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



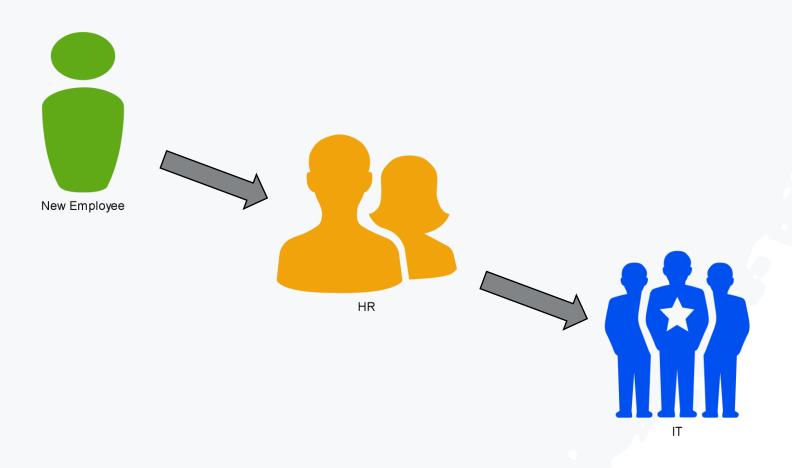
Rik Groenewoud – Customer Success Manager

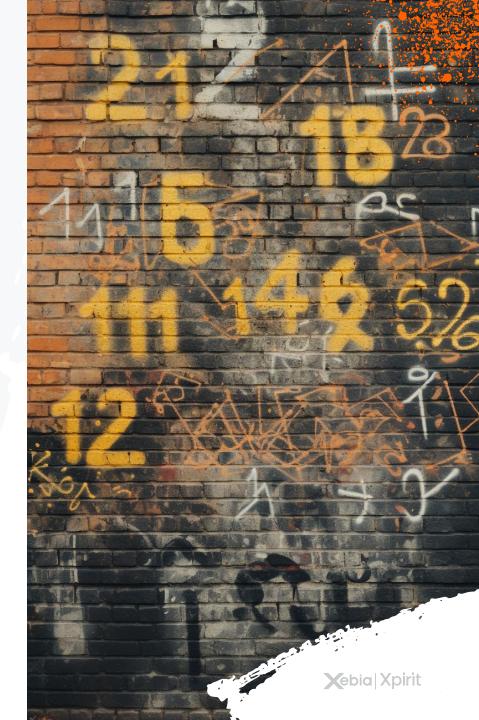
https://www.linkedin.com/in/rikgroenewoud

