Welcome to the MN M365 Spring Workshop Day 2025!

Please help us drive event awareness by tweeting and posting about your experience at the Workshop:

@M365MN #M365WorkshopDay

Please join us following the sessions for Happy Hour… Admin Ales, Workshop Wine, and more!

Thank you for your participation!

Chris Blackburn

23 year Microsoft IT Consultant, now retired & working in corporate IT at Datasite

Married for 25 years, 3 boys
(oldest at UWEC **majoring in AI**, middle is enjoying a work year after high school, youngest in 7th grade)

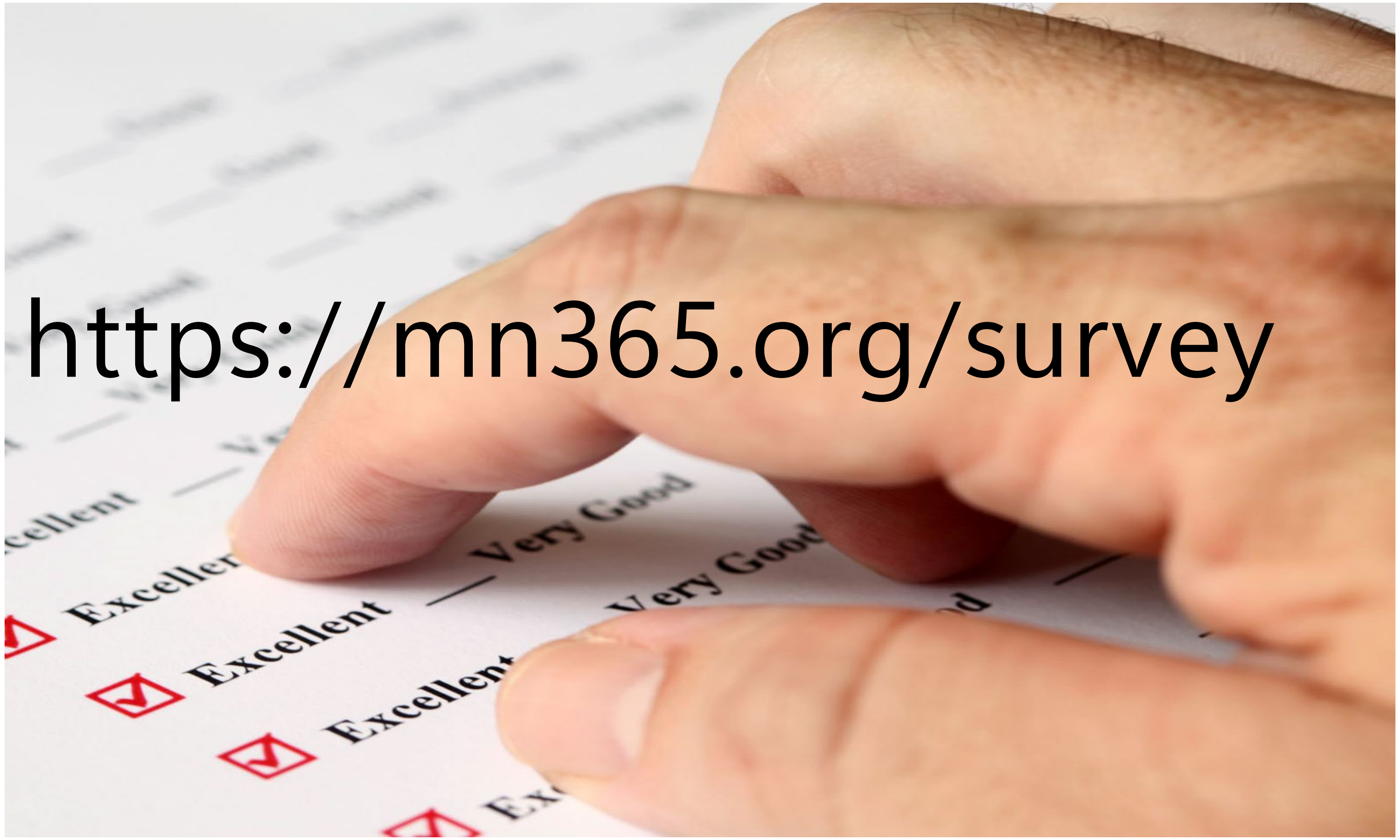
Enterprise Architect on Microsoft 365 end-to-end (Hybrid / Cloud + Identity / Collaboration / Security & Compliance / Endpoint Management) – including Copilot

When he's not behind the keyboard he's traveling across the world as a music fan & renowned DJ, plus a foodie (YES) that loves trying local cuisines around the world

blackburnc

memphistech.net

Workshop Survey



https://mn365.org/survey

Thank You to our Sponsors!

Microsoft

Stop by the Booths for "Vendor Bingo" to win prizes!

MN 365

PLATINUM (Registration, Breakfast, Lunch & Happy Hour)

EMERGENT SOFTWARE

MYTECH PARTNERS

RSM

AVI SPL

GOLD

virteva IT SOLUTIONS PERFECTED

Jabra GN

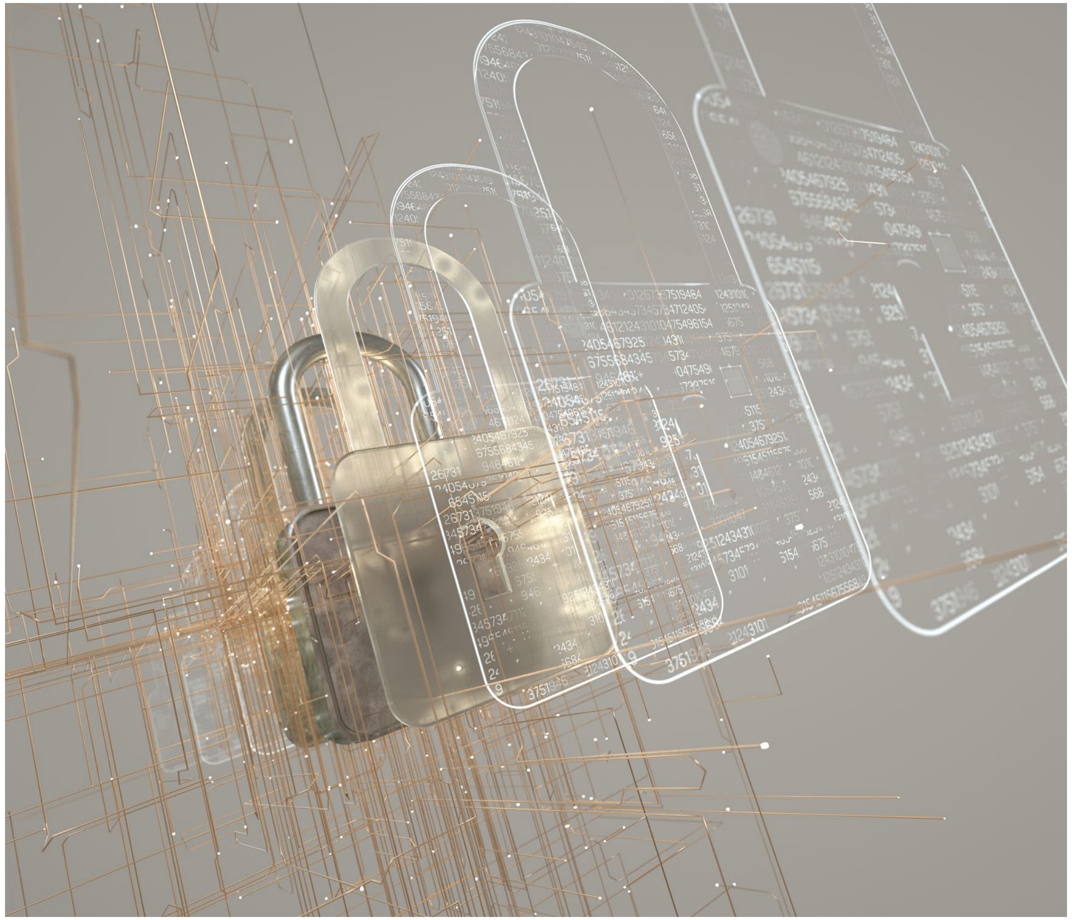
Modernizing User Lifecycles with Entra

Chris Blackburn, Microsoft 365 Architect & Evangelist

Introduction to Microsoft Entra ID Governance

Is an outdated identity and access management system giving you heartburn with it depreciated features, inefficiencies, and looming nearing end of life status? Are you ready to move into the modern age of cutting-edge features and seamless integration with HR platforms and transform your organization?

