**Lab 4B**

**Exercise 1: Create groups in Intune**

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**:

Adatum Mobile Users

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 Adatum 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 Employees in Adatum Organization
* All Android Enterprise devices
* All iOS 11 and older devices
* Marketing
* Human Resources
* All Adatum employees
* All Adatum Consultants
* All WA employees