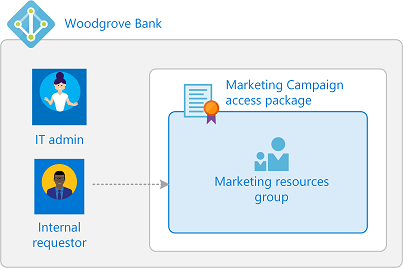
**Lab- Manage access to resources in Azure AD entitlement management**

Managing access to all the resources employees need, such as groups, applications, and sites, is an important function for organizations. You want to grant employees the right level of access they need to be productive and remove their access when it's no longer needed.

In this tutorial, you work for Woodgrove Bank as an IT administrator. You've been asked to create a package of resources for a marketing campaign that internal users can use to self-service request. Requests don't require approval and user's access expires after 30 days. For this tutorial, the marketing campaign resources are just membership in a single group, but it could be a collection of groups, applications, or SharePoint Online sites.



In this tutorial, you learn how to:

* Create an access package with a group as a resource
* Allow a user in your directory to request access
* Demonstrate how an internal user can request the access package

For a step-by-step demonstration of the process of deploying Azure Active Directory entitlement management, including creating your first access package, view the following video:

This rest of this article uses the Azure portal to configure and demonstrate Azure AD entitlement management.

**Prerequisites**

To use Azure AD entitlement management, you must have one of the following licenses:

* Azure AD Premium P2
* Enterprise Mobility + Security (EMS) E5 license

For more information, see [License requirements](https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-overview#license-requirements).

**Step 1: Set up users and group**

A resource directory has one or more resources to share. In this step, you create a group named **Marketing resources** in the Woodgrove Bank directory that is the target resource for entitlement management. You also set up an internal requestor.

**Prerequisite role:** Global administrator or User administrator



1. Sign in to the [Azure portal](https://portal.azure.com/) as a Global administrator or User administrator.
2. In the left navigation, select **Azure Active Directory**.
3. [Create two users](https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-users-azure-active-directory). Use the following names or different names.

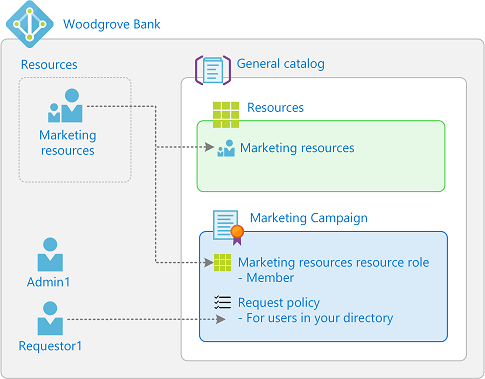
| **Name** | **Directory role** |
| --- | --- |
| **Admin1** | Global administrator, or User administrator. This user can be the user you're currently signed in. |
| **Requestor1** | User |

1. [Create an Azure AD security group](https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-groups-create-azure-portal) named **Marketing resources** with a membership type of **Assigned**. This group will be the target resource for entitlement management. The group should be empty of members to start.

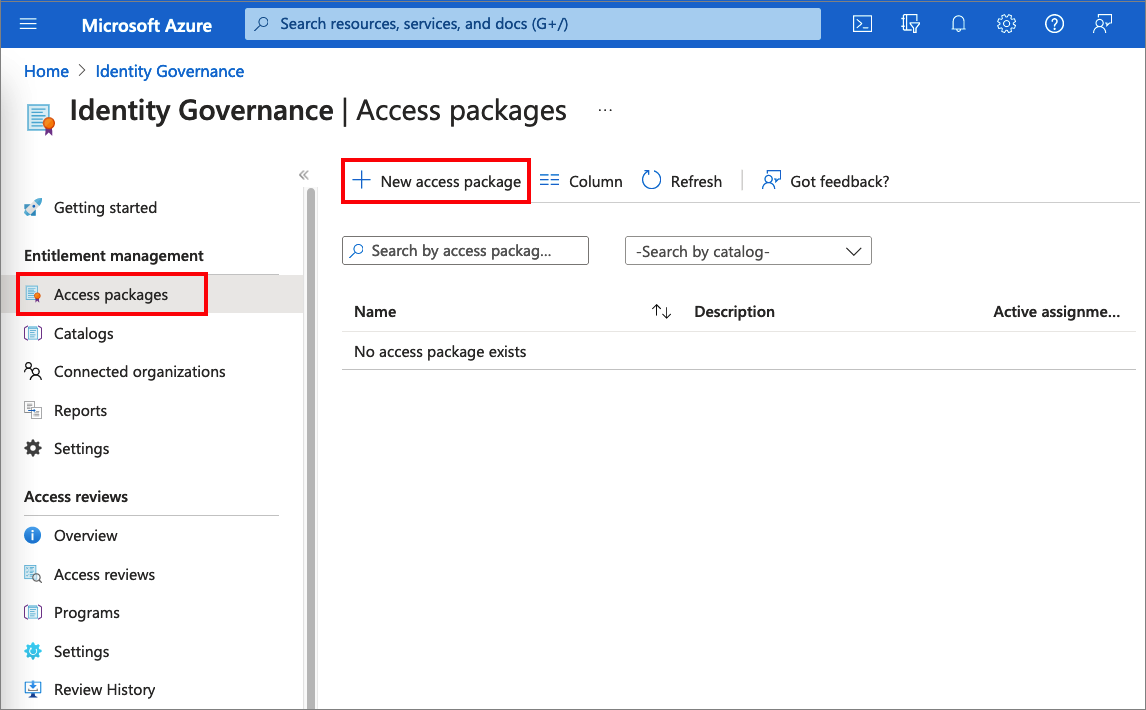
**Step 2: Create an access package**

An *access package* is a bundle of resources that a team or project needs and is governed with policies. Access packages are defined in containers called *catalogs*. In this step, you create a **Marketing Campaign** access package in the **General** catalog.

