Automate Identity Lifecycle Management with Microsoft Entra ID Access Packages

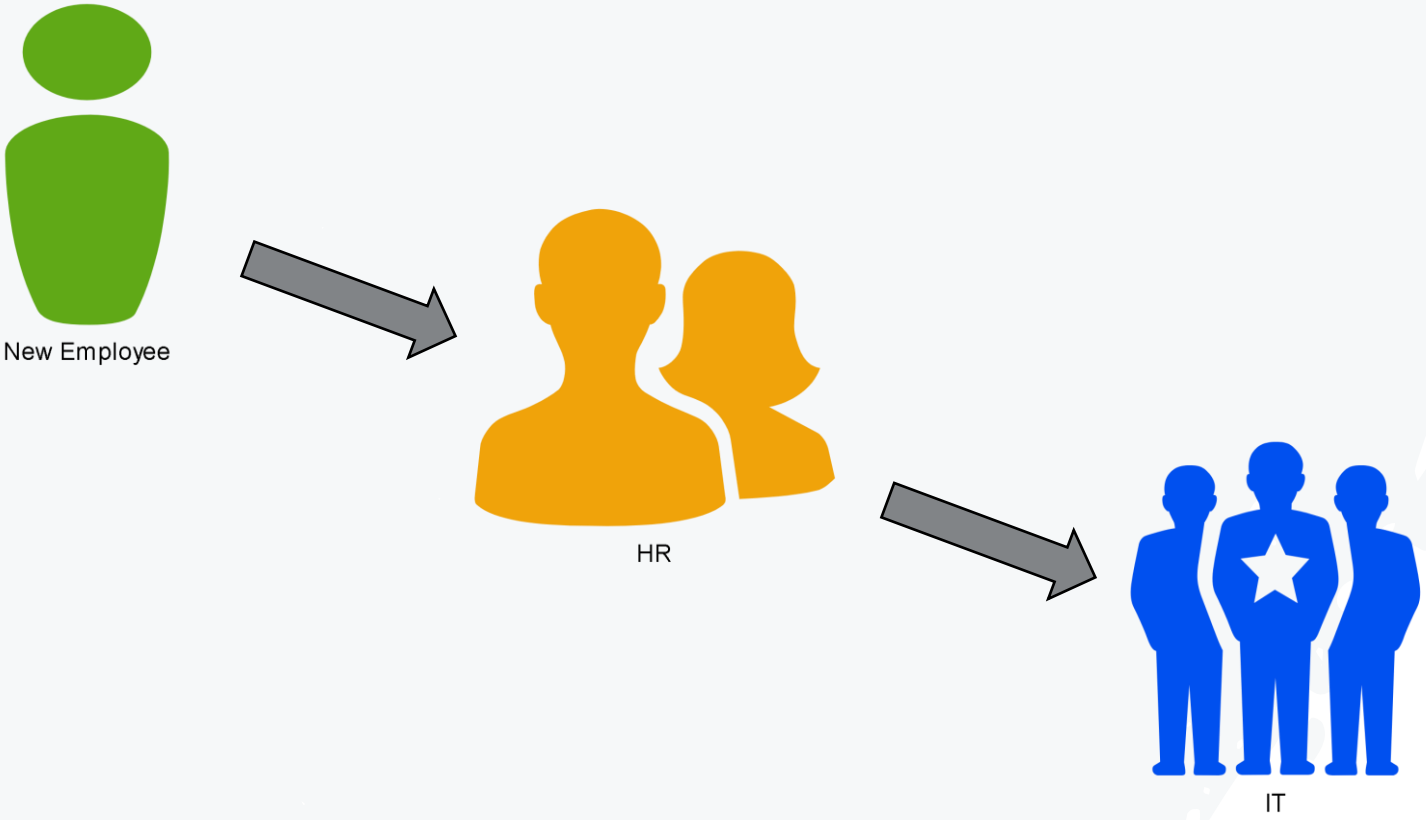
Patrick de Kruijf – Azure Architect

https://www.linkedin.com/in/patrickdk
https://www.azurefreakconfessions.com

Rik Groenewoud – Customer Success Manager

https://www.linkedin.com/in/rikgroenewoud
https://www.cloudwoud.nl

Pain: New employee process



Possible solutions

Privileged Identity Management	Self Service Groups	Identity Governance Access Packages
Azure	Azure	Azure, SharePoint/Teams and Applications
Just in Time (JIT) access	Regular group membership	Conditioned group membership
Short term access	Permanent access	Regulated access
Admin managed	Group owner managed	Self-Service with approvals

