Lab 2 - Identity – Configure Azure Privileged Identity Management (PIM)

In this lab, you will learn how to use Azure Privileged Identity Management (PIM) to enable just-in-time administration and control the number of users who can perform privileged operations. You will also learn about the different directory roles available as well as newer functionality that includes PIM being expanded to role assignments at the resource level.

Want to learn more: What is Privileged Identity Management? - Azure AD | Microsoft Docs

Pre-requisites

Step 1 – Create Demo Tenant

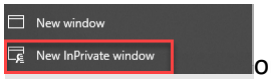
Before you start you should have completed the "Getting started with Labs". If you have not completed this, you will not be able to do this lab. You can find this document which you can download from https://aka.ms/secpractice-labs.

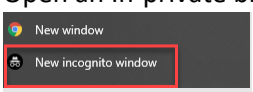
Each tenant can take up to 24 hours to provision so it's important that you complete this prior to when the labs are to be run.

Step 2 – Create yourself an Admin account for your demo tenant.

In this task, you will create a Microsoft 365 user account for yourself, and assign your account the Microsoft 365 Global Administrator role, which gives you the ability to perform all administrative functions within Microsoft 365.

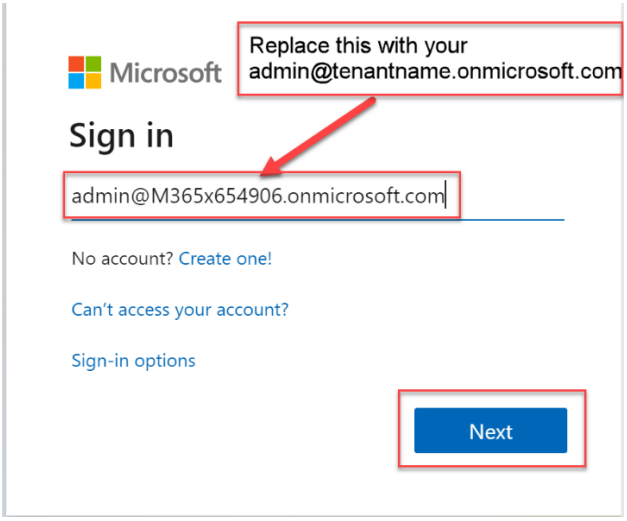
Important: As a best practice in your real-world deployments, you should always write down the first global admin account's credentials (in this lab, the MOD Administrator) and store it away for security reasons. This account is a non-personalized identity that owns the highest privileges possible in a tenant. It is **not** MFA activated (because it is not personalized) and the password for this account is typically shared among several users. Therefore, this first global admin is a perfect target for attacks, so it is recommended to create personalized service admins and keep as few global admins as possible. For those global admins that you do create, they should each be mapped to a single identity, and they should each have MFA enforced.

1. Open an In-private browser (Edge) 

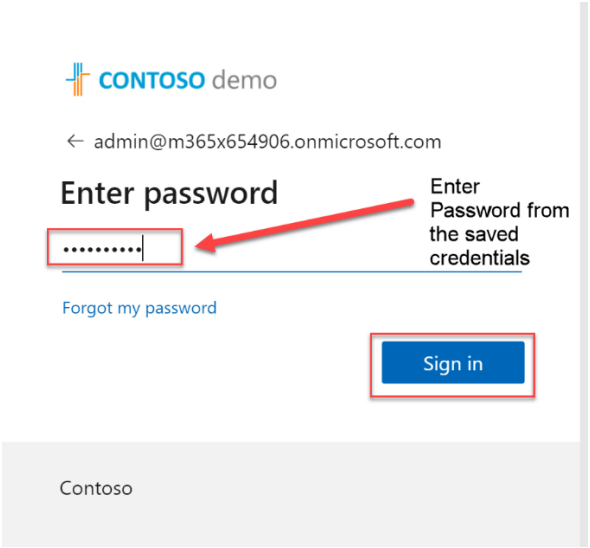
or New in-Cognito (Chrome) 

on your machine and then go to https://admin.microsoft.com/

2. Enter the admin account username that you saved in "Getting started with Microsoft Labs" to gain credentials.
3. Enter your admin credentials in the sign in as below and click NEXT



4. Enter the password and then click "Sign in"



5. In the **Microsoft 365 admin center**, in the left navigation pane, select **Users** and then select **Active users**.
6. In the **Active users** list, you will see the default **MOD Administrator** account as well as some other user accounts.
7. In the **Active Users** window, select **Add a user**.
8. In the **Set up the basics** window, enter the following information:

    - First name: **Your First Name**
    - Last name: **Your Last Name**
    - Display name: When you tab into this field, **YOUR NAME** will appear.
    - Username: When you tab into this field, **YOURFIRSTNAME-LASTNAME** may appear; if not enter this as the username

IMPORTANT: To the right of the **Username** field is the domain field. select the **M365xZZZZZZ.onmicrosoft.com** cloud domain.

After configuring this field, **YOUR username** should appear as:

YOURNAME@M365xZZZZZZ.onmicrosoft.com

- Password settings: select the **Let me create the password** option.
- Password: **Set your own complex Password**
- Uncheck the **Require this user to change their password when they first sign in** checkbox.

9. Select **Next**.
10. In the **Assign product licenses** window, enter the following information:
11. Select location: **United States (Your Location)**
12. Licenses: Under **Assign user a product license**, select **Office 365 E5** and **Enterprise Mobility + Security E5** or if you have **Microsoft 365 E5** select this instead.
13. Select **Next**.
14. In the **Optional settings** window, in the Roles section select **Admin center access** By doing so, all the Microsoft 365 administrator roles are now enabled and available to be assigned.
15. Select **Global Admin** and then select **Next**.
16. On the **Review and finish** window, review your selections. If anything needs to be changed, select the appropriate **Edit** link and make the necessary changes. Otherwise, if everything is correct, select **Finish adding**.
17. Once your new username **has been added to active users** page, select **Close.**

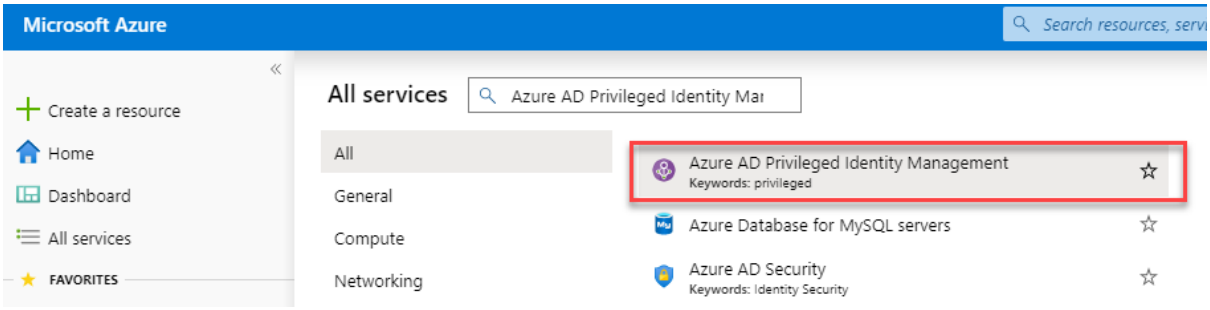
Lab Parts

This lab contains three activities, as shown below:

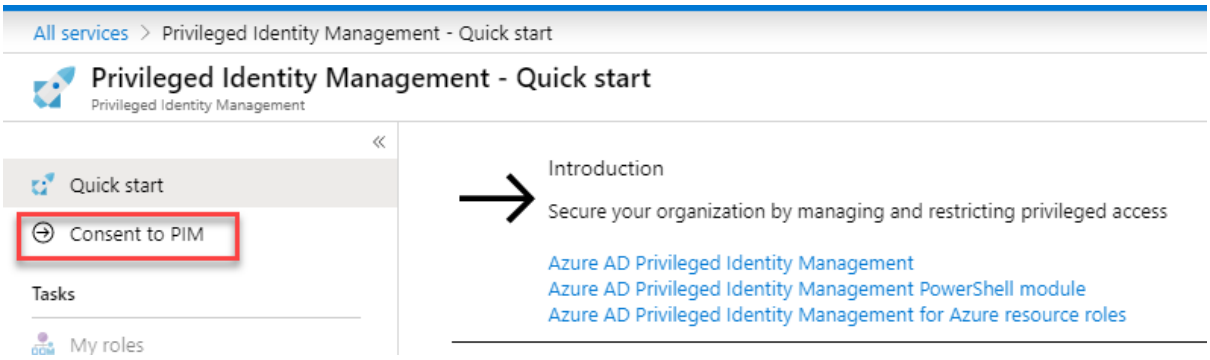
- Part 1 – Enable PIM
- Part 2 – Assign Directory Roles
- Part 3 – Activate and Deactivate PIM Roles
- Part 4 – Directory Roles (General)
- Part 5 – PIM Resource Workflows
- Part 6 – View audit history for Azure AD roles in PIM

