

Create, configure, and manage identities

1. Introduction

<https://learn.microsoft.com/en-us/training/modules/create-configure-manage-identities/1-introduction>

Introduction

Completed

Transitioning workloads to the cloud involves more than just moving servers, websites, and data. Companies need to think about how to secure those resources, by defining authorized users. Next, companies need to ensure that users only have access to data that they need, that user authorization is limited only create services available to them, and that users only perform operations authorized for them to perform. Access to cloud-based workloads is controlled centrally in two ways. First by providing a definitive identity for each user that they use for every service. Then second by ensuring employees and vendors have enough access to do their jobs.

Microsoft Entra ID, the Microsoft cloud-based identity, and access management service, helps make these challenges easier to solve. Microsoft Entra ID provides end-to-end identity management; including single sign-on and multifactor authentication to help protect your users and your data. In this module, you learn the basics of creating, configuring, and managing users and groups of users. You also learn to manage licenses and device registration.

Learning objectives

In this module, you'll:

- Create, configure, and manage users
- Create, configure, and manage groups
- Manage licenses
- Configure and manage device registration
- Explore custom security attributes and automatic provisioning

Prerequisites

- Basic understanding of identity management

- Some experience with Active Directory a plus
- Experience with Zero Trust helpful

2. Create, configure, and manage users

<https://learn.microsoft.com/en-us/training/modules/create-configure-manage-identities/2-users>

Create, configure, and manage users

Completed

Every user who needs access to resources needs a user account in Microsoft Entra ID. A user account contains all the information needed to authenticate the user during the sign-on process. Once authenticated, Microsoft Entra ID builds an access token to authorize the user and determine what resources they can access and what they can do with those resources.

You use the **Microsoft Entra admin center** to work with user objects. Keep in mind that you can only work with a single directory at a time. You can use the **Directory + Subscription** panel to switch directories. The admin center also has a **Switch directory** button in the toolbar, which makes it easy to switch to another available directory.

View users

To view the Microsoft Entra users, select the **Users** entry under **Identity**, then open the **All Users** view. Take a minute to access the admin center and view your users. Notice the **User Type** column to see members and guests, as the following figure depicts.

Display name	User principal name	User type	Country or region	Job title
RN Robina Nauman	RobiNa	Member	United States	Retail Manager
MA Marcos Amboade	MarcAm	Member	United States	Marketing Assistant
CG Chris Green	ChrisG	Member		
CB Carmelo Barese	CarmeB	Member	United States	HR Manager
UJ Umar Javaid	UmaJav	Member	United States	Designer
UF Uxía Feal	UxiaFe	Member	United States	Developer
VS Vishnu Surendran	VishnS	Member	United States	Sales Rep

Typically, Microsoft Entra ID defines users in three ways:

- **Cloud identities** - These users exist only in Microsoft Entra ID. Examples are administrator accounts and users that you manage yourself. Their source is **Microsoft Entra ID** or **External Microsoft Entra directory** if the user is defined in another Microsoft Entra instance but needs access to subscription resources controlled by this directory. When these accounts are removed from the primary directory, they're deleted.
- **Directory-synchronized identities** - These users exist in an on-premises Active Directory. A synchronization activity brings these users into Microsoft Entra ID. **Microsoft Entra Cloud Sync** is the recommended synchronization tool for most organizations—it uses a lightweight cloud-managed agent and supports multiple disconnected forests. **Microsoft Entra Connect Sync** remains available for complex scenarios such as device synchronization or groups with more than 50,000 members. Their source is **Windows Server AD**.
- **Guest users** - These users exist outside your organization. Examples are accounts from other cloud providers and Microsoft accounts. Their source is **Invited user**. This type of account is useful when external vendors or contractors need access to your organization's resources. Once their help is no longer necessary, you can remove the account and all of their access.

3. Exercise - assign licenses to users

<https://learn.microsoft.com/en-us/training/modules/create-configure-manage-identities/3-exercise-assign-licenses-users>

Exercise - assign licenses to users

Completed

Exercise environment needs - this lab assumes you have a basic Microsoft Entra tenant with at least User Administrator rights to complete it. You can get a free trial subscription for at [Try Azure for Free](#).

Create a new user in Microsoft Entra ID

You can skip creating this user if you created the same user in the earlier module.

1. Browse to the Identity menu in the [Microsoft Entra admin center](#).
2. In the left navigation, under select **Users**, then **All Users**.
3. Within the Users page, on the menu, select + **New user** and **Create new user**.
4. Create a user using the following information:

Setting	Value
User principal name	ChrisG
Name	Chris Green
First name	Chris
Last name	Green
Password	make up a unique password

5. When complete, verify the account for Chris Green is shown in the **All users** list.

Create a security group in Microsoft Entra ID

1. Browse to the Microsoft Entra admin center screen.
2. In the left navigation, under **Identity**, select **Groups** and then **All groups**.
3. In the Groups screen, on the menu, select **New group**.
4. Create a group using the following information:

Setting	Value
Group type	Security
Group name	Marketing
Membership type	Assigned
Owners	Assign your own administrator account as the group owner
Members	Chris Green

Home > Licenses | Overview > Groups | All groups >

New Group

Got feedback?

Group type * ⓘ
Security

Group name * ⓘ
Marketing

Group description ⓘ
This is a new group created for the SC-300 training content.

Microsoft Entra roles can be assigned to the group ⓘ
Yes No

Membership type ⓘ
Assigned

Owners
No owners selected

Members
No members selected

Create

Add members

Try changing or adding filters if you don't see what you're looking for.

Search ⓘ
mar
2 results found

All Users Groups Devices Enterprise applications

	Name	Type	User principal name
☐	Marcos Amboade	User	MarcAm
☐	Marykutty Robin	User	MarykR

Selected (0)
Reset
No items selected

Select

5. When complete, verify the group named **Marketing** is shown in the **All groups** list.

Assign a license to a group

License assignment to groups is managed through the Microsoft 365 admin center.

1. Go to the Microsoft 365 admin center at <https://admin.microsoft.com>.
2. Select **Billing** from the menu on the left.
3. Select **Licenses**.
4. From the list of licenses you have available, select one.
5. Select **Groups** from the list near the top of the screen.
6. On the Groups page, select **+ Assign license**.
7. Search for and select the **Marketing** group you created earlier.
8. Select the **Assign** button at the bottom of the dialog.
9. You should get a message that licenses were successfully assigned.

Restore or remove a recently deleted user with Microsoft Entra ID

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 permanent deletion process is automatically started.

You can view your restorable users, restore a deleted user, or permanently delete a user using Microsoft Entra ID user interface.

Important

You can't restore a permanently deleted user.

Required permissions

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

- Global administrator
- Partner Tier-1 Support
- Partner Tier-2 Support
- User administrator

4. Exercise - restore or remove deleted users

Exercise - restore or remove deleted users

Completed

Exercise environment needs - this lab assumes you have a basic Microsoft Entra tenant with at least User Administrator rights to complete it. You can get a free trial subscription at [Try Microsoft Azure for free](#).

Remove a user from Microsoft Entra ID

1. Browse to the [Microsoft Entra admin center](#).
2. In the left navigation, under **Identity**, select **Users**.
3. In the **Users** list, select the check box for a user to delete. For example, select **Chris Green**.

Tip

Selecting users from the list allows you to manage multiple users at the same time. If you select the user, to open that user's page, you'll only be managing that individual user.

The screenshot shows the Microsoft Entra admin center interface. On the left is a navigation pane with 'Users' selected. The main area displays a list of 20 users, with 'Chris Green' selected. The 'Delete' button in the top right corner is highlighted with a red box.