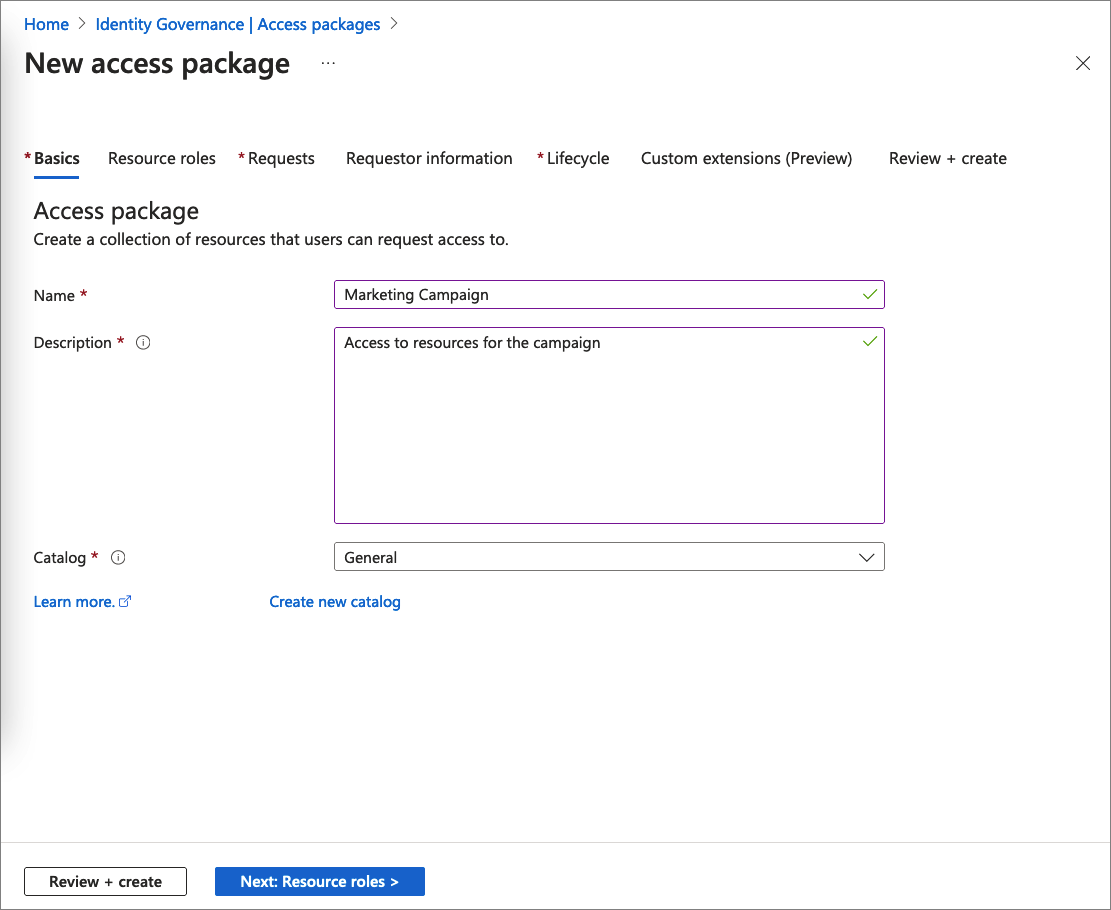
**Prerequisite role:** Global administrator, Identity Governance administrator, User administrator, Catalog owner, or Access package manager



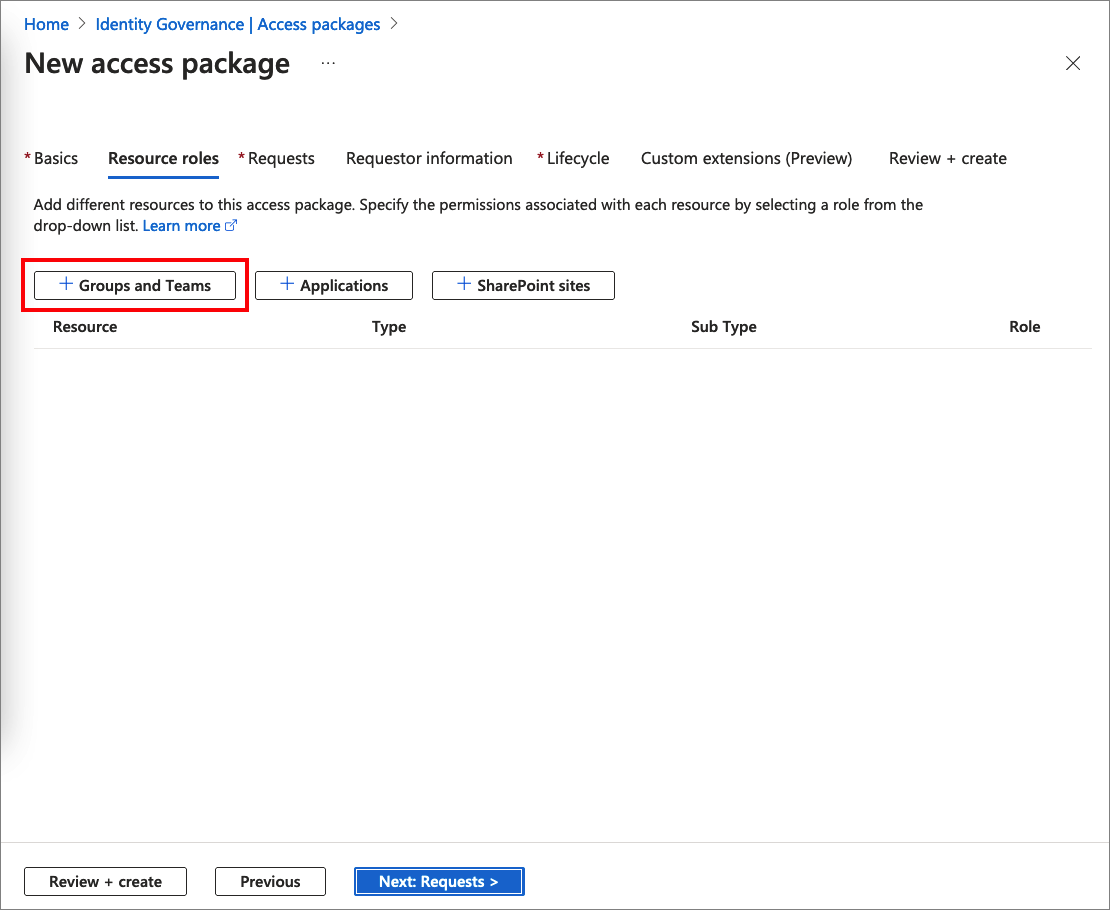
1. In the Azure portal, in the left navigation, select **Azure Active Directory**.
2. In the left menu, select **Identity Governance**
3. In the left menu, select **Access packages**. If you see **Access denied**, ensure that an Azure AD Premium P2 license is present in your directory.
4. Select **New access package**.