Say goodbye to traditional on-premises platforms and embrace the future of user management while improving your lifecycle management through Entra. Walk away with a clear understanding of how to take the first step to elevate your identity strategies and get ahead in the cloud-first world.



What’ We’ll be Talking About

1. **The Entra Provisioning Story:** Learn about the core capabilities and differentiate licensing levels in Entra that help you move to a "cloud first" provisioning posture.
2. **Native HR Integration:** Understand the seamless integration between Entra and popular HR platforms (like Workday), and how to standardize data and attributes across systems.
3. **Modern Identity Governance:** Discover the importance of the user lifecycle and how to use Entra Identity Governance to manage identities across platforms effectively.
4. **Making the Shift:** Explore the journey of transitioning from traditional platforms like MIM to Entra and some important steps you'll want to take now to be successful.
5. **Improving Identity Efficiency:** Learn how to continue the journey of modernizing identity & access management in Entra to streamline other IT processes, reduce administrative overhead, and improve overall operational efficiency.

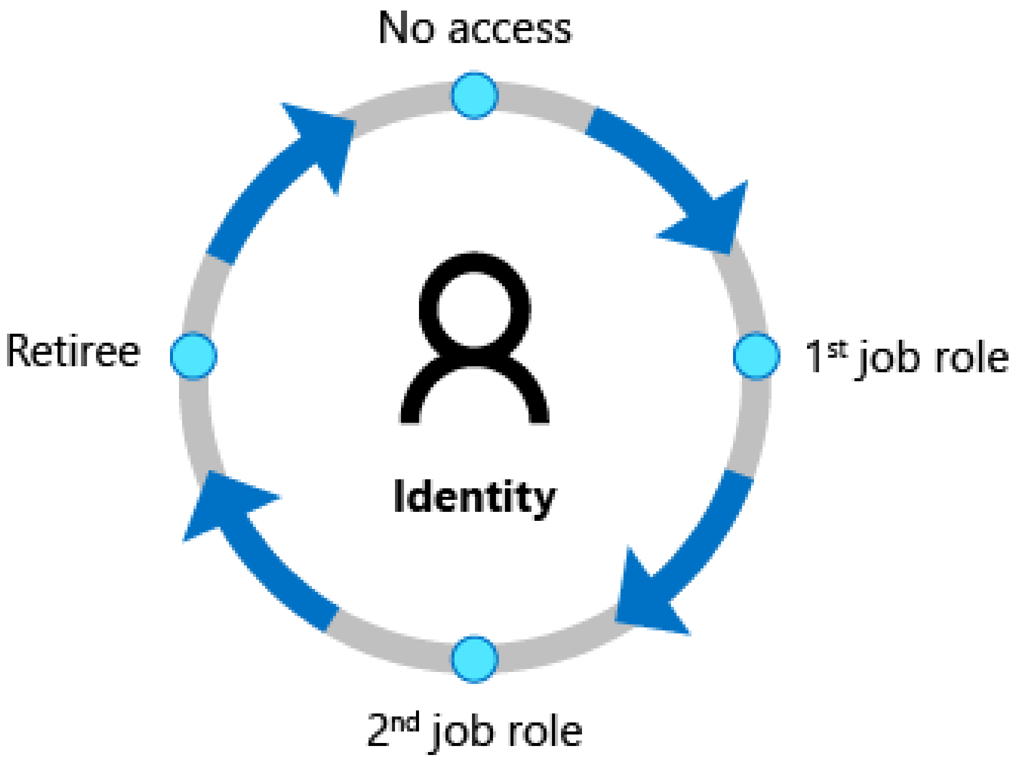
The Entra Provisioning Story

Learn about the core capabilities and differentiate licensing levels in Entra that help you move to a "cloud first" provisioning posture

Governance…. Why?

Productivity - How quickly can a person have access to the resources they need, such as when they join my organization?

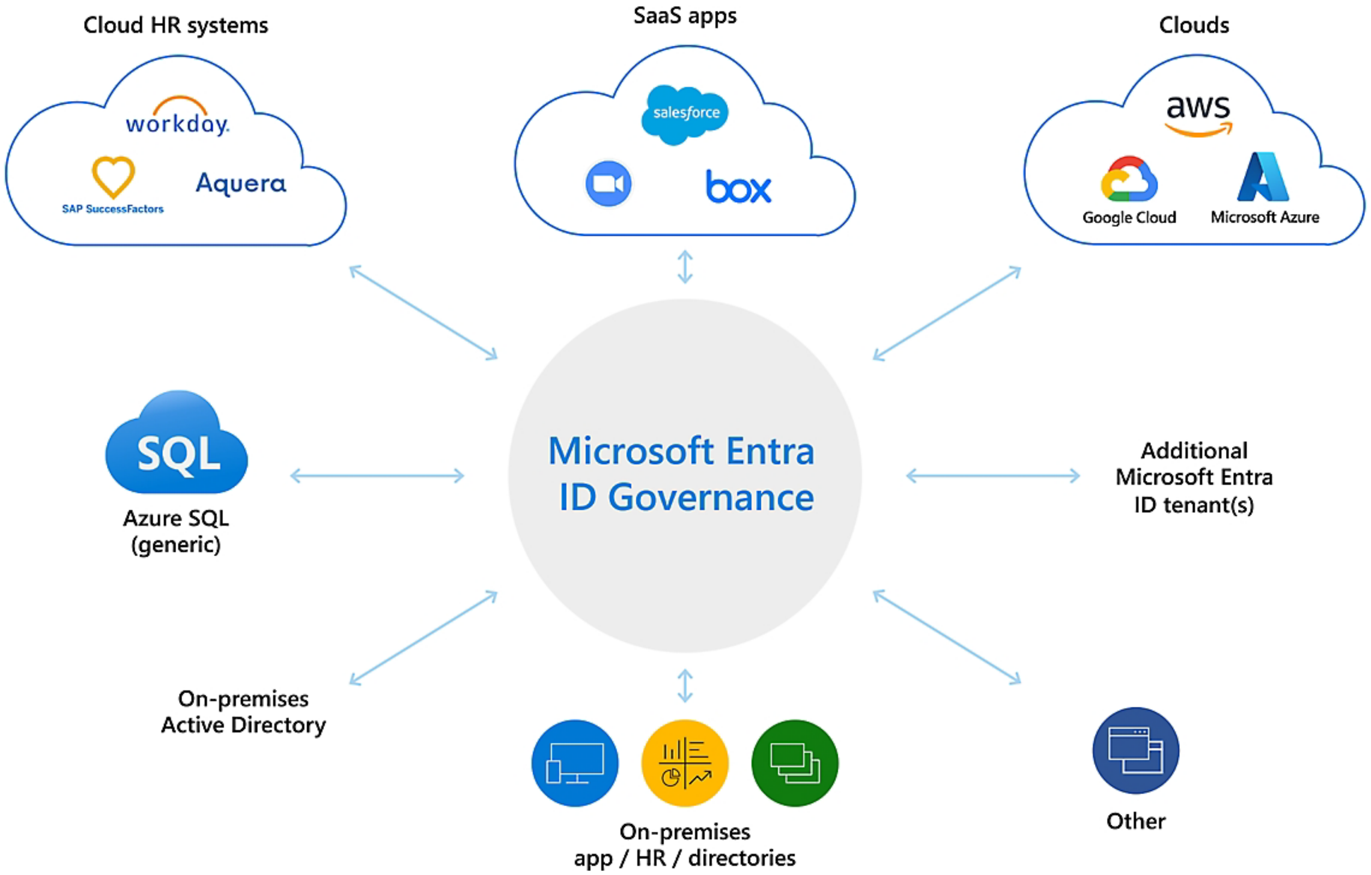
Security - How should their access change over time, such as due to changes to that person's employment status?



Entra…. Why?

Automation - Create user identities and roles in the apps users need to do their jobs while maintaining and removing user identities or role changes as easily.

Zero Trust - Secure access for any identity, from anywhere, to any resource across the cloud and on-premises.



Licensing… How?