What are access packages

Automation

Access Requests

Access Reviews

Expirations

Lifecycle Workflows

Manage access

Entra ID Groups

Applications

SharePoint/ Teams sites

Solves

Clear access requirements and expirations

Clear who should approve requests

Managed access for external users

Access Package requirements

Entra ID Tenant

Least: Catalog Creator and Access Package Manager

~~Easy: Identity Governance Administrator~~

Licenses

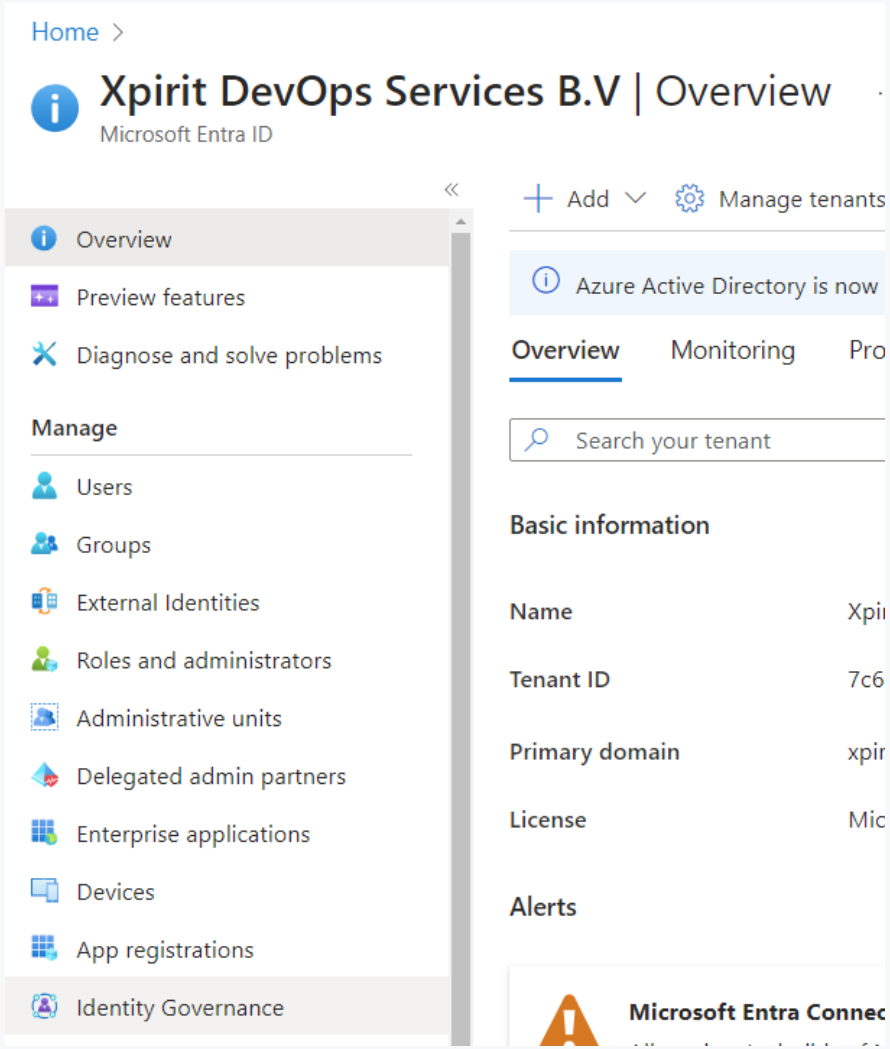
Microsoft Entra ID P2

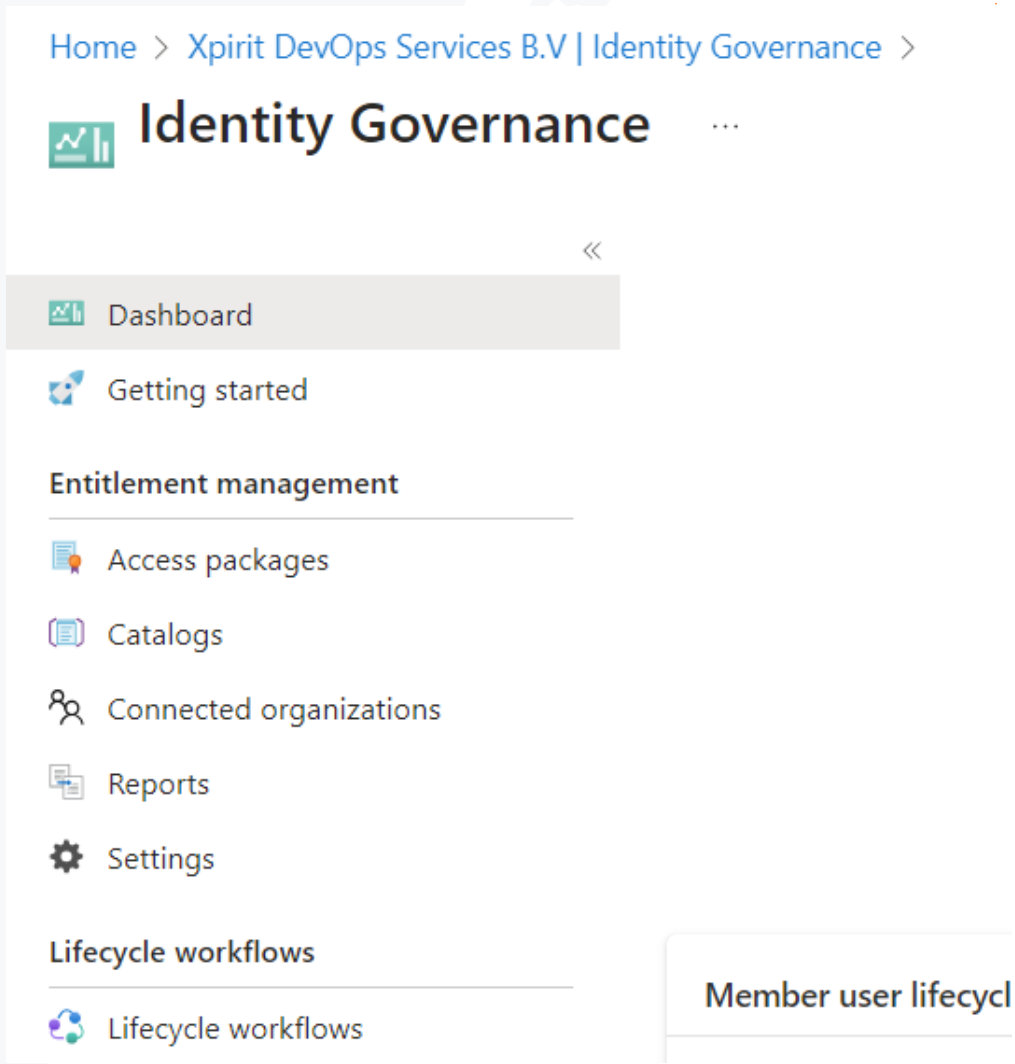
Microsoft Entra ID Governance (step-up for Microsoft Entra ID P2) ➔ *For advanced features*

Advanced Features

- Lifecycle Workflows (LCW)
- Entitlement management + Auto Assignment Policies
- Entitlement management + Custom Extensions (Logic Apps)
- Entitlement management - Guest Conversion API
- Entitlement management - Directly Assign Any User(Preview)

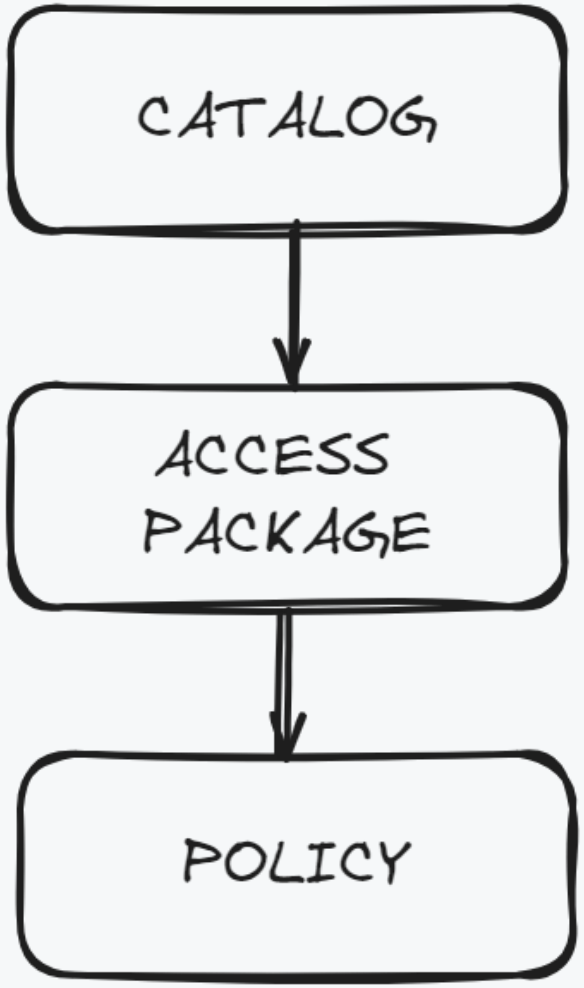
Where to find the Access Packages?