1. On the **Basics** tab, type the name *Marketing Campaign* access package and description *Access to resources for the campaign*.
2. Leave the **Catalog** drop-down list set to **General**.

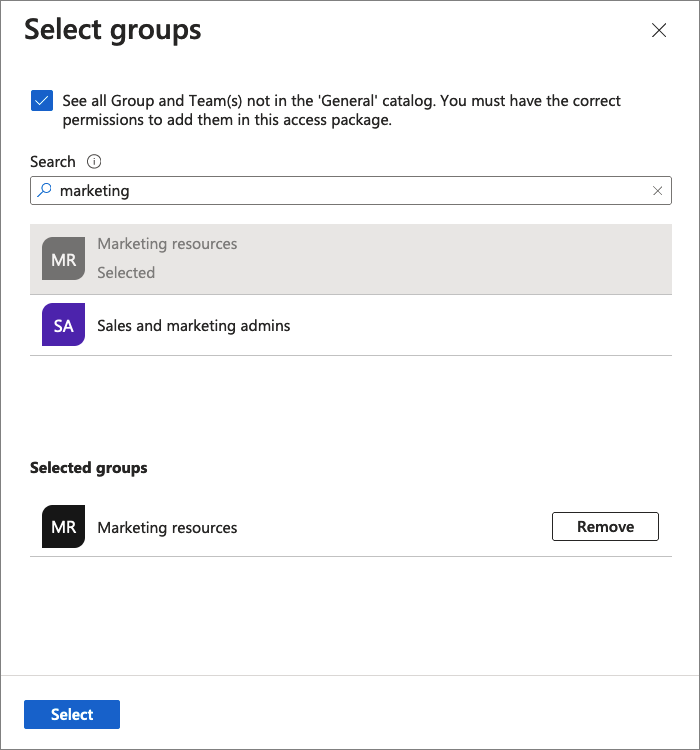


1. Select **Next** to open the **Resource roles** tab. On this tab, select the resources and the resource role to include in the access package. You can choose to manage access to groups and teams, applications, and SharePoint Online sites. In this scenario, select **Groups and Teams**.

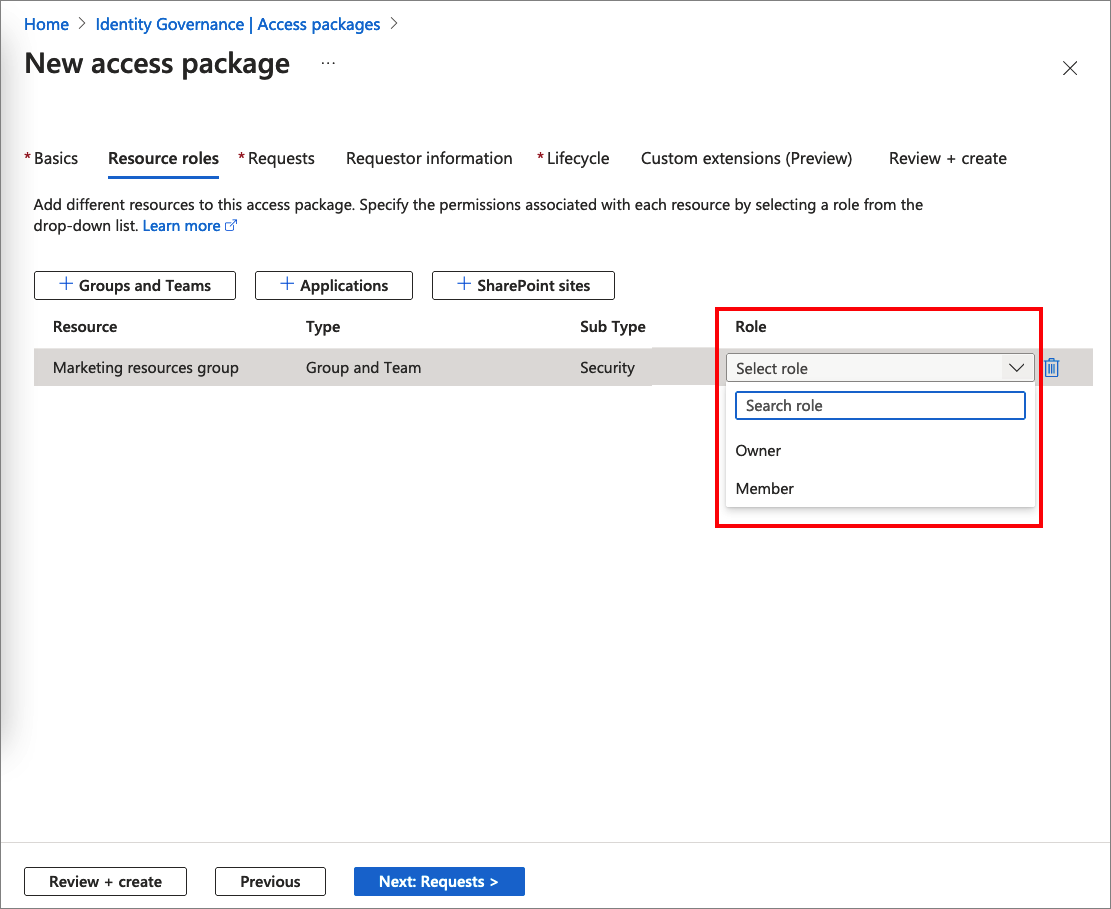


1. In the **Select groups** pane, find and select the **Marketing resources** group you created earlier.

By default, you see groups inside the General catalog. When you select a group outside of the General catalog, which you can see if you check the **See all** check box, it will be added to the General catalog.