	Display name ↑	User type	On-premises sy...
☐	Adele Vance	Member	No
☐	Alex Wilber	Member	No
☒	CG Chris Green	Member	No
☐	Diego Siciliani	Member	No
☐	Grady Archie	Member	No
☐	Henrietta Mueller	Member	No
☐	Isaiah Langer	Member	No
☐	Johanna Lorenz	Member	No

4. With the user account selected, on the menu, select **Delete user**.

5. Review the dialog box and then select **OK**.

Restore a deleted user

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

1. In the Users page, in the left navigation, select **Deleted users**.
2. Review the list of deleted users and select the user you deleted.

Important

By default, deleted user accounts are permanently removed from Microsoft Entra ID automatically after 30 days.

3. On the menu, select **Restore user**.
4. Review the dialog box and then select **OK**.
5. In the left navigation, select **All users**.
6. Verify the user was restored.

5. Create, configure, and manage groups

<https://learn.microsoft.com/en-us/training/modules/create-configure-manage-identities/5-groups>

Create, configure, and manage groups

Completed

A Microsoft Entra group helps organize users, which makes it easier to manage permissions. Using groups lets the resource owner (or Microsoft Entra 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. Groups let you define a security boundary and then add and remove specific users to grant or deny access with a minimum amount of effort. Even better, Microsoft Entra ID supports the ability to define membership based on rules - such as what department a user works in, or the job title they have.

Microsoft Entra ID allows you to define two different types of groups.

- **Security groups** - the most common type of groups and are used to manage access to shared resources. Members of a security group can include users, devices, and service principals. For example, you can create a security group for a specific security policy. By doing it this way, you can give a set of permissions to all the members at once, instead of having to add permissions to each member individually. This option requires a Microsoft Entra administrator.
- **Microsoft 365 groups** - provide collaboration opportunities by giving members access to a shared mailbox, calendar, files, SharePoint site, and more. This option also lets you give people outside of your organization access to the group. This option is available to users and admins.

View available groups

You can view all groups through the **Groups** item under **Identity** in the Microsoft Entra admin center. A new Microsoft Entra ID deployment has no groups defined.

Groups | All groups ...
Microsoft Entra ID for workforce

<< New group Download groups Refresh Manage view ▾

Search

14 groups found

☐	Name ↑	Group type
☐	AD AAD DC Administrators	Security
☐	AC All Company	Microsoft 365

Settings

- General
- Expiration
- Naming policy

The second characteristic of a group that you need to be aware of is the **Membership Type**. This specifies how individual members are added to the group. The three types are:

- **Assigned** - members are added and maintained manually.
- **Dynamic User** - users are added and removed automatically based on rules that evaluate user attributes such as department, job title, or location.
- **Dynamic Device** - devices are added and removed automatically based on rules that evaluate device attributes. Applies to security groups only; Microsoft 365 groups support dynamic users but not dynamic devices.

Dynamic groups

With dynamic membership, Microsoft Entra ID automatically adds or removes users or devices from a group based on rules you define. When a member's attributes change—for example, a user moves to a different department—all dynamic membership rules in the tenant are reevaluated, and the user is added to or removed from groups accordingly.

Dynamic membership requires a **Microsoft Entra ID P1** license (or Intune for Education for device-based rules).

Dynamic membership rules

Save

Discard

Got feedback?

Configure Rules

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. [Learn more](#)

And/Or	Property	Operator	Value	
And	<Choose a Property>	<Choose an Operat...	Add a value	

+ Add expression

+ [Get custom extension properties](#)

Some items could not be displayed in the rule builder. [Learn more](#)

Rule syntax

user.objectId -ne null

Edit

For example, you can create a rule that automatically adds all users whose **Department** attribute equals "Marketing" to a Marketing security group, keeping membership current without manual updates.

6. Exercise - add groups in Microsoft Entra ID

<https://learn.microsoft.com/en-us/training/modules/create-configure-manage-identities/6-exercise-add-groups-azure-active-directory>

Exercise - add groups in Microsoft Entra ID

Completed

Exercise environment needs - this lab assumes you have a basic Microsoft Entra tenant with at least User Administrator rights to complete it. You can get a free trial subscription at [Try Microsoft Azure for free](#).

Create a Microsoft 365 group in Microsoft Entra ID

1. Browse to the [Microsoft Entra admin center](#).

2. In the left navigation, under **Identity**, select **Groups**.
3. In the Groups page, on the menu, select **New group**.
4. Create a group using the following information:

Setting	Value
Group type	Microsoft 365
Group name	Northwest Sales
Membership type	Assigned
Owners	Assign your own administrator account as the group owner
Members	Assign a member of this group

New Group ...

 Got feedback?

Group type * ⓘ

Microsoft 365

Group name * ⓘ

Northwese Sales

Group email address * ⓘ

NorthweseSales @<<domain/tenant>>.onmicrosoft.com

Group description ⓘ

Group containing members of the Sales team in Northwest region

Microsoft Entra roles can be assigned to the group ⓘ

Yes

No

Membership type * ⓘ

Assigned

Owners

1 owner selected

Members

1 member selected

5. When complete, verify the group named **Northwest sales** is shown in the **All groups** list.
6. You have to refresh the **All groups** a couple of times for the new group to show up.

7. Configure and manage device registration

Configure and manage device registration

Completed

With the proliferation of devices of all shapes and sizes and the proliferation of bring-your-own-device (BYOD), IT professionals are faced with two somewhat opposing goals:

- Allow end users to be productive wherever and whenever and on any device
- Protect the organization's assets

To protect these assets, IT-staff needs to first manage the device identities. IT-staff can build on the device identity with tools like Microsoft Intune to ensure standards for security and compliance are met. Microsoft Entra ID enables single sign-on to devices, apps, and services from anywhere through these devices.

- Your users get access to your organization's assets they need.
- Your IT-staff gets the controls they need to secure your organization.

Microsoft Entra registered devices

The goal of Microsoft Entra registered devices is to provide your users with support for the BYOD or mobile device scenarios. In these scenarios, a user can access your organization's Microsoft Entra ID controlled resources using a personal device.

Microsoft Entra registered	Description
Definition	Registered to Microsoft Entra ID without requiring organizational account to sign in to the device
Primary audience	Applicable to Bring your own device (BYOD), and Mobile devices
Device ownership	User or Organization
Operating systems	Windows 10 or newer, macOS 10.15 or newer, iOS 15 or newer, Android, Linux (Ubuntu 20.04/22.04/24.04 LTS, Red Hat Enterprise Linux 8/9 LTS)
Device sign in options	End-user local credentials, Password, Windows Hello, PIN, Biometrics
Device management	Mobile Device Management (example: Microsoft Intune), Mobile Application Management
Key capabilities	SSO to cloud resources, Conditional Access when enrolled in Intune, Conditional Access via App protection policy



Microsoft Entra registered devices are signed in to using a local account like a Microsoft account on a Windows 10 or newer device, but additionally have a Microsoft Entra account attached for access to organizational resources. Access to resources in the organization can be further limited based on that Microsoft Entra account and Conditional Access policies applied to the device identity.

Administrators can secure and further control these Microsoft Entra registered devices using Mobile Device Management (MDM) tools like Microsoft Intune. MDM provides a means to enforce organization-required configurations like requiring storage to be encrypted, password complexity, and security software kept updated.

Microsoft Entra ID registration can be accomplished when accessing a work application for the first time or manually using the Windows 10 or Windows 11 Settings menu.

