

Azure Active Directory Group Management - Adoption Kit

Version: 3.0

For the latest version, please check <https://aka.ms/aadadoptionkits>

Contents

Azure Active Directory Group Management - Adoption Kit.....	1
Awareness	2
Business overview.....	2
Pricing and licensing requirements.....	2
Key benefits	3
Announcements.....	3
Training/learning resources	4
Level 100 concepts.....	4
Training.....	4
Videos.....	4
Online Courses.....	4
Deployment plan.....	5
Plan group types.....	5
Manage group memberships.....	5
Bulk memberships.....	6
Use PowerShell cmdlets.....	6
Troubleshoot.....	6
Manage groups.....	Error! Bookmark not defined.
In Conditional Access policy	7
Assign product licenses	7
In SharePoint and Exchange online.....	7
Access SaaS applications.....	8
Customer stories/case studies	Error! Bookmark not defined.
Support and feedback.....	8

Awareness

This section helps you to analyze the benefits of Azure Active Directory Group Management. You will learn about the ease of use, benefits, pricing, and licensing model. You will also receive up-to-date announcements that discuss ongoing improvements.

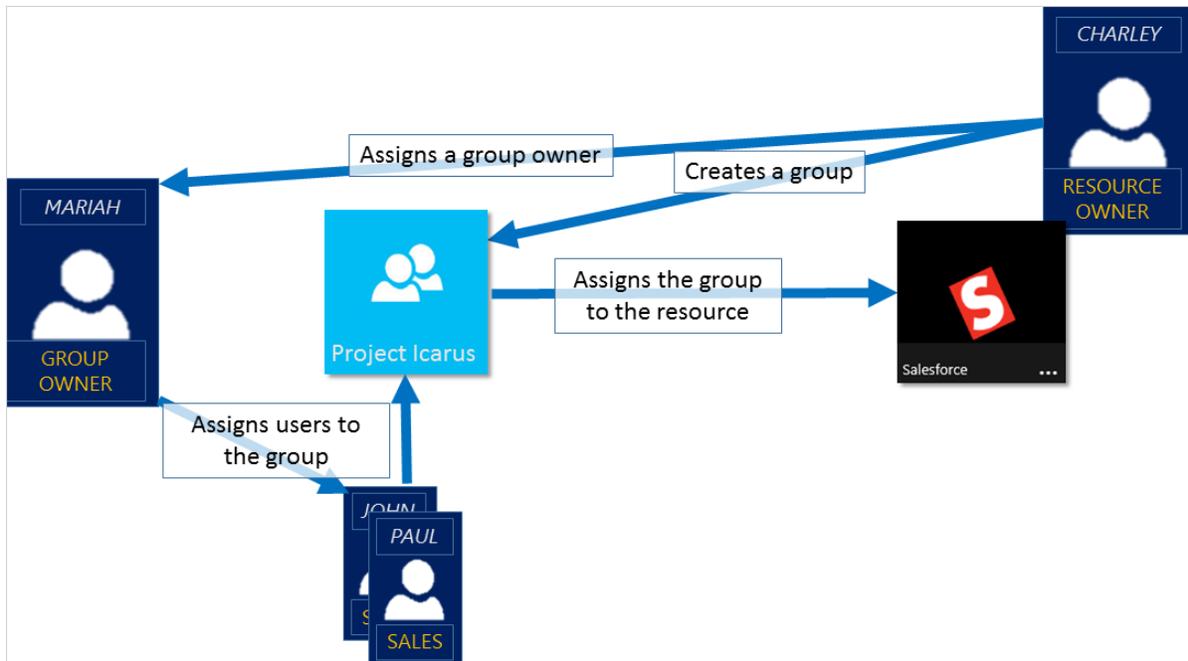
Business overview

An **Azure Active Directory (Azure AD) group** is used to manage member access to shared resources for a group of users. It can also provide collaboration opportunities to members by giving access to shared mailbox, calendar, files and more.