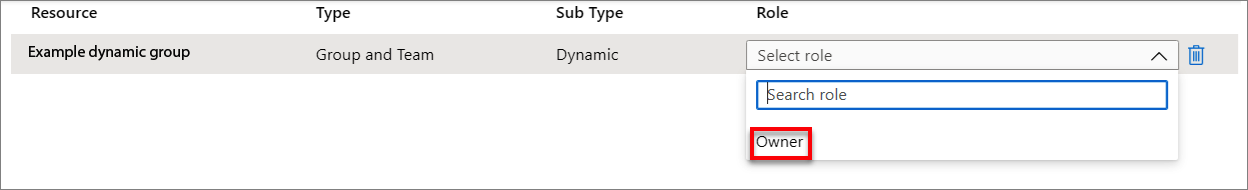
1. Choose **Select** to add the group to the list.
2. In the **Role** drop-down list, select **Member**. If you select the Owner role, it allows users to add or remove other members or owners. For more information on selecting the appropriate roles for a resource, read [add resource roles](https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-resources#add-resource-roles).

[](https://docs.microsoft.com/en-us/azure/active-directory/governance/media/entitlement-management-access-package-first/resource-roles.png#lightbox)

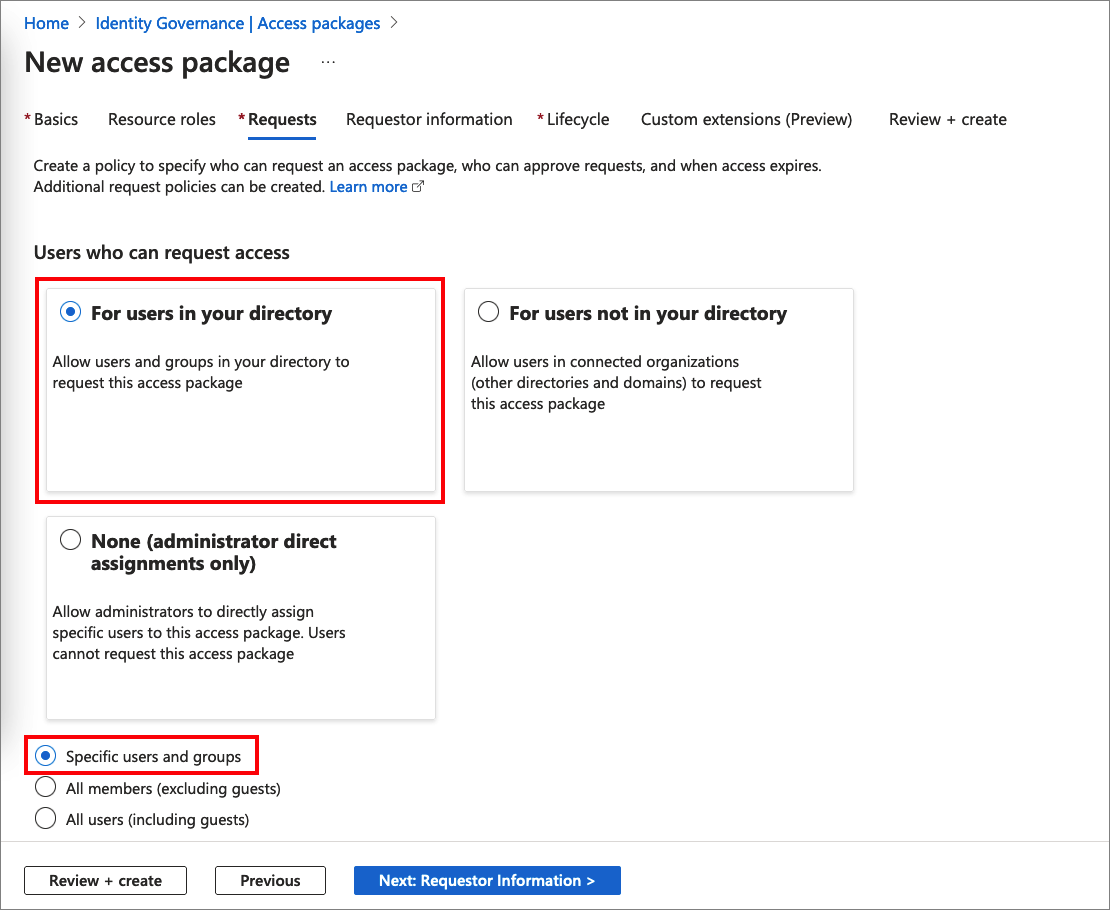
**Important**

The [**role-assignable groups**](https://docs.microsoft.com/en-us/azure/active-directory/roles/groups-concept) added to an access package will be indicated using the Sub Type **Assignable to roles**. For more information, check out the [**Create a role-assignable group**](https://docs.microsoft.com/en-us/azure/active-directory/roles/groups-create-eligible) article. Keep in mind that once a role-assignable group is present in an access package catalog, administrative users who are able to manage in entitlement management, including global administrators, user administrators and catalog owners of the catalog, will be able to control the access packages in the catalog, allowing them to choose who can be added to those groups. If you don't see a role-assignable group that you want to add or you are unable to add it, make sure you have the required Azure AD role and entitlement management role to perform this operation. You might need to ask someone with the required roles add the resource to your catalog. For more information, see [**Required roles to add resources to a catalog**](https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-delegate#required-roles-to-add-resources-to-a-catalog).