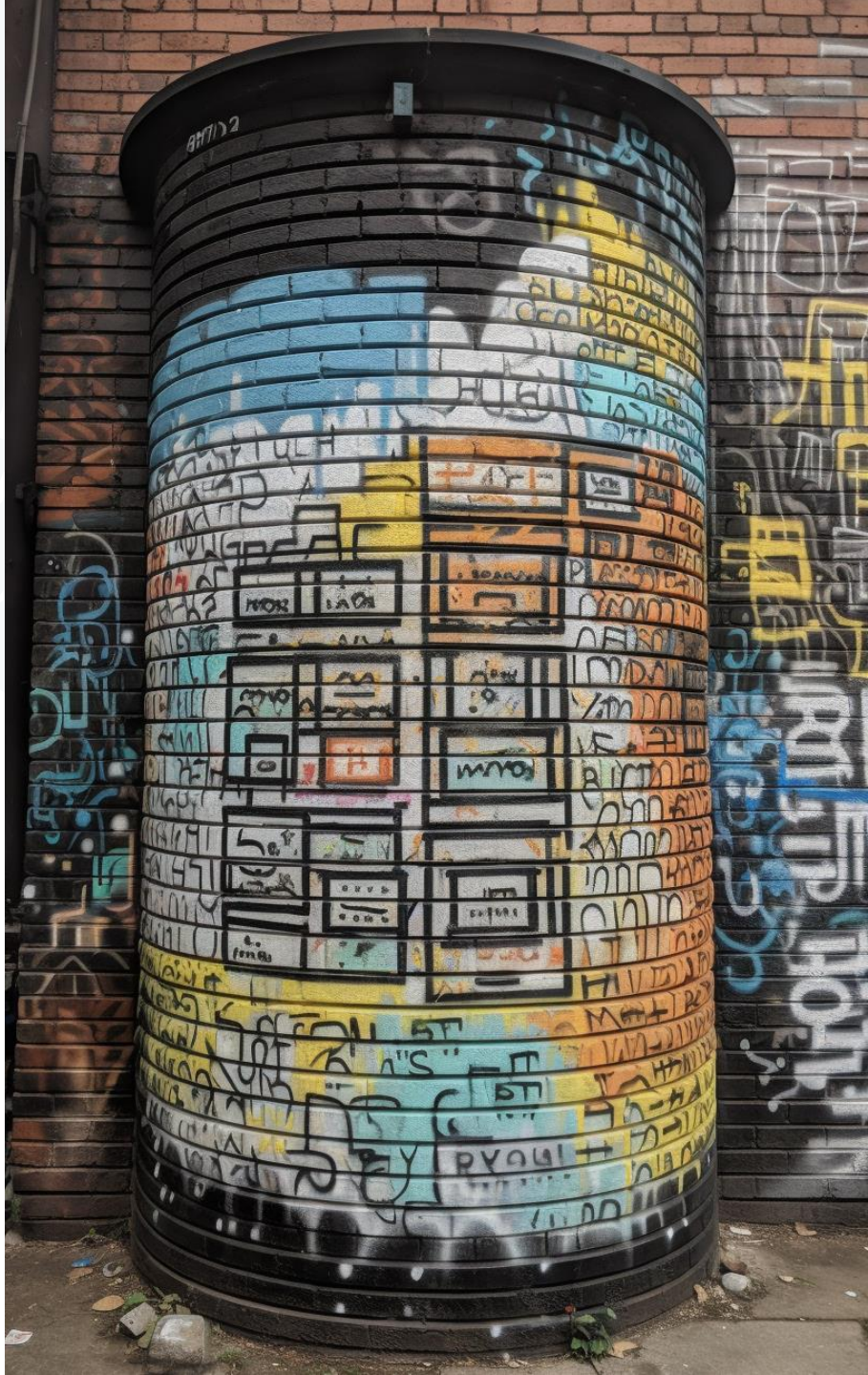




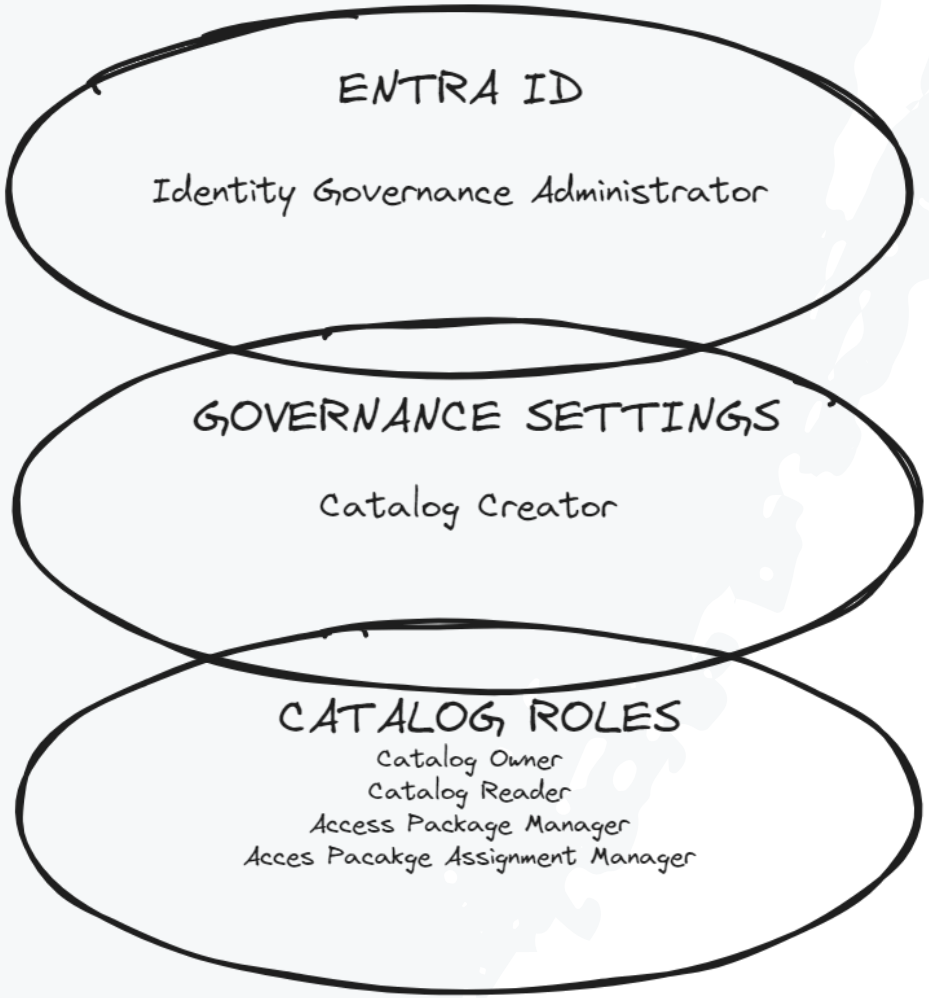
Deep Dive

Structure

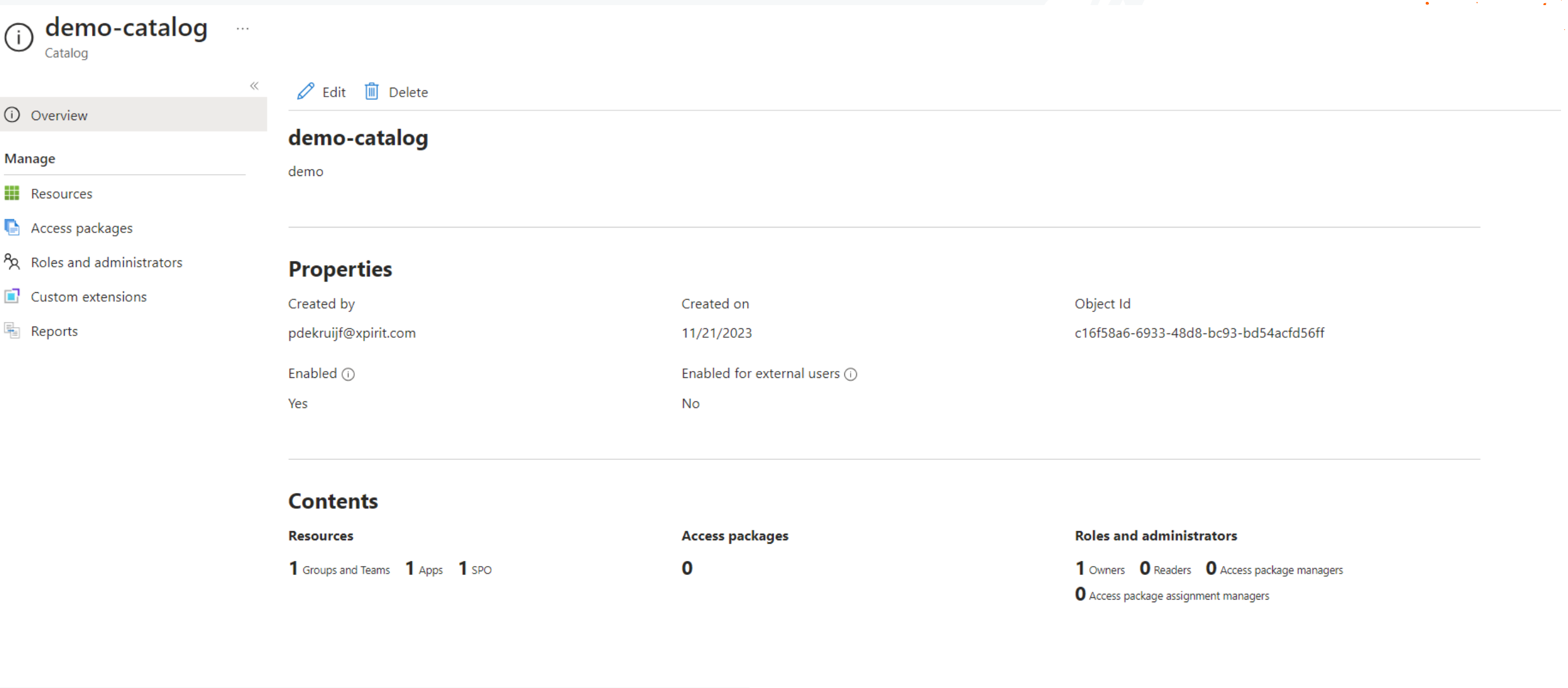




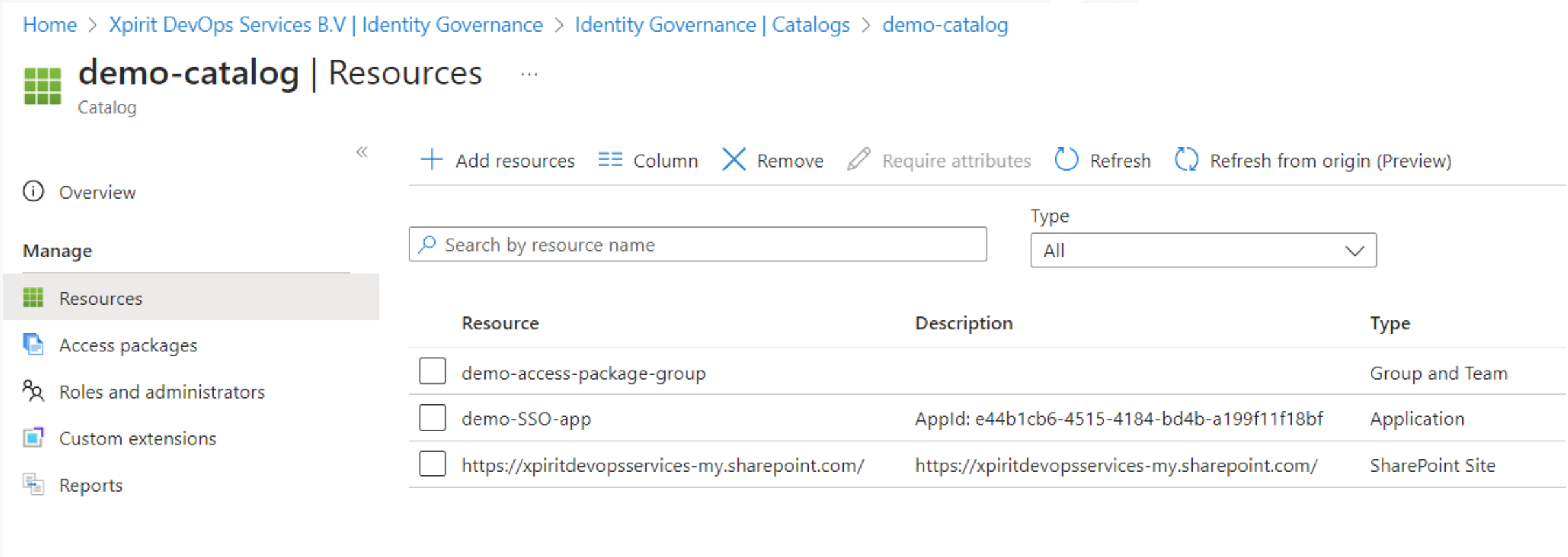
Access Control



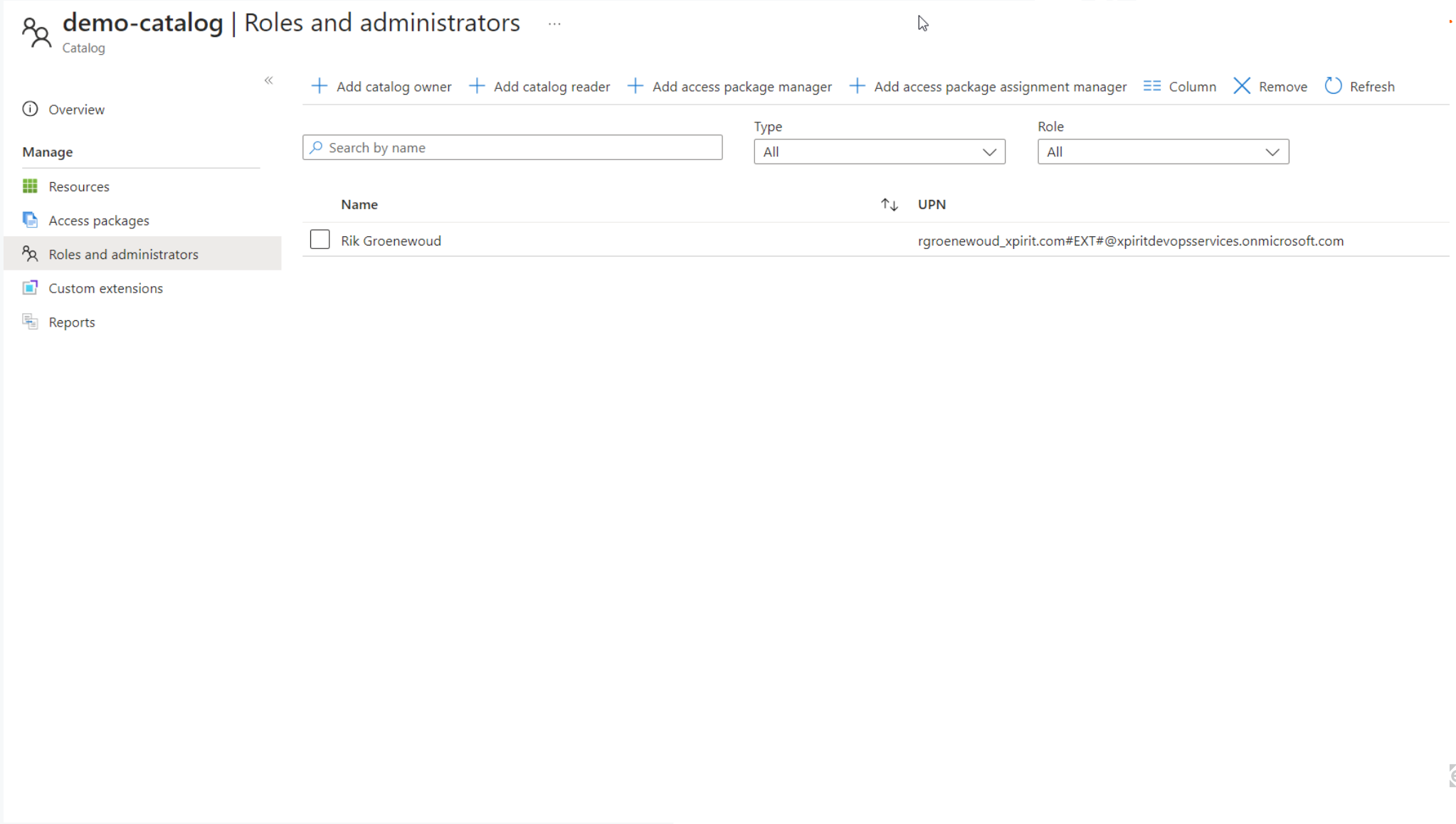
Catalog


demo-catalog
Catalog
Overview
Manage
Resources
Access packages
Roles and administrators
Custom extensions
Reports
Edit
Delete
demo-catalog
demo
Properties
Created by
pdekruijf@xpirit.com
Created on
11/21/2023
Object Id
c16f58a6-6933-48d8-bc93-bd54acfd56ff
Enabled
Yes
Enabled for external users
No
Contents
Resources
1 Groups and Teams
1 Apps
1 SPO
Access packages
0
Roles and administrators
1 Owners
0 Readers
0 Access package managers
0 Access package assignment managers

