

Enterprise user management documentation

Microsoft Entra ID provides user management services so that you can assign licenses, manage your groups and users, and add or manage domain names.

About enterprise user management

OVERVIEW

[Users, groups, domains, and licenses](#)

[Custom roles overview](#)

CONCEPT

[Microsoft Entra organizational independence](#)

[Manage access using groups](#)

Get started

QUICKSTART

[Add a user](#)

[Set expiration policy for groups](#)

[Assign licenses to users](#)

Manage Microsoft Entra domain names

HOW-TO GUIDE

[Add your custom domain name](#)

[Managing custom domain names](#)

Manage groups

 **HOW-TO GUIDE**

[Create a dynamic group](#)

[Group settings in PowerShell](#)

[Set naming policy for groups](#)

Add domains

 **HOW-TO GUIDE**

[Add a custom domain name](#)

[Managing custom domain names](#)

What is enterprise user management?

Article • 01/31/2025

This article introduces an administrator for Microsoft Entra ID, part of Microsoft Entra, to the relationship between top [identity management](#) tasks for users in terms of their groups, licenses, deployed enterprise apps, and administrator roles. As your organization grows, you can use Microsoft Entra groups and administrator roles to:

- Assign licenses to groups instead of assigning licenses to individual users.
- Grant permissions to delegate Microsoft Entra management work to personnel in less-privileged roles.
- Assign enterprise app access to groups.

Assign users to groups

You can use groups in Microsoft Entra ID to assign licenses, or deployed enterprise apps, to large numbers of users. You can also use groups to assign all administrator roles except for Microsoft Entra Global Administrator, or you can grant access to external resources, such as SaaS applications or SharePoint sites.

You can use [dynamic membership groups](#) in Microsoft Entra ID to expand and contract dynamic membership groups automatically. Dynamic groups give you greater flexibility and they reduce dynamic membership group management work.

Note

You need a Microsoft Entra ID P1 license for each unique user that is a member of one or more dynamic membership groups.

Assign licenses to groups

Managing user license assignments individually is time consuming and error prone. If you [assign licenses to groups](#) instead, you experience easier large-scale license management.

Microsoft Entra users who join a licensed group are automatically assigned the appropriate licenses. When users leave the group, Microsoft Entra ID removes their license assignments. Without Microsoft Entra groups, you'd have to write a PowerShell script or use Graph API to bulk add or remove user licenses for users joining or leaving

the organization. For more information about group bulk operations, see [Bulk upload to add or create members of a group](#).

If there aren't enough licenses available, or an issue occurs like service plans that can't be assigned at the same time, you can see the status of any licensing issue for the group in the Azure portal.

Delegate administrator roles

Many large organizations want options for their users to obtain sufficient permissions for their work tasks without assigning the powerful Global Administrator role to, for example, users who must register applications. Here's an example of new Microsoft Entra administrator roles to help you distribute the work of application management with more specificity:

[] [Expand table](#)

Role name	Permissions summary
Application Administrator	Can add and manage enterprise applications and application registrations, and configure proxy application settings. Application Administrators can view Conditional Access policies and devices, but not manage them.
Cloud Application Administrator	Can add and manage enterprise applications and enterprise app registrations. This role has all of the permissions of the Application Administrator, except it can't manage application proxy settings.
Application Developer	Can add and update application registrations, but can't manage enterprise applications or configure an application proxy.

New Microsoft Entra administrator roles are being added. Check the Azure portal or the [administrator role permission reference](#) for current available roles.

Assign app access

You can use Microsoft Entra ID to assign group access to [enterprise apps deployed in your Microsoft Entra organization](#). If you combine dynamic membership groups with group assignment to apps, you can automate user app access assignments as your organization grows. You need a Microsoft Entra ID P1 or Premium P2 license to assign access to enterprise apps.

Microsoft Entra ID also gives you specific control of the data that flows between the app and the groups to whom you assign access. In [Enterprise Applications](#), open an app

and select **Provisioning** to:

- Set up automatic provisioning for apps that support it
- Provide credentials to connect to the app's user management API
- Set up the mappings that control which user attributes flow between Microsoft Entra ID and the app when user accounts are provisioned or updated
- Start and stop the Microsoft Entra provisioning service for an app, clear the provisioning cache, or restart the service
- View the **Provisioning activity report** that provides a log of all users and groups created, updated, and removed between Microsoft Entra ID and the app, and the **Provisioning error report** that provides more detailed error messages

Next steps

If you're a beginning Microsoft Entra administrator, get the basics down in [Microsoft Entra Fundamentals](#).

Or you can start [creating groups](#), [assigning licenses](#), [assigning app access](#) or [assigning administrator roles](#).

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#) ↗

What is delegated administration?

Article • 12/13/2024

Managing permissions for external partners is a key part of your security posture. We've added capabilities to the administrator portal experience in Microsoft Entra ID, part of Microsoft Entra, so that an administrator can see the relationships that their Microsoft Entra tenant has with Microsoft Cloud Service Providers (CSP) who can manage the tenant. This permissions model is called delegated administration. This article introduces the Microsoft Entra administrator to the relationship between the old Delegated Admin Permissions (DAP) permission model and the new [Granular Delegated Admin Permissions \(GDAP\)](#) permission model.

Delegated administration relationships

Delegated administration relationships enable technicians at a Microsoft CSP to administer Microsoft services such as Microsoft 365, Dynamics 365, and Azure on behalf of your organization. These technicians administer these services for you using the same roles and permissions as your organization's own administrators. These roles are assigned to security groups in the CSP's Microsoft Entra tenant, which is why CSP technicians don't need user accounts in your tenant in order to administer services for you.

There are two types of delegated administration relationships that are visible in the Azure portal experience. The newer type of delegated admin relationship is known as Granular Delegated Admin Permission. The older type of relationship is known as Delegated Admin Permission. You can see both types of relationship if you sign in to the Azure portal and then select **Delegated administration**.

Granular delegated admin permission

When a Microsoft CSP creates a GDAP relationship request for your tenant, a Global Administrator needs to approve the request. The GDAP relationship request specifies:

- The CSP partner tenant
- The roles that the partner needs to delegate to their technicians
- The expiration date

If you have GDAP relationships in your tenant, you see a notification banner on the **Delegated Administration** page in the Microsoft Entra admin center. Select the

notification banner to see and manage GDAP relationships in the [Partners](#) page in Microsoft Admin Center.

Delegated admin permission

All DAP relationships enable the CSP to delegate Global Administrator and Helpdesk Administrator roles to their technicians. Unlike a GDAP relationship, a DAP relationship persists until you or your CSP revokes them.

If you have any DAP relationships in your tenant, you can see them in the list on the Delegated Administration page in the Azure portal. To remove a DAP relationship for a CSP, follow the link to the Partners page in the Microsoft Admin Center.

Next steps

If you're a beginning Microsoft Entra administrator, get the basics down in [Microsoft Entra Fundamentals](#).

- [Delegated administration privileges \(DAP\) FAQ](#)
- [Granular delegated admin privileges \(GDAP\) introduction](#)
- [Microsoft-led transition from DAP to GDAP](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Quickstart: Set Microsoft 365 groups to expire in Microsoft Entra ID

Article • 04/25/2025

In this quickstart, you set the expiration policy for your Microsoft 365 groups. When users can set up their own groups, unused groups can multiply. One way to manage unused groups is to set those groups to expire, to reduce the maintenance of manually deleting groups.

Expiration policy is simple:

- Groups with user activities are automatically renewed as the expiration nears
- Group owners are notified to renew an expiring group
- A group that isn't renewed is deleted
- A deleted Microsoft 365 group can be restored within 30 days by a group owner or by a Microsoft Entra administrator

(!) Note

Microsoft Entra ID, part of Microsoft Entra, uses intelligence to automatically renew groups based on whether they have been in recent use. This renewal decision is based on user activity in groups across Microsoft 365 services like Outlook, SharePoint, Teams, Yammer, and others.

If you don't have an Azure subscription, [create a free account](#) before you begin.

Prerequisite

The least-privileged role required to set up group expiration is User Administrator in the organization.

Turn on user creation for groups

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

Microsoft Entra admin center

Home > Groups

Groups | General

Self Service Group Management

Owners can manage group membership requests in My Groups

Restrict user ability to access groups features in My Groups. Group and User Admin will have read-only access when the value of this setting is 'Yes.'

Security Groups

Users can create security groups in Azure portals, API or PowerShell

Microsoft 365 Groups

Users can create Microsoft 365 groups in Azure portals, API or PowerShell

3. Set **Users can create Microsoft 365 groups in Azure portals, API or PowerShell** to Yes.
4. Select **Save** to save the groups settings when you're done.

Set group expiration

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

Home > Groups

Groups | Expiration

All groups

Deleted groups

Diagnose and solve problems

General

Expiration

Naming policy

Activity

Privileged Identity Management

Access reviews

Audit logs

Bulk operation results

Troubleshooting + Support

New support request

Save

Discard

Renewal notifications are emailed to group owners 30 days, 15 days, and one day prior to group expiration. Group owners must have Exchange licenses to receive notification emails. If a group is not renewed, it is deleted along with its associated content from sources such as Outlook, SharePoint, Teams, and PowerBI.

* Group lifetime (in days) 180

* Email contact for groups with no owners example@contoso.com

Enable expiration for these Office 365 groups

All (Selected)

3. Set the expiration interval. Select a preset value or enter a custom value over 31 days.

4. Provide an email address where expiration notifications should be sent when a group has no owner.
5. For this quickstart, set **Enable expiration for these Microsoft 365 groups** to All.
6. Select **Save** to save the expiration settings when you're done.

That's it! In this quickstart, you successfully set the expiration policy for the selected Microsoft 365 groups.

Clean up resources

To remove the expiration policy

1. Sign in to the [Microsoft Entra admin center](#) as at least a **User Administrator**.
2. Browse to **Entra ID > Groups > All groups > Expiration**.
3. Set **Enable expiration for these Microsoft 365 groups** to **None**.

To turn off user creation for groups

1. Browse to **Entra ID > Groups > Group settings > General**.
2. Set **Users can create Microsoft 365 groups in Azure portals** to **No**.

Next steps

For more information about expiration including PowerShell instructions and technical constraints, see the following article:

[Expiration policy PowerShell](#)

Quickstart: Naming policy for groups in Microsoft Entra ID

Article • 12/18/2024

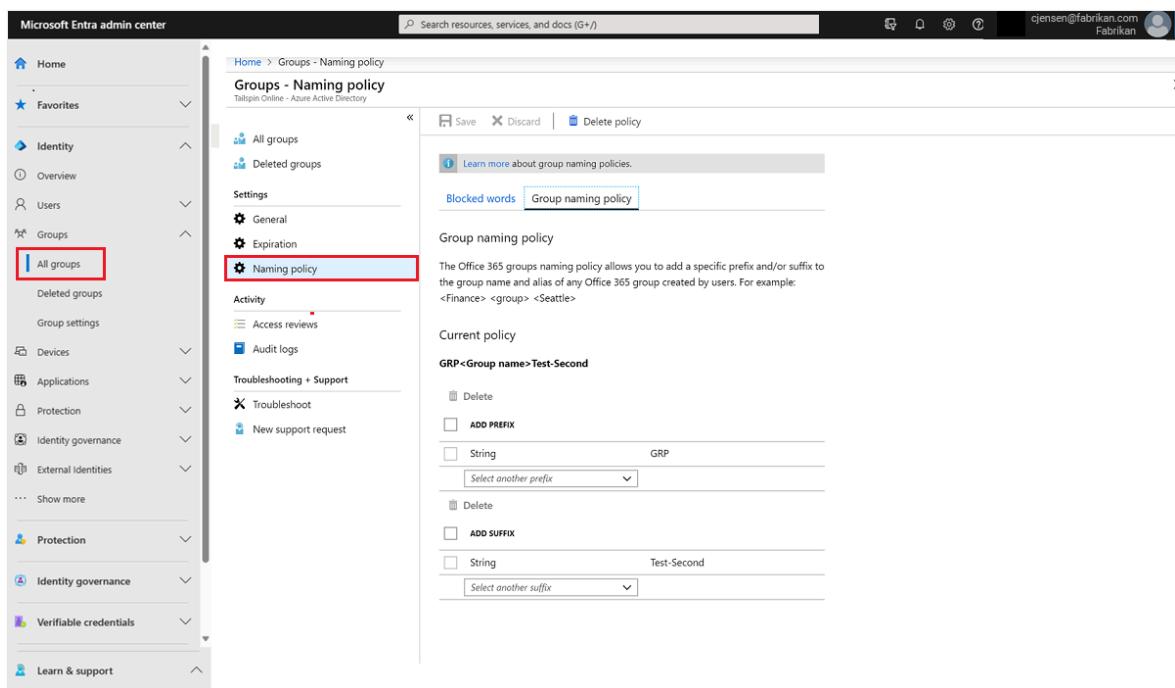
In this quickstart, in Microsoft Entra ID, part of Microsoft Entra, you set up naming policy in your Microsoft Entra organization for user-created Microsoft 365 groups, to help you sort and search your groups. For example, you could use the naming policy to:

- Communicate the function of a group, membership, geographic region, or who created the group.
- Help categorize groups in the address book.
- Block specific words from being used in group names and aliases.

If you don't have an Azure subscription, [create a free account](#) before you begin.

Configure the group naming policy

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Groups Administrator**.
2. Select Microsoft Entra ID.
3. Select **Groups > All groups** then select **Naming policy** to open the Naming policy page.



The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with various sections like Home, Favorites, Identity, Overview, Users, Groups (which is selected and highlighted with a red box), Deleted groups, Devices, Applications, Protection, Identity governance, External identities, and Learn & support. The main content area is titled 'Groups - Naming policy' under 'Tallspin Online - Azure Active Directory'. It has a breadcrumb trail: Home > Groups - Naming policy. There are tabs for 'All groups' and 'Deleted groups'. A 'Settings' section includes 'General', 'Expiration', and 'Naming policy' (which is also highlighted with a red box). Below that is an 'Activity' section with 'Access reviews', 'Audit logs' (selected and highlighted with a blue box), 'Troubleshooting + Support', 'Troubleshoot', and 'New support request'. The main content area contains a 'Group naming policy' section with a sub-section for 'Current policy' showing 'GRP<Group name>Test-Second'. It also includes sections for 'ADD PREFIX' (with a dropdown menu 'Select another prefix' containing 'GRP') and 'ADD SUFFIX' (with a dropdown menu 'Select another suffix' containing 'Test-Second'). At the top right, there are 'Save', 'Discard', and 'Delete policy' buttons, along with a link to 'Learn more about group naming policies'.

View or edit the Prefix-suffix naming policy

1. On the **Naming policy** page, select **Group naming policy**.
2. You can view or edit the current prefix or suffix naming policies individually by selecting the attributes or strings you want to enforce as part of the naming policy.
3. To remove a prefix or suffix from the list, select the prefix or suffix, then select **Delete**. Multiple items can be deleted at the same time.
4. Select **Save** for your changes to the policy to go into effect.

View or edit the custom blocked words

1. On the **Naming policy** page, select **Blocked words**.

The screenshot shows the 'Groups - Naming policy' page in the Azure portal. The left sidebar has a 'Naming policy' section selected. The main content area is titled 'Blocked words' (which is highlighted with a red box). It contains instructions for enabling a custom blocked words list and provides a download link for the current list. There is also a section for uploading a new .csv file, with a 'Select a file' input field and a browse icon.

2. View or edit the current list of custom blocked words by selecting **Download**.
3. Upload the new list of custom blocked words by selecting the file icon.
4. Select **Save** for your changes to the policy to go into effect.

That's it. You finished setting up your naming policy and added your custom blocked words.

Clean up resources

Remove the naming policy

1. On the **Naming policy** page, select **Delete policy**.
2. After you confirm the deletion, the naming policy is removed, including all prefix-suffix naming policy and any custom blocked words.

Next steps

Advance to the next article for more information including the PowerShell cmdlets for naming policy, technical constraints, adding a list of custom blocked words, and the end user experiences across Microsoft 365 apps.

[Naming policy PowerShell](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Add or remove group members automatically

Article • 01/31/2025

In Microsoft Entra ID, part of Microsoft Entra, you can automatically add or remove users to security groups or Microsoft 365 groups, so you don't always have to do it manually. Whenever any properties of a user or device change, Microsoft Entra ID evaluates all rules for dynamic membership groups in your Microsoft Entra organization to see if the change should add or remove members.

In this tutorial, you learn how to:

- ✓ Create an automatically populated group of guest users from a partner company
- ✓ Assign licenses to the group for the partner-specific features for guest users to access
- ✓ Bonus: secure the **All users** group by removing guest users so that, for example, you can give your member users access to internal-only sites

If you don't have an Azure subscription, [create a free account](#) before you begin.

Prerequisites

This feature requires one Microsoft Entra ID P1 or P2 license for the administrator of the organization. If you don't have one, in Microsoft Entra ID, select **Licenses > Products > Try/Buy**.

You're not required to assign licenses to the users for them to be members in dynamic membership groups. You only need the minimum number of available Microsoft Entra ID P1 licenses in the organization to cover all such users.

To create a group of guest users

First, you create a group for your guest users who all are from a single partner company. They need special licensing, so it's often more efficient to create a group for this purpose.

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Groups Administrator**.
2. Select Microsoft Entra ID.
3. Select **Groups > All groups > New group**.

NAME	GROUP TYPE
AAAAAA group	Security
AADtestGroup	Security
Access to Blog	Security
Access to Twitter	Security
ADSyncAdmins	Security
ADSyncBrowse	Security
ADSyncOperators	Security
ADSyncPasswordSet	Security
AFRICA Regional Employees	Security

4. On the New Group pane:

- Enter a *Guest users name, email address, and description* for the group.
- Change **Membership type** to **Dynamic User**.

Home > Groups | All groups >

New Group

Got feedback?

Group type

Microsoft 365

Group name * ⓘ

Enter the name of the group

Group email address * ⓘ

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

Group description ⓘ

Enter a description for the group

Membership type * ⓘ

Dynamic User

Sensitivity label ⓘ

Owners

No owners selected

Dynamic user members * ⓘ

Add dynamic query

5. Select **No owners selected** and on the Add Owners pane, scroll to locate the desired owners. Select on the name to add owners to the group.

6. Select **Select** to save the owners and close the Add Owners pane.

7. Select **Add dynamic query** in the **Dynamic user members** box.

8. On the **Dynamic membership rules** pane:

- In the **Property** field, select on the existing value and select **userType**.
- Verify that the **Operator** field has **Equals** selected.
- Select the **Value** field and enter **Guest**.
- Select the **Add Expression** hyperlink to add another line.
- In the **And/Or** field, select **And**.
- In the **Property** field, select **companyName**.
- Verify that the **Operator** field has **Equals** selected.
- In the **Value** field, enter **Contoso**.
- Select **Get custom extension properties** to enter an application ID to retrieve all available custom extension properties for creating a rule.
- When you're done, select **Save** to close **Dynamic membership rules**.

9. To finish and create the group, select **Create** on the **Group** pane.

Assign licenses

Now that you have your new group, you can apply the licenses that these partner users need.

1. In the Microsoft Entra admin center browse to **Identity > Billing > Licenses > All products**, select one or more licenses, and then select **Licensed groups**.

Name	State	Enabled Services
DS Deschutes Selfhost L3 licensed users	Active	1/15
DS Deschutes Selfhost L4 licensed users	Active	1/15
WB Williams Bay Users - GPU 1	Active	1/15
WB Williams Bay Users - GPU 2	Active	1/15
WB Windows 365 Selfhost - L1 License Users	Active	1/15

2. Search for the group name that you want to add, and then select **Assign**.
3. **Assignment options** allow you to turn on or off the service plans included the licenses that you selected. When you make a change, be sure to select **OK** to save your changes.
4. To complete the assignment, on the **Assign license** pane, select **Assign** at the bottom of the pane.

Remove guests from All users group

Perhaps your ultimate administrative plan is to assign all of your guest users to their own groups by company. You can also now change the **All users** group so that you can limit it to include users in your organization. Then you can use it to assign apps and licenses that are specific to your home organization.

The screenshot shows the Microsoft Entra admin center interface. The top navigation bar includes 'Home', 'f128 photography', 'Groups - All groups', and 'All Users - Dynamic membership rules'. The main title is 'All Users - Dynamic membership rules' with a 'Group' subtitle. On the left, a sidebar menu lists 'Overview', 'Properties', 'Members', 'Owners', 'Group memberships', 'Applications', 'Licenses', 'Azure resources', and 'Dynamic membership rules' (which is highlighted with a red box). The main content area has tabs for 'Save' and 'Discard'. It displays a 'Simple rule' configuration for 'Add dynamic membership rule'. The rule settings are: 'Add users where' dropdown set to 'userType', 'operator' dropdown set to 'Not Equals', and the value input field containing 'Guest'. There is also a 'Advanced rule' tab.

Clean up resources

To remove the guest users group

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Groups Administrator**.
2. Browse to **Groups > All groups**.
3. Select the **Guest users** group, select the ellipsis (...), and then select **Delete**. When you delete the group, any assigned licenses are removed.

To restore the All Users group

1. Select **Identity > Groups > All groups**. Select the name of the **All users** group to open the group.
2. Select **Dynamic membership rules**, clear all the text in the rule, and select **Save**.

Next steps

[Group licensing basics](#)

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 Graph API, 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.

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 ↗](#)

What is group-based licensing in Microsoft Entra ID?

Article • 01/31/2025

ⓘ Note

Starting September 1st, the Microsoft Entra ID Admin Center and the Microsoft Azure portal will no longer support 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, please 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](#)
- [PowerShell examples for group-based licensing in Microsoft Entra ID](#)

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 ↗](#)

Bulk create users in Microsoft Entra ID

Article • 12/19/2024

Microsoft Entra ID, part of Microsoft Entra, supports bulk user create and delete operations and supports downloading lists of users. Just fill out comma-separated values (CSV) template you can download from Microsoft Entra ID.

Required permissions

In order to bulk create users in the administration portal, you must be signed in as at least a User Administrator.

Understand the CSV template

Download and fill in the bulk upload CSV template to help you successfully create Microsoft Entra users in bulk. The CSV template you download might look like this example:

Row 1 must be preserved as-is, and the version number is always required.	
1	version:v1.0
2	Name [displayName] Required
3	Example: Chris Green
4	User name [userPrincipalName] Required chris@contoso.com

Preserve the column headings as-is in row 2. Column headings indicate acceptable values and whether they're required. Don't add additional columns.

Use the entries in row 3 as examples. Remove the row's contents and replace the examples with your entries.

⚠ Warning

If you are adding only one entry using the CSV template, you must preserve row 3 and add your new entry to row 4.

Ensure that you add the `.csv` file extension and remove any leading spaces before `userPrincipalName`, `passwordProfile`, and `accountEnabled`.

CSV template structure

The rows in a downloaded CSV template are as follows:

- **Version number:** The first row containing the version number must be included in the upload CSV.
- **Column headings:** The format of the column headings is `<Item name> [PropertyName] <Required or blank>`. For example, `Name [displayName] Required`. Some older versions of the template might have slight variations.
- **Examples row:** We have included in the template a row of examples of acceptable values for each column. You must remove the examples row and replace it with your own entries.

Additional guidance

- The first two rows of the upload template must not be removed or modified, or the upload can't be processed.
- The required columns are listed first.
- We don't recommend adding new columns to the template. Any additional columns you add are ignored and not processed.
- We recommend that you download the latest version of the CSV template as often as possible.
- Make sure to check there is no unintended whitespace before/after any field. For **User principal name**, having such whitespace would cause import failure.
- Ensure that values in **Initial password** comply with the currently active [password policy](#).

To create users in bulk

1. Sign in to the [Microsoft Entra admin center](#) as at least a **User Administrator**.
2. Select Microsoft Entra ID.
3. Select **All users > Users > Bulk create**.
4. On the **Bulk create user** page, select **Download** to receive a valid comma-separated values (CSV) file of user properties, and then add users you want to create.

The screenshot shows the Microsoft Entra admin center's 'Users' page. In the top right, there's a 'Bulk create users' section with three steps: 1. Download csv template (optional) with a 'Download' button, 2. Edit your csv file, and 3. Upload your csv file with a 'Select a file' input field. Below this is a table of 34 users with columns for User principal name, User type, On-premises sync status, and Identities. At the bottom right of the table is a 'Submit' button.

5. Open the CSV file and add a line for each user you want to create. The only required values are **Name**, **User principal name**, **Initial password**, and **Block sign in (Yes/No)**. Then save the file.

A	B	C	D	E	F
1 version:v1.0					
2 Name [displayName] Required	User name [userPrincipalName] Required	Initial password [passwordProfile] Required	Block sign in (Yes/No) [accountEnabled] Required	First name [givenName] Required	Last name [surname]
3 Example: Chris Green	chris@contoso.com	myPassword1234	No		
4					

6. On the **Bulk create user** page, under **Upload your CSV file**, browse to the file. When you select the file and select **Submit**, validation of the CSV file starts.
7. After the file contents are validated, you'll see **File uploaded successfully**. If there are errors, you must fix them before you can submit the job.
8. When your file passes validation, select **Submit** to start the bulk operation that imports the new users.
9. When the import operation completes, you see a notification of the bulk operation job status.

If you experience errors, you can download and view the results file on the **Bulk operation results** page. The file contains the reason for each error. The file submission must match the provided template and include the exact column names. For more information about bulk operations limitations, see [Bulk import service limits](#).

Check status

You can see the status of all of your pending bulk requests in the **Bulk operation results** page.

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a sidebar with various navigation options like 'All users', 'Deleted users', 'User settings', etc. The 'Bulk operation results' option is highlighted with a red border. The main content area is titled 'Users | Bulk operation results' and contains a table with one row labeled 'No results'. The table has columns for 'File name', 'Upload time', 'Completion time', 'Status', '# Success', '# Failure', 'Total requests', and 'Admin uploaded'. The 'File name' column has a dropdown menu set to 'All'. The 'Upload time' column is highlighted with a red border.

Next, you can check to see that the users you created exist in the Microsoft Entra organization either in the Azure portal or by using PowerShell.

Verify users

1. Sign in to the [Microsoft Entra admin center](#) as at least a [User Administrator](#).
2. Select Microsoft Entra ID.
3. Select **All users > Users**.
4. Under **Show**, select **All users** and verify that the users you created are listed.

Verify users with PowerShell

Run the following command:

```
PowerShell  
  
Get-MgUser -Filter "UserType eq 'Member'"
```

You should see that the users that you created are listed.

Bulk import service limits

! Note

When performing bulk operations, such as import or create, you may encounter a problem if the bulk operation does not 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. For more information, see [Bulk operations service limitations](#).

Next steps

- Bulk delete users
 - Download list of users
 - Bulk restore users
-

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback 

Convert external users to internal users (Preview)

Article • 01/06/2025

Enterprises, such as those going through reorganizations, mergers, and acquisitions, sometimes need to change the way they work with some or all of their existing users. In some cases, administrators need to change existing external users into internal ones.

External user conversion handles the conversion of external users into internal users without the need to delete existing user objects and create new ones. The preservation of the user objects allows users to keep their original account so that their access isn't disrupted. A converted user's account maintains its history of activities intact as their relationship with the host organization changes.

- **Internal users** are users who authenticate with the local tenant.
- **External users** are users who authenticate via a method not managed by the host organization, such as another organization's Microsoft Entra ID, Google federation, or Microsoft account. Many external users have a *userType* of `guest`, but there's no formal relation between *userType* and how a user signs in. External users who have a *userType* of `member`, could also be eligible for conversion.

External user conversion can be performed using [Microsoft Graph API](#) or the Microsoft Entra ID Portal.

Converting external users

It's important to understand that the *userType* for `member` versus `guest` doesn't indicate where a user authenticates; instead, it only defines the level of permissions that a user has in the current tenant. You can update the *userType* for your users, but that alone doesn't change the users' external versus internal state. To change external users to internal users, see [synced user conversion](#).

There are two types of external users that you can convert to internal:

- Cloud-only users
- Synced users

Cloud user conversion

When a cloud user is converted from external to internal, administrators must specify a *UPN* and *password* for the user. Converting cloud users to synced users ensures that the user can authenticate with the current tenant.

Synced user conversion

Synced user conversion allows you to convert a user from external to internal in Microsoft Entra ID. This feature is useful when you want to move a user from a federated identity provider to Microsoft Entra ID or when you want to convert a user from a cloud-only identity to a synced identity.

You can use [Microsoft Entra Connect](#) to synchronize your on-premises identities. When you convert a user from an external user to an internal user, Microsoft Entra Connect synchronizes the user's attributes to Microsoft Entra ID, so the user is managed as an internal user going forward.

Synced user are users synced from on-premises. As these accounts are managed at the source, administrators are unable to specify the UPN for these users.

- Synced users where the tenant uses federated authentication:
 - If Password Hash Sync (PHS) is enabled, administrators are blocked from setting a new password during conversion.
 - If the federated tenant doesn't have PHS enabled, administrators can set a user password.
- In cases where the tenant is managed, meaning it uses cloud authentication, administrators are required to specify a password during conversion.

Note

To unsync a user, you must disable directory synchronization for the user in [Microsoft Entra Connect](#). Once directory sync is disabled for the user, any changes made to the user's attributes in Microsoft Entra ID can no longer be synced to your on-premises directory.

Testing external user conversions

When testing external user conversions, we recommend that you use test accounts or accounts that wouldn't create a disruption if they were to become unavailable.

Requirements

- Converting external users to internal users requires an account with at least the [user administrator](#) role assigned.
- Only users configured with an authentication method external to the host organization are eligible for conversion.

Converting an external user

You can convert external users, such as cloud-only and synced users, to internal users using the Microsoft Entra admin center.

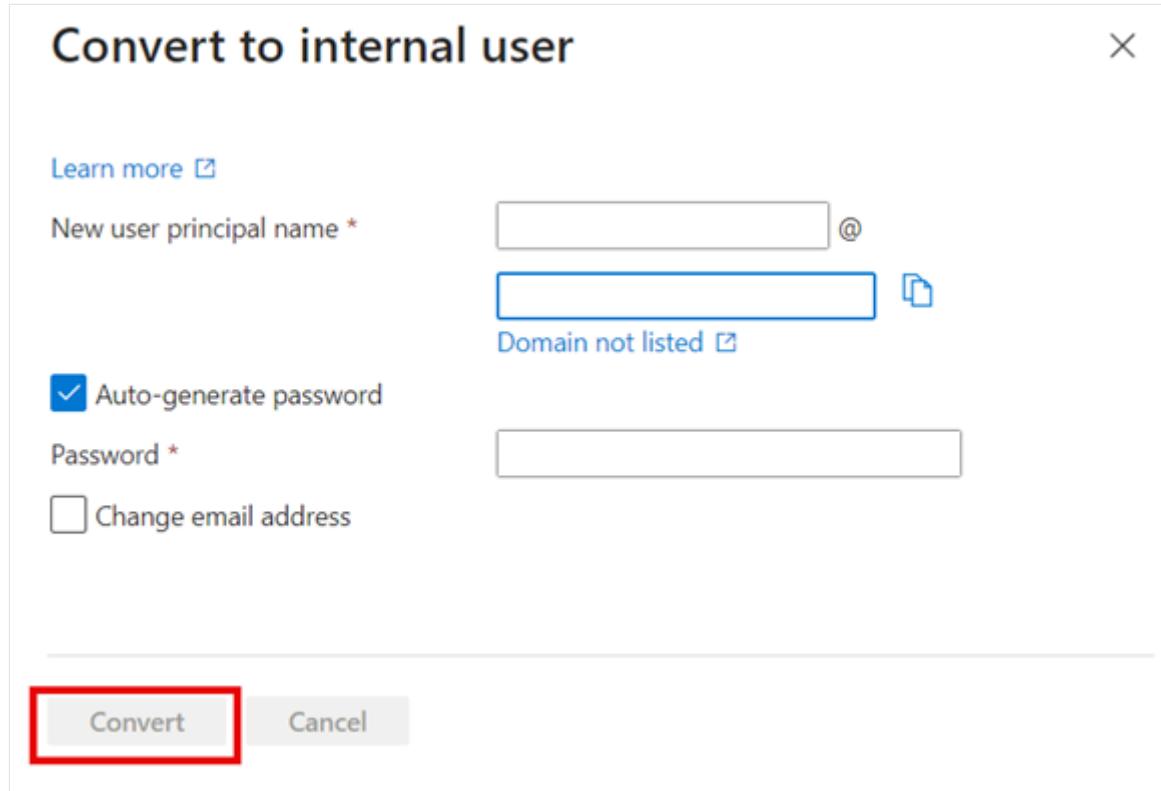
1. Sign in to the [Microsoft Entra admin center](#) as at least a [User Administrator](#).
2. Browse to **Identity > Users > All users**.
3. Select an external user.
4. Select **Convert to internal user**.

The screenshot shows the Microsoft Entra admin center interface for managing users. The user profile for "Chris Q. Public" is displayed, which is identified as an external user ("ExternalAzureAD"). In the bottom right corner of the main user details section, there is a red rectangular box highlighting the "Convert to internal user" button. This button is located within a section titled "B2B collaboration" which states "Current user is external". Above this section, there are other status indicators like "Account status" (Enabled) and "B2B invitation". Below the main user details, there are sections for "My Feed" and "Quick actions".

5. In the **Convert to internal user** section, you need to finalize a couple of steps:
 - a. Provide a **user principal name (UPN)**. This value is the new UPN value for the user. For cloud-only users, the UPN domain must be one that is nonfederated.

For on-premises synced users, you don't need to provide a UPN. The user continues to use the on-premises credentials.

- b. Check the box if you would like an autogenerated password.
- c. Check the box for **Change email address** to specify an optional new email address for cloud users.



6. After reviewing the options and making your selected choices, choose **Convert**.

Related content

- [User management enhancements](#)
- [user: convertExternalToInternalMemberUser Microsoft Graph API](#)

Feedback

Was this page helpful?

Yes

No

[Provide product feedback](#)

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

```
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.

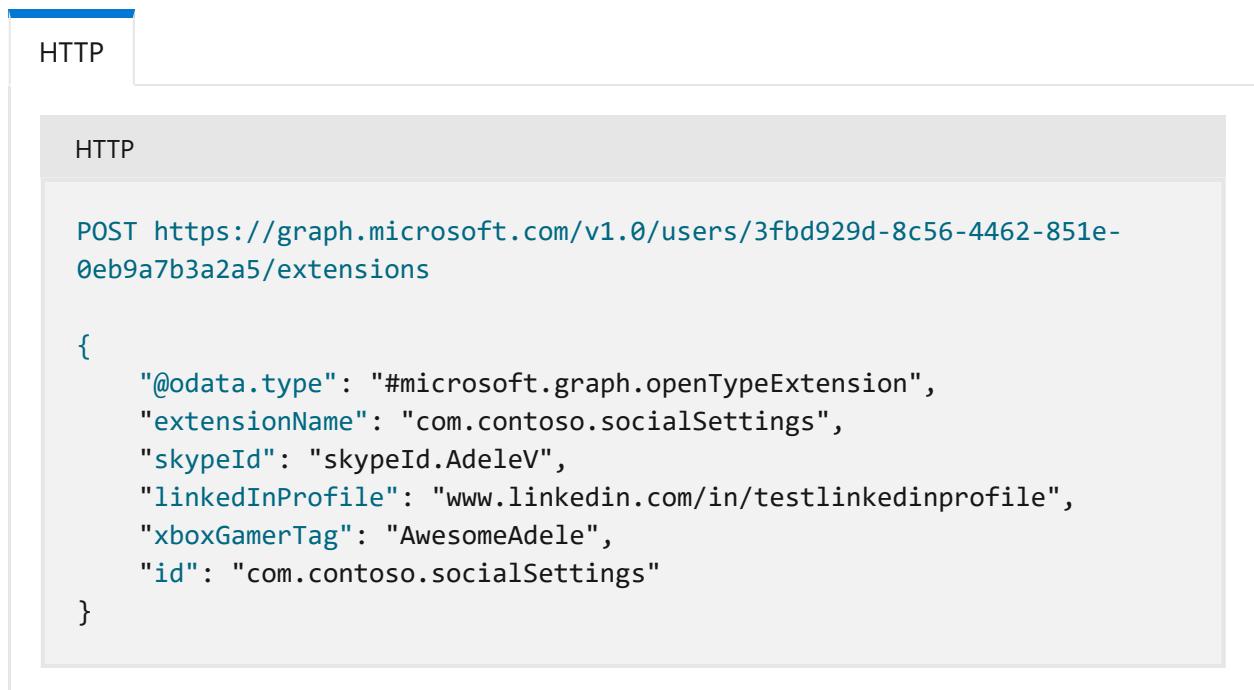
You define and manage open extensions on the fly on resource instances. They're considered unique for each object, and you don't need to apply a universally consistent pattern for all objects. For example, in the same tenant:

- 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 interface with an "HTTP" tab selected. Below it, a larger "HTTP" tab is shown with a grey background. The main content area contains a POST request to Microsoft Graph's users endpoint with an open extension. The request body is a JSON object defining the extension's type, name, and properties.

```
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](#)

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**.

The screenshot shows the Microsoft Entra admin center interface. The top navigation bar includes 'Home', 'Users', and 'Joe'. The main title is 'Joe | Custom security attributes'. Below the title are buttons for 'Save', 'Discard', 'Add assignment', 'Remove assignment', and 'Got feedback?'. A search bar and a 'Add filters' button are also present. On the left, a sidebar titled 'Manage' contains links for 'Custom security attributes' (which is highlighted), 'Assigned roles', 'Administrative units', 'Groups', 'Applications', and 'Licenses'. The main content area displays a table with columns: 'Attribute set', 'Attribute name', 'Attribute descrip...', 'Data type', 'Multi...', and 'Assigned values'. One row is visible: 'Engineering' under 'Attribute set', 'Project' under 'Attribute name', 'Active projects for ...' under 'Attribute descrip...', 'String' under 'Data type', 'Yes' under 'Multi...', and '2 values' under 'Assigned values'. A large circular 'Add' button is located in the bottom right corner of the main content area.

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 on the right, containing fields for 'Filter' (set to 'Custom security attributes (preview)'), 'Attribute set' (set to 'Engineering'), 'Attribute name' (set to 'Project'), 'Operator' (set to '=='), and 'Value' (set to 'Baker'). There are 'Apply' and 'Cancel' buttons at the bottom of the modal.

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>-----</code>
<code>--</code>	<code>-----</code>
<code>-----</code>	<code>-----</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 ↗](#)

Download a list of users in Azure portal

Article • 01/29/2025

Microsoft Entra ID, part of Microsoft Entra, supports bulk user list download operations.

Required permissions

Both admin and standard users can download user lists.

To download a list of users

1. Sign in to the [Microsoft Entra admin center](#).
2. Select Microsoft Entra ID.
3. Select **Users > All users > Download users**. By default, all user profiles are exported.
4. On the **Download users** page, select **Start** to receive a CSV file listing user profile properties. If there are errors, you can download and view the results file on the **Bulk operation results** page. The file contains the reason for each error.

The screenshot shows the 'Download users' page in the Microsoft Entra admin center. At the top, there's a navigation bar with icons for services, and docs, search, notifications, and user profile. Below the navigation is a header with the title 'Download users'. On the left, there are buttons for Bulk create, Bulk invite, Bulk delete, and Download users (which is highlighted with a red box). There are also links for Reset password and a 'File name' input field containing 'exportUser_2019-8-15'. On the right, there's a large red box around the 'Start' button. Below these controls is a table showing user details: dforsberg@contoso.com (Member), goransson@contoso.com (Member), ext-MollieB-contosopictures@contoso.com (Member), and hmurphy@contoso.com (Member). The table has columns for USER NAME and USER TYPE. At the bottom of the table, there are dropdown menus for Search attributes (Name, email (begins with)) and Show (All users).

ⓘ Note

The download file will contain the filtered list of users based on the scope of the filters applied.

The following user attributes are included:

- `userPrincipalName`
- `displayName`
- `surname`
- `mail`
- `givenName`
- `objectId`
- `userType`
- `jobTitle`
- `department`
- `accountEnabled`
- `usageLocation`
- `streetAddress`
- `state`
- `country`
- `physicalDeliveryOfficeName`
- `city`
- `postalCode`
- `telephoneNumber`
- `mobile`
- `authenticationAlternativePhoneNumber`
- `authenticationEmail`
- `alternateEmailAddress`
- `ageGroup`
- `consentProvidedForMinor`
- `legalAgeGroupClassification`

Check status

You can see the status of your pending bulk requests in the **Bulk operation results** page.

The screenshot shows the 'Users | Bulk operation results' page in the Microsoft Entra ID for Workforce portal. The left sidebar includes links for 'All users', 'Deleted users', 'Password reset', 'User settings', 'Diagnose and solve problems', 'Activity' (with 'Sign-ins' and 'Audit logs'), and 'Bulk operation results' (which is highlighted with a red box). The main area features a table with the following columns: File name, Type, Upload time, Completion time, Status, # Success, # Failure, Total requests, and Admin uploaded. The table currently displays 'No results'. At the bottom right of the page is a circular button with a magnifying glass icon.

If you experience errors, you can download and view the results file on the **Bulk operation results** page. The file contains the reason for each error. The file submission must match the provided template and include the exact column names. For more information about bulk operations limitations, see [Bulk download service limits](#).

Bulk download service limits

Note

When performing bulk operations, such as import or create, you can 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 limit the data returned by the bulk operation. For more information, see [Bulk operations service limitations](#).

Next steps

- [Bulk add users](#)
- [Bulk delete users](#)
- [Bulk restore users](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Sharing accounts with Microsoft Entra ID

Article • 12/13/2024

Overview

In Microsoft Entra ID, part of Microsoft Entra, sometimes organizations need to use a single username and password for multiple people, which often happens in the following cases:

- When accessing applications that require a unique sign in and password for each user, whether on-premises apps or consumer cloud services (for example, corporate social media accounts).
- When creating multi-user environments. You might have a single, local account that has elevated privileges and is used to do core setup, administration, and recovery activities. For example, an Application Administrator account for Microsoft 365 or the root account in Salesforce.

Traditionally, these accounts are shared by distributing the credentials (username and password) to the right individuals, or storing them in a shared location where multiple trusted agents can access them.

The traditional sharing model has several drawbacks:

- Enabling access to new applications requires you to distribute credentials to everyone that needs access.
- Each shared application might require its own unique set of shared credentials, requiring users to remember multiple sets of credentials. When users have to remember many credentials, the risk increases that they resort to risky practices. (for example, writing down passwords).
- You can't tell who has access to an application.
- You can't tell who *accessed* an application.
- When you want to remove access to an application, you have to update the credentials and redistribute them to everyone that needs access to that application.

Microsoft Entra account sharing

Microsoft Entra ID provides a new approach to using shared accounts that eliminates these drawbacks.

The Microsoft Entra administrator configures which applications a user can access by using the Access Panel and choosing the type of single sign-on best suited for that application. One of those types, *password-based single-sign on*, lets Microsoft Entra ID act as a kind of "broker" during the sign-on process for that app.

Users sign in once with their organizational account. This account is the same one they regularly use to access their desktop or email. They can discover and access only those applications that they're assigned to. With shared accounts, this list of applications can include any number of shared credentials. The end-user doesn't need to remember or write down the various accounts they might be using.

Shared accounts increase oversight, improve usability, and enhance your security. Users with permissions to use the credentials don't see the shared password, but rather get permissions to use the password as part of an orchestrated authentication flow. Further, some password SSO applications give you the option of using Microsoft Entra ID to periodically rollover (update) passwords. The system uses large, complex passwords, which increase account security. The administrator can easily grant or revoke access to an application, knows who has access to the account, and who accessed it in the past.

Microsoft Entra ID supports shared accounts for any Enterprise Mobility Suite (EMS) or Microsoft Entra ID P1 or P2 license plan, across all types of password single sign-on applications. You can share accounts for any of thousands of preintegrated applications in the application gallery and can add your own password-authenticating application with [custom SSO apps](#).

Microsoft Entra features that enable account sharing include:

- [Password single sign-on](#)
- [Password single sign-on agent](#)
- [Group assignment](#)
- [Custom Password apps](#)
- [App usage dashboard/reports](#)
- [End-user access portals](#)
- [App proxy](#)
- [Azure Marketplace ↗](#)

Sharing an account

To use Microsoft Entra ID to share an account, you need to:

- Add an application [app gallery](#) or [custom application](#)
- Configure the application for password single sign-on (SSO)
- Use [group-based assignment](#) and select the option to enter a shared credential

You can also make your shared account more secure with multifactor authentication (MFA) (learn more about [securing applications with Microsoft Entra ID](#)). You can delegate the ability to manage who has access to the application using [Microsoft Entra self-service group management](#).

Next steps

- [Application Management in Microsoft Entra ID](#)
 - [Protecting apps with Conditional Access](#)
 - [Self-service group management/SSAA](#)
-

Feedback

Was this page helpful?



[Provide product feedback](#)

Assign Microsoft Entra roles

Article • 01/03/2025

This article describes how to assign Microsoft Entra roles to users and groups using the Microsoft Entra admin center, Microsoft Graph PowerShell, or Microsoft Graph API. It also describes how to assign roles at different scopes, such as tenant, application registration, and administrative unit scopes.

You can assign both direct and indirect role assignments to a user. If a user is assigned a role by a group membership, add the user to the group to add the role assignment. For more information, see [Use Microsoft Entra groups to manage role assignments](#).

In Microsoft Entra ID, roles are typically assigned to apply to the entire tenant. However, you can also assign Microsoft Entra roles for different resources, such as application registrations or administrative units. For example, you could assign the Helpdesk Administrator role so that it just applies to a particular administrative unit and not the entire tenant. The resources that a role assignment applies to is also called the scope. Restricting the scope of a role assignment is supported for built-in and custom roles. For more information about scope, see [Overview of role-based access control \(RBAC\) in Microsoft Entra ID](#).

Microsoft Entra roles in PIM

If you have a Microsoft Entra ID P2 license and [Privileged Identity Management \(PIM\)](#), you have additional capabilities when assigning roles, such as making a user eligible for a role assignment or defining the start and end time for a role assignment. For information about assigning Microsoft Entra roles in PIM, see these articles:

[+] [Expand table](#)

Method	Information
Microsoft Entra admin center	Assign Microsoft Entra roles in Privileged Identity Management
Microsoft Graph PowerShell	Tutorial: Assign Microsoft Entra roles in Privileged Identity Management using Microsoft Graph PowerShell
Microsoft Graph API	Manage Microsoft Entra role assignments using PIM APIs Assign Microsoft Entra roles in Privileged Identity Management

Prerequisites

- Privileged Role Administrator
- [Microsoft Graph PowerShell](#) module when using PowerShell
- Admin consent when using Graph Explorer for Microsoft Graph API

For more information, see [Prerequisites to use PowerShell or Graph Explorer](#).

Assign roles with tenant scope

This section describes how to assign roles at tenant scope.

Admin center

Tip

Steps in this article might vary slightly based on the portal you start from.

1. Sign in to the [Microsoft Entra admin center](#) ↗ as at least a [Privileged Role Administrator](#).
2. Browse to **Identity > Roles & admins > Roles & admins**.
3. Select a role name to open the role. Don't add a check mark next to the role.

Role	Description	Privileged	Type
AI Administrator	Manage all aspects of Microsoft 365 Copilot and AI-related enterprise services in Microsoft 365.	0	Built-in
Application Administrator	Can create and manage all aspects of app registrations and enterprise apps.	PRIVILEGED	Built-in
Application Developer	Can create application registrations independent of the 'Users can register applications' setting.	PRIVILEGED	Built-in
Attack Payload Author	Can create attack payloads that an administrator can initiate later.	0	Built-in
Attack Simulation Admin...	Can create and manage all aspects of attack simulation campaigns.	0	Built-in

<input type="checkbox"/>	B2C IEF Keyset Administrator	Can manage secrets for
<input type="checkbox"/>	B2C IEF Policy Administrator	Can create and manage
<input checked="" type="checkbox"/>	Billing Administrator	Can perform common b
<input type="checkbox"/>	Cloud App Security Administrator	Can manage all aspects
<input type="checkbox"/>	Cloud Application Administrator	Can create and manage

4. Select **Add assignments** and then select the users or groups you want to assign to this role.

Only role-assignable groups are displayed. If a group isn't listed, you'll need to create a role-assignable group. For more information, see [Create a role-assignable group in Microsoft Entra ID](#).

If your experience is different than the following screenshot, you might have Microsoft Entra ID P2 and PIM. For more information, see [Assign Microsoft Entra roles in Privileged Identity Management](#).

Name	Type
Alan Steiner	User
Alicia Thomber	User
Allie Bellew	User
Amy Alberts	User
Anne Weller	User
Carlos Grilo	User
Christa Geller	User
Dan Jump	User
David So	User
Diane Prescott	User

5. Select **Add** to assign the role.

Assign roles with app registration scope

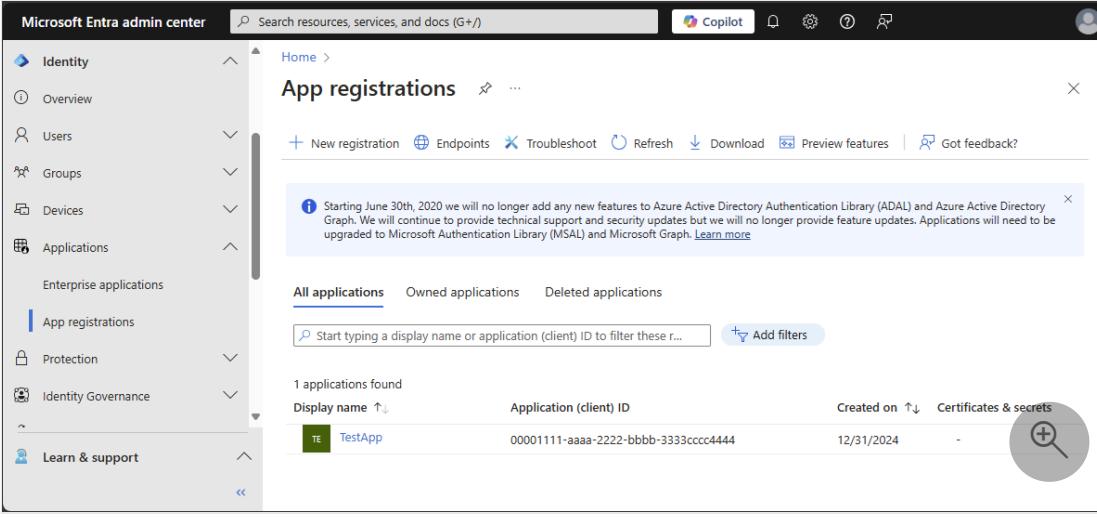
Built-in roles and custom roles are assigned by default at tenant scope to grant access permissions over all app registrations in your organization. Additionally, custom roles

and some relevant built-in roles (depending on the type of Microsoft Entra resource) can also be assigned at the scope of a single Microsoft Entra resource. This allows you to give the user the permission to update credentials and basic properties of a single app without having to create a second custom role.

This section describes how to assign roles at an application registration scope.

Admin center

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Application Developer](#).
2. Browse to **Identity > Applications > App registrations**.
3. Select an application. You can use search box to find the desired app.
You might have to select **All applications** to see the complete list of app registrations in your tenant.



Display name	Application (client) ID	Created on	Certificates & secrets
TestApp	00001111-aaaa-2222-bbbb-3333cccc4444	12/31/2024	-

4. Select **Roles and administrators** from the left navigation menu to see the list of all roles available to be assigned over the app registration.

The screenshot shows the 'TestApp | Roles and administrators' page. On the left, there's a sidebar with links like Overview, Quickstart, Integration assistant, Diagnose and solve problems, Manage, Support + Troubleshooting, and New support request. The main area has a search bar, refresh, preview features, and feedback buttons. A note about PIM (Just-in-time access) is shown. The 'Administrative roles' section is highlighted, explaining they are used for granting access to privileged actions. It lists the 'Cloud Application Administrator' role, which can create and manage all aspects of app registrations and enterprise apps except App Proxy. The role is marked as 'PRIVILEGED' and has a count of 1. The 'Type' is listed as 'Built-in'.

5. Select the desired role.

Tip

You won't see the entire list of Microsoft Entra built-in or custom roles here. This is expected. We show the roles which have permissions related to managing app registrations only.

6. Select **Add assignments** and then select the users or groups you want to assign this role to.

The screenshot shows the 'Add assignments' dialog for the 'Cloud Application' app registration. The sidebar on the left includes links for Diagnose and solve problems, Manage (with 'Assignments' selected), Description, Troubleshooting + Support, and New support request. The main area has a search bar and a note about filtering results. It shows a list of 4 results found, with tabs for All, Users, and Groups. The 'Users' tab is selected. A table lists users: Contoso Helpdesk (Group), Edith (User), and Gary (User). Gary is selected, indicated by a checked checkbox and highlighted in grey. An 'Add' button is at the bottom left, and a 'Selected (1)' section on the right shows Gary's selection.

7. Select **Add** to assign the role scoped over the app registration.

Assign roles with administrative unit scope

In Microsoft Entra ID, for more granular administrative control, you can assign a Microsoft Entra role with a scope that's limited to one or more [administrative units](#). When a Microsoft Entra role is assigned at the scope of an administrative unit, role permissions apply only when managing members of the administrative unit itself, and don't apply to tenant-wide settings or configurations.

For example, an administrator who is assigned the Groups Administrator role at the scope of an administrative unit can manage groups that are members of the administrative unit, but they can't manage other groups in the tenant. They also can't manage tenant-level settings related to groups, such as expiration or group naming policies.

This section describes how to assign Microsoft Entra roles with administrative unit scope.

Prerequisites

- Microsoft Entra ID P1 or P2 license for each administrative unit administrator
- Microsoft Entra ID Free licenses for administrative unit members
- Privileged Role Administrator
- Microsoft Graph PowerShell module when using PowerShell
- Admin consent when using Graph Explorer for Microsoft Graph API

For more information, see [Prerequisites to use PowerShell or Graph Explorer](#).

Roles that can be assigned with administrative unit scope

The following Microsoft Entra roles can be assigned with administrative unit scope. Additionally, any [custom role](#) can be assigned with administrative unit scope as long as the custom role's permissions include at least one permission relevant to users, groups, or devices.

[+] Expand table

Role	Description
Authentication Administrator	Has access to view, set, and reset authentication method information for any non-admin user in the assigned administrative unit only.
Cloud Device Administrator	Limited access to manage devices in Microsoft Entra ID.
Groups Administrator	Can manage all aspects of groups in the assigned administrative unit only.

Role	Description
Helpdesk Administrator	Can reset passwords for non-administrators in the assigned administrative unit only.
License Administrator	Can assign, remove, and update license assignments within the administrative unit only.
Password Administrator	Can reset passwords for non-administrators within the assigned administrative unit only.
Printer Administrator	Can manage printers and printer connectors. For more information, see Delegate administration of printers in Universal Print .
Privileged Authentication Administrator	Can access to view, set and reset authentication method information for any user (admin or non-admin).
SharePoint Administrator	Can manage Microsoft 365 groups in the assigned administrative unit only. For SharePoint sites associated with Microsoft 365 groups in an administrative unit, can also update site properties (site name, URL, and external sharing policy) using the Microsoft 365 admin center. Cannot use the SharePoint admin center or SharePoint APIs to manage sites.
Teams Administrator	Can manage Microsoft 365 groups in the assigned administrative unit only. Can manage team members in the Microsoft 365 admin center for teams associated with groups in the assigned administrative unit only. Cannot use the Teams admin center.
Teams Devices Administrator	Can perform management related tasks on Teams certified devices.
User Administrator	Can manage all aspects of users and groups, including resetting passwords for limited admins within the assigned administrative unit only. Cannot currently manage users' profile photographs.
<Custom role>	Can perform actions that apply to users, groups, or devices, according to the definition of the custom role.

Certain role permissions apply only to nonadministrator users when assigned with the scope of an administrative unit. In other words, administrative unit scoped [Helpdesk Administrators](#) can reset passwords for users in the administrative unit only if those users don't have administrator roles. The following list of permissions are restricted when the target of an action is another administrator:

- Read and modify user authentication methods, or reset user passwords
- Modify sensitive user properties such as telephone numbers, alternate email addresses, or Open Authorization (OAuth) secret keys
- Delete or restore user accounts

Security principals that can be assigned with administrative unit scope

The following security principals can be assigned to a role with an administrative unit scope:

- Users
- Microsoft Entra role-assignable groups
- Service principals

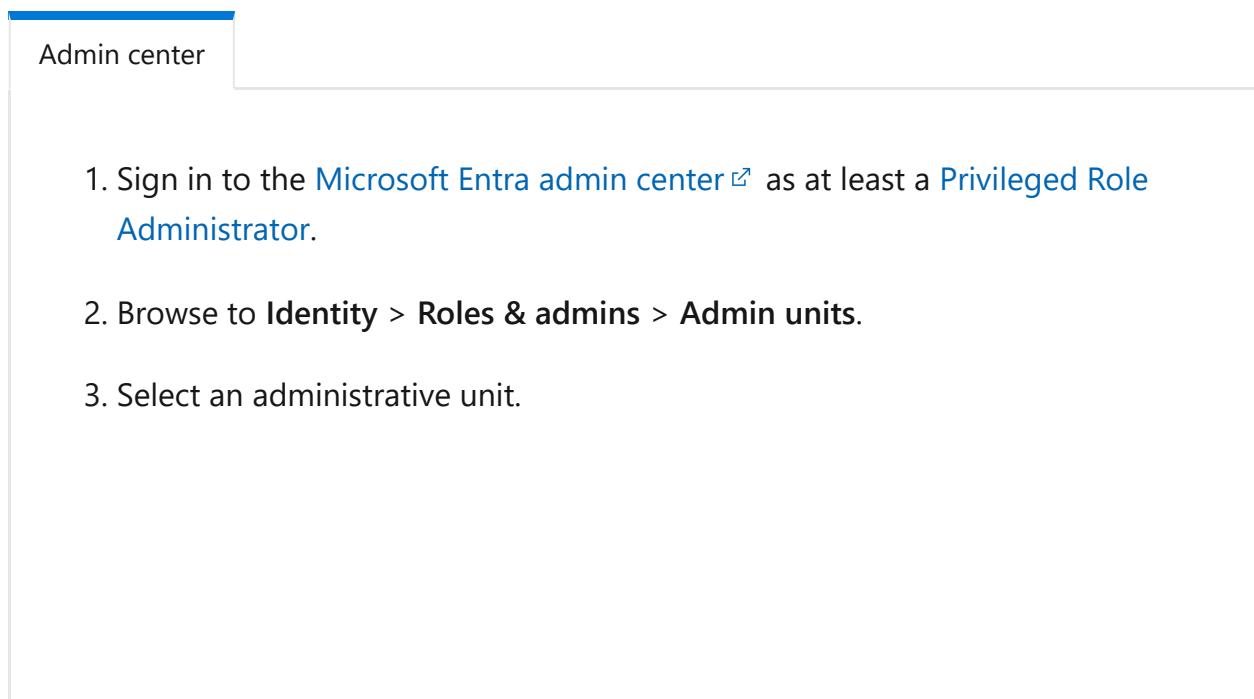
Service principals and guest users

Service principals and guest users won't be able to use a role assignment scoped to an administrative unit unless they're also assigned corresponding permissions to read the objects. This is because service principals and guest users don't receive directory read permissions by default, which are required to perform administrative actions. To enable a service principal or guest user to use a role assignment scoped to an administrative unit, you must assign the [Directory Readers](#) role (or another role that includes read permissions) at a tenant scope.

It isn't currently possible to assign directory read permissions scoped to an administrative unit. For more information about default permissions for users, see [default user permissions](#).

Assign roles with administrative unit scope

This section describes how to assign roles at administrative unit scope.



Admin center

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Privileged Role Administrator](#).
2. Browse to **Identity > Roles & admins > Admin units**.
3. Select an administrative unit.

Microsoft Entra admin center

Home > Administrative units

Learn more Add Delete Refresh Preview features Got feedback?

Name	Description	Restricted management	Membership type
Seattle Operations	Users, groups, and devices in S...	No	Assigned

4. Select **Roles and administrators** from the left navigation menu to see the list of all roles available to be assigned over an administrative unit.

Home > Default > Administrative units > Seattle Operations

Seattle Operations | Roles and administrators

Search Refresh Preview features Got feedback?

Role	Description	Privileged	Ass...	Type
Authentication Administrator	Can access to view, set and reset authentication method information for any non-admin user.	PRIVILEGED	0	Built-in
Cloud Device Administrator	Limited access to manage devices in Microsoft Entra ID.	PRIVILEGED	0	Built-in
Groups Administrator	Members of this role can create/manage groups, create/manage groups settings like naming and expiration policies, and view groups activity and audit reports.		0	Built-in
Helpdesk Administrator	Can reset passwords for non-administrators and Helpdesk Administrators.	PRIVILEGED	2	Built-in

5. Select the desired role.

💡 Tip

You won't see the entire list of Microsoft Entra built-in or custom roles here. This is expected. We show the roles which have permissions related to the objects that are supported within the administrative unit. To see the list of objects supported within an administrative unit, see [Administrative units in Microsoft Entra ID](#).

6. Select **Add assignments** and then select the users or groups you want to assign this role to.
7. Select **Add** to assign the role scoped over the administrative unit.

Next steps

- List Microsoft Entra role assignments
 - Assign Microsoft Entra roles in Privileged Identity Management
 - Use Microsoft Entra groups to manage role assignments
 - Troubleshoot Microsoft Entra roles assigned to groups
-

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

User management enhancements in Microsoft Entra ID

Article • 01/07/2025

This article describes how to use the user management enhancements in the Microsoft Entra admin center. In this article, you review the **All users** and **user profile** pages.

Enhancements include:

- Preloaded scrolling so that you no longer have to select "Load more" to view more users
- More user properties can be added as columns including city, country/region, employee ID, employee type, and external user state
- More user properties can be filtered on including custom security attributes, on-premises extension attributes, and manager
- More ways to customize your view, like using drag-and-drop to reorder columns
- Copy and share your customized All Users view with others
- An enhanced User Profile experience that gives you quick insights about a user and lets you view and edit more properties

ⓘ Note

These enhancements aren't currently available for Azure AD B2C tenants.

All users page

We've made some changes to the columns and filters available on the **All users** page. In addition to the existing columns for managing your list of users, we've added the option to add more user properties as columns and filters including employee ID, employee hire date, on-premises attributes, and more.

The screenshot shows the Microsoft Entra admin center interface. In the left sidebar, under the 'Users' section, the 'All users' link is highlighted with a red box. On the main page, there's a search bar at the top. Below it, a message says 'Want to switch back to the legacy users list experience? Click here to leave the preview.' A search bar labeled 'Search' is followed by a button 'Add filter'. A table displays user information with columns: Display name, User principal name, User type, Employee ID, Employee hire date, and On-premises SAM account name. The 'Employee ID', 'Employee hire date', and 'On-premises SAM account name' columns are also highlighted with red boxes.

Reorder columns

You can customize your list view by reordering the columns on the page in one of two ways. One way is to directly drag and drop the columns on the page. Another way is to select **Columns** to open the column picker and then drag and drop the three-dot "handle" next to any given column.

Share views

If you want to share your customized list view with another person, you can select **Copy link to current view** in the upper right corner to share a link to the view.

User Profile enhancements

The user profile page is now organized into three tabs: **Overview**, **Monitoring**, and **Properties**.

Overview tab

The overview tab contains key properties and insights about a user, such as:

- Properties like user principal name, object ID, created date/time, and user type
- Selectable aggregate values such as the number of groups that the user is a member of, the number of apps to which they have access, and the number of licenses that are assigned to them
- Quick alerts and insights about a user such as their current account enabled status, the last time they signed in, whether they can use multifactor authentication, and

B2B collaboration options

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with categories like Home, Favorites, Identity, Users, Groups, Devices, Applications, Protection, Identity governance, Verifiable credentials, and Learn & support. The main area is titled 'Overview page' under 'User'. A red box highlights the 'Overview' tab in the top navigation bar. Below it, there are three tabs: Overview (which is selected), Monitoring, and Properties. The 'Overview' section contains a 'Basic info' table with the following data:

User principal name	laimab@constoso.com	Group members...	2
Object ID	...	Applications	0
Created date time	Jun 11, 2020, 12:17 AM	Assigned roles	1
User type	Guest	Assigned licenses...	1
Identities	ExternalAzureAD		

Below this is a 'My Feed' section with two cards: 'Account status' (Enabled) and 'Sign-ins' (Last sign-in: May 10, 2021, 10:18 PM). There's also a link to 'See all sign-ins'.

ⓘ Note

Some insights about a user may not be visible to you unless you have sufficient role permissions.

Monitoring tab

The monitoring tab is the new home for the chart showing user sign-ins over the past 30 days.

Properties tab

The properties tab now contains more user properties. Properties are broken up into categories including Identity, Job information, Contact information, Parental controls, Settings, and On-premises.

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with various categories like Home, Favorites, Identity, Users, Groups, Devices, Applications, Roles & admins, Billing, Settings, Protection, Identity governance, External identities, User experiences, Hybrid management, Monitoring & health, and Learn & support. The 'Identity' section is expanded, and 'Overview' is selected, highlighted with a red box. The main content area shows a user profile for 'Laima Baniene'. At the top, there are buttons for Delete, Refresh, Reset password, Revoke sessions, and Got feedback? A search bar is also present. Below the header, there are tabs for Overview, Monitoring, and Properties, with 'Properties' being the active tab, also highlighted with a red box. The 'Identity' section contains a circular placeholder image and a table of user properties. The properties listed include:

	Value
Display name	Laima Baniene
First name	Laima
Last name	Baniene
User principal name	
Object ID	
Identities	ExternalAzureAD
User type	Guest
Creation type	Invitation
Created date time	Jun 11, 2020, 12:17 AM
Last password change	Jun 11, 2020, 12:17 AM
External user state	Accepted
External user state change date	Jun 11, 2020, 12:18 AM
Contact Information	
Street address	
City	
State or province	
ZIP or postal code	
Country or region	
Business phone	
Mobile phone	
Email	
Other emails	View
Proxy addresses	View
Fax number	
IM addresses	
Mail nickname	laimab@contoso.com
Parental controls	
Age group	

You can edit properties by selecting the pencil icon next to any category, which will then redirect you to a new editing experience. Here, you can search for specific properties or scroll through property categories. You can edit one or many properties, across categories, before selecting **Save**.

Laima Baniene

[Properties](#)[All](#) [Identity](#) [Job Information](#) [Contact Information](#) [Parental controls](#) [Settings](#) [On-premises](#)

Search

Showing 13 results

Display name

First name

Last name

User principal name

Object ID

User type

Guest



Creation type

Invitation

Created date time

2019-09-17T20:23:06Z

Last password change date time

2019-09-17T20:23:06Z

External user state

Accepted

External user state change date time

2019-09-20T17:19:54Z

Preferred language

Sign in sessions valid from date time

2019-09-17T20:23:06Z

[Save](#)[Cancel](#)

ⓘ Note

Some properties won't be visible or editable if they are read-only or if you don't have sufficient role permissions to edit them.

Next steps

User operations

- [Add or change profile information](#)
- [Add or delete users](#)

Bulk operations

- [Bulk operations service limitations](#)

- Download list of users
 - Bulk add users
 - Bulk delete users
 - Bulk restore users
-

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

Bulk delete users in Microsoft Entra ID

Article • 12/19/2024

Using the admin center in Microsoft Entra ID, part of Microsoft Entra, you can remove a large number of members to a group by using a comma-separated values (CSV) file to bulk delete users.

To bulk delete users

Tip

Steps in this article might vary slightly based on the portal you start from.

1. Sign in to the [Microsoft Entra admin center](#) as at least a [User Administrator](#).
2. Select Microsoft Entra ID.
3. Select **Users > All users > Bulk operations > Bulk delete**.

The screenshot shows the Microsoft Entra admin center interface. On the left, the navigation menu is open, with 'All users' selected under the 'Users' category. In the main content area, the 'All users' section is highlighted with a red box. At the top of this section, there is a search bar and several buttons: '+ New user', 'Download users', 'Bulk operations' (which is also highlighted with a red box), 'Refresh', 'Manage view', 'Delete', 'Per-user MFA', and 'Get feedback?'. Below the search bar, it says '1,845,603 users found'. A table lists user details: Display name, User principal name, User type, On-premises sync status, Identities, Company name, and Creation type. The table includes many entries starting with '.NET' and other system-related accounts like 'dbn2-bot@microsoft.com' and 'dotnetcomms@micr...'. The 'Bulk operations' button is located at the top right of the user list table.

4. On the **Bulk delete user** page, select **Download** to download the latest version of the CSV template.
5. Open the CSV file and add a line for each user you want to delete. The only required value is **User principal name**. Save the file.
6. On the **Bulk delete user** page, under **Upload your csv file**, browse to the file. When you select the file and select submit, validation of the CSV file starts.

7. When the file contents are validated, you'll see **File uploaded successfully**. If there are errors, you must fix them before you can submit the job.
8. When your file passes validation, select **Submit** to start the bulk operation that deletes the users.
9. When the deletion operation completes, you see a notification that the bulk operation succeeded.

If you experience errors, you can download and view the results file on the **Bulk operation results** page. The file contains the reason for each error. The file submission must match the provided template and include the exact column names. For more information about bulk operations limitations, see [Bulk delete service limits](#).

CSV template structure

The rows in the example downloaded CSV template below are as follows:

- **Version number:** The first row containing the version number must be included in the upload CSV.
- **Column headings:** `User name [userPrincipalName] Required`. Older versions of the template might vary.
- **Examples row:** We have included in the template an example of an acceptable value. `Example: chris@contoso.com` You must remove the example row and replace it with your own entries.

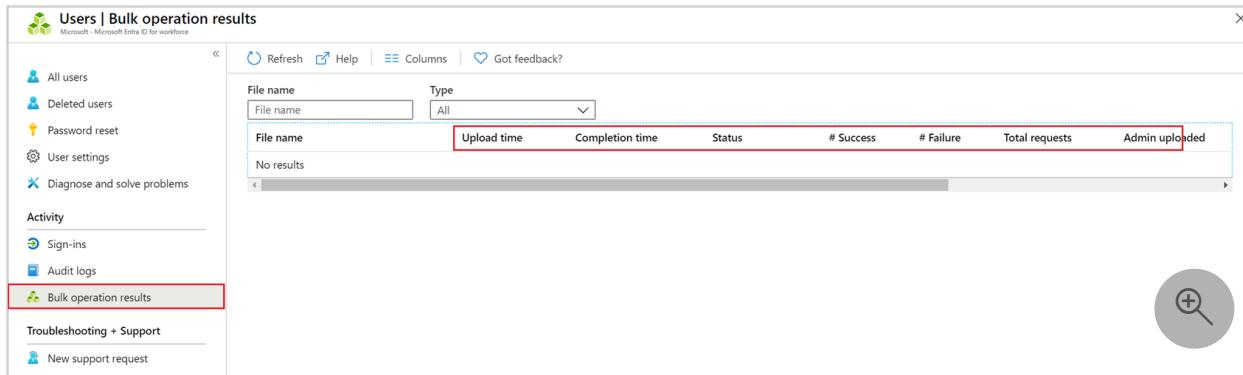
	A	B	C
1	version:v1.0		
2	User name [userPrincipalName] Required		
3	Example: chris@contoso.com		
4			

Additional guidance for the CSV template

- The first two rows of the template must not be removed or modified, or the template can't be processed.
- The required columns are listed first.
- Don't add new columns to the template. Any other columns you add are ignored and not processed.
- Download the latest version of the CSV template before making new changes.

Check status

You can see the status of all of your pending bulk requests in the **Bulk operation results** page.



The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with links like 'All users', 'Deleted users', 'Password reset', 'User settings', 'Diagnose and solve problems', 'Activity' (with 'Sign-ins' and 'Audit logs'), 'Bulk operation results' (which is highlighted with a red box), 'Troubleshooting + Support', and 'New support request'. The main content area has a header with 'Refresh', 'Help', 'Columns', and 'Got feedback?'. Below the header is a search bar with 'File name' and 'Type' dropdowns set to 'All'. A table titled 'File name' lists columns: 'File name', 'Upload time', 'Completion time', 'Status', '# Success', '# Failure', 'Total requests', and 'Admin uploaded'. The table body contains a single row labeled 'No results'. In the bottom right corner of the main area, there's a magnifying glass icon inside a circle.

Next, you can check to see that the users you deleted exist in the Microsoft Entra organization either in the portal or by using PowerShell.

Verify deleted users

1. Sign in to the [Microsoft Entra admin center](#) as at least a **User Administrator**.
2. Select Microsoft Entra ID.
3. Select **All users** only and verify that the users you deleted are no longer listed.

Verify deleted users with PowerShell

Run the following command:

```
PowerShell  
  
Get-MgUser -Filter "UserType eq 'Member'"
```

Verify that the users that you deleted are no longer listed.

Bulk delete service limits

Note

When performing bulk operations, such as import or create, you may encounter a problem if the bulk operation does not 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. For more information, see [Bulk operations service limitations](#).

Next steps

- [Bulk add users](#)
 - [Download list of users](#)
 - [Bulk restore users](#)
-

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Bulk restore deleted users in Microsoft Entra ID

Article • 12/19/2024

Microsoft Entra ID supports bulk user restore operations and downloading lists of users, groups, and group members.

Understand the CSV template

Download and fill in the CSV template to help you successfully restore Microsoft Entra users in bulk. The CSV template you download might look like this example:

	A	B
1	version:v1.0	
2	Object ID [objectId] Required	
3	Example: 9832aad8-e4fe-496b-a604-95c6eF01ae75	
4		

Row 1 must be preserved as-is, and the version number is always required.

Preserve the column headings as-is in row 2. Column headings indicate acceptable values and whether they're required. Don't add additional columns.

Use the entries in row 3 as examples. Remove the row's contents and replace the examples with your entries. Enter only one value per row.

CSV template structure

The rows in a downloaded CSV template are as follows:

- Version number:** The first row containing the version number must be included in the upload CSV.
- Column headings:** The format of the column headings is `<Item name> [PropertyName] <Required or blank>`. For example, `Object ID [objectId] Required`. Some older versions of the template might have slight variations.
- Examples row:** We have included in the template a row of examples of acceptable values for each column. You must remove the examples row and replace it with your own entries.

Additional guidance

- The first two rows of the upload template must not be removed or modified, or the upload can't be processed.

- The required columns are listed first.
- We don't recommend adding new columns to the template. Any additional columns you add are ignored and not processed.
- We recommend that you download the latest version of the CSV template as often as possible.

To bulk restore users

Tip

Steps in this article might vary slightly based on the portal you start from.

1. Sign in to the Microsoft Entra admin center [↗](#) as at least a **User Administrator**.
2. Select Microsoft Entra ID.
3. Select **All users > Users > Deleted**.
4. On the **Deleted users** page, select **Bulk restore** to upload a valid CSV file of properties of the users to restore.

The screenshot shows the Microsoft Entra admin center interface. On the left, the navigation menu is visible with various sections like Home, Identity, Groups, Applications, Protection, and Learn & support. The 'Deleted users' section under 'Users' is selected. In the main content area, the 'Deleted users' page is shown with a table listing three deleted users: Adele Vance (Member, Mar 29, 2024, 5:31 PM), Guest (Guest, Mar 29, 2024, 5:31 PM), and another user (Member, Mar 29, 2024, 5:31 PM). A 'Bulk restore' button is highlighted in red. To the right, a modal window titled 'Bulk restore users' is open. It contains three steps: 1. Download csv template (optional) with a 'Download' button (also highlighted in red). 2. Edit your csv file. 3. Upload your csv file with a 'Select a file' input field. At the bottom of the modal is a 'Submit' button.

5. Open the CSV template and add a line for each user you want to restore. The only required value is **ObjectID**. Then save the file.

A	B
1	version:v1.0
2	Object ID [objectId] Required
3	Example: 9832aad8-e4fe-496b-a604-95c6eF01ae75
4	

6. On the **Bulk restore** page, under **Upload your csv file**, browse to the file. When you select the file and select **Submit**, validation of the CSV file starts.
7. When the file contents are validated, you see **File uploaded successfully**. If there are errors, you must fix them before you can submit the job.
8. When your file passes validation, select **Submit** to start the bulk operation that restores the users.
9. When the restore operation completes, you see a notification that the bulk operation succeeded.

If you experience errors, you can download and view the results file on the **Bulk operation results** page. The file contains the reason for each error. The file submission must match the provided template and include the exact column names. For more information about bulk operations limitations, see [Bulk restore service limits](#).

Check status

You can see the status of all of your pending bulk requests in the **Bulk operation results** page.

File name	Upload time	Completion time	Status	# Success	# Failure	Total requests	Admin uploaded
No results							

Next, you can check to see that the users you restored exist in the Microsoft Entra organization via either Microsoft Entra ID or PowerShell.

View restored users in the Azure portal

1. Sign in to the [Microsoft Entra admin center](#) as at least a **User Administrator**.

2. Select Microsoft Entra ID.
3. Select All users Under Manage, select Users.
4. Under Show, select All users and verify that the users you restored are listed.

View users with PowerShell

Run the following command:

```
PowerShell  
  
Get-MgUser -Filter "UserType eq 'Member'"
```

You should see that the users that you restored are listed.

ⓘ 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.

Bulk restore service limits

ⓘ Note

When performing bulk operations, such as import or create, you may encounter a problem if the bulk operation does not 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. For more information, see [Bulk operations service limitations](#).

Next steps

- Bulk import users
 - Bulk delete users
 - Download list of users
-

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback 

Revoke user access in Microsoft Entra ID

Article • 01/07/2025

Scenarios that could require an administrator to revoke all access for a user include compromised accounts, employee termination, and other insider threats. Depending on the complexity of the environment, administrators can take several steps to ensure access is revoked. In some scenarios, there could be a period between the initiation of access revocation and when access is effectively revoked.

To mitigate the risks, you must understand how tokens work. There are many kinds of tokens, which fall into one of the patterns discussed in this article.

Access tokens and refresh tokens

Access tokens and refresh tokens are frequently used with thick client applications, and also used in browser-based applications such as single page apps.

- When users authenticate to Microsoft Entra ID, part of Microsoft Entra, authorization policies are evaluated to determine if the user can be granted access to a specific resource.
- Once authorized, Microsoft Entra ID issues an access token and a refresh token for the resource.
- If the authentication protocol allows, the app can silently reauthenticate the user by passing the refresh token to Microsoft Entra ID when the access token expires. By default, access tokens issued by Microsoft Entra ID last for 1 hour.
- Microsoft Entra ID then reevaluates its authorization policies. If the user is still authorized, Microsoft Entra ID issues a new access token and refreshes token.

Access tokens may pose a security risk if they need to be revoked within a period shorter than their typical one-hour lifespan. For this reason, Microsoft is actively working to bring [continuous access evaluation](#) to Office 365 applications, which helps ensure invalidation of access tokens in near real time.

Session tokens (cookies)

Most browser-based applications use session tokens instead of access and refresh tokens.