Understanding Entra Feature

Understand required licenses for deployment

Combining licenses effectively

Entra ID Core = EID (P1 / P2)

- Conditional Access
- Role-based access control (RBAC)
- Advanced group management
- Cross-tenant / multitenant organizations
- SharePoint limited access
- Session lifetime management
- Global password protection and management
- Application portal + collections
- Self Service
- Advanced security and usage reports

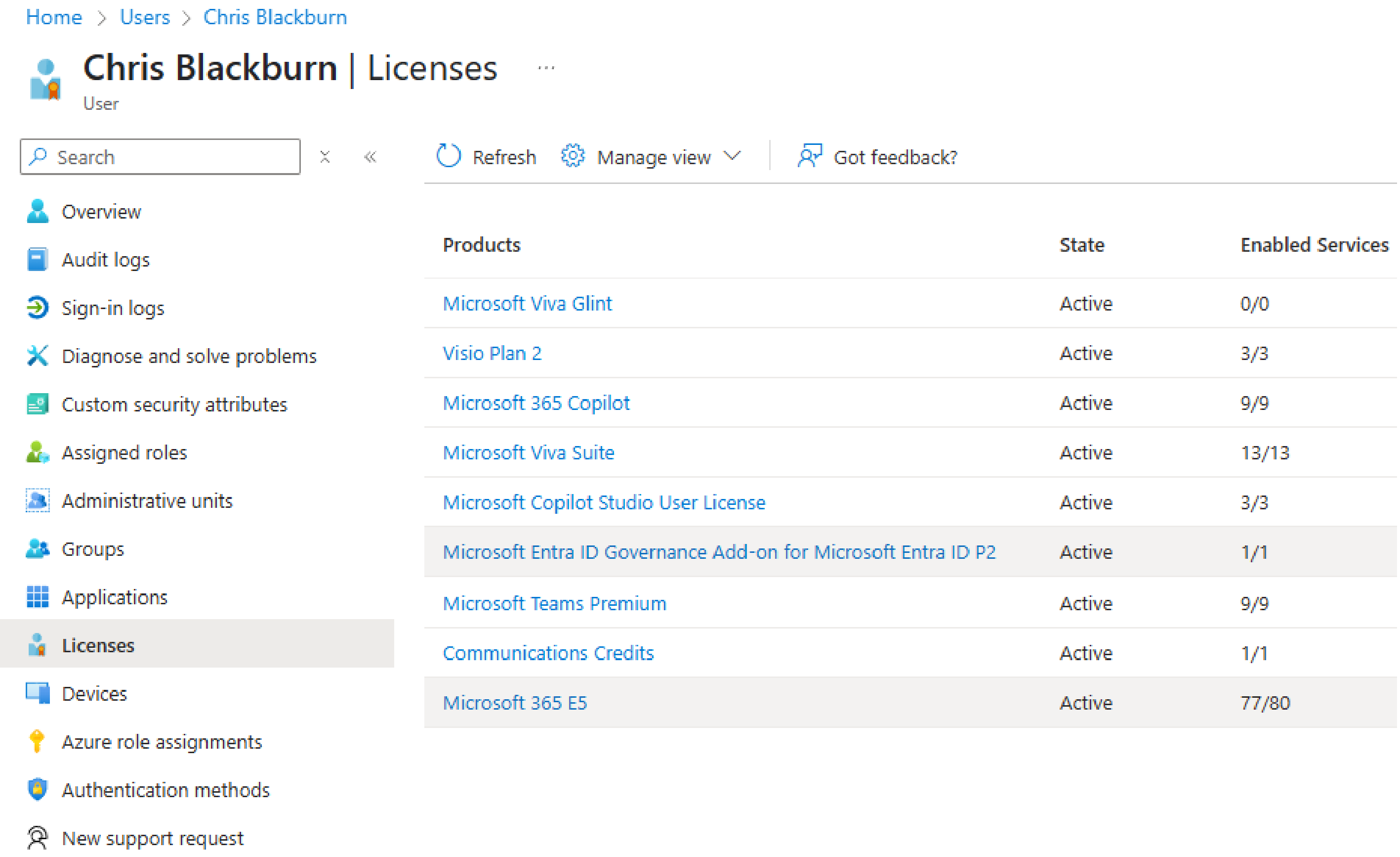
Entra ID Governance = EIDG (Suite/Add-on)

- Machine learning-assisted access certifications and reviews
- Entitlement management custom extensions (Microsoft Azure Logic Apps)
- Entitlement management with Microsoft Entra Verified ID
- Lifecycle workflows
- Identity governance dashboard
- Privileged identity management

At the Core

ALL Internal / External Users will Require:

- Entra ID Plan 2 (included in M365 / EMS E5 / A5 / G5)
- Entra ID Governance license



Home > Users > Chris Blackburn

Chris Blackburn | Licenses

User

Products	State	Enabled Services
Microsoft Viva Glint	Active	0/0
Visio Plan 2	Active	3/3
Microsoft 365 Copilot	Active	9/9
Microsoft Viva Suite	Active	13/13
Microsoft Copilot Studio User License	Active	3/3
Microsoft Entra ID Governance Add-on for Microsoft Entra ID P2	Active	1/1
Microsoft Teams Premium	Active	9/9
Communications Credits	Active	1/1
Microsoft 365 E5	Active	77/80

Licensing Scenario

Scenario	Calculation	Number of licenses
An administrator creates an access review of Group A with 75 users and 1 group owner, and assigns the group owner as the reviewer.	1 license for the group owner as reviewer, and 75 licenses for the 75 users.	**76**
An administrator creates an access review of Group B with 500 users and 3 group owners, and assigns the 3 group owners as reviewers.	500 licenses for users, and 3 licenses for each group owner as reviewers.	**503**
An administrator creates an access review of Group B with 500 users. Makes it a self-review.	500 licenses for each user as self-reviewers	**500**
An administrator creates an access review of Group C with 50 member users. Makes it a self-review.	50 licenses for each user as self-reviewers.	**50**
An administrator creates an access review of Group D with 6 member users. Makes it a self-review.	6 licenses for each user as self-reviewers. No additional licenses are required.	**6**

Licensing Scenario

Scenario	Calculation	Number of licenses
A Lifecycle Workflows Administrator creates a workflow to add new hires in the Marketing department to the Marketing teams group. 250 new hires are assigned to the Marketing teams group via this workflow once. Other 150 new hires are assigned to the Marketing teams group via this workflow later the same year.	1 license for the Lifecycle Workflows Administrator, and 400 licenses for the users.	401
A Lifecycle Workflows Administrator creates a workflow to pre-offboard a group of employees before their last day of employment. The scope of users who will be pre-offboarded are 40 users once. We offboard 40 licensed users. Now, we can re-assign these 40 licenses and assign 10 more licenses later in the year to pre-offboard 50 more users.	50 licenses for users, and 1 license for the Lifecycle Workflows Administrator.	51

Licensing Scenario (PIM)

Scenario	Calculation	Number of licenses
Woodgrove Bank has 10 administrators for different departments and 2 Privileged Role Administrators that configure and manage PIM. They make five administrators eligible.	Five licenses for the administrators who are eligible	5
Graphic Design Institute has 25 administrators of which 14 are managed through PIM. Role activation requires approval and there are three different users in the organization who can approve activations.	14 licenses for the eligible roles + three approvers	17
Contoso has 50 administrators of which 42 are managed through PIM. Role activation requires approval and there are five different users in the organization who can approve activations. Contoso also does monthly reviews of users assigned to administrator roles and reviewers are the users' managers of which six aren't in administrator roles managed by PIM.	42 licenses for the eligible roles + five approvers + six reviewers	53

Licensing can be one of the toughest challenges in the journey to implementing – mission accomplished! 👍

