Internet Protocol Security (IPSec), WiFi, NPS, and VPN access	In a new cloud world, Microsoft Entra ID, is the new control plane for accessing apps versus relying on networking controls. When users authenticate, Conditional Access controls which users have access to which apps under required conditions.

Concept	Windows Server Active Directory	Microsoft Entra ID
Traditional and legacy apps	Most on-premises apps use LDAP, Windows-Integrated Authentication (NTLM and Kerberos), or Header-based authentication to control access to users.	Microsoft Entra ID can provide access to these types of on-premises apps using Microsoft Entra application proxy agents running on-premises. Using this method Microsoft Entra ID can authenticate Active Directory users on-premises using Kerberos while you migrate or need to coexist with legacy apps.
SaaS apps	Active Directory doesn't support SaaS apps natively and requires federation system, such as AD FS.	SaaS apps supporting OAuth2, Security Assertion Markup Language (SAML), and WS-* authentication can be integrated to use Microsoft Entra ID for authentication.
Line of business (LOB) apps with modern authentication	Organizations can use AD FS with Active Directory to support LOB apps requiring modern authentication.	LOB apps requiring modern authentication can be configured to use Microsoft Entra ID for authentication.
Mid-tier/Daemon services	Services running in on-premises environments normally use Microsoft Windows Server Active Directory service accounts or group Managed Service Accounts (gMSA) to run. These apps will then inherit the permissions of the service account.	Microsoft Entra ID provides managed identities to run other workloads in the cloud. The lifecycle of these identities is managed by Microsoft Entra ID and is tied to the resource provider and it can't be used for other purposes to gain backdoor access.
Devices		
Mobile	Active Directory doesn't natively support mobile devices without third-party solutions.	Microsoft's mobile device management solution, Microsoft Intune, is integrated with Microsoft Entra ID. Microsoft Intune provides device state information to the identity system to evaluate during authentication.
Windows desktops	Active Directory provides the ability to domain join Windows devices to manage them using Group Policy, System Center Configuration Manager, or other third-party solutions.	Windows devices can be joined to Microsoft Entra ID . Conditional Access can check if a device is Microsoft Entra joined as part of the authentication process. Windows devices can also be managed with Microsoft Intune . In this case, Conditional Access, will consider whether a device is compliant (for example, up-to-

Concept	Windows Server Active Directory	Microsoft Entra ID
		date security patches and virus signatures) before allowing access to the apps.
Windows servers	Active Directory provides strong management capabilities for on-premises Windows servers using Group Policy or other management solutions.	Windows servers virtual machines in Azure can be managed with Microsoft Entra Domain Services . Managed identities can be used when VMs need access to the identity system directory or resources.
Linux/Unix workloads	Active Directory doesn't natively support non-Windows without third-party solutions, although Linux machines can be configured to authenticate with Active Directory as a Kerberos realm.	Linux/Unix VMs can use managed identities to access the identity system or resources. Some organizations, migrate these workloads to cloud container technologies, which can also use managed identities.

Next steps

- [What is Microsoft Entra ID?](#)
- [Compare self-managed Active Directory Domain Services, Microsoft Entra ID, and managed Microsoft Entra Domain Services](#)
- [Frequently asked questions about Microsoft Entra ID](#)
- [What's new in Microsoft Entra ID?](#)

What are custom security attributes in Microsoft Entra ID?

Article • 10/28/2024

Custom security attributes in Microsoft Entra ID are business-specific attributes (key-value pairs) that you can define and assign to Microsoft Entra objects. These attributes can be used to store information, categorize objects, or enforce fine-grained access control over specific Azure resources. Custom security attributes can be used with [Azure attribute-based access control \(ABAC\)](#).

Why use custom security attributes?

Here are some scenarios where you could use custom security attributes:

- Extend user profiles, such as add Hourly Salary to all my employees.
- Ensure only administrators can see the Hourly Salary attribute in my employees' profiles.
- Categorize hundreds or thousands of applications to easily create a filterable inventory for auditing.
- Grant users access to the Azure Storage blobs belonging to a project.

What can I do with custom security attributes?

Custom security attributes include these capabilities:

- Define business-specific information (attributes) for your tenant.
- Add a set of custom security attributes on users and applications.
- Manage Microsoft Entra objects using custom security attributes with queries and filters.
- Provide attribute governance so attributes determine who can get access.

Custom security attributes aren't supported in the following areas:

- [Microsoft Entra Domain Services](#)
- [Security Assertion Markup Language \(SAML\) token claims](#)

Features of custom security attributes

Custom security attributes include these features:

- Available tenant-wide
- Include a description
- Support different data types: Boolean, integer, string
- Support single value or multiple values
- Support user-defined free-form values or predefined values
- Assign custom security attributes to directory synced users from an on-premises Active Directory

The following example shows several custom security attributes assigned to a user. The custom security attributes are different data types and have values that are single, multiple, free-form, or predefined.

Attribute set	Attribute name	Attribute description	Data type	Multi-valued	Assigned values
Engineering	Certification	Certification status	Boolean	No	true
Engineering	CostCenter	Project cost center	Integer	Yes	2 values
Engineering	Project	Active projects for user	String	Yes	2 values
Engineering	NumVendors	Number of vendors	Integer	No	8
Marketing	EmployeeId	Employee identification	String	No	GS45897
Engineering	ProjectDate	Target completion dat...	String	No	2023-11-15

Objects that support custom security attributes

You can add custom security attributes for the following Microsoft Entra objects:

- Microsoft Entra users
- Microsoft Entra enterprise applications (service principals)

How do custom security attributes compare with extensions?

While both extensions and custom security attributes can be used to extend objects in Microsoft Entra ID and Microsoft 365, they are suitable for fundamentally different custom data scenarios. Here are some ways that custom security attributes compare with [extensions](#):

[] Expand table

Capability	Extensions	Custom security attributes
Extend Microsoft Entra ID and Microsoft 365 objects	Yes	Yes
Supported objects	Depends on the extension type	Users and service principals
Restricted access	No. Anyone with permissions to read the object can read the extension data.	Yes. Read and write access is restricted through a separate set of permissions and role-based access control (RBAC).
When to use	Store data to be used by an application Store non-sensitive data	Store sensitive data Use for authorization scenarios
License requirements	Available in all editions of Microsoft Entra ID	Available in all editions of Microsoft Entra ID

For more information about working with extensions, see [Add custom data to resources using extensions](#).

Steps to use custom security attributes

1. Check permissions

Check that you are assigned the [Attribute Definition Administrator](#) or [Attribute Assignment Administrator](#) roles. If necessary, someone with at least the [Privileged Role Administrator](#) role can assign these roles.



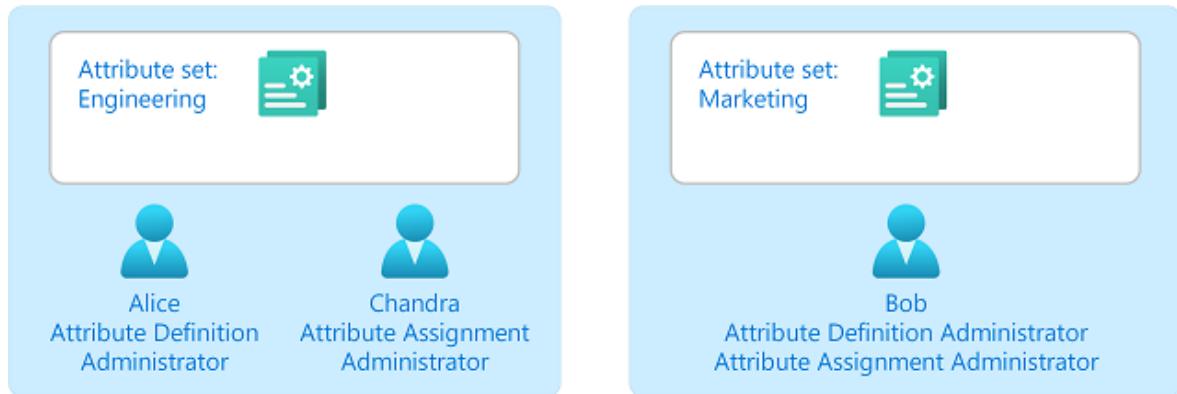
2. Add attribute sets

Add attribute sets to group and manage related custom security attributes. [Learn more](#)



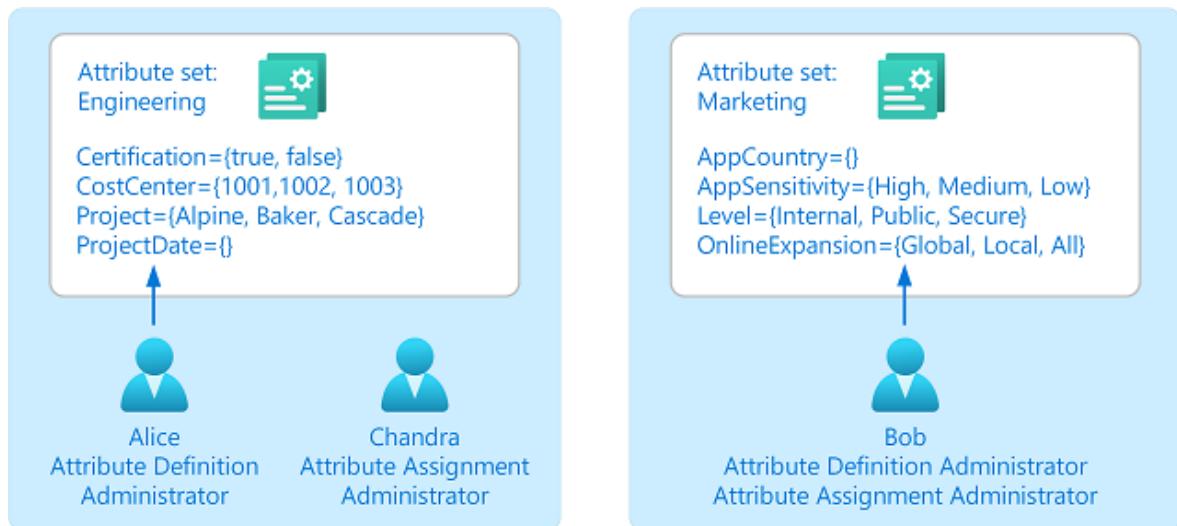
3. Manage attribute sets

Specify who can read, define, or assign custom security attributes in an attribute set. [Learn more](#)



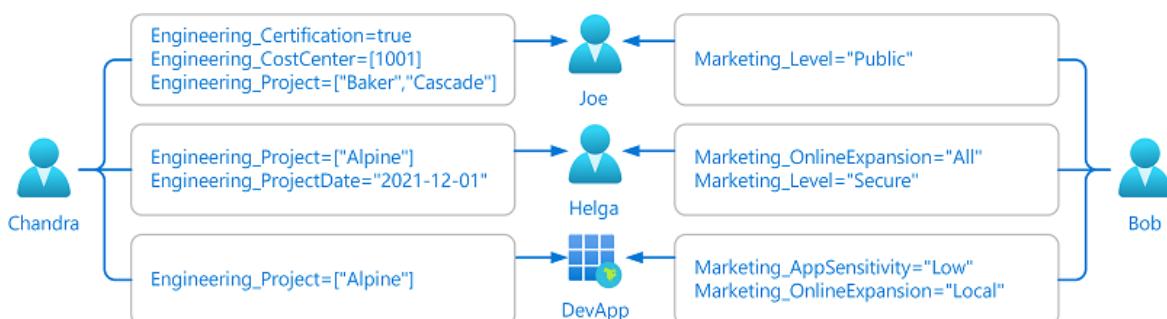
4. Define attributes

Add your custom security attributes to your directory. You can specify the date type (Boolean, integer, or string) and whether values are predefined, free-form, single, or multiple. [Learn more](#)



5. Assign attributes

Assign custom security attributes to Microsoft Entra objects for your business scenarios. [Learn more](#)



6. Use attributes

Filter users and applications that use custom security attributes. [Learn more](#)

Add conditions that use custom security attributes to Azure role assignments for fine-grained access control. [Learn more](#)

Terminology

To better understand custom security attributes, you can refer back to the following list of terms.

[+] [Expand table](#)

Term	Definition
attribute definition	The schema of a custom security attribute or key-value pair. For example, the custom security attribute name, description, data type, and predefined values.
attribute set	A collection of related custom security attributes. Attribute sets can be delegated to other users for defining and assigning custom security attributes.
attribute name	A unique name of a custom security attribute within an attribute set. The combination of attribute set and attribute name forms a unique attribute for your tenant.
attribute assignment	The assignment of a custom security attribute to a Microsoft Entra object, such as users and enterprise applications (service principals).
predefined value	A value that is allowed for a custom security attribute.

Custom security attribute properties

The following table lists the properties you can specify for attribute sets and custom security attributes. Some properties are immutable and cannot be changed later.

[+] [Expand table](#)

Property	Required	Can be changed later	Description
Attribute set name	<input checked="" type="checkbox"/>		Name of the attribute set. Must be unique within a tenant. Cannot include spaces or special characters.

Property	Required	Can be changed later	Description
Attribute set description	<input checked="" type="checkbox"/>		Description of the attribute set.
Maximum number of attributes	<input checked="" type="checkbox"/>		Maximum number of custom security attributes that can be defined in an attribute set. Default value is <code>null</code> . If not specified, the administrator can add up to the maximum of 500 active attributes per tenant.
Attribute set	<input checked="" type="checkbox"/>		A collection of related custom security attributes. Every custom security attribute must be part of an attribute set.
Attribute name	<input checked="" type="checkbox"/>		Name of the custom security attribute. Must be unique within an attribute set. Cannot include spaces or special characters.
Attribute description	<input checked="" type="checkbox"/>		Description of the custom security attribute.
Data type	<input checked="" type="checkbox"/>		Data type for the custom security attribute values. Supported types are <code>Boolean</code> , <code>Integer</code> , and <code>String</code> .
Allow multiple values to be assigned	<input checked="" type="checkbox"/>		Indicates whether multiple values can be assigned to the custom security attribute. If data type is set to <code>Boolean</code> , cannot be set to Yes.
Only allow predefined values to be assigned	<input checked="" type="checkbox"/>		Indicates whether only predefined values can be assigned to the custom security attribute. If set to No, free-form values are allowed. Can later be changed from Yes to No, but cannot be changed from No to Yes. If data type is set to <code>Boolean</code> , cannot be set to Yes.
Predefined values			Predefined values for the custom security attribute of the selected data type. More predefined values can be added later. Values can include spaces, but some special characters are not allowed.
Predefined value is active	<input checked="" type="checkbox"/>		Specifies whether the predefined value is active or deactivated. If set to false, the predefined value cannot be assigned to any additional supported directory objects.
Attribute is active	<input checked="" type="checkbox"/>		Specifies whether the custom security attribute is active or deactivated.

Limits and constraints

Here are some of the limits and constraints for custom security attributes.

[Expand table](#)

Resource	Limit	Notes
Attribute definitions per tenant	500	Applies only to active attributes in the tenant
Attribute sets per tenant	500	
Attribute set name length	32	Unicode characters and case sensitive
Attribute set description length	128	Unicode characters
Attribute name length	32	Unicode characters and case sensitive
Attribute description length	128	Unicode characters
Predefined values		Unicode characters and case sensitive
Predefined values per attribute definition	100	
Attribute value length	64	Unicode characters
Attribute values assigned per object	50	Values can be distributed across single and multivalued attributes. Example: 5 attributes with 10 values each or 50 attributes with 1 value each
Special characters not allowed for: Attribute set name Attribute name	<space> ` ~ ! @ # \$ % ^ & * () _ - + = { [}] \ \ : ; " ' < , > . ? /	Attribute set name and attribute name cannot start with a number
Special characters allowed for attribute values	All special characters	
Special characters allowed for attribute values when used with blob index tags	<space> + - . : = _ /	If you plan to use attribute values with blob index tags , these are the only special characters allowed for blob

Resource	Limit	Notes
		index tags. For more information, see Setting blob index tags .

Custom security attribute roles

Microsoft Entra ID provides built-in roles to work with custom security attributes. The Attribute Definition Administrator role is the minimum role you need to manage custom security attributes. The Attribute Assignment Administrator role is the minimum role you need to assign custom security attribute values for Microsoft Entra objects like users and applications. You can assign these roles at tenant scope or at attribute set scope.

[] [Expand table](#)

Role	Permissions
Attribute Definition Reader	Read attribute sets Read custom security attribute definitions
Attribute Definition Administrator	Manage all aspects of attribute sets Manage all aspects of custom security attribute definitions
Attribute Assignment Reader	Read attribute sets Read custom security attribute definitions Read custom security attribute keys and values for users and service principals
Attribute Assignment Administrator	Read attribute sets Read custom security attribute definitions Read and update custom security attribute keys and values for users and service principals
Attribute Log Reader	Read audit logs for custom security attributes
Attribute Log Administrator	Read audit logs for custom security attributes Configure diagnostic settings for custom security attributes

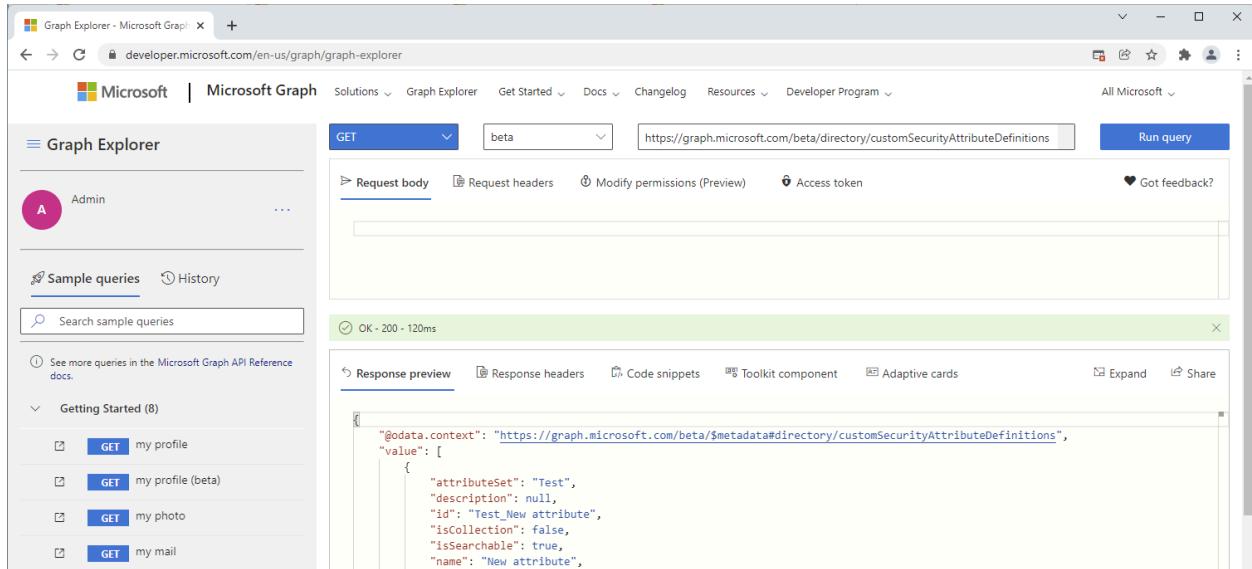
ⓘ Important

By default, [Global Administrator](#) and other administrator roles do not have permissions to read, define, or assign custom security attributes.

Microsoft Graph API

You can manage custom security attributes programmatically using Microsoft Graph API. For more information, see [Overview of custom security attributes using the Microsoft Graph API](#).

You can use an API client such as [Graph Explorer](#) to more easily try the Microsoft Graph API for custom security attributes.



License requirements

Using this feature is free and included in your Azure subscription.

Next steps

- Add or deactivate custom security attribute definitions in Microsoft Entra ID
- Manage access to custom security attributes in Microsoft Entra ID
- Assign, update, list, or remove custom security attributes for a user
- Provision custom security attributes from HR sources (preview)

Feedback

Was this page helpful?

Yes

No

Provide product feedback ↗

Add or deactivate custom security attribute definitions in Microsoft Entra ID

Article • 11/27/2024

Custom security attributes in Microsoft Entra ID are business-specific attributes (key-value pairs) that you can define and assign to Microsoft Entra objects. This article describes how to add, edit, or deactivate custom security attribute definitions.

Prerequisites

To add or deactivate custom security attributes definitions, you must have:

- [Attribute Definition Administrator](#)
- Microsoft.Graph module when using [Microsoft Graph PowerShell](#)
- [AzureADPreview](#) version 2.0.2.138 or later when using Azure AD PowerShell

Important

By default, [Global Administrator](#) and other administrator roles do not have permissions to read, define, or assign custom security attributes.

Add an attribute set

An attribute set is a collection of related attributes. All custom security attributes must be part of an attribute set. Attribute sets cannot be renamed or deleted.

1. Sign in to the [Microsoft Entra admin center](#) as a [Attribute Definition Administrator](#).

2. Browse to **Protection > Custom security attributes**.

3. Select **Add attribute set** to add a new attribute set.

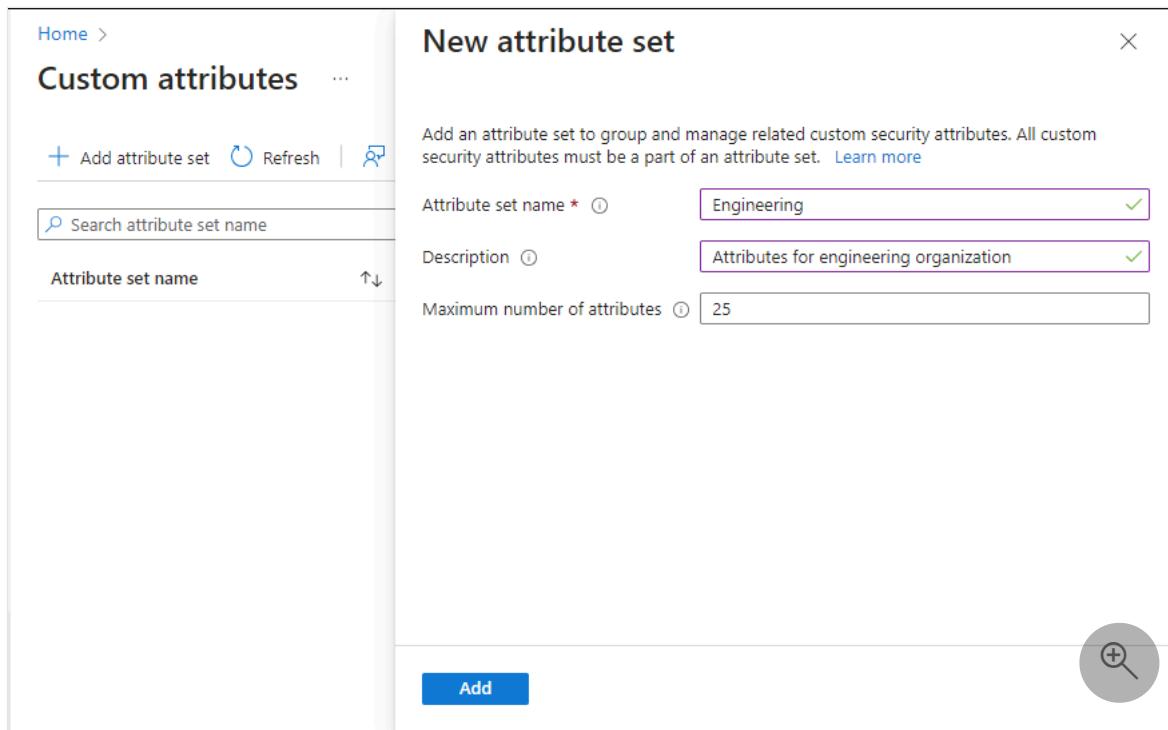
If Add attribute set is disabled, make sure you are assigned the Attribute Definition Administrator role. For more information, see [Troubleshoot custom security attributes](#).

4. Enter a name, description, and maximum number of attributes.

An attribute set name can be 32 characters with no spaces or special characters.

Once you've specified a name, you can't rename it. For more information, see

[Limits and constraints](#).



5. When finished, select Add.

The new attribute set appears in the list of attribute sets.

Add a custom security attribute definition

1. Sign in to the Microsoft Entra admin center [as a Attribute Definition Administrator](#).
2. Browse to **Protection > Custom security attributes**.
3. On the Custom security attributes page, find an existing attribute set or select **Add attribute set** to add a new attribute set.

All custom security attribute definitions must be part of an attribute set.
4. Select to open the selected attribute set.
5. Select **Add attribute** to add a new custom security attribute to the attribute set.

New attribute ...



Add a custom security attribute (key-value pair) to your directory that you can later assign to Microsoft Entra objects, such as users or applications. [Learn more](#)

Attribute name *	<input type="text"/>						
Description	<input type="text"/>						
Data type *	<input type="button" value="String"/>						
Allow multiple values to be assigned	<input type="radio"/> Yes <input checked="" type="radio"/> No						
Only allow predefined values to be assigned	<input type="radio"/> Yes <input checked="" type="radio"/> No						
Predefined values	<input type="button" value="Add value"/> <table border="0"> <tr> <td><input type="button" value="Value"/></td> <td><input type="button" value="↑↓"/></td> <td><input type="button" value="Is active?"/></td> </tr> <tr> <td colspan="3">No results</td> </tr> </table>	<input type="button" value="Value"/>	<input type="button" value="↑↓"/>	<input type="button" value="Is active?"/>	No results		
<input type="button" value="Value"/>	<input type="button" value="↑↓"/>	<input type="button" value="Is active?"/>					
No results							



6. In the **Attribute name** box, enter a custom security attribute name.

A custom security attribute name can be 32 characters with no spaces or special characters. Once you've specified a name, you can't rename it. For more information, see [Limits and constraints](#).

7. In the **Description** box, enter an optional description.

A description can be 128 characters long. If necessary, you can later change the description.

8. From the **Data type** list, select the data type for the custom security attribute.

[\[\] Expand table](#)

Data type	Description
Boolean	A Boolean value that can be true, True, false, or False.
Integer	A 32-bit integer.
String	A string that can be X characters long.

9. For **Allow multiple values to be assigned**, select **Yes** or **No**.

Select **Yes** to allow multiple values to be assigned to this custom security attribute. Select **No** to only allow a single value to be assigned to this custom security attribute.

10. For **Only allow predefined values to be assigned**, select **Yes** or **No**.

Select **Yes** to require that this custom security attribute be assigned values from a predefined values list. Select **No** to allow this custom security attribute to be assigned user-defined values or potentially predefined values.

11. If **Only allow predefined values to be assigned** is **Yes**, select **Add value** to add predefined values.

An active value is available for assignment to objects. A value that is not active is defined, but not yet available for assignment.

The screenshot shows the Microsoft Entra admin center interface. On the left, under 'New attribute', the following fields are filled:

- Attribute name: Project
- Description: Active projects for user
- Data type: String
- Allow multiple values to be assigned: Yes
- Only allow predefined values to be assigned: Yes
- Predefined values: + Add value (button)

A modal window titled 'Add predefined value' is open on the right, containing the following fields:

- Value: Baker
- Is active?: checked

At the bottom of the modal are 'Save' and 'Add' buttons, along with a magnifying glass icon.

12. When finished, select **Save**.

The new custom security attribute appears in the list of custom security attributes.

13. If you want to include predefined values, follow the steps in the next section.

Edit a custom security attribute definition

Once you add a new custom security attribute definition, you can later edit some of the properties. Some properties are immutable and cannot be changed.

1. Sign in to the [Microsoft Entra admin center](#) as a **Attribute Definition Administrator**.
2. Browse to **Protection > Custom security attributes**.
3. Select the attribute set that includes the custom security attribute you want to edit.

4. In the list of custom security attributes, select the ellipsis for the custom security attribute you want to edit, and then select **Edit attribute**.
5. Edit the properties that are enabled.
6. If **Only allow predefined values to be assigned** is **Yes**, select **Add value** to add predefined values. Select an existing predefined value to change the **Is active?** setting.

The screenshot shows the Microsoft Entra admin center interface. On the left, under 'Project', there's a form for defining a custom security attribute. It includes fields for 'Attribute name' (Project), 'Description' (Active projects for user), 'Data type' (String), 'Allow multiple values to be assigned' (Yes selected), 'Only allow predefined values to be assigned' (Yes selected), and a table for 'Predefined values'. The table has one row with 'Value' (Baker) and 'Is active?' (checkbox checked). On the right, a modal window titled 'Add predefined value' is open, asking to add a single predefined value of the selected data type. It shows a 'Value' field with 'Alpine' and an 'Is active?' checkbox which is checked.

Deactivate a custom security attribute definition

Once you add a custom security attribute definition, you can't delete it. However, you can deactivate a custom security attribute definition.

1. Sign in to the [Microsoft Entra admin center](#) as a [Attribute Definition Administrator](#).
2. Browse to **Protection > Custom security attributes**.
3. Select the attribute set that includes the custom security attribute you want to deactivate.
4. In the list of custom security attributes, add a check mark next to the custom security attribute you want to deactivate.
5. Select **Deactivate attribute**.
6. In the Deactivate attribute dialog that appears, select **Yes**.

The custom security attribute is deactivated and moved to the Deactivated attributes list.

PowerShell or Microsoft Graph API

To manage custom security attribute definitions in your Microsoft Entra organization, you can also use PowerShell or Microsoft Graph API. The following examples manage attribute sets and custom security attribute definitions.

Get all attribute sets

The following example gets all attribute sets.

```
PowerShell

Get-MgDirectoryAttributeSet

PowerShell

Get-MgDirectoryAttributeSet | Format-List

Output

Description      : Attributes for engineering team
Id              : Engineering
MaxAttributesPerSet : 25
AdditionalProperties : {}

Description      : Attributes for marketing team
Id              : Marketing
MaxAttributesPerSet : 25
AdditionalProperties : {}
```

Get top attribute sets

The following example gets the top attribute sets.

```
PowerShell

Get-MgDirectoryAttributeSet

PowerShell
```

```
Get-MgDirectoryAttributeSet -Top 10
```

Get attribute sets in order

The following example gets attribute sets in order.

PowerShell

```
Get-MgDirectoryAttributeSet
```

PowerShell

```
Get-MgDirectoryAttributeSet -Sort "Id"
```

Get an attribute set

The following example gets an attribute set.

- Attribute set: Engineering

PowerShell

```
Get-MgDirectoryAttributeSet
```

PowerShell

```
Get-MgDirectoryAttributeSet -AttributeSetId "Engineering" | Format-List
```

Output

```
Description      : Attributes for engineering team
Id            : Engineering
MaxAttributesPerSet : 25
AdditionalProperties : {[@odata.context,
https://graph.microsoft.com/v1.0/$metadata#directory/attributeSets/$entity]}
```

Add an attribute set

The following example adds a new attribute set.

- Attribute set: `Engineering`

PowerShell

New-MgDirectoryAttributeSet

PowerShell

```
$params = @{
    Id = "Engineering"
    Description = "Attributes for engineering team"
    MaxAttributesPerSet = 25
}
New-MgDirectoryAttributeSet -BodyParameter $params
```

Output

Id	Description	MaxAttributesPerSet
--	-----	-----
Engineering	Attributes for engineering team	25

Update an attribute set

The following example updates an attribute set.

- Attribute set: `Engineering`

PowerShell

Update-MgDirectoryAttributeSet

PowerShell

```
$params = @{
    description = "Attributes for engineering team"
    maxAttributesPerSet = 20
}
Update-MgDirectoryAttributeSet -AttributeSetId "Engineering" -
    BodyParameter $params
```

Get all custom security attribute definitions

The following example gets all custom security attribute definitions.

PowerShell

Get-MgDirectoryCustomSecurityAttributeDefinition

PowerShell

```
Get-MgDirectoryCustomSecurityAttributeDefinition | Format-List
```

Output

```
AllowedValues          :  
AttributeSet          : Engineering  
Description           : Target completion date  
Id                   : Engineering_ProjectDate  
IsCollection         : False  
IsSearchable          : True  
Name                 : ProjectDate  
Status               : Available  
Type                 : String  
UsePreDefinedValuesOnly : False  
AdditionalProperties   : {}  
  
AllowedValues          :  
AttributeSet          : Engineering  
Description           : Active projects for user  
Id                   : Engineering_Project  
IsCollection         : True  
IsSearchable          : True  
Name                 : Project  
Status               : Available  
Type                 : String  
UsePreDefinedValuesOnly : True  
AdditionalProperties   : {}  
  
AllowedValues          :  
AttributeSet          : Marketing  
Description           : Country where is application is used  
Id                   : Marketing_AppCountry  
IsCollection         : True  
IsSearchable          : True  
Name                 : AppCountry  
Status               : Available  
Type                 : String  
UsePreDefinedValuesOnly : True  
AdditionalProperties   : {}
```

Filter custom security attribute definitions

The following examples filter custom security attribute definitions.

- Filter: Attribute name eq 'Project' and status eq 'Available'

PowerShell

[Get-MgDirectoryCustomSecurityAttributeDefinition](#)

PowerShell

```
Get-MgDirectoryCustomSecurityAttributeDefinition -Filter "name eq  
'Project' and status eq 'Available'" | Format-List
```

Output

```
AllowedValues      :  
AttributeSet       : Engineering  
Description        : Active projects for user  
Id                : Engineering_Project  
IsCollection      : True  
IsSearchable       : True  
Name              : Project  
Status             : Available  
Type               : String  
UsePreDefinedValuesOnly : True  
AdditionalProperties   : {}
```

- Filter: Attribute set eq 'Engineering' and status eq 'Available' and data type eq 'String'

PowerShell

[Get-MgDirectoryCustomSecurityAttributeDefinition](#)

PowerShell

```
Get-MgDirectoryCustomSecurityAttributeDefinition -Filter "attributeSet  
eq 'Engineering' and status eq 'Available' and type eq 'String'" |  
Format-List
```

Output

```
AllowedValues      :  
AttributeSet       : Engineering
```

```

Description          : Target completion date
Id                  : Engineering_ProjectDate
IsCollection       : False
IsSearchable        : True
Name                : ProjectDate
Status              : Available
Type                : String
UsePreDefinedValuesOnly : False
AdditionalProperties : {}

AllowedValues      :
AttributeSet       : Engineering
Description         : Active projects for user
Id                  : Engineering_Project
IsCollection       : True
IsSearchable        : True
Name                : Project
Status              : Available
Type                : String
UsePreDefinedValuesOnly : True
AdditionalProperties : {}

```

Get a custom security attribute definition

The following example gets a custom security attribute definition.

- Attribute set: `Engineering`
- Attribute: `ProjectDate`

PowerShell

[Get-MgDirectoryCustomSecurityAttributeDefinition](#)

PowerShell

```
Get-MgDirectoryCustomSecurityAttributeDefinition -  
CustomSecurityAttributeDefinitionId "Engineering_ProjectDate" | Format-  
List
```

Output

```

AllowedValues      :
AttributeSet       : Engineering
Description         : Target completion date
Id                  : Engineering_ProjectDate
IsCollection       : False
IsSearchable        : True
Name                : ProjectDate

```

```
Status          : Available
Type           : String
UsePreDefinedValuesOnly : False
AdditionalProperties   : {[@odata.context,
https://graph.microsoft.com/v1.0/$metadata#directory/customSecurityAttributeDefinitions/$entity]}
```

Add a custom security attribute definition

The following example adds a new custom security attribute definition.

- Attribute set: `Engineering`
- Attribute: `ProjectDate`
- Attribute data type: String

PowerShell

[New-MgDirectoryCustomSecurityAttributeDefinition](#)

PowerShell

```
$params = @{
    attributeSet = "Engineering"
    description = "Target completion date"
    isCollection = $false
    isSearchable = $true
    name = "ProjectDate"
    status = "Available"
    type = "String"
    usePreDefinedValuesOnly = $false
}
New-MgDirectoryCustomSecurityAttributeDefinition -BodyParameter $params
| Format-List
```

Output

```
AllowedValues      :
AttributeSet       : Engineering
Description        : Target completion date
Id                : Engineering_ProjectDate
IsCollection      : False
IsSearchable       : True
Name              : ProjectDate
Status            : Available
Type              : String
UsePreDefinedValuesOnly : False
AdditionalProperties : {[@odata.context,
```

```
https://graph.microsoft.com/v1.0/$metadata#directory/customSecurityAttributeDefinitions/$entity]}
```

Add a custom security attribute definition that supports multiple predefined values

The following example adds a new custom security attribute definition that supports multiple predefined values.

- Attribute set: `Engineering`
- Attribute: `Project`
- Attribute data type: Collection of Strings

PowerShell

New-MgDirectoryCustomSecurityAttributeDefinition

PowerShell

```
$params = @{
    attributeSet = "Engineering"
    description = "Active projects for user"
    isCollection = $true
    isSearchable = $true
    name = "Project"
    status = "Available"
    type = "String"
    usePreDefinedValuesOnly = $true
}
New-MgDirectoryCustomSecurityAttributeDefinition -BodyParameter $params
| Format-List
```

Output

```
AllowedValues          :
AttributeSet           : Engineering
Description            : Active projects for user
Id                    : Engineering_Project
IsCollection          : True
IsSearchable           : True
Name                  : Project
Status                : Available
Type                  : String
UsePreDefinedValuesOnly : True
AdditionalProperties   : {[@odata.context,
```

```
https://graph.microsoft.com/v1.0/$metadata#directory/customSecurityAttributeDefinitions/$entity]}
```

Add a custom security attribute definition with a list of predefined values

The following example adds a new custom security attribute definition with a list of predefined values.

- Attribute set: `Engineering`
- Attribute: `Project`
- Attribute data type: Collection of Strings
- Predefined values: `Alpine`, `Baker`, `Cascade`

PowerShell

New-MgDirectoryCustomSecurityAttributeDefinition

PowerShell

```
$params = @{
    attributeSet = "Engineering"
    description = "Active projects for user"
    isCollection = $true
    isSearchable = $true
    name = "Project"
    status = "Available"
    type = "String"
    usePreDefinedValuesOnly = $true
    allowedValues = @(
        @{
            id = "Alpine"
            isActive = $true
        }
        @{
            id = "Baker"
            isActive = $true
        }
        @{
            id = "Cascade"
            isActive = $true
        }
    )
}
New-MgDirectoryCustomSecurityAttributeDefinition -BodyParameter $params
| Format-List
```

Output

```
AllowedValues          : 
AttributeSet          : Engineering
Description           : Active projects for user
Id                   : Engineering_Project
IsCollection         : True
IsSearchable          : True
Name                 : Project
Status               : Available
Type                 : String
UsePreDefinedValuesOnly : True
AdditionalProperties   : {[@odata.context,
https://graph.microsoft.com/v1.0/$metadata#directory/customSecurityAttributeDefinitions/$entity]}
```

Update a custom security attribute definition

The following example updates a custom security attribute definition.

- Attribute set: `Engineering`
- Attribute: `ProjectDate`

PowerShell

[Update-MgDirectoryCustomSecurityAttributeDefinition](#)

PowerShell

```
$params = @{
    description = "Target completion date (YYYY/MM/DD)"
}
Update-MgDirectoryCustomSecurityAttributeDefinition - 
CustomSecurityAttributeDefinitionId "Engineering_ProjectDate" - 
BodyParameter $params
```

Update the predefined values for a custom security attribute definition

The following example updates the predefined values for a custom security attribute definition.

- Attribute set: `Engineering`
- Attribute: `Project`

- Attribute data type: Collection of Strings
- Update predefined value: `Baker`
- New predefined value: `Skagit`

PowerShell

Invoke-MgGraphRequest

ⓘ Note

For this request, you must add the **OData-Version** header and assign it the value `4.01`.

PowerShell

```
$params = @{
    "allowedValues@delta" = @(
        @{
            id = "Baker"
            isActive = $false
        }
        @{
            id = "Skagit"
            isActive = $true
        }
    )
}
$header = @{
    "OData-Version" = 4.01
}
Invoke-MgGraphRequest -Method PATCH -Uri
"https://graph.microsoft.com/v1.0/directory/customSecurityAttributeDefinitions/Engineering_Project5" -Headers $header -Body $params
```

Deactivate a custom security attribute definition

The following example deactivates a custom security attribute definition.

