Contents

1 SC-300: Identity and Access Administrator

- **Download Latest Student Handbook and AllFiles Content**
- **Are you a MCT?** - Have a look at our GitHub User Guide for MCTs
- **Need to manually build the lab instructions?** - Instructions are available in the MicrosoftLearning/Docker-Build repository

1.1 What are we doing?

- To support this course, we will need to make frequent updates to the course content to keep it current with the Azure services used in the course. We are publishing the lab instructions and lab files on GitHub to allow for open contributions between the course authors and MCTs to keep the content current with changes in the Azure platform.
- We hope that this brings a sense of collaboration to the labs like we've never had before - when Azure changes and you find it first during a live delivery, go ahead and make an enhancement right in the lab source. Help your fellow MCTs.

1.2 How should I use these files relative to the released MOC files?

- The instructor handbook and PowerPoints are still going to be your primary source for teaching the course content.
- These files on GitHub are designed to be used in conjunction with the student handbook, but are in GitHub as a central repository so MCTs and course authors can have a shared source for the latest lab files.
- It will be recommended that for every delivery, trainers check GitHub for any changes that may have been made to support the latest Azure services, and get the latest files for their delivery.

1.3 What about changes to the student handbook?

- We will review the student handbook on a quarterly basis and update through the normal MOC release channels as needed.

1.4 How do I contribute?

- Any MCT can submit a pull request to the code or content in the GitHub repro, Microsoft and the course author will triage and include content and lab code changes as needed.
- You can submit bugs, changes, improvement and ideas. Find a new Azure feature before we have? Submit a new demo!

1.5 Notes

1.5.1 Classroom Materials

1.6 It is strongly recommended that MCTs and Partners access these materials and in turn, provide them separately to students. Pointing students directly to GitHub to access Lab steps as part of an ongoing class will require them to access yet another UI as part of the course, contributing to a confusing experience for the student. An explanation to the student regarding why they are receiving separate Lab instructions can highlight the nature of an always-changing cloud-based interface and platform. Microsoft Learning support for accessing files on GitHub and support for navigation of the GitHub site is limited to MCTs teaching this course only.

1.7 title: Online Hosted Instructions permalink: index.html layout: home

2 Content Directory

Hyperlinks to each of the lab exercises and demos are listed below.

2.1 Labs

{% assign labs = site.pages | where_exp:"page", "page.url contains '/Instructions/Labs'" %} | Module | Lab | | --- | --- | {% for activity in labs %}| {{ activity.lab.module }} | [{{ activity.lab.title }}{% if activity.lab.type %} - {{ activity.lab.type }}{% endif %}](/home/ll/Azure_clone/Azure_new/SC-300-Identity-and-Access-Administrator/{{ site.github.url }}{{ activity.url }}) | {% endfor %}

2.2 Demos

2.3 {% assign demos = site.pages | where_exp:"page", "page.url contains '/Instructions/Demos'" %} | Module | Demo | | --- | --- | {% for activity in demos %}| {{ activity.demo.module }} | [{{ activity.demo.title }}](/home/ll/Azure_clone/Azure_new/SC-300-Identity-and-Access-Administrator/{{ site.github.url }}{{ activity.url }}) | {% endfor %} Use this folder to store supplemental files for the labs or demos provided. Use this folder to store any supplemental demo files needed to support demos in this course. Use this folder to store any supplemental lab files needed to support demos in this course. Store demos for the training in this folder.

2.4 lab: title: '01 - Manage user roles' learning path: '01' module: 'Module 01 - Implement an identity management solution'

3 Lab 01: Manage user roles

3.1 Lab scenario

Your company recently hired a new employee who will perform duties as an application administrator. You must create a new user and assign the appropriate role.

3.1.0.1 Estimated time: 10 minutes

3.2 Create an Azure account and add Azure Active Directory Premium P2 trial licenses

The tasks in this exercise and the exercises in this learning path require you to already have and Azure subscription that you can use or to sign up for an Azure trial account. If you already have your own Azure subscription, you may skip this task and continue to the next.

1. In a web browser, go to https://azure.microsoft.com/free.
2. Scroll down through the page to learn more about the benefits and free services available.
3. Select **Start free**.
4. Use the wizard to sign up for your Azure trial subscription.
5. You will need to an Azure AD P2 license to complete some of the exercises. In the organization you created, search for and then select **Azure Active Directory**.
6. In the left navigation menu, select **Getting started**.
7. Under Getting started with Azure AD, select **Get a free trial for Azure AD Premium**.
8. In the Activate pane, under **AZURE AD PREMIUM P2**, select **Free trial** and then select **Activate**.
9. In the navigation menu on the left, select **Overview**.
10. Refresh the browser until you see Azure AD Premium P2 under the organization name. It may take a couple of minutes.
11. You may need to sign out and sign back into Microsoft Azure if you encounter any problems with expected features not being available.

3.3 Add a new user

Now, let's create a user account.

1. Sign in to the https://portal.azure.com as a Global administrator
2. Search for and then select **Azure Active Directory**.
3. In the left navigation menu, under **Manage**, select **Users > New User**.
4. Create a user using the following information:

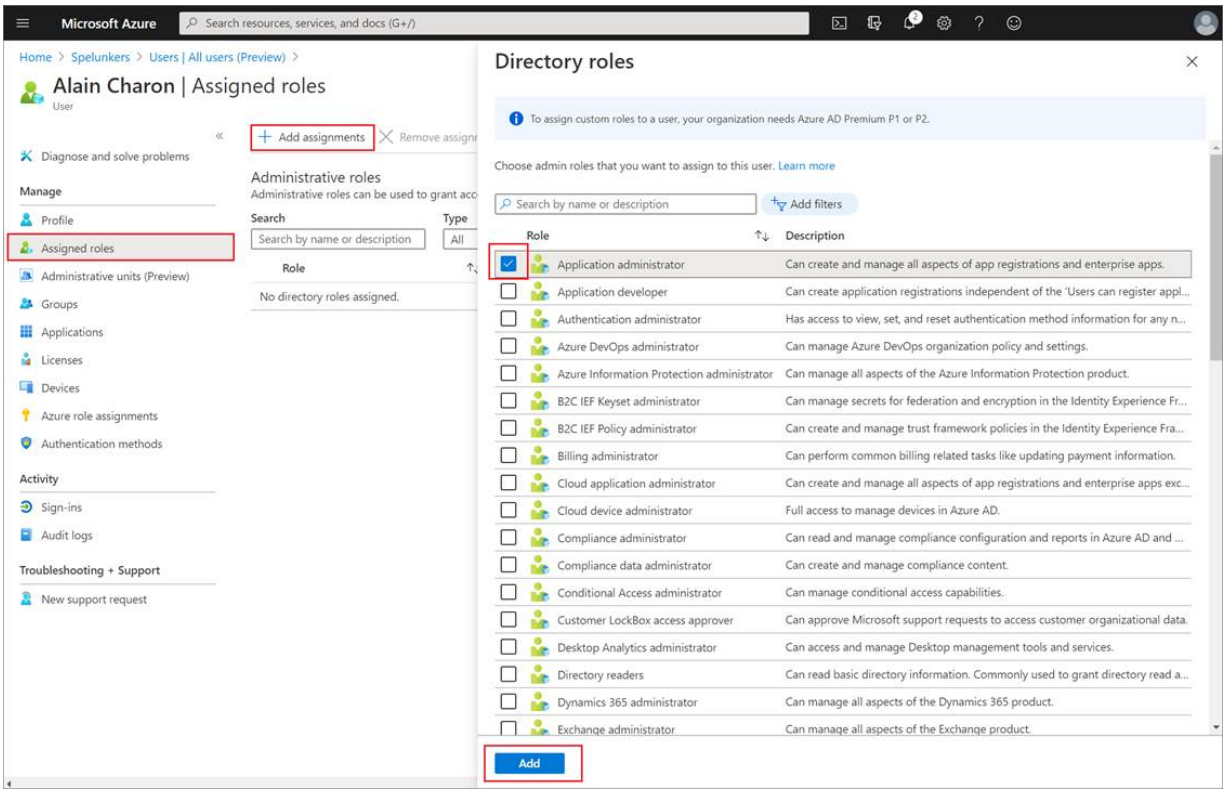
Setting	Value
User name	Chris
Name	Chris Green
First name	Chris
Last name	Green
Password	Pass@word1

5. Select **Create**. The user is now created and registered to your organization.

3.4 Assign a role to a user

Using Azure Active Directory (Azure AD), you can designate limited administrators to manage identity tasks in less-privileged roles. Administrators can be assigned for such purposes as adding or changing users, assigning administrative roles, resetting user passwords, managing user licenses, and managing domain names.

1. In Azure Active Directory, All users blade, select **Chris Green**.
2. On the **user's profile** page, select **Assigned roles**. The **Assigned roles** page appears.
3. Select **Add assignments**, select the **Application administrator** role and then select **Add**.

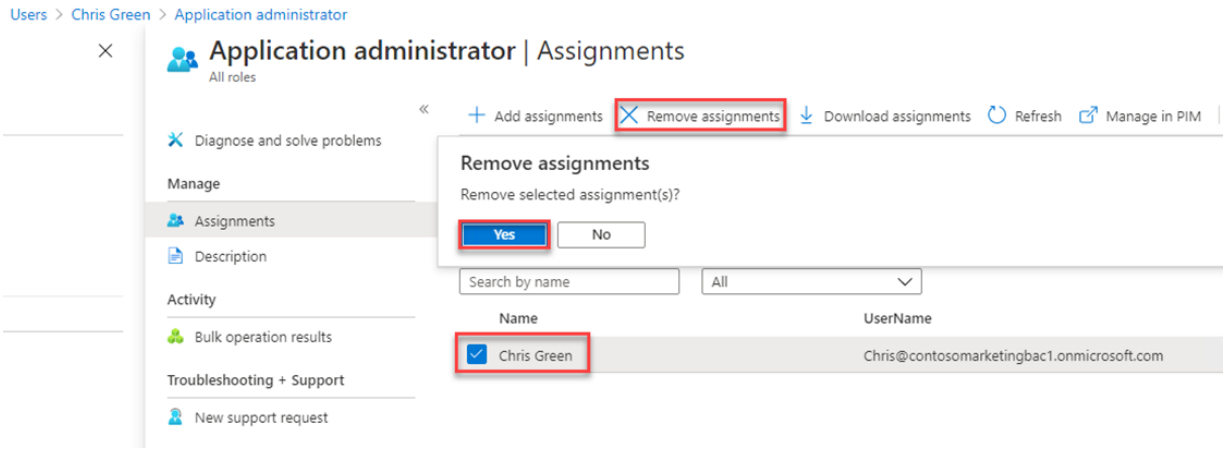


The newly assigned Application administrator role appears on the user's **Assigned roles** page.

3.5 Remove a role assignment

If you need to remove the role assignment from a user, you can also do that from the **Assigned roles** page.

1. In **Azure Active Directory**, select **Users**, and then select the user getting the role assignment removed. For example, *Chris Green*.
2. Select **Assigned roles**, select the name of the role your wish to removed.
3. Select the check box for the user who will be removed from the role, and then select **Remove assignments**.



The Application administrator role is removed from the user and it no longer appears on the **Alain Charon – Assigned roles** page.

3.6 lab: title: '02 - Working with tenant properties' learning path: '01' module: 'Module 01 - Implement an identity management solution'

4 Lab 02: Working with tenant properties

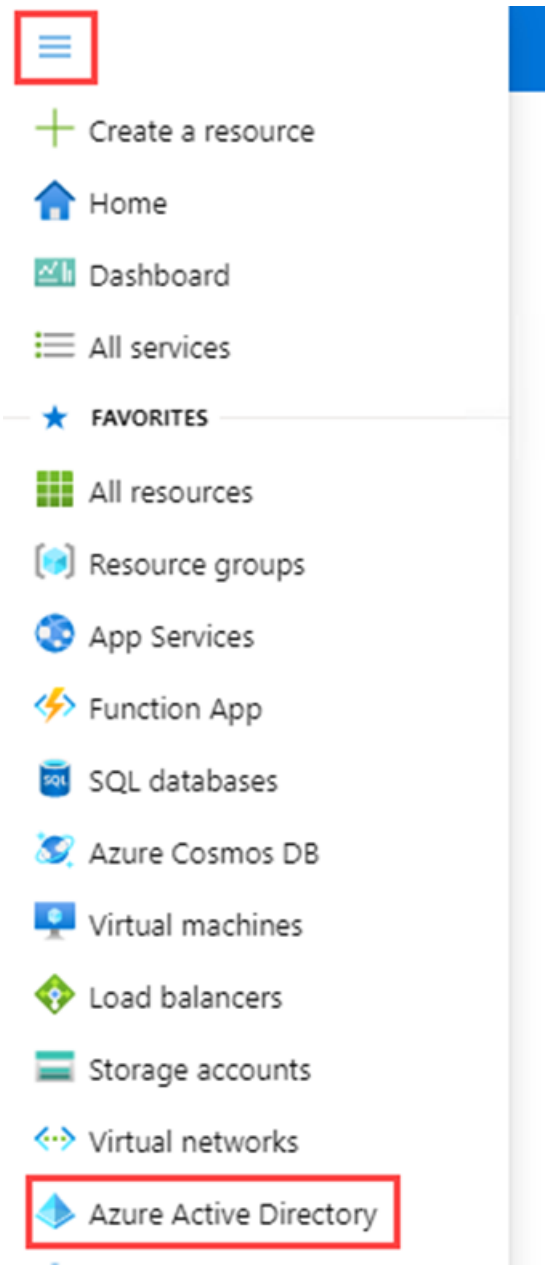
4.1 Lab scenario

You need to identify and update the different properties associated with your tenant.

4.1.0.1 Estimated time: 10 minutes

4.2 Changing the tenant display name

1. Browse to the https://portal.azure.com and sign in using a Global administrator account for the directory.
2. Select the **Show portal menu** hamburger icon and then select **Azure Active Directory**.



3. In the left navigation, in the Manage section, select **Properties**.
4. In the **Name** box, change the tenant name. For example, Contoso Marketing Company can be changed to Contoso Marketing Company 2.
5. Select **Save** to update the tenant properties.

4.3 Finding the Country or region associated with your tenant

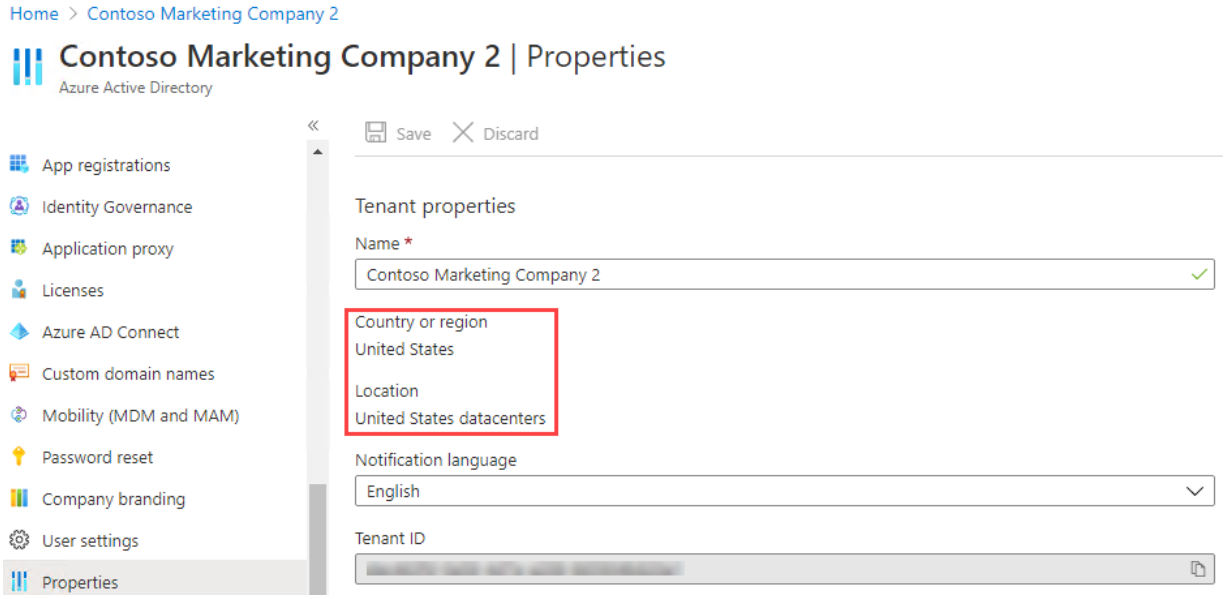
1. In the **Azure Active Directory** blade, in the Manage section, select **Properties**.
2. Under **Tenant properties**, locate **Country or region** and review the information.

   [!IMPORTANT] When the tenant is created, the Country or region are specified at that time. This setting cannot be changed later.

4.4 Finding the location associated with your tenant

Just as the Country or region are found in the Azure Active Directory Properties blade, so is the location information.

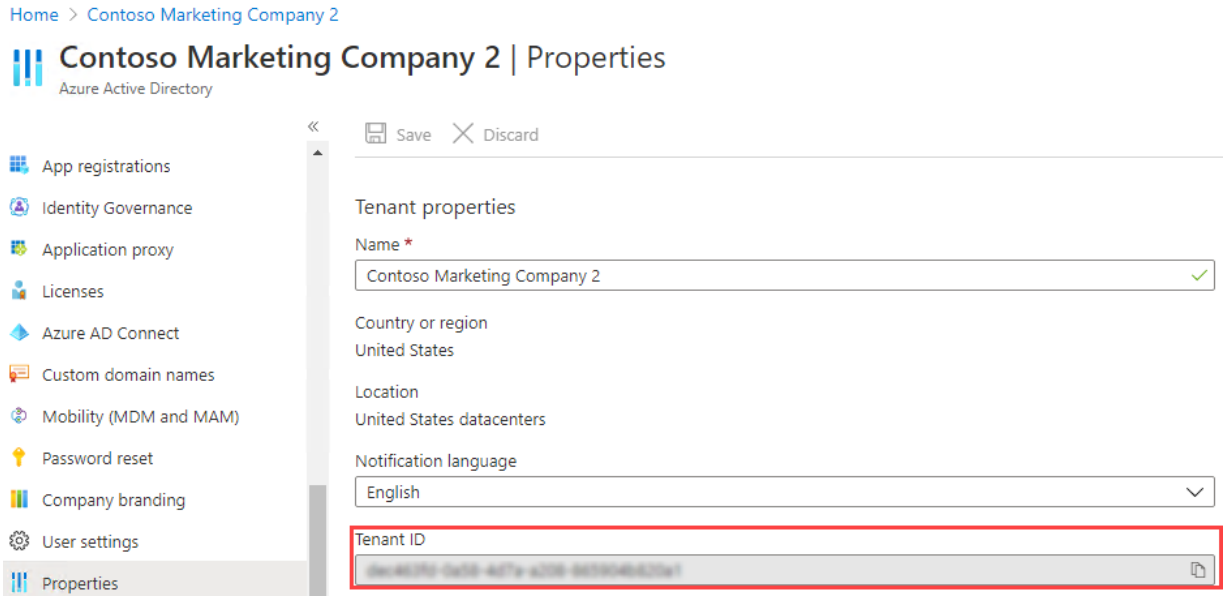
1. In the **Properties** blade, under **Tenant properties**, locate **Location** and review the information.



4.5 Finding the tenant ID

Azure subscriptions have a trust relationship with Azure Active Directory (Azure AD). Azure AD is trusted to authenticate users, services, and devices for the subscription. Each subscription has a tenant ID associated with it, and there are a few ways you can find the tenant ID for your subscription.

1. In the **Azure Active Directory** blade, in the Manage section, select **Properties**.
2. Under **Tenant properties**, locate **Tenant ID**. This is your unique tenant identifier.



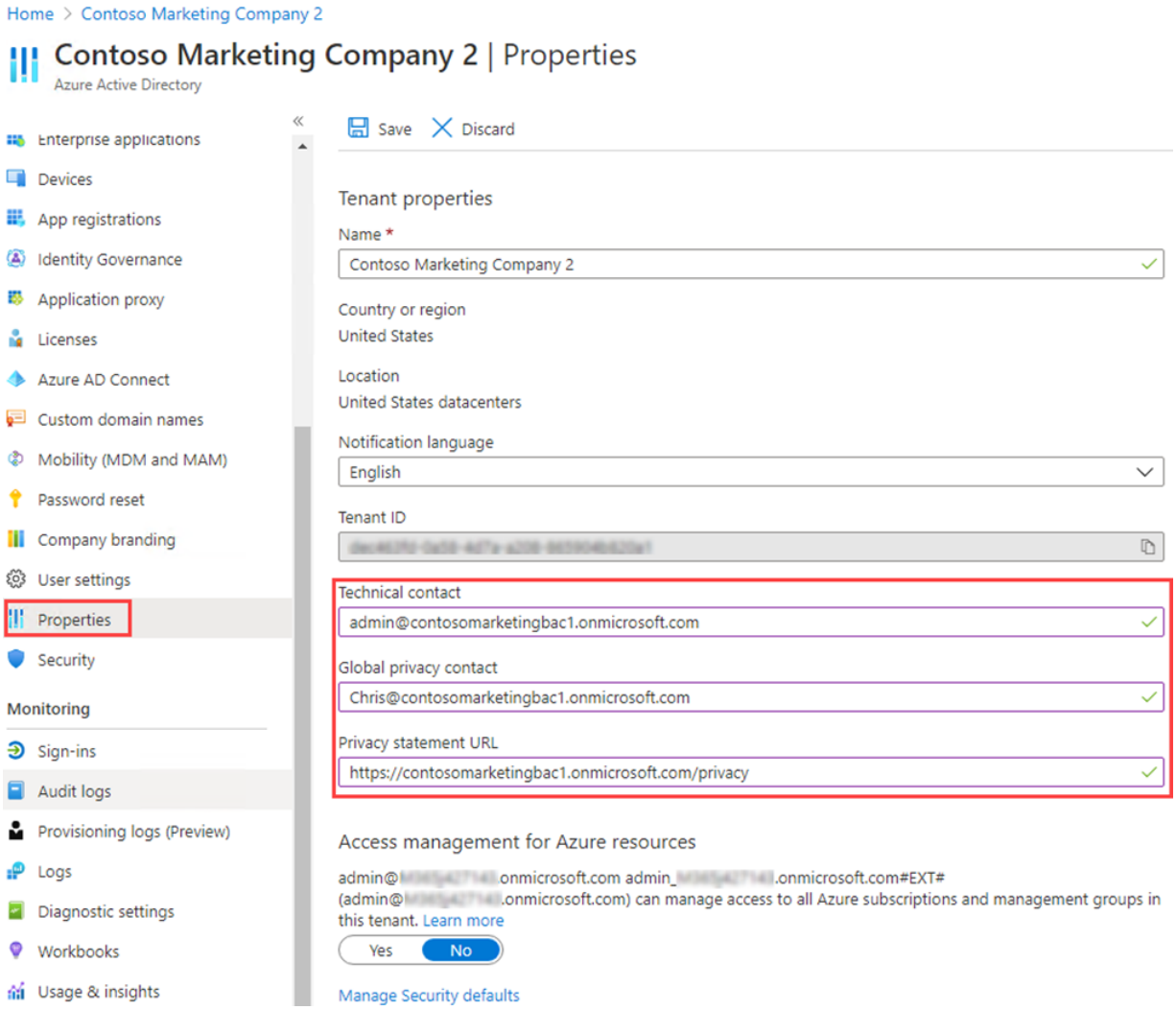
4.6 Changing the Technical contact and adding your privacy info on Azure AD, including Global privacy contact and Privacy statement URL

Microsoft strongly recommends you add both your global privacy contact and your organization's privacy statement, so your internal employees and external guests can review your policies. Because privacy statements are uniquely created and tailored for each business, we strongly recommend you contact a lawyer for assistance.

```
> [!NOTE]
> For information about viewing or deleting personal data, see [https://docs.microsoft.com/microsoft-36
```

You add your organization's privacy information in the **Properties** area of Azure AD. To access the Properties area and add your privacy information:

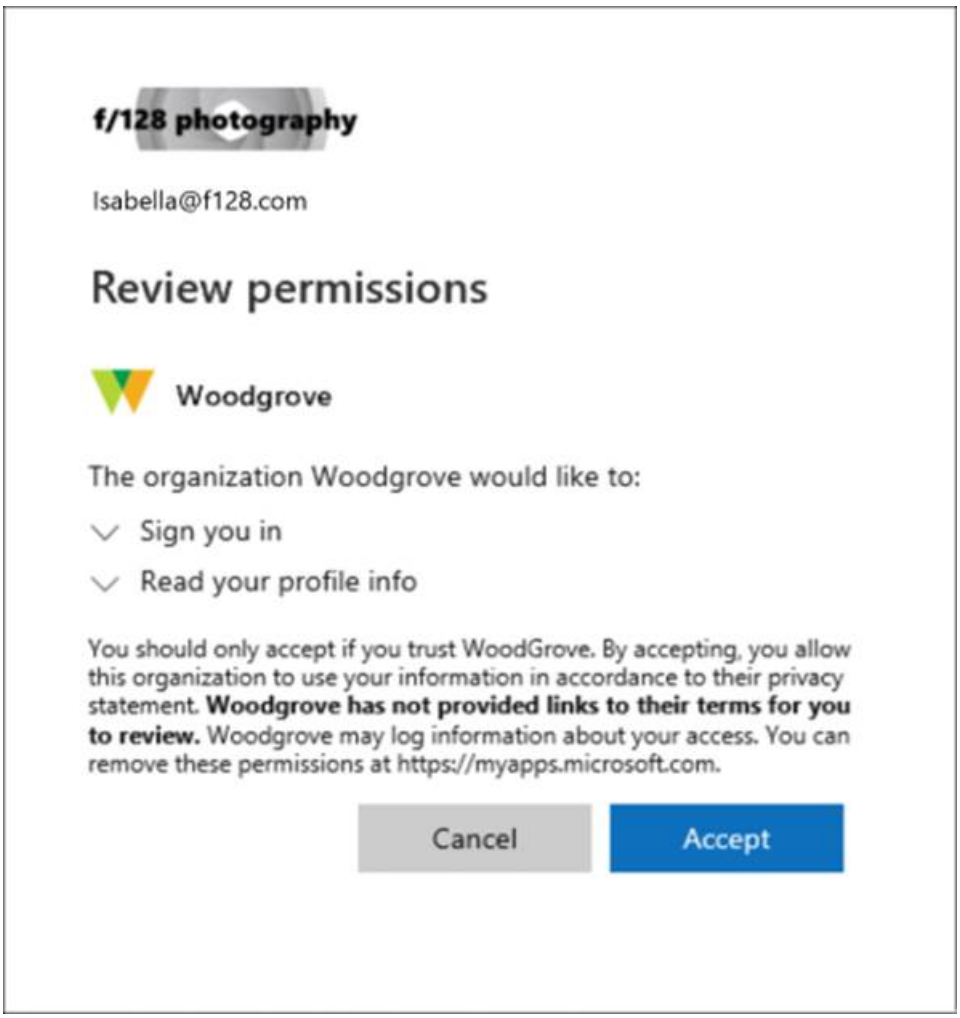
1. In the **Azure Active Directory** blade, in the Manage section, select **Properties**.



2. Add your privacy info for your employees:

- **Technical contact**. Type the email address for the person to contact for technical support within your organization.
- **Global privacy contact**. Type the email address for the person to contact for inquiries about personal data privacy. This person is also who Microsoft contacts if there's a data breach. If there's no person listed here, Microsoft contacts your global administrators.
- **Privacy statement URL**. Type the link to your organization's document that describes how your organization handles both internal and external guest's data privacy.

  [!IMPORTANT] If you don't include either your own privacy statement or your privacy contact, your external guests will see text in the Review Permissions box that says, <your org name> has not provided links to their terms for you to review. For example, a guest user will see this message when they receive an invitation to access an organization through B2B collaboration.



1. Select **Save**.

4.7 lab: title: '03 - Assigning licenses using group membership' learning path: '01' module: 'Module 02 - Create, configure, and manage identities'

5 Lab 03: Assigning licenses using group membership

5.1 Lab scenario

Your organization has decided to use security groups in Azure AD to manage licenses. You need to configure a new security and assign a license to that group and verify group member license's have been updated.

5.1.0.1 Estimated time: 10 minutes

5.2 Create a new user in Azure Active Directory

1. Browse to https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview and sign in as a Global Administrator.
2. In the left navigation, under **Mange**, select **Users**.
3. In the Users blade, on the menu, select **New user**.
4. Create a user using the following information:

Setting	Value
User name	Chris
Name	Chris Green

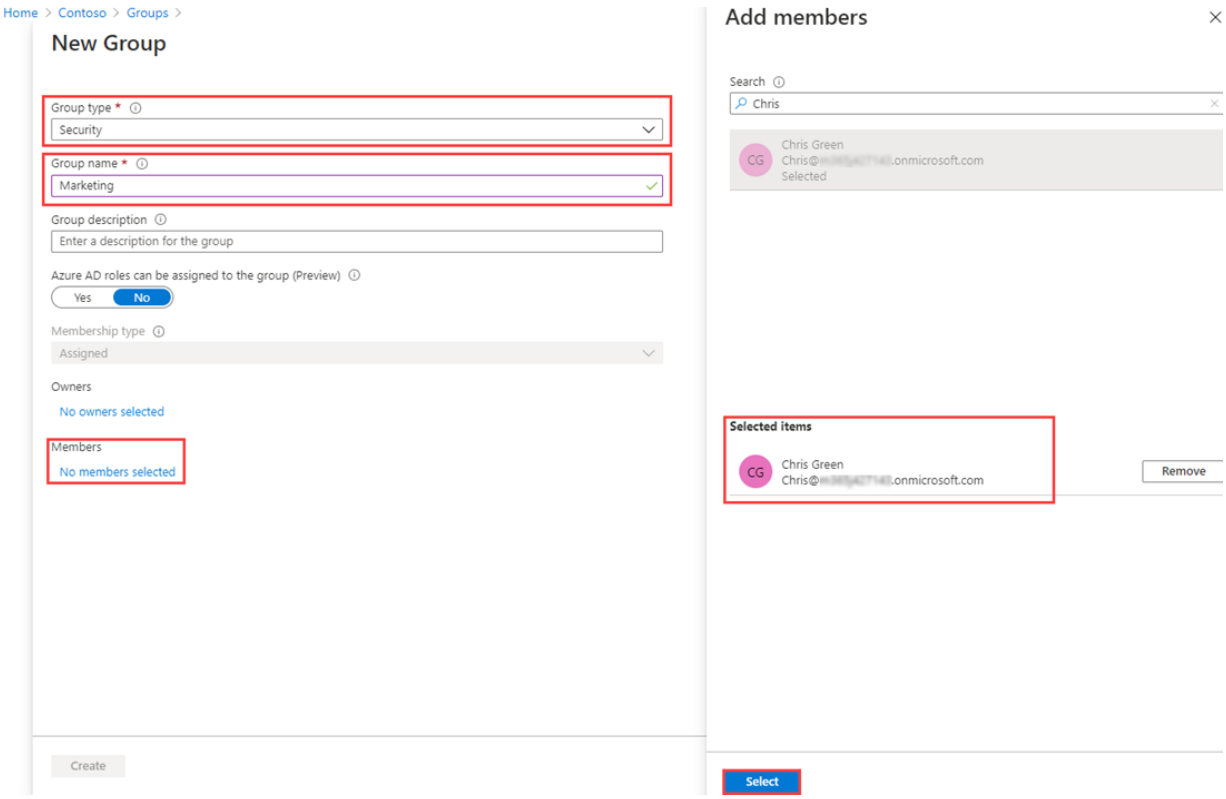
Setting	Value
First name	Chris
Last name	Green
Password	Pass@word1

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

5.3 Create a security group in Azure Active Directory

1. Browse to https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview.
2. In the left navigation, under **Mange**, select **Groups**.
3. In the Groups blade, 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



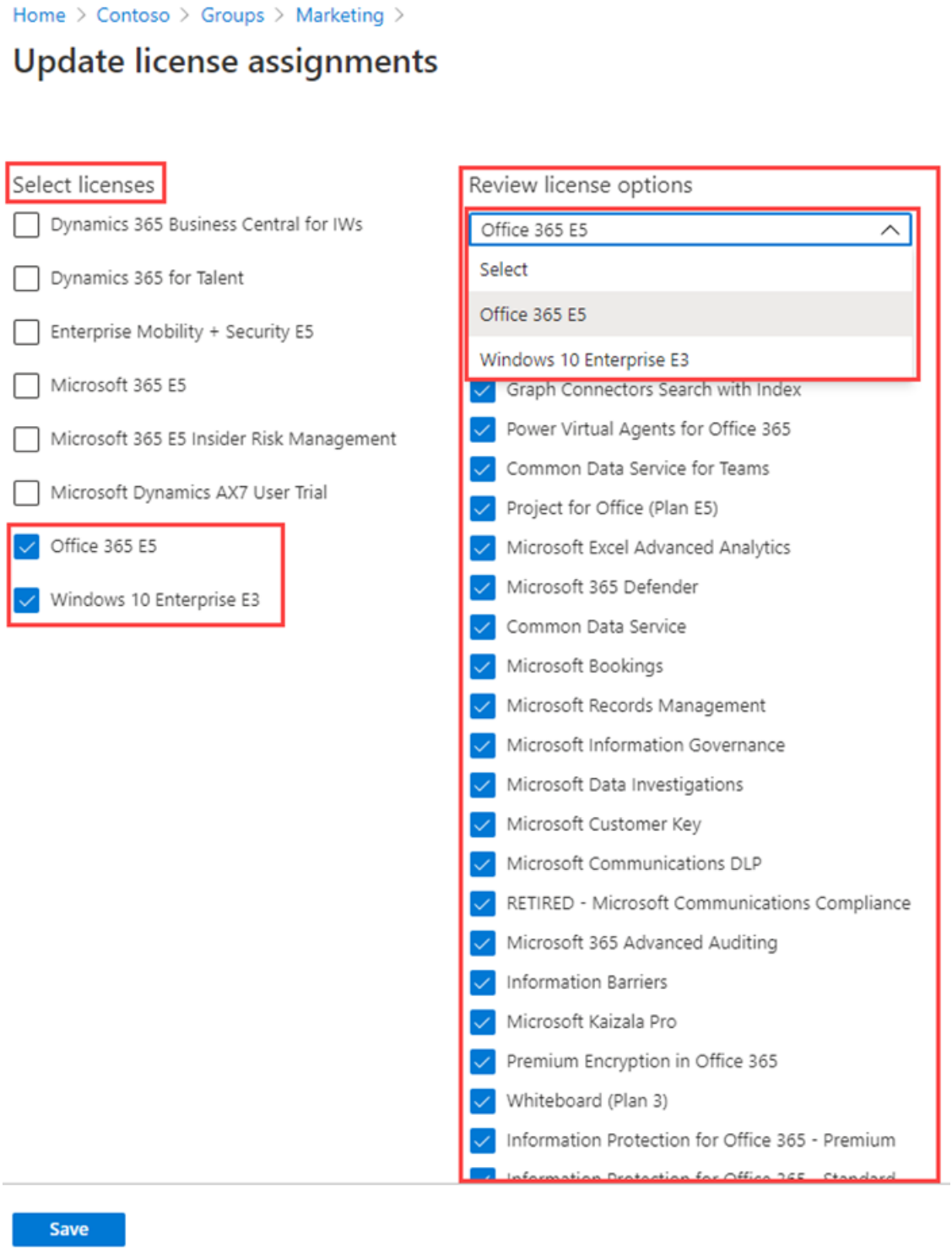
5. When complete, verify the group named **Marketing** is shown in the **All groups** list.