As your organization grows, you can use groups to:

- Assign licenses to groups and make large scale license management easier
- Assign group access to the enterprise apps that are deployed in your Azure AD organization.
- Grant access to resources that are external, such as SaaS applications or SharePoint sites
- Target specific set of users in a conditional access policy and more

Using groups lets the resource owner (or Azure AD directory owner), assign a set of access permissions to all the members of the group, instead of having to provide the rights one-by-one. A user inherits the policy of the group it is a member of.



Pricing and licensing requirements

The Azure AD Group Management features helps to accomplish tasks quickly and accommodate growth. The availability of a feature is dependent on the type of Azure AD license (free or paid). For example, group-based licensing is available on purchase of Azure AD Premium P1.

To learn more about the pricing of Azure AD editions that offer group management, and other advanced group features, refer to [Azure AD pricing](#).

Key benefits

Using Azure AD Group Management offers the following benefits:



Intuitive usage

You can manage your groups from a simple, easy to deploy and customizable access portal. There are added policy controls for administrators and groups owners and enhanced visual design to provide a better end-user experience.



Cost-effective

Dynamic group membership and self-service group management reduces the administrative overhead of adding and removing users. This reduces the cost, time, and workload of IT support.



Security

Groups can be used as a decision signal when you create a Conditional Access policy. This allows streamlined and secured resource access. Administrators can set rules for groups that are created in Azure AD based on user attributes. This allows members to be automatically added to or removed from a security group.



Self-service

Self-Service feature delegates group management to your employees. This enables employees to create groups and manage memberships in groups they own.

Announcements

Azure AD receives improvements on an ongoing basis. To stay up to date with the most recent developments, refer to [What's new in Azure AD?](#)

Training/learning resources

The following resources would be a good start to learn more about Azure AD Group Management. These include level 100 concepts, videos by our experts and links to online courses.

Level 100 concepts

Refer the following links to get started with Azure AD Group Management:

- Learn [what is enterprise user management?](#)
- Learn how you can [manage app and resource access with Azure AD groups](#)
- Understand [the types of groups and its memberships](#)
- What are [dynamic groups](#)?
- Know more about [Office 365 groups](#)
- Understand [group-based licensing in Azure AD](#)
- Learn about [self-service group management](#).

To learn more, deep-dive into [Enterprise User Management](#) documentation.

Training

Videos

Watch this video - [Group management | Azure Active Directory](#).

Learn about group functionalities and how your organization can leverage the latest features of Azure AD groups for your own group management.

Online Courses

Refer to the following Azure AD Group Management courses on [PluralSight.com](#):

Course	Description
Managing identities in Microsoft Azure AD	Learn the basics of managing an Azure AD environment, including users, groups, devices, and applications. Refer to Managing Azure Active Directory Users and Groups module.
Managing Microsoft Azure AD	Explore the key management activities and actions related to Azure AD. Refer to User and Group Management using the Azure portal module.
Getting started with the Microsoft Enterprise Mobility Suite	Learn the best practices for extending on-premises assets to the cloud in a manner that allows for authentication, authorization, encryption, and a secured mobile experience.

Deployment plan

This section provides guidance to create groups, manage group memberships, and troubleshoot group issues.

Plan group types

There are two types of groups:

Security. Use these groups to [manage member access to shared resources](#). Your resources can be part of the Azure AD organization, such as permissions to manage objects through roles in Azure AD, or external to the organization, such as for Software as a Service (SaaS) apps, Azure services, SharePoint sites, and on-premises resources.

Office 365. Groups in [Office 365](#) let you choose a set of people that you wish to collaborate with and easily set up a collection of resources for those people to share. Resources such as a shared Outlook inbox, shared calendar, or a document library for collaborating on files.

For Office365 groups, follow these best practices:

- [Set up a group naming policy for your organization](#). For example, you could use the naming policy to communicate the function of a group, membership, geographic region, or who created the group.
- [Configure the expiration policy](#) to manage the lifecycle of Office 365 group.
- [Assign sensitivity labels](#) published by Office 365 compliance center. Sensitivity labels apply to group across services like Outlook, Microsoft Teams, and SharePoint.