- Attribute set: `Engineering`
- Attribute: `Project`

PowerShell

Update-MgDirectoryCustomSecurityAttributeDefinition

PowerShell

```
$params = @{
    status = "Deprecated"
}
Update-MgDirectoryCustomSecurityAttributeDefinition -  
CustomSecurityAttributeDefinitionId "Engineering_ProjectDate" -  
BodyParameter $params
```

Get all predefined values

The following example gets all predefined values for a custom security attribute definition.

- Attribute set: `Engineering`
- Attribute: `Project`

PowerShell

[Get-MgDirectoryCustomSecurityAttributeDefinitionAllowedValue](#)

PowerShell

```
Get-MgDirectoryCustomSecurityAttributeDefinitionAllowedValue -  
CustomSecurityAttributeDefinitionId "Engineering_Project" | Format-List
```

Output

```
Id : Skagit
IsActive : True
AdditionalProperties : {}

Id : Baker
IsActive : False
AdditionalProperties : {}

Id : Cascade
IsActive : True
AdditionalProperties : {}

Id : Alpine
IsActive : True
AdditionalProperties : {}
```

Get a predefined value

The following example gets a predefined value for a custom security attribute definition.

- Attribute set: `Engineering`
- Attribute: `Project`
- Predefined value: `Alpine`

PowerShell

[Get-MgDirectoryCustomSecurityAttributeDefinitionAllowedValue](#)

PowerShell

```
Get-MgDirectoryCustomSecurityAttributeDefinitionAllowedValue -  
CustomSecurityAttributeDefinitionId "Engineering_Project" -  
AllowedValueId "Alpine" | Format-List
```

Output

```
Id : Alpine  
IsActive : True  
AdditionalProperties : {[@odata.context,  
https://graph.microsoft.com/v1.0/$metadata#directory/customSecurityAttri  
buteDefinitions('Engineering_Project')/al  
lowedValues/$entity]}
```

Add a predefined value

The following example adds a predefined value for a custom security attribute definition.

You can add predefined values for custom security attributes that have

`usePreDefinedValuesOnly` set to `true`.

- Attribute set: `Engineering`
- Attribute: `Project`
- Predefined value: `Alpine`

PowerShell

[New-MgDirectoryCustomSecurityAttributeDefinitionAllowedValue](#)

PowerShell

```
$params = @{
    id = "Alpine"
    isActive = $true
}
New-MgDirectoryCustomSecurityAttributeDefinitionAllowedValue -  
CustomSecurityAttributeDefinitionId "Engineering_Project" -BodyParameter  
$params | Format-List
```

Output

```
Id : Alpine
IsActive : True
AdditionalProperties : {[@odata.context,
https://graph.microsoft.com/v1.0/$metadata#directory/customSecurityAttributeDefinitions('Engineering_Project')/allowedValues/$entity]}
```

Deactivate a predefined value

The following example deactivates a predefined value for a custom security attribute definition.

- Attribute set: `Engineering`
- Attribute: `Project`
- Predefined value: `Alpine`

PowerShell

[Update-MgDirectoryCustomSecurityAttributeDefinitionAllowedValue](#)

PowerShell

```
$params = @{
    isActive = $false
}
Update-MgDirectoryCustomSecurityAttributeDefinitionAllowedValue -  
CustomSecurityAttributeDefinitionId "Engineering_Project" -  
AllowedValueId "Alpine" -BodyParameter $params
```

Frequently asked questions

Can you delete custom security attribute definitions?

No, you can't delete custom security attribute definitions. You can only [deactivate custom security attribute definitions](#). Once you deactivate a custom security attribute, it can no longer be applied to the Microsoft Entra objects. Custom security attribute assignments for the deactivated custom security attribute definition are not automatically removed. There is no limit to the number of deactivated custom security attributes. You can have 500 active custom security attribute definitions per tenant with 100 allowed predefined values per custom security attribute definition.

Next steps

- [Manage access to custom security attributes in Microsoft Entra ID](#)
 - [Assign, update, list, or remove custom security attributes for a user](#)
 - [Assign, update, list, or remove custom security attributes for an application](#)
-

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#) ↗

Manage access to custom security attributes in Microsoft Entra ID

Article • 03/30/2025

For people in your organization to effectively work with [custom security attributes](#), you must grant the appropriate access. Depending on the information you plan to include in custom security attributes, you might want to restrict custom security attributes or you might want to make them broadly accessible in your organization. This article describes how to manage access to custom security attributes.

Prerequisites

To manage access to custom security attributes, you must have:

- [Attribute Assignment Administrator](#)
- Microsoft.Graph module when using [Microsoft Graph PowerShell](#)

Important

By default, [Global Administrator](#) and other administrator roles do not have permissions to read, define, or assign custom security attributes.

Step 1: Determine how to organize your attributes

Every custom security attribute definition must be part of an attribute set. An attribute set is a way to group and manage related custom security attributes. You'll need to determine how you want to add attributes sets for your organization. For example, you might want to add attribute sets based on departments, teams, or projects. Your ability to grant access to custom security attributes depends on how you organize your attribute sets.

Attribute set:
Engineering



Certification={true, false}
CostCenter={1001,1002, 1003}
Project={Alpine, Baker, Cascade}
ProjectDate={}

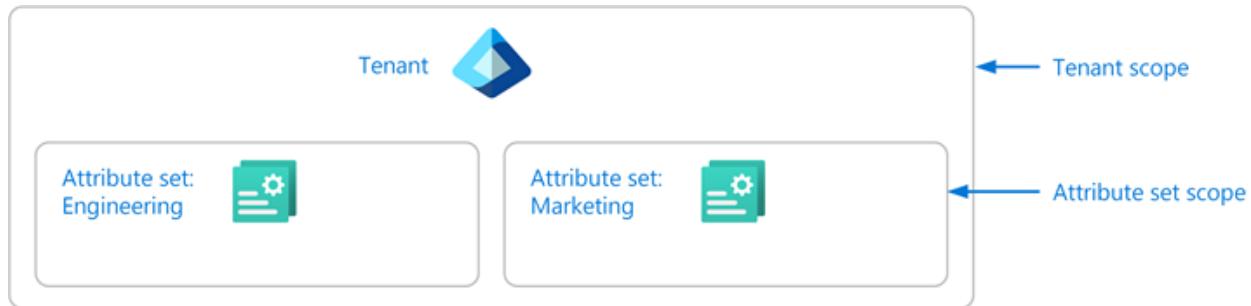
Attribute set:
Marketing



AppCountry={}
AppSensitivity={High, Medium, Low}
Level={Internal, Public, Secure}
OnlineExpansion={Global, Local, All}

Step 2: Identify the needed scope

Scope is the set of resources that the access applies to. For custom security attributes, you can assign roles at tenant scope or at attribute set scope. If you want to assign broad access, you can assign roles at tenant scope. However, if you want to limit access to particular attribute sets, you can assign roles at attribute set scope.



Microsoft Entra role assignments are an additive model, so your effective permissions are the sum of your role assignments. For example, if you assign a user a role at tenant scope and assign the same user the same role at attribute set scope, the user will still have permissions at tenant scope.

Step 3: Review the available roles

You need to determine who needs access to work with custom security attributes in your organization. To help you manage access to custom security attributes, there are four Microsoft Entra built-in roles. If necessary, someone with at least the [Privileged Role Administrator](#) role can assign these roles.

- [Attribute Definition Administrator](#)
- [Attribute Assignment Administrator](#)
- [Attribute Definition Reader](#)
- [Attribute Assignment Reader](#)

The following table provides a high-level comparison of the custom security attributes roles.

[Expand table](#)

Permission	Attribute Definition Admin	Attribute Assignment Admin	Attribute Definition Reader	Attribute Assignment Reader
Read attribute sets	✓	✓	✓	✓
Read attribute definitions	✓	✓	✓	✓

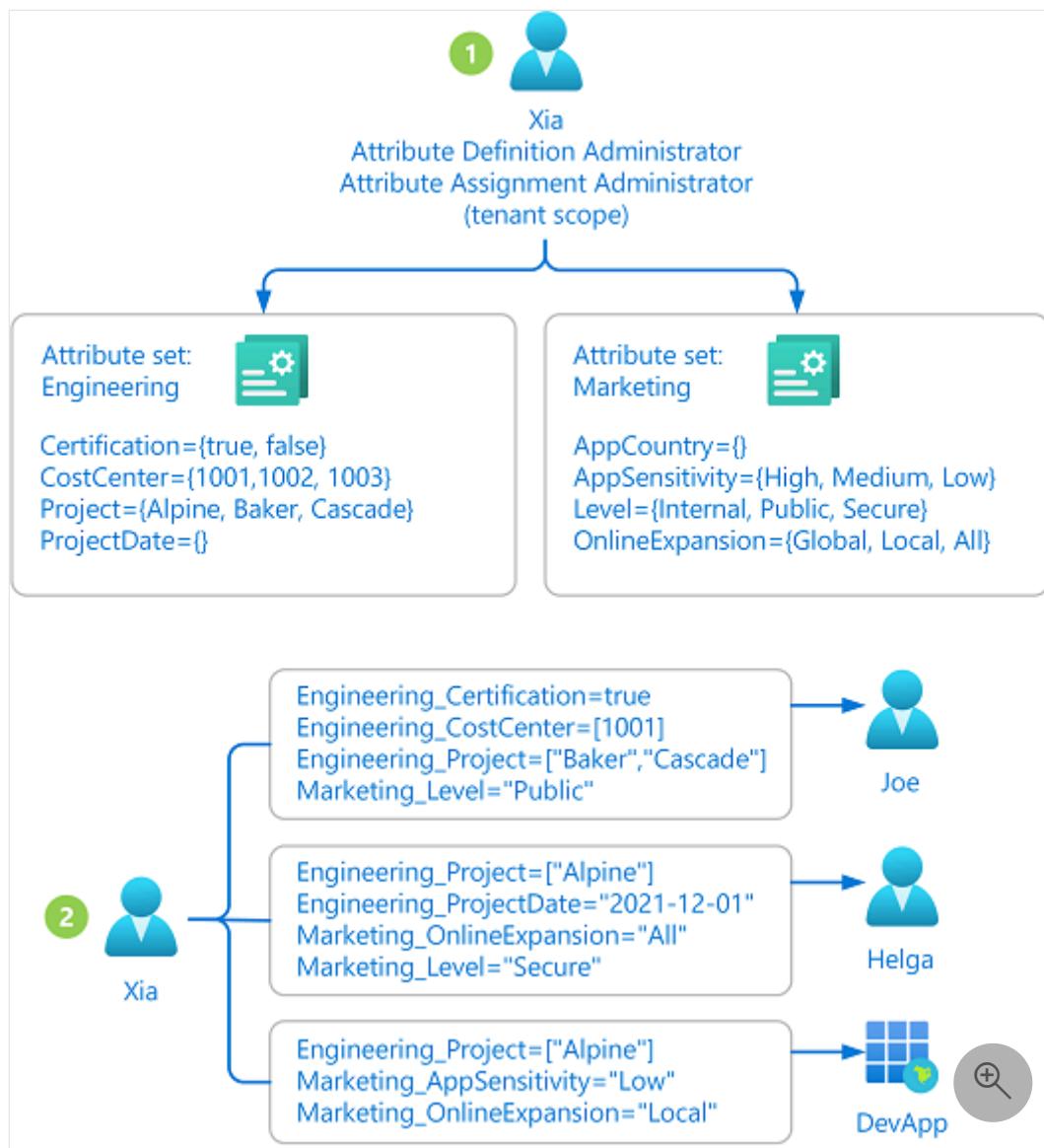
Permission	Attribute Definition Admin	Attribute Assignment Admin	Attribute Definition Reader	Attribute Assignment Reader
Read attribute assignments for users and applications (service principals)		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
Add or edit attribute sets	<input checked="" type="checkbox"/>			
Add, edit, or deactivate attribute definitions	<input checked="" type="checkbox"/>			
Assign attributes to users and applications (service principals)		<input checked="" type="checkbox"/>		

Step 4: Determine your delegation strategy

This step describes two ways you can manage access to custom security attributes. The first way is to manage them centrally and the second way is to delegate management to others.

Manage attributes centrally

An administrator that has been assigned the Attribute Definition Administrator and Attribute Assignment Administrator roles at tenant scope can manage all aspects of custom security attributes. The following diagram shows how custom security attributes are defined and assigned by a single administrator.



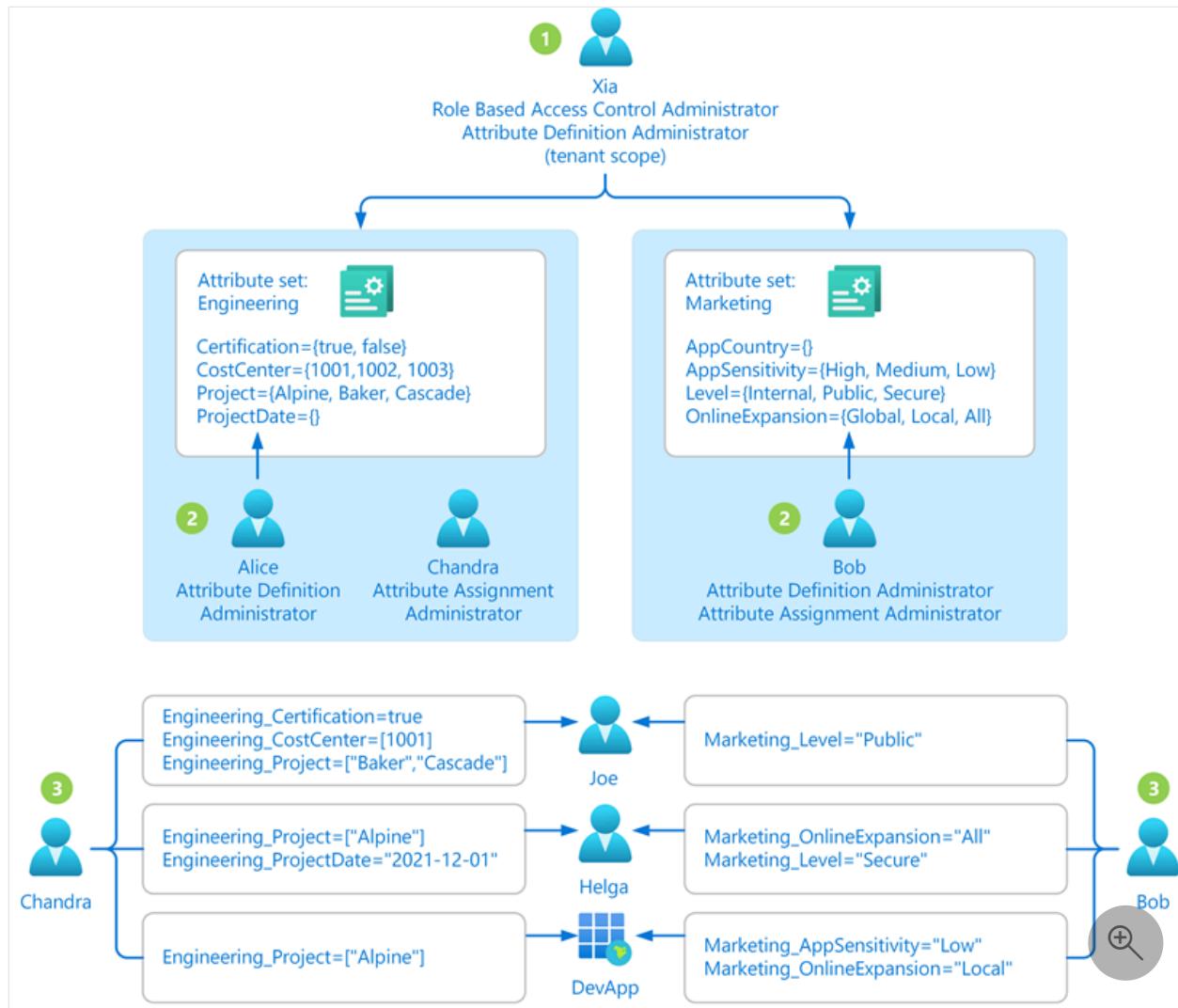
1. The administrator (Xia) has both the Attribute Definition Administrator and Attribute Assignment Administrator roles assigned at tenant scope. The administrator adds attribute sets and defines attributes.
2. The administrator assigns attributes to Microsoft Entra objects.

Managing attributes centrally has the advantage that it can be managed by one or two administrators. The disadvantage is that the administrator might get several requests to define or assign custom security attributes. In this case, you might want to delegate management.

Manage attributes with delegation

An administrator might not know all the situations of how custom security attributes should be defined and assigned. Typically it's users within the respective departments, teams, or projects who know the most about their area. Instead of assigning one or two administrators to manage all custom security attributes, you can instead delegate the management at attribute set scope. This also follows the best practice of least privilege

to grant just the permissions other administrators need to do their job and avoid unnecessary access. The following diagram shows how the management of custom security attributes can be delegated to multiple administrators.



1. The administrator (Xia) with the Attribute Definition Administrator role assigned at tenant scope adds attribute sets. The administrator also has permissions to assign roles to others (Privileged Role Administrator) and delegates who can read, define, or assign custom security attributes for each attribute set.
2. The delegated Attribute Definition Administrators (Alice and Bob) define attributes in the attribute sets they have been granted access to.
3. The delegated Attribute Assignment Administrators (Chandra and Bob) assign attributes from their attribute sets to Microsoft Entra objects.

Step 5: Select the appropriate roles and scope

Once you have a better understanding of how your attributes will be organized and who needs access, you can select the appropriate custom security attribute roles and scope. The following table can help you with the selection.

I want to grant this access	Assign this role	Scope
<ul style="list-style-type: none"> • Read all attribute sets in a tenant • Read all attribute definitions in a tenant • Add or edit all attribute sets in a tenant • Add, edit, or deactivate all attribute definitions in a tenant 	Attribute Definition Administrator	 Tenant
<ul style="list-style-type: none"> • Read attribute definitions in a scoped attribute set • Add, edit, or deactivate attribute definitions in a scoped attribute set • Cannot update the scoped attribute set • Cannot read, add, or update other attribute sets 	Attribute Definition Administrator	 Attribute set
<ul style="list-style-type: none"> • Read all attribute sets in a tenant • Read all attribute definitions in a tenant • Read all attribute assignments in a tenant for users • Read all attribute assignments in a tenant for applications (service principals) • Assign all attributes in a tenant to users • Assign all attributes in a tenant to applications (service principals) • Author Azure role assignment conditions that use the Principal attribute for all attributes in a tenant 	Attribute Assignment Administrator	 Tenant
<ul style="list-style-type: none"> • Read attribute definitions in a scoped attribute set • Read attribute assignments that use attributes in a scoped attribute set for users • Read attribute assignments that use attributes in a scoped attribute set for applications (service principals) • Assign attributes in a scoped attribute set to users • Assign attributes in a scoped attribute set to applications (service principals) • Author Azure role assignment conditions that use the Principal attribute for all attributes in a scoped attribute set • Cannot read attributes in other attribute sets • Cannot read attribute assignments that use attributes in other attribute sets 	Attribute Assignment Administrator	 Attribute set
<ul style="list-style-type: none"> • Read all attribute sets in a tenant • Read all attribute definitions in a tenant 	Attribute Definition Reader	 Tenant

I want to grant this access	Assign this role	Scope
<ul style="list-style-type: none"> • Read attribute definitions in a scoped attribute set • Cannot read other attribute sets 	Attribute Definition Reader	 Attribute set
<ul style="list-style-type: none"> • Read all attribute sets in a tenant • Read all attribute definitions in a tenant • Read all attribute assignments in a tenant for users • Read all attribute assignments in a tenant for applications (service principals) 	Attribute Assignment Reader	 Tenant
<ul style="list-style-type: none"> • Read attribute definitions in a scoped attribute set • Read attribute assignments that use attributes in a scoped attribute set for users • Read attribute assignments that use attributes in a scoped attribute set for applications (service principals) • Cannot read attributes in other attribute sets • Cannot read attribute assignments that use attributes in other attribute sets 	Attribute Assignment Reader	 Attribute set

Step 6: Assign roles

To grant access to the appropriate people, follow these steps to assign one of the custom security attribute roles.