5.4 Assign a license to a group

1. In the **All groups** list, select **Marketing**.
2. In the Marketing blade, under **Mange**, select **Licenses**.
3. On the menu, select **Assignments**.
4. In the update license assignments blade, under **Select licenses**, review the list of available licenses and then select the check box for one of the licenses.

5. Under **Review license options**, review the available options for the license you have selected.

   [!Tip] When multiple licenses are selected, you can use the Review license options menu to select a specific license and view the license option for that license.



6. Select **Save**.

5.5 lab: title: '04 - Restore a deleted user' learning path: '01' module: 'Module 02 - Create, configure, and manage identities'

6 Lab 04: Restore a deleted user

6.1 Lab scenario

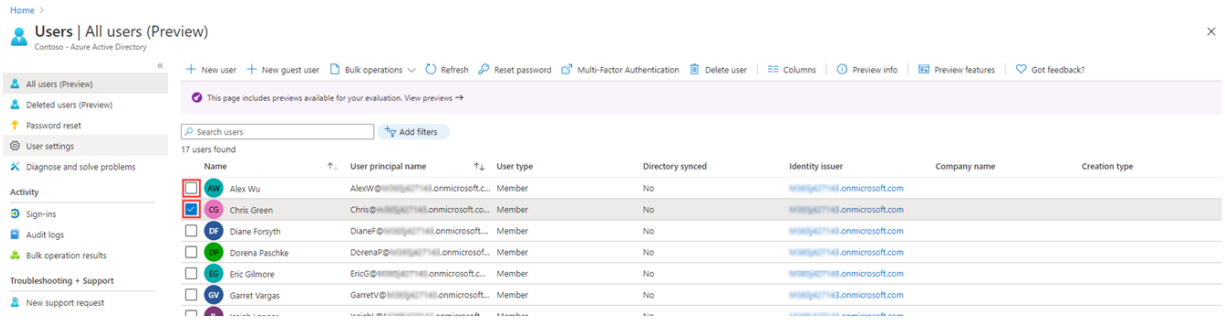
It may happen that an account is deleted and then needs to be recovered. You need to verify you can recover an account that has been deleted recently.

6.1.0.1 Estimated time: 5 minutes

6.2 Remove a user from Azure Active Directory

1. Browse to https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview.
2. In the left navigation, under **Manage**, select **Users**.
3. In the **Users** list, select the check box for a user that will be deleted. 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 blade, you will only be managing that individual user.



4. With the user account selected, on the menu, select **Delete user**.
5. Review the dialog box and then select **OK**.

6.3 Restore a deleted user

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

   [!Important] By default, deleted user accounts are permanently removed from Azure Active Directory 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 has been restored.

6.4 lab: title: '05 - Adding groups to Azure AD' learning path: '01' module: 'Module 02 - Create, configure, and manage identities'

7 Lab 05: Adding groups to Azure AD

7.1 Lab scenario

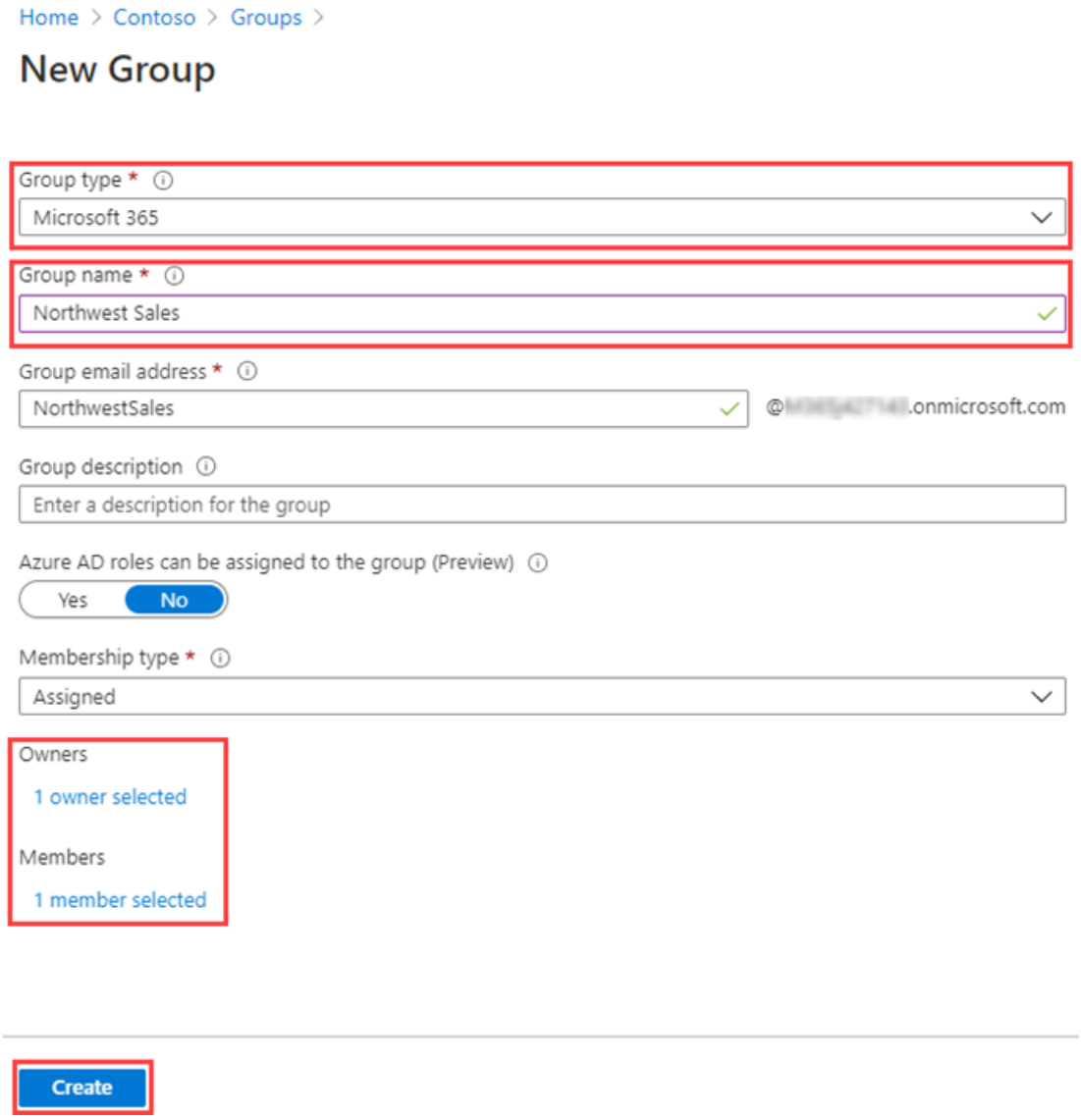
Part of your duties as an Azure AD administrator is to create different types of groups. You need to create a new Microsoft 365 group for your organization's sales department.

7.1.0.1 Estimated time: 5 minutes

7.2 Create an Microsoft 365 group in Azure Active Directory

1. Browse to https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview.
2. In the left navigation, under **Manage**, select **Groups**.
3. In the Groups blade, 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*



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

7.3 lab: title: '06 - Change group license assignments' learning path: '01' module: 'Module 02 - Create, configure, and manage identities'

8 Lab 06: Change group license assignments

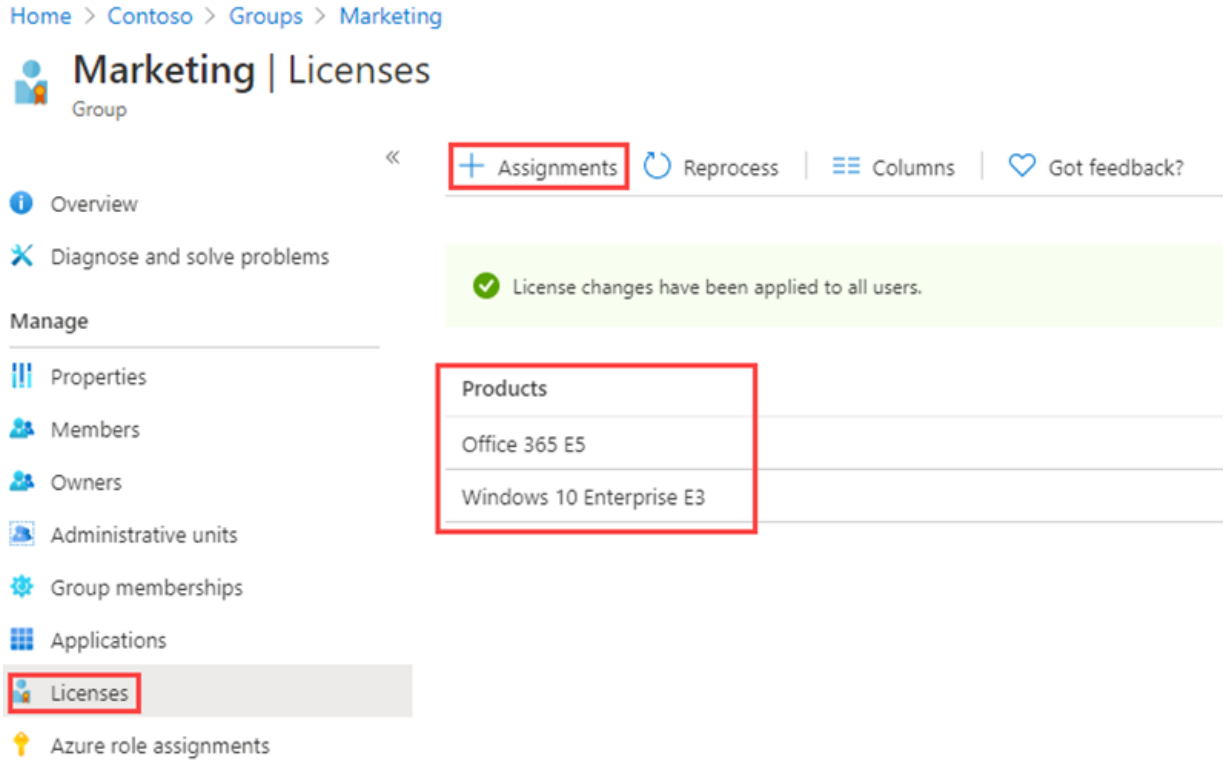
8.1 Lab scenario

Occasionally, you may need to change the license assignment that are used by an Azure AD security group. You must ensure you are familiar with the procedure for changing a group's license assignment.

8.1.0.1 Estimated time: 5 minutes

8.2 Change group license assignments

1. Browse to https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview.
2. In the left navigation, under **Manage**, select **Groups**.
3. Select one of the available groups. For example, Marketing.
4. In the left navigation, under **Manage**, select **Licenses**.
5. Review the current assignments and then, on the menu, select + **Assignments**.



6. On the Update license assignments blade, select another license, clear the selection of an existing license, add or remove license options, or any combination.
7. When complete, select **Save**.
8. On the group's Licenses page, review the change.

8.3 lab: title: '07 - Change user account license assignments' learning path: '01' module: 'Module 02 - Create, configure, and manage identities'

9 Lab 07: Change user account license assignments

9.1 Lab scenario

Some user accounts in your organization will not be provided all available products in their assigned license or will need updates or additions to their license assignment. You need to ensure you are able to update a user account's license assignment in Azure AD.

9.1.0.1 Estimated time: 5 minutes

9.2 Create a new user in Azure Active Directory

1. Browse to https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview.
2. In the left navigation, under **Mange**, select **Users**.
3. In the Users blade, on the menu, select **New user**.
4. Create a user using the following information:

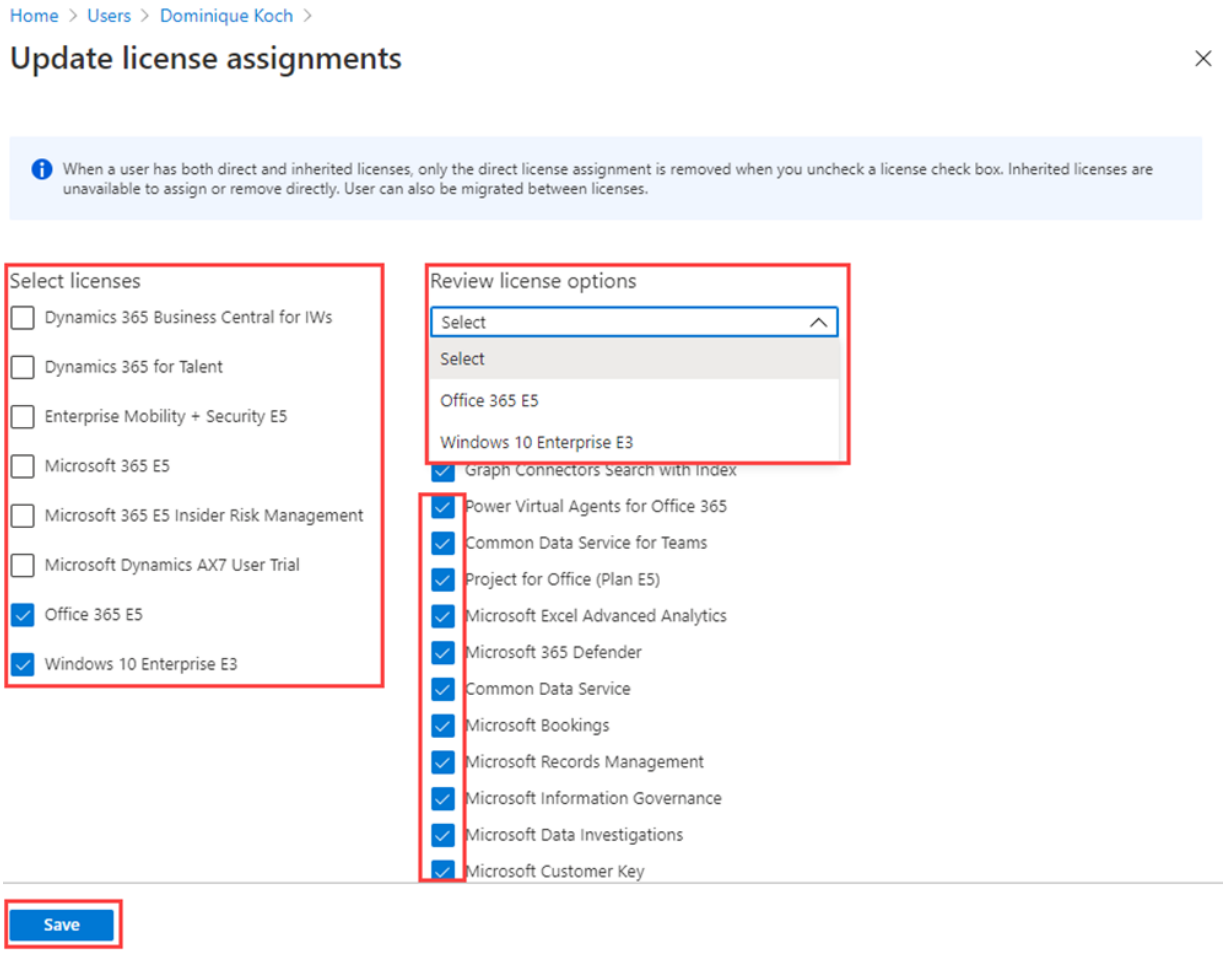
Setting	Value
User name	Dominique
Name	Dominique Koch
First name	Dominique
Last name	Koch
Password	Pass@word1
Usage location	*Select your preferred usage location*

Warning To assign a license to a user, the user must assigned a usage location.

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

9.3 Update user license assignments

1. Browse to https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview.
2. In the left navigation, under **Manage**, select **Users**
3. In the Users blade, select **Dominique Koch**.
4. In the left navigation, select **Licenses**.
5. On the Update license assignments blade, select the check box for a single or multiple licenses.



6. When complete, select **Save**.

9.4 lab: title: '08 - Configure external collaboration settings' learning path: '01' module: 'Module 03 - Implement and manage external identities'

10 Lab 08: Configure external collaboration settings

10.1 Lab scenario

You must enable external collaboration settings for your organization for approved guests access.

10.1.0.1 Estimated timing: 5 minutes

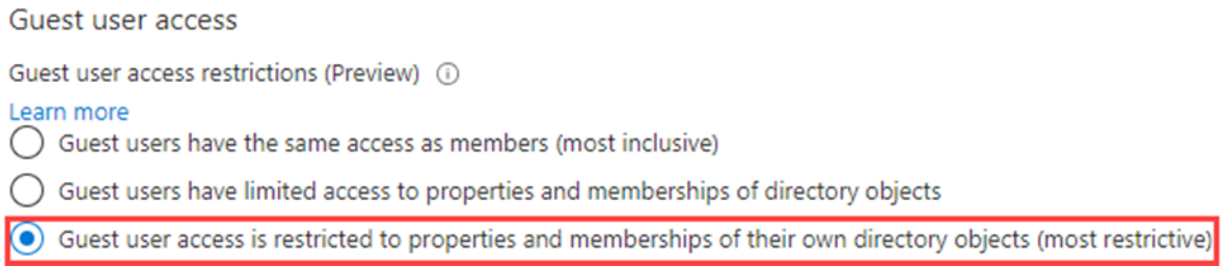
10.1.1 Configure external collaboration settings

1. Sign in to the https://portal.azure.com as a tenant administrator.
2. Select **Azure Active Directory**.
3. Select **External Identities > External collaboration settings**.
4. Under **Guest user access**, review access levels that are available and then select **Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)**.

   [!NOTE]

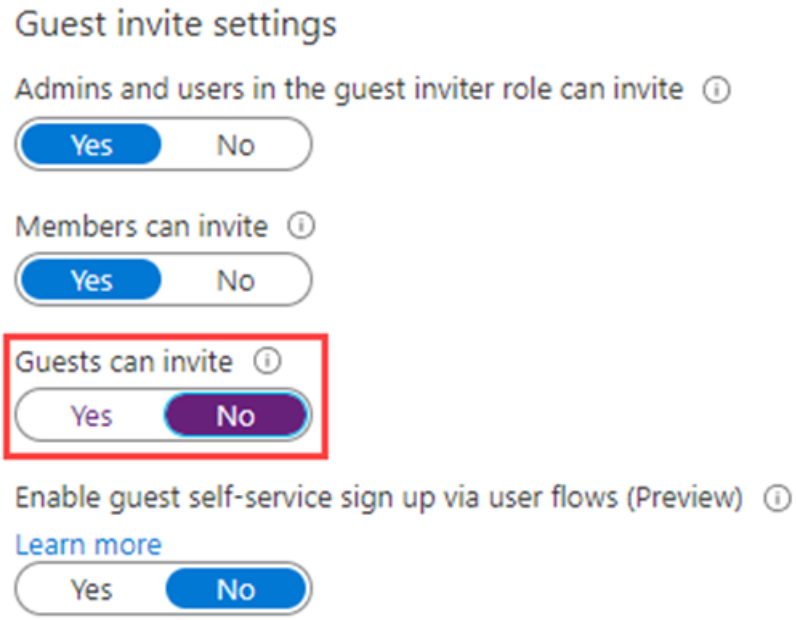
   - Guest users have the same access as members (most inclusive): This option gives guests the same access to Azure AD resources and directory data as member users.
   - Guest users have limited access to properties and memberships of directory objects: (Default) This setting blocks guests from certain directory tasks, like enumerating users, groups, or other directory resources. Guests can see membership of all non-hidden groups.

- Guest user access is restricted to properties and memberships of their own directory objects (most restrictive): With this setting, guests can access only their own profiles. Guests are not allowed to see other users' profiles, groups, or group memberships.



5. Under **Guest invite settings**, under **Guests can invite**, select **No**.

   [!NOTE] Admins and users in the guest inviter role can invite: To allow admins and users in the "Guest Inviter" role to invite guests, set this policy to Yes. Members can invite: To allow non-admin members of your directory to invite guests, set this policy to Yes. Guests can invite: To allow guests to invite other guests, set this policy to Yes. Enable guest self-service sign up via user flows (Preview): Enables or disables self-service sign up for guests via user flows associated with applications in your directory. When disabled, guests are required to be invited to your directory. If Members can invite is set to No and Admins and users in the guest inviter role can invite is set to Yes, users in the Guest Inviter role will still be able to invite guests.



6. Under **Email one-time passcode for guests**, use the default setting.

   [!NOTE]

   - Automatically enable email one-time passcode for guests in March 2021. (Default) If the email one-time passcode feature is not already enabled for your tenant, it will be automatically turned on in March 2021. No further action is necessary if you want the feature enabled at that time. If you've already enabled or disabled the feature, this option will be unavailable.
   - Enable email one-time passcode for guests effective now. Turns on the email one-time passcode feature for your tenant.
   - Disable email one-time passcode for guests. Turns off the email one-time passcode feature for your tenant and prevents the feature from turning on in March 2021.

7. Under **Collaboration restrictions**, review the available options and accept the default settings.

   [!IMPORTANT] You can create either an allow list or a deny list. You can't set up both types of lists. By default, whatever domains are not in the allow list are on the deny list, and vice versa. You can create only one policy per organization. You can update the policy to include more

domains, or you can delete the policy to create a new one. The number of domains you can add to an allow list or deny list is limited only by the size of the policy. The maximum size of the entire policy is 25 KB (25,000 characters), which includes the allow list or deny list and any other parameters configured for other features. This list works independently from OneDrive for Business and SharePoint Online allow/block lists. If you want to restrict individual file sharing in SharePoint Online, you need to set up an allow or deny list for OneDrive for Business and SharePoint Online. The list does not apply to external users who have already redeemed the invitation. The list will be enforced after the list is set up. If a user invitation is in a pending state, and you set a policy that blocks their domain, the user's attempt to redeem the invitation will fail.

8. When finished, save your changes.

10.2 lab: title: '09 - Add guest users to the directory' learning path: '01' module: 'Module 03 - Implement and manage external identities'

11 Lab 09: Add guest users to the directory

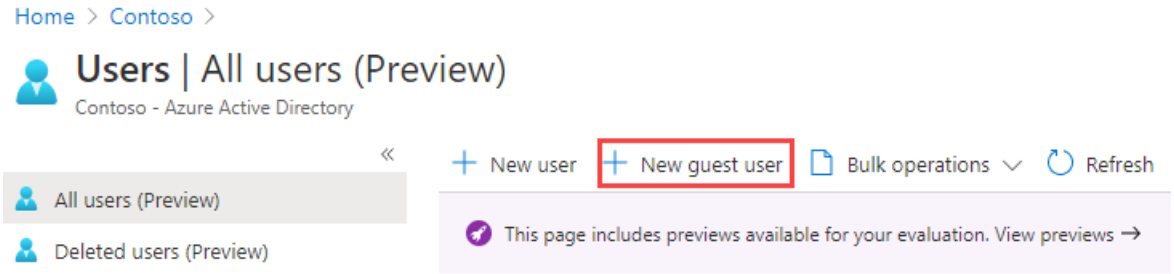
11.1 Lab scenario

Your company works with many vendors and, on occasion, you need to add some vendor accounts to your directory as a guest.

11.1.0.1 Estimated time: 5 minutes

11.2 Add guest users to the directory

1. Sign in to the https://portal.azure.com as a user who is assigned a limited administrator directory role or the Guest Inviter role.
2. Select **Azure Active Directory**.
3. Under **Manage**, select **Users**.
4. Select **New guest user**.



5. On the New user page, select **Invite user** and then add your information as the guest user.

   [!NOTE] Group email addresses are not supported; enter the email address for an individual. Also, some email providers allow users to add a plus symbol (+) and additional text to their email addresses to help with things like inbox filtering. However, Azure AD does not currently support plus symbols in email addresses. To avoid delivery issues, omit the plus symbol and any characters following it up to the @ symbol.

6. When complete, select **Invite**.
7. On the Users blade, verify your account is listed and, in the **User type** column, verify **Guest** is shown.

11.3 After you send the invitation, the user account is automatically added to the directory as a guest.

11.4 lab: title: 10 - Invite guest users in bulk' learning path: '01' module: 'Module 03 - Implement and manage external identities'

12 Lab 10: Invite guest users in bulk

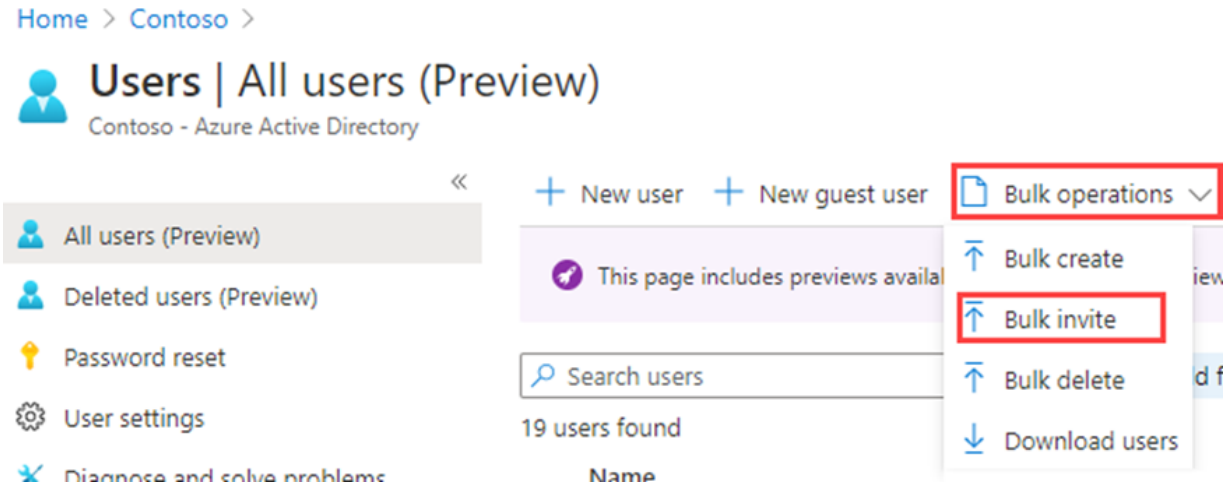
12.1 Lab scenario

A recent partnership has been established with another company. For now, employees of the partner company will be added as guests. You need to ensure you can import multiple guest users at one time.

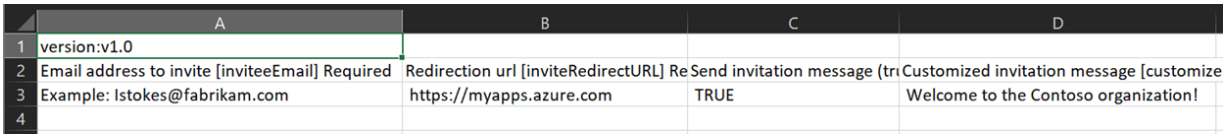
12.1.0.1 Estimated time: 10 minutes

12.2 Invite guest users in bulk

1. Sign in to the https://portal.azure.com with an account that is a User administrator in the organization.
2. In the navigation pane, select **Azure Active Directory**.
3. Under **Manage**, select **Users**.
4. On the Users blade, on the menu, select **Bulk operations > Bulk invite**.



5. In the Bulk invite users pane, select **Download** to a sample CSV template with invitation properties.
6. Using an editor to view the CSV file, review the template.
7. Open the .csv template and add a line for each guest user. Required values are:
   - **Email address to invite** - the user who will receive an invitation
   - **Redirection url** - the URL to which the invited user is forwarded after accepting the invitation.

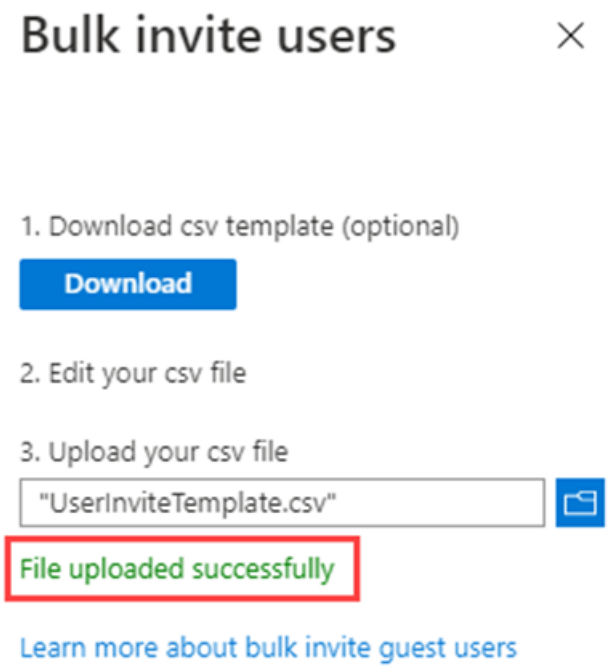


	A	B	C	D
1	version:v1.0			
2	Email address to invite [inviteeEmail] Required	Redirection url [inviteRedirectURL] Re	Send invitation message (tr	Customized invitation message [customize
3	Example: lstokes@fabrikam.com	https://myapps.azure.com	TRUE	Welcome to the Contoso organization!
4				

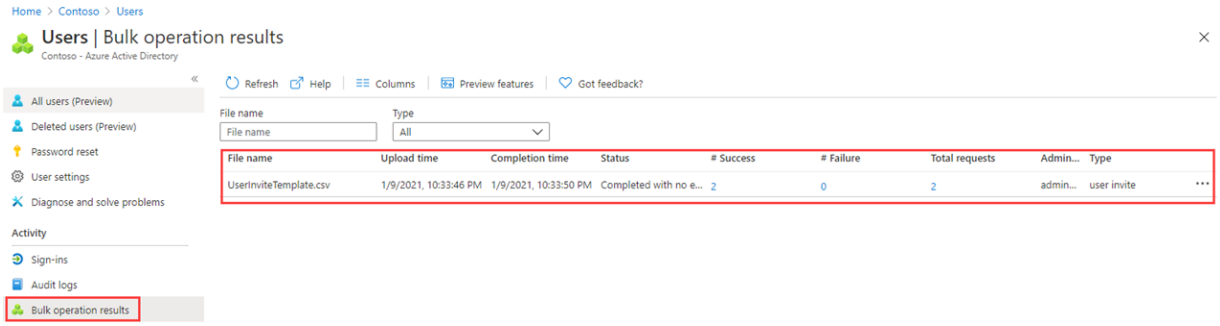
8. Save the file.
9. On the Bulk invite users page, under **Upload your csv file**, browse to the file.

When you select the file, validation of the .csv file starts.

1. After the file contents are validated, you will see **File uploaded successfully**. If there are errors, you must fix them before you can submit the job.



2. When your file passes validation, select **Submit** to start the Azure bulk operation that adds the invitations.
3. To view the job status, select **Click here to view the status of each operation**. Or, you can select **Bulk operation results** in the Activity section. For details about each line item within the bulk operation, select the values under the **# Success**, **# Failure**, or **Total Requests** columns. If failures occurred, the reasons for failure will be listed.



4. When the job completes, you will see a notification that the bulk operation succeeded.

12.3 lab: title: '11 - Working with dynamic groups' learning path: '01' module: 'Module 03 - Implement and manage external identities'

13 Lab 11: Working with dynamic groups

13.1 Lab scenario

As your company grows, manually group management is too time consuming. Since standardizing the directory, you can now take advantage of dynamic groups. You must create a new dynamic group to ensure you're ready for dynamic group creation in production.

13.1.0.1 Estimated time: 10 minutes

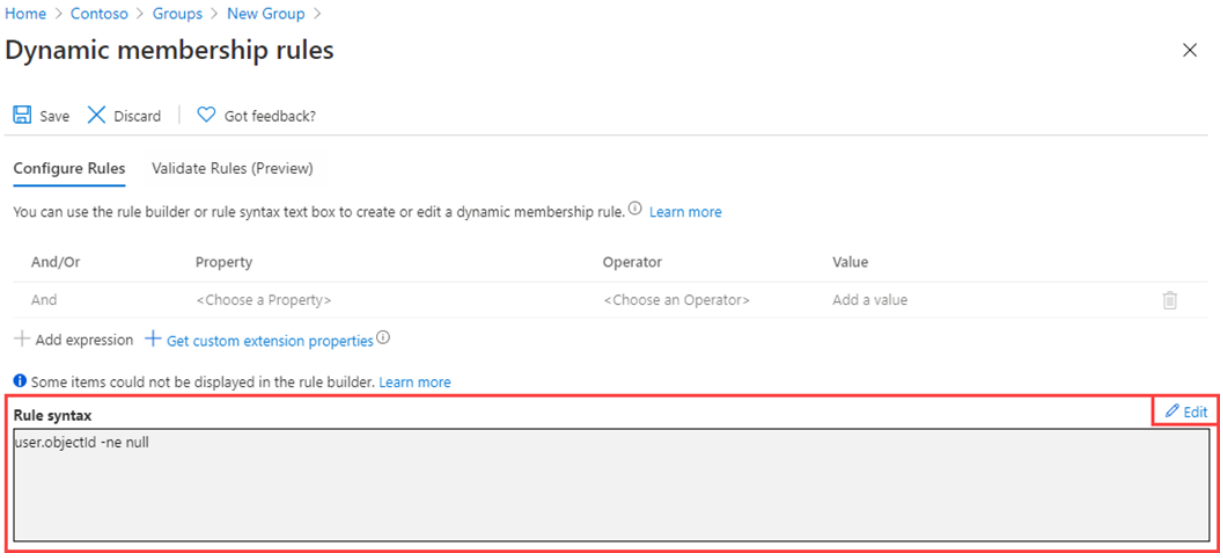
13.2 Creating a dynamic group with all users as members

1. Sign in to the https://portal.azure.com with an account that is assigned the Global administrator or User administrator role in the tenant.
2. Select **Azure Active Directory**.

3. Under **Manage**, select **Groups**, and then select **New group**.
4. On the New Group page, under **Group type**, select **Security**.
5. In the **Group name** box, enter **All company users dynamic group**.
6. Select the **Membership type** menu and then select **Dynamic User**.
7. Under **Dynamic user members**, select **Add dynamic query**.
8. On the right above the **Rule syntax** box, select **Edit**.
9. In the Edit rule syntax pane, enter the following expression in the **Rule syntax** box:

   ```
   user.objectId -ne null
   ```

10. Select **OK**. The rule appears in the Rule syntax box.



11. Select **Save**. The new dynamic group will now include B2B guest users as well as member users.
12. On the New group page, select **Create** to create the group.

13.3 lab: title: '12 - Enable Azure AD multi-factor authentication' learning path: '02' module: 'Module 01 - Plan and implement Azure multifactor authentication'

14 Lab 12 - Enable Azure AD multi-factor authentication

14.1 Lab scenario

To improve security in your organization, you've been directed to enable multi-factor authentication for Azure Active Directory.

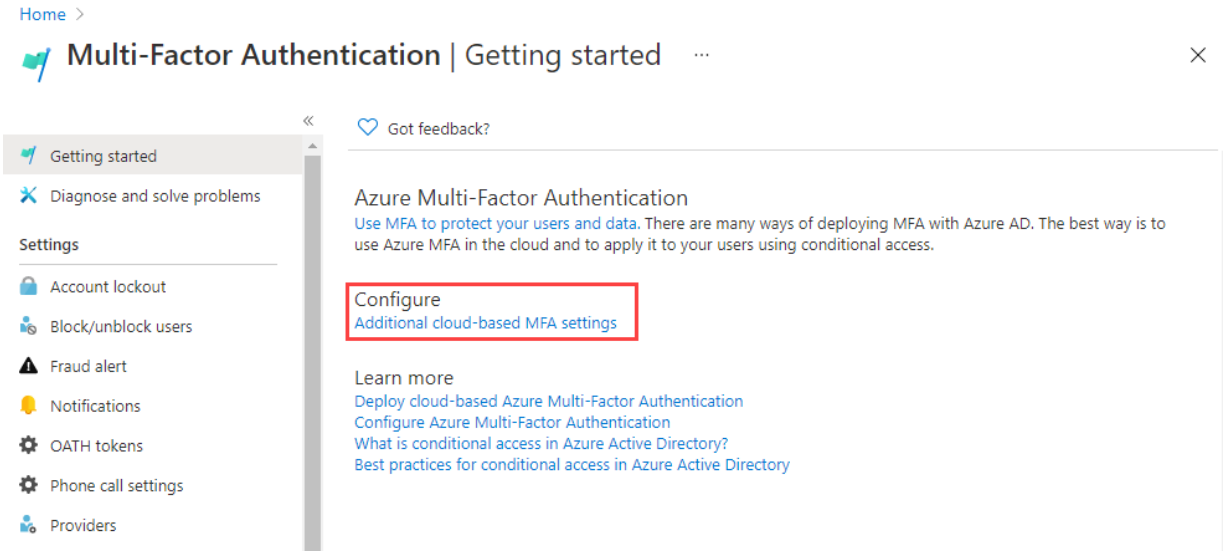
14.1.0.1 Estimated time: 10 minutes

[!IMPORTANT] Azure AD Premium is need for this exercise. You can use a 30-day free trial to try this feature out, or just read through the instructions below to understand the flow.