- When a user opens a browser and authenticates to an application via Microsoft Entra ID, the user receives two session tokens. One from Microsoft Entra ID and

another from the application.

- Once the application issues its own session token, the application controls access based on its authorization policies.
- The authorization policies of Microsoft Entra ID are reevaluated as often as the application sends the user back to Microsoft Entra ID. Reevaluation usually happens silently, though the frequency depends on how the application is configured. It's possible that the app may never send the user back to Microsoft Entra ID as long as the session token is valid.
- For a session token to be revoked, the application must revoke access based on its own authorization policies. Microsoft Entra ID can't directly revoke a session token issued by an application.

Revoke access for a user in the hybrid environment

For a hybrid environment with on-premises Active Directory synchronized with Microsoft Entra ID, Microsoft recommends IT admins to take the following actions. If you have a **Microsoft Entra-only environment**, skip to the [Microsoft Entra environment](#) section.

On-premises Active Directory environment

As an admin in the Active Directory, connect to your on-premises network, open PowerShell, and take the following actions:

- Disable the user in Active Directory. Refer to [Disable-ADAccount](#).

```
PowerShell
```

```
Disable-ADAccount -Identity johndoe
```

- Reset the user's password twice in the Active Directory. Refer to [Set-ADAccountPassword](#).

ⓘ Note

The reason for changing a user's password twice is to mitigate the risk of pass-the-hash, especially if there are delays in on-premises password

replication. If you can safely assume this account isn't compromised, you may reset the password only once.

ⓘ Important

Don't use the example passwords in the following cmdlets. Be sure to change the passwords to a random string.

PowerShell

```
Set-ADAccountPassword -Identity johndoe -Reset -NewPassword (ConvertTo-SecureString -AsPlainText "p@ssw0rd1" -Force)
Set-ADAccountPassword -Identity johndoe -Reset -NewPassword (ConvertTo-SecureString -AsPlainText "p@ssw0rd2" -Force)
```

Microsoft Entra environment

As an administrator in Microsoft Entra ID, open PowerShell, run `Connect-MgGraph`, and take the following actions:

1. Disable the user in Microsoft Entra ID. Refer to [Update-MgUser](#).

PowerShell

```
$User = Get-MgUser -Search UserPrincipalName:'johndoe@contoso.com' -ConsistencyLevel eventual
Update-MgUser -UserId $User.Id -AccountEnabled:$false
```

2. Revoke the user's Microsoft Entra ID refresh tokens. Refer to [Revoke-MgUserSignInSession](#).

PowerShell

```
Revoke-MgUserSignInSession -UserId $User.Id
```

3. Disable the user's devices. Refer to [Get-MgUserRegisteredDevice](#).

PowerShell

```
$Device = Get-MgUserRegisteredDevice -UserId $User.Id
Update-MgDevice -DeviceId $Device.Id -AccountEnabled:$false
```

Note

For information on specific roles that can perform these steps review [Microsoft Entra built-in roles](#)

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.

When access is revoked

Once admins take the above steps, the user can't gain new tokens for any application tied to Microsoft Entra ID. The elapsed time between revocation and the user losing their access depends on how the application is granting access:

- For **applications using access tokens**, the user loses access when the access token expires.
- For **applications that use session tokens**, the existing sessions end as soon as the token expires. If the disabled state of the user is synchronized to the application, the application can automatically revoke the user's existing sessions if it's configured to do so. The time it takes depends on the frequency of synchronization between the application and Microsoft Entra ID.

Best practices

- Deploy an automated provisioning and deprovisioning solution. Deprovisioning users from applications is an effective way of revoking access, especially for applications that use sessions tokens or allow users to sign in directly without a Microsoft Entra or Windows Server AD token. Develop a process to also

deprovision users to apps that don't support automatic provisioning and deprovisioning. Ensure applications revoke their own session tokens and stop accepting Microsoft Entra access tokens even if they're still valid.

- Use [Microsoft Entra app provisioning](#). Microsoft Entra app provisioning typically runs automatically every 20-40 minutes. [Configure Microsoft Entra provisioning](#) to deprovision or deactivate users in SaaS and on-premises applications. If you were using [Microsoft Identity Manager](#) to automate the deprovisioning of users from on-premises applications, you can use Microsoft Entra app provisioning to reach on-premises applications with a [SQL database, non-AD directory server](#) or [other connectors](#).
 - For on-premises applications using Windows Server AD, you can configure Microsoft Entra Lifecycle Workflows to [update users in AD \(preview\)](#) when employees leave.
 - Identify and develop a process for applications that require manual deprovisioning. For example, the [automated ServiceNow ticket creation with Microsoft Entra Entitlement Management](#) can open a ticket when employees lose access. Ensure admins and application owners can quickly run the required manual tasks to deprovision the user from these apps when needed.
- Manage your devices and applications with [Microsoft Intune](#). Intune-managed devices can be reset to factory settings. If the device is unmanaged, you can [wipe the corporate data from managed apps](#). These processes are effective for removing potentially sensitive data from end users' devices. However, for either process to be triggered, the device must be connected to the internet. If the device is offline, it still has access to any locally stored data.

 **Note**

Data on the device can't be recovered after a wipe.

- Use [Microsoft Defender for Cloud Apps to block data download](#) when appropriate. If the data can only be accessed online, organizations can monitor sessions and achieve real-time policy enforcement.
- Use [Continuous Access Evaluation \(CAE\) in Microsoft Entra ID](#). CAE allows admins to revoke the session tokens and access tokens for applications that are CAE capable.

Next steps

- Secure access practices for Microsoft Entra administrators
 - Add or update user profile information
 - Remove or Delete a former employee
-

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Close your work or school account in an unmanaged Microsoft Entra organization

Article • 11/18/2024

If you are a user in an unmanaged organization (tenant) in Microsoft Entra ID, and you no longer need to use apps from that organization or maintain any association with it, you can close your account at any time. An unmanaged organization does not have an administrator. Users in an unmanaged organization can close their accounts on their own, without contacting an administrator.

Users in an unmanaged organization are often created during self-service sign-up. An example of this occurring is when an information worker in an organization signs up for a free service. For more information about self-service sign-up, see [What is self-service sign-up for Microsoft Entra ID?](#).

Note

This article provides steps about how to delete personal data from the device or service and can be used to support your obligations under the GDPR. For general information about GDPR, see the [GDPR section of the Microsoft Trust Center](#) and the [GDPR section of the Service Trust portal](#).

Before you begin

Before you can close your account, you'll need to confirm the following items:

- Make sure you are a user of an unmanaged Microsoft Entra organization. You can't close your account if you belong to a managed organization. If you belong to a managed organization and want to close your account, you must contact your administrator. For information about how to determine whether you belong to an unmanaged organization, see [Delete the user from Unmanaged Tenant](#).
- Save any data you want to keep. For information about how to submit an export request, see [Accessing and exporting system-generated logs for Unmanaged Tenants](#).

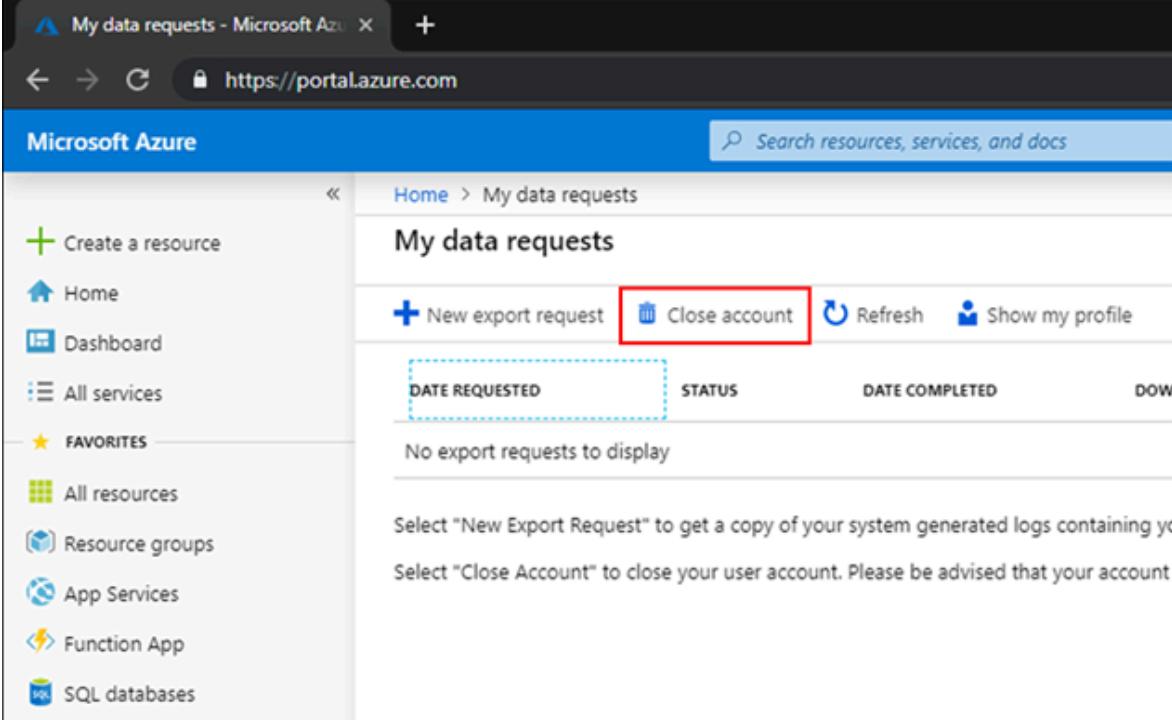
Warning

Closing your account is irreversible. When you close your account, all personal data will be removed. You won't have access to your account and you will no longer have access to the data associated with your account.

Close your account

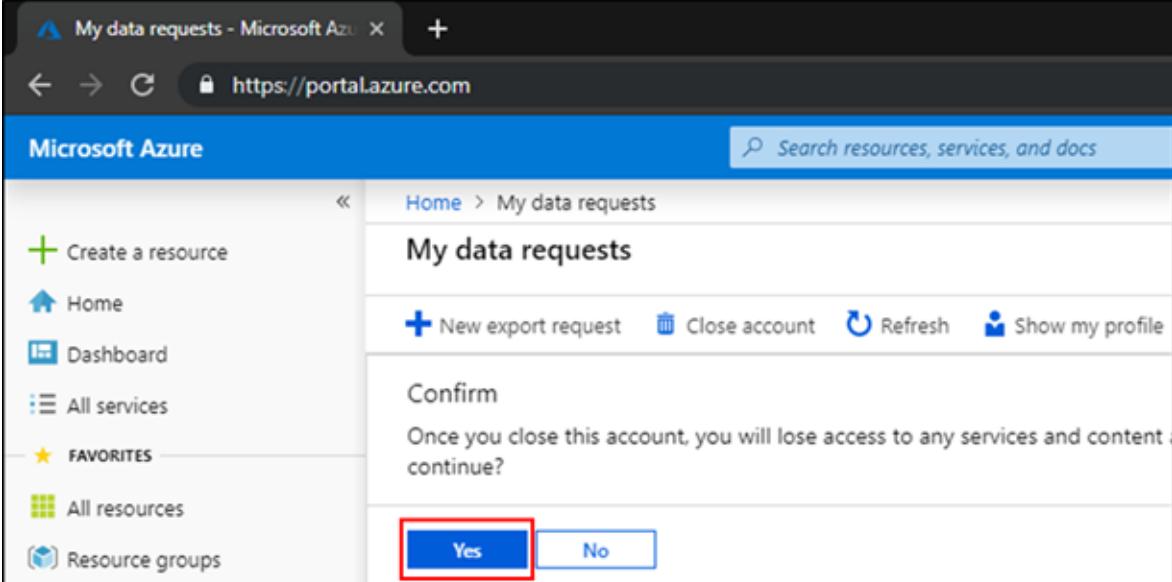
To close an unmanaged work or school account, follow these steps:

1. Sign in to [close your account](#), using the account that you want to close.
2. On **My data requests**, select **Close account**.



The screenshot shows the Microsoft Azure portal interface. The left sidebar includes links for 'Create a resource', 'Home', 'Dashboard', 'All services', and 'FAVORITES' (which lists 'All resources', 'Resource groups', 'App Services', 'Function App', and 'SQL databases'). The main content area is titled 'My data requests'. It features a toolbar with 'New export request', 'Close account' (which is highlighted with a red box), 'Refresh', and 'Show my profile'. Below the toolbar is a table with columns 'DATE REQUESTED', 'STATUS', 'DATE COMPLETED', and 'DOW'. A message below the table states 'No export requests to display'. At the bottom, there's a note: 'Select "New Export Request" to get a copy of your system generated logs containing your data. Select "Close Account" to close your user account. Please be advised that your account'. The URL in the browser bar is https://portal.azure.com.

3. Review the confirmation message and then select **Yes**.



The screenshot shows the Microsoft Azure portal interface after selecting 'Close account'. A confirmation dialog box is displayed in the center. It contains the text 'Confirm' and 'Once you close this account, you will lose access to any services and content. Continue?'. At the bottom are two buttons: 'Yes' (highlighted with a red box) and 'No'. The URL in the browser bar is https://portal.azure.com.

Next steps

- [What is self-service sign-up for Microsoft Entra ID?](#)
 - [Delete the user from Unmanaged Tenant](#)
 - [Accessing and exporting system-generated logs for Unmanaged Tenants](#)
-

Feedback

Was this page helpful?

 Yes

 No

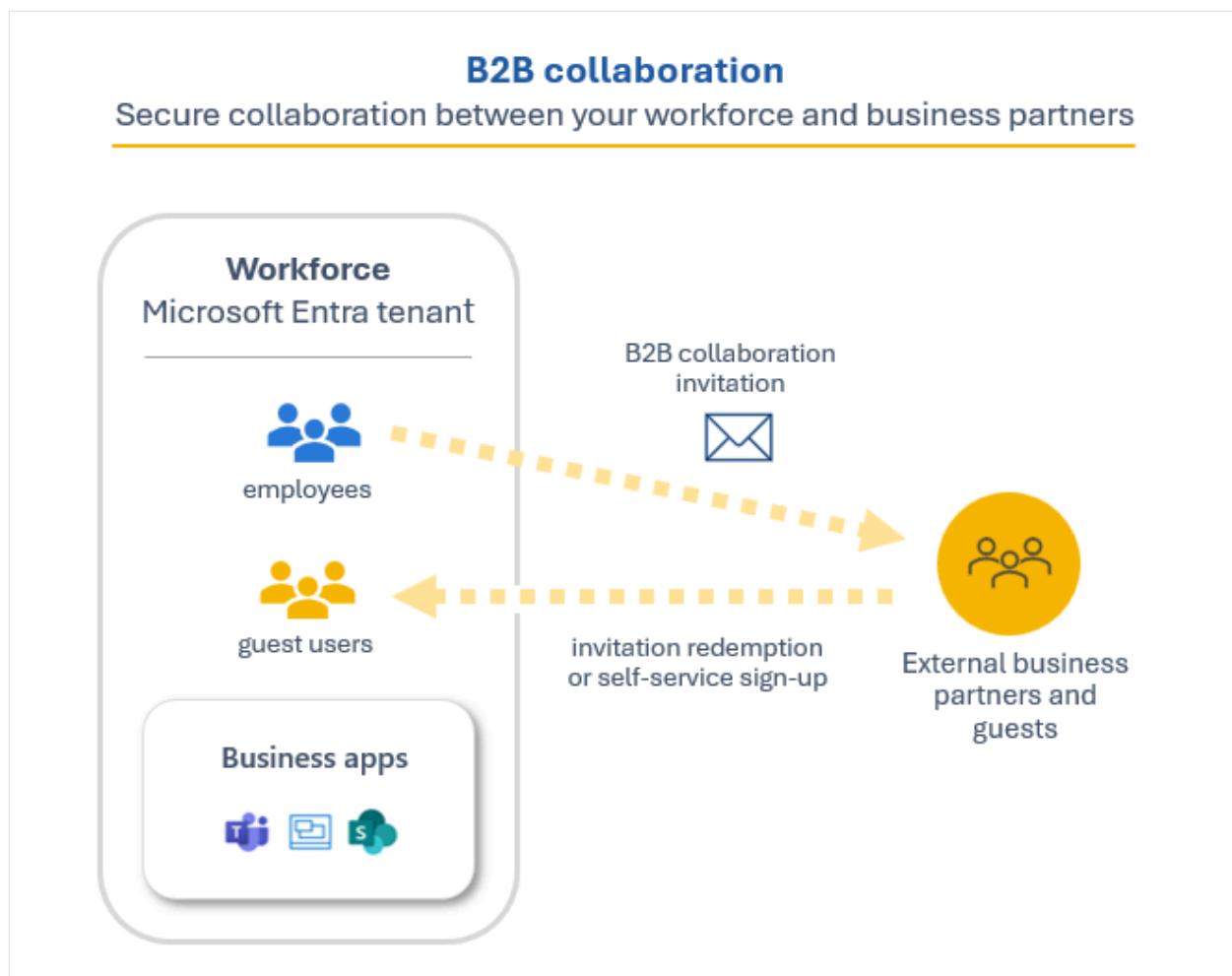
[Provide product feedback](#) ↗

Overview: B2B collaboration with external guests for your workforce

Article • 02/19/2025

Applies to: ✓ Workforce tenants ✖ External tenants ([learn more](#))

Microsoft Entra External ID includes collaboration capabilities that allow your workforce to work securely with business partners and guests. In your workforce tenant, you can use B2B collaboration to share your company's applications and services with guests, while maintaining control over your own corporate data. Work securely with external partners, even if they don't have Microsoft Entra ID or an IT department.



A simple invitation and redemption process lets partners use their own credentials to access your company's resources. You can also enable self-service sign-up user flows to let guests sign up for apps or resources themselves. Once the guest redeems their invitation or completes sign-up, they're represented in your directory as a user object. The user type for these B2B collaboration users is typically set to "guest" and their user principal name contains the #EXT# identifier.

Developers can use Microsoft Entra business-to-business APIs to customize the invitation process or write applications like self-service sign-up portals. For licensing and pricing information related to guest users, refer to [Billing model for Microsoft Entra External ID](#).

 **Important**

The [email one-time passcode](#) feature is now turned on by default for all new tenants and for any existing tenants where you haven't explicitly turned it off. When this feature is turned off, the fallback authentication method is to prompt invitees to create a Microsoft account.

Collaborate with any partner using their identities

With Microsoft Entra B2B, the partner uses their own identity management solution, so there's no external administrative overhead for your organization. Guest users sign in to your apps and services with their own work, school, or social identities.

- The partner uses their own identities and credentials, whether or not they have a Microsoft Entra account.
- You don't need to manage external accounts or passwords.
- You don't need to sync accounts or manage account lifecycles.

Manage B2B collaboration with other organizations

B2B collaboration is enabled by default, but comprehensive admin settings let you control your inbound and outbound B2B collaboration with external partners and organizations.

- **Cross-tenant access settings.** For B2B collaboration with other Microsoft Entra organizations, use [cross-tenant access settings](#) to control which users can authenticate with which resources. Manage inbound and outbound B2B collaboration, and scope access to specific users, groups, and applications. Set a default configuration that applies to all external organizations, and then create individual, organization-specific settings as needed. Using cross-tenant access settings, you can also trust multifactor (MFA) and device claims (compliant claims and Microsoft Entra hybrid joined claims) from other Microsoft Entra organizations.

- **External collaboration settings.** Use [external collaboration settings](#) to define who can invite external users into your organization as guests. By default, all users in your organization, including B2B collaboration guest users, can invite external users to B2B collaboration. If you want to limit the ability to send invitations, you can turn invitations on or off for everyone, or limit invitations to certain roles. You can also allow or block B2B specific domains and set restrictions on guest user access to your directory.

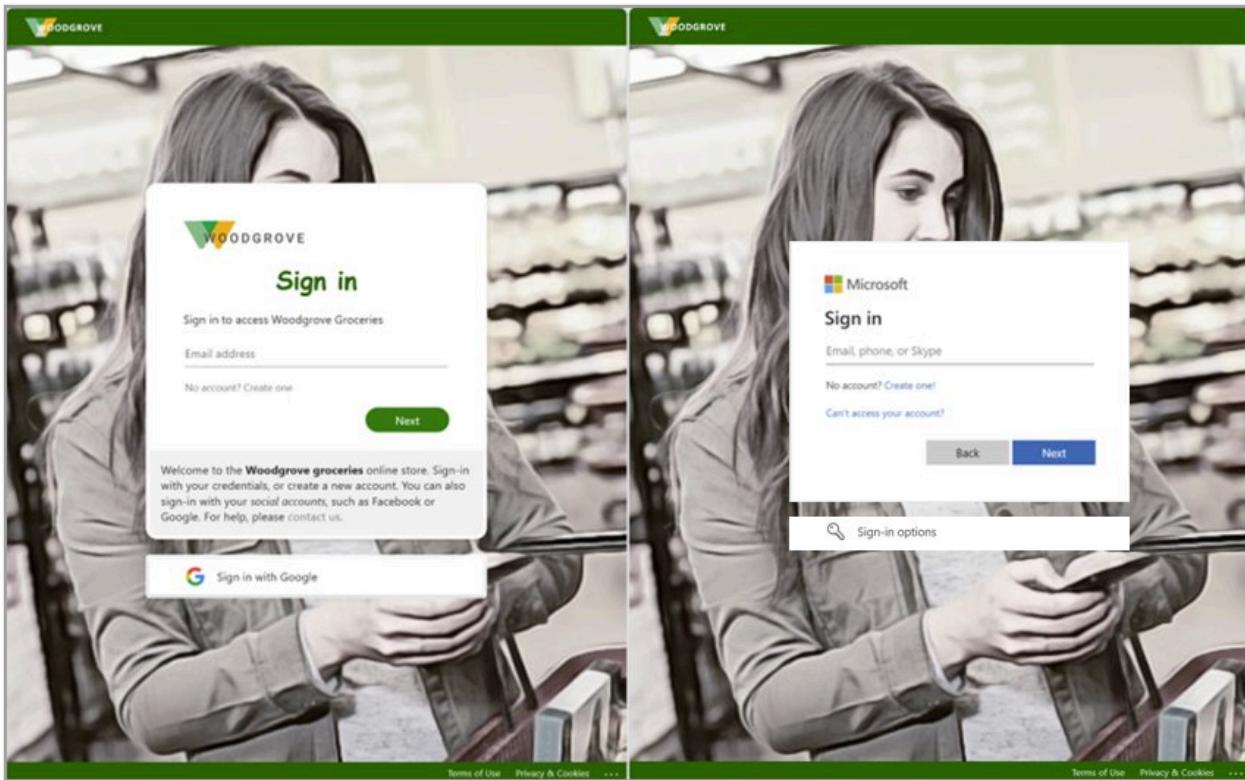
These settings are used to manage two different aspects of B2B collaboration. Cross-tenant access settings control whether users can authenticate with external Microsoft Entra tenants. They apply to both inbound and outbound B2B collaboration. By contrast, external collaboration settings control which users in your organization are allowed to send B2B collaboration invitations to guests from any organization.

How cross-tenant access and external collaboration settings work together

When you're considering B2B collaboration with a specific external Microsoft Entra organization, determine whether your cross-tenant access settings allow B2B collaboration with that organization. Also consider whether your external collaboration settings allow your users to send invitations to that organization's domain. Here are some examples:

- **Example 1:** You previously added `adatum.com` (a Microsoft Entra organization) to the list of blocked domains in your external collaboration settings, but your cross-tenant access settings enable B2B collaboration for all Microsoft Entra organizations. In this case, the most restrictive setting applies. Your external collaboration settings prevent your users from sending invitations to users at `adatum.com`.
- **Example 2:** You allow B2B collaboration with Fabrikam in your cross-tenant access settings, but then you add `fabrikam.com` to your blocked domains in your external collaboration settings. Your users can't invite new Fabrikam business guests, but existing Fabrikam guests can continue using B2B collaboration.

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. The example on the right displays the default branding for the user's home tenant.



Manage B2B collaboration with other Microsoft Clouds

Microsoft Azure cloud services are available in separate national clouds, which are physically isolated instances of Azure. Increasingly, organizations are finding the need to collaborate with organizations and users across global cloud and national cloud boundaries. With Microsoft cloud settings, you can establish mutual B2B collaboration between the following Microsoft Azure clouds:

- Microsoft Azure global cloud and [Microsoft Azure Government](#)
- Microsoft Azure global cloud and [Microsoft Azure operated by 21Vianet](#)

To set up B2B collaboration between tenants in different clouds, both tenants configure their Microsoft cloud settings to enable collaboration with the other cloud. Then each tenant configures inbound and outbound cross-tenant access with the tenant in the other cloud. See [Microsoft cloud settings](#) for details.

Easily invite guest users from the Microsoft Entra admin center

As an administrator, you can easily add guest users to your organization in the admin center.

- [Create a new guest user](#) in Microsoft Entra ID, similar to how you'd add a new user.
- Assign guest users to apps or groups.

- Send an invitation email that contains a redemption link, or send a direct link to an app you want to share.

Microsoft Entra admin center

Search resources, services, and docs (G+)

Home > Users > Invite external user

Invite an external user to collaborate with your organization

Basics Properties Assignments Review + invite

Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating. Learn more

Identity

Email

Display name

Invitation message

Send invite message

Message

Cc recipient

- Guest users follow a few simple redemption steps to sign in.

Microsoft

Review permissions

Contoso contoso.com

This resource is not shared by Microsoft.

The organization Contoso would like to:

- ✓ Sign you in
- ✓ Read your name, email address, and photo

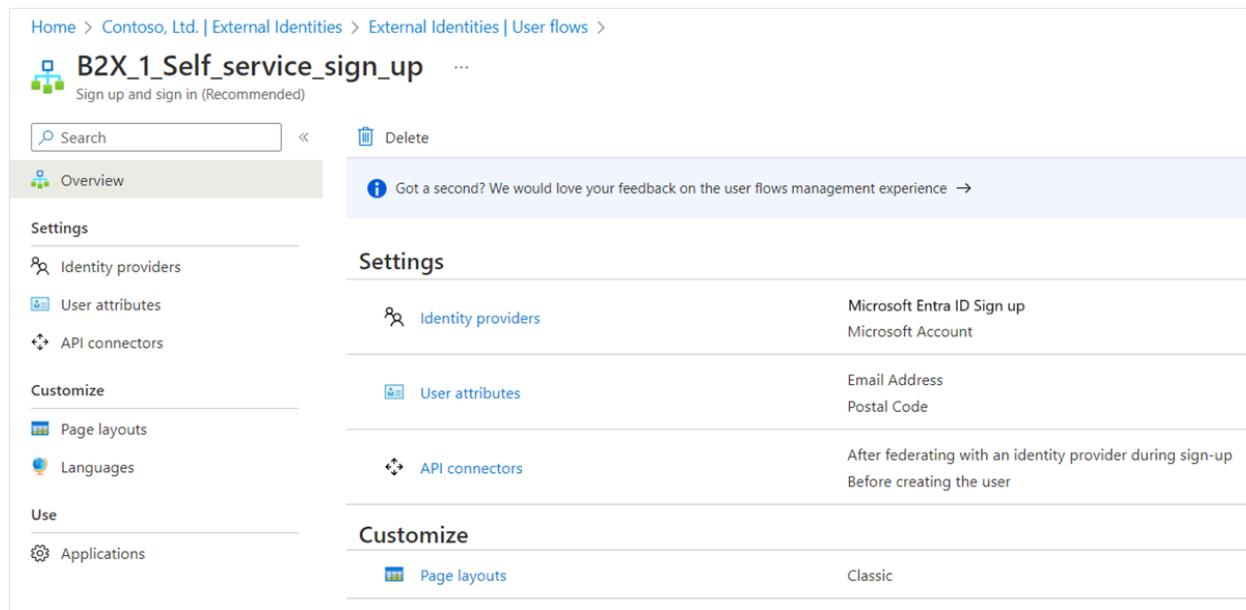
You should only accept if you trust Contoso. By accepting, you allow this organization to access and process your data to create, control, and administer an account according to their policies. [Read Contoso's privacy statement](#). Contoso may log information about your access. You can remove these permissions at <https://myapps.microsoft.com/contoso.com>

Cancel Accept

Allow self-service sign-up

With a self-service sign-up user flow, you can create a sign-up experience for guests who want to access your apps. As part of the sign-up flow, you can provide options for different social or enterprise identity providers, and collect information about the user. Learn about [self-service sign-up and how to set it up](#).

You can also use API connectors to integrate your self-service sign-up user flows with external cloud systems. You can connect with custom approval workflows, perform identity verification, validate user-provided information, and more.



The screenshot shows the Microsoft Entra ID portal interface for managing user flows. The top navigation bar includes 'Home', 'Contoso, Ltd.', 'External Identities', 'External Identities', 'User flows', and a search bar. The main title is 'B2X_1_Self_service_sign_up' with a 'Sign up and sign in (Recommended)' badge. A 'Delete' button is visible. A feedback message says, 'Got a second? We would love your feedback on the user flows management experience'. The left sidebar has sections for 'Overview', 'Settings' (Identity providers, User attributes, API connectors), 'Customize' (Page layouts, Languages), and 'Use' (Applications). The 'Settings' section on the right lists configurations: 'Identity providers' (Microsoft Entra ID Sign up, Microsoft Account); 'User attributes' (Email Address, Postal Code); 'API connectors' (After federating with an identity provider during sign-up, Before creating the user); and 'Customize' (Page layouts set to 'Classic').

Use policies to securely share your apps and services

You can use authentication and authorization policies to protect your corporate content. Conditional Access policies, such as multifactor authentication, can be enforced:

- At the tenant level
- At the application level
- For specific guest users to protect corporate apps and data

Security | Getting started

The screenshot shows the Microsoft Security | Getting started page. At the top left is a search bar with a magnifying glass icon. To its right is a back arrow icon. Below the search bar is a grey navigation bar containing two items: 'Getting started' with a gear icon and 'Diagnose and solve problems' with a cross icon. To the right of the navigation bar is a blue square icon with a white diagonal line pattern. The main content area has a heading 'Protect' followed by a horizontal line. Below this are five items: 'Conditional Access' with a green shield icon, 'Identity Protection' with a blue person icon, 'Security Center' with a blue lock icon, and 'Verifiable credentials (Preview)' with a purple shield icon. The 'Conditional Access' item is highlighted with a red rectangular border.

Let application and group owners manage their own guest users

You can delegate guest user management to application owners. This allows them to add guest users directly to any application they want to share, whether it's a Microsoft application or not.

- Administrators set up self-service app and group management.
- Nonadministrators use their [Access Panel](#) to add guest users to applications or groups.

The screenshot shows the Microsoft Access Panel interface. At the top is a browser-style header with 'My Apps' and a search bar labeled 'Search apps'. Below the header is a toolbar with icons for 'Edit', 'List view', and more. The main area is titled 'My Apps' and shows a grid of application icons: Salesforce, Google Cloud / G Suite Connector by.., Oracle Access Manager for Oracle.., and SAP Cloud Platform. In the bottom-left corner of the grid, there is a context menu for the Salesforce icon. The menu items are 'Copy link', 'Manage your application' (which is highlighted with a red rectangular border), 'Remove', and '+ Add to collection'. To the right of the grid is a large circular button with a magnifying glass and a plus sign inside.

Customize the onboarding experience for B2B guest users

Bring your external partners on board in ways customized to your organization's needs.

- Use [Microsoft Entra entitlement management](#) to configure policies that [manage access for external users](#).
- Use the [B2B collaboration invitation APIs](#) to customize your onboarding experiences.

Integrate with Identity providers

Microsoft Entra External ID supports external identity providers like Facebook, Microsoft accounts, Google, or enterprise identity providers. You can set up federation with identity providers. This way your guests can sign in with their existing social or enterprise accounts instead of creating a new account just for your application. Learn more about [identity providers for External ID](#).

The screenshot shows the Microsoft Entra External Identities interface. The left sidebar has a navigation menu with items like Overview, Cross-tenant access settings, All identity providers (which is selected and highlighted in grey), External collaboration settings, Diagnose and solve problems, Self-service sign up, Custom user attributes, All API connectors, and Custom authentication extensions (Preview). The main content area is titled "External Identities | All identity providers" and shows "Contoso - Microsoft Entra ID for workforce". It includes a search bar, navigation links for Google, Facebook, and New SAML/WS-Fed IdP, and a "Got feedback?" link. The "Configured identity providers" section lists Microsoft Entra ID, Microsoft Account, and Email one-time passcode. The "SAML/WS-Fed identity providers" section has a search bar and tabs for Display name, Configuration, and Domains.

Integrate with SharePoint and OneDrive

You can [enable integration with SharePoint and OneDrive](#) to share files, folders, list items, document libraries, and sites with people outside your organization, while using Microsoft Entra B2B for authentication and management. The users you share resources with are typically guest users in your directory, and permissions and groups work the same for these guests as they do for internal users. When enabling integration with

SharePoint and OneDrive, you also enable the [email one-time passcode](#) feature in Microsoft Entra B2B to serve as a fallback authentication method.

Configure identity provider

i Users who don't already have a Microsoft Entra or Microsoft account can sign in without having to create an account. Each time the user signs in to your directory, they receive a passcode via email for authentication. You can also enable self-service sign-up with email one-time passcode for specific apps in your user flows. ↗

Email one-time passcode for guests

Yes No

Related content

To learn more about B2B collaboration users, see the following article: [Add B2B collaboration guest users in the admin center](#). To learn more about how to establish mutual trust relationships between organizations for seamless collaboration using Microsoft Teams shared channels, see the following article: [B2B direct connect](#).

Feedback

Was this page helpful?

👍 Yes

👎 No

[Provide product feedback ↗](#)

Restrict guest access permissions in Microsoft Entra ID

Article • 12/19/2024

Microsoft Entra ID, part of Microsoft Entra, allows you to restrict what external guest users can see in their organization in Microsoft Entra ID. Guest users are set to a limited permission level by default in Microsoft Entra ID, while the default for member users is the full set of user permissions. There's another guest user permission level in your Microsoft Entra organization's external collaboration settings for even more restricted access, so that the guest access levels are:

[+] Expand table

Permission level	Access level	Value
Same as member users	Guests have the same access to Microsoft Entra resources as member users	a0b1b346-4d3e-4e8b-98f8-753987be4970
Limited access (default)	Guests can see membership of all non-hidden groups	10dae51f-b6af-4016-8d66-8c2a99b929b3
Restricted access (new)	Guests can't see membership of any groups	2af84b1e-32c8-42b7-82bc-daa82404023b

When guest access is restricted, guests can view only their own user profile. Permission to view other users isn't allowed even if the guest is searching by User Principal Name or objectId. Restricted access also restricts guest users from seeing the membership of groups they're in. For more information about the overall default user permissions, including guest user permissions, see [What are the default user permissions in Microsoft Entra ID?](#).

Update in the Microsoft Entra admin center



Steps in this article might vary slightly based on the portal you start from.

We've made changes to the existing Azure portal controls for guest user permissions.

1. Sign in to the [Microsoft Entra admin center](#) as a [User administrator](#).

2. Select **Identity > External Identities**.
3. Select **External collaboration settings**.
4. On the **External collaboration settings** page, select **Guest user access is restricted to properties and memberships of their own directory objects** option.

External collaboration settings

Save Discard

Email one-time passcode for guests has been moved to All Identity Providers. →

Guest user access

Guest user access restrictions ⓘ

[Learn more](#)

Guest users have the same access as members (most inclusive)
 Guest users have limited access to properties and memberships of directory objects
 Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

Guest invite settings

Guest invite restrictions ⓘ

[Learn more](#)

Anyone in the organization can invite guest users including guests and non-admins (most inclusive)
 Member users and users assigned to specific admin roles can invite guest users including guests with member permissions
 Only users assigned to specific admin roles can invite guest users
 No one in the organization can invite guest users including admins (most restrictive)

Enable guest self-service sign up via user flows ⓘ

[Learn more](#)

Yes No

External user leave settings

Allow external users to remove themselves from your organization (recommended) ⓘ

[Learn more](#)

Yes No

Collaboration restrictions

Allow invitations to be sent to any domain (most inclusive)
 Deny invitations to the specified domains
 Allow invitations only to the specified domains (most restrictive)

5. Select **Save**. The changes can take up to 15 minutes to take effect for guest users.

Update with the Microsoft Graph API

There is a new Microsoft Graph API to configure guest permissions in your Microsoft Entra organization. The following API calls can be made to assign any permission level.

The value for guestUserId used here is to illustrate the most restricted guest user setting. For more information about using the Microsoft Graph to set guest permissions, see [authorizationPolicy resource type](#).

Configuring for the first time

PowerShell

```
POST  
https://graph.microsoft.com/beta/policies/authorizationPolicy/authorizationPolicy  
  
{  
    "guestUserId": "2af84b1e-32c8-42b7-82bc-daa82404023b"  
}
```

Response should be Success 204.

ⓘ 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.

Updating the existing value

PowerShell

```
PATCH  
https://graph.microsoft.com/beta/policies/authorizationPolicy/authorizationPolicy  
  
{  
    "guestUserId": "2af84b1e-32c8-42b7-82bc-daa82404023b"  
}
```

Response should be Success 204.

View the current value

PowerShell

```
GET  
https://graph.microsoft.com/beta/policies/authorizationPolicy/authorizationPolicy
```

Example response:

PowerShell

```
{  
    "@odata.context":  
    "https://graph.microsoft.com/beta/$metadata#policies/authorizationPolicy/$entity",  
    "id": "authorizationPolicy",  
    "displayName": "Authorization Policy",  
    "description": "Used to manage authorization related settings across the company.",  
    "enabledPreviewFeatures": [],  
    "guestUserRole": "10dae51f-b6af-4016-8d66-8c2a99b929b3",  
    "permissionGrantPolicyIdsAssignedToDefaultUserRole": [  
        "user-default-legacy"  
    ]  
}
```

Update with PowerShell cmdlets

With this feature, we've added the ability to configure the restricted permissions via PowerShell v2 cmdlets. Get and Update PowerShell cmdlets have been published in version 2.0.2.85.

Get command: Get-MgPolicyAuthorizationPolicy

Example:

PowerShell

```
Get-MgPolicyAuthorizationPolicy | Format-List
```

Output

```
AllowEmailVerifiedUsersToJoinOrganization : True
AllowInvitesFrom                      : everyone
AllowUserConsentForRiskyApps          :
AllowedToSignUpEmailBasedSubscriptions : True
AllowedToUseSspr                       : True
BlockMsolPowerShell                   : False
DefaultUserRolePermissions            :
Microsoft.Graph.PowerShell.Models.MicrosoftGraphDefaultUserRolePermissions
DeletedDateTime                      :
Description                           : Used to manage authorization
related settings across the company.
DisplayName                          : Authorization Policy
GuestUserRole_Id                     : 10dae51f-b6af-4016-8d66-
8c2a99b929b3
Id                                  : authorizationPolicy
AdditionalProperties                 : {[@odata.context,
https://graph.microsoft.com/v1.0/$metadata#policies/authorizationPolicy/$ent
ity]}}
```

Update command: Update-MgPolicyAuthorizationPolicy

Example:

PowerShell

```
Update-MgPolicyAuthorizationPolicy -GuestUserRole_Id '2af84b1e-32c8-42b7-
82bc-daa82404023b'
```

Supported Microsoft 365 services

Supported services

By supported we mean that the experience is as expected; specifically, that it's same as current guest experience.

- Teams
- Outlook (OWA)
- SharePoint
- Planner in Teams
- Planner mobile app
- Planner web app
- Project for the web
- Project Operations

Services currently not supported

Service without current support might have compatibility issues with the new guest restriction setting.

- Forms
- Project Online
- Yammer
- Planner in SharePoint

Frequently asked questions (FAQ)

[] Expand table

Question	Answer
Where do these permissions apply?	<p>These directory level permissions are enforced across Microsoft Entra services including the Microsoft Graph, PowerShell v2, the Azure portal, and My Apps portal. Microsoft 365 services using Microsoft 365 groups for collaboration scenarios are also affected, specifically Outlook, Microsoft Teams, and SharePoint.</p>
How do restricted permissions affect which groups guests can see?	<p>Regardless of default or restricted guest permissions, guests can't enumerate the list of groups or users. Guests can see groups they're members of in both the Azure portal and the My Apps portal depending on permissions:</p> <ul style="list-style-type: none">• Default permissions: To find the groups they're members of in the Azure portal, the guest must search for their object ID in the All users list, and then select Groups. Here they can see the list of groups that they're members of, including all the group details, including name, email, and so on. In the My Apps portal, they can see a list of groups they own and groups they're in.• Restricted guest permissions: In the Azure portal, they can find the list of groups they're in by searching for their object ID in the All users list, and then selecting Groups. They can see only limited details about the group, notably the object ID. By design, the Name and Email columns are blank and Group Type is Unrecognized. In the My Apps portal, they're not able to access the list of groups they own or groups they're a member of.
	<p>For more detailed comparison of the directory permissions that come from the Graph API, see Default user permissions.</p>
Which parts of the My Apps portal will this feature affect?	<p>The groups functionality in the My Apps portal honors these new permissions. This functionality includes all paths to view the groups list and group memberships in My Apps. No changes were made to the</p>

Question	Answer
	group tile availability. The group tile availability is still controlled by the existing group setting in the Azure portal.
Do these permissions override SharePoint or Microsoft Teams guest settings?	No. Those existing settings still control the experience and access in those applications. For example, if you see issues in SharePoint, double check your external sharing settings. Guests added by team owners at the team level have access to channel meeting chat only for standard channels, excluding any private and shared channels.
What are the known compatibility issues in Yammer?	With permissions set to "restricted", guests signed into Yammer aren't able to leave the group.
Will my existing guest permissions be changed in my tenant?	No changes were made to your current settings. We maintain backward compatibility with your existing settings. You decide when you want to make changes.
Will these permissions be set by default?	No. The existing default permissions remain unchanged. You can optionally set the permissions to be more restrictive.
Are there any license requirements for this feature?	No, there are no new licensing requirements with this feature.

Next steps

- To learn more about existing guest permissions in Microsoft Entra ID, see [What are the default user permissions in Microsoft Entra ID?](#)
- To see the Microsoft Graph API methods for restricting guest access, see [authorizationPolicy resource type](#)
- To revoke all access for a user, see [Revoke user access in Microsoft Entra ID](#)

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

Clean up unmanaged Microsoft Entra accounts

Article • 10/23/2023

Prior to August 2022, Microsoft Entra B2B supported self-service sign-up for email-verified users. With this feature, users create Microsoft Entra accounts, when they verify email ownership. These accounts were created in unmanaged (or viral) tenants: users created accounts with an organization domain, not under IT team management. Access persists after users leave the organization.

To learn more, see, [What is self-service sign-up for Microsoft Entra ID?](#)

Note

Unmanaged Microsoft Entra accounts via Microsoft Entra B2B were deprecated. As of August 2022, new B2B invitations can't be redeemed. However, invitations prior to August 2022 were redeemable with unmanaged Microsoft Entra accounts.

Remove unmanaged Microsoft Entra accounts

Use the following guidance to remove unmanaged Microsoft Entra accounts from Microsoft Entra tenants. Tool features help identify viral users in the Microsoft Entra tenant. You can reset the user redemption status.

- Use the sample application in [Azure-samples/Remove-unmanaged-guests](#) .
- Use PowerShell cmdlets in [MSIdentityTools](#) .

Redeem invitations

After you run a tool, users with unmanaged Microsoft Entra accounts access the tenant, and re-redeem their invitations. However, Microsoft Entra ID prevents users from redeeming with an unmanaged Microsoft Entra account. They can redeem with another account type. Google Federation and SAML/WS-Federation aren't enabled by default. Therefore, users redeem with a Microsoft account (MSA) or email one-time password (OTP). MSA is recommended.

Learn more: [Invitation redemption flow](#)

Overtaken tenants and domains

It's possible to convert some unmanaged tenants to managed tenants.

Learn more: [Take over an unmanaged directory as administrator in Microsoft Entra ID](#)

Some overtaken domains might not be updated. For example, a missing DNS TXT record indicates an unmanaged state. Implications are:

- For guest users from unmanaged tenants, redemption status is reset. A consent prompt appears.
 - Redemption occurs with same account
- The tool might identify unmanaged users as false positives after you reset unmanaged user redemption status

Reset redemption with a sample application

Use the sample application on [Azure-Samples/Remove-Unmanaged-Guests](#).

Reset redemption using **MSIdentityTools** PowerShell module

The **MSIdentityTools** PowerShell module is a collection of cmdlets and scripts, which you use in the Microsoft identity platform and Microsoft Entra ID. Use the cmdlets and scripts to augment PowerShell SDK capabilities. See, [microsoftgraph/msgraph-sdk-powershell](#).

Run the following cmdlets:

- `Install-Module Microsoft.Graph -Scope CurrentUser`
- `Install-Module MSIdentityTools`
- `Import-Module msidentitytools,microsoft.graph`

To identify unmanaged Microsoft Entra accounts, run:

- `Connect-MgGraph -Scope User.Read.All`
- `Get-MsIdUnmanagedExternalUser`

To reset unmanaged Microsoft Entra account redemption status, run:

- `Connect-MgGraph -Scopes User.ReadWriteAll`
- `Get-MsIdUnmanagedExternalUser | Reset-MsIdExternalUser`

To delete unmanaged Microsoft Entra accounts, run:

- `Connect-MgGraph -Scopes User.ReadWriteAll`
- `Get-MsIdUnmanagedExternalUser | Remove-MgUser`

Resource

The following tool returns a list of external unmanaged users, or viral users, in the tenant.

See, [Get-MSIdUnmanagedExternalUser ↗](#).

Monitor and clean up stale guest accounts using access reviews

Article • 12/30/2024

As users collaborate with external partners, it's possible that many guest accounts get created in Microsoft Entra tenants over time. When collaboration ends and the users no longer access your tenant, the guest accounts may become stale. Administrators can monitor guest accounts at scale using inactive guest insights. Administrators can also use Access Reviews to automatically review inactive guest users, block them from signing in, and, delete them from the directory.

Learn more about [how to manage inactive user accounts in Microsoft Entra ID](#).

There are a few recommended patterns that are effective at monitoring and cleaning up stale guest accounts:

1. Monitor guest accounts at scale with intelligent insights into inactive guests in your organization using inactive guest report. 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 may be inactive.
2. Create a multi-stage review whereby guests self-attest whether they still need access. A second-stage reviewer assesses results and makes a final decision. Guests with denied access are disabled and later deleted.
3. Create a review to remove inactive external guests. Admins define inactive as period of days. They disable and later delete guests that don't sign in to the tenant within that time frame. By default, this doesn't affect recently created users. [Learn more about how to identify inactive accounts](#).

Use the following instructions to learn how to enhance monitoring of inactive guest accounts at scale and create Access Reviews that follow these patterns. Consider the configuration recommendations and then make the needed changes that suit your environment.

License requirements

Using this feature requires Microsoft Entra ID Governance or Microsoft Entra Suite licenses. To find the right license for your requirements, see [Microsoft Entra ID Governance licensing fundamentals](#).

Monitor guest accounts at scale with inactive guest insights

💡 Tip

Steps in this article might vary slightly based on the portal you start from.

1. Sign in to the [Microsoft Entra admin center](#).
2. Browse to **Identity governance > Dashboard**
3. Access the inactive guest account report by navigating to the **Guest access governance** card then select **View inactive guests**.
4. You will see the inactive guest report which will provide insights about inactive guest users based on 90 days of inactivity. The threshold is set to 90 days by default but can be configured using "Edit inactivity threshold" based on your organization's needs.
5. The following insights are provided as part of this report:
 - Guest account overview (total guests and inactive guests with further categorization of guests who have never signed in or signed in at least once)
 - Guest inactivity distribution (Percentage distribution of guest users based on days since last sign in)
 - Guest inactivity overview (Guest inactivity guidance to configure inactivity threshold)
 - Guest accounts summary (An exportable tabular view with details of all guest accounts with insights into their activity state. The Activity state could be active or inactive based on the configured inactivity threshold)
6. The inactive days are calculated based on last sign in date if the user has signed in at least once. For users who have never signed in, the inactive days are calculated based on creation date.

ⓘ Note

The report with guest insights can be downloaded using "Download all data". Each action to download may take some time depending on the count of guest users and enables the download for up to 1 Million guest users.

Create a multi-stage review for guests to self-attest continued access

1. Create a [dynamic group](#) for the guest users you want to review. For example,

```
(user.userType -eq "Guest") and (user.mail -contains "@contoso.com") and  
(user.accountEnabled -eq true)
```

2. To [create an Access Review](#) for the dynamic group, navigate to **Microsoft Entra ID** > **Identity Governance** > **Access Reviews**.
3. Select **New access review**.
4. Configure Review type.

 [Expand table](#)

Property	Value
Select what to review	Teams + Groups
Review scope	Select Teams + groups
Group	Select the dynamic group
Scope	Guest users only
(Optional) Review inactive guests	Check the box for Inactive users (on tenant level) only . Enter the number of days that constitute inactivity.

* [Review type](#) * [Reviews](#) [Settings](#) * [Review + Create](#)

Schedule an access review to ensure the right people have the right access to access packages, groups, apps, and privileged roles.
[Learn more](#)

Select what to review *

Teams + Groups ▼

Review scope *

All Microsoft 365 groups with guest users ⓘ

Select Teams + groups

Group *

All Guests

Scope *

Guest users only

All users ⓘ

i In public preview, B2B direct connect users and teams in shared channels are included in access reviews. B2B direct connect users and teams are not supported in reviews of 'All Microsoft 365 groups with guest users', as well as reviews scoped to inactive users. Click here to learn more.

Inactive users (on tenant level) only ⓘ

5. Select Next: Reviews.

6. Configure Reviews:

[+] Expand table

Property	Value
First stage review	
Multi-stage review	Check the box
Select reviewers	Users review their own access
Stage duration (in days)	Enter the number of days
Second stage review	
Select reviewers	Group owner(s) or Selected user(s) or group(s)
Stage duration (in days)	Enter the number of days. (Optional) Specify a fallback reviewer.
Specify recurrence of review	
Review recurrence	Select your preference from the drop-down
Start date	Select a date
End	Select your preference
Specify reviewees to go to the next stage	
Reviewees going to the next stage	Select reviewees. For example, select users who self-approved or responded Don't know .

Determine review stages, reviewers, and timeline below.

Multi-stage review * ⓘ



First stage review

Select reviewers *

Users review their own access



Stage duration (in days) *

7



Second stage review

i Reviewers in later stage can overwrite decisions from previous stage

Select reviewers *

Group owner(s)



Fallback reviewers ⓘ

+ Select fallback reviewers

Stage duration (in days) *

7



[+ Add a stage](#)

Reveal review results

Show previous stage(s) decisions to later stage reviewers ⓘ



Specify recurrence of review

i Your sum duration of all review stages cannot be longer than the recurrence period.

Duration (in days)

14

Review recurrence *

Monthly



Start date *

12/20/2023



End

Never

End on specific date

End after number of occurrences

Specify reviewees to go to next stage

Reviewees going to the next stage *

Approved reviewees, Reviewees m...



7. Select Next: **Settings**.

8. Configure Settings:

[] Expand table

Property	Value
Upon completion settings	
Auto apply results to resource	Check the box
If reviewers don't respond	Remove access
Action to apply on denied guest users	Block user from signing in for 30 days, then remove user from the tenant
(Optional) At end of review, send notification to	Specify other users or groups to notify.
Enable reviewer decision helpers	
Additional content for reviewer email	Add a custom message for reviewers
All other fields	Leave the default values for the remaining options.

* Review type * Reviews **Settings** * Review + Create

Configure additional settings, including decision helpers and email notifications.

Upon completion settings

Auto apply results to resource

If reviewers don't respond Remove access

⚠ Setting 'If reviewers don't respond' to 'Remove access' or 'Take recommendations' while 'Auto-apply results to resource' is enabled could potentially lead to all access to this resource being revoked if the reviewers fail to respond.

Action to apply on denied guest users Block user from signing-in for 30 ...

At end of review, send notification to

+ Select User(s) or Group(s)

Enable reviewer decision helpers

No sign-in within 30 days

User-to-Group Affiliation

Advanced settings

Justification required

Email notifications

Reminders

Additional content for reviewer email

Please review whether or not you still need access.

< Previous

Next: Review + Create

9. Select **Next: Review + Create**

10. Enter an Access Review name. (Optional) provide description.

11. Select **Create**.

Create a review to remove inactive external guests

1. Create a [dynamic group](#) for the guest users you want to review. For example,

```
(user.userType -eq "Guest") and (user.mail -contains "@contoso.com") and  
(user.accountEnabled -eq true)
```

2. To [create an access review](#) for the dynamic group, navigate to **Microsoft Entra ID** > **Identity Governance** > **Access Reviews**.
3. Select **New access review**.
4. Configure Review type:

[] [Expand table](#)

Property	Value
Select what to review	Teams + Groups
Review scope	Select Teams + groups
Group	Select the dynamic group
Scope	Guest users only
Inactive users (on tenant level) only	<input checked="" type="checkbox"/>
Days inactive	Enter the number of days that constitutes inactivity

! Note

The inactivity time you configure will not affect recently created users. The Access Review will check if the user has been created in the timeframe you configure and ignore users who haven't existed for at least that amount of time. For example, if you set the inactivity time as 90 days and a guest user was created/invited less than 90 days ago, the guest user will not be in scope of the Access Review. This ensures that guests can sign in once before being removed.

*Review type *Reviews Settings *Review + Create

Schedule an access review to ensure the right people have the right access to access packages, groups, apps, and privileged roles.
[Learn more](#)

Select what to review *

Teams + Groups



Review scope *

All Microsoft 365 groups with guest users ⓘ

Select Teams + groups

Group *

Contoso Team

Scope *

Guest users only

All users ⓘ

i In public preview, B2B direct connect users and teams in shared channels are included in access reviews. B2B direct connect users and teams are not supported in reviews of 'All Microsoft 365 groups with guest users', as well as reviews scoped to inactive users. Click here to learn more.

Inactive users (on tenant level) only ⓘ



Days inactive

30



5. Select Next: Reviews.

6. Configure Reviews:

[Expand table](#)

Property	Value
Specify reviewers	
Select reviewers	Select Group owner(s) or a user or group. (Optional) To enable the process to remain automated, select a reviewer who will take no action.
Specify recurrence of review	
Duration (in days)	Enter or select a value based on your preference
Review recurrence	Select your preference from the drop-down
Start date	Select a date
End	Choose an option

7. Select Next: Settings.

* Review type * **Reviews** Settings * Review + Create

Determine review stages, reviewers, and timeline below.

Multi-stage review * ⓘ



Specify reviewers

Select reviewers *

Group owner(s) ▾

Fallback reviewers ⓘ

+ Select fallback reviewers

Specify recurrence of review

Duration (in days) *

6

Review recurrence *

Weekly ▾

Start date *

12/20/2023



End

Never

End on specific date

End after number of occurrences

8. Configure Settings:

[+] Expand table

Property	Value
Upon completion settings	
Auto apply results to resource	Check the box
If reviews don't respond	Remove access
Action to apply on denied guest users	Block user from signing in for 30 days, then remove user from the tenant
Enable reviewer decision helpers	
No sign-in within 30 days	Check the box
All other fields	Check/uncheck the boxes based on your preference.

* Review type * Reviews Settings * Review + Create

Configure additional settings, including decision helpers and email notifications.

Upon completion settings

Auto apply results to resource ⓘ



If reviewers don't respond ⓘ

Remove access



Action to apply on denied guest users ⓘ

Block user from signing-in for 30 ...



At end of review, send notification to

+ Select User(s) or Group(s)

Enable reviewer decision helpers

No sign-in within 30 days ⓘ



Advanced settings

Justification required ⓘ



Email notifications ⓘ



Reminders ⓘ



Additional content for reviewer email ⓘ

9. Select Next: Review + Create.

10. Enter an Access Review name. (Optional) provide description.

11. Select Create.

Guest users who don't sign into the tenant for the number of days you configured are disabled for 30 days, then deleted. After deletion, you can restore guests for up to 30 days, after which a new invitation is needed.

Note

If the access review decisions are not yet applied , the API [accessReviewInstance:stopApplyDecisions](#) can be used to stop active applying decisions.

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Create and manage dynamic membership groups for B2B collaboration in Microsoft Entra External ID

Article • 04/25/2025

Applies to:  Workforce tenants  External tenants ([learn more](#))

What are dynamic membership groups?

A dynamic membership group is a security-based configuration for Microsoft Entra available in the [Microsoft Entra admin center](#). Administrators can set rules to populate dynamic membership groups that are created in Microsoft Entra ID based on user attributes (such as `userType`, department, or country/region). Members can be automatically added to or removed from a security group based on their attributes. These groups can provide access to applications or cloud resources (SharePoint sites, documents) and to assign licenses to members. Learn more about [dedicated groups in Microsoft Entra ID](#).

Prerequisites

[Microsoft Entra ID P1 or P2 licensing](#) is required to create and use dynamic membership groups. Learn more in [Create attribute-based rules for dynamic membership groups in Microsoft Entra ID](#).

Creating an "all users" dynamic group

You can create a group containing all users within a tenant using a membership rule. When users are added or removed from the tenant in the future, the group's membership is adjusted automatically.

1. Sign in to the [Microsoft Entra admin center](#) as at least a [User Administrator](#).
2. Browse to **Entra ID > Groups > All groups**, and then select **New group**.
3. On the **New Group** page, under **Group type**, select **Security**. Enter a **Group name** and **Group description** for the new group.
4. Under **Membership type**, select **Dynamic User**, and then select **Add dynamic query**.
5. Above the **Rule syntax** text box, select **Edit**. On the **Edit rule syntax** page, type the following expression in the text box:

```
user.ObjectId -ne null
```

6. Select **OK**. The rule appears in the Rule syntax box:

The screenshot shows the 'Dynamic membership rules' configuration page. At the top, there are 'Save' and 'Discard' buttons, and a 'Got feedback?' link. Below this, there are tabs for 'Configure Rules' (which is selected) and 'Validate Rules (Preview)'. A note says you can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. There's a link to 'Learn more'. The main area has a table with columns 'And/Or', 'Property', 'Operator', and 'Value'. A single row is shown with 'And' under 'And/Or', '<Choose a Property>' under 'Property', '<Choose an Operator>' under 'Operator', and 'Add a value' under 'Value'. Below the table, there are links for 'Add expression' and 'Get custom extension properties'. A note says some items could not be displayed in the rule builder, with a 'Learn more' link. At the bottom, there's a 'Rule syntax' box containing 'user.ObjectId -ne null', an 'Edit' button, and a search icon.

7. Select **Save**. The new dynamic group will now include B2B guest users and member users.

8. Select **Create** on the **New group** page to create the group.

Creating a group of members only

If you want your group to exclude guest users and include only members of your tenant, create a dynamic group as described above, but in the **Rule syntax** box, enter the following expression:

```
(user.ObjectId -ne null) and (user.userType -eq "Member")
```

The following image shows the rule syntax for a dynamic group modified to include members only and exclude guests.

Dynamic membership rules ...



Save Discard Got feedback?

Configure Rules Validate Rules (Preview)

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. [Learn more](#)

And/Or	Property	Operator	Value	
	objectId	Not Equals	null	
And	userType	Equals	Member	

[+ Add expression](#) [+ Get custom extension properties](#)

Edit

Rule syntax

(user.ObjectId -ne null) and (user.userType -eq "Member")



Creating a group of guests only

You might also find it useful to create a new dynamic group that contains only guest users, so that you can apply policies (such as Microsoft Entra Conditional Access policies) to them. Create a dynamic group as described above, but in the **Rule syntax** box, enter the following expression:

```
(user.ObjectId -ne null) and (user.userType -eq "Guest")
```

The following image shows the rule syntax for a dynamic group modified to include guests only and exclude member users.

Dynamic membership rules ...



Save Discard Got feedback?

Configure Rules Validate Rules (Preview)

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. [Learn more](#)

And/Or	Property	Operator	Value	
	objectId	Not Equals	null	
And	userType	Equals	Guest	

[+ Add expression](#) [+ Get custom extension properties](#)

Edit

Rule syntax

(user.ObjectId -ne null) and (user.userType -eq "Guest")



Next steps

- [B2B collaboration user properties](#)

- Reset redemptions status
- Conditional Access for B2B collaboration users

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 

Delete a tenant in Microsoft Entra ID

Article • 12/19/2024

When an organization (tenant) is deleted in Microsoft Entra ID, all resources in the organization are also deleted. Prepare your organization by minimizing its associated resources before you delete. Only a Global Administrator can delete a Microsoft Entra organization from the Microsoft Entra admin center.

Prepare the organization

You can't delete an organization in Microsoft Entra ID until it passes several checks. These checks reduce the risk that deleting a Microsoft Entra organization negatively affects user access, such as the ability to sign in to Microsoft 365 or access resources in Azure. For example, if the organization associated with a subscription is unintentionally deleted, users can't access the Azure resources for that subscription.

Check the following conditions:

- You paid all outstanding invoices and amounts due or overdue.
- No users are in the Microsoft Entra tenant, except one Global Administrator responsible for organization deletion. You must delete any other users before you can delete the organization.

If users are synchronized from on-premises, turn off the sync first. You must delete the users in the cloud organization by using the Microsoft Entra admin center or Azure PowerShell cmdlets.

- No applications are in the organization. You must remove any applications before you can delete the organization.
- No multifactor authentication providers are linked to the organization.
- No subscriptions for any Microsoft Online Services offerings (such as Azure, Microsoft 365, or Microsoft Entra ID P1 or P2) are associated with the organization.

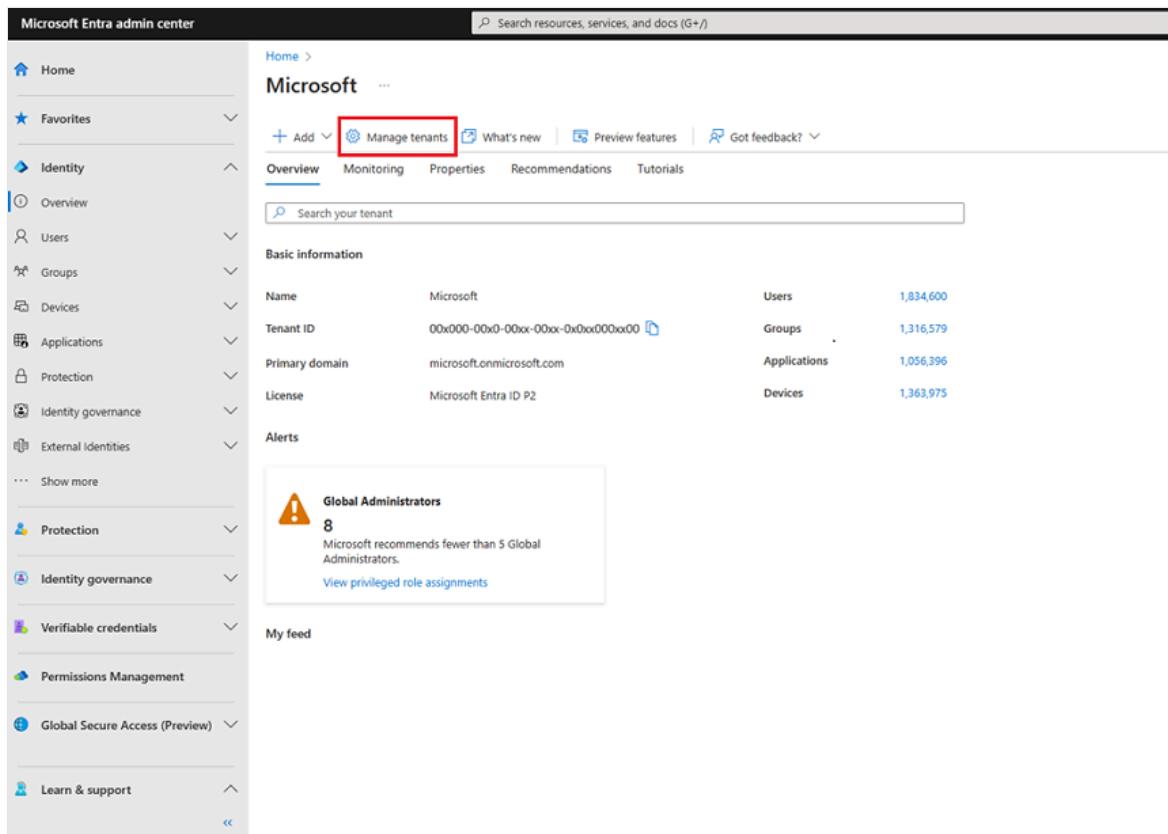
For example, if a default Microsoft Entra tenant was created for you, you can't delete this organization if your subscription still relies on it for authentication. You also can't delete a tenant if an association with another user's subscription remains.

 Note

Microsoft is aware that customers with certain tenant configurations might be unable to successfully delete their Microsoft Entra organization. We're working to address this problem. If you need more information, contact Microsoft support.

Delete the organization

1. Sign in to the [Microsoft Entra admin center](#) as a **Global Administrator**.
2. Select Microsoft Entra ID.
3. On a tenant's **Overview** page, select **Manage tenants**.



The screenshot shows the Microsoft Entra admin center interface. The left sidebar contains navigation links for Home, Favorites, Identity (Overview, Users, Groups, Devices, Applications, Protection, Identity governance, External identities), Protection, Identity governance, Verifiable credentials, Permissions Management, Global Secure Access (Preview), and Learn & support. The main content area is titled 'Microsoft' and shows the tenant overview. At the top of the main area is a navigation bar with 'Add', 'Manage tenants' (which is highlighted with a red box), 'What's new', 'Preview features', and 'Got feedback?'. Below the navigation bar are tabs for 'Overview', 'Monitoring', 'Properties', 'Recommendations', and 'Tutorials'. A search bar labeled 'Search your tenant' is present. Under 'Basic information', there is a table with the following data:

Name	Microsoft	Users	1,834,600
Tenant ID	00x000-00x0-00xx-00xx-0x0x0000x00	Groups	1,316,579
Primary domain	microsoft.onmicrosoft.com	Applications	1,056,396
License	Microsoft Entra ID P2	Devices	1,363,975

Below the table is an 'Alerts' section with a warning icon. It displays 'Global Administrators' (8) and a note: 'Microsoft recommends fewer than 5 Global Administrators.' There is also a link to 'View privileged role assignments'. At the bottom of the main content area is a 'My feed' section.

4. Select the checkbox for the tenant that you want to delete, and then select **Delete**.

The screenshot shows the Microsoft Entra admin center interface. On the left is a navigation sidebar with categories like Home, Favorites, Identity, Protection, and Learn & support. The main area displays a list of tenants under 'Current tenant: Seattle main'. The list includes columns for Organization name and Domain name. A search bar and filter button are at the top of the list. The 'Delete' button in the toolbar is highlighted with a red box.

Organization name	Domain name
Default Directory	globalmain.onmicrosoft.com
Fabrikam	tarkenton.onmicrosoft.com
Seattle main	dprice.onmicrosoft.com
Premium tenant license (Default)	PremiumTenant.onmicrosoft.com
Spelunkers	spelunking.onmicrosoft.com

5. If your organization doesn't pass one or more checks, you get a link to more information on how to pass. After you pass all checks, select **Delete** to complete the process.

Deprovision subscriptions to allow organization deletion

If you also activated license-based subscriptions for your organization, like Microsoft Entra ID P2, Microsoft 365 Business Standard, or Enterprise Mobility + Security E5 you can't delete an organization until the subscriptions are fully deleted. The subscriptions must be in a **Deprovisioned** state to allow organization deletion. An **Expired** or **Canceled** subscription moves to the **Disabled** state, and the final stage is the **Deprovisioned** state.

For what to expect when a trial Microsoft 365 subscription expires (not including paid Partner/CSP, Enterprise Agreement, or Volume Licensing), see the following table. For more information on Microsoft 365 data retention and subscription lifecycle, see [What happens to my data and access when my Microsoft 365 for business subscription ends?](#).

[] Expand table

Subscription state	Data	Access to data
Active (30 days for trial)	Data is accessible to all.	Users have normal access to Microsoft 365 files or apps. Admins have normal access to the Microsoft 365 admin center and resources.
Expired (30 days)	Data is accessible to all.	Users have normal access to Microsoft 365 files or apps. Admins have normal access to the Microsoft 365 admin center and resources.
Disabled (30 days)	Data is accessible to admins only.	Users can't access Microsoft 365 files or apps. Admins can access the Microsoft 365 admin center but can't assign licenses to or update users.
Deprovisioned (30 days after Disabled)	Data is deleted (automatically deleted if no other services are in use).	Users can't access Microsoft 365 files or apps. Admins can access the Microsoft 365 admin center to purchase and manage other subscriptions.

Delete an Office 365 or Microsoft 365 subscription

You can use the Microsoft admin center to put a subscription into the **Deprovisioned** state for deletion in three days:

1. Sign in to the [Microsoft 365 admin center](#) with an account that is a Global Administrator in your organization. If you're trying to delete the Contoso organization that has the initial default domain `contoso.onmicrosoft.com`, sign in with a User Principal Name (UPN) such as `admin@contoso.onmicrosoft.com`.
2. You need to cancel a subscription before you can delete it. Select **Billing > Your products**, and then select **Cancel subscription** for the subscription that you want to cancel.

The screenshot shows the Microsoft 365 Admin Center interface. On the left, a navigation sidebar lists various categories: Home, Users, Teams & groups, Billing, Purchase services, Your products, Licenses, Bills & payments, Billing accounts, and Payment methods. The 'Billing' and 'Your products' items are highlighted with red boxes. The main content area is titled 'Your products' and contains a message: 'These are products owned by your organization that were bought from Microsoft or 3rd-party providers. Select a product to manage product and billing settings or assign licenses.' Below this, there are two tabs: 'Products' (which is selected) and 'Benefits'. A section titled 'Microsoft products (1)' is shown, listing one item: 'Product name ↑'. The list includes: Microsoft 365 E5 Trial, Microsoft Intune Suite Trial, Windows 365 Enterprise 2 vCPU, 4 GB, 128 GB Trial, and Windows 365 Enterprise 2 vCPU, 8 GB, 256 GB Trial.

3. Complete the feedback form, and then select **Cancel subscription**.

The screenshot shows the Microsoft 365 Admin Center interface with the 'Your products' page visible in the background. A modal dialog box titled 'Cancel subscription' is open on the right. The dialog contains the following text:
When you select **Cancel subscription** this Microsoft 365 E5 Trial subscription will be turned off immediately.
You'll still be able to access information about it here for 30 days. After that, all info and customer data for this subscription will be deleted.
[Learn more about canceling subscriptions](#)
You'll receive a final invoice for this subscription in about 30 days, and it will include a prorated refund if you're eligible.
This subscription will expire on 6/9/2024. You can use it until it expires, or select **Cancel subscription** to cancel your subscription now.
Please tell us why you're canceling: *

Additional feedback?

Your feedback will be used to improve Microsoft products and services. IT admins of your organization will be able to view your feedback. [Privacy policy](#)

4. Select **Delete** for the subscription that you want to delete. If you can't find the subscription on the **Your products** page, make sure that you have **Subscription status** set to **All**.

The screenshot shows the Microsoft 365 admin center interface. On the left, there's a navigation sidebar with categories like Home, Users, Devices, Teams & groups, Billing, Purchase services, Your products, Licenses, Bills & payments, Billing accounts, Payment methods, Billing notifications, Setup, and Show all. The 'Your products' section is selected. The main area is titled 'Your products' and contains a message about owned products from Microsoft or 3rd-party providers. Below this is a table titled 'Products from Microsoft and others (4)'. The columns are Product name, Assigned licenses, Purchased quantity, Subscription status, and Purchase chan. The first row shows 'Microsoft 365 E5 Trial' with 20 assigned licenses, 25 purchased, and active until 6/9/2024. The second row shows 'Microsoft Intune Suite Trial' with 20 assigned licenses, 20 purchased, and active until 6/9/2024. The third row shows 'Windows 365 Enterprise 2 vCPU, 4 GB, 128 GB Trial' with 1 assigned license, 4 purchased, and active until 6/9/2024. The fourth row shows 'Windows 365 Enterprise 2 vCPU, 8 GB, 256 GB Trial' with 1 assigned license, 2 purchased, and active until 6/9/2024. A red box highlights the 'Search' and 'Filter' buttons at the top right of the table.

5. Select the checkbox to accept terms and conditions, and then select **Delete subscription**. All data for the subscription is permanently deleted in three days. You can [reactivate the subscription](#) during the three-day period if you change your mind.

The dialog box has a large title 'Delete subscription'. Below it is a warning icon with the text: '⚠️ Deleting your subscription blocks all users from accessing their Office 365 data and email, and deletes all data and email.' An explanatory text follows: 'An email notification will be sent to all administrators on your account. There is a 3 day grace period where the subscription can be reactivated before it is deleted. [Learn more](#) about deleting your subscriptions. Please review our [Privacy statement](#)'.

[I understand the impact](#) of this action and have the authority to request Microsoft to delete the subscription to Office 365 Business Essentials Engineering Feedback Program.

[Close](#) [Delete subscription](#)

Now the subscription state is **Disabled**, and the subscription is marked for deletion. The subscription enters the **Deprovisioned** state 72 hours later.

6. After 72 hours from the time you deleted a subscription, sign in to the Microsoft Entra admin center again. Confirm that no required actions or subscriptions are blocking your organization deletion. You should be able to successfully delete your Microsoft Entra organization.

Resource	Status	Required action
Users	⚠	Delete all users
LinkedIn application ⓘ	⚠	Delete LinkedIn application
App registrations ⓘ	✓	--
Enterprise applications ⓘ	⚠	Delete all enterprise applications
License-based subscriptions ⓘ	⚠	Delete all license-based subscriptions
Microsoft Azure subscriptions ⓘ	✓	--
Self-service sign up products	✓	--

Delete an Azure subscription

If you have an active or canceled Azure subscription associated with your Microsoft Entra tenant, you can't delete the tenant. After you cancel, billing is stopped immediately. After you cancel a subscription, your billing stops immediately. You can delete your subscription directly using the Azure portal seven days after you cancel it, when the **Deleted subscription** option becomes available. Once your subscription is deleted, Microsoft waits 30 to 90 days before permanently deleting your data in case you need to access it or reactivate your subscription. We don't charge you for retaining this data. To learn more, see [Microsoft Trust Center - How we manage your data ↗](#).

If you have a free trial or pay-as-you-go subscription. You can delete your subscription three days after you cancel it, when the **Delete subscription** option becomes available. For details, read through [Delete free trial or pay-as-you-go subscriptions](#).

All other subscription types are deleted only through the [subscription cancellation](#) process. In other words, you can't delete a subscription directly unless it's a free trial or pay-as-you-go subscription.

Alternatively, you can move the Azure subscription to another tenant. When you transfer billing ownership of your subscription to an account in another tenant, you can move the subscription to the new account's tenant. Performing a **Switch Directory** action on the subscription wouldn't help, because the billing would still be aligned with the Microsoft Entra tenant that was used to sign up for the subscription. For more information, review [Transfer a subscription to another Microsoft Entra tenant account](#).

After you have all the Azure, Office 365, and Microsoft 365 subscriptions canceled and deleted, you can clean up the rest of the things within a Microsoft Entra tenant before you delete it.

Remove enterprise apps that you can't delete

A few enterprise applications can't be deleted in the Microsoft Entra admin center and might block you from deleting the tenant.

⚠️ Warning

This code is provided as an example for demonstration purposes. If you intend to use it in your environment, consider testing it first on a small scale, or in a separate test organization. You may have to adjust the code to meet the specific needs of your environment.

Use the following PowerShell code to remove those applications:

1. [Install](#) the Microsoft Graph PowerShell module by running the following command:

```
PowerShell  
  
Install-Module Microsoft.Graph
```

2. Install the Az PowerShell module by running the following command:

```
PowerShell  
  
Install-Module -Name Az
```

3. Create or use a managed administrative account from the tenant that you want to delete. For example: `newAdmin@tenanttodelete.onmicrosoft.com`.

4. Open PowerShell and connect to Microsoft Entra ID by using admin credentials with the following command: `Connect-MgGraph`

⚠️ Warning

You must run PowerShell by using admin credentials for the tenant that you're trying to delete. Only homed-in admins have access to manage the directory via Powershell. You can't use guest user admins, Microsoft accounts, or multiple directories.

Before you proceed, verify that you're connected to the tenant that you want to delete with the Microsoft Graph PowerShell module. We recommend that

you run the `Get-MgDomain` command to confirm that you're connected to the correct tenant ID and `onmicrosoft.com` domain.

5. Run the following commands to set the tenant context. DO NOT skip these steps or you run the risk of deleting enterprise apps from the wrong tenant.

PowerShell

```
Clear-AzContext -Scope CurrentUser  
Connect-AzAccount -Tenant <object id of the tenant you are attempting  
to delete>  
Get-AzContext
```

⚠ Warning

Before you proceed, verify that you're connected to the tenant that you want to delete with the Az PowerShell module. We recommend that you run the `Get-AzContext` command to check the connected tenant ID and `onmicrosoft.com` domain. Do NOT skip the above steps or you run the risk of deleting enterprise apps from the wrong tenant.

6. Run the following command to remove any enterprise apps that you can't delete:

PowerShell

```
Get-MgServicePrincipal | ForEach-Object { Remove-MgServicePrincipal -  
ObjectId $_.Id }
```

7. Run the following command to remove applications and service principals:

PowerShell

```
Get-MgServicePrincipal | ForEach-Object { Remove-MgServicePrincipal -  
ServicePrincipalId $_.Id }
```

8. Run the following command to disable any blocking service principals:

PowerShell

```
$ServicePrincipalUpdate =@{ "accountEnabled" = "false" }  
  
Get-MgServicePrincipal | ForEach-Object { Update-MgServicePrincipal -  
ServicePrincipalId $_.Id -BodyParameter $ServicePrincipalUpdate }
```

9. Sign in to the Microsoft Entra admin center [↗](#) as a [Global Administrator](#), and remove any new admin account that you created in step 3.

10. Retry tenant deletion from the Microsoft Entra admin center.

Handle a trial subscription that blocks deletion

There are [self-service sign-up products](#) like Microsoft Power BI, Azure Rights Management, Microsoft Power Apps, and Dynamics 365. Individual users can sign up via Microsoft 365, which also creates a guest user for authentication in your Microsoft Entra organization.

These self-service products block directory deletions until the products are fully deleted from the organization, to avoid data loss. Only the Microsoft Entra admin can delete them, whether the user signed up individually or was assigned the product.

There are two types of self-service sign-up products, in terms of how they're assigned:

- Organizational-level assignment: a Microsoft Entra administrator assigns the product to the entire organization. A user can actively use the service with the organizational-level assignment, even if the user isn't licensed individually.
- User-level assignment: An individual user during self-service sign-up essentially self-assigns the product without an admin. After an admin starts managing the organization (see [Administrator takeover of an unmanaged organization](#)), the admin can directly assign the product to users without self-service sign-up.

When you begin the deletion of a self-service sign-up product, the action permanently deletes the data and removes all user access to the service. Any user who was assigned the offer individually or on the organization level is then blocked from signing in or accessing any existing data. If you want to prevent data loss with a self-service sign-up product like [Microsoft Power BI dashboards](#) or [Azure RMS policy configuration](#), ensure that the data is backed up and saved elsewhere.