The first step is getting users out of your HR platform into Entra

Native HR Integration

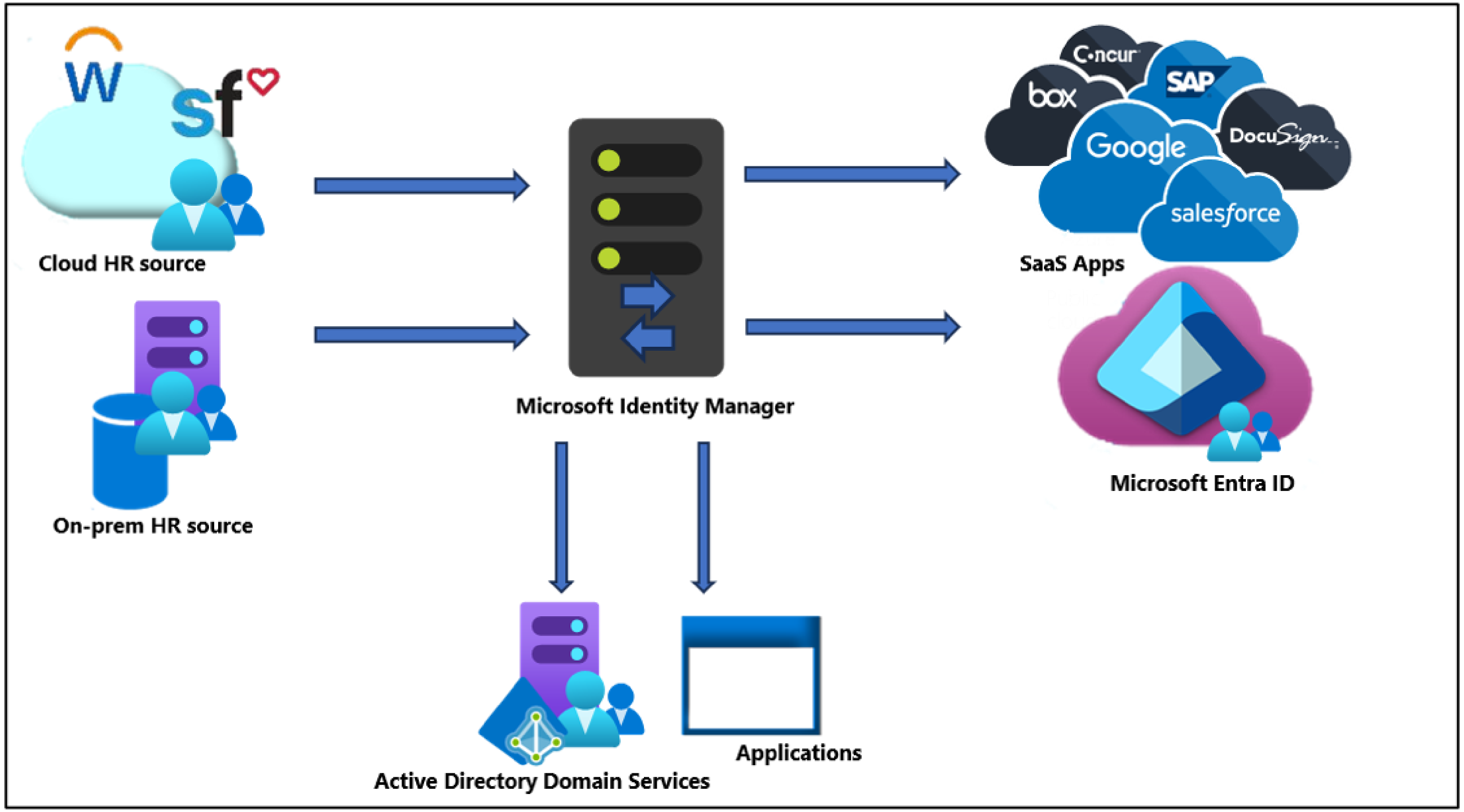
Understand the seamless integration between Entra and popular HR platforms (like Workday), and how to standardize data and attributes across systems.

Creating Users

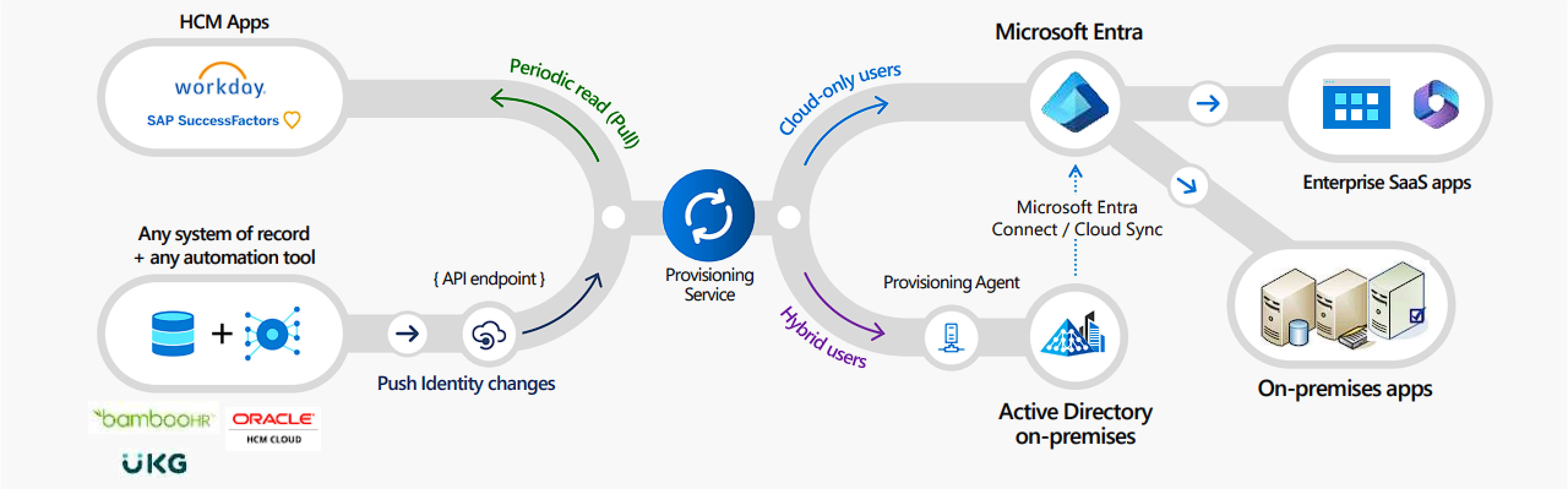
- User Provisioning
- 1st Party Connectors
- HR Provisioning Apps in Entra
- Attribute Mapping
- Lessons Learned
- HR Workflow

User Provisioning

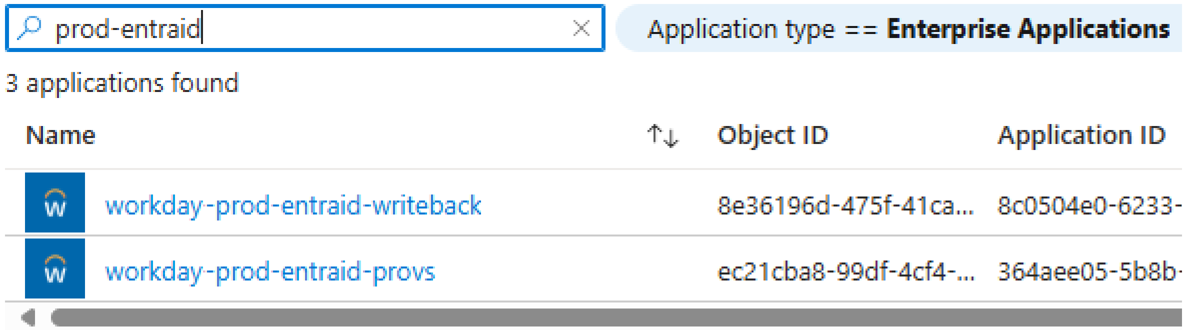
Whether it's Entra or other HR sources, importing users, aggregating them in the metaverse and then provisioning them to different repositories is a core function.