https://www.cloudwoud.nl



Pain: New employee process





Possible solutions

Privileged Identity
Management

Self Service Groups

Identity Governance Access Packages

Azure

Just in Time (JIT)
access

Short term access

Admin managed

Azure

Regular group membership

Permanent access

Group owner managed

Azure,
SharePoint/Teams
and Applications

Conditioned group membership

Regulated access

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

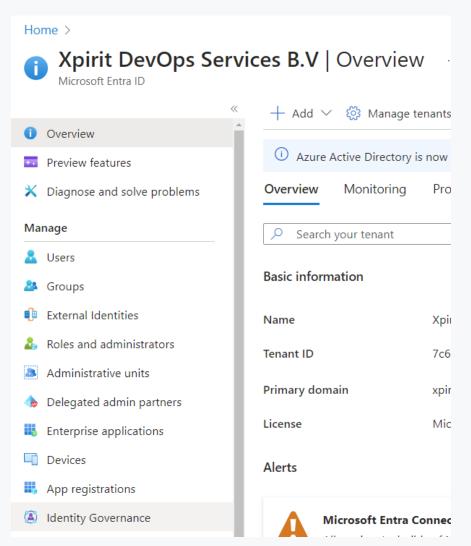
Microsoft Entra ID P2

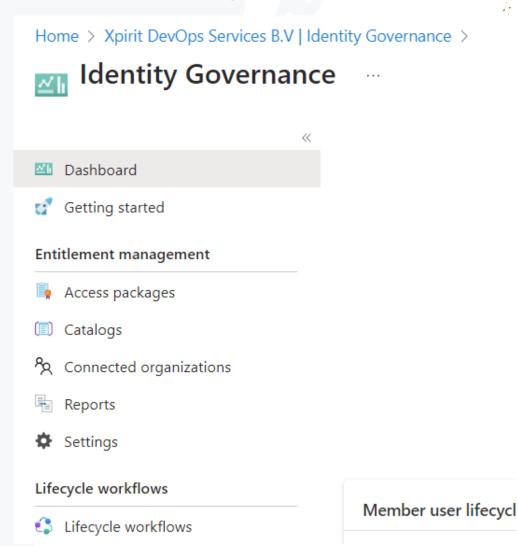
Microsoft Entra ID Governance (step-up for Microsoft Entra ID P2) → For advanced features

Advanced Features

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

Where to find the Access Packages?