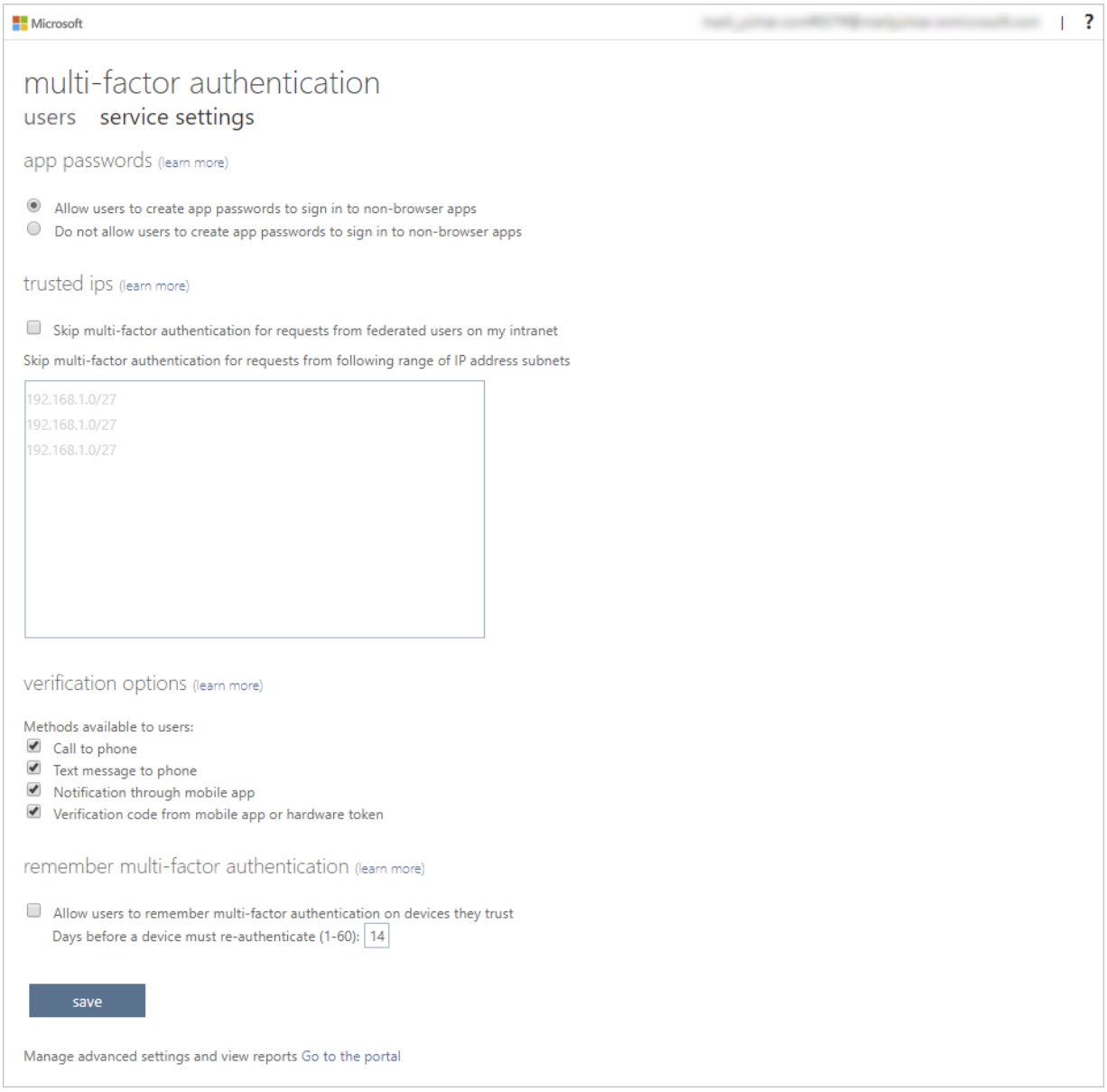
14.2 Configure Multi-Factor Authentication options

1. Browse to the https://portal.azure.com and sign in using a Global administrator account for the directory.
2. Use the search feature and search for **multi-factor**.
3. In the search results, select **Multi-Factor Authentication**.

4. On the Getting started page, under **Configure**, select **Additional cloud-based MFA settings**.



5. In the new browser page, you can see the MFA options for Azure users and service settings.



This is where you would select the supported authentication methods, in the screen above, all of them are

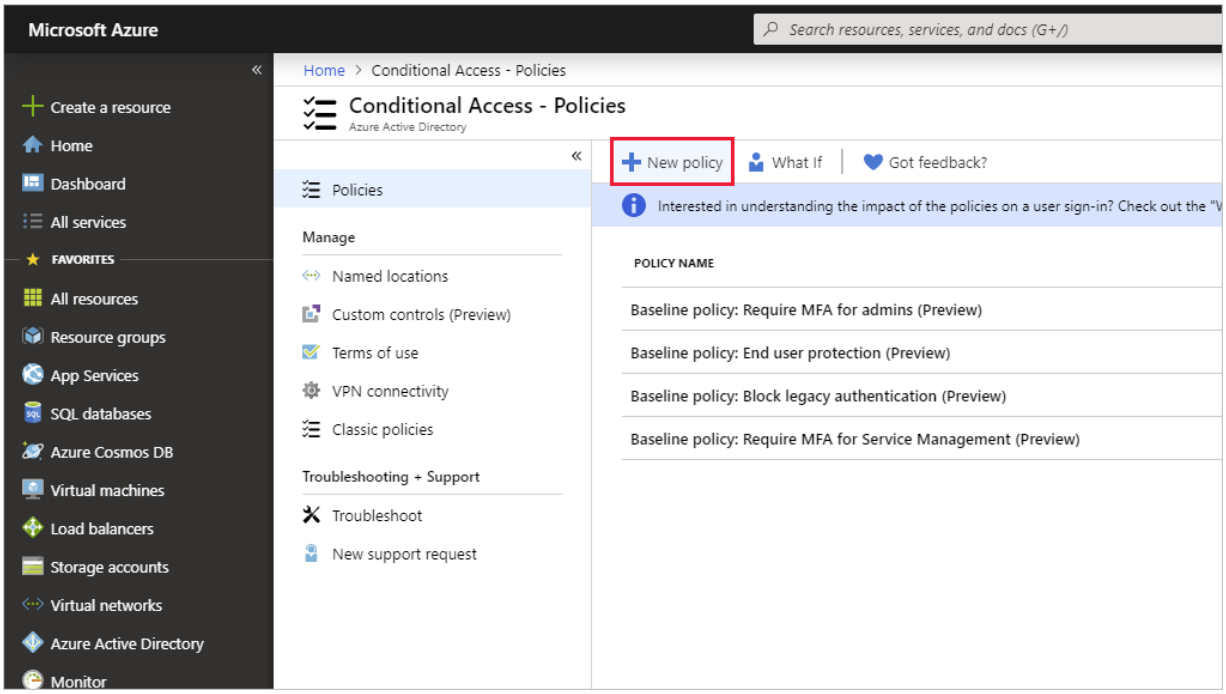
selected.

You can also enable or disable app passwords here, which allow users to create unique account passwords for apps that don't support multi-factor authentication. This feature lets the user authenticate with their Azure AD identity using a different password specific to that app.

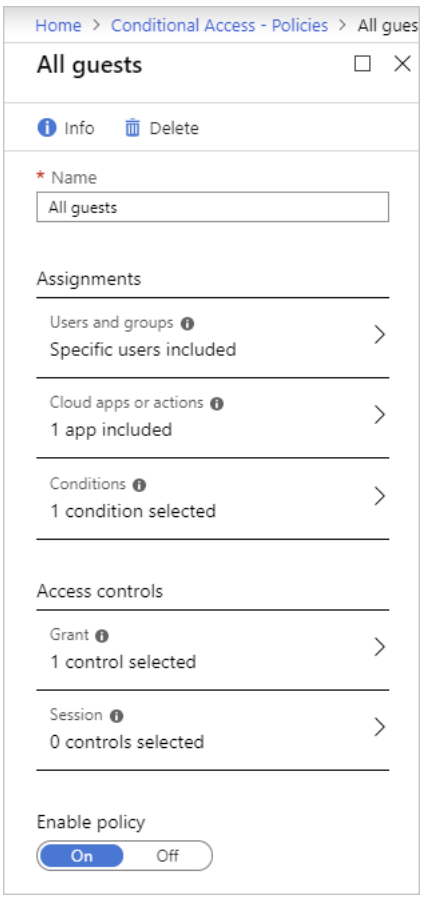
14.3 Setup conditional access rules for MFA

Next let's examine how to set up Conditional Access policy rules that would enforce MFA for guest users accessing specific apps on your network.

1. Switch back to the Azure portal and select **Azure Active Directory** > **Security** > **Conditional access**.
2. On the menu, select **New policy**.



3. Name your policy, for example **All guests**.
4. Select **Users and group**.
   - Select **Select users and groups**
   - Select the **All guest and external users** check box to apply this to all guests.
   - Select **Done**.
5. Select **Cloud apps or actions**.
   - Select **Select apps**.
   - Choose an app you want to enable Azure AD MFA such as Visual Studio App Center.
   - Select **Select** and then select **Done**.
6. Review the Conditions section.
   - Select **Locations** and then configure it for **Any location**.
7. Under **Access Controls** select **Grant** and verify **Grant access** is selected.
8. Select the **Require multi-factor authentication** check box to enforces MFA.
9. Select **Select**.
10. Set **Enable policy** to **On**.
11. Select **Create to create the policy**.

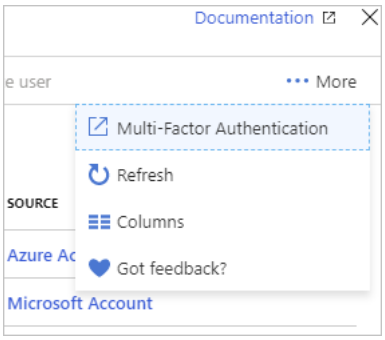


MFA is now enabled for your selected application(s). The next time a guest tries to sign into that app they will be prompted to register for MFA.

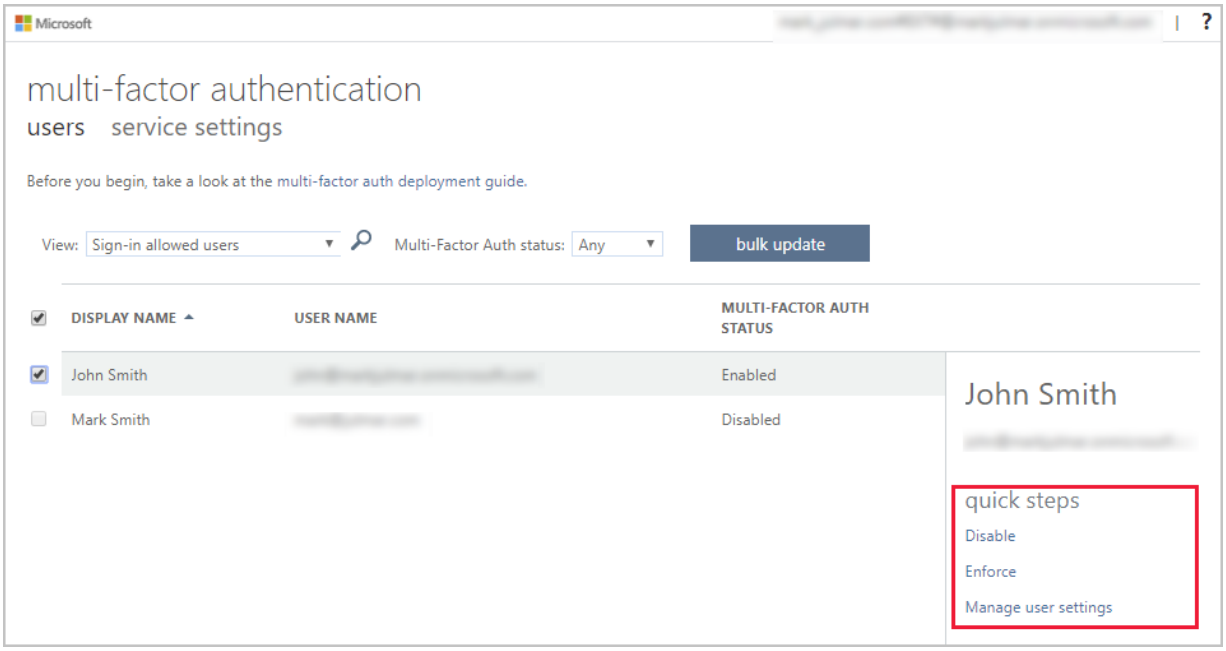
14.4 Configure Azure AD MFA for passwords

Finally, let's look at how to configure MFA for user accounts. This is another way to get to the multi-factor auth settings.

1. Switch back to the Azure Active Directory dashboard in the Azure portal.
2. Select **Users**.
3. At the top of the Users pane, select **Multi-Factor Authentication**.



You can enable or disable MFA on a user basis by selecting a user and then using the quick steps on the right side.



4. Select **service settings**.
   This displays the same global MFA options we saw earlier. Let's explore these in a bit more detail.

14.5 lab: title: '13 - Enable Azure AD multi-factor authentication' learning path: '02' module: 'Module 02 - Manage user authentication'

15 Lab 13 - Configure and deploy self-service password reset

15.1 Lab scenario

The company has decided to empower the employees and enable self-service password reset. You must configure this setting in your organization.

15.1.0.1 Estimated time: 15 minutes

15.2 Add a new user

1. Sign in to https://portal.azure.com using a Global administrator account.
2. Open the portal menu and then select **Azure Active Directory**.
3. In the Azure AD organization you created, under **Manage**, select **Users** > **New User**.
4. The User pane now appears. Enter the following values:

- **User name**: Utu
- **Name**: Utu Linna

1. Select **Show Password** and then copy it somewhere to reference it later.
2. Select **Create**.

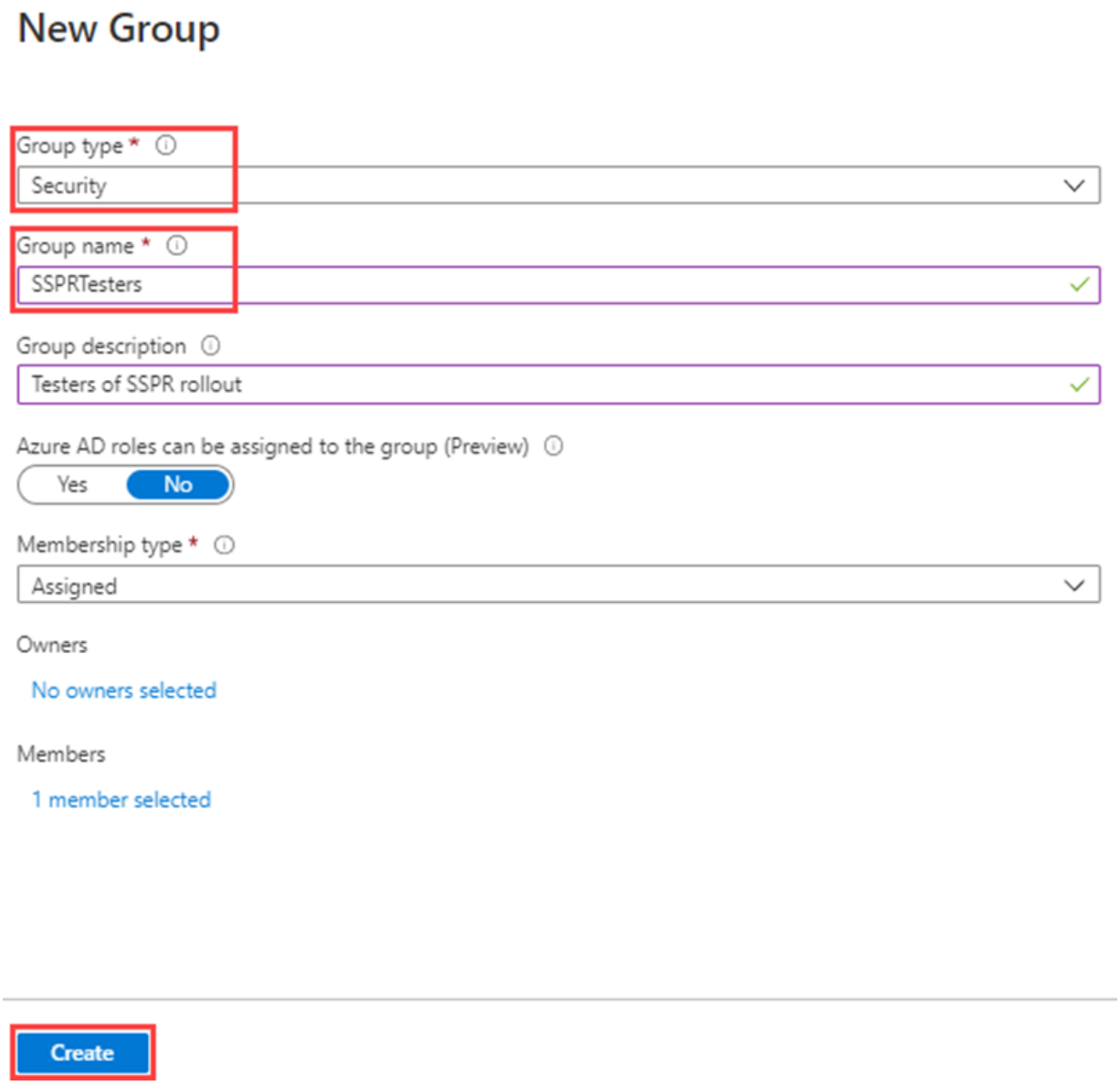
15.3 Create a group

You want to roll out SSPR to a limited set of users first to make sure your SSPR configuration works as expected. Let's create a security group for the limited rollout and add a user to the group.

1. On the Azure Active Directory blade, under **Manage**, select **+ New Group**.
2. Create a new group using the following information:

Setting	Value
Group type	Security
Group name	SSPRTesters
Group description	Testers of SSPR rollout
Membership type	Assigned
Members	Utu Linna

3. Select **Create**.



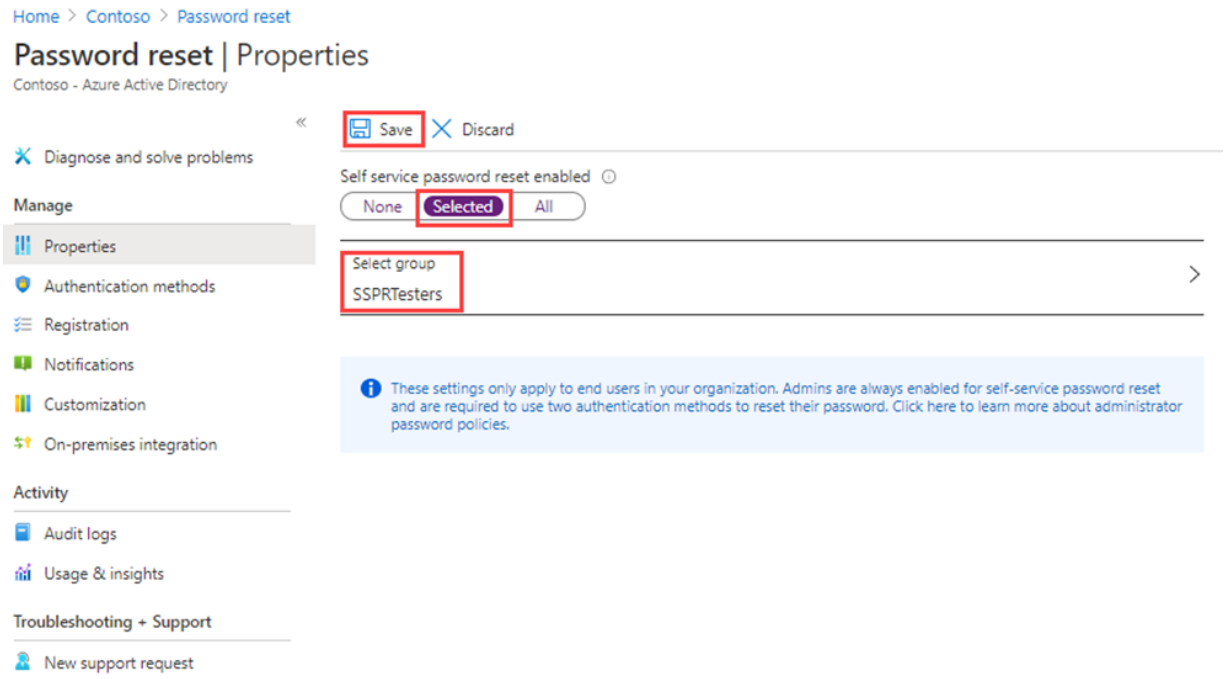
15.4 Enable SSPR

Enable SSPR for the group.

1. Browse back to the Azure Active Directory blade.
2. Under **Manage**, select **Password reset**.

   Note If the Password reset page still displays the message Get a free Premium trial to use this feature, wait for a few minutes and then refresh the page. On the Password reset blade Properties page, under **Self service password reset enabled**, select **Selected**.
3. Select **Select group**.
4. In the Default password reset policy pane, select the **SSPRTesters** group.

5. On the Password reset blade Properties page, select **Save**.



6. Under **Manage**, select and review the default values for the **Authentication methods**, **Registration**, **Notifications**, and **Customization** settings.

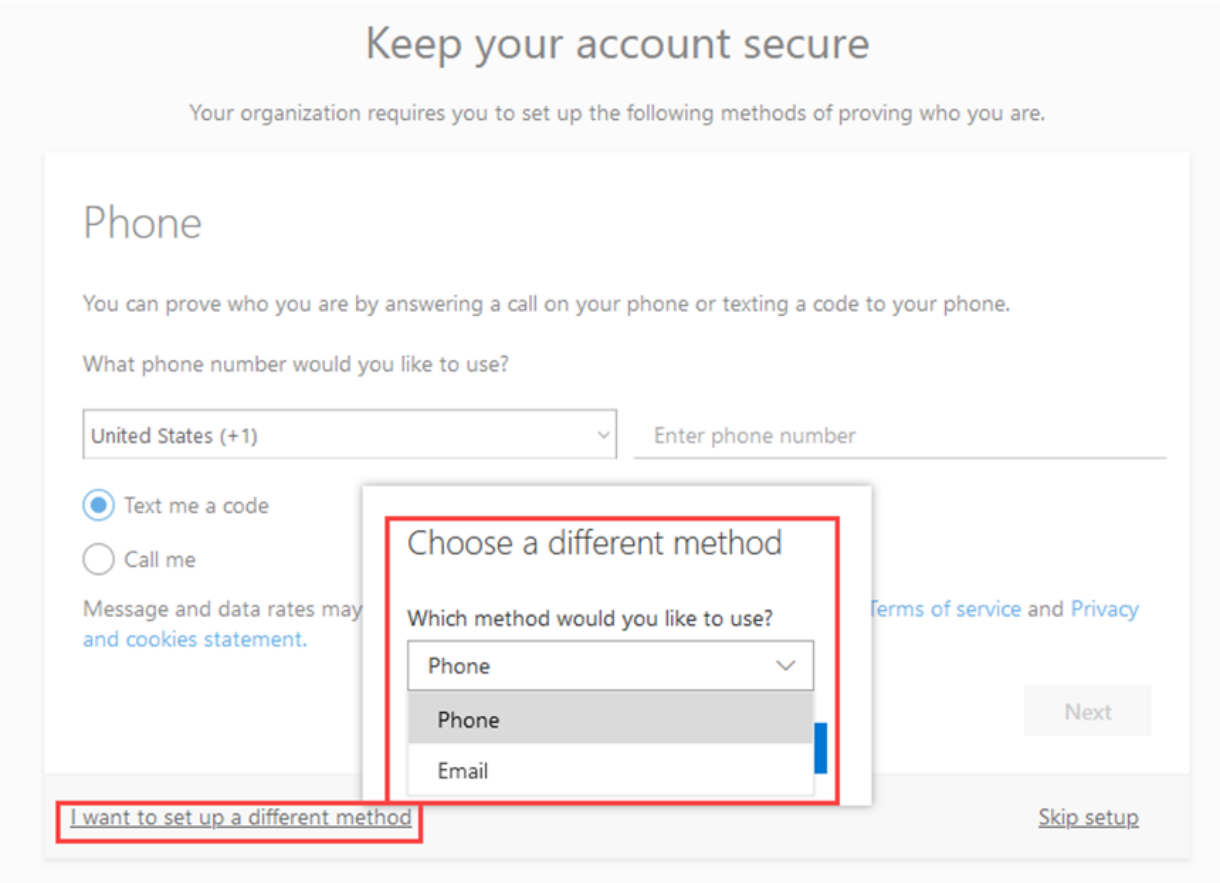
15.5 Register for SSPR

Now that the SSPR configuration is complete, register a mobile phone number for the user you created.

1. Open a different browser or open an InPrivate or Incognito browser session and then browse tohttps://aka.ms/ssprsetup.

   This is to ensure you well be prompted for user authentication.

2. Sign in as **uta@*organization-domain-name*.onmicrosoft.com** with the password that you noted earlier.
3. Replace the organization-domain-name with your domain name.
4. When prompted to update your password, enter a new password of your choice. Be sure to record the new password.
5. In the **More information required** dialog box, select **Next**.
6. On the Keep your account secure page, user the **Phone** option or select the **I want to set up a different method** link.



7. In this example, you will use the **Phone** option. Enter your mobile phone details.
8. Select **Text me a code**.
9. When you receive the code on your mobile phone, enter the code in the text box and then select **Next**.
10. After your phone has been registered, select **Next** and then select **Done**.
11. Close the browser. You do not need to complete the sign in process.

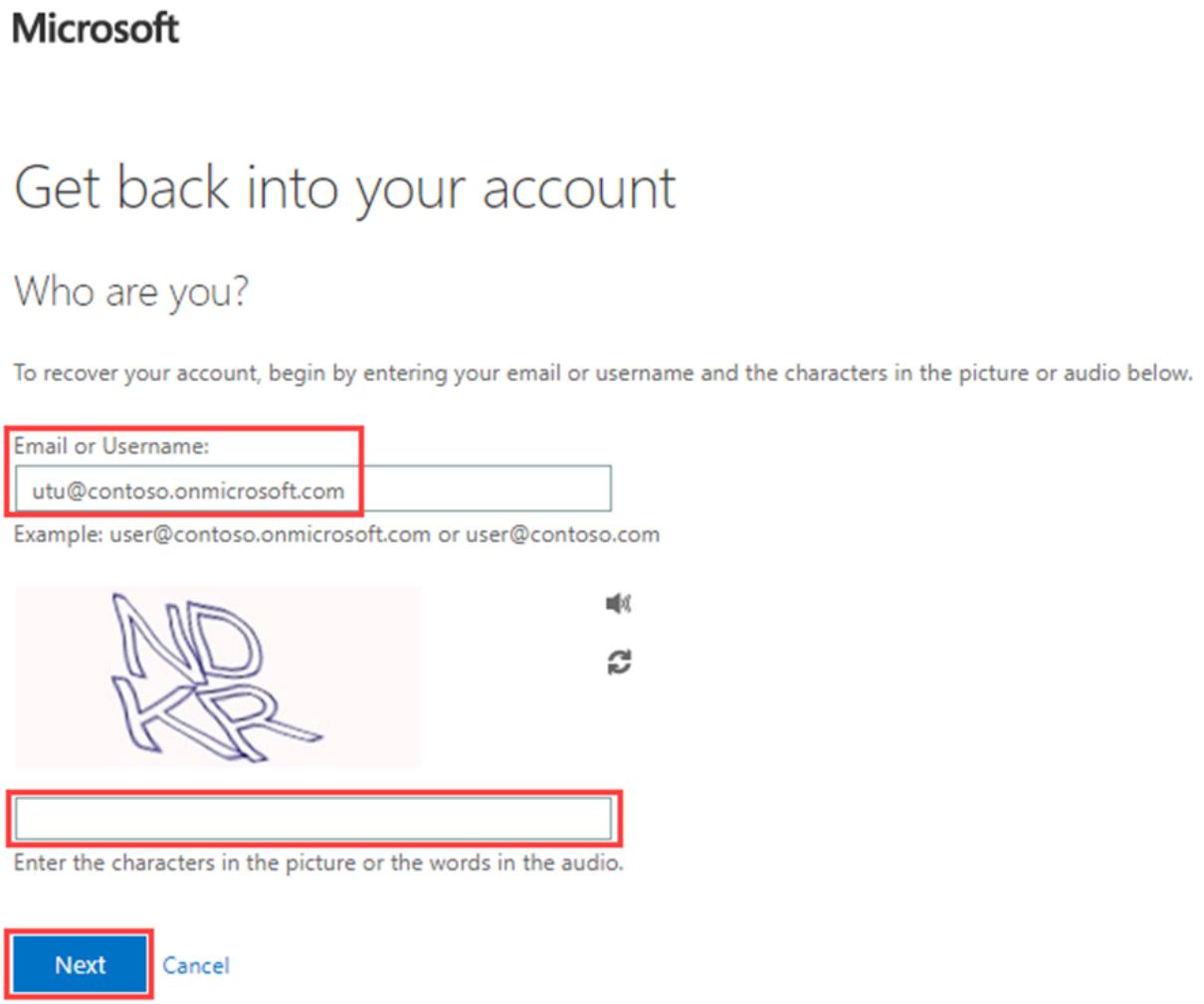
15.6 Test SSPR

Now let's test whether the user can reset their password.

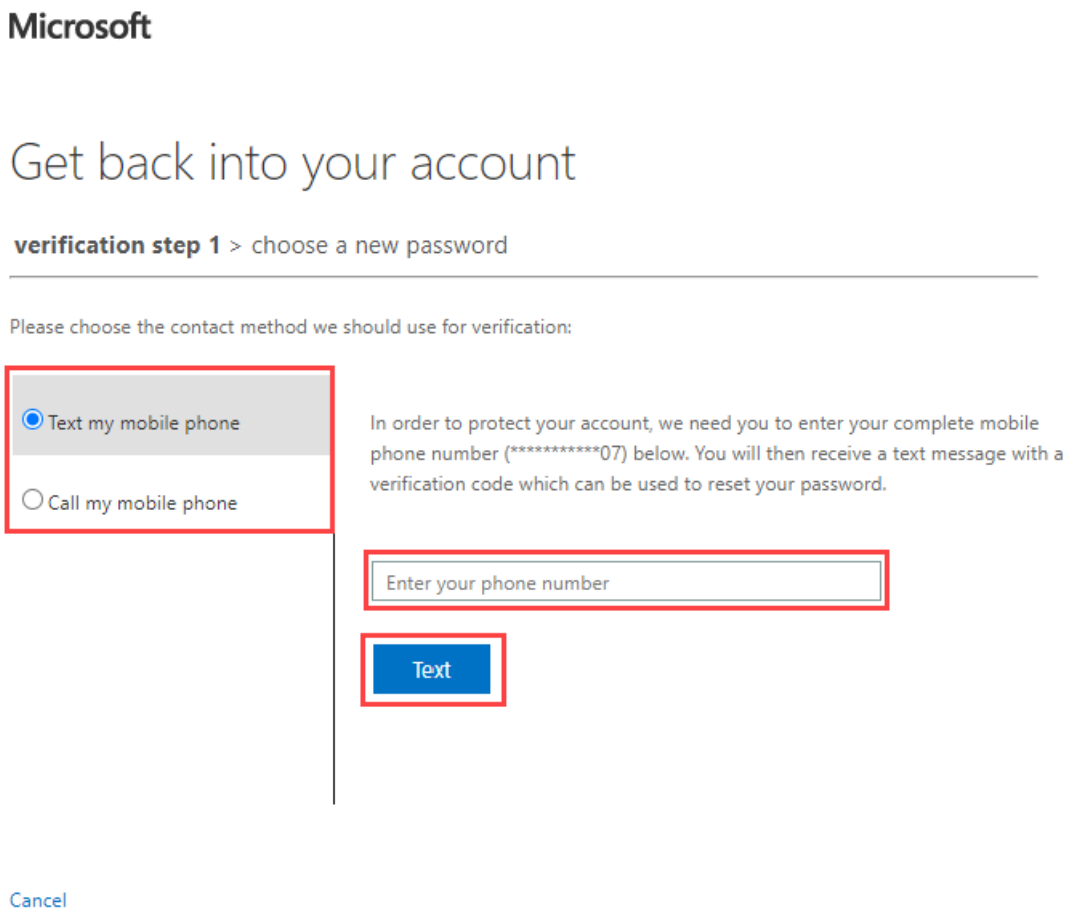
1. Open a different browser or open an InPrivate or Incognito browser session and then browse to https://aka.ms/ssprsetup.

   This is to ensure you well be prompted for user authentication.

2. In the **Email**, **phone**, **or Skype** box, enter **uta@*organization-domain-name*.onmicrosoft.com** and then select **Next**.
3. Replace the organization-domain-name with your domain name.
4. On the Enter password page, select **Forgot my password**.
5. On the Get back into your account page, complete the requested information and then select **Next**.



6. In the **verification step 1** task, select **Text my mobile phone** or **Call my mobile phone**, enter your phone number and then select **Text**.



7. Enter your verification code and then select **Next**.
8. In the choose a new password step, enter and then confirm your new password.
9. When complete, select **Finish**.
10. Sign in as **Utu** with the new password you created.
11. Enter your verification code and then verify you can complete the sign in process.
12. When finished, close your browser.

15.7 lab: title: '14 - Enable Azure AD multi-factor authentication' learning path: '02' module: 'Module 03 -Plan, implement, and administer conditional access'

16 Lab 14 - Working with security defaults

16.1 Lab scenario

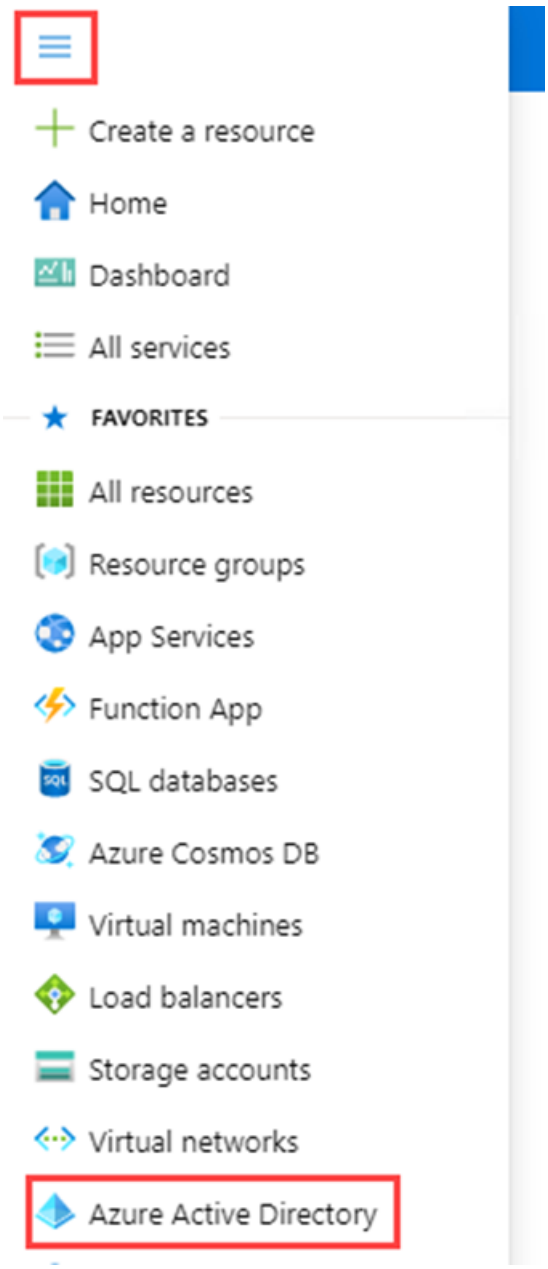
You must configure the Azure Active Directory security default settings in your organization.

