Azure Active Directory Self-Service Group Management - Adoption Kit

Contents

Awareness

This section helps you to analyze the benefits of Azure Active Directory (Azure AD) Group Management. You will learn about the ease of use, pricing, and licensing model, as well as customer stories about how it helped improve their business. You will also receive up-to-date announcements and access to blogs that discuss ongoing improvements.

Business Overview

Management of Azure AD Groups helps to accomplish tasks quickly and accommodate growth. You can use Groups in Azure AD to simplify tasks when you want to target many users for the operation. Within Azure AD, a Group is a collection of users and is primarily used to assign permissions to use resources. A user inherits the policies of the Group they are a member of.

There are two ways to add members to a Group:

- **Assigned (static):** Used when administrators and users add and remove members manually or
- **Dynamic:** Used when membership is determined by a query based on user properties.

You can change a group's membership from assigned (static) to dynamic (or vice-versa) In Azure AD. Refer to Change static group membership to dynamic in Azure Active Directory.

Once groups are defined, you can use them as follows:

- **Set up self-service group management**
  You can enable users to create and manage their own security groups or Office 365 groups in Azure AD. 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. Refer to Set up self-service group management in Azure Active Directory.

- **In a Conditional access policy**
  Select **specific users and groups** in the policy. For example, you can select a group that contains all members of the HR department when an HR app is selected as the cloud app. A group can be any type of group in Azure AD, including dynamic or assigned security and distribution groups. Refer to What are conditions in Azure Active Directory conditional access?

- **Assign licenses**
  You can assign one or more product licenses to a group. 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. Refer to What is group-based licensing in Azure Active Directory?

- **In SharePoint and Exchange online**
  You can use Azure AD to assign group access to the enterprise apps that are deployed in your Azure AD tenant. Using Azure AD Conditional Access, groups can control how users access your cloud apps such as SharePoint online and Exchange online. As an example, Microsoft Teams relies heavily on Exchange Online and SharePoint Online for core productivity scenarios, like meetings, calendars, and file sharing. Conditional

access policies that are set for these cloud apps apply to Microsoft Teams when a user signs directly into Microsoft Teams. Refer to How To: Set up SharePoint Online and Exchange Online for Azure Active Directory conditional access

- **For application access**
  You can use groups to assign access to a SaaS application that's 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. Refer to Using a group to manage access to SaaS applications

Pricing and Licensing Requirements

The Azure AD Group Management features help in simplifying the tasks when you are targeting many users for the operations. Therefore, 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 Active Directory pricing.

Key Benefits

Here are the key benefits of using Azure AD Group Management:

Security
Streamlined, simplified, and secured resource management. 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. These groups can be used to provide access to applications or cloud resources and to assign licenses to members.

Cost-effective
Reduces the cost, time, and workload of IT support with self-service group membership. The self-service group management feature gives you the ability to delegate group management to your employees. With this feature they can create groups and manage memberships in groups they own.

Self-service
Delegates group management to your employees. The self-service group management feature capabilities enable employees to create groups and manage memberships in groups they own.

Customer stories/Case studies

Discover how Azure AD customers are gaining more insights into their on-premises identity solution with Azure AD Group Management. Read this featured story:

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

The George Washington University: Enhancing digital and physical security on campus with cloud-based identity and access management. "Dynamic group management for the students will ensure automatic access to the software and apps required by each program of study."

To learn more about customer and partner experiences on Azure AD Group Management, visit See the amazing things people are doing with Azure.

Announcements/Blogs

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 Active Directory.

Blogs by the Tech Community and Microsoft Identity Division:

- November 26, 2018, Ignite Recap 1: Automating the Identity Lifecycle Process
- November 02, 2018, Azure AD group-based license management is now generally available!

Training/Learning Resources

The section provides concepts, role-based guidance, online training and lists resources available on Azure AD Group Management.

Level 100 Knowledge/Concepts

Learn what Azure AD Group Management is and how it helps you perform access and resource management. See Users, groups, licensing, and roles for large organizations

Additionally, refer to the following links:

- Add/Remove/Update groups (Assigned):
  - Watch this video: How to configure and assign groups in Windows Azure AD?
  - How to Create a basic group and add members using Azure Active Directory?
  - How do you Edit your group information using Azure Active Directory
- Dynamic group:
  - Watch this video: Azure AD: Introduction to Dynamic Memberships for Groups
  - How to Create a dynamic group and check status
  - Dynamic membership rules for groups in Azure Active Directory
  - Change static group membership to dynamic in Azure Active Directory
  - Follow Tutorial: Add or remove group members automatically
- Group-based licensing:
  - What is group-based licensing in Azure Active Directory?
- Conditional access

    - What are conditions in Azure Active Directory conditional access?
- Self-Service
    - Set up self-service group management in Azure Active Directory
- Access Reviews
    - How do you Manage app and resource access using Azure Active Directory groups?

