User Management in Microsoft Azure

Virtualization and Cloud Computing

APRIL 27, 2020

SUBMITTED BY: M. IFTIKHAR UDDIN KHAN SAMI
022-16-113275

Submitted by: M. Iftikhar Uddin Khan Sami (022-16-113275)

Contents

Submitted by: M. Iftikhar Uddin Khan Sami (022-16-113275)

Assignment- Briefly discuss how Microsoft Azure manages Users ?

Users, groups, licensing, and roles for large organizations

- Assign users to groups
- Assign licenses to groups
- Delegate administrator roles

Assign users to groups

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

For additional flexibility and to reduce the work of managing group membership, you can use dynamic groups in Azure AD to expand and contract group membership automatically. You'll need an Azure AD Premium P1 license for each unique user that is a member of one or more dynamic groups.

Assign licenses to groups

Assigning or removing licenses from users individually can demand time and attention. If you assign licenses to groups instead, you can make your large-scale license management easier.

In Azure AD, when users join a licensed group, they're automatically assigned the appropriate licenses. When users leave the group, Azure AD removes their license assignments. Without Azure AD 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.

If there are not enough available licenses, or an issue occurs like service plans that can't be assigned at the same time, you can see 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 Azure AD administrator roles to help you distribute the work of application management with more granularity:

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.

User Management in Azure

Add or delete users using Azure Active Directory

Add a new user

You can create a new user using the Azure Active Directory portal.

To add a new user, follow these steps:

1. Sign in to the Azure portal as a User administrator for the organization.
2. Search for and select *Azure Active Directory* from any page.
3. Select Users, and then select New user.
4. On the User page, enter information for this user:
    - Name. Required. The first and last name of the new user. For example, *Mary Parker*.
    - User name. Required. The user name of the new user. For example, mary@contoso.com.
    - Groups. Optionally, you can add the user to one or more existing groups. You can also add the user to groups at a later time. For more information about adding users to groups, see Create a basic group and add members using Azure Active Directory.
    - Directory role: If you require Azure AD administrative permissions for the user, you can add them to an Azure AD role. You can assign the user to be a Global administrator or one or more of the limited administrator roles in Azure AD. For more information about assigning roles, see How to assign roles to users.
    - Job info: You can add more information about the user here, or do it later. For more information about adding user info, see How to add or change user profile information.
5. Copy the autogenerated password provided in the Password box. You'll need to give this password to the user to sign in for the first time.
6. Select Create.

The user is created and added to your Azure AD organization.

Add a new guest user

You can also invite new guest user to collaborate with your organization by selecting Invite user from the New user page. If your organization's external collaboration settings are configured such that you're allowed to invite guests, the user will be emailed an invitation they must accept in order to begin collaborating.

Add a consumer user

There might be scenarios in which you want to manually create consumer accounts in your Azure Active Directory B2C (Azure AD B2C) directory.

Add a new user within a hybrid environment

If you have an environment with both Azure Active Directory (cloud) and Windows Server Active Directory (on-premises), you can add new users by syncing the existing user account data.

Delete a user

You can delete an existing user using Azure Active Directory portal.

To delete a user, follow these steps:

1. Sign in to the Azure portal using a User administrator account for the organization.
2. Search for and select *Azure Active Directory* from any page.
3. Search for and select the user you want to delete from your Azure AD tenant. For example, *Mary Parker*.
4. Select **Delete user**.

The user is deleted and no longer appears on the **Users - All users** page. The user can be seen on the **Deleted users** page for the next 30 days and can be restored during that time.

Add or update a user's profile information using Azure Active Directory

Add or change profile information

As you'll see, there's more information available in a user's profile than what you're able to add during the user's creation. All this additional information is optional and can be added as needed by your organization.

To add or change profile information

1. Sign in to the Azure portal as a User administrator for the organization.
2. Select Azure Active Directory, select Users, and then select a user. For example, Alain Charon.
3. Select Edit to optionally add or update the information included in each of the available sections.