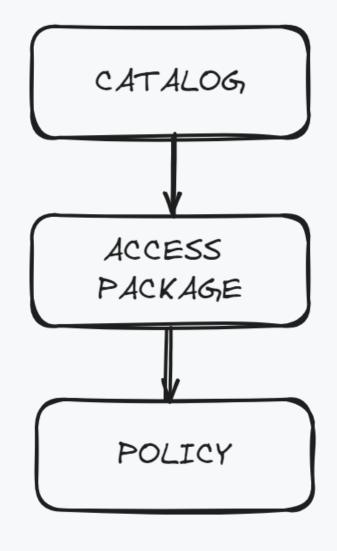






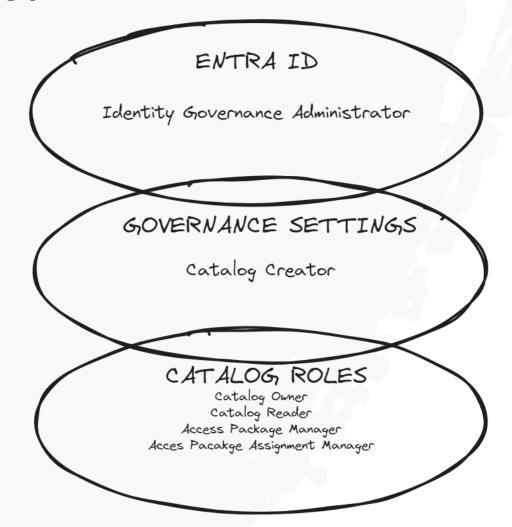


Structure

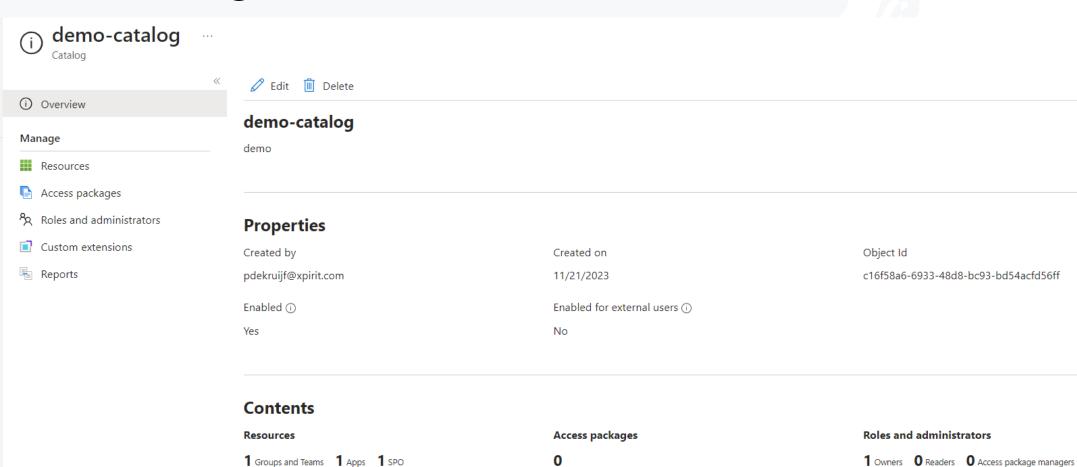




Access Control



Catalog



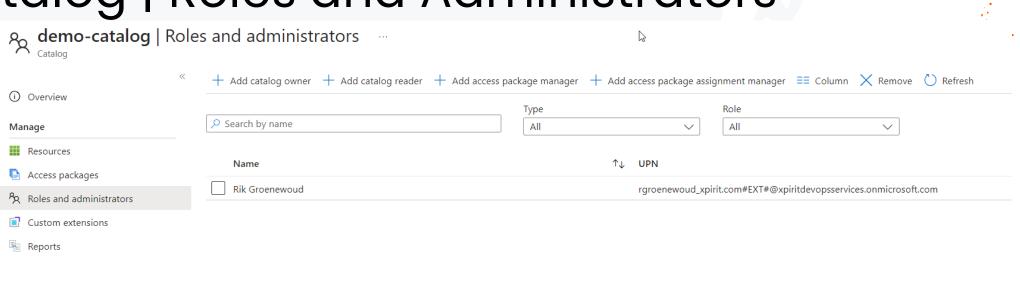
• Access package assignment managers

Catalog | Resources

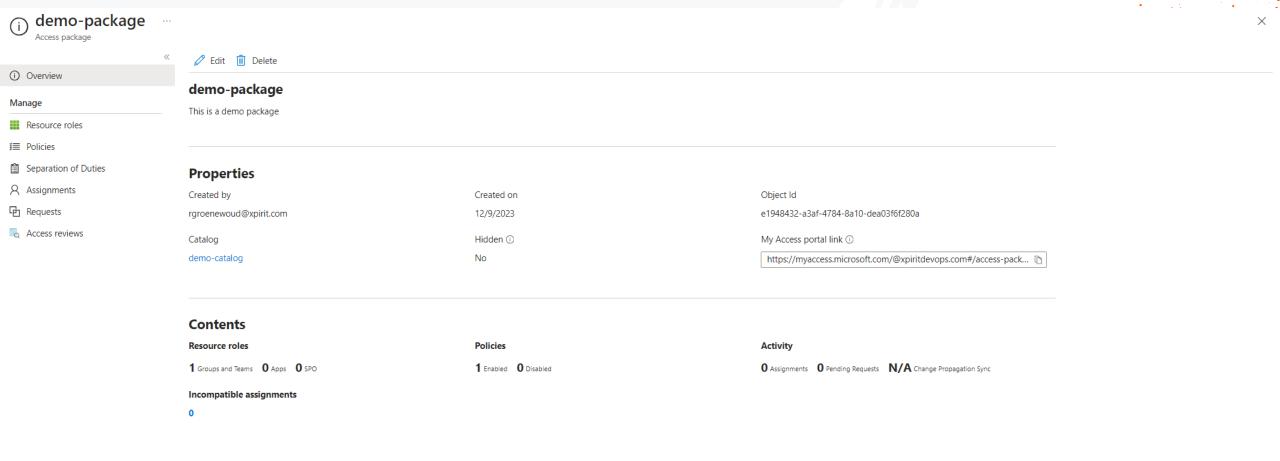
Home > Xpirit DevOps Services B.V Identity Governance > Identity Governance Catalogs > demo-catalog					
demo-catalog Resources					
« «	+ Add resources ≡≡ Column X Remove Ø Require attributes C Refresh C Refresh from origin (Preview)				
(i) Overview		Туре			
Manage	Search by resource name	All	~		
Resources	Deserves	Description	Tomas		
Access packages	Resource	Description	Туре		
Roles and administrators	demo-access-package-group		Group and Team		
Custom extensions	demo-SSO-app	Appld: e44b1cb6-4515-4184-bd4b-a199f11f18bf	Application		
	https://xpiritdevopsservices-my.sharepoint.com/	https://xpiritdevopsservices-my.sharepoint.com/	SharePoint Site		
Reports					