16.1.0.1 Estimated time: 5 minutes

16.2 Enabling security defaults

To enable security defaults in your directory:

1. Browse to https://portal.azure.com and sign in using a Global administrator account for the directory.
2. Select the **Show portal menu** hamburger icon and then select **Azure Active Directory**.



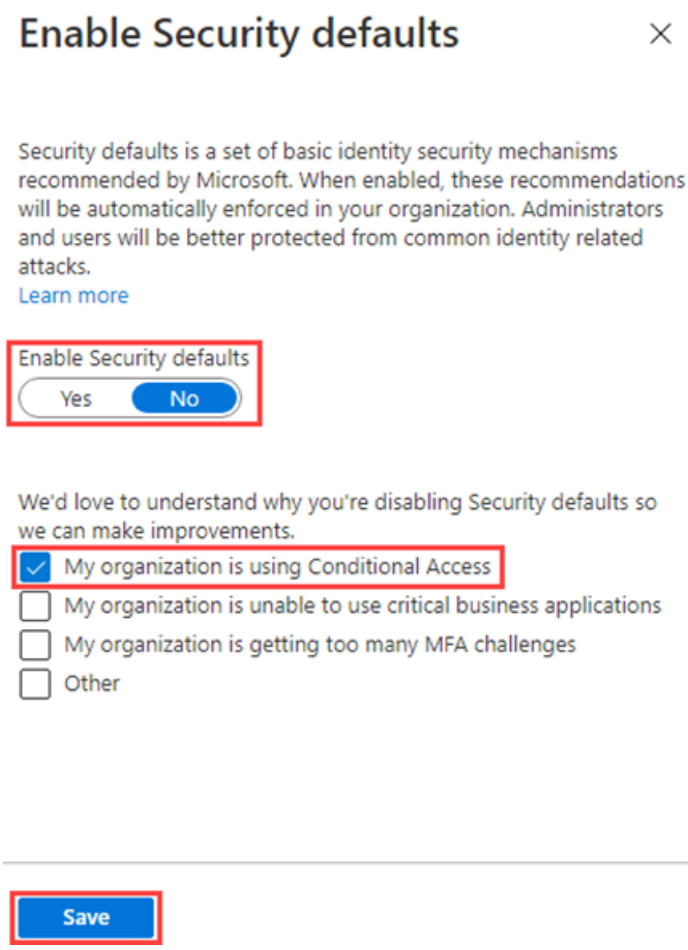
3. In the left navigation, in the Manage section, select **Properties**.
4. At the bottom of the Properties blade, select **Manage Security defaults**.
5. Set the **Enable security defaults** toggle to **Yes**.
6. This may already be enabled.
7. Select **Save**.

16.2.1 Disabling security defaults

Organizations that choose to implement Conditional Access policies that replace security defaults must disable security defaults.

To disable security defaults in your directory:

1. Browse to the https://portal.azure.com and sign in using a Global administrator account for the directory.
2. Select the **Show portal menu** hamburger icon and then select **Azure Active Directory**.
3. At the bottom of the Properties blade, select **Manage Security defaults**.
4. Set the **Enable security defaults** toggle to **No**.



5. Select **Save**.

16.3 lab: title: '15 - Implement and test a conditional access policy' learning path: '02' module: 'Module 03 -Plan, implement, and administer conditional access'

17 Lab 15 - Implement and test a conditional access policy

17.1 Lab scenario

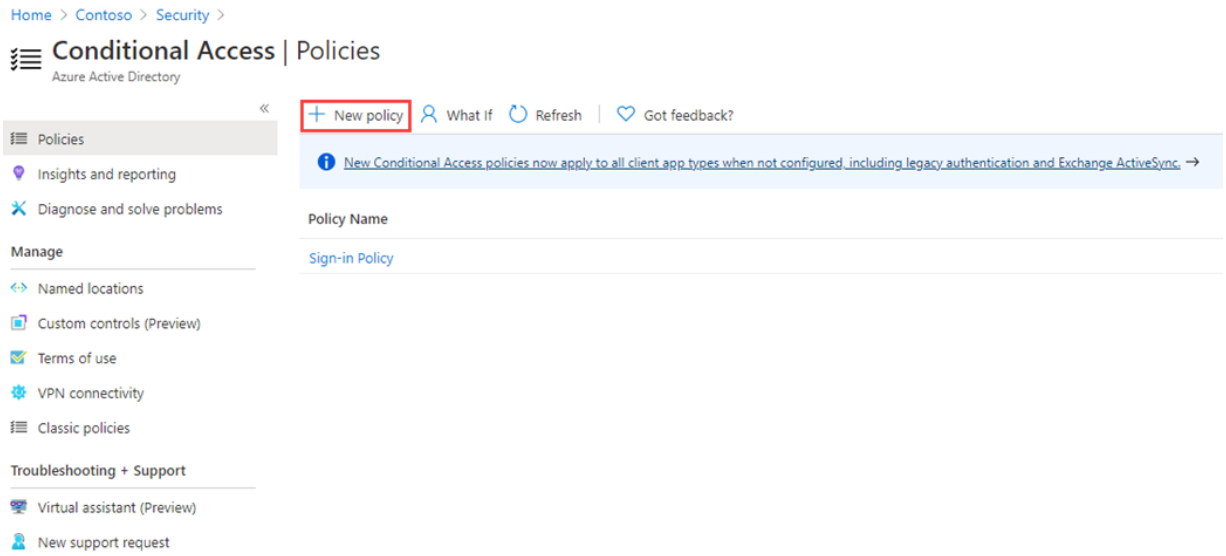
Your organization needs to be able to limit user access to its internal applications. You must deploy an Azure Active Directory conditional access policy.

17.1.0.1 Estimated time: 10 minutes

17.2 Create a conditional access policy

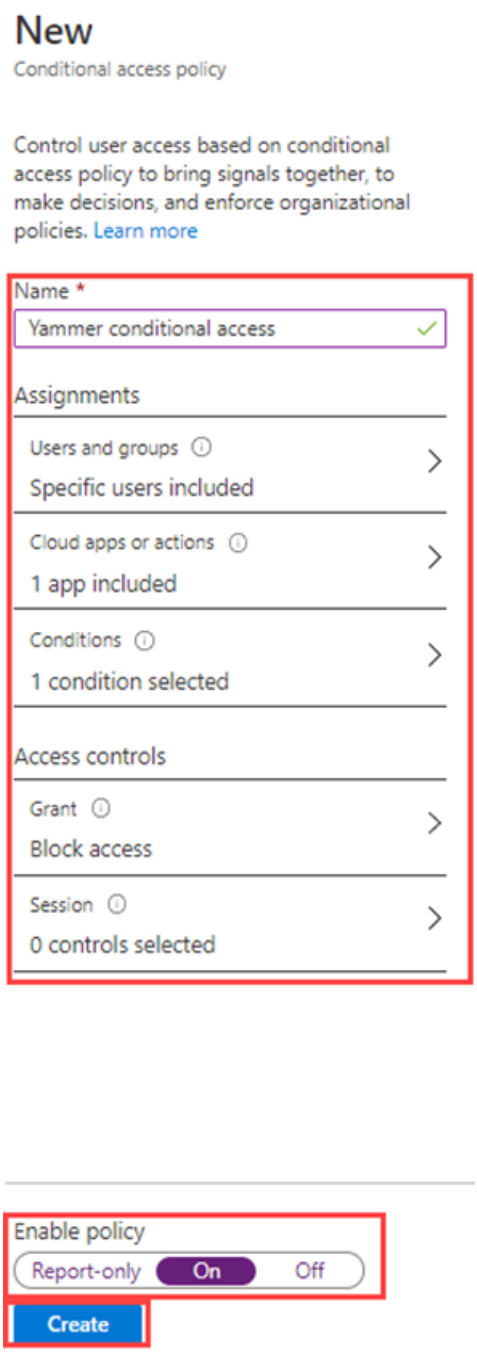
Azure Active Directory conditional access is an advanced feature of Azure AD that allows you to specify detailed policies that control who can access your resources. Using Conditional Access, you can protect your applications by limiting users' access based on things like groups, device type, location, and role.

1. Browse to https://portal.azure.com and sign in using a Global administrator account for the directory.
2. Open the portal menu and then select **Azure Active Directory**.
3. On the Azure Active Directory blade, under **Manage**, select **Security**.
4. On the Security blade, in the left navigation, select **Conditional access**.
5. On the top menu, select **New policy**.



6. In the **Name** box, enter **Yammer conditional access**.
7. This is the name being using for this exercise, you may choose another name if you wish.
8. Under **Assignments**, select **Users and groups**.
9. On the Include tab, select the **Users and groups** check box.
10. In the Select pane, select your administrator account and then select **Select**.
11. Select **Cloud apps or actions**.
12. Verify **Cloud apps** is selected and then select **Select apps**.
13. In the Select pane, select **Office 365 Yammer** and then select **Select**.
14. Select **Conditions** and then select **Conditions**.
15. Under **Configure**, select **Yes** and then select **Any location**.
16. Under **Access controls**, select **Grant**.
17. In the Grant pane, select **Block access** and then select **Select**.

    Note This policy is being configure for the exercise only and is being used to quickly demonstrate a conditional access policy.
18. Under **Enable policy**, select **On**, and then select **Create**.



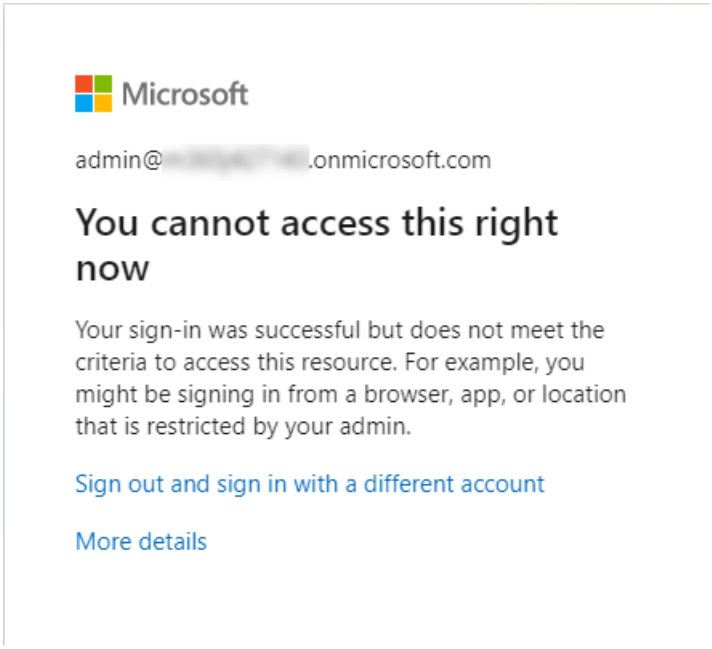
17.3 Test the conditional access policy

You should test your conditional access policies to ensure they working as expected.

1. Open a new browser tab and then browse to https://www.yammer.com/office365.

   Your credentials should be passed through.

2. Verify you are prevented from successfully access Microsoft Yammer.



3. If you are signed in, close the tab, wait 1-2 minutes, and then retry.
4. Close the tab and return to the Conditional Access blade.
5. Select the **Yammer conditional access** policy.
6. Under **Enable policy**, select **Off** and then select **Save**.

17.4 lab: title: '16 - Configure authentication session controls' learning path: '02' module: 'Module 03 -Plan, implement, and administer conditional access'

18 Lab 16 - Configure authentication session controls

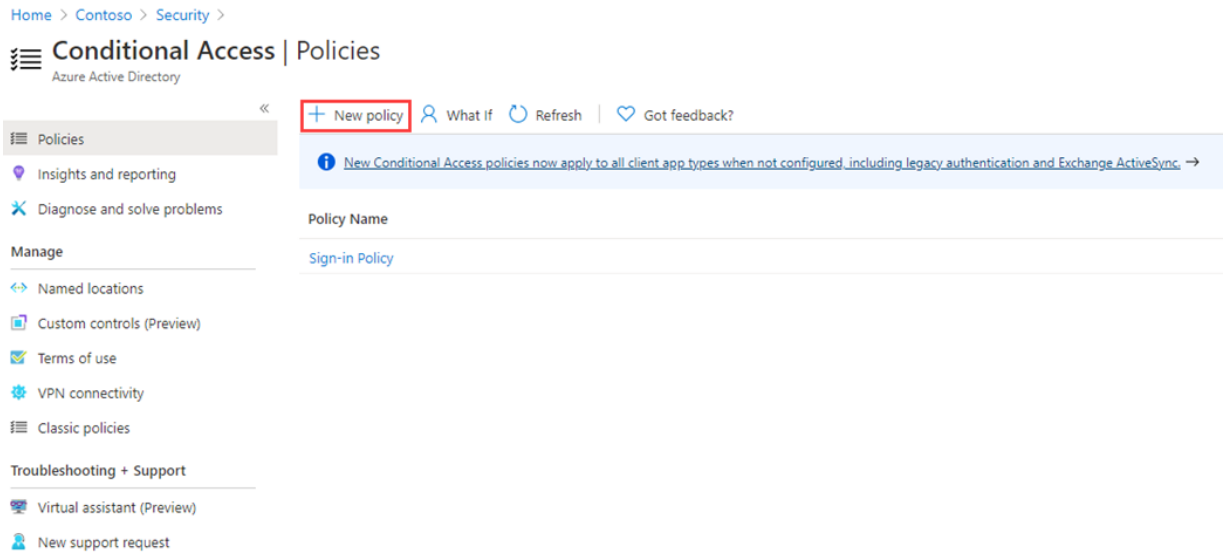
18.1 Lab scenario

As part of your company's larger security configuration, you must test a conditional access policy that can be used to control sign in frequency.

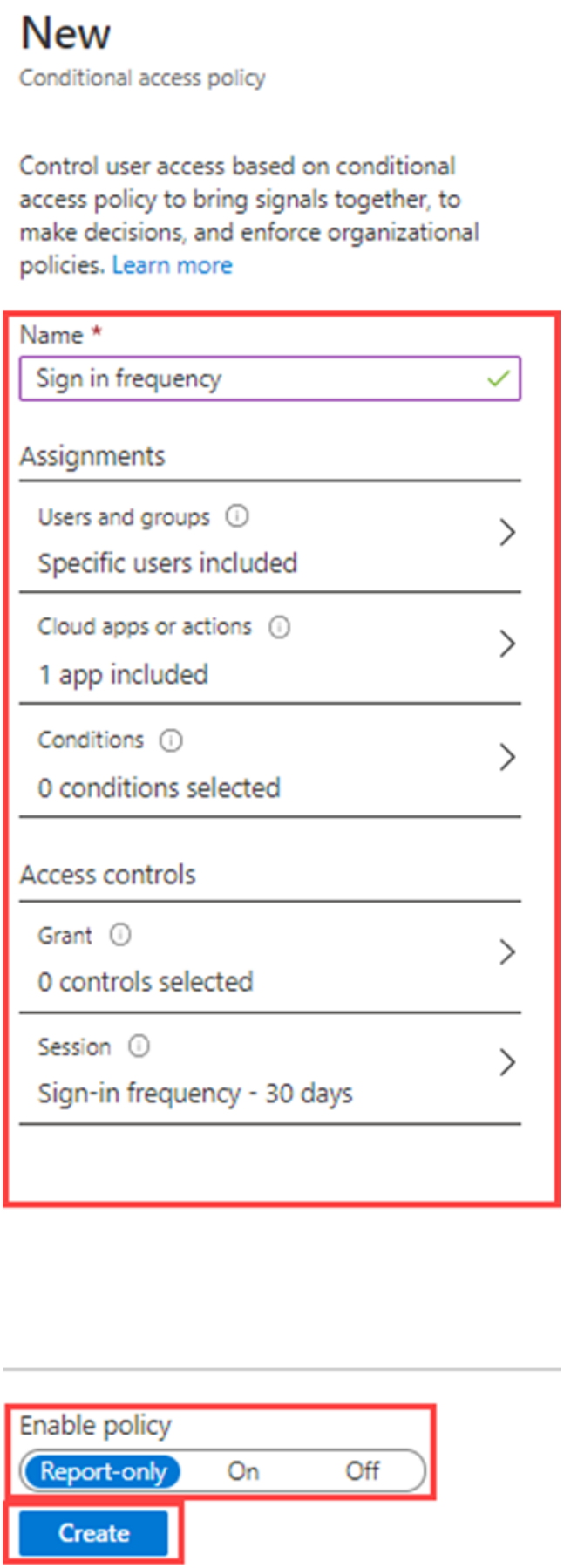
18.1.0.1 Estimated time: 10 minutes

18.2 Configure sign in frequency controls using a conditional access policy

1. Browse to https://portal.azure.com and sign in using a Global administrator account for the directory.
2. Open the portal menu and then select **Azure Active Directory**.
3. On the Azure Active Directory blade, under **Manage**, select **Security**.
4. On the Security blade, in the left navigation, select **Conditional access**.
5. On the top menu, select **New policy**.



6. In the **Name** box, enter **Sign in frequency**.
7. Under **Assignments**, select **Users and groups**.
8. On the Include tab, select the **Users and groups** check box.
9. In the Select pane, select your administrator account and then select **Select**.
10. Select **Cloud apps or actions**.
11. Verify **Cloud apps** is selected and then select **Select apps**.
12. In the Select pane, select **Office 365** and then select **Select**.
13. Under **Access controls**, select **Session**.
14. In the Session pane, select **Sign-in frequency**.
15. In the value box, enter **30**.
16. Select the units menu, select **Days**, and then select **Select**.
17. Under **Enable policy**, select **Report-only**, and then select **Create**.



[!NOTE] Report-only mode is a new Conditional Access policy state that allows administrators to evaluate the impact of Conditional Access policies before enabling them in their environment. With the release of report-only mode:

- Conditional Access policies can be enabled in report-only mode.
- During sign-in, policies in report-only mode are evaluated but not enforced.
- Results are logged in the Conditional Access and Report-only tabs of the Sign-in log details.
- Customers with an Azure Monitor subscription can monitor the impact of their Conditional Access policies using the Conditional Access insights workbook.

18.3 lab: title: '17 - Manage Azure AD smart lockout values' learning path: '02' module: 'Module 03 -Plan, implement, and administer conditional access'

19 Lab 17 - Manage Azure AD smart lockout values

19.1 Lab scenario

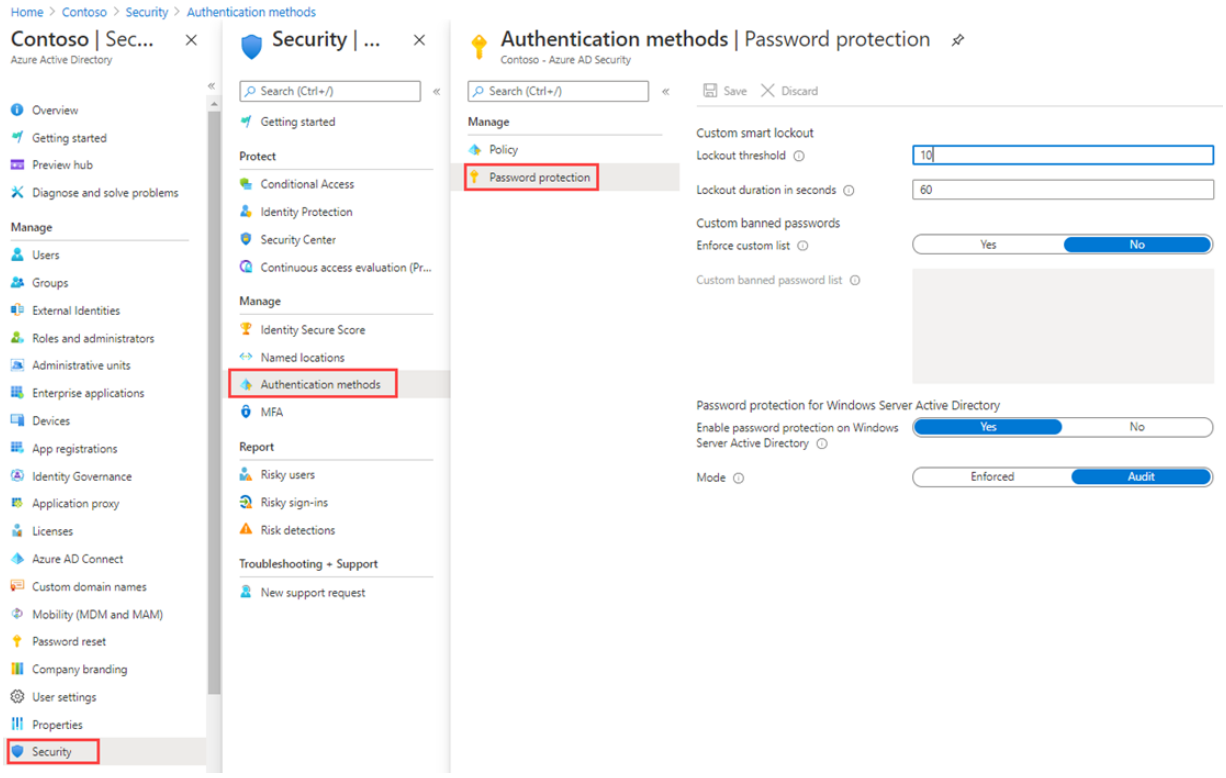
You must configure the additional password protection settings for your organization.

19.1.0.1 Estimated time: 5 minutes

19.2 Manage Azure AD smart lockout values

Based on your organizational requirements, you can customize the Azure AD smart lockout values. Customization of the smart lockout settings, with values specific to your organization, requires Azure AD Premium P1 or higher licenses for your users.

1. Browse to https://portal.azure.com and sign in using a Global administrator account for the directory.
2. Open the portal menu and then select **Azure Active Directory**.
3. On the Azure Active Directory blade, under **Manage**, select **Security**.
4. On the Security blade, in the left navigation, select **Authentication methods**.
5. In the left navigation, select **Password protection**.



6. In the Password protection settings, in the **Lockout duration in seconds** box, set the value to **120**.
7. Next to **Mode**, select **Enforced**.
8. Save your changes.

[!NOTE] When the smart lockout threshold is triggered, you will get the following message while the account is locked: Your account is temporarily locked to prevent unauthorized use. Try again later, and if you still have trouble, contact your admin.

19.3 lab: title: '18 - Enable sign in and user risk policies' learning path: '02' module: 'Module 04 -Manage Azure AD identity protection'

20 Lab 18 - Enable sign in and user risk policies

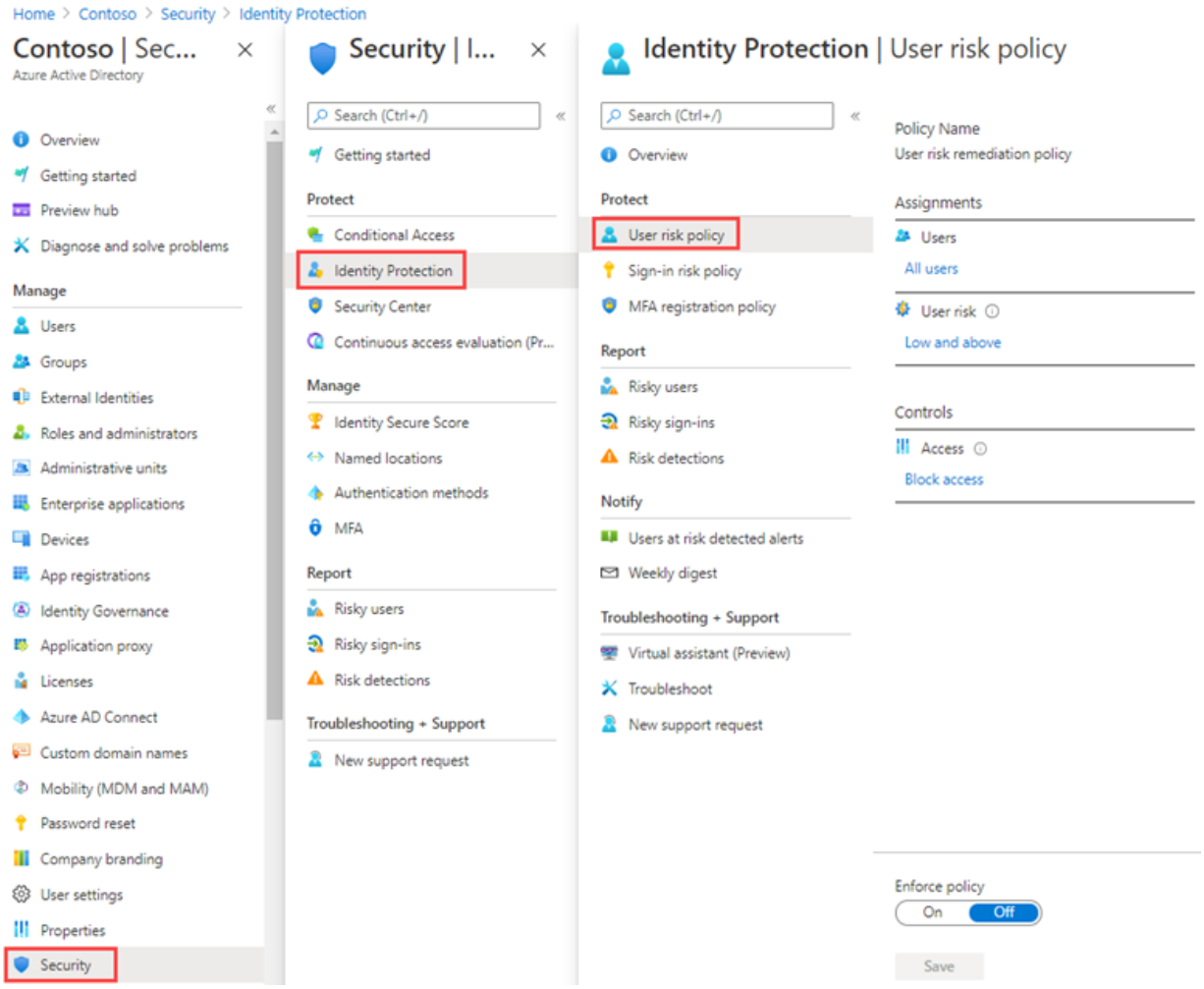
20.1 Lab scenario

As an additional layer of security, you need to enable and configure your Azure AD organization's sign in and user risk policies.

20.1.0.1 Estimated time: 10 minutes

20.2 Enable User risk policy

1. Sign in to the https://portal.azure.com using a Global administrator account.
2. Open the portal menu and then select **Azure Active Directory**.
3. On the Azure Active Directory blade, under **Manage**, select **Security**.
4. On the Security blade, in the left navigation, select **Identity protection**.
5. In the Identity protection blade, in the left navigation, select **User risk policy**.



6. Under **Assignments**, select **All users** and review the available options.

7. You can select from **All users** or **Select individuals and groups** if limiting your rollout.
8. Additionally, you can choose to exclude users from the policy.
9. Under **User risk**, select **Low and above**.
10. In the User risk pane, select **High** and then select **Done**.
11. Under **Controls** > **Access**, select **Block access**.
12. In the Access pane, review the available options.

    Tip Microsoft's recommendation is to Allow access and Require password change.
13. Select the **Require password change** check box and then select **Done**.
14. Under **Enforce Policy**, select **On** and then select **Save**.

20.3 Enable Sign-in risk policy

1. On the Identity protection blade, in the left navigation, select **Sign-in risk policy**.
2. As with the User risk policy, the Sign-in risk policy can be assigned to users and groups and allows you to exclude users from the policy.
3. Under **Sign-in risk**, select **Medium and above**.
4. In the Sign-in risk pane, select **High** and then select **Done**.
5. Under **Controls** > **Access**, select **Block access**.
6. Select the **Require password change** check box and then select **Done**.
7. Under **Enforce Policy**, select **On** and then select **Save**.

20.4 lab: title: '19 - Configure an Azure AD multi-factor authentication registration policy' learning path: '02' module: 'Module 04 -Manage Azure AD identity protection'

21 Lab 19 - Configure an Azure AD multi-factor authentication registration policy

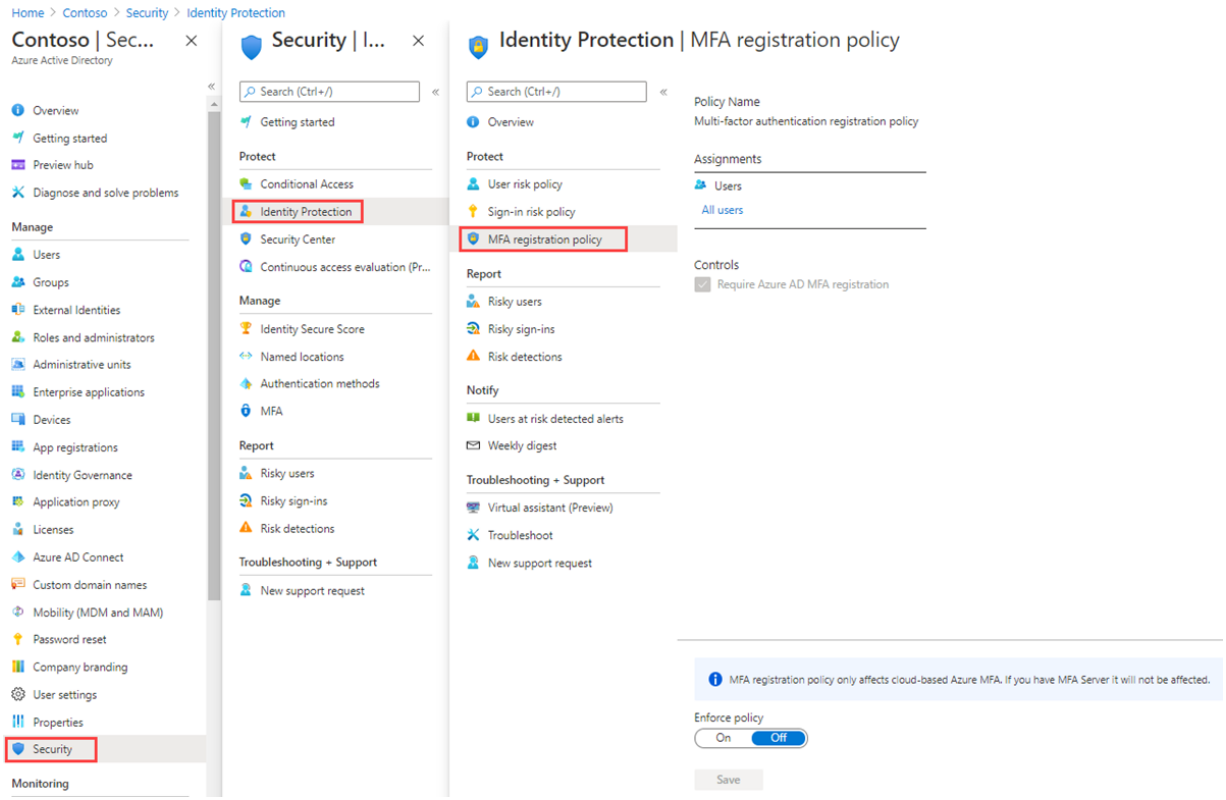
21.1 Lab scenario

Azure AD multi-factor authentication provides a means to verify who you are using more than just a username and password. It provides a second layer of security to user sign-ins. For users to be able to respond to MFA prompts, they must first register for Azure AD Multi-Factor Authentication. You must configure your Azure AD organization's MFA registration policy to be assigned to all users.

21.1.0.1 Estimated time: 5 minutes

21.2 Policy configuration

1. Sign in to the https://portal.azure.com using a Global administrator account.
2. Open the portal menu and then select **Azure Active Directory**.
3. On the Azure Active Directory blade, under **Manage**, select **Security**.
4. On the Security blade, in the left navigation, select **Identity protection**.
5. In the Identity protection blade, in the left navigation, select **MFA registration policy**.



6. Under **Assignments**
7. Under **Assignments**, select **All users** and review the available options.
8. You can select from **All users** or **Select individuals and groups** if limiting your rollout.
9. Additionally, you can choose to exclude users from the policy.
10. Under **Controls**, notice that the **Require Azure AD MFA registration** is selected and cannot be changed.
11. Under **Enforce Policy**, select **On** and then select **Save**.

21.3 lab: title: '20 - Implement access management for apps' learning path: '03' module: 'Module 01 -Plan and design the integration of enterprise apps for SSO'

22 Lab 20 - Implement access management for apps

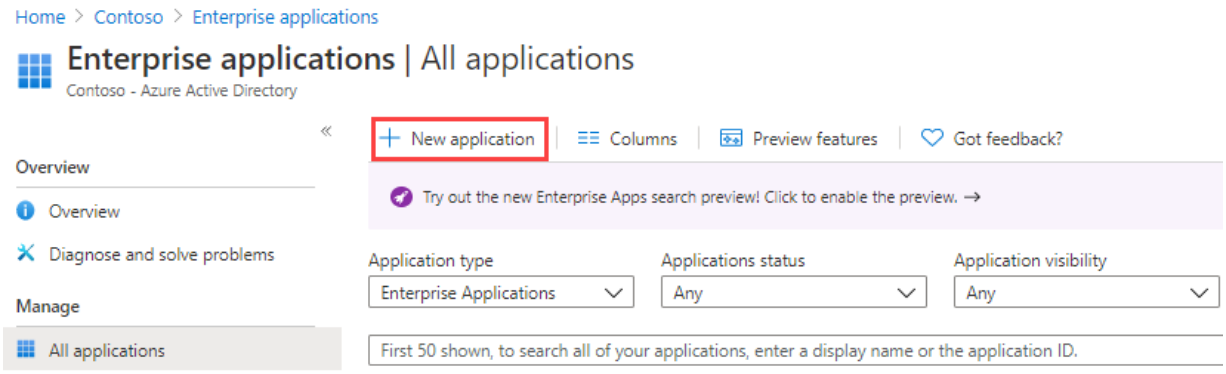
22.1 Lab scenario

Your organization requires that only specific users or groups have access to enterprise applications. You must assign a user to a specific application.