For more information about currently available self-service sign-up products and services, see [Available self-service programs](#).

For what to expect when a trial Microsoft 365 subscription expires (not including paid Partner/CSP, Enterprise Agreement, or Volume Licensing), see the following table. For more information on Microsoft 365 data retention and subscription lifecycle, see [What happens to my data and access when my Microsoft 365 for Business subscription ends?](#).

Product state	Data	Access to data
Active (30 days for trial)	Data is accessible to all.	Users have normal access to self-service sign-up products, files, or apps. Admins have normal access to the Microsoft 365 admin center and resources.
Deleted	Data is deleted.	Users can't access self-service sign-up products, files, or apps. Admins can access the Microsoft 365 admin center to purchase and manage other subscriptions.

Delete a self-service sign-up product

You can put a self-service sign-up product like Microsoft Power BI or Azure RMS into a **Delete** state to be immediately deleted in the Microsoft Entra admin center:

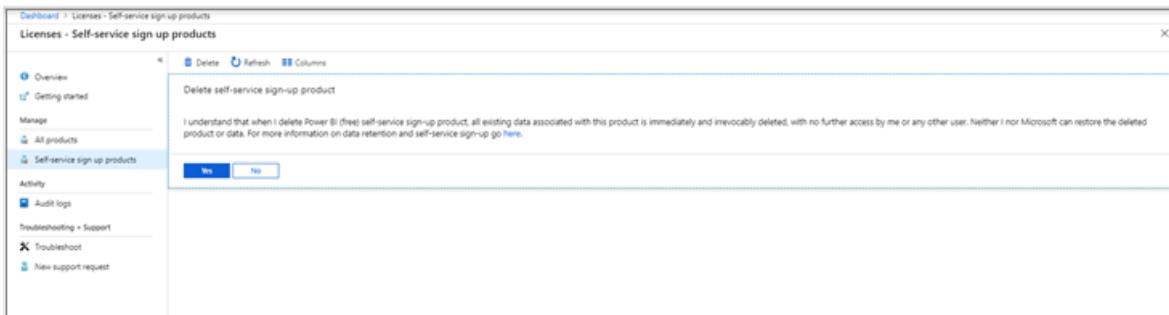
ⓘ Note

If you're trying to delete the Contoso organization that has the initial default domain `contoso.onmicrosoft.com`, sign in with a UPN such as `admin@contoso.onmicrosoft.com`.

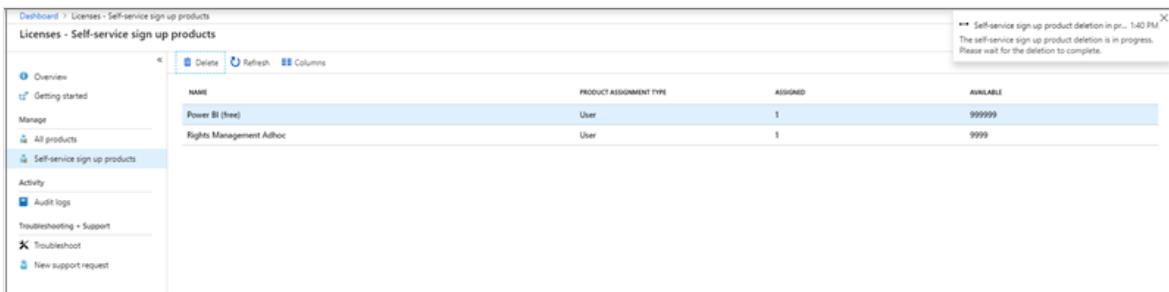
1. Sign in to the [Microsoft Entra admin center](#) as a **Global Administrator**.
2. Select Microsoft Entra ID.
3. Select **Licenses**, and then select **Self-service sign-up products**. You can see all the self-service sign-up products separately from the seat-based subscriptions. Choose the product that you want to permanently delete. Here's an example in Microsoft Power BI:

NAME	PRODUCT ASSIGNMENT TYPE	ASSIGNED	AVAILABLE
Power BI (free)	User	1	999999
Rights Management Adhoc	User	1	9999

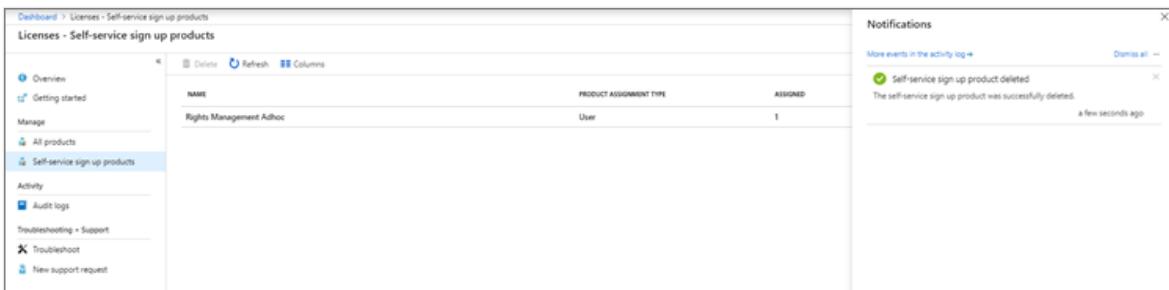
4. Select **Delete** to delete the product. This action removes all users and removes organization access to the product. A dialog warns you that product deletion is immediate and irrevocable. Select **Yes** to confirm.



A notification tells you that the deletion is in progress.



5. The self-service sign-up product state is **Deleted**. Refresh the page, and verify that the product is removed from the **Self-service sign-up products** page.



6. After you delete all the products, sign in to the Microsoft Entra admin center again. Confirm that no required actions or products are blocking your organization deletion. You should be able to successfully delete your Microsoft Entra organization.

Resource	Status	Required action
Users	⚠	Delete all users
LinkedIn application ⓘ	⚠	Delete LinkedIn application
App registrations ⓘ	✓	--
Enterprise applications ⓘ	⚠	Delete all enterprise applications
License-based subscriptions ⓘ	⚠	Delete all license-based subscriptions
Microsoft Azure subscriptions ⓘ	✓	--
Self-service sign up products	✓	--

Next steps

[Microsoft Entra documentation](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Understand how multiple Microsoft Entra tenant organizations interact

Article • 04/25/2025

In Microsoft Entra ID, part of Microsoft Entra, each Microsoft Entra organization is fully independent: a peer that is logically independent from the other Microsoft Entra organizations that you manage. This independence between organizations includes resource independence, administrative independence, and synchronization independence. There's no parent-child relationship between organizations.

Resource independence

- If you create or delete a Microsoft Entra resource in one organization, it has no effect on any resource in another organization, with the partial exception of external users.
- If you register one of your domain names with one organization, you can't use it for any other organization.

Administrative independence

If a non-administrative user of organization 'Contoso' creates a test organization 'Test,' then:

- By default, the user who creates an organization is added as an external user to that new organization, and assigned the Global Administrator role.
- The administrators of organization 'Contoso' have no direct administrative privileges to organization 'Test,' unless an administrator of 'Test' specifically grants them these privileges.
- If you add or remove a Microsoft Entra role for a user in one organization, the change doesn't affect other roles. For example, roles that the user assigns in any other Microsoft Entra organization.

Synchronization independence

You can configure each Microsoft Entra organization independently to get data synchronized from different AD forests, using the Microsoft Entra Connect tool. See [topologies for Microsoft Entra Connect](#) for more information on supported topologies when there are multiple Microsoft Entra tenants.

Add a Microsoft Entra organization

1. Sign in to the [Microsoft Entra admin center](#) as at least a Tenant Creator.
2. Browse to **Entra ID > Overview**.
3. Select **Manage tenants**.
4. Choose **Create**.
5. Select **Workforce** and provide the requested information. Microsoft Entra ID creates a new organization and appears in the list of organizations.

 **Note**

Unlike other Azure resources, your Microsoft Entra organizations are not child resources of an Azure subscription. If your Azure subscription is canceled or expired, you can still access your Microsoft Entra organization's data using Azure PowerShell, the Microsoft Graph API, or the Microsoft 365 admin center. You can also [associate another subscription with the organization](#).

 **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.

Next steps

For Microsoft Entra ID licensing considerations and best practices, see [What is Microsoft Entra ID licensing?](#)

Take over an unmanaged directory as administrator in Microsoft Entra ID

Article • 01/06/2025

This article describes two ways to take over a DNS domain name in an unmanaged directory in Microsoft Entra ID. When a self-service user signs up for a cloud service that uses Microsoft Entra ID, they're added to an unmanaged Microsoft Entra directory based on their email domain. For more about self-service or "viral" sign-up for a service, see [What is self-service sign-up for Microsoft Entra ID?](#)

<https://www.youtube-nocookie.com/embed/GOSpjHtrRsg>

Decide how you want to take over an unmanaged directory

During the process of admin takeover, you can prove ownership as described in [Add a custom domain name to Microsoft Entra ID](#). The next sections explain the admin experience in more detail, but here's a summary:

- When you perform an ["internal" admin takeover](#) of an unmanaged Azure directory, you're added as the Global Administrator of the unmanaged directory. No users, domains, or service plans are migrated to any other directory you administer.
- When you perform an ["external" admin takeover](#) of an unmanaged Azure directory, you add the DNS domain name of the unmanaged directory to your managed Azure directory. When you add the domain name, a mapping of users to resources is created in your managed Azure directory so that users can continue to access services without interruption.

Note

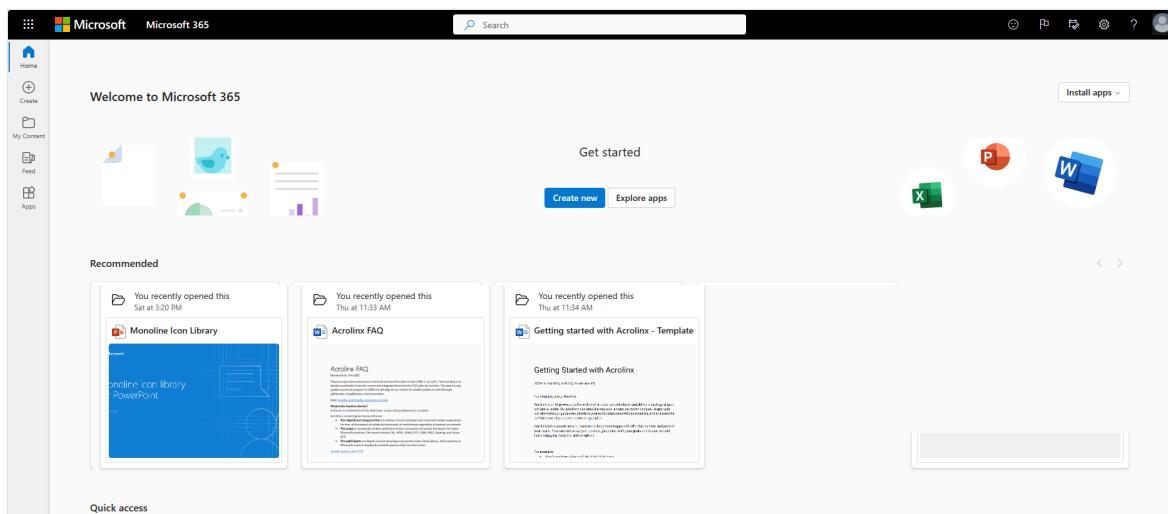
An ["internal" admin takeover](#) requires you to have some level of access to the unmanaged directory. If you are unable to access the directory that you're attempting to takeover, you need to perform an ["external" admin takeover](#).

Internal admin takeover

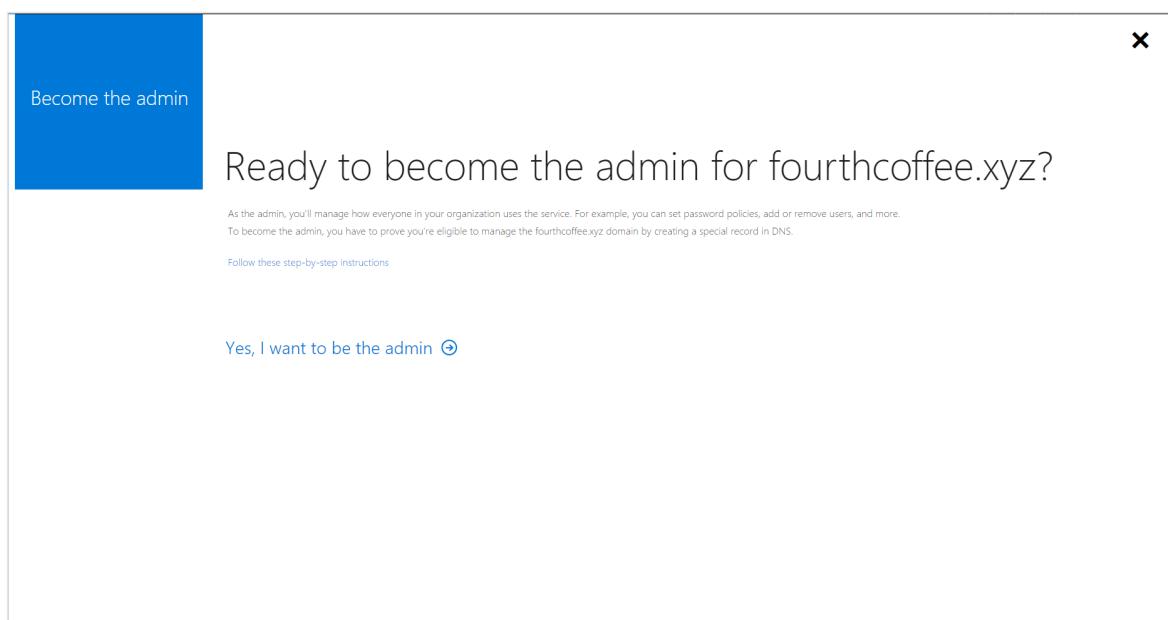
Some products that include SharePoint and OneDrive, such as Microsoft 365, don't support external takeover. If that is your scenario, or if you're an admin and want to take

over an unmanaged or "shadow" Microsoft Entra organization created by users who used self-service sign-up, you can do this with an internal admin takeover.

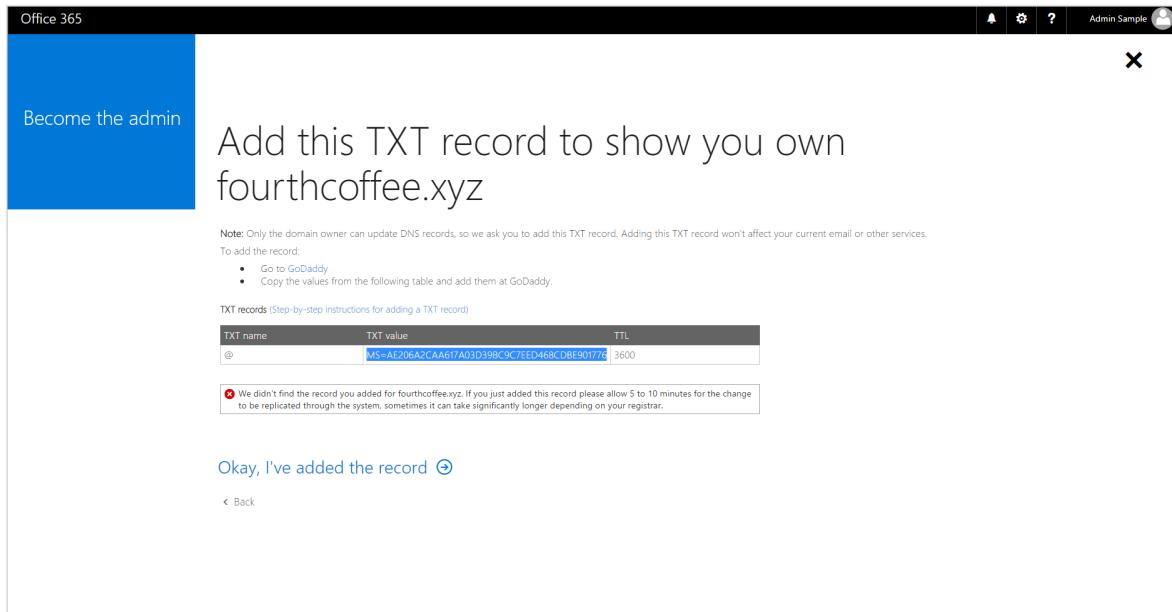
1. Create a user context in the unmanaged organization through signing up for Power BI. For convenience of example, these steps assume that path.
2. Open the [Power BI site](#) and select **Start Free**. Enter a user account that uses the domain name for the organization; for example, `admin@fourthcoffee.xyz`. After you enter in the verification code, check your email for the confirmation code.
3. In the confirmation email from Power BI, select **Yes, that's me**.
4. Sign in to the [Microsoft 365 admin center](#) with the Power BI user account.



5. You receive a message that instructs you to **Become the Admin** of the domain name that was already verified in the unmanaged organization. select **Yes, I want to be the admin**.



6. Add the TXT record to prove that you own the domain name **fourthcoffee.xyz** at your domain name registrar. In this example, it's GoDaddy.com.



When the DNS TXT records are verified at your domain name registrar, you can manage the Microsoft Entra organization.

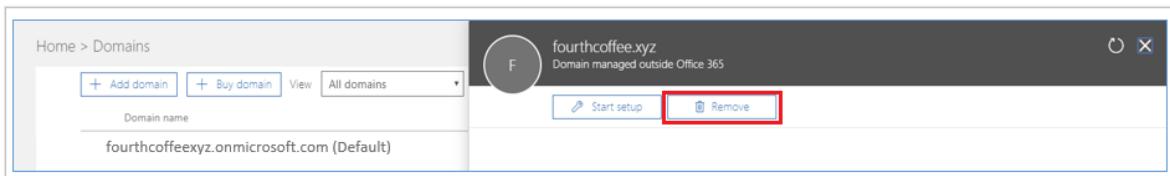
When you complete the preceding steps, you're now the Global Administrator of the Fourth Coffee organization in Microsoft 365. To integrate the domain name with your other Azure services, you can remove it from Microsoft 365 and add it to a different managed organization in Azure.

Adding the domain name to a managed organization in Microsoft Entra ID

Tip

Steps in this article might vary slightly based on the portal you start from.

1. Open the [Microsoft 365 admin center](#).
2. Select **Users** tab, and create a new user account with a name like *user@fourthcoffeexyz.onmicrosoft.com* that doesn't use the custom domain name.
3. Ensure that the new user account has Global Administrator privileges for the Microsoft Entra organization.
4. Open the **Domains** tab in the Microsoft 365 admin center, select the domain name and select **Remove**.



5. If you have any users or groups in Microsoft 365 that reference the removed domain name, they must be renamed to the .onmicrosoft.com domain. If you force delete the domain name, all users are automatically renamed, in this example to *user@fourthcoffeexyz.onmicrosoft.com*.
6. Sign in to the [Microsoft Entra admin center](#) as a **Global Administrator**.
7. In the search box at the top of the page, search for **Domain Names**.
8. Select **+ Add custom domain names**, then add the domain name. You have to enter the DNS TXT records to verify ownership of the domain name.

A screenshot of the Microsoft Entra admin center. On the left, there's a navigation sidebar with various categories like Home, Favorites, Identity, Overview, Users, Groups, Devices, Applications, Protection, Identity governance, External Identities, and more. The main area is titled 'Custom domain names' and shows a table with one row. The table columns are Name, Status, Federated, and Primary. The single entry is 'M365x30474673.onmicrosoft.com' with 'Available' status. At the top of this section, there's a '+ Add custom domain' button which is highlighted with a red box.

Note

Any users of Power BI or Azure Rights Management service who have licenses assigned in the Microsoft 365 organization must save their dashboards if the domain name is removed. They must sign in with a user name like *user@fourthcoffeexyz.onmicrosoft.com* rather than *user@fourthcoffee.xyz*.

External admin takeover

If you already manage an organization with Azure services or Microsoft 365, you can't add a custom domain name if it's already verified in another Microsoft Entra

organization. However, from your managed organization in Microsoft Entra ID you can take over an unmanaged organization as an external admin takeover. The general procedure follows the article [Add a custom domain to Microsoft Entra ID](#).

When you verify ownership of the domain name, Microsoft Entra ID removes the domain name from the unmanaged organization and moves it to your existing organization. External admin takeover of an unmanaged directory requires the same DNS TXT validation process as internal admin takeover. The difference is that the following are also moved over with the domain name:

- Users
- Subscriptions
- License assignments

Support for external admin takeover

External admin takeover is supported by the following online services:

- Azure Rights Management
- Exchange Online

The supported service plans include:

- Power Apps Free
- Power Automate Free
- RMS for individuals
- Microsoft Stream
- Dynamics 365 free trial

External admin takeover isn't supported for any service that has service plans that include SharePoint, OneDrive, or Skype For Business; for example, through an Office free subscription.

Note

External admin takeover isn't supported cross cloud boundaries (ex. Azure Commercial to Azure Government). In these scenarios it is recommended to perform External admin takeover into another Azure Commercial tenant, and then delete the domain from this tenant so you may verify successfully into the destination Azure Government tenant.

More information about RMS for individuals

For [RMS for individuals](#), when the unmanaged organization is in the same region as the organization that you own, the automatically created [Azure Information Protection organization key](#) and [default protection templates](#) are additionally moved over with the domain name.

The key and templates aren't moved over when the unmanaged organization is in a different region. For example, if the unmanaged organization is in Europe and the organization that you own is in North America.

Although RMS for individuals is designed to support Microsoft Entra authentication to open protected content, it doesn't prevent users from also protecting content. If users did protect content with the RMS for individuals subscription, and the key and templates weren't moved over, that content isn't accessible after the domain takeover.

PowerShell cmdlets for the ForceTakeover option

You can see these cmdlets used in [PowerShell example](#).

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.

 Expand table

cmdlet	Usage
<code>connect-mggraph</code>	When prompted, sign in to your managed organization.
<code>get-mgdomain</code>	Shows your domain names associated with the current organization.
<code>new-mgdomain -BodyParameter @{Id="<your domain name>"; IsDefault="False"}</code>	Adds the domain name to organization as Unverified (no DNS verification has been performed yet).

cmdlet	Usage
<code>get-mgdomain</code>	The domain name is now included in the list of domain names associated with your managed organization, but is listed as Unverified .
<code>Get-MgDomainVerificationDnsRecord</code>	Provides the information to put into new DNS TXT record for the domain (MS=xxxxx). Verification might not happen immediately because it takes some time for the TXT record to propagate, so wait a few minutes before considering the -ForceTakeover option.
<code>confirm-mgdomain -Domainname <domainname></code>	<ul style="list-style-type: none"> - If your domain name is still not verified, you can proceed with the -ForceTakeover option. It verifies that the TXT record was created and kicks off the takeover process. - The -ForceTakeover option should be added to the cmdlet only when forcing an external admin takeover, such as when the unmanaged organization has Microsoft 365 services blocking the takeover.
<code>get-mgdomain</code>	The domain list now shows the domain name as Verified .

! Note

The unmanaged Microsoft Entra organization is deleted 10 days after you exercise the external takeover force option.

PowerShell example

1. Connect to Microsoft Graph using the credentials that were used to respond to the self-service offering:

```
PowerShell
Install-Module -Name Microsoft.Graph
Connect-MgGraph -Scopes "User.ReadWrite.All", "Domain.ReadWrite.All"
```

2. Get a list of domains:

```
PowerShell
Get-MgDomain
```

3. Run the New-MgDomain cmdlet to add a new domain:

```
PowerShell
```

```
New-MgDomain -BodyParameter @{Id=<your domain name>;  
IsDefault="False"}
```

4. Run the Get-MgDomainVerificationDnsRecord cmdlet to view the DNS challenge:

```
PowerShell
```

```
(Get-MgDomainVerificationDnsRecord -DomainId <your domain name> | ?  
{$_.recordtype -eq "Txt"}).AdditionalProperties.text
```

For example:

```
PowerShell
```

```
(Get-MgDomainVerificationDnsRecord -DomainId "contoso.com" | ?  
{$_.recordtype -eq "Txt"}).AdditionalProperties.text
```

5. Copy the value (the challenge) that is returned from this command. For example:

```
PowerShell
```

```
MS=ms18939161
```

6. In your public DNS namespace, create a DNS txt record that contains the value that you copied in the previous step. The name for this record is the name of the parent domain, so if you create this resource record by using the DNS role from Windows Server, leave the Record name blank and just paste the value into the Text box.

7. Run the Confirm-MgDomain cmdlet to verify the challenge:

```
PowerShell
```

```
Confirm-MgDomain -DomainId <your domain name>
```

For example:

```
PowerShell
```

```
Confirm-MgDomain -DomainId "contoso.com"
```

 **Note**

The Confirm-MgDomain Cmdlet is being updated. You can monitor the [Confirm-MgDomain Cmdlet](#) article for updates.

A successful challenge returns you to the prompt without an error.

Next steps

- [Add a custom domain name to Microsoft Entra ID](#)
- [How to install and configure Azure PowerShell](#)
- [Azure PowerShell](#)
- [Azure Cmdlet Reference](#)
- [Find Azure AD PowerShell and MSOnline cmdlets in Microsoft Graph PowerShell](#)

Feedback

Was this page helpful?



Yes



No

[Provide product feedback](#) ↗

Managing custom domain names in your Microsoft Entra ID

Article • 12/19/2024

A domain name is an important part of the identifier for resources in many Microsoft Entra deployments. It's part of a user name or email address for a user, part of the address for a group, and is sometimes part of the app ID URI for an application. A resource in Microsoft Entra ID can include a domain name that's owned by the Microsoft Entra organization (sometimes called a tenant) that contains the resource. [Global Administrators](#) and [Domain name administrators](#) can manage domains in Microsoft Entra ID.

Set the primary domain name for your Microsoft Entra organization

Tip

Steps in this article might vary slightly based on the portal you start from.

When your organization is created, the initial domain name, such as "contoso.onmicrosoft.com," is also the primary domain name. The primary domain is the default domain name for a new user when you create a new user. Setting a primary domain name streamlines the process for an administrator to create new users in the portal. To change the primary domain name:

1. Sign in to the [Microsoft Entra admin center](#) as a [Global Administrator](#).
2. Select Microsoft Entra ID.
3. Select **Custom domain names**.

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with sections like Home, What's new, Diagnose & solve problems, Favorites, Identity, Protection, Identity governance, External Identities, and Learn & support. The main area is titled 'Custom domain names'. At the top, there's a search bar and several buttons: '+ Add custom domain' (highlighted with a red box), 'Diagnose and solve problems', 'Refresh', 'Columns', and 'Got feedback?'. Below this is a message: 'Looking to move an on-premises application to the cloud and use Microsoft Entra Domain Services?'. There's also a 'Search' input field and a 'Add filter' button. The main table lists a single domain: 'fourthcoffee.com' under 'Name', 'Available' under 'Status', and a dropdown arrow under 'Primary'. The table has columns for Name, Status, Federated, and Primary.

4. Select the name of the domain that you want to be the primary domain.
5. Select the **Make primary** command. Confirm your choice when prompted.

The screenshot shows the details for the 'fourthcoffee.com' domain. The top navigation bar shows 'Home > Custom domain names > fourthcoffee.com'. Below the title, it says 'Custom domain name'. There are two buttons: a checked 'Make primary' button (highlighted with a red box) and a 'Delete' button. A confirmation dialog box asks 'Do you want to make fourthcoffee.com your primary domain?' with 'Yes' and 'No' buttons. Below this, there's a table with two rows. The first row has two columns: 'Primary domain' (status: 'In use') and 'No'. The second row has two columns: 'Initial domain' (status: 'Yes') and '1 resources referencing this domain name'.

Primary domain	No
In use	Yes 1 resources referencing this domain name
Initial domain	No

You can change the primary domain name for your organization to be any verified custom domain that isn't federated. Changing the primary domain for your organization doesn't change the user name for any existing users.

Add custom domain names to your Microsoft Entra organization

You can add up to 5000 managed domain names. If you're configuring all your domains for federation with on-premises Active Directory, you can add up to 2,500 domain names in each organization.

Add subdomains of a custom domain

If you want to add a subdomain name such as 'europe.contoso.com' to your organization, you should first add and verify the root domain, such as contoso.com. Microsoft Entra ID automatically verifies the subdomain. To see that the subdomain you added is verified, refresh the domain list in the browser.

If you have already added a contoso.com domain to one Microsoft Entra organization, you can also verify the subdomain europe.contoso.com in a different Microsoft Entra organization. When adding the subdomain, you are prompted to add a TXT record in the Domain Name Server (DNS) hosting provider.

What to do if you change the DNS registrar for your custom domain name

If you change the DNS registrars, there are no other configuration tasks in Microsoft Entra ID. You can continue using the domain name with Microsoft Entra ID without interruption. If you use your custom domain name with Microsoft 365, Intune, or other services that rely on custom domain names in Microsoft Entra ID, see the documentation for those services.

Delete a custom domain name

You can delete a custom domain name from your Microsoft Entra ID if your organization no longer uses that domain name, or if you need to use that domain name with another Microsoft Entra organization.

To delete a custom domain name, you must first ensure that no resources in your organization rely on the domain name. You can't delete a domain name from your organization if:

- Any user has a user name, email address, or proxy address that includes the domain name.
- Any group has an email address or proxy address that includes the domain name.
- Any application in your Microsoft Entra ID has an app ID URI that includes the domain name.

You must change or delete any such resource in your Microsoft Entra organization before you can delete the custom domain name.

 **Note**

To delete the custom domain, use a Global Administrator account that is based on either the default domain (onmicrosoft.com) or a different custom domain (mydomainname.com).

ForceDelete option

You can **ForceDelete** a domain name in the [Azure portal](#) or using [Microsoft Graph API](#). These options use an asynchronous operation and update all references from the custom domain name like "user@contoso.com" to the initial default domain name such as "user@contoso.onmicrosoft.com."

To call **ForceDelete** in the Azure portal, you must ensure that there are fewer than 1,000 references to the domain name, and any references where Exchange is the provisioning service must be updated or removed in the [Exchange Admin Center \(EAC\)](#). This includes Exchange Mail-Enabled Security Groups and distributed lists. For more information, see [Removing mail-enabled security groups](#). Also, the **ForceDelete** operation doesn't succeed if either of the following is true:

- You purchased a domain via Microsoft 365 domain subscription services
- You are a partner administering on behalf of another customer organization

The following actions are performed as part of the **ForceDelete** operation:

- Renames the UPN, EmailAddress, and ProxyAddress of users with references to the custom domain name to the initial default domain name.
- Renames the EmailAddress of groups with references to the custom domain name to the initial default domain name.
- Renames the identifierUris of applications with references to the custom domain name to the initial default domain name.
- Disables user accounts impacted by the ForceDelete option in the Azure/Microsoft Microsoft Entra admin center and optionally when using the Graph API.

An error is returned when:

- The number of objects to be renamed is greater than 1000
- One of the applications to be renamed is a multitenant app

Best Practices for Domain Hygiene

Use a reputable registrar that provides ample notifications for domain name changes, registration expiry, a grace period for expired domains, and maintains high security standards for controlling who has access to your domain name configuration and TXT records. Keep your domain names current with your Registrar, and verify TXT records for accuracy.

- If you purposefully are expiring your domain name or turning over ownership to someone else (separately from your Microsoft Entra tenant), you should delete it from your Microsoft Entra tenant before expiring or transferring.
- If you do allow your domain name to expire, if you are able to reactivate it/regain control of it, carefully review all TXT records with the registrar to ensure no tampering of your domain name took place.
- If you can't reactivate or regain control of your domain name immediately, you should delete it from your Microsoft Entra tenant. Don't read/re-verify until you are able to resolve ownership of the domain name and verify the full TXT record for correctness.

ⓘ Note

Microsoft will not allow a domain name to be verified with more than one Microsoft Entra tenant. Once you delete a domain name from your tenant, you will not be able to re-add/re-verify it with your Microsoft Entra tenant if it is subsequently added and verified with another Microsoft Entra tenant.

Frequently asked questions

Q: Why is the domain deletion failing with an error that states that I have Exchange mastered groups on this domain name?

A: Today, certain groups like Mail-Enabled Security groups and distributed lists are provisioned by Exchange and need to be manually cleaned up in [Exchange Admin Center](#). There may be lingering ProxyAddresses, which rely on the custom domain name and will need to be updated manually to another domain name.

Q: I am logged in as admin@contoso.com but I cannot delete the domain name "contoso.com"?

A: You can't reference the custom domain name you are trying to delete in your user account name. Ensure that the Global Administrator account is using the initial default domain name (.onmicrosoft.com) such as admin@contoso.onmicrosoft.com. Sign in with

a different Global Administrator account that such as admin@contoso.onmicrosoft.com or another custom domain name like "fabrikam.com" where the account is admin@fabrikam.com.

Q: I clicked the Delete domain button and see `In Progress` status for the Delete operation. How long does it take? What happens if it fails?

A: The delete domain operation is an asynchronous background task that renames all references to the domain name. It may take up to 24 hours to complete. If domain deletion fails, ensure that you don't have:

- Apps configured on the domain name with the appIdentifierURI
- Any mail-enabled group referencing the custom domain name
- More than 1000 references to the domain name
- The domain to be removed the set as the Primary domain of your organization

Also note that the ForceDelete option won't work if the domain uses Federated authentication type. In that case the users/groups on the domain must be renamed or removed using the on-premises Active Directory before reattempting the domain removal. If you find that any of the conditions haven't been met, manually clean up the references, and try to delete the domain again.

Use PowerShell or the Microsoft Graph API to manage domain names

Most management tasks for domain names in Microsoft Entra ID can also be completed using Microsoft PowerShell, or programmatically using the Microsoft Graph API.

- [Using PowerShell to manage domain names in Microsoft Entra ID](#)
- [Domain resource type](#)

Next steps

- [Add custom domain names](#)
- [Remove Exchange mail-enabled security groups in Exchange Admin Center on a custom domain name in Microsoft Entra ID](#)
- [ForceDelete a custom domain name with Microsoft Graph API](#)

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback 

Change subdomain authentication type in Microsoft Entra ID

Article • 11/25/2024

After a root domain is added to Microsoft Entra ID, part of Microsoft Entra, all subsequent subdomains added to that root in your Microsoft Entra organization automatically inherit the authentication setting from the root domain. However, if you want to manage domain authentication settings independently from the root domain settings, you can now with the Microsoft Graph API. For example, if you have a federated root domain such as contoso.com, this article can help you verify a subdomain such as child.contoso.com as managed instead of federated.

In the Azure portal, when the parent domain is federated and the admin tries to verify a managed subdomain on the [Custom domain names](#) page, the page displays a 'Failed to add domain' error with the reason "One or more properties contains invalid values." If you try to add this subdomain from the Microsoft 365 admin center, you receive a similar error. For more information about the error, see [A child domain doesn't inherit parent domain changes in Office 365, Azure, or Intune](#).

Because subdomains inherit the authentication type of the root domain by default, you must promote the subdomain to a root domain in Microsoft Entra ID using the Microsoft Graph so you can set the authentication type to your desired type.

⚠️ Warning

This code is provided as an example for demonstration purposes. If you intend to use it in your environment, consider testing it first on a small scale, or in a separate test organization. You may have to adjust the code to meet the specific needs of your environment.

Add the subdomain

1. Use PowerShell to add the new subdomain, which has its root domain's default authentication type. The Microsoft Entra ID and Microsoft 365 admin centers don't yet support this operation.

PowerShell

```
# Connect to Microsoft Graph with the required scopes
```

```

Connect-MgGraph -Scopes "Domain.ReadWrite.All"

# Define the parameters for the new domain
$domainParams = @{
    Name = "child6.mydomain.com"
    AuthenticationType = "Federated"
}

# Create a new domain with the specified parameters
New-MgDomain @domainParams

```

1. Use the following example to GET the domain. Because the domain isn't a root domain, it inherits the root domain authentication type. Your command and results might look as follows, using your own tenant ID:

 **Note**

Issuing this request can be performed directly in [Graph Explorer](#).

HTTP

GET <https://graph.microsoft.com/v1.0/domains/foo.contoso.com/>

Return:

```

{
    "authenticationType": "Federated",
    "availabilityStatus": null,
    "isAdminManaged": true,
    "isDefault": false,
    "isDefaultForCloudRedirections": false,
    "isInitial": false,
    "isRoot": false,           ----- Not a root domain, so it
inherits parent domain's authentication type (federated)
    "isVerified": true,
    "name": "child.mydomain.com",
    "supportedServices": [],
    "forceDeleteState": null,
    "state": null,
    "passwordValidityPeriodInDays": null,
    "passwordNotificationWindowInDays": null
},

```

Change subdomain to a root domain

Use the following command to promote the subdomain:

HTTP

```
POST https://graph.microsoft.com/v1.0/{tenant-id}/domains/foo.contoso.com/promote
```

Promote command error conditions

[+] Expand table

Scenario	Method	Code	Message
Invoking API with a subdomain whose parent domain is unverified	POST	400	Unverified domains can't be promoted. Please verify the domain before promotion.
Invoking API with a federated verified subdomain with user references	POST	400	Promoting a subdomain with user references isn't allowed. Please migrate the users to the current root domain before promotion of the subdomain.

Change the subdomain authentication type to managed

ⓘ Important

If you are changing the authentication type for a federated subdomain, you should take note of the existing federation configuration values before completing the steps below. This information may become necessary if you decide to reimplement federation prior to promoting a domain.

1. Use the following command to change the subdomain authentication type:

PowerShell

```
Connect-MGGraph -Scopes "Domain.ReadWrite.All",
"Directory.AccessAsUser.All"
Update-MgDomain -DomainId "test.contoso.com" -BodyParameter
@{AuthenticationType="Managed"}
```

2. Verify via GET in Microsoft Graph API that subdomain authentication type is now managed:

HTTP

```
GET https://graph.microsoft.com/v1.0/domains/foo.contoso.com/
```

Return:

```
{  
    "authenticationType": "Managed",   <----- Now this domain is  
    successfully added as Managed and not inheriting Federated status  
    "availabilityStatus": null,  
    "isAdminManaged": true,  
    "isDefault": false,  
    "isDefaultForCloudRedirections": false,  
    "isInitial": false,  
    "isRoot": true,   <----- Also a root  
    domain, so not inheriting from parent domain any longer  
    "isVerified": true,  
    "name": "child.mydomain.com",  
    "supportedServices": [  
        "Email",  
        "OfficeCommunicationsOnline",  
        "Intune"  
    ],  
    "forceDeleteState": null,  
    "state": null,  
    "passwordValidityPeriodInDays": null,  
    "passwordNotificationWindowInDays": null }
```

Next steps

- Upgrade from Azure AD PowerShell to Microsoft Graph PowerShell
- Add custom domain names
- Manage domain names
- ForceDelete a custom domain name with Microsoft Graph API

Feedback

Was this page helpful?



Provide product feedback ↗

What is self-service sign-up for Microsoft Entra ID?

Article • 12/13/2024

This article explains how to use self-service sign-up to populate an organization in Microsoft Entra ID, part of Microsoft Entra. If you want to take over a domain name from an unmanaged Microsoft Entra organization, see [Take over an unmanaged tenant as administrator](#).

Why use self-service sign-up?

- Get customers to services they want faster
- Create email-based offers for a service
- Create email-based sign-up flows that quickly allow users to create identities using their easy-to-remember work email aliases
- A self-service-created Microsoft Entra tenant can be turned into a managed tenant that can be used for other services

Terms and definitions

- **Self-service sign-up** is the method by which a user signs up for a cloud service and has an identity automatically created for them in Microsoft Entra ID based on their email domain.
- An **unmanaged Microsoft Entra tenant** is the tenant where that identity is created. An unmanaged tenant is a tenant that has no Global Administrator.
- An **email-verified user** is a type of user account in Microsoft Entra ID. A user who has an identity created automatically after signing up for a self-service offer is known as an email-verified user. An email-verified user is a regular member of a tenant tagged with creationmethod=EmailVerified.

How do I control self-service settings?

Admins have two self-service controls today. They can control whether:

- Users can join the tenant via email
- Users can license themselves for applications and services

How can I control these capabilities?

An admin can configure these capabilities using the following Microsoft Entra cmdlet `Update-MgPolicyAuthorizationPolicy` parameters:

- **allowEmailVerifiedUsersToJoinOrganization** controls whether users can join the tenant by email validation. To join, the user must have an email address in a domain that matches one of the verified domains in the tenant. This setting is applied company-wide for all domains in the tenant. If you set that parameter to `$false`, no email-verified user can join the tenant.
- **allowedToSignUpEmailBasedSubscriptions** controls the ability for users to perform self-service sign-up. If you set that parameter to `$false`, no user can perform self-service sign-up.

`allowEmailVerifiedUsersToJoinOrganization` and `allowedToSignUpEmailBasedSubscriptions` are tenant-wide settings that can be applied to a managed or unmanaged tenant. Here's an example where:

- You administer a tenant with a verified domain such as contoso.com
- You use B2B collaboration from a different tenant to invite a user that doesn't already exist (`userdoesnotexist@contoso.com`) in the home tenant of contoso.com
- The home tenant has the `allowedToSignUpEmailBasedSubscriptions` turned on

If the preceding conditions are true, then a member user is created in the home tenant, and a B2B guest user is created in the inviting tenant.

 **Note**

Office 365 for Education users, are currently the only ones who are added to existing managed tenants even when this toggle is enabled

For more information on Flow and Power Apps trial sign-ups, see the following articles:

- [How can I prevent my existing users from starting to use Power BI?](#) ↗
- [Flow in your organization Q&A](#)

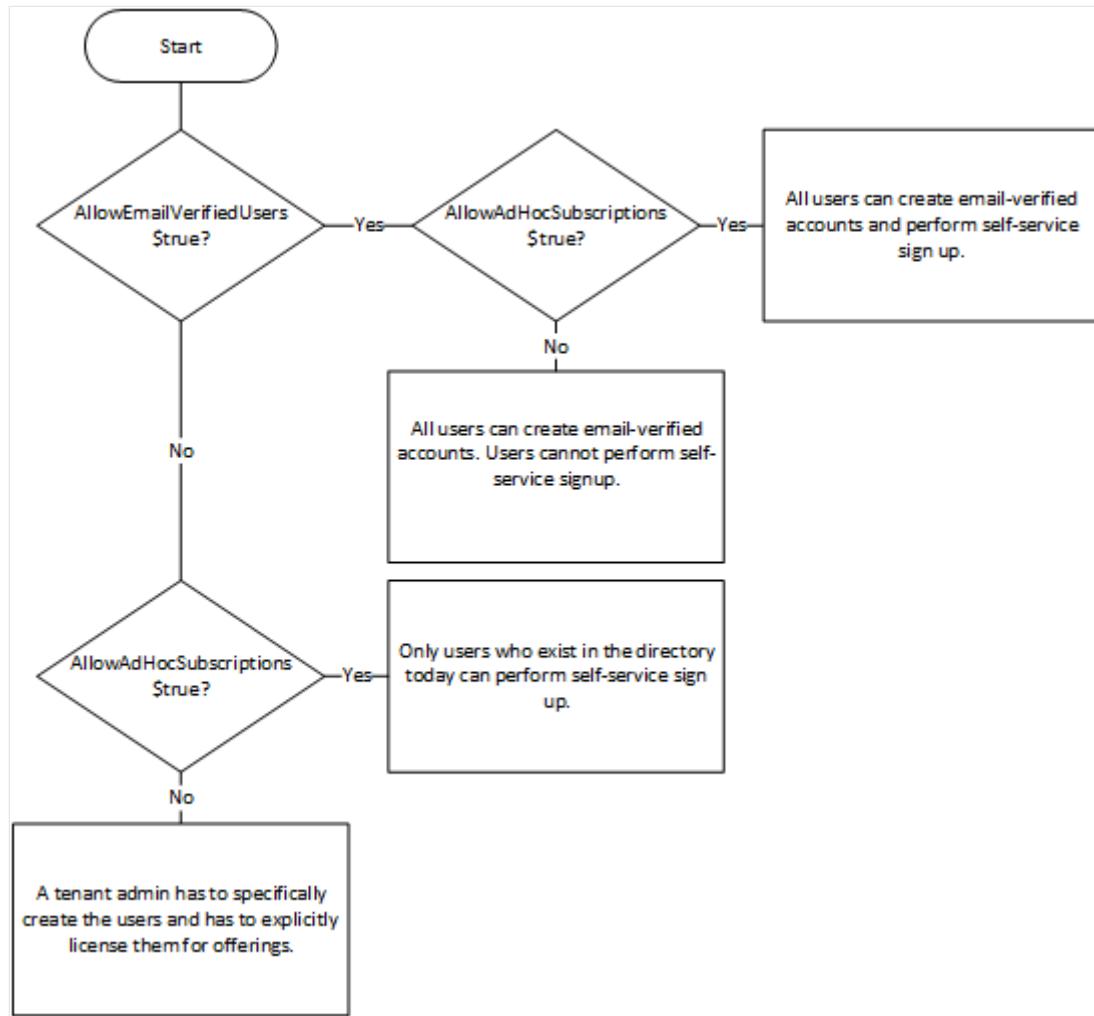
How do the controls work together?

These two parameters can be used in conjunction to define more precise control over self-service sign-up. For example, the following command allows users to perform self-service sign-up, but only if those users already have an account in Microsoft Entra ID (in other words, users who would need an email-verified account to be created first can't perform self-service sign-up):

PowerShell

```
Import-Module Microsoft.Graph.Identity.SignIns
connect-MgGraph -Scopes "Policy.ReadWrite.Authorization"
$param = @{
    allowedToSignUpEmailBasedSubscriptions=$true
    allowEmailVerifiedUsersToJoinOrganization=$false
}
Update-MgPolicyAuthorizationPolicy -BodyParameter $param
```

The following flowchart explains the different combinations for these parameters and the resulting conditions for the tenant and self-service sign-up.



You can retrieve this setting's details using the PowerShell cmdlet `Get-MgPolicyAuthorizationPolicy`. For more information, see [Get-MgPolicyAuthorizationPolicy](#).

PowerShell

```
Get-MgPolicyAuthorizationPolicy | Select-Object
    AllowedToSignUpEmailBasedSubscriptions,
    AllowEmailVerifiedUsersToJoinOrganization
```

For more information and examples of how to use these parameters, see [Update-MgPolicyAuthorizationPolicy](#).

Next steps

- Add a custom domain name to Microsoft Entra ID
 - How to install and configure Azure PowerShell
 - Azure PowerShell
 - Azure Cmdlet Reference
 - [Update-MgPolicyAuthorizationPolicy](#)
 - Close your work or school account in an unmanaged tenant
-

Feedback

Was this page helpful?

 Yes

 No

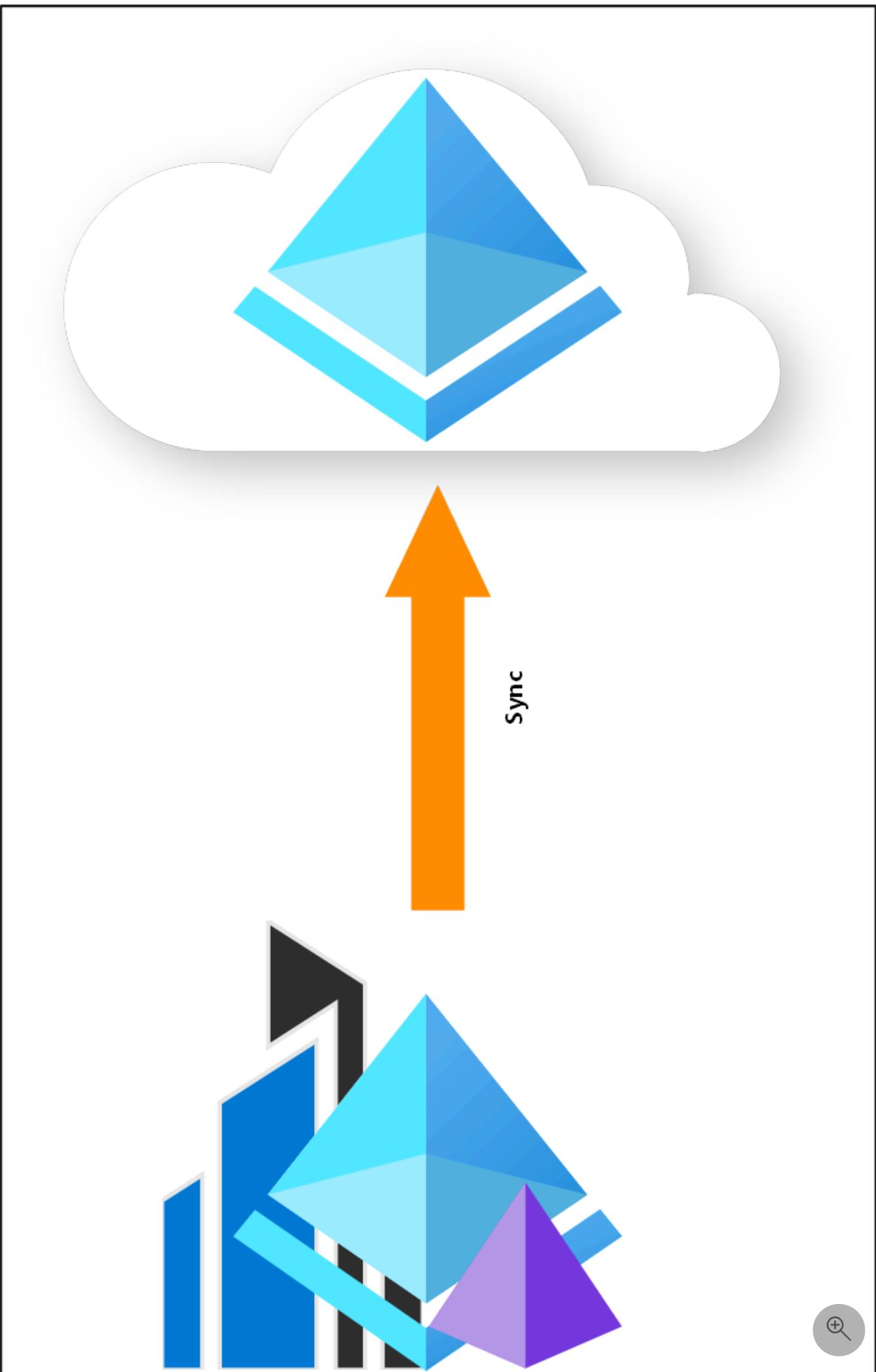
[Provide product feedback ↗](#)

What is hybrid identity with Microsoft Entra ID?

Article • 04/09/2025

Today, businesses, and corporations are increasingly deploying a combination of on-premises and cloud applications. Users require access to those applications both on-premises and in the cloud. Managing users both on-premises and in the cloud poses challenging scenarios.

Microsoft's identity solutions span on-premises and cloud-based capabilities. These solutions create a common user identity for authentication and authorization to all resources, regardless of location. We call this **hybrid identity**.



Hybrid identity is accomplished through provisioning and synchronization. Provisioning is the process of creating an object based on certain conditions, keeping the object up to date and deleting the object when conditions are no longer met. Synchronization is responsible for making sure identity information for your on-premises users and groups is matching the cloud.

For more information, see [What is provisioning?](#) and [What is inter-directory provisioning?](#).

License requirements for using Microsoft Entra Connect

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

Next Steps

- [What is Microsoft Entra Connect and Connect Health?](#)
- [What is password hash synchronization \(PHS\)?](#)
- [What is pass-through authentication \(PTA\)?](#)
- [What is federation?](#)
- [What is single-sign on?](#)

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 ↗](#)

Microsoft Entra version 2 cmdlets for group management

Article • 03/10/2025

This article contains examples of how to use PowerShell to manage your groups in Microsoft Entra ID, part of Microsoft Entra. It also tells you how to get set up with the Microsoft Graph PowerShell module. First, you must [download the Microsoft Graph PowerShell module](#).

Install the Microsoft Graph PowerShell module

To install the MgGroup PowerShell module, use the following commands:

PowerShell

```
PS C:\Windows\system32> Install-module Microsoft.Graph
```

To verify that the module is ready to use, use the following command:

PowerShell

```
PS C:\Windows\system32> Get-Module -Name "*graph*"

ModuleType Version      PreRelease Name
ExportedCommands
-----  -----      -----
...
Script    1.27.0          Microsoft.Graph.Authentication {Add-MgEnvironment, Connect-MgGraph, Disconnect-MgGraph, Get-MgContext...}
Script    1.27.0          Microsoft.Graph.Groups       {Add-MgGroupDriveListContentTypeCopy, Add-MgGroupDriveListContentTypeCopyF...
```

Now you can start using the cmdlets in the module. For a full description of the cmdlets in the Microsoft Graph module, refer to the online reference documentation for [Microsoft Graph PowerShell](#).

Connect to the directory

Before you can start managing groups using Microsoft Graph PowerShell cmdlets, you must connect your PowerShell session to the directory you want to manage. Use the following command:

PowerShell

```
PS C:\Windows\system32> Connect-MgGraph -Scopes "Group.ReadWrite.All"
```

The cmdlet prompts you for the credentials you want to use to access your directory. In this example, we're using karen@drumkit.onmicrosoft.com to access the demonstration directory. The cmdlet returns a confirmation to show the session was connected successfully to your directory:

```
PowerShell
```

```
Welcome To Microsoft Graph!
```

Now you can start using the MgGraph cmdlets to manage groups in your directory.

Retrieve groups

To retrieve existing groups from your directory, use the Get-MgGroups cmdlet.

To retrieve all groups in the directory, use the cmdlet without parameters:

```
PowerShell
```

```
PS C:\Windows\system32> Get-MgGroup -All
```

The cmdlet returns all groups in the connected directory.

You can use the -GroupId parameter to retrieve a specific group for which you specify the group's objectID:

```
PowerShell
```

```
PS C:\Windows\system32> Get-MgGroup -GroupId 5e3eba05-6c2b-4555-9909-c08e997aab18 | fl
```

The cmdlet now returns the group whose objectID matches the value of the parameter you entered:

```
PowerShell
```

```
AcceptedSenders      :  
AllowExternalSenders :  
AppRoleAssignments  :  
AssignedLabels      :  
AssignedLicenses    :  
AutoSubscribeNewMembers :
```

```

Calendar : Microsoft.Graph.PowerShell.Models.MicrosoftGraphCalendar
CalendarView : 
Classification : 
Conversations : 
CreatedDateTime : 14-07-2023 14:25:49
CreatedOnBehalfOf : 
Microsoft.Graph.PowerShell.Models.MicrosoftGraphDirectoryObject
DeletedDateTime : 
Description : Sales and Marketing
DisplayName : Sales and Marketing
Id : f76cbbb8-0581-4e01-a0d4-133d3ce9197f
IsArchived : 
IsAssignableToRole : 
IsSubscribedByMail : 
LicenseProcessingState : 
Microsoft.Graph.PowerShell.Models.MicrosoftGraphLicenseProcessingState
Mail : SalesAndMarketing@M365x64647001.onmicrosoft.com
MailEnabled : True
MailNickname : SalesAndMarketing
RejectedSenders : 
RenewedDateTime : 14-07-2023 14:25:49
SecurityEnabled : True

```

You can search for a specific group using the `-filter` parameter. This parameter takes an ODATA filter clause and returns all groups that match the filter, as in the following example:

PowerShell

```
PS C:\Windows\system32> Get-MgGroup -Filter "DisplayName eq 'Intune Administrators'"
```

```

DeletionTimeStamp : 
ObjectId : aaaaaaaaa-0000-1111-2222-bbbbbbbbbb
ObjectType : Group
Description : Intune Administrators
DirSyncEnabled : 
DisplayName : Intune Administrators
LastDirSyncTime : 
Mail : 
MailEnabled : False
MailNickname : 4dd067a0-6515-4f23-968a-cc2ffc2eff5c
OnPremisesSecurityIdentifier : 
ProvisioningErrors : {}
ProxyAddresses : {}
SecurityEnabled : True

```

 **Note**

The MgGroup PowerShell cmdlets implement the OData query standard. For more information, see \$filter in [OData system query options using the OData endpoint](#).

Here you have an example that shows how to pull all groups that don't have an expiration policy applied

PowerShell

```
Connect-MgGraph -Scopes 'Group.Read.All'  
Get-MgGroup -ConsistencyLevel eventual -Count groupCount -Filter "NOT  
(expirationDateTime+ge+1900-01-01T00:00:00Z)" | Format-List Id
```

This example does the same as the previous one, but the script also exports the results to CSV.

PowerShell

```
Connect-MgGraph -Scopes 'Group.Read.All'  
Get-MgGroup -ConsistencyLevel eventual -Count groupCount -Filter "NOT  
(expirationDateTime+ge+1900-01-01T00:00:00Z)" | Format-List Id | Export-Csv -Path  
{path} -NoTypeInformation
```

This last example shows you how to retrieve only groups that belong to Teams

PowerShell

```
Get-MgGroup -ConsistencyLevel eventual -Count groupCount -Filter "NOT  
(expirationDateTime+ge+1900-01-01T00:00:00Z) and  
resourceProvisioningOptions/any(p:p eq 'Team'))" | Format-List Id,  
expirationDateTime, resourceProvisioningOptions
```

Create groups

To create a new group in your directory, use the New-MgGroup cmdlet. This cmdlet creates a new security group called "Marketing":

PowerShell

```
$param = @{  
    description="My Demo Group"  
    displayName="DemoGroup"  
    mailEnabled=$false  
    securityEnabled=$true  
    mailNickname="Demo"  
}
```

```
New-MgGroup @param
```

Update groups

To update an existing group, use the Update-MgGroup cmdlet. In this example, we're changing the DisplayName property of the group "Intune Administrators." First, we're finding the group using the Get-MgGroup cmdlet and filter using the DisplayName attribute:

PowerShell

```
PS C:\Windows\system32> Get-MgGroup -Filter "DisplayName eq 'Intune Administrators'"
```

```
DeletionTimeStamp      :  
ObjectId              : aaaaaaaaa-0000-1111-2222-bbbbbbbbbbbb  
ObjectType            : Group  
Description           : Intune Administrators  
DirSyncEnabled        :  
DisplayName           : Intune Administrators  
LastDirSyncTime       :  
Mail                  :  
MailEnabled            : False  
MailNickname          : 4dd067a0-6515-4f23-968a-cc2ffc2eff5c  
OnPremisesSecurityIdentifier :  
ProvisioningErrors    : {}  
ProxyAddresses         : {}  
SecurityEnabled        : True
```

Next, we're changing the Description property to the new value "Intune Device Administrators":

PowerShell

```
PS C:\Windows\system32> Update-MgGroup -GroupId 958d212c-14b0-43d0-a052-d0c2bb555b8b -Description "Demo Group Updated"
```

Now, if we find the group again, we see the Description property is updated to reflect the new value:

PowerShell

```
PS C:\Windows\system32> Get-MgGroup -GroupId 958d212c-14b0-43d0-a052-d0c2bb555b8b | select displayname, description  
  
DisplayName Description
```

Delete groups

To delete groups from your directory, use the Remove-MgGroup cmdlet as follows:

PowerShell

```
PS C:\Windows\system32> Remove-MgGroup -GroupId 958d212c-14b0-43d0-a052-d0c2bb555b8b
```

Manage group membership

Add members

To add new members to a group, use the New-MgGroupMember cmdlet. This command adds a member to the Intune Administrators group we used in the previous example:

PowerShell

```
PS C:\Windows\system32> New-MgGroupMember -GroupId f76cbbb8-0581-4e01-a0d4-133d3ce9197f -DirectoryObjectId a88762b7-ce17-40e9-b417-0add1848eb68
```

The `-GroupId` parameter is the group ObjectID. We need to specify the ObjectID of the group we are using. The `-DirectoryObjectId` is the ObjectID of the user we want to add as a group member.

Get members

To get the existing members of a group, use the Get-MgGroupMember cmdlet, as in this example:

PowerShell

```
PS C:\Windows\system32> Get-MgGroupMember -GroupId 2c52c779-8587-48c5-9d4a-c474f2a66cf4
```

Id	DeletedDateTime
aaaaaaaa-bbbb-cccc-1111-222222222222	
bbbbbbbb-cccc-dddd-2222-333333333333	

Remove members

To remove the member we previously added to the group, use the Remove-MgGroupMember cmdlet, as is shown here:

```
PowerShell
```

```
PS C:\Windows\system32> Remove-MgGroupMemberByRef -DirectoryObjectId 00aa00aa-bb11-cc22-dd33-44ee44ee44ee -GroupId 2c52c779-8587-48c5-9d4a-c474f2a66cf4
```

Verify members

To verify the group memberships of a user, use the Select-MgGroupIdsUserIsMemberOf cmdlet. This cmdlet takes as its parameters the ObjectId of the user for which to check the group memberships, and a list of groups for which to check the memberships. The list of groups must be provided in the form of a complex variable of type “Microsoft.Open.AzureAD.Model.GroupIdsForMembershipCheck”, so we first must create a variable with that type:

```
PowerShell
```

```
Get-MgUserMemberOf -UserId 00aa00aa-bb11-cc22-dd33-44ee44ee44ee

Id                               DisplayName Description GroupTypes AccessType
--                               -----
5dc16449-3420-4ad5-9634-49cd04eceba0 demogroup    demogroup {Unified}
```

The value returned is a list of groups of which this user is a member. You can also apply this method to check Contacts, Groups, or Service Principals membership for a given list of groups, using Select-MgGroupIdsContactIsMemberOf, Select-MgGroupIdsGroupIsMemberOf, or Select-MgGroupIdsServicePrincipalsMemberOf

Disable group creation by your users

You can prevent standard users from creating security groups. The default behavior in Microsoft Online Directory Services (MSODS) is to allow standard users to create groups, whether or not self-service group management (SSGM) is also enabled. The SSGM setting controls behavior only in the My Groups portal.

To disable group creation for standard users:

1. Verify that standard users are allowed to create groups:

PowerShell

```
PS C:\> Get-MgBetaDirectorySetting | select -ExpandProperty values
```

Name	Value
----	----
NewUnifiedGroupWritebackDefault	true
EnableMIPLabels	false
CustomBlockedWordsList	
EnableMSStandardBlockedWords	false
ClassificationDescriptions	
DefaultClassification	
PrefixSuffixNamingRequirement	
AllowGuestsToBeGroupOwner	false
AllowGuestsToAccessGroups	true
GuestUsageGuidelinesUrl	
GroupCreationAllowedGroupId	
AllowToAddGuests	true
UsageGuidelinesUrl	
ClassificationList	
EnableGroupCreation	true

2. If it returns `EnableGroupCreation : True`, then standard users can create groups. To disable this feature:

PowerShell

```
Install-Module Microsoft.Graph.Beta.Identity.DirectoryManagement
Import-Module Microsoft.Graph.Beta.Identity.DirectoryManagement
$params = @{
    TemplateId = "62375ab9-6b52-47ed-826b-58e47e0e304b"
    Values = @(
        @{
            Name = "EnableGroupCreation"
            Value = "false"
        }
    )
}
Connect-MgGraph -Scopes "Directory.ReadWrite.All"
New-MgBetaDirectorySetting -BodyParameter $params
```

Manage owners of groups

To add owners to a group, use the `New-MgGroupOwner` cmdlet:

PowerShell

```
PS C:\Windows\system32> New-MgGroupOwner -GroupId 0e48dc96-3bff-4fe1-8939-4cd680163497 -DirectoryObjectId 92a0dad0-7c9e-472f-b2a3-0fe2c9a02867
```

The `-GroupId` parameter is the ObjectID of the group to which we want to add an owner. The `-DirectoryObjectId` is the ObjectID of the user or service principal we want to add as an owner.

To retrieve the owners of a group, use the `Get-MgGroupOwner` cmdlet:

```
PowerShell
```

```
PS C:\Windows\system32> Get-MgGroupOwner -GroupId 0e48dc96-3bff-4fe1-8939-4cd680163497
```

The cmdlet returns the list of owners (users and service principals) for the specified group:

```
PowerShell
```

Id	DeletedDateTime
--	-----
8ee754e0-743e-4231-ace4-c28d20cf2841	
85b1df54-e5c0-4cf0-a20b-8bc1a2ca7865	
4451b332-2294-4dcf-a214-6cc805016c50	

If you want to remove an owner from a group, use the `Remove-MgGroupOwnerByRef` cmdlet:

```
PowerShell
```

```
PS C:\Windows\system32> Remove-MgGroupOwnerByRef -GroupId 0e48dc96-3bff-4fe1-8939-4cd680163497 -DirectoryObjectId 92a0dad0-7c9e-472f-b2a3-0fe2c9a02867
```

Reserved aliases

When you create a group, users specify a mailNickname or alias that the system uses as part of the email address of the group. The creation of groups with any of the highly privileged email aliases listed is limited to Microsoft Entra Global Administrators.

- abuse
- admin
- administrator
- hostmaster
- majordomo
- postmaster
- root

- secure
- security
- ssl-admin
- webmaster

Group writeback to on-premises

Today, many groups are still managed in on-premises Active Directory. To answer requests to sync cloud groups back to on-premises, the groups writeback feature for Microsoft Entra ID using Microsoft Entra cloud sync is now available.

Important

The public preview of Group Writeback v2 in Microsoft Entra Connect Sync is no longer available as of **June 30, 2024**. This feature was discontinued on this date, and you're no longer supported in Microsoft Entra Connect Sync to provision cloud security groups to Active Directory. The feature continues to operate beyond the discontinuation date; however, it no longer receives support and might cease functioning at any time without notice.

We offer similar functionality in Microsoft Entra Cloud Sync called [Group Provision to Active Directory](#) that you can use instead of Group Writeback v2 for provisioning cloud security groups to Active Directory. We're working on enhancing this functionality in Microsoft Entra Cloud Sync along with other new features that we're developing in Microsoft Entra Cloud Sync.

Customers who use this preview feature in Microsoft Entra Connect Sync should [switch their configuration from Microsoft Entra Connect Sync to Microsoft Entra Cloud Sync](#).

You can choose to move all your hybrid sync to Microsoft Entra Cloud Sync (if it supports your needs). You can also run Microsoft Entra Cloud Sync side by side and move only cloud security group provisioning to Active Directory onto Microsoft Entra Cloud Sync.

For customers who provision Microsoft 365 groups to Active Directory, you can keep using Group Writeback v1 for this capability.

You can evaluate moving exclusively to Microsoft Entra Cloud Sync by using the [user synchronization wizard](#).

Next steps

You can find more Microsoft Entra ID PowerShell documentation at [Microsoft Entra Cmdlets](#).

- Managing access to resources with Microsoft Entra groups
- Integrating your on-premises identities with Microsoft Entra ID

Microsoft Entra cmdlets for configuring group settings

Article • 04/30/2025

This article contains instructions for using PowerShell cmdlets to create and update groups in Microsoft Entra ID, part of Microsoft Entra. This content applies only to Microsoft 365 groups.

ⓘ Important

Some settings require a Microsoft Entra ID P1 license. For more information, see the [Template settings](#) table.

For more information on how to prevent nonadministrator users from creating security groups, set the `AllowedToCreateSecurityGroups` property to False as described in [Update-MgPolicyAuthorizationPolicy](#).

Microsoft 365 groups settings are configured using a `Settings` object and a `SettingsTemplate` object. Initially, you don't see any `Settings` objects in your directory, because your directory is configured with the default settings. To change the default settings, you must create a new `Settings` object using a `SettingsTemplate`. Microsoft provides several `SettingsTemplate`s. To configure Microsoft 365 group settings for your directory, you use the template named "Group.Unified". To configure Microsoft 365 group settings on a single group, use the template named "Group.Unified.Guest". This template is used to manage guest access to a Microsoft 365 group.

The cmdlets are part of the [Microsoft Graph PowerShell](#) module. For instructions how to download and install the module on your computer, see [Install the Microsoft Graph PowerShell SDK](#).

ⓘ Note

Even with the restrictions enabled to prevent the addition of guests to Microsoft 365 groups, administrators can still add guest users. The restriction only applies to non-admin users.

Install PowerShell cmdlets

Install the Microsoft Graph cmdlets as described in [Install the Microsoft Graph PowerShell SDK](#).

1. Open the Windows PowerShell app as an administrator.

2. Install the Microsoft Graph cmdlets.

```
PowerShell
```

```
Install-Module Microsoft.Graph -Scope AllUsers
```

3. Install the Microsoft Graph beta cmdlets.

```
PowerShell
```

```
Install-Module Microsoft.Graph.Beta -Scope AllUsers
```

Create settings at the directory level

These steps create settings at directory level, which apply to all Microsoft 365 groups in the directory.

1. In the DirectorySettings cmdlets, you must specify the ID of the SettingsTemplate you want to use. If you don't know this ID, this cmdlet returns the list of all settings templates:

```
PowerShell
```

```
Get-MgBetaDirectorySettingTemplate
```

This cmdlet call returns all templates that are available:

```
Output
```

Id	DisplayName	Description
--	-----	-----
62375ab9-6b52-47ed-826b-58e47e0e304b	Group.Unified	...
08d542b9-071f-4e16-94b0-74abb372e3d9	Group.Unified.Guest	Settings for a specific Microsoft 365 group
16933506-8a8d-4f0d-ad58-e1db05a5b929	Company.BuiltIn	Setting templates define the different settings that can be used for the associ...
4bc7f740-180e-4586-adb6-38b2e9024e6b	Application...	
898f1161-d651-43d1-805c-3b0b388a9fc2	Custom Policy	Settings ...
5cf42378-d67d-4f36-ba46-e8b86229381d	Password Rule	Settings ...

2. To add a usage guideline URL, first you need to get the SettingsTemplate object that defines the usage guideline URL value; that is, the Group. Unified template:

```
PowerShell
```

```
$TemplateId = (Get-MgBetaDirectorySettingTemplate | where { $_.DisplayName -eq "Group.Unified" }).Id
$template = Get-MgBetaDirectorySettingTemplate | where -Property Id -Value $TemplateId -EQ
```

3. Create an object that contains values to be used for the directory setting. These values change the usage guideline value and enable sensitivity labels. Set these or any other setting in the template as required:

PowerShell

```
$params = @{
    templateId = "$TemplateId"
    values = @(
        @{
            name = "UsageGuidelinesUrl"
            value = "https://guideline.example.com"
        }
        @{
            name = "EnableMIPLabels"
            value = "True"
        }
    )
}
```

4. Create the directory setting by using the [New-MgBetaDirectorySetting](#):

PowerShell

```
New-MgBetaDirectorySetting -BodyParameter $params
```

5. You can read the values by using the following commands:

PowerShell

```
$Setting = Get-MgBetaDirectorySetting | where { $_.DisplayName -eq "Group.Unified" }
$Setting.Values
```

Update settings at the directory level

To update the value for UsageGuideLinesUrl in the setting template, read the current settings from Microsoft Entra ID, otherwise we could end up overwriting existing settings other than the UsageGuideLinesUrl.

1. Get the current settings from the Group.Unified SettingsTemplate:

```
PowerShell
```

```
$Setting = Get-MgBetaDirectorySetting | where { $_.DisplayName -eq "Group.Unified"}
```

2. Check the current settings:

```
PowerShell
```

```
$Setting.Values
```

This command returns the following values:

```
Output
```

Name	Value
EnableMIPLabels	True
CustomBlockedWordsList	
EnableMSStandardBlockedWords	False
ClassificationDescriptions	
DefaultClassification	
PrefixSuffixNamingRequirement	
AllowGuestsToBeGroupOwner	False
AllowGuestsToAccessGroups	True
GuestUsageGuidelinesUrl	
GroupCreationAllowedGroupId	
AllowToAddGuests	True
UsageGuidelinesUrl	https://guideline.example.com
ClassificationList	
EnableGroupCreation	True
NewUnifiedGroupWritebackDefault	True

3. To remove the value of UsageGuideLinesUrl, edit the URL to be an empty string:

```
PowerShell
```

```
$params = @{
    Values = @(
        @{
            Name = "UsageGuidelinesUrl"
            Value = ""
        }
    )
}
```

4. Update the value by using the [Update-MgBetaDirectorySetting](#) cmdlet:

```
PowerShell
```

```
Update-MgBetaDirectorySetting -DirectorySettingId $Setting.Id -BodyParameter  
$params
```

Template settings

Here are the settings defined in the `Group.Unified SettingsTemplate`. Unless otherwise indicated, these features require a Microsoft Entra ID P1 license.

 Expand table

Setting	Description
EnableGroupCreation Type: Boolean Default: True	This flag indicates whether nonadmin users can create Microsoft 365 groups in the directory. This setting doesn't require a Microsoft Entra ID P1 license.
GroupCreationAllowedGroupId Type: String Default: ""	GUID of the security group for which the members are allowed to create Microsoft 365 groups even when <code>EnableGroupCreation == false</code> .
UsageGuidelinesUrl Type: String Default: ""	A link to the Group Usage Guidelines.
ClassificationDescriptions Type: String Default: ""	A comma-delimited list of classification descriptions. The value of <code>ClassificationDescriptions</code> is only valid in this format: <code>\$setting["ClassificationDescriptions"]</code> <code>="Classification:Description,Classification:Description"</code> where Classification matches an entry in the ClassificationList. This setting doesn't apply when <code>EnableMIPLabels == True</code> . Character limit for property <code>ClassificationDescriptions</code> is 300, and commas can't be escaped.
DefaultClassification Type: String Default: ""	The classification that is to be used as the default classification for a group if none was specified. This setting doesn't apply when <code>EnableMIPLabels == True</code> .
PrefixSuffixNamingRequirement Type: String Default: ""	String of a maximum length of 64 characters that defines the naming convention configured for Microsoft 365 groups. For more information, see Enforce a naming policy for Microsoft 365 groups .
CustomBlockedWordsList Type: String	Comma-separated string of phrases that users aren't allowed to use in group names or aliases. For more information, see Enforce a

Setting	Description
Default: <code>""</code>	naming policy for Microsoft 365 groups.
EnableMSStandardBlockedWords Type: <code>Boolean</code> Default: <code>False</code>	Deprecated. Don't use.
AllowGuestsToBeGroupOwner Type: <code>Boolean</code> Default: <code>False</code>	Boolean indicating whether or not a guest user can be an owner of groups.
AllowGuestsToAccessGroups Type: <code>Boolean</code> Default: <code>True</code>	Boolean indicating whether or not a guest user can have access to Microsoft 365 groups content. This setting doesn't require a Microsoft Entra ID P1 license.
GuestUsageGuidelinesUrl Type: <code>String</code> Default: <code>""</code>	The URL of a link to the guest usage guidelines.
AllowToAddGuests Type: <code>Boolean</code> Default: <code>True</code>	<p>A boolean indicating whether or not it is allowed to add guests to this directory.</p> <p>This setting may be overridden and become read-only if <code>EnableMIPLabels</code> is set to <code>True</code> and a guest policy is associated with the sensitivity label assigned to the group.</p> <p>If the <code>AllowToAddGuests</code> setting is set to <code>False</code> at the organization level, any <code>AllowToAddGuests</code> setting at the group level is ignored. If you want to enable guest access for only a few groups, you must set <code>AllowToAddGuests</code> to be <code>true</code> at the organization level, and then selectively disable it for specific groups.</p>
ClassificationList Type: <code>String</code> Default: <code>""</code>	<p>A comma-delimited list of valid classification values that can be applied to Microsoft 365 groups.</p> <p>This setting doesn't apply when <code>EnableMIPLabels == True</code>.</p>
EnableMIPLabels Type: <code>Boolean</code> Default: <code>False</code>	<p>The flag indicating whether sensitivity labels published in Microsoft Purview portal can be applied to Microsoft 365 groups. For more information, see Assign Sensitivity Labels for Microsoft 365 groups.</p>
NewUnifiedGroupWritebackDefault Type: <code>Boolean</code> Default: <code>True</code>	<p>The flag that allows an admin to create new Microsoft 365 groups without setting the <code>groupWritebackConfiguration</code> resource type in the request payload. This setting is applicable when group writeback is configured in Microsoft Entra Connect.</p> <p><code>NewUnifiedGroupWritebackDefault</code> is a global Microsoft 365 group setting. Default value is true. Updating the setting value to false changes the default writeback behavior for newly created Microsoft 365 groups, and doesn't change the <code>isEnabled</code> property value for existing Microsoft 365 groups. Group admin needs to</p>

Setting	Description
	explicitly update the group isEnabled property value to change the writeback state for existing Microsoft 365 groups.

Example: Configure Guest policy for groups at the directory level

1. Get all the setting templates:

```
PowerShell
```

```
Get-MgBetaDirectorySettingTemplate
```

2. To set guest policy for groups at the directory level, you need the Group.Unified template.

```
PowerShell
```

```
$Template = Get-MgBetaDirectorySettingTemplate | where -Property Id -Value "62375ab9-6b52-47ed-826b-58e47e0e304b" -EQ
```

3. Set a value for AllowToAddGuests for the specified template:

```
PowerShell
```

```
$params = @{
    templateId = "62375ab9-6b52-47ed-826b-58e47e0e304b"
    values = @(
        @{
            name = "AllowToAddGuests"
            value = "False"
        }
    )
}
```

4. Next, create a new settings object by using the [New-MgBetaDirectorySetting](#) cmdlet:

```
PowerShell
```

```
$Setting = New-MgBetaDirectorySetting -BodyParameter $params
```

5. You can read the values using:

```
PowerShell
```

```
$Setting.Values
```

Read settings at the directory level

If you know the name of the setting you want to retrieve, you can use the below cmdlet to retrieve the current settings value. In this example, we're retrieving the value for a setting named `UsageGuidelinesUrl`.

PowerShell

```
(Get-MgBetaDirectorySetting).Values | where -Property Name -Value UsageGuidelinesUrl -EQ
```

These steps read settings at directory level, which apply to all Office groups in the directory.

1. Read all existing directory settings:

PowerShell

```
Get-MgBetaDirectorySetting -All
```

This cmdlet returns a list of all directory settings:

Output

Id	DisplayName	TemplateId
Values		
--	-----	-----
c391b57d-5783-4c53-9236-cefb5c6ef323	Group.Unified	62375ab9-6b52-47ed-826b-58e47e0e304b
{class SettingValue { ... }}		

2. Read all settings for a specific group:

PowerShell

```
Get-MgBetaGroupSetting -GroupId "ab6a3887-776a-4db7-9da4-ea2b0d63c504"
```

3. Read all directory settings values of a specific directory settings object, using Settings ID GUID:

PowerShell

```
(Get-MgBetaDirectorySetting -DirectorySettingId "c391b57d-5783-4c53-9236-  
cefb5c6ef323").values
```

This cmdlet returns the names and values in this settings object for this specific group:

Output

Name	Value
ClassificationDescriptions	
DefaultClassification	
PrefixSuffixNamingRequirement	
CustomBlockedWordsList	
AllowGuestsToBeGroupOwner	False
AllowGuestsToAccessGroups	True
GuestUsageGuidelinesUrl	
GroupCreationAllowedGroupId	
AllowToAddGuests	True
UsageGuidelinesUrl	https://guideline.example.com
ClassificationList	
EnableGroupCreation	True

Remove settings at the directory level

This step removes settings at directory level, which apply to all Office groups in the directory.