Onboard via 1st party connectors



HR Provisioning Apps in Entra

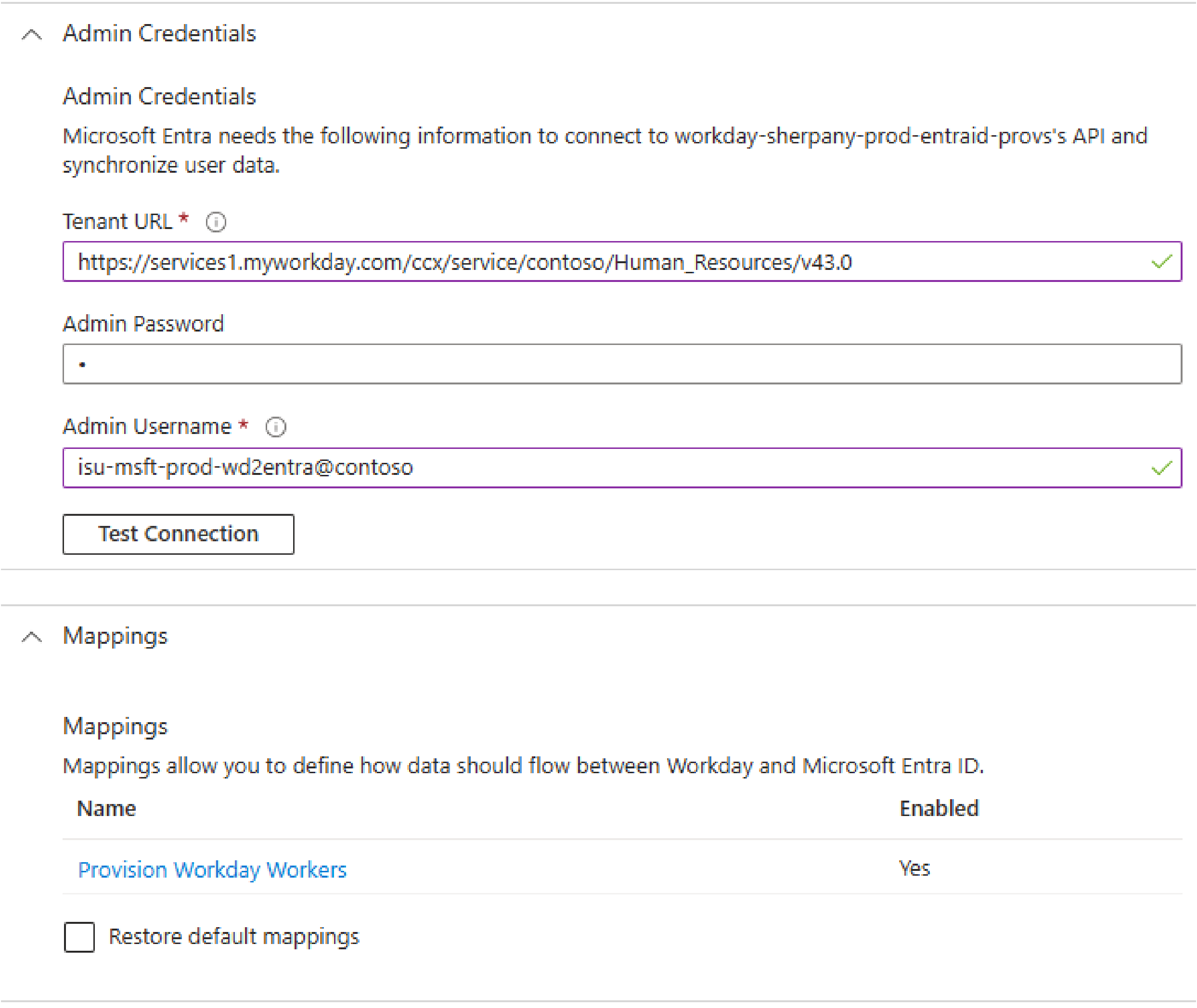


prod-entraid

Application type == **Enterprise Applications**

3 applications found

Name	Object ID	Application ID
workday-prod-entraid-writeback	8e36196d-475f-41ca...	8c0504e0-6233-
workday-prod-entraid-provs	ec21cba8-99df-4cf4-...	364aee05-5b8b-



Admin Credentials

Admin Credentials

Microsoft Entra needs the following information to connect to workday-sherpany-prod-entraid-provs's API and synchronize user data.

Tenant URL *
https://services1.myworkday.com/ccx/service/contoso/Human_Resources/v43.0

Admin Password
•

Admin Username *
isu-msft-prod-wd2entra@contoso

Test Connection

Mappings

Mappings

Mappings allow you to define how data should flow between Workday and Microsoft Entra ID.

Name	Enabled
Provision Workday Workers	Yes

□ Restore default mappings

Under the hood of the Provisioning process lies the Entra ID Provisioning Engine via enterprise apps.

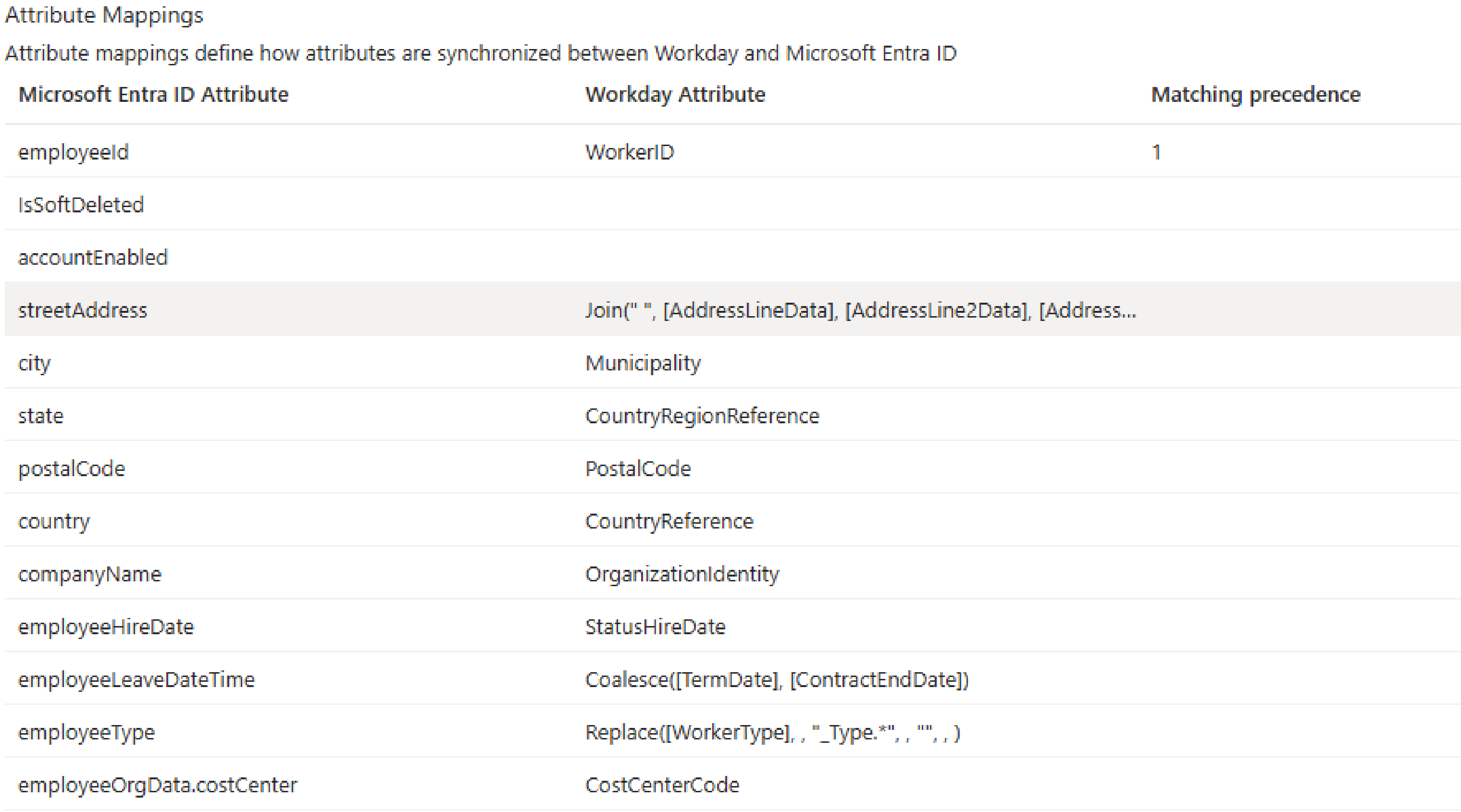
One applications reads inbound to create the users account and populate attributes from the HR system

One application writes back key attributes back into the HR system

Attribute Mapping - Overview

Attribute mapping are CRITICAL to the success of your onboarding process.