Scenarios for registered devices

A user in your organization wants to access tools for email, reporting time-off, and benefits enrollment from their home PC. Your organization has these tools behind a Conditional Access policy that requires access from an Intune compliant device. The user adds their organization account and registers their home PC with Microsoft Entra ID and the required Intune policies are enforced giving the user access to their resources.

Another user wants to access their organizational email on their personal Android phone infected by a root-kit. Your company requires a compliant device and created an Intune compliance policy to block any rooted devices. The employee is stopped from accessing organizational resources on this device.

Microsoft Entra joined devices

Microsoft Entra joined is intended for organizations that want to be cloud-first or cloud-only. Any organization can deploy Microsoft Entra joined devices no matter the size or industry. Microsoft Entra joined enables access to both cloud and on-premises apps and resources.

Microsoft Entra joined	Description
Definition	Joined only to Microsoft Entra ID requiring organizational account to sign in to the device
Primary audience	Suitable for both cloud-only and hybrid organizations
Device ownership	Organization
Operating systems	All Windows 10 and Windows 11 devices (except Home editions); Windows Server 2019 and newer VMs in Azure (Server Core not supported); macOS 13 or newer (preview)
Device management	Mobile Device Management (example: Microsoft Intune)
Key capabilities	SSO to both cloud and on-premises resources, Conditional Access, Self-service Password Reset and Windows Hello PIN reset

Microsoft Entra joined devices are signed in to using an organizational Microsoft Entra account. Access to resources in the organization can be further limited based on that Microsoft Entra account

and Conditional Access policies applied to the device identity.

Administrators can secure and further control Microsoft Entra joined devices using Mobile Device Management (MDM) tools like Microsoft Intune or in co-management scenarios using Microsoft Endpoint Configuration Manager. These tools provide a means to enforce organization-required configurations like requiring storage to be encrypted, password complexity, software installations, and software updates. Administrators can make organization applications available to Microsoft Entra joined devices using Configuration Manager.

Microsoft Entra joined can be accomplished using self-service options like the Out of Box Experience (OOBE), bulk enrollment, or Windows Autopilot.

Microsoft Entra joined devices can still maintain single sign-on access to on-premises resources when they are on the organization's network. Microsoft Entra joined devices authenticate to on-premises servers like for file, print, and other applications.

Scenarios for joined devices

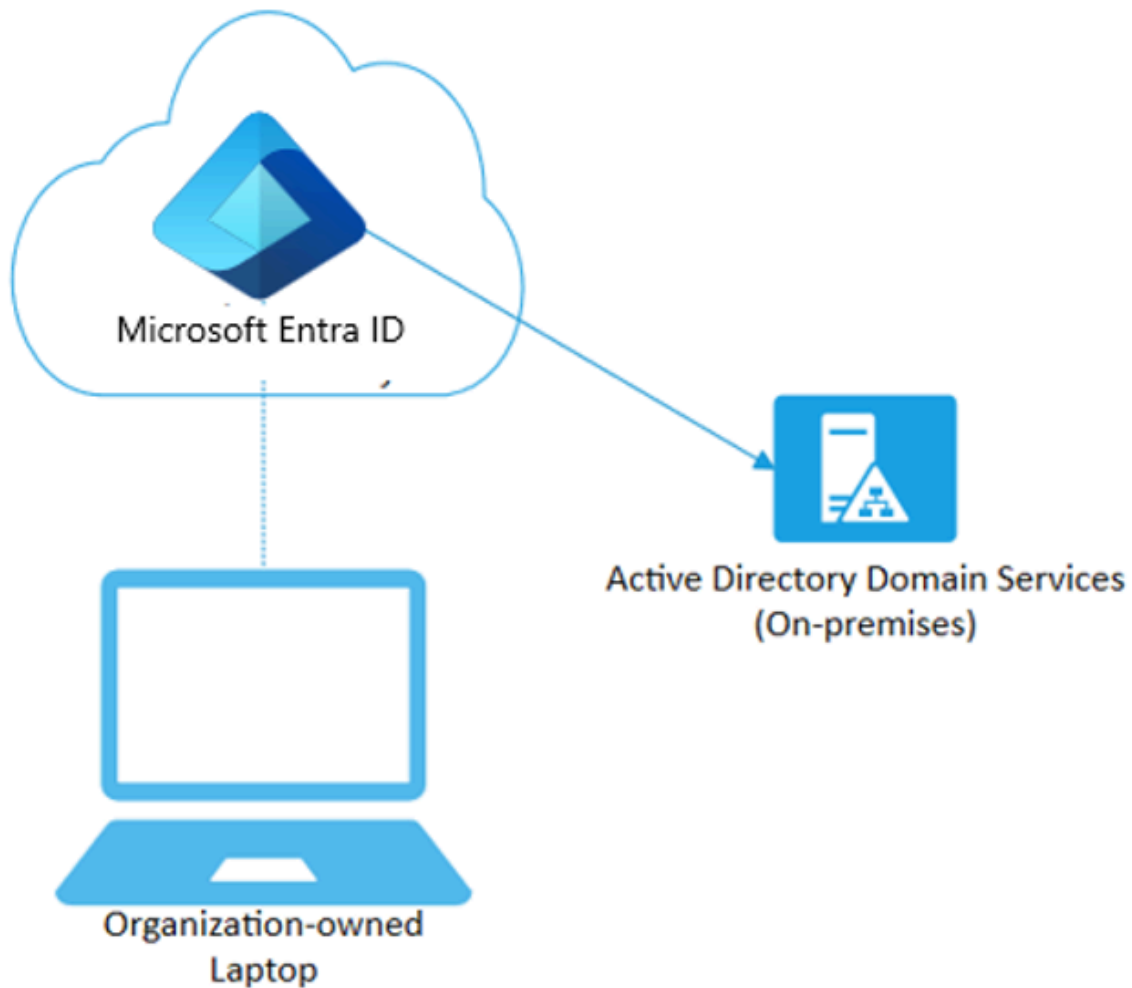
Although Microsoft Entra joined is primarily intended for organizations that don't have an on-premises Windows Server Active Directory infrastructure, you can certainly use it in scenarios where:

- You want to transition to cloud-based infrastructure using Microsoft Entra ID and MDM like Intune.
- You can't use an on-premises domain join, for example, if you need to get mobile devices such as tablets and phones under control.
- Your users primarily need to access Microsoft 365 or other SaaS apps integrated with Microsoft Entra ID.
- You want to manage a group of users in Microsoft Entra ID instead of in Active Directory. This scenario can apply, for example, to seasonal workers, contractors, or students.
- You want to provide joining capabilities to workers in remote branch offices with limited on-premises infrastructure.

You can configure Microsoft Entra joined devices for all Windows 10 and Windows 11 devices except for the Home editions.

The goal of Microsoft Entra joined devices is to simplify:

- Windows deployments of work-owned devices
- Access to organizational apps and resources from any Windows device
- Cloud-based management of work-owned devices
- Users to sign in to their devices with their Microsoft Entra ID or synced Active Directory work or school accounts.



Microsoft Entra Joined can be deployed by using many different methods.

