# Exercise 02 - Sign in to Microsoft Intune

Once you have signed up for Intune, you can use any device with a [supported browser](https://docs.microsoft.com/en-us/mem/intune/fundamentals/supported-devices-browsers#intune-supported-web-browsers) to sign in to the [Microsoft Endpoint Manager admin center](https://go.microsoft.com/fwlink/??zure-portal=true&linkid=2109431) to administer the Intune service.

**Note**

Microsoft Intune is a part of Microsoft Endpoint Manager. Microsoft Endpoint Manager is the overall management platform for managing, protecting, and monitoring all of your organization's endpoints.

1. In a supported web browser, navigate to the [Microsoft Endpoint Manager admin center](https://go.microsoft.com/fwlink/?linkid=2109431).
2. Sign in using your newly created user name and password.

# Exercise 03 - View Intune free trial details

To view the Intune product details for your free trial, use the following steps:

1. Sign in to the [Microsoft 365 admin center](https://go.microsoft.com/fwlink/p/?LinkId=698854).
2. Select **Your products** > **Microsoft Intune Trial**.

The **Microsoft Intune Trial** pane provides license, subscription, and product details.

# Exercise 04 - Add users to Intune

The people in your organization each need a user account before they can sign in and access Microsoft Intune. To create user accounts, you can add users to Intune. Once added, you can grant permissions and assign licenses to users. Then later, you can assign different types of policies to users to help and protect them.

As an administrator, you can add users individually or in bulk to Intune. The easiest way to add user accounts is to add them one at a time in the Microsoft Endpoint Manager admin center.

**Note**

You must be an admin (global, license, or a user admin) to add users to Intune. If you set up Intune using the free trial, you are a global admin.

## Add individual Intune users one at a time

The following steps allow you to add individual users to Intune:

1. In the [Microsoft Endpoint Manager admin center](https://go.microsoft.com/fwlink/?linkid=2109431%3Fazure-portal%3Dtrue), choose **Users** > **All users** > **New user** > **Create user**.
2. Specify the following user details:
   * **User name** - The new name that the user will use to sign in to Azure Active Directory.
   * **Name** - The user's given name.
3. Choose whether you want to create the password for the new user or have it autogenerated.
4. (Optional) If you have already created a new group, you can assign the new user to the group. To assign the new user to groups, choose **0 groups selected** to open the **Groups** pane. Here you can select the groups you want to assign to the user. When finished selecting groups, choose **Select**.
5. (Optional) By default, the new user is assigned the role of **User**. If you want to add roles to the user, select **User** next to **Roles**. In the **Directory roles** pane, select the roles you want to assign to the user and then choose **Select**.
6. If you want to block the user from signing in, you can select **Yes** for **Block sign in**. Make sure to switch this back to **No** when you're ready to let the user sign in.
7. Choose a **Usage location** for the new user. Usage location is required before you can assign the new user an Intune license.
8. (Optional) You can also provide information for the **Job title**, **Department**, **Company name**, and **Manager** fields.
9. Select **Create** to add the new user to Intune.

## Add multiple Intune users at the same time

You can add Intune users in bulk by uploading a csv file containing the full list of users. The following steps allow you to add multiple users to Intune:

1. In the [Microsoft Endpoint Manager admin center](https://go.microsoft.com/fwlink/?linkid=2109431%3Fazure-portal%3Dtrue), choose **Users** > **All users** > **Bulk operations** > **Bulk create**. The **Bulk create user** pane is displayed.
2. Download, edit, and upload a *csv* template containing a list of users that you want to add to Intune.

The *csv* file is a comma-separated value list that can be edited in Notepad or Excel. For more information about using a *csv* file to add Intune users, see [Bulk create users in Azure Active Directory](https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/users-bulk-add).

**Note:** If you're using [**Microsoft Endpoint Configuration Manager**](https://docs.microsoft.com/en-us/learn/modules/intro-to-endpoint-manager/4-endpoint-configuration-manager) for your on-premises device management, you can configure directory synchronization to import user accounts from your on-premises Active Directory to Microsoft Azure Active Directory (Azure AD). Having your on-premises Active Directory service connected with all of your Azure Active Directory-based services makes managing user identity much simpler. You can use the [**Azure AD Connect wizard**](https://www.microsoft.com/download/details.aspx?id=47594) to connect your on-premises identity infrastructure to the cloud.

You can also add users manually using the Microsoft 365 admin center. For more information, see [Add Intune users in the Microsoft 365 admin center](https://docs.microsoft.com/en-us/mem/intune/fundamentals/users-add#add-intune-users-in-the-microsoft-365-admin-center?azure-portal=true) and [Add users and assign licenses at the same time](https://support.office.com/article/Add-users-individually-or-in-bulk-to-Office-365-Admin-Help-1970f7d6-03b5-442f-b385-5880b9c256ec).