Catalog | Roles and Administrators



Access Package | Overview



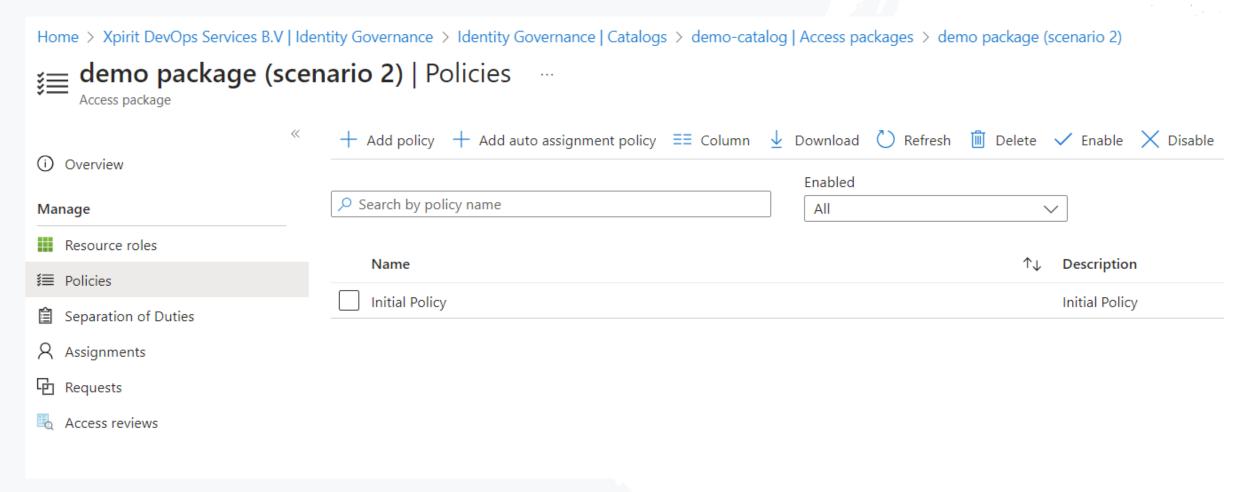


Access Package | Resource Roles

Home > Xpirit DevOps Services B.V Identity Governance > Identity Governance Catalogs > demo-catalog Access packages > demo package (scenario 2)				
demo package (scenario 2) Resource roles				
« «	+ Add resource roles ≡≡ Column X Re	move 🖉 Require attributes 💍 Refresh 🗘 Refresh fr	om origin (Preview)	
① Overview				
Manage	∠ Search by name	Type All	$\overline{}$	
Resource roles				
≨ Policies	Resource	Description	Туре	
Separation of Duties	demo-access-package-group	-	Group and Team	
Assignments	demo-SSO-app	Appld: e44b1cb6-4515-4184-bd4b-a199f11f18bf	Application	
Requests				
Access reviews				