Hybrid Microsoft Entra joined devices

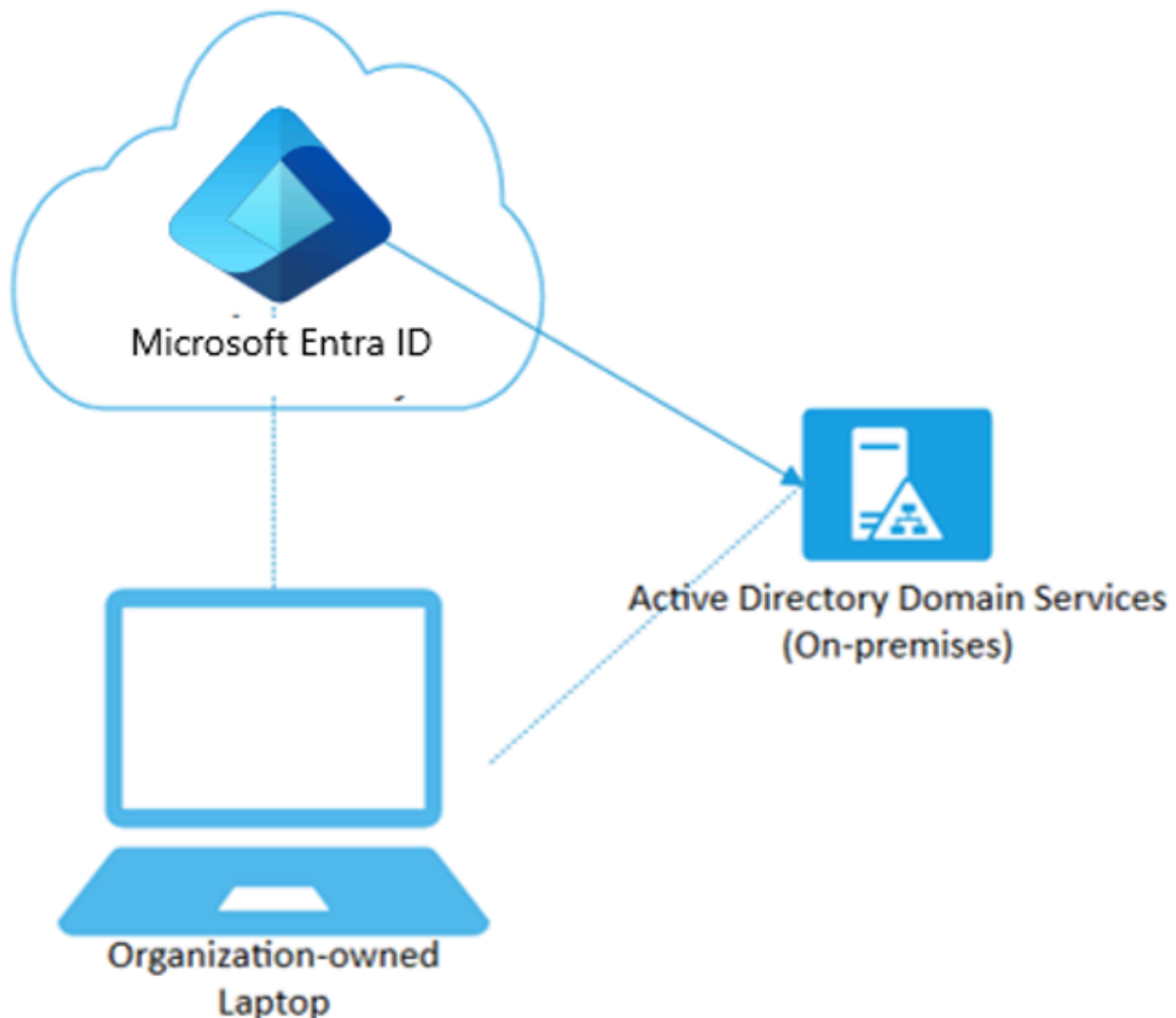
For more than a decade, many organizations have used the domain join to their on-premises Active Directory to enable:

- IT departments to manage work-owned devices from a central location.
- Users to sign in to their devices with their Active Directory work or school accounts.

Typically, organizations with an on-premises footprint rely on imaging methods to configure devices, and they often use **Configuration Manager** or **group policy (GP)** to manage them.

If your environment has an on-premises AD footprint and you also want benefit from the capabilities provided by Microsoft Entra ID, you can implement hybrid Microsoft Entra joined devices. These devices are devices that are joined to your on-premises Active Directory and registered with your Microsoft Entra directory.

Hybrid Microsoft Entra joined	Description
Definition	Joined to on-premises AD and Microsoft Entra ID requiring organizational account to sign in to the device
Primary audience	Suitable for hybrid organizations with existing on-premises AD infrastructure
Device ownership	Organization
Operating systems	Windows 10, Windows 11 (except Home editions), Windows Server 2016, 2019, and 2022
Device sign in options	Password or Windows Hello for Business
Device management	Group Policy, Configuration Manager standalone, or co-management with Microsoft Intune
Key capabilities	SSO to both cloud and on-premises resources, Conditional Access, Self-service Password Reset and Windows Hello PIN reset



Scenarios for hybrid joined

Use Microsoft Entra hybrid joined devices if:

- You have Win32 apps deployed to these devices that rely on Active Directory machine authentication.
- You want to continue to use Group Policy to manage device configuration.
- You want to continue to use existing imaging solutions to deploy and configure devices.

Device writeback (no longer supported)

Device writeback is no longer supported and is no longer a recommended approach for hybrid identity scenarios. It is replaced by **Cloud Kerberos Trust**, which allows Microsoft Entra joined and hybrid joined devices to authenticate to on-premises resources without requiring device objects to be written back to on-premises Active Directory.

For organizations planning new hybrid deployments, use Cloud Kerberos Trust to enable on-premises SSO and Windows Hello for Business in hybrid environments. See [Configure Microsoft Entra Kerberos for on-premises single sign-on](#) for guidance.

8. Manage licenses

<https://learn.microsoft.com/en-us/training/modules/create-configure-manage-identities/8-manage-licenses>

Manage licenses

Completed

Microsoft paid cloud services, such as Microsoft 365, Enterprise Mobility + Security, Dynamics 365, and other similar products, require licenses. These licenses are assigned to each user who needs access to these services. To manage licenses, administrators use the [Microsoft 365 admin center](#) or PowerShell and Microsoft Graph API. Microsoft Entra ID is the underlying infrastructure that supports identity management for all Microsoft cloud services. Microsoft Entra ID stores information about license assignment states for users.

Without group-based licensing, assigning licenses at the individual user level makes large-scale management difficult. For example, to add or remove user licenses based on organizational changes, such as users joining or leaving the organization or a department, an administrator often must write a complex PowerShell script. This script makes individual calls to the cloud service.

To address those challenges, Microsoft Entra ID now includes group-based licensing. You can assign one or more product licenses to a group. Microsoft Entra ID ensures that the licenses are assigned to all members of the group. Any new members who join the group are assigned the appropriate licenses. When they leave the group, those licenses are removed. This licensing management

eliminates the need for automating license management via PowerShell to reflect changes in the organization and departmental structure on a per-user basis.

License requirements

You must have one of the following licenses to use group-based licensing:

- Paid or trial subscription for Microsoft Entra ID Premium P1 and greater
- Paid or trial edition Office 365 Enterprise E3 or greater

Required number of licenses

For any groups assigned a license, you must also have a license for each unique member. While you don't have to assign each member of the group a license, you must have at least enough licenses to include all of the members. For example, if you have 1,000 unique members who are part of licensed groups in your tenant, you must have at least 1,000 licenses to meet the licensing agreement.