# Exercise 05 - Create groups in Intune

Intune uses Azure Active Directory (Azure AD) groups to organize and manage devices and users. As an Intune admin, you can set up groups to suit your organizational needs. For instance, you can create groups to organize users or devices by geographic location, department, or hardware characteristics. Also, you can use groups to manage tasks at scale. For example, you can set policies for many users or deploy apps to a set of devices based on groups.

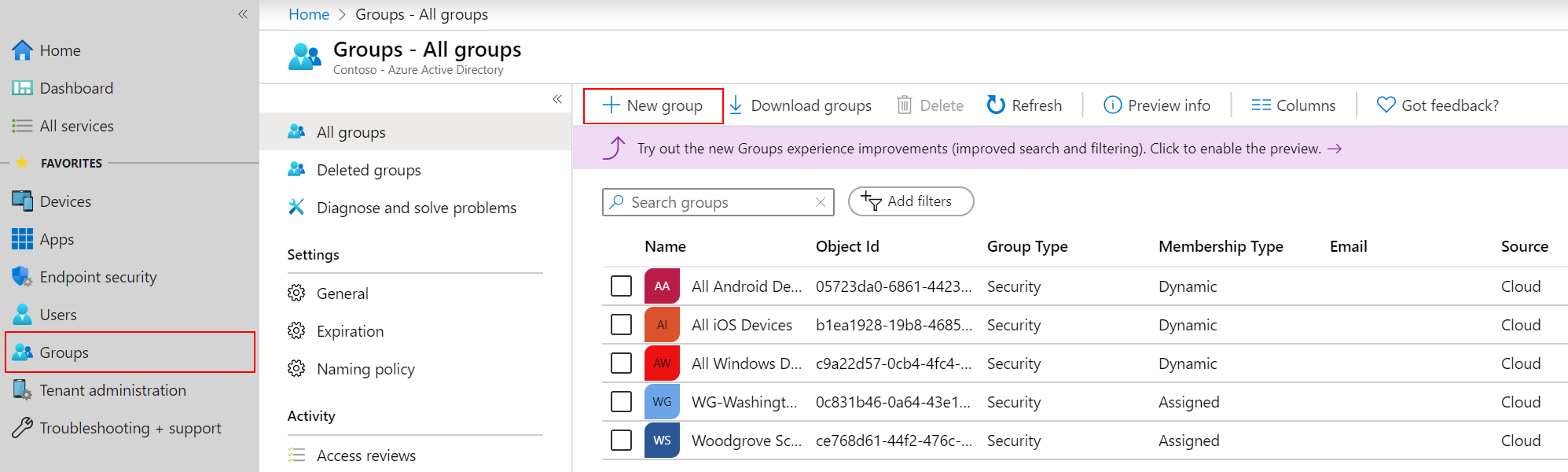
You can add the following types of groups in Intune:

* **Assigned groups** - Manually add users or devices into a static group.
* **Dynamic groups** (Requires [Azure AD Premium](https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-get-started-premium)) - Automatically add users or devices to user groups or device groups based on an expression you create. For example, when a user is added with the manager title, the user is automatically added to an **All managers** users group. Or, when a device has the iOS/iPadOS device OS type, the device is automatically added to an **All iOS/iPadOS devices** group.

## Add a new group

Use the following steps to create a new group:

1. Sign in to the [Microsoft Endpoint Manager admin center](https://go.microsoft.com/fwlink/?linkid=2109431).
2. Select **Groups** > **New group**:



1. In **Group type**, choose one of the following options:
   * **Security**: Security groups are used to assign apps, resources, and licenses to group members. Group members can be users, devices, service principals, and other groups. Security groups are recommended for your groups in Intune. You can create groups for users, such as **All Charlotte employees** or **Remote workers**. Or, create groups for devices, such as **All iOS/iPadOS devices** or **All Windows 10 student devices**.
   * **Microsoft 365**: Microsoft 365 groups collaboration opportunities by members access to a shared mailbox, calendar, files, SharePoint sites, and more. Group members can only be users. This option also lets you give people outside of your organization access to the group. For more information, see [Learn about Microsoft 365 Groups](https://support.office.com/article/learn-about-office-365-groups-b565caa1-5c40-40ef-9915-60fdb2d97fa2).

**Tip**

The users and groups created can also be seen in the [**Microsoft 365 admin center**](https://admin.microsoft.com/), [**Azure Active Directory admin center**](https://aad.portal.azure.com/), and [**Microsoft Intune in the Endpoint Manager admin center**](https://go.microsoft.com/fwlink/?linkid=2090973). In your organization tenant, you can create and manage groups in all these areas.