Assign roles at attribute set scope

The following examples show how to assign a custom security attribute role to a principal at an attribute set scope named Engineering.

Admin center
<ol style="list-style-type: none"> 1. Sign in to the Microsoft Entra admin center as a Attribute Assignment Administrator. 2. Browse to Protection > Custom security attributes. 3. Select the attribute set you want grant access to. 4. Select Roles and administrators.

The screenshot shows the 'Engineering' tenant's 'Roles and administrators' page. The 'Active attributes' section is selected. A note at the top right says: 'Get just-in-time access to a role when you need it using PIM. Learn more about PIM →'. Below is a table of administrative roles:

Role	Description	Privileged	Type
Attribute Assignment Administrator	Assign custom security attribute keys and values to supported Microsoft Entra objects.	Built-in	...
Attribute Assignment Reader	Read custom security attribute keys and values for supported Microsoft Entra objects.	Built-in	...
Attribute Definition Administrator	Define and manage the definition of custom security attributes.	Built-in	...
Attribute Definition Reader	Read the definition of custom security attributes.	Built-in	...

5. Add assignments for the custom security attribute roles.

⚠ Note

If you are using Microsoft Entra Privileged Identity Management (PIM), eligible role assignments at attribute set scope currently aren't supported. Permanent role assignments at attribute set scope are supported.

Assign roles at tenant scope

The following examples show how to assign a custom security attribute role to a principal at tenant scope.

Admin center

1. Sign in to the [Microsoft Entra admin center](#) as a [Attribute Assignment Administrator](#).
2. Browse to **Identity > Roles & admins > Roles & admins**.

Role	Description	Privileged	Type
Attribute Assignment Administrator	Assign custom security attribute keys and values to supported Microsoft Entra objects.	6	Built-in
Attribute Assignment Reader	Read custom security attribute keys and values for supported Microsoft Entra objects.	1	Built-in
Attribute Definition Administrator	Define and manage the definition of custom security attributes.	3	Built-in
Attribute Definition Reader	Read the definition of custom security attributes.	1	Built-in
Attribute Log Administrator	Read audit logs and configure diagnostic settings for events related to custom security attributes.	0	Built-in
Attribute Log Reader	Read audit logs related to custom security attributes.	0	Built-in
External ID User Flow Attribute Administrator	Can create and manage the attribute schema available to all user flows.	0	Built-in

3. Add assignments for the custom security attribute roles.

Custom security attribute audit logs

Sometimes you need information about custom security attribute changes for auditing or troubleshooting purposes. Anytime someone makes changes to definitions or assignments, the activities get logged.

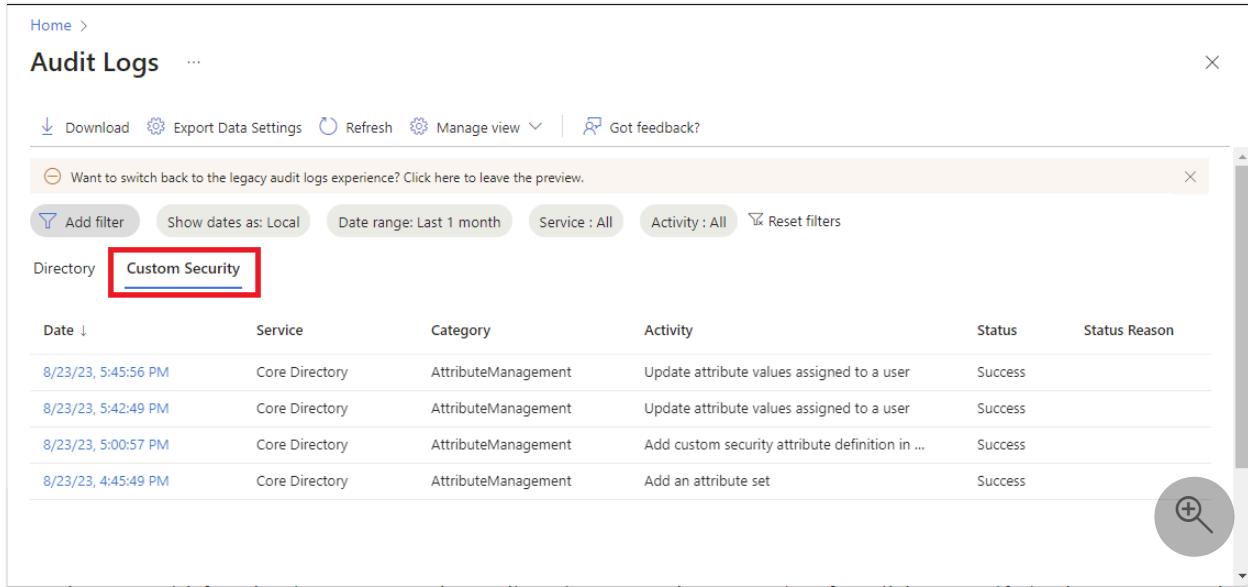
Custom security attribute audit logs provide you with the history of activities related to custom security attributes, such as adding a new definition or assigning an attribute value to a user. Here are the custom security attribute-related activities that are logged:

- Add an attribute set
- Add custom security attribute definition in an attribute set
- Update an attribute set
- Update attribute values assigned to a servicePrincipal
- Update attribute values assigned to a user
- Update custom security attribute definition in an attribute set

View audit logs for attribute changes

To view the custom security attribute audit logs, sign in to the Microsoft Entra admin center, browse to **Audit Logs**, and select **Custom Security**. To view custom security attribute audit logs, you must be assigned one of the following roles. If necessary, someone with at least the **Privileged Role Administrator** role can assign these roles.

- [Attribute Log Reader](#)
- [Attribute Log Administrator](#)



The screenshot shows the Microsoft Audit Logs interface. At the top, there are navigation links: Home > Audit Logs. Below the header are several buttons: Download, Export Data Settings, Refresh, Manage view, Got feedback?, and a note about switching back to the legacy audit logs experience. Filter options include Add filter, Show dates as: Local, Date range: Last 1 month, Service: All, Activity: All, and Reset filters. The main table has columns: Date, Service, Category, Activity, Status, and Status Reason. The 'Custom Security' tab is highlighted with a red box. The table data is as follows:

Date	Service	Category	Activity	Status	Status Reason
8/23/23, 5:45:56 PM	Core Directory	AttributeManagement	Update attribute values assigned to a user	Success	
8/23/23, 5:42:49 PM	Core Directory	AttributeManagement	Update attribute values assigned to a user	Success	
8/23/23, 5:00:57 PM	Core Directory	AttributeManagement	Add custom security attribute definition in ...	Success	
8/23/23, 4:45:49 PM	Core Directory	AttributeManagement	Add an attribute set	Success	

For information about how to get the custom security attribute audit logs using the Microsoft Graph API, see the [customSecurityAttributeAudit resource type](#). For more information, see [Microsoft Entra audit logs](#).

Diagnostic settings

To export custom security attribute audit logs to different destinations for additional processing, you use diagnostic settings. To create and configure diagnostic settings for custom security attributes, you must be assigned the [Attribute Log Administrator](#) role.

Tip

Microsoft recommends that you keep your custom security attribute audit logs separate from your directory audit logs so that attribute assignments are not revealed inadvertently.

The following screenshot shows the diagnostic settings for custom security attributes. For more information, see [How to configure diagnostic settings](#).

The screenshot shows the 'Diagnostic settings | Custom security attributes' page in the Azure portal. The left sidebar has 'Diagnostic settings' selected. The main area displays diagnostic settings for three resources: 'EventHub1', 'log_analytics', and 'log_storage'. Each resource has a 'Storage account' and 'Event hub' listed. The 'Log Analytics workspace' column shows 'EventHubCSALog/cs...' for EventHub1, 'csworkspace' for log_analytics, and 'csastorage3' for log_storage. The 'Edit setting' column for each row contains a link labeled 'Edit setting'. A red box highlights the 'Custom security attributes' link in the sidebar. Below the table, there's a note about adding diagnostic settings and a plus sign icon.

Changes to audit logs behavior

Changes have been made to custom security attribute audit logs for general availability that might affect your daily operations. If you have been using custom security attribute audit logs during preview, here are the actions you must take to ensure your audit log operations aren't disrupted.

- Use new audit logs location
- Assign Attribute Log roles to view audit logs
- Create new diagnostic settings to export audit logs

Use new audit logs location

During the preview, custom security attribute audit logs were written to the directory audit logs endpoint. In October 2023, a new endpoint was added exclusively for custom security attribute audit logs. The following screenshot shows the directory audit logs and the new custom security attribute audit logs location. To get the custom security attribute audit logs using the Microsoft Graph API, see the [customSecurityAttributeAudit](#) resource type.

Home >

Audit Logs

Download Export Data Settings Refresh Manage view

Want to switch back to the legacy audit logs experience? Click here to leave the preview.

Add filter Show dates as: Local Date range: Last 1 month Service Category

Directory Custom Security

Date ↓ Service Category

Custom Security

There is a transition period where custom security audit logs are written to both the directory and custom security attributes audit log endpoints. Going forward, you must use the custom security attributes audit log endpoint to find custom security attribute audit logs.

The following table lists the endpoint where you can find custom security attributes audit logs during the transition period.

[+] Expand table

Event date	Directory endpoint	Custom security attributes endpoint
Oct 2023	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Feb 2024		<input checked="" type="checkbox"/>

Assign Attribute Log roles to view audit logs

During the preview, custom security attribute audit logs could be viewed by those with at least the [Security Administrator](#) role in the directory audit logs. You are no longer able to use these roles to view custom security attribute audit logs using the new endpoint. To view the custom security attribute audit logs, you must be assigned either the [Attribute Log Reader](#) or [Attribute Log Administrator](#) role.

Create new diagnostic settings to export audit logs

During the preview, if you configured to export audit logs, custom security audit attribute audit logs were sent to your current diagnostic settings. To continue to receive

custom security audit attribute audit logs, you must create new diagnostic settings as described in the previous [Diagnostic settings](#) section.

Next steps

- Add or deactivate custom security attribute definitions in Microsoft Entra ID
 - Assign, update, list, or remove custom security attributes for a user
 - Troubleshoot custom security attributes in Microsoft Entra ID
-

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#) ↗

Assign, update, list, or remove custom security attributes for a user

Article • 03/25/2025

Custom security attributes in Microsoft Entra ID, part of Microsoft Entra, are business-specific attributes (key-value pairs) that you can define and assign to Microsoft Entra objects. For example, you can assign custom security attribute to filter your employees or to help determine who gets access to resources. This article describes how to assign, update, list, or remove custom security attributes for Microsoft Entra ID.

Prerequisites

To assign or remove custom security attributes for a user in your Microsoft Entra tenant, you need:

- [Attribute Assignment Administrator](#)
- Microsoft.Graph module when using [Microsoft Graph PowerShell](#)

i Important

By default, [Global Administrator](#) and other administrator roles do not have permissions to read, define, or assign custom security attributes.

Assign custom security attributes to a user

1. Sign in to the Microsoft Entra admin center  as an [Attribute Assignment Administrator](#).
2. Make sure that you have defined custom security attributes. For more information, see [Add or deactivate custom security attribute definitions in Microsoft Entra ID](#).
3. Browse to **Identity > Users > All users**.
4. Find and select the user you want to assign custom security attributes to.
5. In the Manage section, select **Custom security attributes**.
6. Select **Add assignment**.
7. In **Attribute set**, select an attribute set from the list.

8. In **Attribute name**, select a custom security attribute from the list.
9. Depending on the properties of the selected custom security attribute, you can enter a single value, select a value from a predefined list, or add multiple values.
 - For freeform, single-valued custom security attributes, enter a value in the **Assigned values** box.
 - For predefined custom security attribute values, select a value from the **Assigned values** list.
 - For multi-valued custom security attributes, select **Add values** to open the **Attribute values** pane and add your values. When finished adding values, select **Done**.

Attribute set	Attribute name	Attribute descrip...	Data type	Multi...	Assigned values
Engineering	Project	Active projects for ...	String	Yes	2 values

10. When finished, select **Save** to assign the custom security attributes to the user.

Update custom security attribute assignment values for a user

1. Sign in to the [Microsoft Entra admin center](#) as an **Attribute Assignment Administrator**.
2. Browse to **Identity > Users > All users**.
3. Find and select the user that has a custom security attribute assignment value you want to update.
4. In the Manage section, select **Custom security attributes**.
5. Find the custom security attribute assignment value you want to update.

Once you have assigned a custom security attribute to a user, you can only change the value of the custom security attribute. You can't change other properties of the

custom security attribute, such as attribute set or attribute name.

6. Depending on the properties of the selected custom security attribute, you can update a single value, select a value from a predefined list, or update multiple values.

7. When finished, select **Save**.

Filter users based on custom security attribute assignments

You can filter the list of custom security attributes assigned to users on the All users page.

1. Sign in to the [Microsoft Entra admin center](#) as an [Attribute Assignment Reader](#).
2. Browse to **Identity > Users > All users**.
3. Select **Add filter** to open the Add filter pane.
4. Select **Custom security attributes**.
5. Select your attribute set and attribute name.
6. For **Operator**, you can select equals (==), not equals (!=), or starts with.
7. For **Value**, enter or select a value.

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a sidebar with links like 'Audit logs', 'Sign-in logs', 'Diagnose and solve problems', 'Deleted users (preview)', 'Password reset', 'User settings', 'Bulk operation results', 'New support request', and 'Troubleshooting + Support'. The main area shows a list of 1,068 users with columns for 'Display name' and 'User principal name'. A modal window titled 'Add filter' is open over the list. The 'Filter' section contains 'Custom security attributes (preview)' in the input field. The 'Attribute set' dropdown is set to 'Engineering'. The 'Attribute name' dropdown is set to 'Project'. The 'Operator' dropdown is set to '==' with a dropdown arrow. The 'Value' dropdown is set to 'Baker' with a dropdown arrow. At the bottom of the modal are 'Apply' and 'Cancel' buttons.

8. To apply the filter, select **Apply**.

Remove custom security attribute assignments from a user

1. Sign in to the Microsoft Entra admin center [↗](#) as an [Attribute Assignment Administrator](#).
2. Browse to **Identity > Users > All users**.
3. Find and select the user that has the custom security attribute assignments you want to remove.
4. In the Manage section, select **Custom security attributes**.
5. Add check marks next to all the custom security attribute assignments you want to remove.
6. Select **Remove assignment**.

PowerShell or Microsoft Graph API

To manage custom security attribute assignments for users in your Microsoft Entra organization, you can use PowerShell or Microsoft Graph API. The following examples can be used to manage assignments.

Assign a custom security attribute with a string value to a user

The following example assigns a custom security attribute with a string value to a user.

- Attribute set: `Engineering`
- Attribute: `ProjectDate`
- Attribute data type: String
- Attribute value: `"2024-11-15"`

PowerShell

[Update-MgUser](#)

PowerShell

```
$customSecurityAttributes = @{
    "Engineering" = @{
        "@odata.type" =
        "#Microsoft.DirectoryServices.CustomSecurityAttributeValue"
```

```
        "ProjectDate" = "2024-11-15"
    }
}
Update-MgUser -UserId $userId -CustomSecurityAttributes
$customSecurityAttributes
```

Assign a custom security attribute with a multi-string value to a user

The following example assigns a custom security attribute with a multi-string value to a user.

- Attribute set: `Engineering`
- Attribute: `Project`
- Attribute data type: Collection of Strings
- Attribute value: `["Baker", "Cascade"]`

PowerShell

[Update-MgUser](#)

PowerShell

```
$customSecurityAttributes = @{
    "Engineering" = @{
        "@odata.type" =
        "#Microsoft.DirectoryServices.CustomSecurityAttributeValue"
        "Project@odata.type" = "#Collection(String)"
        "Project" = @("Baker", "Cascade")
    }
}
Update-MgUser -UserId $userId -CustomSecurityAttributes
$customSecurityAttributes
```

Assign a custom security attribute with an integer value to a user

The following example assigns a custom security attribute with an integer value to a user.

- Attribute set: `Engineering`
- Attribute: `NumVendors`
- Attribute data type: Integer

- Attribute value: 4

```
PowerShell
```

Update-MgUser

```
PowerShell
```

```
$customSecurityAttributes = @{
    "Engineering" = @{
        "@odata.type" =
"#Microsoft.DirectoryServices.CustomSecurityAttributeValue"
        "NumVendors@odata.type" = "#Int32"
        "NumVendors" = 4
    }
}
Update-MgUser -UserId $userId -CustomSecurityAttributes
$customSecurityAttributes
```

Assign a custom security attribute with a multi-integer value to a user

The following example assigns a custom security attribute with a multi-integer value to a user.

- Attribute set: Engineering
- Attribute: CostCenter
- Attribute data type: Collection of Integers
- Attribute value: [1001,1003]

```
PowerShell
```

Update-MgUser

```
PowerShell
```

```
$customSecurityAttributes = @{
    "Engineering" = @{
        "@odata.type" =
"#Microsoft.DirectoryServices.CustomSecurityAttributeValue"
        "CostCenter@odata.type" = "#Collection(Int32)"
        "CostCenter" = @(1001,1003)
    }
}
```

```
Update-MgUser -UserId $userId -CustomSecurityAttributes  
$customSecurityAttributes
```

Assign a custom security attribute with a Boolean value to a user

The following example assigns a custom security attribute with a Boolean value to a user.

- Attribute set: `Engineering`
- Attribute: `Certification`
- Attribute data type: Boolean
- Attribute value: `true`

PowerShell

Update-MgUser

```
PowerShell  
  
$customSecurityAttributes = @{  
    "Engineering" = @{  
        "@odata.type" =  
        "#Microsoft.DirectoryServices.CustomSecurityAttributeValue"  
        "Certification" = $true  
    }  
}  
Update-MgUser -UserId $userId -CustomSecurityAttributes  
$customSecurityAttributes
```

Update a custom security attribute assignment with an integer value for a user

The following example updates a custom security attribute assignment with an integer value for a user.

- Attribute set: `Engineering`
- Attribute: `NumVendors`
- Attribute data type: Integer
- Attribute value: `8`

PowerShell

Update-MgUser

PowerShell

```
$customSecurityAttributes = @{
    "Engineering" = @{
        "@odata.type" =
        "#Microsoft.DirectoryServices.CustomSecurityAttributeValue"
        "NumVendors@odata.type" = "#Int32"
        "NumVendors" = 8
    }
}
Update-MgUser -UserId $userId -CustomSecurityAttributes
$customSecurityAttributes
```

Update a custom security attribute assignment with a Boolean value for a user

The following example updates a custom security attribute assignment with a Boolean value for a user.

- Attribute set: `Engineering`
- Attribute: `Certification`
- Attribute data type: Boolean
- Attribute value: `false`

PowerShell

Update-MgUser

PowerShell

```
$customSecurityAttributes = @{
    "Engineering" = @{
        "@odata.type" =
        "#Microsoft.DirectoryServices.CustomSecurityAttributeValue"
        "Certification" = $false
    }
}
Update-MgUser -UserId $userId -CustomSecurityAttributes
$customSecurityAttributes
```

Update a custom security attribute assignment with a multi-string value for a user

The following example updates a custom security attribute assignment with a multi-string value for a user.

- Attribute set: Engineering
- Attribute: Project
- Attribute data type: Collection of Strings
- Attribute value: ("Alpine", "Baker")

PowerShell

Update-MgUser

PowerShell

```
$customSecurityAttributes = @{
    "Engineering" = @{
        "@odata.type" =
        "#Microsoft.DirectoryServices.CustomSecurityAttributeValue"
        "Project@odata.type" = "#Collection(String)"
        "Project" = @("Alpine", "Baker")
    }
}
Update-MgUser -UserId $userId -CustomSecurityAttributes
$customSecurityAttributes
```

Get the custom security attribute assignments for a user

The following example gets the custom security attribute assignments for a user.