Features

Here are the main features of group-based licensing:

- Licenses can be assigned to any security group in Microsoft Entra ID. Security groups can be synced from on-premises by using Microsoft Entra Cloud Sync (recommended) or Microsoft Entra Connect Sync. You can also create security groups directly in Microsoft Entra ID (also called cloud-only groups), or automatically via the Microsoft Entra dynamic group feature.
- When a product license is assigned to a group, the administrator can disable one or more service plans in the product. Typically, this assignment is done when the organization isn't yet ready to start using a service included in a product. For example, the administrator might assign Microsoft 365 to a department, but temporarily disable the Viva Engage service.
- All Microsoft cloud services that require user-level licensing are supported. This support includes all Microsoft 365 products, Enterprise Mobility + Security, and Dynamics 365.
- Group-based licensing is currently available only through the [Microsoft 365 admin center](#).
- Microsoft Entra ID automatically manages license modifications that result from group membership changes. Typically, license modifications are effective within minutes of a membership change.
- A user can be a member of multiple groups with license policies specified. A user can also have some licenses that were directly assigned, outside of any groups. The resulting user state is a combination of all assigned product and service licenses. If a user is assigned same license from multiple sources, the license is consumed only once.
- In some cases, licenses can't be assigned to a user. For example, there might not be enough available licenses in the tenant, or conflicting services are assigned at the same time. Administrators have access to information about users for whom Microsoft Entra ID couldn't fully process group licenses. They can then take corrective action based on that information.

Some Microsoft services aren't available in all locations. The administrator, before assigning a license to a user, should specify usage location in the User Profile.

For group license assignment, any users without a usage location specified inherit the location of the directory. If you have users in multiple locations, we recommend that you always set usage location as part of your user creation. Usage location helps ensure the result of license assignment is always correct and users don't receive services in locations that aren't allowed.

9. Exercise - change group license assignments

<https://learn.microsoft.com/en-us/training/modules/create-configure-manage-identities/9-exercise-change-group-license-assignments>

Exercise - change group license assignments

Completed

Exercise environment needs - this lab assumes you have a basic Microsoft Entra tenant with at least User Administrator rights to complete it. You can get a free trial subscription at [Try Microsoft Azure for free](#).

Change group license assignment

1. Open <https://entra.microsoft.com> to get to the Microsoft Entra admin center.
2. In the left navigation, open **Groups**.
3. Select **All groups**, then select one of the available groups.
4. In the left navigation, under **Manage**, select **Licenses**.

You see a list of any license assignments that are currently made. And you find that you have to use the Microsoft 365 Admin Center to make any updates.

5. Review the current assignments and then, on the menu, select **+ Assignments**.
6. Open <https://admin.microsoft.com> to open the Microsoft 365 admin center.
7. Select **Billing**. Then select **Licenses**.
8. Select an available license from the list.
9. Select **Groups** from the menu near the top of the page.
10. Select the **+ Assign licenses** option.
11. Pick the group you were looking at earlier in Microsoft Entra. Then select the **Assign** button at the bottom of the page.
12. On the group's Licenses page, review the change. You should be able to see the change in both the Microsoft Entra admin center and the Microsoft 365 admin center.

Identify and resolve license assignment problems for a group in Microsoft Entra ID

Group-based licensing in Microsoft Entra ID introduces the concept of users in a licensing error state. In this section, we explain the reasons why users might end up in this state.

When you assign licenses directly to individual users, without using group-based licensing, the assignment operation might fail. For example, when you execute the PowerShell cmdlet `Set-MgUserLicense` on a user object, the cmdlet can fail for many reasons that are related to business logic. For example, there might be an insufficient number of licenses or a conflict between two service plans that can't be assigned at the same time. The problem is immediately reported back to you.

When you're using group-based licensing the same errors can occur, but they happen in the background while the Microsoft Entra service is assigning licenses. For this reason, the errors can't be communicated to you immediately. Instead, they're recorded on the user object and then reported via the administrative portal. The original intent to license the user is never lost, but it's recorded in an error state for future investigation and resolution.

Not enough licenses

Problem: There aren't enough available licenses for one of the products specified in the group. You need to either purchase more licenses for the product or free up unused licenses from other users or groups.

To see how many licenses are available, go to **Microsoft Entra - Identity - Billing**, then **Licenses**, then **All products**.

To see which users and groups are consuming licenses, select a product. Under **Licensed users**, you see a list of all users who have licenses assigned directly or via one or more groups. Under **Licensed groups**, you see all groups with product licenses assigned.

PowerShell: PowerShell cmdlets report this error as *CountViolation*.

Service plans that conflict

Problem: One of the products specified in the group contains a service plan that conflicts with another service plan that's already assigned to the user via a different product. Some service plans are configured in a way that they can't be assigned to the same user as another, related service plan.

Consider the following example. A user has a license for Office 365 Enterprise *E1* assigned directly, with all the plans enabled. The user is added to a group that has the Office 365 Enterprise *E3* product assigned to it. The E3 product contains service plans that can't overlap with the plans that are included in E1, so the group license assignment fails with the **Conflicting service plans** error. In this example, the conflicting service plans are:

- SharePoint Online (Plan 2) conflicts with SharePoint Online (Plan 1).
- Exchange Online (Plan 2) conflicts with Exchange Online (Plan 1).

To solve this conflict, you need to disable two of the plans. You can disable the E1 license directly assigned to the user. Or, you need to modify the entire group license assignment and disable the plans in the E3 license. Alternatively, you might decide to remove the E1 license from the user if it's redundant in the context of the E3 license.

The decision about how to resolve conflicting product licenses always belongs to the administrator. Microsoft Entra ID doesn't automatically resolve license conflicts.

PowerShell: PowerShell cmdlets report this error as *MutuallyExclusiveViolation*.

Other products depend on this license

Problem: One of the products specified in the group contains a service plan that must be enabled for another service plan, in another product, to function. This error occurs when Microsoft Entra ID attempts to remove the underlying service plan. For example, this can happen when you remove the user from the group.

To solve this problem, you need to make sure that the required plan is still assigned to users through some other method or that the dependent services are disabled for those users. After doing that, you can properly remove the group license from those users.

PowerShell: PowerShell cmdlets report this error as *DependencyViolation*.

Usage location isn't allowed

Problem: Some Microsoft services aren't available in all locations because of local laws and regulations. Before you can assign a license to a user, you must specify the **Usage location** property for the user. You can specify the location under the **User**, then **Profile**, then **Edit** the section in the Azure portal.

When Microsoft Entra ID attempts to assign a group license to a user whose usage location isn't supported, it fails and records an error on the user.

To solve this problem, remove users from unsupported locations from the licensed group. Alternatively, if the current usage location values don't represent the actual user location, you can modify them so that the licenses are correctly assigned next time (if the new location is supported). You can specify the usage location under the user's **Properties** tab in the [Microsoft Entra admin center](#).

PowerShell: PowerShell cmdlets report this error as *ProhibitedInUsageLocationViolation*.

Note

When Microsoft Entra ID assigns group licenses, any users without a specified usage location inherit the location of the directory. We recommend that administrators set the correct usage location values on users before using group-based licensing to comply with local laws and regulations.

Duplicate proxy addresses

If you use Exchange Online, some users in your organization might be incorrectly configured with the same proxy address value. When group-based licensing tries to assign a license to such a user, it fails and shows "Proxy address is already being used."

After you resolve any proxy address problems for the affected users, make sure to force license processing on the group to ensure that the licenses can now be applied.

Microsoft Entra Mail and ProxyAddresses attribute change

Problem: While updating license assignment on a user or a group, you might see that the Microsoft Entra Mail and ProxyAddresses attribute of some users are changed.

Updating license assignment on a user causes the proxy address calculation to be triggered, which can change user attributes.