Role-Based Guidance

IT Administrator Staff

The Global Administrator has access to all administrative features. By default, the person who signs up for an Azure subscription is assigned the Global Administrator role for the directory. Only Global Administrators and Privileged Role Administrators can delegate administrator roles. To reduce risk for your business we recommend that you assign this role to only a few people in your company. Refer to Elevate access to manage all Azure subscriptions and management groups?

For more information, refer to the following links for group management:

- Add/Remove/Update groups (Assigned)
    - How to Create a basic group and add members using Azure Active Directory?
    - How do you Edit your group information using Azure Active Directory
    - How to Add or remove a group from another group using Azure Active Directory?
    - How to Add or remove group members using Azure Active Directory?
    - How to Add or remove group owners in Azure Active Directory?
- Dynamic groups
    - How to Create a dynamic group and check status?
    - Dynamic membership rules for groups in Azure Active Directory
    - Change static group membership to dynamic in Azure Active Directory
    - Follow Tutorial: Add or remove group members automatically
- Group-based licensing
    - What is group-based licensing in Azure Active Directory?
- Conditional access
    - What are conditions in Azure Active Directory conditional access?
    - How To: Set up SharePoint Online and Exchange Online for Azure Active Directory conditional access
- PowerShell
    - How do I manage az ad group using PowerShell?
    - PowerShell examples: Azure Active Directory version 2 cmdlets for group management
    - What are the Azure Active Directory cmdlets for configuring group settings?
- Self-Service
    - Set up self-service group management in Azure Active Directory
- Access Reviews
    - How do you Manage app and resource access using Azure Active Directory groups?

Help Desk Staff

- Search the Microsoft Support Knowledge Base for solutions to common technical issues.

- Search for and browse technical questions and answers from the community, or ask your own question in the Azure Active Directory Forum.

Training

Videos

- Azure videos: Azure AD: Introduction to Dynamic Memberships for Groups
- YouTube: Azure Management Group in Enterprise Mobility Suite
- Channel 9: How to configure and assign groups in Windows Azure AD?
- Channel 9: Azure Active Directory Core Skills: Azure AD Users, Groups, and Authentication
- LinkedIn Learning: Office 365: Manage Identities using Azure AD Connect

Online Courses

- PluralSight.com: Managing Identities in Microsoft Azure Active Directory
  "In this course, you will learn the basics of managing an Azure Active Directory environment, including users, groups, devices, and applications." Azure AD groups are covered in the "Managing Azure Active Directory Users and Groups" module.

- PluralSight.com: Managing Microsoft Azure Active Directory
  "This course explores the key management activities and actions related to Azure Active Directory." Azure AD groups are covered in the "User and Group Management Using the Azure Portal" module.

- PluralSight.com: Getting Started with the Microsoft Enterprise Mobility Suite
  "This course will provide best practices that you need to know for extending on-premises assets to the cloud in a manner that allows for authentication, authorization, encryption, and a secured mobile experience." Learn how to configure dynamic groups in the "Configuring Advanced Features of Microsoft Azure Active Directory Premium" module.

Books

O'Reilly - Mastering Identity and Access Management with Microsoft Azure by Jochen Nickel

"Beginning with the basics of features and licenses, this book quickly moves on to the user and group lifecycle required to design roles and administrative units for role-based access control (RBAC). Get to grips with how to configure and manage users, groups, roles, and administrative units to provide a user- and group-based application and self-service access including the audit functionality." Group management is covered in the "Planning and Designing Cloud Identities" chapter.

Tutorials

- Quickstart: View your organization's groups and members in Azure Active Directory
  In this QuickStart, you view all your organization's existing groups and view the assigned members.

- Quickstart: Set Office 365 groups to expire in Azure Active Directory
  In this QuickStart, you set the expiration policy for your Office 365 groups. When users can set up their own groups, unused groups can multiply.

- Quickstart: Naming policy for groups in Azure Active Directory
  In this QuickStart, you set up a naming policy in your Azure Active Directory (Azure AD) tenant for user-created Office 365 groups, to help you sort and search your tenant's groups.

- Tutorial: Add or remove group members automatically
  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

End-user readiness and communication

Not required

Planning and Change Management

This section provides the deployment plan, prerequisites and high-level design to plan the Azure AD Group Management deployment.