Access Package | Policies



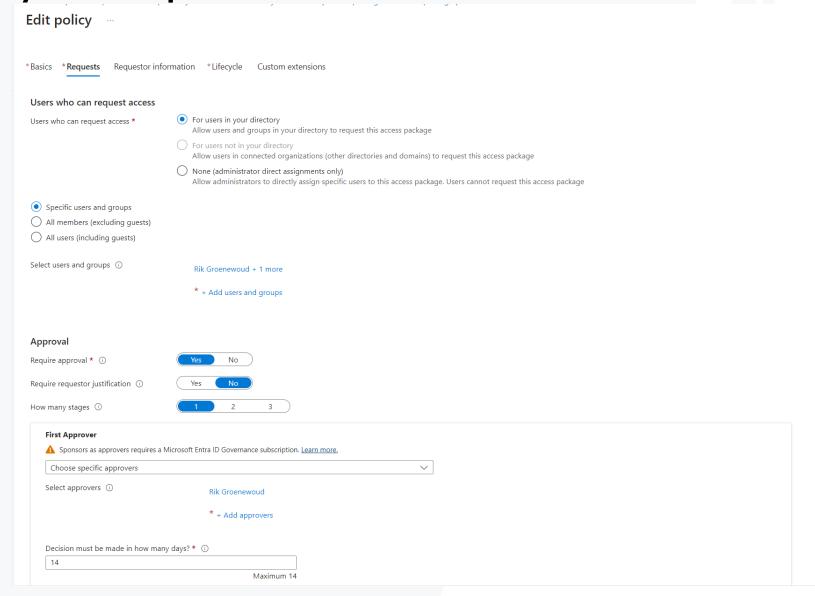


Policy | Basics

Requestor information *Lifecycle Custom extensions

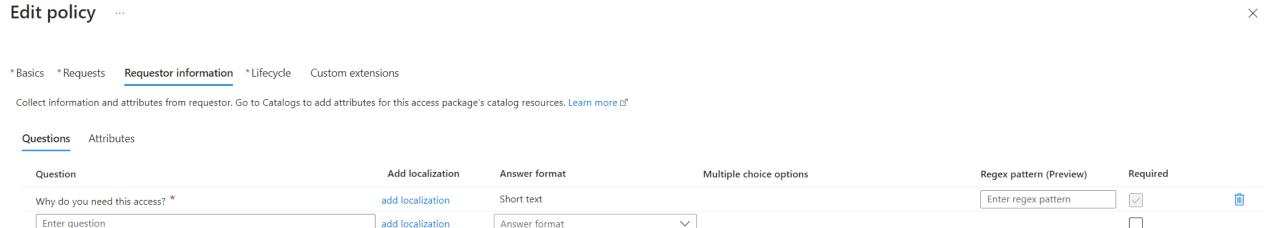
Create a policy to specify who car	n request an access package, who can approve requests, and when access expires. Additional request p	olicies can be created. Learn more ₫			
Name *	Initial Policy	✓			
Description * ①	Initial Policy				

Policy | Requests





Policy | Requestor Information



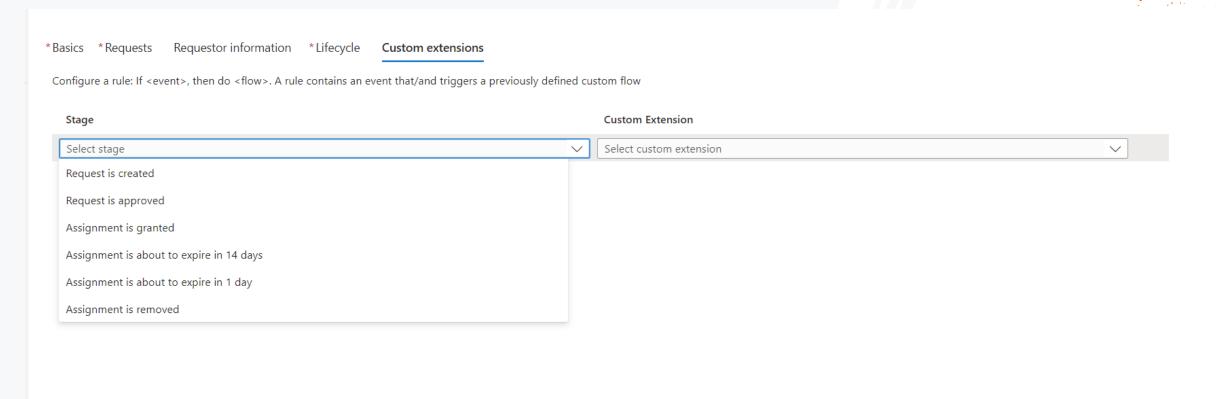


Policy | Lifecycle

Edit policy ...