LicenseAssignmentAttributeConcurrencyException in audit logs

Problem: User has LicenseAssignmentAttributeConcurrencyException for license assignment in audit logs. When group-based licensing tries to process concurrent license assignment of the same license to a user, this exception is recorded on the user. This typically happens when a user is a member of more than one group with same assigned license. Microsoft Entra ID retries processing the user license and will resolve the issue. There's no action required from the customer to fix this issue.

More than one product license assigned to a group

You can assign more than one product license to a group. For example, you can assign Office 365 Enterprise E3 and Enterprise Mobility + Security to a group to easily enable all included services for users.

Microsoft Entra ID attempts to assign all licenses that are specified in the group to each user. If Microsoft Entra ID can't assign one of the products because of business logic problems, it won't assign the other licenses in the group either. An example is if there aren't enough licenses for all, or if there are conflicts with other services that are enabled on the user.

You can see the users who failed to get assigned and check which products are affected by this problem.

When a licensed group is deleted

You must remove all licenses assigned to a group before you can delete the group. However, removing licenses from all the users in the group can take time. There can be failures if user has a dependent license assigned. If a user has a license that's dependent on a license, which is being removed due to group deletion, the license assignment to the user is converted from inherited to direct.

For example, consider a group that has Office 365 E3/E5 assigned with a Skype for Business service plan enabled. Also imagine that a few members of the group have Audio Conferencing licenses assigned directly. When the group is deleted, group-based licensing tries to remove Office 365 E3/E5 from all users. Because Audio Conferencing is dependent on Skype for Business, for any users with Audio Conferencing assigned, group-based licensing converts the Office 365 E3/E5 licenses to direct license assignment.

Manage licenses for products with prerequisites

Some Microsoft Online products you might own are *add-ons*. Add-ons require a prerequisite service plan to be enabled for a user or a group before they can be assigned a license. With group-based licensing, the system requires that both the prerequisite and add-on service plans be present in the same group to ensure that any users who are added to the group can receive the fully working product. Let's consider the following example:

Microsoft Workplace Analytics is an add-on product. It contains a single service plan with the same name. We can only assign this service plan to a user, or group, when one of the following prerequisites is also assigned:

- Exchange Online (Plan 1)
- Exchange Online (Plan 2)

If we try to assign this product on its own to a group, the portal returns a notification message. If we select the item details, it shows the following error message:

License operation failed. Make sure that the group has necessary services before adding or removing a dependent service. **The service Microsoft Workplace Analytics requires Exchange Online (Plan 2) to be enabled as well.**

To assign this add-on license to a group, we must ensure that the group also contains the prerequisite service plan. For example, we might update an existing group that already contains the full Office 365 E3 product, and then add the add-on product to it.

It's also possible to create a standalone group that contains only the minimum required products to make the add-on work. It can then be used to license only selected users for the add-on product. Based on the previous example, you would assign the following products to the same group:

- Office 365 Enterprise E3 with only the Exchange Online (Plan 2) service plan enabled
- Microsoft Workplace Analytics

From now on, any users added to this group consume one license of the E3 product and one license of the Workplace Analytics product. At the same time, those users can be members of another group that gives them the full E3 product, and they still consume only one license for that product.

Tip

You can create multiple groups for each prerequisite service plan. For example, if you use both Office 365 Enterprise E1 and Office 365 Enterprise E3 for your users, you can create two groups to license Microsoft Workplace Analytics: one that uses E1 as a prerequisite and the other that uses E3. This lets you distribute the add-on to E1 and E3 users without consuming more licenses.

Force the group license process to resolve errors

Depending on what steps taken to resolve the errors, it might be necessary to manually trigger the processing of a group to update the user state.

For example, if you free up some licenses by removing direct license assignments from users, you need to trigger the processing of groups that previously failed to fully license all user members. To reprocess a group, go to the group pane, open **Licenses**, and then select the **Reprocess** button on the toolbar.

Force the user license process to resolve errors

Depending on what steps taken to resolve the errors, it might be necessary to manually trigger the processing of a user to update the user's state.

For example, after you resolve duplicate proxy address problem for an affected user, you need to trigger the processing of the user. To reprocess a user, go to the user pane, open **Licenses**, and then select the **Reprocess** button on the toolbar.

How to migrate users with individual licenses to group licenses

You can have existing licenses deployed to users in the organizations via direct assignment; that is, using PowerShell scripts or other tools to assign individual user licenses. Before you begin using group-based licensing to manage licenses in your organization, you can use this migration plan to seamlessly replace existing solutions with group-based licensing.

Keep in mind that you should avoid a situation in which migrating to group-based licensing results in users temporarily losing their currently assigned licenses. Any process that result in removal of licenses should be avoided to remove the risk of users losing access to services and their data.

Recommended migration process

1. You have existing automation (for example, PowerShell) managing license assignment and removal for users. Leave it running as is.
2. Create a new licensing group (or decide which existing groups to use) and make sure that all required users are added as members.
3. Assign the required licenses to those groups; your goal should be to reflect the same licensing state your existing automation (for example, PowerShell) is applying to those users.
4. Verify that licenses are applied to all users in those groups. This application can be done by checking the processing state on each group and by checking Audit Logs.
 - You can perform a random check of a few individual users by looking at their license details. You see that they have the same licenses assigned "directly" and "inherited" from groups.
 - You can run a PowerShell script to [verify how licenses are assigned to users](#).
 - When the same product license is assigned to the user both directly and through a group, only one license is consumed by the user. Hence no more licenses are required to perform migration.
5. Verify that no license assignments failed by checking each group for users in error state.

Consider removing the original direct assignments. We recommend that you do it gradually, and monitor the outcome on a subset of users first. If you leave the original direct assignments on users, when the users leave their licensed groups they retain the directly assigned licenses, which might not be what you want.

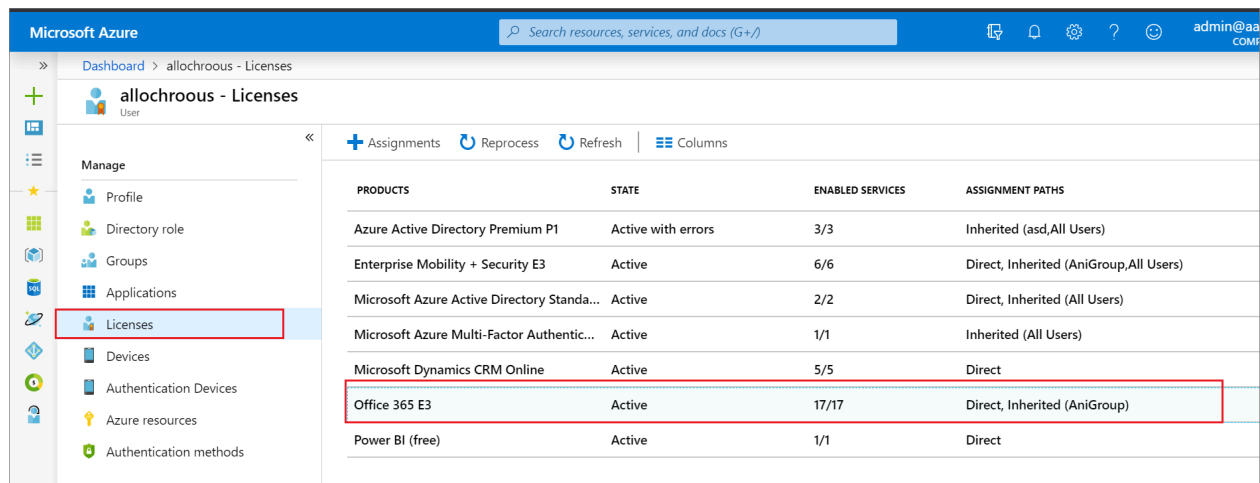
An example

An organization has 1,000 users. All users require Office 365 Enterprise E3 licenses. Currently the organization has a PowerShell script running on premises, adding and removing licenses from users as they come and go. However, the organization wants to replace the script with group-based licensing so licenses can be managed automatically by Microsoft Entra ID.