Part 1 – Enable PIM

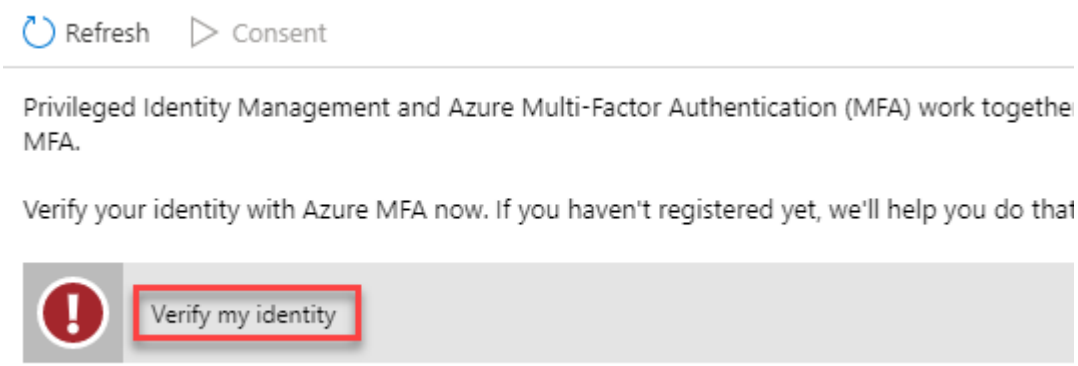
1. Go to the Azure Portal (https://portal.azure.com/) as Global Administrator that you created. Click More services and search for and select Azure AD Privileged Identity Management.



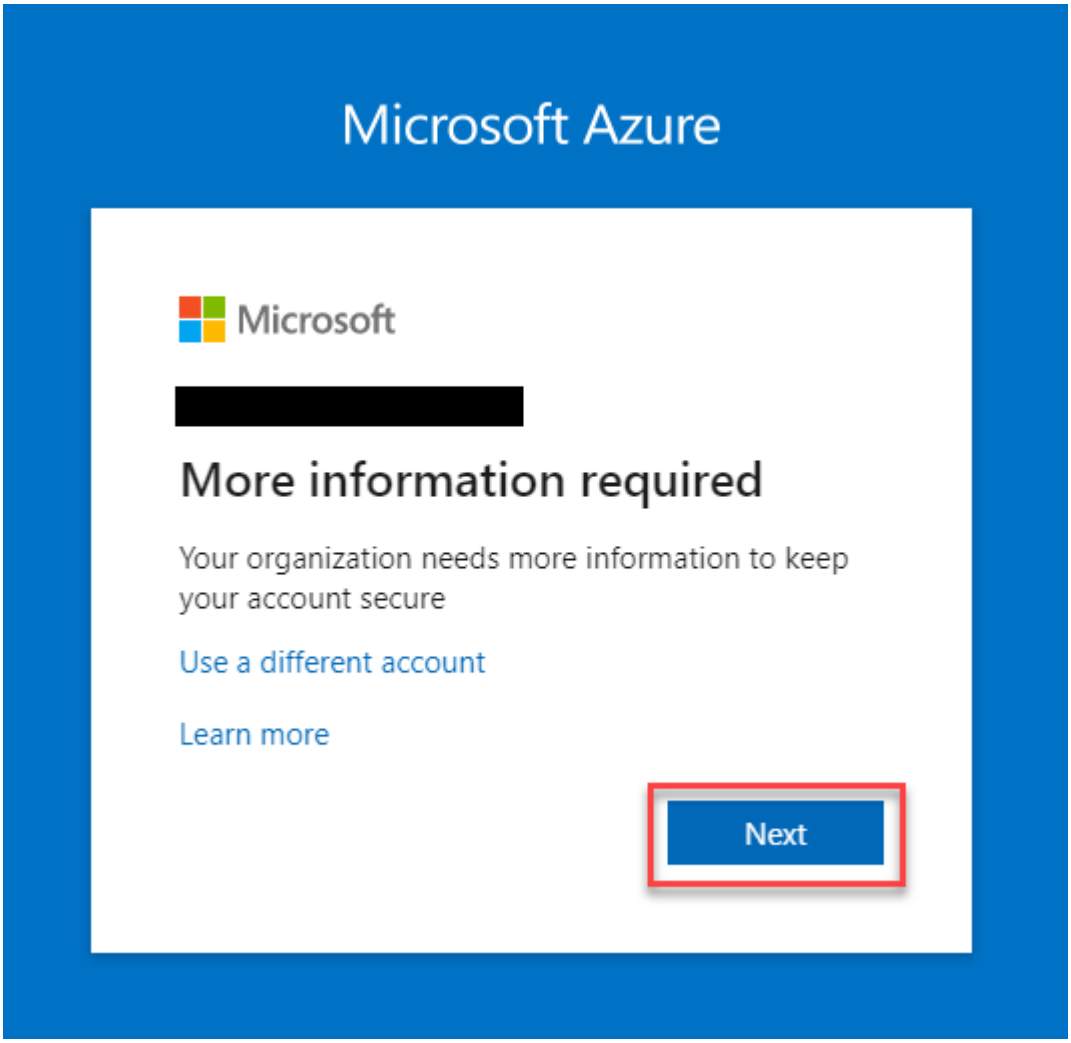
2. Click consent to PIM if it appears. In some tenants PIM is already enabled and therefore these steps are unnecessary.



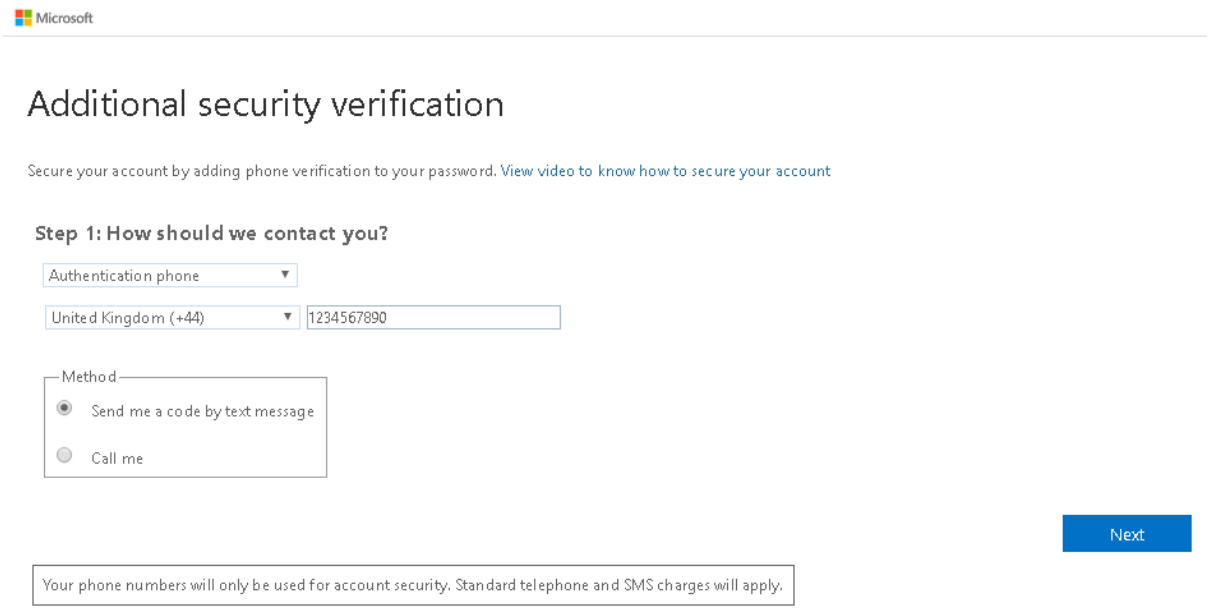
3. Click **Verify my identity** if it appears.