PowerShell

```
Remove-MgBetaDirectorySetting -DirectorySettingId "c391b57d-5783-4c53-9236-  
cefb5c6ef323c"
```

Create settings for a specific group

1. Get the settings templates.

PowerShell

```
Get-MgBetaDirectorySettingTemplate
```

2. In the results, find for the settings template named "Groups.Unified.Guest":

Output

Id	DisplayName	Description
--	-----	-----
62375ab9-6b52-47ed-826b-58e47e0e304b	Group.Unified	...
08d542b9-071f-4e16-94b0-74abb372e3d9	Group.Unified.Guest	Settings for a specific Microsoft 365 group
4bc7f740-180e-4586-adb6-38b2e9024e6b	Application	...
898f1161-d651-43d1-805c-3b0b388a9fc2	Custom Policy Settings	...
5cf42378-d67d-4f36-ba46-e8b86229381d	Password Rule Settings	...

3. Retrieve the template object for the Groups.Unified.Guest template:

PowerShell

```
$Template1 = Get-MgBetaDirectorySettingTemplate | where -Property Id -Value "08d542b9-071f-4e16-94b0-74abb372e3d9" -EQ
```

4. Get the ID of the group you want to apply this setting to:

PowerShell

```
$GroupId = (Get-MgGroup -Filter "DisplayName eq '<YourGroupName>'").Id
```

5. Create the new setting:

PowerShell

```
$params = @{
    templateId = "08d542b9-071f-4e16-94b0-74abb372e3d9"
    values = @(
        @{
            name = "AllowToAddGuests"
            value = "False"
        }
    )
}
```

6. Create the group setting:

PowerShell

```
New-MgBetaGroupSetting -GroupId $GroupId -BodyParameter $params
```

7. To verify the settings, run this command:

PowerShell

```
Get-MgBetaGroupSetting -GroupId $GroupId | FL Values
```

Update settings for a specific group

1. Get the ID of the group whose setting you want to update:

```
PowerShell
```

```
$groupId = (Get-MgGroup -Filter "DisplayName eq '<YourGroupName>'").Id
```

2. Retrieve the setting of the group:

```
PowerShell
```

```
$Setting = Get-MgBetaGroupSetting -GroupId $GroupId
```

3. Update the setting of the group as you need:

```
PowerShell
```

```
$params = @{
    values = @(
        @{
            name = "AllowToAddGuests"
            value = "True"
        }
    )
}
```

4. Then you can set the new value for this setting:

```
PowerShell
```

```
Update-MgBetaGroupSetting -DirectorySettingId $Setting.Id -GroupId $GroupId -BodyParameter $params
```

5. You can read the value of the setting to make sure it has been updated correctly:

```
PowerShell
```

```
Get-MgBetaGroupSetting -GroupId $GroupId | FL Values
```

Cmdlet syntax reference

You can find more Microsoft Graph PowerShell documentation at [Microsoft Entra Cmdlets](#).

Manage group settings using Microsoft Graph

To configure and manage group settings using Microsoft Graph, see the [groupSetting resource type](#) and its associated methods.

Additional reading

- [Managing access to resources with Microsoft Entra groups](#)
- [Integrating your on-premises identities with Microsoft Entra ID](#)

Search groups and members in Microsoft Entra ID

Article • 01/15/2025

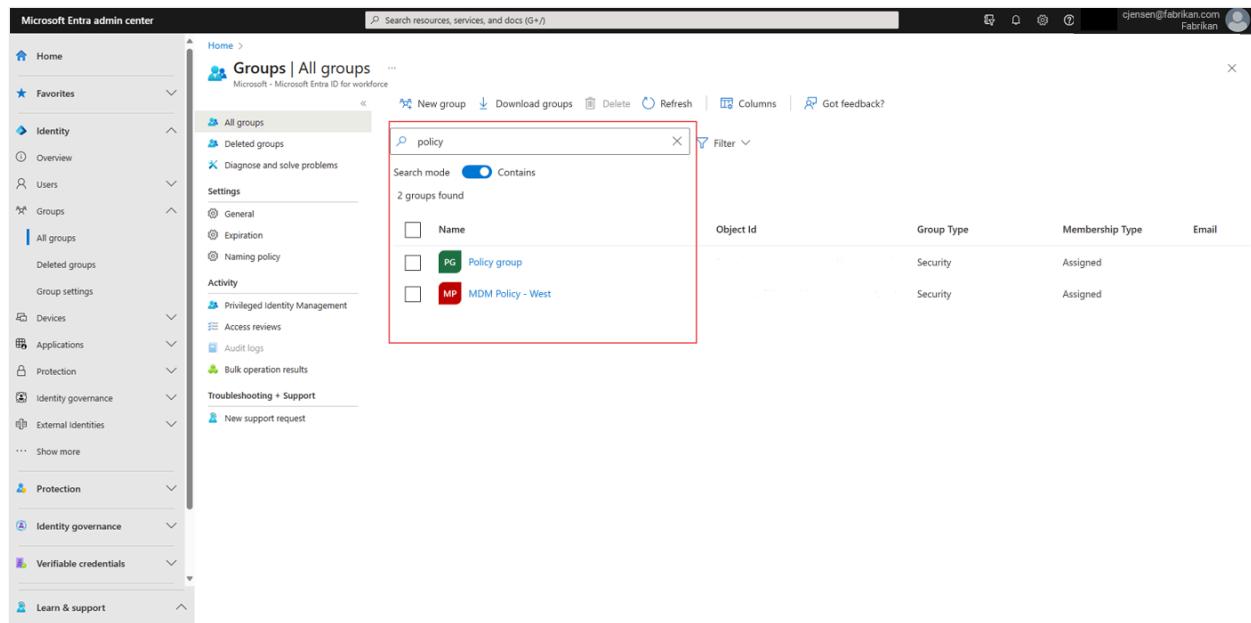
This article tells you how to search for members and owners of a group and how to use search filters in Microsoft Entra ID, part of Microsoft Entra. Search functions for groups include:

- Groups search capabilities, such as substring search in group names
- Filtering and sorting options on member and owner lists
- Search capabilities for member and owner lists

Group search and sort

On the **All groups** page, when you enter a search string, you can now toggle between "contains" and "starts with" searches on the **All groups** page only.

The substring search is done using whole words only, and any special characters are searched for also as an ANDed search. For example, searching for **-Name** starts a search for the substring **"Name"** and a search for **"-"**. Substring search is case-sensitive. Object ID or mailNickname properties are also searched.



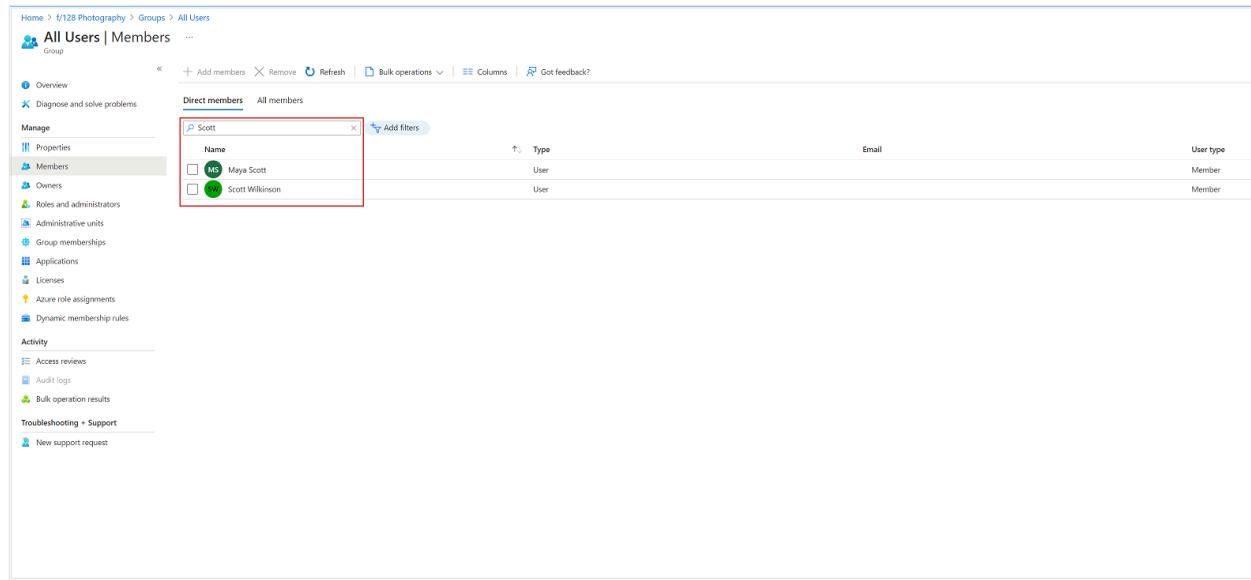
The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with categories like Home, Favorites, Identity, Groups, Devices, Applications, Protection, Identity governance, Verifiable credentials, and Learn & support. Under the Groups section, 'All groups' is selected. The main content area is titled 'Groups | All groups' and shows a search bar with the placeholder 'Search resources, services, and docs (G+ /)'. Below the search bar, there are buttons for 'New group', 'Download groups', 'Delete', 'Refresh', 'Columns', and 'Got feedback?'. A search results panel is open, showing a search for 'policy'. The search mode is set to 'Contains'. The results list shows two groups: 'Policy group' (Object Id: PG, Group Type: Security, Membership Type: Assigned) and 'MDM Policy - West' (Object Id: MP, Group Type: Security, Membership Type: Assigned). The entire search results panel is highlighted with a red border.

For example, a search for "policy" returns both "MDM policy – West" and "Policy group." A group named "New_policy" wouldn't be returned. You can sort the **All groups** list by name in ascending or descending order.

Group member search and filter

Search group member and owner lists

You can search the members or owners of a specific group by name, and when you enter a search string, a `contains` search is automatically done. For example, a search for "Scott" returns both Scott Wilkinson and Maya Scott.



The screenshot shows the 'All Users' page for a group named 'f1128 Photography'. The left sidebar has sections for Overview, Diagnose and solve problems, Manage (Properties, Members, Owners, Roles and administrators, Administrative units, Group memberships, Applications, Licenses, Azure role assignments, Dynamic membership rules), Activity (Access reviews, Audit logs, Bulk operation results), and Troubleshooting + Support (New support request). The main area shows 'Direct members' and 'All members' tabs. A search bar at the top contains the text 'Scott'. Below it, a table lists users: Maya Scott (User, Member) and Scott Wilkinson (User, Member). Both users have green profile icons. A red box highlights the search bar and the table area.

Filter member and owner lists

You can also filter the group members and owners lists by user type. This information is found in the **User Type** column in the members or owners list. You can filter the list to see only members or guests.

The **Members** page includes all the unique members of group including anyone who inherits their group membership from another group.

You can also search and filter the lists individually. Filtering the all members list doesn't affect filters that are applied to the direct members list.

Group memberships

You can also view group memberships on the **Group memberships** page. The **Group memberships** page supports search, sort, and filter operations that are similar to the other Groups pages.

Group member counts

The group **Overview** page provides member counts for groups. You can see the total number of direct members for a group and the total membership count (all the unique members of group including inherited memberships) on the **Overview** page.



Next steps

These articles provide additional information on working with groups in Microsoft Entra ID.

- [View your groups and members](#)
- [Manage group memberships](#)
- [Manage rules for dynamic membership groups](#)
- [Edit your group settings](#)
- [Manage access to resources using groups](#)
- [Manage access to SaaS apps using groups](#)
- [Manage groups using PowerShell commands](#)
- [Add an Azure subscription to Microsoft Entra ID](#)

Feedback

Was this page helpful?

Yes

No

[Provide product feedback ↗](#)

Understand and manage dynamic group processing in Microsoft Entra ID

Article • 04/30/2025

Dynamic membership groups in Microsoft Entra ID are a powerful feature that enables administrators to automate the management of group memberships. Changes to memberships are typically processed within a few hours.

However, under certain conditions, customers can experience delays in membership updates. Processing can take more than 24 hours. Understanding the underlying causes can help admins optimize their configurations and avoid unnecessary processing bottlenecks.

How dynamic group processing works

Dynamic group processing operates in a sequential manner. Changes for a single tenant are evaluated and applied in order, rather than all at once. Large volumes of changes, especially when they affect many users or devices, can lead to long processing queues. The long queues can extend the time required for updates to finish processing.

Key factors that affect processing time

The three biggest factors that influence processing and can cause membership updates to take longer are:

- **Number of dynamic groups:** Tenants that have a large number of dynamic groups require more evaluations, increasing processing time.
- **Number of object changes:** A high volume of user or device changes can create a long processing queue and extend the processing time. Examples include changes to extension attributes, device additions or removals, and bulk user updates.
- **Rule configuration:** Certain rule configurations can affect processing time. For instance, the choice of inefficient operators like `Match`, `Contains`, or `memberof` can increase processing time. Rule complexity is also a contributing factor.

Best practices for managing dynamic membership groups in your tenant

To help ensure efficient processing and minimize delays, consider the following best practices.

Monitor the number of dynamic membership groups in your tenant

Regularly review the number of groups in your tenant. Delete inactive or outdated groups.

Pause nonessential groups

You can pause nonessential groups to improve processing performance. You might consider pausing group processing in these circumstances:

- **Planned large-scale updates:** You anticipate making a large number of changes to group membership. For example, you plan to make changes to more than 500 groups or make more than 20,000 membership changes.
- **Unexpected delays:** You notice that group membership hasn't changed and you encounter unexpected delays.

To temporarily halt processing, use the **Pause All Groups** script. Allow the service to recover before resuming.

Don't unpause the groups immediately. We recommend waiting a minimum of 24 hours to allow group processing to catch up. Then, check your audit logs to see if they're back to baseline. If necessary, unpause groups in phases rather than all at once.

Optimize rule efficiency

- Avoid the use of the `Match` operator in rules as much as possible. Instead, use the `StartsWith`, `Equals`, or `EndsWith` operator.
- Avoid the use of the `Contains` operator in rules as much as possible. It can lead to increased processing time.
- Use fewer `-or` operators. Instead, use the `-in` operator to group rules into a single criterion. Grouping rules makes them easier to evaluate.
- Avoid the use of the `memberOf` operator if possible. It's currently in preview, and it comes with bugs and limitations. It can also introduce more complexity, particularly if a tenant has a large number of groups or frequent updates. The recommendation is to delete existing `memberOf` groups in your tenant.

For more help with optimizing dynamic group processing, review [Create simpler, more efficient rules for dynamic membership groups in Microsoft Entra ID](#).

Summary

Delays in dynamic group processing primarily happen due to high volumes of changes and large numbers of groups. By following best practices like optimizing rule efficiency, monitoring changes, and pausing nonessential groups when necessary, IT administrators can improve processing performance and avoid unnecessary delays.

Related content

- [Manage rules for dynamic membership groups in Microsoft Entra ID](#)
- [Troubleshoot dynamic groups](#)

Create or update a dynamic membership group in Microsoft Entra ID

Article • 04/30/2025

You can use rules to determine dynamic membership groups based on user or device properties in Microsoft Entra ID. This article describes how to set up a rule for a dynamic membership group in the Azure portal.

Group membership based on user or device properties is supported for security groups and Microsoft 365 groups. When you apply a rule for a dynamic membership group, user and device attributes are evaluated for matches with the membership rule. When an attribute changes for a user or device, all rules for dynamic membership groups in the organization are processed for changes. Users and devices are added or removed if they meet the conditions for a dynamic membership group. In Microsoft Entra ID, a single tenant can have a maximum of 15,000 dynamic membership groups.

ⓘ Note

Security groups can include either devices or users, but Microsoft 365 groups can include only users.

Using dynamic membership groups requires a Microsoft Entra ID P1 license or an Intune for Education license. For more information, see [Manage rules for dynamic membership groups in Microsoft Entra ID](#).

Rule builder in the Azure portal

Microsoft Entra ID provides a rule builder to create and update your important rules more quickly. The rule builder supports the construction of up to five expressions.

Home > Contoso > Groups - All groups > Conditional Access Exceptions - Dynamic membership rules

Conditional Access Exceptions - Dynamic membership rules

Group

Overview

Manage

- Properties
- Members
- Owners
- Group memberships
- Applications
- Licenses
- Azure resources
- Dynamic membership rules**

Activity

Access reviews

Audit logs

Bulk operation results (Preview)

Save | Discard | Got feedback?

Configure Rules

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. [Learn more](#)

And/Or	Property	Operator	Value
Or	userPrincipalName	Equals	gorans
Or	userPrincipalName	Equals	byrnem

[Add expression](#) [Get custom extension properties](#)

Rule syntax

```
(user.userPrincipalName -eq "goransson@contoso.com") or (user.userPrincipalName -eq "byrnem@contoso.com") or (
```

The rule builder makes it easier to form a rule with a few simple expressions. However, it can't be used to reproduce every rule. If the rule builder doesn't support the rule that you want to create, you can use the text box.

Here are some examples of advanced rules or syntax for which we recommend that you use the text box:

- Rule with more than five expressions
- Rule for direct reports
- Setting [operator precedence](#)
- [Rule with complex expressions](#); for example, `(user.proxyAddresses -any (_ -contains "contoso"))`

! Note

The rule builder might not be able to display some rules constructed in the text box. You might see a message when the rule builder can't display the rule. The rule builder doesn't change the supported syntax, validation, or processing of rules for dynamic membership groups in any way.

For examples of syntax and supported properties, operators, and values for a membership rule, see [Manage rules for dynamic membership groups in Microsoft Entra ID](#).

Create a rule for a dynamic membership group

1. Sign in to the Microsoft Entra admin center [as at least a Groups Administrator](#).

2. Select Microsoft Entra ID > Groups.

3. Select All groups, and then select New group.

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with various categories like Home, Favorites, Identity, Groups (which is selected and highlighted with a red box), and others. The main content area is titled 'Groups | All groups' and shows a list of existing groups. At the top of this list, there's a 'New group' button, which is also highlighted with a red box. The table lists groups such as 'AADTestGroup', 'AADTestGroup2', 'Access to Blog', etc., with columns for Name, Group Type, Membership Type, Email, and Source.

4. On the Group pane, enter a name and description for the new group. Select a Membership type value for either users or devices, and then select Add dynamic query.

5. In the rule builder, add up to five expressions. To add more than five expressions, you must use the text box.

This screenshot shows the 'Dynamic membership rules' configuration page. It has a header with 'Save', 'Discard', and 'Got feedback?' buttons. Below that is a 'Configure Rules' section with a note about using the rule builder or rule syntax text box. The main area is a table for defining membership rules. One row is visible, showing 'accountEnabled' as the property with 'All' as the operator and 'byrnem@contoso.com' as the value. A red box highlights the 'Add expression' button in the bottom-left corner of the table. At the bottom, there's a 'Rule syntax' section with the generated rule: '(user.accountEnabled -all) and (user.userPrincipalName -all "byrnem@contoso.com") and (user.userPrincipalName -all "forsbergd@contoso.com")'.

6. To see the custom extension properties that are available for your membership query:

- a. Select **Get custom extension properties**.
- b. Enter the application ID, and then select **Refresh properties**.

7. After you finish creating the rule, select **Save**.

8. On the **New group** page, select **Create** to create the group.

If the rule that you entered isn't valid, the portal displays an explanation of why the rule couldn't be processed. Read it carefully to understand how to fix the rule.

Update an existing rule

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Groups Administrator**.
2. Select **Microsoft Entra ID**.
3. Select **Groups > All groups**.
4. Select a group to open its profile.
5. On the profile page for the group, select **Dynamic membership rules**. The rule builder supports up to five expressions. To add more than five expressions, you must use the text box.

The screenshot shows the 'Conditional Access Exceptions - Dynamic membership rules' page in the Microsoft Entra admin center. The left sidebar has a 'Dynamic membership rules' link highlighted with a red box. The main pane displays a table with two expressions:

And/Or	Property	Operator	Value
Or	userPrincipalName	Equals	gorans
Or	userPrincipalName	Equals	byrnem

Below the table are 'Add expression' and 'Get custom extension properties' buttons, and a 'Rule syntax' section with the formula '(user.userPrincipalName -eq "goransson@contoso.com") or (user.userPrincipalName -eq "byrnem@contoso.com") or (user.userPrincipalName -eq "forsbe@contoso.com")'.

6. To see the custom extension properties that are available for your membership rule:
 - a. Select **Get custom extension properties**.
 - b. Enter the application ID, and then select **Refresh properties**.
7. After you finish updating the rule, select **Save**.

Turn on or off the welcome email

When an admin creates a new Microsoft 365 group, the users who are added to the group receive a welcome email notification. Later, if any attributes of a user or device (only for security groups) change, all rules for dynamic membership groups in the organization are processed for changes. Users who are added then also receive the welcome notification.

You can turn on or turn off this behavior in [Exchange PowerShell](#).

Check the processing status for a rule

You can see the rule processing status and the date of the last membership change on the overview page for the dynamic membership group.

The screenshot shows the Microsoft 365 Groups overview page for a group named "Test123". The page includes a navigation bar with "Home > Groups | All groups >" and a "Delete" button. On the left, there's a sidebar with sections like "Overview", "Diagnose and solve problems", "Manage" (Properties, Members, Owners, Roles and administrators, Administrative units, Group memberships, Applications, Licenses, Azure role assignments, Dynamic membership rules), "Activity" (Access reviews, Audit logs, Bulk operation results), and "Troubleshooting + Support" (New support request). The main content area displays the group's name "Test123" and a purple square icon with "TE". It shows the following details:

Setting	Value
Membership type	Dynamic
Source	Cloud
Type	Security
Object Id	[Redacted]
Created at	4/25/2022, 2:15:17 PM
Dynamic rule processing status	Update complete For more recent activity, visit Audit logs
Last membership change	10/19/2022, 11:19:10 AM For more recent activity, visit Audit logs
Pause processing	<input checked="" type="checkbox"/> No
Direct members	687 Total 687 User(s)
Group memberships	0 Group(s)
Owners	0
Total members	687

The following status messages can appear for **Dynamic rule processing status**:

- **Evaluating:** The group change was received and the updates are being evaluated.
- **Processing:** Updates are being processed.

- **Update complete:** Processing finished and all applicable updates were made.
- **Processing error:** Processing couldn't finish because of an error in evaluating the membership rule.
- **Update paused:** The administrator paused the rule to update dynamic membership groups. `MembershipRuleProcessingState` is set to `Paused`.
- **Not started:** Processing hasn't started.

Note

This page now has a **Pause processing** option. Previously, this option was available only through the modification of the `membershipRuleProcessingState` property. Someone who has at least the [Groups Administrator](#) role can manage this setting and can pause and resume the processing of dynamic membership groups. Group owners who don't have the correct roles don't have the necessary rights to edit this setting.

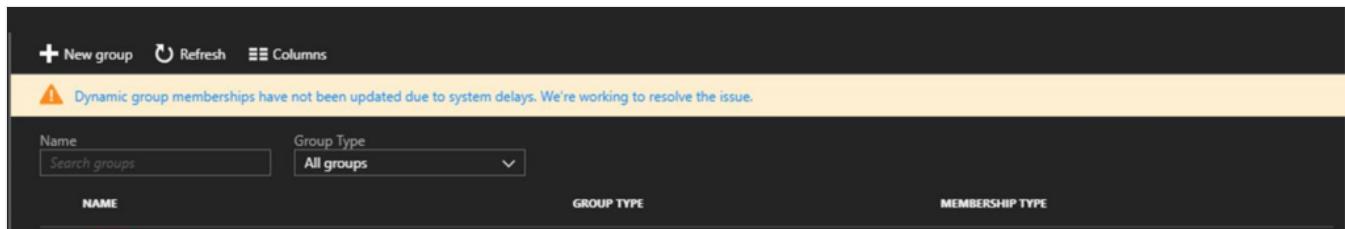
The following status messages appear for **Last membership change**:

- **<Date and time>**: The membership was last updated at this date and time.
- **In Progress**: Updates are currently in progress.
- **Unknown**: The last update time can't be retrieved. The group might be new.

Important

After you pause and unpause the processing of dynamic membership groups, the **Last membership change** date shows a placeholder value. This value is updated after the processing finishes.

If an error occurs during processing of the membership rule for a specific group, an alert appears on the top of the overview page for the group. If no pending updates for dynamic membership groups can be processed for all the groups within the organization for more than 24 hours, an alert appears above **All groups**.



Related content

- [Create a group with members and view all groups and members](#)

- Manage Microsoft Entra groups and group membership
- Manage rules for dynamic membership groups in Microsoft Entra ID

Manage rules for dynamic membership groups in Microsoft Entra ID

Article • 04/30/2025

You can create user-based or device attribute-based rules to enable membership for dynamic membership groups in Microsoft Entra ID. You can add and remove dynamic membership groups automatically by using membership rules based on member attributes. In Microsoft Entra, a single tenant can have a maximum of 15,000 dynamic membership groups.

This article details the properties and syntax to create rules for dynamic membership groups based on users or devices.

! Note

Security groups can include either devices or users, but Microsoft 365 groups can include only users.

Considerations for dynamic membership groups

When the attributes of a user or a device change, the system evaluates all rules for dynamic membership groups in a directory to see if the change would trigger any group additions or removals. If users or devices satisfy a rule on a group, they're added as members of that group. If they no longer satisfy the rule, they're removed. You can't manually add or remove a member of a dynamic membership group.

Also keep these limitations in mind:

- You can create a dynamic membership groups for users or devices, but you can't create a rule that contains both users and devices.
- You can't create a device membership group based on the user attributes of the device owner. Device membership rules can reference only device attributes.

License requirements

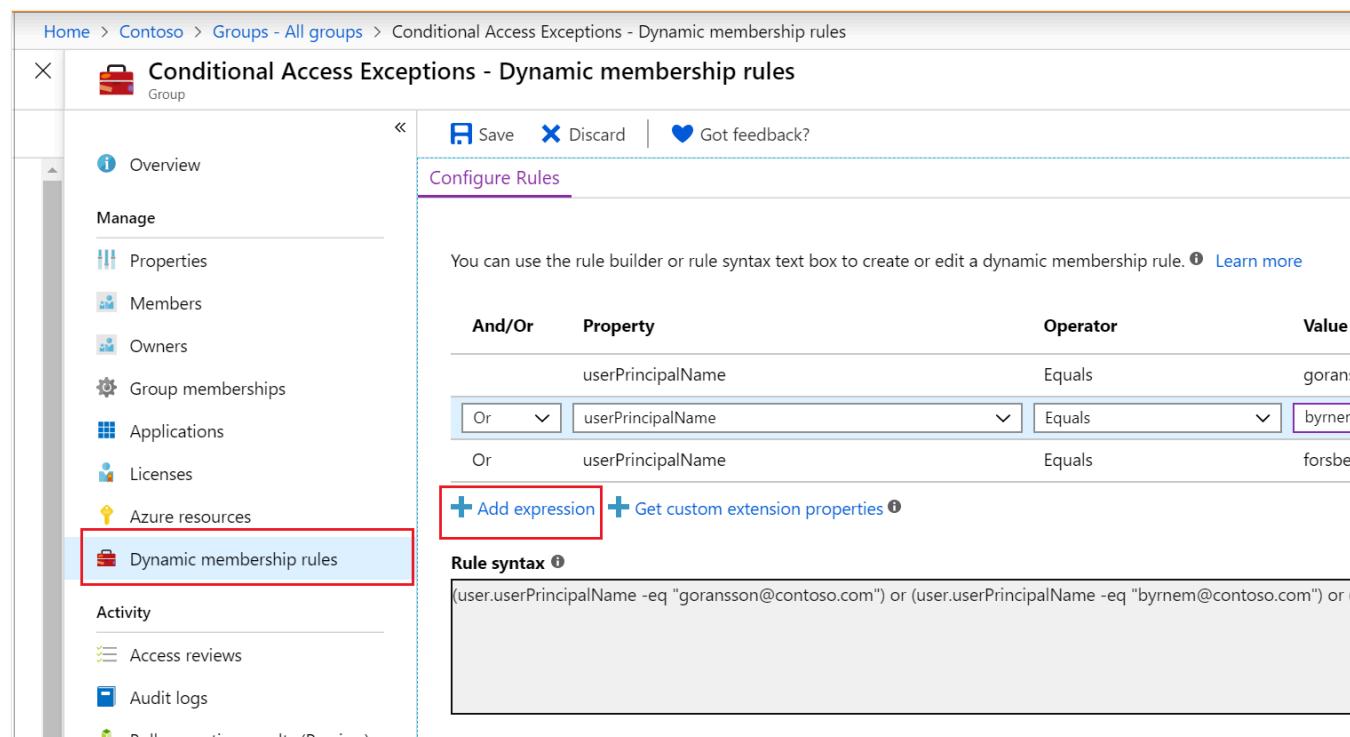
The feature of dynamic membership groups requires a Microsoft Entra ID P1 license or an Intune for Education license for each unique user who's a member of one or more dynamic membership groups. You don't have to assign licenses to users for them to be members of dynamic membership groups. But you must have the minimum number of licenses in the Microsoft Entra organization to cover all such users.

For example, if you have a total of 1,000 unique users in all dynamic membership groups in your organization, you need at least 1,000 licenses for Microsoft Entra ID P1 to meet the license requirement.

No license is required for devices that are members of a dynamic membership group based on a device.

Rule builder in the Azure portal

Microsoft Entra ID provides a rule builder to create and update your important rules more quickly. The rule builder supports the construction of up to five expressions. You can use the rule builder to form a rule with a few simple expressions, but you can't use it to reproduce every rule. If the rule builder doesn't support the rule that you want to create, you can use the text box.



The screenshot shows the Azure portal interface for managing conditional access exceptions. The left sidebar lists various management options like Properties, Members, Owners, Group memberships, Applications, Licenses, and Azure resources. The 'Dynamic membership rules' option is selected and highlighted with a red box. The main pane displays the 'Configure Rules' section, which includes a note about using the rule builder or rule syntax text box. Below this is a table for defining expressions, showing two entries: one for 'userPrincipalName' with 'Equals' operator and value 'gorans', and another 'Or' condition for 'userPrincipalName' with 'Equals' operator and value 'byrnem'. At the bottom of the rule builder interface is a red box highlighting the '+ Add expression' button. The 'Rule syntax' section at the bottom contains a preview of the generated rule syntax.

For step-by-step instructions, see [Create or update a dynamic membership group](#).

Important

The rule builder is available only for user-based dynamic membership groups. You can create device-based dynamic membership groups only by using the text box.

Here are some examples of advanced rules or syntax that require the use of the text box:

- Rule with more than five expressions
- Rule for direct reports

- Rule with a `-contains` or `-notContains` operator
- Setting [operator precedence](#)
- [Rule with complex expressions](#); for example, `(user.proxyAddresses -any (_ -startsWith "contoso"))`

! Note

The rule builder might not be able to display some rules constructed in the text box. You might see a message when the rule builder can't display the rule. The rule builder doesn't change the supported syntax, validation, or processing of rules for dynamic membership groups in any way.

Rule syntax for a single expression

A single expression is the simplest form of a membership rule. A rule with a single expression takes the form of `<Property> <Operator> <Value>`, where the syntax for the property is the name of `<object>.<property>`.

The following example illustrates a properly constructed membership rule with a single expression:

```
user.department -eq "Sales"
```

Parentheses are optional for a single expression. The total length of the body of your membership rule can't exceed 3,072 characters.

Constructing the body of a membership rule

A membership rule that automatically populates a group with users or devices is a binary expression that results in a true or false outcome. The three parts of a simple rule are:

- Property
- Operator
- Value

The order of the parts within an expression is important to avoid syntax errors.

Supported properties

You can use three types of properties to construct a membership rule:

- Boolean
- Date/time
- String
- String collection

You can use the following user properties to create a single expression.

Properties of type Boolean

[Expand table](#)

Property	Allowed values	Usage
accountEnabled	true, false	user.accountEnabled -eq true
dirSyncEnabled	true, false	user.dirSyncEnabled -eq true

Properties of type date/time

[Expand table](#)

Property	Allowed values	Usage
employeeHireDate (preview)	Any <code>DateTimeOffset</code> value or keyword <code>system.now</code>	user.employeeHireDate -eq "value"

Properties of type string

[Expand table](#)

Property	Allowed values	Usage
city	Any string value or <code>null</code>	user.city -eq "value"
country	Any string value or <code>null</code>	user.country -eq "value"
companyName	Any string value or <code>null</code>	user.companyName -eq "value"
department	Any string value or <code>null</code>	user.department -eq "value"
displayName	Any string value	user.displayName -eq "value"

Property	Allowed values	Usage
employeeId	Any string value	<code>user.employeeId -eq "value"</code> <code>user.employeeId -ne "null"</code>
facsimileTelephoneNumber	Any string value or <code>null</code>	<code>user.facsimileTelephoneNumber -eq "value"</code>
givenName	Any string value or <code>null</code>	<code>user.givenName -eq "value"</code>
jobTitle	Any string value or <code>null</code>	<code>user.jobTitle -eq "value"</code>
mail	Any string value or <code>null</code> (SMTP address of the user)	<code>user.mail -eq "value"</code> <code>user.mail -notEndsWith "@Contoso.com"</code>
mailNickname	Any string value (mail alias of the user)	<code>user.mailNickname -eq "value"</code> <code>user.mailNickname -endsWith "-vendor"</code>
memberOf	Any string value (valid group object ID)	<code>user.memberOf -any (group.objectId -in ['value'])</code>
mobile	Any string value or <code>null</code>	<code>user.mobile -eq "value"</code>
objectId	GUID of the user object	<code>user.objectId -eq "aaaaaaaa-0000-1111-2222-bbbbbbbbbbbb"</code>
onPremisesDistinguishedName	Any string value or <code>null</code>	<code>user.onPremisesDistinguishedName -eq "value"</code>
onPremisesSecurityIdentifier	On-premises security identifier (SID) for users who were synchronized from on-premises to the cloud	<code>user.onPremisesSecurityIdentifier -eq "S-1-1-1111111111-1111111111-1111111111-11111111"</code>
passwordPolicies	<code>None</code> , <code>DisableStrongPassword</code> , <code>DisablePasswordExpiration</code> , <code>DisablePasswordExpiration</code> , <code>DisableStrongPassword</code>	<code>user.passwordPolicies -eq "DisableStrongPassword"</code>
physicalDeliveryOfficeName	Any string value or <code>null</code>	<code>user.physicalDeliveryOfficeName -eq "value"</code>
postalCode	Any string value or <code>null</code>	<code>user.postalCode -eq "value"</code>
preferredLanguage	ISO 639-1 code	<code>user.preferredLanguage -eq "en-US"</code>

Property	Allowed values	Usage
sipProxyAddress	Any string value or <code>null</code>	<code>user.sipProxyAddress -eq "value"</code>
state	Any string value or <code>null</code>	<code>user.state -eq "value"</code>
streetAddress	Any string value or <code>null</code>	<code>user.streetAddress -eq "value"</code>
surname	Any string value or <code>null</code>	<code>user.surname -eq "value"</code>
telephoneNumber	Any string value or <code>null</code>	<code>user.telephoneNumber -eq "value"</code>
usageLocation	Two-letter country or region code	<code>user.usageLocation -eq "US"</code>
userPrincipalName	Any string value	<code>user.userPrincipalName -eq "alias@domain"</code>
userType	<code>member</code> , <code>guest</code> , <code>null</code>	<code>user.userType -eq "Member"</code>

Properties of type string collection

[Expand table](#)

Property	Allowed values	Examples
otherMails	Any string value	<code>user.otherMails -startsWith "alias@domain"</code> <code>user.otherMails -endsWith "@contoso.com"</code>
proxyAddresses	<code>SMTP: alias@domain</code> , <code>smtp: alias@domain</code>	<code>user.proxyAddresses -startsWith "SMTP: alias@domain"</code> <code>user.proxyAddresses -notEndsWith "@outlook.com"</code>

For the properties used for device rules, see [Rules for devices](#).

Supported expression operators

The following table lists all the supported operators and their syntax for a single expression. You can use operators with or without the hyphen (-) prefix. The `Contains` operator does partial string matches but not matches for items in a collection.

Caution

For best results, minimize the use of `Match` or `Contains` as much as possible. The article [Create simpler, more efficient rules for dynamic membership groups](#) provides guidance on how to create rules that result in better dynamic group processing times. The `memberOf` operator is in preview and has some limitations, so use it with caution.

 Expand table

Operator	Syntax
Ends With	<code>-endsWith</code>
Not Ends With	<code>-notEndsWith</code>
Not Equals	<code>-ne</code>
Equals	<code>-eq</code>
Not Starts With	<code>-notStartsWith</code>
Starts With	<code>-startsWith</code>
Not Contains	<code>-notContains</code>
Contains	<code>-contains</code>
Not Match	<code>-notMatch</code>
Match	<code>-match</code>
In	<code>-in</code>
Not In	<code>-notIn</code>

Using the `-in` and `-notIn` operators

If you want to compare the value of a user attribute against multiple values, you can use the `-in` or `-notIn` operator. Use the bracket symbols (`[` and `]`) to begin and end the list of values.

In the following example, the expression evaluates to `true` if the value of `user.department` equals any of the values in the list:

```
user.department -in  
["50001", "50002", "50003", "50005", "50006", "50007", "50008", "50016", "50020", "50024", "50038", "50039", "51100"]
```

Using the -le and -ge operators

You can use the less than (-le) or greater than (-ge) operator when you're using the `employeeHireDate` attribute in rules for dynamic membership groups.

Here are examples:

```
user.employeeshiredate -ge system.now -plus p1d  
user.employeeshiredate -le 2020-06-10T18:13:20Z
```

Using the -match operator

You can use the `-match` operator for matching any regular expression.

For the following example, `Da`, `Dav`, and `David` evaluate to `true`. `aDa` evaluates to `false`.

```
user.displayName -match "^Da.*"
```

For the following example, `David` evaluates to `true`. `Da` evaluates to `false`.

```
user.displayName -match ".*vid"
```

Supported values

The values that you use in an expression can consist of several types:

- Strings
- Boolean (`true`, `false`)
- Numbers
- Arrays (number array, string array)

When you specify a value within an expression, it's important to use the correct syntax to avoid errors. Here are some syntax tips:

- Double quotation marks are optional unless the value is a string.

- Regex and string operations aren't case sensitive.
- Ensure that property names are correctly formatted as shown, because they're case sensitive.
- When a string value contains double quotation marks, you should escape both quotation marks by using the backslash (\) character. For example, `user.department -eq "Sales"` is the proper syntax when `Sales` is the value. Escape single quotation marks by using two single quotation marks instead of one each time.
- You can also perform null checks by using `null` as a value; for example, `user.department -eq null`.

Use of null values

To specify a `null` value in a rule:

- Use `-eq` or `-ne` when you're comparing the `null` value in an expression.
- Use quotation marks around the word `null` only if you want it to be interpreted as a literal string value.
- Don't use the `-not` operator as a comparative operator for the null value. If you use it, you get an error whether you use `null` or `$null`.

The correct way to reference the `null` value is as follows:

```
user.mail -ne null
```

Rules with multiple expressions

Rules for dynamic membership groups can consist of more than one single expression connected by the `-and`, `-or`, and `-not` logical operators. You can also use logical operators in combination.

The following are examples of properly constructed membership rules with multiple expressions:

```
(user.department -eq "Sales") -or (user.department -eq "Marketing")
(user.department -eq "Sales") -and -not (user.jobTitle -startsWith "SDE")
```

Operator precedence

The following list shows all operators in order of precedence from highest to lowest. Operators on the same line are of equal precedence.

```
-eq -ne -startsWith -notStartsWith -contains -notContains -match -notMatch -in -  
notIn  
-not  
-and  
-or  
-any -all
```

The following example illustrates operator precedence where two expressions are being evaluated for the user:

```
user.department -eq "Marketing" -and user.country -eq "US"
```

You need parentheses only when precedence doesn't meet your requirements. For example, if you want the department to be evaluated first, the following code shows how you can use parentheses to determine the order:

```
user.country -eq "US" -and (user.department -eq "Marketing" -or user.department  
-eq "Sales")
```

Rules with complex expressions

A membership rule can consist of complex expressions where the properties, operators, and values take on more complex forms. Expressions are considered complex when any of the following points are true:

- The property consists of a collection of values; specifically, multi-value properties.
- The expressions use the `-any` and `-all` operators.
- The value of the expression can itself be one or more expressions.

Multi-value properties

Multi-value properties are collections of objects of the same type. You can use them to create membership rules by using the `-any` and `-all` logical operators.

[Expand table](#)

Property	Values	Usage
<code>assignedPlans</code>	Each object in the collection exposes the following string properties: <code>capabilityStatus</code> , <code>service</code> , <code>servicePlanId</code>	<code>user.assignedPlans -any (assignedPlan.servicePlanId -eq "aaaa0a0a-bb1b-cc2c-dd3d-effff4e4e4e" -and assignedPlan.capabilityStatus -eq "Enabled")</code>
<code>proxyAddresses</code>	<code>SMTP: alias@domain</code> , <code>smtp: alias@domain</code>	<code>(user.proxyAddresses -any (_ -startsWith "contoso"))</code>

Using the `-any` and `-all` operators

You can use the following operators to apply a condition to one or all of the items in the collection:

- `-any`: Satisfied when at least one item in the collection matches the condition.
- `-all`: Satisfied when all items in the collection match the condition.

Example 1

`assignedPlans` is a multi-value property that lists all service plans assigned to the user. The following expression selects users who have the Exchange Online (Plan 2) service plan (as a GUID value) that's also in an `Enabled` state:

```
user.assignedPlans -any (assignedPlan.servicePlanId -eq "efb87545-963c-4e0d-99df-69c6916d9eb0" -and assignedPlan.capabilityStatus -eq "Enabled")
```

You can use a rule like this one to group all users for whom a Microsoft 365 or other Microsoft Online Services capability is enabled. You could then apply the rule with a set of policies to the group.

Example 2

The following expression selects all users who have any service plan that's associated with the Intune service (identified by the service name `sco`):

```
user.assignedPlans -any (assignedPlan.service -eq "SCO" -and  
assignedPlan.capabilityStatus -eq "Enabled")
```

Example 3

The following expression selects all users who have no assigned service plan:

```
user.assignedPlans -all (assignedPlan.servicePlanId -eq null)
```

Using the underscore (_) syntax

The underscore (_) syntax matches occurrences of a specific value in one of the multi-value string collection properties to add users or devices to a dynamic membership group. You use it with the `-any` or `-all` operator.

Here's an example of using the underscore in a rule to add members based on `user.proxyAddress`. (It works the same for `user.otherMails`.) This rule adds any user who has a proxy address that starts with `contoso` to the group.

```
(user.proxyAddresses -any (_ -startsWith "contoso"))
```

Other properties and common rules

Create a rule for direct reports

You can create a group that contains all direct reports of a manager. When the manager's direct reports change in the future, the group's membership is adjusted automatically.

You construct the direct reports rule by using the following syntax:

```
Direct Reports for "{objectID_of_manager}"
```

Here's an example of a valid rule, where `aaaaaaaa-0000-1111-2222-bbbbbbbbbbbb` is the object ID of the manager:

```
Direct Reports for "aaaaaaaa-0000-1111-2222-bbbbbbbbbbbb"
```

The following tips can help you use the rule properly:

- The *manager ID* is the object ID of the manager. You can find it in the manager's profile.
- For the rule to work, make sure that the `Manager` property is set correctly for users in your organization. You can check the current value in the user's profile.
- This rule supports only the manager's direct reports. You can't create a group that has the manager's direct reports *and* their reports.
- You can't combine this rule with any other membership rules.

Create a rule for all users

You can create a group that contains all users within an organization by using a membership rule. When users are added or removed from the organization in the future, the group's membership is adjusted automatically.

You construct the rule for all users by using a single expression that includes the `-ne` operator and the `null` value. This rule adds business-to-business guest users and member users to the group.

```
user.objectId -ne null
```

If you want your group to exclude guest users and include only members of your organization, you can use the following syntax:

```
(user.objectId -ne null) -and (user.userType -eq "Member")
```

Create a rule for all devices

You can create a group that contains all devices within an organization by using a membership rule. When devices are added or removed from the organization in the future, the group's membership is adjusted automatically.

You construct the rule for all devices by using single expression that includes the `-ne` operator and the `null` value:

```
device.objectId -ne null
```

Extension attributes and custom extension properties

Extension attributes and custom extension properties are supported as string properties in rules for dynamic membership groups.

You can [sync extension attributes](#) from on-premises Windows Server Active Directory. Or you can update extension attributes by using Microsoft Graph.

Extension attributes take the format of `ExtensionAttribute<x>`, where `<x>` equals `1 - 15`. Multi-value extension properties aren't supported in rules for dynamic membership groups.

Here's an example of a rule that uses an extension attribute as a property:

```
(user.extensionAttribute15 -eq "Marketing")
```

You can [sync custom extension properties](#) from on-premises Windows Server Active Directory or from a connected software as a service (SaaS) application. You can create custom extension properties by using Microsoft Graph.

Custom extension properties take the format of `user.extension_[GUID]_[Attribute]`, where:

- `[GUID]` is the stripped version of the unique identifier in Microsoft Entra ID for the application that created the property. It contains only characters 0-9 and A-Z.
- `[Attribute]` is the name of the property as it was created.

An example of a rule that uses a custom extension property is:

```
user.extension_c272a57b722d4eb29bfe327874ae79cb_OfficeNumber -eq "123"
```

Custom extension properties are also called directory or Microsoft Entra extension properties.

You can find the custom property name in the directory by querying a user's property in Graph Explorer and searching for the property name. Also, you can now select the **Get custom extension properties** link in the dynamic rule builder to enter a unique app ID and receive the full list of custom extension properties to use when creating a rule for dynamic membership groups. You can refresh this list to get any new custom extension properties for that app. Extension attributes and custom extension properties must be from applications in your tenant.

For more information, see [Use the attributes in dynamic membership groups](#).

Rules for devices

You can create a rule that selects device objects for membership in a group. You can't have both users and devices as group members.

! Note

The `organizationalUnit` attribute is no longer listed, and you shouldn't use it. Intune sets this string in specific cases, but Microsoft Entra ID doesn't recognize it. No devices are added to groups based on this attribute.

The `systemlabels` attribute is read-only. You can't set it with Intune.

For Windows 10, the correct format of the `deviceOSVersion` attribute is `device.deviceOSVersion -startsWith "10.0.1"`. You can validate the formatting by using the `Get-MgDevice` PowerShell cmdlet:

```
Get-MgDevice -Search "displayName:YourMachineNameHere" -ConsistencyLevel eventual  
| Select-Object -ExpandProperty 'OperatingSystemVersion'
```

You can use the following device attributes.

 [Expand table](#)

Device attribute	Values	Examples
<code>accountEnabled</code>	<code>true</code> , <code>false</code>	<code>device.accountEnabled -eq true</code>
<code>deviceCategory</code>	A valid device category name	<code>device.deviceCategory -eq "BYOD"</code>
<code>deviceId</code>	A valid Microsoft Entra device ID	<code>device.deviceId -eq "d4fe7726-5966-431c-b3b8-cddc8fdb717d"</code>

Device attribute	Values	Examples
deviceManagementAppId	A valid application ID for mobile device management in Microsoft Entra ID	<pre>device.deviceManagementAppId -eq "0000000a-0000-0000-c000-000000000000"</pre> <p>for Microsoft Intune managed devices</p> <pre>"54b943f8-d761-4f8d-951e-9cea1846db5a"</pre> <p>for System Center Configuration Manager co-managed devices</p>
deviceManufacturer	Any string value	<pre>device.deviceManufacturer -eq "Samsung"</pre>
deviceModel	Any string value	<pre>device.deviceModel -eq "iPad Air"</pre>
displayName	Any string value	<pre>device.displayName -eq "Rob iPhone"</pre>
deviceOSType	Any string value	<pre>(device.deviceOSType -eq "iPad") -or (device.deviceOSType -eq "iOS")</pre> <pre>device.deviceOSType -startsWith "AndroidEnterprise"</pre> <pre>device.deviceOSType -eq "AndroidForWork"</pre> <pre>device.deviceOSType -eq "Windows"</pre>
deviceOSVersion	Any string value	<pre>device.deviceOSVersion -eq "9.1"</pre> <pre>device.deviceOSVersion -startsWith "10.0.1"</pre>
deviceOwnership ¹	Personal, Company, Unknown	<pre>device.deviceOwnership -eq "Company"</pre>
devicePhysicalIds	Any string value that Windows Autopilot uses, such as all Windows Autopilot devices, OrderID, or PurchaseOrderID	<pre>device.devicePhysicalIDs -any _ -startsWith "[ZTDId]"</pre> <pre>device.devicePhysicalIDs -any _ -eq "[OrderID]:179887111881"</pre> <pre>device.devicePhysicalIDs -any _ -eq "[PurchaseOrderId]:76222342342"</pre>
deviceTrustType ²	AzureAD, ServerAD, Workplace	<pre>device.deviceTrustType -eq "AzureAD"</pre>
enrollmentProfileName	Profile name for Apple Automated Device Enrollment, Android Enterprise corporate-owned dedicated device enrollment, or Windows Autopilot	<pre>device.enrollmentProfileName -eq "DEP iPhones"</pre>

Device attribute	Values	Examples
extensionAttribute1 ³	Any string value	device.extensionAttribute1 -eq "some string value"
extensionAttribute2	Any string value	device.extensionAttribute2 -eq "some string value"
extensionAttribute3	Any string value	device.extensionAttribute3 -eq "some string value"
extensionAttribute4	Any string value	device.extensionAttribute4 -eq "some string value"
extensionAttribute5	Any string value	device.extensionAttribute5 -eq "some string value"
extensionAttribute6	Any string value	device.extensionAttribute6 -eq "some string value"
extensionAttribute7	Any string value	device.extensionAttribute7 -eq "some string value"
extensionAttribute8	Any string value	device.extensionAttribute8 -eq "some string value"
extensionAttribute9	Any string value	device.extensionAttribute9 -eq "some string value"
extensionAttribute10	Any string value	device.extensionAttribute10 -eq "some string value"
extensionAttribute11	Any string value	device.extensionAttribute11 -eq "some string value"
extensionAttribute12	Any string value	device.extensionAttribute12 -eq "some string value"
extensionAttribute13	Any string value	device.extensionAttribute13 -eq "some string value"
extensionAttribute14	Any string value	device.extensionAttribute14 -eq "some string value"
extensionAttribute15	Any string value	device.extensionAttribute15 -eq "some string value"
isRooted	true , false	device.isRooted -eq true
managementType	Mobile device management (for mobile devices)	device.managementType -eq "MDM"

Device attribute	Values	Examples
<code>memberOf</code>	Any string value (valid group object ID)	<code>device.memberOf -any (group.objectId -in ['value'])</code>
<code>objectId</code>	A valid Microsoft Entra object ID	<code>device.objectId -eq "aaaaaaaa-0000-1111-2222-bbbbbbbbbbbb"</code>
<code>profileType</code>	A valid profile type in Microsoft Entra ID	<code>device.profileType -eq "RegisteredDevice"</code>
<code>systemLabels</code> ⁴	A read-only string that matches the Intune device property for tagging Modern Workplace devices	<code>device.systemLabels -startsWith "M365Managed" SystemLabels</code>

¹ When you use `deviceOwnership` to create dynamic membership groups for devices, you need to set the value equal to `Company`. On Intune, the device ownership is represented instead as `Corporate`. For more information, see [ownerTypes](#).

² When you use `deviceTrustType` to create dynamic membership groups for devices, you need to set the value equal to `AzureAD` to represent Microsoft Entra joined devices, `ServerAD` to represent Microsoft Entra hybrid joined devices, or `Workplace` to represent Microsoft Entra registered devices.

³ When you use `extensionAttribute1-15` to create dynamic membership groups for devices, you need to set the value for `extensionAttribute1-15` on the device. [Learn more about how to write extensionAttributes on a Microsoft Entra device object](#).

⁴ When you use `systemLabels`, a read-only attribute that's used in various contexts (such as device management and sensitivity labeling) is not editable through Intune.

Related content

- [Create a group with members and view all groups and members](#)
- [Manage Microsoft Entra groups and group membership](#)
- [Create or update a dynamic membership group in Microsoft Entra ID](#)

Validate rules for dynamic membership groups in Microsoft Entra ID

Article • 04/30/2025

Microsoft Entra ID provides the means to validate rules for dynamic membership groups. On the **Validate rules** tab, you can validate a rule against sample group members to confirm that the rule is working as expected.

When you create or update rules for dynamic membership groups, you want to know whether a user or a device is a member of the group. This knowledge helps you evaluate whether a user or device meets the rule criteria. It also helps you troubleshoot when membership isn't expected.

Prerequisites

To evaluate the rule for dynamic membership groups, the administrator must be at least a [Groups Administrator](#).

Tip

Assigning one of the required roles via indirect dynamic membership groups is not supported.

Validate a rule for dynamic membership groups

1. Sign in to the [Microsoft Entra admin center](#) as at least a Groups Administrator.
2. Browse to Entra ID > Groups > All groups.
3. Select an existing dynamic group or create a new dynamic group, and then select **Dynamic membership rules**.

The screenshot shows the Microsoft Entra admin center interface. On the left, the navigation menu is expanded, with 'Groups' selected. Under 'Groups', 'All groups' is highlighted with a red box. In the main content area, the title is '0123Group - Dynamic membership rules'. The 'Configure Rules' tab is active. The 'Rule syntax' section contains the expression '(user.city -eq "Seattle")'. Below it, a note says 'Add users to validate against this rule.' with a 'Learn more' link. There are two buttons: '+ Add users' (highlighted with a red box) and 'Validate'. A table below shows validation results for one user: 'Name' (No users added yet for validation), 'Status' (In group, indicated by a green checkmark icon).

4. On the **Validate Rules** tab, select users to validate their memberships. You can select 20 users or devices at one time.

This screenshot is identical to the previous one, but the 'Validate Rules (Preview)' tab is now highlighted with a red box. The rest of the interface remains the same, showing the dynamic membership rule configuration and validation status.

5. After you finish selecting users or devices, choose **Select**. Validation automatically starts. The validation results show whether a user is a member of the group or not.

Rule syntax

```
(user.city -eq "Seattle")
```

Add users to validate against this rule. [Learn more](#)

+ Add users [Validate](#)

Name	Status
JW James Wang aad292.ccscpt.net	✓ In group ✓ View details
JW James Wong 0c564b79-19d4-41ba-814c-105405134acf@aad292.ccscpt.net	✗ Not in group ✗ View details
JA Jamesw jamesw@aad292.ccscpt.net	? Unknown ? View details

6. If the rule isn't valid or if there's a network problem, the results show **Unknown**. If the value is **Unknown**, select **View details**. The detailed error message describes the problem and the necessary actions.

Verification details

User James Wang

Status

- ✗ (user.city -eq "Seattle") and (user.department -eq "Engineering")
- and
 - ✓ user.city -eq "Seattle"
 - ✗ user.department -eq "Engineering"

Add users to validate a

+ Add users [Val](#)

Name
JW James Wang aad292.ccscpt.net
JW James Wong 0c564b79-19d4-41ba-814c-105405134acf@aad292.ccscpt.net

7. You can modify the rule to trigger a new validation of memberships. To see why a user isn't a member of the group, select **View details**. Verification details show the result of each expression that composes the rule. Select **OK** to close the details.

Related content

- [Manage rules for dynamic membership groups in Microsoft Entra ID](#)

Create simpler, more efficient rules for dynamic membership groups in Microsoft Entra ID

Article • 04/30/2025

This article discusses the most common methods that you can use to simplify your rules for dynamic membership groups. Rules that are simpler and more efficient result in better processing times for dynamic groups.

When you're writing membership rules for dynamic membership groups, follow the tips in this article to ensure that you create these rules as efficiently as possible.

Minimize use of the -match operator

Minimize your use of the `-match` operator in rules as much as possible. Instead, explore if it's possible to use the `-startswith` or `-eq` operator. Consider using other properties that allow you to write rules to select the users for a group without using the `-match` operator.

For example, if you want a rule for the group that contains all users whose city is Lagos, don't use a rule like these:

- `user.city -match "ago"`
- `user.city -match ".*?ago.*"`

It's better to use a rule like this example:

- `user.city -startswith "Lag"`

Or, best of all:

- `user.city -eq "Lagos"`

Minimize use of the -contains operator

As with `-match`, minimize your use of the `-contains` operator in rules as much as possible. Instead, explore if it's possible to use the `-startswith` or `-eq` operator. Using `-contains` can increase processing times, especially for tenants that have many dynamic membership groups.

Use fewer -or operators

Identify when your rule uses various values for the same property, linked together with `-or` operators. Instead, use the `-in` operator to group them into a single criterion. A single criterion makes the rule easier to evaluate.

For example, don't use a rule like this one:

```
(user.department -eq "Accounts" -and user.city -eq "Lagos") -or  
(user.department -eq "Accounts" -and user.city -eq "Ibadan") -or  
(user.department -eq "Accounts" -and user.city -eq "Kaduna") -or  
(user.department -eq "Accounts" -and user.city -eq "Abuja") -or  
(user.department -eq "Accounts" -and user.city -eq "Port Harcourt")
```

It's better to use a rule like this example:

- `user.department -eq "Accounts" -and user.city -in ["Lagos", "Ibadan", "Kaduna", "Abuja", "Port Harcourt"]`

Conversely, identify similar subcriteria with the same property not equal to various values that are linked with `-and` operators. Then use the `-notin` operator to group them into a single criterion to make the rule easier to understand and evaluate.

For example, don't use a rule like this one:

- `(user.city -ne "Lagos") -and (user.city -ne "Ibadan") -and (user.city -ne "Kaduna") -and (user.city -ne "Abuja") -and (user.city -ne "Port Harcourt")`

It's better to use a rule like this example:

- `user.city -notin ["Lagos", "Ibadan", "Kaduna", "Abuja", "Port Harcourt"]`

Avoid redundant criteria

Ensure that you aren't using redundant criteria in your rule. For example, don't use a rule like this one:

- `user.city -eq "Lagos" or user.city -startswith "Lag"`

It's better to use a rule like this example:

- `user.city -startswith "Lag"`

Related content

- Manage rules for dynamic membership groups in Microsoft Entra ID

Change static groups to dynamic membership groups in Microsoft Entra ID

Article • 04/30/2025

You can change a group's membership from static to dynamic (or vice versa) in Microsoft Entra ID. Microsoft Entra ID keeps the same group name and ID in the system, so all existing references to the group are still valid. If you create a new group instead, you need to update those references.

Creating dynamic membership groups eliminates the management overhead of adding and removing users. This article shows you how to convert existing membership groups from static to dynamic, by using either the Azure portal or PowerShell cmdlets. In Microsoft Entra, a single tenant can have a maximum of 15,000 dynamic membership groups.

⚠ Warning

When you change an existing static group to a dynamic group, all existing members are removed from the group. The membership rule is then 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 [Resolve group license problems](#).

Prerequisites

- To change the membership type by using the portal, you need an account that has at least the [Groups Administrator](#) role.
- To change dynamic group properties by using PowerShell, you need to use cmdlets from the Microsoft Graph PowerShell module. For more information, see [Install the Microsoft Graph PowerShell SDK](#).

Change the membership type for a group (portal)

1. Sign in to the [Microsoft Entra admin center](#) as at least a Groups Administrator.
2. Select **Microsoft Entra ID**.

3. Select Groups.

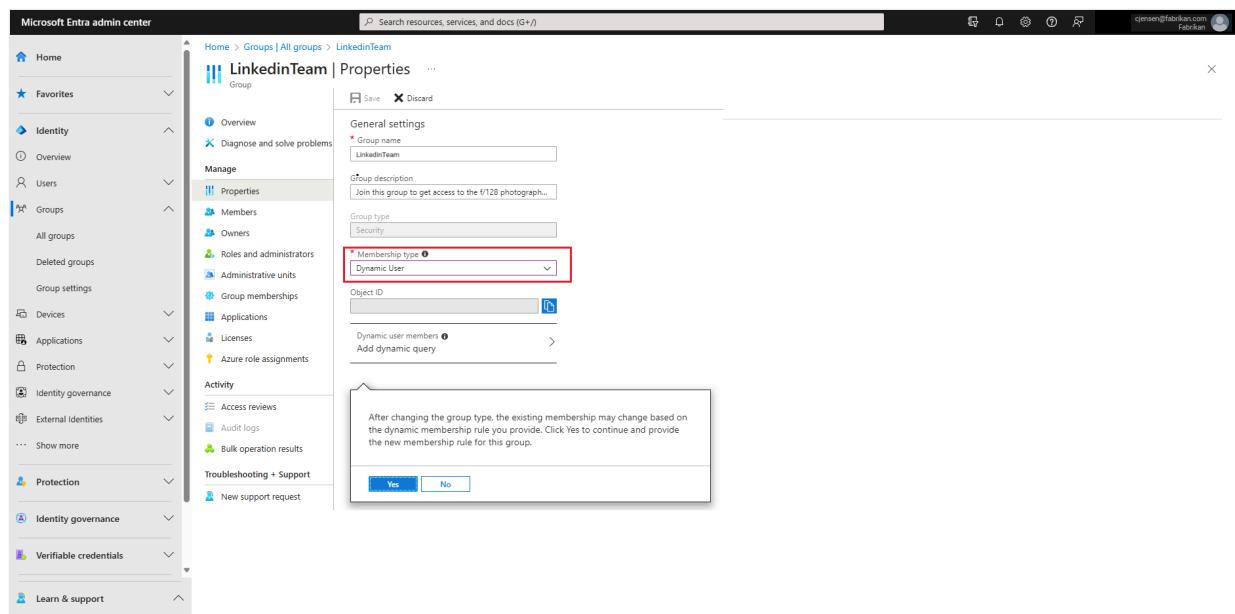
4. In the **All groups** list, open the group that you want to change.

5. Select Properties.

6. On the **Properties** page for the group, select a **Membership type** value of **Assigned (static)**, **Dynamic User**, or **Dynamic Device**, depending on your desired membership type. For dynamic membership groups, you can use the rule builder to select options for a simple rule or write a membership rule yourself.

The following steps are an example of changing a group of users from static to dynamic membership groups:

- a. For **Membership type**, select **Dynamic User**. In the dialog that explains the changes to the dynamic membership groups, select **Yes** to continue.



- b. Select **Add dynamic query**, and then provide the rule.

Dynamic membership rules



Add dynamic membership rule

[Simple rule](#) [Advanced rule](#)

Add users where

extension_8d346f30f8634e6ebc5680a95e69e0df_employeeID

Starts With

7. After you create the rule, select **Add query**.

8. On the **Properties** page for the group, select **Save** to save your changes. The **Membership type** of the group is immediately updated in the group list.

💡 Tip

Group conversion might fail if the membership rule that you entered was incorrect. In the upper-right corner of the portal, a notification explains why the rule can't be accepted. Read it carefully to understand how you can adjust the rule to make it valid. For examples of rule syntax and a complete list of the supported properties, operators, and values for a membership rule, see [Manage rules for dynamic membership groups in Microsoft Entra ID](#).

Change the membership type for a group (PowerShell)

Here's an example of functions that switch membership management on an existing group. This example correctly manipulates the `GroupTypes` property to preserve any values that are unrelated to dynamic membership groups.

PowerShell

```
#The moniker for dynamic membership groups, as used in the GroupTypes property of a group object
$dynamicGroupTypeString = "DynamicMembership"

function ConvertDynamicGroupToStatic
{
```

```

Param([string]$groupId)

#Existing group types
[System.Collections.ArrayList]$groupTypes = (Get-MgGroup -GroupId
$groupId).GroupTypes

if($groupTypes -eq $null -or !$groupTypes.Contains($dynamicGroupTypeString))
{
    throw "This group is already a static group. Aborting conversion.";
}

#Remove the type for dynamic membership groups, but keep the other type values
$groupTypes.Remove($dynamicGroupTypeString)

#Modify the group properties to make it a static group: change GroupTypes to
remove the dynamic type, and then pause execution of the current rule
Update-MgGroup -GroupId $groupId -GroupTypes $groupTypes.ToArray() -
MembershipRuleProcessingState "Paused"
}

function ConvertStaticGroupToDynamic
{
    Param([string]$groupId, [string]$dynamicMembershipRule)

    #Existing group types
    [System.Collections.ArrayList]$groupTypes = (Get-MgGroup -GroupId
$groupId).GroupTypes

    if($groupTypes -ne $null -and $groupTypes.Contains($dynamicGroupTypeString))
    {
        throw "This group is already a dynamic group. Aborting conversion.";
    }
    #Add the dynamic group type to existing types
    $groupTypes.Add($dynamicGroupTypeString)

    #Modify the group properties to make it a static group: change GroupTypes to
    add the dynamic type, start execution of the rule, and then set the rule
    Update-MgGroup -GroupId $groupId -GroupTypes $groupTypes.ToArray() -
    MembershipRuleProcessingState "On" -MembershipRule $dynamicMembershipRule
}

```

To make a group static, use this command:

PowerShell

```
ConvertDynamicGroupToStatic "a58913b2-eee4-44f9-beb2-e381c375058f"
```

To make a group dynamic, use this command:

PowerShell

```
ConvertStaticGroupToDynamic "a58913b2-eee4-44f9-beb2-e381c375058f"  
"user.displayName -startsWith ""Peter"""
```

Related content

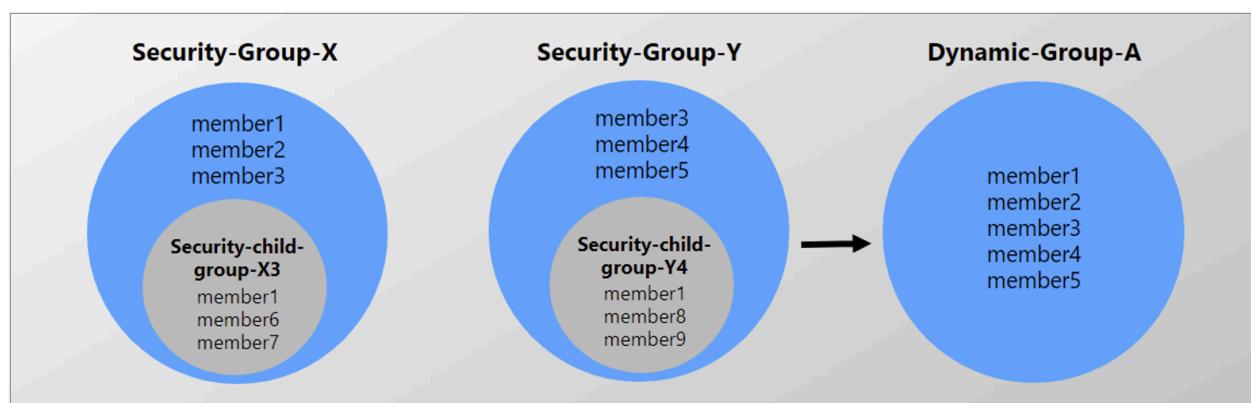
- [Create a group with members and view all groups and members](#)
- [Manage Microsoft Entra groups and group membership](#)
- [Manage rules for dynamic membership groups in Microsoft Entra ID](#)

Configure dynamic membership groups with the memberOf attribute in the Azure portal

Article • 12/30/2024

This feature preview in Microsoft Entra ID enables admins to create dynamic membership groups and administrative units that populate by adding members of other groups using the `memberOf` attribute. Apps that couldn't read group-based membership previously in Microsoft Entra ID can now read the entire membership of these new `memberOf` groups. Not only can these groups be used for apps but they can also be used for licensing assignments.

The following diagram illustrates how you could create Dynamic-Group-A with members of Security-Group-X and Security-Group-Y. Members of the groups inside Security-Group-X and Security-Group-Y don't become members of Dynamic-Group-A.



With this preview, admins can configure dynamic membership groups with the `memberOf` attribute in the Azure portal, Microsoft Graph, and PowerShell. Security groups, Microsoft 365 groups, and groups that are synced from on-premises Active Directory can all be added as members of these dynamic membership groups. They can also all be added to a single group. For example, the dynamic group could be a security group, but you can use Microsoft 365 groups, security groups, and groups that are synced from on-premises to define its membership.

Prerequisites

You must be at least a [User Administrator](#) to use the `memberOf` attribute to create a Microsoft Entra dynamic group. You must have a Microsoft Entra ID P1 or P2 license for the Microsoft Entra tenant.

Preview limitations

- Each Microsoft Entra tenant is limited to 500 dynamic membership groups using the `memberOf` attribute. The `memberOf` groups count toward the total dynamic group member quota of 15,000.
- Each dynamic group can have up to 50 member groups.
- When you add members of security groups to `memberOf` dynamic membership groups, only direct members of the security group become members of the dynamic group.
- You can't use one `memberOf` dynamic group to define the membership of another `memberOf` dynamic group. For example, Dynamic Group A, with members of group B and C in it, can't be a member of Dynamic Group D.
- The `memberOf` attribute can't be used with other rules. For example, a rule that states dynamic group A should contain members of group B and also should contain only users located in Redmond will fail.
- The dynamic group rule builder and validate feature can't be used for `memberOf` at this time.
- The `memberOf` attribute can't be used with other operators. For example, you can't create a rule that states "Members Of group A can't be in Dynamic group B."
- Users included in `memberOf` dynamic membership groups may cause a slower processing time for your tenant, if the tenant has a large number of groups or frequent dynamic membership groups updates.

Get started

This feature can be used in the Azure portal, Microsoft Graph, and PowerShell. Because `memberOf` isn't yet supported in the rule builder, you must enter your rule in the rule editor.

Create a memberOf dynamic group

1. Sign in to the [Microsoft Entra admin center](#) as at least a **User Administrator**.
2. Browse to **Identity > Groups > All groups**.
3. Select **New group**.
4. Fill in group details. The group type can be **Security** or **Microsoft 365**, and the membership type can be set to **Dynamic User** or **Dynamic Device**.
5. Select **Add dynamic query**.
6. MemberOf isn't yet supported in the rule builder. Select **Edit** to write the rule in the **Rule syntax** box.

- a. Example user rule: `user.memberof -any (group.objectId -in ['groupId', 'groupId'])`
 - b. Example device rule: `device.memberof -any (group.objectId -in ['groupId', 'groupId'])`
7. Select **OK**.
8. Select **Create group**.
-

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

Bulk add group members in Microsoft Entra ID

Article • 12/19/2024

You can add multiple members to a group by using a comma-separated values (CSV) file to bulk import group members in the portal for Microsoft Entra ID.

Understand the CSV template

Download and fill in the bulk upload CSV template to successfully add Microsoft Entra group members in bulk. Your CSV template might look like this example:

A		B
1	version:v1.0	
2	Member object ID or user principal name [memberObjectIdOrUpn] Required	
3	Example: 9832aad8-e4fe-496b-a604-95c6eF01ae75	
4		

Row 1 must be preserved as-is, and the version number is always required.

Preserve the column headings as-is in row 2. Column headings indicate acceptable values and whether they're required. Don't add additional columns.

Use the entries in row 3 as examples. Remove the row's contents and replace the examples with your entries. When two values are possible, enter only one.

CSV template structure

The rows in a downloaded CSV template are:

- Version number:** The first row that contains the version number must be included in the upload CSV.
- Column headings:** The format of the column headings is `<Item name> [PropertyName] <Required or blank>`. An example is `Member object ID or user principal name [memberObjectIdOrUpn] Required`. Some older versions of the template might have slight variations. For group membership changes, you can choose the member object ID or the user principal name.
- Examples row:** The template includes a row of examples of acceptable values for each column. You must remove the examples row and replace it with your own entries.

More guidance

- The first two rows of the upload template must not be removed or modified or the upload can't be processed.
- The required columns are listed first.
- We don't recommend adding new columns to the template. Any other columns you add are ignored and not processed.
- We recommend that you download the latest version of the CSV template as often as possible.
- Add at least two users' UPNs or object IDs to successfully upload the file.

Bulk import group members

💡 Tip

Steps in this article might vary slightly based on the portal you start from.

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Groups Administrator](#).
 2. Select **Microsoft Entra ID**.
- ### ⓘ Note
- Group owners can also bulk import members of groups they own.
3. Select **Groups > All groups**.
 4. Open the group to which you're adding members and then select **Members**.
 5. On the **Members** page, select **bulk operations** and then choose **Import members**.
 6. On the **Bulk import group members** page, select **Download** to get the CSV file template with required group member properties.

7. Open the CSV file and add a line for each group member you want to import into the group. Required values are either **Member object ID** or **User principal name**. Then save the file.

	A	B
1	version:v1.0	
2	Member object ID or user principal name [memberObjectIdOrUpn] Required	
3	Example:	
4		

8. On the **Bulk import group members** page, under **Upload your csv file**, browse to the file. When you select the file, validation of the CSV file starts.
9. When the file contents are validated, the bulk import page displays **File uploaded successfully**. If there are errors, you must fix them before you can submit the job.
10. When your file passes validation, select **Submit** to start the bulk operation that imports the group members to the group.
11. When the import operation finishes, a notification states that the bulk operation succeeded.

If you experience errors, you can download and view the results file on the **Bulk operation results** page. The file contains the reason for each error. The file submission must match the provided template and include the exact column names. For more information about bulk operations limitations, see [Bulk import service limits](#).

Check import status

You can see the status of all your pending bulk requests on the **Bulk operation results** page.

The screenshot shows the Microsoft Entra ID for workforce interface. On the left, there's a sidebar with various links: All users, Deleted users, Password reset, User settings, Diagnose and solve problems, Activity (Sign-ins, Audit logs), Bulk operation results (which is selected and highlighted with a red box), Troubleshooting + Support, and New support request. The main content area has a search bar at the top with 'File name' and 'Type' dropdowns set to 'All'. Below is a table titled 'Bulk operation results' with the following columns: File name, Upload time, Completion time, Status, # Success, # Failure, Total requests, and Admin uploaded. There is one entry: 'No results'.

For details about each line item within the bulk operation, select the values under the **# Success**, **# Failure**, or **Total Requests** columns. If failures occurred, the reasons for failure are listed.

Bulk import service limits

ⓘ Note

When performing bulk operations, such as import or create, you may encounter a problem if the bulk operation does not 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. For more information, see [Bulk operations service limitations](#).

Next steps

- [Bulk remove group members](#)
- [Download members of a group](#)
- [Download a list of all groups](#)

Feedback

Was this page helpful?

Yes

No

[Provide product feedback ↗](#)

Bulk remove group members in Microsoft Entra ID

Article • 01/29/2025

You can remove a large number of members from a group by using a comma-separated values (CSV) file to remove group members in bulk using the portal for Microsoft Entra ID.

Understand the CSV template

Download and fill in the bulk upload CSV template to successfully add Microsoft Entra group members in bulk. Your CSV template might look like this example:

Preserve the column headings as-is in row 2. Column headings indicate acceptable values and whether they're required. Don't add additional columns.	<table border="1"><thead><tr><th>A</th><th>B</th></tr></thead><tbody><tr><td>1</td><td>version:v1.0</td></tr><tr><td>2</td><td>Member object ID or user principal name [memberObjectIdOrUpn] Required</td></tr><tr><td>3</td><td>Example: 9832aad8-e4fe-496b-a604-95c6eF01ae75</td></tr><tr><td>4</td><td></td></tr></tbody></table>	A	B	1	version:v1.0	2	Member object ID or user principal name [memberObjectIdOrUpn] Required	3	Example: 9832aad8-e4fe-496b-a604-95c6eF01ae75	4		Row 1 must be preserved as-is, and the version number is always required.
A	B											
1	version:v1.0											
2	Member object ID or user principal name [memberObjectIdOrUpn] Required											
3	Example: 9832aad8-e4fe-496b-a604-95c6eF01ae75											
4												
		Use the entries in row 3 as examples. Remove the row's contents and replace the examples with your entries. Enter only one value per row.										

CSV template structure

The rows in a downloaded CSV template are:

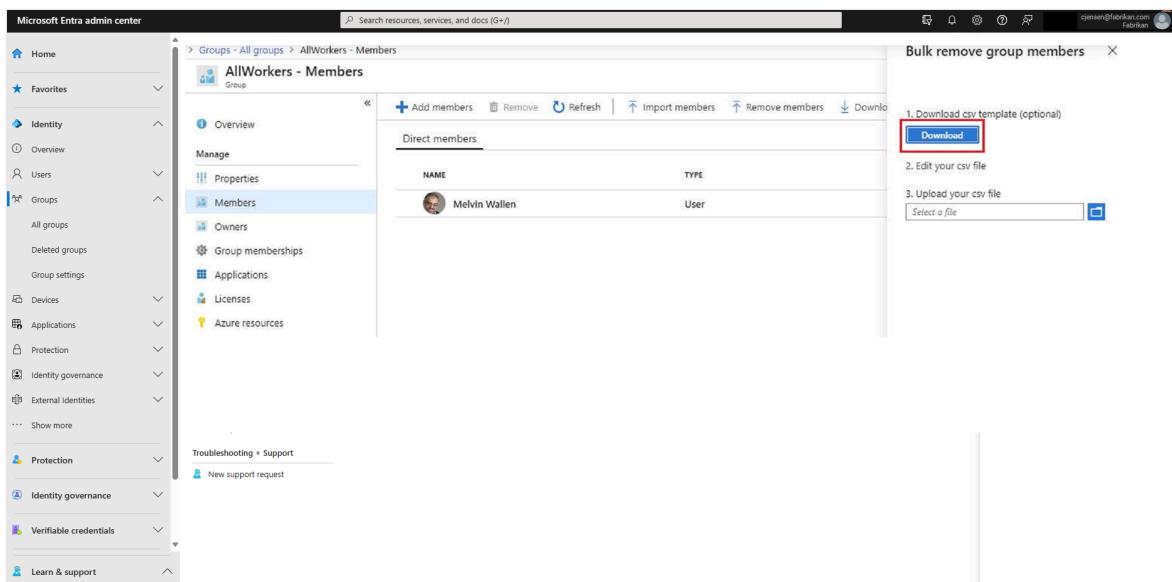
- **Version number:** The first row that contains the version number must be included in the upload CSV.
- **Column headings:** The format of the column headings is `<Item name> [PropertyName] <Required or blank>`. An example is `Member object ID or user principal name [memberObjectIdOrUpn] Required`. Some older versions of the template might have slight variations. For group membership changes, you can choose the member object ID or the user principal name.
- **Examples row:** The template includes a row of examples of acceptable values for each column. You must remove the examples row and replace it with your own entries.

More guidance

- The first two rows of the upload template must not be removed or modified or the upload can't be processed.
- The required columns are listed first.
- We don't recommend adding new columns to the template. Any other columns you add are ignored and not processed.
- We recommend that you download the latest version of the CSV template as often as possible.

Bulk remove group members

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Groups Administrator**.
2. Select **Identity**.
3. Select **Groups > All groups**.
4. Open the group from which you're removing members and then select **Members**.
5. On the **Members** page, select **Remove members**.
6. On the **Bulk remove group members** page, select **Download** to get the CSV file template with required group member properties.



7. Open the CSV file and add a line for each group member you want to remove from the group. Required values are **Member object ID** or **User principal name**. Then save the file.