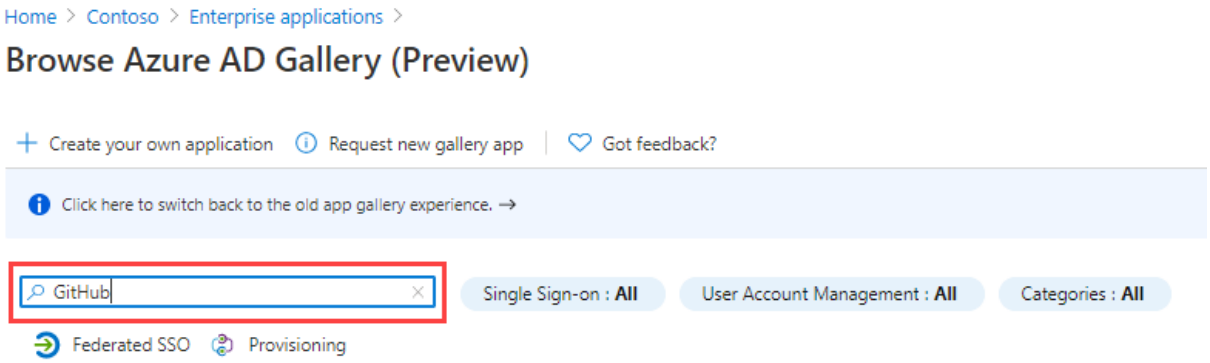
22.1.0.1 Estimated time: 5 minutes

22.2 Add an app to your Azure AD tenant

1. Sign in to the https://portal.azure.com using a Global administrator account.
2. Open the portal menu and then select **Azure Active Directory**.
3. On the Azure Active Directory blade, under **Manage**, select **Enterprise applications**.
4. In the Enterprise applications pane, select + **New application**.



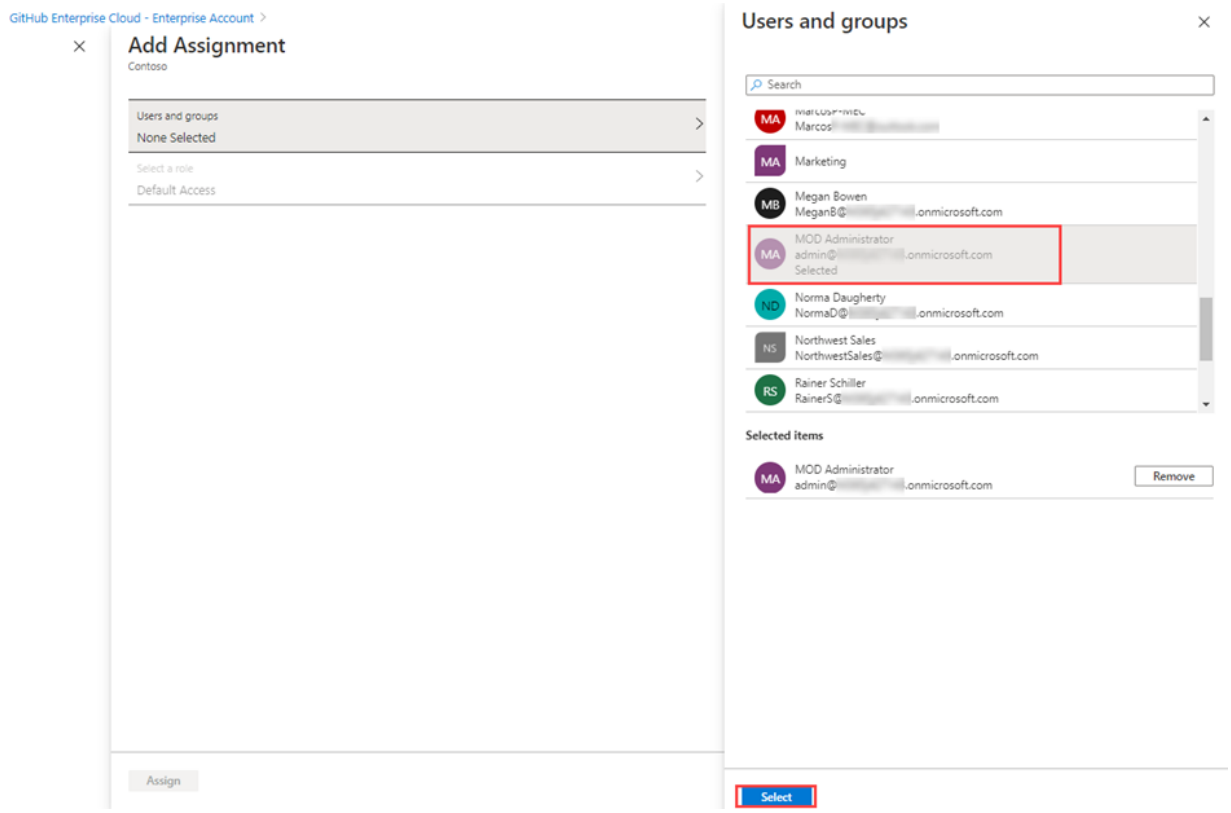
5. In the Browse Azure AD Gallery (Preview) blade, in the **Search application** box, enter **GitHub**.



6. In the results, select **GitHub Enterprise Cloud – Enterprise Account**.
7. In the **GitHub Enterprise Cloud – Enterprise Account**, review the settings and then select **Create**.
8. Once created, you will be redirected to the GitHub Enterprise Cloud – Enterprise Account blade.

22.3 Assign users to an app

1. On the GitHub Enterprise Cloud – Enterprise Account blade, on the Overview page, under **Getting Started**, select **1. Assign users and groups**.
2. Alternatively, in the left navigation, under **Manage**, you can select **Users and groups**.
3. On the Users and groups page, on the menu, select **+Add user/group**.
4. On the Add Assignment blade, select **Users and groups**.
5. In the Users and groups pane, select your administrator account and then select **Select**.



6. Select **Assign**.

22.4 lab: title: '21 - Create a new custom role to grant access to manage app registrations' learning path: '03' module: 'Module 01 - Plan and design the integration of enterprise apps for SSO'

23 Lab 21 - Implement access management for apps

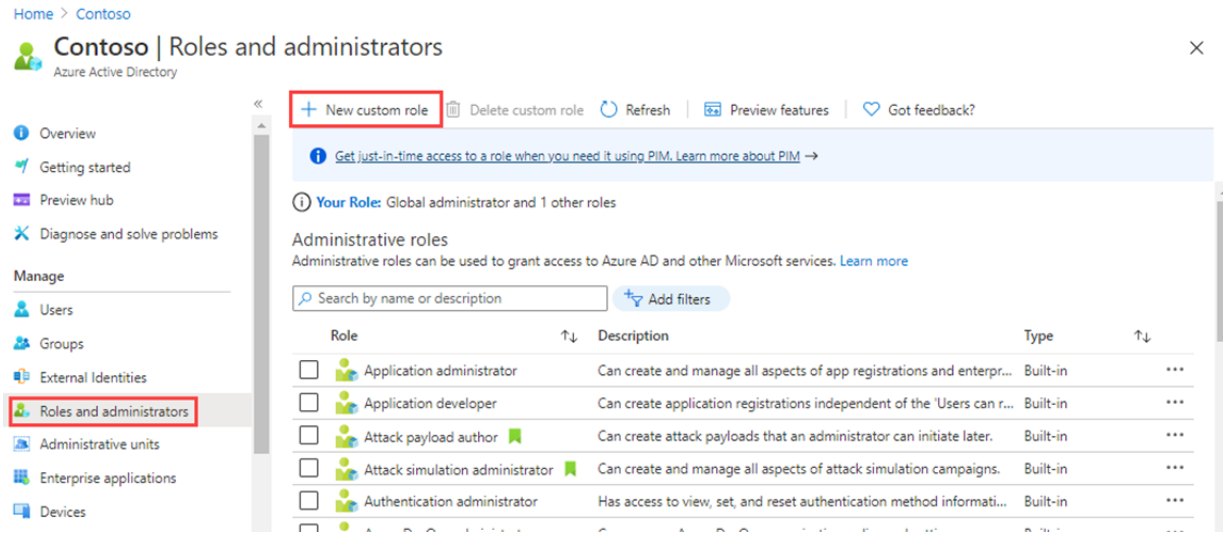
23.1 Lab scenario

You need to create a new custom role for app management. This new role should be limited to only the specific permissions required to perform credential management.

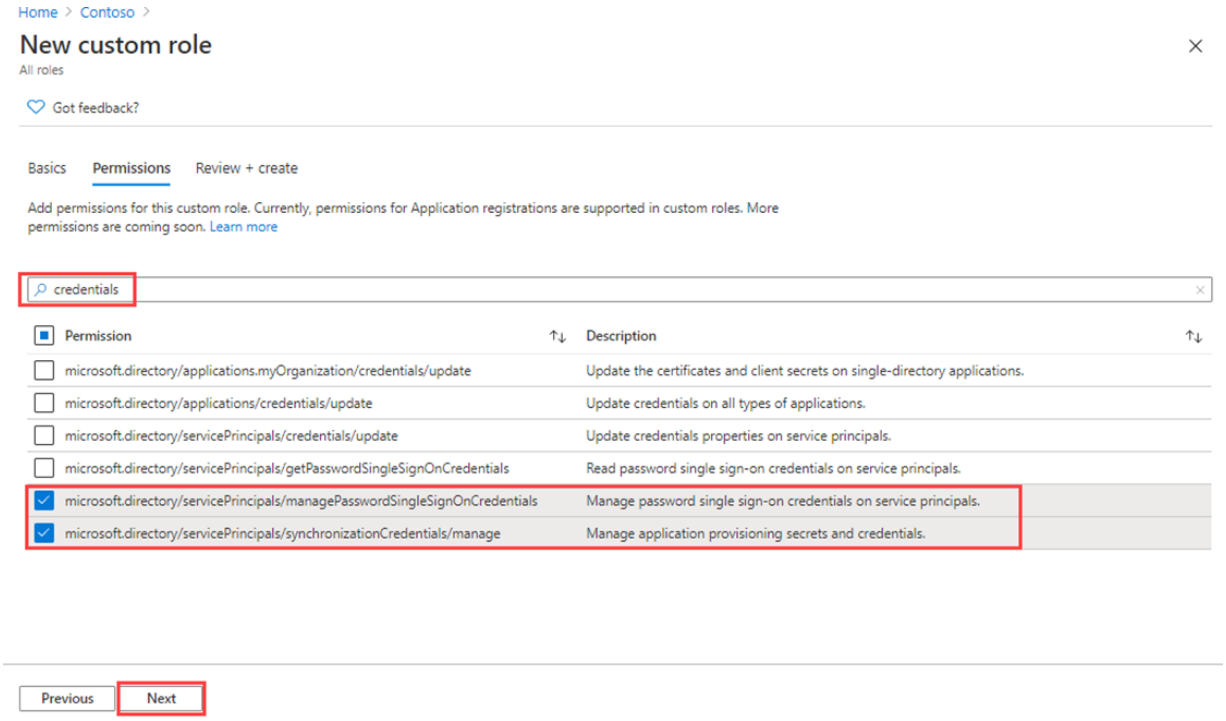
23.1.0.1 Estimated time: 5 minutes

23.2 Create a new custom role to grant access to manage app registrations

1. Sign in to the https://portal.azure.com using a Global administrator account.
2. Open the portal menu and then select **Azure Active Directory**.
3. On the Azure Active Directory blade, under **Manage**, select **Roles and administrators**.
4. On the Roles and administrators blade, on the menu, select **New custom role**.



5. In the New custom role blade, on the Basics tab, in the name box, enter **My custom app role**.
6. Review the remaining options and then select **Next**.
7. On the Permissions tab, review the available permissions.
8. In the **Search by permission name or description** box, enter **credentials**.
9. In the results, select the **Manage** permissions and then select **Next**.



10. Review the changes and then select **Create**.

23.3 lab: title: '22 - Register an application' learning path: '03' module: 'Module 03 - Implement app registrations'

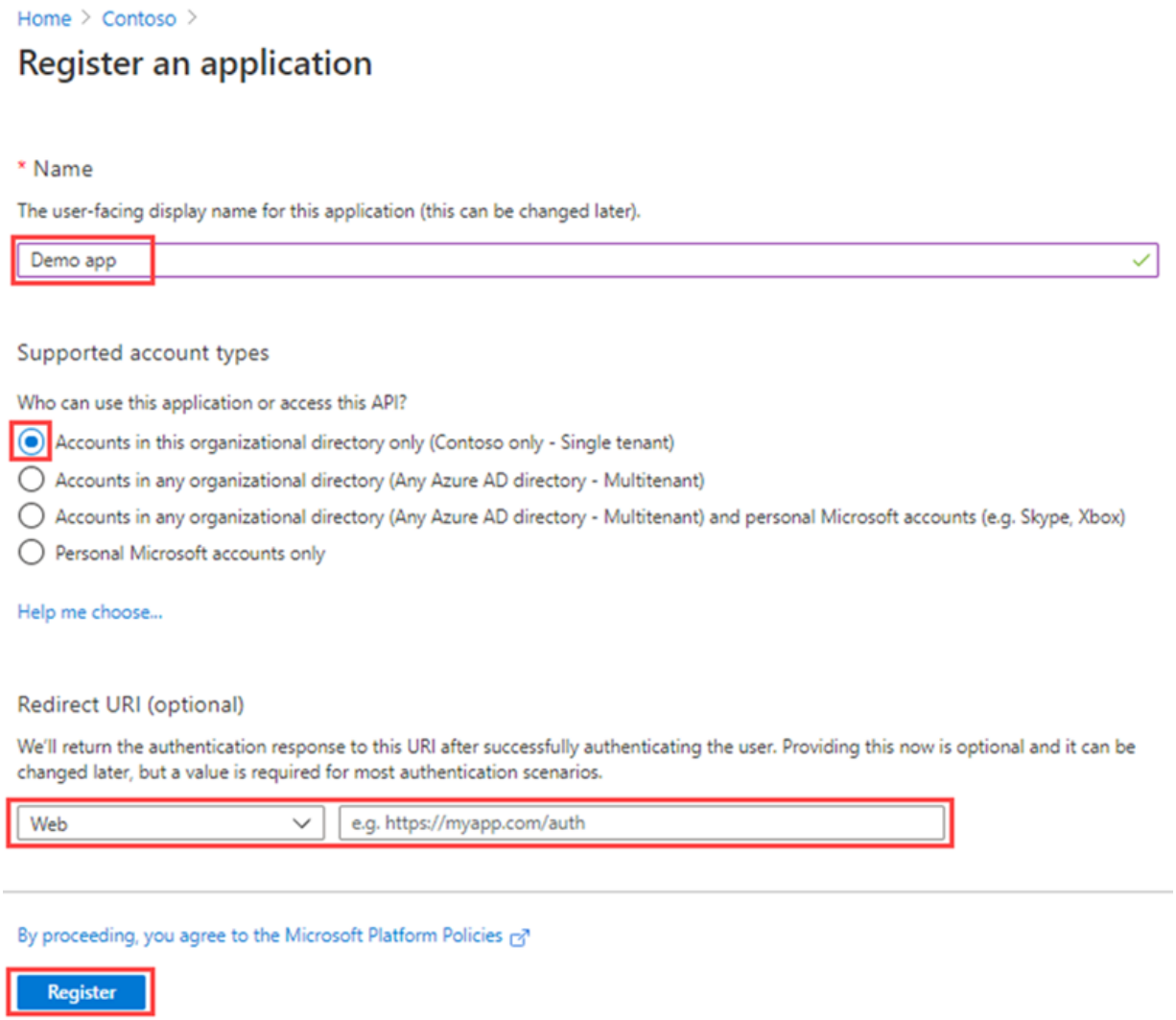
24 Lab 22 - Register an application

24.0.0.1 Estimated time: 20 minutes

24.1 Register an application

Registering your application establishes a trust relationship between your app and the Microsoft identity platform. The trust is unidirectional: Your app trusts the Microsoft identity platform—not the other way around.

1. Sign in to https://portal.azure.com using a Global Administrator account.
2. Open the portal menu and then select **Azure Active Directory**.
3. On the **Azure Active Directory** blade, under **Manage**, select **App registrations.**
4. On the **App registrations** page, on the menu, select + **New registration**.
5. On the **register an application** blade, register an app named **Demo app** using the default values. You do not need to enter the redirect URI.



6. When complete, you will be directed to the **Demo app** blade.

24.2 Add a redirect URI

A redirect URI is the location where the Microsoft identity platform redirects a user's client and sends security tokens after authentication. In a production web application, for example, the redirect URI is often a public endpoint where your app is running. During development, it's common to also add the endpoint where you run your app locally.

1. Add and modify redirect URIs for your registered applications by configuring their platform settings.

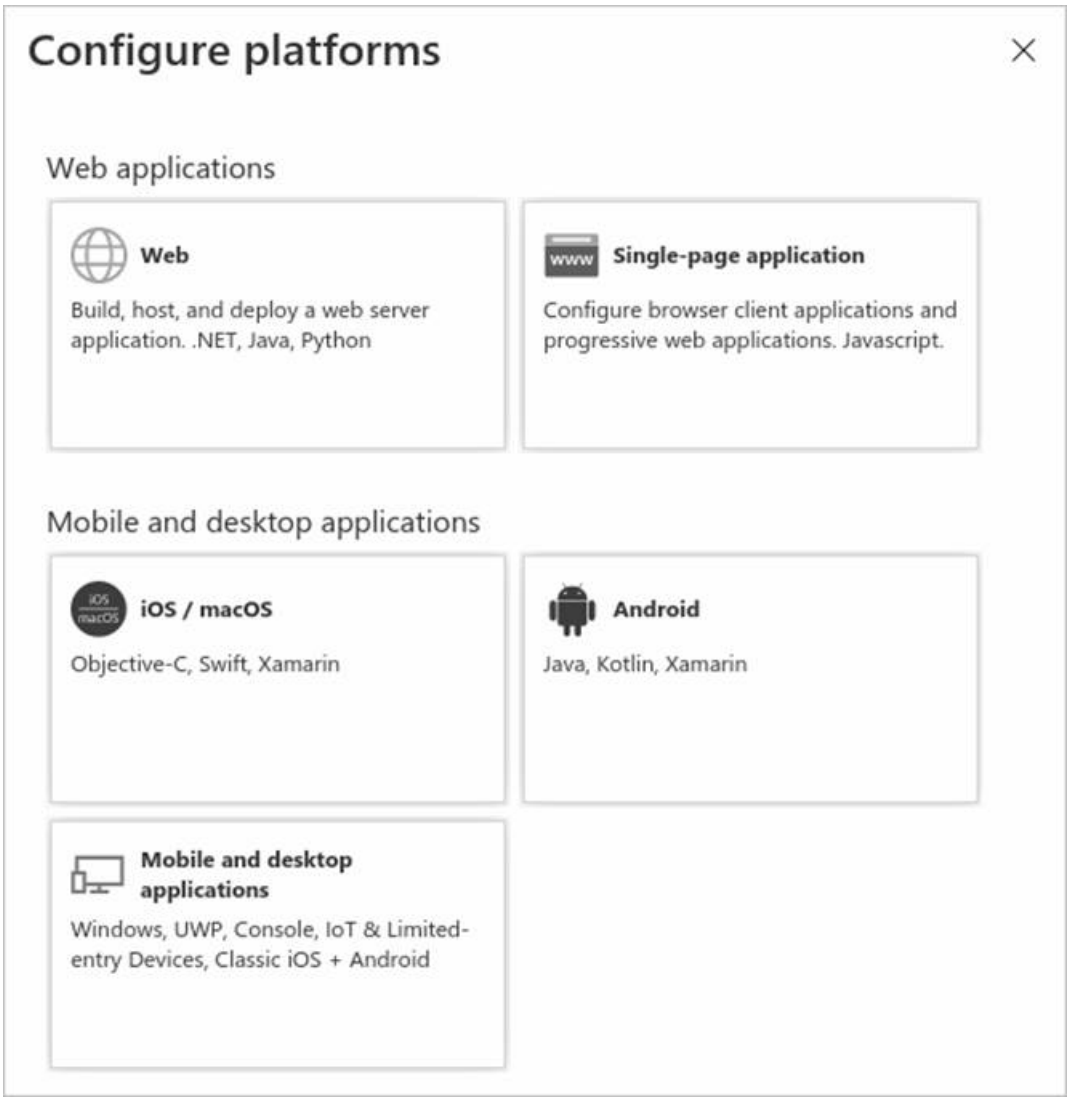
24.3 Configure platform settings

Settings for each application type, including redirect URIs, are configured in **Platform configurations** in the Azure portal. Some platforms, like **Web** and **Single-page applications**, require you to manually specify a

redirect URI. For other platforms, like mobile and desktop, you can select from redirect URIs generated for you when you configure their other settings.

To configure application settings based on the platform or device you're targeting:

1. Select your application in **App registrations** in the Azure portal.
2. Under **Manage**, select **Authentication**.
3. Under **Platform configurations**, select **Add a platform**.
4. In **Configure platforms**, select the tile for your application type (platform) to configure its settings.



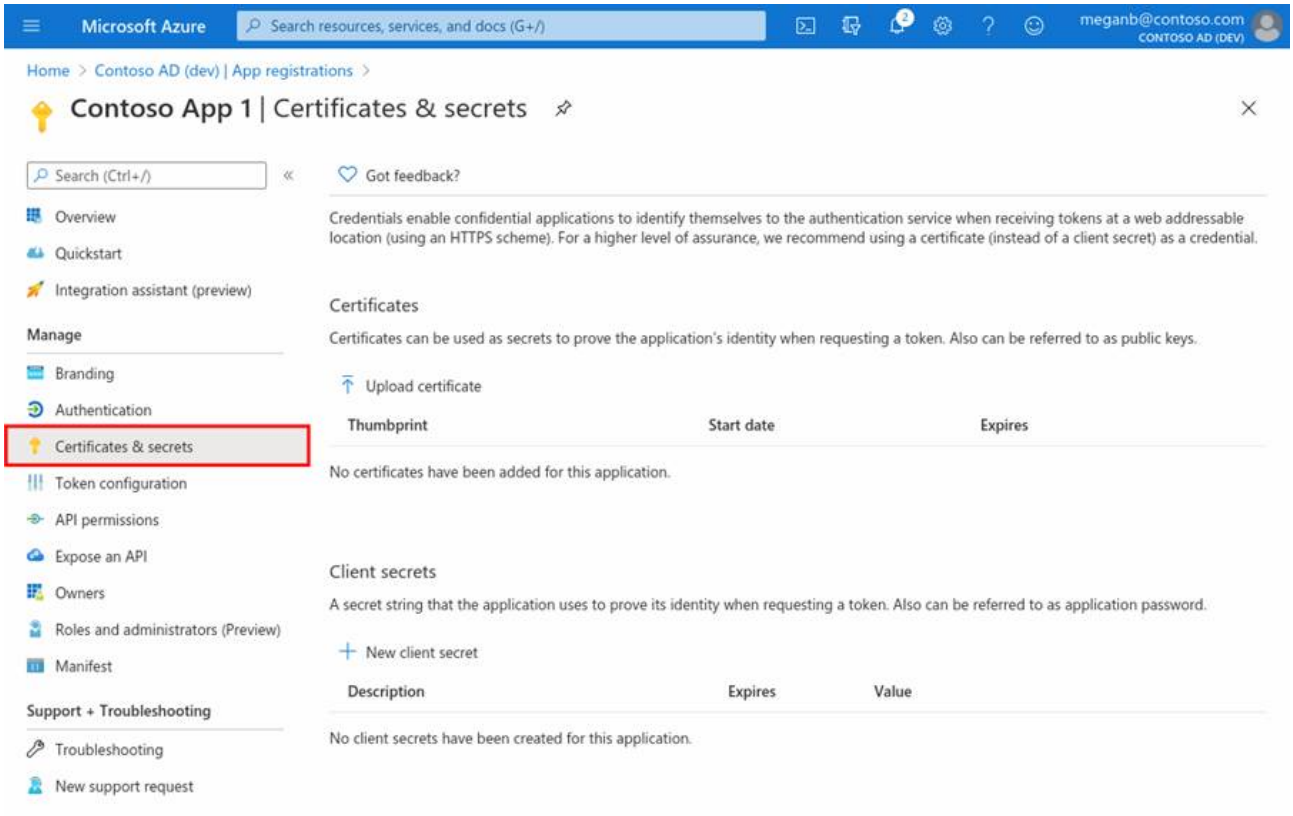
Platform	Configuration settings
Web	Enter a **Redirect URI** for your app, the location where Microsoft identity platform red
Single-page application	Enter a **Redirect URI** for your app, the location where Microsoft identity platform red
iOS/macOS	Enter the app **Bundle ID**, found in XCode in *Info.plist* or Build Settings. A redirect U
Android	Enter the app **Package name**, which you can find in the AndroidManifest.xml file, and
Mobile and desktop applications	Select one of the **Suggested redirect URIs** or specify a **Custom redirect URI**. For

5. Select **Configure** to complete the platform configuration.

24.4 Add credentials

Credentials are used by confidential client applications that access a web API. Examples of confidential clients include web apps, other web APIs, and service-type and daemon-type applications. Credentials allow your application to authenticate as itself, requiring no interaction from a user at runtime.

You can add both certificates and client secrets (a string) as credentials to your confidential client app registration.



24.5 Add a certificate

Sometimes called a *public key*, certificates are the recommended credential type, because as they provide a higher level of assurance than a client secret. When using a trusted public certificate, you can add the certificate using the Certificates & secrets feature. Your certificate must be one of the following file types: .cer, .pem, .crt.

24.6 Add a client secret

The client secret, also known as an *application password*, is a string value your app can use in place of a certificate to identity itself. It's the easier of the two credential types to use. It's often used during development, but is considered less secure than a certificate. You should use certificates in your applications running in production.

1. Select your application in **App registrations** in the Azure portal.
2. Select **Certificates & secrets** > **New client secret**.
3. Add a description for your client secret.
4. Select a duration.
5. Select **Add**.
6. **Record the secret's value** for use in your client application code; It's *never displayed again* after you leave this page.

24.7 Register the web API

To provide scoped access to the resources in your web API, you must first register the API with the Microsoft identity platform.

1. Perform the steps above.
2. Skip the **Add a redirect URI** and **Configure platform settings** sections. You don't need to configure a redirect URI for a web API since no user is logged in interactively.
3. Skip the **Add credentials** section for now. Only if your API accesses a downstream API would it need its own credentials—a scenario not covered in this article.

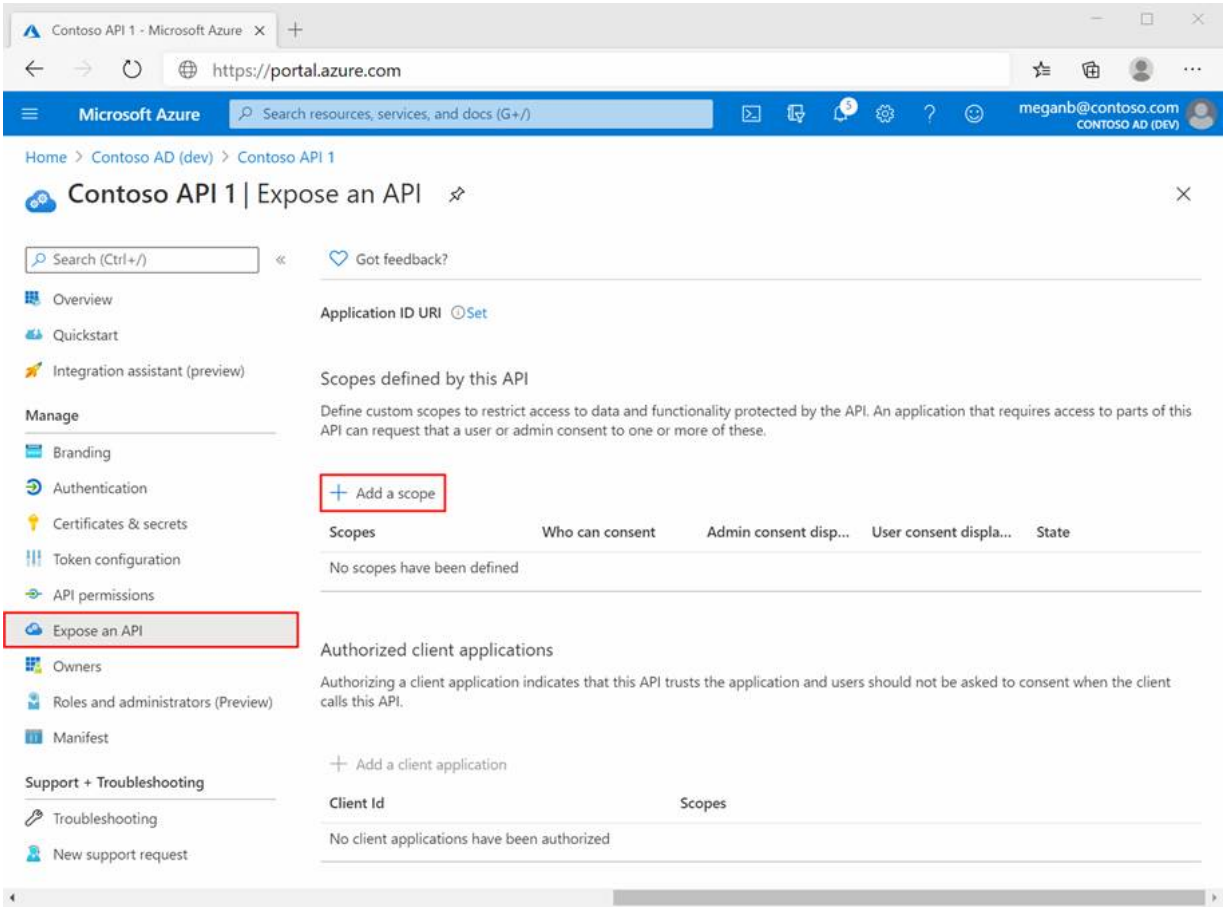
With your web API registered, you're ready to add the scopes that your API's code can use to provide granular permission to consumers of your API.

24.8 Add a scope

The code in a client application requests permission to perform operations defined by your web API by passing an access token along with its requests to the protected resource (the web API). Your web API then performs the requested operation only if the access token it receives contains the scopes (also known as application permissions) required for the operation.

First, follow these steps to create an example scope named Employees.Read.All:

1. Sign in to the Azure portal.
2. If you have access to multiple tenants, use the **Directory + subscription** filter in the top menu to select the tenant containing your client app's registration.
3. Select **Azure Active Directory** > **App registrations**, and then select your API's app registration.
4. Select **Expose an API** > **Add a scope**.



5. You're prompted to set an **Application ID URI** if you haven't yet configured one. The App ID URI acts as the prefix for the scopes you'll reference in your API's code, and it must be globally unique. You can use the default value provided, which is in the form api://<application-client-id>, or specify a more readable URI like `https://contoso.com/api`.
6. Next, specify the scope's attributes in the **Add a scope pane**. For this walk-through, you can use the example values or specify your own.

Field	Description
Scope name	The name of your scope. A common scope naming convention is resource.operation.constrai
Who can consent	Whether this scope can be consented to by users or if admin consent is required. Select Adr
Admin consent display name	A short description of the scope's purpose that only admins will see.
Admin consent description	A more detailed description of the permission granted by the scope that only admins will se
User consent display name	A short description of the scope's purpose. Shown to users only if you set Who can consent

Field	Description
User consent description	A more detailed description of the permission granted by the scope. Shown to users only if

7. Set the **State** to **Enabled**, and then select **Add scope**.
8. (Optional) To suppress prompting for consent by users of your app to the scopes you've defined, you can *pre-authorize* the client application to access your web API. Pre-authorize *only* those client applications you trust since your users won't have the opportunity to decline consent.
    1. Under **Authorized client applications**, select **Add a client application.**
    2. Enter the **Application (client) ID** of the client application you want to pre-authorize. For example, that of a web application you've previously registered.
    3. Under **Authorized scopes**, select the scopes for which you want to suppress consent prompting, then select **Add application**.
    4. If you followed this optional step, the client app is now a pre-authorized client app (PCA), and users won't be prompted for their consent when signing into it.

24.9 Add a scope requiring admin consent

Next, add another example scope named Employees.Write.All that only admins can consent to. Scopes that require admin consent are typically used for providing access to higher-privileged operations, often by client applications that run as backend services or daemons that don't sign in a user interactively.

1. To add the Employees.Write.All example scope, follow the steps above and specify these values in the **Add a scope** pane:

Field	Example value
Scope name	Employees.Write.All
Who can consent	Admins only
Admin consent display name	Write access to employee records
Admin consent description	Allow the application to have write access to all employee data.
User consent display name	None (leave empty)
User consent description	None (leave empty)

24.10 Verify the exposed scopes

If you successfully added both example scopes described in the previous sections, they'll appear in the **Expose an API** pane of your web API's app registration, similar to this image:

As shown in the image, a scope's full string is the concatenation of your web API's **Application ID URI** and the scope's **Scope name**.

For example, if your web API's application ID URI is `https://contoso.com/api` and the scope name is Employees.Read.All, the full scope is:

```
https://contoso.com/api/Employees.Read.All
```

24.11 Using the exposed scopes

Next, you will configure a client app's registration with access to your web API and the scopes you defined by following the steps above.

Once a client app registration is granted permission to access your web API, the client can be issued an OAuth 2.0 access token by the Microsoft identity platform. When the client calls the web API, it presents an access token whose scope (scp) claim is set to the permissions you've specified in the client's app registration.

24.12 You can expose additional scopes later as necessary. Consider that your web API can expose multiple scopes associated with several operations. Your resource can control access to the web API at runtime by evaluating the scope (scp) claim(s) in the OAuth 2.0 access token it receives.

24.13 lab: title: '23 - Grant tenant-wide admin consent to an application' learning path: '03' module: 'Module 03 - Implement app registrations'

25 Lab 23: Grant tenant-wide admin consent to an application

25.1 Lab scenario

For applications your organization has developed or for those that are registered directly in your Azure AD tenant, you can grant tenant-wide admin consent from App registrations in the Azure portal.

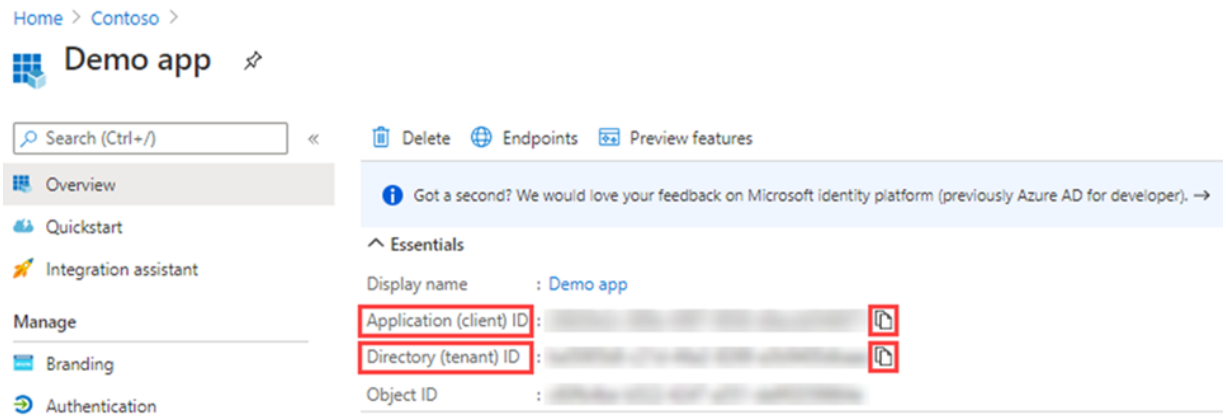
25.1.0.1 Estimated time: 10 minutes

25.2 Grant admin consent in App registrations

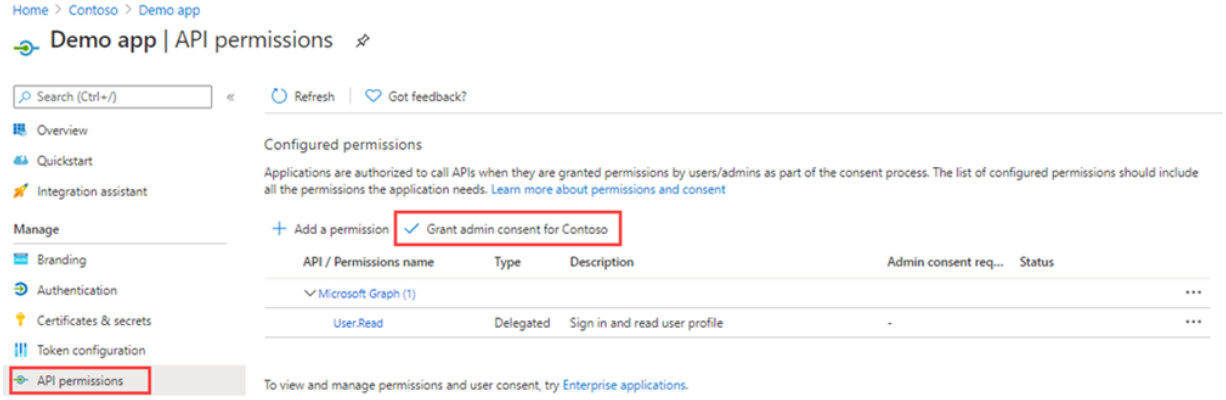
> [!WARNING] Warning Granting tenant-wide admin consent to an application will grant the app and the app's publisher access to your organization's data. Carefully review the permissions the application is requesting before granting consent.