- **Profile picture.** Select a thumbnail image for the user's account. This picture appears in Azure Active Directory and on the user's personal pages, such as the myapps.microsoft.com page.
- **Identity.** Add or update an additional identity value for the user, such as a married last name. You can set this name independently from the values of First name and Last name. For example, you could use it to include initials, a company name, or to change the sequence of names shown. In another example, for two users whose names are 'Chris Green' you could use the Identity string to set their names to 'Chris B. Green' 'Chris R. Green (Contoso).'
- **Job info.** Add any job-related information, such as the user's job title, department, or manager.
- **Settings.** Decide whether the user can sign in to Azure Active Directory tenant. You can also specify the user's global location.
- **Contact info.** Add any relevant contact information for the user, except for some user's phone or mobile contact info (only a global administrator can update for users in administrator roles).
- **Authentication contact info.** Verify this information to make sure there's an active phone number and email address for the user. This information is used by Azure Active Directory to make sure the user is really the user during sign-in. Authentication contact info can be updated only by a global administrator.

4. Select Save.

All your changes are saved for the user.

Reset a user's password using Azure Active Directory

To reset a password

1. Sign in to the Azure portal as a user administrator, or password administrator. For more information about the available roles, see Assigning administrator roles in Azure Active Directory
2. Select Azure Active Directory, select Users, search for and select the user that needs the reset, and then select Reset Password.
3. In the Reset password page, select Reset password.
4. Copy the password and give it to the user. The user will be required to change the password during the next sign-in process.

Assign administrator and non-administrator roles to users with Azure Active Directory

Assign roles

A common way to assign Azure AD roles to a user is on the Directory role page for a user.

You can also assign roles using Privileged Identity Management (PIM).

Assign a role to a user

1. Go to the Azure portal and log in using a Global administrator account for the directory.
2. Search for and select **Azure Active Directory**.
3. Select Users.
4. Search for and select the user getting the role assignment. For example, Alain Charon.
5. On the Alain Charon - Profile page, select Assigned roles.

   The Alain Charon - Directory role page appears.
6. Select Add assignment, select the role to assign to Alain (for example, Application administrator), and then choose Select.

Remove a role assignment

If you need to remove the role assignment from a user, you can also do that from the **Alain Charon - Directory role** page.

- **To remove a role assignment from a user**

1. Select **Azure Active Directory**, select **Users**, and then search for and select the user getting the role assignment removed. For example, *Alain Charon*.
2. Select **Assigned roles**, select **Application administrator**, and then select **Remove assignment**.

Restore or remove a recently deleted user using Azure Active Directory

After you delete a user, the account remains in a suspended state for 30 days. During that 30-day window, the user account can be restored, along with all its properties. After that 30-day window passes, the user is automatically, and permanently, deleted.

You can view your restorable users, restore a deleted user, or permanently delete a user using Azure Active Directory (Azure AD) in the Azure portal.

Required permissions

You must have one of the following roles to restore and permanently delete users.

- Global administrator
- Partner Tier1 Support
- Partner Tier2 Support
- User administrator

View your restorable users

You can see all the users that were deleted less than 30 days ago. These users can be restored.

To view your restorable users

1. Sign in to the Azure portal using a Global administrator account for the organization.
2. Select Azure Active Directory, select Users, and then select Deleted users.
3. Review the list of users that are available to restore.

Restore a recently deleted user

When a user account is deleted from the organization, the account is in a suspended state and all the related organization information is preserved. When you restore a user, this organization information is also restored.

To restore a user

1. On the **Users - Deleted users** page, search for and select one of the available users. For example, *Mary Parker*.
2. Select **Restore user**.

Permanently delete a user

You can permanently delete a user from your organization without waiting the 30 days for automatic deletion. A permanently deleted user can't be restored by you, another administrator, nor by Microsoft customer support.

To permanently delete a user

1. On the **Users - Deleted users** page, search for and select one of the available users. For example, *Rae Huff*.
2. Select **Delete permanently**.

References:

- ✓ https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-users-azure-active-directory
- ✓ https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-overview-user-model