***Protip:* DO NOT take Microsoft default mappings as gospel!**



Attribute Mappings

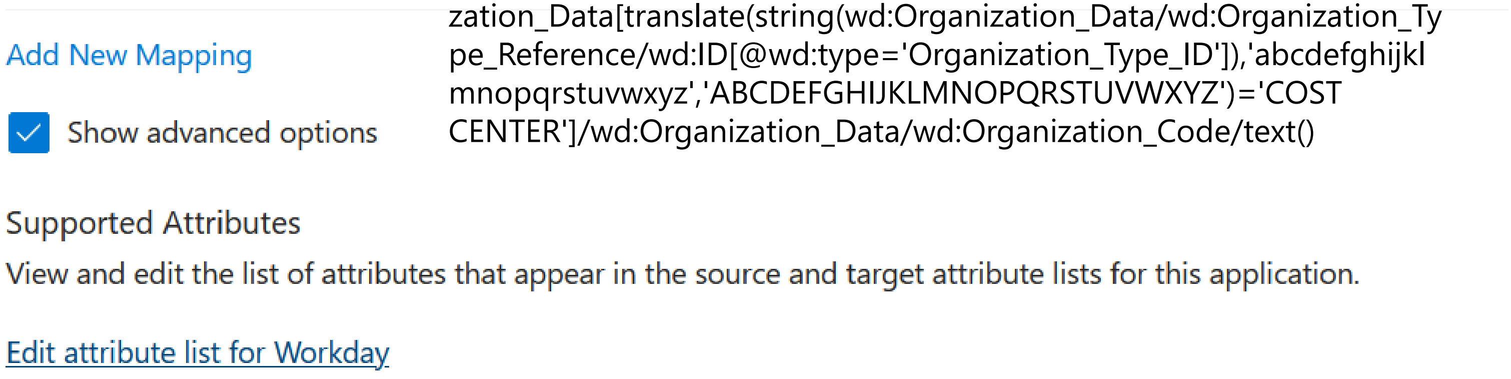
Attribute mappings define how attributes are synchronized between Workday and Microsoft Entra ID

Microsoft Entra ID Attribute	Workday Attribute	Matching precedence
employeeId	WorkerID	1
IsSoftDeleted		
accountEnabled		
streetAddress	Join(" ", [AddressLineData], [AddressLine2Data], [Address...	
city	Municipality	
state	CountryRegionReference	
postalCode	PostalCode	
country	CountryReference	
companyName	OrganizationIdentity	
employeeHireDate	StatusHireDate	
employeeLeaveDateTime	Coalesce([TermDate], [ContractEndDate])	
employeeType	Replace([WorkerType], , "_Type.*", , "", ,)	
employeeOrgData.costCenter	CostCenterCode	

Attribute Mapping - Overview

If all else fails, you may have to update the XPATH mapping

wd:Worker/wd:Worker_Data/wd:Organization_Data/wd:Worker_Organization_Data[translate(string(wd:Organization_Data/wd:Organization_Type_Reference/wd:ID[@wd:type='Organization_Type_ID']),'abcdefghijklmnopqrstuvwxyz','ABCDEFGHIJKLMNOPQRSTUVWXYZ')='COST CENTER']/wd:Organization_Data/wd:Organization_Code/text()



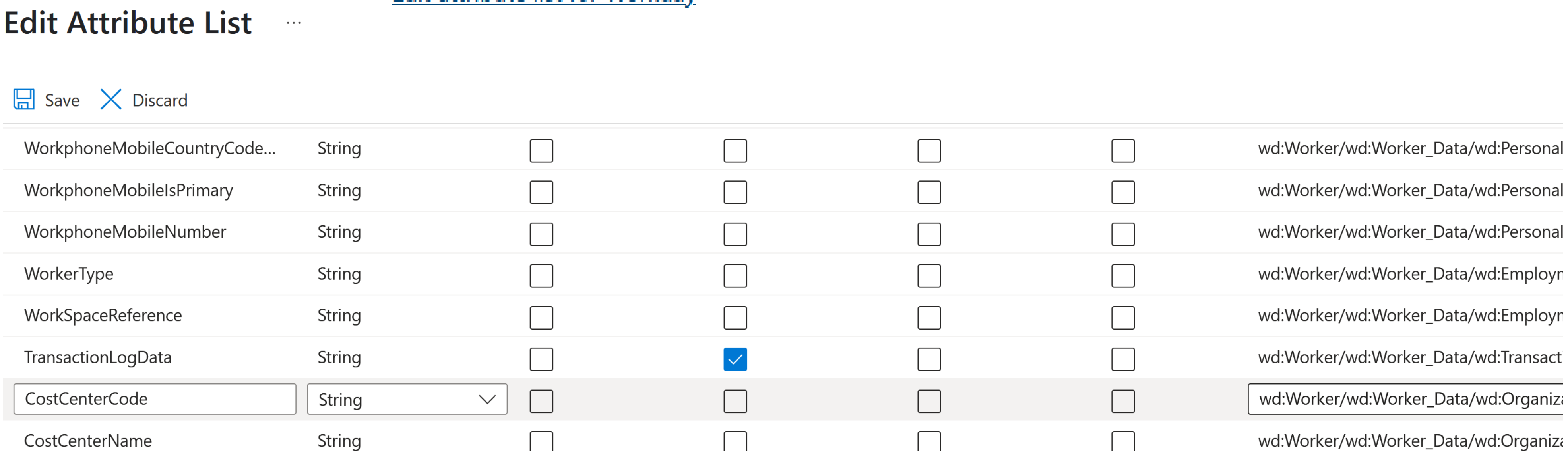
Add New Mapping

☑ Show advanced options

Supported Attributes

View and edit the list of attributes that appear in the source and target attribute lists for this application.

Edit attribute list for Workday



Edit Attribute List

WorkphoneMobileCountryCode...	String	□	□	□	□	wd:Worker/wd:Worker_Data/wd:Personal
WorkphoneMobileIsPrimary	String	□	□	□	□	wd:Worker/wd:Worker_Data/wd:Personal
WorkphoneMobileNumber	String	□	□	□	□	wd:Worker/wd:Worker_Data/wd:Personal
WorkerType	String	□	□	□	□	wd:Worker/wd:Worker_Data/wd:Employn
WorkSpaceReference	String	□	□	□	□	wd:Worker/wd:Worker_Data/wd:Employn
TransactionLogData	String	□	☑	□	□	wd:Worker/wd:Worker_Data/wd:Transact
CostCenterCode	String	□	□	□	□	wd:Worker/wd:Worker_Data/wd:Organiz
CostCenterName	String	□	□	□	□	wd:Worker/wd:Worker_Data/wd:Organiz

Attribute Mapping - Lessons Learned

1. employeeID are important as the key source of truth
   (if you're not populating userprincipal names in your HR system, don't let it fall in the matching preference
2. accountEnabled shouldn't have a value from your HR system if you're not controlling security from your HR system – again, **your mileage may vary**!
3. employeeType may need some massaging with coming off your HR system
4. employeeLeaveDateTime may need some work if you manage full time and temp employyes
   a. ***Protip:*** use Coalesce to look at fields if they're populated and populate one if the other is empty
      ```
      Coalesce([TermDate], [ContractEndDate])
      ```
5. mailNickname feeds into your Exchange Online environment and based on naming may need some normalization…. more on this in the userPrincipalName…..
6. userPrincipalName, like mailnickname, may need some normalization
   a. ***Protip:*** Use NormalizeDiacritics to fix non-English names and StripSpaces
      ```
      Join("@", Replace(NormalizeDiacritics(StripSpaces(Join(".",
      [PreferredFirstName], [PreferredLastName]))), , "[^a-zA-Z0-9\\.]*", , "",
      , ), "contoso.com")
      ```
7. extensionAttributes are your friend – you can so more where your HR system cant!

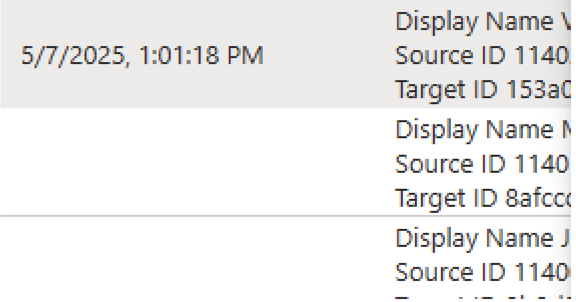
Attribute Mapping – extension Attributes

extensionAttributes are your friend – you can so more where your HR system's static values end
We'll take this a little further in our Identity Governance section

- extensionAttribute2 `Replace([WorkerType], , "_Type.*", , "", , )`
  - ***Protip:*** Remove the specific text and anything afterwards
- extensionAttribute3 `IIF(DateDiff("d", Now(), CDate([ContractEndDate]))>="0", "True", "False")`
  - ***Protip:*** If the contract end date is not earlier than today, its False, otherwise True (then we run a workflow to disable the account)
  - If there isn't a date then this value is blank and thus it won't be populated
- extensionAttribute4 `Replace([WorkerSubType], "_", , , "-", , )`
  - ***Protip:*** Remove the specific text and anything afterwards

Let's see this in action in the real world…..