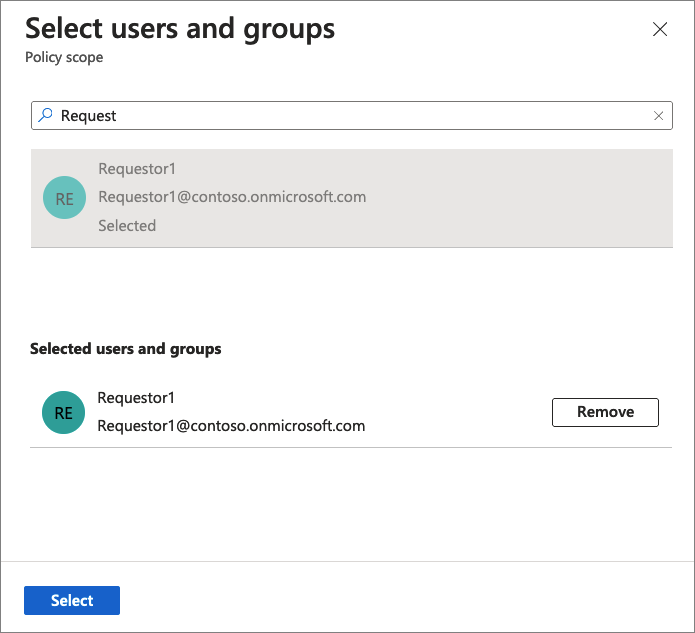
**Note**

When using [**dynamic groups**](https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-create-rule) you will not see any other roles available besides owner. This is by design. 

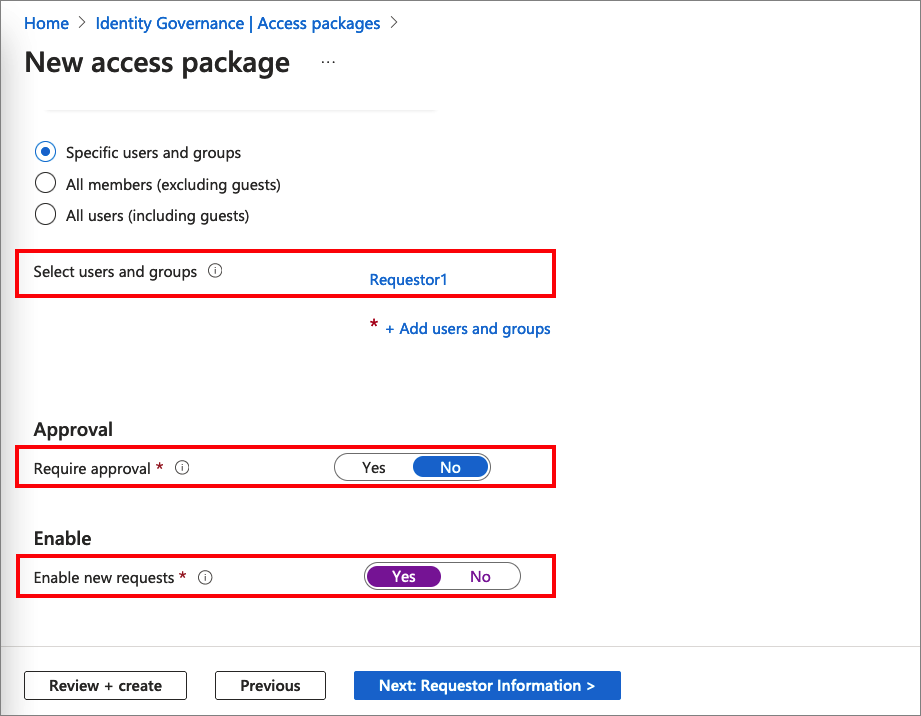
1. Select **Next** to open the **Requests** tab. On the Requests tab, you create a request policy. A *policy* defines the rules or guardrails to access an access package. You create a policy that allows a specific user in the resource directory to request this access package.
2. In the **Users who can request access** section, select **For users in your directory** and then select **Specific users and groups**.

[](https://docs.microsoft.com/en-us/azure/active-directory/governance/media/entitlement-management-access-package-first/new-access-package-requests.png#lightbox)

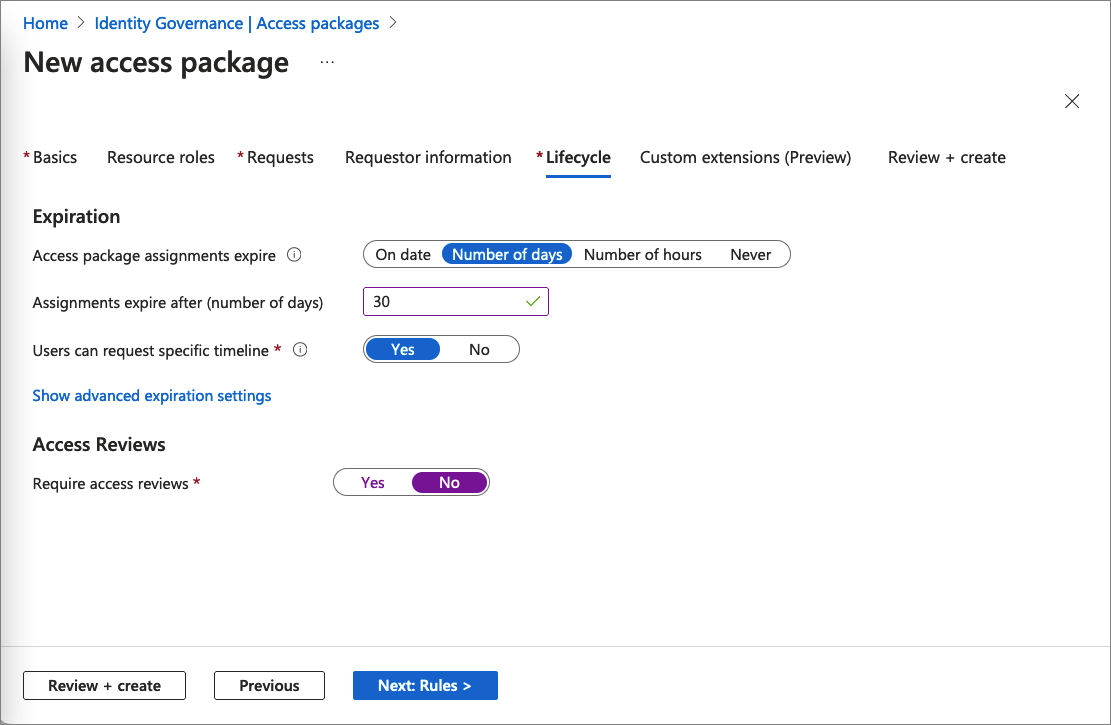
1. Select **Add users and groups**.
2. In the Select users and groups pane, select the **Requestor1** user you created earlier.