Here is what the migration process could look like:

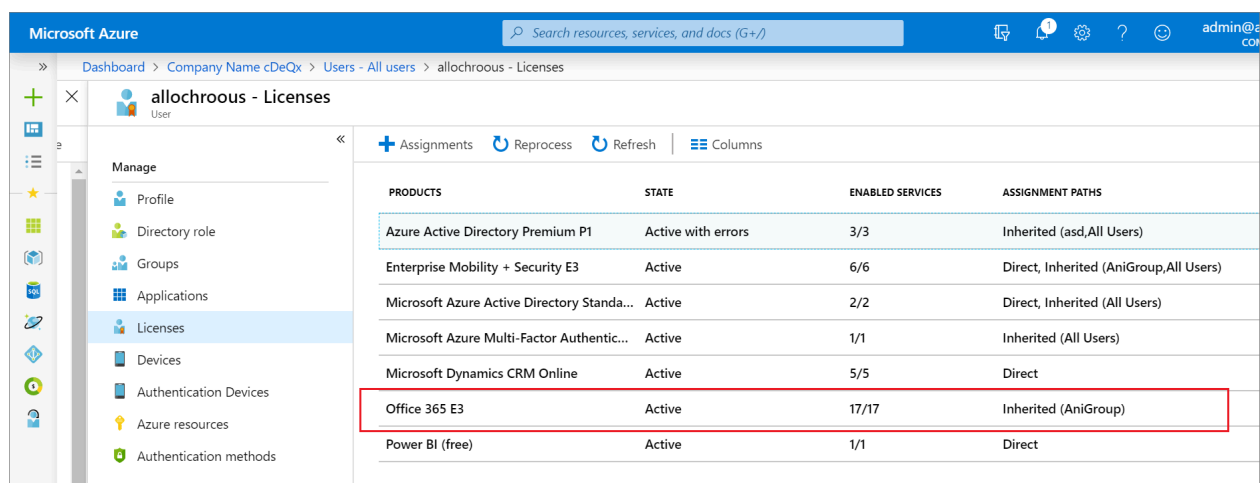
1. Using the Azure portal, assign the Office 365 E3 license to the **All users** group in Microsoft Entra ID.
2. Confirm that license assignment has completed for all users. Go to the overview page for the group, select **Licenses**, and check the processing status at the top of the **Licenses** page.
 - Look for "Latest license changes have been applied to all users" to confirm processing has completed.
 - Look for a notification on top about any users for whom licenses were not successfully assigned. Did we run out of licenses for some users? Do some users have conflicting license plans that prevent them from inheriting group licenses?

3. You need to check a few users to verify that they have both the direct and group licenses applied. Go to the profile page for a user, select Licenses, and examine the state of licenses.
- This is the expected user state during migration:



PRODUCTS	STATE	ENABLED SERVICES	ASSIGNMENT PATHS
Azure Active Directory Premium P1	Active with errors	3/3	Inherited (asd,All Users)
Enterprise Mobility + Security E3	Active	6/6	Direct, Inherited (AniGroup,All Users)
Microsoft Azure Active Directory Standa...	Active	2/2	Direct, Inherited (All Users)
Microsoft Azure Multi-Factor Authentic...	Active	1/1	Inherited (All Users)
Microsoft Dynamics CRM Online	Active	5/5	Direct
Office 365 E3	Active	17/17	Direct, Inherited (AniGroup)
Power BI (free)	Active	1/1	Direct

4. After confirming that both direct and group licenses are equivalent, you can start removing direct licenses from users. You can test this by removing them for individual users in the portal and then run automation scripts to have them removed in bulk. Here's an example of the same user with the direct licenses removed through the portal. Notice that the license state remains unchanged, but we no longer see direct assignments.



PRODUCTS	STATE	ENABLED SERVICES	ASSIGNMENT PATHS
Azure Active Directory Premium P1	Active with errors	3/3	Inherited (asd,All Users)
Enterprise Mobility + Security E3	Active	6/6	Direct, Inherited (AniGroup,All Users)
Microsoft Azure Active Directory Standa...	Active	2/2	Direct, Inherited (All Users)
Microsoft Azure Multi-Factor Authentic...	Active	1/1	Inherited (All Users)
Microsoft Dynamics CRM Online	Active	5/5	Direct
Office 365 E3	Active	17/17	Inherited (AniGroup)
Power BI (free)	Active	1/1	Direct

Change license assignments for a user or group in Microsoft Entra ID

This section describes how to move users and groups between service license plans in Microsoft Entra ID. The goal is to ensure that there's no loss of service or data during the license change. Users should switch between services seamlessly. The license plan assignment steps in this section describe changing a user or group on Office 365 E1 to Office 365 E3, but the steps apply to all license plans. When you update license assignments for a user or group, the license assignment removals and new

assignments are made simultaneously so that users don't lose access to their services during license changes or see license conflicts between plans.

Before you update the license assignments, verify certain assumptions are true for all of the users or groups to be updated. If the assumptions aren't true for all of the users in a group, the migration might fail for some. As a result, some of the users might lose access to services or data. Ensure that:

- Users have the current license plan that's assigned to a group and inherited by the user and not assigned directly.
- You have enough available licenses for the license plan you're assigning. If you don't have enough licenses, some users might not be assigned the new license plan. You can check the number of available licenses.
- Always confirm users don't have assigned service licenses that can conflict with the desired license or prevent removal of the current license. For example, a license from a service such as Workplace Analytics or Project Online that has a dependency on other services.
- If you manage groups on-premises and sync them into Microsoft Entra ID via Microsoft Entra Connect, then you add or remove users by using your on-premises system. It can take some time for the changes to sync with Microsoft Entra ID to be picked up by group licensing.
- If you're using Microsoft Entra dynamic group memberships, you add or remove users by changing their attributes, but the update process for license assignments remains the same.

10. Exercise - change user license assignments

<https://learn.microsoft.com/en-us/training/modules/create-configure-manage-identities/10-exercise-change-user-license-assignments>

Exercise - change user license assignments

Completed

Exercise environment needs - this lab assumes you have a basic Microsoft Entra tenant with at least User Administrator rights to complete it. You can get a free trial subscription at [Try Microsoft Azure for free](#).

Create a new user in Microsoft Entra ID

1. Browse to the [Microsoft Entra admin center](#).
2. In the left navigation, under **Identity**, select **Users**.
3. In the Users page, on the menu, select + **New user** and then **Create new user**.

4. Create a user using the following information:

Setting	Value
User name	DominiqueK
Name	Dominique Koch
First name	Dominique
Last name	Koch
Password	Make a unique password for the user
Usage location	Select your preferred usage location

5. When complete, verify the account for Dominique Koch is shown in the **All users** list.

Update user license assignments

License assignment to individual users is managed through the Microsoft 365 admin center.

1. Open the [Microsoft 365 admin center](#).
2. Select **Billing**, then select **Licenses**.
3. Select an available license from the list.
4. Select **Licensed users** from the menu near the top of the page.
5. Select **+ Assign licenses**.
6. Search for and select **Dominique Koch**, then select **Assign** at the bottom of the page.
7. When complete, verify the license is listed on Dominique Koch's profile in the Microsoft Entra admin center under **Identity** > **Users** > select the user > **Licenses**.