The Global Administrator role is required in order to provide admin consent for application permissions to the Microsoft Graph API.

1. In a previous exercise, you created an app named Demo app. If necessary, in Microsoft Azure, browse to **Azure Active Directory > App registrations > Demo app.**
2. On the **Demo app** blade, locate and copy and save each **Application (client) ID** and **Directory (tenant) ID** values so that you can use them later.



3. In the left navigation, under **Manage**, select **API permissions**.
4. Under **Configured permissions**, select **Grant admin consent**.



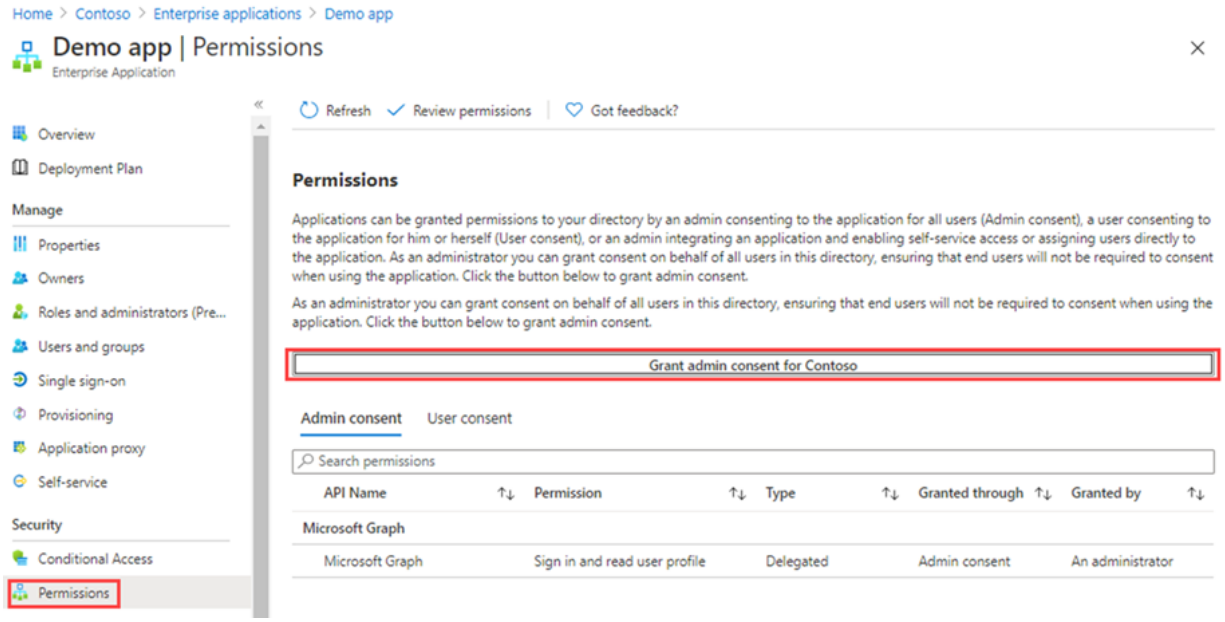
5. Review the dialogue box, and then select **Yes.**

   [!WARNING] Warning Granting tenant-wide admin consent through App registrations will revoke any permissions that had previously been granted tenant-wide. Permissions previously granted by users on their own behalf will not be affected.

25.3 Grant admin consent in Enterprise apps

You can grant tenant-wide admin consent through Enterprise applications if the application has already been provisioned in your tenant.

1. In Microsoft Azure, browse to **Azure Active Directory > Enterprise applications > Demo app.**
2. On the **Demo app** blade, in the left navigation, under **Security,** select **Permissions.**
3. Under **Permissions,** select **Grant admin consent.**



   [!WARNING] Warning Granting tenant-wide admin consent through App registrations will revoke any permissions that had previously been granted tenant-wide. Permissions previously granted by users on their own behalf will not be affected.

4. When prompted, sign in using your Global Administrator account.
5. In the **Permissions requested** dialog box, review the information and then select **Accept**.

25.4 lab: title: '24 - Add app roles to your app and receive them in the token' learning path: '03' module: 'Module 03 - Implement app registrations'

26 Lab 24: Add app roles to your app and receive them in the token

26.1 Lab scenario

Role-based access control (RBAC) is a popular mechanism to enforce authorization in applications. When using RBAC, an administrator grants permissions to roles, and not to individual users or groups. The administrator can then assign roles to different users and groups to control who has access to what content and functionality. You plan to implement RBAC roles and need to verify you understand how to perform the procedure.

26.1.0.1 Estimated time: 10 minutes

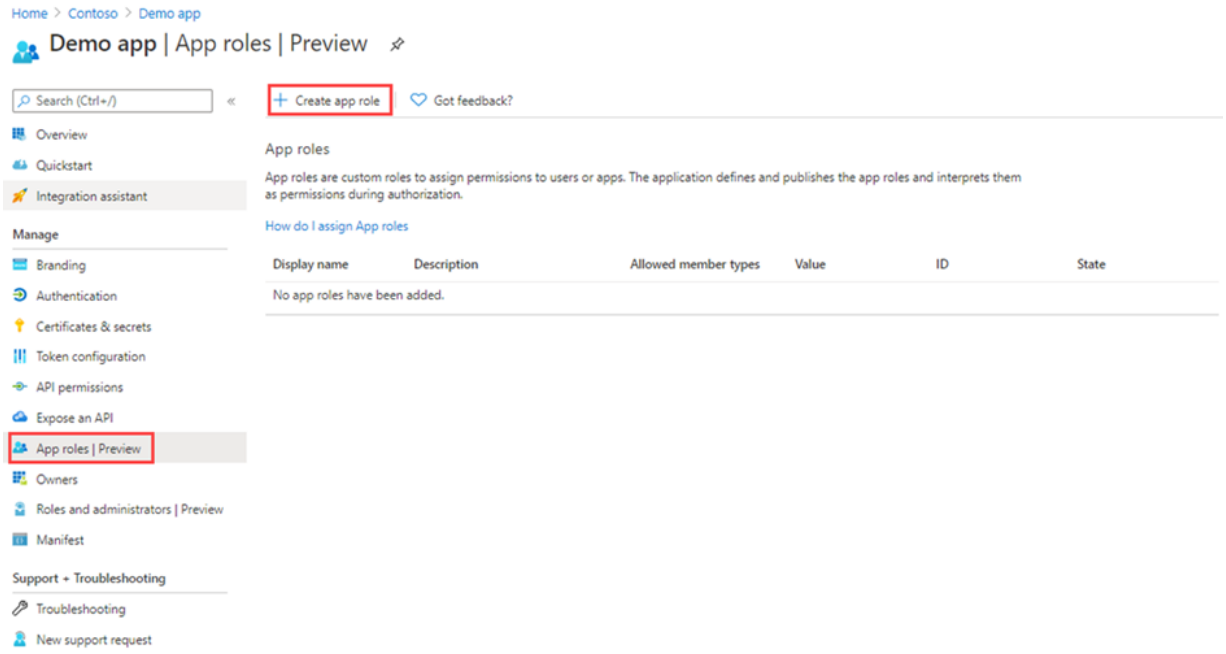
26.2 Declare app roles using the App roles UI

[!IMPORTANT] The app roles portal UI feature is in public preview. This preview is provided without a service-level agreement and isn't recommended for production workloads. Certain features

might be unsupported or have constrained capabilities.

To create an app role by using the Azure portal's user interface:

1. Sign in to https://portal.azure.com using a Global Administrator account.
2. Open the portal menu and then select **Azure Active Directory**.
3. On the **Azure Active Directory** blade, under **Manage,** select **App registrations**.
4. Select **App roles | Preview**, and then select **Create app role**.



5. In the **Create app role** pane, in the **Display name** box, enter **Survey Writer**.
6. Under **Allow member types**, select **User/Groups**.
7. In the **Value** box, enter **Survey.Create**.
8. In the **Description** box, enter **Writers can create surveys**.
9. Notice that the description is a mandatory field.
10. Verify the **Do you want to enable this app role** is selected and then select **Apply.**

26.3 Assign users and groups to roles

Once you've added app roles in your application, you can assign users and groups to the roles. Assign users and groups to roles through the portal's UI or programmatically using https://docs.microsoft.com/graph/api/user-post-approleassignments. When the users assigned to the various app roles sign in to the application, their tokens will have their assigned roles in the roles claim.

To assign users and groups to roles by using the Azure portal:

1. Sign in to [https:portal.azure.com] (https:portal.azure.com).
2. In Azure Active Directory, in the navigation menu on the left, select **Enterprise applications.**
3. In the **All applications** list, select **Demo app**.
4. This app was created in an earlier exercise.
5. Under **Manage**, select **Users and groups.**
6. On the menu, select **+ Add user/group.**
7. On the **Add Assignment** blade, select **Users and groups**.
8. A list of users and security groups is displayed. You can search for a certain user or group, as well as select multiple users and groups that appear in the list.

9. After you have selected users and groups, select **Select**.
10. When using the **Select a role** assignment, all the roles that you've defined for the application are displayed.
11. Choose a role and then select **Select**.
12. Select **Assign** to finish the assignment of users and groups to the app.
13. Confirm that the users and groups you added appear in the **Users and groups** list.

26.4 lab: title: '25 - Create and manage a catalog of resources in Azure AD entitlement management' learning path: '04' module: 'Module 01 - Plan and implement entitlement management'

27 Lab 25: Create and manage a catalog of resources in Azure AD entitlement management

27.1 Lab scenario

A catalog is a container of resources and access packages. You create a catalog when you want to group related resources and access packages. Whoever creates the catalog becomes the first catalog owner. A catalog owner can add additional catalog owners. You must create and configure a catalog in your organization.

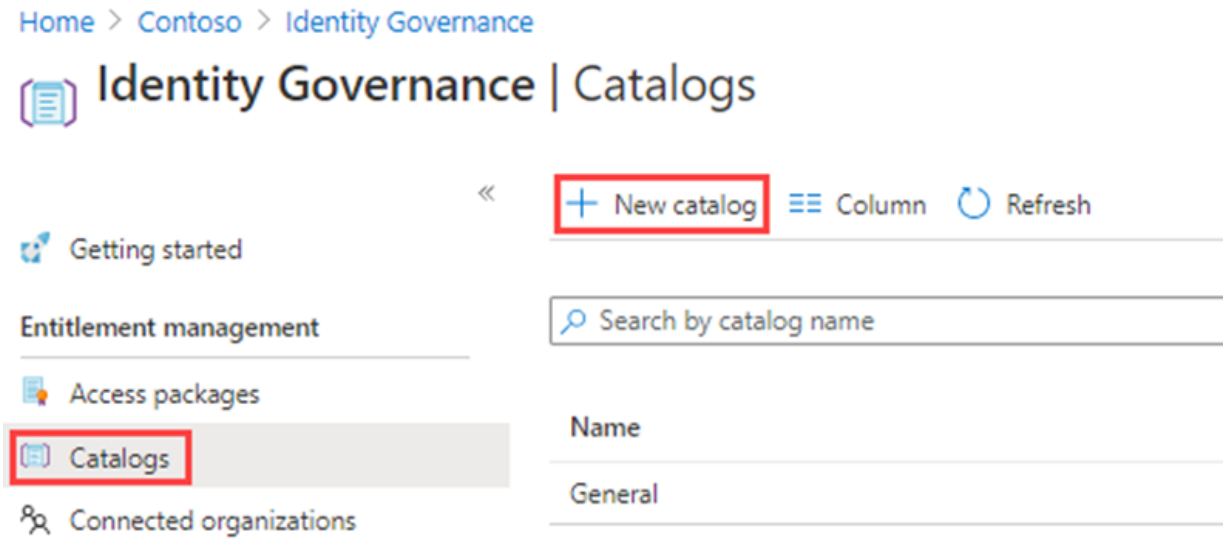
27.1.0.1 Estimated time: 15 minutes

27.2 Create a catalog

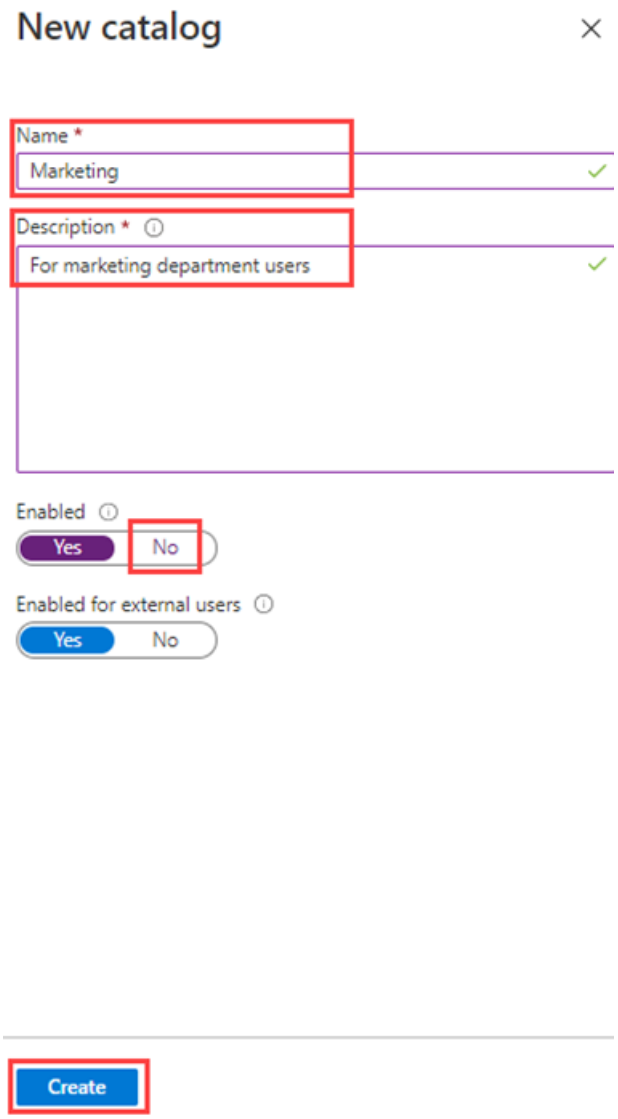
1. Sign in to https://portal.azure.com using a Global Administrator account.

   Important To use and configure Azure AD terms of use, you must have:

   - Azure AD Premium P1, P2, EMS E3, or EMS E5 subscription.
   - If you don't have one of these subscriptions, you can get Azure AD Premium or enable Azure AD Premium trial.
   - One of the following administrator accounts for the directory you want to configure:
     - Global Administrator
     - Security Administrator
     - Conditional Access Administrator
2. Open **Azure Active Directory** and the select **Identity Governance**.
3. In the left menu, under **Entitlement management**, select **Catalogs**.
4. On the top menu, select **+New Catalog**.



5. In the New catalog pane, in the **Name** box, enter **Marketing**.
6. In the **Description** box, enter **For marketing department users**. Users will see this information in an access package's details.
7. **Enabled for external users** allows users in selected external directories to be able to request access packages in this catalog. No changes will be made to this setting.
8. Under **Enabled, select No**.
9. You may choose to enable the catalog for immediate use or disable if you intend to stage it or keep it unavailable until you intend to use it. For this exercise, the catalog does not need to be enabled.



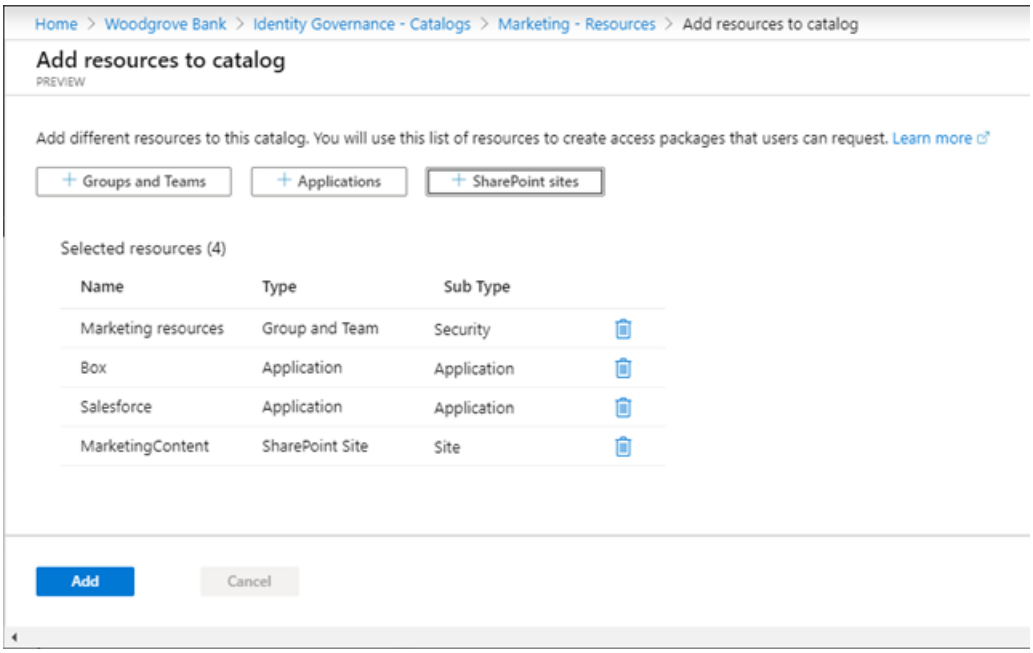
10. Select Create.

27.3 Add resources to a catalog

To include resources in an access package, the resources must exist in a catalog. The types of resources you can add are groups, applications, and SharePoint Online sites. The groups can be cloud-created Microsoft 365 Groups or cloud-created Azure AD security groups. The applications can be Azure AD enterprise applications, including both SaaS applications and your own applications federated to Azure AD. The sites can be SharePoint Online sites or SharePoint Online site collections.

1. On the Identity Governance blade, if necessary, select **Catalogs**.
2. In the **Catalogs** list, select **Marketing**.
3. In the left navigation, under **Manage**, select **Resources**.

4. On the menu, select + **Add resources**.
5. In the Add resources to catalog blade, review the available options.
6. You may not have any resources in Groups and Teams, Applications, or SharePoint sites. Select any resource category and then select a resource from that category.
7. For this exercise, it is okay to choose any resource you may have available.

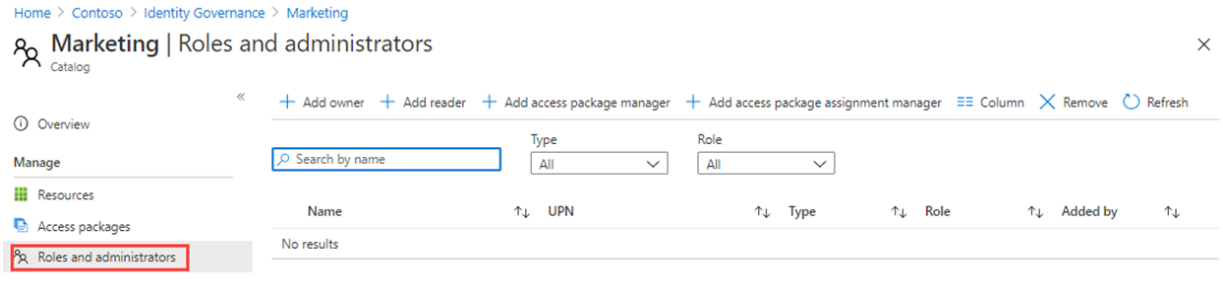


8. When finished, click **Add**. These resources can now be included in access packages within the catalog.

27.4 Add additional catalog owners

The user that created a catalog becomes the first catalog owner. To delegate management of a catalog, you add users to the catalog owner role. This helps share the catalog management responsibilities.

1. In the Marketing catalog blade, in the left navigation menu, select Roles and administrators.
2. If necessary, in the Azure portal, browse to **Azure Active Directory** > **Identity Governance** > **Catalogs** and then select **Marketing**.



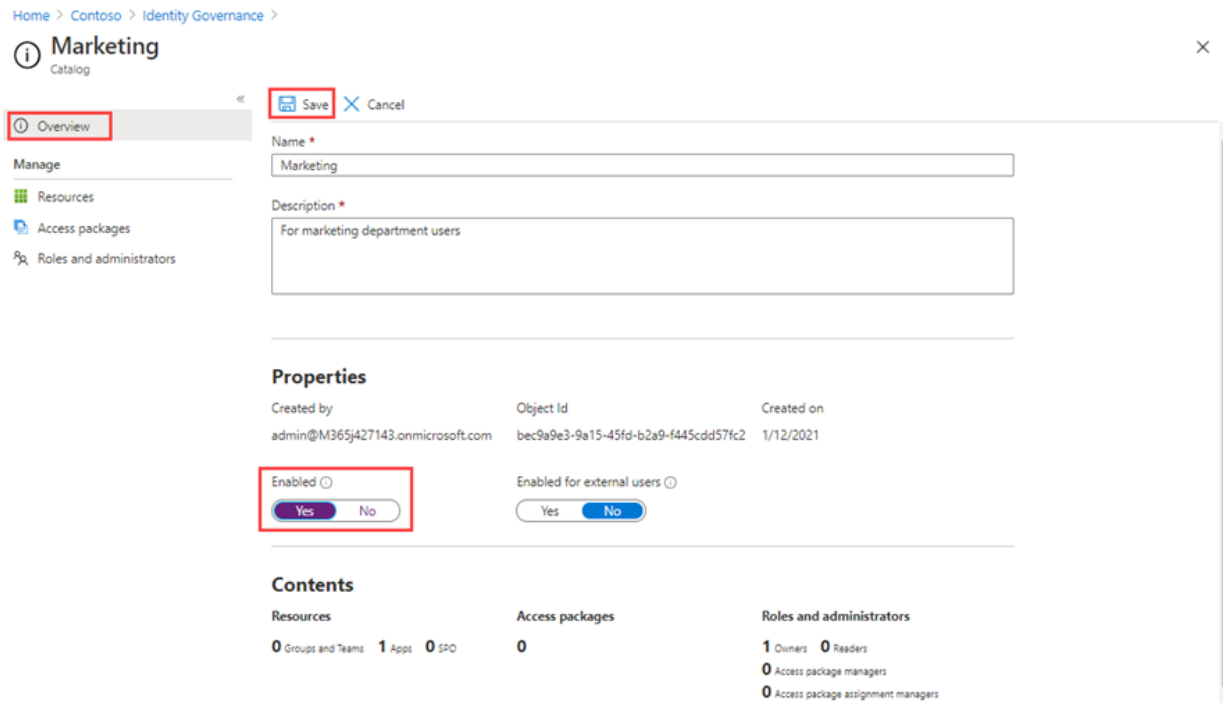
3. On the top menu, review the available roles and then select + **Add owner**.
4. In the Select members pane, select your administrator account and then select **Select**.
5. Review the newly added role in the Roles and administrators list.

27.5 Edit a catalog

You can edit the name and description for a catalog. Users see this information in an access package's details.

1. In the Marketing blade, in the left navigation, select **Overview**.
2. On the top menu, select **Edit**.

3. Review the setting and, under **Properties** > **Enabled**, select **Yes**.



4. Select **Save**.

27.6 Delete a catalog

You can delete a catalog, but only if it does not have any access packages.

1. In the Marketing catalog's Overview page, on the top menu, select Delete.
2. In the Delete dialog box, review the information and then select **Yes**.

27.7 lab: title: '26 - Add terms of use and acceptance reporting' learning path: '04' module: 'Module 01 - Plan and implement entitlement management'

28 Lab 26: Add terms of use and acceptance reporting

28.1 Lab scenario

Azure AD terms of use policies provide a simple method that organizations can use to present information to end users. This presentation ensures users see relevant disclaimers for legal or compliance requirements. This article describes how to get started with terms of use (ToU) policies.

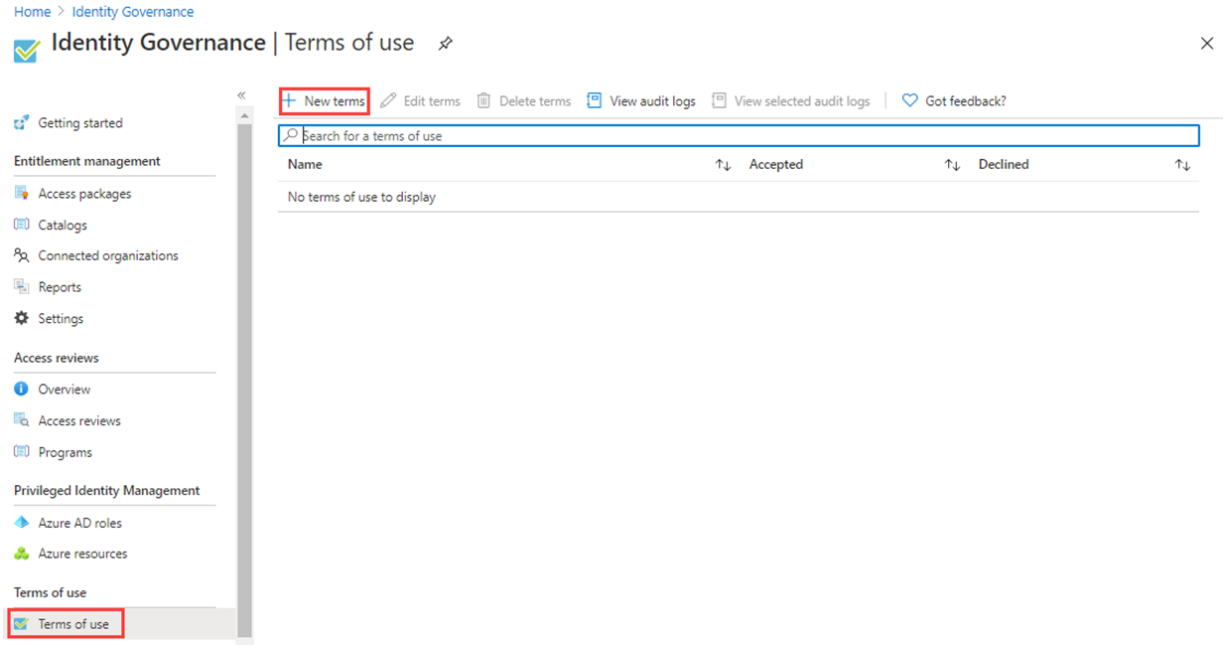
You must create and enforce a ToU policy for your organization.

28.1.0.1 Estimated time: 20 minutes

28.2 Add terms of use

Once you have finalized your terms of use document, use the following procedure to add it.

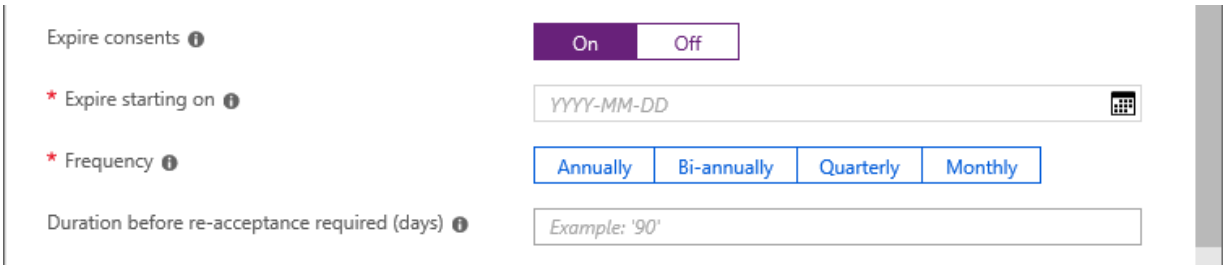
1. Sign in to https://portal.azure.com using a Global Administrator account.
2. Open **Azure Active Directory** and the select **Identity Governance**.
3. In the left navigation menu, under **Terms of use**, select **Terms of use**.
4. On the Terms of use page, on the top menu, select + **New terms**



5. In the **Name** box, enter **Testing terms of use**.
6. This is the terms of use that will be used in the Azure portal.
7. In the **Display name** box, enter **Contoso Terms of Use**.
8. This is the title that users see when they sign in.
9. Select the **Terms of use document box**, browse to your finalized terms of use PDF and select it.
10. For this exercise you can choose any PDF you may have or, using Microsoft Word, create a simple terms of use doc and then print to PDF.
11. Select the language for your terms of use document.
12. The language option allows you to upload multiple terms of use, each with a different language. The version of the terms of use that an end user will see will be based on their browser preferences.
13. To require end users to view the terms of use prior to accepting them, set **Require users to expand the terms of use** to **On**.
14. To require end users to accept your terms of use on every device they are accessing from, set **Require users to consent on every device** to **On**. Users may be required to install additional applications if this option is enabled.

    [!Warning]
    Consent on every device will require users to register each device with Azure AD prior to getting access.

15. If you want to expire terms of use consents on a schedule, set **Expire consents** to **On**. When set to On, two additional schedule settings are displayed.



16. Use the **Expire starting on** and **Frequency** settings to specify the schedule for terms of use expirations. The following table shows the result for a couple of example settings:

Expire starting on	Frequency	Result
Today's date	Monthly	Starting today, users must accept the terms of use and then reaccept every month.
Date in the future	Monthly	Starting today, users must accept the terms of use. When the future date occurs, consent

For example, if you set the expire starting on date to **Jan 1** and frequency to **Monthly**, here is how expirations might occur for two users:

User	First accept date	First expire date	Second expire date	Third expire date
Alice	Jan 1	Feb 1	Mar 1	Apr 1
Bob	Jan 15	Feb 1	Mar 1	Apr 1

17. Use the **Duration before re-acceptance requires (days)** setting to specify the number of days before the user must reaccept the terms of use. This allows users to follow their own schedule. For example, if you set the duration to **30** days, here is how expirations might occur for two users:

User	First accept date	First expire date	Second expire date	Third expire date
Alice	Jan 1	Jan 31	Mar 2	Apr 1
Bob	Jan 15	Feb 14	Mar 16	Apr 15

[!Note]
It is possible to use the Expire consents and Duration before re-acceptance requires (days) settings together, but typically you use one or the other.

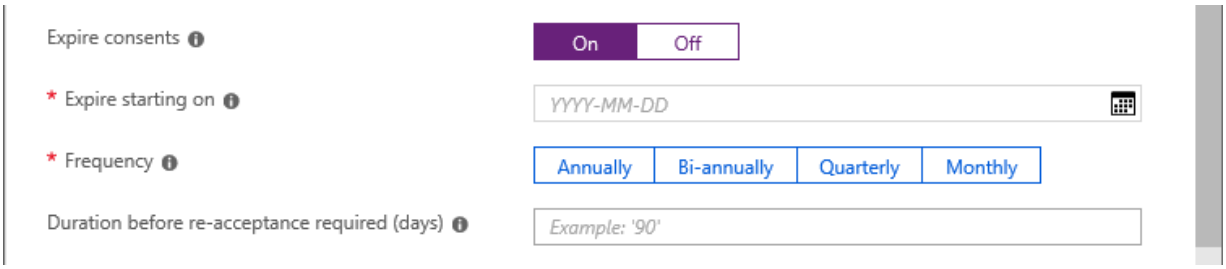
18. Under **Conditional Access**, select **Custom policy**.

Template	Description
Access to cloud apps for all guests	A Conditional Access policy will be created for all guests and all cloud apps.
Access to cloud apps for all users	A Conditional Access policy will be created for all users and all cloud apps.
Custom policy	Select the users, groups, and apps that this terms of use will be applied to.
Create Conditional Access policy later	This terms of use will appear in the grant control list when creating a Condi

[!IMPORTANT]
Conditional Access policy controls (including terms of use) do not support enforcement on service accounts. We recommend excluding all service accounts from the Conditional Access policy.

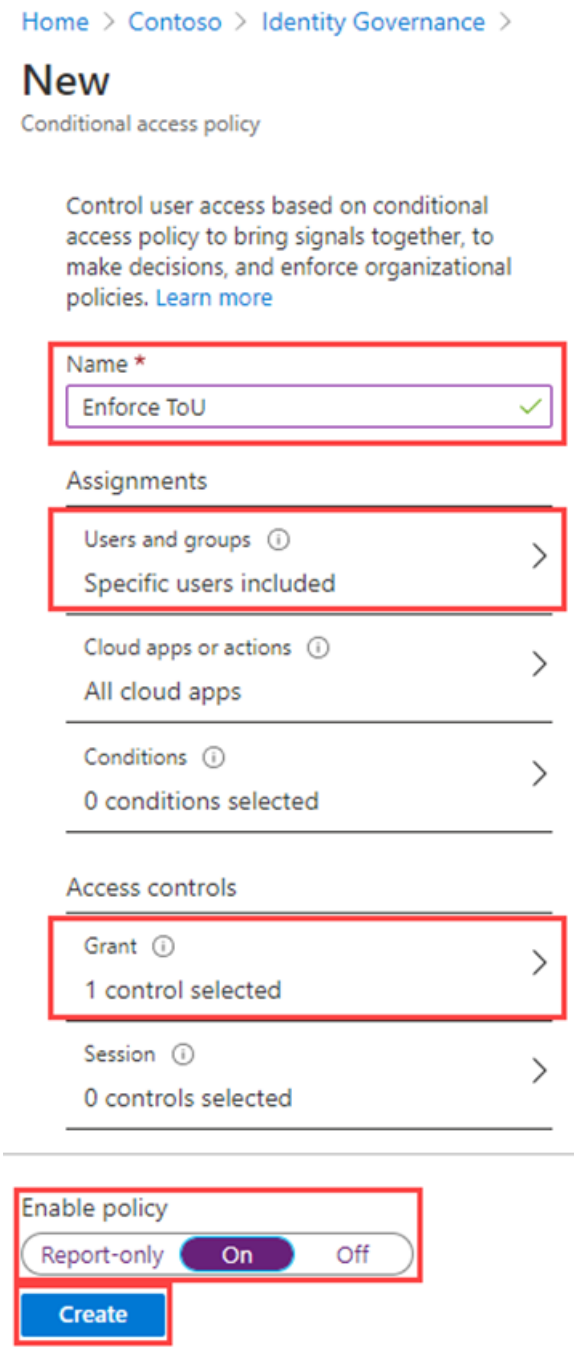
Custom Conditional Access policies enable granular terms of use, down to a specific cloud application or group of users. For more information, see https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/require-tou.

19. When complete, select **Create**.



20. When the terms of use is created, you will automatically be redirected to the Conditional access policy page. On the page, in the **Name** box, enter **Enforce ToU**.
21. Under **Assignments**, select **Users and groups**.
22. On the include tab, select **Users and groups** check box.
23. In the Select pane, select an account you would like to use to test the terms of use policy.