1. Choose **Select** to add the user to the list.
2. Scroll down to the **Approval** and **Enable requests** sections.
3. Leave **Require approval** set to **No**.
4. For **Enable requests**, select **Yes** to enable this access package to be requested as soon as it's created.
5. Select **Next** to open the **Requestor information** tab.

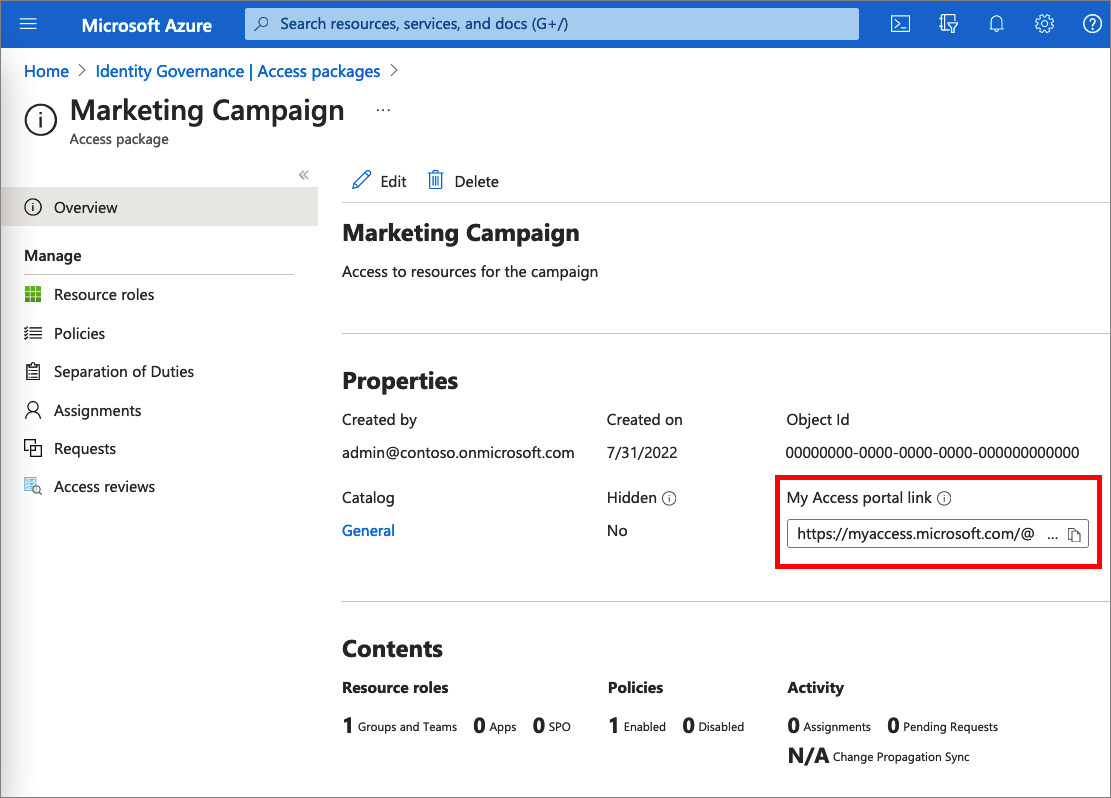


1. On the **Requestor information** tab, you can ask questions to collect more information from the requestor. The questions are shown on the request form and can be either required or optional. In this scenario, you haven't been asked to include requestor information for the access package, so you can leave these boxes empty. Select **Next** to open the **Lifecycle** tab.
2. On the **Lifecycle** tab, you specify when a user's assignment to the access package expires. You can also specify whether users can extend their assignments. In the **Expiration** section:
   1. Set the **Access package assignments expire** to **Number of days**.
   2. Set the **Assignments expire after** to **30** days.
   3. Leave the **Users can request specific timeline** default value, **Yes**.
   4. Set the **Require access reviews** to **No**.



1. Skip the **Custom extensions (Preview)** step.
2. Select **Next** to open the **Review + Create** tab.
3. On the **Review + Create** tab, select **Create**. After a few moments, you should see a notification that the access package was successfully created.
4. In left menu of the Marketing Campaign access package, select **Overview**.
5. Copy the **My Access portal link**.

You'll use this link for the next step.



**Step 3: Request access**

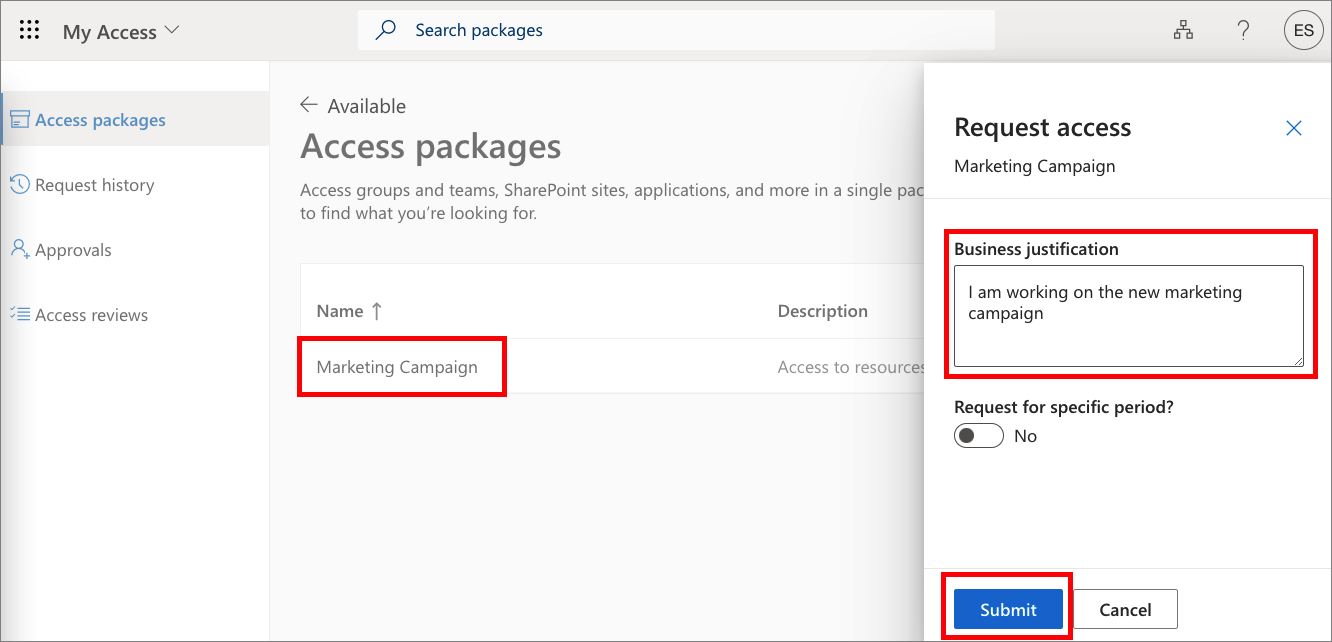
In this step, you perform the steps as the **internal requestor** and request access to the access package. Requestors submit their requests using a site called the My Access portal. The My Access portal enables requestors to submit requests for access packages, see the access packages they already have access to, and view their request history.