Manage group memberships

There are many ways to manage group memberships in the Azure portal.

Assigned group. When you assign a group, you add specific users to be members of this group and have unique permissions. Learn to [create a basic group and add members](#) at the same time.

Dynamic group. Use dynamic membership rules to automatically add and remove members. If a member's attributes change, the system looks at your dynamic group rules for the directory to see if the member meets the rule requirements (is added) or no longer meets the rules requirements (is removed). You can also create dynamic groups to add or remove devices based on rules. You can create a dynamic group for either devices or users, but not for both. You also cannot create a device group based on the device owners' attributes. Device membership rules can only reference device attributions.

Learn to [enable dynamic membership](#) based on complex attribute-based rules.

Self-Service Group Management. You can also [set up self-service group management](#) to enable users to create and manage their own groups. The owner of the group can approve or deny membership requests and can delegate control of group membership. Self-service group management features are not available for mail-enabled security groups or distribution lists.

Once your groups are created, you can perform these operations:

Links	Description
Manage memberships of a group	Add or remove members to an existing group.
Add or remove group owners	Groups are owned and managed by group owners. Group owners can be users or service principals and are able to manage the group including membership. It is recommended for every group to have at least one owner.
Manage settings of a group	Edit a group's settings, including updating its name, description, or membership type.
Delete a group	Typically, a group will be deleted because - you incorrectly set the Group type to the wrong option, created the wrong or a duplicate group by mistake or no longer need the group.
Restore a deleted Office 365 group	When you delete an Office 365 group in the Azure AD, 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.
Add or remove a group from another group	You can add an existing Security group to another existing Security group (also known as nested groups), creating a member group (subgroup) and a parent group. The member group inherits the attributes and properties of the parent group, saving you configuration time.
Manage dynamic rules for users in a group	Create complex attribute-based rules to enable dynamic memberships for groups.
Validate a dynamic membership rule	Evaluate whether user or device meets the rule criteria and aid in troubleshooting when membership is not expected.
Change static group membership to dynamic	Convert existing groups from static to dynamic membership using either Azure AD Admin center or PowerShell cmdlets
See existing groups	View your organization's existing groups and group members using the Azure portal.

Bulk memberships

Manage bulk memberships in the Azure portal using comma-separated values (CSV) files. Refer to the following links:

- [Bulk add group members](#)
- [Bulk remove group members](#)
- [Bulk download members of a group](#)
- [Bulk download a list of groups](#)

Use PowerShell cmdlets

Office365 groups can also be managed using PowerShell cmdlets. See [Azure Active Directory cmdlets for configuring group settings](#).

Troubleshoot

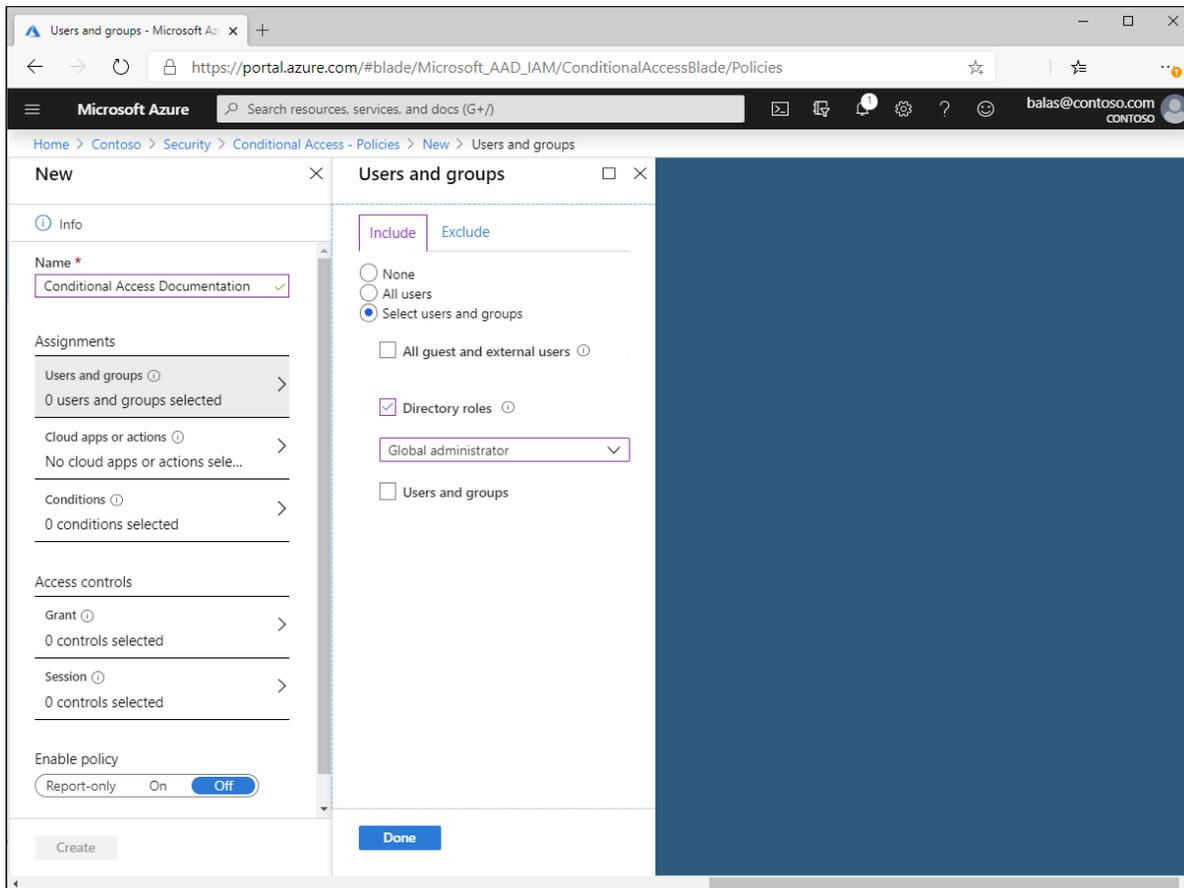
Refer to [Troubleshoot and resolve groups issues](#).

Advanced features of Group Management

Azure AD Groups can be used to manage multiple identity management tasks. This section walks you through these tasks.

Set Conditional Access policy

Users and groups are one of the signals in the decision process when you [create a Conditional Access policy](#). This allows targeting of specific set of users. For example, organizations can select a group that contains all members of the HR department when an HR app is selected as the cloud app.



Assign product licenses

For large scale management, Azure AD now includes [group-based licensing](#). Azure AD ensures that the licenses are assigned to all members of the group. Any new members who join the group are automatically 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.

Access SharePoint and Exchange online

You can assign group access to [enterprise apps such as Exchange Online and SharePoint Online](#) deployed on your Azure AD tenant. For example, Microsoft Teams relies heavily on Exchange Online and SharePoint Online for core productivity scenarios, like meetings, calendars, and file sharing.

Access SaaS applications

You can use groups to [assign access to a SaaS applications that are integrated with Azure AD](#). For example, if you want to assign access for the marketing department to use five different SaaS applications, you can create a group that contains the users in the marketing department, and then assign that group to those five SaaS applications that are needed by the marketing department.

Support and feedback

How can we improve Azure AD Group Management? This section provides links to discussion forums and technical community support email IDs.

We encourage you to join our [Technical Community](#), a platform to Microsoft Azure Active Directory users and Microsoft to interact. It is a central destination for education and thought leadership on best practices, product news, live events, and roadmap.

If you have technical questions or need help with Azure, please try [StackOverflow](#) or visit the MSDN [Azure AD forums](#).

Tell us what you think of Azure and what you want to see in the future. If you have suggestions, please submit an idea or vote up an idea at our User Voice Channel - feedback.azure.com.

Next steps

- [Azure AD fundamentals](#)
- [Understand resource access in Azure](#)