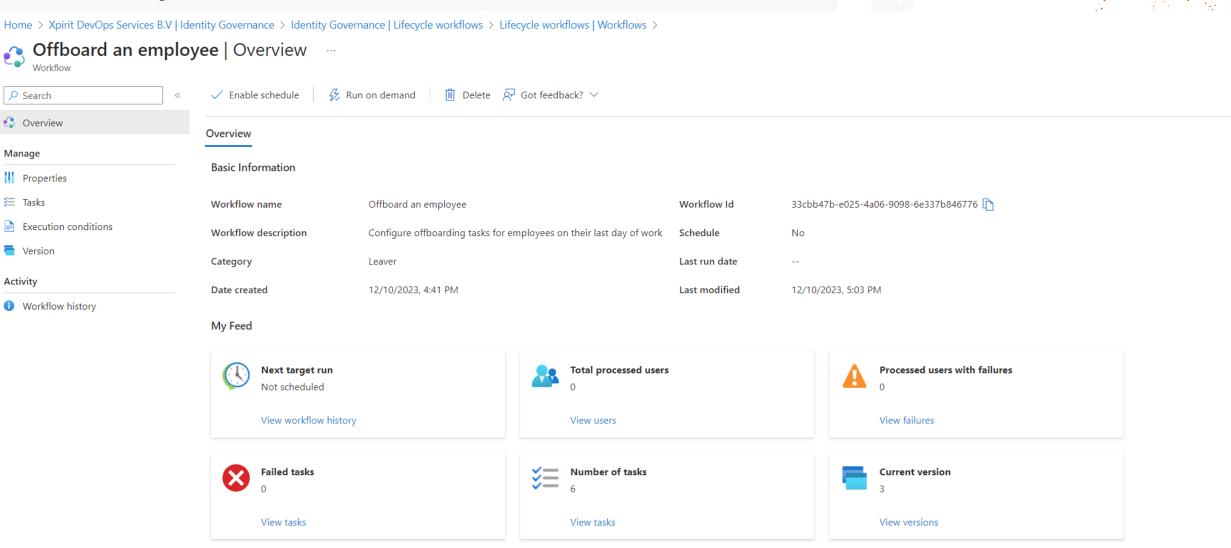
*Basics *Requests Requestor information *Lifecycle Custom extensions				
Expiration				
Access package assignments expire ①	On date Number of days Number of hours Never			
Assignments expire after (number of days) *	365			
Users can request specific timeline * ① Yes No				
Show advanced expiration settings				
Access Reviews				
Require access reviews *	Yes No			
Starting on ①	12/09/2023			
Review frequency ①	Annually Bi-annually Quarterly Monthly Weekly			
Duration (in days) * ①	25 Maximum 80			
Reviewers ①	Self-review Specific reviewer(s) Manager			
Select reviewers ①	Patrick de Kruijf + 1 more * + Add reviewers			
Show advanced access review settings				

