200 XP

What are user accounts in Azure Active Directory?

7 minutes

In Azure Active Directory (Azure AD), all user accounts are granted a set of default permissions. A user's account access consists of the type of user, their role assignments, and their ownership of individual objects.

There are different types of user accounts in Azure AD. Each type has a level of access specific to the scope of work expected to be done under each type of user account. Administrators have the highest level of access, followed by the member user accounts in the Azure AD organization. Guest users have the most restricted level of access.

Permissions and roles

Azure AD uses permissions to help you control the access rights a user or group is granted. This is done through roles. Azure AD has many roles with different permissions attached to them. When a user is assigned a specific role, they inherit permissions from that role. For example, a user assigned to the User Administrator role can create and delete user accounts.

Understanding when to assign the correct type of role to the right user is a fundamental and crucial step in maintaining privacy and security compliance. If the wrong role is assigned to the wrong user, the permissions that come with that role can allow the user to cause serious damage to an organization.

Administrator roles

Administrator roles in Azure AD allow users elevated access to control who is allowed to do what. You assign these roles to a limited group of users to manage identity tasks in an Azure AD organization. You can assign administrator roles that allow a user to create or edit users, assign administrative roles to others, reset user passwords, manage user licenses, and more.

If your user account has the User Administrator or Global Administrator role, you can create a new user in Azure AD by using the Azure portal, the Azure CLI, or PowerShell. In PowerShell, run

the cmdlet `New-AzureADUser`. In the Azure CLI, use `az ad user create`.

Member users

A member user account is a native member of the Azure AD organization that has a set of default permissions like being able to manage their profile information. When someone new joins your organization, they typically have this type of account created for them.

Anyone who isn't a guest user or isn't assigned an administrator role falls into this type. A member user role is meant for users who are considered internal to an organization and are members of the Azure AD organization. However, these users shouldn't be able to manage other users by, for example, creating and deleting users. Member users don't have the same restrictions that are typically placed on guest users.

Guest users

Guest users have restricted Azure AD organization permissions. When you invite someone to collaborate with your organization, you add them to your Azure AD organization as a guest user. Then, you can either send an invitation email that contains a redemption link or send a direct link to an app you want to share. Guest users sign in with their own work, school, or social identities. By default, Azure AD member users can invite guest users. Someone with the User Administrator role can disable this default.

Your organization might need to work with external partners. To collaborate with your organization, these partners often need to have a certain level of access to specific resources. For this sort of situation, it's a good idea to use guest user accounts. You'll then make sure partners have the right level of access to do their work, without having a higher level of access than they need.

Add user accounts

You can add individual user accounts through the Azure portal, Azure PowerShell, or the Azure CLI.

If you want to use the Azure CLI, run the following cmdlet:

Azure CLI

```
# create a new user
az ad user create
```

This command creates a new user by using the Azure CLI.

For Azure PowerShell, run the following cmdlet:

PowerShell

```
# create a new user
New-AzureADUser
```

You can bulk create member users and guests accounts. The following example shows how to bulk invite guest users.

PowerShell

```
$invitations = import-csv c:\bulkinvite\invitations.csv

$messageInfo = New-Object Microsoft.Open.MSGraph.Model.InvitedUserMessageInfo

$messageInfo.customizedMessageBody = "Hello. You are invited to the Contoso
organization."

foreach ($email in $invitations)
   {New-AzureADMSInvitation `
      -InvitedUserEmailAddress $email.InvitedUserEmailAddress `
      -InvitedUserDisplayName $email.Name `
      -InviteRedirectUrl https://myapps.microsoft.com `
      -InvitedUserMessageInfo $messageInfo `
      -SendInvitationMessage $true
   }
```

You create the comma-separated values (CSV) file with the list of all the users you want to add. An invitation is sent to each user in that CSV file.

Delete user accounts

You can also delete user accounts through the Azure portal, Azure PowerShell, or the Azure CLI. In PowerShell, run the cmdlet `Remove-AzADUser`. In the Azure CLI, run the cmdlet `az ad user delete`.

When 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.

Check your knowledge

1. If you delete a user account by mistake, can it be restored? *

- ◯ When a user account is deleted, it's gone forever and can't be restored.
- ◯ The user account can be restored, but only if it was created within the last 30 days.
- ◯ The user account can be restored, but only if it was deleted within the last 30 days.

2. What kind of account would you create to allow an external organization easy access? *

- ◯ A guest user account for each member of the external team.
- ◯ An external account for each member of the external team.
- ◯ An administrator account for each member of the external team.

Check your answers

How are we doing? ☆ ☆ ☆ ☆ ☆