Create an Assigned Security Group and Add Members

1. Go to Microsoft Entra admin center → Identity → Groups.
2. Click New group.
3. Select:
   a. Group type: Security
   b. Group name: YourName-Access-Assigned
   c. Description: "Group for manual membership assignment"
   d. Membership type: Assigned
4. Create the group.
5. After creation, open the group and go to Members → Add members.
6. Add at least two user accounts.
7. Verify the group membership.

Create a Dynamic Group Based on User Attributes

Automatically group all users whose department = IT.

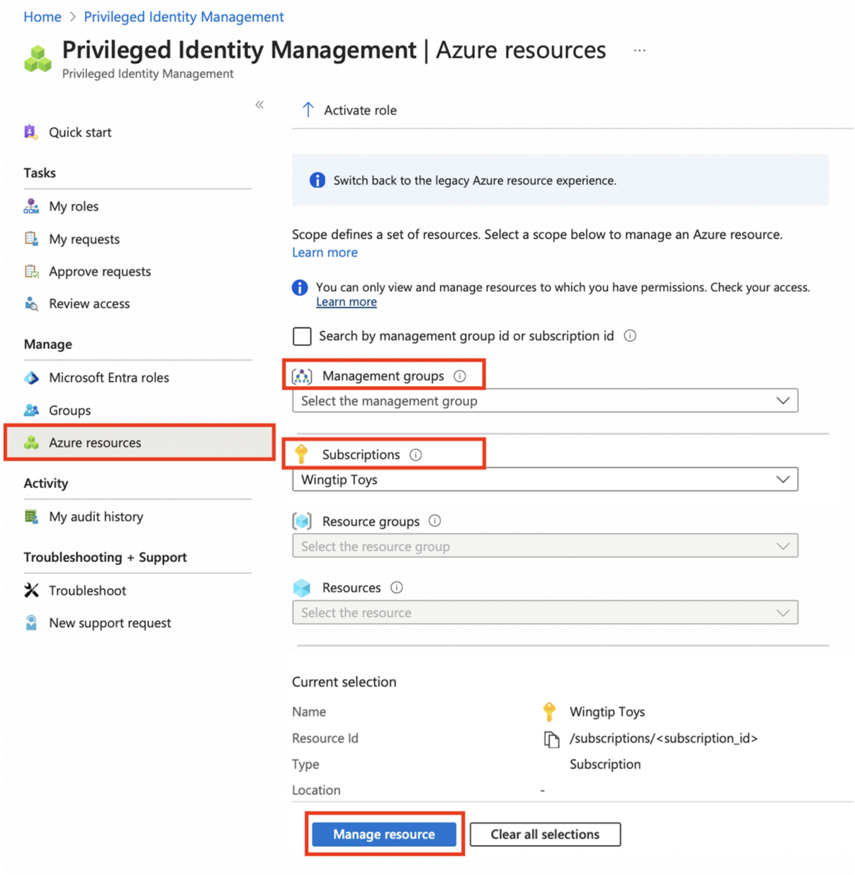
1. Go to Microsoft Entra admin center → Identity → Groups.
2. Click New group.
3. Select:
   - Group type: Security
   - Group name: IT-Department-Dynamic
   - Description: "Automatically includes users from IT department"
   - Membership type: Dynamic User
4. In Dynamic user members, click Add dynamic query.
5. Add this rule:
   - (user.department -eq "IT")
6. Save the rule → Create the group.
7. Go to Dynamic membership to see evaluation results.

The group is automatically populated with all users whose Department = IT, and updates itself whenever user attributes change.

Configure Azure resource role settings in Privileged Identity Management

Configure PIM for Azure Resources Roles

1. Go to Entra admin center ID Governance > Privileged Identity Management > Azure Resources
   - https://entra.microsoft.com/
2. Select the resource type you want to manage.
   - Start at either the Management group dropdown
   - Subscriptions dropdown
   - Resource groups
   - Resources



Home > Privileged Identity Management

Privileged Identity Management | Azure resources ···

Privileged Identity Management

«

Quick start

Tasks

My roles

My requests

Approve requests

Review access

Manage

Microsoft Entra roles

Groups

Azure resources

Activity

My audit history

Troubleshooting + Support

Troubleshoot

New support request

Activate role

Switch back to the legacy Azure resource experience.