Attribute Mapping – extension Attributes

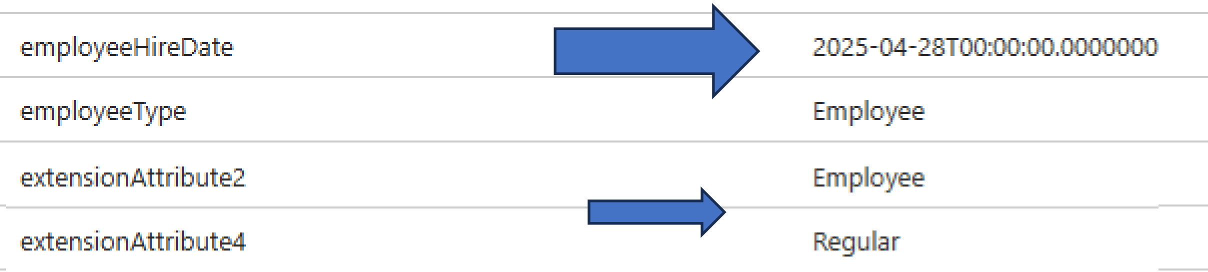


5/7/2025, 1:01:18 PM

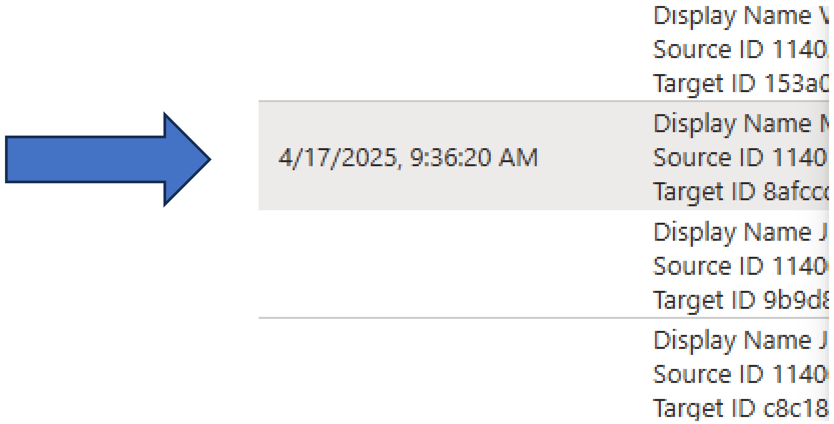
Display Name V
Source ID 1140
Target ID 153a0

Display Name M
Source ID 1140
Target ID 8afcc

Display Name J
Source ID 1140



employeeHireDate	2025-04-28T00:00:00.0000000
employeeType	Employee
extensionAttribute2	Employee
extensionAttribute4	Regular



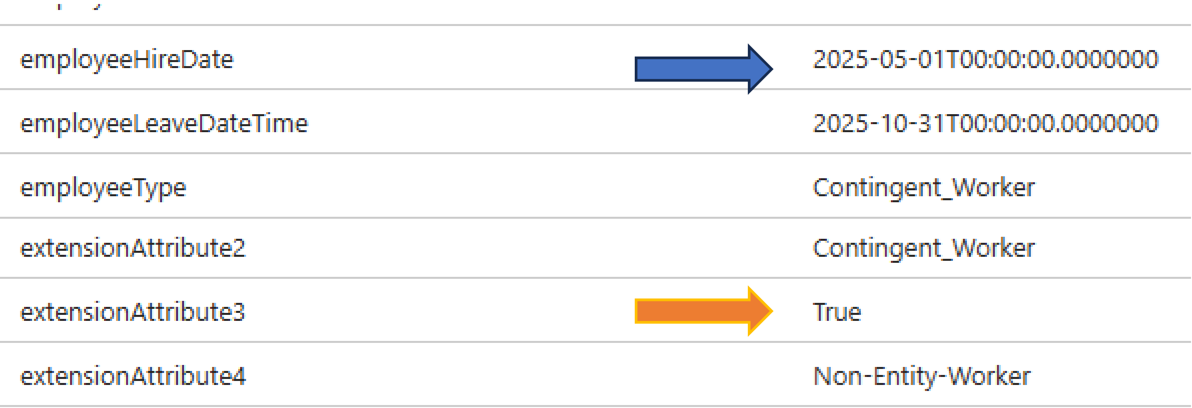
Display Name V
Source ID 1140
Target ID 153a0

4/17/2025, 9:36:20 AM

Display Name M
Source ID 1140
Target ID 8afcc

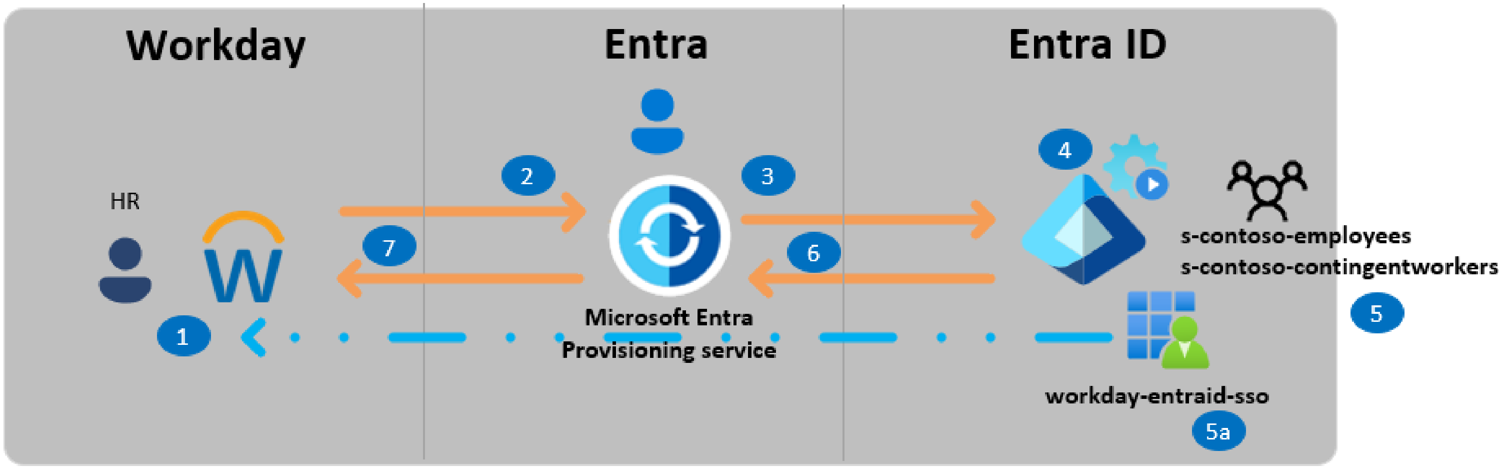
Display Name J
Source ID 1140
Target ID 9b9d8

Display Name J
Source ID 1140
Target ID c8c18



employeeHireDate	2025-05-01T00:00:00.0000000
employeeLeaveDateTime	2025-10-31T00:00:00.0000000
employeeType	Contingent_Worker
extensionAttribute2	Contingent_Worker
extensionAttribute3	True
extensionAttribute4	Non-Entity-Worker

HR Workflow



1. The HR team performs worker transactions (Joiners/Movers/Leavers or New Hires/Transfers/Terminations) in Workday Employee Central
2. The Microsoft Entra provisioning service runs scheduled synchronizations of identities from Workday EC and identifies new users that need to be provisioned into Entra ID based on the business line (text) being **Consoso**.
3. The Microsoft Entra provisioning service determines the attribute changes and writes them to the user object
4. The Entra Lifecycle Workflow engine invokes update/enable/disable operation for the user in Microsoft Entra ID.
5. User is dynamically populated into either **s-contoso-employees & s-contoso-contingentworkers** group(s) based their CompanyName (as Contoso) or extensonattribute2 [as **Contingent_Worker_Type_ID**] for contractors
    a. This will also grant them access into Workday by way of the **workday-entra-sso** Enterprise App
6. Workday Writeback app is configured, it retrieves attributes such as email, username and phone number from Microsoft Entra ID.
7. Microsoft Entra provisioning service sets userID as userprincipalname in Workday.

This is just the first step on your modernized user management journey

The next step is how to manage the accounts once they're there!