Policy | Custom Extensions



Lifecyle Workflows

Quick Action



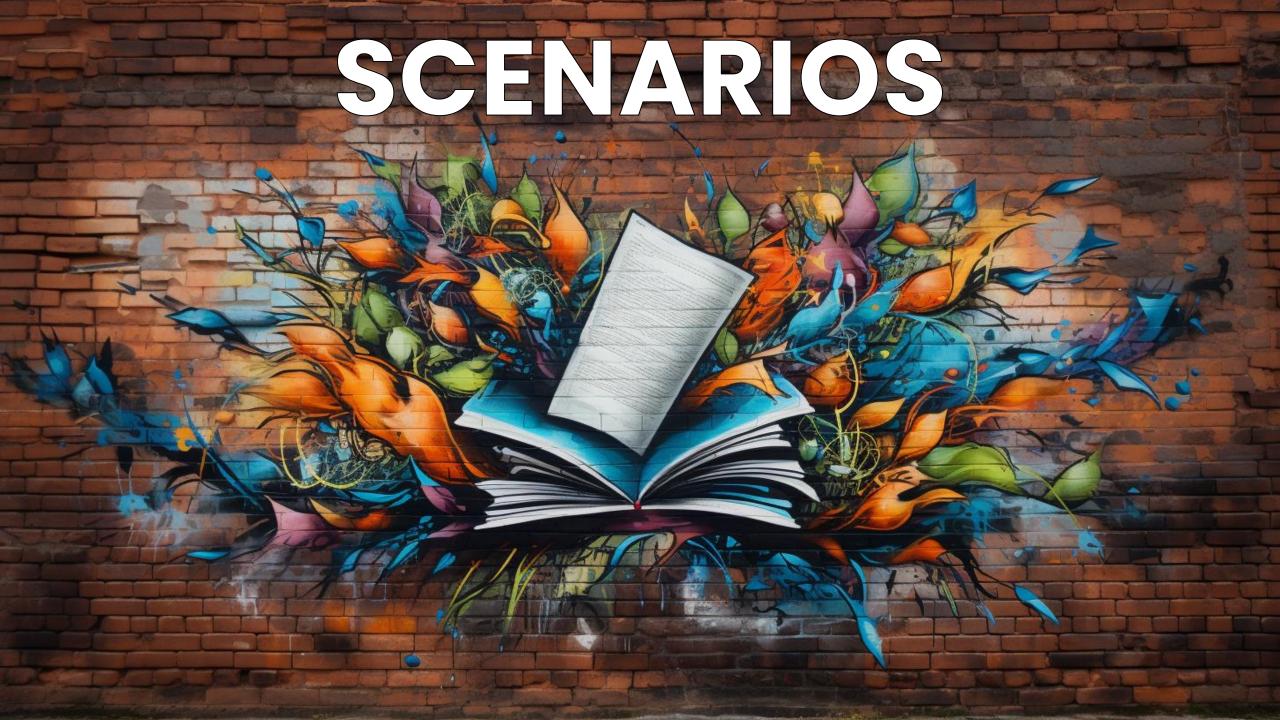
Lifecyle Workflows | Tasks

	Task order	Name	Enabled
:	1	☑ Disable User Account	Yes
:	2		Yes
:	3	 Cancel all pending access package assignment requests for user 	Yes



Set Leave Date

```
Connect-MgGraph -Scopes "User.Read.All", "User-LifeCycleInfo.ReadWrite.All"
1
     Select-MgProfile -Name "beta"
     $UserId = "0eac2b5d-8c9e-41e9-8c38-294534710c5e"
     $employeeLeaveDateTime = "2023-12-09T23:59:59Z"
 6
     Update-MgBetaUser -UserId $UserId -EmployeeLeaveDateTime $employeeLeaveDateTime
8
     $User = Get-MgBetaUser -UserId $UserId
 9
     $User.EmployeeLeaveDateTime
10
```



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

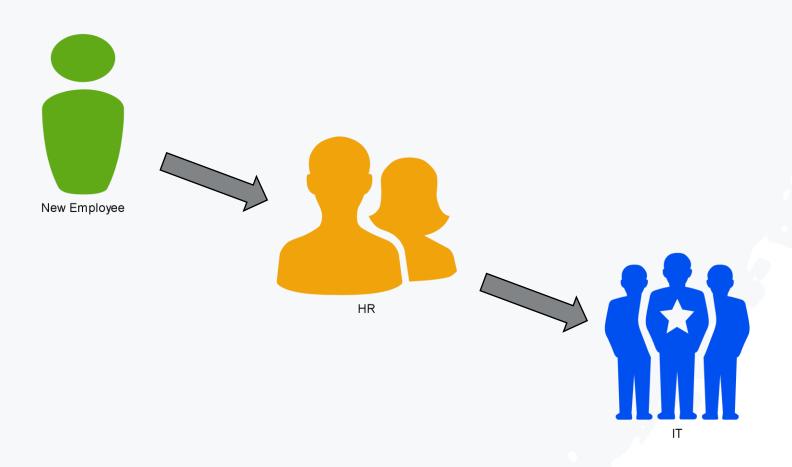


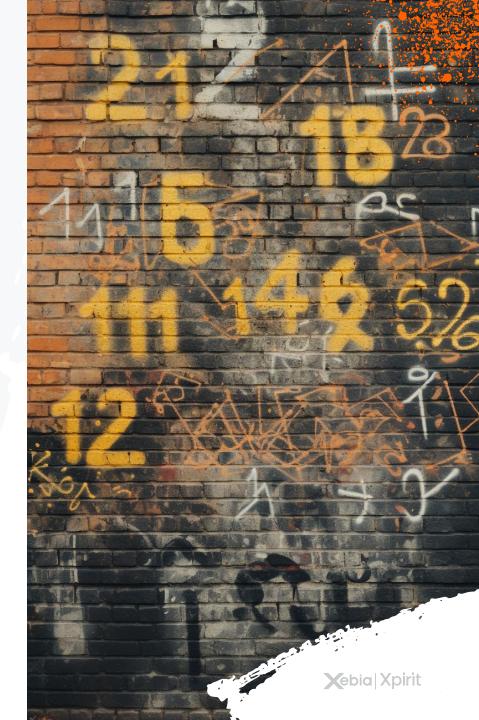
Scenario 3: Offboarding

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



Remember this?





Now using Access Packages