11. Create custom security attributes

<https://learn.microsoft.com/en-us/training/modules/create-configure-manage-identities/11-create-custom-security-attributes>

Create custom security attributes

Completed

Home > Security | Getting started >

Custom attributes

[+ Add attribute set](#) [Refresh](#) [Got feedback?](#)

Search attribute set name

Attribute set name	Description
Banker	This person can write checks against the bank

New attribute set

Add an attribute set to group and manage related custom security attributes. All custom security attributes must be a part of an attribute set. [Learn more](#)

Attribute set name *

Description

Maximum number of attributes

New attribute

Add a custom security attribute (key-value pair) to your directory that you can later assign to Microsoft Entra objects, such as users or applications. [Learn more](#)

Attribute name *

Description

Data type *

Allow multiple values to be assigned ☐ Yes ☒ No

Only allow predefined values to be assigned ☐ Yes ☒ No

Predefined values

Value	Is active?
No results	

What is a custom security attribute?

Custom security attributes in Microsoft Entra ID are business-specific attributes (key-value pairs) that you can define and assign to Microsoft Entra objects. These attributes can be used to store information, categorize objects, or enforce fine-grained access control over specific Azure resources.

Why use custom security attributes?

- Extend user profiles, such as add Hourly Salary to all my employees.
- Ensure only administrators can see the Hourly Salary attribute in my employees' profiles.
- Categorize hundreds or thousands of applications to easily create a filterable inventory for auditing.
- Grant users access to the Azure Storage blobs belonging to a project.

What can I do with custom security attributes?

- Define business-specific information (attributes) for your tenant.
- Add custom security attributes to Microsoft Entra users and enterprise applications (service principals).
- Manage Microsoft Entra objects using custom security attributes with queries and filters.
- Provide attribute governance so attributes determine who can get access.

Custom security attributes are **not** supported in Microsoft Entra Domain Services, SAML token claims, or JSON Web Token (JWT) claims.

Features of custom security attributes

- Available tenant-wide
- Include a description
- Support different data types: Boolean, integer, string
- Support single value or multiple values
- Support user-defined free-form values or predefined values

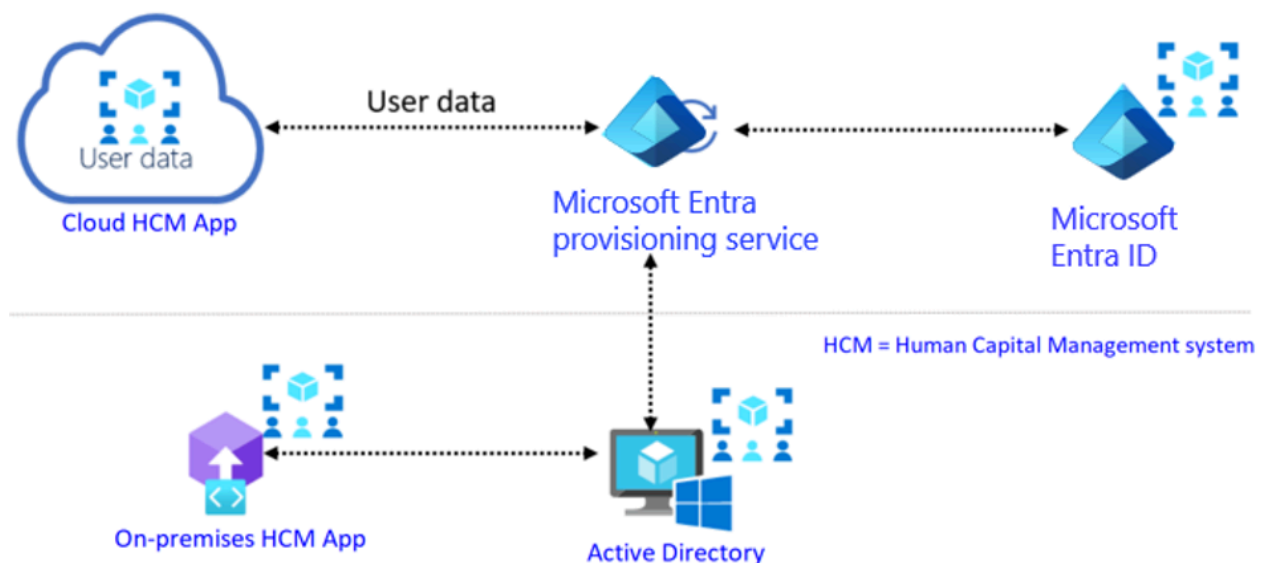
- Assign custom security attributes to directory synced users from an on-premises Active Directory

12. Explore automatic user creation

<https://learn.microsoft.com/en-us/training/modules/create-configure-manage-identities/12-explore-automatic-user-creation>

Explore automatic user creation

Completed



Components of SCIM (System for Cross-Domain Identity Management)

- **HCM system** - Applications and technologies that enable Human Capital Management process and practices that support and automate HR processes throughout the employee lifecycle.
- **Microsoft Entra Provisioning Service** - Uses the SCIM 2.0 protocol for automatic provisioning. The service connects to the SCIM endpoint for the application, and uses the SCIM user object schema and REST APIs to automate provisioning and deprovisioning of users and groups.
- **Microsoft Entra ID** - User repository used to manage the lifecycle of identities and their entitlements.

- **Target system** - Application or system that has SCIM endpoint and works with the Microsoft Entra provisioning to enable automatic provisioning of users and groups.

Why use SCIM?

System for Cross-Domain Identity Management (SCIM) is an open standard protocol for automating the exchange of user identity information between identity domains and IT systems. SCIM ensures that employees added to the Human Capital Management (HCM) system automatically have accounts created in Microsoft Entra ID or Windows Server Active Directory. User attributes and profiles are synchronized between the two systems, updating, or removing users based on the user status or role change.

The key is keeping your identity systems up to date. If a user can be automatically deprovisioned from Microsoft Entra ID as soon as they're removed from your HR systems, you have less worry about a possible breach.

API-driven inbound provisioning

Not all HR systems expose a SCIM endpoint. For these scenarios, Microsoft Entra ID supports **API-driven inbound provisioning**, which reached general availability in March 2024. Instead of requiring the source system to push data via SCIM, any automation tool, or script can retrieve workforce data from any system of record and send it to the Microsoft Entra provisioning API. Supported authoritative sources include Workday, SAP SuccessFactors, and any custom HR system integrated via the API. This approach gives organizations flexibility to automate identity lifecycle management regardless of their HR platform's native integration capabilities.

13. Module assessment

<https://learn.microsoft.com/en-us/training/modules/create-configure-manage-identities/13-knowledge-check>

Module assessment

Completed

14. Summary and resources

Summary and resources

Completed

You completed this module, you are able to:

- Create, configure, and manage users
- Create, configure, and manage groups
- Manage licenses
- Configure and manage device registration
- Explore custom security attributes and automatic account provisioning

Resources

Use these resources to discover more:

- [Quickstart: Create and assign a user account](#)
- [Bulk create users in Microsoft Entra ID](#)
- [Create a basic group and add members using Microsoft Entra ID](#)
- [Create or update a dynamic membership group in Microsoft Entra ID](#)
- [What is Microsoft Entra Cloud Sync?](#)
- [Manage license requests](#)
- [Assign licenses to users - Microsoft 365 Admin Center](#)
- [Plan Microsoft Entra device deployment](#)
- [API-driven inbound provisioning concepts](#)