PowerShell

Get-MgUser

PowerShell

```
$userAttributes = Get-MgUser -UserId $userId -Property
"customSecurityAttributes"
$userAttributes.CustomSecurityAttributes.AdditionalProperties | Format-
List
$userAttributes.CustomSecurityAttributes.AdditionalProperties.Engineerin
```

```
g  
$userAttributes.CustomSecurityAttributes.AdditionalProperties.Marketing
```

Output

```
Key : Engineering  
Value : {[@odata.type, #microsoft.graph.customSecurityAttributeValue],  
[Project@odata.type, #Collection(String)], [Project, System.Object[]],  
[ProjectDate, 2024-11-15]...}
```

```
Key : Marketing  
Value : {[@odata.type, #microsoft.graph.customSecurityAttributeValue],  
[EmployeeId, GS45897]}
```

Key	Value
---	-----
@odata.type	#microsoft.graph.customSecurityAttributeValue
Project@odata.type	#Collection(String)
Project	{Baker, Alpine}
ProjectDate	2024-11-15
NumVendors	8
CostCenter@odata.type	#Collection(Int32)
CostCenter	{1001, 1003}
Certification	False

Key	Value
---	-----
@odata.type	#microsoft.graph.customSecurityAttributeValue
EmployeeId	KX45897

If there are no custom security attributes assigned to the user or if the calling principal does not have access, the response will be empty.

List all users with a custom security attribute assignment that equals a value

The following example lists all users with a custom security attribute assignment that equals a value. It retrieves users with a custom security attribute named `AppCountry` with a value that equals `Canada`. The filter value is case sensitive. You must add `ConsistencyLevel=eventual` in the request or the header. You must also include `$count=true` to ensure the request is routed correctly.

- Attribute set: `Marketing`
- Attribute: `AppCountry`

- Filter: AppCountry eq 'Canada'

PowerShell

[Get-MgUser](#)

PowerShell

```
$userAttributes = Get-MgUser -CountVariable CountVar -Property
"id,displayName,customSecurityAttributes" -Filter
"customSecurityAttributes/Marketing/AppCountry eq 'Canada'" -
ConsistencyLevel eventual
$userAttributes | select Id,DisplayName,CustomSecurityAttributes
$userAttributes.CustomSecurityAttributes.AdditionalProperties | Format-
List
```

Output

Id	DisplayName
CustomSecurityAttributes	
--	-----
-	
00aa00aa-bb11-cc22-dd33-44ee44ee44ee Jiya	Microsoft.Graph.PowerShell.Models.MicrosoftGraphCustomSecurityAttributeValue
11bb11bb-cc22-dd33-ee44-55ff55ff55ff Jana	Microsoft.Graph.PowerShell.Models.MicrosoftGraphCustomSecurityAttributeValue
Key : Engineering	
Value : {[@odata.type, #microsoft.graph.customSecurityAttributeValue], [Datacenter@odata.type, #Collection(String)], [Datacenter, System.Object[]]}	
Key : Marketing	
Value : {[@odata.type, #microsoft.graph.customSecurityAttributeValue], [AppCountry@odata.type, #Collection(String)], [AppCountry, System.Object[], [EmployeeId, KX19476]]}	
Key : Marketing	
Value : {[@odata.type, #microsoft.graph.customSecurityAttributeValue], [AppCountry@odata.type, #Collection(String)], [AppCountry, System.Object[], [EmployeeId, GS46982]]}	

List all users with a custom security attribute assignment that starts with a value

The following example lists all users with a custom security attribute assignment that starts with a value. It retrieves users with a custom security attribute named `EmployeeId` with a value that starts with `GS`. The filter value is case sensitive. You must add `ConsistencyLevel=eventual` in the request or the header. You must also include `$count=true` to ensure the request is routed correctly.

- Attribute set: `Marketing`
- Attribute: `EmployeeId`
- Filter: `EmployeeId` startsWith 'GS'

PowerShell

[Get-MgUser](#)

PowerShell

```
$userAttributes = Get-MgUser -CountVariable CountVar -Property
"id,displayName,customSecurityAttributes" -Filter
"startsWith(customSecurityAttributes/Marketing/EmployeeId,'GS'))" -
ConsistencyLevel eventual
$userAttributes | select Id,DisplayName,CustomSecurityAttributes
$userAttributes.CustomSecurityAttributes.AdditionalProperties | Format-
List
```

Output

Id CustomSecurityAttributes	DisplayName
--	-----
-	
22cc22cc-dd33-ee44-ff55-66aa66aa66aa	Chandra
Microsoft.Graph.PowerShell.Models.MicrosoftGraphCustomSecurityAttributeValue	
11bb11bb-cc22-dd33-ee44-55ff55ff55ff	Jana
Microsoft.Graph.PowerShell.Models.MicrosoftGraphCustomSecurityAttributeValue	
33dd33dd-ee44-ff55-aa66-77bb77bb77bb	Joe
Microsoft.Graph.PowerShell.Models.MicrosoftGraphCustomSecurityAttributeValue	
Key : Marketing	
Value : {[@odata.type, #microsoft.graph.customSecurityAttributeValue],	
[EmployeeId, GS36348]}	
Key : Marketing	
Value : {[@odata.type, #microsoft.graph.customSecurityAttributeValue],	
[AppCountry@odata.type, #Collection(String)], [AppCountry,	
System.Object[],	
[EmployeeId, GS46982]}	

```
Key : Engineering
Value : {[@odata.type, #microsoft.graph.customSecurityAttributeValue],
[Project@odata.type, #Collection(String)], [Project, System.Object[]],
[ProjectDate, 2024-11-15]...}
```

```
Key : Marketing
Value : {[@odata.type, #microsoft.graph.customSecurityAttributeValue],
[EmployeeId, GS45897]}
```

List all users with a custom security attribute assignment that does not equal a value

The following example lists all users with a custom security attribute assignment that does not equal a value. It retrieves users with a custom security attribute named `AppCountry` with a value that does not equal `Canada`. The filter value is case sensitive. You must add `ConsistencyLevel=eventual` in the request or the header. You must also include `$count=true` to ensure the request is routed correctly.

- Attribute set: `Marketing`
- Attribute: `AppCountry`
- Filter: `AppCountry ne 'Canada'`

PowerShell

[Get-MgUser](#)

PowerShell

```
$userAttributes = Get-MgUser -CountVariable CountVar -Property
"id,displayName,customSecurityAttributes" -Filter
"customSecurityAttributes/Marketing/AppCountry ne 'Canada'" -
ConsistencyLevel eventual
$userAttributes | select Id,DisplayName,CustomSecurityAttributes
```

Output

<code>Id</code>	<code>DisplayName</code>
<code>CustomSecurityAttributes</code>	
--	-----
-----	-----
<code>22cc22cc-dd33-ee44-ff55-66aa66aa66aa</code>	<code>Chandra</code>
<code>Microsoft.Graph.PowerShell.Models.MicrosoftGraphCustomSecurityAttributeValue</code>	
<code>44ee44ee-ff55-aa66-bb77-88cc88cc88cc</code>	<code>Isabella</code>

```
Microsoft.Graph.PowerShell.Models.MicrosoftGraphCustomSecurityAttributeValue
00aa00aa-bb11-cc22-dd33-44ee44ee44ee Alain
Microsoft.Graph.PowerShell.Models.MicrosoftGraphCustomSecurityAttributeValue
33dd33dd-ee44-ff55-aa66-77bb77bb77bb Joe
Microsoft.Graph.PowerShell.Models.MicrosoftGraphCustomSecurityAttributeValue
00aa00aa-bb11-cc22-dd33-44ee44ee44ee Dara
Microsoft.Graph.PowerShell.Models.MicrosoftGraphCustomSecurityAttributeValue
```

Remove a single-valued custom security attribute assignment from a user

The following example removes a single-valued custom security attribute assignment from a user by setting the value to null.

- Attribute set: `Engineering`
- Attribute: `ProjectDate`
- Attribute value: `null`

PowerShell

Invoke-MgGraphRequest

PowerShell

```
$params = @{
    "customSecurityAttributes" = @{
        "Engineering" = @{
            "@odata.type" =
"#Microsoft.DirectoryServices.CustomSecurityAttributeValue"
            "ProjectDate" = $null
        }
    }
}
Invoke-MgGraphRequest -Method PATCH -Uri
"https://graph.microsoft.com/v1.0/users/$userId" -Body $params
```

Remove a multi-valued custom security attribute assignment from a user

The following example removes a multi-valued custom security attribute assignment from a user by setting the value to an empty collection.

- Attribute set: Engineering
- Attribute: Project
- Attribute value: []

PowerShell

Update-MgUser

PowerShell

```
$customSecurityAttributes = @{
    "Engineering" = @{
        "@odata.type" =
    "#Microsoft.DirectoryServices.CustomSecurityAttributeValue"
        "Project" = @()
    }
}
Update-MgUser -UserId $userId -CustomSecurityAttributes
$customSecurityAttributes
```

Frequently asked questions

Where are custom security attribute assignments for users supported?

Custom security attribute assignments for users are supported in Microsoft Entra admin center, PowerShell, and Microsoft Graph APIs. Custom security attribute assignments are not supported in My Apps or Microsoft 365 admin center.

Who can view the custom security attributes assigned to a user?

Only users that have been assigned the Attribute Assignment Administrator or Attribute Assignment Reader roles at tenant scope can view custom security attributes assigned to any users in the tenant. Users cannot view the custom security attributes assigned to their own profile or other users. Guests cannot view the custom security attributes regardless of the guest permissions set on the tenant.

Do I need to create an app to add custom security attribute assignments?

No, custom security attributes can be assigned to user objects without requiring an application.

Why do I keep getting an error trying to save custom security attribute assignments?

You don't have permissions to assign custom security attributes to users. Make sure that you are assigned the Attribute Assignment Administrator role.

Can I assign custom security attributes to guests?

Yes, custom security attributes can be assigned to members or guests in your tenant.

Can I assign custom security attributes to directory synced users?

Yes, directory synced users from an on-premises Active Directory can be assigned custom security attributes.

Are custom security attribute assignments available for rules for dynamic membership groups?

No, custom security attributes assigned to users are not supported for configuring rules for dynamic membership groups.

Are custom security attributes the same as the custom attributes in B2C tenants?

No, custom security attributes are not supported in B2C tenants and are not related to B2C features.

Next steps

- [Add or deactivate custom security attribute definitions in Microsoft Entra ID](#)
- [Assign, update, list, or remove custom security attributes for an application](#)
- [Examples: Assign, update, list, or remove custom security attribute assignments using the Microsoft Graph API](#)
- [Troubleshoot custom security attributes in Microsoft Entra ID](#)

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Manage custom security attributes for an application

Article • 03/06/2025

Custom security attributes in Microsoft Entra ID are business-specific attributes (key-value pairs) that you can define and assign to Microsoft Entra objects. For example, you can assign custom security attribute to filter your applications or to help determine who gets access. This article describes how to assign, update, list, or remove custom security attributes for Microsoft Entra enterprise applications.

Prerequisites

To assign or remove custom security attributes for an application in your Microsoft Entra tenant, you need:

- A Microsoft Entra account with an active subscription. [Create an account for free](#).
- **Attribute Assignment Administrator** role.
- Make sure you have existing custom security attributes. To learn how to create a security attribute, see [Add or deactivate custom security attributes in Microsoft Entra ID](#).

 **Important**

By default, [Global Administrator](#) and other administrator roles do not have permissions to read, define, or assign custom security attributes.

Assign, update, list, or remove custom attributes for an application

Learn how to work with custom attributes for applications in Microsoft Entra ID.

Assign custom security attributes to an application

Undertake the following steps to assign custom security attributes through the Microsoft Entra admin center.

1. Sign in to the [Microsoft Entra admin center](#) as an [Attribute Assignment Administrator](#).

2. Browse to **Identity > Applications > Enterprise applications**.
3. Find and select the application you want to add a custom security attribute to.
4. In the Manage section, select **Custom security attributes**.
5. Select **Add assignment**.
6. In **Attribute set**, select an attribute set from the list.
7. In **Attribute name**, select a custom security attribute from the list.
8. Depending on the properties of the selected custom security attribute, you can enter a single value, select a value from a predefined list, or add multiple values.
 - For freeform, single-valued custom security attributes, enter a value in the **Assigned values** box.
 - For predefined custom security attribute values, select a value from the **Assigned values** list.
 - For multi-valued custom security attributes, select **Add values** to open the **Attribute values** pane and add your values. When finished adding values, select **Done**.

The screenshot shows the 'Custom security attributes' page for the 'TestApp' application. The left sidebar lists various application management sections: Single sign-on, Provisioning, Application proxy, Self-service, and Custom security attributes (which is selected). The main area displays a table of assigned attributes. One row is visible, showing 'Engineering' as the attribute set, 'Project' as the attribute name, 'Active projects for ...' as the description, 'String' as the data type, 'Yes' as the multi-valued status, and '1 value' as the count. A large search bar at the top is empty. A magnifying glass icon is in the bottom right corner of the main area.

Attribute set	Attribute name	Attribute descrip...	Data type	Multi-valued	Assigned val...
Engineering	Project	Active projects for ...	String	Yes	1 value

9. When finished, select **Save** to assign the custom security attributes to the application.

Update custom security attribute assignment values for an application

1. Sign in to the [Microsoft Entra admin center](#) as an **Attribute Assignment Administrator**.
2. Browse to **Identity > Applications > Enterprise applications**.

3. Find and select the application that has a custom security attribute assignment value you want to update.

4. In the Manage section, select **Custom security attributes**.

5. Find the custom security attribute assignment value you want to update.

Once you assigned a custom security attribute to an application, you can only change the value of the custom security attribute. You can't change other properties of the custom security attribute, such as attribute set or custom security attribute name.

6. Depending on the properties of the selected custom security attribute, you can update a single value, select a value from a predefined list, or update multiple values.

7. When finished, select **Save**.

Filter applications based on custom security attributes

You can filter the list of custom security attributes assigned to applications on the **All applications** page.

1. Sign in to the [Microsoft Entra admin center](#) as at least an **Attribute Assignment Reader**.

2. Browse to **Identity > Applications > Enterprise applications**.

3. Select **Add filters** to open the Pick a field pane.

If you don't see **Add filters**, select the banner to enable the Enterprise applications search preview.

4. For **Filters**, select **Custom security attribute**.

5. Select your attribute set and attribute name.

6. For **Operator**, you can select equals (==), not equals (!=), or starts with.

7. For **Value**, enter or select a value.

8. To apply the filter, select **Apply**.

Remove custom security attribute assignments from applications

1. Sign in to the Microsoft Entra admin center  as a [Attribute Assignment Administrator](#).
2. Browse to **Identity > Applications > Enterprise applications**.
3. Find and select the application that has the custom security attribute assignments you want to remove.
4. In the **Manage** section, select **Custom security attributes (preview)**.
5. Add check marks next to all the custom security attribute assignments you want to remove.
6. Select **Remove assignment**.

Next steps

- [Add or deactivate custom security attributes in Microsoft Entra ID](#)
 - [Assign, update, list, or remove custom security attributes for a user](#)
 - [Troubleshoot custom security attributes in Microsoft Entra ID](#)
-

Feedback

Was this page helpful?

 Yes

 No

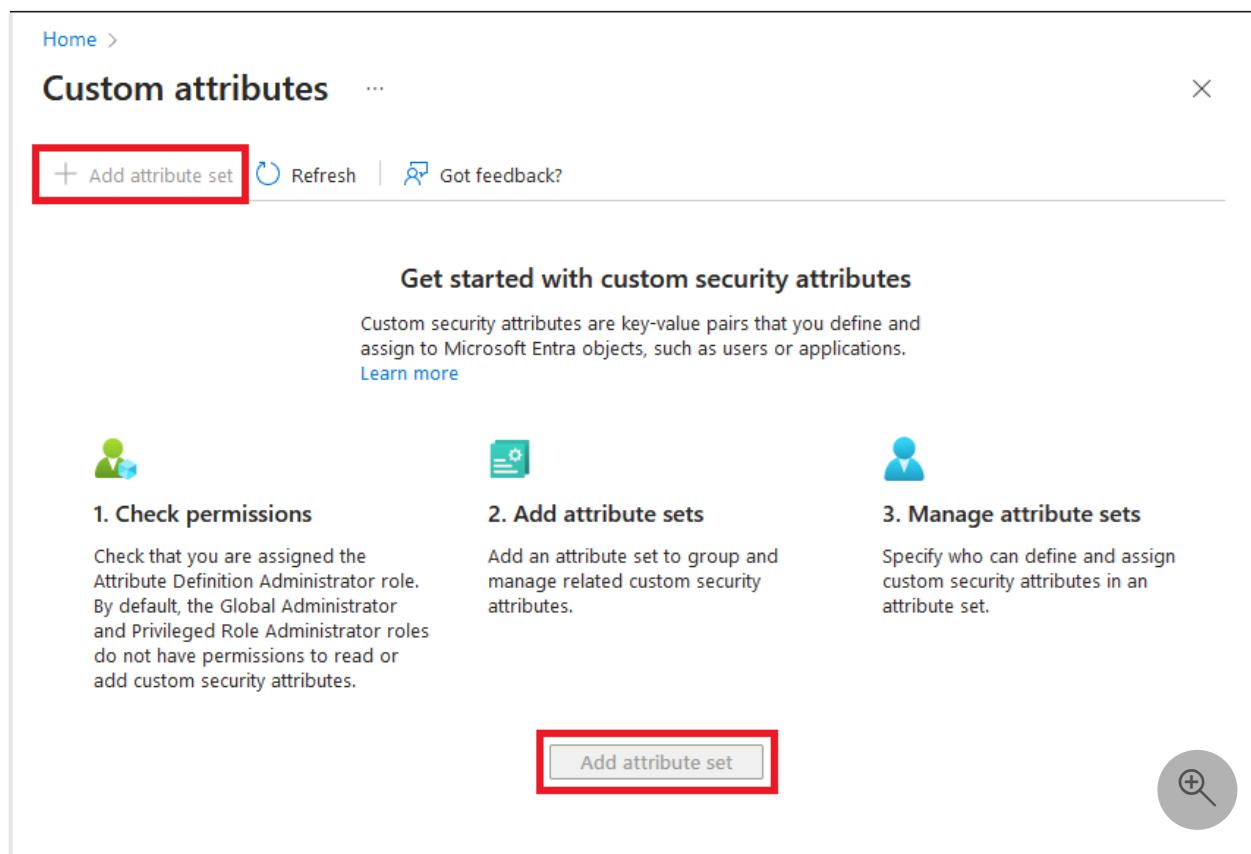
[Provide product feedback !\[\]\(2723f5c5d166266ae8c4befe5af8c966_img.jpg\)](#)

Troubleshoot custom security attributes in Microsoft Entra ID

Article • 11/27/2024

Symptom - Add attribute set is disabled

When signed in to the [Microsoft Entra admin center](#) and you try to select the **Custom security attributes > Add attribute set** option, it's disabled.



The screenshot shows the Microsoft Entra admin center interface. At the top, there's a navigation bar with 'Home' and a search bar. Below that is a header for 'Custom attributes'. On the left, there's a sidebar with a 'Custom attributes' section. The main content area has a heading 'Get started with custom security attributes' followed by a brief description and a 'Learn more' link. Below this are three numbered steps: 1. Check permissions, 2. Add attribute sets, and 3. Manage attribute sets. Each step has a corresponding icon and a brief description. At the bottom of the main content area is a large 'Add attribute set' button, which is also highlighted with a red box. To the right of the main content area is a circular search icon.

Cause

You don't have permissions to add an attribute set. To add an attribute set and custom security attributes, you must be assigned the [Attribute Definition Administrator](#) role.

ⓘ Important

By default, [Global Administrator](#) and other administrator roles do not have permissions to read, define, or assign custom security attributes.

Solution

Make sure that you're assigned the [Attribute Definition Administrator](#) role at either the tenant scope or attribute set scope. For more information, see [Manage access to custom security attributes in Microsoft Entra ID](#).