Scope defines a set of resources. Select a scope below to manage an Azure resource. Learn more

You can only view and manage resources to which you have permissions. Check your access. Learn more

□ Search by management group id or subscription id ⓘ

Management groups ⓘ

Select the management group

Subscriptions ⓘ

Wingtip Toys

Resource groups ⓘ

Select the resource group

Resources ⓘ

Select the resource

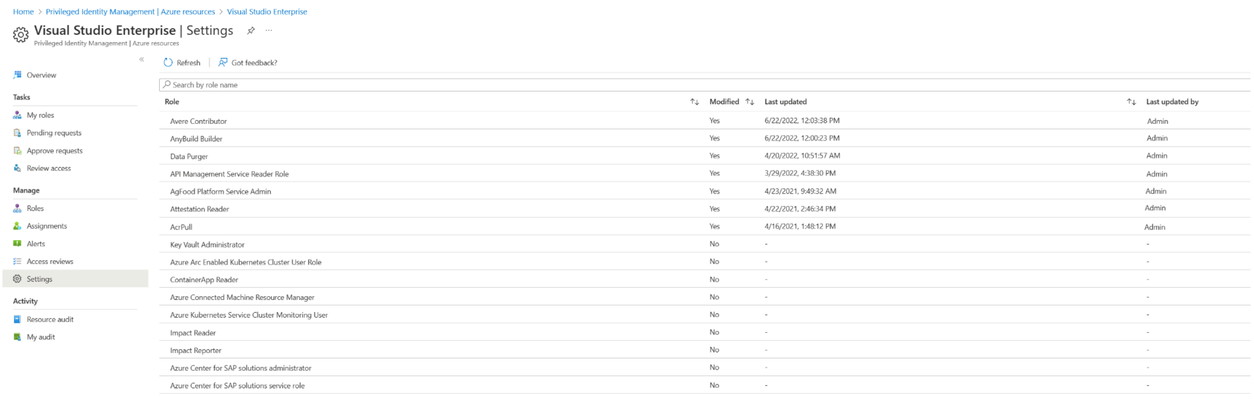
Current selection

Name	Wingtip Toys
Resource Id	/subscriptions/<subscription_id>
Type	Subscription
Location	-

Manage resource

Clear all selections

3. Select the resource for which you need to configure PIM role settings.
4. Select Settings. View a list of PIM policies for a selected resource.
5. Select the role or policy that you want to configure.
6. Select Edit to update role settings.
7. Select Update.

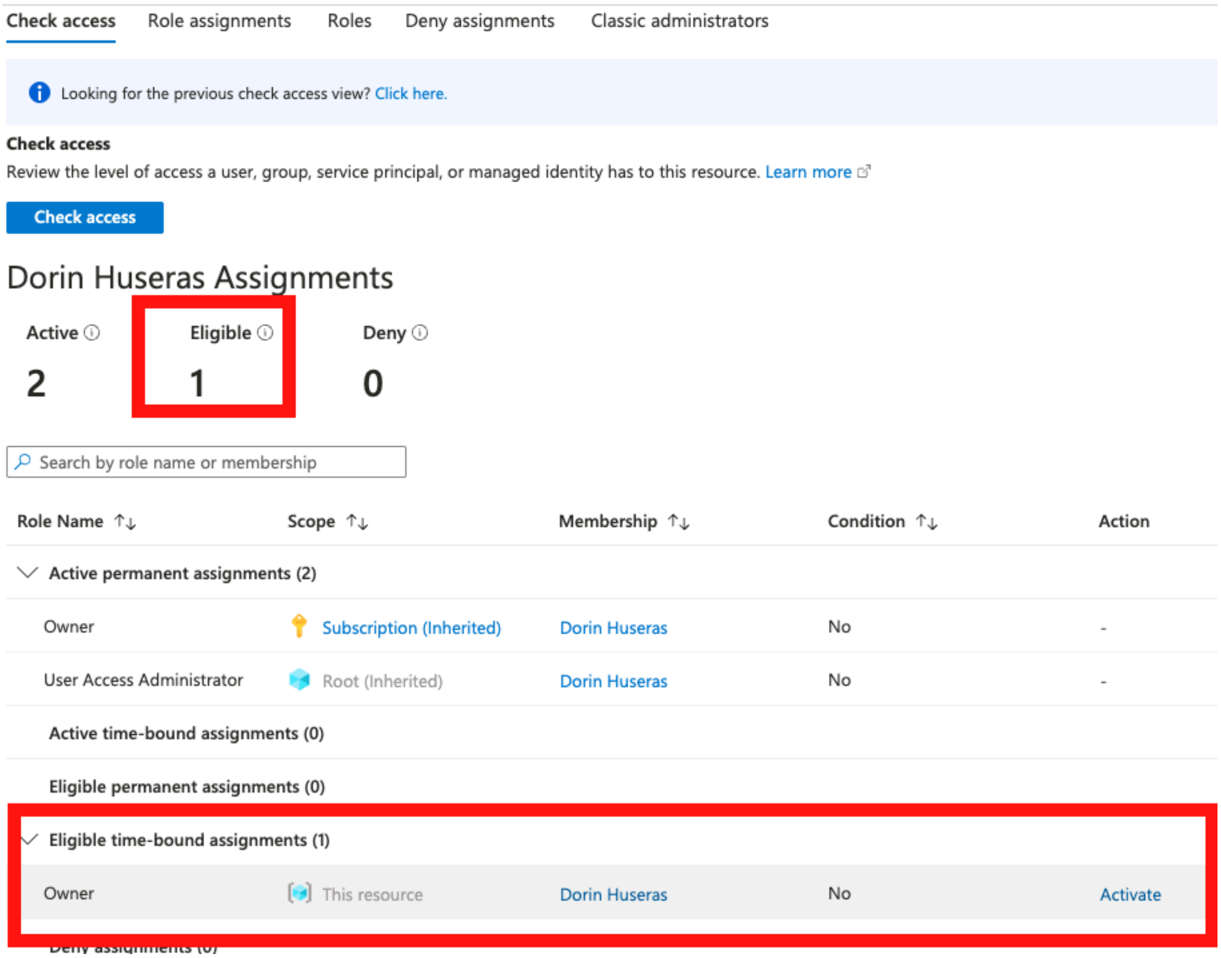


Home > Privileged Identity Management | Azure resources > Visual Studio Enterprise

Visual Studio Enterprise | Settings

Privileged Identity Management | Azure resources

Role ↑↓	Modified ↑↓	Last updated ↑↓	Last updated by
Avere Contributor	Yes	6/22/2022, 12:03:38 PM	Admin
AnyBuild Builder	Yes	6/22/2022, 12:00:23 PM	Admin
Data Purger	Yes	4/20/2022, 10:51:57 AM	Admin
API Management Service Reader Role	Yes	3/29/2022, 4:38:30 PM	Admin
AgFood Platform Service Admin	Yes	4/23/2021, 9:49:32 AM	Admin
Attestation Reader	Yes	4/22/2021, 2:46:34 PM	Admin
AcrPull	Yes	4/16/2021, 1:48:12 PM	Admin
Key Vault Administrator	No	-	-
Azure Arc Enabled Kubernetes Cluster User Role	No	-	-
ContainerApp Reader	No	-	-
Azure Connected Machine Resource Manager	No	-	-
Azure Kubernetes Service Cluster Monitoring User	No	-	-
Impact Reader	No	-	-
Impact Reporter	No	-	-
Azure Center for SAP solutions administrator	No	-	-
Azure Center for SAP solutions service role	No	-	-



Looking for the previous check access view? Click here.

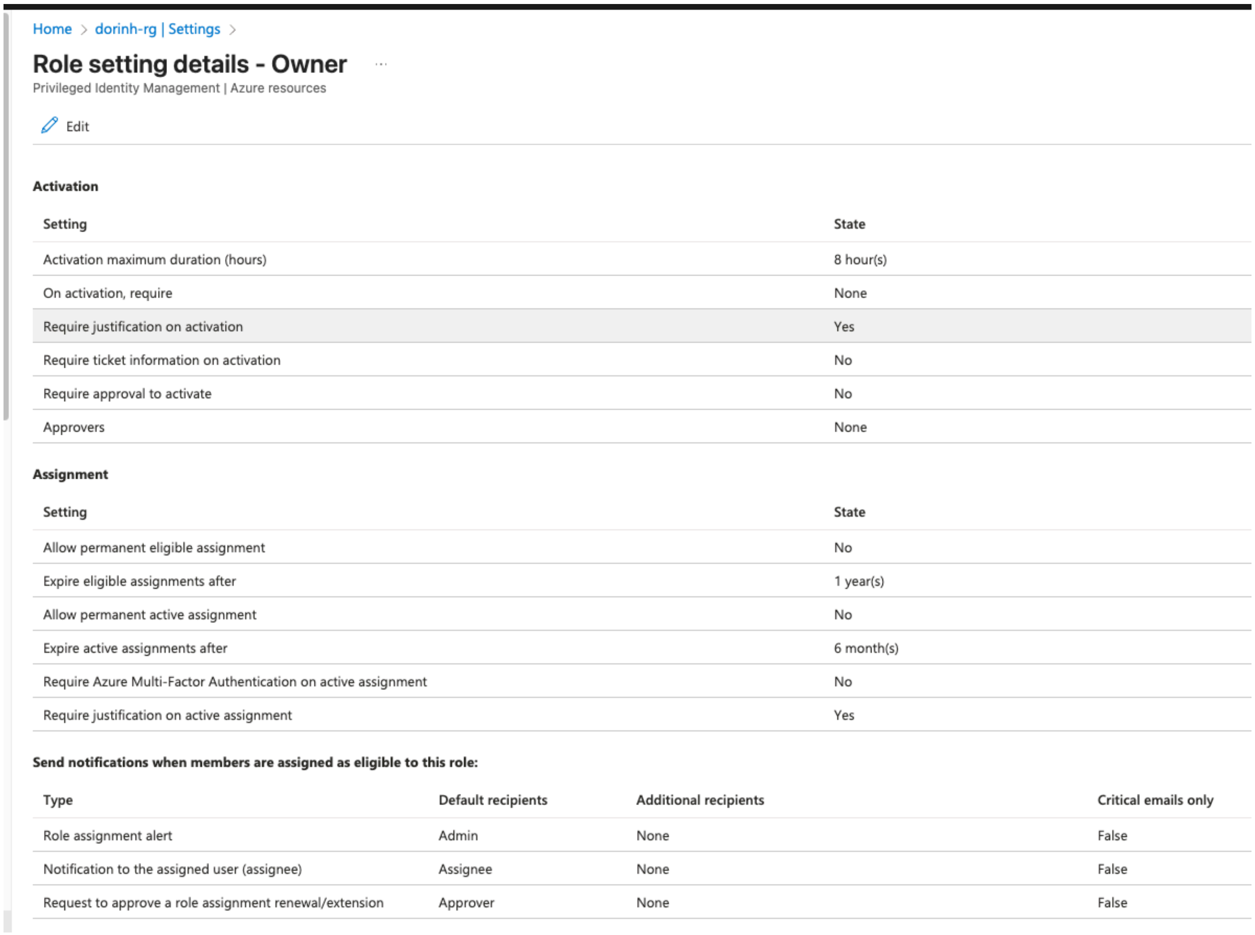
Check access

Review the level of access a user, group, service principal, or managed identity has to this resource. Learn more

Dorin Huseras Assignments

Active	Eligible	Deny
2	1	0

Role Name ↑↓	Scope ↑↓	Membership ↑↓	Condition ↑↓	Action
Active permanent assignments (2)				
Owner	Subscription (Inherited)	Dorin Huseras	No	-
User Access Administrator	Root (Inherited)	Dorin Huseras	No	-
Active time-bound assignments (0)				
Eligible permanent assignments (0)				
Eligible time-bound assignments (1)				
Owner	This resource	Dorin Huseras	No	Activate
Deny assignments (0)				



Home > dorinh-rg | Settings >

Role setting details - Owner

Privileged Identity Management | Azure resources

Edit

Activation

Setting	State
Activation maximum duration (hours)	8 hour(s)
On activation, require	None
Require justification on activation	Yes
Require ticket information on activation	No
Require approval to activate	No
Approvers	None