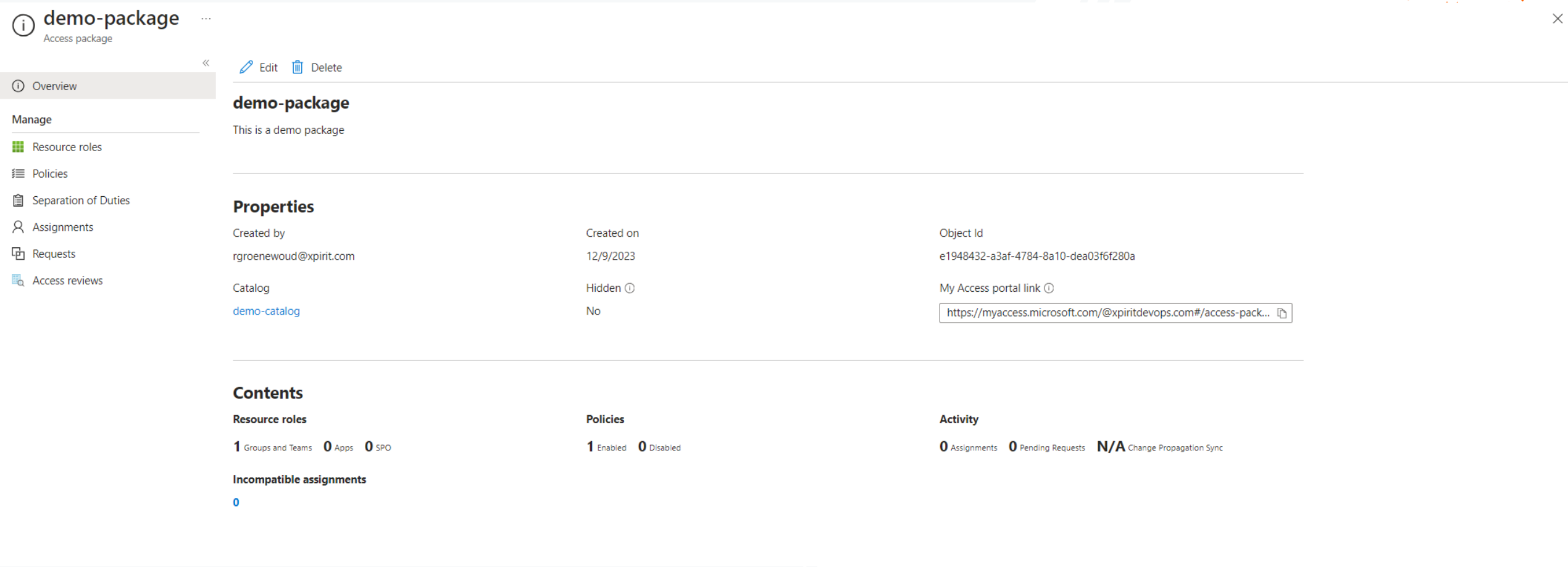
Catalog | Resources



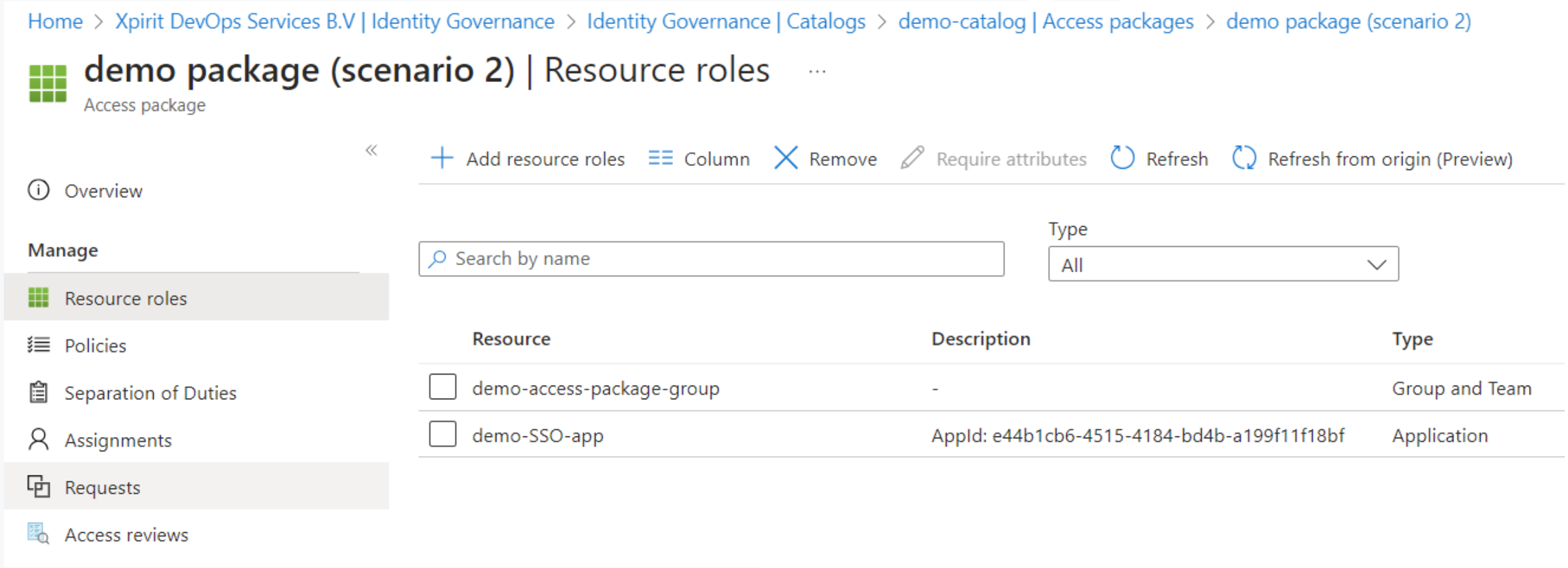
Catalog | Roles and Administrators



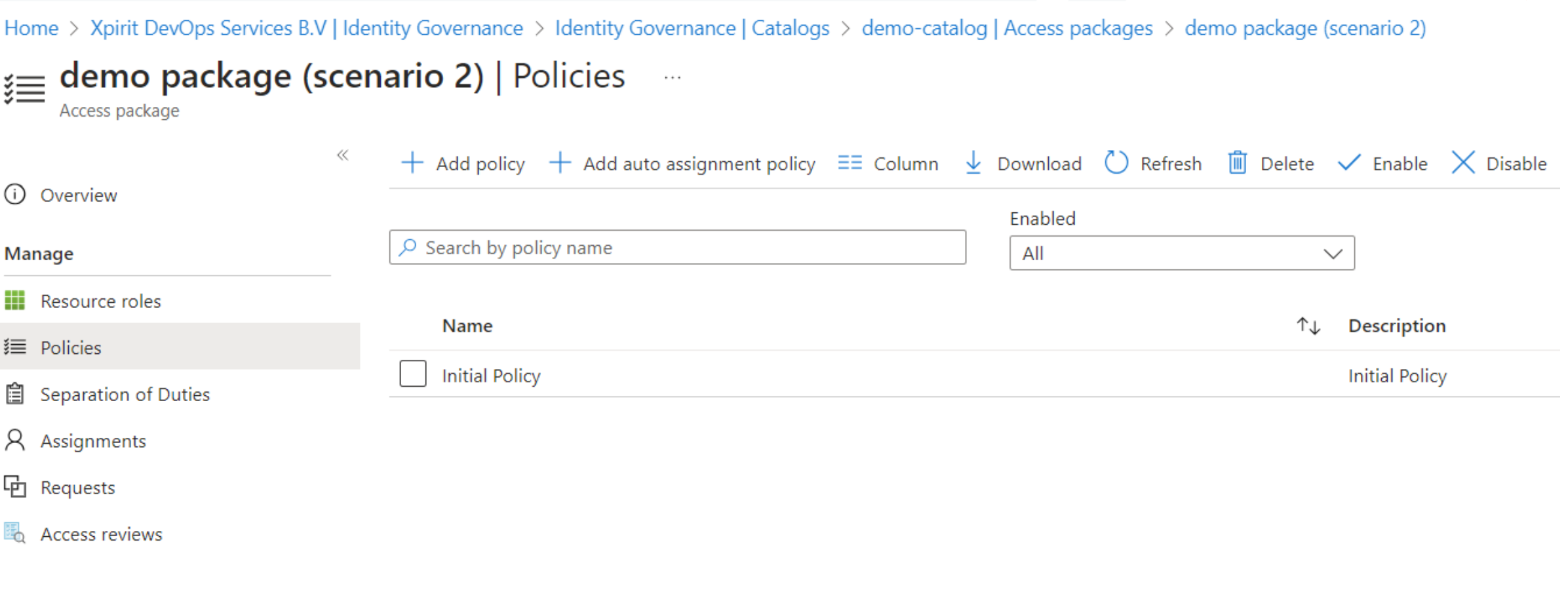
Access Package | Overview



Access Package | Resource Roles



Access Package | Policies



Policy | Basics

*Basics *Requests Requestor information *Lifecycle Custom extensions

Create a policy to specify who can request an access package, who can approve requests, and when access expires. Additional request policies can be created. Learn more