**Prerequisite role:** Internal requestor

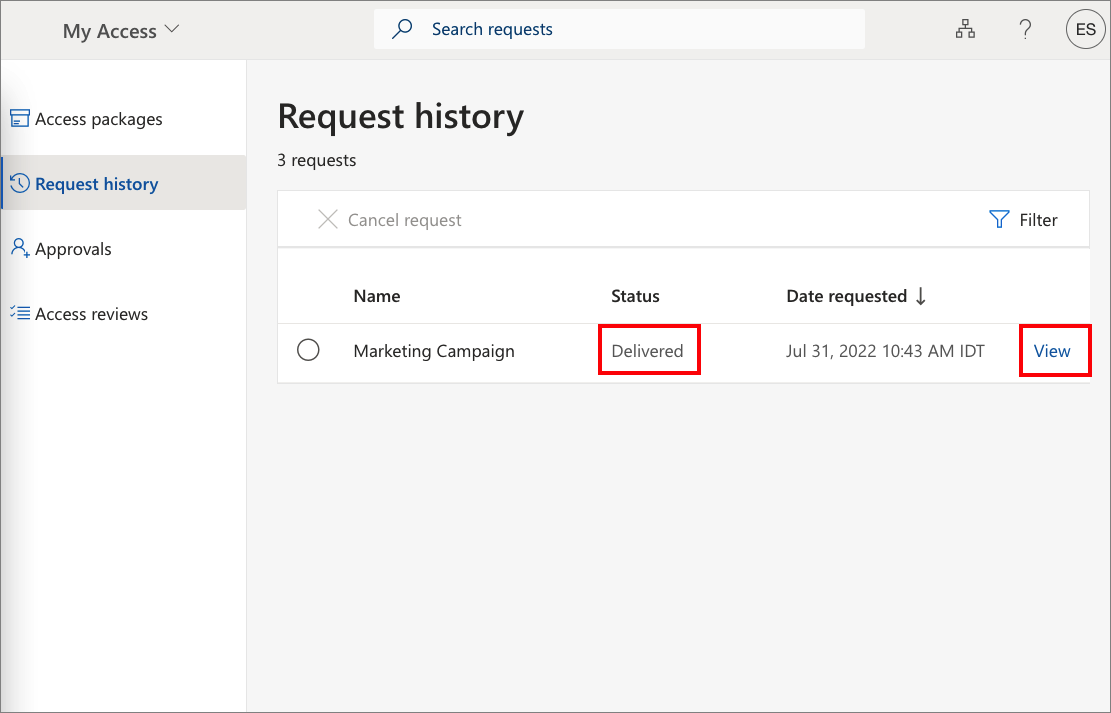
1. Sign out of the Azure portal.
2. In a new browser window, navigate to the My Access portal link you copied in the previous step.
3. Sign in to the My Access portal as **Requestor1**.

You should see the **Marketing Campaign** access package.

1. In the **Business justification** box, type the justification *I'm working on the new marketing campaign*.



1. Select **Submit**.
2. In the left menu, select **Request history** to verify that your request was delivered. For more details, select **View**.