A	B
1	version:v1.0
2	Member object ID or user principal name [memberObjectIdOrUpn] Required
3	Example:
4	

8. On the **Bulk remove group members** page, under **Upload your csv file**, browse to the file. When you select the file, validation of the CSV file starts.
9. When the file contents are validated, the bulk import page displays **File uploaded successfully**. If there are errors, you must fix them before you can submit the job.
10. When your file passes validation, select **Submit** to start the bulk operation that removes the group members from the group.
11. When the removal operation finishes, a notification states that the bulk operation succeeded.

If you experience errors, you can download and view the results file on the **Bulk operation results** page. The file contains the reason for each error. The file submission must match the provided template and include the exact column names. For more information about bulk operations limitations, see [Bulk removal service limits](#).

Check removal status

You can see the status of all your pending bulk requests on the **Bulk operation results** page.

File name	Type	Upload time	Completion time	Status	# Success	# Failure	Total requests	Admin uploaded
No results								

For details about each line item within the bulk operation, select the values under the **# Success**, **# Failure**, or **Total Requests** columns. If failures occurred, the reasons for failure are listed.

Bulk removal service limits

Note

When performing bulk operations, such as import or create, you can 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 limit the data returned by the bulk operation. For more information, see [Bulk operations service limitations](#).

Next steps

- [Bulk import group members](#)
 - [Download members of a group](#)
 - [Download a list of all groups](#)
-

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#) 

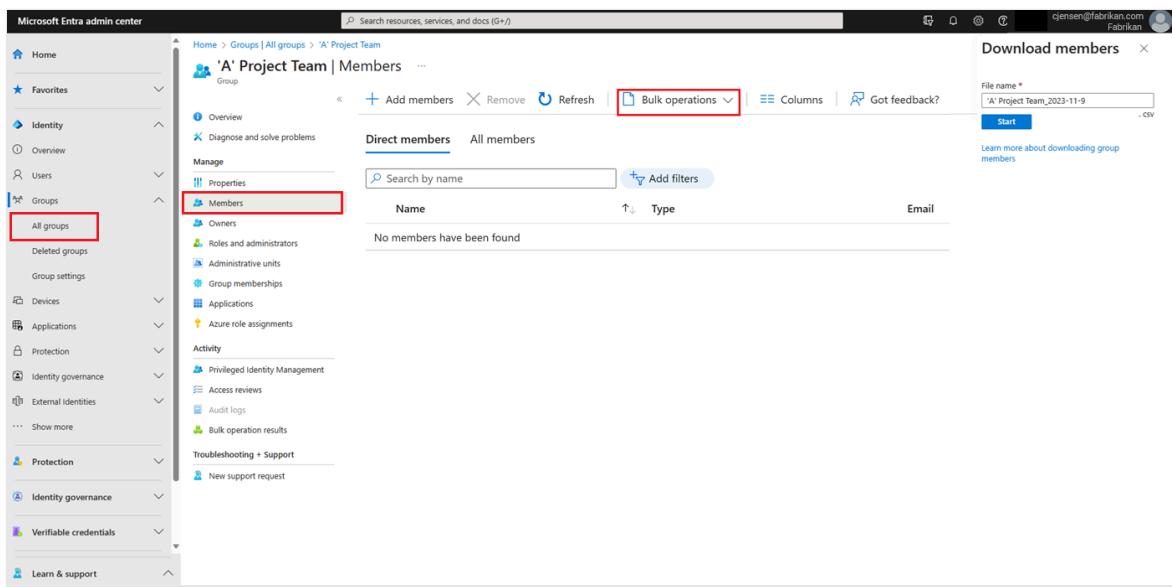
Bulk download members of a group in Microsoft Entra ID

Article • 12/19/2024

You can bulk download the members of a group in your organization to a comma-separated values (CSV) file from the Microsoft Entra admin center. All admins and nonadmin users can download group membership lists.

Bulk download group membership

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Groups Administrator**.
2. Select **Microsoft Entra ID**.
3. Select **Groups > All groups**.
4. Open the group whose membership you want to download, and then select **Members**.
5. On the **Members** page, select **Bulk operations** and choose **Download members** to download a CSV file that lists the group members.



The screenshot shows the Microsoft Entra admin center interface. In the left sidebar, under the 'Groups' section, the 'All groups' link is highlighted with a red box. The main content area shows the 'Members' page for a group named "'A' Project Team'. The 'Bulk operations' dropdown menu is open, and the 'Download members' option is selected. A red box highlights the 'Bulk operations' button. The right side of the screen shows a 'Download members' dialog box with a 'File name' field containing 'A' Project Team_2023-11-9' and a 'Start' button.

If you experience errors, you can download and view the results file on the **Bulk operation results** page. The file contains the reason for each error. The file submission must match the provided template and include the exact column names. For more information about bulk operations limitations, see [Bulk download service limits](#).

Check download status

You can see the status of all of your pending bulk requests on the **Bulk operation results** page.

File name	Type	Upload time	Completion time	Status	# Success	# Failure	Total requests	Admin uplo
No results								

Bulk download service limits

ⓘ Note

When performing bulk operations, such as import or create, you may encounter a problem if the bulk operation does not 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. For more information, see [Bulk operations service limitations](#).

Next steps

- [Bulk import group members](#)
- [Bulk remove group members](#)

Feedback

Was this page helpful?

Yes

No

[Provide product feedback ↗](#)

Bulk download a list of groups in Microsoft Entra ID

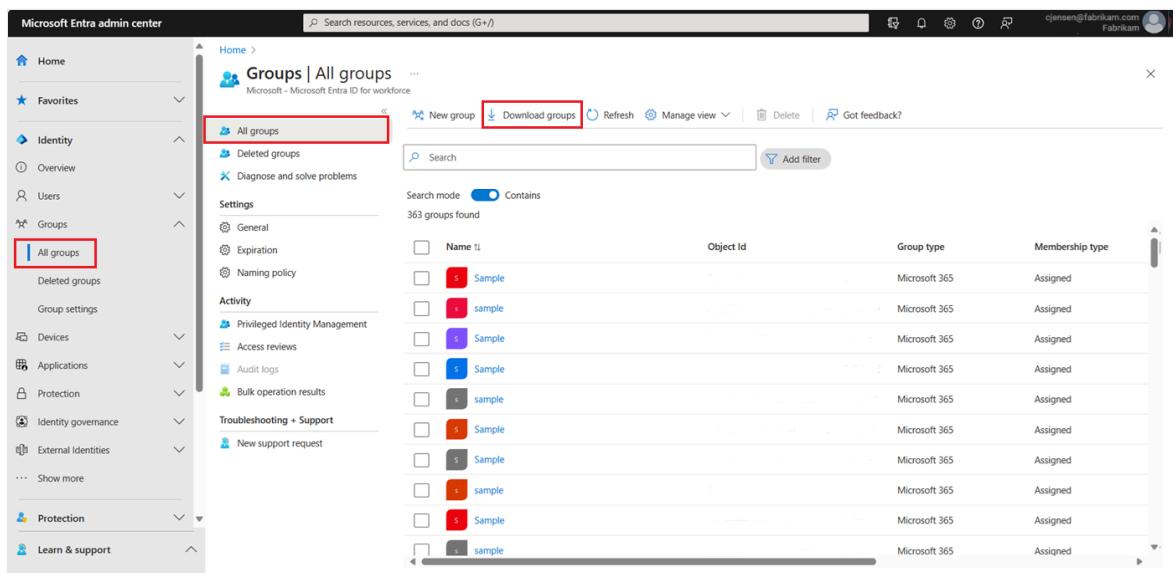
Article • 01/29/2025

You can download a list of all the groups in your organization to a comma-separated values (CSV) file in the portal for Microsoft Entra ID. All admins and nonadmin users can download group lists.

Download a list of groups

The columns downloaded are predefined.

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



The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with sections like Home, Favorites, Identity (with 'All groups' selected), Users, Groups (with 'All groups' selected), Devices, Applications, Protection, Identity governance, External identities, and more. The main content area is titled 'Groups | All groups' and shows a list of 363 groups. At the top of this list, there are buttons for 'New group' and 'Download groups'. The 'Download groups' button is highlighted with a red box. The list includes columns for Name, Object Id, Group type, and Membership type. Each group entry has a small colored square icon next to its name.

Name	Object Id	Group type	Membership type
Sample		Microsoft 365	Assigned
sample		Microsoft 365	Assigned
Sample		Microsoft 365	Assigned
Sample		Microsoft 365	Assigned
sample		Microsoft 365	Assigned
Sample		Microsoft 365	Assigned
sample		Microsoft 365	Assigned
Sample		Microsoft 365	Assigned
sample		Microsoft 365	Assigned
Sample		Microsoft 365	Assigned
sample		Microsoft 365	Assigned

4. On the **Groups download** page, select **Start** to receive a CSV file that lists your groups.

The screenshot shows the 'Groups - All groups' page in the Microsoft Groups interface. On the left, there's a sidebar with options like 'All groups', 'Deleted groups', 'Settings' (General, Expiration, Naming policy), 'Activity' (Access reviews, Audit logs, Bulk operation results), and 'Troubleshooting + Support' (Troubleshoot, New support request). The main area lists '363 groups found' with columns for Name, Object Id, and Group type (all listed as Microsoft 365). At the top right, there's a 'Download groups' button (highlighted with a red box) and a 'Groups download' dialog box. The dialog has a 'File name' field containing 'exportGroup_2019-5-13' and a 'Start' button.

If you experience errors, you can download and view the results file on the **Bulk operation results** page. The file contains the reason for each error. The file submission must match the provided template and include the exact column names. For more information about bulk operations limitations, see [Bulk download service limits](#).

Check download status

You can see the status of all your pending bulk requests on the **Bulk operation results** page.

The screenshot shows the 'Users | Bulk operation results' page. The sidebar includes 'All users', 'Deleted users', 'Password reset', 'User settings', 'Diagnose and solve problems', 'Activity' (Sign-ins, Audit logs), and 'Bulk operation results' (highlighted with a red box). The main area displays a table with columns: File name, Type (dropdown set to 'All'), Upload time, Completion time, Status, # Success, # Failure, Total requests, and Admin uploaded. The table currently shows 'No results'. A search icon is located in the bottom right corner of the main area.

Bulk download service limits

! Note

When performing bulk operations, such as import or create, you can 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 limit the data returned by the bulk operation. For more information, see [Bulk operations service limitations](#).

Next steps

- [Bulk remove group members](#)
 - [Download members of a group](#)
-

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Restore a deleted Microsoft 365 group in Microsoft Entra ID

Article • 01/15/2025

When you delete a Microsoft 365 group in Microsoft Entra ID, the deleted group is retained but not visible for 30 days from the deletion date. This behavior is so that the group and its contents can be restored if needed. This functionality is restricted exclusively to Microsoft 365 groups in Microsoft Entra ID. It isn't available for security groups and distribution groups. The 30-day group restoration period isn't customizable.

Permissions that are required to restore a group are listed in the following table.

 Expand table

Role	Permissions
Global Administrator, Group Administrator, Partner Tier 2 Support, and Intune Administrator	Can restore any deleted Microsoft 365 group
User Administrator and Partner Tier 1 Support	Can restore any deleted Microsoft 365 group except those groups assigned to the Global Administrator role
User	Can restore any deleted Microsoft 365 group that they own

View and manage the deleted Microsoft 365 groups that are available to restore

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Groups Administrator](#).
2. Select Microsoft Entra ID.
3. Select **Groups > All groups** and then select **Deleted groups** to view the deleted groups that are available to restore.

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with various sections like Home, Favorites, Identity, Users, Groups, Devices, Applications, Protection, Identity governance, External identities, and more. Under the Groups section, 'Deleted groups' is highlighted with a red box. The main content area is titled 'Groups | Deleted groups' and shows a list of deleted groups. It includes a 'Search groups' bar, a note about permanent deletion after 30 days, and a table with columns for NAME, MEMBERSHIP TYPE, DELETION DATE, and PERMANENT DELETION DATE. Three groups are listed: Project Firecracker, Project Management, and Engineering Team, all marked as Assigned.

NAME	MEMBERSHIP TYPE	DELETION DATE	PERMANENT DELETION DATE
Project Firecracker	Assigned	2/14/2019, 4:45:25 PM	3/16/2019, 5:45:25 PM
Project Management	Assigned	2/14/2019, 4:45:29 PM	3/16/2019, 5:45:29 PM
Engineering Team	Assigned	2/14/2019, 4:45:39 PM	3/16/2019, 5:45:39 PM

4. On the Deleted groups pane, you can:

- Restore the deleted group and its contents by selecting **Restore group**.
- Permanently remove the deleted group by selecting **Delete permanently**. To permanently remove a group, you must be an administrator.

View the deleted Microsoft 365 groups that are available to restore by using PowerShell

Use the following cmdlets to view the deleted groups. You need to verify that the groups you're interested in weren't permanently purged. These cmdlets are part of the [Microsoft Graph PowerShell module](#). For more information about this module, see [Microsoft Graph PowerShell overview](#).

Run the following cmdlet to display all deleted Microsoft 365 groups in your Microsoft Entra organization that are still available to restore. Install the [Graph](#) beta version if it isn't already installed on the machine.

PowerShell

```
Install-Module Microsoft.Graph.Beta
Connect-MgGraph -Scopes "Group.ReadWrite.All"
Get-MgBetaDirectoryDeletedGroup
```

Alternatively, if you know the object ID of a specific group (and you can get it from the cmdlet in step 1), run the following cmdlet. You need to verify that the specific deleted group wasn't permanently purged.

PowerShell

```
Get-MgBetaDirectoryDeletedGroup -DirectoryObjectId <objectId>
```

Restore your deleted Microsoft 365 group

After you verify that the group is still available to restore, restore the deleted group with one of the following steps. If the group contains documents, SharePoint sites, or other persistent objects, it might take up to 24 hours to fully restore a group and its contents.

Run the following cmdlet to restore the group and its contents.

PowerShell

```
Restore-MgBetaDirectoryDeletedItem -DirectoryObjectId <objectId>
```

Alternatively, you can run the following cmdlet to permanently remove the deleted group.

PowerShell

```
Remove-MgBetaDirectoryDeletedItem -DirectoryObjectId <objectId>
```

How do you know restoration worked?

To verify that you successfully restored a Microsoft 365 group, run the `Get-MgBetaGroup -GroupId <objectId>` cmdlet to display information about the group. After the restore request is completed:

- The group appears in the left navigation pane on Exchange.
- The plan for the group appears in Planner.
- Any SharePoint sites and all their contents are available.
- You can access the group from any of the Exchange endpoints and other Microsoft 365 workloads that support Microsoft 365 groups.

Next steps

For more information on Microsoft Entra groups:

- [See existing groups](#)
- [Manage settings of a group](#)
- [Manage members of a group](#)

- Manage memberships of a group
 - Manage rules for dynamic membership groups
-

Feedback

Was this page helpful?

 Yes

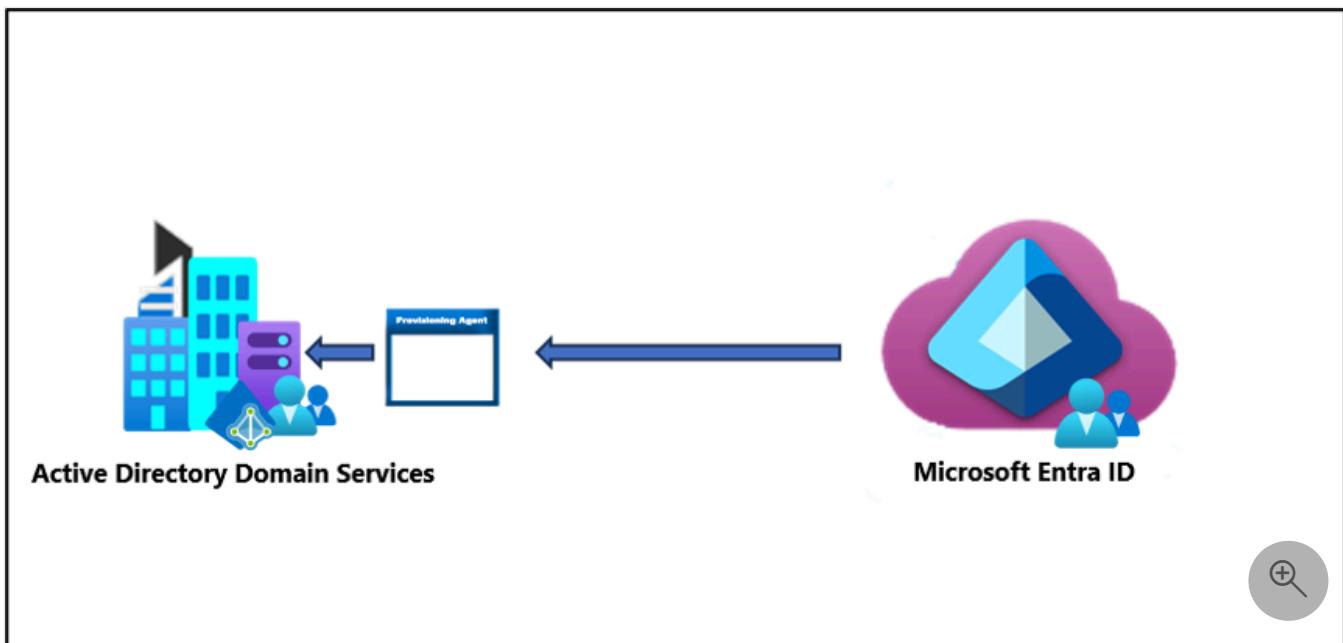
 No

Provide product feedback ↗

Group writeback with Microsoft Entra Cloud Sync

Article • 04/09/2025

With the release of provisioning agent [1.1.1370.0](#), cloud sync now has the ability to perform group writeback. This feature means that cloud sync can provision groups directly to your on-premises Active Directory environment. You can also now use identity governance features to govern access to AD-based applications, such as by including a [group in an entitlement management access package](#).



i Important

The public preview of Group Writeback v2 in Microsoft Entra Connect Sync is no longer available as of **June 30, 2024**. This feature was discontinued on this date, and you're no longer supported in Microsoft Entra Connect Sync to provision cloud security groups to Active Directory. The feature continues to operate beyond the discontinuation date; however, it no longer receives support and might cease functioning at any time without notice.

We offer similar functionality in Microsoft Entra Cloud Sync called [Group Provision to Active Directory](#) that you can use instead of Group Writeback v2 for provisioning cloud security groups to Active Directory. We're working on enhancing this functionality in Microsoft Entra Cloud Sync along with other new features that we're developing in Microsoft Entra Cloud Sync.

Customers who use this preview feature in Microsoft Entra Connect Sync should [switch their configuration from Microsoft Entra Connect Sync to Microsoft Entra Cloud Sync](#).

You can choose to move all your hybrid sync to Microsoft Entra Cloud Sync (if it supports your needs). You can also run Microsoft Entra Cloud Sync side by side and move only cloud security group provisioning to Active Directory onto Microsoft Entra Cloud Sync.

For customers who provision Microsoft 365 groups to Active Directory, you can keep using Group Writeback v1 for this capability.

You can evaluate moving exclusively to Microsoft Entra Cloud Sync by using the [user synchronization wizard](#).

Provision Microsoft Entra ID to Active Directory - Prerequisites

The following prerequisites are required to implement provisioning groups to Active Directory.

License requirements

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](#).

General requirements

- Microsoft Entra account with at least a [Hybrid Identity Administrator](#) role.
- On-premises Active Directory Domain Services environment with Windows Server 2016 operating system or later.
 - Required for AD Schema attribute - msDS-ExternalDirectoryObjectId
- Provisioning agent with build version [1.1.1370.0](#) or later.

! Note

The permissions to the service account are assigned during clean install only. In case you're upgrading from the previous version then permissions need to be assigned manually using PowerShell cmdlet:

```
$credential = Get-Credential  
  
Set-AADCloudSyncPermissions -PermissionType UserGroupCreateDelete -  
TargetDomain "FQDN of domain" -EACredential $credential
```

If the permissions are set manually, you need to ensure that Read, Write, Create, and Delete all properties for all descendent Groups and User objects.

These permissions aren't applied to AdminSDHolder objects by default [Microsoft Entra provisioning agent gMSA PowerShell cmdlets](#)

- The provisioning agent must be able to communicate with one or more domain controllers on ports TCP/389 (LDAP) and TCP/3268 (Global Catalog).
 - Required for global catalog lookup to filter out invalid membership references
- Microsoft Entra Connect Sync with build version [2.2.8.0](#) or later
 - Required to support on-premises user membership synchronized using Microsoft Entra Connect Sync
 - Required to synchronize AD:user:objectGUID to AAD:user:onPremisesObjectIdentifier

Supported groups and scale limits

The following is supported:

- Only cloud created [Security groups](#) are supported
- These groups can have assigned or dynamic membership groups.
- These groups can only contain on-premises synchronized users and / or additional cloud created security groups.
- The on-premises user accounts that are synchronized and are members of this cloud created security group, can be from the same domain or cross-domain, but they all must be from the same forest.
- These groups are written back with the AD groups scope of [universal](#). Your on-premises environment must support the universal group scope.
- Groups that are larger than 50,000 members aren't supported.
- Tenants that have more than 150,000 objects aren't supported. Meaning, if a tenant has any combination of users and groups that exceeds 150K objects, the tenant isn't supported.
- Each direct child nested group counts as one member in the referencing group
- Reconciliation of groups between Microsoft Entra ID and Active Directory isn't supported if the group is manually updated in Active Directory.

Additional information

The following is additional information on provisioning groups to Active Directory.

- Groups provisioned to AD using cloud sync can only contain on-premises synchronized users and / or additional cloud created security groups.

- These users must have the `onPremisesObjectIdentifier` attribute set on their account.
- The `onPremisesObjectIdentifier` must match a corresponding `objectGUID` in the target AD environment.
- An on-premises users `objectGUID` attribute to a cloud users `onPremisesObjectIdentifier` attribute can be synchronized using either Microsoft Entra Cloud Sync ([1.1.1370.0](#)) or Microsoft Entra Connect Sync ([2.2.8.0](#))
- If you're using Microsoft Entra Connect Sync ([2.2.8.0](#)) to synchronize users, instead of Microsoft Entra Cloud Sync, and want to use Provisioning to AD, it must be [2.2.8.0](#) or later.
- Only regular Microsoft Entra ID tenants are supported for provisioning from Microsoft Entra ID to Active Directory. Tenants such as B2C aren't supported.
- The group provisioning job is scheduled to run every 20 minutes.

Supported scenarios for group writeback with Microsoft Entra Cloud Sync

The following sections describe the supported scenarios for group writeback with Microsoft Entra Cloud Sync.

- [Migrate Microsoft Entra Connect Sync group writeback V2 to Microsoft Entra Cloud Sync](#)
- [Govern on-premises Active Directory based apps \(Kerberos\) using Microsoft Entra ID Governance](#)

Migrate Microsoft Entra Connect Sync group writeback V2 to Microsoft Entra Cloud Sync

Scenario: Migrate group writeback using Microsoft Entra Connect Sync (formerly Azure AD Connect) to Microsoft Entra Cloud Sync. This scenario is **only** for customers who are currently using Microsoft Entra Connect group writeback v2. The process outlined in this document pertains only to cloud-created security groups that are written back with a universal scope. Mail-enabled groups and DLs written back using Microsoft Entra Connect group writeback V1 or V2 aren't supported.

For more information see [Migrate Microsoft Entra Connect Sync group writeback V2 to Microsoft Entra Cloud Sync](#).

Govern on-premises Active Directory based apps (Kerberos) using Microsoft Entra ID Governance

Scenario: Manage on-premises applications with Active Directory groups that are provisioned from and managed in the cloud. Microsoft Entra Cloud Sync allows you to fully govern application assignments in AD while taking advantage of Microsoft Entra ID Governance features to control and remediate any access related requests.

For more information see [Govern on-premises Active Directory based apps \(Kerberos\) using Microsoft Entra ID Governance](#).

Next steps

- Provision groups to Active Directory using Microsoft Entra Cloud Sync
- Govern on-premises Active Directory based apps (Kerberos) using Microsoft Entra ID Governance
- Migrate Microsoft Entra Connect Sync group writeback V2 to Microsoft Entra Cloud Sync
- Scoping filter and attribute mapping - Microsoft Entra ID to Active Directory

Use a group to manage access to SaaS applications

Article • 01/29/2025

When you use Microsoft Entra ID with a Microsoft Entra ID P1 or P2 license plan, you can use groups to assign access to software as a service (SaaS) applications integrated with Microsoft Entra ID.

For example, if you want to assign access for a marketing department to use five different SaaS applications, you can create an Office 365 or security group that contains the users in the marketing department. Then you can assign that group to the five SaaS applications that the marketing department needs.

With Microsoft Entra ID, you can save time by managing the membership of the marketing department in one place. Users then are assigned to the application when they're added as members of the marketing group. They have their assignments removed from the application when they're removed from the marketing group. You can use this capability with hundreds of applications that you can add from within the Microsoft Entra Application Gallery.

Important

You can use this feature only after you start a Microsoft Entra ID P1 or P2 trial or purchase a Microsoft Entra ID P1 or P2 license plan. Group-based assignment is supported only for security groups. Nested group memberships aren't supported for group-based assignment to applications at this time.

Assign access for a user or group to a SaaS application

1. Sign in to the [Microsoft Entra admin center](#)  as at least a [User Administrator](#).
2. Go to **Applications > Enterprise applications** to open **All applications** in the Application Gallery.

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with sections like Home, Diagnose & solve problems, Favorites, Identity, Users, Groups, Devices, Applications, and Protection. Under Applications, 'Enterprise applications' is selected and highlighted with a red box. The main content area is titled 'Enterprise applications | All applications' and shows a list of 11 applications found. The columns in the table are Name, Object ID, Application ID, Homepage URL, Created on, and Certificate Expiry. Applications listed include LinkedIn, ProvisioningP..., BrowserStack, Salesforce, MOD Demo P..., Contoso Prod..., dprovisionin..., ProvisioningH..., Graph Explorer, and Box.

3. Select an application that you added from the Application Gallery to open it.
4. On the left pane, select **Users and groups**, and then select **Add user/group**.
5. On **Add Assignment**, select **Users and groups** to open the **Users and groups** selection list.
6. Select as many groups or users as you want, and then select or tap **Select** to add them to the **Add Assignment** list. You can also assign a role to a user at this stage.
7. Select **Assign** to assign the users or groups to the selected enterprise application.

Next steps

For more information on Microsoft Entra ID, see:

- [Managing access to resources with Microsoft Entra groups](#)
- [Application management in Microsoft Entra ID](#)
- [Microsoft Entra cmdlets for configuring group settings](#)
- [What is Microsoft Entra ID?](#)
- [Integrating your on-premises identities with Microsoft Entra ID](#)

Feedback

Was this page helpful?

Yes

No

[Provide product feedback](#)

Enforce a naming policy on Microsoft 365 groups in Microsoft Entra ID

Article • 01/14/2025

To enforce consistent naming conventions for Microsoft 365 groups created or edited by your users, set up a group naming policy for your organizations in Microsoft Entra ID. For example, you could use the naming policy to communicate the function of a group, membership, geographic region, or person who created the group. You could also use the naming policy to help categorize groups in the address book. You can use the policy to block specific words from being used in group names and aliases.

Important

Using a Microsoft Entra ID naming policy for Microsoft 365 groups requires that you possess but not necessarily assign a Microsoft Entra ID P1 license or Microsoft Entra Basic EDU license for each unique user who's a member of one or more Microsoft 365 groups.

The naming policy is applied to creating or editing groups created across workloads, for example, Outlook, Microsoft Teams, SharePoint, Exchange, or Planner, even if no editing changes are made. It's applied to both the group name and group alias. If you set up your naming policy in Microsoft Entra ID and you have an existing Exchange group naming policy, the Microsoft Entra ID naming policy is enforced in your organization.

When a group naming policy is configured, the policy is applied to new Microsoft 365 groups created by users. A naming policy doesn't apply to certain directory roles, such as Global Administrator or User Administrator. (For the complete list of roles exempted from a group naming policy, see the "Roles and permissions" section.) For existing Microsoft 365 groups, the policy isn't immediately applied at the time of configuration. After a group owner edits the group name for these groups, the naming policy is enforced even if no changes are made.

Naming policy features

You can enforce a naming policy for groups in two different ways:

- **Prefix-suffix naming policy:** You can define prefixes or suffixes that are then added automatically to enforce a naming convention on your groups. For example, in the

group name `GRP_JAPAN_My Group_Engineering`, the prefix is `GRP_JAPAN_` and the suffix is `_Engineering`.

- **Custom blocked words:** You can upload a set of blocked words specific to your organization to be blocked in groups created by users. For example, you might use `Payroll,CEO,HR`.

Prefix-suffix naming policy

The general structure of the naming convention is `Prefix[GroupName]Suffix`. While you can define multiple prefixes and suffixes, you can have only one instance of the `[GroupName]` in the setting. The prefixes or suffixes can be either fixed strings or user attributes, such as `[Department]`, that are substituted based on the user who's creating the group. The total allowable number of characters for your prefix and suffix strings including group name is 63 characters.

Prefixes and suffixes can contain special characters that are supported in a group name and a group alias. Any characters in the prefix or suffix that aren't supported in the group alias are still applied in the group name but removed from the group alias. Because of this restriction, the prefixes and suffixes applied to the group name might be different from the ones applied to the group alias.

Fixed strings

You can use strings to make it easier to scan and differentiate groups in the global address list and in the left navigation links of group workloads. Some of the common prefixes are keywords like `Grp_Name`, `#Name`, and `_Name`.

User attributes

You can use attributes that can help you and your users identify which department, office, or geographic region for which the group was created. For example, if you define your naming policy as `PrefixSuffixNamingRequirement = "GRP [GroupName][Department]"` and `User's department = Engineering`, then an enforced group name might be `"GRP My Group Engineering."` Supported Microsoft Entra attributes are `\[Department\]`, `\[Company\]`, `\[Office\]`, `\[StateOrProvince\]`, `\[CountryOrRegion\]`, and `\[Title\]`. Unsupported user attributes are treated as fixed strings. An example is `"\[postalCode\]"`. Extension attributes and custom attributes aren't supported.

We recommend that you use attributes that have values filled in for all users in your organization and don't use attributes that have long values.

Custom blocked words

A blocked word list is a comma-separated list of phrases to be blocked in group names and aliases. No substring searches are performed. An exact match between the group name and one or more of the custom blocked words is required to trigger a failure. Substring search isn't performed so that users can use common words like "Class" even if "lass" is a blocked word.

Blocked word list rules:

- Blocked words aren't case sensitive.
- When a user enters a blocked word as part of a group name, they see an error message with the blocked word.
- There are no character restrictions on blocked words.
- There's an upper limit of 5,000 phrases that you can configure in the blocked words list.

Roles and permissions

To configure a naming policy, one of the following roles is required:

- Global Administrator
- Group Administrator
- Directory Writer

Some administrator roles are exempted from these policies, across all group workloads and endpoints, so that they can create groups by using blocked words and with their own naming conventions. The following administrator roles are exempted from the group naming policy:

- Global Administrator
- User Administrator

Configure a naming policy

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Group Administrator](#).
2. Select **Microsoft Entra ID**.
3. Select **All groups > Groups**, and then select **Naming policy** to open the **Naming policy** page.

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with sections like Home, Favorites, Identity, Overview, Users, Groups (with 'All groups' selected), Deleted groups, Group settings, Devices, Applications, Protection, Identity governance, External identities, Show more, Protection, Identity governance, Verifiable credentials, and Learn & support. The main content area is titled 'Groups - Naming policy' and shows a 'Group naming policy' section. It includes a 'Learn more about group naming policies.' link, a 'Blocked words' tab (selected), and a 'Group naming policy' tab. Below this, it says 'Group naming policy' and describes how it allows adding prefixes or suffixes to group names. It shows a current policy 'GRP<Group name>Test-Second' and two sections for 'ADD PREFIX' and 'ADD SUFFIX' with dropdown menus for strings. There are also 'Delete' and 'Save' buttons.

View or edit the prefix-suffix naming policy

1. On the **Naming policy** page, select **Group naming policy**.
2. You can view or edit the current prefix or suffix naming policies individually by selecting the attributes or strings you want to enforce as part of the naming policy.
3. To remove a prefix or suffix from the list, select the prefix or suffix, and then select **Delete**. You can delete multiple items at the same time.
4. Save your changes for the new policy to go into effect by selecting **Save**.

Edit custom blocked words

1. On the **Naming policy** page, select **Blocked words**.

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with sections like Home, Favorites, Identity, Overview, Users, Groups (with 'All groups' selected), Deleted groups, Group settings, Devices, Applications, Protection, Identity governance, External identities, Show more, Protection, Identity governance, Verifiable credentials, and Learn & support. The main content area is titled 'Groups - Naming policy' and shows a 'Blocked words' section. It includes a 'Learn more about group naming policies.' link, a 'Blocked words' tab (selected), and a 'Group naming policy' tab. Below this, it says 'Enable custom blocked words list' and provides instructions for uploading a CSV file of blocked words. It shows a 'Blocked words stored and available for download' message with a green checkmark. It also lists steps to view and edit the blocked words list: 1. Download .csv file of blocked words (with a 'Download' button), 2. Add or remove terms (5,000 word maximum), and 3. Upload your .csv file. There's a 'Select a file' input field.

2. View or edit the current list of custom blocked words by selecting **Download**. You must add new entries to the existing entries.
3. Upload the new list of custom blocked words by selecting the **file** icon.
4. Save your changes for the new policy to go into effect by selecting **Save**.

Install PowerShell cmdlets

Install the Microsoft Graph cmdlets as described in [Install the Microsoft Graph PowerShell SDK](#).

 **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.

1. Open the Windows PowerShell app as an administrator.
2. Install the Microsoft Graph cmdlets.

```
PowerShell  
Install-Module Microsoft.Graph -Scope AllUsers
```

3. Install the Microsoft Graph beta cmdlets.

```
PowerShell  
Install-Module Microsoft.Graph.Beta -Scope AllUsers
```

Configure a naming policy in PowerShell

1. Open a Windows PowerShell window on your computer. You can open it without elevated privileges.
2. Run the following command to prepare to run the cmdlets.

```
PowerShell
```

```
Connect-MgGraph -Scopes "Directory.ReadWrite.All"
```

On the **Sign in to your Account** screen that opens, enter your admin account and password to connect to your service.

3. Follow the steps in [Microsoft Entra cmdlets for configuring group settings](#) to create group settings for this organization.

View the current settings

1. Fetch the current naming policy to view the current settings.

```
PowerShell
```

```
$Setting = Get-MgBetaDirectorySetting -DirectorySettingId (Get-MgBetaDirectorySetting | where -Property DisplayName -Value "Group.Unified" -EQ).id
```

2. Display the current group settings.

```
PowerShell
```

```
$Setting.Values
```

Set the naming policy and custom blocked words

1. Get the setting.

```
PowerShell
```

```
$Setting = Get-MgBetaDirectorySetting -DirectorySettingId (Get-MgBetaDirectorySetting | where -Property DisplayName -Value "Group.Unified" -EQ).id
```

2. Set the group name prefixes and suffixes. For the feature to work properly, [GroupName] must be included in the setting. Also, set the custom blocked words

that you want to restrict.

PowerShell

```
$params = @{
    values = @(
        @{
            name = "PrefixSuffixNamingRequirement"
            value = "GRP_[GroupName]_[Department]"
        }
        @{
            name = "CustomBlockedWordsList"
            value = "Payroll,CEO,HR"
        }
    )
}
```

3. Update the settings for the new policy to go into effect, as shown in the following example.

PowerShell

```
Update-MgBetaDirectorySetting -DirectorySettingId $Setting.Id -  
BodyParameter $params
```

That's it. You set your naming policy and added your blocked words.

Export or import custom blocked words

For more information, see [Microsoft Entra cmdlets for configuring group settings](#).

Here's an example of a PowerShell script to export multiple blocked words.

PowerShell

```
$Words = (Get-MgBetaDirectorySetting).Values | where -Property Name -Value  
CustomBlockedWordsList -EQ  
Add-Content "c:\work\currentblockedwordslist.txt" -Value  
$Words.value.Split(",").Replace(`", "", "")
```

Here's an example PowerShell script to import multiple blocked words.

PowerShell

```
$BadWords = Get-Content "C:\work\currentblockedwordslist.txt"  
$BadWords = [string]::join(",", $BadWords)  
$Setting = Get-MgBetaDirectorySetting | where {$_.DisplayName -eq
```

```

"Group.Unified"}
if ($Setting.Count -eq 0) {
    $Template = Get-MgBetaDirectorySettingTemplate | where {$_.DisplayName - 
eq "Group.Unified"}
    $Params = @{
        templateId = $Template.Id
    }
    $Setting = New-MgBetaDirectorySetting -BodyParameter $Params
}
$params = @{
    values = @(
        @{
            name = "PrefixSuffixNamingRequirement"
            value = "GRP_[GroupName]_[Department]"
        }
        @{
            name = "CustomBlockedWordsList"
            value = "$BadWords"
        }
    )
}
Update-MgBetaDirectorySetting -DirectorySettingId $Setting.Id -BodyParameter
$params

```

Remove the naming policy

You can use the Azure portal or Microsoft Graph PowerShell to remove a naming policy.

Remove the naming policy by using the Azure portal

1. On the **Naming policy** page, select **Delete policy**.
2. After you confirm the deletion, the naming policy is removed, including all prefix-suffix naming policies and any custom blocked words.

Remove the naming policy by using Microsoft Graph PowerShell

1. Get the setting.

PowerShell

```
$Setting = Get-MgBetaDirectorySetting -DirectorySettingId (Get-
MgBetaDirectorySetting | where -Property DisplayName -Value
"Group.Unified" -EQ).id
```

2. Empty the group name prefixes and suffixes. Empty the custom blocked words.

PowerShell

```

$params = @{
    values = @(
        @{
            name = "PrefixSuffixNamingRequirement"
            value = ""
        }
        @{
            name = "CustomBlockedWordsList"
            value = ""
        }
    )
}

```

3. Update the setting.

PowerShell

```
Update-MgBetaDirectorySetting -DirectorySettingId $Setting.Id -  
BodyParameter $params
```

Experience across Microsoft 365 apps

After you set a group naming policy in Microsoft Entra ID, when a user creates a group in a Microsoft 365 app, they see:

- A preview of the name according to your naming policy (with prefixes and suffixes) as soon as the user enters the group name.
- If the user enters blocked words, they see an error message, so they can remove the blocked words.

[\[+\] Expand table](#)

Workload	Compliance
Azure portal	The Azure portal and the Access Panel portal show the naming policy-enforced name when the user enters a group name when creating or editing a group. When a user enters a custom blocked word, an error message with the blocked word appears so that the user can remove it.
Outlook Web Access (OWA)	Outlook Web Access shows the naming policy-enforced name when the user enters a group name or group alias. When a user enters a custom blocked word, an error message appears in the UI along with the blocked word so that the user can remove it.
Outlook desktop	Groups created in Outlook desktop are compliant with the naming policy settings. The Outlook desktop app doesn't yet show the preview of the

Workload	Compliance
	enforced group name and doesn't return the custom blocked-word errors when the user enters the group name. However, the naming policy is automatically applied when the user creates or edits a group. Users see error messages if there are custom blocked words in the group name or alias.
Microsoft Teams	Microsoft Teams shows the group naming policy-enforced name when the user enters a team name. When a user enters a custom blocked word, an error message appears along with the blocked word so that the user can remove it.
SharePoint	SharePoint shows the naming policy-enforced name when the user enters a site name or group email address. When a user enters a custom blocked word, an error message appears, along with the blocked word so that the user can remove it.
Microsoft Stream	Microsoft Stream shows the group naming policy-enforced name when the user enters a group name or group email alias. When a user enters a custom blocked word, an error message appears along with the blocked word so that the user can remove it.
Outlook iOS and Android app	Groups created in Outlook apps are compliant with the configured naming policy. The Outlook mobile app doesn't yet show the preview of the naming policy-enforced name. The app doesn't return custom blocked-word errors when the user enters the group name. However, the naming policy is automatically applied when the user selects Create or Edit . Users see error messages if there are custom blocked words in the group name or alias.
Groups mobile app	Groups created in the Groups mobile app are compliant with the naming policy. The groups mobile app doesn't show the preview of the naming policy and doesn't return custom blocked-word errors when the user enters the group name. But the naming policy is automatically applied when the user creates or edits a group. Users are presented with appropriate errors if there are custom blocked words in the group name or alias.
Planner	Planner is compliant with the naming policy. Planner shows the naming policy preview when the user enters the plan name. When a user enters a custom blocked word, an error message appears when the user creates the plan.
Project for the web	Project for the web is compliant with the naming policy.
Dynamics 365 for Customer Engagement	Dynamics 365 for Customer Engagement is compliant with the naming policy. Dynamics 365 shows the naming policy-enforced name when the user enters a group name or group email alias. When the user enters a custom blocked word, an error message appears with the blocked word so that the user can remove it.
School Data Sync (SDS)	Groups created through SDS comply with a naming policy, but the naming policy isn't applied automatically. SDS administrators have to append the

Workload	Compliance
	prefixes and suffixes to class names for which groups need to be created and then uploaded to SDS. Otherwise, create or edit for groups would fail.
Classroom app	Groups created in the Classroom app comply with the naming policy, but the naming policy isn't applied automatically. The naming policy preview isn't shown to users when they enter a classroom group name. Users must enter the enforced classroom group name with prefixes and suffixes. If not, the classroom group create or edit operation fails with errors.
Power BI	Power BI workspaces are compliant with the naming policy.
Yammer	<p>When a user signs in to Yammer with their Microsoft Entra account to create a group or edit a group name, the group name complies with the naming policy. This feature applies both to Microsoft 365 connected groups and all other Yammer groups.</p> <p>If a Microsoft 365 connected group was created before the naming policy is in place, the group name doesn't automatically follow the naming policies. When a user edits the group name, they're prompted to add the prefix and suffix.</p>
StaffHub	StaffHub teams don't follow the naming policy, but the underlying Microsoft 365 group does. A StaffHub team name doesn't apply the prefixes and suffixes and doesn't check for custom blocked words. But StaffHub does apply the prefixes and suffixes and removes blocked words from the underlying Microsoft 365 group.
Exchange PowerShell	Exchange PowerShell cmdlets are compliant with the naming policy. Users receive appropriate error messages with suggested prefixes and suffixes and for custom blocked words if they don't follow the naming policy in the group name and group alias (mailNickname).
Microsoft Graph PowerShell cmdlets	Microsoft PowerShell cmdlets are compliant with a naming policy. Users receive appropriate error messages with suggested prefixes and suffixes and for custom blocked words if they don't follow the naming convention in group names and group alias.
Exchange admin center	Exchange admin center is compliant with a naming policy. Users receive appropriate error messages with suggested prefixes and suffixes and for custom blocked words if they don't follow the naming convention in the group name and group alias.
Microsoft 365 admin center	Microsoft 365 admin center is compliant with a naming policy. When a user creates or edits group names, the naming policy is automatically applied. Users receive appropriate errors when they enter custom blocked words. The Microsoft 365 admin center doesn't yet show a preview of the naming policy and doesn't return custom blocked-word errors when the user enters the group name.

Next steps

For more information on Microsoft Entra groups, see:

- Existing groups
 - Expiration policy for Microsoft 365 groups
 - Manage settings of a group
 - Manage members of a group
 - Manage memberships of a group
 - Manage rules for dynamic membership groups
-

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Configure the expiration policy for Microsoft 365 groups

Article • 01/15/2025

This article tells you how to manage the lifecycle of Microsoft 365 groups by setting an expiration policy for them. You can set an expiration policy only for Microsoft 365 groups in Microsoft Entra ID.

After you set a group to expire:

- Groups with user activities are automatically renewed as the expiration nears.
- Owners of the group are notified to renew the group, if the group isn't autorenewed.
- Any group that isn't renewed is deleted.
- Any Microsoft 365 group that was deleted can be restored within 30 days by the group owners or the administrator.

Currently, you can configure only one expiration policy for all Microsoft 365 groups in a Microsoft Entra organization.

ⓘ Note

Configuring and using the expiration policy for Microsoft 365 groups requires you to possess but not necessarily assign Microsoft Entra ID P1 or P2 licenses for the members of all groups to which the expiration policy is applied.

For information on how to download and install Microsoft Graph PowerShell cmdlets, see [Install the Microsoft Graph PowerShell SDK](#).

ⓘ 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.

Activity-based automatic renewal

With Microsoft Entra intelligence, groups are now automatically renewed based on whether they were recently used. This feature eliminates the need for manual action by group owners. It's based on user activity in groups across Microsoft 365 services like Outlook, SharePoint, Teams, or Viva Engage.

For example, an owner or a group member might do something like:

- Send an email to the group in Outlook.
- Upload a document to SharePoint.
- Visit a Teams channel.
- View a post in Viva Engage.

In the preceding scenarios, the group is automatically renewed around 35 days before the group expires and the owner doesn't get any renewal notifications.

Now consider an expiration policy that was set so that a group expires after 30 days of inactivity. To keep from sending an expiration email the day that group expiration is enabled (because there's no record activity yet), Microsoft Entra first waits five days.

Then:

- If there's activity in those five days, the expiration policy works as expected.
- If there's no activity within five days, Microsoft Entra ID sends an expiration or renewal email.
- If the group was inactive for five days, an email was sent, and then the group was active, Microsoft Entra autorenews it and starts the expiration period again.

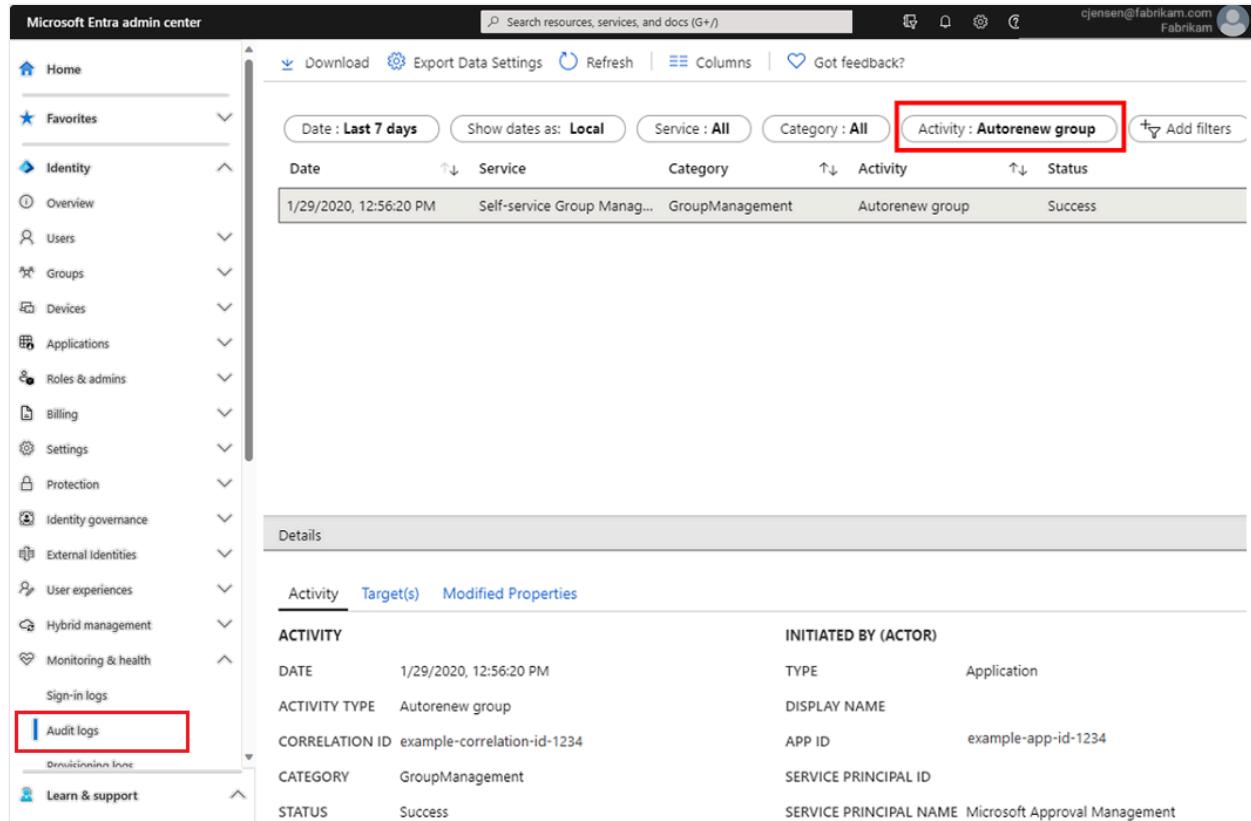
Activities that automatically renew group expiration

The following user actions cause automatic group renewal:

- **SharePoint:** View, edit, download, move, share, or upload files.
- **Outlook:** Join a group, read or write a group message from a group space, or "like" a message (in Outlook Web Access).
- **Teams:** Visit a Teams channel.
- **Viva Engage:** View a post within a Viva Engage community or an interactive email in Outlook.

Auditing and reporting

Administrators can get a list of automatically renewed groups from the activity audit logs in Microsoft Entra ID.



The screenshot shows the Microsoft Entra admin center interface. On the left is a navigation sidebar with various options like Home, Favorites, Identity, Overview, Users, Groups, Devices, Applications, Roles & admins, Billing, Settings, Protection, Identity governance, External Identities, User experiences, Hybrid management, Monitoring & health, Sign-in logs, and Audit logs. The Audit logs option is highlighted with a red box. The main area has a search bar at the top. Below it are filter buttons for Date (Last 7 days), Show dates as (Local), Service (All), Category (All), and Activity (Autorenew group, also highlighted with a red box). A 'Columns' button and a 'Got feedback?' link are also present. The main content area displays a table of audit log entries. One entry is shown in detail: Date 1/29/2020, 12:56:20 PM, Service Self-service Group Management, Category GroupManagement, Activity Autorenew group, Status Success. Below this, a 'Details' section shows activity properties: ACTIVITY INITIATED BY (ACTOR), DATE 1/29/2020, 12:56:20 PM, ACTIVITY TYPE Application, DISPLAY NAME Autorenew group, CORRELATION ID example-correlation-id-1234, APP ID example-app-id-1234, CATEGORY GroupManagement, SERVICE PRINCIPAL ID, STATUS Success, SERVICE PRINCIPAL NAME Microsoft Approval Management.

Roles and permissions

The following roles can configure and use expiration for Microsoft 365 groups in Microsoft Entra ID.

[] Expand table

Role	Permissions
Groups Administrator, or User Administrator	Can create, read, update, or delete the Microsoft 365 groups expiration policy settings Can renew any Microsoft 365 group
User	Can renew a Microsoft 365 group that they own Can restore a Microsoft 365 group that they own Can read the expiration policy settings

For more information on permissions to restore a deleted group, see [Restore a deleted Microsoft 365 group in Microsoft Entra ID](#).

Set group expiration

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Groups Administrator**.
2. Select **Microsoft Entra ID**.
3. Select **Groups > All groups**, and then select **Expiration** to open the expiration settings.

The screenshot shows the 'Groups | Expiration' page in the Microsoft Entra admin center. The left sidebar has sections for 'All groups', 'Deleted groups', 'Diagnose and solve problems', 'Settings' (with 'General' and 'Expiration' selected), 'Naming policy', 'Activity' (with 'Privileged Identity Management', 'Access reviews', 'Audit logs', and 'Bulk operation results'), and 'Troubleshooting + Support' (with 'New support request'). The main area shows renewal notification details: 'Renewal notifications are emailed to group owners 30 days, 15 days, and one day prior to group expiration. Group owners must have Exchange licenses to receive notification emails. If a group is not renewed, it is deleted along with its associated content from sources such as Outlook, SharePoint, Teams, and PowerBI.' Below this are fields for 'Group lifetime (in days)' set to 180, 'Email contact for groups with no owners' set to admin@contoso.com, and a button to 'Enable expiration for these Office 365 groups' with options 'All', 'Selected', and 'None'.

4. On the **Expiration** page, you can:

- Set the group lifetime in days. You can select one of the preset values or a custom value. It should be 30 days or more.
- Specify an email address where the renewal and expiration notifications are sent when a group has no owner.
- Select which Microsoft 365 groups expire. You can set expiration for:
 - **All** Microsoft 365 groups.
 - **Selected** Microsoft 365 groups.
 - **None** to restrict expiration for all groups.
- Save your settings when you're done by selecting **Save**.

ⓘ Note

- When you first set up expiration, any groups that are older than the expiration interval are set to 35 days until expiration unless the group is automatically renewed or the owner renews it.
- When a dynamic group is deleted and restored, it's seen as a new group and repopulated according to the rule. This process can take up to 24 hours.

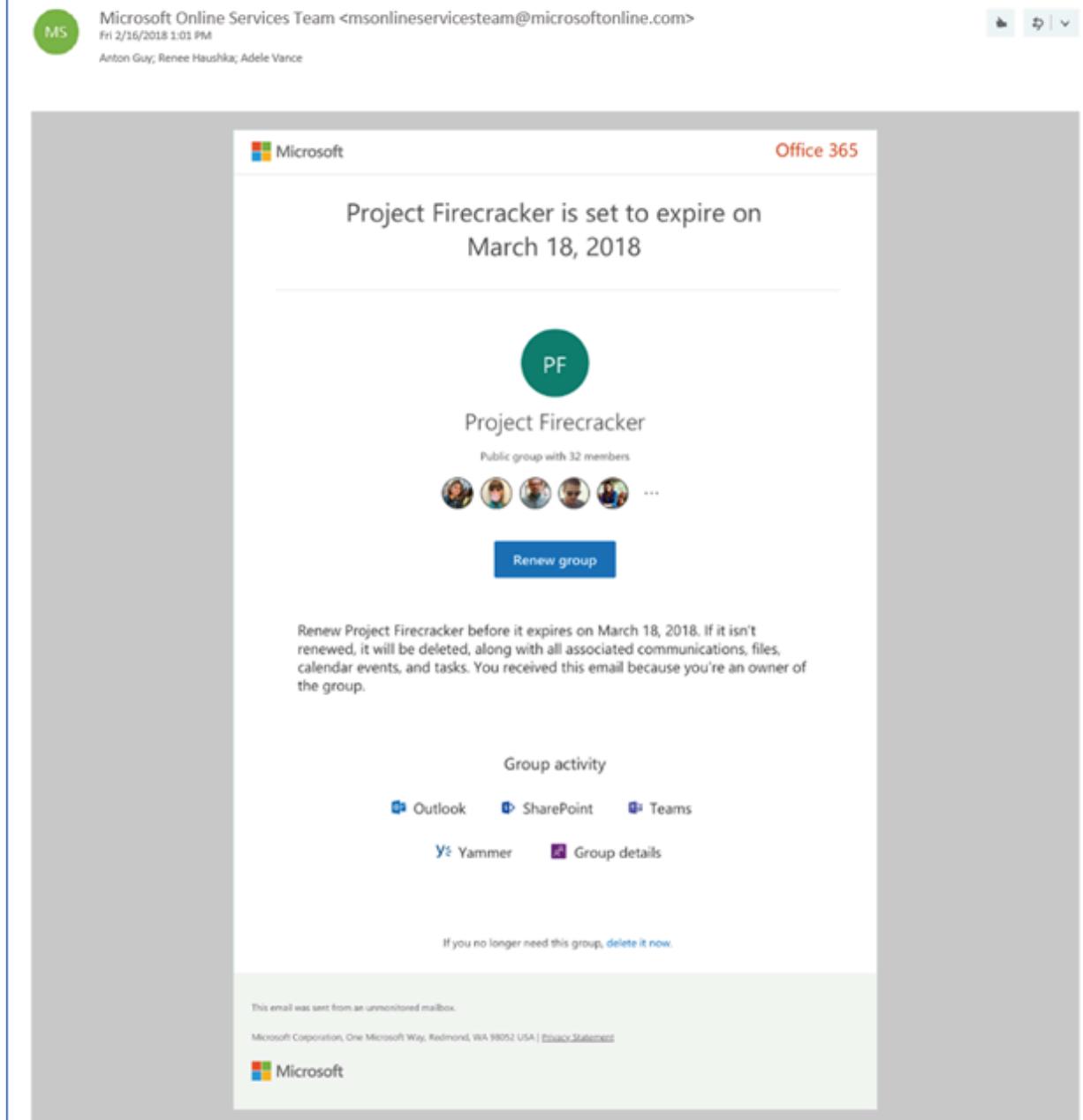
- Expiration notices for groups used in Teams appear in the Teams Owners feed.
- When you enable expiration for selected groups, you can add up to 500 groups to the list. If you need to add more than 500 groups, you can enable expiration for all your groups. In that scenario, the 500-group limitation doesn't apply.
- Groups don't renew immediately when auto-renew activities occur. In the event of an activity, a flag is placed on the group to indicate it's ready for renewal when it's near expiry. If the group is near expiry, renewal occurs within 24 hours.

Email notifications

If groups aren't automatically renewed, email notifications like the following example are sent to the Microsoft 365 group owners 30 days, 15 days, and 1 day before group expiration.

The groups owner's preferred language or the Microsoft Entra language setting determines the language of the email. If the group owner defined a preferred language, or multiple owners have the same preferred language, that language is used. For all other cases, the Microsoft Entra language setting is used.

Action Required: Renew Project Firecracker by March 11, 2018



From the **Renew group** notification email, group owners can directly access the group details page in the [Access Panel](#). There, users can get more information about the group, such as its description, when it was last renewed, when it expires, and also the ability to renew the group. The group details page now also includes links to the Microsoft 365 group resources so that the group owner can conveniently view the content and activity in their group.

ⓘ Important

If there's any problem with the notification emails and they aren't sent out or they're delayed, be assured that Microsoft never deletes a group before the last email is sent.

When a group expires, the group is deleted one day after the expiration date. An email notification such as this one is sent to the Microsoft 365 group owners informing them about the expiration and subsequent deletion of their Microsoft 365 group.

Attention: Project Firecracker was deleted. Restore it by September 17, 2018

Microsoft Online Services Team <msonlineservicesteam@microsoftonline.com>
Sat 8/18/2018 1:31 PM
Anton Guy, Renee Haushka, Adele Vance

The screenshot shows an email from Microsoft Online Services Team. The subject is "Attention: Project Firecracker was deleted. Restore it by September 17, 2018". The email header includes the sender's name and a timestamp. Below the header is the Microsoft logo and the "Office 365" logo. The main content of the email is titled "Restore project Firecracker by September 17, 2018". It features a green circular icon with the letters "PF" and the text "Project Firecracker" below it. It says "Public group with 32 members" and shows a grid of small user profile pictures. A blue button labeled "Restore group" is visible. A paragraph of text explains that the group expired on August 18, 2018, and provides instructions for restoration. At the bottom, there is a note about unmonitored mailboxes and Microsoft's address, followed by the Microsoft logo.

You can restore the group within 30 days of its deletion by selecting **Restore group** or by using PowerShell cmdlets. For more information, see [Restore a deleted Microsoft 365 group in Microsoft Entra ID](#). The 30-day group restoration period isn't customizable.

If the group you're restoring contains documents, SharePoint sites, or other persistent objects, it might take up to 24 hours to fully restore the group and its contents.

Retrieve the Microsoft 365 group expiration date

In addition to using Access Panel to view group details like expiration date and last renewed date, you can retrieve the expiration date of a Microsoft 365 group from Microsoft Graph REST API Beta. The group property `expirationDateTime` is enabled in

Microsoft Graph Beta. You can retrieve it with a GET request. For more information, see [this example](#).

 **Note**

To manage group memberships on the Access Panel, **Restrict access to Groups in Access Panel** must be set to **No** in the Microsoft Entra groups **General** setting.

Microsoft 365 group expiration with a mailbox on legal hold

When a group expires and is deleted, 30 days after deletion the group's data from apps like Planner, Sites, or Teams is permanently deleted. The group mailbox that's on legal hold is retained and isn't permanently deleted. The administrator can use Exchange cmdlets to restore the mailbox to fetch the data.

Microsoft 365 group expiration with a retention policy

You can configure the retention policy in the Security & Compliance portal. There you can set up a retention policy for Microsoft 365 groups. When a group expires and is deleted, the group conversations in the group mailbox and files in the group site are retained in the retention container for the specific number of days defined in the retention policy. Users won't see the group or its content after expiration. They can recover the site and mailbox data via e-discovery.

PowerShell examples

Here are examples of how you can use PowerShell cmdlets to configure the expiration settings for Microsoft 365 groups in your Microsoft Entra organization:

1. Install the Microsoft Graph PowerShell module and sign in at the PowerShell prompt.

PowerShell

```
Install-Module Microsoft.Graph -Scope CurrentUser  
Connect-MgGraph -Scopes "Directory.ReadWrite.All"
```

2. Configure the expiration settings. Use the [New-MgGroupLifecyclePolicy](#) cmdlet to set the lifetime for all Microsoft 365 groups in the Microsoft Entra organization to 365 days. Renewal notifications for Microsoft 365 groups without owners are sent to `emailaddress@contoso.com`.

```
PowerShell
```

```
New-MgGroupLifecyclePolicy -AlternateNotificationEmails  
emailaddress@contoso.com`  
-GroupLifetimeInDays 365 -ManagedGroupTypes All
```

3. Retrieve the existing policy by using [Get-MgGroupLifecyclePolicy](#). This cmdlet retrieves the current Microsoft 365 group expiration settings that were configured.

```
PowerShell
```

```
Get-MgGroupLifecyclePolicy
```

In this example, you can see:

- The policy ID.
- Renewal notifications for Microsoft 365 groups without owners are sent to `emailaddress@contoso.com`.
- The lifetime for all Microsoft 365 groups in the Microsoft Entra organization is set to 365 days.

```
Output
```

Id	AlternateNotificationEmails
GroupLifetimeInDays	ManagedGroupTypes
--	-----
-----	-----
1aaaaaaaa1-2bb2-3cc3-4dd4-5eeeeeeeeee5	emailaddress@contoso.com
All	365

4. Update the existing policy by using [Update-MgGroupLifecyclePolicy](#). This cmdlet is used to update an existing policy. In the following example, the group lifetime in the existing policy is changed from 365 days to 180 days.

```
PowerShell
```

```
Update-MgGroupLifecyclePolicy -GroupLifecyclePolicyId "1aaaaaaaa1-2bb2-  
3cc3-4dd4-5eeeeeeeeee5" -GroupLifetimeInDays 180 -  
AlternateNotificationEmails "emailaddress@contoso.com"
```

5. Add specific groups to the policy by using [Add-MgGroupToLifecyclePolicy](#). This cmdlet adds a group to the lifecycle policy. As an example:

```
PowerShell
```

```
Add-MgGroupToLifecyclePolicy -GroupLifecyclePolicyId "1aaaaaaaa1-2bb2-3cc3-4dd4-5eeeeeeeeee5" -GroupId "cffd97bd-6b91-4c4e-b553-6918a320211c"
```

6. Remove the existing policy by using [Remove-MgGroupLifecyclePolicy](#). This cmdlet deletes the Microsoft 365 group expiration settings but requires the policy ID. This cmdlet disables expiration for Microsoft 365 groups.

```
PowerShell
```

```
Remove-MgGroupLifecyclePolicy -GroupLifecyclePolicyId "1aaaaaaaa1-2bb2-3cc3-4dd4-5eeeeeeeeee5"
```

You can use the following cmdlets to configure the policy in more detail. For more information, see [Microsoft Graph PowerShell documentation](#).

- [Get-MgGroupLifecyclePolicy](#)
- [New-MgGroupLifecyclePolicy](#)
- [Remove-MgGroupLifecyclePolicy](#)
- [Update-MgGroupLifecyclePolicy](#)
- [Add-MgGroupToLifecyclePolicy](#)
- [Remove-MgGroupFromLifecyclePolicy](#)
- [Invoke-MgRenewGroup](#)

Next steps

For more information on Microsoft Entra groups, see:

- [Existing groups](#)
- [Manage settings of a group](#)
- [Manage members of a group](#)
- [Manage memberships of a group](#)
- [Manage rules for dynamic membership groups](#)

Feedback

Was this page helpful?

 Yes

 No

Provide product feedback 

Set up self-service group management in Microsoft Entra ID

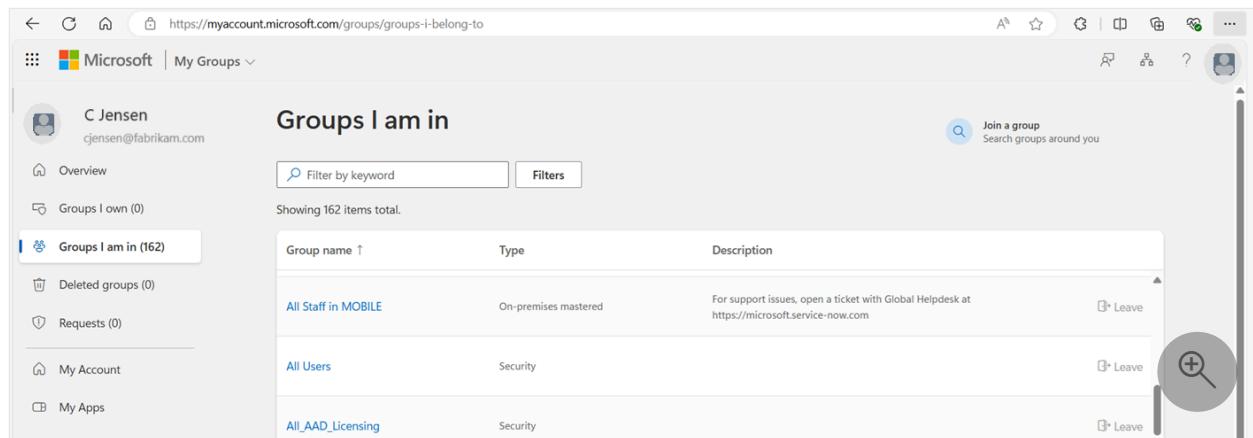
Article • 02/12/2025

Microsoft Entra ID provides self-service group management features that enable users to create and manage their own security groups or Microsoft 365 groups. The owner of the group can approve or deny membership requests and delegate control of group membership. Self-service group management features aren't available for [mail-enabled security groups or distribution lists](#).

Self-service group membership

You can allow users to create security groups to manage access to shared resources.

Users can create security groups from the [Microsoft Entra admin center](#), using PowerShell, or from the [My Groups portal](#).



The screenshot shows the Microsoft My Groups portal at https://myaccount.microsoft.com/groups/groups-i-belong-to. On the left, there's a sidebar with user info (C Jensen, cjensen@fabrikam.com), navigation links (Overview, Groups I own (0), Groups I am in (162) - which is selected, Deleted groups (0), Requests (0), My Account, My Apps), and a search bar. The main area is titled 'Groups I am in' and shows a table with three rows:

Group name ↑	Type	Description	Action
All Staff in MOBILE	On-premises mastered	For support issues, open a ticket with Global Helpdesk at https://microsoft.service-now.com	Leave
All Users	Security		Leave
All_AAD_Licensing	Security		Leave

There are also 'Join a group' and 'Search groups around you' buttons, and a magnifying glass icon for search.

Only the group's owners can update membership. You can give group owners the ability to approve or deny membership requests from the My Groups portal. Security groups created by self-service through the My Groups portal are available to join for all users, whether owner-approved or autoapproved. In the My Groups portal, you can change membership options when you create the group.

Microsoft 365 groups provide collaboration opportunities for your users. You can create groups in any of the Microsoft 365 applications, such as SharePoint, and Microsoft Teams. You can also create Microsoft 365 groups in Azure portals by using Microsoft Graph PowerShell or from the My Groups portal. For more information on the difference between security groups and Microsoft 365 groups, see [Learn about groups](#).

[\[\] Expand table](#)

Groups created in	Security group default behavior	Microsoft 365 group default behavior
Microsoft Graph PowerShell	Only owners can add members. Visible but not available to join in MyApp Groups Access Panel.	Open to join for all users.
Azure portal ↗	Only owners can add members. Visible but not available to join in My Groups portal. Owner isn't assigned automatically at group creation.	Open to join for all users.
My Groups portal ↗	Users can manage groups and request access to join groups here. Membership options can be changed when a group is created.	Open to join for all users. Membership options can be changed when a group is created.

Self-service group management scenarios

Two scenarios help to explain self-service group management.

Delegated group management

In this example scenario, an administrator manages access to a Software as a Service (SaaS) application that the company is using. Managing the access rights is cumbersome, so the administrator asks the business owner to create a new group. The administrator assigns access for the application to the new group and adds to the group all people already accessing the application. The business owner then can add more users, and those users are automatically provisioned to the application.

The business owner doesn't need to wait for the administrator to manage access for users. If the administrator grants the same permission to a manager in a different business group, that person can also manage access for their own group members. The business owner and the manager can't view or manage each other's group memberships. The administrator can still see all users who have access to the application and block access rights, if needed.

ⓘ Note

For delegated scenarios, the administrator needs to have at least a [Privileged Role Administrator Microsoft Entra](#) role.

Self-service group management

In this example scenario, two users have SharePoint Online sites that they set up independently. They want to give each other's teams access to their sites. To accomplish this task, they can create one group in Microsoft Entra ID. In SharePoint Online, each of them selects that group to provide access to their sites.

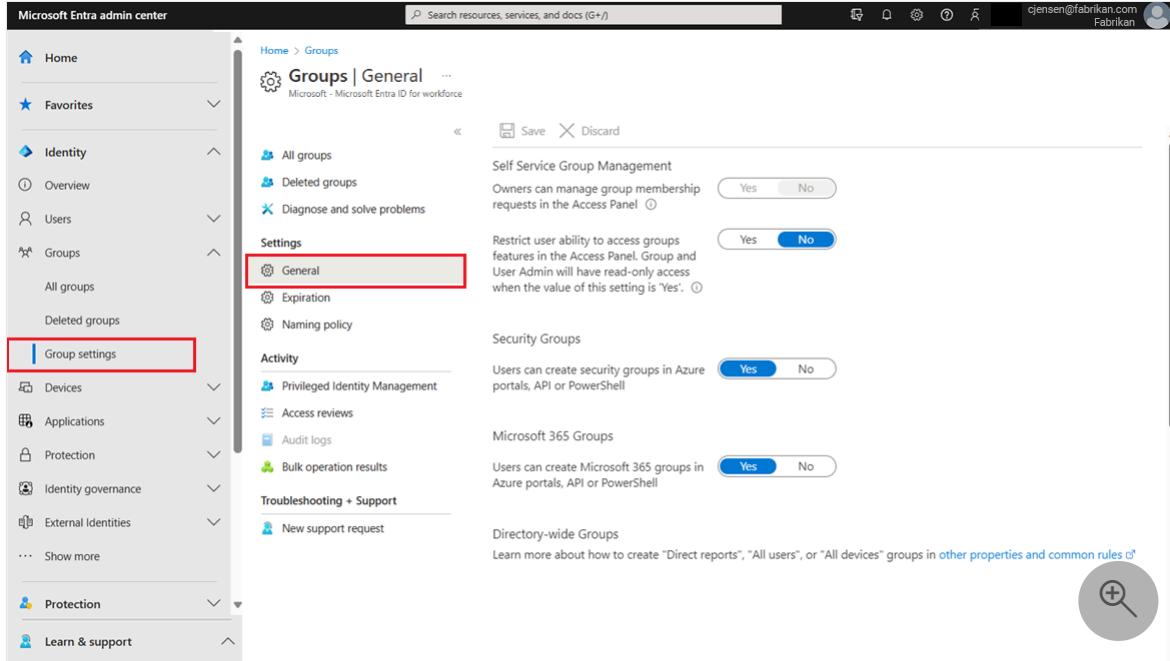
When someone wants access, they request it from the [My Groups portal](#). After approval, they get access to both SharePoint Online sites automatically. Later, one of them decides that all people accessing the site should also get access to a particular SaaS application. The administrator of the SaaS application can add access rights for the application to the SharePoint Online site. From then on, any requests that get approved give access to the two SharePoint Online sites and also to the SaaS application.

Make a group available for user self-service

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Global Administrator](#).
2. Select **Microsoft Entra ID**.
3. Select **All groups > Groups**, and then select **General** settings.

! Note

This setting only restricts access of group information in [My Groups](#). It doesn't restrict access to group information via other methods like Microsoft Graph API calls or the Microsoft Entra admin center.



 **Note**

Changes regarding the Self Service Group Management setting, are currently under review and won't take place as originally planned. A deprecation date will be announced in the future.

4. Set **Owners can manage group membership requests in the Access Panel** to Yes.
5. Set **Restrict user ability to access groups features in the Access Panel** to No.
6. Set **Users can create security groups in Azure portals, API or PowerShell** to Yes or No.
For more information about this setting, see [Group settings](#).
7. Set **Users can create Microsoft 365 groups in Azure portals, API or PowerShell** to Yes or No.
For more information about this setting, see [Group settings](#).

You can also use **Owners who can assign members as group owners in the Azure portal** to achieve more granular access control over self-service group management for your users.

When users can create groups, all users in your organization are allowed to create new groups. As the default owner, they can then add members to these groups. You can't specify individuals who can create their own groups. You can specify individuals only for making another group member a group owner.

 **Note**

A Microsoft Entra ID P1 or P2 license is required for users to request to join a security group or Microsoft 365 group and for owners to approve or deny membership requests. Without a Microsoft Entra ID P1 or P2 license, users can still manage their groups in the MyApp Groups Access Panel. But they can't create a group that requires owner approval, and they can't request to join a group.

Group settings

The group settings enable you to control who can create security and Microsoft 365 groups.

General

User Admin will have read-only access when the value of this setting is 'Yes'. [\(i\)](#)

Expiration

Naming policy

Activity

- Privileged access groups (Preview)
- Access reviews
- Audit logs
- Bulk operation results

Troubleshooting + Support

Security Groups

Users can create security groups in Azure portals, API or PowerShell Yes No

Microsoft 365 Groups

Users can create Microsoft 365 groups in Azure portals, API or PowerShell Yes No

The following table helps you decide which values to choose.

[\[+\] Expand table](#)

Setting	Value	Effect on your tenant
Users can create security groups in the Azure portal, API, or PowerShell.	Yes	All users in your Microsoft Entra organization are allowed to create new security groups and add members to these groups in the Azure portal, API, or PowerShell. These new groups also show up in the Access Panel for all other users. If the policy setting on the group allows it, other users can create requests to join these groups.
	No	Users can't create security groups. They can still manage the membership of groups for which they're an owner and approve requests from other users to join their groups.
Users can create Microsoft 365 groups in the Azure portal, API, or PowerShell.	Yes	All users in your Microsoft Entra organization are allowed to create new Microsoft 365 groups and add members to these groups in the Azure portal, API, or PowerShell. These new groups also show up in the Access Panel for all other users. If the policy setting on the group allows it, other users can create requests to join these groups.
	No	Users can't create Microsoft 365 Groups. They can still manage the membership of groups for which they're an owner and approve requests from other users to join their groups.

Here are some more details about these group settings:

- These settings can take up to 15 minutes to take effect.
- If you want to enable some, but not all, of your users to create groups, you can assign those users a role that can create groups, such as [Groups Administrator](#).
- These settings are for users and don't affect service principals. For example, if you had a service principal with permissions to create groups, even if you set these

settings to **No**, the service principal can still create groups.

Configure group settings by using Microsoft Graph

To configure the **Users can create Microsoft 365 groups in Azure portals, API or PowerShell** setting by using Microsoft Graph, configure the `EnableGroupCreation` object in the `groupSettings` object. For more information, see [Overview of group settings](#).

To configure the **Users can create security groups in Azure portals, API or PowerShell** setting by using Microsoft Graph, update the `allowedToCreateSecurityGroups` property of `defaultUserRolePermissions` in the `authorizationPolicy` object.

Next steps

For more information on Microsoft Entra ID, see:

- [Manage access to resources with Microsoft Entra groups](#)
- [Microsoft Entra cmdlets for configuring group settings](#)
- [Application management in Microsoft Entra ID](#)
- [What is Microsoft Entra ID?](#)
- [Integrate your on-premises identities with Microsoft Entra ID](#)

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)

Assign sensitivity labels to Microsoft 365 groups in Microsoft Entra ID

Article • 03/25/2025

Microsoft Entra ID supports applying [sensitivity labels](#) to Microsoft 365 groups when those labels are published in the [Microsoft Purview portal](#) or the [Microsoft Purview compliance portal](#) and the labels are configured for groups and sites.

Sensitivity labels can be applied to groups across apps and services such as Outlook, Microsoft Teams, and SharePoint. For more information, see [Support for sensitivity labels](#) from the Purview documentation.

ⓘ Important

To configure this feature, there must be at least one active Microsoft Entra ID P1 license in your Microsoft Entra organization.

Enable sensitivity label support in PowerShell

To apply published labels to groups, you must first enable the feature. These steps enable the feature in Microsoft Entra ID. The Microsoft Graph PowerShell SDK comes in two modules, `Microsoft.Graph` and `Microsoft.Graph.Beta`.

All Microsoft operated regions should choose Microsoft. All other regions should choose their operator if one is listed.

Microsoft

1. Open a PowerShell prompt on your computer and install the Graph modules required to run the cmdlets.

PowerShell

```
Install-Module Microsoft.Graph -Scope CurrentUser  
Install-Module Microsoft.Graph.Beta -Scope CurrentUser
```

2. Connect to your tenant.

PowerShell

```
Connect-MgGraph -Scopes "Directory.ReadWrite.All"
```

3. Fetch the current group settings for the Microsoft Entra organization and display the current group settings.

PowerShell

```
$grpUnifiedSetting = Get-MgBetaDirectorySetting | Where-Object {  
    $_.Values.Name -eq "EnableMIPLabels" }  
$grpUnifiedSetting.Values
```

If no group settings were created for this Microsoft Entra organization, you get an empty screen. In this case, you must first create the settings. Follow the steps in [Microsoft Entra cmdlets for configuring group settings](#) to create group settings for this Microsoft Entra organization.

 **Note**

If the sensitivity label was enabled previously, you see `EnableMIPLabels = True`. In this case, you don't need to do anything. Also make sure that `EnableGroupCreation = False` if you don't want non-admin users to be able to create groups. See [Template settings](#) for details.