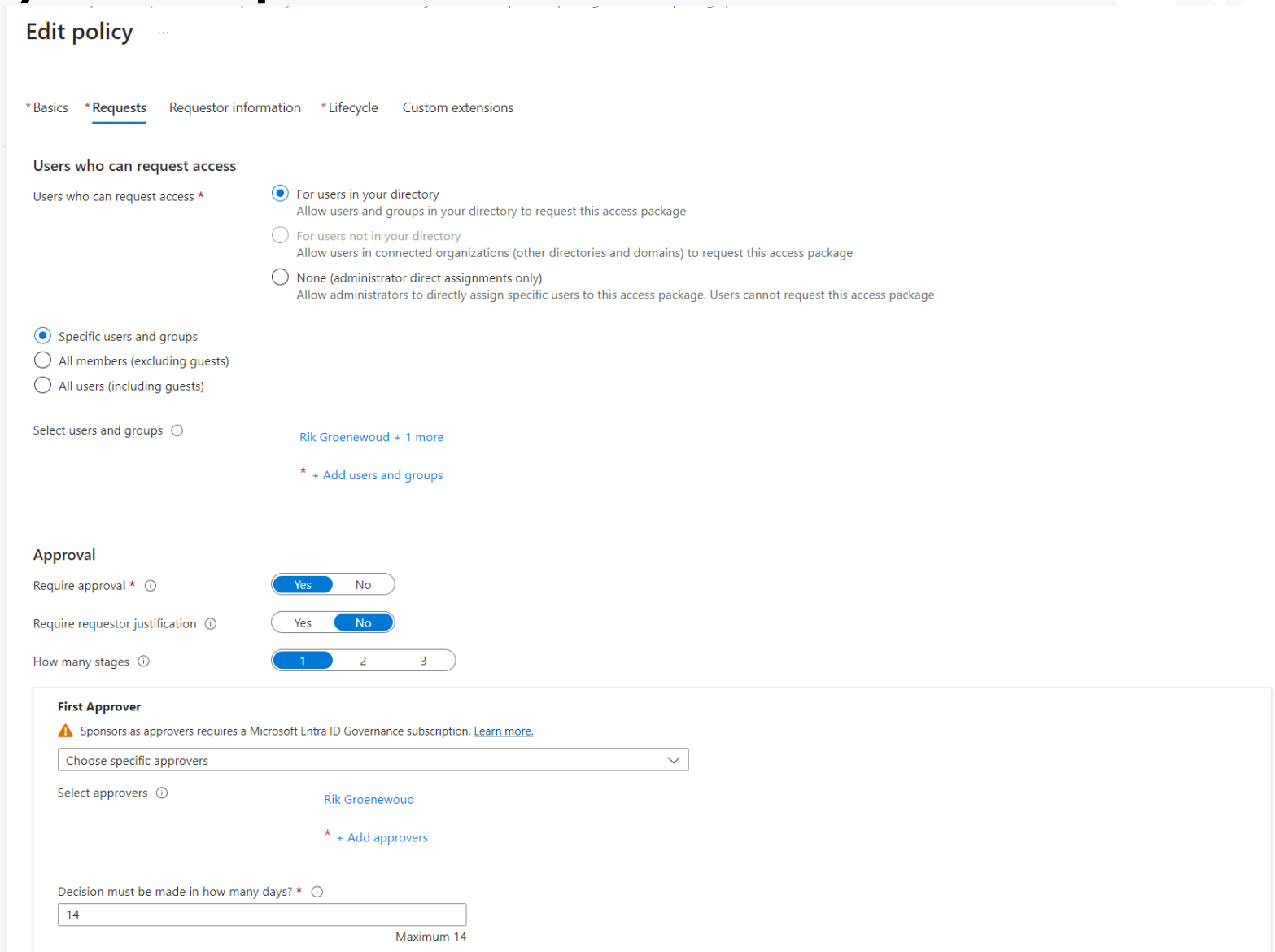
Name *

Initial Policy

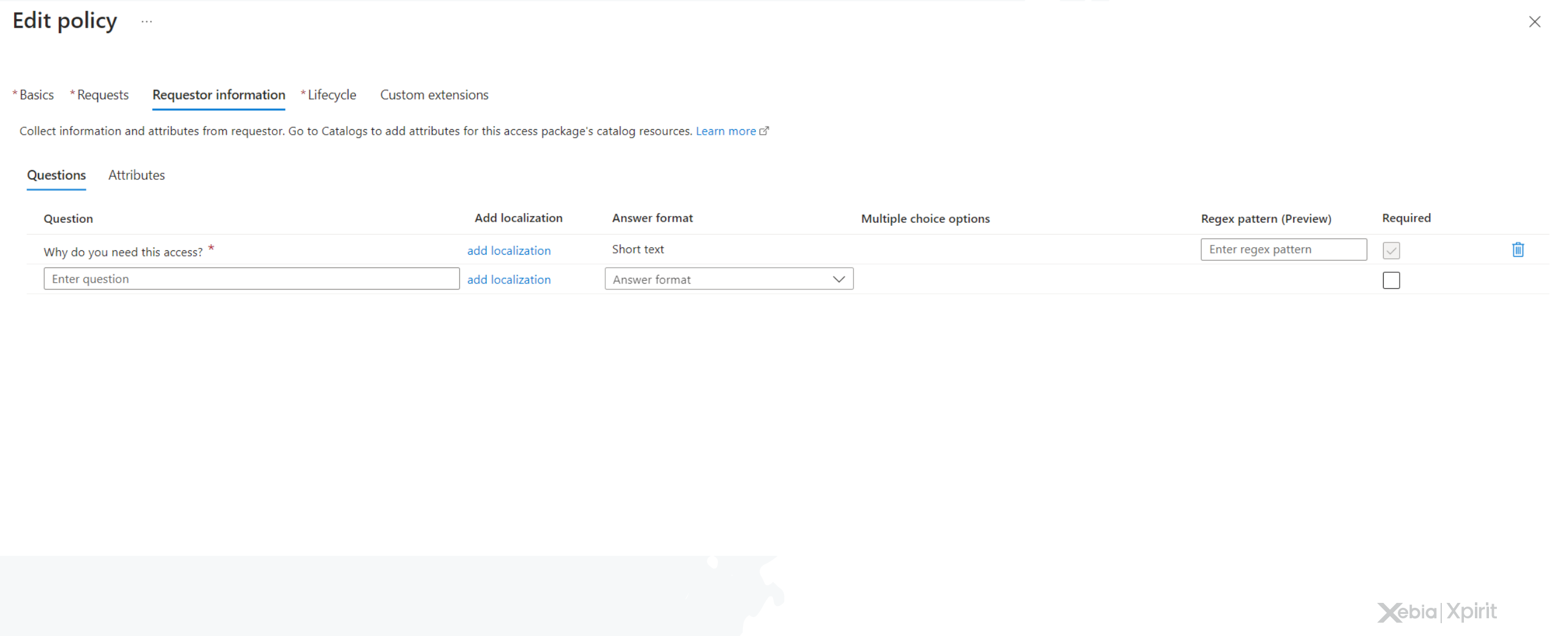
Description *

Initial Policy

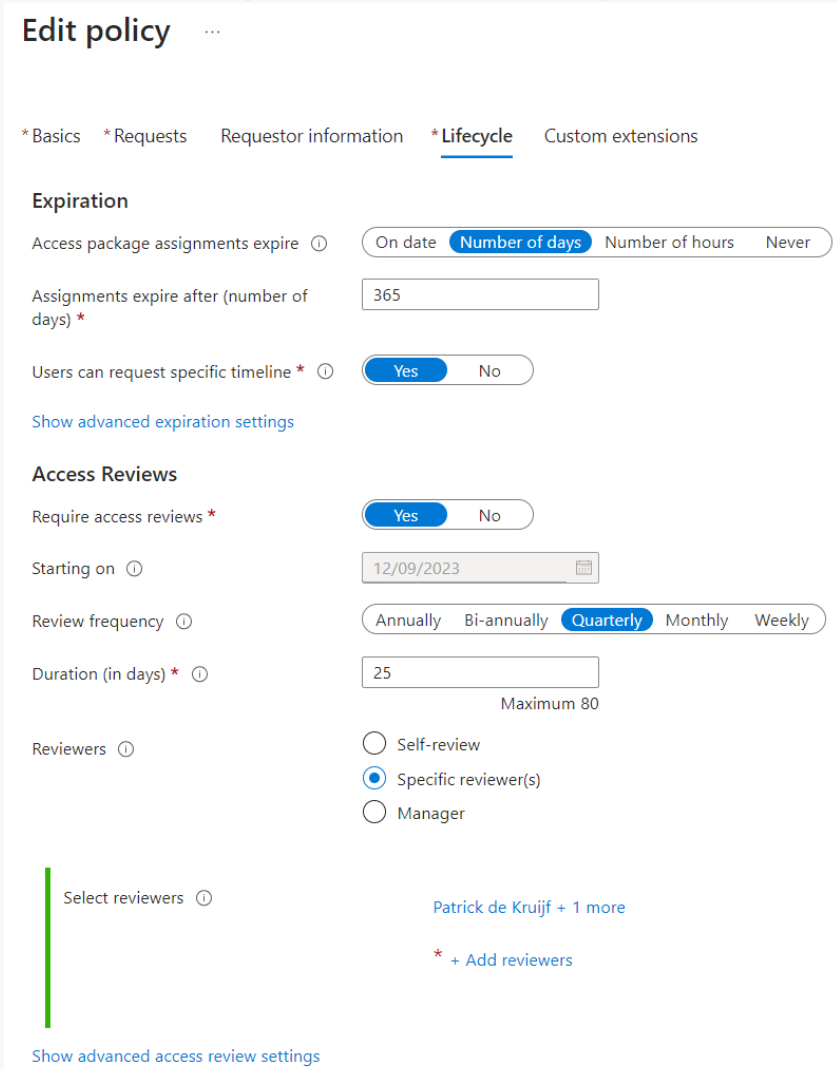
Policy | Requests



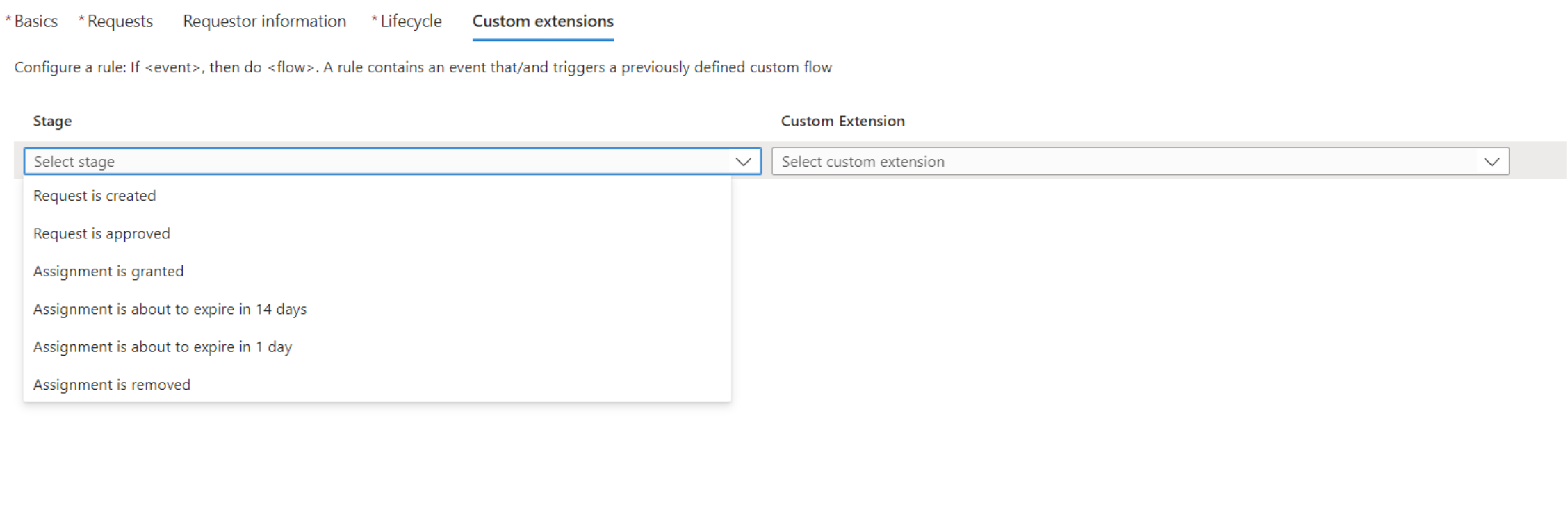
Policy | Requestor Information



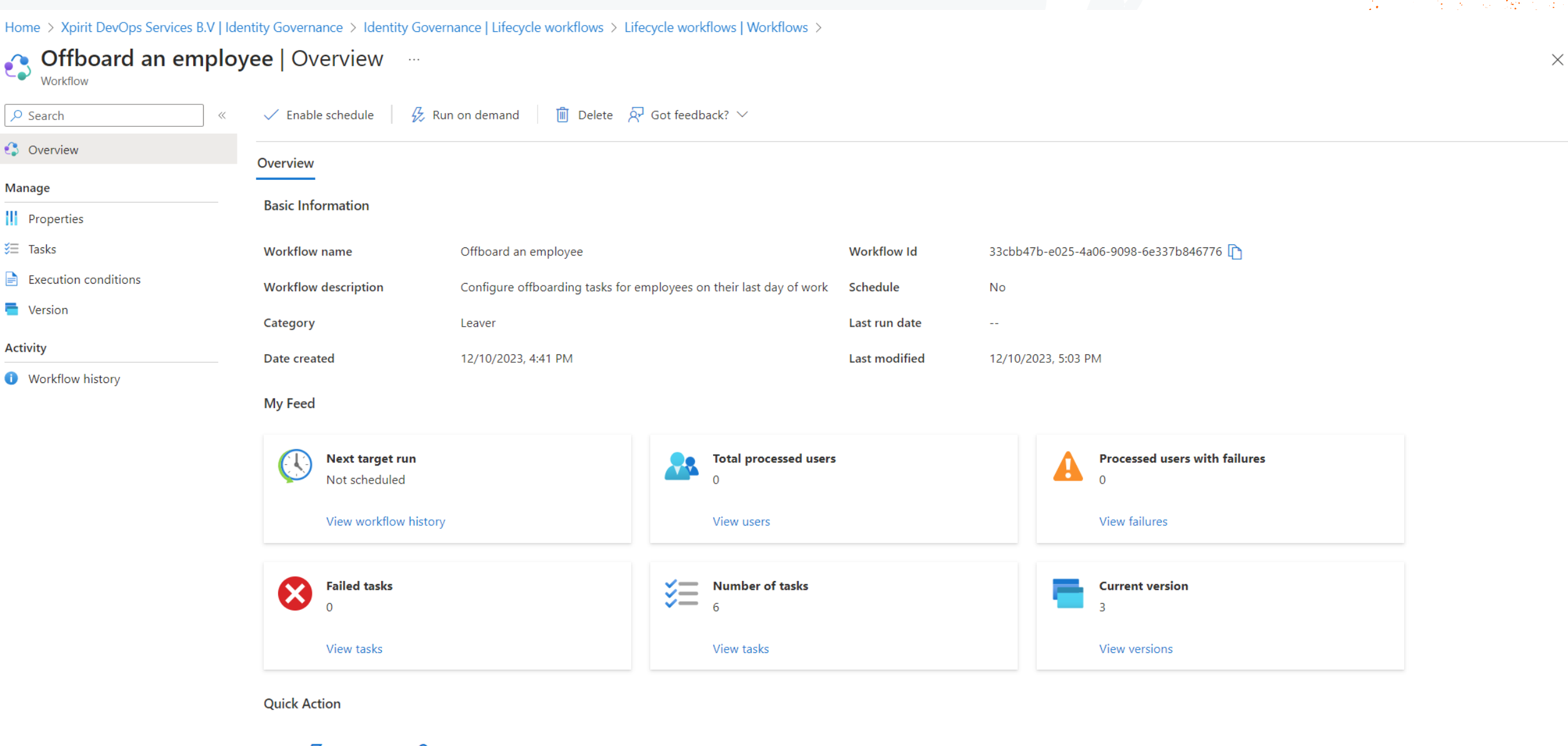
Policy | Lifecycle



Policy | Custom Extensions



Lifecyle Workflows



Lifecyle Workflows | Tasks

	Task order	Name	Enabled
⋮ ☐	1	Disable User Account	Yes
⋮ ☐	2	Remove all access package assignments for user	Yes
