* 10 minutes

While they share a similar name, Azure AD is *not* a cloud version of Windows Server Active Directory. It’s also not intended as a complete replacement for an on-premises Active Directory. Instead, if you’re already using a Windows AD server, you can connect it to Azure AD to extend your directory into Azure. This approach allows users to use the same credentials to access local and cloud-based resources.

![Conceptual art showing Windows AD and Azure AD controlling resources.](data:image/png;base64;base64,)

Conceptual art showing Windows AD and Azure AD controlling resources.

A user can also use Azure AD independently of Windows AD. Smaller companies can use Azure AD as their only directory service to control access to their applications and SaaS products, such as Microsoft 365, Salesforce, and Dropbox.

Note

Keep in mind that this approach doesn’t provide a completely centralized administrative model - for example, local Windows machines would authenticate using local credentials. Users can write applications to use Azure AD and provide authentication and authorization to be administered by a user in a single place.

## Directories, subscriptions, and users

Microsoft offers several cloud-based offerings today - all of which can use Azure AD to identify users and control access.

* Microsoft Azure
* Microsoft 365
* Microsoft Intune
* Microsoft Dynamics 365

When a company or organization signs up to use one of these offerings, they are assigned a default *directory*, an instance of Azure AD. This directory holds the users and groups that will have access to each of the services the company has purchased. This default directory can be referred to as a *tenant*. A tenant represents the organization and the default directory assigned to it.

*Subscriptions* in Azure are both a billing entity and a security boundary. Resources such as virtual machines, websites, and databases are associated with a single subscription. Each subscription also has a single account *owner* responsible for any charges incurred by resources in that subscription. If your organization wants a subscription billed to another account, you can transfer the subscription. A subscription is associated with a **single Azure AD directory**. Multiple subscriptions can trust the same directory, but a subscription can only trust one directory.

Users and groups can be added to multiple subscriptions - this allows the user to create, control, and access resources in the subscription. When you add a user to a subscription, the user must be known to the associated directory as shown in the following image.

![Conceptual art showing users, directories, and subscriptions in Azure.](data:image/png;base64;base64,)

Conceptual art showing users, directories, and subscriptions in Azure.

If you belong to multiple directories, you can switch the current directory you are working in through the **Directory + subscription** button in the Azure portal header.

![Screenshot showing the Directory selection dialog in Azure portal.](data:image/png;base64;base64,)

Screenshot showing the Directory selection dialog in Azure portal.

You can also decide how the default directory is selected: last visited or a specific directory. You can also set the default filter for displayed subscriptions. Default filters are useful if you have access to several subscriptions but typically only work in a few of them.

## Create a new directory

An organization (tenant) has one associated default Azure AD directory. However, owners can create additional directories to support the development or testing purposes or because they want to have separate directories to synchronize with their local Windows Server AD forests.

Important

The steps to create a new directory follow; however, unless you are an owner of your Azure account, this option won’t be available to you. The Azure Sandbox doesn’t allow you to create new Azure AD directories.

1. Sign in to the [Azure portal](https://portal.azure.com/).
2. On the Azure home page, under **Azure services**, select **Create a resource**. The **Create a resource** pane appears.
3. In the left menu pane, select **Identity**, and then search for an select **Azure Active Directory**. The **Azure Active Directory** pane appears.
4. Select **Create**. The **Create tenant** pane appears.
5. Enter the following values for each setting.
   * **Organization name**: Enter a name for the directory to help distinguish it from your other directories. The directory to be created will be used in production; provide a name that your users will recognize as your organization’s name. You can change the name later if you want.
   * **Initial domain name**: Enter a domain name associated with your organization. Azure will give a validation error unless the domain is not known. The default domain name will always have the suffix .onmicrosoft.com. You can not change the default domain. If you choose to, you can add a custom domain owned by your organization so defined users can use a traditional company email such as john@contoso.com.
   * **Country or region**: Select the country the directory should reside. The country will identify the region and data center where the Azure AD instance will live; you can not change it later.

* ![Screenshot showing the AD creation process.](data:image/png;base64;base64,)
* Screenshot showing the AD creation process.

1. Select **Create** to create the new directory. A free tier directory will be created where you can add users, create roles, register apps and devices, and control licenses.

After you have created the directory, select **Click here to manage your new tenant** to go to the Overview dashboard that lets you control all directory aspects.

![Screenshot of the Azure AD dashboard.](data:image/png;base64;base64,)

Screenshot of the Azure AD dashboard.

Let’s explore one of the primary elements you’ll work with in Azure AD: **users**.

## Check your knowledge

Need help? See our [troubleshooting guide](https://docs.microsoft.com/en-us/learn/support/troubleshooting?uid=learn.azure-security.manage-users-and-groups-in-aad.create-aad&documentId=0a9037f9-8f8a-222a-d301-4da76253ff15&versionIndependentDocumentId=0c984bc8-6a7f-277c-1eda-e2f6963a8449&contentPath=%2FMicrosoftDocs%2Flearn-pr%2Fblob%2Flive%2Flearn-pr%2Fazure%2Fmanage-users-and-groups-in-aad%2F2-create-aad.yml&url=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Flearn%2Fmodules%2Fmanage-users-and-groups-in-aad%2F2-create-aad&author=curtand) or provide specific feedback by [reporting an issue](https://docs.microsoft.com/en-us/learn/support/troubleshooting?uid=learn.azure-security.manage-users-and-groups-in-aad.create-aad&documentId=0a9037f9-8f8a-222a-d301-4da76253ff15&versionIndependentDocumentId=0c984bc8-6a7f-277c-1eda-e2f6963a8449&contentPath=%2FMicrosoftDocs%2Flearn-pr%2Fblob%2Flive%2Flearn-pr%2Fazure%2Fmanage-users-and-groups-in-aad%2F2-create-aad.yml&url=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Flearn%2Fmodules%2Fmanage-users-and-groups-in-aad%2F2-create-aad&author=curtand#report-feedback).