24. If you choose your administrator account, like all conditional access policies, be sure you have another account with enough permissions to change the conditional access policy. This is to ensure your administrator account will not be locked out should the conditional access policy result in an undesirable outcome.
25. Select **Cloud apps or actions.**
26. Select **All cloud apps**.
27. Under **Access controls**, select **Grant**.
28. In the Grant pane, select **Testing terms of use** and then select **Select**.
29. Under **Enable policy**, select **On**.
30. When complete, select **Create**.

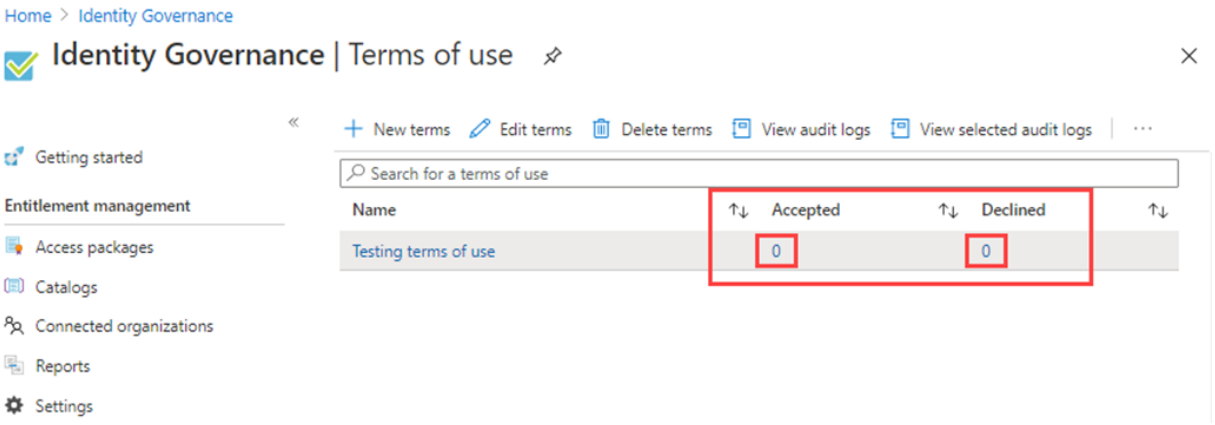


31. If you chose to use your own account, you can refresh your browser. You will be prompted to sign in again. When you sign in, you will be required to accept the terms of use.

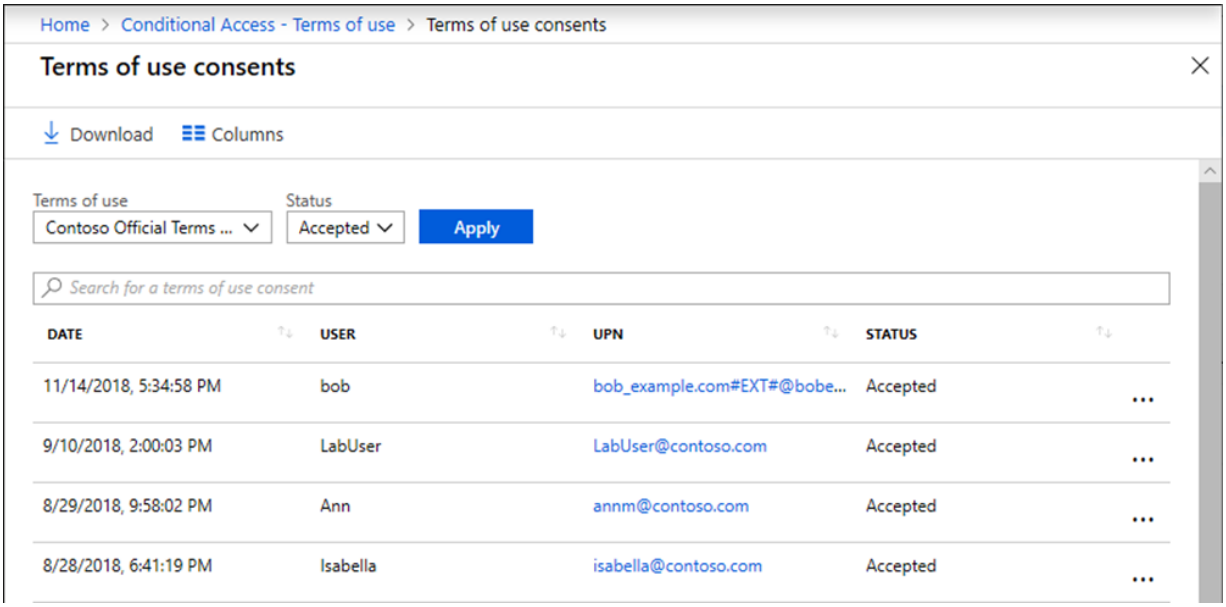
28.3 View report of who has accepted and declined

The Terms of use blade shows a count of the users who have accepted and declined. These counts and who accepted/declined are stored for the life of the terms of use.

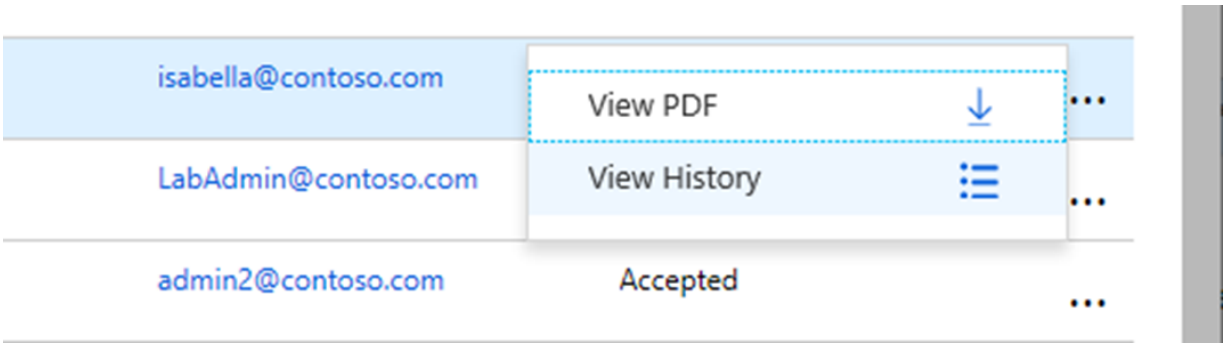
1. In Microsoft Azure, in **Identity Governance > Terms of use**, locate your terms of use.
2. For a terms of use, select the numbers under **Accepted** or **Declined** to view the current state for users.



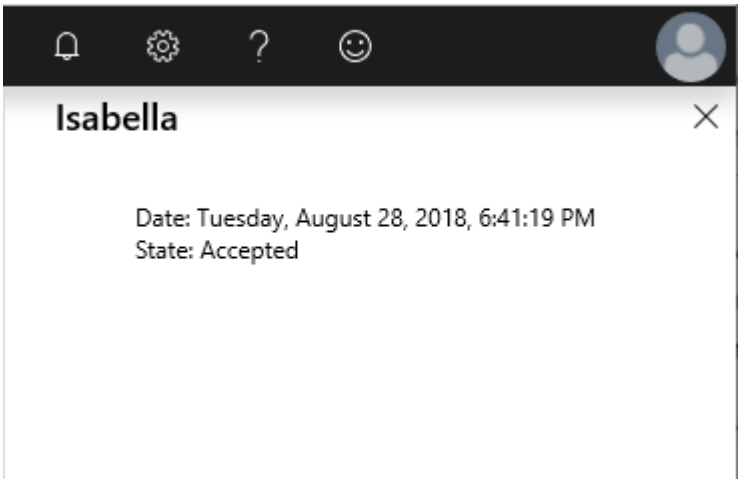
3. In this exercise you may not have any accepted or declined terms of use. In the following example, the **Accepted** value was selected. You can see the reported user information for those that have accepted the terms of use.



4. To view the history for an individual user, select the ellipsis to the right of the user name and then **View History**.

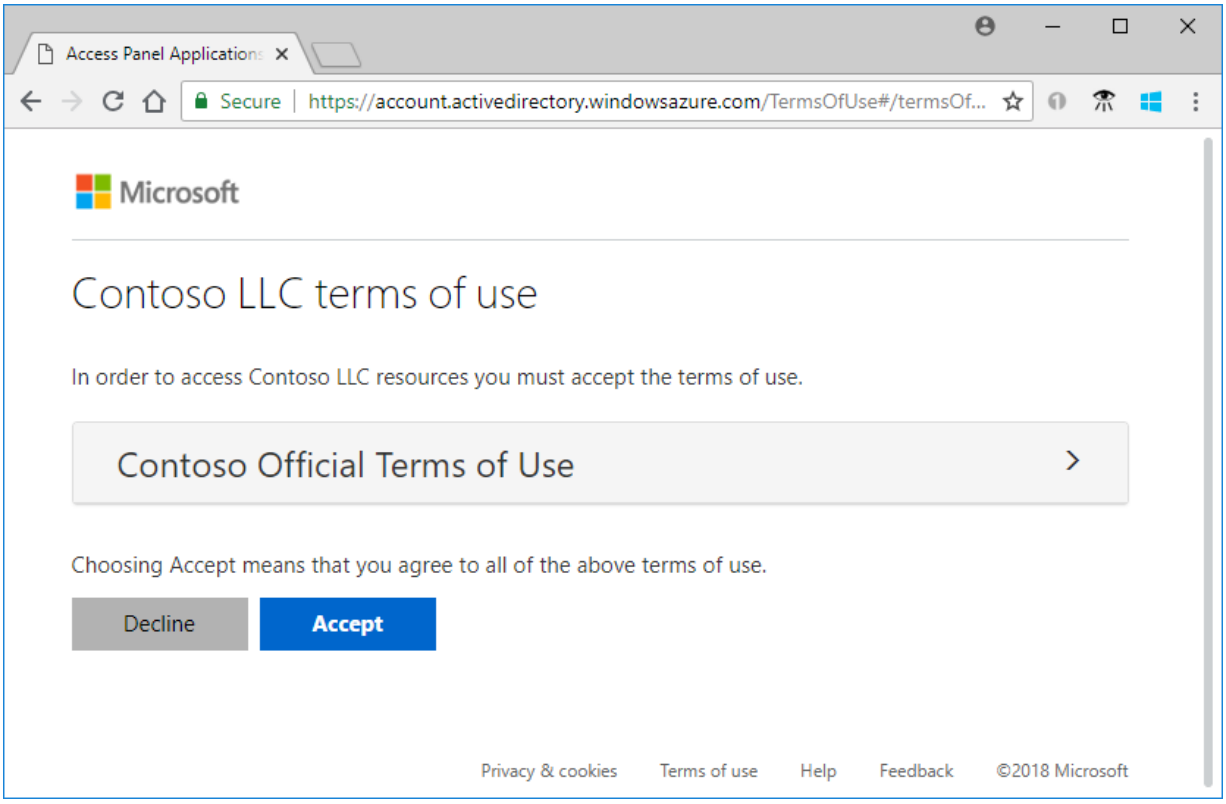


5. In the view history pane, you see a history of all the accepts, declines, and expirations.

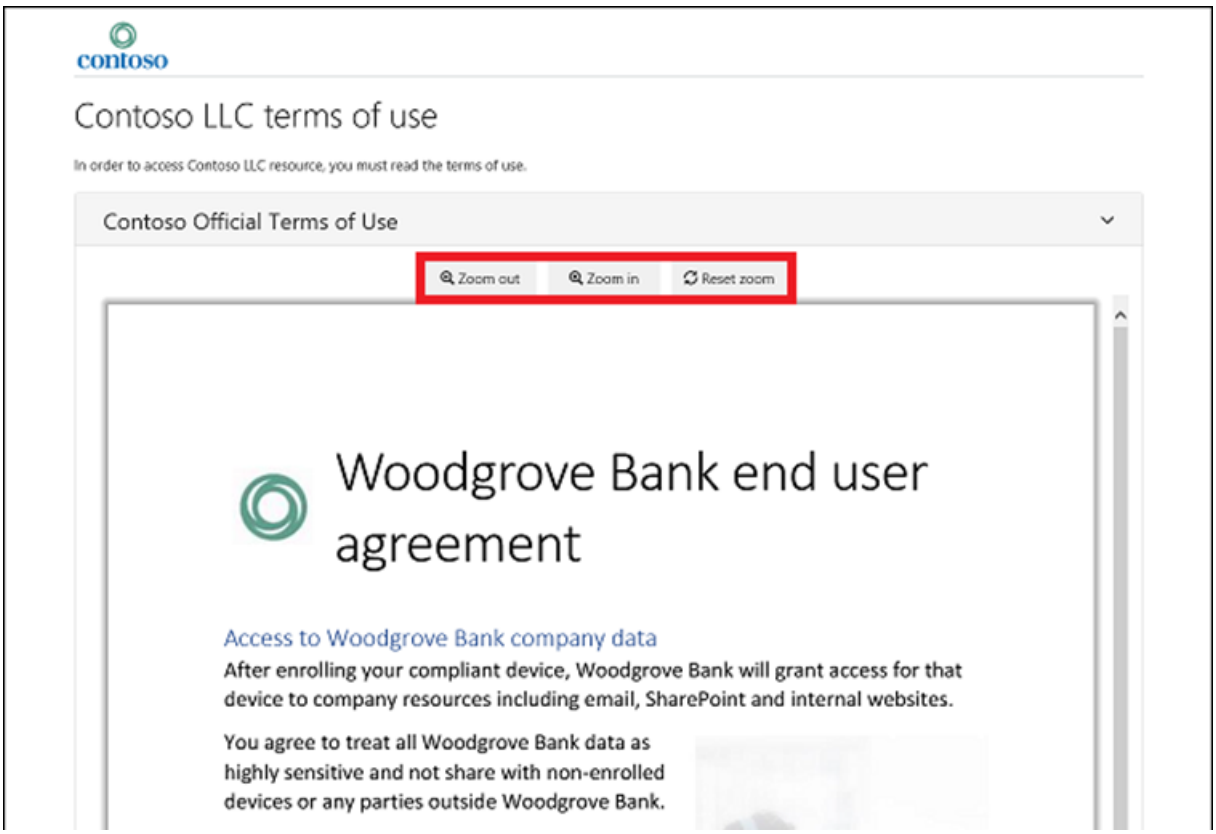


28.4 What terms of use looks like for users

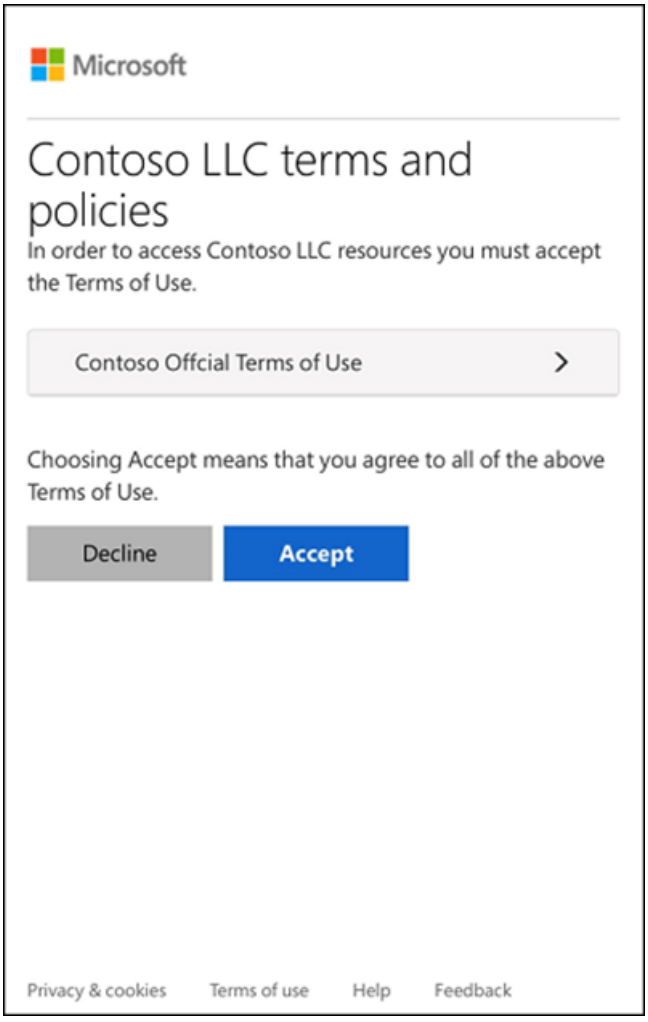
1. Once a terms of use is created and enforced, users who are in scope will see the terms of use page.



2. Users can view the terms of use and, if necessary, use buttons to zoom in and out.



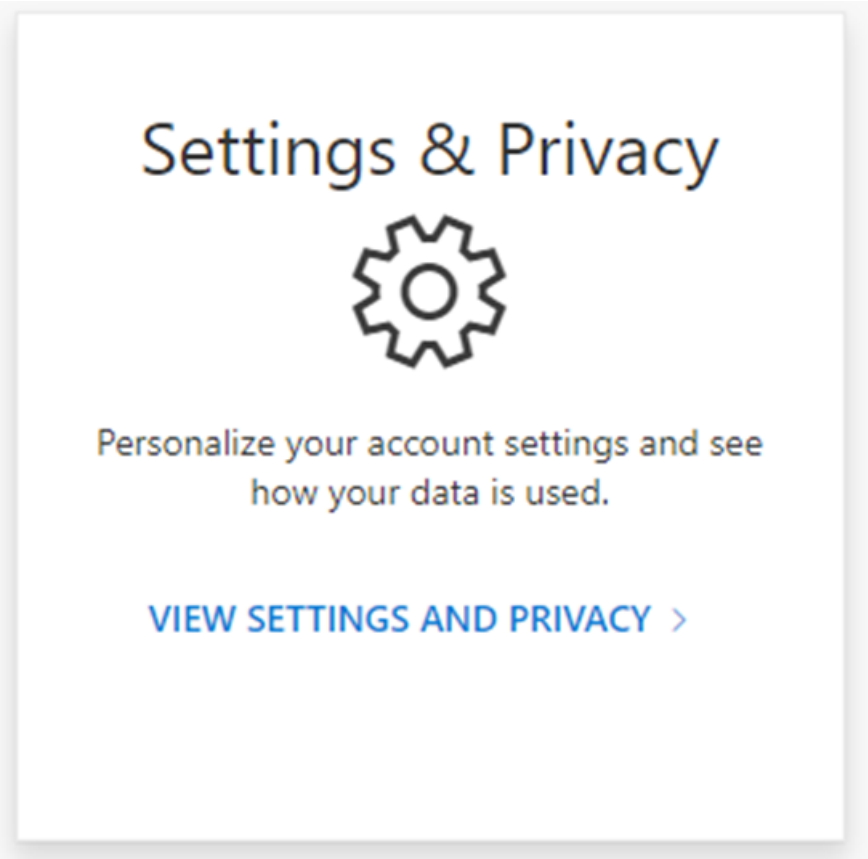
3. On mobile devices, the terms of use will be displayed similar to the following example.



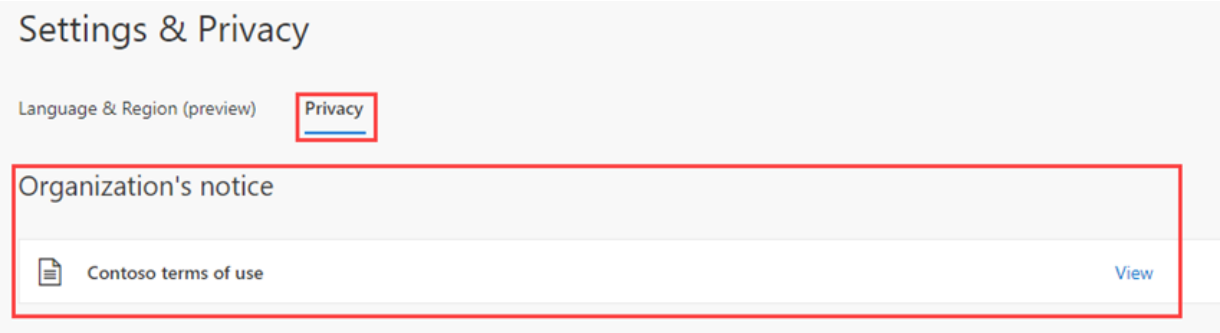
28.4.1 How users can review their terms of use

Users can review and see the terms of use that they have accepted by using the following procedure.

1. Browse to https://myapps.microsoft.com and then sign in using your user account.
2. On the Overview page, select VIEW SETTINGS AND PRIVACY.



3. On the Settings & Privacy page, select the **Privacy** tab.



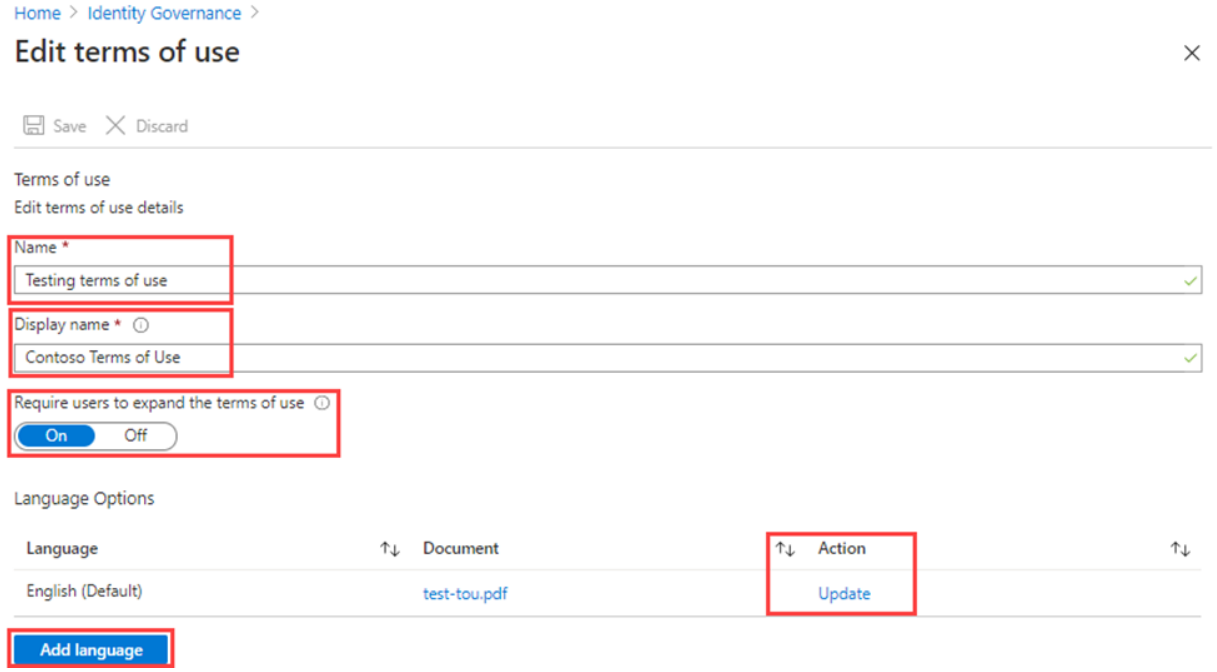
4. Under **Organization's notice**, you can review the terms of use you have accepted.

28.5 Edit terms of use details

You can edit some details of terms of use, but you can't modify an existing document. The following procedure describes how to edit the details.

1. Sign in to the https://portal.azure.com as a Global administrator.
2. Open Azure Active Directory and the select **Identity Governance**.
3. In the left navigation menu, under **Terms of use**, select **Terms of use**.
4. Select the terms of use you want to edit.
5. On the top menu, select **Edit terms**.

6. In the Edit terms of use pane, you can change the following:
    - **Name** – this is the internal name of the ToU that is not shared with end users
    - **Display name** – this is the name that end users can see when viewing the ToU
    - **Require users to expand the terms of use** – Setting this to **On** will force the end use to expand the terms of use document before accepting it.
    - **Update an existing terms of use** document.
    - You can add a language to an existing ToU If there are other settings you would like to change, such as require users to consent on every device, expire consents, duration before reacceptance, or Conditional Access policy, you must create a new terms of use.

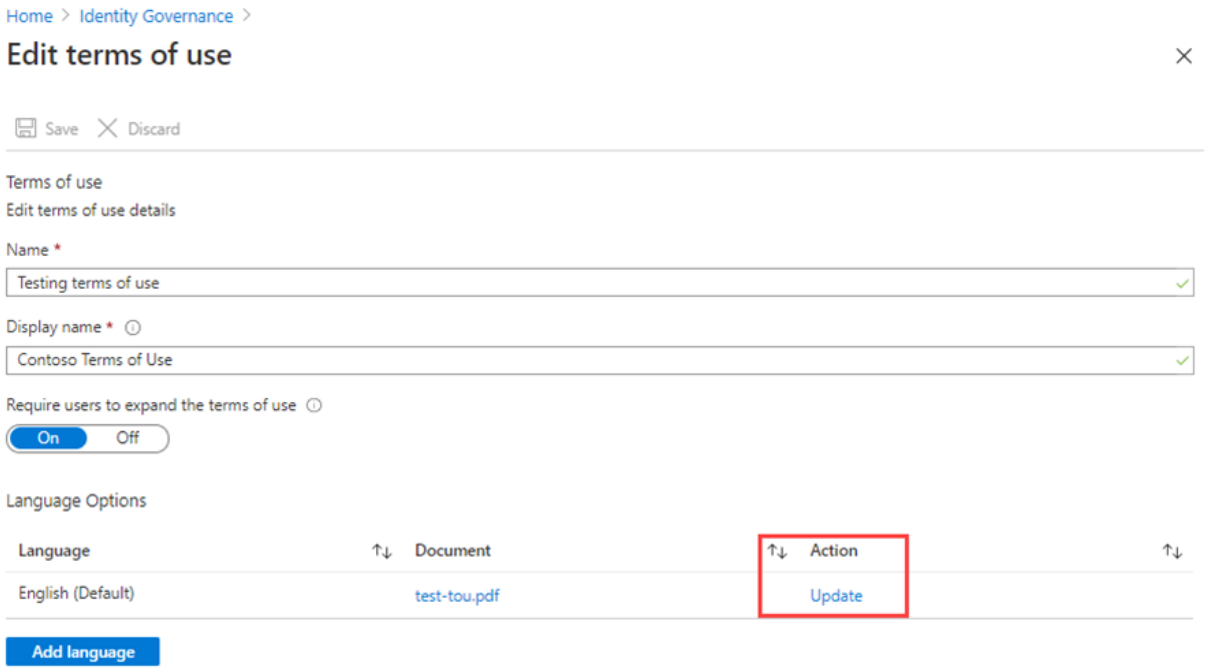


7. Once you are done, select **Save** to save your changes.

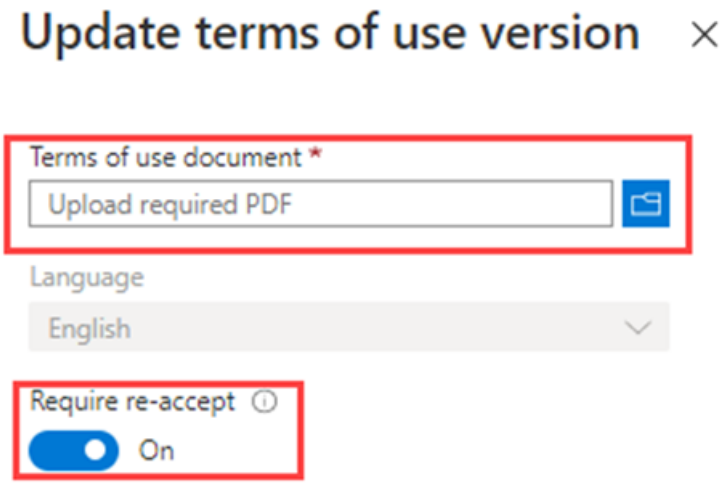
28.6 Update an existing terms of use document

You may, on occasion, be required to update the terms of use document.

1. Select the terms of use you want to edit.
2. Select **Edit terms**.
3. In the **Language Options** table, identify the terms of use language you want to update and then, in the **Action** column, select **Update**.



4. In the Update terms of use version pane, you can upload a new version of your terms of use document.
5. Additionally, you can use the **Require reaccept** toggle button if you want to require your users to accept this new version the next time they sign in. If you do not require your users to re-accept, their previous consent will stay current and only new users who have not consented before or whose consent expires will see the new version.



6. Once you have uploaded your new pdf and decided on re-accept, select **Add**.
7. You will now see the most recent version under the Document column.

28.7 lab: title: '27 - Manage the lifecycle of external users in Azure AD Identity Governance settings' learning path: '04' module: 'Module 01 - Plan and implement entitlement management'

29 Lab 27: Manage the lifecycle of external users in Azure AD Identity Governance settings

29.1 Lab scenario

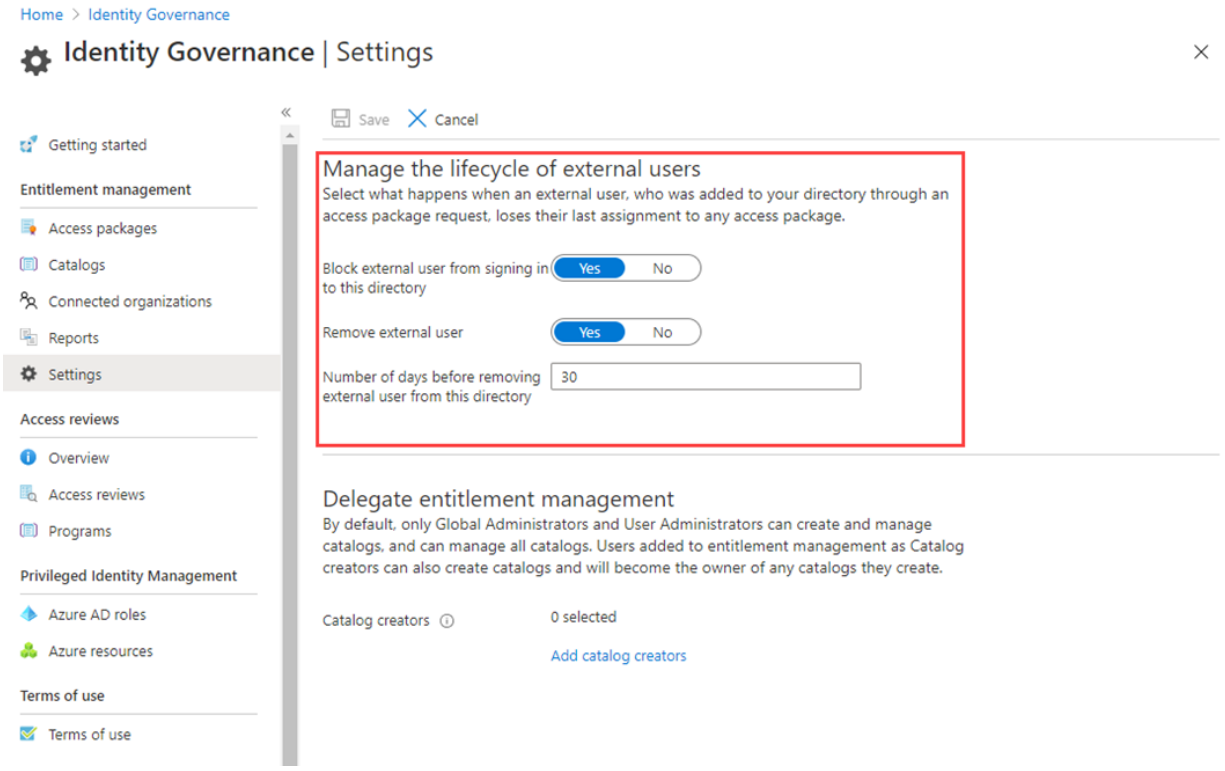
You can select what happens when an external user, who was invited to your directory through an access package request being approved, no longer has any access package assignments. This can happen if the user

relinquishes all their access package assignments, or their last access package assignment expires. By default, when an external user no longer has any access package assignments, they are blocked from signing in to your directory. After 30 days, their guest user account is removed from your directory.

29.1.0.1 Estimated time: 5 minutes

29.2 Manage the lifecycle of external users in Azure AD Identity Governance settings

1. Sign in to the https://portal.azure.com as a Global administrator.
2. An account with Global administrator or User administrator is required to complete these tasks.
3. Open Azure Active Directory and the select **Identity Governance**.
4. In the left navigation menu, under **Entitlement management**, select **Settings**.
5. On the top menu, select **Edit**.



6. In the **Manage the lifecycle of external users** section, review the different settings for external users.
7. When an external user loses their last assignment to any access packages, if you want to block them from signing in to this directory, set the **Block external user from signing in to this directory** to **Yes**.
8. If a user is blocked from signing in to the directory, the user will be unable to re-request the access package or request additional access in this directory. Do not configure blocking them from signing in if they will subsequently need to request access to other access packages.
9. Once an external user loses their last assignment to any access packages, if you want to remove their guest user account in this directory, set **Remove external** user to **Yes**.
10. Entitlement management only removes accounts that were invited through entitlement management. Also, note that a user will be blocked from signing in and removed from this directory even if that user was added to resources in this directory that were not access package assignments. If the guest was present in this directory prior to receiving access package assignments, they will remain. However, if the guest was invited through an access package assignment, and after being invited was also assigned to a OneDrive for Business or SharePoint Online site, they will still be removed.
11. If you want to remove the guest user account in this directory, you can set the number of days before it is removed. If you want to remove the guest user account as soon as they lose their last assignment to any access packages, set **Number of days before removing external user from this directory** to **0**.

12. If you've made any changes, select **Save**.

29.3 lab: title: '28 - Configure Privileged Identity Management for Azure AD roles' learning path: '04' module: 'Module 03 - Plan and implement privileged access'

30 Lab 28: Configure Privileged Identity Management for Azure AD roles

30.1 Lab scenario

A Privileged role administrator can customize Privileged Identity Management (PIM) in their Azure Active Directory (Azure AD) organization, including changing the experience for a user who is activating an eligible role assignment. You must become familiar with configuring PIM.

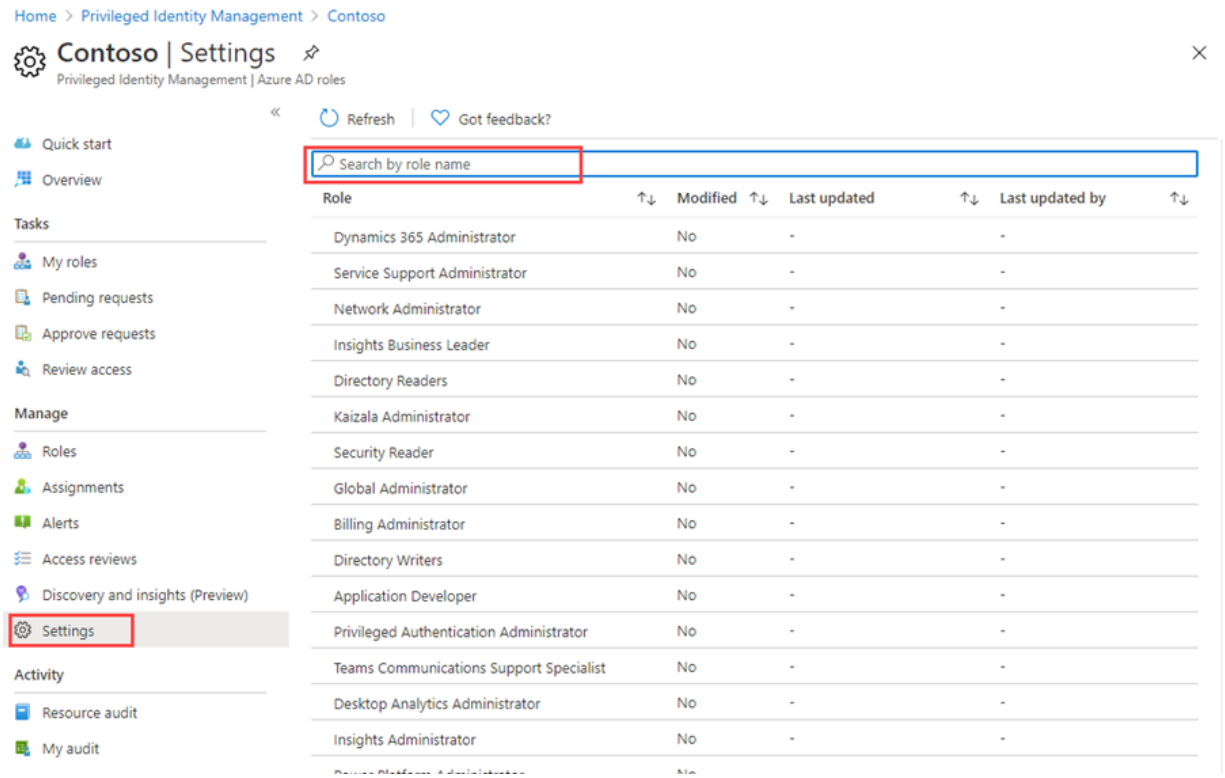
30.1.0.1 Estimated time: 15 minutes

30.2 Configure Azure AD role settings

30.2.1 Open role settings

Follow these steps to open the settings for an Azure AD role.