⋮ ☐	3	Cancel all pending access package assignment requests for user	Yes

Set Leave Date

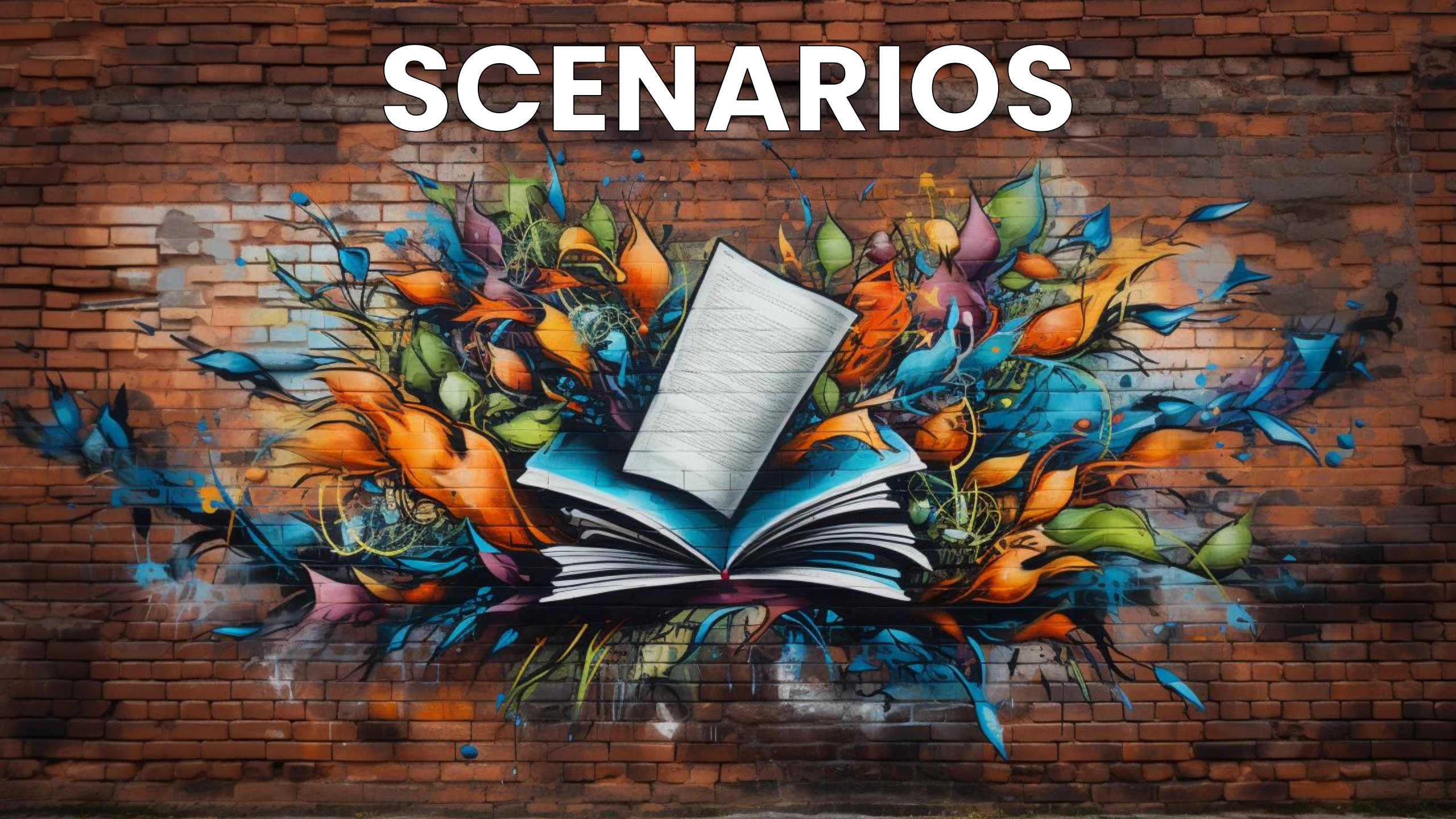
```powershell
Connect-MgGraph -Scopes "User.Read.All","User-LifeCycleInfo.ReadWrite.All"
Select-MgProfile -Name "beta"

$UserId = "0eac2b5d-8c9e-41e9-8c38-294534710c5e"
$employeeLeaveDateTime = "2023-12-09T23:59:59Z"

Update-MgBetaUser -UserId $UserId -EmployeeLeaveDateTime $employeeLeaveDateTime

$User = Get-MgBetaUser -UserId $UserId
$User.EmployeeLeaveDateTime
```