Symptom - Error when you try to assign a custom security attribute

When you try to save a custom security attribute assignment, you get the message:

Insufficient privileges to save custom security attributes
This account does not have the necessary admin privileges to change custom security attributes

Cause

You don't have permissions to assign custom security attributes. To assign custom security attributes, you must be assigned the [Attribute Assignment Administrator](#) role.

Important

By default, [Global Administrator](#) and other administrator roles do not have permissions to read, define, or assign custom security attributes.

Solution

Make sure that you're assigned the [Attribute Assignment Administrator](#) role at either the tenant scope or attribute set scope. For more information, see [Manage access to custom security attributes in Microsoft Entra ID](#).

Symptom - Can't filter custom security attributes for users or applications

Cause 1

You don't have permissions to filter custom security attributes. To read and filter custom security attributes for users or enterprise applications, you must be assigned the [Attribute Assignment Reader](#) or [Attribute Assignment Administrator](#) role.

Important

By default, [Global Administrator](#) and other administrator roles do not have permissions to read, define, or assign custom security attributes.

Solution 1

Make sure that you're assigned one of the following Microsoft Entra built-in roles at either the tenant scope or attribute set scope. For more information, see [Manage access to custom security attributes in Microsoft Entra ID](#).

- [Attribute Assignment Administrator](#)
- [Attribute Assignment Reader](#)

Cause 2

You're assigned the Attribute Assignment Reader or Attribute Assignment Administrator role, but you haven't been assigned access to an attribute set.

Solution 2

You can delegate the management of custom security attributes at the tenant scope or at the attribute set scope. Make sure you have been assigned access to an attribute set at either the tenant scope or attribute set scope. For more information, see [Manage access to custom security attributes in Microsoft Entra ID](#).

Cause 3

There are no custom security attributes defined and assigned yet for your tenant.

Solution 3

Add and assign custom security attributes to users or enterprise applications. For more information, see [Add or deactivate custom security attribute definitions in Microsoft Entra ID](#), [Assign, update, list, or remove custom security attributes for a user](#), or [Assign, update, list, or remove custom security attributes for an application](#).

Symptom - Custom security attributes can't be deleted

Cause

You can only activate and deactivate custom security attribute definitions. Deletion of custom security attributes isn't supported. Deactivated definitions don't count toward the tenant wide 500 definition limit.

Solution

Deactivate the custom security attributes you no longer need. For more information, see [Add or deactivate custom security attribute definitions in Microsoft Entra ID](#).

Symptom - Can't add a role assignment at an attribute set scope using PIM

When you try to add an eligible Microsoft Entra role assignment using [Microsoft Entra Privileged Identity Management \(PIM\)](#), you can't set the scope to an attribute set.

Cause

PIM currently doesn't support adding an eligible Microsoft Entra role assignment at an attribute set scope.

Symptom - Insufficient privileges to complete the operation

When you try to use [Graph Explorer](#) to call Microsoft Graph API for custom security attributes, you see a message similar to the following:

```
Forbidden - 403. You need to consent to the permissions on the Modify
permissions (Preview) tab
Authorization_RequestDenied
Insufficient privileges to complete the operation.
```

The screenshot shows the Microsoft Graph Explorer interface. In the top navigation bar, there are links for Microsoft, Microsoft Graph, Solutions, Graph Explorer, Get Started, Docs, Changelog, Resources, and Developer Program. The main area is titled "Graph Explorer" and shows a user profile icon labeled "A Admin". Below this are sections for "Sample queries" and "Getting Started (8)". Under "Getting Started", there are several GET requests listed: "my profile", "my profile (beta)", "my photo", "my mail", and "all the items in my drive". On the right side, there is a "Request body" section with a text input field, and a "Response preview" section displaying a JSON error response. The error message is as follows:

```
{"error": { "code": "Authorization_RequestDenied", "message": "Insufficient privileges to complete the operation.", "innerError": { "date": "2022-01-14T00:09:53", "request-id": "client-request-id" } }}
```

Or when you try to use a PowerShell command, you see a message similar to the following:

The screenshot shows a PowerShell window with the following error message displayed:

```
Insufficient privileges to complete the operation.  
Status: 403 (Forbidden)  
ErrorCode: Authorization_RequestDenied
```

Cause 1

You're using Graph Explorer and you haven't consented to the required custom security attribute permissions to make the API call.

Solution 1

Open the Permissions panel, select the appropriate custom security attribute permission, and select **Consent**. In the Permissions requested window that appears, review the requested permissions.

Permissions

To try out different Microsoft Graph API endpoints, choose the permissions, and then click Consent.

The screenshot shows a search bar at the top with the text "attribute". Below it is a table with columns: "Permission", "Admin consent requir...", and "Status". There are two entries:

Permission	Admin consent requir...	Status
CustomSecAttributeAssignment (1)	CustomSecAttributeAssignme...	Consented
CustomSecAttributeDefinition (1)	CustomSecAttributeDefinition....	

At the bottom, a message says "1 selected: CustomSecAttributeDefinition.ReadWrite.All" next to a "Consent" button and a "Cancel" button. A magnifying glass icon is also present.

Cause 2

You aren't assigned the required custom security attribute role to make the API call.

ⓘ Important

By default, [Global Administrator](#) and other administrator roles do not have permissions to read, define, or assign custom security attributes.

Solution 2

Make sure that you're assigned the required custom security attribute role. For more information, see [Manage access to custom security attributes in Microsoft Entra ID](#).

Cause 3

You're trying to remove a single-valued custom security attribute assignment by setting it to `null` using the [Update-MgUser](#) or [Update-MgServicePrincipal](#) command.

Solution 3

Use the [Invoke-MgGraphRequest](#) command instead. For more information, see [Remove a single-valued custom security attribute assignment from a user](#) or [Remove custom security attribute assignments from applications](#).

Symptom - Request_UnsupportedQuery error

When you try to call Microsoft Graph API for custom security attributes, you see a message similar to the following:

```
Bad Request - 400
Request_UnsupportedQuery
Unsupported or invalid query filter clause specified for property
'<AttributeSet>_<Attribute>' of resource 'CustomSecurityAttributeValue'.
```

Cause

The request isn't formatted correctly.

Solution

If required, add `ConsistencyLevel=eventual` in the request or the header. You might also need to include `$count=true` to ensure the request is routed correctly. For more information, see [Examples: Assign, update, list, or remove custom security attribute assignments using the Microsoft Graph API](#).

The screenshot shows the Microsoft Graph Explorer interface. In the top navigation bar, there are links for Microsoft Graph, Explore, Graph Explorer, Docs, API, Learn, Developer Program, Support, and All Microsoft. On the right side, there are buttons for Tenant, Default Directory, and a user profile icon.

The main area is titled "Graph Explorer" and contains a search bar for "Sample queries" and "Resources". Below the search bar, there is a "Request body" section with a table for adding key-value pairs. One row in the table has "ConsistencyLevel" as the key and "eventual" as the value, both of which are highlighted with a red border.

Under the "Request body" section, there is a status message: "OK - 200 - 213ms". Below this, there is a "Response preview" section showing the JSON response from the API call. The JSON output includes the context URL, the count of users (2), and the list of users themselves.

Next steps

- Manage access to custom security attributes in Microsoft Entra ID
- Troubleshoot Azure role assignment conditions

Feedback

Was this page helpful?

Yes

No

Provide product feedback ↗

Manage Microsoft Entra identity and network access capabilities by using Microsoft Graph

Article • 01/07/2025

Important

APIs under the `/beta` version in Microsoft Graph are subject to change. Use of these APIs in production applications is not supported. To determine whether an API is available in v1.0, use the **Version** selector.

With Microsoft Graph, you can manage identity and network access capabilities, most of which are available through [Microsoft Entra](#). The APIs in Microsoft Graph help you to automate identity and network access management tasks and integrate with any application, and are the programmatic alternative to the administrator portals such as the Microsoft Entra admin center.

Microsoft Entra is a family of identity and network access capabilities that are available in the following products. All these capabilities are available through Microsoft Graph APIs:

- Microsoft Entra ID that groups identity and access management (IAM) capabilities.
- Microsoft Entra ID Governance
- Microsoft Entra External ID
- Microsoft Entra Verified ID
- Microsoft Entra Permissions Management
- Microsoft Entra Internet Access and Network Access

Manage user identities

Users are the main identities in any identity and access solution. You can manage the entire lifecycle of users in your organization, including guests, and their entitlements like licenses or group memberships, using Microsoft Graph APIs. For more information, see [Working with users in Microsoft Graph](#).

Manage groups

Groups are the containers that allow you to efficiently manage the entitlements for identities as a unit. For example, through a group, you can grant users access to a resource, such as a

SharePoint site. Or you can grant them licenses to use a service. For more information, see [Working with groups in Microsoft Graph](#).

Manage applications

You can use Microsoft Graph APIs to register and manage your applications programmatically, enabling you to use Microsoft's IAM capabilities. For more information, see [Manage Microsoft Entra applications and service principals by using Microsoft Graph](#).

Tenant administration or directory management

A core functionality of identity and access management is managing your tenant configuration, administrative roles, and settings. Microsoft Graph provides APIs to manage your Microsoft Entra tenant for the following scenarios:

 Expand table

Use cases	API operations
Manage administrative units including the following operations: <ul style="list-style-type: none">• Create administrative units• Create and manage members and membership rules of administrative units• Assign administrator roles that are scoped to administrative units	administrativeUnit resource type and its associated APIs
Grant, revoke, and retrieve app roles on a resource application for users, groups, or service principals	appRoleAssignment resource type and its associated APIs
Retrieve BitLocker recovery keys	bitlockerRecoveryKey resource type and its associated APIs
Manage custom security attributes	See Overview of custom security attributes using the Microsoft Graph API
Manage deleted directory objects. The functionality to store deleted objects in a "recycle bin" is supported for the following objects: <ul style="list-style-type: none">• Administrative units• Applications• External user profiles• Groups	<ul style="list-style-type: none">• Get or List deleted objects• Permanently delete a deleted object• Restore a deleted item• List deleted items owned by user

Use cases	API operations
<ul style="list-style-type: none"> • Pending external user profiles • Service principals • Users 	
Manage devices in the cloud	device resource type and its associated APIs
<p>View local administrator credential information for all device objects in Microsoft Entra ID that are enabled with Local Admin Password Solution (LAPS). This feature is the cloud-based LAPS solution</p>	deviceLocalCredentialInfo resource type and its associated APIs
<p>Directory objects are the core objects in Microsoft Entra ID, such as users, groups, and applications. You can use the directoryObject resource type and its associated APIs to check memberships of directory objects, track changes for multiple directory objects, or validate that a Microsoft 365 group's display name or mail nickname complies with naming policies</p>	directoryObject resource type and its associated APIs
<p>Administrator roles, including Microsoft Entra administrator roles, are one of the most sensitive resources in a tenant. You can manage the lifecycle of their assignment in the tenant, including creating custom roles, assigning roles, tracking changes to role assignments, and removing assignees from roles</p>	<p>directoryRole resource type and directoryRoleTemplate resource type and their associated APIs</p> <p>roleManagement resource type and its associated APIs (recommended)</p> <p>These APIs allow you to make direct role assignments. Alternatively, you can use Privileged Identity Management APIs for Microsoft Entra roles and groups to make just-in-time and time-bound role assignments, instead of direct forever active assignments.</p>
<p>Define the following configurations that can be used to customize the tenant-wide and object-specific restrictions and allowed behavior.</p> <ul style="list-style-type: none"> • Settings for Microsoft 365 groups such as guest user access, classifications, and naming policies • Password rule settings such as banned password lists and lockout duration • Prohibited names for applications, reserved words, and blocking trademark violations • Custom conditional access policy URL 	<p>groupSetting resource type and groupSettingTemplate resource type and their associated APIs</p> <p>For more information, see Overview of group settings.</p>

Use cases	API operations
<ul style="list-style-type: none"> Consent policies such as user consent requests, group-specific consent, and consent for risky apps 	
<p>Domain management operations such as:</p> <ul style="list-style-type: none"> associating a domain with your tenant retrieving DNS records verifying domain ownership associating specific services with specific domains deleting domains 	domain resource type and its associated APIs
<p>Configure and manage staged rollout of specific Microsoft Entra ID features</p>	featureRolloutPolicy resource type and its associated APIs
<p>Monitor licenses and subscriptions for the tenant</p>	<ul style="list-style-type: none"> companySubscription resource type and its associated APIs subscribedSku resource type and its associated APIs
<p>Configure options that are available in Microsoft Entra Cloud Sync such as preventing accidental deletions and managing group writebacks</p>	onPremisesDirectorySynchronization resource type and its associated APIs
<p>Manage the base settings for your Microsoft Entra tenant</p>	organization resource type and its associated APIs
<p>Retrieve the organizational contacts that might be synchronized from on-premises directories or from Exchange Online</p>	orgContact resource type and its associated APIs
<p>Discover the basic details of other Microsoft Entra tenants by querying using the tenant ID or the domain name</p>	tenantInformation resource type and its associated APIs
<p>Manage the delegated permissions and their assignments to service principals in the tenant</p>	OAuth2PermissionGrant resource type and its associated APIs

Identity and sign-in

[Expand table](#)

Use cases	API operations
<p>Configure listeners that monitor events that should trigger or invoke custom logic, typically</p>	authenticationEventListener resource type and its associated APIs

Use cases	API operations
defined outside Microsoft Entra ID	
Manage authentication methods that are supported in Microsoft Entra ID	See Microsoft Entra authentication methods API overview and Microsoft Entra authentication methods policies API overview
Manage the authentication methods or combinations of authentication methods that you can apply as grant control in Microsoft Entra Conditional Access	See Microsoft Entra authentication strengths API overview
<p>Manage tenant-wide authorization policies such as:</p> <ul style="list-style-type: none"> • enable SSPR for administrator accounts • enable self-service join for guests • limit who can invite guests • whether users can consent to risky apps • block the use of MSOL • customize the default user permissions • identity private preview features enabled • Customize the guest user permissions between <i>User</i>, <i>Guest User</i>, and <i>Restricted Guest User</i> 	authorizationPolicy resource type and its associated APIs
Manage the policies for certificate-based authentication in the tenant	certificateBasedAuthConfiguration resource type and its associated APIs
Manage Microsoft Entra conditional access policies	conditionalAccessRoot resource type and its associated APIs
Manage cross-tenant access settings and manage outbound restrictions, inbound restrictions, tenant restrictions, and cross-tenant synchronization of users in multitenant organizations	See Cross-tenant access settings API overview
Configure how and which external systems interact with Microsoft Entra ID during a user authentication session	customAuthenticationExtension resource type and its associated APIs
Manage requests against user data in the organization, such as exporting personal data	dataPolicyOperation resource type and its associated APIs
Force autoacceleration sign-in to skip the username entry screen and automatically forward users to federated sign-in endpoints	homeRealmDiscoveryPolicy resource type resource type and its associated APIs
Detect, investigate, and remediate identity-based risks using Microsoft Entra ID Protection and feed the data into security information and	See Use the Microsoft Graph identity protection APIs

Use cases	API operations
event management (SIEM) tools for further investigation and correlation	
<p>Manage identity providers for Microsoft Entra ID, Microsoft Entra External ID, and Azure AD B2C tenants. You can perform the following operations:</p> <ul style="list-style-type: none"> • Manage identity providers for external identities, including social identity providers, OIDC, Apple, SAML/WS-Fed, and built-in providers • Manage configuration for federated domains and token validation 	identityProviderBase resource type and its associated APIs
Define a group of tenants belonging to your organization and streamline intra-organization cross-tenant collaboration	See Multitenant organization API overview
Customize sign-in UIs to match your company branding, including applying branding that's based on the browser language	organizationalBranding resource type and its associated APIs
User flows for Microsoft Entra External ID in workforce tenants	<p>The following resource types and their associated APIs:</p> <ul style="list-style-type: none"> • b2xIdentityUserFlow to configure the base user flow and its properties such as identity providers • identityUserFlowAttribute to manage built-in and custom user flow attributes • identityUserFlowAttributeAssignment to manage user flow attribute assignments • userFlowLanguageConfiguration resource type to configure custom languages for user flows
User flows for Microsoft Entra External ID in external tenants	<p>The following resource types and their associated APIs:</p> <ul style="list-style-type: none"> • authenticationEventsFlow resource type and its associated APIs • identityUserFlowAttribute to manage built-in and custom user flow attributes
Manage app consent policies and condition sets	permissionGrantPolicy resource type
Enable or disable security defaults in Microsoft Entra ID	identitySecurityDefaultsEnforcementPolicy resource type

Identity governance

For more information, see [Overview of Microsoft Entra ID Governance using Microsoft Graph](#).

Microsoft Entra External ID in external tenants

The following API use cases are supported to customize how users interact with your customer-facing applications. For administrators, most of the features available in Microsoft Entra ID are also supported for Microsoft Entra External ID in external tenants. For example, domain management, application management, and conditional access.

[] [Expand table](#)

Use cases	API operations
User flows for Microsoft Entra External ID in external tenants and self-service sign-up experiences	authenticationEventsFlow resource type and its associated APIs
Manage identity providers for Microsoft Entra External ID. You can identify the identity providers that are supported or configured in the tenant	See identityProviderBase resource type and its associated APIs
Configuring custom URL domains in Microsoft Entra External ID in external tenants	The <code>CustomUrlDomain</code> value for the supportedServices property of domain resource type and its associated APIs
Customize sign-in UIs to match your company branding, including applying branding that's based on the browser language	organizationalBranding resource type and its associated APIs
Manage identity providers for Microsoft Entra External ID, such as social identities	identityProviderBase resource type and its associated APIs
Manage user profiles in Microsoft Entra External ID for customers	For more information, see Default user permissions in customer tenants
Add your own business logic to the authentication experiences by integrating with systems that are external to Microsoft Entra ID	authenticationEventListener resource type and customAuthenticationExtension resource type and their associated APIs

Partner tenant management

Microsoft Graph also provides the following identity and access capabilities for Microsoft partners in the Cloud Solution Provider (CSP), Value Added Reseller (VAR), or Advisor programs to help manage their customer tenants.

Use cases	API operations
Manage contracts for the partner with its customers	contract resource type and its associated APIs
Microsoft partners can empower their customers to ensure the partners have least privileged access to their customers' tenants. This feature gives extra control to customers over their security posture while allowing them to receive support from the Microsoft resellers	See Granular delegated admin privileges (GDAP) API overview

Identity and access reports

Microsoft Entra records *every* activity in your tenant and produces reports and audit logs that you can analyze for monitoring, compliance, and troubleshooting. Records of these activities are also available through Microsoft Graph reporting and audit logs APIs, which allow you to analyze the activities with Azure Monitor logs and Log Analytics, or stream to third-party SIEM tools for further investigations. For more information, see [Identity and access reports API overview](#).

Zero Trust

This feature helps organizations to align their tenants with the three guiding principles of a Zero Trust architecture:

- Verify explicitly
- Use least privilege
- Assume breach

To find out more about Zero Trust and other ways to align your organization to the guiding principles, see the [Zero Trust Guidance Center](#).

Licensing

Microsoft Entra licenses include Microsoft Entra ID Free, P1, P2, and Governance; Microsoft Entra Permissions Management; and Microsoft Entra Workload ID.

For detailed information about licensing for different features, see [Microsoft Entra ID licensing](#).

Related content

- [Implement identity standards with Microsoft Entra ID](#)
- [Microsoft Entra ID Guide for independent software developers](#)
- Review the [Microsoft Entra deployment plans](#) to help you build your plan to deploy the Microsoft Entra suite of capabilities.

Add custom data to resources using extensions

Article • 10/30/2024

Microsoft Graph provides a single API endpoint to access rich people-centric data and insights through resources such as [user](#) and [message](#). You can also extend Microsoft Graph by adding custom properties to resource instances without requiring an external data store.

This article describes how Microsoft Graph supports extending its resources, the options available to add custom properties, and when to use them.

Important

Do not use extensions to store sensitive personally identifiable information, such as account credentials, government identification numbers, cardholder data, financial account data, healthcare information, or sensitive background information.