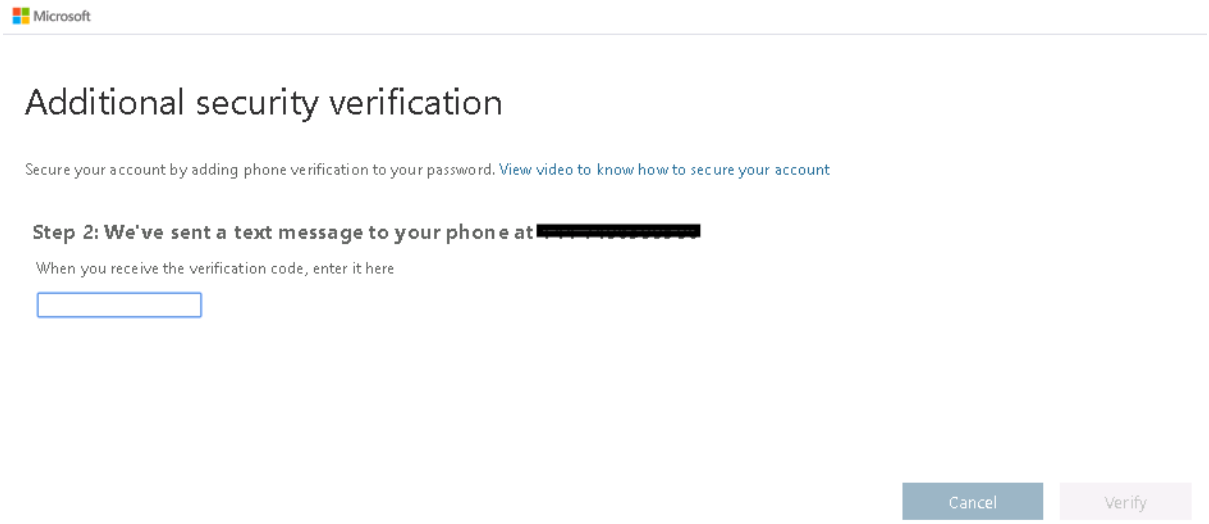
4. Click **Next**.



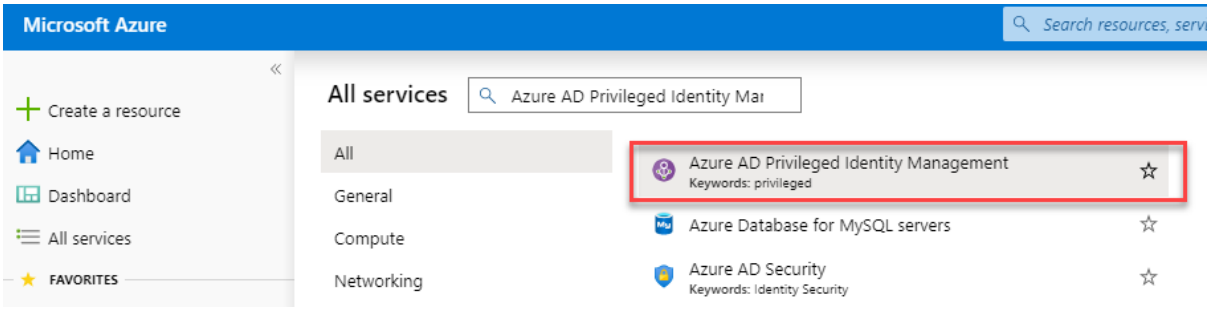
5. Enter your mobile/cell phone details and click **Next**.



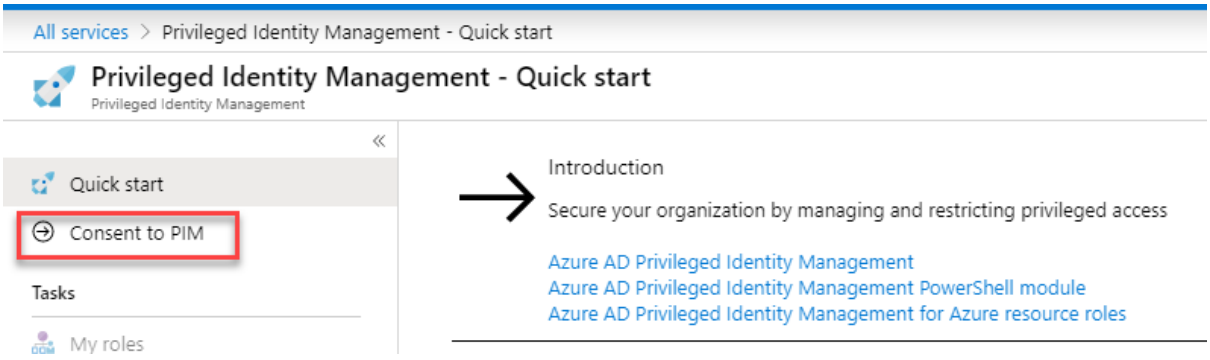
6. Enter the code when you receive it via SMS and click **Verify**.



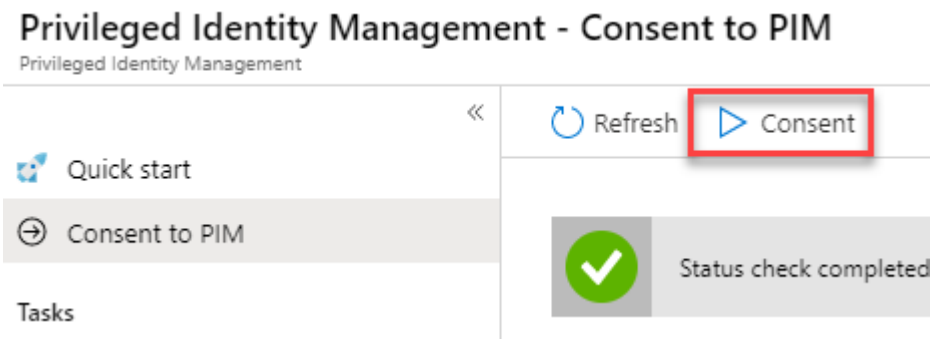
7. Once the verification is successful, click **Done**.
8. In the Azure Portal, click **All services** and search for and select **Azure AD Privileged Identity Management**.



9. Click consent to PIM if it appears.



10. Back on the **Consent to PIM blade** click **Consent** and click **Yes**.



11. Refresh the Azure Portal by pressing **F5**.

Note: If by refreshing the portal in the browser does not display PIM as being enabled then log out and back into the Azure Portal.

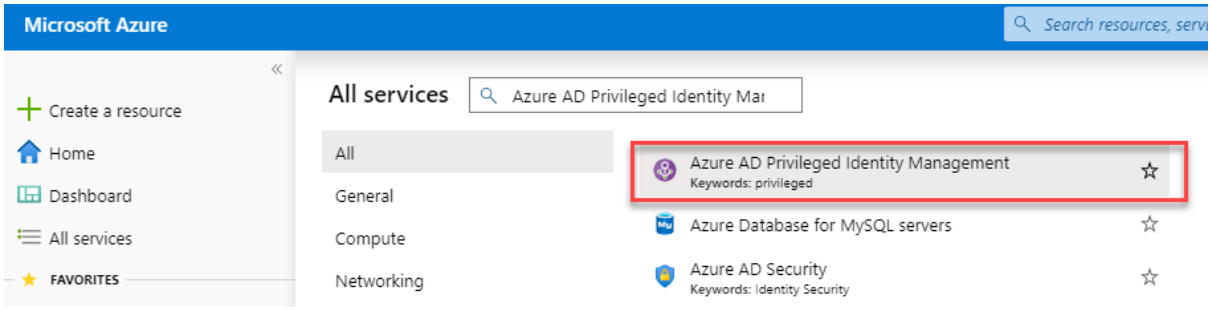
Part 1 – Complete.

Part 2 – Assign Directory Roles

Task 1: Make a user eligible for a role.

In the following task you will make a user eligible for an Azure AD directory role.

1. Sign in to Azure portal
2. In the Azure Portal, click **All services** and search for and select **Azure AD Privileged Identity Management**.

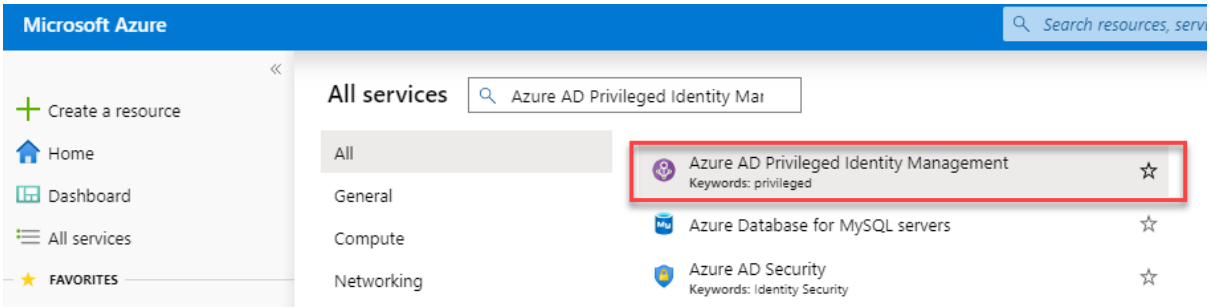


3. Select **Roles**. If this is option is still greyed you may need to refresh your browser.
4. Select **Billing Administrator**.
5. Select **+ Add assignments** to open Select a member. In the Add assignments screen click **No member selected**.
6. In the **Select a member screen** select **Patti Fernandez** and then click **Select**.
7. In Add assignments screen on the Setting tab unmark the **Permanently eligible** checkbox. Click **Assign**. Review the added member in the assignment window.
8. When the role is assigned, the user you selected will appear in the members list as **Eligible** for the role.