4. Apply the new settings.

PowerShell

```
$params = @{  
    Values = @(  
        @{  
            Name = "EnableMIPLabels"  
            Value = "True"  
        }  
    )  
}  
  
Update-MgBetaDirectorySetting -DirectorySettingId  
$grpUnifiedSetting.Id -BodyParameter $params
```

5. Verify that the new value is present.

PowerShell

```
$Setting = Get-MgBetaDirectorySetting -DirectorySettingId  
$grpUnifiedSetting.Id  
$Setting.Values
```

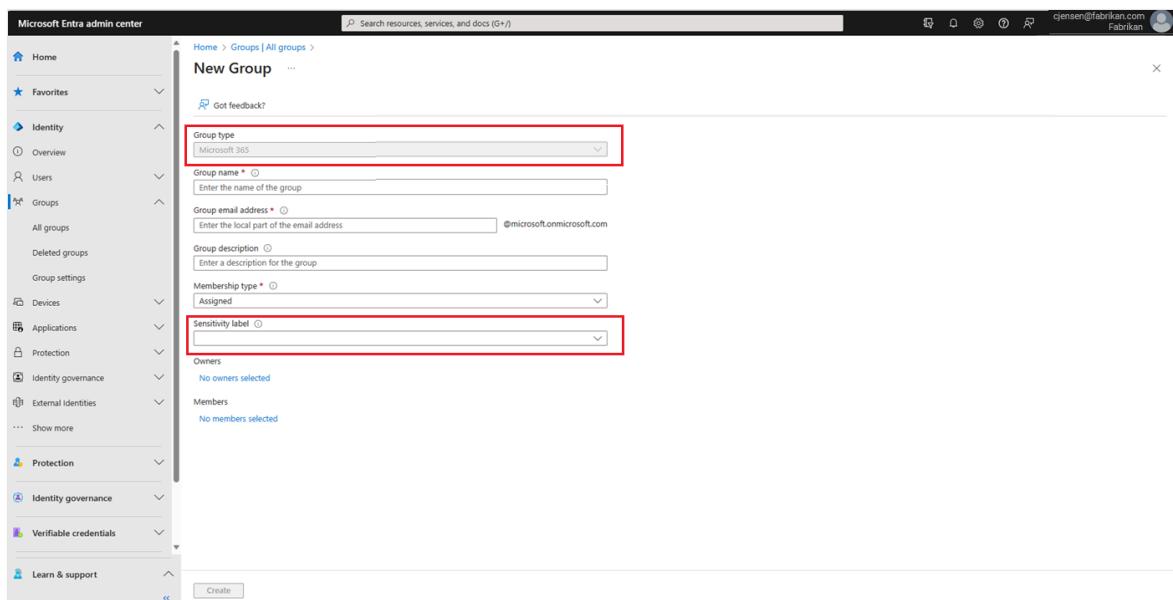
If you receive a `Request_BadRequest` error, it's because the settings already exist in the tenant. When you try to create a new `property:value` pair, the result is an error. In this case, follow these steps:

1. Issue a `Get-MgBetaDirectorySetting | FL` cmdlet and check the ID. If several ID values are present, use the one where you see the `EnableMIPLabels` property on the **Values** settings.
2. Issue the `Update-MgBetaDirectorySetting` cmdlet by using the ID that you retrieved.

You also need to synchronize your sensitivity labels to Microsoft Entra ID. For instructions, see [Enable sensitivity labels for containers and synchronize labels](#).

Assign a label to a new group in the Microsoft Entra admin center

1. Sign in to the Microsoft Entra admin center [↗](#) as at least a [Groups Administrator](#).
2. Select Microsoft Entra ID.
3. Select Groups > All groups > New group.
4. On the New Group page, select Microsoft 365. Then fill out the required information for the new group and select a sensitivity label from the list.



5. Select **Create** to save your changes.

Your group is created and the site and group settings associated with the selected label are then automatically enforced.

Assign a label to an existing group in the Microsoft Entra admin center

1. Sign in to the [Microsoft Entra admin center](#) as at least a **Groups Administrator**.
2. Select **Microsoft Entra ID**.
3. Select **Groups**.
4. From the **All groups** page, select the group that you want to label.
5. On the selected group's page, select **Properties** and select a sensitivity label from the list.

The screenshot shows the 'A' Project Team Properties page. The 'Properties' tab is selected. The 'Sensitivity label' dropdown is open, showing 'Confidential\Internal only'. The 'Members' tab is also highlighted with a red box.

6. Select **Save** to save your changes.

Remove a label from an existing group in the Microsoft Entra admin center

1. Sign in to the Microsoft Entra admin center [↗](#) as at least a **Groups Administrator**.
2. Select **Microsoft Entra ID**.
3. Select **Groups > All groups**.
4. On the **All groups** page, select the group that you want to remove the label from.
5. On the **Group** page, select **Properties**.
6. Select **Remove**.
7. Select **Save** to apply your changes.

Use classic Microsoft Entra classifications

After you enable this feature, the "classic" classifications for groups appear only on existing groups and sites. You should use them for new groups only if you create groups in apps that don't support sensitivity labels. Your admin can convert them to sensitivity labels later, if needed. Classic classifications are the old classifications you set up previously. When this feature is enabled, those classifications aren't applied to groups.

Troubleshooting issues

This section offers troubleshooting tips for common issues.

Sensitivity labels aren't available for assignment on a group

The sensitivity label option appears for groups only when all the following conditions are met:

1. The organization has an active Microsoft Entra ID P1 license.
2. The feature is enabled and `EnableMIPLabels` is set to **True** in the Microsoft Graph PowerShell module.
3. The sensitivity labels are published in the Microsoft Purview portal or the Microsoft Purview compliance portal for this Microsoft Entra organization.
4. Labels are synchronized to Microsoft Entra ID with the `Execute-AzureAdLabelSync` cmdlet in the Security & Compliance PowerShell module. It can take up to 24 hours after synchronization for the label to be available to Microsoft Entra ID.
5. The **sensitivity label scope** must be configured for Groups & Sites.
6. The group is a Microsoft 365 group.
7. The current signed-in user:
 - a. Has sufficient privileges to assign sensitivity labels. The user must be the group owner or at least a Groups Administrator.
 - b. Must be within the scope of the **sensitivity label publishing policy**.

Make sure all the preceding conditions are met to assign labels to a group.

The label you want to assign isn't in the list

If the label you're looking for isn't in the list:

- The label might not be published in the Microsoft Purview portal or the Microsoft Purview compliance portal. Also, the label might no longer be published. Check with your administrator for more information.
- The label might be published, but it isn't available to the user who is signed in. Check with your administrator for more information on how to get access to the label.

Change the label on a group

Labels can be swapped at any time by using the same steps as assigning a label to an existing group:

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Groups Administrator](#).
2. Select **Microsoft Entra ID**.
3. Select **Groups > All groups**, and then select the group that you want to label.
4. On the selected group's page, select **Properties** and select a new sensitivity label from the list.
5. Select **Save**.

Group setting changes to published labels aren't updated on the groups

When you make changes to group settings for a published label in the [Microsoft Purview portal](#) or the [Microsoft Purview compliance portal](#), those policy changes aren't automatically applied on the labeled groups. After the sensitivity label is published and applied to groups, Microsoft recommends that you don't change the group settings for the label in the portal.

If you must make a change, use a [PowerShell script](#) to manually apply updates to the affected groups. This method makes sure that all existing groups enforce the new setting.

Next steps

- Use sensitivity labels to protect content in Microsoft Teams, Microsoft 365 groups, and SharePoint sites
 - Update groups after label policy change manually with Azure AD PowerShell script ↗
 - Edit your group settings
 - Manage groups using PowerShell commands
-

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"/> (<i>Microsoft Entra Global Administrator accounts only</i>)	<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				✓	✓
Custom caller ID for phone calls				✓	✓
Trusted IPs				✓	✓
Remember MFA for trusted devices		✓	✓	✓	✓
MFA for on- premises applications				✓	✓
Conditional Access				✓	✓
Risk-based Conditional Access					✓
Self-service password reset (SSPR)	✓	✓	✓	✓	✓
SSPR with writeback				✓	✓

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 associated with identity governance are available with each license. For more information on other features, see [Microsoft Entra plans and pricing](#). 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					

Feature	Free	Microsoft Entra ID P1	Microsoft Entra ID P2	Microsoft Entra ID Governance	Microsoft Entra Suite
Entitlement management - Directly Assign Any User (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)					

Feature	Free	Microsoft Entra ID P1	Microsoft Entra ID P2	Microsoft Entra ID Governance	Microsoft Entra Suite
LCW + Custom Extensions (Logic Apps)				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Identity governance dashboard	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<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](#).

Related content

- [Microsoft Entra pricing](#)

Assign licenses to users by group membership using the Microsoft 365 admin center

Article • 01/15/2025

This article shows you how to use the Microsoft 365 license center to assign licenses to security groups.

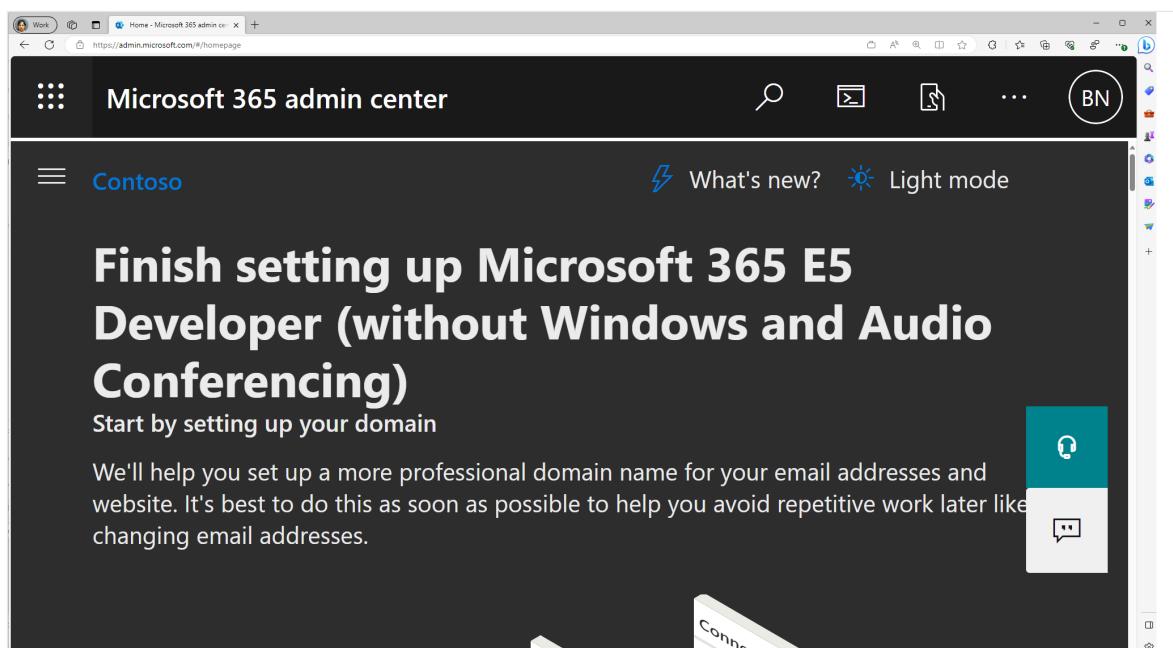
ⓘ Note

Some Microsoft services aren't available in all locations. Before a license can be assigned to a user, the administrator has to specify the Usage location property on the user.

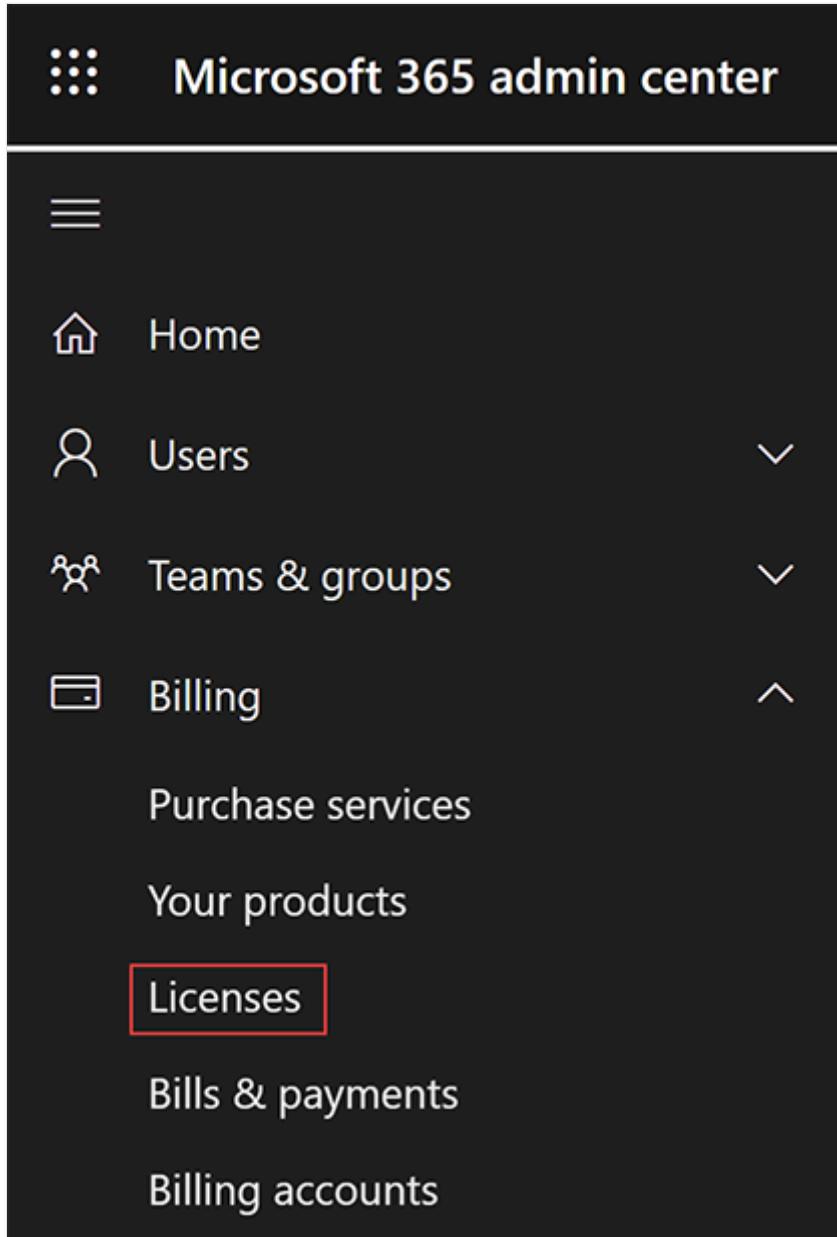
For group license assignment, any users without a usage location specified inherit the location of the directory. If you have users in multiple locations, we recommend that you always set usage location as part of your user creation flow in Microsoft Entra ID. For example, configure Microsoft Entra Connect configuration to set usage location. This recommendation makes sure the result of license assignment is always correct and users don't receive services in locations that aren't allowed.

Assign a license

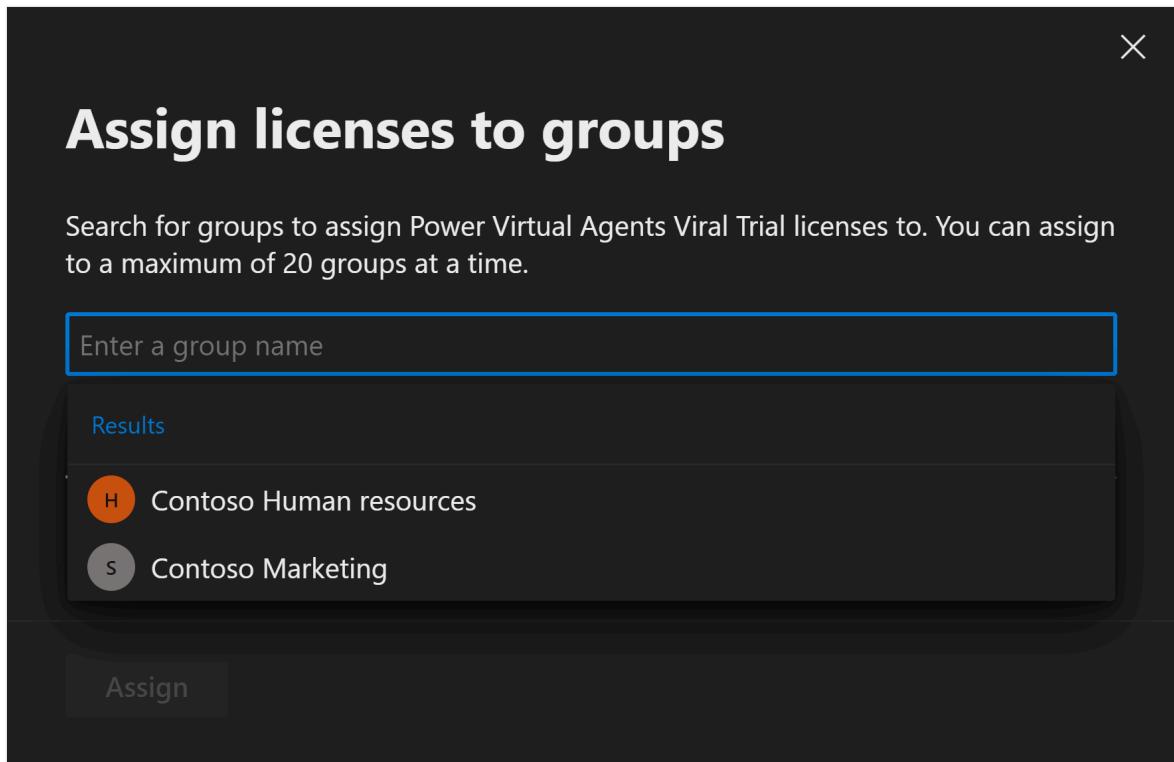
1. Sign in to the [Microsoft 365 admin center](#) as at least a [License Administrator](#).



2. Browse to **Billing > Licenses** to open a page where you can see all licenses available in your organization.



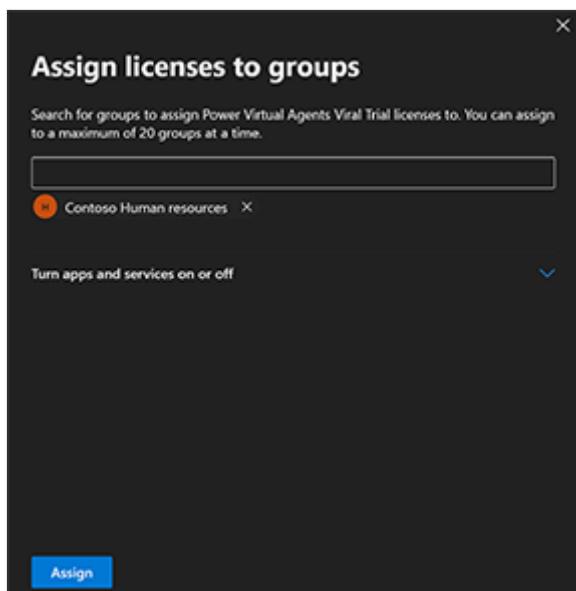
3. Under **Licenses**, select the license that you would like to assign.
4. In the License details section, choose **Groups** at the top of the page.
5. Choose **+ Assign licenses**
6. From the **+ Assign licenses** page search for the group that you would like to use for license assignment.



ⓘ Note

When assigning licenses to a group with service plans that have dependencies on other service plans, they must both be assigned together in the same group, otherwise the service plan with the dependency will be disabled.

7. To complete the assignment, on the **Assign license** page, select **Assign** at the bottom of the page.



When assign licenses to a group, Microsoft Entra ID processes all existing members of that group. This process might take some time depending on the size of the group.



! You assigned licenses to Contoso Human resources

Licenses are being assigned to Contoso Human resources, it might take a moment for the process to complete. The assignment and its status will appear in the groups list shortly. Feel free to close this panel.

Verify that the initial assignment finished

1. From the Admin Center, go to **Billing > Licenses**. Select the license that you assigned.
2. On the **License details** page, you can view the status of the license assignment operation. For example, in the image shown, you can see that **Contoso marketing** shows a status of **All licenses assigned** while **Contoso human resources** shows a status of **In progress**.

The screenshot shows the 'Groups' tab selected in the navigation bar. A message at the top says, 'You can now manage, and view licenses assigned to groups.' Below this, there are two buttons: '+ Assign licenses' and 'Refresh'. The main area displays a table with two rows:

<input type="checkbox"/>	Name ↑	Status
<input type="checkbox"/>	Contoso Human resources	: In progress
<input type="checkbox"/>	Contoso marketing	: All licenses assigned

[Read this section](#) to learn more about how audit logs can be used to analyze changes made by group-based licensing.

License assignment move to the Microsoft 365 admin center

Upcoming changes to license assignment processes, and move to the Microsoft 365 admin center require changes to the way you manage licenses. This section covers the reasons for the change, the timeline, license assignments options, and addresses common questions and known issues.

Why is this change happening?

This update is designed to streamline the license management process within the Microsoft ecosystem.

When are these changes happening?

The changes will start taking effect from September 9, and will complete by September 15.

How do I use MS Graph/PowerShell to assign licenses?

You can assign licenses using PowerShell or Microsoft Graph by following the detailed guides available on the Microsoft Learn website for user and group license assignments.

- [Assign Microsoft 365 licenses to user accounts with PowerShell](#)
- [Assign licenses to users with Microsoft Graph v1.0](#)
- [Assign Licenses to a Group with Microsoft Graph API](#)

Are license assignment audit logs affected?

There are no changes to the audit logs and you can still see all assigned licenses in the Microsoft Entra Admin Center.

Is there any loss of functionality with this change?

No. There's no loss of functionality. This change is limited to the user interface. API and PowerShell access remain unaffected. However to assign licenses to a group via the Microsoft 365 Admin Center, the admin must have the License Administrator role. Group Administrators can still assign Group based licenses using the API and PowerShell.

The admin portal doesn't provide functionality to reprocess group licenses.

The "reprocessing" button was originally introduced to address an issue with conversion between user and group based licensing. When debugging licensing issues, you can still reprocess users via Microsoft Graph and PowerShell using one of the following options:

- Use the Microsoft Graph PowerShell SDK module:

PowerShell

```
Import-Module Microsoft.Graph.Users.Actions  
Invoke-MgLicenseUser -UserId $userId
```

- Use the REST API directly

PowerShell

```
Invoke-MgGraphRequest -Uri  
"https://graph.microsoft.com/v1.0/users/$userid/reprocessLicense"
```

What if I don't have a Microsoft 365 Admin account or license and I manage licenses from the Azure portal?

For non-Microsoft 365 users, transitioning to managing licenses through a Microsoft 365 Admin Center account is essential.

Microsoft Entra ID roles: Global Administrator, User Administrator, and License Administrator have access to the Microsoft 365 Admin Center to manage licenses using their existing Microsoft Entra ID account. You don't have to be a Microsoft 365 customer to use the Microsoft 365 admin center. You don't have to be a Microsoft 365 customer to use the Microsoft 365 admin center, and can manage licenses there regardless. You don't have to be a Microsoft 365 customer to use the Microsoft 365 admin center, and can manage licenses there regardless. All Microsoft Entra customers have access to the Microsoft 365 Admin Center for domain and license management.

How can I view license consumption and utilization now?

License consumption and utilization can still be viewed in the Microsoft 365 Admin Center under **Billing -> Licenses**.

Who should I contact if I need help with these changes?

For questions, engage with community experts via Microsoft Questions and Answers. If you need technical assistance and have a support plan, you can create a support request.

For detailed instructions on assigning licenses, visit the [Microsoft 365 Admin Center guide](#).

Known Issues:

- Users with the Group Administrator role won't be able to assign licenses in the Microsoft 365 Admins Center.
 - This functionality was fully supported in both the Azure portal and Microsoft Entra admin center.
 - PowerShell continues to support the use of the Group Administrator role for license assignment.
 - Alternatively Group Administrators can be given the Licenses Administrator role in order to assign group based Licenses from the Microsoft 365 Admin Portal.
- We are loosing some detailed group license assignments logging. The Azure portal was able to provide a detailed error to administrators.

Next steps

To learn more about the feature set for license assignment using groups, see the following articles:

- [What is group-based licensing in Microsoft Entra ID?](#)
- [Identifying and resolving license problems for a group in Microsoft Entra ID](#)
- [Scenarios, limitations, and known issues using groups to manage licensing in Microsoft Entra ID](#)

Feedback

Was this page helpful?



[Provide product feedback ↗](#)

Scenarios, limitations, and known issues using groups to manage licensing in Microsoft Entra ID

Article • 01/15/2025

Use the following information and examples to gain a more advanced understanding of group-based licensing in Microsoft Entra ID, part of Microsoft Entra.

Usage location

Tip

Steps in this article might vary slightly based on the portal you start from.

Some Microsoft services aren't available in all locations. For group license assignment, any users without a usage location specified inherit the location of the directory. If you have users in multiple locations, make sure to reflect that correctly in your user resources before adding users to groups with licenses. Before a license can be assigned to a user, the administrator should specify the **Usage location** property on the user.

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Groups Administrator](#).
2. Select Microsoft Entra ID.
3. Go to **Users > All users** and select a user.

4. Select **Edit properties**.
5. Select the **Settings** tab and enter a location for the user.
6. Select the **Save** button.

Note

Group license assignment never modifies an existing usage location value on a user. We recommend that you always set usage location as part of your user creation flow in Microsoft Entra ID (for example, via [Microsoft Entra Connect](#) configuration). Following such a process ensures the result of license assignment is always correct, and users don't receive services in locations that aren't allowed.

Use group-based licensing with dynamic membership groups

You can use group-based licensing with any security group, including dynamic membership groups. Rules for dynamic membership groups are run against user resource attributes to automatically add and remove members. Attributes can be department, job title, work location, or other custom attribute. Each group is assigned the licenses that you want members to receive. If an attribute changes, the member leaves the group, and the licenses are removed.

You can assign the attribute on-premises and sync it with Microsoft Entra ID, or you can manage the attribute directly in the cloud.

Warning

Use caution when modifying an existing group's membership rule. When a rule is changed, the membership of the group is re-evaluated. Users who no longer match the new rule are removed (users who still match the new rule aren't affected during this process). Those users have their licenses removed during the process which could result in loss of service, or in some cases, loss of data.

If you have a large dynamic group you depend on for license assignment, consider validating any major changes on a smaller test group before applying them to the main group. If you encounter errors during your test, see [Resolve group license problems](#).

Multiple groups and multiple licenses

A user can be a member of multiple groups with licenses. Here are some things to consider:

- Multiple licenses for the same product can overlap, and they result in all enabled services being applied to the user. An example could be that *M365-P1* contains the foundational services to deploy to all users, and *M365-P2* contains the P2 services to deploy only to some users. You can add a user to one or both groups and only use one license for the product.
- Select a license to see more details, such as information on the services activated for the user by the group license assignment.

Direct licenses coexist with group licenses

When a user inherits a license from a group, you can't directly remove or modify that license in the user's properties. You can change the license assignment only in the group and the changes are then propagated to all group members. If you need to assign other features to a user that has their license from a group license assignment, you must create another group to assign the other features to the user.

When you use group-based licensing, consider the following scenarios:

- Group members inherit licenses assigned to the group.
- License options for group-based licenses must be changed at the group level.
- If different license options need to be assigned to a user, create a new group, assign a license to the group, then add the user to that group.

- Users still use only one license of a product if different license options for that product are used in the different group-based licenses.

When you use direct assignment, the following operations are allowed:

- Licenses not already assigned through group-based licensing can be changed for an individual user.
- Other services can be enabled, as part of a directly assigned license.
- Directly assigned licenses can be removed and don't affect a user's inherited licenses.

Managing new services added to products

When Microsoft adds a new service to a product license plan, it's enabled by default in all groups used to assign the product license. Users in your organization who are subscribed to notifications about product changes receive emails ahead of time notifying them about the upcoming service additions.

As an administrator, you can review all groups affected by the change and take action, such as disabling the new service in each group. For example, if you created groups targeting only specific services for deployment, you can revisit those groups and make sure that any newly added services are disabled.

Here's an example of what this process may look like:

1. Originally, you assigned the *Microsoft 365 E5* product to several groups. One of those groups, called *Microsoft 365 E5 - Exchange only* was designed to enable only the *Exchange Online (Plan 2)* service for its members.
2. You received a notification from Microsoft that the E5 product is being extended with a new service - *Microsoft Stream*. When the service becomes available in your organization, you can complete the following steps:
 3. a. Sign in to the [Microsoft Entra admin center](#)
 4. Select Microsoft Entra ID.
 5. Select **Billing > Licenses > All products** and select *Microsoft 365 Enterprise E5*, then select **Licensed Groups** to view a list of all groups with that product.
 6. Select the group you want to review (in this case, *Microsoft 365 E5 - Exchange only*). The **Licenses** tab opens. Select the E5 license to view all enabled services.

Dashboard > Company Name cDeQx > Licenses - Overview > Products > O365 E5 - Exchange only > O365 E5 - Exchange only - Licenses > Office 365 E5

Office 365 E5

[Save](#) [Discard](#) [Remove license](#)

Service	On/Off
Office 365 E5	On
Audio Conferencing	On
Azure Rights Management	On
Customer Lockbox	On
Exchange Online (Plan 2)	On
Flow for Office 365	On
Information Barriers	On
Information Protection for Office 365 - Premium	On
Information Protection for Office 365 - Standard	On
Insights by MyAnalytics	On
Microsoft Forms (Plan E5)	On
Microsoft Kaizala Pro	On
Microsoft MyAnalytics (Full)	On
Microsoft Planner	On
Microsoft StaffHub	On
Microsoft Stream for O365 E5 SKU	On
Microsoft Teams	On

- If you want to disable the new service in this group, select the On/Off toggle next to the service, and select the **Save** button to confirm the change. Microsoft Entra ID now processes all users in the group to apply the change; any new users added to the group won't have the *Microsoft Stream* service enabled.

! Note

Users may still have the service enabled through some other license assignment (another group they are members of or a direct license assignment).

- If needed, perform the same steps for other groups with this product assigned.

Use PowerShell to view inherited and direct license assignments

You can use a PowerShell script to check if users have a license assigned directly or inherited from a group.

- Run the `Connect-MgGraph -Scopes "Organization.Read.All"` cmdlet to authenticate and connect to your organization using Microsoft Graph.

2. `Get-MgSubscribedSku -All | Select-Object skuid -ExpandProperty serviceplans | select serviceplanid, serviceplanname` can be used to discover all provisioned product licenses in the Microsoft Entra organization.

```
PS C:\> Get-MgSubscribedSku -All | Select-Object skuid -ExpandProperty serviceplans | select serviceplanid, serviceplanname
ServicePlanId          ServicePlanName
-----
f6de4823-28fa-440b-b886-4783fa86ddba M365_AUDIT_PLATFORM
b76fb638-6ba6-402a-b9f9-83d28acb3d86 VIVA_LEARNING_SEEDED
db4d623d-b514-490b-b7ef-8885eee514de Nucleus
cd31b152-6326-4d1b-ae1b-997b625182e6 MIP_S_Exchange
a413a9ff-720c-4822-98ef-2f37c2a21f4c MICROSOFT_COMMUNICATION_COMPLIANCE
a6520331-d7d4-4276-95f5-15c0933bc757 GRAPH_CONNECTORS_SEARCH_INDEX
d9fa6af4-e046-4c89-9226-729a0786685d Content_Explorer
ded3d325-1bdc-453e-8432-5bac26d7a014 POWER_VIRTUAL_AGENTS_0365_P3
afa73018-811e-46e9-988ff-f75d2b1b8430 CDS_0365_P3
b21a6b06-1988-436e-a07b-51ec6d9f252ad PROJECT_0365_P3
d587c7a3-bda9-4f99-8776-9bcf59c84f73 INSIDER_RISK
531ee2f8-b1cb-453b-9c21-d2180d014ca5 EXCEL_PREMIUM
bf28f719-7844-4079-9c78-c1307898e192 MTP
94065c59-bc8e-4eb8-89e5-5138d471eaff MICROSOFT_SEARCH
28b0fa46-c39a-4188-89e2-58e979a6b014 DYN365_CDS_0365_P3
199a5c09-e0ca-4e37-8f7c-b05d533e1ea2 MICROSOFTBOOKINGS
65cc641f-cccd-4643-97e0-a17e3045e54f RECORDS_MANAGEMENT
d2d51368-76c9-4317-adca-2a12c004c432f ML_CLASSIFICATION
9d0c4ee5-e4a1-4625-ab39-d82b619b1a34 INSIDER_RISK_MANAGEMENT
e26c2fcc-ab91-4a61-b35c-03cdc8ddf66 INFO_GOVERNANCE
46129a58-a698-46f0-aab5-17f6586297d9 DATA_INVESTIGATIONS
6db1f1db-2b46-403f-be40-e39395f08dbb CUSTOMER_KEY
6dc145d6-95dd-4191-b9c3-185575ee6f6b COMMUNICATIONS_DLP
41fcdd7d-4733-4863-9cf4-c65b83ce2df4 COMMUNICATIONS_COMPLIANCE
bf6f5520-59e3-4f82-974b-7dbbc4fd27c7 SAFEDOCS
2f442157-allc-46b9-ae5b-6e39ff4e5849 M365_ADVANCED_AUDITING
7547a3fe-08ee-4ccb-b430-5077c5041653 YAMMER_ENTERPRISE
4a51bca5-1eff-43f5-878c-177680f191af WHITEBOARD_PLAN3
3fb26009-8c27-4f7b-bd51-30634711ee67 BPOS_S_TODO_3
a23b959c-7ce8-4e57-9140-b90e0b88a9e97 SWAY
0feaeb32-d00e-4d66-bd5a-43b5b83db82c MCOSTANDARD
5dbe027f-2339-4123-9542-606e4d348a72 SHAREPOINTENTERPRISE
9c0dab89-a30c-4117-86e7-97bda240acd2 POWERAPPS_0365_P3
```

3. Use the *ServicePlanId* value for the license you're interested in with [this PowerShell script](#). A list populates the users who have this license and information about how the license is assigned.

Use Audit logs to monitor group-based licensing activity

You can use [Microsoft Entra audit logs](#) to see all activity related to group-based licensing, including:

- who changed licenses on groups
- when the system started processing a group license change, and when it finished
- what license changes were made to a user as a result of a group license assignment.

Audit logs related to group-based licensing can be accessed from the Audit logs in the Groups or Licensing areas of Microsoft Entra ID or use the following filter combinations from the main Audit logs:

- **Service:** Core Directory
- **Category:** GroupManagement or UserManagement

The screenshot shows the Microsoft Entra ID Audit logs interface. On the left, there's a sidebar with various log categories like Cross-tenant synchronization, Microsoft Entra Connect, and Audit logs (which is selected and highlighted with a red box). The main area has a header with 'Date : Last 24 hours', 'Show dates as : Local', and 'Service : Core Directory' (also highlighted with a red box). Below that are filters for 'Category : GroupManagement' and 'Activity : All', along with an 'Add filters' button. A large table lists audit log entries with columns for Date, Category, Activity, and Status. One row in the table is highlighted with a red box, showing a 'Category' of 'GroupManagement'. The table also includes rows for other categories like Device, DeviceConfiguration, and Policy.

Find out who modified a license

1. To see the logs for group license changes, use the following Audit log filter options:
 - **Service:** Core Directory
 - **Category:** GroupManagement
 - **Activity:** Set group license
2. Select a row in the resulting table to view the details.
3. Select the **Modified Properties** tab see the old and new values for the license agreement.

The following example shows the filter settings listed above, plus the *Target* filter set to all groups that start with "EMS."

Home >

Contoso | Audit logs

Microsoft - Microsoft Entra ID for workforce

Download Export Data Settings Refresh Columns Got feedback?

Date : Last 24 hours Show dates as : Local Service : Core Directory Category : GroupManagement

Activity : Set group license Target starts with EMS Add filters

Date	Service	Category	Activity	Status	Target(s)
12/6/2022, 9:39:36 AM	Core Directory	GroupManagement	Set group license	Success	EMS-P2
12/6/2022, 9:39:21 AM	Core Directory	GroupManagement	Set group license	Success	EMS-P1
12/6/2022, 9:36:58 AM	Core Directory	GroupManagement	Set group license	Success	EMS-P1
12/6/2022, 9:36:09 AM	Core Directory	GroupManagement	Set group license	Success	EMS-P2
12/6/2022, 9:31:14 AM	Core Directory	GroupManagement	Set group license	Success	EMS-ALI

To see license changes for a specific user, use the following filters:

- **Service:** Core Directory
- **Category:** UserManagement
- **Activity:** Change user license

Find out when group changes started and finished processing

When a license changes on a group, Microsoft Entra ID starts applying the changes to all users, but the changes could take time to process.

1. To see when groups started processing, use the following filters:
 - **Service:** Core Directory
 - **Category:** GroupManagement
 - **Activity:** Start applying group based license to users
2. Select a row in the resulting table to view the details.
3. Select the **Modified Properties** tab see the license changes that were picked up for processing.
 - Use these details if you're making multiple changes to a group and aren't sure which license processed.
 - The actor for the operation is *Microsoft Entra group-Based Licensing*, which is a system account that is used to execute all group license changes.

To see when groups finished processing, change the **Activity** filter to *Finish applying group based license to users*. In this case, the **Modified Properties** field contains a

summary of the results, which is useful to quickly check if processing resulted in any errors. Sample output:

```
Modified Properties
...
Name : Result
Old Value : []
New Value : [Users successfully assigned licenses: 6, Users for whom
license assignment failed: 0.];
```

To see the complete log for how a group was processed, including all user changes, add the following filters:

- **Target:** Group name
- **Initiated By (Actor):** Microsoft Entra group-Based Licensing (case-sensitive)
- **Date Range (optional):** Custom range for when you know a specific group started and finished processing

This image shows licensing change processing from start to finish.

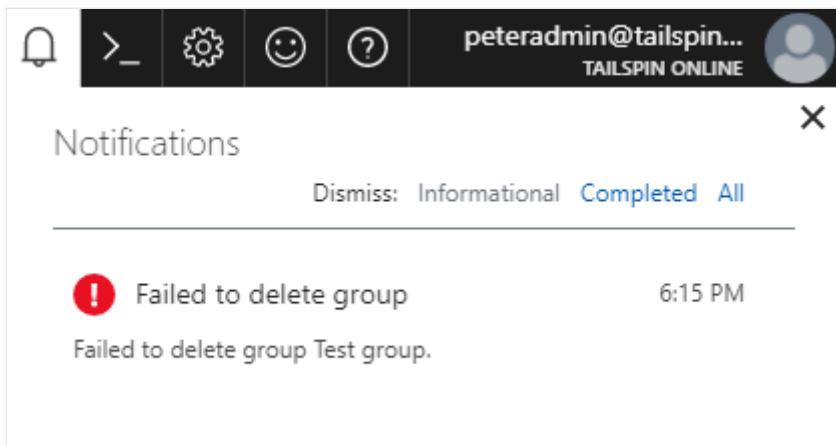
The screenshot shows the Microsoft Entra Audit logs interface for the Contoso tenant. The top navigation bar includes 'Home >', the tenant name 'Contoso | Audit logs', and a 'Microsoft - Microsoft Entra ID for workforce' link. Below the navigation are standard UI elements: 'Download', 'Export Data Settings', 'Refresh', 'Columns', and 'Got feedback?'. The main search/filter area contains 'Date : Last 24 hours', 'Show dates as : Local', 'Service : Core Directory', 'Category : GroupManagement', 'Activity : All', and two active filters: 'Initiated by (actor) starts with Microsoft Entra ID' and 'Target starts with EMS-P2'. A 'Add filters' button is also present. The data table below has columns: Date, Service, Category, Activity, Status, Target(s), and Initiated by (actor). Two rows of data are shown, both timestamped at 12/6/2022, 9:36:30 AM, under the 'Core Directory' service and 'GroupManagement' category. The first row's activity is 'Start applying group based license to u...' and its status is 'Success'. The second row's activity is 'Finish applying group based license to ...' and its status is also 'Success'. Both rows have 'EMS-P2' listed under 'Target(s)' and 'Microsoft Entra ID Group-Based Licensing' under 'Initiated by (actor)'. The 'Status' column for both rows is highlighted with a red box.

Date	Service	Category	Activity	Status	Target(s)	Initiated by (actor)
12/6/2022, 9:36:30 AM	Core Directory	GroupManagement	Start applying group based license to u...	Success	EMS-P2	Microsoft Entra ID Group-Based Licensing
12/6/2022, 9:36:30 AM	Core Directory	GroupManagement	Finish applying group based license to ...	Success	EMS-P2	Microsoft Entra ID Group-Based Licensing

Deleting a group with an assigned license

It isn't possible to delete a group with an active license assigned. The reason is to prevent the unintended deletion of a group used for license assignment. For this reason we require any licenses to be removed from the group first, before it can be deleted.

When trying to delete a group in the portal, you may see an error notification like this:



Go to the **Licenses** tab on the group and see if there are any licenses assigned. If yes, remove those licenses and try to delete the group again.

You may see similar errors when trying to delete the group through PowerShell or Graph API. If you're using a group synced from on-premises, Microsoft Entra Connect may also report errors if it's failing to delete the group in Microsoft Entra ID. In all such cases, make sure to check if there are any licenses assigned to the group, and remove them first.

Limitations and known issues

If you use group-based licensing, it's a good idea to familiarize yourself with the following list of limitations and known issues.

- Group-based licensing currently doesn't support groups that contain other groups (nested groups). If you apply a license to a nested group, only the immediate first-level user members of the group have the licenses applied.
- The feature can only be used with security groups, and Microsoft 365 groups that have `securityEnabled=TRUE`.
- When licenses are assigned or modified for a large group (for example, 100,000 users), it could affect performance. Specifically, the volume of changes generated by Microsoft Entra automation might negatively affect the performance of your directory synchronization between Microsoft Entra ID and on-premises systems.
- If you're using dynamic membership groups to manage your users' memberships, verify that the user is part of the group, which is necessary for license assignment. If not, [check processing status for the membership rule](#) of the dynamic group.
- In certain high load situations, it may take a long time to process license changes for groups or membership changes to groups with existing licenses. If you see your

changes take more than 24 hours to process group size of 60 K users or less, please [open a support ticket](#) to allow us to investigate.

Next steps

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

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

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)

Group-based licensing PowerShell examples

Article • 03/20/2025

Group-based licensing in Microsoft Entra ID, part of Microsoft Entra, is available through the [Azure portal](#). There are useful tasks that can be performed using [Microsoft Graph PowerShell Cmdlets](#).

In this article, we go over some examples using Microsoft Graph PowerShell.

⚠️ Warning

These samples are provided for demonstration purposes only. We recommend testing them on a smaller scale or in a separate test environment before relying on them in your production environment. You can modify the samples to meet your specific environment's requirements.

Before you begin running cmdlets, make sure you connect to your organization first, by running the `Connect-MgGraph` cmdlet-.

Assign licenses to a group

[Group based licensing](#) provides a convenient way to manage license assignment. You can assign one or more product licenses to a group and those licenses are assigned to all members of the group.

PowerShell

```
# Import the Microsoft.Graph.Groups module
Import-Module Microsoft.Graph.Groups
# Define the group ID - replace with your actual group ID
$groupId = "11111111-1111-1111-1111-111111111111"

# Create a hashtable to store the parameters for the Set-MgGroupLicense
# cmdlet
$params = @{
    AddLicenses = @(
        @{
            # Remove the DisabledPlans key as we don't need to disable any
            # service plans
            # Specify the SkuId of the license you want to assign
            SkuId = "11111111-1111-1111-1111-111111111111"
        }
    )
}
```

```

        )
    # Keep the RemoveLicenses key empty as we don't need to remove any
    licenses
    RemoveLicenses = @(
        )
    }

# Call the Set-MgGroupLicense cmdlet to update the licenses for the
# specified group
# Replace $groupId with the actual group ID
Set-MgGroupLicense -GroupId $groupId -BodyParameter $params

```

View product licenses assigned to a group

PowerShell

The [\[Get-MgGroup\]\(\)](#)[\(/powershell/module/microsoft.graph.groups/get-mggroup\)](#) cmdlet can be used to retrieve the group object and check the *AssignedLicenses* property: it lists all product licenses currently assigned to the group.

```

```powershell
Define the group ID
$groupId = "99c4216a-56de-42c4-a4ac-e411cd8c7c41"

Get the group with the specified ID and its assigned licenses
$group = Get-MgGroup -GroupId $groupId -Property "AssignedLicenses"

Extract the assigned licenses
$assignedLicenses = $group | Select-Object -ExpandProperty AssignedLicenses

Extract the SKU IDs from the assigned licenses
$skuIds = $assignedLicenses | Select-Object -ExpandProperty SkuId

For each SKU ID, get the corresponding SKU part number
$skuPartNumbers = $skuIds | ForEach-Object {
 $skuId = $_
 $subscribedSku = Get-MgSubscribedSku | Where-Object { $_.SkuId -eq
$skuId }
 $skuPartNumber = $subscribedSku | Select-Object -ExpandProperty
SkuPartNumber
 $skuPartNumber
}

Output the SKU part numbers
$skuPartNumbers

```

This output is what the results look like:

## Output

```
SkuPartNumber

ENTERPRISEPREMIUM
EMSPREMIUM
```

# Get all groups with assigned licenses

You can find all groups with any license assigned by running the following command:

## PowerShell

```
Get-MgGroup -All -Property Id, MailNickname, DisplayName, GroupTypes,
Description, AssignedLicenses | Where-Object {$_._AssignedLicenses -ne $null
}
```

More details can be displayed about what products are assigned:

## PowerShell

```
Get all groups with assigned licenses
$groups = Get-MgGroup -All -Property Id, MailNickname, DisplayName,
GroupTypes, Description, AssignedLicenses | Where-Object
{$_._AssignedLicenses -ne $null }

Process each group
$groupInfo = foreach ($group in $groups) {
 # For each group, get the SKU part numbers of the assigned licenses
 $skuPartNumbers = foreach ($skuId in $group.AssignedLicenses.SkuId) {
 $subscribedSku = Get-MgSubscribedSku | Where-Object { $_.SkuId -eq
$skuId }
 $subscribedSku.SkuPartNumber
 }

 # Create a custom object with the group's object ID, display name, and
 # license SKU part numbers
 [PSCustomObject]@{
 ObjectId = $group.Id
 DisplayName = $group.DisplayName
 Licenses = $skuPartNumbers -join ', '
 }
}

$groupInfo
```

This output is what the results look like:

## Output

Id	DisplayName
AssignedLicenses	
--	-----
--	-----
7023a314-6148-4d7b-b33f-6c775572879a	EMS E5 - Licensed users
cf41f428-3b45-490b-b69f-a349c8a4c38e	PowerBi - Licensed users
POWER_BI_STANDARD	
962f7189-59d9-4a29-983f-556ae56f19a5	0365 E3 - Licensed users
c2652d63-9161-439b-b74e-fcd8228a7074	EMSSandOffice
{ENTERPRISEPREMIUM, EMSPREMIUM}	

## View all disabled service plan licenses assigned to groups

### PowerShell

```
$groups = Get-MgGroup -All
$groupsWithLicenses = @()

foreach ($group in $groups) {
 $licenses = Get-MgGroup -GroupId $group.Id -Property "AssignedLicenses, Id,
 DisplayName" |
 Select-Object AssignedLicenses, DisplayName, Id

 if ($licenses.AssignedLicenses) {
 foreach ($license in $licenses.AssignedLicenses) {
 $skuId = $license.SkuId
 $disabledPlans = $license.DisabledPlans

 $skuDetails = Get-MgSubscribedSku | Where-Object { $_.SkuId -eq
$skuId }
 $skuPartNumber = $skuDetails.SkuPartNumber

 $disabledPlanDetails = @()
 if ($disabledPlans.Count -gt 0) {
 foreach ($planId in $disabledPlans) {
 $planDetails = $skuDetails.ServicePlans | Where-Object {
 $_.ServicePlanId -eq $planId }

 if ($planDetails) {
 $disabledPlanDetails += "$($planDetails.ServicePlanName)
($planId)"
 }
 }
 } else {
 $disabledPlanDetails = "None"
 }
 }
 }
}
```

```

 $groupsWithLicenses += [PSCustomObject]@{
 GroupObjectId = $group.Id
 DisplayName = $group.DisplayName
 SkuId = $skuId
 SkuPartNumber = $skuPartNumber
 DisabledPlans = ($disabledPlanDetails -join ", ")
 }
 }
}

Export to CSV
$csvPath = "$env:USERPROFILE\Documents\GroupLicenses.csv"
$groupsWithLicenses | Export-Csv -Path $csvPath -NoTypeInformation -Encoding UTF8

Write-Host "Export completed: $csvPath"

```

## Get statistics for groups with licenses

PowerShell

```

Import User Graph Module
Import-Module Microsoft.Graph.Users
Authenticate to MS Graph
Connect-MgGraph -Scopes "User.Read.All", "Directory.Read.All",
"Group.ReadWrite.All"
#get all groups with licenses
$groups = Get-MgGroup -All -Property LicenseProcessingState, DisplayName,
Id, AssignedLicenses | Select-Object displayname, Id,
LicenseProcessingState, AssignedLicenses | Select-Object DisplayName, Id,
AssignedLicenses -ExpandProperty LicenseProcessingState | Select-Object
DisplayName, State, Id, AssignedLicenses | Where-Object {$_.State -eq
"ProcessingComplete"}
$groupInfoArray = @()
Filter the groups to only include those that have licenses assigned
$groups = $groups | Where-Object {$_.AssignedLicenses -ne $null}
For each group, get the group name, license types, total user count,
licensed user count, and license error count
foreach ($group in $groups) {
 $groupInfo = New-Object PSObject
 $groupInfo | Add-Member -MemberType NoteProperty -Name "Group Name" -
Value $group.DisplayName
 $groupInfo | Add-Member -MemberType NoteProperty -Name "Group ID" -Value
$group.Id
 $groupInfo | Add-Member -MemberType NoteProperty -Name "License Types" -
Value ($group.AssignedLicenses | Select-Object -ExpandProperty SkuId)
 $groupInfo | Add-Member -MemberType NoteProperty -Name "Total User
Count" -Value (Get-MgGroupMember -GroupId $group.Id -All | Measure-
Object).Count
 $groupInfo | Add-Member -MemberType NoteProperty -Name "Licensed User
Count" -Value (Get-MgGroupMember -GroupId $group.Id -All | Where-Object {$_.

```

```

LicenseProcessingState -eq "ProcessingComplete"} | Measure-Object).Count
$groupInfo | Add-Member -MemberType NoteProperty -Name "License Error
Count" -Value (Get-MgGroupMember -GroupId $group.Id -All | Where-Object
{$_._LicenseProcessingState -eq "ProcessingFailed"} | Measure-Object).Count
$groupInfoArray += $groupInfo
}

Format the output and print it to the console
$groupInfoArray | Format-Table -AutoSize

```

## Get all groups with license errors

PowerShell

```

Get all groups that have assigned licenses
$groups = Get-MgGroup -All -Property DisplayName, Id, AssignedLicenses |
 Where-Object { $_.AssignedLicenses -ne $null } |
 Select-Object DisplayName, Id, AssignedLicenses

Initialize an array to store group information
$groupInfo = @()

Iterate over each group
foreach ($group in $groups) {
 $groupId = $group.Id
 $groupName = $group.DisplayName

 # Initialize counters for total members and members with license errors
 $totalCount = 0
 $licenseErrorCount = 0

 # Get all members of the group that have license errors
 $members = Get-MgGroupMemberWithLicenseError -GroupId $groupId

 # Process each member
 foreach ($member in $members) {
 $totalCount++

 # If the member has a license error (indicated by a non-empty Id),
 increment the error count
 if (![[string]::IsNullOrEmpty($member.Id)) {
 $licenseErrorCount++
 }
 }

 # Create a custom object with the group's information and counts
 $groupInfo += [PSCustomObject]@{
 GroupName = $groupName
 GroupId = $groupId
 TotalUserCount = $totalCount
 LicenseErrorCount = $licenseErrorCount
 }
}

```

```

 }

Display the groups with licensing errors
$groupInfo | Where-Object { $_.LicenseErrorCount -gt 0 } | Format-Table -
Property GroupName, GroupId, TotalUserCount, LicenseErrorCount

```

## Get all users with license errors in a group

Given a group that contains some license-related errors, you can now list all users affected by those errors. A user can have errors from other groups, too. However, in this example we limit results only to errors relevant to the group in question by checking the **ReferencedObjectId** property of each **IndirectLicenseError** entry on the user.

PowerShell

```

Import necessary modules
Import-Module Microsoft.Graph.Users
Import-Module Microsoft.Graph.Groups

Specify the group ID you want to check
$groupId = "ENTER-YOUR-GROUP-ID-HERE"

Authenticate to Microsoft Graph
Connect-MgGraph -Scopes "Group.Read.All", "User.Read.All"

Get the specified group
$group = Get-MgGroup -GroupId $groupId -Property DisplayName, Id,
AssignedLicenses
Write-Host "Checking license errors for group: $($group.DisplayName)" -
ForegroundColor Cyan

Initialize output array
$groupInfoArray = @()

Get all members from the group and check their license status
$groupMembers = Get-MgGroupMember -GroupId $group.Id -All
$errorCount = 0

Process each member
foreach ($memberId in $groupMembers.Id) {
 # Get user details
 $user = Get-MgUser -UserId $memberId -Property DisplayName, Id,
LicenseAssignmentStates

 # Check for license errors
 $licenseErrors = $user.LicenseAssignmentStates | Where-Object {
 $_.AssignedByGroup -eq $groupId -and $_.Error -ne "None"
 }

 if ($licenseErrors) {

```

```

$errorCount++
$userInfo = [PSCustomObject]@{
 GroupName = $group.DisplayName
 GroupId = $group.Id
 UserName = $user.DisplayName
 UserId = $user.Id
 Error = ($licenseErrors.Error -join ", ")
 ErrorSubcode = ($licenseErrors.ErrorSubcode -join ", ")
}
$groupInfoArray += $userInfo
}

Summary
Write-Host "Found $errorCount users with license errors in group $($group.DisplayName)" -ForegroundColor Yellow

Format the output and print it to the console

if ($groupInfoArray.Length -gt 0) {
 $groupInfoArray | Format-Table -AutoSize
}
else {
 Write-Host "No License Errors"
}

```

## Get all users with license errors in the entire organization

The following script can be used to get all users who have license errors from one or more groups. The script prints one row per user, per license error, which allows you to clearly identify the source of each error.

PowerShell

```

Connect to Microsoft Graph
Connect-MgGraph -Scopes "User.Read.All", "Directory.Read.All",
"Organization.Read.All"

Retrieve all SKUs in the tenant
$skus = Get-MgSubscribedSku -All | Select-Object SkuId, SkuPartNumber

Retrieve all users in the tenant with required properties
$users = Get-MgUser -All -Property AssignedLicenses,
LicenseAssignmentStates, DisplayName, Id, UserPrincipalName

Initialize an empty array to store the user license information
$allUserLicenses = @()

```

```

foreach ($user in $users) {
 # Initialize a hash table to track all assignment methods for each license
 $licenseAssignments = @{}
 $licenseErrors = @()

 # Loop through license assignment states
 foreach ($assignment in $user.LicenseAssignmentStates) {
 $skuId = $assignment.SkuId
 $assignedByGroup = $assignment.AssignedByGroup
 $assignmentMethod = if ($assignedByGroup -ne $null) {
 # If the license was assigned by a group, get the group name
 $group = Get-MgGroup -GroupId $assignedByGroup
 if ($group) { $group.DisplayName } else { "Unknown Group" }
 } else {
 # If the license was assigned directly by the user
 "User"
 }

 # Check for errors in the assignment state and capture them
 if ($assignment.Error -ne $null -or $assignment.ErrorSubcode -ne $null) {
 $errorDetails = @{
 Error = $assignment.Error
 ErrorSubcode = $assignment.ErrorSubcode
 SkuId = $skuId
 AssignedBy = $assignmentMethod
 }
 $licenseErrors += $errorDetails
 }

 # Ensure all assignment methods are captured
 if (-not $licenseAssignments.ContainsKey($skuId)) {
 $licenseAssignments[$skuId] = @($assignmentMethod)
 } else {
 $licenseAssignments[$skuId] += $assignmentMethod
 }
 }

 # Process assigned licenses
 foreach ($skuId in $licenseAssignments.Keys) {
 # Get SKU details from the pre-fetched list
 $sku = $skus | Where-Object { $_.SkuId -eq $skuId } | Select-Object -First 1
 $skuPartNumber = if ($sku) { $sku.SkuPartNumber } else { "Unknown SKU" }

 # Sort and join the assignment methods
 $assignmentMethods = ($licenseAssignments[$skuId] | Sort-Object -Unique) -join ", "

 # Clean up license errors to make them more legible
 $errorDetails = if ($licenseErrors.Count -gt 0) {
 $errorMessage = $licenseErrors | Where-Object { $_.SkuId -eq $skuId } | ForEach-Object {

```

```

 # Check if error or subcode are empty, and filter them out
 if ($_.Error -ne "None" -and $_.ErrorSubcode) {
 "$($_.AssignedBy): Error: $($_.Error) Subcode:
$($_.ErrorSubcode)"
 } elseif ($_.Error -ne "None") {
 "$($_.AssignedBy): Error: $($_.Error)"
 } elseif ($_.ErrorSubcode) {
 "$($_.AssignedBy): Subcode: $($_.ErrorSubcode)"
 }
 }

 # Join filtered error messages into a clean output
 $errorMessages -join "; "
} else {
 "No Errors"
}

Construct a custom object to store the user's license information
$userLicenseInfo = [PSCustomObject]@{
 UserId = $user.Id
 UserDisplayName = $user.DisplayName
 UserPrincipalName = $user.UserPrincipalName
 SkuId = $skuId
 SkuPartNumber = $skuPartNumber
 AssignedBy = $assignmentMethods
 LicenseErrors = $errorDetails
}
}

Add the user's license information to the array
$allUserLicenses += $userLicenseInfo
}
}

Export the results to a CSV file
$path = Join-path $env:LOCALAPPDATA ("UserLicenseAssignments_" + [string]
(Get-Date -UFormat %Y%m%d) + ".csv")
$allUserLicenses | Export-Csv $path -Force -NoTypeInformation

Display the location of the CSV file
Write-Host "CSV file generated at: $((Get-Item $path).FullName)"

```

### ⓘ Note

This script retrieves a list of all licensed users in your environment, showing which licenses are assigned and the method of assignment. In the results, where "AssignedBy" shows "User", it indicates a direct license assignment. Where "SkuPartNumber" shows "Unknown SKU", it indicates the specific license SKU is disabled in your tenant. The script exports the complete results to a CSV file in your local AppData folder for further analysis.

# Check if user license is assigned directly or inherited from a group

PowerShell

```
Retrieve all SKUs in the tenant
$skus = Get-MgSubscribedSku -All | Select-Object SkuId, SkuPartNumber

Retrieve all users in the tenant with required properties
$users = Get-MgUser -All -Property AssignedLicenses,
LicenseAssignmentStates, DisplayName, Id, UserPrincipalName

Initialize an empty array to store the user license information
$allUserLicenses = @()

foreach ($user in $users) {
 # Initialize a hash table to track all assignment methods for each
 # license
 $licenseAssignments = @{}

 # Loop through license assignment states
 foreach ($assignment in $user.LicenseAssignmentStates) {
 $skuId = $assignment.SkuId
 $assignedByGroup = $assignment.AssignedByGroup
 $assignmentMethod = if ($assignedByGroup -ne $null) {
 # If the license was assigned by a group, get the group name
 $group = Get-MgGroup -GroupId $assignedByGroup
 if ($group) { $group.DisplayName } else { "Unknown Group" }
 } else {
 # If the license was assigned directly by the user
 "User"
 }

 # Ensure all assignment methods are captured
 if (-not $licenseAssignments.ContainsKey($skuId)) {
 $licenseAssignments[$skuId] = @($assignmentMethod)
 } else {
 $licenseAssignments[$skuId] += $assignmentMethod
 }
 }

 # Process assigned licenses
 foreach ($skuId in $licenseAssignments.Keys) {
 # Get SKU details from the pre-fetched list
 $sku = $skus | Where-Object { $_.SkuId -eq $skuId } | Select-Object
 -First 1
 $skuPartNumber = if ($sku) { $sku.SkuPartNumber } else { "Unknown
SKU" }

 # Sort and join the assignment methods
 $assignmentMethods = ($licenseAssignments[$skuId] | Sort-Object -
 Unique) -join ", "
 }
}
```

```

Construct a custom object to store the user's license information
$userLicenseInfo = [PSCustomObject]@{
 UserId = $user.Id
 UserDisplayName = $user.DisplayName
 UserPrincipalName = $user.UserPrincipalName
 SkuId = $skuId
 SkuPartNumber = $skuPartNumber
 AssignedBy = $assignmentMethods
}

Add the user's license information to the array
$allUserLicenses += $userLicenseInfo
}

}

Export the results to a CSV file
$path = Join-path $env:LOCALAPPDATA ("UserLicenseAssignments_" + [string]
(Get-Date -UFormat %Y%m%d) + ".csv")
$allUserLicenses | Export-Csv $path -Force -NoTypeInformation

Display the location of the CSV file
Write-Host "CSV file generated at: $((Get-Item $path).FullName)"

```

## Remove direct licenses for users with group licenses

The purpose of this script is to remove unnecessary direct licenses from users who already inherit the same license from a group; for example, as part of a [transition to group-based licensing](#).

### Note

To ensure that users don't lose access to services and data, it's important to confirm that directly assigned licenses don't provide more service functionality than the inherited licenses. It isn't currently possible to use PowerShell to determine which services are enabled through inherited licenses versus direct licenses. Therefore, the script uses a minimum level of services that are known to be inherited from groups to check and ensure that users don't experience unexpected service loss.

## Variables

- `$GroupLicenses`: Represents the licenses assigned to the group.
- `$GroupMembers`: Contains the members of the group.

- `$UserLicenses`: Holds the licenses directly assigned to a user.
- `$DirectLicensesToRemove`: Stores the licenses that need to be removed from the user.

PowerShell

```
Define the group ID containing the assigned license
$GroupId = "objectID of Group"

Force all errors to be terminating errors
$ErrorActionPreference = "Stop"

Get the group's assigned licenses
$Group = Get-MgGroup -GroupId $GroupId -Property AssignedLicenses
$GroupLicenses = $Group.AssignedLicenses.SkuId

if (-not $GroupLicenses) {
 Write-Host "No licenses assigned to the specified group. Exiting
script."
 return
}

Get all members of the group
$GroupMembers = Get-MgGroupMember -GroupId $GroupId -All

foreach ($User in $GroupMembers) {
 $UserId = $User.Id

 # Get user's assigned licenses
 $UserData = Get-MgUser -UserId $UserId -Property
 DisplayName,Mail,UserPrincipalName,AssignedLicenses
 $UserLicenses = $UserData.AssignedLicenses.SkuId

 # Identify direct licenses that match the group's assigned licenses
 $DirectLicensesToRemove = @()
 foreach ($License in $UserLicenses) {
 if ($GroupLicenses -contains $License) {
 $DirectLicensesToRemove += $License
 }
 }

 # Print user info before taking action
 Write-Host ("{} {} {} {}" -f $UserData.Id,
 $UserData.DisplayName, $UserData.Mail, $UserData.UserPrincipalName)

 # Skip users who have no direct licenses matching the group
 if ($DirectLicensesToRemove.Count -eq 0) {
 Write-Host "No direct licenses to remove. (Only inherited licenses
detected)"
 Write-Host -----
 continue
 }
}
```

```

Attempt to remove direct licenses
try {
 Write-Host "Removing direct license(s)..."
 Set-MgUserLicense -UserId $UserId -RemoveLicenses
$DirectLicensesToRemove -AddLicenses @() -ErrorAction Stop
 Write-Host "✓ License(s) removed successfully."
}
catch {
 $ErrorMessage = $_.Exception.Message

 if ($ErrorMessage -match "User license is inherited from a group membership") {
 Write-Host "⚠️ Skipping removal - License is inherited from a group."
 } else {
 Write-Host "✗ Unexpected error: $ErrorMessage"
 }
}
Write-Host "-----"
}