**Step 4: Validate that access has been assigned**

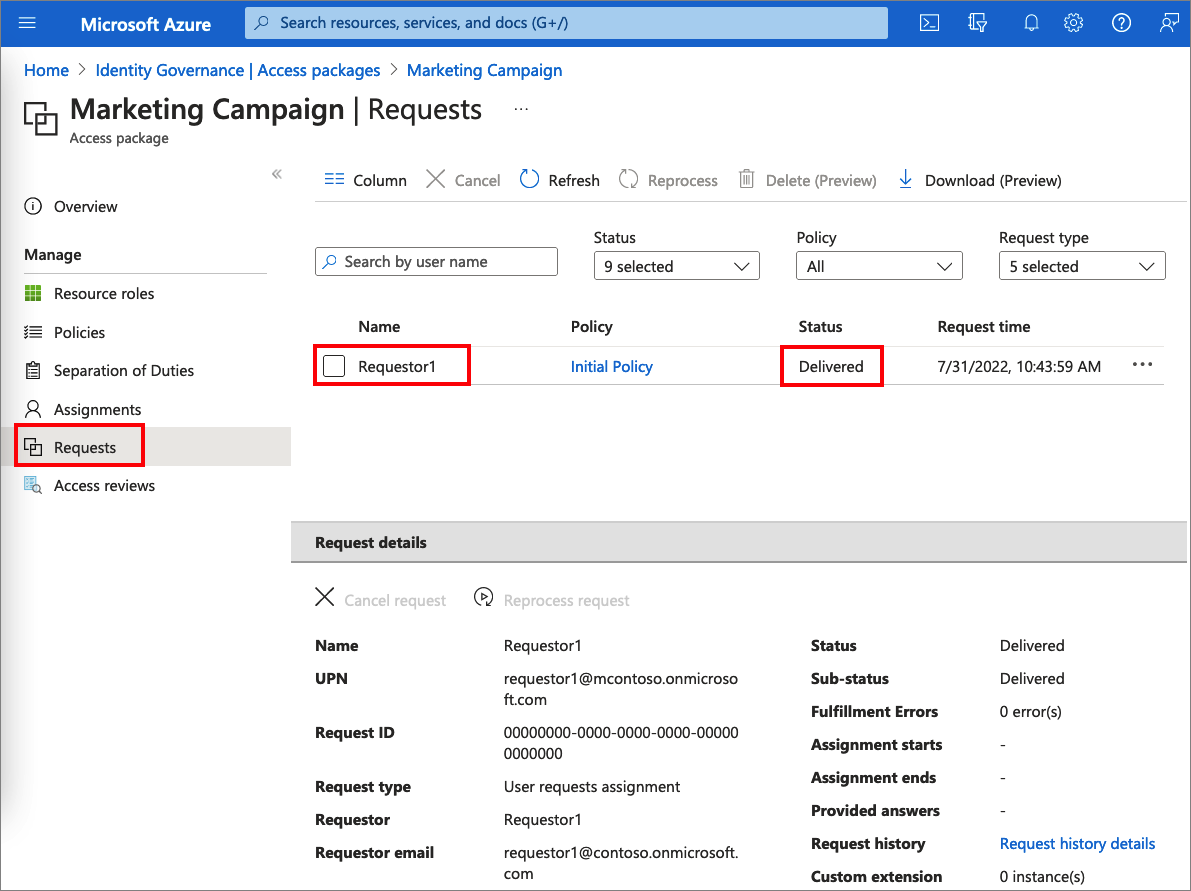
In this step, you confirm that the **internal requestor** was assigned the access package and that they're now a member of the **Marketing resources** group.

**Prerequisite role:** Global administrator, User administrator, Catalog owner, or Access package manager

1. Sign out of the My Access portal.
2. Sign in to the [Azure portal](https://portal.azure.com/) as **Admin1**.
3. Select **Azure Active Directory** and then select **Identity Governance**.
4. In the left menu, select **Access packages**.
5. Find and select **Marketing Campaign** access package.
6. In the left menu, select **Requests**.

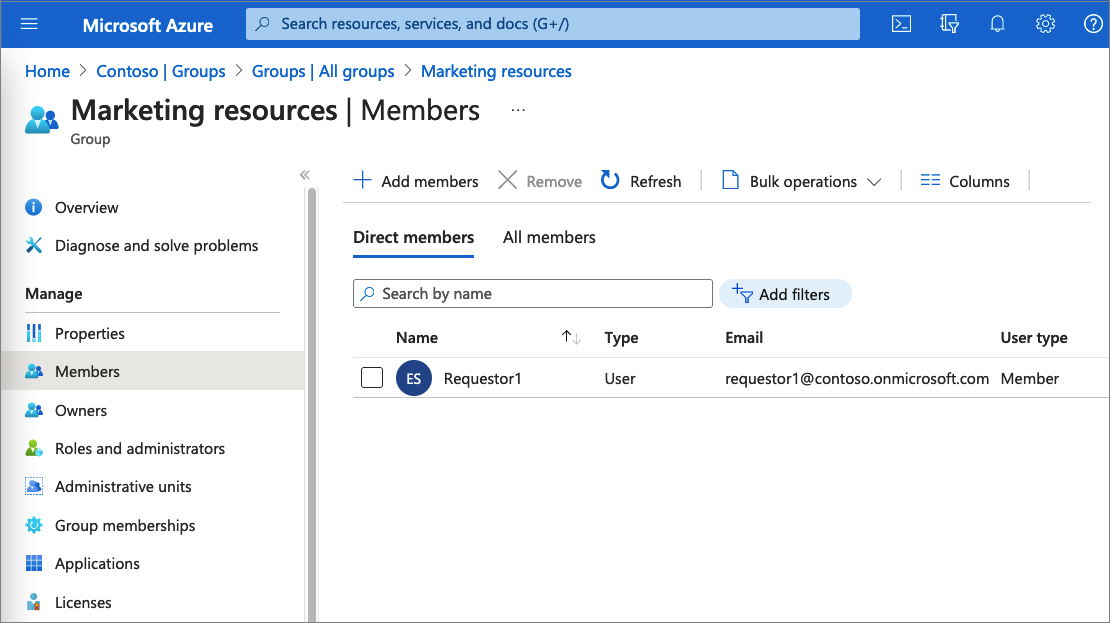
You should see Requestor1 and the Initial policy with a status of **Delivered**.

1. Select the request to see the request details.

[](https://docs.microsoft.com/en-us/azure/active-directory/governance/media/entitlement-management-access-package-first/request-details.png#lightbox)

1. In the left navigation, select **Azure Active Directory**.
2. Select **Groups** and open the **Marketing resources** group.
3. Select **Members**.

You should see **Requestor1** listed as a member.



**Step 5: Clean up resources**

In this step, you remove the changes you made and delete the **Marketing Campaign** access package.

**Prerequisite role:** Global administrator or User administrator

1. In the Azure portal, select **Azure Active Directory** and then select **Identity Governance**.
2. Open the **Marketing Campaign** access package.
3. Select **Assignments**.
4. For **Requestor1**, select the ellipsis (**...**) and then select **Remove access**. In the message that appears, select **Yes**.

After a few moments, the status will change from Delivered to Expired.

1. Select **Resource roles**.
2. For **Marketing resources**, select the ellipsis (**...**) and then select **Remove resource role**. In the message that appears, select **Yes**.
3. Open the list of access packages.
4. For **Marketing Campaign**, select the ellipsis (**...**) and then select **Delete**. In the message that appears, select **Yes**.
5. In Azure Active Directory, delete any users you created such as **Requestor1** and **Admin1**.
6. Delete the **Marketing resources** group.