Task 2: Make a role assignment permanent.

Follow these steps if you want to make a role assignment permanent.

1. In the Azure Portal, click **All services,** and search for and select **Azure AD Privileged Identity Management**.



2. Click **Azure AD roles**.
3. Click **Assignments**.

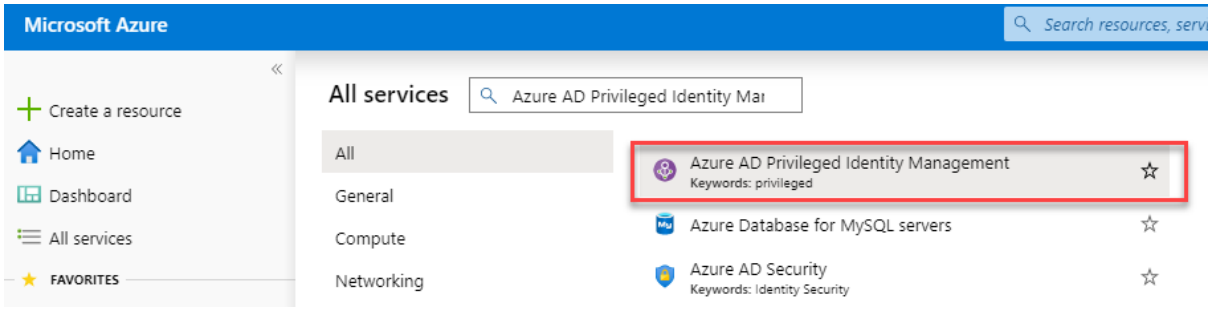
4. Click **Update** for Patti as Billing Administrator and then mark the **Permanently eligble** box. In Membership settings click **Save**.

Results: The Billing Administrator role is now listed as **permanent** for Patti Fernandez. In other words, Patti is permanently eligible to be elevated to the Billing Administrator role.

Task 3: Remove a user from a role.

You can remove users from role assignments, but make sure there is always at least one user who is a permanent Global Administrator.

1. In the Azure Portal, click **All services** and search for and select **Azure AD Privileged Identity Management**.



2. Click **Azure AD roles**.
3. Click **Assignments**.
4. Use the Member filter to again select Patti Fernandez.
5. In the Action area under Eligible assignments click **Remove**.
6. In the message that asks you to confirm, click **Yes**. The role assignment will be removed.

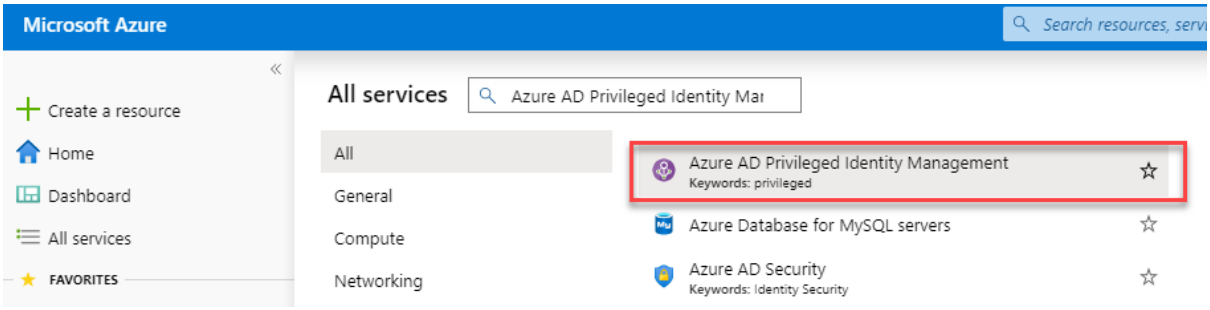
Part 2 – Complete.

Part 3 – Activate and Deactivate PIM Roles

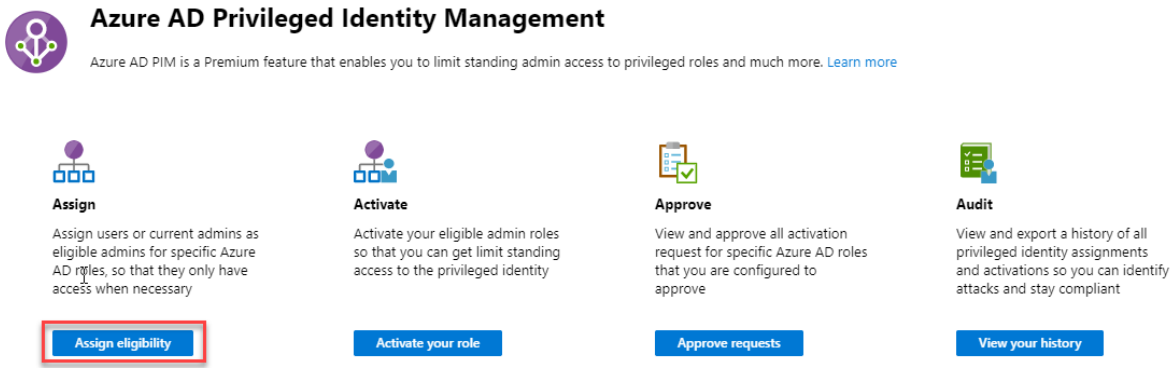
Task 1: Activate a role.

When you need to take on an Azure AD directory role, you can request activation by using the **My roles** navigation option in PIM.

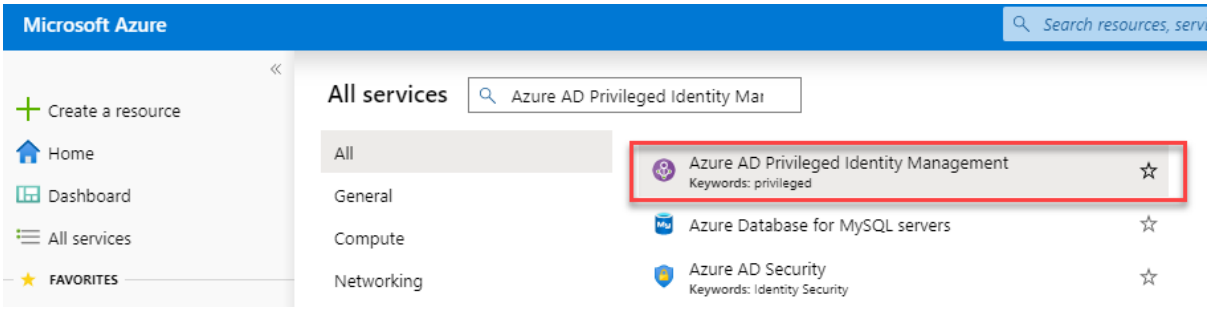
1. In the Azure Portal, signed-in as Global Admin, click **All services** and search for and select **Azure AD Privileged Identity Management**.



2. Click **Azure AD roles**.
3. Click **Quick Start** and click **Assign eligibility**.



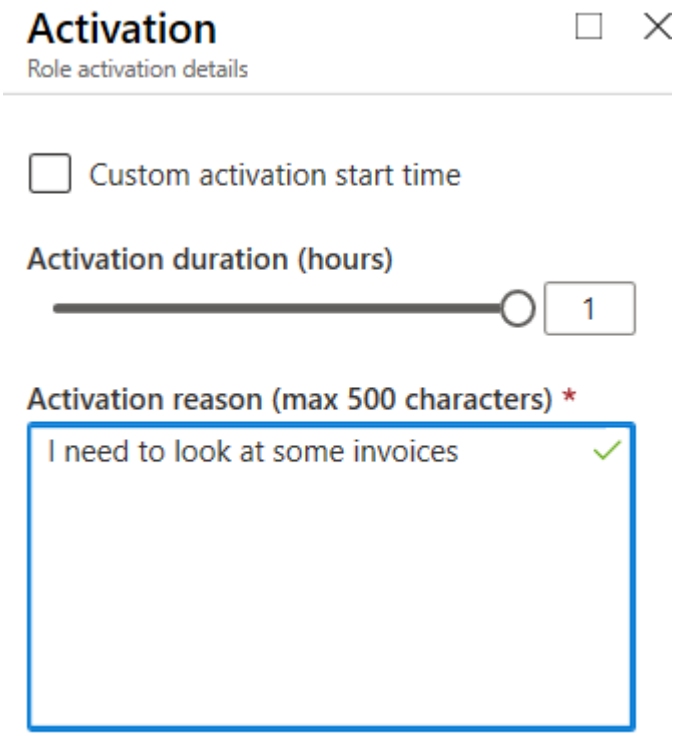
4. Click **Billing Administrator** and add Patti Fernandez back into the **Billing Administrators** role.
5. Open an **In Private** browsing session and navigate to **https://portal.azure.com** and login as **Patti** using her UPN. example PattiF@YourTenantHere.onmicrosoft.com with the password given by your lab host (hint: the password is likely the same as the MOD Administrator password).
6. In the Azure Portal, click **All services,** and search for and select **Azure AD Privileged Identity Management**.