The extensions mentioned in this article are not similar to the following features:

- [Custom security attributes](#). To understand their differences, see [How do custom security attributes compare with extensions?](#)
- [Custom authentication extensions](#) that are supported for token customization and extending authentication flows.

Why add custom data to Microsoft Graph?

- As an ISV developer, you might decide to keep your app lightweight and store app-specific user profile data in Microsoft Graph by extending the [user](#) resource.
- Alternatively, you might want to retain your app's existing user profile store, and add an app-specific identifier to the [user](#) resource.
- As an enterprise developer, the in-house applications that you build might rely on your organization's HR-specific data. Integration within multiple applications can be simplified by storing this custom data in Microsoft Graph.

Custom data options in Microsoft Graph

Microsoft Graph offers four types of extensions for adding custom data.

- Extension attributes
- Directory (Microsoft Entra ID) extensions
- Schema extensions
- Open extensions

Extension attributes

Microsoft Entra ID offers a set of 15 extension attributes with predefined names on the [user](#) and [device](#) resources. These properties were initially custom attributes provided in on-premises Active Directory (AD) and Microsoft Exchange. However, they can now be used for more than syncing on-premises AD and Microsoft Exchange data to Microsoft Entra ID through Microsoft Graph.

For more information about these attributes in Microsoft Exchange, see [Custom attributes in Exchange Server](#).

Developer experience

You can use the 15 extension attributes to store String values on [user](#) or [device](#) resource instances, through the **onPremisesExtensionAttributes** and **extensionAttributes** properties respectively. You can assign the values while creating a new resource instance or while updating an existing resource instance. You can also filter by the values.

Add or update data in extension attributes

The following example shows how to store data in **extensionAttribute1** and delete existing data from **extensionAttribute13** through an update operation with a PATCH method.

```
HTTP  
  
HTTP  
  
PATCH https://graph.microsoft.com/v1.0/users/071cc716-8147-4397-a5ba-b2105951cc0b  
  
{  
    "onPremisesExtensionAttributes": {  
        "extensionAttribute1": "skypeId.adeleVance",  
        "extensionAttribute13": null  
    }  
}
```

The request returns a `204 No Content` response object.

Read the extension attributes

Request

```
HTTP  
msgraph  
GET https://graph.microsoft.com/v1.0/users?  
$select=id,displayName,onPremisesExtensionAttributes
```

Response

```
HTTP  
{  
    "@odata.context":  
    "https://graph.microsoft.com/v1.0/$metadata#users(id,displayName,onPremisesE  
xtensionAttributes)",  
    "value": [  
        {  
            "id": "071cc716-8147-4397-a5ba-b2105951cc0b",  
            "displayName": "Adele Vance",  
            "onPremisesExtensionAttributes": {  
                "extensionAttribute1": "Contractor",  
                "extensionAttribute2": "50",  
                "extensionAttribute3": null,  
                "extensionAttribute4": "1478354",  
                "extensionAttribute5": "10239390",  
                "extensionAttribute6": null,  
                "extensionAttribute7": null,  
                "extensionAttribute8": null,  
                "extensionAttribute9": null,  
                "extensionAttribute10": "11",  
                "extensionAttribute11": null,  
                "extensionAttribute12": "/o=ExchangeLabs/ou=Exchange  
Administrative Group  
(FYDIBOHF47SPDLT)/cn=Recipients/cn=5ee781fc7egc7aa0b9394bddb44e7f04-Adele  
Vance",  
                "extensionAttribute13": null,  
                "extensionAttribute14": null,  
                "extensionAttribute15": null  
            }  
        }  
    ]
```

```
    ]  
}
```

Considerations for using extension attribute properties

The `onPremisesExtensionAttributes` object can be updated only for objects that aren't synced from on-premises AD.

The 15 extension attributes are already predefined in Microsoft Graph and their property names can't be changed. Therefore, you can't use custom names such as `SkypeId` for the extension attributes. Your organization must therefore track the extension attribute properties in use to avoid inadvertently overwriting their data.

Directory (Microsoft Entra ID) extensions

Directory extensions provide developers with a strongly typed, discoverable and filterable extension experience for directory objects.

Directory extensions are first registered on an application through the [Create extensionProperty](#) operation and must be explicitly targeted to specific and supported directory objects. After a user or an admin has consented to the application in the tenant, the extension properties become immediately accessible in the tenant. All authorized applications in the tenant can read and write data on any extension properties defined on an instance of the target directory object.

For the list of resource types that can be specified as target objects for a directory extension, see [Comparison of extension types](#).

Developer experience

Directory extension definitions are managed through the `extensionProperty` resource and its associated methods. The data is managed through the REST API requests that you use to manage the resource instance.

Define the directory extension

Before you can add a directory extension to a resource instance, you must first define the directory extension.

Request

In the following request, `30a5435a-1871-485c-8c7b-65f69e287e7b` is the object ID of the application that owns the directory extension. You can create directory extensions that store a collection of values.

HTTP

```
HTTP

POST https://graph.microsoft.com/v1.0/applications/30a5435a-1871-485c-8c7b-65f69e287e7b/extensionProperties

{
    "name": "jobGroupTracker",
    "dataType": "String",
    "targetObjects": [
        "User"
    ]
}
```

Response

A directory extension property named

`extension_b7d8e648520f41d3b9c0fdeb91768a0a_jobGroupTracker` is created with an extension name that follows the following naming convention: *extension_{appId-without-hyphens}_{extensionProperty-name}*.

HTTP

```
HTTP/1.1 201 Created
Content-type: application/json

{
    "@odata.context":
    "https://graph.microsoft.com/v1.0/$metadata#applications('30a5435a-1871-485c-8c7b-65f69e287e7b')/extensionProperties/$entity",
    "id": "4e3dbc8f-ca32-41b4-825a-346215d7d20f",
    "deletedDateTime": null,
    "appDisplayName": "HR-sync-app",
    "dataType": "String",
    "isMultiValued": false,
    "isSyncedFromOnPremises": false,
    "name": "extension_b7d8e648520f41d3b9c0fdeb91768a0a_jobGroupTracker",
    "targetObjects": [
        "User"
    ]
}
```

Add a directory extension property to a target object

After defining the directory extension, you can now add it to an instance of a target object type. You can store data in the directory extension when creating a new instance of the target object or when updating an existing object. The following example shows how to store data in the directory extension when creating a new `user` object.

HTTP

```
msgraph
POST https://graph.microsoft.com/v1.0/users

{
    "accountEnabled": true,
    "displayName": "Adele Vance",
    "mailNickname": "AdeleV",
    "userPrincipalName": "AdeleV@contoso.com",
    "passwordProfile": {
        "forceChangePasswordNextSignIn": false,
        "password": "xWwvJ]6NMw+bWH-d"
    },
    "extension_b7d8e648520f41d3b9c0fdeb91768a0a_jobGroupTracker": "JobGroupN"
}
```

The request returns a `201 Created` response code and a `user` object in the response body.

Retrieve a directory extension

The following example shows how the directory extensions and associated data are presented on a resource instance. The extension property is returned by default through the `beta` endpoint, but only on `$select` through the `v1.0` endpoint.

Request

HTTP

```
msgraph
GET https://graph.microsoft.com/beta/users?
$select=id,displayName,extension_b7d8e648520f41d3b9c0fdeb91768a0a_jobGro
```

```
upTracker,extension_b7d8e648520f41d3b9c0fdeb91768a0a_permanent_pensionable
```

Response

HTTP

HTTP/1.1 200 OK

Content-type: application/json

```
{
    "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#users(id,displayName,extension_b7d8e648520f41d3b9c0fdeb91768a0a_jobGroupTracker,extension_b7d8e648520f41d3b9c0fdeb91768a0a_permanent_pensionable)",
    "value": [
        {
            "id": "63384f56-42d2-4aa7-b1d6-b10c78f143a2",
            "displayName": "Adele Vance",
            "extension_b7d8e648520f41d3b9c0fdeb91768a0a_jobGroupTracker": "E4",
            "extension_b7d8e648520f41d3b9c0fdeb91768a0a_permanent_pensionable": true
        }
    ]
}
```

Update or delete directory extensions

To update or delete the value of the directory extension for a resource instance, use the PATCH method. To delete the extension property and its associated value, set its value to `null`.

The following request updates the value of one directory extension and deletes another extension property.

HTTP

HTTP

```
PATCH https://graph.microsoft.com/v1.0/users/63384f56-42d2-4aa7-b1d6-b10c78f143a2
```

```
{
    "extension_b7d8e648520f41d3b9c0fdeb91768a0a_permanent_pensionable": null,
```

```
        "extension_b7d8e648520f41d3b9c0fdeb91768a0a_jobGroupTracker": "E4"  
    }
```

The request returns a `204 No Content` response code.

Considerations for using directory extensions

If you accidentally delete a directory extension definition, any data stored in the associated property becomes undiscoverable. To recover the data, create a new directory extension definition with the same name as the deleted definition, on the same owner app.

When a definition object is deleted before the corresponding extension property is updated to `null`, the property counts against the 100-limit for the object.

When the definition is deleted before data in the associated extension property is deleted, there's no way to know the existence of the extension property via Microsoft Graph - even though the undiscoverable property counts against the 100-limit.

Deleting an owner app in the home tenant makes the associated directory extensions and their data undiscoverable. When you restore an owner app, it restores the directory extension definitions *but doesn't* make the directory extension properties or their data immediately discoverable; because restoring an app doesn't automatically restore the associated service principal in the tenant. To make the directory extension properties and their data discoverable, either create a new service principal or restore the deleted service principal. NO changes are made to other tenants where the app has been consented to.

Schema extensions

[Microsoft Graph schema extensions](#) are conceptually similar to directory extensions. First, you define your schema extension. Then, use it to extend supported resource instances with strongly typed custom properties. In addition, you can control the [status](#) of your schema extension and let it be discoverable by other apps.

For the list of resource types that support schema extensions, see [Comparison of extension types](#).

[https://www.youtube-nocookie.com/embed/3MOAIUFNus0 ↗](https://www.youtube-nocookie.com/embed/3MOAIUFNus0)

Developer experience

When creating a schema extension definition, you must provide a unique name for its **id**. There are two naming options:

- If you already have a vanity `.com`, `.net`, `.gov`, `.edu`, or a `.org` domain that's verified with your tenant, you can use the domain name along with the schema name to define a unique name, in this format `{domainName}_{schemaName}`. For example, if your vanity domain is `contoso.com`, you can define an **id** of `contoso_mySchema`. This option is highly recommended.
- Alternatively, you can set the **id** to a schema name (without a domain name prefix). For example, `mySchema`. Microsoft Graph assigns a string ID for you based on the supplied name, in this format: `ext{8-random-alphanumeric-chars}_{schema-name}`. For example, `extkvbmkofy_mySchema`.

The **id** is the name of the complex type that stores your data on the extended resource instance.

After you register a schema extension, it's available for use by all applications in the same tenant as the associated owner application (when in the `InDevelopment` state) or by all applications in any tenant (when in the `Available` state). Like directory extensions, authorized apps have the ability to read and write data on any extensions defined on the target object.

You manage the [schema extension definitions](#) and the data in the corresponding schema extension property by using separate sets of API operations. To manage the schema extension data on the extended resource instance, use the same REST request that you use to manage the resource instance.

- Use POST to store data in the schema extension property when you're creating a new user.
- Use PATCH to either store data in the schema extension property or update or delete the stored data.
 - To delete data from a property, set its value to `null`.
 - To delete data from *all* properties, set every property to `null`. If all properties are `null`, the schema extension object is also deleted.
 - To update any property, specify only the changed properties in the request body. Omitted properties are not updated and retain their previous value.
- Use GET to read the schema extension properties for all users or individual users in the tenant.

Define a schema extension

Request

HTTP

```
msgraph

POST https://graph.microsoft.com/v1.0/schemaExtensions

{
    "id": "graphLearnCourses",
    "description": "Graph Learn training courses extensions",
    "targetTypes": [
        "user"
    ],
    "properties": [
        {
            "name": "courseId",
            "type": "Integer"
        },
        {
            "name": "courseName",
            "type": "String"
        },
        {
            "name": "courseType",
            "type": "String"
        }
    ]
}
```

Response

HTTP

```
{
    "@odata.context": "https://graph.microsoft.com/beta/$metadata#schemaExtensions/$entity",
    "id": "extkmpdyld2_graphLearnCourses",
    "description": "Graph Learn training courses extensions",
    "targetTypes": [
        "user"
    ],
    "status": "InDevelopment",
    "properties": [
        {
            "name": "courseId",
            "type": "Integer"
        },
        {
            "name": "courseName",
            "type": "String"
        }
    ]
}
```

```
        "type": "String"
    },
{
    "name": "courseType",
    "type": "String"
}
]
}
```

Add a schema extension to a resource instance

After defining the schema extension, you can now add the extension property to an instance of a target object type. You can store data in the schema extension when creating a new instance of the target object or when updating an existing object. The following example shows how to store data in the schema extension property when creating a new user object.

HTTP

HTTP

POST https://graph.microsoft.com/beta/users

```
{
    "accountEnabled": true,
    "displayName": "Adele Vance",
    "mailNickname": "AdeleV",
    "userPrincipalName": "AdeleV@contoso.com",
    "passwordProfile": {
        "forceChangePasswordNextSignIn": false,
        "password": "xWwvJ]6NMw+bWH-d"
    },
    "extkmpdyld2_graphLearnCourses": {
        "courseId": 100,
        "courseName": "Explore Microsoft Graph",
        "courseType": "Online"
    }
}
```

The request returns a `201 Created` response code and a `schemaExtension` object in the response body

Update or delete a schema extension property

Use the PATCH operation to update a schema extension or delete an existing schema extension. To delete the extension property and its associated value from the resource instance, set its value to `null`.

The following example deletes the value of the `courseId` property and updates the `courseType` property. To delete the `extkmpdyld2_graphLearnCourses` extension property in its entirety, set its value to `null`.

HTTP

```
PATCH https://graph.microsoft.com/beta/users/0668e673-908b-44ea-861d-0661297e1a3e

{
    "extkmpdyld2_graphLearnCourses": {
        "courseType": "Instructor-led",
        "courseId": null
    }
}
```

The request returns a `204 No Content` response object.

Retrieve the schema extension property

To read the schema extension properties on a resource instance, specify the extension name in a `$select` request.

Request

HTTP

```
msgraph

GET https://graph.microsoft.com/beta/users/0668e673-908b-44ea-861d-0661297e1a3e?$select=id,displayName,extkmpdyld2_graphLearnCourses
```

Response

HTTP

```
HTTP/1.1 200 OK
Content-type: application/json

{
    "@odata.context": "https://graph.microsoft.com/beta/$metadata#users(id,displayName,extkmpdyld2_graphLearnCourses)/$entity",
    "id": "63384f56-42d2-4aa7-b1d6-b10c78f143a2",
    "displayName": "Adele Vance",
    "extkmpdyld2_graphLearnCourses": {
        "@odata.type": "#microsoft.graph.ComplexExtensionValue",
        "courseType": "Instructor-led",
        "courseName": "Explore Microsoft Graph",
        "courseId": null
    }
}
```

Considerations for using schema extensions

A schema extension must have an owner app. Ownership of the schema extension can't be reassigned to another app.

Deleting a schema extension definition without setting the schema extension to `null` makes the property and its associated user data undiscoverable.

Deleting an owner app in the home tenant doesn't delete the associated schema extension definition or the property and the data it stores. The schema extension property can still be read, deleted, or updated for users. However, the schema extension definition can't be updated.

Open extensions

Microsoft Graph open extensions are [open types](#) that offer a simple and flexible way to add untyped data directly to a resource instance. These extensions aren't strongly typed, discoverable, or filterable.

For the list of resource types that support Microsoft Graph open extensions, see [Comparison of extension types](#).

<https://www.youtube-nocookie.com/embed/ibdlADb8lZc>

Developer experience

Open extensions, together with their data, are accessible through the `extensions` navigation property of the resource instance. They allow you to group related properties

for easier access and management.

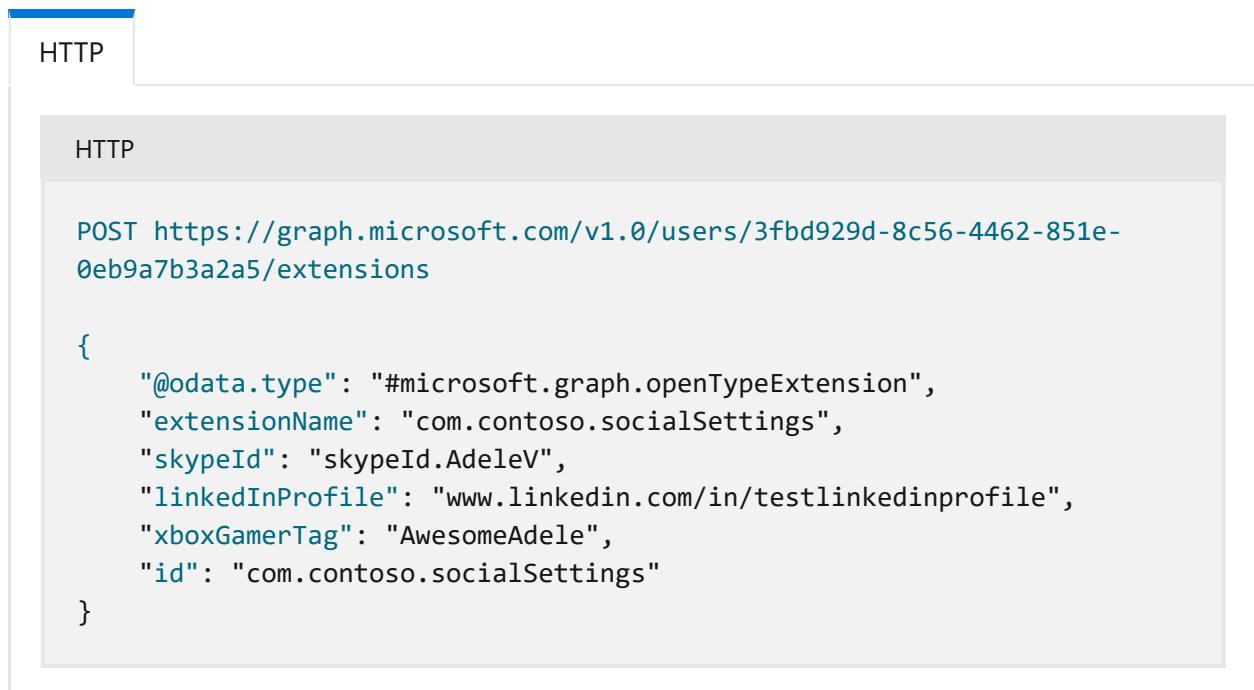
You define and manage open extensions on the fly on resource instances. They're considered unique for each object, and you don't need to apply a universally consistent pattern for all objects. For example, in the same tenant:

- The user object for Adele can have an open extension named *socialSettings* that has three properties: **linkedInProfile**, **skypeId**, and **xboxGamertag**.
- The user object for Bruno can have no open extension property.
- The user object for Alex can have an open extension named *socialSettings* with five properties: **theme**, **color**, **language**, **font**, and **fontSize**.

Additionally, open extension properties can have any valid JSON structure.

Create an open extension

The following example shows an open extension definition with three properties and how the custom properties and associated data are presented on a resource instance.



The screenshot shows a browser's developer tools Network tab with an "HTTP" filter selected. A single request is visible, labeled "HTTP". The request method is "POST", the URL is "https://graph.microsoft.com/v1.0/users/3fbd929d-8c56-4462-851e-0eb9a7b3a2a5/extensions", and the body contains the following JSON:

```
POST https://graph.microsoft.com/v1.0/users/3fbd929d-8c56-4462-851e-0eb9a7b3a2a5/extensions

{
    "@odata.type": "#microsoft.graph.openTypeExtension",
    "extensionName": "com.contoso.socialSettings",
    "skypeId": "skypeId.AdeleV",
    "linkedInProfile": "www.linkedin.com/in/testlinkedinprofile",
    "xboxGamerTag": "AwesomeAdele",
    "id": "com.contoso.socialSettings"
}
```

The request returns a `201 Created` response code and an `openTypeExtension` object in the response body.