Write-Host "Script execution complete."

```

## Next steps

To learn more about the feature set for license management through groups, see the following articles:

- [What is group-based licensing in Microsoft Entra ID?](#)
- [Assigning licenses to a group in Microsoft Entra ID](#)
- [Identifying and resolving license problems for a group in Microsoft Entra ID](#)

## Feedback

Was this page helpful?



[Provide product feedback ↗](#)

# Product names and service plan identifiers for licensing

Article • 04/08/2025

When [managing licenses in the Azure portal](#) or the [Microsoft 365 admin center](#), you see product names that look something like *Office 365 E3*. When you use PowerShell v1.0 cmdlets, the same product is identified using a specific but less friendly name: *ENTERPRISEPACK*. When using PowerShell v2.0 cmdlets or [Microsoft Graph](#), the same product is identified using a GUID value: *6fd2c87f-b296-42f0-b197-1e91e994b900*. The following table lists the most commonly used Microsoft online service products and provides their various ID values. These tables are for reference purposes in Microsoft Entra ID, part of Microsoft Entra, and are accurate only as of the date when this article was last updated. Microsoft will continue to make periodic updates to this document.

- **Product name:** Used in management portals
- **String ID:** Used by PowerShell v1.0 cmdlets when performing operations on licenses or by the **skuPartNumber** property of the **subscribedSku** Microsoft Graph API
- **GUID:** GUID used by the **skuid** property of the **subscribedSku** Microsoft Graph API
- **Service plans included:** A list of service plans in the product that correspond to the string ID and GUID
- **Service plans included (friendly names):** A list of service plans (friendly names) in the product that correspond to the string ID and GUID

## ⓘ Note

This information was last updated on March 26, 2025.  
You can also download a CSV version of this table [here](#).

 Expand table

Product name	String ID	GUID
10-Year Audit Log Retention Add On	10_ALR_ADDON	c2e41e49-e2a2-4c55-832a-cf13ffba1d6a
Advanced Communications	ADV_COMMS	e4654015-5daf-4a48-9b37-4f309dddd88b
AI Builder Capacity add-on	CDSAICAPACITY	d2dea78b-507c-4e56-b400-39447f4738f8
App Connect IW	SPZA_IW	8f0c5670-4e56-4892-b06d-91c085d7004f
App governance add-on to Microsoft Defender for Cloud Apps	Microsoft_Cloud_App_Security_App_Governance_Add_On	9706eed9-966f-4f1b-94f6-bb2b4af99a5b
Microsoft 365 Audio Conferencing	MCOMEETADV	0c266dff-15dd-4b49-8397-2bb16070ed52
Microsoft 365 Audio Conferencing for faculty	MCOMEETADV_FACULTY	c2cda955-3359-44e5-989f-852ca0cfa02f
Microsoft Entra Basic	AAD_BASIC	2b9c8e7c-319c-43a2-a2a0-48c5c6161de7

Product name	String ID	GUID
Microsoft Entra ID P1	AAD_PREMIUM	078d2b04-f1bd-4111-bbd4-b4b1b354cef4
Microsoft Entra ID P1 for faculty	AAD_PREMIUM_FACULTY	30fc3c36-5a95-4956-ba57-c09c2a600bb9
Microsoft Entra ID P1_USGOV_GCCHIGH	AAD_PREMIUM_USGOV_GCCHIGH	de597797-22fb-4d65-a9fe-b7dbe8893914
Microsoft Entra ID P2	AAD_PREMIUM_P2	84a661c4-e949-4bd2-a560-ed7766fcacf2b
Azure Information Protection Plan 1	RIGHTSMANAGEMENT	c52ea49f-fe5d-4e95-93ba-1de91d380f89
Azure Information Protection Plan 1	RIGHTSMANAGEMENT_CE	a0e6a48f-b056-4037-af70-b9ac53504551
Azure Information Protection Premium P1 for Government	RIGHTSMANAGEMENT_CE_GOV	78362de1-6942-4bb8-83a1-a32aa67e6e2c
Azure Information Protection Premium P1_USGOV_GCCHIGH	RIGHTSMANAGEMENT_CE_USGOV_GCCHIGH	c57afa2a-d468-46c4-9a90-f86cb1b3c54a
Basic Collaboration	OFFICEBASIC	4468c39a-28b2-42fb-9094-840bcf28771f

Product name	String ID	GUID
Business Apps (free)	SMB_APPS	90d8b3f8-712e-4f7b-aa1e-62e7ae6cbe96
Career Coach for faculty	CAREERCOACH_FACULTY	95de1760-7682-406d-98c9-52ef14e51e2b
Career Coach for students	CAREERCOACH_STUDENTS	01c8007a-57d2-41e0-a3c3-0b46ead16cc4
Clipchamp Premium	Clipchamp_Premium	0fe440c5-f2bf-442b-a4f4-9a7af77a200b
Clipchamp Standard	Clipchamp_Standard	481f3bc2-5756-4b28-9375-5c8c86b99e6b
Common Data Service for Apps File Capacity	CDS_FILE_CAPACITY	631d5fb1-a668-4c2a-9427-8830665a742e
Common Data Service Database Capacity	CDS_DB_CAPACITY	e612d426-6bc3-4181-9658-91aa906b0ac0
Common Data Service Database Capacity for Government	CDS_DB_CAPACITY_GOV	eddf428b-da0e-4115-accf-b29eb0b83965
Common Data Service Log Capacity	CDS_LOG_CAPACITY	448b063f-9cc6-42fc-a0e6-40e08724a395
Communications Credits	MCOPSTNC	47794cd0-f0e5-45c5-9033-2eb6b5fc84e0
Compliance Manager Premium Assessment Add-On	CMPA_addon	8a5fbbed-8b8c-41e5-907e-c50c471340fd
Compliance Manager Premium Assessment Add-On for GCC	CMPA_addon_GCC	a9d7ef53-9bea-4a2a-9650-fa7df58fe094
Copilot for Microsoft 365	Microsoft_365_Copilot	639dec6b-bb19-468b-871c-c5c441c4b0cb

Product name	String ID	GUID
Defender Threat Intelligence	Defender_Threat_Intelligence	a9c51c15-ffad-4c66-88c0-8771455c832d
Digital Messaging for GCC Test SKU	MESSAGING_GCC_TEST	064a9707-9dba-4cc1-9902-38bfcfda6328
Dynamics 365 - Additional Database Storage (Qualified Offer)	CRMSTORAGE	328dc228-00bc-48c6-8b09-1fbcb8bc3435d
Dynamics 365 - Additional Production Instance (Qualified Offer)	CRMINSTANCE	9d776713-14cb-4697-a21d-9a52455c738a
Dynamics 365 - Additional Non-Production Instance (Qualified Offer)	CRMTESTINSTANCE	e06abcc2-7ec5-4a79-b08b-d9c282376f72
Dynamics 365 AI for Market Insights (Preview)	SOCIAL_ENGAGEMENT_APP_USER	c6df1e30-1c9f-427f-907c-3d913474a1c7
Dynamics 365 Asset Management Addl Assets	DYN365_ASSETMANAGEMENT	673afb9d-d85b-40c2-914e-7bf46cd5cd75
Dynamics 365 Business Central Additional Environment Addon	DYN365_BUSCENTRAL_ADD_ENV_ADDON	a58f5506-b382-44d4-bfab-225b2fbf8390
Dynamics 365 Business Central Database Capacity	DYN365_BUSCENTRAL_DB_CAPACITY	7d0d4f9a-2686-4cb8-814c-efff3fdab6d74
Dynamics 365 Business Central Essentials	DYN365_BUSCENTRAL_ESSENTIAL	2880026b-2b0c-4251-

Product name	String ID	GUID
		8656- 5d41ff11e3aa
Dynamics 365 Business Central Essentials Attach	Dynamics_365_Business_Central_Essentials_Attach	1d506c23- 1702-46f1- b940- 160c55f98d05
Dynamics 365 Business Central External Accountant	DYN365_FINANCIALS_ACCOUNTANT_SKU	9a1e33ed- 9697-43f3- b84c- 1b0959dbb1d4
Dynamics 365 Business Central for IWs	PROJECT_MADEIRA_PREVIEW_IW_SKU	6a4a1628- 9b9a-424d- bed5- 4118f0ede3fd
Dynamics 365 Business Central Premium	DYN365_BUSCENTRAL_PREMIUM	f991cecc-3f91- 4cd0-a9a8- bf1c8167e029
Dynamics 365 Business Central Team Members	DYN365_BUSCENTRAL_TEAM_MEMBER	2e3c4023- 80f6-4711- aa5d- 29e0ecb46835
Dynamics 365 Commerce	DYN365_RETAIL	79909bd8- 4c69-4202- 939e- 11bc4385b134

Product name	String ID	GUID
Dynamics 365 Commerce Trial	DYN365_RETAIL_TRIAL	1508ad2d-5802-44e6-bfe8-6fb65de63d28
Dynamics 365 Plan 1 Enterprise Edition	DYN365_ENTERPRISE_PLAN1	ea126fc5-a19e-42e2-a731-da9d437bfff
Dynamics 365 Customer Insights Attach	DYN365_CUSTOMER_INSIGHTS_ATTACH	a3d0cd86-8068-4071-ad40-4dc5b5908c4b
Dynamics 365 Customer Insights Standalone	DYN365_CUSTOMER_INSIGHTS_BASE	0c250654-c7f7-461f-

Product name	String ID	GUID
		871a- 7222f6592cf2
Dynamics 365 Customer Insights vTrial	DYN365_CUSTOMER_INSIGHTS_VIRAL	036c2481- aa8a-47cd- ab43- 324f0c157c2d
Dynamics 365 for Customer Service Chat for Government	DYN365_CS_CHAT_GOV	1b399f66- be2a-479c- a79d- 84a43a46f79e
Dynamics 365 for Customer Service Digital Messaging add-on for Government	DYN365_CS_MESSAGING_GOV	336dfe1f- 3b33-4ab4- b395- cba8f614976d
Dynamics 365 Customer Service Digital Messaging and Voice Add-in for Government	DYN365_CS_OC_MESSAGING_VOICE_GOV	6ec542c9- 2a86-4d4a- 8a52- d233eb58ef0a
Dynamics 365 Customer Service Digital Messaging and Voice Add-in for Government for Test	DYN365_CS_OC_MESSAGING_VOICE_GOV_TEST	ea9ba490- 50b8-474e- 8671- 9fec0f1268f3

Product name	String ID	GUID
Dynamics 365 Customer Service Enterprise Viral Trial	Dynamics_365_Customer_Service_Enterprise_viral_trial	1e615a51-59db-4807-9957-aa83c3657351
Dynamics 365 for Customer Service Enterprise Attach to Qualifying Dynamics 365 Base Offer A	D365_CUSTOMER_SERVICE_ENT_ATTACH	eb18b715-ea9d-4290-9994-2ebf4b5042d2
Dynamics 365 Customer Service Insights Trial	DYN365_AI_SERVICE_INSIGHTS	61e6bd70-fbdb-4deb-82ea-912842f39431
Dynamics 365 Customer Voice Trial	FORMS_PRO	bc946dac-7877-4271-b2f7-99d2db13cd2c
Dynamics 365 Customer Service Professional	DYN365_CUSTOMER_SERVICE_PRO	1439b6e2-5d59-4873-8c59-d60e2a196e92
Dynamics 365 Customer Voice	DYN365_CUSTOMER_VOICE_BASE	359ea3e6-8130-4a57-9f8f-ad897a0342f1
Dynamics 365 Customer Voice Additional Responses	Forms_Pro_AddOn	446a86f8-a0cb-4095-

Product name	String ID	GUID
		83b3-d100eb050e3d
Dynamics 365 Customer Voice Additional Responses	DYN365_CUSTOMER_VOICE_ADDON	65f71586-ade3-4ce1-afc0-1b452eaf3782
Dynamics 365 Customer Voice USL	Forms_Pro_USL	e2ae107b-a571-426f-9367-6d4c8f1390ba
Dynamics 365 Enterprise Edition - Additional Database Storage for Government	CRMSTORAGE_GCC	4aed5dd6-eb9c-4143-8f14-368d70287121
Dynamics 365 - Additional Non- Production Instance for Government	CRMTESTINSTANCE_NOPREREQ	2cf302fe-62db-4e20-b573-e0998b1208b5
Dynamics 365 Enterprise Edition - Additional Non-Production Instance for Government	CRMTESTINSTANCE_GCC	1d2756cb-2147-4b05-b4d5-f013c022dc9
Dynamics 365 Enterprise Edition - Additional Portal (Qualified Offer)	CRM_ONLINE_PORTAL	a4fbfb28e-becc-41b0-a454-ac680dc258d3
Dynamics 365 Enterprise Edition - Additional Portal for Government	CRM_ONLINE_PORTAL_GCC	cb9bc974-a47b-4123-998d-a383390168cc
Dynamics 365 Enterprise Edition - Additional Portal for Government	CRM_ONLINE_PORTAL_NOPREREQ	67f58b51-af53-4344-9663-9a2beb1d8a8e
Dynamics 365 Enterprise Edition - Additional Production Instance for Government	CRMINSTANCE_GCC	2bd3cb20-1bb6-446b-b4d0-089af3a05c52
Dynamics 365 Field Service Viral Trial	Dynamics_365_Field_Service_Enterprise_viral_trial	29fcfd665-d8d1-4f34-8eed-3811e3fca7b3
Dynamics 365 Finance	DYN365_FINANCE	55c9eb4e-c746-45b4-b255-9ab6b19d5c62

Product name	String ID	GUID
Dynamics 365 for Case Management Enterprise Edition	DYN365_ENTERPRISE_CASE_MANAGEMENT	d39fb075-21ae-42d0-af80-22a2599749e0
Dynamics 365 for Case Management, Enterprise Edition for Government	D365_ENTERPRISE_CASE_MANAGEMENT_GOV	5cd0b796-9ac8-4792-9f0b-796ca9044e4a
Dynamics 365 for Case Management, Enterprise Edition for Government	DYN365_ENTERPRISE_CASE_MANAGEMENT_GOV	ff5a82be-1edd-4d48-94e0-52527825b589
Dynamics 365 Customer Service Enterprise Admin	Dynamics_365_Customer_Service_Enterprise_admin_trial	94a6fb4-6a2f-4990-b356-dc7dd8bed08a

Product name	String ID	GUID
Dynamics 365 for Customer Service Enterprise Edition	DYN365_ENTERPRISE_CUSTOMER_SERVICE	749742bf-0d37-4158-a120-33567104deeb
Dynamics 365 for Customer Service, Enterprise Edition for Government	DYN365_ENTERPRISE_CUSTOMER_SERVICE_GOV	3c74d823-8f01-4fe8-82d5-f089a5504cec
Dynamics 365 for Customer Service Enterprise for Government	D365_ENTERPRISE_CUSTOMER_SERVICE_GOV	65758a5f-2e16-43b3-a8cb-296cd8f69e09

<b>Product name</b>	<b>String ID</b>	<b>GUID</b>
Dynamics 365 for Customer Service Chat	DYN365_CS_CHAT	7d7af6c2-0be6-46df-84d1-c181b0272909
Dynamics 365 for Customer Service Professional Attach to Qualifying Dynamics 365 Base Offer	D365_CUSTOMER_SERVICE_PRO_ATTACH	19dec69d-d9f3-4792-8a39-d8ecdf51937b
Dynamics 365 for Field Service Attach to Qualifying Dynamics 365 Base Offer	D365_FIELD_SERVICE_ATTACH	a36cdcaa2-a806-4b6e-9ae0-28dbd993c20e
Dynamics 365 for Field Service Enterprise Edition	DYN365_ENTERPRISE_FIELD_SERVICE	c7d15985-e746-4f01-b113-20b575898250
Dynamics 365 Field Service Contractor for Government	D365_FIELD_SERVICE_CONTRACTOR_GOV	e7965e3a-1f49-4d67-a3de-ad1ce460bbcc
Dynamics 365 Field Service, Enterprise Edition - Resource Scheduling Optimization	CRM_AUTO_ROUTING_ADDON	977464c4-bfaf-4b67-b761-a9bb735a2196
Dynamics 365 for Field Service for Government	D365_ENTERPRISE_FIELD_SERVICE_GOV	8eac9119-7e6b-4278-9dc4-e3458993b08a

Product name	String ID	GUID
Dynamics 365 for Field Service Enterprise Edition for Government	DYN365_ENTERPRISE_FIELD_SERVICE_GOV	c3d74ead- 70b7-4513- 8dce- 797be3fbe07a
Dynamics 365 for Financials Business Edition	DYN365_FINANCIALS_BUSINESS_SKU	cc13a803- 544e-4464- b4e4- 6d6169a138fa
Dynamics 365 Guides vTrial	Dynamics_365_Guides_vTrial	99cb3f83-fbec- 4aa1-8262- 9679e6df7c53
Dynamics 365 Hybrid Connector	CRM_HYBRIDCONNECTOR	de176c31- 616d-4eae- 829a- 718918d7ec23
Dynamics 365 for Marketing Additional Application	DYN365_MARKETING_APPLICATION_ADDON	99c5688b- 6c75-4496- 876f- 07f0fbdb69add
Dynamics 365 for Marketing Additional Contacts Tier 3	DYN365_MARKETING_CONTACT_ADDON_T3	23053933- 0fd4-431f- 9a5b- a00fd78444c1
Dynamics 365 for Marketing Additional Non-Prod Application	DYN365_MARKETING_SANDBOX_APPLICATION_ADDON	c393e9bd- 2335-4b46- 8b88- 9e2a86a85ec1
Dynamics 365 for Marketing Addnl Contacts Tier 5	DYN365_MARKETING_CONTACT_ADDON_T5	d8eec316- 778c-4f14- a7d1- a0aca433b4e7

<b>Product name</b>	<b>String ID</b>	<b>GUID</b>
Dynamics 365 for Marketing Attach	DYN365_MARKETING_APP_ATTACH	85430fb9-02e8-48be-9d7e-328beb41fa29
Dynamics 365 for Marketing Business Edition	DYN365_BUSINESS_MARKETING	238e2f8d-e429-4035-94db-6926be4ffe7b
Dynamics 365 for Marketing USL	D365_MARKETING_USER	4b32a493-9a67-4649-8eb9-9fc5a5f75c12
Dynamics 365 Multi-app	Dynamics_365_Multi_app_	6c75fb1b-61f2-42d0-b1b8-6492ca9ae159

<b>Product name</b>	<b>String ID</b>	<b>GUID</b>
Dynamics 365 Operations – Activity	Dyn365_Operations_Activity	b75074f1-4c54-41bf-970f-c9ac871567f5
Dynamics 365 Project Operations Attach	DYN365_PROJECT_OPERATIONS_ATTACH	af739e8e-dd11-4eb5-a986-5908f595c603
Dynamics 365 for Project Service Automation for Government	D365_ENTERPRISE_PROJECT_SERVICE_AUTOMATION_GOV	6c827f0a-42cb-4cff-b1cd-f4104c16ede3
Dynamics 365 for Project Service Automation Enterprise Edition for Government	DYN365_ENTERPRISE_PROJECT_SERVICE_AUTOMATION_GOV	1ec19b5f-7542-4b20-b01f-fb5d3f040e2d

Product name	String ID	GUID
Dynamics 365 for Sales and Customer Service Enterprise Edition	DYN365_ENTERPRISE_SALES_CUSTOMERSERVICE	8edc2cf8-6438-4fa9-b6e3-aa1660c640cc
Dynamics 365 for Sales Enterprise Edition	DYN365_ENTERPRISE_SALES	1e1a282c-9c54-43a2-9310-98ef728faace
Dynamics 365 for Sales, Enterprise Edition for Government	DYN365_ENTERPRISE_SALES_GOV	28b275ce-aec7-4c26-82e2-1ffbc2746ad4
Dynamics 365 for Sales Enterprise for Government	D365_ENTERPRISE_SALES_GOV	e85b3345-2fd5-45cf-a196-7968d3e18e56

Product name	String ID	GUID
Dynamics 365 Sales, Field Service and Customer Service Partner Sandbox	Dynamics_365_Sales_Field_Service_and_Customer_Service_Partner_Sandbox	494721b8-1f30-4315-aba6-70ca169358d9
Dynamics 365 Sales Premium	DYN365_SALES_PREMIUM	2edaa1dc-966d-4475-93d6-8ee8dfd96877
Dynamics 365 for Sales Professional	D365_SALES_PRO	be9f9771-1c64-4618-9907-244325141096
Dynamics 365 for Sales Professional for Government	D365_SALES_PRO_GOV	229fa362-9d30-4dbc-8110-21b77a7f9b26

Product name	String ID	GUID
Dynamics 365 for Sales Professional Trial	D365_SALES_PRO_IW	9c7bff7a-3715-4da7-88d3-07f57f8d0fb6
Dynamics 365 for Sales Professional Attach to Qualifying Dynamics 365 Base Offer	D365_SALES_PRO_ATTACH	245e6bf9-411e-481e-8611-5c08595e2988
Dynamics 365 for Supply Chain Management	DYN365_SCM	f2e48cb3-9da0-42cd-8464-4a54ce198ad0
Dynamics 365 for Talent	SKU_Dynamics_365_for_HCM_Trial	3a256e9a-15b6-4092-b0dc-82993f4debc6
Dynamics 365 for Team Members Enterprise Edition	DYN365_ENTERPRISE_TEAM_MEMBERS	8e7a3d30-d97d-43ab-837c-d7701cef83dc

Product name	String ID	GUID
Dynamics 365 for Team Members Enterprise Edition for Government	DYN365_ENTERPRISE_TEAM_MEMBERS_GOV	ba05762f-32ff-4fac-a096-55309b3700a3
Dynamics 365 Guides	GUIDES_USER	0a389a77-9850-4dc4-b600-bc66fdfefc60
Dynamics 365 Operations - Device	Dynamics_365_for_Operations_Devices	3bbd44ed-8a70-4c07-9088-6232ddbd5ddd
Dynamics 365 Operations - Sandbox Tier 2:Standard Acceptance Testing	Dynamics_365_for_Operations_Sandbox_Tier2_SKU	e485d696-4c87-4aac-bf4a-91b2fb6f0fa7
Dynamics 365 Operations - Sandbox Tier 4:Standard Performance Testing	Dynamics_365_for_Operations_Sandbox_Tier4_SKU	f7ad4bca-7221-452c-bdb6-3e6089f25e06
Dynamics 365 P1 Trial for Information Workers	DYN365_ENTERPRISE_P1_IW	338148b6-1b11-4102-afb9-f92b6cdc0f8d
Dynamics 365 Project Operations	DYN365_PROJECT_OPERATIONS	98619618-9dc8-48c6-

Product name	String ID	GUID
		8f0c- 741890ba5f93
Dynamics 365 Regulatory Service - Enterprise Edition Trial	DYN365_REGULATORY_SERVICE	7ed4877c- 08e3-4f69- 9187- 245487128d4f
Dynamics 365 Remote Assist	MICROSOFT_REMOTE_ASSIST	7a551360- 26c4-4f61- 84e6- ef715673e083
Dynamics 365 Remote Assist HoloLens	MICROSOFT_REMOTE_ASSIST_HOOLENS	e48328a2- 8e98-4484- a70f- a99f8ac9ec89
Dynamics 365 Sales Enterprise Attach to Qualifying Dynamics 365 Base Offer	D365_SALES_ENT_ATTACH	5b22585d- 1b71-4c6b- b6ec- 160b1a9c2323
Dynamics 365 Sales Premium Viral Trial	Dynamics_365_Sales_Premium_Viral_Trial	6ec92958- 3cc1-49db- 95bd- bc6b3798df71
Dynamics 365 for Supply Chain Management Attach to Qualifying Dynamics 365 Base Offer	DYN365_SCM_ATTACH	090b4a96- 8114-4c95- 9c91- 60e81ef53302

<b>Product name</b>	<b>String ID</b>	<b>GUID</b>
Dynamics 365 Talent: Attract	Dynamics_365_Hiring_SKU	e561871f-74fa-4f02-abee-5b0ef54dd36d
Dynamics 365 Talent: Onboard	DYNAMICS_365_ONBOARDING_SKU	b56e7ccc-d5c7-421f-a23b-5c18bdbad7c0
Dynamics 365 Team Members_wDynamicsRetail	DYN365_TEAM_MEMBERS	7ac9fe77-66b7-4e5e-9e46-10eed1cff547
Dynamics 365 UNF OPS Plan ENT Edition	Dynamics_365_for_Operations	ccba3cfe-71ef-423a-bd87-b6df3dce59a9

<b>Product name</b>	<b>String ID</b>	<b>GUID</b>
Enterprise Mobility + Security A3 for Faculty	EMS_EDU_FACULTY	aedfac18- 56b8-45e3- 969b- 53edb4ba4952
Enterprise Mobility + Security E3	EMS	efccb6f7-5641- 4e0e-bd10- b4976e1bf68e
Enterprise Mobility + Security E5	EMSPREMIUM	b05e124f- c7cc-45a0- a6aa- 8cf78c946968
Enterprise Mobility + Security E5_USGOV_GCCHIGH	EMSPREMIUM_USGOV_GCCHIGH	a461b89c- 10e3-471c- 82b8- aae4d820fccb

Product name	String ID	GUID
Enterprise Mobility + Security G3 GCC	EMS_GOV	c793db86- 5237-494e- 9b11- dcd4877c2c8c
Enterprise Mobility + Security G5 GCC	EMSPREMIUM_GOV	8a180c2b-f4cf- 4d44-897c- 3d32acc4a60b
Exchange Enterprise CAL Services (EOP, DLP)	EOP_ENTERPRISE_PREMIUM	e8ecdf70- 47a8-4d39- 9d15- 093624b7f640
Exchange Online (Plan 1)	EXCHANGESTANDARD	4b9405b0- 7788-4568- add1- 99614e613b69
Exchange Online (Plan 1) for Students	EXCHANGESTANDARD_STUDENT	ad2fe44a- 915d-4e2b- ade1- 6766d50a9d9c
Exchange Online (Plan 1) for Alumni with Yammer	EXCHANGESTANDARD_ALUMNI	aa0f9eb7-eff2- 4943-8424- 226fb137fcad

Product name	String ID	GUID
Exchange Online (PLAN 2)	EXCHANGEENTERPRISE	19ec0d23-8335-4cbd-94ac-6050e30712fa
Exchange Online (Plan 2) for Faculty	EXCHANGEENTERPRISE_FACULTY	0b7b15a8-7fd2-4964-bb96-5a566d4e3c15
Exchange Online (Plan 2) for GCC	EXCHANGEENTERPRISE_GOV	7be8dc28-4da4-4e6d-b9b9-c60f2806df8a
Exchange Online Archiving for Exchange Online	EXCHAGEARCHIVE_ADDON	ee02fd1b-340e-4a4b-b355-4a514e4c8943
Exchange Online Archiving for Exchange Server	EXCHAGEARCHIVE	90b5e015-709a-4b8b-b08e-3200f994494c
Exchange Online Essentials (ExO P1 Based)	EXCHANGEESSENTIALS	7fc0182e-d107-4556-8329-7caa511197b
Exchange Online Essentials	EXCHANGE_S_ESSENTIALS	e8f81a67-bd96-4074-b108-cf193eb9433b
Exchange Online Kiosk	EXCHANGEDECKLESS	80b2d799-d2ba-4d2a-8842-fb0d0f3a4b82
Exchange Online (Plan 1) for GCC	EXCHANGESTANDARD_GOV	f37d5ebf-4bf1-4aa2-8fa3-50c51059e983
Exchange Online POP	EXCHANGETELCO	cb0a98a8-11bc-494c-83d9-c1b1ac65327e
Exchange Online Protection	EOP_ENTERPRISE	45a2423b-e884-448d-a831-d9e139c52d2f
Intune	INTUNE_A	061f9ace-7d42-4136-88ac-31dc755f143f
Intune for Education	INTUNE_EDU	d9d89b70-a645-4c24-b041-8d3cb1884ec7

<b>Product name</b>	<b>String ID</b>	<b>GUID</b>
Microsoft Dynamics AX7 User Trial	AX7_USER_TRIAL	fecd1f9-a91e-488d-a918-a96cdb6ce2b0
Microsoft Azure Multi-Factor Authentication	MFA_STANDALONE	cb2020b1-d8f6-41c0-9acd-8ff3d6d7831b
Microsoft Defender for Office 365 (Plan 2)	THREAT_INTELLIGENCE	3dd6cf57-d688-4eed-ba52-9e40b5468c3e
Microsoft 365 A1	M365EDU_A1	b17653a4-2443-4e8c-a550-18249dda78bb
Microsoft 365 A3 for faculty	M365EDU_A3_FACULTY	4b590615-0888-425a-a965-b3bf7789848d

Product name	String ID	GUID
Microsoft 365 A3 for students	M365EDU_A3_STUDENT	7cf9a2b-e110-4c39-bf20-c6a3f36a3121

Product name	String ID	GUID
Microsoft 365 A3 student use benefits	M365EDU_A3_STUUSEBNFT	18250162-5d87-4436-

Product name	String ID	GUID
		a834- d795c15c80f3

Product name	String ID	GUID
Microsoft 365 A3 Suite features for faculty	Microsoft_365_A3_Suite_features_for_faculty	32a0e471- 8a27-4167- b24f- 941559912425
Microsoft 365 A3 - Unattended License for students use benefit	M365EDU_A3_STUUSEBNFT_RPA1	1aa94593- ca12-4254- a738- 81a5972958e8

Product name	String ID	GUID
Microsoft 365 A5 for Faculty	M365EDU_A5_FACULTY	e97c048c-37a4-45fb-ab50-922fbf07a370

Product name	String ID	GUID

Product name	String ID	GUID
Microsoft 365 A5 for students	M365EDU_A5_STUDENT	46c119d4-0379-4a9d-85e4-97c66d3f909e

Product name	String ID	GUID

Product name	String ID	GUID
Microsoft 365 A5 student use benefits	M365EDU_A5_STUUSEBNFT	31d57bc7-3a05-4867-ab53-97a17835a411

Product name	String ID	GUID
Microsoft 365 A5 Suite features for faculty	M365_A5_SUITE_COMPONENTS_FACULTY	9b8fe788- 6174-4c4e- 983b- 3330c93ec278
Microsoft 365 A5 without Audio Conferencing for students use benefit	M365EDU_A5_NOPSTNCONF_STUUSEBNFT	81441ae1- 0b31-4185- a6c0- 32b6b84d419f

Product name	String ID	GUID

Product name	String ID	GUID
Microsoft 365 Apps for Business	O365_BUSINESS	cdd28e44-67e3-425e-be4c-737fab2899d3
Microsoft 365 Apps for Business	SMB_BUSINESS	b214fe43-f5a3-4703-beeb-fa97188220fc
Microsoft 365 Apps for enterprise	OFFICESUBSCRIPTION	c2273bd0-dff7-4215-9ef5-2c7bcfb06425
Microsoft 365 Apps for enterprise (device)	OFFICE_PROPLUS_DEVICE1	ea4c5ec8-50e3-4193-89b9-50da5bd4cdc7
Microsoft 365 Apps for Faculty	OFFICESUBSCRIPTION_FACULTY	12b8c807-2e20-48fc-b453-542b6ee9d171

Product name	String ID	GUID
Microsoft 365 Apps for Students	OFFICESUBSCRIPTION_STUDENT	c32f9321-a627-406d-a114-1f9c81aaafac
Microsoft 365 Audio Conferencing for GCC	MCOMEETADV_GOV	2d3091c7-0712-488b-b3d8-6b97bde6a1f5
Microsoft 365 Audio Conferencing - GCCHigh Tenant (AR)_USGOV_GCCHIGH	MCOACBYOT_AR_GCCHIGH_USGOV_GCCHIGH	170ba00c-38b2-468c-a756-24c05037160a
Microsoft 365 Audio Conferencing_USGOV_GCCHIGH	MCOMEETADV_USGOV_GCCHIGH	4dee1f32-0808-4fd2-a2ed-fdd575e3a45f
Microsoft 365 Audio Conferencing Pay-Per-Minute - EA	MCOMEETACPEA	df9561a4-4969-4e6a-8e73-c601b68ec077
Microsoft 365 Business Basic	O365_BUSINESS_ESSENTIALS	3b555118-da6a-4418-894f-7df1e2096870

Product name	String ID	GUID
Microsoft 365 Business Basic	SMB_BUSINESS_ESSENTIALS	dab7782a-93b1-4074-8bb1-0e61318bea0b
Microsoft 365 Business Basic EEA (no Teams)	Microsoft_365_Business_Basic_EEA_(no_Teams)	b1f3042b-a390-4b56-ab61-b88e7e767a97

Product name	String ID	GUID
Microsoft 365 Business Basic (no Teams)	Microsoft_365_Business_Basic_(no Teams)	21502a13- c8dc-4744- be9c- 177fd9d2eafc

Product name	String ID	GUID
Microsoft 365 Business Standard	O365_BUSINESS_PREMIUM	f245ecc8-75af-4f8e-b61f-27d8114de5f3

Product name	String ID	GUID
Microsoft 365 Business Standard (no Teams)	MICROSOFT_365_BUSINESS_STANDARD_NO_TEAMS	5a1c7b8d-0739-4ca8-bf69-ec87e69133ac

Product name	String ID	GUID
Microsoft 365 Business Standard EEA (no Teams)	Microsoft_365_Business_Standard_EEA_(no_Teams)	ffa3a2a0-3820-462a-aa81-8a4d741f0cba

Product name	String ID	GUID
Microsoft 365 Business Standard EEA (no Teams)	Office_365_w/o_Teams_Bundle_Business_Standard	c1f79c29-5d7a-4bec-a2c1-1a76774864c0

Product name	String ID	GUID
Microsoft 365 Business Standard - Prepaid Legacy	SMB_BUSINESS_PREMIUM	ac5cef5d-921b-4f97-9ef3-c99076e5470f
Microsoft 365 Business Premium	SPB	cbdc14ab-d96c-4c30-b9f4-6ada7cdc1d46

Product name	String ID	GUID

Product name	String ID	GUID
Microsoft 365 Business Premium (no Teams)	Microsoft_365_Business_Premium_(no Teams)	00e1ec7b-e4a3-40d1-9441-b69b597ab222

Product name	String ID	GUID
Microsoft 365 Business Premium Donation	Microsoft_365_Business_Premium_Donation_(Non_Profit_Pricing)	24c35284-d768-4e53-84d9-b7ae73dddf69

Product name	String ID	GUID

Product name	String ID	GUID
Microsoft 365 Business Premium EEA (no Teams)	Office_365_w/o_Teams_Bundle_Business_Premium	a3f586b6-8cce-4d9b-99d6-55238397f77a

Product name	String ID	GUID
Microsoft 365 Business Voice (US)	BUSINESS_VOICE_MED2_TELCO	08d7bcce8- 6e16-490e- 89db- 1d508e5e9609
Microsoft 365 Business Voice (without Calling Plan)	BUSINESS_VOICE_DIRECTROUTING	d52db95a- 5ecb-46b6- beb0- 190ab5cd4a8
Microsoft 365 Business Voice	BUSINESS_VOICE_MED2	a6051f20- 9cbc-47d2- 930d- 419183bf6cf1
Microsoft 365 Business Voice (UK)	BUSINESS_VOICE	e5a17adf- 8f0d-4b57- bc14- d331235f9307

<b>Product name</b>	<b>String ID</b>	<b>GUID</b>
Microsoft 365 Copilot (Education Faculty)	Microsoft_365_Copilot_EDU	ad9c22b3- 52d7-4e7e- 973c- 88121ea96436
Microsoft 365 Copilot for Sales	Microsoft_Copilot_for_Sales	15f2e9fc-b782- 4f73-bf51- 81d8b7fff6f4
Microsoft 365 Domestic Calling Plan (120 minutes) – US	MCOPSTN5_US	d13e9d1b- 316a-4946- 98c6- 362c97a4fdfe
Microsoft 365 Domestic Calling Plan for GCC	MCOPSTN_1_GOV	923f58ab-fca1- 46a1-92f9- 89fda21238a8
Microsoft 365 E3	SPE_E3	05e9a617- 0261-4cee- bb44- 138d3ef5d965

Product name	String ID	GUID

Product name	String ID	GUID
Microsoft 365 E3 (no Teams)	Microsoft_365_E3_(no_Teams)	dcf0408c-aaec-446c-afd4-43e3683943ea

Product name	String ID	GUID
Microsoft 365 E3 EEA (no Teams)	O365_w/o Teams Bundle_M3	c2fe850d-fbbb-4858-b67d-bd0c6e746da3

Product name	String ID	GUID
Microsoft 365 E3 EEA (no Teams) - Unattended License	Microsoft_365_E3_EEA_(no_Teams)_Unattended_License	a23dbafb-3396-48b3-ad9c-a304fe206043

Product name	String ID	GUID

Product name	String ID	GUID
Microsoft 365 E3 EEA (no Teams) (500 seats min)_HUB	O365_w/o Teams Bundle_M3_(500_seats_min)_HUB	602e6573-55a3-46b1-a1a0-cc267991501a

Product name	String ID	GUID
Microsoft 365 E3 Extra Features	Microsoft_365_E3_Extra_Features	f5b15d67-b99e-406b-90f1-308452f94de6
Microsoft 365 E3 - Unattended License	SPE_E3_RPA1	c2ac2ee4-9bb1-47e4-8541-d689c7e83371

Product name	String ID	GUID

Product name	String ID	GUID
Microsoft 365 E3 (500 seats min)_HUB	Microsoft_365_E3	0c21030a-7e60-4ec7-9a0f-0042e0e0211a

Product name	String ID	GUID
Microsoft 365 E3_USGOV_DOD	SPE_E3_USGOV_DOD	d61d61cc-f992-433f-a577-5bd016037eeb
Microsoft 365 E3_USGOV_GCCHIGH	SPE_E3_USGOV_GCCHIGH	ca9d1dd9-dfe9-4fef-b97c-9bc1ea3c3658

Product name	String ID	GUID
Microsoft 365 E5	SPE_E5	06ebc4ee-1bb5-47dd-8120-11324bc54e06

Product name	String ID	GUID

Product name	String ID	GUID
Microsoft 365 E5 (500 seats min)_HUB	Microsoft_365_E5	db684ac5-c0e7-4f92-8284-ef9ebde75d33

Product name	String ID	GUID

Product name	String ID	GUID
Microsoft 365 E5 Developer (without Windows and Audio Conferencing)	DEVELOPERPACK_E5	c42b9cae- ea4f-4ab7- 9717- 81576235ccac

Product name	String ID	GUID

Product name	String ID	GUID

Product name	String ID	GUID
Microsoft 365 E5 Compliance	INFORMATION_PROTECTION_COMPLIANCE	184efa21-98c3-4e5d-95ab-d07053a96e67
Microsoft 365 E5 EEA (no Teams)	O365_w/o_Teams_Bundle_M5	3271cf8e-2be5-4a09-a549-70fd05baaa17

Product name	String ID	GUID

Product name	String ID	GUID

Product name	String ID	GUID
Microsoft 365 E5 EEA (no Teams) (500 seats min)_HUB	O365_w/o_Teams_Bundle_M5_(500_seats_min)_HUB	1e988bf3-8b7c-4731-bec0-4e2a2946600c

Product name	String ID	GUID

Product name	String ID	GUID
Microsoft 365 E5 EEA (no Teams) with Calling Minutes	Microsoft_365_E5_EEA_(no_Teams)_with_Calling_Minutes	6ee4114a-9b2d-4577-9e7a-49fa43d222d3

Product name	String ID	GUID

Product name	String ID	GUID
Microsoft 365 E5 EEA (no Teams) without Audio Conferencing	Microsoft_365_E5_EEA_(no_Teams)_without_Audio_Conferencing	90277bc7-a6fe-4181-99d8-712b08b8d32b

Product name	String ID	GUID

Product name	String ID	GUID
Microsoft 365 E5 EEA (no Teams) without Audio Conferencing (500 seats min) _HUB	Microsoft_365_E5_EEA_(no_Teams)without_Audio_Conferencing(500_seats_min)_HUB	a640eead-25f6-4bec-97e3-23cf382d7c2

Product name	String ID	GUID

Product name	String ID	GUID
Microsoft 365 E5 Security	IDENTITY_THREAT_PROTECTION	26124093-3d78-432b-b5dc-48bf992543d5

Product name	String ID	GUID
Microsoft 365 E5 Security for EMS E5	IDENTITY_THREAT_PROTECTION_FOR_EMS_E5	44ac31e7-2999-4304-ad94-c948886741d4
Microsoft 365 E5 with Calling Minutes	SPE_E5_CALLINGMINUTES	a91fc4e0-65e5-4266-aa76-4037509c1626

Product name	String ID	GUID

Product name	String ID	GUID
Microsoft 365 E5 without Audio Conferencing	SPE_E5_NOPSTNCONF	cd2925a3-5076-4233-8931-638a8c94f773

Product name	String ID	GUID

Product name	String ID	GUID

Product name	String ID	GUID
Microsoft 365 E5 without Audio Conferencing (500 seats min)_HUB	Microsoft_365_E5_without_Audio_Conferencing	2113661c-6509-4034-98bb-9c47bd28d63c

Product name	String ID	GUID

Product name	String ID	GUID
Microsoft 365 F1	M365_F1	44575883- 256e-4a79- 9da4- ebe9acabe2b2
Microsoft 365 F1 EEA (no Teams)	Microsoft_365_F1_EEA_(no_Teams)	0666269f- b167-4c5b- a76f- fc574f2b1118

Product name	String ID	GUID
Microsoft 365 F3	SPE_F1	66b55226- 6b4f-492c- 910c- a3b7a3c9d993

Product name	String ID	GUID
Microsoft 365 F3 EEA (no Teams)	Microsoft_365_F3_EEA_(no_Teams)	f7ee79a7-7aec-4ca4-9fb9-34d6b930ad87

Product name	String ID	GUID
Microsoft 365 F5 Compliance Add-on	SPE_F5_COMP	91de26be-adfa-4a3d-989e-9131cc23dda7

Product name	String ID	GUID
Microsoft 365 F5 Compliance Add-on AR_DOD_USGOV_DOD	SPE_F5_COMP_AR_D_USGOV_DOD	9cf6bc3- 84cd-4274- 8a21- 8c7c41d6c350
Microsoft 365 F5 Compliance Add-on AR_USGOV_GCCHIGH	SPE_F5_COMP_AR_USGOV_GCCHIGH	9f436c0e-fb32- 424b-90be- 6a9f2919d506

Product name	String ID	GUID
Microsoft 365 F5 Compliance Add-on GCC	SPE_F5_COMP_GCC	3f17cf90-67a2-4fdb-8587-37c1539507e1
Microsoft 365 F5 Security Add-on	SPE_F5_SEC	67ffe999-d9ca-49e1-9d2c-03fb28aa7a48
Microsoft 365 F5 Security + Compliance Add-on	SPE_F5_SECCOMP	32b47245-eb31-44fc-b945-a8b1576c439f

Product name	String ID	GUID
Microsoft Power Automate Free	FLOW_FREE	f30db892-07e9-47e9-837c-80727f46fd3d
Microsoft 365 E5 Extra Features	M365_E5_SUITE_COMPONENTS	99cc8282-2f74-4954-83b7-c6a9a1999067

Product name	String ID	GUID
Microsoft 365 F1	M365_F1_COMM	50f60901- 3181-4b75- 8a2c- 4c8e4c1d5a72
Microsoft 365 E5_USGOV_GCCHIGH	SPE_E5_USGOV_GCCHIGH	4eb45c5b- 0d19-4e33- b87c- adfc25268f20

Product name	String ID	GUID

Product name	String ID	GUID
Microsoft 365 F3 GCC	M365_F1_GOV	2a914830-d700-444a-b73c-e3f31980d833
Microsoft 365 G3 GCC	M365_G3_GOV	e823ca47-49c4-46b3-b38d-ca11d5abe3d2

Product name	String ID	GUID
Microsoft 365 G3 - Unattended License for GCC	M365_G3_RPA1_GOV	5c739a73- 651d-4c2c- 8a4e- fe4ba12253b0

Product name	String ID	GUID
Microsoft 365 GCC G5	M365_G5_GCC	e2be619b- b125-455f- 8660- fb503e431a5d

Product name	String ID	GUID

Product name	String ID	GUID
Microsoft 365 GCC G5 w/o WDATP/CAS Unified	M365_G5_GOV	b0f809d5- a662-4391- a5aa- 136e9c565b9d

Product name	String ID	GUID
Microsoft 365 Lighthouse	Microsoft365_Lighthouse	9c0587f3-8665-4252-a8ad-b7a5ade57312
Microsoft 365 Security and Compliance for Firstline Workers	M365_SECURITY_COMPLIANCE_FOR_FLW	2347355b-4e81-41a4-9c22-55057a399791

Product name	String ID	GUID
Microsoft Business Center	MICROSOFT_BUSINESS_CENTER	726a0894-2c77-4d65-99da-9775ef05aad1
Microsoft Cloud for Sustainability vTrial	Microsoft_Cloud_for_Sustainability_vTrial	556640c0-53ea-4773-907d-29c55332983f
Microsoft Cloud App Security	ADALLOM_STANDALONE	df845ce7-05f9-4894-b5f2-11bbfbcd2b6
Microsoft Copilot Studio	Power_Virtual_Agents	75564b9c-51e8-431c-b8fe-d472d5a545c8

<b>Product name</b>	<b>String ID</b>	<b>GUID</b>
Microsoft Copilot Studio for GCC	Power_Virtual_Agents_for_GCC_GCC	d7974fa0-ddd7-4899-9589-1ea04273aa26
Microsoft Copilot Studio User License for GCC	VIRTUAL_AGENT_USL_GCC	f1de227b-f1bd-4959-bd80-b80547095e6d
Microsoft Copilot Studio User License for GCC High	VIRTUAL_AGENT_USL_AR_USGOV_GCCHIGH	470845c0-6884-47e1-89d0-9d6244a77b44
Microsoft Copilot Studio USGOV GCCHIGH	Power_Virtual_Agents_USGOV_GCCHIGH	84ed7c30-3738-43a0-aa03-cf6c577d8dbb
Microsoft Copilot Studio Viral Trial	CCIBOTS_PRIVPREV_VIRAL	606b54a9-78d8-4298-ad8b-df6ef4481c80
Microsoft Copilot Studio User License	VIRTUAL_AGENT_USL	4b74a65c-8b4a-4fc8-9f6b-5177ed11ddfa
Microsoft Defender for Business	MDE_SMB	5e1e7702-a2b7-4360-8d07-2f515792896f
Microsoft Defender for Endpoint	WIN_DEF_ATP	111046dd-295b-4d6d-9724-d52ac90bd1f2
Microsoft Defender for Endpoint F2	Microsoft_Defender_for_Endpoint_F2	e430a580-c37b-4d16-adba-d881d7cd0364
Microsoft Defender for Endpoint P1	DEFENDER_ENDPOINT_P1	16a55f2f-ff35-4cd5-9146-fb784e3761a5

Product name	String ID	GUID
Microsoft Defender for Endpoint P1 for EDU	DEFENDER_ENDPOINT_P1_EDU	bba890d4-7881-4584-8102-0c3fdffb739a7
Microsoft Defender for Endpoint P2_XPLAT	MDATP_XPLAT	b126b073-72db-4a9d-87a4-b17afe41d4ab
Microsoft Defender for Endpoint Server	MDATP_Server	509e8ab6-0274-4cda-bcbd-bd164fd562c4
Microsoft Defender for Office 365 (Plan 1) Faculty	ATP_ENTERPRISE_FACULTY	26ad4b5c-b686-462e-84b9-d7c22b46837f
Microsoft Dynamics CRM Online Basic	CRMPLAN2	906af65a-2970-46d5-9b58-4e9aa50f0657
Microsoft Defender for Identity	ATA	98defdf7-f6c1-44f5-a1f6-943b6764e7a5
Microsoft Defender for Office 365 (Plan 1) GCC	ATP_ENTERPRISE_GOV	d0d1ca43-b81a-4f51-81e5-a5b1ad7bb005
Microsoft Defender for Office 365 (Plan 1) Student	ATP_ENTERPRISE_STUDENT	917fb2b4-f71c-43a1-8edc-75532b554bb5
Microsoft Defender for Office 365 (Plan 1) Student use benefit	ATP_ENTERPRISE_STUDENTS_USE_BENEFIT	a237b6d8-572e-4839-bffd-7786d32a5d0e
Microsoft Defender for Office 365 (Plan 1)_USGOV_GCCHIGH	ATP_ENTERPRISE_USGOV_GCCHIGH	550f19ba-f323-4a7d-a8d2-8971b0d9ea85
Microsoft Defender for Office 365 (Plan 2) GCC	THREAT_INTELLIGENCE_GOV	56a59ffb-9df1-421b-9e61-8b568583474d
Microsoft Defender Vulnerability Management	TVM_Premium_Standalone	1925967e-8013-495f-9644-c99f8b463748

Product name	String ID	GUID
Microsoft Defender Vulnerability Management Add-on	TVM_Premium_Add_on	ad7a56e0-6903-4d13-94f3-5ad491e78960
Microsoft Dynamics CRM Online	CRMSTANDARD	d17b27af-3f49-4822-99f9-56a661538792
Microsoft Dynamics CRM Online Basic for Government	CRMPLAN2_GCC	3856cd1b-8033-458e-8d0f-9909ec6e6e6d
Microsoft Dynamics CRM Online for Government	CRMSTANDARD_GCC	ba051a1a-4c3d-4ccd-9890-6fa6a4e696e7
Microsoft Entra ID Governance	Microsoft_Entra_ID_Governance	cf6b0d46-4093-4546-a0ab-0b1546dcc10e
Microsoft Fabric (Free)	POWER_BI_STANDARD	a403ebcc-fae0-4ca2-8c8c-7a907fd6c235
Microsoft Fabric (Free) for faculty	POWER_BI_STANDARD_FACULTY	ade29b5f-397e-4eb9-a287-0344bd46c68d
Microsoft Fabric (Free) for student	POWER_BI_STANDARD_STUDENT	bdcacf6aa-04c1-4b8f-b64e-6e3bd505ac64
Microsoft Imagine Academy	IT_ACADEMY_AD	ba9a34de-4489-469d-879c-0f0f145321cd
Microsoft Intune Device	INTUNE_A_D	2b317a4a-77a6-4188-9437-b68a77b4e2c6
Microsoft Intune Device for Government	INTUNE_A_D_GOV	2c21e77a-e0d6-4570-

<b>Product name</b>	<b>String ID</b>	<b>GUID</b>
		b38a-7ff2dc17d2ca
Microsoft Intune Government	INTUNE_A_GOV	2b26f637-35a0-4dbc-b69e-ff674782be9d
Microsoft Intune Plan 1 A VL_USGOV_GCCHIGH	INTUNE_A_VL_USGOV_GCCHIGH	b4288abe-01be-47d9-ad20-311d6e83fc24
Microsoft Intune Suite	Microsoft_Intune_Suite	a929cd4d-8672-47c9-8664-159c1f322ba8
Microsoft Power Apps Plan 2 Trial	POWERAPPS_VIRAL	dcb1a3ae-b33f-4487-846a-a640262fadf4
Microsoft Power Automate Plan 2	FLOW_P2	4755df59-3f73-41ab-a249-596ad72b5504
Microsoft Intune SMB	INTUNE_SMB	e6025b08-2fa5-4313-bd0a-7e5ffca32958
Microsoft PowerApps for Developer	POWERAPPS_DEV	5b631642-bd26-49fe-bd20-1daaa972ef80
Microsoft Power Apps Plan 2 (Qualified Offer)	POWERFLOW_P2	ddfae3e3-fcb2-4174-8ebd-3023cb213c8b
Microsoft Relationship Sales solution	DYN365_ENTERPRISE_RELATIONSHIP_SALES	4f05b1a3-a978-462c-b93f-781c6bee998f

Product name	String ID	GUID
Microsoft Stream	STREAM	1f2f344a-700d-42c9-9427-5cea1d5d7ba6
Microsoft Stream Plan 2	STREAM_P2	ec156933-b85b-4c50-84ec-c9e5603709ef
Microsoft Stream Storage Add-On (500 GB)	STREAM_STORAGE	9bd7c846-9556-4453-a542-191d527209e8
Microsoft Sustainability Manager Premium	Microsoft_Sustainability_Manager_Premium	aecb477b-2f56-4e38-b711-b752c24fc19b
Microsoft Sustainability Manager USL Essentials	Microsoft_Cloud_for_Sustainability_USL	ece037b4-a52b-4cf8-93ea-649e5d83767a
Microsoft Teams Audio Conferencing with dial-out to USA/CAN	Microsoft_Teams_Audio_Conferencing_select_dial_out	1c27243e-fb4d-42b1-ae8c-fe25c9616588
Microsoft Teams (Free)	TEAMS_FREE	16ddbfbfc-09ea-4de2-b1d7-312db6112d70
Microsoft Teams Calling Plan pay-as-you-go (country zone 1	Microsoft_Teams_Calling_Plan_pay_as_you_go_(country_zone_1_US)	9b196e97-5830-4c2e-

<b>Product name</b>	<b>String ID</b>	<b>GUID</b>
- US)		adc2- 1e10ebf5dee5
Microsoft Teams Domestic Calling Plan (240 min)	MCOPSTN_6	729dbb8f- 8d56-4994- 8e33- 2f218f549544
Microsoft Teams EEA	Microsoft_Teams_EEA_New	7e74bd05- 2c47-404e- 829a- ba95c66fe8e5
Microsoft Teams Essentials	Teams_Ess	fde42873- 30b6-436b- b361- 21af5a6b84ae
Microsoft Teams Essentials (Microsoft Entra identity)	TEAMS_ESSENTIALS_AAD	3ab6abff-666f- 4424-bfb7- f0bc274ec7bc
Microsoft Teams Exploratory	TEAMS_EXPLORATORY	710779e8- 3d4a-4c88- adb9- 386c958d1fdf

Product name	String ID	GUID
Microsoft Teams Exploratory Dept	Microsoft_Teams_Exploratory_Dept	e0dfc8b9- 9531-4ec8- 94b4- 9fec23b05fc8

Product name	String ID	GUID
Microsoft Teams Phone Standard	MCOEV	e43b5b99-8dfb-405f-9987-dc307f34bcfd
Microsoft Teams Phone Standard for DOD	MCOEV_DOD	d01d9287-694b-44f3-bcc5-ada78c8d953e
Microsoft Teams Phone Standard for Faculty	MCOEV_FACULTY	d979703c-028d-4de5-acbf-7955566b69b9
Microsoft Teams Phone Standard for GCC	MCOEV_GOV	a460366a-ade7-4791-b581-9fbff1bdaaa85
Microsoft Teams Phone Standard for GCCHIGH	MCOEV_GCCHIGH	7035277a-5e49-4abc-a24f-0ec49c501bb5
Microsoft Teams Phone Standard for Small and Medium Business	MCOEV_SMB_1	aa6791d3-bb09-4bc2-afed-c30c3fe26032
Microsoft Teams Phone Standard for Student	MCOEV_STUDENT	1f338bbc-767e-4a1e-a2d4-b73207cc5b93
Microsoft Teams Phone Standard for TELSTRA	MCOEV_TELSTRA	ffaf2d68-1c95-4eb3-9ddd-59b81fba0f61
Microsoft Teams Phone Standard_System_USGOV_DOD	MCOEV_USGOV_DOD	b0e7de67-e503-4934-b729-53d595ba5cd1
Microsoft Teams Phone Standard_USGOV_GCCHIGH	MCOEV_USGOV_GCCHIGH	985fcbb6-7b94-475b-b512-89356697be71
Microsoft Teams Phone Resource Account	PHONESYSTEM_VIRTUALUSER	440eaaa8-b3e0-484b-a8be-62870b9ba70a
Microsoft Teams Phone Resource Account for Faculty	PHONESYSTEM_VIRTUALUSER_FACULTY	0e142028-345e-45da-8d92-8bfd4093bbb9
Microsoft Teams Phone Resource Account for GCC	PHONESYSTEM_VIRTUALUSER_GOV	2cf22bcb-0c9e-4bc6-8daf-7e7654c0f285
Microsoft Teams Phone Resource Account_USGOV_GCCHIGH	PHONESYSTEM_VIRTUALUSER_USGOV_GCCHIGH	e3f0522e-ebb7-4561-9f90-b44516d65b77
Microsoft Teams Premium Introductory Pricing	Microsoft_Teams_Premium	36a0f3b3-adb5-49ea-

<b>Product name</b>	<b>String ID</b>	<b>GUID</b>
		bf66- 762134cf063a
Microsoft Teams Rooms Basic	Microsoft_Teams_Rooms_Basic	6af4b3d6- 14bb-4a2a- 960c- 6c902aad34f3
Microsoft Teams Rooms Basic for EDU	Microsoft_Teams_Rooms_Basic_FAC	a4e376bd- c61e-4618- 9901- 3fc0cb1b88bb
Microsoft Teams Rooms Basic without Audio Conferencing	Microsoft_Teams_Rooms_Basic_without_Audio_Conferencing	50509a35- f0bd-4c5e- 89ac- 22f0e16a00f8
Microsoft Teams Rooms Pro	Microsoft_Teams_Rooms_Pro	4cde982a- ede4-4409- 9ae6- b003453c8ea6
Microsoft Teams Rooms Pro for EDU	Microsoft_Teams_Rooms_Pro_FAC	c25e2b36- e161-4946- bef2- 69239729f690

<b>Product name</b>	<b>String ID</b>	<b>GUID</b>
Microsoft Teams Rooms Pro for GCC	Microsoft_Teams_Rooms_Pro_GCC	31ecb341- 2a17-483e- 9140- c473006d1e1a
Microsoft Teams Rooms Pro without Audio Conferencing	Microsoft_Teams_Rooms_Pro_without_Audio_Conferencing	21943e3a- 2429-4f83- 84c1- 02735cd49e78
Microsoft Teams Rooms Standard	MEETING_ROOM	6070a4c8- 34c6-4937- 8dfb- 39bbc6397a60
Microsoft Teams Rooms Standard for GCC	MEETING_ROOM_GOV	9571e9ac- 2741-4b63- 95fd- a79696f0d0ac

Product name	String ID	GUID
Microsoft Teams Rooms Standard for GCC without Audio Conferencing	MEETING_ROOM_GOV_NOAUDIOCONF	b4348f75-a776-4061-ac6c-36b9016b01d1
Microsoft Teams Shared Devices	MCOCAP	295a8eb0-f78d-45c7-8b5b-1eed5ed02dff
Microsoft Teams Shared Devices for Faculty	MCOCAP_FACULTY	420c7602-7f70-4895-9394-d3d679ea36fb
Microsoft Teams Shared Devices for GCC	MCOCAP_GOV	b1511558-69bd-4e1b-8270-59ca96dba0f3
Microsoft Teams Trial	MS_TEAMS_IW	74fbf1bb-47c6-4796-9623-77dc7371723b

Product name	String ID	GUID
Microsoft Threat Experts - Experts on Demand	EXPERTS_ON_DEMAND	9fa2f157-c8e4-4351-a3f2-ffa506da1406
Microsoft Workplace Analytics	WORKPLACE_ANALYTICS	3d957427-ecdc-4df2-aacd-01cc9d519da8
Microsoft Viva Goals	Microsoft_Viva_Goals	ba929637-f158-4dee-927c-eb7cdefcd955
Microsoft Viva Glint	Viva_Glint_Standalone	3dc7332d-f0fa-40a3-81d3-dd6b84469b78
Microsoft Viva Suite	VIVA	61902246-d7cb-453e-85cd-53ee28eec138
Minecraft Education Faculty	MEE_FACULTY	984df360-9a74-4647-8cf8-696749f6247a
Minecraft Education Student	MEE_STUDENT	533b8f26-f74b-4e9c-9c59-50fc4b393b63
Office 365 Multi-Geo Capabilities	OFFICE365_MULTIGEO	84951599-62b7-46f3-9c9d-30551b2ad607
Nonprofit Portal	NONPROFIT_PORTAL	aa2695c9-8d59-4800-

<b>Product name</b>	<b>String ID</b>	<b>GUID</b>
		9dc8- 12e01f1735af
Office 365 A1 for Faculty	STANDARDWOFFPACK_FACULTY	94763226- 9b3c-4e75- a931- 5c89701abe66
Office 365 A1 Plus for Faculty	STANDARDWOFFPACK_IW_FACULTY	78e66a63- 337a-4a9a- 8959- 41c6654dfb56

Product name	String ID	GUID
Office 365 A1 for Students	STANDARDWOFFPACK_STUDENT	314c4481-f395-4525-be8b-2ec4bb1e9d91

Product name	String ID	GUID
Office 365 A1 Plus for Students	STANDARDWOFFPACK_IW_STUDENT	e82ae690-a2d5-4d76-8d30-7c6e01e6022e

Product name	String ID	GUID
Office 365 A3 for Faculty	ENTERPRISEPACKPLUS_FACULTY	e578b273-6db4-4691-bba0-8d691f4da603
Office 365 A3 for Students	ENTERPRISEPACKPLUS_STUDENT	98b6e773-24d4-4c0d-a968-6e787a1f8204

Product name	String ID	GUID
Office 365 A5 for faculty	ENTERPRISEPREMIUM_FACULTY	a4585165-0533-458a-97e3-c400570268c4

Product name	String ID	GUID

Product name	String ID	GUID
Office 365 A5 for students	ENTERPRISEPREMIUM_STUDENT	ee656612-49fa-43e5-b67e-cb1fdf7699df

Product name	String ID	GUID

<b>Product name</b>	<b>String ID</b>	<b>GUID</b>
Office 365 Advanced Compliance	EQUIVIO_ANALYTICS	1b1b1f7a-8355-43b6-829f-336cfccb744c
Microsoft Copilot for Microsoft 365	M365_Copilot	a809996b-059e-42e2-9866-db24b99a9782
Microsoft Defender for Office 365 (Plan 1)	ATP_ENTERPRISE	4ef96642-f096-40de-a3e9-d83fb2f90211
Office 365 Extra File Storage for GCC	SHAREPOINTSTORAGE_GOV	e5788282-6381-469f-84f0-3d7d4021d34d
Microsoft Teams Commercial Cloud	TEAMS_COMMERCIAL_TRIAL	29a2f828-8f39-4837-b8ff-c957e86abe3c

<b>Product name</b>	<b>String ID</b>	<b>GUID</b>
Microsoft Teams EEA	Microsoft_Teams_EEA_New	7e74bd05-2c47-404e-829a-ba95c66fe8e5
Microsoft Sales Copilot	Microsoft_Viva_Sales	3227bcb2-8448-4f81-b3c2-8c2074e15a2a
Office 365 Cloud App Security	ADALLOM_O365	84d5f90f-cd0d-4864-b90b-1c7ba63b4808
Office 365 Extra File Storage	SHAREPOINTSTORAGE	99049c9c-6011-4908-bf17-15f496e6519d
Office 365 E1	STANDARDPACK	18181a46-0d4e-45cd-891e-60aab171b4e

Product name	String ID	GUID

Product name	String ID	GUID
Office 365 E1 EEA (no Teams)	Office_365_w/o_Teams_Bundle_E1	b57282e3-65bd-4252-9502-c0eae1e5ab7f
Office 365 E1_USGOV_GCCHIGH	STANDARDPACK_USGOV_GCCHIGH	f698ca06-024f-4562-b029-9cb1f1e02646

Product name	String ID	GUID
Office 365 E2	STANDARDWOFFPACK	6634e0ce-1a9f-428c-a498-f84ec7b8aa2e
Office 365 E3	ENTERPRISEPACK	6fd2c87f-b296-42f0-b197-1e91e994b900

Product name	String ID	GUID
Office 365 E3 (no Teams)	Office_365_E3_(no_Teams)	46c3a859-c90d-40b3-9551-6178a48d5c18

Product name	String ID	GUID
Office 365 E3 EEA (no Teams)	O365_w/o_Teams_Bundle_E3	d711d25a-a21c-492f-bd19-aae1e8ebaf30

Product name	String ID	GUID
Office 365 E3 Developer	DEVELOPERPACK	189a915c-fe4f-4ffa-bde4-85b9628d07a0

Product name	String ID	GUID
Office 365 E3_USGOV_DOD	ENTERPRISEPACK_USGOV_DOD	b107e5a3-3e60-4c0d-a184-a7e4395eb44c
Office 365 E3_USGOV_GCCHIGH	ENTERPRISEPACK_USGOV_GCCHIGH	aea38a85-9bd5-4981-aa00-616b411205bf
Office 365 E4	ENTERPRISEWITHSCAL	1392051d-0cb9-4b7a-88d5-621fee5e8711

Product name	String ID	GUID
Office 365 E5	ENTERPRISEPREMIUM	c7df2760- 2c81-4ef7- b578- 5b5392b571df

Product name	String ID	GUID
Office 365 E5 EEA (no Teams)	Office_365_w/o_Teams_Bundle_E5	cf50bae9- 29e8-4775- b07c- 56ee10e3776d

Product name	String ID	GUID

Product name	String ID	GUID
Office 365 E5 EEA (no Teams) without Audio Conferencing	Office_365_E5_EEA_(no_Teams)_without_Audio_Conferencing	71772aeb- 4bb8-4f74- 9dd4- 36c7a9b5ca74

Product name	String ID	GUID

Product name	String ID	GUID
Office 365 E5 without Audio Conferencing	ENTERPRISEPREMIUM_NOPSTNCONF	26d45bd9-adf1-46cd-a9e1-51e9a5524128

Product name	String ID	GUID
Office 365 F3	DESKLESSPACK	4b585984- 651b-448a- 9e53- 3b10f069cf7f

Product name	String ID	GUID
Office 365 F3 EEA (no Teams)	Office_365_F3_EEA_(no_Teams)	d1f0495b- cb7b-4e11- 8b85- daee7e7e5664

Product name	String ID	GUID
Office 365 F3_USGOV_GCCHIGH	DESKLESSPACK_USGOV_GCCHIGH	74039b88-bd62-4b5c-9d9c-7a92bbc0bfd
Office 365 G1 GCC	STANDARDPACK_GOV	3f4babde-90ec-47c6-995d-d223749065d1

Product name	String ID	GUID
Office 365 G3 GCC	ENTERPRISEPACK_GOV	535a3a29-c5f0-42fe-8215-d3b9e1f38c4a
Office 365 G3 without Microsoft 365 Apps GCC	ENTERPRISEPACKWITHOUTPROPLUS_GOV	24aebea8-7fac-48d0-8750-de4ee1fde205

Product name	String ID	GUID
Office 365 G5 GCC	ENTERPRISEPREMIUM_GOV	8900a2c0- edba-4079- bdf3- b276e293b6a8

Product name	String ID	GUID
Office 365 GCC G5 without Power BI and Phone System	ENTERPRISEPREMIUM_NOPBIPBX_GOV	2f105cc2-c2c1-435b-a955-c5e82156c05d

Product name	String ID	GUID

Product name	String ID	GUID
Office 365 GCC G5 without Audio Conferencing	ENTERPRISEPREMIUM_NOPSTNCONF_NOPBI_GOV	1341559b- 49df-443c- 8e79- fa604fed2d82

Product name	String ID	GUID
Office 365 Advanced Compliance for GCC	EQUIVIO_ANALYTICS_GOV	1a585bba-1ce3-416e-b1d6-9c482b52fcf6
Office 365 Midsize Business	MIDSIZEPACK	04a7fb0d-32e0-4241-

Product name	String ID	GUID
		b4f5-3f7618cd1162
Office 365 Small Business	LITEPACK	bd09678e-b83c-4d3f-aaba-3dad4abd128b
Office 365 Small Business Premium	LITEPACK_P2	fc14ec4a-4169-49a4-a51e-2c852931814b
Office Mobile Apps for Office 365 for GCC	OFFICEMOBILE_SUBSCRIPTION_GOV_TEST	64fca79f-c471-4e13-a335-9069cddf8aeb
OneDrive for Business (Plan 1)	WACONEDRIVESTANDARD	e6778190-713e-4e4f-9119-8b8238de25df
OneDrive for Business (Plan 2)	WACONEDRIVEENTERPRISE	ed01faf2-1d88-4947-ae91-45ca18703a96
PowerApps & Flow GCC Test - O365 & Dyn365 Plans	POWERFLOWGCC_TEST	0f13a262-dc6f-4800-8dc6-a62f72c95fad

Product name	String ID	GUID
Power Apps and Logic Flows	POWERAPPS_INDIVIDUAL_USER	87bbbc60-4754-4998-8c88-227dca264858
Power Apps per app baseline access	POWERAPPS_PER_APP_IW	bf666882-9c9b-4b2e-aa2f-4789b0a52ba2
Power Apps per app Plan	POWERAPPS_PER_APP	a8ad7d2b-b8cf-49d6-b25a-69094a0be206
Power Apps per app Plan (1 app or portal)	POWERAPPS_PER_APP_NEW	b4d7b828-e8dc-4518-

Product name	String ID	GUID
		91f9-e123ae48440d
Power Apps Per App BD Only for GCC	POWERAPPS_PER_APP_BD_ONLY_GCC	cdc8d0fc-fd16-4954-aae6-ed89a99f5620
Power Apps per app plan (1 app or website) BD Only – GCC	Power_Apps_per_app_plan_(1_app_or_portal)_BD_Only_GCC	816ee058-f70c-42ad-b433-d6171984ea20
Power Apps per app plan (1 app or website) for Government	POWERAPPS_PER_APP_GCC_NEW	c14d7f00-457c-4e3e-8960-48f35459b3c9
Power Apps per app plan for Government	POWERAPPS_PER_APP_GCC	8623b2d7-5e24-4281-b6b7-086a5f3b0b1c
Power Apps Per User BD Only	POWERAPPS_PER_USER_BD_ONLY	2ced8a00-3ed1-4295-ab7c-57170ff28e58
Power Apps Premium	POWERAPPS_PER_USER	b30411f5fea1-4a59-9ad9-3db7c7ead579
Power Apps Premium for Government	POWERAPPS_PER_USER_GCC	8e4c6baa-f2ff-4884-9c38-93785d0d7ba1

Product name	String ID	GUID
Power Apps Plan 1 for Government	POWERAPPS_P1_GOV	eca22b68-b31f-4e9c-a20c-4d40287bc5dd
Power Apps Portals login capacity add-on Tier 2 (10 unit min)	POWERAPPS_PORTALS_LOGIN_T2	57f3babd-73ce-40de-bcb2-dadbfbff9f7
Power Apps Portals login capacity add-on Tier 2 (10 unit min) for Government	POWERAPPS_PORTALS_LOGIN_T2_GCC	26c903d5-d385-4cb1-b650-8d81a643b3c4
Power Apps Portals login capacity add-on Tier 3 (50 unit min)	POWERAPPS_PORTALS_LOGIN_T3	927d8402-8d3b-40e8-b779-34e859f7b497
Power Apps Portals page view capacity add-on	POWERAPPS_PORTALS_PAGEVIEW	a0de5e3a-2500-4a19-b8f4-ec1c64692d22
Power Apps Portals page view capacity add-on for Government	POWERAPPS_PORTALS_PAGEVIEW_GCC	15a64d3e-5b99-4c4b-ae8f-aa6da264bfe7
Power Automate per flow plan	FLOW_BUSINESS_PROCESS	b3a42176-0a8c-4c3f-ba4e-f2b37fe5be6b
Power Automate per flow plan for Government	FLOW_BUSINESS_PROCESS_GCC	d9de51e5-d8cd-45bb-8da3-1d55e28c52e6

Product name	String ID	GUID
Power Automate per user plan	FLOW_PER_USER	4a51bf65-409c-4a91-b845-1121b571cc9d
Power Automate per user plan dept	FLOW_PER_USER_DEPT	d80a4c5d-8f05-4b64-9926-6574b9e6aee4
Power Automate per user plan for Government	FLOW_PER_USER_GCC	c8803586-c136-479a-8ff3-f5f32d23a68e
Power Automate Premium	POWERAUTOMATE_ATTENDED_RPA	eda1941c-3c4f-4995-b5eb-e85a42175ab9
Power Automate Plan 1 for Government (Qualified Offer)	FLOW_P1_GOV	2b3b0c87-36af-4d15-8124-04a691cc2546
Power Automate Premium for Government	POWERAUTOMATE_ATTENDED_RPA_GCC	d3987516-4b53-4dc0-8335-411260bf5626
Power Automate Process	Power_Automate_per_process	253ce8d3-6122-4240-8b04-f434a8fa831f
Power Automate unattended RPA add-on	POWERAUTOMATE_UNATTENDED_RPA	3539d28c-6e35-4a30-b3a9-cd43d5d3e0e2
Power Automate unattended RPA add-on for Government	POWERAUTOMATE_UNATTENDED_RPA_GCC	086e9b70-4720-4442-ab6d-3ef32bfb4721
Power BI	POWER_BI_INDIVIDUAL_USER	e2767865-c3c9-4f09-9f99-6eee6eef861a

Product name	String ID	GUID
Power BI for Office 365 Add-On	POWER_BI_ADDON	45bc2c81-6072-436a-9b0b-3b12eefbc402
Power BI Premium P1	PBI_PREMIUM_P1_ADDON	7b26f5ab-a763-4c00-a1ac-f6c4b5506945
Power BI Premium P1 GCC	PBI_PREMIUM_P1_ADDON_GCC	f59b22a0-9819-48bf-b01d-715ef2b31027
Power BI Premium Per User	PBI_PREMIUM_PER_USER	c1d032e0-5619-4761-9b5c-75b6831e1711
Power BI Premium Per User Add-On	PBI_PREMIUM_PER_USER_ADDON	de376a03-6e5b-42ec-855f-093fb50b8ca5
Power BI Premium Per User Add-On for GCC	PBI_PREMIUM_PER_USER_ADDON_GCC	1b572d5e-1bf8-4b19-9259-f9eda31a6972
Power BI Premium Per User Add-On for GCC	PBI_PREMIUM_PER_USER_ADDON_CE_GCC	66024bbf-4cd4-4329-95c8-c932e2ae01a8
Power BI Premium Per User for Faculty	PBI_PREMIUM_PER_USER_FACULTY	060d8061-f606-4e69-a4e7-e8fff75ea1f5
Power BI Premium Per User Dept	PBI_PREMIUM_PER_USER_DEPT	f168a3fb-7bcf-4a27-98c3-c235ea4b78b4
Power BI Premium Per User for Government	PBI_PREMIUM_PER_USER_GCC	e53d92fc-778b-4a8b-83de-791240ebff88d
Power BI Pro	POWER_BI_PRO	f8a1db68-be16-40ed-86d5-cb42ce701560
Power BI Pro CE	POWER_BI_PRO_CE	420af87e-8177-4146-a780-3786adaffbca
Power BI Pro Dept	POWER_BI_PRO_DEPT	3a6a908c-09c5-406a-

Product name	String ID	GUID
		8170- 8ebb63c42882
Power BI Pro for Faculty	POWER_BI_PRO_FACULTY	de5f128b- 46d7-4fcfc- b915- a89ba060ea56
Power BI Pro for GCC	POWERBI_PRO_GOV	f0612879- 44ea-47fb- baf0- 3d76d9235576
Power Pages authenticated users T1 100 users/per site/month capacity pack	Power_Pages_authenticated_users_T1_100_users/per_site/month_capacity_pack	debc9e58- f2d7-412c- a0b6- 575608564228
Power Pages authenticated users T1 100 users/per site/month capacity pack CN_CN	Power_Pages_authenticated_users_T1_CN_CN	9a3c2a19- 06c0-41b1- b2ea- 13528d7b2e17
Power Pages authenticated users T1 100 users/per site/month capacity pack_GCC	Power_Pages_authenticated_users_T1_100_users/per_site/month_capacity_pack_GCC	27cb5f12-2e3f- 4997-a649- 45298673e6a1
Power Pages authenticated users T1 100 users/per site/month capacity pack_USGOV_DOD	Power_Pages_authenticated_users_T1_100_users/per_site/month_capacity_pack_USGOV_DOD	b54f012e- 69e1-43b1- 87d0- 666def064940
Power Pages authenticated users T1 100 users/per site/month capacity pack_USGOV_GCCHIGH	Power_Pages_authenticated_users_T1_100_users/per_site/month_capacity_pack_USGOV_GCCHIGH	978ec396- f930-4ee1- 85f3- e1d82e8f73a4
Power Pages authenticated users T2 min 100 units - 100 users/per site/month capacity pack	Power_Pages_authenticated_users_T2_min_100_units_100_users/per_site/month_capacity_pack	6fe1e61a- 91e5-40d7- a547- 0d2dcc81bce8
Power Pages authenticated users T2 min 100 units - 100 users/per site/month capacity pack CN_CN	Power_Pages_authenticated_users_T2_CN_CN	7d2bb54a- a870-41c2- 98d1- 1f3b5b523275

Product name	String ID	GUID
Power Pages authenticated users T2 min 100 units - 100 users/per site/month capacity pack_GCC	Power_Pages_authenticated_users_T2_min_100_units_100_users/per_site/month_capacity_pack_GCC	5f43d48c-dd3d-4dd8-a059-70c2f040f979
Power Pages authenticated users T2 min 100 units - 100 users/per site/month capacity pack_USGOV_DOD	Power_Pages_authenticated_users_T2_min_100_units_100_users/per_site/month_capacity_pack_USGOV_DOD	f3d55e2d-4367-44fa-952e-83d0b5dd53fc
Power Pages authenticated users T2 min 100 units - 100 users/per site/month capacity pack_USGOV_GCCHIGH	Power_Pages_authenticated_users_T2_min_100_units_100_users/per_site/month_capacity_pack_USGOV_GCCHIGH	7cae5432-61bb-48c3-b75c-831394ec13a0
Power Pages authenticated users T3 min 1,000 units - 100 users/per site/month capacity pack CN_CN	Power_Pages_authenticated_users_T3_min_1,000_units_100_users/per_site/month_capacity_pack	878b8bbd-3cd0-4b44-9a56-3406741e65e0
Power Pages authenticated users T3 min 1,000 units - 100 users/per site/month capacity pack GCC	Power_Pages_authenticated_users_T3_min_1,000_units_100_users/per_site/month_capacity_pack_GCC	53265c61-c78c-4223-ab30-422da0c97fb
Power Pages authenticated users T3 min 1,000 units - 100 users/per site/month capacity pack_USGOV_DOD	Power_Pages_authenticated_users_T3_min_1,000_units_100_users/per_site/month_capacity_pack_USGOV_DOD	398d37b5-8deb-48db-8f7f-703eb2fb7c72
Power Pages authenticated users T3 min 1,000 units - 100 users/per site/month capacity pack_USGOV_GCCHIGH	Power_Pages_authenticated_users_T3_min_1,000_units_100_users/per_site/month_capacity_pack_USGOV_GCCHIGH	01d46c34-3525-47d5-bd1a-5f19979938a0
Power Pages vTrial for Makers	Power_Pages_vTrial_for_Makers	3f9f06f5-3c31-472c-985f-62d9c10ec167
Power BI Premium EM1	PBI_PREMIUM_EM1_ADDON	bc757c42-5622-4583-

Product name	String ID	GUID
		a483- a9e537fcb71c
Power BI Premium EM2	PBI_PREMIUM_EM2_ADDON	8ecbd3c1- b108-437c- a859- e3c125e3f83f
Power Virtual Agent	VIRTUAL_AGENT_BASE	e4e55366- 9635-46f4- a907- fc8c3b5ec81f
Power Virtual Agent for GCC	VIRTUAL_AGENT_BASE_GCC	9900a3e2- 6660-4c52- 9074- 60c949991389
Privacy Management – risk	PRIVACY_MANAGEMENT_RISK	e42bc969- 759a-4820- 9283- 6b73085b68e6
Privacy Management - risk for EDU	PRIVACY_MANAGEMENT_RISK_EDU	dcdbaae7- d8c9-40cb- 8bb1- 62737b9e5a86
Privacy Management - risk GCC	PRIVACY_MANAGEMENT_RISK_GCC	046f7d3b- 9595-4685- a2e8- a2832d2b26aa
Privacy Management - risk_USGOV_DOD	PRIVACY_MANAGEMENT_RISK_USGOV_DOD	83b30692- 0d09-435c- a455- 2ab220d504b9
Privacy Management - risk_USGOV_GCCHIGH	PRIVACY_MANAGEMENT_RISK_USGOV_GCCHIGH	787d7e75- 29ca-4b90- a3a9- 0b780b35367c
Privacy Management - subject rights request (1)	PRIVACY_MANAGEMENT_SUB_RIGHTS_REQ_1_V2	d9020d1c- 94ef-495a- b6de- 818cbbcaa3b8
Privacy Management - subject rights request (1) for EDU	PRIVACY_MANAGEMENT_SUB_RIGHTS_REQ_1_EDU_V2	475e3e81- 3c75-4e07- 95b6- 2fed374536c8

Product name	String ID	GUID
Privacy Management - subject rights request (1) GCC	PRIVACY_MANAGEMENT_SUB_RIGHTS_REQ_1_V2_GCC	017fb6f8-00dd-4025-be2b-4eff067cae72
Privacy Management - subject rights request (1) USGOV_DOD	PRIVACY_MANAGEMENT_SUB_RIGHTS_REQ_1_V2_USGOV_DOD	d3c841f3-ea93-4da2-8040-6f2348d20954
Privacy Management - subject rights request (1) USGOV_GCCHIGH	PRIVACY_MANAGEMENT_SUB_RIGHTS_REQ_1_V2_USGOV_GCCHIGH	706d2425-6170-4818-ba08-2ad8f1d2d078
Privacy Management - subject rights request (10)	PRIVACY_MANAGEMENT_SUB_RIGHTS_REQ_10_V2	78ea43ac-9e5d-474f-8537-4abb82dafe27
Privacy Management - subject rights request (10) for EDU	PRIVACY_MANAGEMENT_SUB_RIGHTS_REQ_10_EDU_V2	e001d9f1-5047-4ebf-8927-148530491f83
Privacy Management - subject rights request (10) GCC	PRIVACY_MANAGEMENT_SUB_RIGHTS_REQ_10_V2_GCC	a056b037-1fa0-4133-a583-d05cff47d551
Privacy Management - subject rights request (10) USGOV_DOD	PRIVACY_MANAGEMENT_SUB_RIGHTS_REQ_10_V2_USGOV_DOD	ab28dfa1-853a-4f54-9315-f5146975ac9a
Privacy Management - subject rights request (10) USGOV_GCCHIGH	PRIVACY_MANAGEMENT_SUB_RIGHTS_REQ_10_V2_USGOV_GCCHIGH	f6aa3b3d-62f4-4c1d-a44f-0550f40f729c

Product name	String ID	GUID
Privacy Management - subject rights request (50)	PRIVACY_MANAGEMENT_SUB_RIGHTS_REQ_50	c416b349-a83c-48cb-9529-c420841dedd6
Privacy Management - subject rights request (50)	PRIVACY_MANAGEMENT_SUB_RIGHTS_REQ_50_V2	f6c82f13-9554-4da1-bed3-c024cc906e02
Privacy Management - subject rights request (50) for EDU	PRIVACY_MANAGEMENT_SUB_RIGHTS_REQ_50_EDU_V2	ed45d397-7d61-4110-acc0-95674917bb14
Privacy Management - subject rights request (100)	PRIVACY_MANAGEMENT_SUB_RIGHTS_REQ_100_V2	cf4c6c3b-f863-4940-97e8-1d25e912f4c4
Privacy Management - subject rights request (100) for EDU	PRIVACY_MANAGEMENT_SUB_RIGHTS_REQ_100_EDU_V2	9b85b4f0-92d9-4c3d-b230-041520cb1046
Privacy Management - subject rights request (100) GCC	PRIVACY_MANAGEMENT_SUB_RIGHTS_REQ_100_V2_GCC	91bbc479-4c2c-4210-9c88-e5b468c35b83
Privacy Management - subject rights request (100) USGOV_DOD	PRIVACY_MANAGEMENT_SUB_RIGHTS_REQ_100_V2_USGOV_DOD	ba6e69d5-ba2e-47a7-b081-66c1b8e7e7d4

<b>Product name</b>	<b>String ID</b>	<b>GUID</b>
Privacy Management - subject rights request (100) USGOV_GCCHIGH	PRIVACY_MANAGEMENT_SUB_RIGHTS_REQ_100_V2_USGOV_GCCHIGH	cee36ce4-cc31-481f-8cab-02765d3e441f
Project for Office 365	PROJECTCLIENT	a10d5e58-74da-4312-95c8-76be4e5b75a0
Project Online Essentials	PROJECTESSENTIALS	776df282-9fc0-4862-99e2-70e561b9909e
Project Online Essentials for Faculty	PROJECTESSENTIALS_FACULTY	e433b246-63e7-4d0b-9efa-7940fa3264d6
Project Online Essentials for GCC	PROJECTESSENTIALS_GOV	ca1a159a-f09e-42b8-bb82-cb6420f54c8e
Project Online Premium	PROJECTPREMIUM	09015f9f-377f-4538-bbb5-f75ceb09358a
Project Online Premium without Project Client	PROJECTONLINE_PLAN_1	2db84718-652c-47a7-860c-f10d8abbdæ3

<b>Product name</b>	<b>String ID</b>	<b>GUID</b>
Project Online with Project for Office 365	PROJECTONLINE_PLAN_2	f82a60b8-1ee3-4cfb-a4fe-1c6a53c2656c
Planner Plan 1	PROJECT_P1	beb6439c-caad-48d3-bf46-0c82871e12be
Project Plan 1 (for Department)	PROJECT_PLAN1_DEPT	84cd610f-a3f8-4beb-84ab-d9d2c902c6c9
Planner and Project Plan 3	PROJECTPROFESSIONAL	53818b1b-4a27-454b-8896-0dba576410e6
Project Plan 3 (for Department)	PROJECT_PLAN3_DEPT	46102f44-d912-47e7-b0ca-1bd7b70ada3b

<b>Product name</b>	<b>String ID</b>	<b>GUID</b>
Project Plan 3 for Faculty	PROJECTPROFESSIONAL_FACULTY	46974aed- 363e-423c- 9e6a- 951037cec495
Project Plan 3 for GCC	PROJECTPROFESSIONAL_GOV	074c6829- b3a0-430a- ba3d- aca365e57065
Project Plan 3 for GCC TEST	Project_Professional_TEST_GCC	5d505572- 203c-4b83- aa9b- dab50fb46277
Project Plan 3_USGOV_GCCHIGH	PROJECTPROFESSIONAL_USGOV_GCCHIGH	64758d81- 92b7-4855- bcac- 06617becb3e8
Project Plan 5 for faculty	PROJECTPREMIUM_FACULTY	930cc132- 4d6b-4d8c- 8818- 587d17c50d56

Product name	String ID	GUID
Project Plan 5 for GCC	PROJECTPREMIUM_GOV	f2230877-72be-4fec-b1ba-7156d6f75bd6
Project Plan 5 without Project Client for Faculty	PROJECTONLINE_PLAN_1_FACULTY	b732e2a7-5694-4dff-a0f2-9d9204c794ac
Rights Management Adhoc	RIGHTSMANAGEMENT_ADHOC	8c4ce438-32a7-4ac5-91a6-e22ae08d9c8b
Rights Management Service Basic Content Protection	RMSBASIC	093e8d14-a334-43d9-93e3-30589a8b47d0
Sensor Data Intelligence Additional Machines Add-in for Dynamics 365 Supply Chain Management	DYN365_IOT_INTELLIGENCE_ADDL_MACHINES	08e18479-4483-4f70-8f17-6f92156d8ea9
Sensor Data Intelligence Scenario Add-in for Dynamics 365 Supply Chain Management	DYN365_IOT_INTELLIGENCE_SCENARIO	9ea4bdef-a20b-4668-b4a7-73e1f7696e0a

Product name	String ID	GUID
SharePoint Online (Plan 1)	SHAREPOINTSTANDARD	1fc08a02-8b3d-43b9-831e-f76859e04e1a
SharePoint Online (Plan 2)	SHAREPOINTENTERPRISE	a9732ec9-17d9-494c-a51c-d6b45b384dcb
SharePoint Syntex	Intelligent_Content_Services	f61d4aba-134f-44e9-a2a0-f81a5adb26e4
Skype for Business Online (Plan 1)	MCOIMP	b8b749f8-a4ef-4887-9539-c95b1eaa5db7
Skype for Business Online (Plan 2)	MCOSTANDARD	d42c793f-6c78-4f43-92ca-e8f6a02b035f
Skype for Business PSTN Domestic and International Calling	MCOPSTN2	d3b4fe1f-9992-4930-8acb-ca6ec609365e
Skype for Business PSTN Domestic Calling	MCOPSTN1	0dab259f-bf13-4952-b7f8-7db8f131b28d
Skype for Business PSTN Domestic Calling (120 Minutes)	MCOPSTN5	54a152dc-90de-4996-93d2-bc47e670fc06
Skype for Business PSTN Calling Domestic Small	MCOPSTN5	d43177b5-475b-4880-92d4-d54c27b5efbd
Skype for Business PSTN Usage Calling Plan	MCOPSTNPP	06b48c5f-01d9-4b18-9015-03b52040f51a
Teams Phone Mobile	Operator_Connect_Mobile	b84d58c9-0a0d-46cf-8a4b-d9f23c1674d5
Teams Phone with Calling Plan	MCOTEAMS_ESSENTIALS	ae2343d1-0999-43f6-ae18-d816516f6e78
Teams Premium (for Departments)	Teams_Premium_(for_Departments)	52ea0e27-ae73-4983-a08f-13561ebdb823

Product name	String ID	GUID
TELSTRA Calling for O365	MCOPSTNEAU2	de3312e1-c7b0-46e6-a7c3-a515ff90bc86
Universal Print	UNIVERSAL_PRINT	9f3d9c1d-25a5-4aaa-8e59-23a1e6450a67
Visio Plan 1	VISIO_PLAN1_DEPT	ca7f3140-d88c-455b-9a1c-7f0679e31a76
Visio Plan 2	VISIO_PLAN2_DEPT	38b434d2-a15e-4cde-9a98-e737c75623e1
Visio Plan 1	VISIOONLINE_PLAN1	4b244418-9658-4451-a2b8-b5e2b364e9bd
Visio Plan 2 for Faculty	VISIOCLIENT_FACULTY	bf95fd32-576a-4742-8d7a-6dc4940b9532
Visio Plan 2	VISIOCLIENT	c5928f49-12ba-48f7-ada3-0d743a3601d5
Visio Plan 2 for GCC	VISIOCLIENT_GOV	4ae99959-6b0f-43b0-b1ce-68146001bdbba
Visio Plan 2_USGOV_GCCHIGH	VISIOCLIENT_USGOV_GCCHIGH	80e52531-ad7f-44ea-abc3-28e389462f1b

Product name	String ID	GUID
Viva Goals User-led	Viva_Goals_User_led	3a349c99-ffec-43d2-a2e8-6b97fcb71103
Viva Topics	TOPIC_EXPERIENCES	4016f256-b063-4864-816e-d818aad600c9
Viva Learning	VIVA_LEARNING	c9d442fc-21fb-4bd7-89e0-a710d74987f6
Windows 10/11 Enterprise E5 (Original)	WIN_ENT_E5	1e7e1070-8ccb-4aca-b470-d7cb538cb07e
Windows 10/11 Enterprise A3 for faculty	WIN10_ENT_A3_FAC	8efbe2f6-106e-442f-97d4-a59aa6037e06
Windows 10/11 Enterprise A3 for students	WIN10_ENT_A3_STU	d4ef921e-840b-4b48-9a90-ab6698bc7b31
Windows 10/11 Enterprise A5 for faculty	WIN10_ENT_A5_FAC	7b1a89a9-5eb9-4cf8-9467-20c943f1122c
WINDOWS 10/11 ENTERPRISE E3	WIN10_PRO_ENT_SUB	cb10e6cd-9da4-4992-867b-67546b1db821
WINDOWS 10/11 ENTERPRISE E3	WIN10_VDA_E3	6a0f6da5-0b87-4190-a6ae-9bb5a2b9546a

Product name	String ID	GUID
Windows 10/11 Enterprise E5	WIN10_VDA_E5	488ba24a-39a9-4473-8ee5-19291e71b002
Windows 10/11 Enterprise E5 Commercial (GCC Compatible)	WINE5_GCC_COMPAT	938fd547-d794-42a4-996c-1cc206619580
Windows 10/11 Enterprise VDA	E3_VDA_only	d13ef257-988a-46f3-8fce-f47484dd4550
Windows 365 Business 1 vCPU 2 GB 64 GB	CPC_B_1C_2RAM_64GB	816eacd3-e1e3-46b3-83c8-1ffd37e053d9
Windows 365 Business 2 vCPU 4 GB 128 GB	CPC_B_2C_4RAM_128GB	135bee78-485b-4181-ad6e-40286e311850
Windows 365 Business 2 vCPU 4 GB 256 GB	CPC_B_2C_4RAM_256GB	805d57c3-a97d-4c12-a1d0-858ffe5015d0
Windows 365 Business 2 vCPU 4 GB 64 GB	CPC_B_2C_4RAM_64GB	42e6818f-8966-444b-

Product name	String ID	GUID
		b7ac-0027c83fa8b5
Windows 365 Business 2 vCPU 8 GB 128 GB	CPC_B_2C_8RAM_128GB	71f21848-f89b-4aaa-a2dc-780c8e8aac5b
Windows 365 Business 2 vCPU 8 GB 256 GB	CPC_B_2C_8RAM_256GB	750d9542-a2f8-41c7-8c81-311352173432
Windows 365 Business 4 vCPU 16 GB 128 GB	CPC_B_4C_16RAM_128GB	ad83ac17-4a5a-4ebb-adb2-079fb277e8b9
Windows 365 Business 4 vCPU 16 GB 128 GB (with Windows Hybrid Benefit)	CPC_B_4C_16RAM_128GB_WHB	439ac253-bfbc-49c7-acc0-6b951407b5ef
Windows 365 Business 4 vCPU 16 GB 256 GB	CPC_B_4C_16RAM_256GB	b3891a9f-c7d9-463c-a2ec-0b2321bda6f9
Windows 365 Business 4 vCPU 16 GB 512 GB	CPC_B_4C_16RAM_512GB	1b3043ad-dfc6-427e-a2c0-5ca7a6c94a2b
Windows 365 Business 8 vCPU 32 GB 128 GB	CPC_B_8C_32RAM_128GB	3cb45fab-ae53-4ff6-af40-24c1915ca07b
Windows 365 Business 8 vCPU 32 GB 256 GB	CPC_B_8C_32RAM_256GB	fbc79df2-da01-4c17-8d88-17f8c9493d8f

Product name	String ID	GUID
Windows 365 Business 8 vCPU 32 GB 512 GB	CPC_B_8C_32RAM_512GB	8ee402cd-e6a8-4b67-a411-54d1f37a2049
Windows 365 Business 16 vCPU, 64 GB, 512 GB	Windows_365_Business_16_vCPU,_64_GB,_512_GB	93d9955a-ec70-44d5-8faa-a194492390f7
Windows 365 Business 16 vCPU, 64 GB, 1 TB	Windows_365_Business_16_vCPU,_64_GB,_1_TB	24be3cd7-82ca-41a5-94a7-4903373cdcae
Windows 365 Enterprise 1 vCPU 2 GB 64 GB	CPC_E_1C_2GB_64GB	0c278af4-c9c1-45de-9f4b-cd929e747a2c
Windows 365 Enterprise 2 vCPU 4 GB 128 GB	CPC_E_2C_4GB_128GB	226ca751-f0a4-4232-9be5-73c02a92555e
Windows 365 Enterprise 2 vCPU 4 GB 256 GB	CPC_E_2C_4GB_256GB	5265a84e-8def-4fa2-ab4b-5dc278df5025
Windows 365 Enterprise 2 vCPU 4 GB 64 GB	CPC_E_2C_4GB_64GB	7bb14422-3b90-4389-a7be-f1b745fc037f
Windows 365 Enterprise 2 vCPU 8 GB 128 GB	CPC_E_2C_8GB_128GB	e2aebe6c-897d-480f-9d62-fff1381581f7
Windows 365 Enterprise 2 vCPU 8 GB 256 GB	CPC_E_2C_8GB_256GB	1c79494f-e170-431f-a409-428f6053fa35
Windows 365 Enterprise 4 vCPU 16 GB 128 GB	CPC_E_4C_16GB_128GB	d201f153-d3b2-4057-be2f-fe25c8983e6f
Windows 365 Enterprise 4 vCPU vCPU, 16 GB, 256 GB	CPC_E_4C_16GB_256GB	96d2951e-cb42-4481-9d6d-cad3baac177e
Windows 365 Enterprise 4 vCPU 16 GB 512 GB	CPC_E_4C_16GB_512GB	0da63026-e422-4390-89e8-b14520d7e699

Product name	String ID	GUID
Windows 365 Enterprise 8 vCPU 32 GB 128 GB	CPC_E_8C_32GB_128GB	c97d00e4-0c4c-4ec2-a016-9448c65de986
Windows 365 Enterprise 8 vCPU 32 GB 256 GB	CPC_E_8C_32GB_256GB	7818ca3e-73c8-4e49-bc34-1276a2d27918
Windows 365 Enterprise 8 vCPU 32 GB 512 GB	CPC_E_8C_32GB_512GB	9fb0ba5f-4825-4e84-b239-5167a3a5d4dc
Windows 365 Enterprise 2 vCPU 4 GB 128 GB (Preview)	CPC_LVL_1	bce09f38-1800-4a51-8d50-5486380ba84a
Windows 365 Shared Use 2 vCPU 4 GB 64 GB	Windows_365_S_2vCPU_4GB_64GB	1f9990ca-45d9-4c8d-8d04-a79241924ce1
Windows 365 Shared Use 2 vCPU 4 GB 128 GB	Windows_365_S_2vCPU_4GB_128GB	90369797-7141-4e75-8f5e-d13f4b6092c1
Windows 365 Shared Use 2 vCPU 4 GB 256 GB	Windows_365_S_2vCPU_4GB_256GB	8fe96593-34d3-49bb-aeee-fb794fed0800
Windows 365 Shared Use 2 vCPU 8 GB 128 GB	Windows_365_S_2vCPU_8GB_128GB	2d21fc84-b918-491e-ad84-e24d61ccce94
Windows 365 Shared Use 2 vCPU 8 GB 256 GB	Windows_365_S_2vCPU_8GB_256GB	2eaa4058-403e-4434-9da9-ea693f5d96dc
Windows 365 Shared Use 4 vCPU 16 GB 128 GB	Windows_365_S_4vCPU_16GB_128GB	1bf40e76-4065-4530-ac37-f1513f362f50
Windows 365 Shared Use 4 vCPU 16 GB 256 GB	Windows_365_S_4vCPU_16GB_256GB	a9d1e0df-df6f-48df-9386-76a832119cca
Windows 365 Shared Use 4 vCPU 16 GB 512 GB	Windows_365_S_4vCPU_16GB_512GB	469af4da-121c-4529-8c85-9467bbebaa4b
Windows 365 Shared Use 8 vCPU 32 GB 128 GB	Windows_365_S_8vCPU_32GB_128GB	f319c63a-61a9-42b7-b786-5695bc7edbaf
Windows 365 Shared Use 8 vCPU 32 GB 256 GB	Windows_365_S_8vCPU_32GB_256GB	fb019e88-26a0-4218-bd61-7767d109ac26
Windows 365 Shared Use 8 vCPU 32 GB 512 GB	Windows_365_S_8vCPU_32GB_512GB	f4dc1de8-8c94-4d37-af8a-1fca6675590a

Product name	String ID	GUID
Windows Store for Business	WINDOWS_STORE	6470687e-a428-4b7a-bef2-8a291ad947c9
Windows Store for Business EDU Faculty	WSFB_EDU_FACULTY	c7e9d9e6-1981-4bf3-bb50-a5bdcaa06fb2
Workload Identities Premium	Workload_Identities_Premium_CN	73fa80b5-689f-4db9-bbe4-bd414bc41e44

## Service plans that cannot be assigned at the same time

Some products contain service plans that cannot be assigned to the same user at the same time. For example, if you have *Office 365 E1* and *Office 365 E3* in your tenant, and you try to assign both licenses to the same user, the operation fails. This is because the E3 product contains the following service plans that conflict with their E1 counterparts:

- SharePoint Online (Plan 2) conflicts with SharePoint Online (Plan 1).
- Exchange Online (Plan 2) conflicts with Exchange Online (Plan 1).

When using group-based licensing, you experience [this error condition](#). When using PowerShell, you see the *MutuallyExclusiveViolation* error.

This section lists the most common service plans that are mutually exclusive, grouped by service type. You can use this information to plan your license deployment and avoid assignment errors. These tables are for reference purposes and are accurate only as of the date when this article was last updated. Microsoft does not plan to update them for newly added services periodically.

## Service: *Microsoft Entra ID*

### ⓘ Note

All service plans related to Microsoft Entra ID can now be assigned together, to the same user. This simplifies certain license management scenarios, such as moving users from Microsoft Entra Basic to Microsoft Entra ID P1.

## Service: *Dynamics CRM*

The following service plans cannot be assigned together:

[Expand table](#)

Service Plan Name	GUID
CRMPLAN1	119cf168-b6cf-41fb-b82e-7fee7bae5814
CRMPLAN2	bf36ca64-95c6-4918-9275-eb9f4ce2c04f
CRMSTANDARD	f9646fb2-e3b2-4309-95de-dc4833737456
DYN365_ENTERPRISE_P1_IW	056a5f80-b4e0-4983-a8be-7ad254a113c9
DYN365_ENTERPRISE_SALES	2da8e897-7791-486b-b08f-cc63c8129df7
DYN365_ENTERPRISE_TEAM_MEMBERS	6a54b05e-4fab-40e7-9828-428db3b336fa
EMPLOYEE_SELF_SERVICE	ba5f0cfa-d54a-4ea0-8cf4-a7e1dc4423d8

## Service: *Exchange Online*

The following service plans cannot be assigned together:

[Expand table](#)

Service Plan Name	GUID
EXCHANGE_B_STANDARD	90927877-dcff-4af6-b346-2332c0b15bb7
EXCHANGE_S_ARCHIVE	da040e0a-b393-4bea-bb76-928b3fa1cf5a
EXCHANGE_S_DESKLESS	4a82b400-a79f-41a4-b4e2-e94f5787b113
EXCHANGE_S_ESSENTIALS	1126bef5-da20-4f07-b45e-ad25d2581aa8
EXCHANGE_S_STANDARD	9aaf7827-d63c-4b61-89c3-182f06f82e5c
EXCHANGE_S_STANDARD_MIDMARKET	fc52cc4b-ed7d-472d-bbe7-b081c23ecc56

## Service: Microsoft 365

The following service plans cannot be assigned together:

[Expand table](#)

Service Plan Name	GUID
RMS_S_ENTERPRISE	bea4c11e-220a-4e6d-8eb8-8ea15d019f90
RMS_S_ENTERPRISE_GOV	6a76346d-5d6e-4051-9fe3-ed3f312b5597

## Service: Intune

The following service plans cannot be assigned together:

[Expand table](#)

Service Plan Name	GUID
INTUNE_A	c1ec4a95-1f05-45b3-a911-aa3fa01094f5
INTUNE_A_VL	3e170737-c728-4eae-bbb9-3f3360f7184c
INTUNE_B	2dc63b8a-df3d-448f-b683-8655877c9360

## Service: SharePoint Online

The following service plans cannot be assigned together:

[Expand table](#)

Service Plan Name	GUID
ONEDRIVEENTERPRISE	afcaca6a-d966-4462-918c-ec0b4e0fe642
SHAREPOINT_S_DEVELOPER	a361d6e2-509e-4e25-a8ad-950060064ef4
SHAREPOINTDESKTOPLESS	902b47e5-dcb2-4fdc-858b-c63a90a2bdb9
SHAREPOINTENTERPRISE	5dbe027f-2339-4123-9542-606e4d348a72
SHAREPOINTENTERPRISE_EDU	63038b2c-28d0-45f6-bc36-33062963b498
SHAREPOINTENTERPRISE_MIDMARKET	6b5b6a67-fc72-4a1f-a2b5-beecf05de761
SHAREPOINTLITE	a1f3d0a8-84c0-4ae0-bae4-685917b8ab48
SHAREPOINTSTANDARD	c7699d2e-19aa-44de-8edf-1736da088ca1
SHAREPOINTSTANDARD_EDU	0a4983bb-d3e5-4a09-95d8-b2d0127b3df5
SHAREPOINTSTANDARD_YAMMERSHADOW	4c9efd0c-8de7-4c71-8295-9f5fdb0dd048

## Service: *Skype for Business*

The following service plans cannot be assigned together:

[Expand table](#)

Service Plan Name	GUID
MCOIMP	afc06cb0-b4f4-4473-8286-d644f70d8faf
MCOSTANDARD_MIDMARKET	b2669e95-76ef-4e7e-a367-002f60a39f3e
MCOSTANDARD	0feaeb32-d00e-4d66-bd5a-43b5b83db82c
MCOLITE	70710b6b-3ab4-4a38-9f6d-9f169461650a

The following service plans cannot be assigned together:

[Expand table](#)

Service Plan Name	GUID
MCOPSTN1	4ed3ff63-69d7-4fb7-b984-5aec7f605ca8
MCOPSTN2	5a10155d-f5c1-411a-a8ec-e99aae125390
MCOPSTNS	54a152dc-90de-4996-93d2-bc47e670fc06

## Service: *Yammer*

The following service plans cannot be assigned together:

[Expand table](#)

Service Plan Name	GUID
YAMMER_ENTERPRISE	7547a3fe-08ee-4ccb-b430-5077c5041653
YAMMER_EDU	2078e8df-cff6-4290-98cb-5408261a760a
YAMMER_MIDSIZE	41bf139a-4e60-409f-9346-a1361efc6dfb

## Next steps

To learn more about the feature set for license management through groups, see the following:

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

# 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

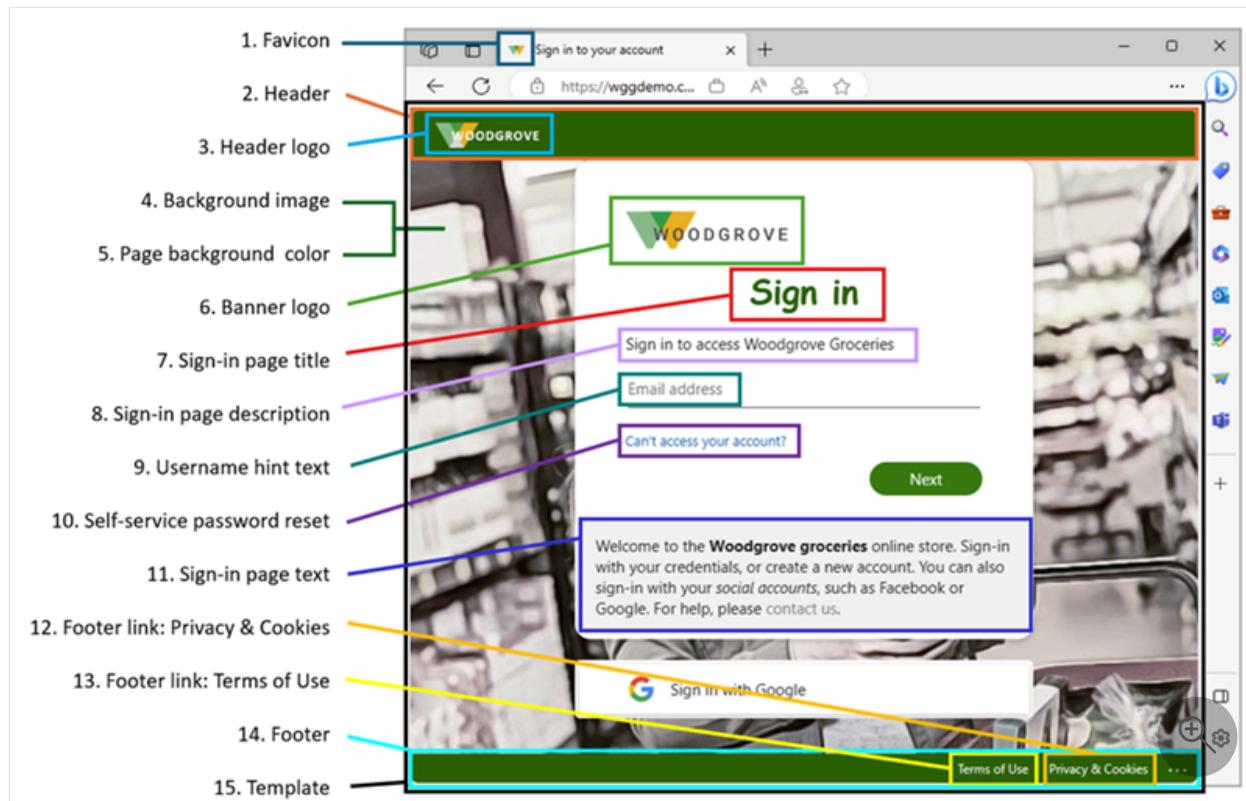
requirements you need. You might need to use a photo editor to create the right size images. The preferred image type for all images is PNG, but JPG is accepted.

**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

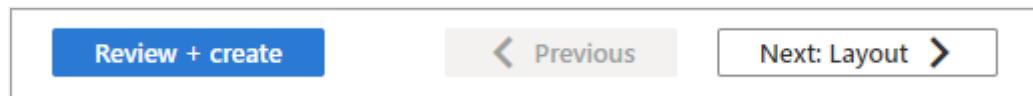
7. **Sign-in page title:** Larger text that appears below the banner logo.
8. **Sign-in page description:** Text to describe the sign-in page.
9. **Username hint and text:** The text that appears before a user enters their information.
10. **Self-service password reset:** A link you can add below the 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.

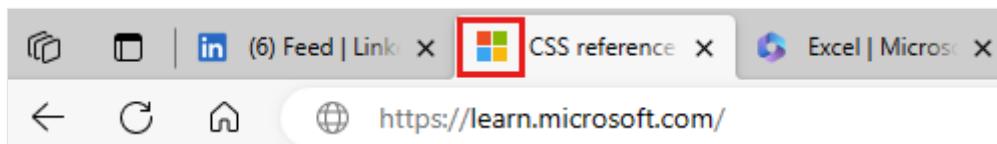
The screenshot shows the Microsoft Entra admin center interface. The left sidebar has a tree view with 'Identity' expanded, showing 'Overview', 'Users', 'Groups', 'Devices', 'Applications', 'Roles & admins', 'Billing', 'Settings', 'Protection', 'Identity governance', 'External Identities', 'User experiences' (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 an 'Add browser language' button. There is also a 'Customize your end user experiences' section with a link to learn more.

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

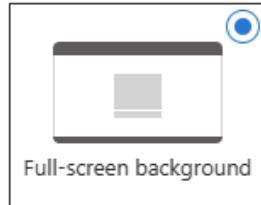
Basics   Layout   Header   Footer   Sign-in form   Review

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

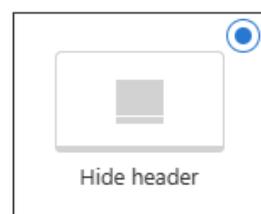


Partial-screen background

Header ⓘ

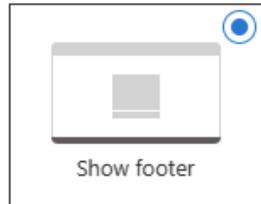


Show header



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.

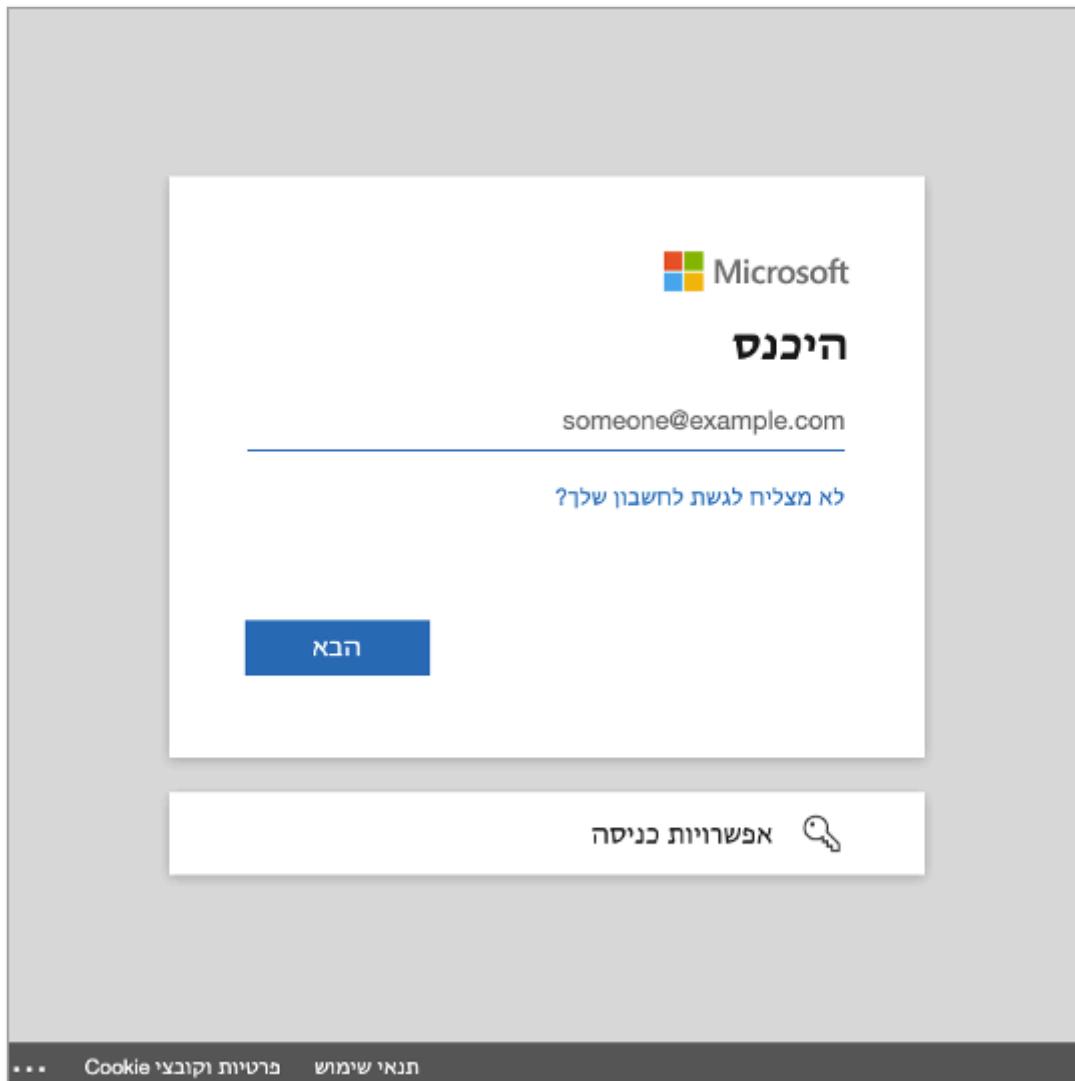
## Customize the sign-in experience by browser language

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.

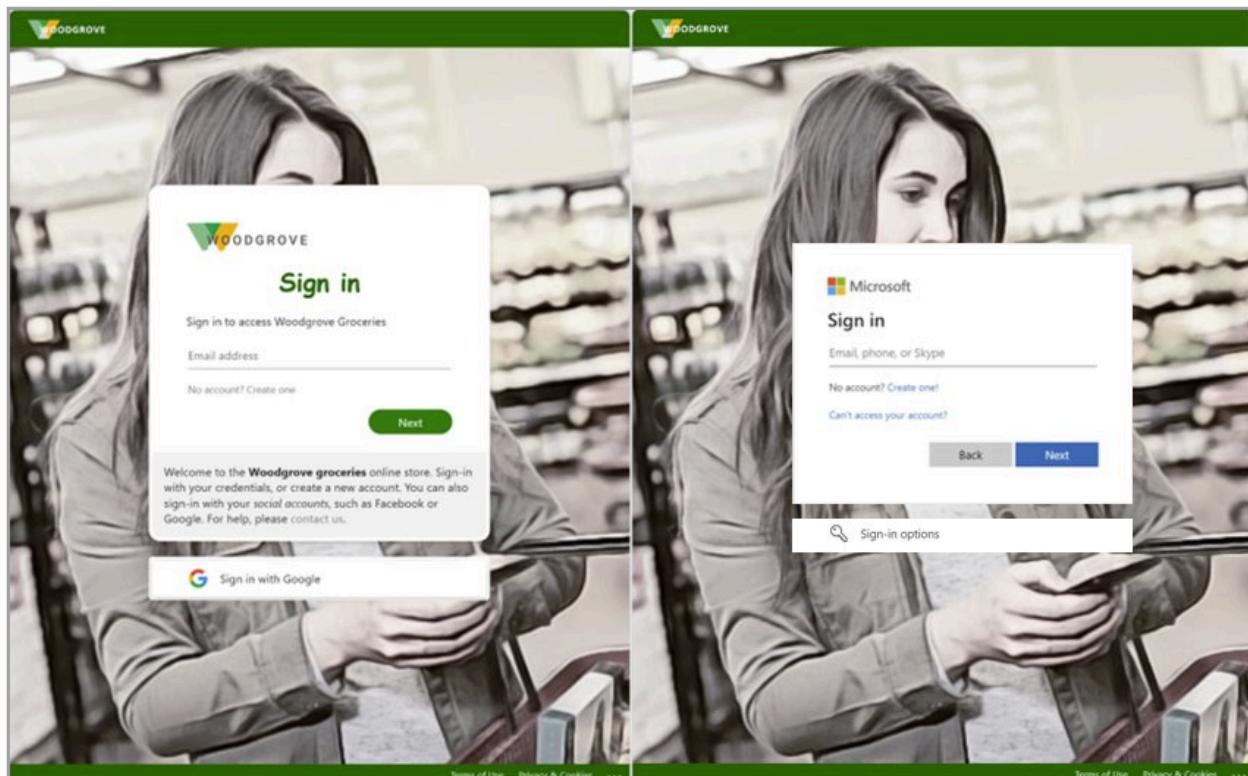
In the following examples, replace the contoso.com with your own tenant name, or verified domain name:

- 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](#) ↗

# Sign-in options for Microsoft accounts in Microsoft Entra ID

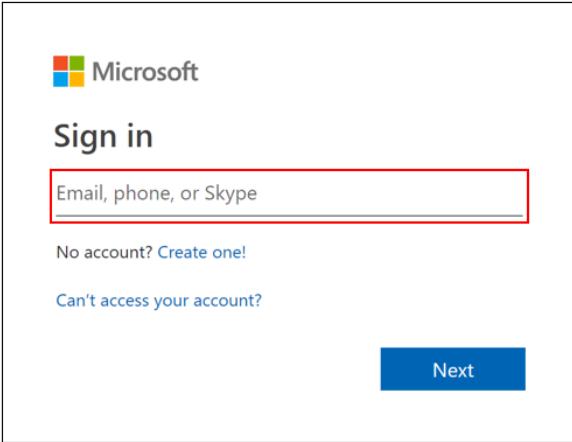
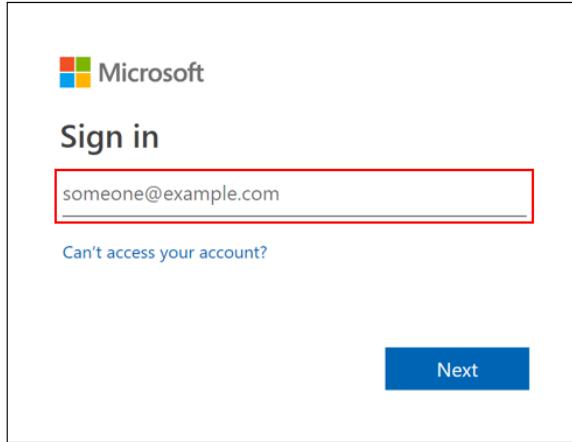
Article • 12/16/2024

The Microsoft 365 sign-in page for Microsoft Entra ID, part of Microsoft Entra, supports work or school accounts and Microsoft accounts, but depending on the user's situation, it could be one or the other or both. For example, the Microsoft Entra sign-in page supports:

- Apps that accept sign-ins from both types of account
- Organizations that accept guests

## Identification

You can tell if the sign-in page your organization uses supports Microsoft accounts by looking at the hint text in the username field. If the hint text says "Email, phone, or Skype", the sign-in page supports Microsoft accounts.

Supports personal accounts	Does not support personal accounts
 The Microsoft sign-in page for personal accounts. It features the Microsoft logo and a "Sign in" button. Below the button is a red-bordered input field containing the placeholder text "Email, phone, or Skype". Underneath the input field are two links: "No account? Create one!" and "Can't access your account?". A blue "Next" button is located at the bottom right. <p>Microsoft</p> <p>Sign in</p> <p>Email, phone, or Skype</p> <p>No account? Create one!</p> <p>Can't access your account?</p> <p>Next</p>	 The Microsoft sign-in page for non-personal accounts. It features the Microsoft logo and a "Sign in" button. Below the button is a red-bordered input field containing the placeholder text "someone@example.com". Underneath the input field is a link: "Can't access your account?". A blue "Next" button is located at the bottom right. <p>Microsoft</p> <p>Sign in</p> <p>someone@example.com</p> <p>Can't access your account?</p> <p>Next</p>

[Additional sign-in options that work only for personal Microsoft accounts ↗](#), but this option can't be used for signing in to work or school account resources.

## Next steps

[Customize your sign-in branding](#)

---

## Feedback

Was this page helpful?

 Yes

 No

Provide product feedback 

# Home realm discovery for Microsoft Entra sign-in pages

Article • 01/20/2025

We are changing sign-in behavior in Microsoft Entra ID, part of Microsoft Entra, to make room for new authentication methods and improve usability. During sign-in, Microsoft Entra ID determines where a user needs to authenticate. Microsoft Entra ID makes intelligent decisions by reading organization and user settings for the username entered on the sign-in page. This is a step towards a password-free future that enables other credentials like FIDO 2.0.

## Home realm discovery behavior

Traditionally, home realm discovery depended on either the domain provided at sign-in or a Home Realm Discovery policy for legacy applications. For instance, if a Microsoft Entra user entered their username incorrectly but included their organization's domain name, such as "contoso.com," they would still be directed to their organization's credential collection screen. This method didn't allow for customized experiences on an individual user level.

To enhance usability and support a broader range of credentials, Microsoft Entra ID uses a different process. Microsoft Entra ID's username lookup behavior during sign-in intelligently assesses organization-level and user-level settings based on the entered username. If the username is found within the specified domain, the user is directed accordingly; otherwise, the user is redirected to provide their credentials.

Another benefit of this work is improved error messaging. Here are some examples of the improved error messaging when signing in to an application that supports Microsoft Entra users only.

- The username is mistyped or the username hasn't yet been synced to Microsoft Entra ID:

The first screenshot shows a Microsoft sign-in page with the Microsoft logo and the word "Sign in". A text input field contains "keily@contoso.com". Below the input field is a link "Can't access your account?". A blue "Next" button is at the bottom right, with a yellow circular progress indicator partially visible. A large grey arrow points to the right, leading to the second screenshot.

The second screenshot shows the same Microsoft sign-in page. The text input field now contains "keily@contoso.com" in red text, indicating it is incorrect. Above the input field is a red error message: "This username may be incorrect. Make sure you typed it correctly. Otherwise, contact your admin." The "Next" button and progress indicator remain the same.

- The domain name is mistyped:

The first screenshot shows a Microsoft sign-in page with the Microsoft logo and the word "Sign in". A text input field contains "kelly@constosa.com". Below the input field is a link "Can't access your account?". A blue "Next" button is at the bottom right, with a yellow circular progress indicator partially visible. A large grey arrow points to the right, leading to the second screenshot.

The second screenshot shows the same Microsoft sign-in page. The text input field now contains "kelly@contosa.com" in red text, indicating it is incorrect. Above the input field is a red error message: "contosa.com isn't in our system. Make sure you typed it correctly." The "Next" button and progress indicator remain the same.

- User tries to sign in with a known consumer domain:

The first screenshot shows a Microsoft sign-in page with the Microsoft logo and the word "Sign in". A text input field contains "kelly@yahoo.com". Below the input field is a link "Can't access your account?". A blue "Next" button is at the bottom right, with a yellow circular progress indicator partially visible. A large grey arrow points to the right, leading to the second screenshot.

The second screenshot shows the same Microsoft sign-in page. The text input field now contains "kelly@yahoo.com" in red text, indicating it is incorrect. Above the input field is a red error message: "You can't sign in here with a personal account. Use your work or school account instead..". The "Next" button and progress indicator remain the same.

- The password is mistyped but the username is accurate:

The first screenshot shows a Microsoft sign-in page with the Microsoft logo and the word "Sign in". A text input field contains "kelly@contoso.com". Below the input field is a link "Can't access your account?". A blue "Next" button is at the bottom right, with a yellow circular progress indicator partially visible. A large grey arrow points to the right, leading to the second screenshot.

The second screenshot shows a Microsoft password entry page with the Microsoft logo and the word "Enter password". Above the input field is the text "← kelly@contoso.com". A text input field contains a series of dots ".....". Below the input field is a link "Forgot my password". A blue "Sign in" button is at the bottom right, with a yellow circular progress indicator partially visible. A large grey arrow points to the right, leading to the third screenshot.

The third screenshot shows the same Microsoft password entry page. The text input field now contains "....." in red text, indicating it is incorrect. Above the input field is a red error message: "Your username or password is incorrect. If you don't remember your password, reset it now.". The "Sign in" button and progress indicator remain the same.

## ⓘ Important

This feature might have an impact on federated domains relying on the old domain-level Home Realm Discovery to force federation. Federated domain support for this new behavior it's not currently available. In the meantime, some organizations have trained their employees to sign in with a username that doesn't exist in Microsoft Entra ID but contains the proper domain name, because the domain names routes users currently to their organization's domain endpoint. The new sign-in behavior doesn't allow this. The user is notified to correct the user name, and they aren't allowed to sign in with a username that does not exist in Microsoft Entra ID. If you or your organization have practices that depend on the old behavior, it is important for organization administrators to update employee sign-in and authentication documentation and to train employees to use their Microsoft Entra username to sign in. If you have concerns with the new behavior, leave your remarks in the **Feedback** section of this article.

## Next steps

[Customize your sign-in branding](#)

---

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#) 

# Integrate LinkedIn account connections in Microsoft Entra ID

Article • 01/28/2025

You can allow users in your organization to access their LinkedIn connections within some Microsoft apps. No data is shared until users consent to connect their accounts. You can integrate your organization with Microsoft Entra ID, part of Microsoft Entra.

## Important

The LinkedIn account connections setting is currently being rolled out to Microsoft Entra organizations. When it is rolled out to your organization, it is enabled by default.

Exceptions:

- The setting is not available for customers using Microsoft Cloud for US Government, Microsoft Cloud Germany, or Azure and Microsoft 365 operated by 21Vianet in China.
- The setting is off by default for Microsoft Entra organizations provisioned in Germany. Note that the setting is not available for customers using Microsoft Cloud Germany.
- The setting is off by default for organizations provisioned in France.

Once LinkedIn account connections are enabled for your organization, the account connections work after users consent to apps accessing company data on their behalf. For information about the user consent setting, see [How to remove a user's access to an application](#).

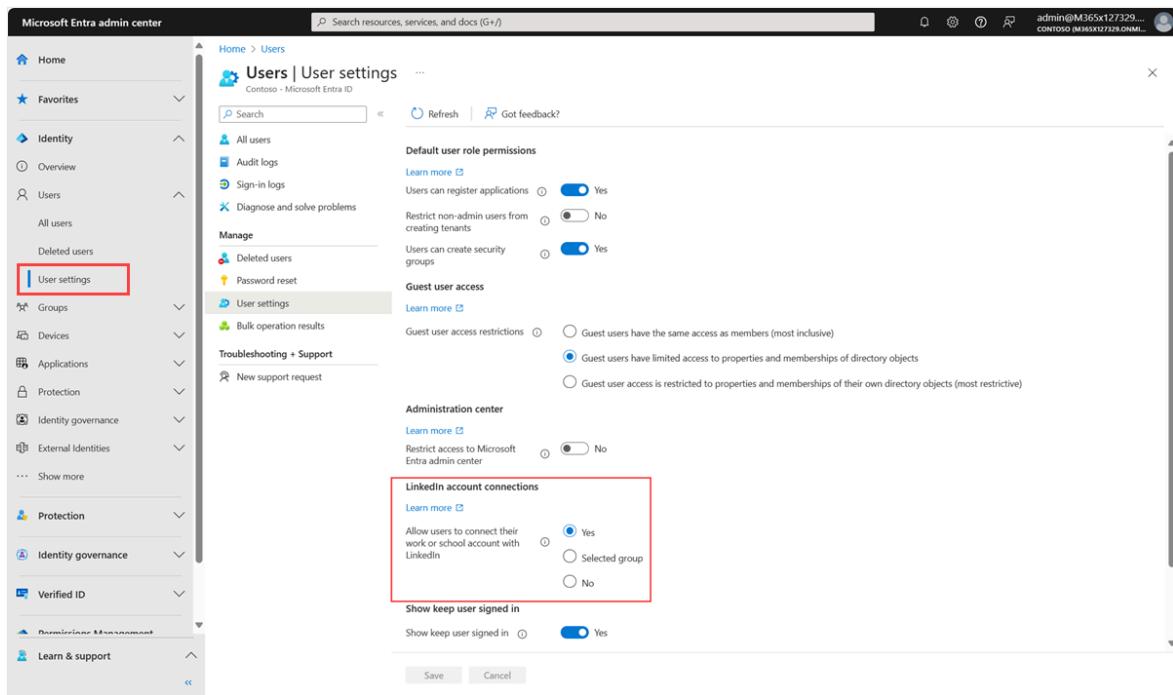
## Enable LinkedIn account connections in the Azure portal

You can enable LinkedIn account connections for only the users you want to have access, from your entire organization to only selected users in your organization.

## Important

Microsoft recommends that you use roles with the fewest permissions. This practice helps improve security for your organization. Global Administrator is a highly privileged role that should be limited to emergency scenarios or when you can't use an existing role.

1. Sign in to the Microsoft Entra admin center [↗](#) as a **Global Administrator**.
2. Select Microsoft Entra ID.
3. Select **Users > All users**.
4. Select **User settings**.
5. Under **LinkedIn account connections**, allow users to connect their accounts to access their LinkedIn connections within some Microsoft apps. No data is shared until users consent to connect their accounts.
  - Select **Yes** to enable the service for all users in your organization.
  - Select **Selected group** to enable the service for only a group of selected users in your organization.
  - Select **No** to withdraw consent from all users in your organization.



6. When you're done, select **Save** to save your settings.

## **ⓘ Important**

While LinkedIn integration is not fully enabled until your users consent to connect their accounts, access to public LinkedIn profile information is available without

requiring individual consent. Full integration (two-way consent and additional fields) is not enabled without each user's consent. Your users can see the available LinkedIn profile of anyone that matches the name searched, regardless of whether that match is in the same enabled group or not.

## Assign selected users with a group

We replaced the 'Selected' option that specifies a list of users with the option to select a group of users so that you can enable the ability to connect LinkedIn and Microsoft accounts for a single group instead of many individual users. If you don't have LinkedIn account connections enabled for selected individual users, you don't need to do anything. If you have previously enabled LinkedIn account connections for selected individual users, you should:

1. Get the current list of individual users.
2. Move the currently enabled individual users to a group.
3. Use the group from the previous as the selected group in the LinkedIn account connections setting in the Azure portal.

### ⓘ Note

Even if you don't move your currently selected individual users to a group, they can still see LinkedIn information in Microsoft apps.

## Move currently selected users to a group

1. Create a CSV file of the users who are selected for LinkedIn account connections.
2. Sign into Microsoft 365 with your administrator account.
3. Launch PowerShell.
4. Install the Microsoft Graph PowerShell module by running `Install-Module Microsoft.Graph -Scope CurrentUser`.
5. Run the following script:

PowerShell