7. Click **Azure AD roles**.
8. Click **Quick start** and click **Activate your role**.
9. On the Billing Administrator role, scroll to the right and click **Activate**.

10. Click **Verify your identity before proceeding** if this appears here. You only have to authenticate once per session. Run through the wizard to authenticate Patti.
11. Once returned to the Azure Portal, click **All services** and search for and select **Azure AD Privileged Identity Management**.
12. Select **Azure AD Roles** then click click **Activate your role** on the Quick start blade.
13. On the Billing Administrator role, scroll to the right and click **Activate**.

14. Enter an activation reason and click **Activate**



By default, roles do not require approval unless configured explicitly in settings.

If the role does not require approval, it is activated and added to the list of active roles. If you want to use the role right away, follow the steps in the next section.

If the role requires approval to activate, a notification will appear in the upper right corner of your browser informing you the request is pending approval.

Task 2: Use a role immediately after activation.

When you activate a role in PIM, it can take up to 10 minutes before you can access the desired administrative portal or perform functions within a specific administrative workload. To force an update of your permissions, use the **Application access** page as described in the following steps.

1. Click **Sign Out**.
2. Log back in as Patti in the inPrivate browsing session.

Task 3: View the status of your requests.

You can view the status of your pending requests to activate.

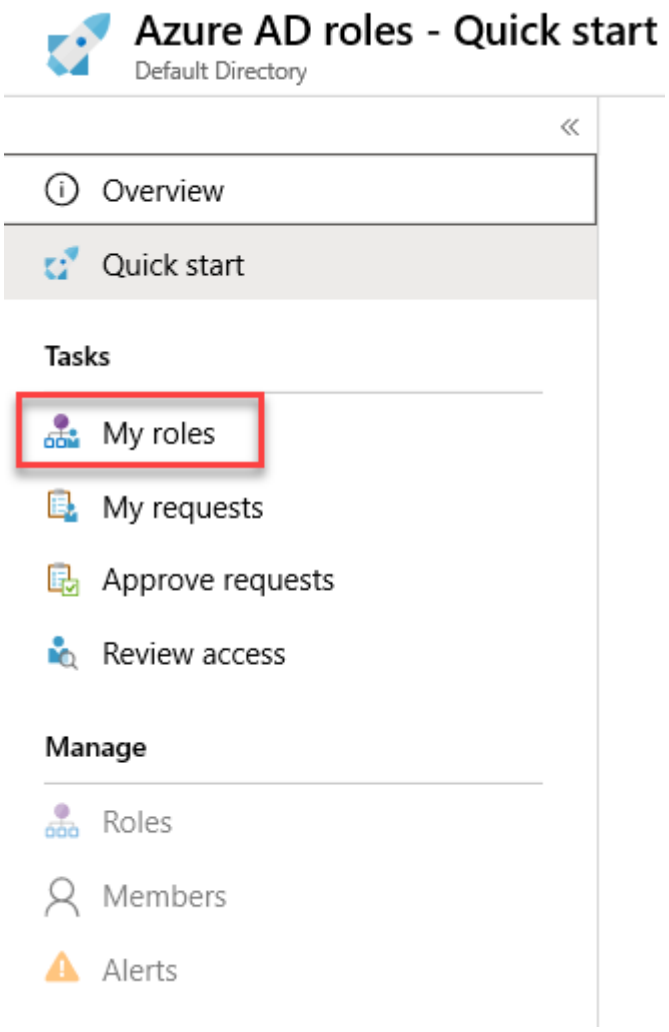
1. Still signed in as **Patti**, in the Azure Portal, click **All services** and search for and select **Azure AD Privileged Identity Management**.
2. Click **Azure AD Roles**.
3. Click **Pending requests** to see a list of your requests.

Task 4: Deactivate a role.

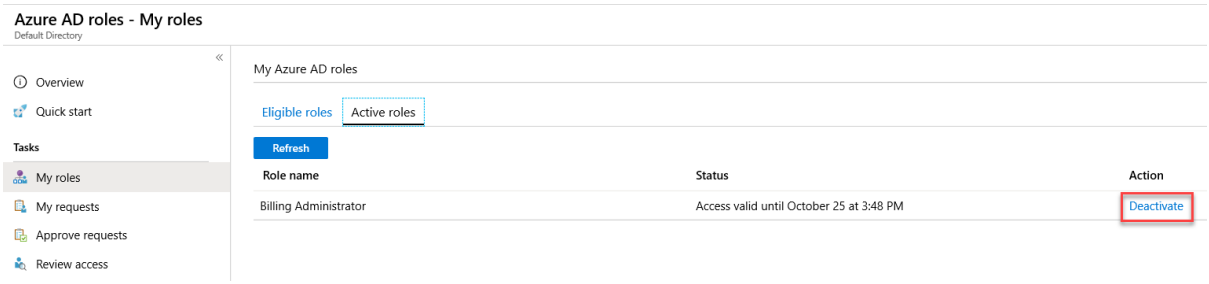
Once a role has been activated, it automatically deactivates when its time limit (eligible duration) is reached.

If you complete your administrator tasks early, you can also deactivate a role manually in Azure AD Privileged Identity Management.

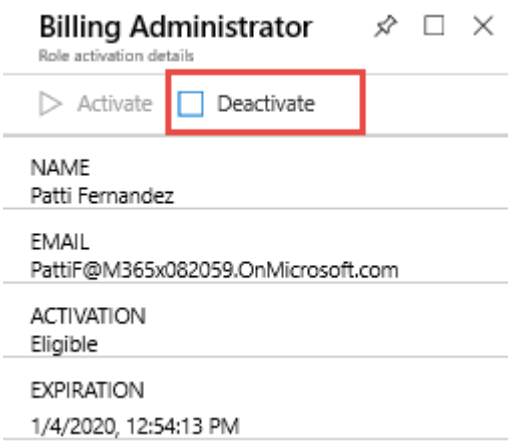
1. Still signed in as **Patti**, open Azure AD Privileged Identity Management.
2. Click **Azure AD roles**.
3. Click **My roles**.



4. Click **Active assignments** to see your list of active roles.
5. Find the role you're done using and then click **Deactivate**.



