**How to Deploy PIM**

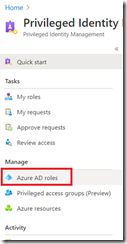
**I. Start Using PIM with Wizard**

1. The below security wizard is a simple way to begin rolling out PIM The Discovery and insights (Preview) feature in the Privileged Identity Management blade provides the easy to use wizard to begin leveraging PIM features: (https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-security-wizard).



**II. Configuring a PIM Administrator with an Active Assignment**

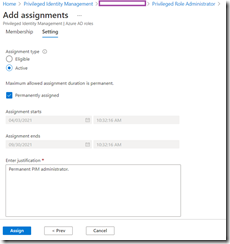
1. Assuming there is an already a planned account, The first step would be to assign the planned account to Privileged Role Administrator role for PIM administration.
2. Navigate to Azure AD roles under Manage:



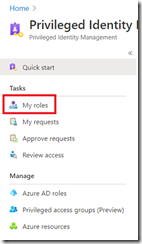
B. Then Roles and type in Privileged Role Administrator to list the PIM role, then select it: Once in the properties of the role, proceed to use the Add assignments button to add a user into the role.

(<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-give-access-to-pim#delegate-access-to-manage-pim>)

C. Configure this assignment to be active and permanently assigned but keep in mind that it is generally advised that most active assignments should be configured with a start and end time/date if possible.



1. The account specified should now be displayed under the Active assignments tab:
2. Navigating back to the Privileged Role Management page and selecting My roles:



D. Then under Azure AD roles and Active Assignments should display the roles I am currently a part of (Global Administrator and Privileged Role Administrator):

Note: that the act of granting my account the Privileged Role Administrator role will send the following notification to my email address about the assignment.

**III. Privileged Identity Management Alerts**

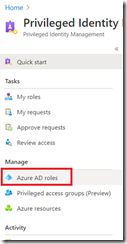
1. You can instantly view a list of issues as identified by PIM by clicking on the Alerts under the Manage settings:



1. The 3 alerts that are raised for this environment:
2. Roles don’t require multi-factor authentication for activation
3. Potential stale accounts in a privileged role
4. There are too many global administrators
5. Clicking on the Settings button will go into the configuration set for identifying these risks:
6. You can click on each of the alerts to see what configuration changes you can make as well as whether to disable them:

**IV. Assigning a User with Eligible Role (J.I.T)**

1. Next, proceed to assigning a user with the eligible role for the Global Admin role. Begin by navigating to Azure AD roles under Manage:



1. Then Roles and type in Global Admins to list the PIM role, then select it:
2. Click on Add assignments:
3. Select a user to be added the assignment
4. In the Setting tab, we will configure the Assignment type as Eligible with Permanently eligible disabled and a Assignment starts and Assignment ends date/time specified to be one day:
5. Assignment starts and Assignment ends date/time cannot exceed more than a year or the error message “Time duration specified exceeds maximum allowed” will show up
6. The role assignment should now be displayed under the Eligible assignments tab
7. After completion of assignment Admin user to the eligible role, notification emails would have been sent to the admins.

**V. Testing a User with Eligible Role**

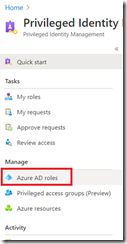
1. With the eligible role assigned to an account, we can log into the Azure portal and confirm that the user does not have the ability to create new users or reset passwords as he is eligible but not a Global Admin yet:
2. Next, navigate to the Privileged Identity Management section, click on Azure AD roles under Activate, then see that we can eligible for the Global Administrator role with the option of activating it:
3. We’ll notice that attempting to activate the role indicates we are prompted with: “Additional verification required. Click to continue”
4. The reason why this prompt is displayed is because this account does not have MFA set up and the default settings for activation is to have MFA setup
5. Proceed to set up MFA:
6. Once MFA is successfully set up, the following activation options will be displayed. Note: how there are various parameters we can configure such as the activation start time, the duration, and a reason, which is required for activation:



1. Set a duration of 2 hours mimicking the scenario that I only need 2 hours of elevated permissions. My reason for the activation will be to: Test Global Admin activation
2. The activation proceeds through 3 stages and will complete fairly quickly
3. .Upon completion of activation, the Eligible assignments tab will refresh and display the following message:”You have just activated a role. Click here to view your active roles”
4. Clicking the Click here to view your active roles will change the table to Active assignments which will display the activated state. Note the End time listed is 2 hours from when I activated it:
5. The test account user will now be able to create accounts:
6. Upon activating the Global Admin assignment, notification emails will be sent to the admins:
7. When the duration has expired an email will also be sent:

**VI Activation Role Settings Configuration**

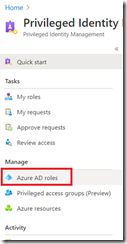
1. It is possible to customize the activation role settings in the previous activation by navigating to Azure AD roles under Manage:



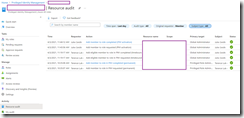
1. Roles and type in Global Admins to list the PIM role, then select it:
2. Click on Role settings to list the parameters that we can edit:
3. The configuration settings are partitioned into tabs, which I have combined into one screenshot.
4. The Activation tab allows us to:
5. Change the activation maximum duration in hours, which defaults to 8 and is customizable during the activation process
6. Requires the account to have MFA setup – why John Smith had to set up MFA
7. Require a justification – why we had to enter a reason
8. Require ticket information on activation – this will provide two fields – 1. ticket number, 2. ticketing system link
9. Require approval to activate – this feature will require another administrator to interactively approve the activation from the Azure portal
10. The Assignment tab allows us to:
11. Allow permanent eligible assignment – this can be changed to limit the amount of time an eligible assignment can be
12. Allow permanent active assignments after – this enables or disables permanent active assignment and if it is disabled, the active assignment can be force to expire after a period of time (1 year, 6 months, 3m months, 1 month, 15 days)
13. Require Azure MFA on active assignment – this will force MFA for active assignments
14. Require justification on active assignment – forces a reason to be entered
15. The Notification tab allows us to specify various notification settings for when activation or assignments take place.
16. These configuration settings are set independently for each role.

**VII: PIM Auditing**

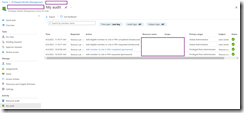
1. To perform an audit of on the activities of privileged accounts, navigate to Azure AD roles under Manage:



1. Select Resource Audit under Activity and you will see the actions of PIM administrators as well as users who have activated their eligibility for configured roles:

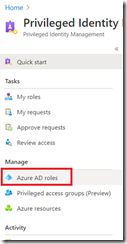


1. Clicking on a line item will bring the details of the action:
2. Navigating to the My audit section will display all the PIM activities the account logged in has made:



**VIII Creating an Access Review**

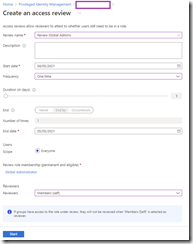
1. You can create an access review to list the specific PIM activities of a role such Global Admin by navigating to Azure AD roles under Manage:



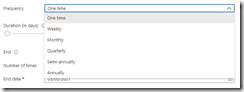
1. Then Access reviews and select New:



1. Then configure the review as required:



1. The frequency can be set to the following:



1. Note the Upon completion settings and Advanced settings that are available:
2. A review will be created in the Access reviews:
3. Clicking into the report will provide information about the PIM activity for Global Admins:

