Azure/EntraID Role Assignments

Thimo Limpert
Azure DevOps Engineer

Sponsors

FEITIAN
WE BUILD SECURITY

glueck kanja

q.beyond

VISORIAN

What to expect?

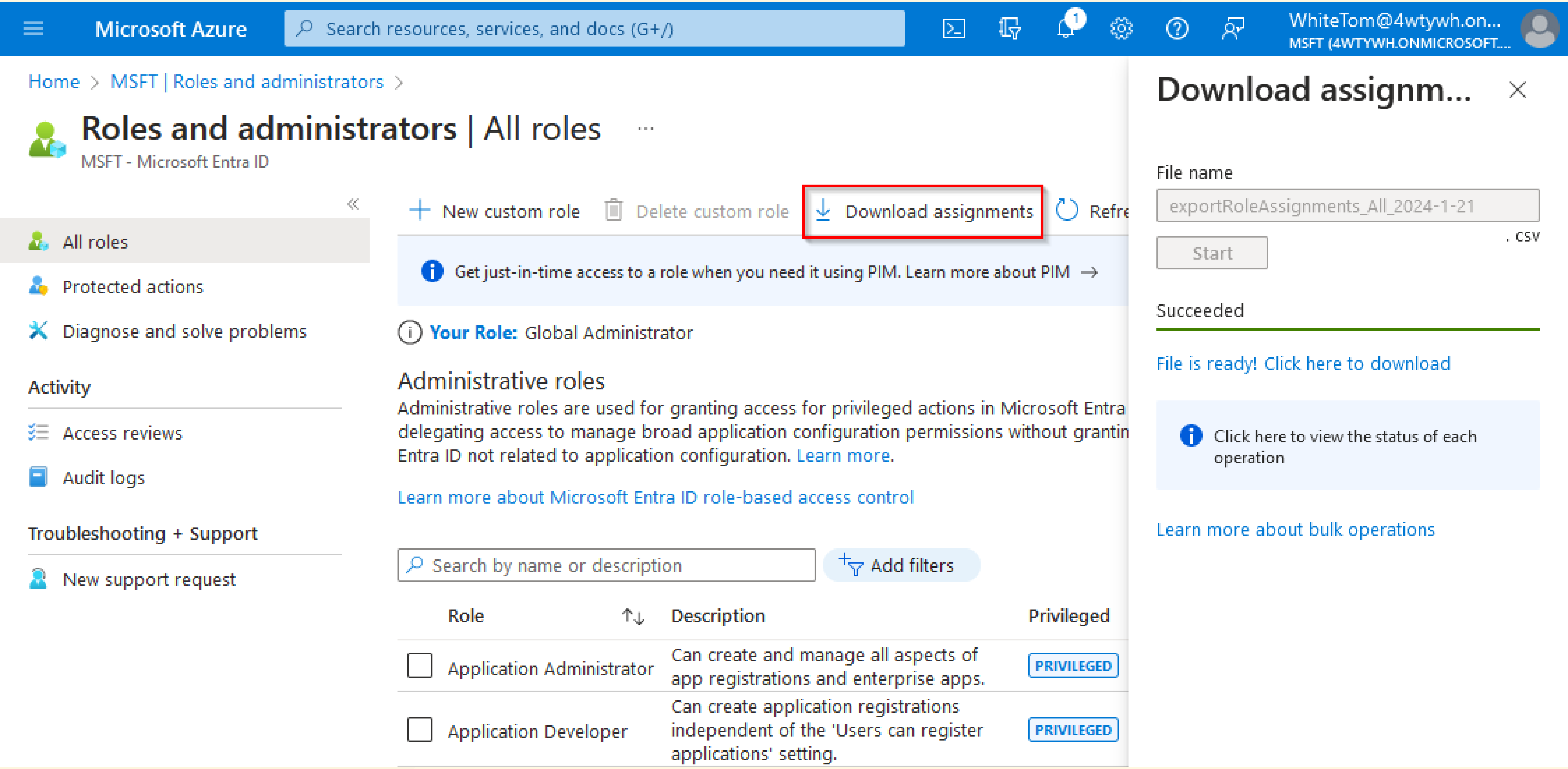
- Invisible not yet active Eligible Role Assignments in Portal
- Role Assignments that's shouldn't be possible

How it all started

> “ I want to check if only Admin Users have assigned Roles. Therefore, I need a report about all Role Assignments in Azure & EntraID. ”

Start with Entra ID

Naive Thimo



Microsoft Azure
Search resources, services, and docs (G+/)
WhiteTom@4wtywh.on...
MSFT (4WTYWH.ONMICROSOFT....
Home > MSFT | Roles and administrators >
All roles
Protected actions
Diagnose and solve problems
Activity
Access reviews
Audit logs
Troubleshooting + Support
New support request
New custom role
Delete custom role
Download assignments
Refre
Search by name or description
Add filters

Roles and administrators | All roles

MSFT - Microsoft Entra ID

Get just-in-time access to a role when you need it using PIM. Learn more about PIM →

Your Role: Global Administrator

Administrative roles

Administrative roles are used for granting access for privileged actions in Microsoft Entra delegating access to manage broad application configuration permissions without grantin Entra ID not related to application configuration. Learn more.

Learn more about Microsoft Entra ID role-based access control

	Role	Description	Privileged
□	Application Administrator	Can create and manage all aspects of app registrations and enterprise apps.	PRIVILEGED
□	Application Developer	Can create application registrations independent of the 'Users can register applications' setting.	PRIVILEGED

Download assignm...

File name

exportRoleAssignments_All_2024-1-21 .csv

Start

Succeeded

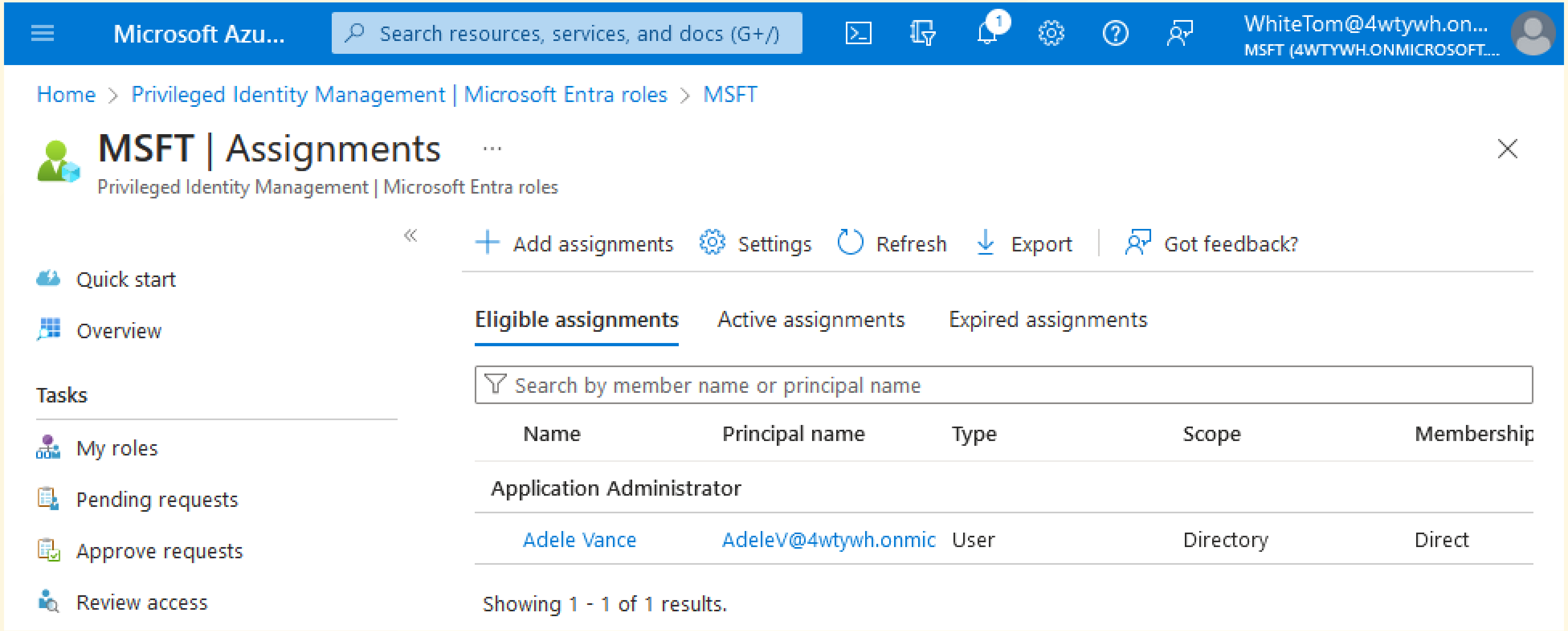
File is ready! Click here to download

Click here to view the status of each operation

Learn more about bulk operations

Privileged Identity Management

- manage, control, and monitor access to important resources
- Allows Eligible assignments, that users can activate when needed



MSFT | Assignments

Privileged Identity Management | Microsoft Entra roles

Name	Principal name	Type	Scope	Membership
Application Administrator				
Adele Vance	AdeleV@4wtywh.onmic	User	Directory	Direct

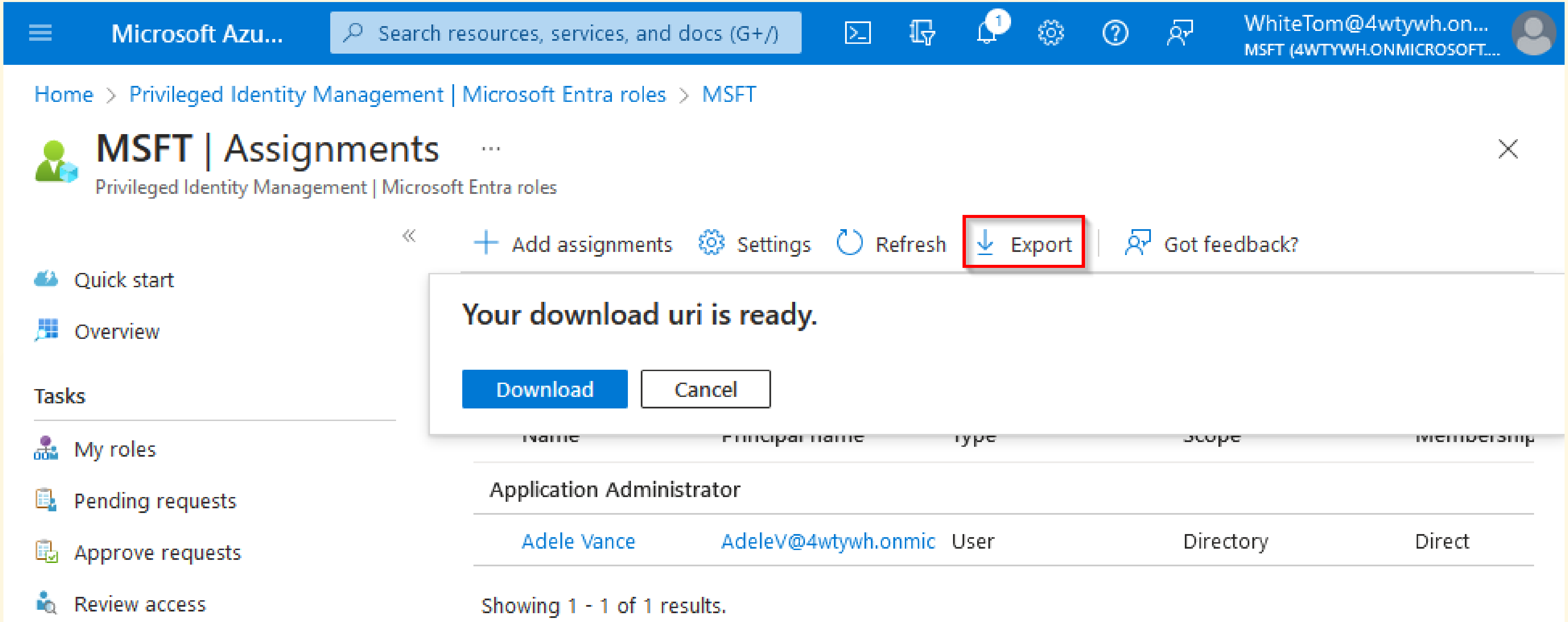
Showing 1 - 1 of 1 results.

EntraID Export results

displayName	roleDisplayName	directoryScopeId	And More...
WhiteTom	Global Administrator	/	

- ✓ Looks good!
- ⏸ Wait! What about PIM?

Export via PIM



MSFT | Assignments

Privileged Identity Management | Microsoft Entra roles

Your download uri is ready.

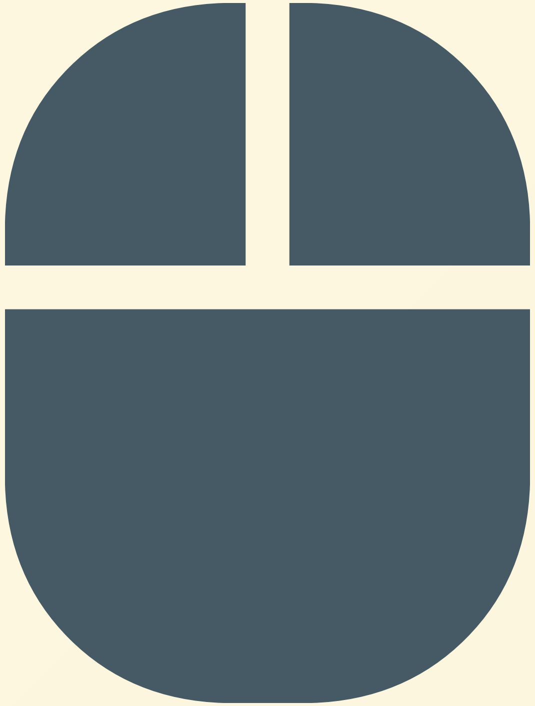
Download | Cancel

Name	Principal name	Type	Scope	Membership
Application Administrator				
Adele Vance	AdeleV@4wtywh.onmic	User	Directory	Direct

Showing 1 - 1 of 1 results.

What is included in the export?

State	User Group Name	Role Name	Start Time	End Time	Member Type
Eligible	Adele Vance	Application Administrator	2024-01-21 13:05:43Z	Permanent	Direct
Active	Adele Vance	Application Administrator	2024-01-21 14:11:13Z	2024-01-21 22:11:13Z	Direct
Active	WhiteTom	Global Administrator		Permanent	Direct



- Who likes to use the Mouse?
  - 😠 I don't!

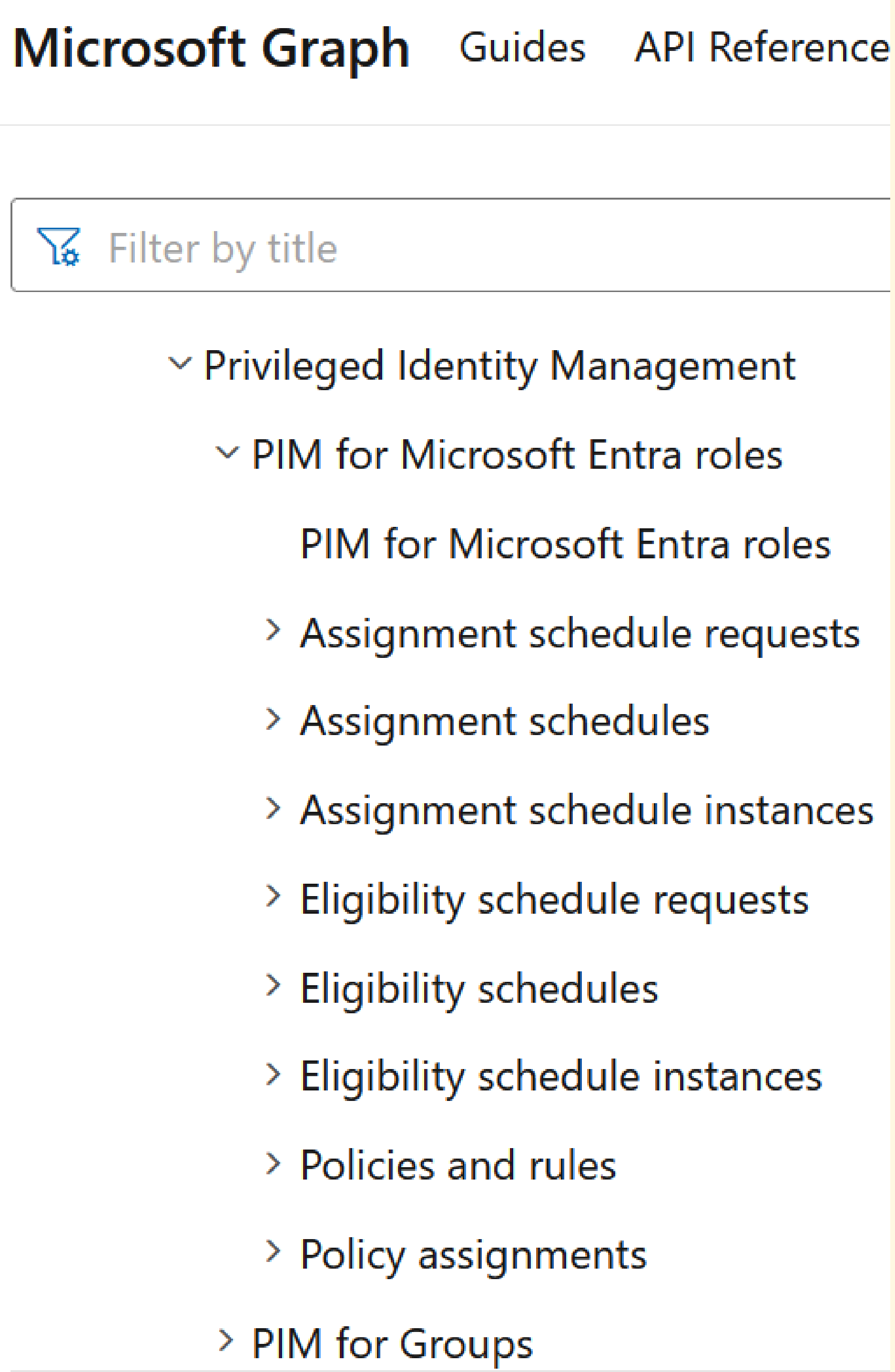
Graph APIs

> “ Microsoft Graph is a RESTful web API that enables you to access Microsoft Cloud service resources. ”

- Everyone seems to use `roleManagement/directory/roleAssignments` as *Active* role assignments
- Some refer to `/roleManagement/directory/roleEligibilityScheduleInstances` as *Eligible* role assignments in PIM

Documentation

- `Assignment *`
  - Ignored, we got the other API for that
- `Eligibility schedule requests`
  - Represents a request for a role eligibility
- `Eligibility Schedule` vs. `Eligibility Schedule Instance`



Microsoft Graph Guides API Reference

Filter by title

- Privileged Identity Management
  - PIM for Microsoft Entra roles
    - PIM for Microsoft Entra roles
    - Assignment schedule requests
    - Assignment schedules
    - Assignment schedule instances
    - Eligibility schedule requests
    - Eligibility schedules
    - Eligibility schedule instances
    - Policies and rules
    - Policy assignments
  - PIM for Groups

Eligibility Schedule Instance

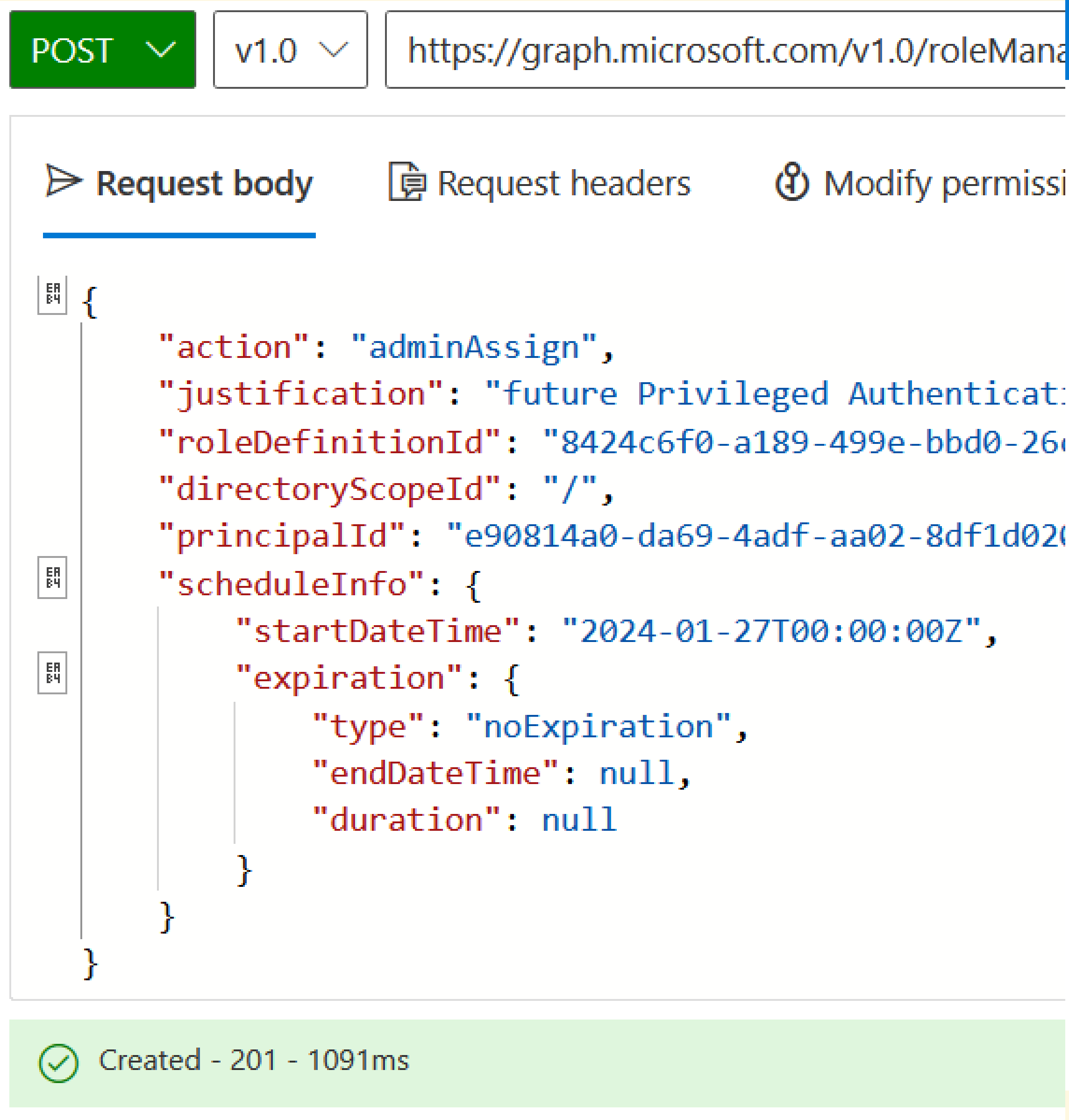
> Represents the instance for a role eligibility in your tenant.

- Used by most people in the Internet & Azure Portal
- Outputs all Eligibility visible in Portal
- ? What is *Eligibility Schedule*?

Eligibility Schedule

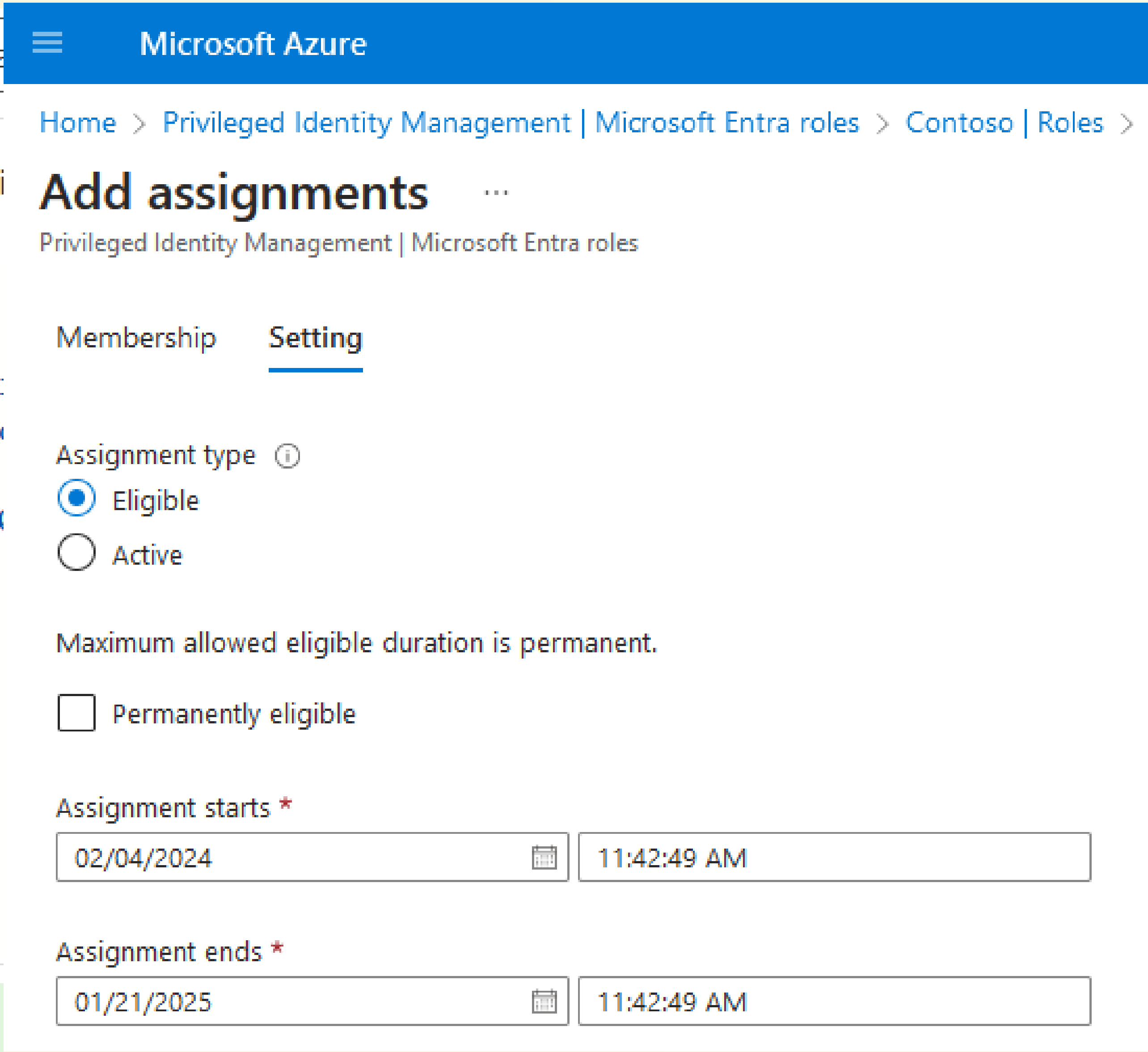
> “ Represents a schedule for a role eligibility in your tenant and is used to instantiate a EligibilityScheduleInstance. ”

- ⓘ What is the difference?
- `EligibilityScheduleInstance` has Properties `startDateTime`, `endDateTime`, `roleEligibilityScheduleId`
- `EligibilitySchedule` has Property `scheduleInfo` of type `requestSchedule`



```
{
    "action": "adminAssign",
    "justification": "future Privileged Authenticat
    "roleDefinitionId": "8424c6f0-a189-499e-bbd0-26
    "directoryScopeId": "/",
    "principalId": "e90814a0-da69-4adf-aa02-8df1d02
    "scheduleInfo": {
        "startDateTime": "2024-01-27T00:00:00Z",
        "expiration": {
            "type": "noExpiration",
            "endDateTime": null,
            "duration": null
        }
    }
}
```

Created - 201 - 1091ms


Microsoft Azure
Home > Privileged Identity Management | Microsoft Entra roles > Contoso | Roles >

Add assignments ...

Privileged Identity Management | Microsoft Entra roles

Assignment type

● Eligible

○ Active

Maximum allowed eligible duration is permanent.

□ Permanently eligible

Assignment starts *

02/04/2024 11:42:49 AM

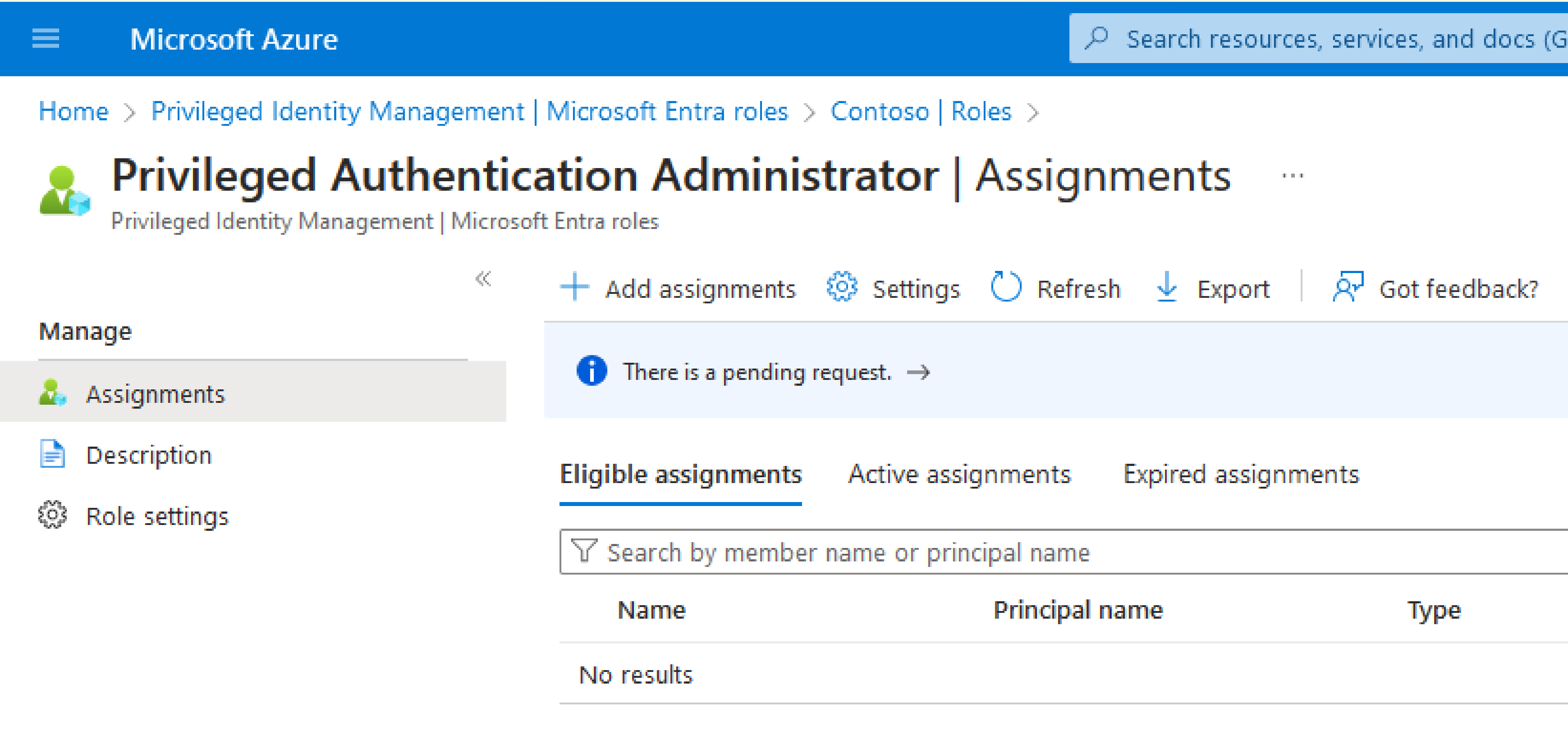
Assignment ends *

01/21/2025 11:42:49 AM

```
flowchart LR
    EligibilityScheduleRequest -- "Approved" --> EligibilitySchedule
    EligibilitySchedule -- at start Time --> EligibilityScheduleInstance
```

What do we see in Portal/Exports?

- ❗ Current Eligible Assignments
- 😢 No Eligible Assignments in the future 😢
  - BUT: Microsoft is improving and adding a hint



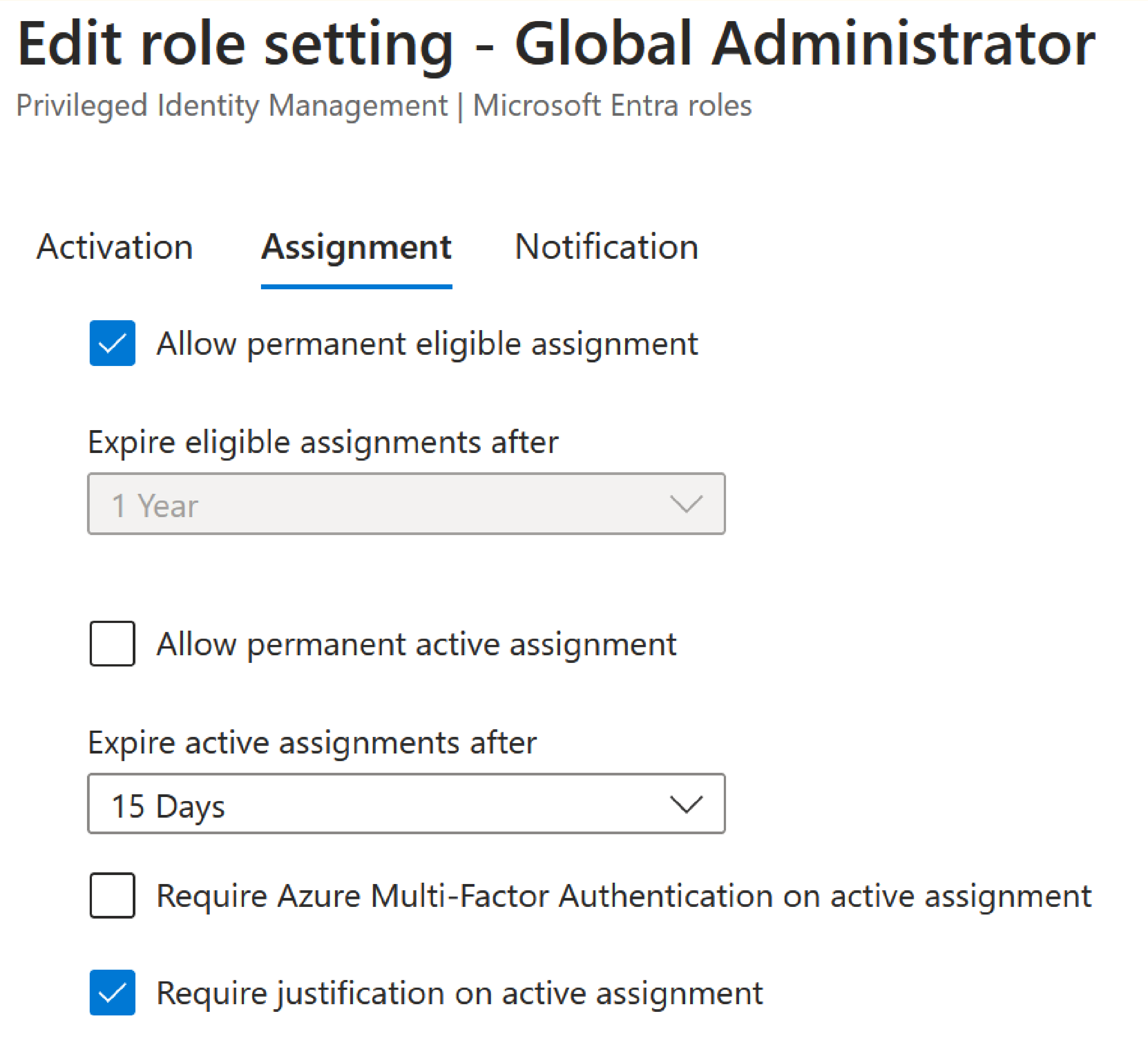
Microsoft Azure
Search resources, services, and docs (G
Home > Privileged Identity Management | Microsoft Entra roles > Contoso | Roles >
Privileged Authentication Administrator | Assignments ...
Privileged Identity Management | Microsoft Entra roles
Manage
Assignments
Description
Role settings
+ Add assignments
Settings
Refresh
Export
Got feedback?
Eligible assignments
Active assignments
Expired assignments
Search by member name or principal name

There is a pending request. →

Name	Principal name	Type
No results		

PIM Settings

- What happens, when you create a permanent active assignment?



Edit role setting - Global Administrator

Privileged Identity Management | Microsoft Entra roles

☑ Allow permanent eligible assignment

Expire eligible assignments after

1 Year

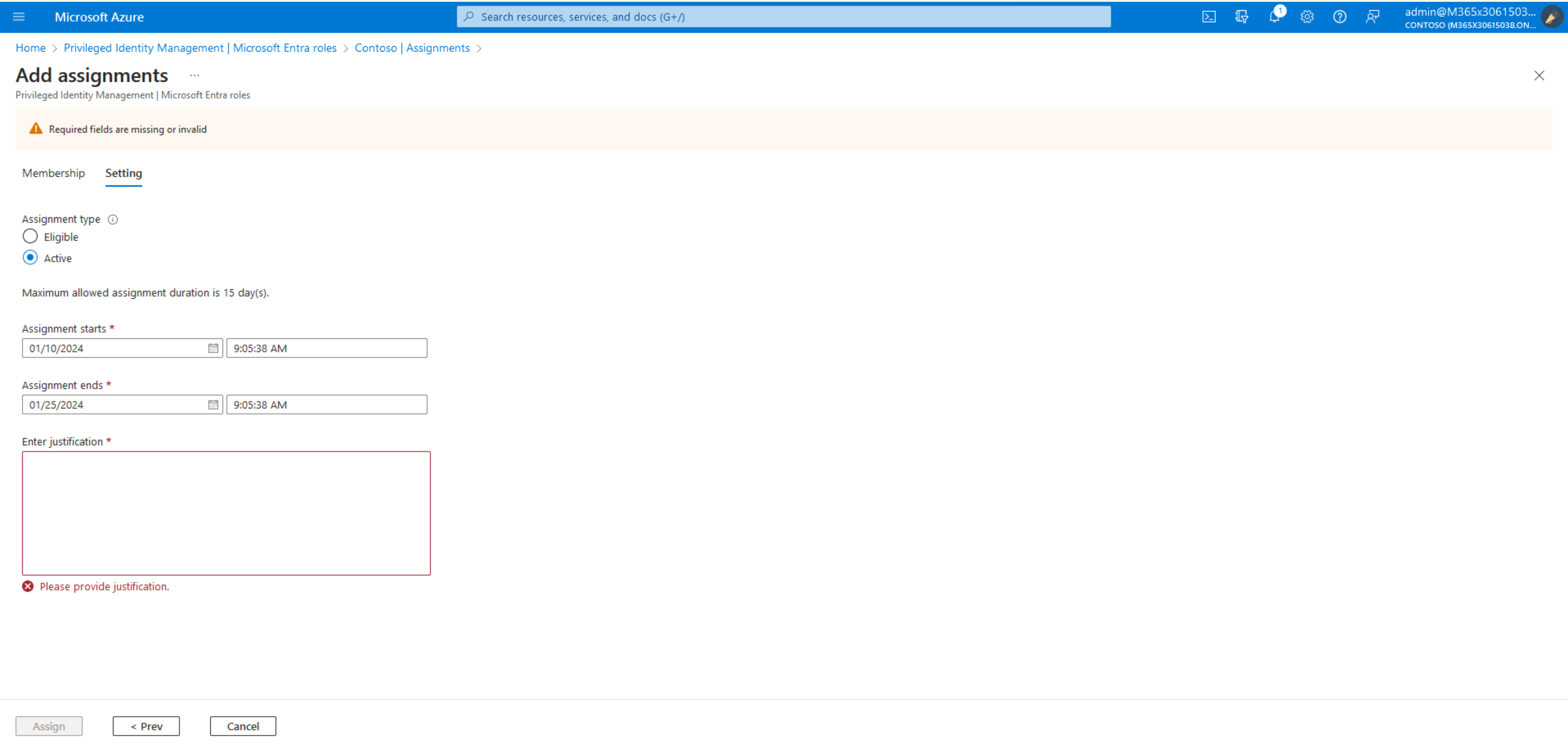
□ Allow permanent active assignment

Expire active assignments after

15 Days

□ Require Azure Multi-Factor Authentication on active assignment

☑ Require justification on active assignment


Microsoft Azure
Search resources, services, and docs (G+/)
admin@M365x3061503...
CONTOSO (M365X30615038.ON...
Home > Privileged Identity Management | Microsoft Entra roles > Contoso | Assignments >
Membership
Setting
Assign
< Prev
Cancel

Add assignments

Privileged Identity Management | Microsoft Entra roles

Required fields are missing or invalid

Assignment type

○ Eligible

● Active

Maximum allowed assignment duration is 15 day(s).

Assignment starts *

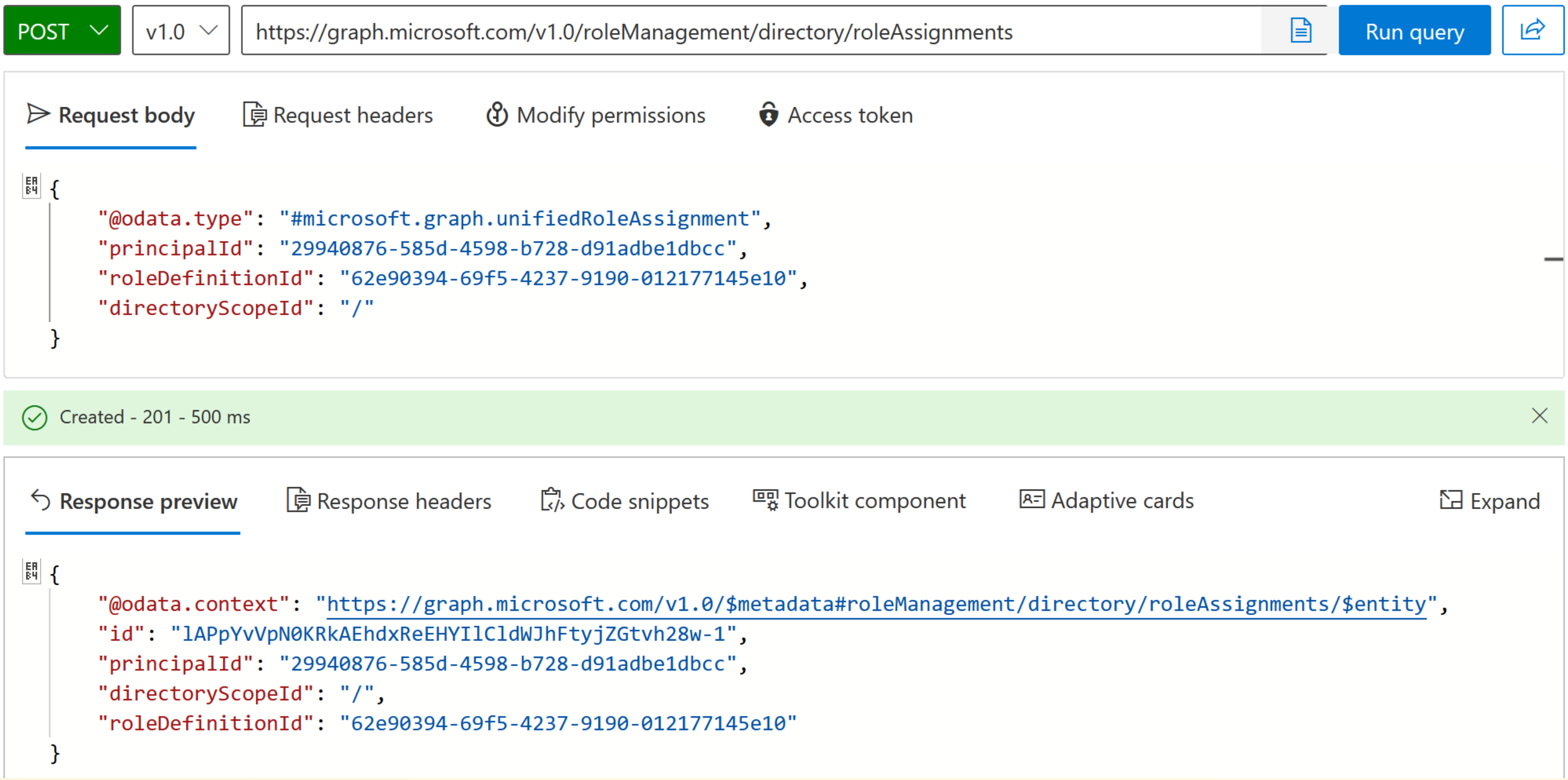
01/10/2024 9:05:38 AM

Assignment ends *

01/25/2024 9:05:38 AM

Enter justification *

Please provide justification.



https://graph.microsoft.com/v1.0/roleManagement/directory/roleAssignments

```
{
    "@odata.type": "#microsoft.graph.unifiedRoleAssignment",
    "principalId": "29940876-585d-4598-b728-d91adbe1dbcc",
    "roleDefinitionId": "62e90394-69f5-4237-9190-012177145e10",
    "directoryScopeId": "/"
}
```

Created - 201 - 500 ms

```
{
    "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#roleManagement/directory/roleAssignments/$entity",
    "id": "lAPpYvVpN0KRkAEhdxReEHYIlCldWJhFtyjZGtvh28w-1",
    "principalId": "29940876-585d-4598-b728-d91adbe1dbcc",
    "directoryScopeId": "/",
    "roleDefinitionId": "62e90394-69f5-4237-9190-012177145e10"
}
```

Summary

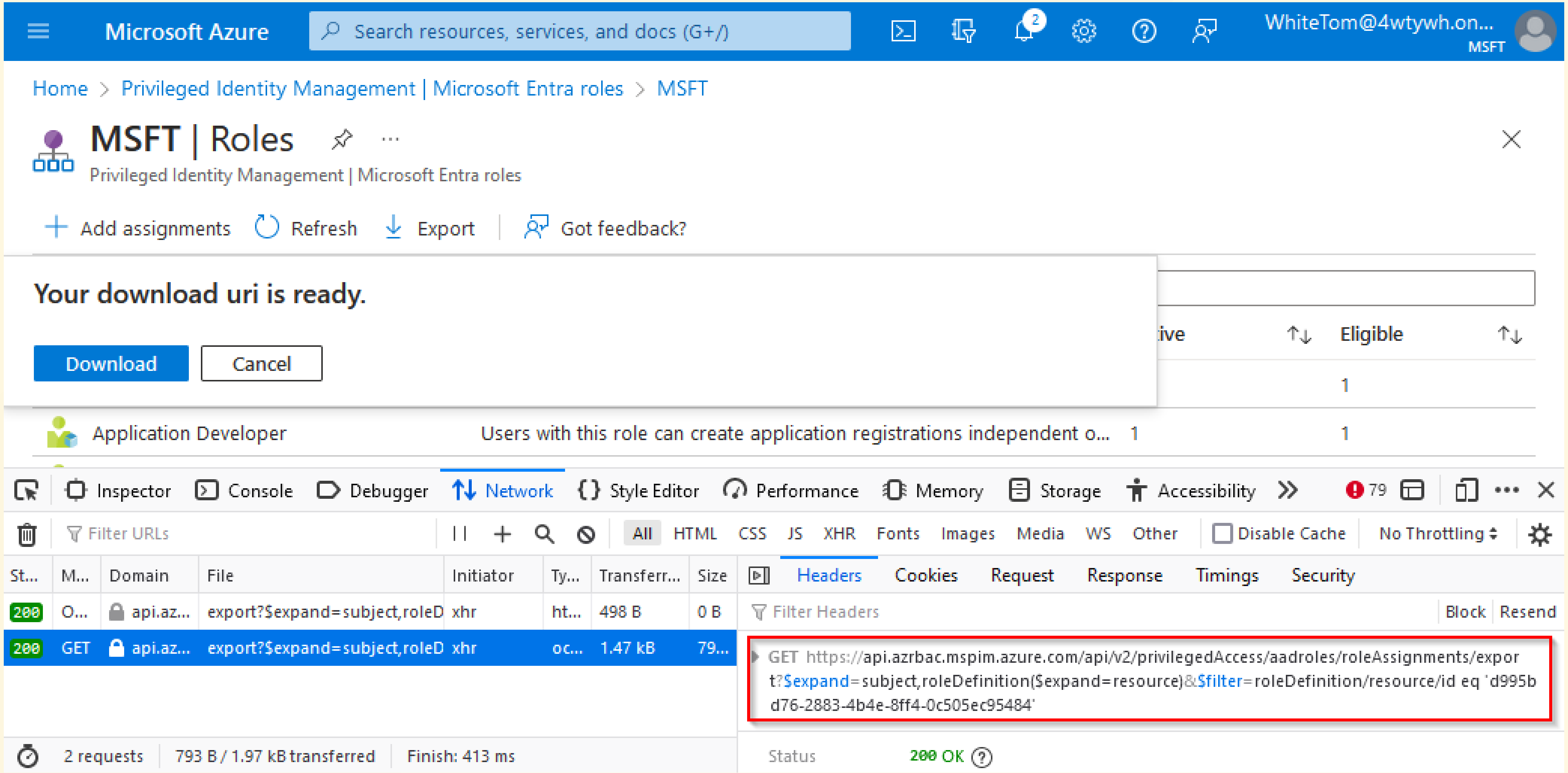
- Not all Export Buttons do the same
- Not yet instantiated Eligible assignments ~~neither shown~~, nor exported
    - at least a hint in PIM is there now
- Permanent Active Assignments seem possible although not allowed

Additional Information

Comparison EntraID Export vs PIM Export

- EntraID Export
  - ✕ Doesn't include PIM Eligible roles
  - ❕ Contains activated roles (without end date)
- PIM Export
  - ✓ Includes Active & Eligible Assignments
  - ❕ Doesn't include transitive group assignments
  - ❔ Purpose of Member Type

API used by Portal Export



Your download uri is ready.

Download | Cancel

Application Developer	Users with this role can create application registrations independent o...	1	1

St...	M...	Domain	File	Initiator	Ty...	Transferr...	Size
200	O...	api.az...	export?$expand=subject,roleD	xhr	ht...	498 B	0 B
200	GET	api.az...	export?$expand=subject,roleD	xhr	oc...	1.47 kB	79...

2 requests | 793 B / 1.97 kB transferred | Finish: 413 ms

```
GET https://api.azrbac.mspim.azure.com/api/v2/privilegedAccess/aadroles/roleAssignments/export?$expand=subject,roleDefinition($expand=resource)&$filter=roleDefinition/resource/id eq 'd995bd76-2883-4b4e-8ff4-0c505ec95484'
```

Status 200 OK

```
https://api.azrbac.mspim.azure.com/api/v2/privilegedAccess/aadroles/
  roleAssignments/export?
    $expand=subject,roleDefinition($expand=resource)&
    $filter=roleDefinition/resource/id eq 'd995bd76-2883-4b4e-8ff4-0c505ec95484'
```

Anyone knows this API?

- internal API for PIM
- Let's not use that! Alternatives?
- Use `Graph API` instead