SCENARIOS



Scenario 1: Direct Assignment

- New employee starts and needs access to the resources for his role

- IT team grants the permissions on behalf of the HR team

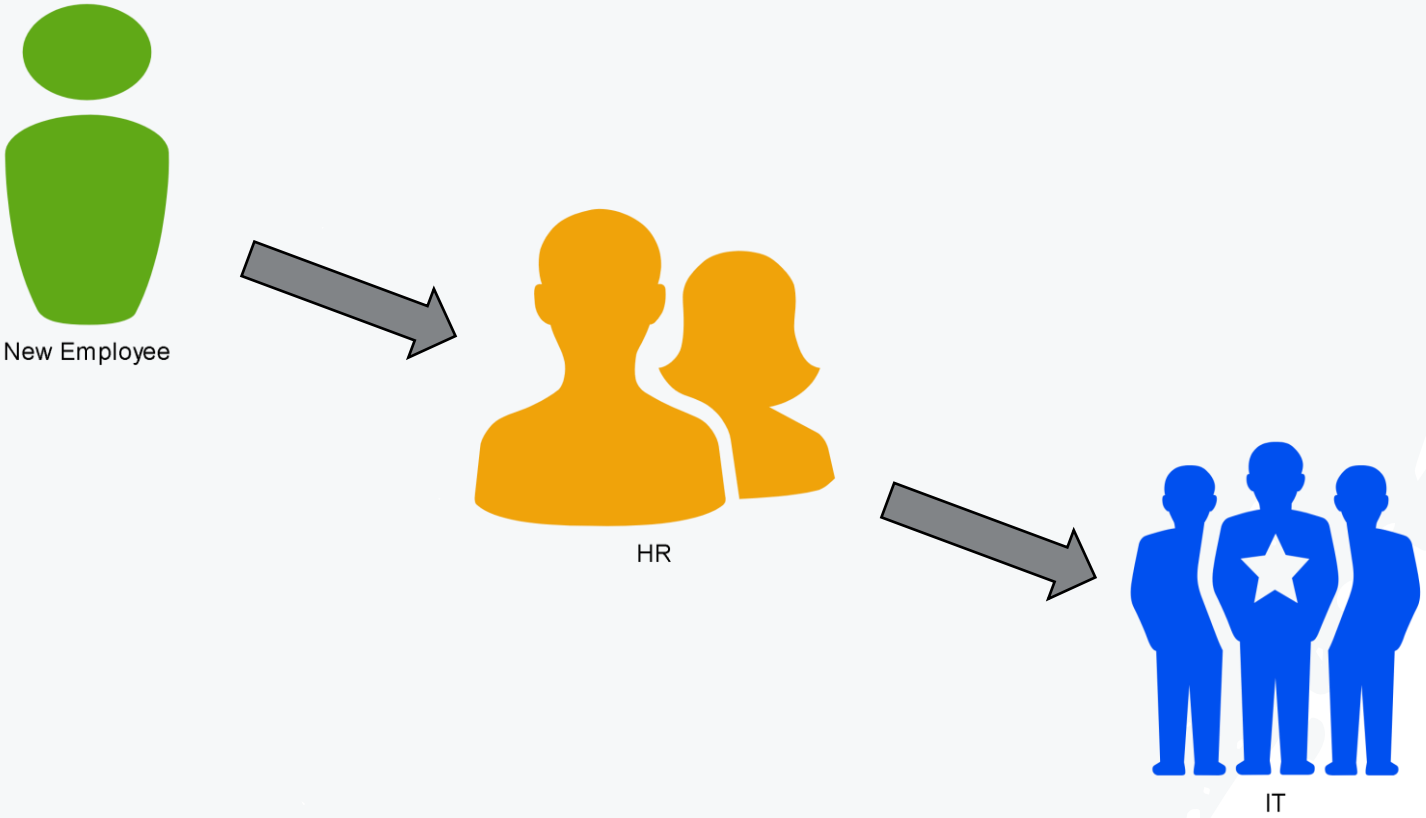
Scenario 2: Request more access

- Employee need more permissions
- Employee requests access using myAccess
- Approval flow kicks in

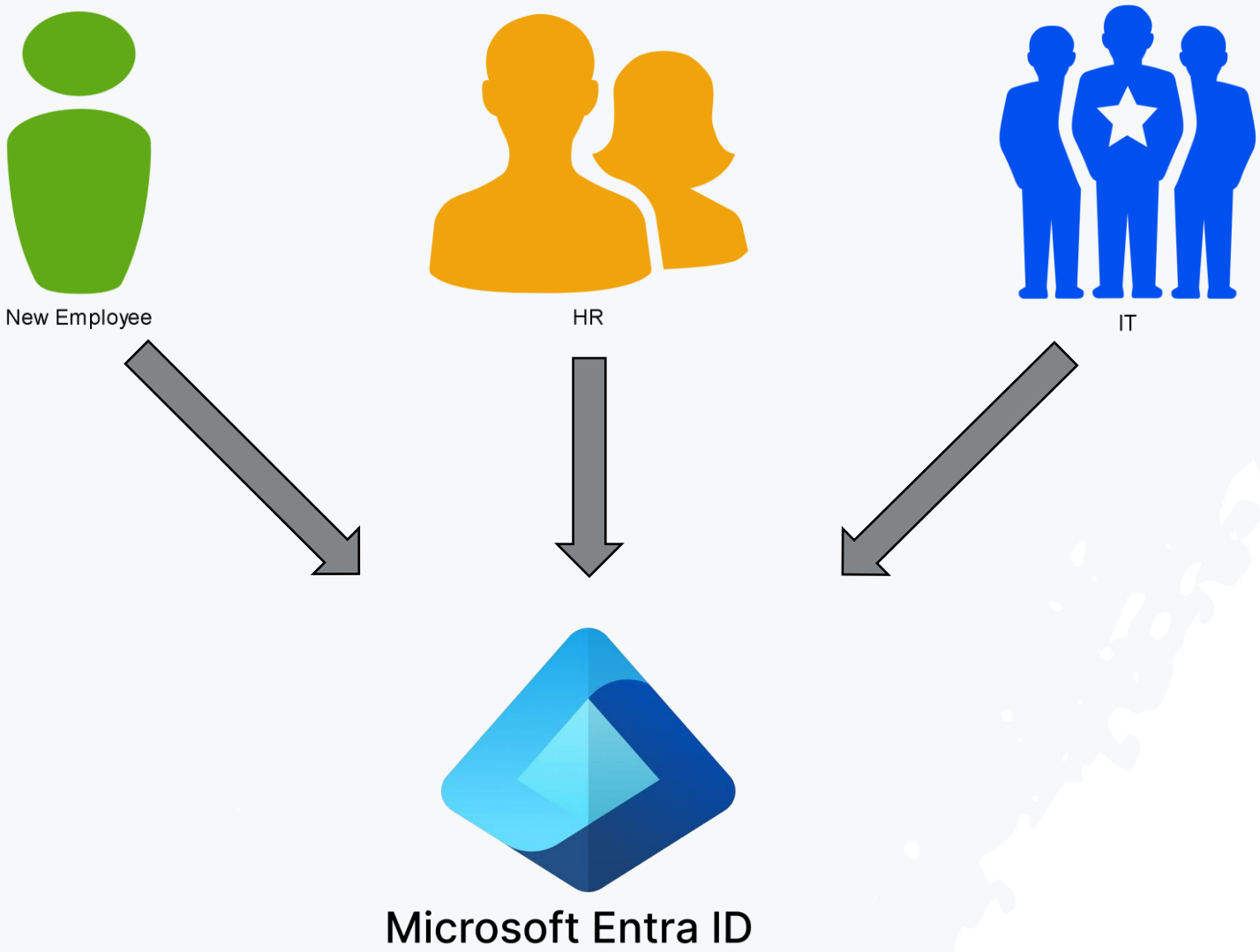
Scenario 3: Offboarding

- Employee has left the company
- Clean up assignments using lifecycle workflow

Remember this?



Now using Access Packages




THANK YOU
Will you