100 XP

Create user accounts

3 minutes

Every user who wants access to Azure resources needs an Azure user account. A user account has all the information required to authenticate the user during the sign-in process. Azure Active Directory (Azure AD) supports three types of user accounts. The types indicate where the user is defined (in the cloud or on-premises), and whether the user is internal or external to your Azure AD organization.

Things to know about user accounts

The following table describes the user accounts supported in Azure AD. As you review these options, consider what types of user accounts suit your organization.

User account	Description
Cloud identity	A user account with a *cloud identity* is defined only in Azure AD. This type of user account includes administrator accounts and users who are managed as part of your organization. A cloud identity can be for user accounts defined in your Azure AD organization, and also for user accounts defined in an external Azure AD instance. When a cloud identity is removed from the primary directory, the user account is deleted.
Directory-synchronized identity	User accounts that have a *directory-synchronized identity* are defined in an on-premises Active Directory. A synchronization activity occurs via Azure AD Connect to bring these user accounts in to Azure. The source for these accounts is Windows Server Active Directory.
Guest user	*Guest user* accounts are defined outside Azure. Examples include user accounts from other cloud providers, and Microsoft accounts like an Xbox LIVE account. The source for guest user accounts is Invited user. Guest user accounts are useful when external vendors or contractors need access to your Azure resources.

Things to consider when choosing user accounts

- **Consider where users are defined**. Determine where your users are defined. Are all your users defined within your Azure AD organization, or are some users defined in external Azure AD instances? Do you have users who are external to your organization? It's common for businesses to support two or more account types in their infrastructure.
- **Consider support for external contributors**. Allow external contributors to access Azure resources in your organization by supporting the **Guest user** account type. When the external contributor no longer requires access, you can remove the user account and their access privileges.
- **Consider a combination of user accounts**. Implement the user account types that enable your organization to satisfy their business requirements. Support directory-synchronized identity user accounts for users defined in Windows Server Active Directory. Support cloud identities for users defined in your internal Azure AD structure or for user defined in an external Azure AD instance.

Next unit: Manage user accounts

Continue