```
$groupId = "GUID of the target group"
$users = Get-Content
```

Path to the CSV file

```
$i = 1
foreach($user in $users) {
 New-MgGroupMember -GroupId "$groupId" -DirectoryObjectId "$user" ;
 Write-Host $i Added $user ; $i++ ;
 Start-Sleep -Milliseconds 10
}
```

To use the group from step two as the selected group in the LinkedIn account connections setting in the Azure portal, see [Enable LinkedIn account connections in the Azure portal](#).

## Use Group Policy to enable LinkedIn account connections

1. Download the [Office 2016 Administrative Template files \(ADMX/ADML\)](#).
2. Extract the **ADMX** files and copy them to your central store.
3. Open Group Policy Management.
4. Create a Group Policy Object with the following setting: **User Configuration > Administrative Templates > Microsoft Office 2016 > Miscellaneous > Show LinkedIn features in Office applications**.
5. Select **Enabled** or **Disabled**.

[+] Expand table

State	Effect
Enabled	The <b>Show LinkedIn features in Office applications</b> setting in Office 2016 Options is enabled. Users in your organization can use LinkedIn features in their Office 2016 applications.
Disabled	The <b>Show LinkedIn features in Office applications</b> setting in Office 2016 Options is disabled and end users can't change this setting. Users in your organization can't use LinkedIn features in their Office 2016 applications.

This group policy affects only Office 2016 apps for a local computer. If users disable LinkedIn in their Office 2016 apps, they can still see LinkedIn features in Microsoft 365.

## Next steps

- User consent and data sharing for LinkedIn
  - LinkedIn information and features in your Microsoft apps ↗
  - LinkedIn help center ↗
  - View your current LinkedIn integration setting in the Azure portal ↗
- 

## Feedback

Was this page helpful?

 Yes

 No

Provide product feedback ↗

# LinkedIn account connections data sharing and consent

Article • 12/19/2024

You can enable users in your organization in Microsoft Entra ID, part of Microsoft Entra, to consent to connect their Microsoft work or school account with their LinkedIn account. After a user connects their accounts, information and highlights from LinkedIn are available in some Microsoft apps and services. Users can also expect their networking experience on LinkedIn to be improved and enriched with information from Microsoft.

To see LinkedIn information in Microsoft apps and services, users must consent to connect their own Microsoft and LinkedIn accounts. Users are prompted to connect their accounts the first time they select to see someone's LinkedIn information on a profile card in Outlook, OneDrive, or SharePoint Online. LinkedIn account connections aren't fully enabled for your users until they consent to the experience and to connect their accounts.

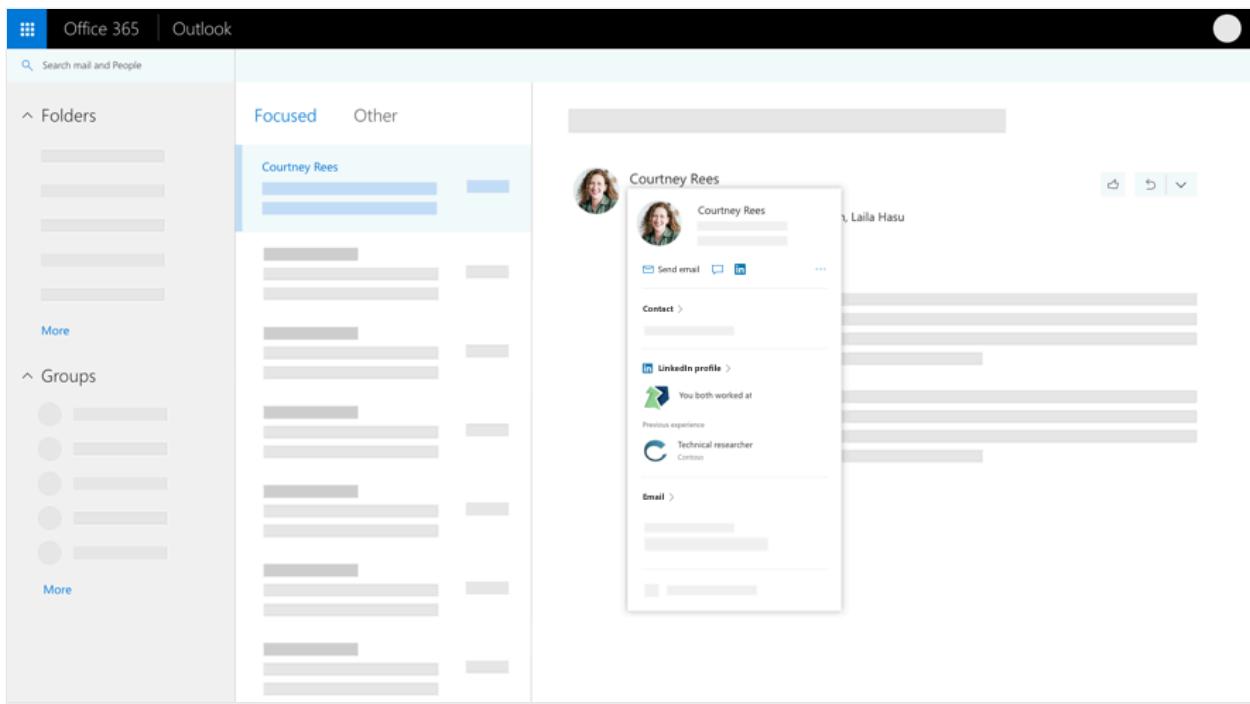
## Note

For information about viewing or deleting personal data, please review Microsoft's guidance on the [Windows data subject requests for the GDPR](#) site. For general information about GDPR, see the [GDPR section of the Microsoft Trust Center](#) and the [GDPR section of the Service Trust portal](#).

## Benefits of sharing LinkedIn information

Access to LinkedIn information within Microsoft apps and services makes it easier for your users to connect, engage, and build professional relationships with colleagues, customers, and partners inside and outside your organization. New users can get up to speed faster by connecting with colleagues, learning more about them, and easily accessing more information.

The image shows an example of how LinkedIn information appears on the profile card in Microsoft apps:



## Enable and announce LinkedIn integration

You must be a Microsoft Entra Admin to manage the setting for your organization. You can enable it for all users, or for a specific set of users.

1. To enable or disable the integration, follow the steps in [Consent to LinkedIn integration for your Microsoft Entra organization](#).
2. When you announce the LinkedIn integration in your organization, point your users to the FAQ about [LinkedIn information in Microsoft apps and services](#). The article provides information about where LinkedIn information shows up, [data sharing and privacy](#), [how to connect accounts](#) and more.

You must announce LinkedIn Integration to your users providing them all the information related to [Data sharing and privacy with LinkedIn Integration](#).

## User consent for data access in Microsoft and LinkedIn

Data that is accessed from LinkedIn isn't stored permanently in Microsoft services. Data that is accessed from Microsoft isn't stored permanently with LinkedIn.

When users connect their accounts, information and insights from LinkedIn are available in some Microsoft apps, like the profile card. Users can also expect their networking experience on LinkedIn to be improved and enriched with information from Microsoft. When users in your organization connect their LinkedIn and Microsoft work or school accounts, they have two options:

- Give permission for data to be accessed from both accounts. This means that they give permission for their Microsoft or work account to access data from their LinkedIn account, and for [their LinkedIn account to access data from their Microsoft work or school account ↗](#).
- Give permission for only the LinkedIn data to be accessed by their Microsoft work and school account.

Users can disconnect accounts and remove data access permissions at any time, and [users can control how their own LinkedIn profile is viewed ↗](#), including whether their profile can be viewed in Microsoft apps.

## LinkedIn account data

When you connect your Microsoft and LinkedIn accounts, you allow LinkedIn to provide the following data to Microsoft:

- Profile data - includes LinkedIn identity, contact information, and the information you share with others on your [LinkedIn profile ↗](#).
- Interests data - includes interests on LinkedIn, such as people and topics you follow, courses groups, and content you like and share.
- Subscriptions data - includes subscriptions to LinkedIn applications and services along with associated data.
- Connections data - includes your [LinkedIn network ↗](#) including profiles and contact information of your 1st-degree connections.

Data that is accessed from LinkedIn isn't stored permanently in Microsoft services. For more information about Microsoft's use of personal data, see the [Microsoft Privacy Statement ↗](#).

## Microsoft work or school account data

When you connect your Microsoft and LinkedIn accounts, you allow Microsoft to provide the following data to LinkedIn:

- Profile data - includes information like your first name, last name, profile photo, email address, manager, and people that you manage.
- Calendar data - includes meetings in your calendars, their times, locations, and attendees' contact information. Information about the meeting, like agenda, content, or meeting title isn't included in the calendar data.
- Interests data - includes the interests associated with your account, based on your use of Microsoft services, such as Cortana and Bing for Business.

- Subscriptions data - includes subscriptions provided by your organization to Microsoft apps and services, such as Microsoft 365.
- Contacts data - includes contact lists in Outlook, Skype, and other Microsoft account services, including the contact information for people you frequently communicate or collaborate with. Contacts are periodically imported, stored, and used by LinkedIn, for example to suggest connections, help organize contacts, and show updates about contacts.

Data that is accessed from Microsoft isn't stored permanently with LinkedIn. For more information on LinkedIn's use of personal data, see the [LinkedIn Privacy Policy](#). For LinkedIn services, data transfer, and storage, data can flow from the European Union to the United States and back, and your privacy is protected as described in [European Union data transfers](#).

## Next steps

- [LinkedIn in Microsoft applications with your work or school account](#)
- 

## 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. On the left, there's a navigation menu with items like Home, What's new, and Diagnose & solve problems (which is highlighted with a red box). The main content area is titled "Diagnose and solve problems". It features a search bar at the top and a "How can we help you?" section with a search input field. Below this is a "Troubleshooters" section with three cards: "Diagnose SSO problems", "Windows 10+ related issue?", and "Sign-in Diagnostic". Under "Common problems", there are three cards: "1603 error/Unable to install the synchronization service", "App Registration", and "Configuration and installation issues with Microsoft Entra Connect". Each card has a "View guidance" button.

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

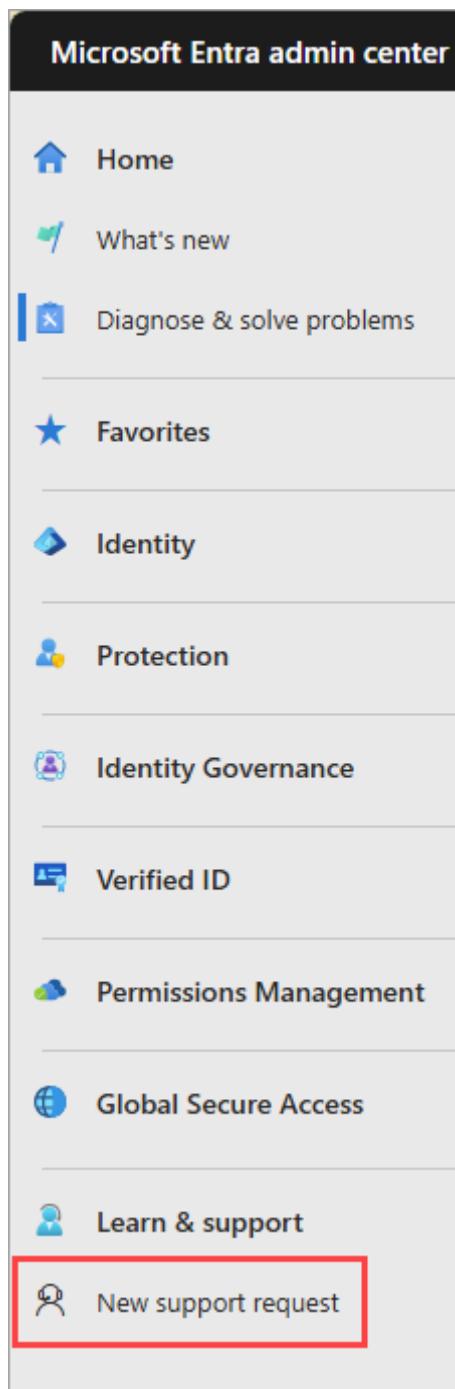
If you're unable to find answers by using the previously mentioned resources, you can open an online support request.

Online support requests can be created from several places in the admin center:

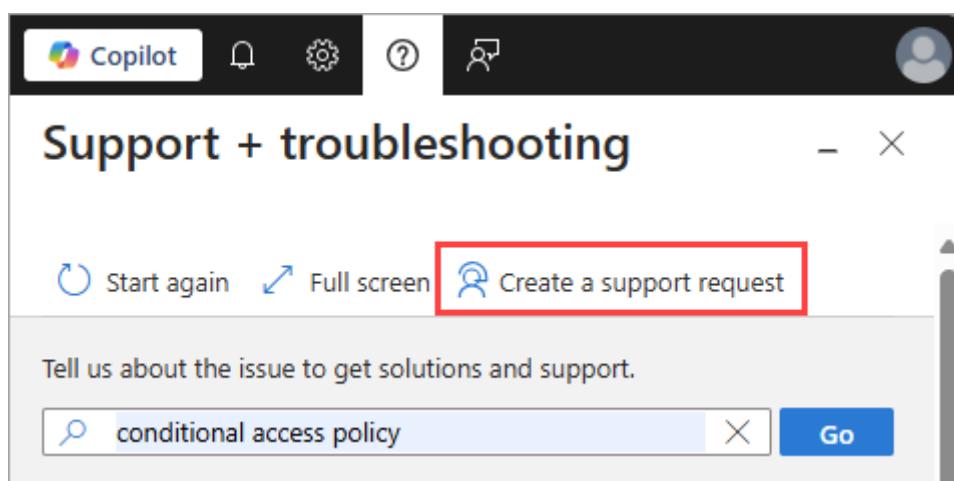
- From the **Diagnose and solve problems** page:

This screenshot shows the same "Diagnose and solve problems" page as the previous one, but with the "New Support Request" button in the top navigation bar highlighted with a red box.

- 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](#)

# Troubleshoot and resolve groups issues

Article • 01/15/2025

This article contains troubleshooting information for groups in Microsoft Entra ID, part of Microsoft Entra.

## Troubleshoot group creation issues

I disabled security group creation in the Azure portal but groups can still be created via PowerShell

The **User can create security groups in Azure portals** setting in the Azure portal controls whether or not non-admin users can create security groups in the Access panel or the Azure portal. It doesn't control security group creation via PowerShell.

To disable group creation for nonadmin users in PowerShell:

1. Verify that nonadmin users are allowed to create groups:

```
PowerShell

Get-MgBetaDirectorySetting | select -ExpandProperty values
```

2. If it returns `EnableGroupCreation : True`, then nonadmin users can create groups.

To disable this feature:

```
PowerShell

Install-Module Microsoft.Graph.Beta.Identity.DirectoryManagement
Import-Module Microsoft.Graph.Beta.Identity.DirectoryManagement
$params = @{
 TemplateId = "62375ab9-6b52-47ed-826b-58e47e0e304b"
 Values = @(
 @{
 Name = "EnableGroupCreation"
 Value = "false"
 }
)
}
Connect-MgGraph -Scopes "Directory.ReadWrite.All"
New-MgBetaDirectorySetting -BodyParameter $params
```

I received a max groups allowed error when trying to create a Dynamic Group in PowerShell

The max number of Dynamic groups per organization is 5,000. When you reach the maximum number of Dynamic groups in your organization, you receive a message in PowerShell that says *Dynamic group policies max allowed groups count reached*.

If you run into this limit, to create any new Dynamic groups, you first need to delete some existing Dynamic groups. There's no way to increase the limit.

## Troubleshoot dynamic membership groups

### I configured a rule on a group but no memberships get updated in the group

1. Verify the values for user or device attributes in the rule. Ensure there are users that satisfy the rule. For devices, check the device properties to ensure any synced attributes contain the expected values.
2. Check the membership processing status to confirm if it's complete. You can check the [membership processing status](#) and the last updated date on the [Overview](#) page for the group.

If everything looks good, allow some time for the group to populate. Depending on the size of your Microsoft Entra organization, the group could take up to 24 hours for populating for the first time or after a rule change.

### I configured a rule, but now the existing members of the rule are removed

This is expected behavior. Existing members of the group are removed when a rule is enabled or changed. Not all existing members are deleted, only users who no longer meet the new rule. The users returned from evaluation of the new rule are added as members to the group. Users who meet both existing rules and new rules remain in the dynamic group. Their license assignments aren't temporarily deleted and their role assignments aren't removed.

### I don't see membership changes instantly when I add or change a rule, why not?

Dedicated membership evaluation is done periodically in an asynchronous background process. Both the number of users in your directory and the size of the resulting group affect processing time.

Typically, directories with small numbers of users see the dynamic membership group changes in less than a few minutes. Directories with a large number of users can take 30 minutes or longer to populate.

### How can I force the group to be processed now?

Currently, there's no way to automatically trigger the group to be processed on

demand. However, you can manually trigger the reprocessing by updating the membership rule to add a whitespace at the end.

## I encountered a rule processing error

The following table lists common rule errors for dynamic membership groups and how to correct them.

[+] [Expand table](#)

Rule parser error	Error usage	Corrected usage
Error: Attribute not supported.	(user.invalidProperty -eq "Value")	(user.department -eq "value")  Make sure the attribute is on the <a href="#">supported properties list</a> .
Error: Operator isn't supported on attribute.	(user.accountEnabled -contains true)	(user.accountEnabled -eq true)  The operator used isn't supported for the property type (in this example, -contains can't be used on type boolean). Use the correct operators for the property type.
Error: Query compilation error.	1. (user.department -eq "Sales") (user.department -eq "Marketing") 2. (user.userPrincipalName -match "*@domain.ext")	1. Missing operator. Use -and or -or to join predicates (user.department -eq "Sales") -or (user.department -eq "Marketing") 2. Error in regular expression used with -match (user.userPrincipalName -match ".*@domain.ext") or alternatively: (user.userPrincipalName -match "@domain.ext\$")

## Next steps

These articles provide additional information on Microsoft Entra ID.

- [Managing access to resources with Microsoft Entra groups](#)
- [Application Management in Microsoft Entra ID](#)
- [What is Microsoft Entra ID?](#)
- [Integrating your on-premises identities with Microsoft Entra ID](#)

# 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	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 associated with identity governance are available with each license. For more information on other features, see [Microsoft Entra plans and pricing](#). 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					

Feature	Free	Microsoft Entra ID P1	Microsoft Entra ID P2	Microsoft Entra ID Governance	Microsoft Entra Suite
Entitlement management - Directly Assign Any User (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)					

Feature	Free	Microsoft Entra ID P1	Microsoft Entra ID P2	Microsoft Entra ID Governance	Microsoft Entra Suite
LCW + Custom Extensions (Logic Apps)				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Identity governance dashboard	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<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 <b>All employees</b> (2,000 employees) can request a specific set of access packages. 150 employees request the access packages.	2,000 employees who <b>can</b> request the access packages	2,000
An Identity Governance Administrator at Woodgrove Bank creates initial catalogs. They create an auto-assignment policy that grants <b>All members of the Sales department</b> (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 <a href="#">Privileged Role Administrators</a> 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](#).

## Related content

- [Microsoft Entra pricing](#)

# 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"><li>• Create administrative units</li><li>• Create and manage members and membership rules of administrative units</li><li>• Assign administrator roles that are scoped to administrative units</li></ul>	<a href="#">administrativeUnit resource type</a> and its associated APIs
Grant, revoke, and retrieve app roles on a resource application for users, groups, or service principals	<a href="#">appRoleAssignment resource type</a> and its associated APIs
Retrieve BitLocker recovery keys	<a href="#">bitlockerRecoveryKey resource type</a> and its associated APIs
Manage custom security attributes	See <a href="#">Overview of custom security attributes using the Microsoft Graph API</a>
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"><li>• Administrative units</li><li>• Applications</li><li>• External user profiles</li><li>• Groups</li></ul>	<ul style="list-style-type: none"><li>• <a href="#">Get</a> or <a href="#">List</a> deleted objects</li><li>• <a href="#">Permanently delete</a> a deleted object</li><li>• <a href="#">Restore a deleted item</a></li><li>• <a href="#">List deleted items owned by user</a></li></ul>

Use cases	API operations
<ul style="list-style-type: none"> <li>• Pending external user profiles</li> <li>• Service principals</li> <li>• Users</li> </ul>	
Manage devices in the cloud	<a href="#">device resource type</a> 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>	<a href="#">deviceLocalCredentialInfo resource type</a> 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 <a href="#">directoryObject</a> 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>	<a href="#">directoryObject</a> 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><a href="#">directoryRole</a> resource type and <a href="#">directoryRoleTemplate</a> resource type and their associated APIs</p> <p><a href="#">roleManagement</a> resource type and its associated APIs (<b>recommended</b>)</p> <p>These APIs allow you to make direct role assignments. Alternatively, you can use Privileged Identity Management APIs for <a href="#">Microsoft Entra roles</a> and <a href="#">groups</a> 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"> <li>• Settings for Microsoft 365 groups such as guest user access, classifications, and naming policies</li> <li>• Password rule settings such as banned password lists and lockout duration</li> <li>• Prohibited names for applications, reserved words, and blocking trademark violations</li> <li>• Custom conditional access policy URL</li> </ul>	<p><a href="#">groupSetting</a> resource type and <a href="#">groupSettingTemplate</a> resource type and their associated APIs</p> <p>For more information, see <a href="#">Overview of group settings</a>.</p>

Use cases	API operations
<ul style="list-style-type: none"> <li>Consent policies such as user consent requests, group-specific consent, and consent for risky apps</li> </ul>	
<p>Domain management operations such as:</p> <ul style="list-style-type: none"> <li>associating a domain with your tenant</li> <li>retrieving DNS records</li> <li>verifying domain ownership</li> <li>associating specific services with specific domains</li> <li>deleting domains</li> </ul>	<a href="#">domain resource type</a> and its associated APIs
<p>Configure and manage staged rollout of specific Microsoft Entra ID features</p>	<a href="#">featureRolloutPolicy resource type</a> and its associated APIs
<p>Monitor licenses and subscriptions for the tenant</p>	<ul style="list-style-type: none"> <li><a href="#">companySubscription resource type</a> and its associated APIs</li> <li><a href="#">subscribedSku resource type</a> and its associated APIs</li> </ul>
<p>Configure options that are available in Microsoft Entra Cloud Sync such as preventing accidental deletions and managing group writebacks</p>	<a href="#">onPremisesDirectorySynchronization resource type</a> and its associated APIs
<p>Manage the base settings for your Microsoft Entra tenant</p>	<a href="#">organization resource type</a> and its associated APIs
<p>Retrieve the organizational contacts that might be synchronized from on-premises directories or from Exchange Online</p>	<a href="#">orgContact resource type</a> 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>	<a href="#">tenantInformation resource type</a> and its associated APIs
<p>Manage the delegated permissions and their assignments to service principals in the tenant</p>	<a href="#">OAuth2PermissionGrant resource type</a> 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>	<a href="#">authenticationEventListener resource type</a> and its associated APIs

Use cases	API operations
defined outside Microsoft Entra ID	
Manage authentication methods that are supported in Microsoft Entra ID	See <a href="#">Microsoft Entra authentication methods API overview</a> and <a href="#">Microsoft Entra authentication methods policies API overview</a>
Manage the authentication methods or combinations of authentication methods that you can apply as grant control in Microsoft Entra Conditional Access	See <a href="#">Microsoft Entra authentication strengths API overview</a>
<p>Manage tenant-wide authorization policies such as:</p> <ul style="list-style-type: none"> <li>• enable SSPR for administrator accounts</li> <li>• enable self-service join for guests</li> <li>• limit who can invite guests</li> <li>• whether users can consent to risky apps</li> <li>• block the use of MSOL</li> <li>• customize the default user permissions</li> <li>• identity private preview features enabled</li> <li>• Customize the guest user permissions between <i>User</i>, <i>Guest User</i>, and <i>Restricted Guest User</i></li> </ul>	<a href="#">authorizationPolicy resource type</a> and its associated APIs
Manage the policies for certificate-based authentication in the tenant	<a href="#">certificateBasedAuthConfiguration resource type</a> and its associated APIs
Manage Microsoft Entra conditional access policies	<a href="#">conditionalAccessRoot resource type</a> 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 <a href="#">Cross-tenant access settings API overview</a>
Configure how and which external systems interact with Microsoft Entra ID during a user authentication session	<a href="#">customAuthenticationExtension resource type</a> and its associated APIs
Manage requests against user data in the organization, such as exporting personal data	<a href="#">dataPolicyOperation resource type</a> and its associated APIs
Force autoacceleration sign-in to skip the username entry screen and automatically forward users to federated sign-in endpoints	<a href="#">homeRealmDiscoveryPolicy resource type</a> 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 <a href="#">Use the Microsoft Graph identity protection APIs</a>

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"> <li>• Manage identity providers for external identities, including social identity providers, OIDC, Apple, SAML/WS-Fed, and built-in providers</li> <li>• Manage configuration for federated domains and token validation</li> </ul>	<a href="#">identityProviderBase resource type</a> and its associated APIs
Define a group of tenants belonging to your organization and streamline intra-organization cross-tenant collaboration	See <a href="#">Multitenant organization API overview</a>
Customize sign-in UIs to match your company branding, including applying branding that's based on the browser language	<a href="#">organizationalBranding resource type</a> 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"> <li>• <a href="#">b2xIdentityUserFlow</a> to configure the base user flow and its properties such as identity providers</li> <li>• <a href="#">identityUserFlowAttribute</a> to manage built-in and custom user flow attributes</li> <li>• <a href="#">identityUserFlowAttributeAssignment</a> to manage user flow attribute assignments</li> <li>• <a href="#">userFlowLanguageConfiguration resource type</a> to configure custom languages for user flows</li> </ul>
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"> <li>• <a href="#">authenticationEventsFlow resource type</a> and its associated APIs</li> <li>• <a href="#">identityUserFlowAttribute</a> to manage built-in and custom user flow attributes</li> </ul>
Manage app consent policies and condition sets	<a href="#">permissionGrantPolicy resource type</a>
Enable or disable security defaults in Microsoft Entra ID	<a href="#">identitySecurityDefaultsEnforcementPolicy resource type</a>

## 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	<a href="#">authenticationEventsFlow resource type</a> 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 <a href="#">identityProviderBase resource type</a> and its associated APIs
Configuring custom URL domains in Microsoft Entra External ID in external tenants	The <code>CustomUrlDomain</code> value for the <b>supportedServices</b> property of <a href="#">domain resource type</a> and its associated APIs
Customize sign-in UIs to match your company branding, including applying branding that's based on the browser language	<a href="#">organizationalBranding resource type</a> and its associated APIs
Manage identity providers for Microsoft Entra External ID, such as social identities	<a href="#">identityProviderBase resource type</a> and its associated APIs
Manage user profiles in Microsoft Entra External ID for customers	For more information, see <a href="#">Default user permissions in customer tenants</a>
Add your own business logic to the authentication experiences by integrating with systems that are external to Microsoft Entra ID	<a href="#">authenticationEventListener resource type</a> and <a href="#">customAuthenticationExtension resource type</a> 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	<a href="#">contract resource type</a> 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 <a href="#">Granular delegated admin privileges (GDAP)</a> <a href="#">API overview</a>

## 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.

# az ad

Reference

## ! Note

This command group has commands that are defined in both Azure CLI and at least one extension. Install each extension to benefit from its extended capabilities. [Learn more](#) about extensions.

Manage Microsoft Entra ID (formerly known as Azure Active Directory, Azure AD, AAD) entities needed for Azure role-based access control (Azure RBAC) through Microsoft Graph API.

## Commands

[Expand table](#)

Name	Description	Type	Status
<a href="#">az ad app</a>	Manage Microsoft Entra applications.	Core	GA
<a href="#">az ad app create</a>	Create an application.	Core	GA
<a href="#">az ad app credential</a>	Manage an application's password or certificate credentials.	Core	GA
<a href="#">az ad app credential delete</a>	Delete an application's password or certificate credentials.	Core	GA
<a href="#">az ad app credential list</a>	List an application's password or certificate credential metadata. (The content of the password or certificate credential is not retrievable.).	Core	GA
<a href="#">az ad app credential reset</a>	Reset an application's password or certificate credentials.	Core	GA
<a href="#">az ad app delete</a>	Delete an application.	Core	GA
<a href="#">az ad app federated-credential</a>	Manage application federated identity credentials.	Core	GA
<a href="#">az ad app federated-credential create</a>	Create application federated identity credential.	Core	GA
<a href="#">az ad app federated-credential</a>	Delete application federated identity credential.	Core	GA

Name	Description	Type	Status
delete			
az ad app federated-credential list	List application federated identity credentials.	Core	GA
az ad app federated-credential show	Show application federated identity credential.	Core	GA
az ad app federated-credential update	Update application federated identity credential.	Core	GA
az ad app list	List applications.	Core	GA
az ad app owner	Manage application owners.	Core	GA
az ad app owner add	Add an application owner.	Core	GA
az ad app owner list	List application owners.	Core	GA
az ad app owner remove	Remove an application owner.	Core	GA
az ad app permission	Manage an application's OAuth2 permissions.	Core	GA
az ad app permission add	Add an API permission.	Core	GA
az ad app permission admin-consent	Grant Application & Delegated permissions through admin-consent.	Core	GA
az ad app permission delete	Remove an API permission.	Core	GA
az ad app permission grant	Grant the app an API Delegated permissions.	Core	GA
az ad app permission list	List API permissions the application has requested.	Core	GA
az ad app permission list-grants	List Oauth2 permission grants.	Core	GA
az ad app show	Get the details of an application.	Core	GA

Name	Description	Type	Status
<a href="#">az ad app update</a>	Update an application.	Core	GA
<a href="#">az ad ds</a>	Manage domain service with azure active directory.	Extension	Experimental
<a href="#">az ad ds create</a>	Create a new domain service with the specified parameters.	Extension	Experimental
<a href="#">az ad ds delete</a>	The Delete Domain Service operation deletes an existing Domain Service.	Extension	Experimental
<a href="#">az ad ds list</a>	List domain services in resource group or in subscription.	Extension	Experimental
<a href="#">az ad ds show</a>	Get the specified domain service.	Extension	Experimental
<a href="#">az ad ds update</a>	Update the existing deployment properties for domain service.	Extension	Experimental
<a href="#">az ad ds wait</a>	Place the CLI in a waiting state until a condition of the ad ds is met.	Extension	Experimental
<a href="#">az ad group</a>	Manage Microsoft Entra groups.	Core	GA
<a href="#">az ad group create</a>	Create a group.	Core	GA
<a href="#">az ad group delete</a>	Delete a group.	Core	GA
<a href="#">az ad group get-member-groups</a>	Get a collection of object IDs of groups of which the specified group is a member.	Core	GA
<a href="#">az ad group list</a>	List groups in the directory.	Core	GA
<a href="#">az ad group member</a>	Manage group members.	Core	GA
<a href="#">az ad group member add</a>	Add a member to a group.	Core	GA
<a href="#">az ad group member check</a>	Check if a member is in a group.	Core	GA
<a href="#">az ad group member list</a>	Get the members of a group.	Core	GA
<a href="#">az ad group member remove</a>	Remove a member from a group.	Core	GA
<a href="#">az ad group owner</a>	Manage group owners.	Core	GA
<a href="#">az ad group owner</a>	Add a group owner.	Core	GA

Name	Description	Type	Status
<a href="#">add</a>			
<a href="#">az ad group owner list</a>	List group owners.	Core	GA
<a href="#">az ad group owner remove</a>	Remove a group owner.	Core	GA
<a href="#">az ad group show</a>	Get the details of a group.	Core	GA
<a href="#">az ad signed-in-user</a>	Show graph information about current signed-in user in CLI.	Core	GA
<a href="#">az ad signed-in-user list-owned-objects</a>	Get the list of directory objects that are owned by the user.	Core	GA
<a href="#">az ad signed-in-user show</a>	Get the details for the currently logged-in user.	Core	GA
<a href="#">az ad sp</a>	Manage Microsoft Entra service principals.	Core	GA
<a href="#">az ad sp create</a>	Create a service principal.	Core	GA
<a href="#">az ad sp create-for-rbac</a>	Create an application and its associated service principal, optionally configure the service principal's RBAC role assignments.	Core	GA
<a href="#">az ad sp credential</a>	Manage a service principal's password or certificate credentials.	Core	GA
<a href="#">az ad sp credential delete</a>	Delete a service principal's password or certificate credentials.	Core	GA
<a href="#">az ad sp credential list</a>	List a service principal's password or certificate credential metadata. (The content of the password or certificate credential is not retrievable.).	Core	GA
<a href="#">az ad sp credential reset</a>	Reset a service principal's password or certificate credentials.	Core	GA
<a href="#">az ad sp delete</a>	Delete a service principal.	Core	GA
<a href="#">az ad sp list</a>	List service principals.	Core	GA
<a href="#">az ad sp owner</a>	Manage service principal owners.	Core	GA
<a href="#">az ad sp owner list</a>	List service principal owners.	Core	GA
<a href="#">az ad sp show</a>	Get the details of a service principal.	Core	GA
<a href="#">az ad sp update</a>	Update a service principal.	Core	GA

Name	Description	Type	Status
<a href="#">az ad user</a>	Manage Microsoft Entra users.	Core	GA
<a href="#">az ad user create</a>	Create a user.	Core	GA
<a href="#">az ad user delete</a>	Delete a user.	Core	GA
<a href="#">az ad user get-member-groups</a>	Get groups of which the user is a member.	Core	GA
<a href="#">az ad user list</a>	List users.	Core	GA
<a href="#">az ad user show</a>	Get the details of a user.	Core	GA
<a href="#">az ad user update</a>	Update a user.	Core	GA

# Microsoft Entra service limits and restrictions

Article • 01/31/2025

This article contains the usage constraints and other service limits for the Microsoft Entra ID, part of Microsoft Entra, service. If you're looking for the full set of Microsoft Azure service limits, see [Azure Subscription and Service Limits, Quotas, and Constraints](#).

Here are the usage constraints and other service limits for the Microsoft Entra service.

[+] [Expand table](#)

Category	Limit
Tenants	<ul style="list-style-type: none"><li>A single user can belong to a maximum of 500 Microsoft Entra tenants as a member or a guest.</li><li>Create a maximum of 200 tenants.</li><li>Limit of 300 <a href="#">license-based subscriptions</a> (such as Microsoft 365 subscriptions) per tenant</li></ul>
Domains	<ul style="list-style-type: none"><li>You can add no more than 5,000 managed domain names.</li><li>If you set up all of your domains for federation with on-premises Active Directory, you can add no more than 2,500 domain names in each tenant.</li></ul>
Resources	<ul style="list-style-type: none"><li>By default, a maximum of 50,000 Microsoft Entra resources can be created in a single tenant by users of the Microsoft Entra ID Free edition. If you have at least one verified domain, the default Microsoft Entra service quota for your organization is extended to 300,000 Microsoft Entra resources. The Microsoft Entra service quota for organizations created by self-service sign-up remains 50,000 Microsoft Entra resources, even after you perform an internal admin takeover and the organization is converted to a managed tenant with at least one verified domain. This service limit is unrelated to the pricing tier limit of 500,000 resources on the Microsoft Entra pricing page. To go beyond the default quota, you must contact Microsoft Support.</li><li>A non-admin user can create no more than 250 Microsoft Entra resources. Both active resources and deleted resources that are available to restore count toward this quota. Only deleted Microsoft Entra resources that were deleted fewer than 30 days ago are available to restore. Deleted Microsoft Entra resources that are no longer available to restore count toward this quota at a value of one-quarter for 30 days. If you have developers who are likely to repeatedly exceed this quota in the course of their regular duties, you can <a href="#">create and assign a custom role</a> with permission to create a limitless number of app registrations.</li></ul>

Category	Limit
	<ul style="list-style-type: none"> <li>Resource limitations apply to all directory objects in a given Microsoft Entra tenant, including users, groups, applications, and service principals.</li> </ul>
Schema extensions	<ul style="list-style-type: none"> <li>String-type extensions can have a maximum of 256 characters.</li> <li>Binary-type extensions are limited to 256 bytes.</li> <li>Only 100 extension values, across <i>all</i> types and <i>all</i> applications, can be written to any single Microsoft Entra resource.</li> <li>Only User, Group, TenantDetail, Device, Application, and ServicePrincipal entities can be extended with string-type or binary-type single-valued attributes.</li> </ul>
Applications	<ul style="list-style-type: none"> <li>A maximum of 100 users and service principals can be owners of a single application.</li> <li>A user, group, or service principal can have a maximum of 1,500 app role assignments. The limitation is on the assigned service principal, user, or group across all app roles and not on the number of assignments of a single app role. This limit includes app role assignments where the resource service principal has been soft-deleted.</li> <li>A user can have credentials configured for a maximum of 48 apps using password-based single sign-on. This limit only applies for credentials configured when the user is directly assigned the app, not when the user is a member of a group that is assigned.</li> <li>A group can have credentials configured for a maximum of 48 apps using password-based single sign-on.</li> <li>See additional limits in <a href="#">Validation differences by supported account types</a>.</li> </ul>
Application manifest	<p>A maximum of 1,200 entries can be added to the application manifest.</p> <p>See additional limits in <a href="#">Validation differences by supported account types</a>.</p>
Groups	<ul style="list-style-type: none"> <li>A non-admin user can create a maximum of 250 groups in a Microsoft Entra organization. Any Microsoft Entra admin who can manage groups in the organization can also create an unlimited number of groups (up to the Microsoft Entra object limit). If you assign a role to a user to remove the limit for that user, assign a less privileged, built-in role such as User Administrator or Groups Administrator.</li> <li>A Microsoft Entra organization can have a maximum of 15,000 dynamic groups and dynamic administrative units combined.</li> <li>A maximum of 500 <a href="#">role-assignable groups</a> can be created in a single Microsoft Entra organization (tenant).</li> <li>A maximum of 100 users can be owners of a single group.</li> <li>Any number of Microsoft Entra resources can be members of a single group.</li> </ul>

Category	Limit
	<ul style="list-style-type: none"> <li>• A user can be a member of any number of groups. When security groups are being used in combination with SharePoint Online, a user can be a part of 2,049 security groups in total. This includes both direct and indirect group memberships. When this limit is exceeded, authentication and search results become unpredictable.</li> <li>• Starting with Microsoft Entra Connect v2.0, the V2 endpoint is the default API. The number of members in a group that you can synchronize from your on-premises Active Directory to Microsoft Entra ID by using Microsoft Entra Connect is limited to 250,000 members. For more information, see <a href="#">Microsoft Entra Connect Sync V2</a>.</li> <li>• When you select a list of groups, you can assign a group expiration policy to a maximum of 500 Microsoft 365 groups. There's no limit when the policy is applied to all Microsoft 365 groups.</li> </ul>

At this time, the following scenarios are supported with nested groups:

- One group can be added as a member of another group, and you can achieve group nesting.
- Group membership claims. When an app is configured to receive group membership claims in the token, nested groups in which the signed-in user is a member are included.
- Conditional Access (when a Conditional Access policy has a group scope).
- Restricting access to self-serve password reset.
- Restricting which users can do Microsoft Entra join and device registration.

The following scenarios are *not* supported with nested groups:

- App role assignment, for both access and provisioning. Assigning groups to an app is supported, but any groups nested within the directly assigned group won't have access.
- Group-based licensing (assigning a license automatically to all members of a group).
- Microsoft 365 Groups.

Category	Limit
Application Proxy	<ul style="list-style-type: none"> <li>A maximum of 500 transactions* per second per Application Proxy application.</li> <li>A maximum of 750 transactions per second for the Microsoft Entra organization.</li> </ul>
	<p>*A transaction is defined as a single HTTP request and response for a unique resource. When clients are throttled, they receive a 429 response (too many requests). Transaction metrics are collected on each connector and can be monitored using performance counters under the object name <code>Microsoft Entra private network connector</code>.</p>
Access Panel	There's no limit to the number of applications per user that can be displayed in the Access Panel, regardless of the number of assigned licenses.
Reports	A maximum of 1,000 rows can be viewed or downloaded in any report. Any additional data is truncated.
Administrative units	<ul style="list-style-type: none"> <li>A Microsoft Entra resource can be a member of no more than 30 administrative units.</li> <li>A maximum of 100 restricted management administrative units in a tenant.</li> <li>A Microsoft Entra organization can have a maximum of 15,000 dynamic membership groups and dynamic administrative units combined.</li> </ul>
Microsoft Entra roles and permissions	<ul style="list-style-type: none"> <li>A maximum of 100 <a href="#">Microsoft Entra custom roles</a> can be created in a Microsoft Entra organization.</li> <li>A maximum of 150 Microsoft Entra custom role assignments for a single principal at any scope.</li> <li>A maximum of 100 Microsoft Entra built-in role assignments for a single principal at non-tenant scope (such as an administrative unit or Microsoft Entra object). There's no limit to Microsoft Entra built-in role assignments at tenant scope. For more information, see <a href="#">Assign Microsoft Entra roles</a>.</li> <li>A group can't be added as a <a href="#">group owner</a>.</li> <li>A user's ability to read other users' tenant information can be restricted only by the Microsoft Entra organization-wide switch to disable all non-admin users' access to all tenant information (not recommended). For more information, see <a href="#">To restrict the default permissions for member users</a>.</li> <li>It might take up to 15 minutes or you might have to sign out and sign back in before admin role membership additions and revocations take effect.</li> </ul>
Conditional Access Policies	A maximum of 195 policies can be created in a single Microsoft Entra organization (tenant).

Category	Limit
Terms of use	You can add no more than 40 terms to a single Microsoft Entra organization (tenant).
Multitenant organizations	<ul style="list-style-type: none"><li>A maximum of 100 active tenants, including the owner tenant. The owner tenant can add more than 100 pending tenants, but they won't be able to join the multitenant organization if the limit is exceeded. This limit is applied at the time a pending tenant joins a multitenant organization.</li></ul> <p>This limit is specific to the number of tenants in a multitenant organization. It doesn't apply to cross-tenant synchronization by itself.</p>

## Related content

- [Configure group claims for applications by using Microsoft Entra ID](#)
- [Sign up for Azure as an organization](#)
- [How Azure subscriptions are associated with Microsoft Entra ID](#)

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback ↗](#)