6. Click **Deactivate** again.



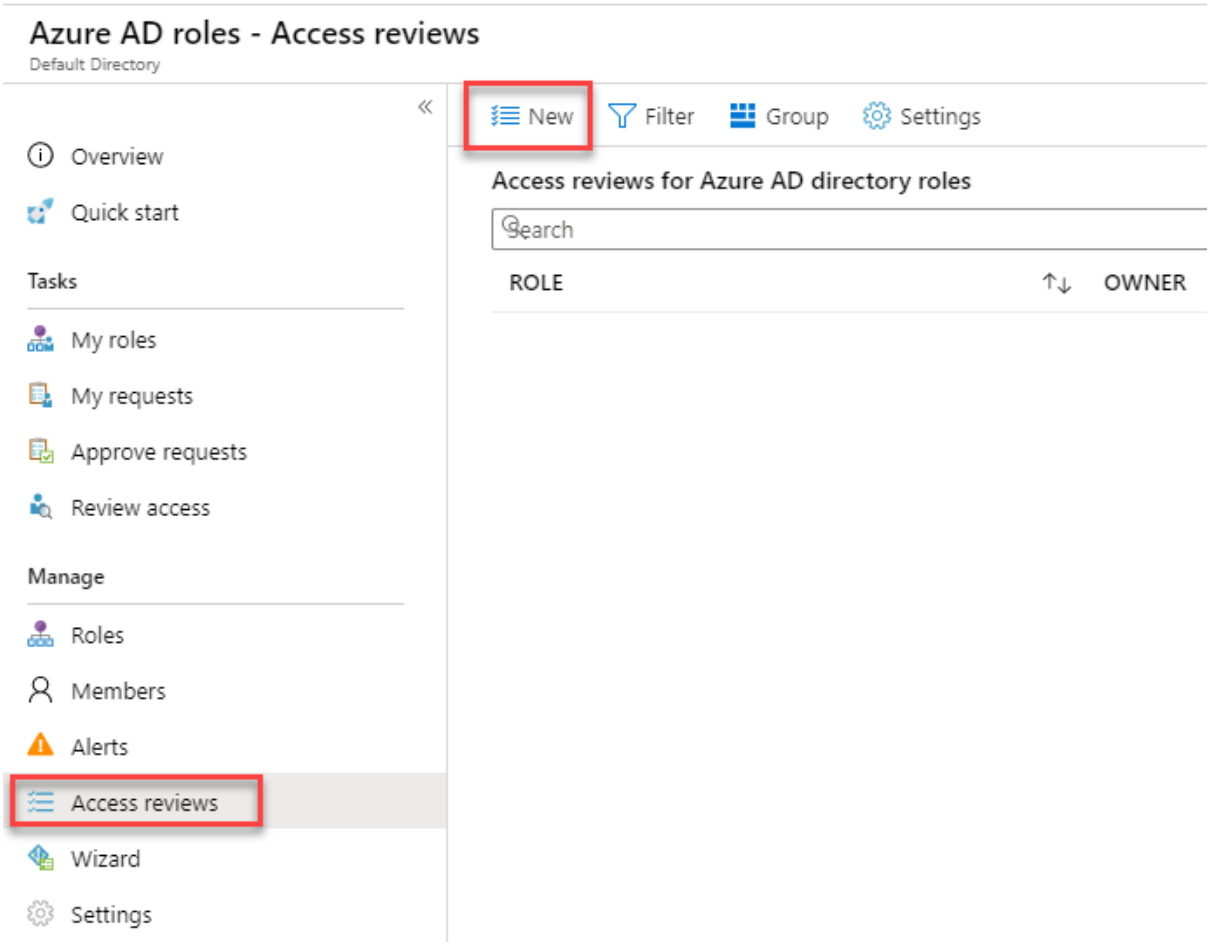
Part 3 – Complete.

Part 4 – Directory Roles (General)

Task 1: Start an access review for Azure AD directory roles in PIM.

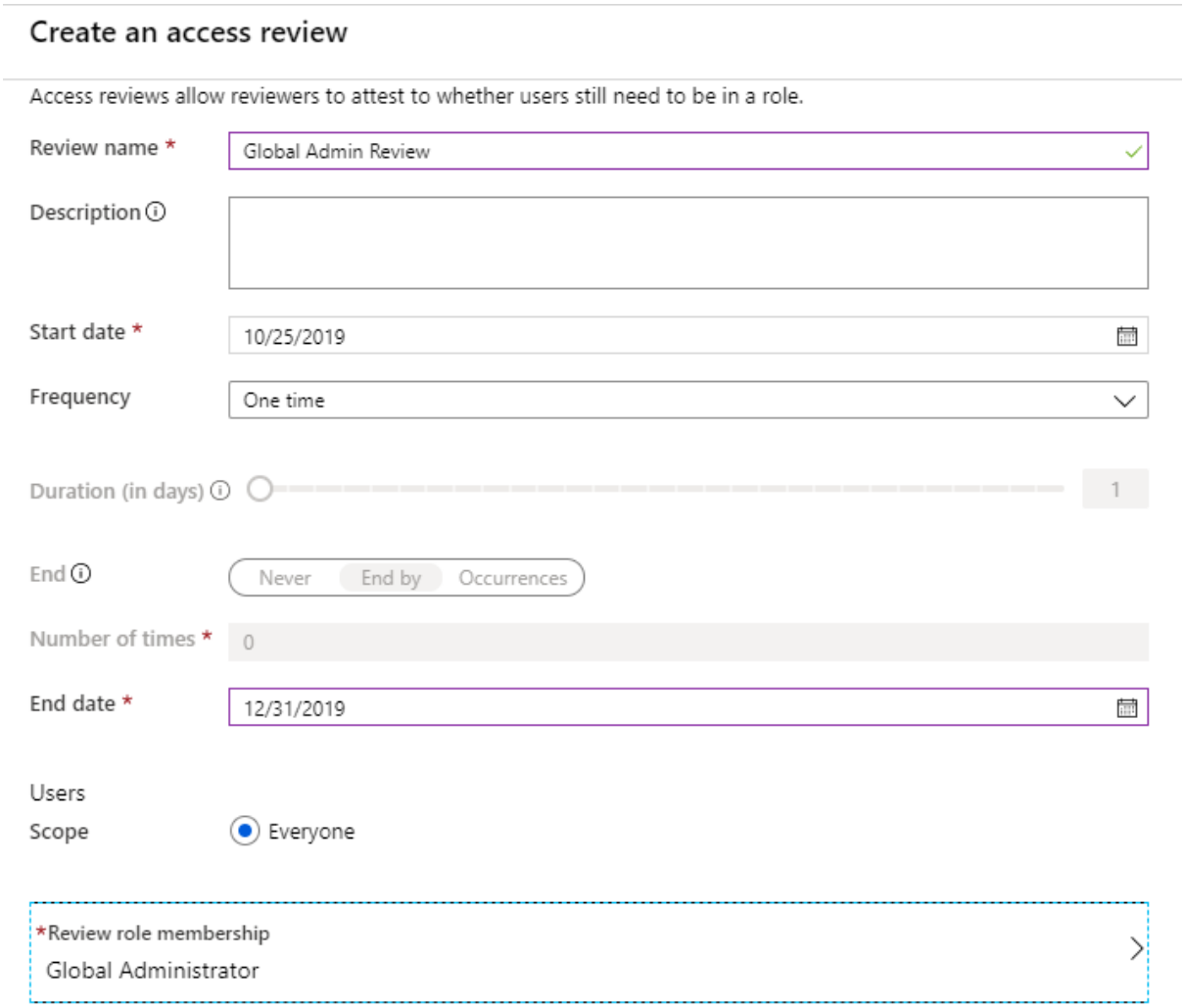
Role assignments become "stale" when users have privileged access that they don't need anymore. In order to reduce the risk associated with these stale role assignments, privileged role administrators or global administrators should regularly create access reviews to ask admins to review the roles that users have been given. This task covers the steps for starting an access review in Azure AD Privileged Identity Management (PIM).

1. Return to the browser that is logged in as your Global Admin Account.
2. From the PIM application main page select **Azure AD Roles** under the **Manage** section select **Access reviews** and Select **New**.

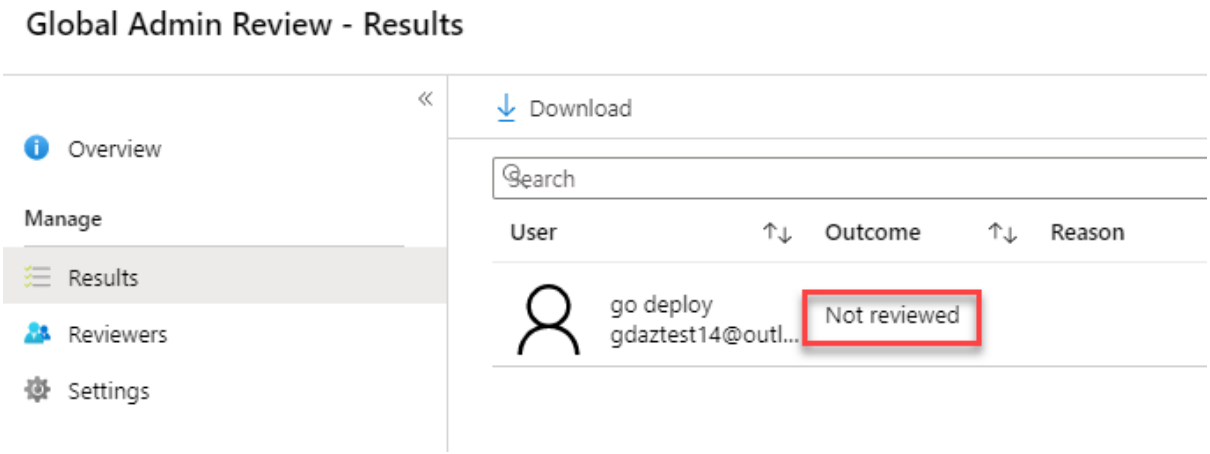


3. Enter the following details and click **Start**:
   - Review name: **Global Admin Review**
   - Start Date: **Today's Date**
   - Frequency: **One time**
   - End Date: **End of next month**
   - Review role membership: **Global Administrator**