1. Sign in to the https://portal.azure.com as a Global administrator.
2. Search for and then select **Azure AD Privileged Identity Management.**
3. In the Privileged Identity Management blade, in the left navigation, select **Azure AD roles.**
4. On the Quick start page, in the left navigation, select **Settings.**

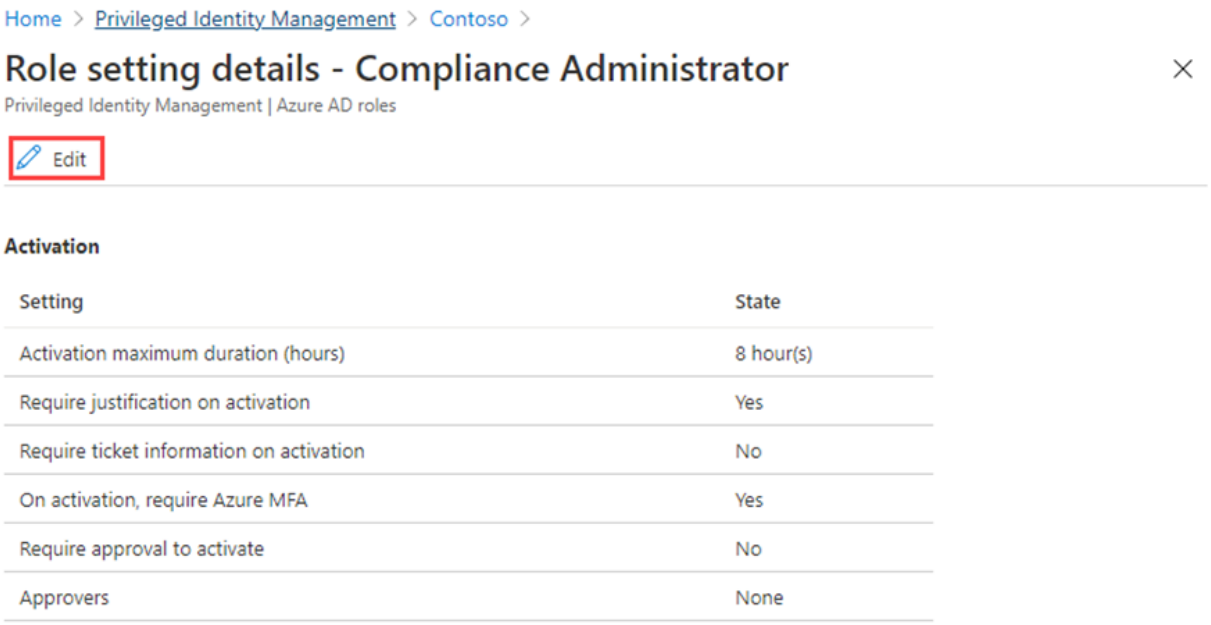


5. Review the list of roles and then, in the **Search by role name**, enter **compliance**.
6. In the results, select **Compliance Administrator**.
7. Review the role setting details information.

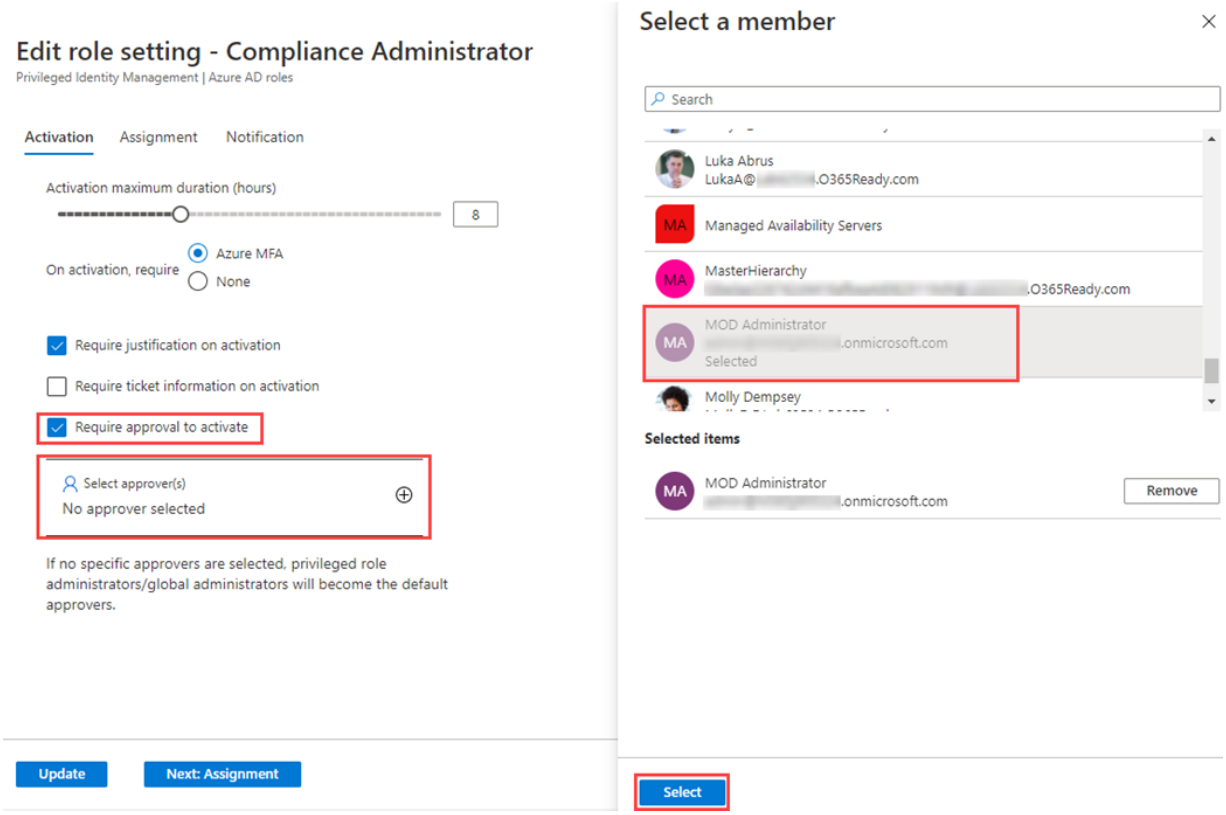
30.2.2 Require approval to activate

If setting multiple approvers, approval completes as soon as one of them approves or denies. You cannot require approval from at least two users. To require approval to activate a role, follow these steps.

1. In the Role setting details page, on the top menu, select **Edit**.



2. In the Edit role setting – Compliance Administrator blade, select the **Require approval to activate** check box.
3. Select **Select approvers**.
4. In the Select a member pane, select your administrator account and then select **Select**.



5. Once you have configured the role settings, select **Update** to save your changes.

30.3 lab: title: '29 - Configure Privileged Identity Management for Azure AD roles' learning path: '04' module: 'Module 03 - Plan and implement privileged access'

31 Lab 29: Assign Azure AD roles in Privileged Identity Management

31.1 Lab scenario

With Azure Active Directory (Azure AD), a Global administrator can make permanent Azure AD admin role assignments. These role assignments can be created using the Azure portal or using PowerShell commands.

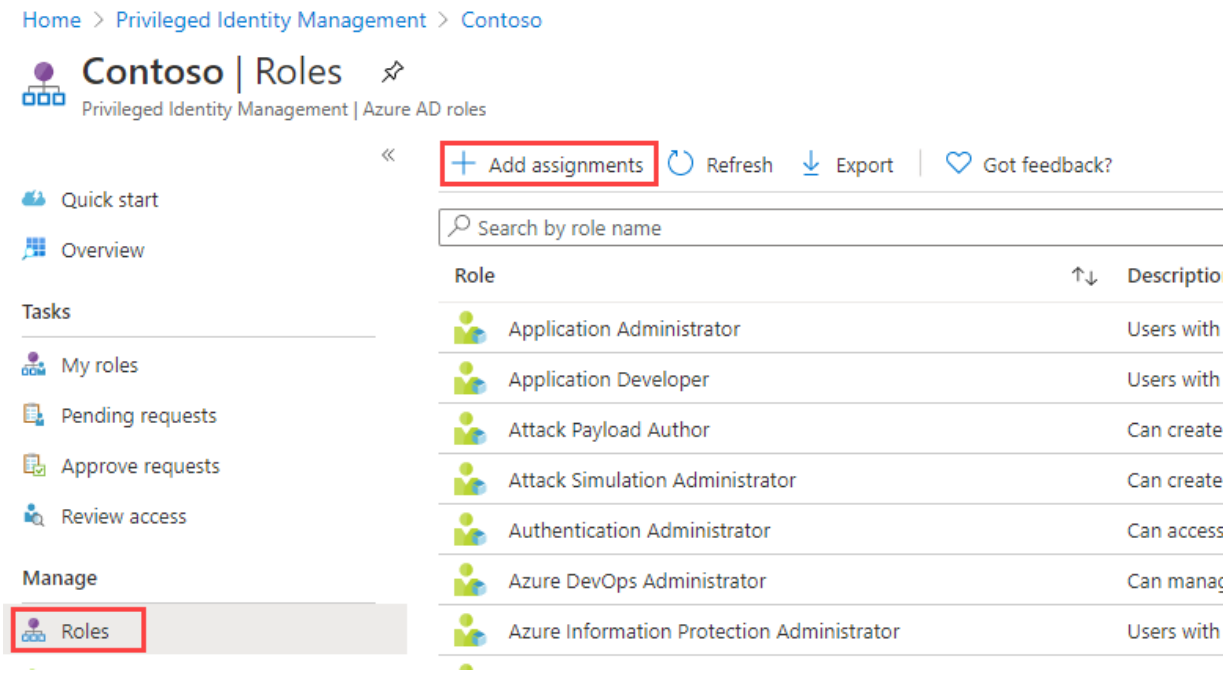
The Azure AD Privileged Identity Management (PIM) service also allows Privileged role administrators to make permanent admin role assignments. Additionally, Privileged role administrators can make users eligible for Azure AD admin roles. An eligible administrator can activate the role when they need it, and then their permissions expire once they're done.

31.1.0.1 Estimated time: 15 minutes

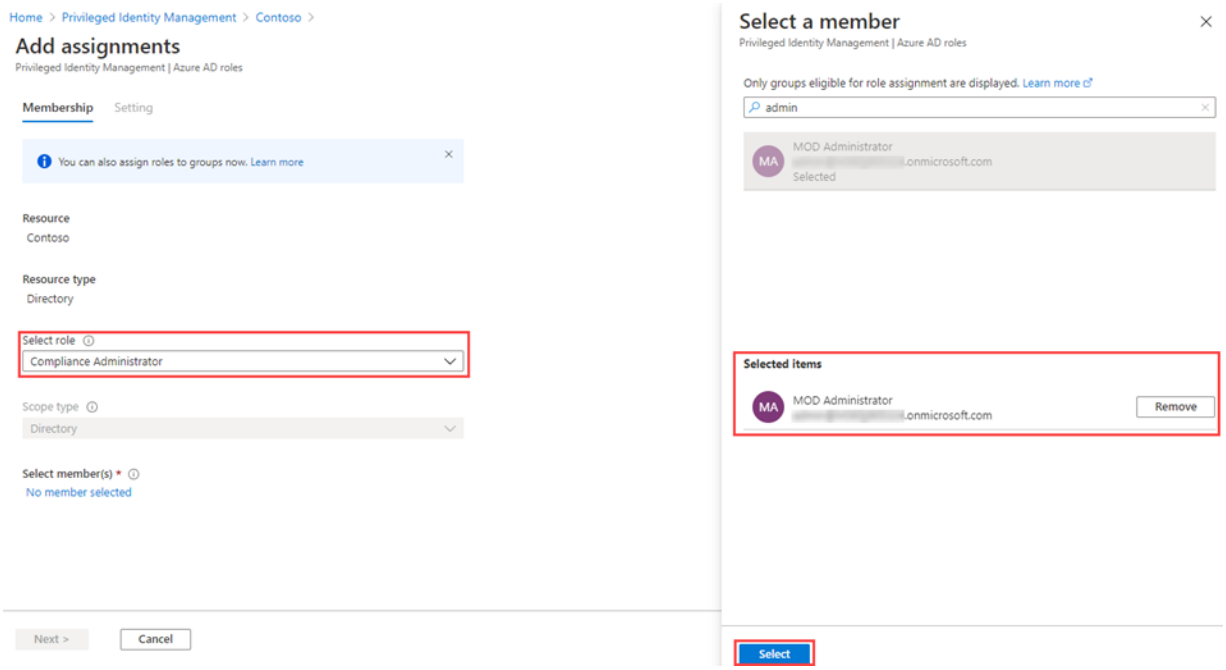
31.2 Assign a role

Follow these steps to make a user eligible for an Azure AD admin role.

1. Sign in to https://portal.azure.com using a Global Administrator account.
2. Search for and then select **Azure AD Privileged Identity Management.**
3. In the Privileged Identity Management blade, in the left navigation, select **Azure AD roles.**
4. On the Quick start page, in the left navigation, select **Roles**.
5. On the top menu, select **+ Add assignments.**



6. In the Add assignments blade, on the **Membership** tab, review the settings.
7. Select the **Select role** menu and then select **Compliance Administrator**.
8. You can use the **Search role by name** filter to help located a role.
9. Under **Select member(s),** select **No members selected**.
10. In the Select a member pane, select your administrator account and then select **Select**.

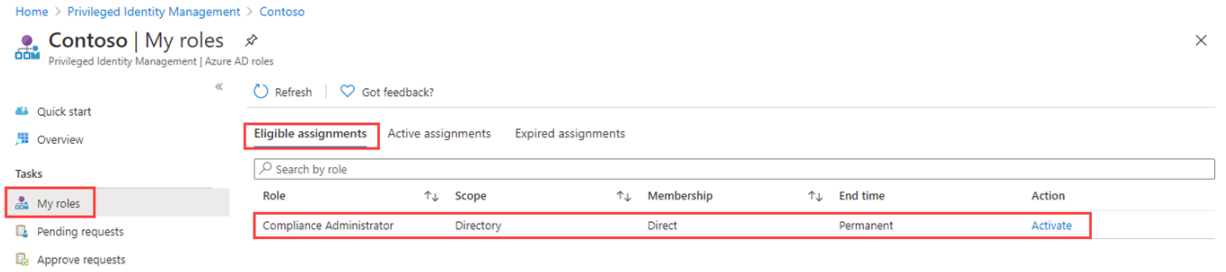


11. In the Add assignments blade, select **Next**.
12. On the **Settings** tab, under **Assignment type**, review the available options. For this task, use the default setting.
    - Eligible assignments require the member of the role to perform an action to use the role. Actions might include performing a multi-factor authentication (MFA) check, providing a business justification, or requesting approval from designated approvers.
    - Active assignments do not require the member to perform any action to use the role. Members assigned as active have the privileges always assigned to the role.
13. Review the remaining settings and then select **Assign**.

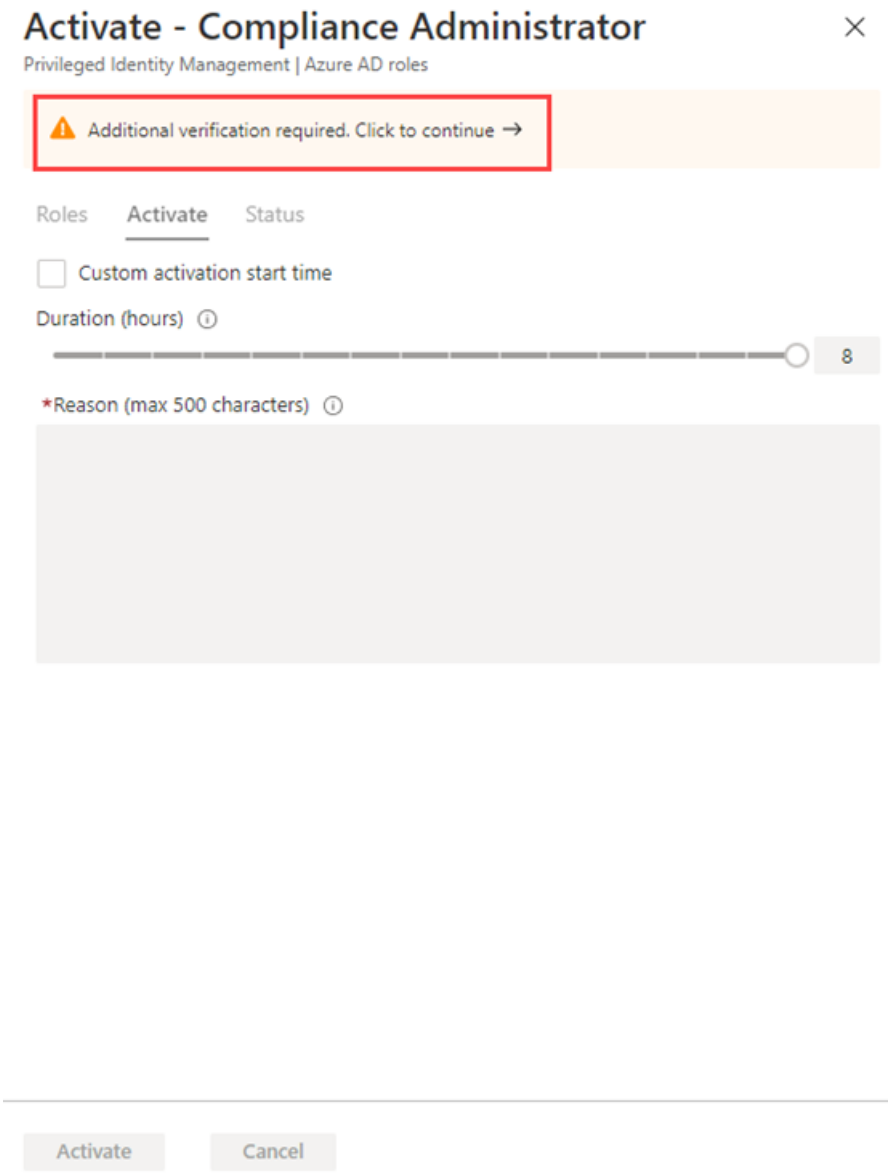
31.3 Activate your Azure AD roles

When you need to assume an Azure AD role, you can request activation by opening **My roles** in Privileged Identity Management.

1. On the Privileged Identity Management blade, in the left navigation menu, select **My roles.**
2. In the My roles blade, review the list of eligible assignments.



3. In the Compliance Administrator role row, select **Activate**.
4. In the Activate – Compliance Administrator pane, select **Additional verification required** and then follow the instructions to provide additional security verification. You are required to authenticate only once per session.



5. After you have completed the additional security verification, in the Activate – Compliance Administrator pane, in the **Reason** box, enter the justification for activating this role.
6. Select **Activate**.

31.4 Assign a role with restricted scope

For certain roles, the scope of the granted permissions can be restricted to a single admin unit, service principal, or application. This procedure is an example if assigning a role that has the scope of an administrative unit.

1. Browse to the Privileged Identity Management blade, and in the left navigation menu, select Azure **AD roles.**
2. In the Roles blade, on the top menu, select **+ Add assignments.**
3. In the Add assignments blade, select the **Select role** menu and then select **User administrator.**
4. Select the **Scope type** menu and review the available options. For now, you will use the **Directory** scope type.

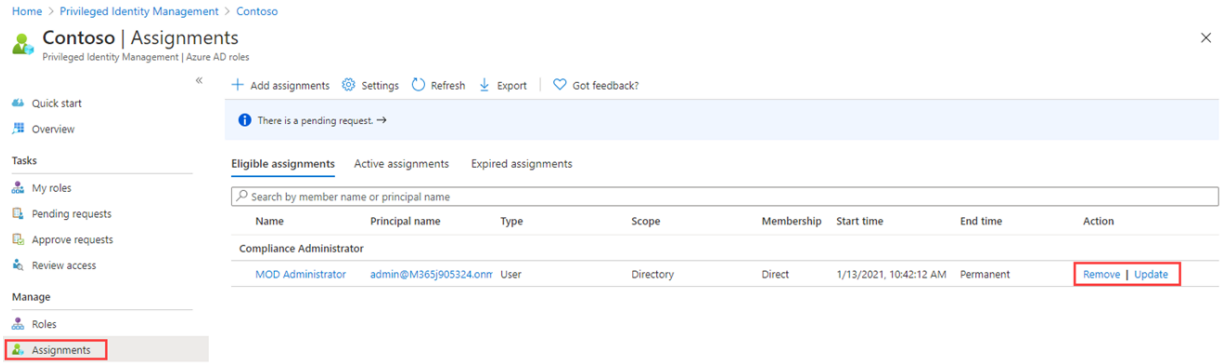
   [!Tip] Go to https://docs.microsoft.com/en-us/azure/active-directory/roles/admin-units-manage for more information about the administrative unit scope type.

1. As you did when assigning a role without a restricted scope, you would add members and complete the settings options. For now, select **Cancel**.

31.5 Update or remove an existing role assignment

Follow these steps to update or remove an existing role assignment.

1. In the Open Azure AD Privileged Identity Management > Azure AD roles blade, in the left navigation, select **Assignments**.
2. In **Assignments** list, for Compliance Administrator, review the options in the **Action** column.



3. Select **Update** and review the options available in the Membership settings pane. When complete, close the pane.
4. Select **Remove**.
5. In the **Remove** dialog box, review the information and then select **Yes**.

31.6 lab: title: '30 - Assign Azure resource roles in Privileged Identity Management' learning path: '04' module: 'Module 03 - Plan and implement privileged access'

32 Lab 30: Assign Azure resource roles in Privileged Identity Management

32.1 Lab scenario

Azure Active Directory (Azure AD) Privileged Identity Management (PIM) can manage the built-in Azure resource roles, as well as custom roles, including (but not limited to):

- Owner
- User Access Administrator
- Contributor
- Security Admin
- Security Manager

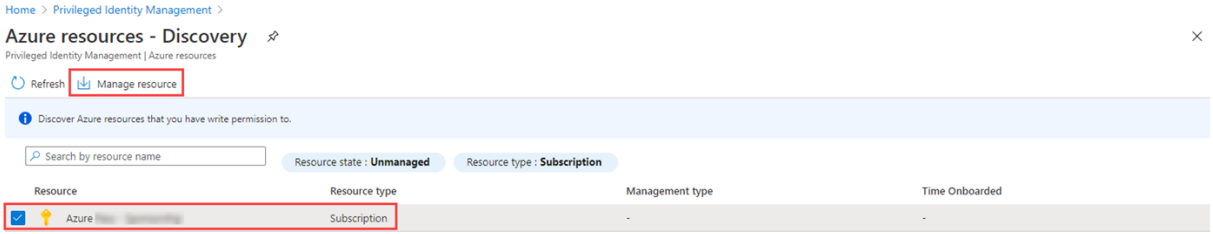
You need to make a user eligible for an Azure resource role.

32.1.0.1 Estimated time: 10 minutes

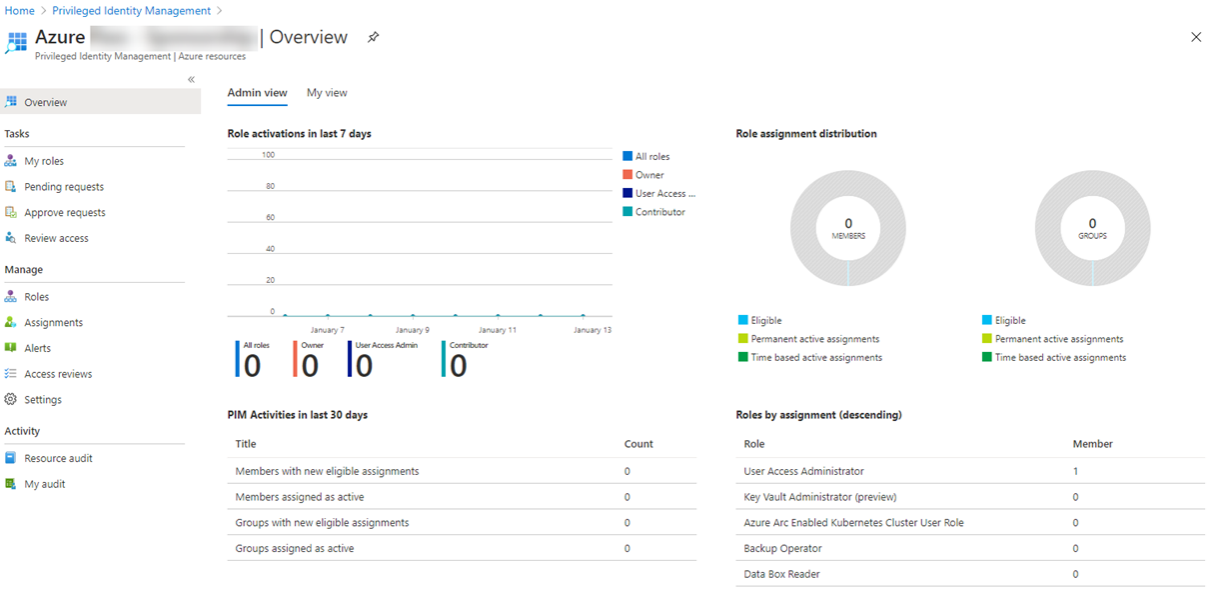
32.2 Assign Azure resource roles

1. Sign in to https://portal.azure.com using a Global Administrator account.
2. Search for and then select **Azure AD Privileged Identity Management.**
3. In the Privileged Identity Management blade, in the left navigation, select **Azure resources.**
4. On the top menu, select **Discover resources**.

5. In the Azure resources – Discovery blade, select your subscription and then, on the top menu, select **Manage resource**.



6. In the **Onboarding selected resource for management** dialog box, review the information and then select **OK**.
7. When onboarding completes, close the Azure resources – Discovery blade.
8. In the Azure resources blade, select the resource you just added.



9. In the left navigation menu, under **Manage**, select **Roles** to see the list of roles for Azure resources.
10. On the top menu, select + **Add assignments**.
11. In the Add assignments blade, select the **Select role** menu and then select **API Management Service Contributor.**
12. Under **Select member(s),** select **No member selected**.
13. In the Select a member or group pane, select an account from your organization that will be assigned the role.
14. Select **Next**.
15. On the **Settings** tab, under **Assignment type**, select **Eligible**.
    - **Eligible** assignments require the member of the role to perform an action to use the role. Actions might include performing a multi-factor authentication (MFA) check, providing a business justification, or requesting approval from designated approvers.
    - **Active** assignments do not require the member to perform any action to use the role. Members assigned as active have the privileges always assigned to the role.
16. Specify an assignment duration by changing the start and end dates and times.
17. When finished, select **Assign**.
18. After the new role assignment is created, a status notification is displayed.

32.3 Update or remove an existing resource role assignment

Follow these steps to update or remove an existing role assignment.

1. Open **Azure AD Privileged Identity Management**.
2. Select **Azure resources**.
3. Select the resource you want to manage to open its overview page.
4. Under **Manage**, select **Assignments**.
5. On the **Eligible roles** tab, in the Action column, review the available options.
6. Select **Remove**.
7. In the **Remove** dialog box, review the information and then select **Yes**.

32.4 lab: title: '31 - Connect data from Azure Active Directory (Azure AD) to Azure Sentinel' learning path: '04' module: 'Module 04 - Monitor and maintain Azure Active Directory'

33 Lab 31: Connect data from Azure Active Directory (Azure AD) to Azure Sentinel

33.1 Lab scenario

Your company expects to begin using a Security information and event management (SIEM) solution. You know you have access to Azure Sentinel and need to become familiar with connecting it to your Azure AD.

33.1.0.1 Estimated time: 10 minutes

33.2 Prerequisites

- Any Azure AD license (Free/O365/P1/P2) is sufficient to ingest sign-in logs into Azure Sentinel. Additional per-gigabyte charges may apply for Azure Monitor (Log Analytics) and Azure Sentinel.
- Your user must be assigned the Azure Sentinel Contributor role on the workspace.
- Your user must be assigned the Global Administrator or Security Administrator roles on the tenant you want to stream the logs from.
- Your user must have read and write permissions to the Azure AD diagnostic settings to be able to see the connection status.

33.3 Create and add an Azure Sentinel workspace

Use these instructions if you do not already have a workspace available to Azure Sentinel.

1. Sign in to https://portal.azure.com using a Global Administrator account.
2. Search for and select **Azure Sentinel**.
3. In the Azure Sentinel workspaces blade, on the menu, select + **Add**.
4. If you already have an Azure Sentinel workspace, you can select that and continue to the next task.
5. In the Add Azure Sentinel to a workspace blade, select **Create a new workspace**.
6. Use the following information to create a new log analytics workspace:

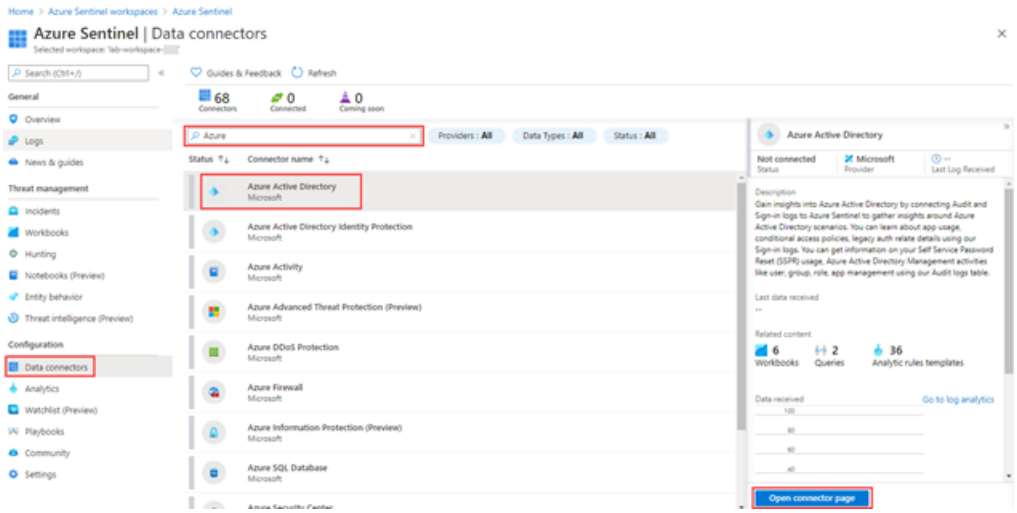
Setting	Value
Subscription	Use your current subscription.
Resource group	Use an existing resource group or create a new one.
Name	**Lab-workspace-yourinitialsanddate**The workspace must be a globally unique value.
Pricing tier	Pay-as-you-go

7. When complete, select your new workspace and then select **Add** to add the workspace to Azure Sentinel.

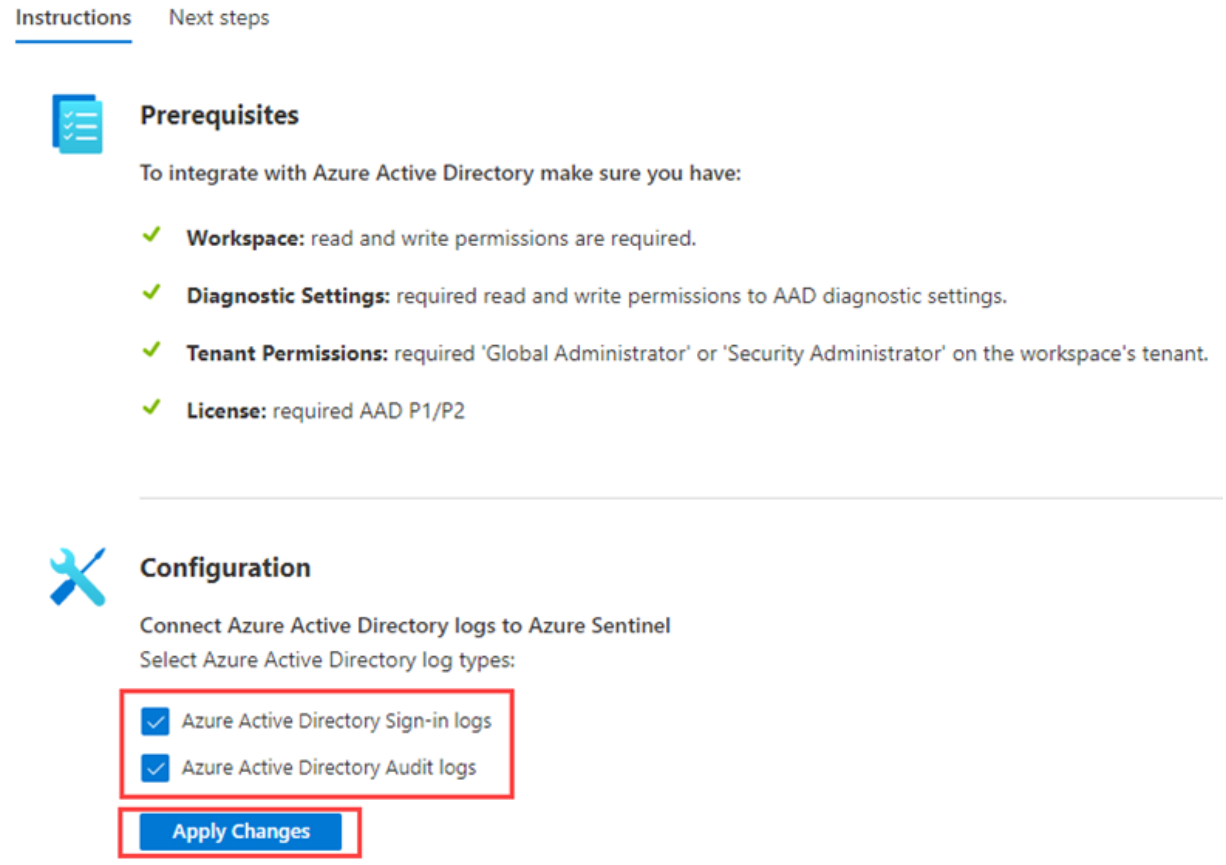
33.4 Connect to Azure Active Directory

You can use Azure Sentinel's built-in connector to collect data from https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis and stream it into Azure Sentinel. The connector allows you to stream https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins and https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-audit-logs.

1. In Azure Sentinel, in the navigation menu on the left, under **Configuration**, select **Data connectors**.
2. In the **Data connectors** list, select **Azure Active Directory** and then select **Open connector page**.



3. Under **Configuration**, select the **Azure Active Directory Sign-in logs** and **Audit logs** checkboxes and then select **Apply changes**.



4. Close the Azure Active Directory connector page.