If your primary role is device management, we recommend you use the [**Microsoft Endpoint Manager admin center**](https://go.microsoft.com/fwlink/?linkid=2109431).

1. Enter a **Group name** and **Group description** for the new group.
2. Select whether Azure AD roles can be assigned to the group. If you choose **Yes**, you can assign a cloud group to Azure AD built-in roles. With this feature, you can use groups to grant admin access in Azure AD with minimal effort from your Global and Privileged role admins. Once set, the group's eligibility for role assignment is permanent.​ For more information, see [Use cloud groups to manage role assignments in Azure Active Directory](https://docs.microsoft.com/en-us/azure/active-directory/roles/groups-concept).
3. Select the **Membership type**. Your options include the following choices:
   * **Assigned**: Administrators manually assign users or devices to this group, and manually remove users or devices.
   * **Dynamic User**: Administrators create membership rules to automatically add and remove members.
   * **Dynamic Device**: Administrators create dynamic group rules to automatically add and remove devices.

**Note**

In this admin center, when you create users or groups, you might not see the **Azure Active Directory** branding. But, that's what you're using.

1. Choose whether you want to add owners and members at this time.
2. Click **Create** to add the new group. Your group is shown in the list.

You can create a wide variety of dynamic user and device groups you, such as:

* All Students in Contoso high school
* All Android Enterprise devices
* All iOS 11 and older devices
* Marketing
* Human Resources
* All Charlotte employees
* All WA employees

## Exercise 06 - Assign an Intune license to user

The following steps allow you to assign an Intune license to a user:

1. In the [Microsoft Endpoint Manager admin center](https://go.microsoft.com/fwlink/?linkid=2109431), select **Users** > **All Users** > the user's name > **Licenses** > **Assignments**. The **Update license assignments** pane is displayed.
2. Choose the box for **Intune** > **Save**.

The user account now has the permissions needed to use the service and enroll devices into management.

## Assign Intune licenses to multiple users

The following steps allow you to assign Intune licenses to multiple users all at once:

1. Sign in to the [**Azure AD admin center**](https://aad.portal.azure.com/).

**Note**

To manage licenses, the admin account must be a license administrator, user administrator, or global administrator. The account you create using the Intune free trial is a global administrator.

1. Select **Azure Active Directory** > **Licenses** > **All products** to see and manage all licensable products that you have available for your organization.
2. Select the box next to **Intune**.
3. Click **Assign** > **Add users and groups**.
4. If you have created a group of users, click the group to add it to the **Selected items** list. Otherwise, select individual users that you have created earlier. Click **Select** to confirm your selection.
5. Click **Next: Assignment options** to confirm **Microsoft Intune** is **On**.
6. Click **Review + assign** to confirm your license assignment settings.
7. Click **Assign** to assign the licenses to the selected users.

A notification is displayed in the upper-right corner that shows the status and outcome of the process. If the assignment to the group couldn't be completed (for example, because of pre-existing licenses in the group), you can click the notification to view details.

# Give permissions in Microsoft Endpoint Manager admin center

Because Intune is a part of Microsoft Endpoint Manager, you can add roles using Microsoft Endpoint Manager admin center. To grant permissions, follow these steps:

1. Sign in to the [Microsoft Endpoint Manager admin center](https://go.microsoft.com/fwlink/?linkid=2109431) with a global administrator account > **Users** > **All users** > the user's name. You'll see the user's **Profile**.
2. Select **Assigned roles** > **Add assignments**.
3. In the **Directory roles** pane, select the roles you want to assign to the user.
4. Click **Add**.

### Give permissions in Microsoft 365 admin center

You can also use the Microsoft 365 admin center to add roles. There are a number of additional roles available in the Microsoft 365 admin center that you can use with a variety of Microsoft services. The Microsoft 365 admin center also lets you manage Azure AD roles and Microsoft Intune roles.

**Tip**

To access the Microsoft 365 admin center, your account must have a **Sign-in allowed** set. In the portal under **Profile**, set **Block sign in** to **No** to allow access. This status is different from having a license to the subscription. By default, all user accounts are **Allowed**. Users without administrator permissions can use the Microsoft 365 admin center to reset Intune passwords.

To grant permissions, follow these steps:

1. Sign in to the [Microsoft 365 admin center](https://admin.microsoft.com/) with a global administrator account > select **Users** > **Active users** > choose the user to give admin permissions.
2. In the user pane, choose **Manage roles** under **Roles**.

**Note**

If you don't see a **Roles** section in the user pane, check whether the user has a license in the **Active users** list.

1. In the **Manage admin roles** pane, choose the admin permission to grant from the list of available roles.
2. Click **Save changes**.