Assignment

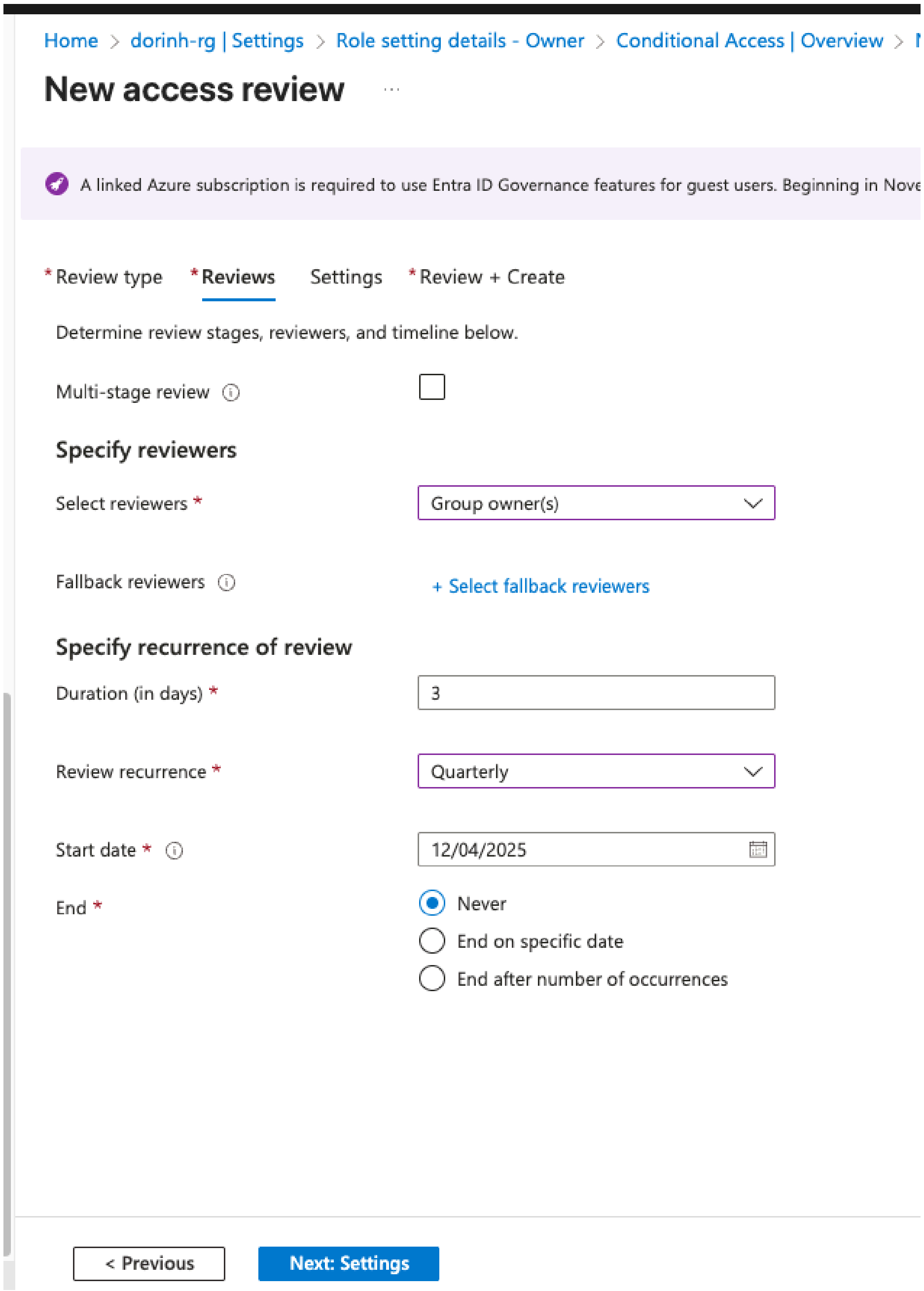
Setting	State
Allow permanent eligible assignment	No
Expire eligible assignments after	1 year(s)
Allow permanent active assignment	No
Expire active assignments after	6 month(s)
Require Azure Multi-Factor Authentication on active assignment	No
Require justification on active assignment	Yes

Send notifications when members are assigned as eligible to this role:

Type	Default recipients	Additional recipients	Critical emails only
Role assignment alert	Admin	None	False
Notification to the assigned user (assignee)	Assignee	None	False
Request to approve a role assignment renewal/extension	Approver	None	False

Create a single-stage access review

1. Sign in to the Microsoft Entra admin center as at least an Identity Governance Administrator.
2. Browse to ID Governance > Access Reviews.
3. Select New access review to create a new access review.
4. On review Type:
   - ○ Select Teams+Grouop
   - ○ Select the group that you created
5. Select a reviewer
6. Select a Start Date


Home > dorinh-rg | Settings > Role setting details - Owner > Conditional Access | Overview > I
*Review type
*Reviews
Settings
*Review + Create
< Previous
Next: Settings

New access review ···

A linked Azure subscription is required to use Entra ID Governance features for guest users. Beginning in Nove

Determine review stages, reviewers, and timeline below.

Multi-stage review ⓘ □

Specify reviewers

Select reviewers * Group owner(s)

Fallback reviewers ⓘ + Select fallback reviewers

Specify recurrence of review

Duration (in days) * 3

Review recurrence * Quarterly

Start date * ⓘ 12/04/2025

End *
● Never
○ End on specific date
○ End after number of occurrences