- Reviewers: **<your Global Admin>**



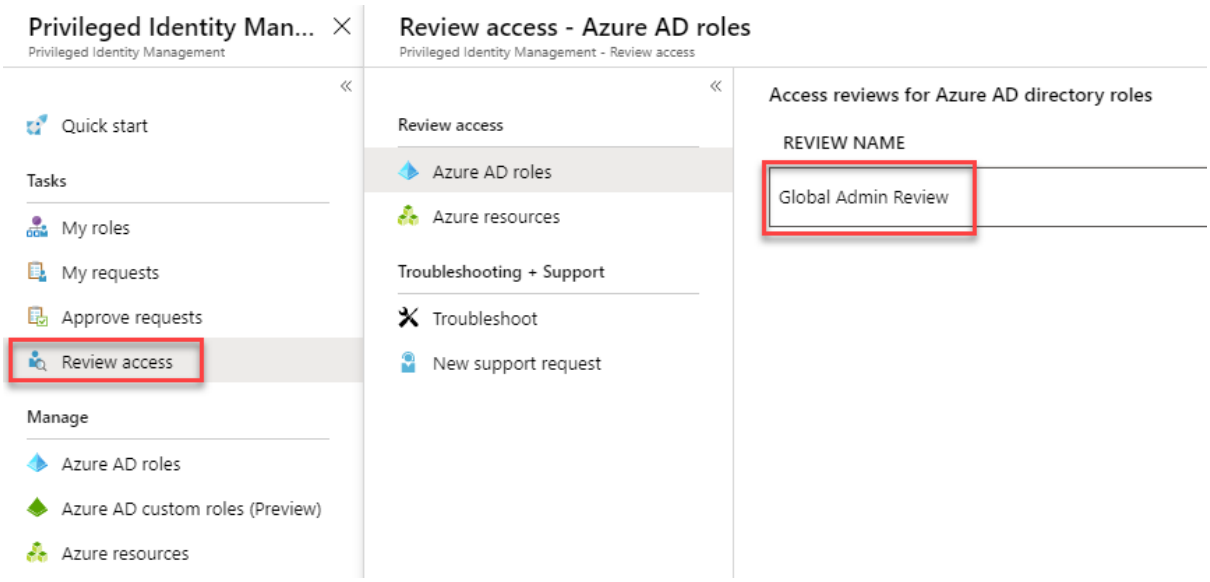
4. Once the review has completed and has a status of Active, click on the **Global Admin Review**. You may need to refresh the view in Azure.
5. Select **Results** and see the outcome of **Not reviewed**.



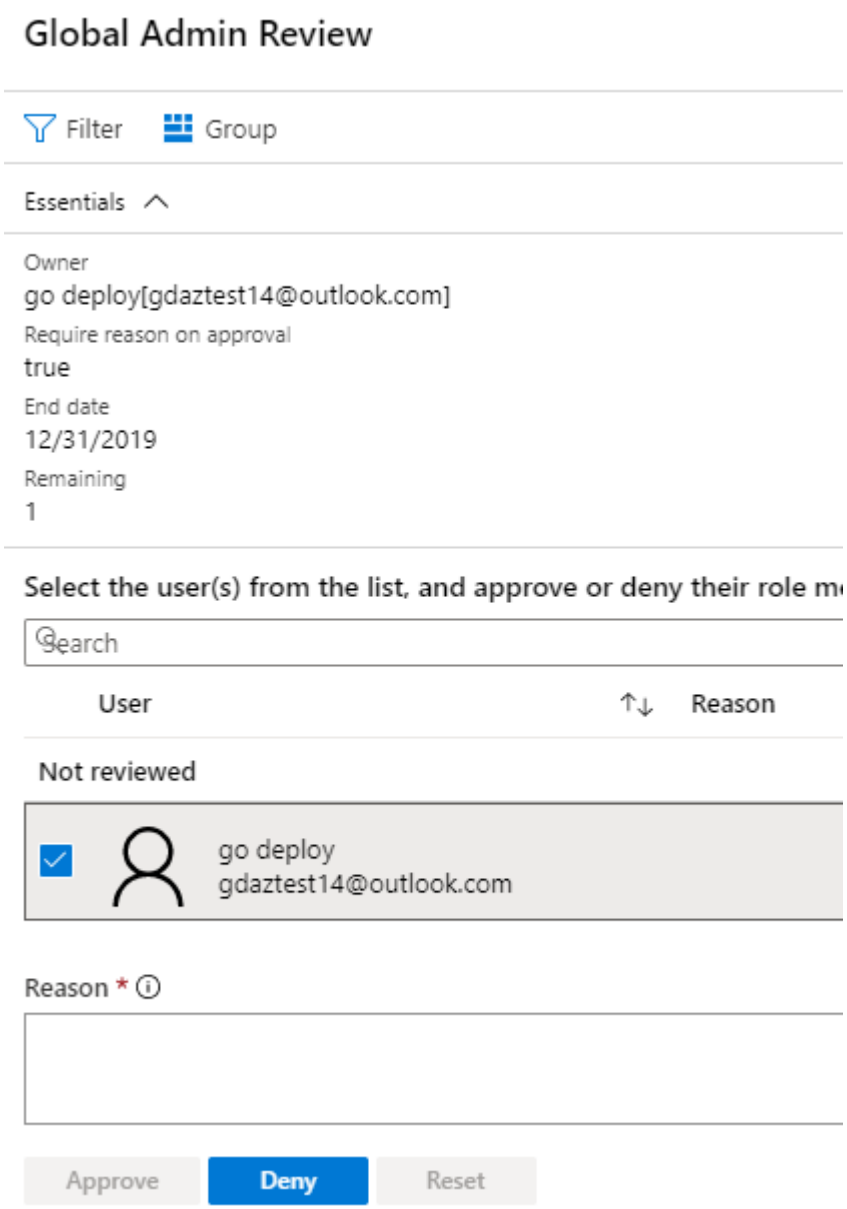
Task 2: Approve or deny access.

When you approve or deny access, you are just telling the reviewer whether you still use this role or not. Choose Approve if you want to stay in the role or Deny if you don't need the access anymore. Your status won't change right away, until the reviewer applies the results. Follow these steps to find and complete the access review:

1. In the PIM application, select **Review access**.
2. Select the **Global Admin Review**.



3. Unless you created the review, you appear as the only user in the review. Select the check box next to a user.



4. Close the **Review Azure AD roles** blade.

Task 3: Complete an access review for Azure AD directory roles in PIM.

Privileged role administrators can review privileged access once an access review has been started. Azure AD Privileged Identity Management (PIM) will automatically send an email prompting users to review their access. If a user did not get an email, you can send them the instructions in how to perform an access review.

After the access review period is over, or all the users have finished their self-review, follow the steps in this task to manage the review and see the results.

1. Go to the Azure portal and select the **Azure AD Privileged Identity Management**.

2. Select **Azure AD Roles**.
3. Select the **Access reviews**.
4. Select the Global Admin Review. Review the blade.

Task 4: Configure security alerts for Azure AD directory roles in PIM.

You can customize some of the security alerts in PIM to work with your environment and security goals. Follow these steps to open the security alert settings:

1. Open **Azure AD Privileged Identity Management**.
2. Click **Azure AD roles**.
3. Click **Alerts** and then **Setting**.
4. Click an alert name to configure the setting for that alert.

Part 4 – Complete.

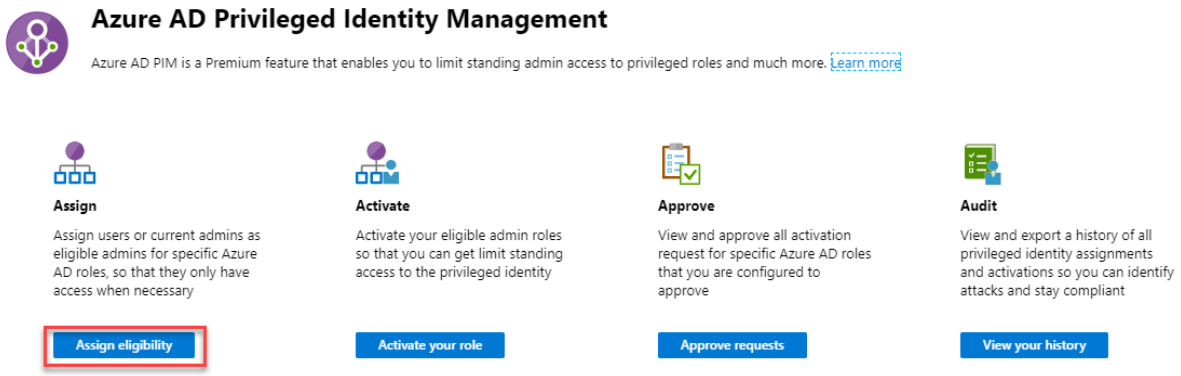
Part 5 – PIM Resource Workflows

Task 1: Configure the Global Administrator role to require approval.

