Please note that to start this process, you must be a global administrator. It is recommended that the person determining access has a good understanding of internal IT functions throughout your organization.

Required Licensing: Azure AD Premium P2

**Determine necessary access:**

1. Read through the role descriptions at[**https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles#available-roles**](https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles#available-roles)**.** Go through the roles and determine a list of the least privileged roles for each position in your IT Department.
2. Determine roles that a user would occasionally need, and roles that the user always needs (the later should only be used for reader roles, as well as roles the user spends multiple hours a day using every day.)
3. Set up time with one person in each differing position to verify that they agree with your designations. It is typically better in this stage if there is any confusion about what a role offers, to simply offer the role with eligible status and then audit usage.
4. After implementation (see below) wait a month and audit access by completing the following steps.
5. Go to PIM <https://portal.azure.com/#blade/Microsoft_Azure_PIMCommon/CommonMenuBlade/quickStart>
6. Click “Azure AD Roles”
7. Click “Resource Audit”
8. Search for the employee who access is being audited for
9. Look for action types “[Add member to role completed (PIM activation)](https://portal.azure.com/)”
10. Click the line item
11. To discover what role was checked out Look at the field “Primary Target”
12. Review the reasoning. If the reason seems adequate, that is an appropriate role. If the reasoning can be handled with lesser roles, notate what the appropriate role will be.
13. Complete audit cycle until the correct least privileged roles have been found. Once your team determines the best access, it is recommended to complete an audit of current roles on a quarterly basis.

Configure settings for individual roles

**Assigning roles**

**Note: Before assigning roles, please create groups for each position. This is recommended even for titles with one user, as when they leave the company the new employee will only have to be put into the group rather than individually assigned each role.**

1. To assign a role the user must be assigned “Privileged Role Administrator.” To do so have another global admin assign you the role with the below steps.
2. Go to PIM <https://portal.azure.com/#blade/Microsoft_Azure_PIMCommon/CommonMenuBlade/quickStart>
3. Click “Azure AD Roles”
4. Click “roles”
5. Click on the role you will be assigning
6. Click “add assignment”
7. Choose the role group that will be assigned the role
8. Choose if the access will be permanent or eligible, and for how long.
9. Click assign

**Recommended Settings**

For roles that grant higher access it is highly recommended that settings are customized. Below are recommendations of the most crucial:

* Determine if approval is required to activate the eligible role. This will require a user from the list of approvers to review the access request and decide to approve or deny the request. By default, the approvers will be any one with that same role (eligible or active), however it is recommended that you customize the list.
* If MFA is enabled on your tenant (recommended) require MFA on Active assignment, and on activation.
* For roles being used for a project, limit the amount of time a role can be assigned. In our tenant, we had a project that required exchange admin all day for about a month. In this situation, we limited the role to a month but made a permanent assignment. This makes it so that the user has the role 24 hours a day for that time, and then it expires.
* Maximum duration. For roles that are typically used in short bursts, minimize the duration the user is able to check out a role.

**PIM user guide**

This should be sent to users who need to know how to check out a PIM role

1. Go to PIM: <https://portal.azure.com/#blade/Microsoft_Azure_PIMCommon/CommonMenuBlade/quickStart>
2. Click “Azure AD roles”
3. Click “my roles”
4. Choose the role you need to activate. If you are unsure of what role you need, descriptions can be found at [**https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles#available-roles**](https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles#available-roles)**.** Most Microsoft docs list the PIM role that you will need also, this typically is requires a bit less reading.
5. Click Activate
6. Choose a duration. Please choose a realistic amount of time. For example, if a task typically takes 30 minutes, don’t check out the role for 8 hours.
7. Give a reason as to why to role is needed.
8. Click Activate and wait for the page to refresh. Please note that if you have multiple tabs open, only that tab will have the new role. If you notice you can’t complete the task you were working on, sign in and out.

**Approving a PIM request**

1. When a PIM request comes through that requires approval, an email will be sent out from azure-noreply@microsoft.com to designated approvers.



1. Verify that the user is a user you would expect to be making this request.
2. Verify that the role is the least priviledged role they can use for the task
3. Verify that the reasoning is expected.
4. Decide to approve or deny based on this analysis.
5. Click the link that says “approve or deny request”
6. Choose the option previously chosen and state a reason.
7. Click confirm.