Deployment Plan

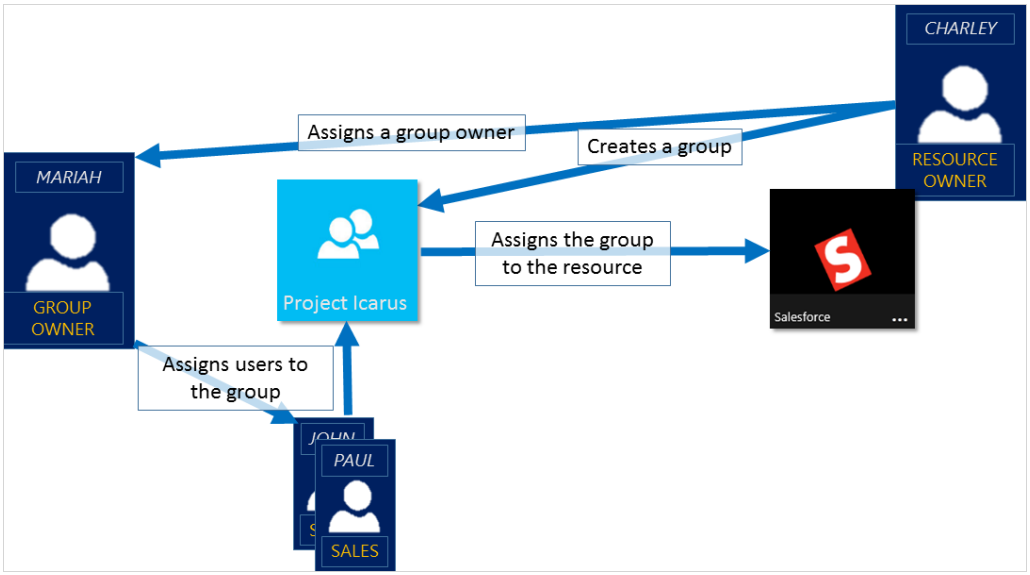
<Not available>

Architecture Plan/Topology

Azure AD helps you to manage cloud-based apps, on-premises apps, and your resources using your organization's groups. Your resources can be part of the directory, such as permissions to manage objects through roles in the directory, or external to the directory, such as for Software as a Service (SaaS) apps, Azure services, SharePoint sites, and on-premises resources.

How does group management in Azure AD work?

Azure AD helps you give access to your organization's resources by providing access rights to a single user or to an entire Azure AD group. 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.



There are four ways to assign groups. Refer to [Ways to assign access rights](#).

The group owner can let users find their own groups to join, instead of assigning them. The owner can also set up the group to automatically accept all users that join or to require approval. For more information and instructions about how to let your users request to join groups. Refer to [Set up self-service group management in Azure Active Directory.](#)

Testing

This section provides the plan to test the functionality of Azure AD Group Management in a sandbox or test lab environment before the customer rolls it into production.

<Not available>

Deployment

How can I get Azure AD Group Management deployed in my environment? This section provides resource links to help with implementation of your solution.

Refer to the following links:

- Add/Remove/Update groups (Assigned)
  - How to [Create a basic group and add members using Azure Active Directory](#)
  - How To [Edit your group information using Azure Active Directory](#)
  - How to [Add or remove a group from another group using Azure Active Directory](#)
  - How to [Add or remove group members using Azure Active Directory](#)
  - How to [Add or remove group owners in Azure Active Directory](#)
- Dynamic groups
  - How to [Create a dynamic group and check status](#)?
  - [Dynamic membership rules for groups in Azure Active Directory](#)
  - [Change static group membership to dynamic in Azure Active Directory](#)

You can delegate the group management to employees using self-service. To enable self-service group management, see Set up self-service group management in Azure Active Directory

Operations

How do I manage and maintain Azure AD Group Management? This section provides troubleshooting info, Azure AD Connect Health operation and management details, and other important references.

Once the groups are defined, you can use them for one or more of the following:

- Conditional access
  - What are conditions in Azure Active Directory conditional access?
- Group-based licenses
  - What is group-based licensing in Azure Active Directory?
  - QuickStart: Assign or remove licenses using the Azure Active Directory portal
  - How to add migrate users with individual licenses to groups for licensing
  - Assign licenses to users by group membership in Azure Active Directory
  - Change the license for a single user in a licensed group in Azure Active Directory
  - Azure Active Directory group-based licensing additional scenarios
  - PowerShell examples for group-based licensing in Azure Active Directory
- SharePoint and Exchange online
  - How To: Set up SharePoint Online and Exchange Online for Azure Active Directory conditional access
- SaaS App access
  - Using a group to manage access to SaaS applications

Monitoring and Support

You can manage your groups in Azure AD using the following methods:

- Admin-managed
  - Elevate access to manage all Azure subscriptions and management groups
- Self-Service
  - Set up self-service group management in Azure Active Directory.
- Access reviews
  - Manage user access with Azure AD access reviews so that the right users have the right access.
- PowerShell cmdlets and API
  - What are the Azure Active Directory cmdlets for configuring group settings?
  - Download the Azure AD PowerShell module.
  - PowerShell examples : Azure Active Directory version 2 cmdlets for group management

Troubleshooting

Refer to the following links:

- Troubleshoot and resolve groups issues
- Identify and resolve license assignment problems for a group in Azure Active Directory

References

Additionally, you can refer to:

- Azure AD Connect sync: Understanding Users, Groups, and Contacts
- Authorization in a web app using Azure AD groups & group claims
- Working with Azure Active Directory resources in Microsoft Graph

Support and Feedback

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

The product documentation for Azure AD Group Management is available online. There you can use the built-in search or your favorite search engine to find information on Azure AD Connect Health.

If you have a general question about Azure AD and Azure AD Group Management, you can ask the community for assistance on the Azure AD forums.

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 suggestions, please submit an idea or vote up an idea at our User Voice Channel - feedback.azure.com.