Update an existing open extension

To update an open extension, you must specify all its properties in the request body. Otherwise, the unspecified properties are deleted from the open extension. You can however explicitly set a property to `null` to retain it in the open extension.

The following request specifies only the `linkedInProfile` and `xboxGamerTag` properties. The value of the `xboxGamerTag` property is being updated while the `linkedInProfile` property remains the same. This request also deletes the unspecified `skypeId` property.

```
HTTP  
  
HTTP  
  
PATCH https://graph.microsoft.com/v1.0/users/3fb929d-8c56-4462-851e-0eb9a7b3a2a5/extensions/com.contoso.socialSettings  
  
{  
    "xboxGamerTag": "FierceAdele",  
    "linkedInProfile": "www.linkedin.com/in/testlinkedinprofile"  
}
```

This request returns a `204 No Content` response code.

Retrieve the open extensions

```
HTTP  
  
msgraph  
  
GET https://graph.microsoft.com/v1.0/users/3fb929d-8c56-4462-851e-0eb9a7b3a2a5/extensions/com.contoso.socialSettings  
  
{  
    "@odata.context":  
    "https://graph.microsoft.com/beta/$metadata#users('3fb929d-8c56-4462-851e-0eb9a7b3a2a5')/extensions/$entity",  
    "@odata.type": "#microsoft.graph.openTypeExtension",  
    "xboxGamerTag": "FierceAdele",  
    "linkedInProfile": "www.linkedin.com/in/testlinkedinprofile",  
    "id": "com.contoso.socialSettings"  
}
```

Considerations for using open extensions

Deleting a creator app doesn't affect the open extension and the data it stores.

Comparison of extension types

The following table compares the extension types, which should help you decide which option is most appropriate for your scenario.

[Expand table](#)

Capability	Extension attributes 1-15	Directory extensions	Schema extensions	Open extensions
Supported resource types	user device	user group administrativeUnit application device organization	user group administrativeUnit contact device event ¹ (both user and group calendars) message organization post	user group contact device event ¹ (both user and group calendars) message organization post todoTask todoTaskList
Strongly typed	No	Yes	Yes	No
Filterable	Yes	Yes	Yes	No
Can store a collection	No	Yes	No	Yes
Tied to an "owner" application	No	Yes	Yes	No
Managed via	Microsoft Graph Exchange admin center	Microsoft Graph	Microsoft Graph	Microsoft Graph
Sync data from on-premises to extensions using AD connect	Yes, for users	Yes	No	No
Create dynamic membership rules using custom extension	Yes	Yes	No	No

Capability	Extension attributes 1-15	Directory extensions	Schema extensions	Open extensions
properties and data				
Usable for customizing token claims	Yes	Yes (1, 2)	No	No
Available in Azure AD B2C	Yes	Yes	Yes	Yes
Available in Microsoft Entra External ID	Yes	Yes	Yes	Yes
Limits	<ul style="list-style-type: none"> • 15 predefined attributes per user or device resource instance 	<ul style="list-style-type: none"> • 100 extension values per resource instance 	<ul style="list-style-type: none"> • Maximum of five definitions per owner app • 100 extension values per resource instance (directory objects only) 	<ul style="list-style-type: none"> • Two open extensions per creator app per resource instance² • Max. of 2 Kb per open extension² • For Outlook resources, each open extension is stored in a MAPI named property³

ⓘ Note

¹ Due to an existing service limitation, delegates cannot create open extension-appended events in shared mailbox calendars. Attempts to do so will result in an `ErrorAccessDenied` response.

² These limits on open extensions apply to the following directory resources: **user**, **group**, **device**, and **organization**.

³ Each **open extension** is stored in a [MAPI named property](#), which are a limited resource in a user's mailbox. This limit applies to the following Outlook resources: **message**, **event**, and **contact**

You can manage all extensions when you're signed in with a work or school account. Additionally, you can manage open extensions for the following resources

when signed-in with a personal Microsoft account: **event**, **post**, **group**, **message**, **contact**, and **user**.

Permissions and privileges

The same privileges that your app requires to read from or write to a resource instance are also required to manage any extensions data on that resource instance. For example, in a delegated scenario, an app can only update any user's extension data if it's granted the *User.ReadWrite.All* permission and the signed-in user has a supported Microsoft Entra administrator role.

Related content

- [Tutorial: Add custom data to users using open extensions](#)
- [Tutorial: Add custom data to groups using schema extensions](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)

Frontline worker management

Article • 03/21/2025

Frontline workers account for over 80 percent of the global workforce. Yet because of high scale, rapid turnover, and fragmented processes, frontline workers often lack the tools to make their demanding jobs a little easier. Frontline worker management brings digital transformation to the entire frontline workforce. The workforce might include managers, frontline workers, operations, and IT.

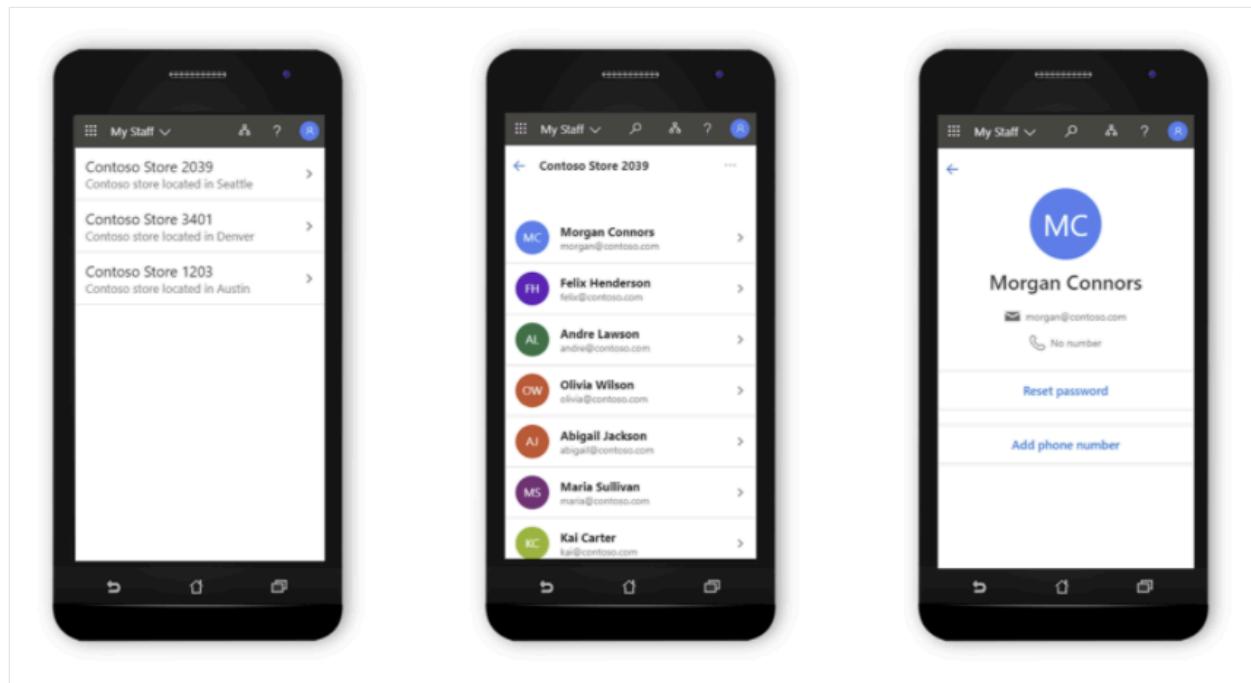
Frontline worker management empowers the frontline workforce by making the following activities easier to accomplish:

- Streamlining common IT tasks with My Staff
- Easy onboarding of frontline workers through simplified authentication
- Seamless provisioning of shared devices and secure sign-out of frontline workers

Delegated user management through My Staff

Microsoft Entra ID in the My Staff portal enables delegation of user management.

Frontline managers can save valuable time and reduce risks using the [My Staff portal](#). When an administrator enables simplified password resets and phone management directly from the store or factory floor, managers can grant access to employees without routing the request through the help-desk, IT, or operations.

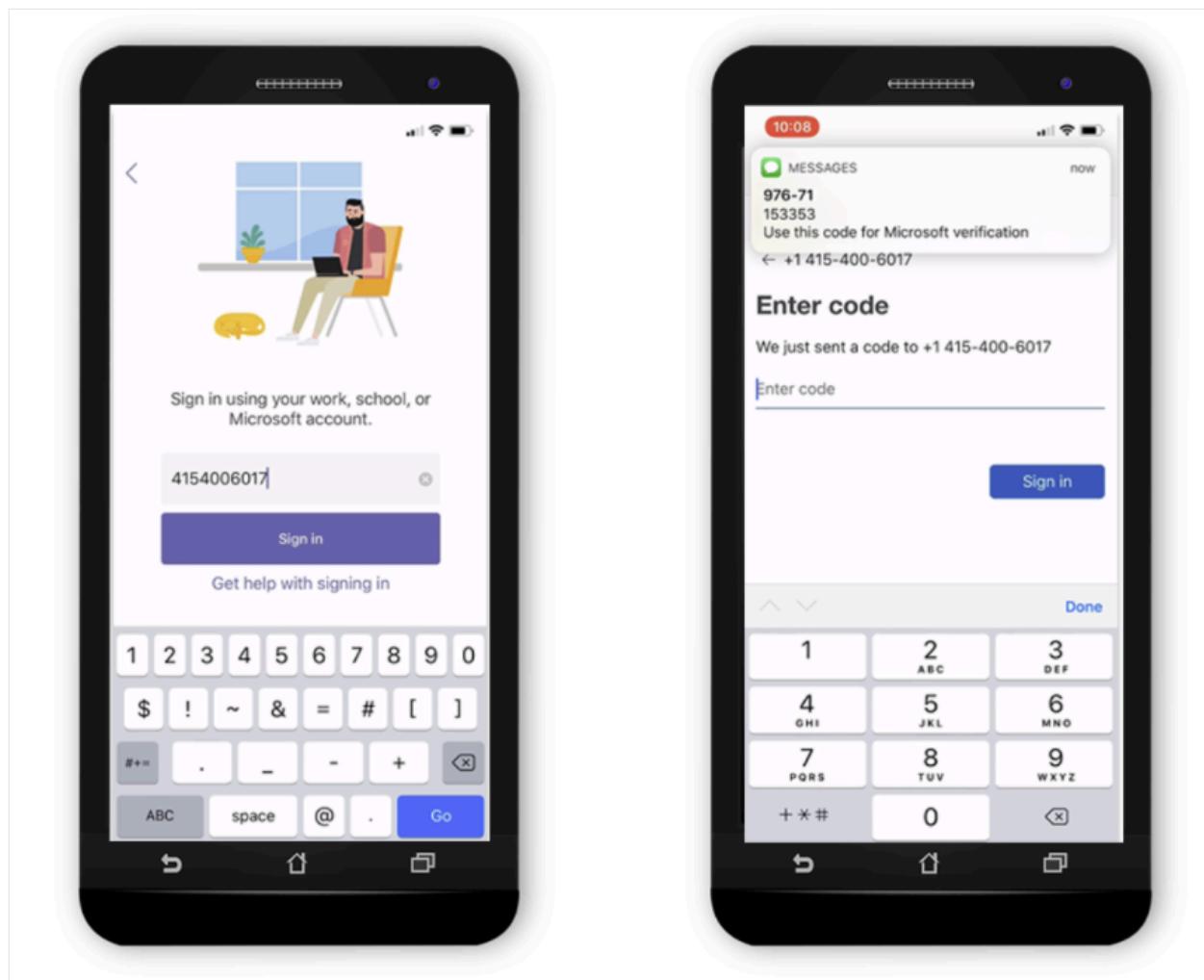


Accelerated onboarding with simplified authentication

Frontline workers often need quick and easy access to tools and information. Microsoft Entra ID provides accelerated onboarding with simplified authentication to meet this need. Frontline workers can use SMS sign-in or QR code sign-in to access their devices and applications easily.

SMS authentication

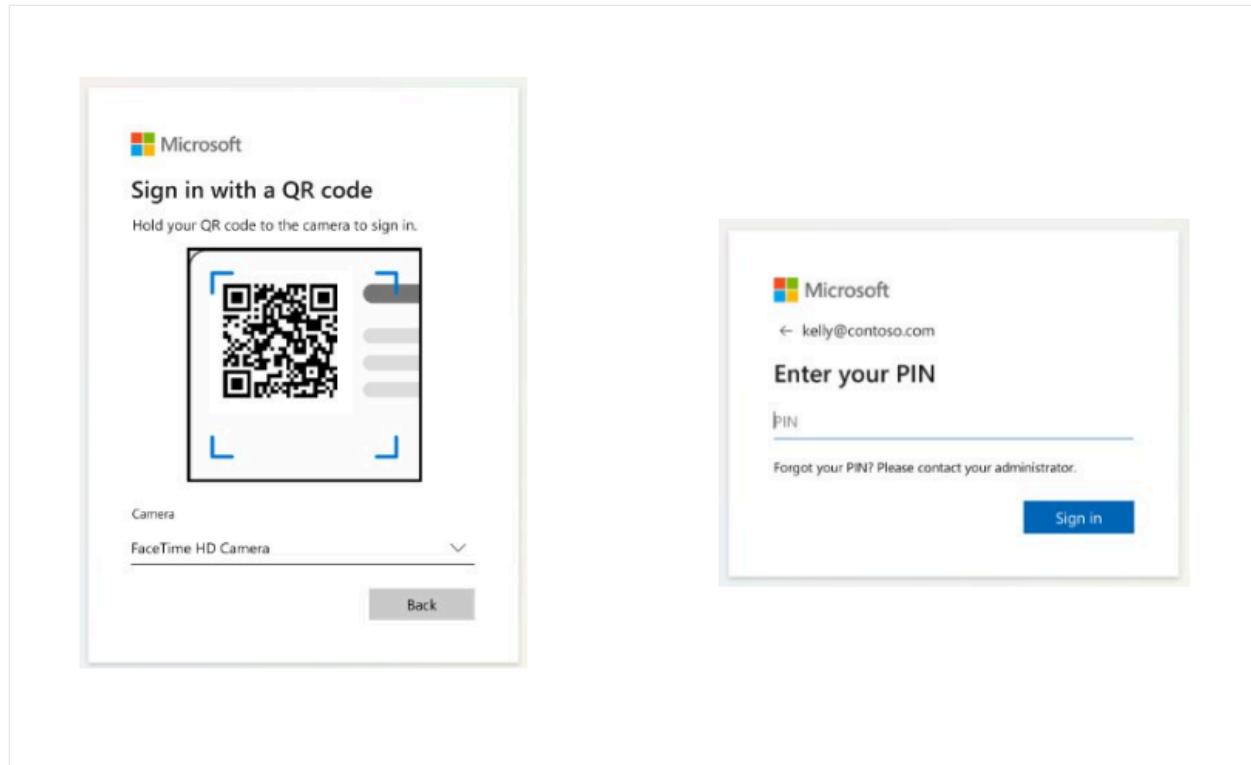
My Staff also enables frontline managers to register their team members' phone numbers for [SMS sign-in](#). In many verticals, frontline workers maintain a local username and password combination, a solution that is often cumbersome, expensive, and error-prone. When IT enables authentication using SMS sign-in, frontline workers can sign in with [single sign-on \(SSO\)](#) for Microsoft Teams and other applications using just their phone number and a one-time passcode (OTP) sent via SMS. Single sign-on makes signing in for frontline workers simple and secure, delivering quick access to the apps they need most.



QR code authentication (preview)

QR code authentication provides a fast and cost-effective way to sign in, improving productivity and offering a seamless experience for frontline workers. This method uses a QR code and a user-defined 8-digit PIN. You use the QR code and PIN together to sign in to a device or application.

The QR code includes a User Principal Name (UPN), tenant ID, and a secret key. You set the PIN, which replaces the default temporary PIN assigned by the administrator. The PIN works only with the QR code and not with other identifiers like UPN or phone numbers. You also can't use the QR code without the PIN.



The QR code authentication method offers two main advantages for frontline workers compared to traditional methods:

- **Faster sign-in:** QR code authentication eliminates the need for usernames and passwords, which benefits users who are less tech-savvy or have accessibility challenges. Scanning a QR code reduces login time by about two seconds, enhancing worker productivity. It also decreases IT tickets related to forgotten usernames, as users don't need to remember them for sign-in.
- **Cost-effective:** Printing QR codes is cheaper than providing hardware keys and workers can attach the QR code to a badge or wearable. Organizations prefer this method because frontline workers often hold temporary positions and may not return, reducing the risk of investment loss in costly devices.

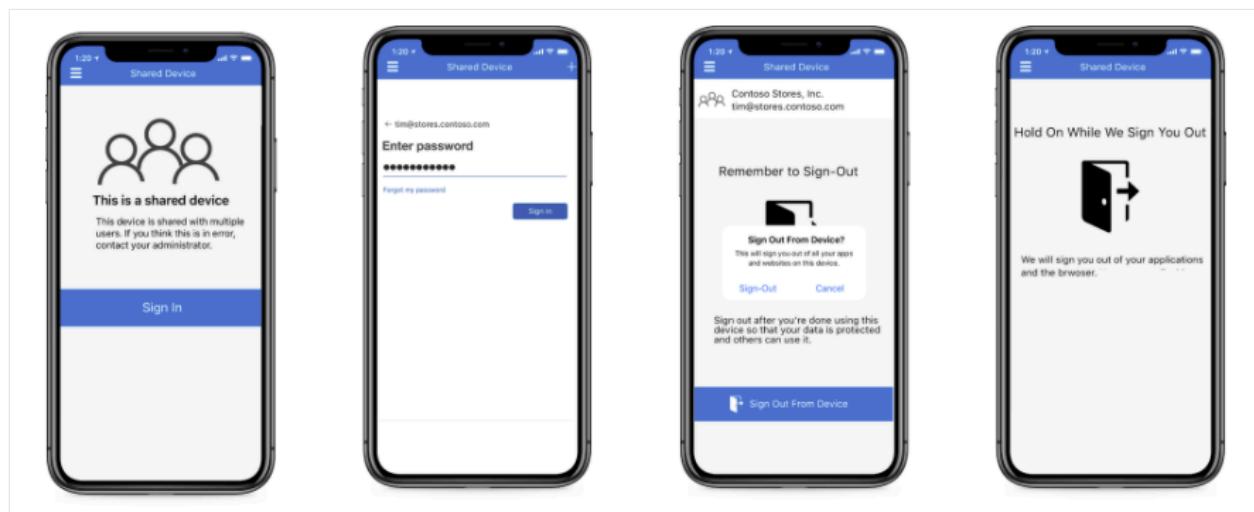
Learn more about [QR code authentication](#) and how to [enable it](#) for your organization.

Shared devices for frontline workers

Frontline managers can also use Managed Home Screen (MHS) application to allow workers to have access to a specific set of applications on their Intune-enrolled Android dedicated devices. The dedicated devices are enrolled with [Microsoft Entra shared device mode](#). When configured in multiapp kiosk mode in the Microsoft Intune admin center, MHS is automatically launched as the default home screen on the device and appears to the end user as the *only* home screen. To learn more, see how to [configure the Microsoft Managed Home Screen app for Android Enterprise](#).

Secure sign-out of frontline workers from shared devices

Frontline workers in many companies use shared devices to do inventory management and sales transactions. Sharing devices reduces the IT burden of provisioning and tracking them individually. With shared device sign-out, it's easy for a frontline worker to securely sign out of all apps on any shared device before handing it back to a hub or passing it off to a teammate on the next shift. Frontline workers can use Microsoft Teams to view their assigned tasks. Once a worker signs out of a shared device, Intune and Microsoft Entra ID clear all of the company data so the device can safely be handed off to the next associate. You can choose to integrate this capability into all your line of business [iOS](#) and [Android](#) apps using the [Microsoft Authentication Library](#).



Next steps

- For more information on delegated user management, see [My Staff user documentation](#).
- To learn more about the frontline worker persona, see [this article](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)