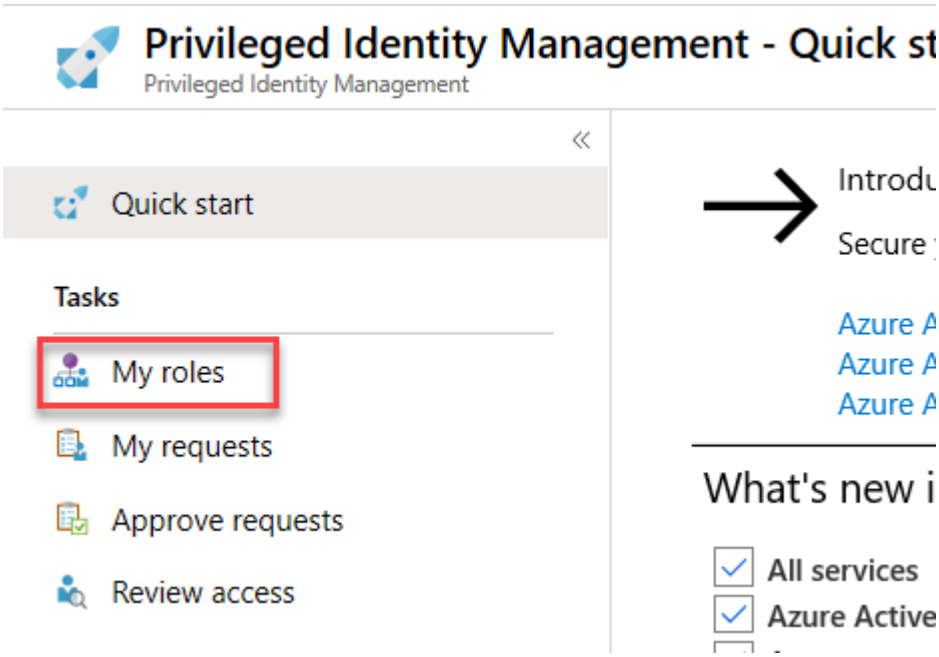
1. You should still be logged in as Global Admin from the previous exercise. Open **Azure AD Privileged Identity Management**.
2. Click **Azure AD roles**.
3. Click **Settings**
4. Select **Global Administrator**.
5. Click **Edit**, scroll down and mark **Require Approval to activate**.
6. Click **Select approver(s)** and assign Global Admin as the approver and click **Select**. Then click **Update**.

Task 2: Enable Patti for Global Administrator privileges.

1. Open **Azure AD Privileged Identity Management**.
2. Click **Azure AD roles**.
3. Click the **Quick Start** and select **Assign eligibility**.



4. Select **Global Administrator**.
5. Select **+ Add assignments** and select **Patti Fernandez**. Click **Select**.
6. Click **Next** and then click **Assign**.
7. Open an in Private Browsing session and login to https://portal.azure.com as Patti Fernandez. You might still have this browser open from earlier exercise.
8. Open **Azure AD Privileged Identity Management**.
9. Select **My Roles**.



10. **Activate** the Global Administrator Role.

11. Verify Patti's identity using the wizard if necessary.
12. Return back to **My Roles** in **Azure AD Privileged Identity Management**.
13. Click **Activate** near the Global Administrator Role.
14. Enter a reason for the activation **I need to carry out some administrative tasks** and click **Activate**.

Eventually you should see a notice that your request is "pending approval".

Task 3: Approve or deny requests for Azure resource roles in PIM.

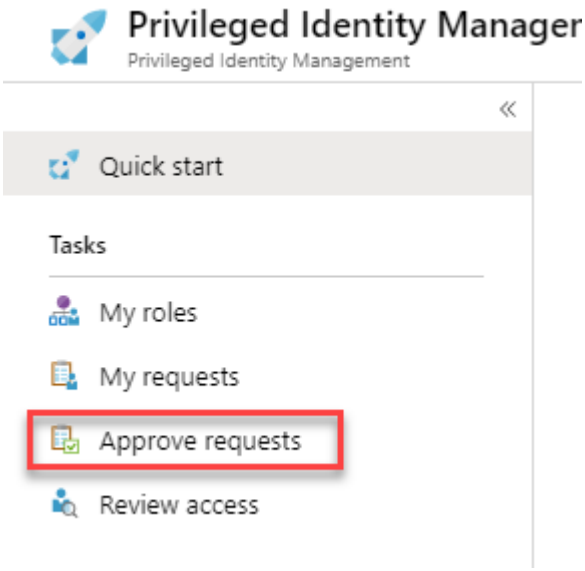
With Azure AD Privileged Identity Management (PIM), you can configure roles to require approval for activation, and choose one or multiple users or groups as delegated approvers. Follow the steps in this article to approve or deny requests for Azure resource roles.

View pending requests.

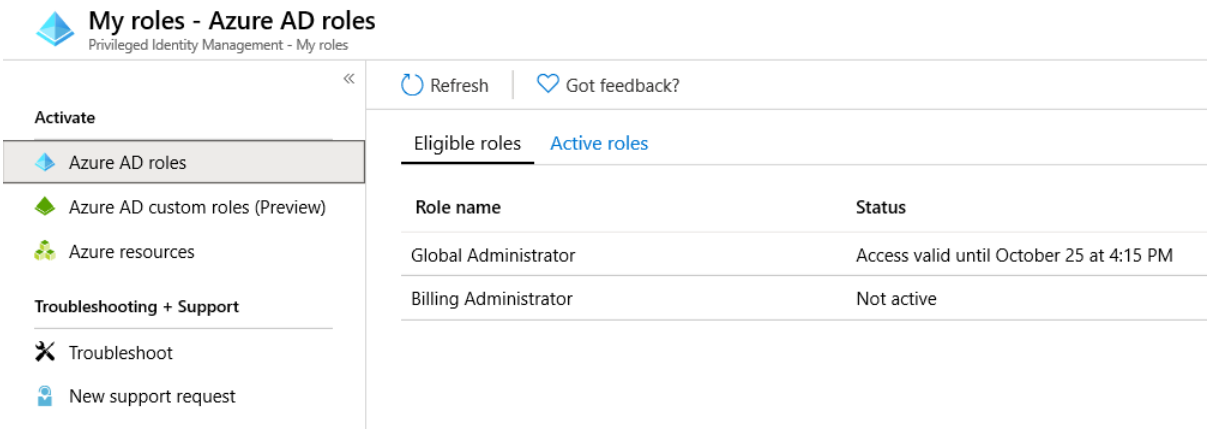
As a delegated approver, you will receive an email notification when an Azure resource role request is pending your approval. You can view these pending requests in PIM.

1. Switch back to the browser you are signed in with your Global Administrative account.

2. Open **Azure AD Privileged Identity Management**.
3. Click **Approve requests**.



4. Select the request from Patti and click **Approve**.
5. Enter a reason **Granted for this task** and click **Confirm**.
6. A notification appears that Patti is approved.
7. Switch back to the In Private Browsing session where Patti is signed in and click **My Roles** and then select **Active assignments** note the status is now activated for Global Administrator.



Part 5 – Complete.

Part 6 – View audit history for Azure AD roles in PIM

You can use the Azure Active Directory (Azure AD) Privileged Identity Management (PIM) audit history to see all the role assignments and activations within the past 30 days for all privileged roles. If you want to see the full audit history of activity in your directory, including administrator, end user, and synchronization activity, you can use the Azure Active Directory security and activity reports.

Task 1: View audit history.

Follow these steps to view the audit history for Azure AD roles.

1. As Global Admin, open **Azure AD Privileged Identity Management**.
2. Click **Azure AD roles**.
3. Click **View your history** button from the Quick start area.
4. Depending on your audit history, a column chart is displayed along with the total activations, max activations per day, and average activations per day.
5. At the bottom of the page, a table is displayed with information about each action in the available audit history. The columns have the following meanings:
6. To change the variable select the different options and click **Apply**.
7. If you desire you can export the data results by clicking the **Export** button. This will export the results to a *.CSV file.

Results: You have now completed this lab.

End lab

Thank you for taking the time to complete this lab, we hope you enjoyed it.

Please visit https://aka.ms/secpractice-labs to access further labs.