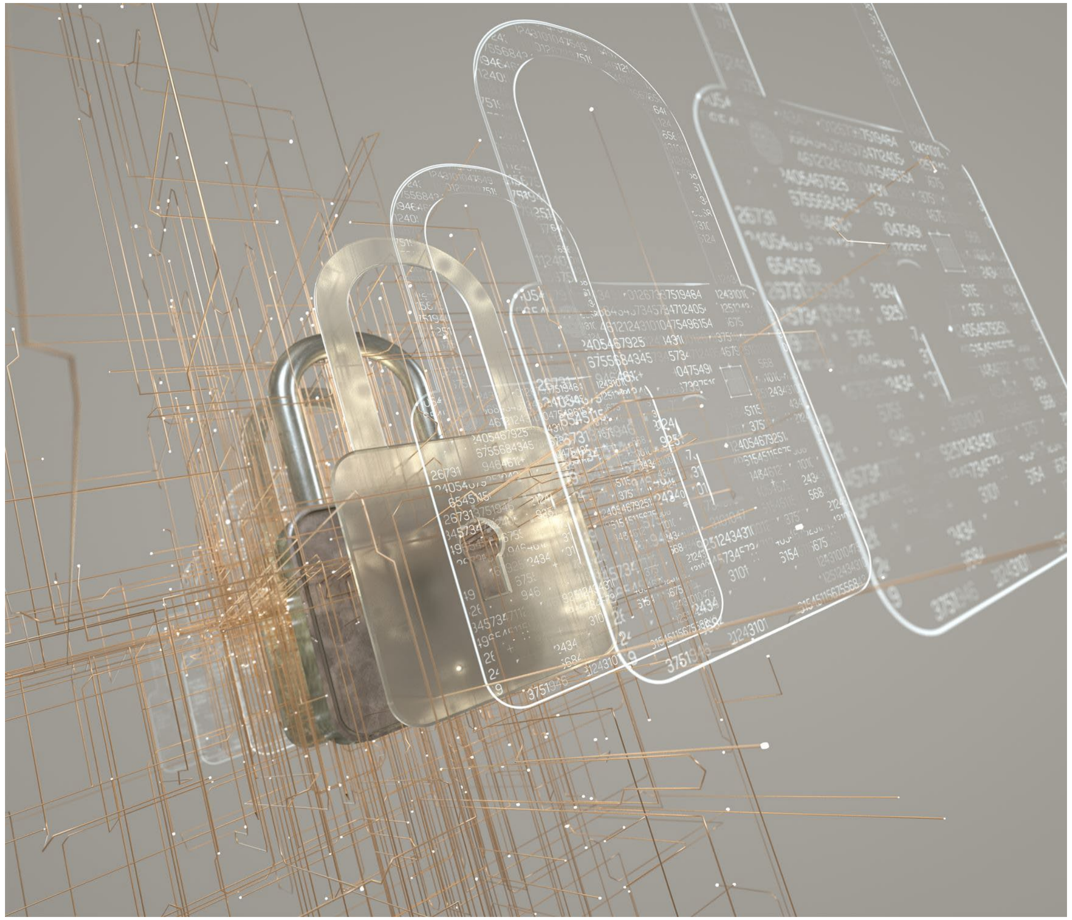
(thanks Copilot for the imagine!

Modern Identity Governance

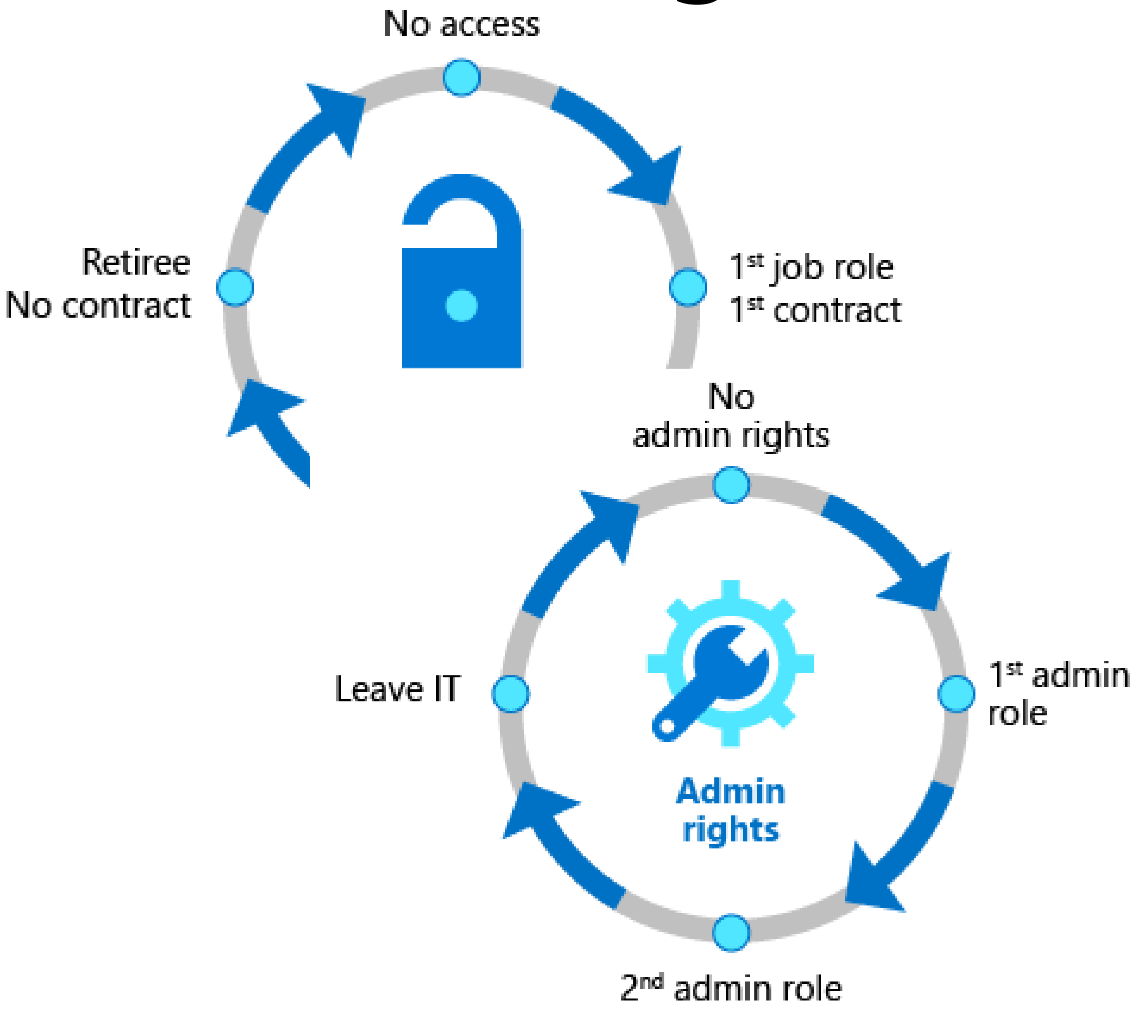
Discover the importance of the user lifecycle and how to use Entra Identity Governance to manage identities across platforms effectively.

Introduction to Microsoft Entra ID Governance

- Automating the Identity Lifecycle
- Key Jobs in Identity Governance
- Microsoft Entra ID Governance (EIDG) Core Services



Automating the Identity Lifecycle



- inbound provisioning from your organization's HR sources, including retrieving from your HR system, to automatically maintain user identities in both Active Directory and Microsoft Entra ID.
- lifecycle workflows to automate workflow tasks that run at certain key events, such before a new employee is scheduled to start work at the organization, as they change status during their time in the organization, and as they leave the organization.
- automatic assignment policies in entitlement management to add and remove a user's group memberships, application roles, and SharePoint site roles, based on changes to the user's attributes.
- user provisioning to create, update, and remove user accounts in other applications, with connectors to hundreds of cloud and on-premises applications via SCIM, LDAP and SQL.
- Privileged Identity Management (PIM) provides additional controls tailored to securing access rights for resources, across Microsoft Entra, Azure, other Microsoft Online Services and other applications.

Key Jobs in Identity Governance

- **Joiner**: Templates and automated actions through workflows make the identity process efficient and infallible for IT admins and enables access quicker for new team members
- **Mover**: Team members who have experienced change get access to new resources immediately, while outdated access is removed without IT
- **Leaver**: Customizable workflow templates for common offboarding tasks ensures timely, reliable resource access removal for IT, and peace of mind for former team members

EIDG Core Services

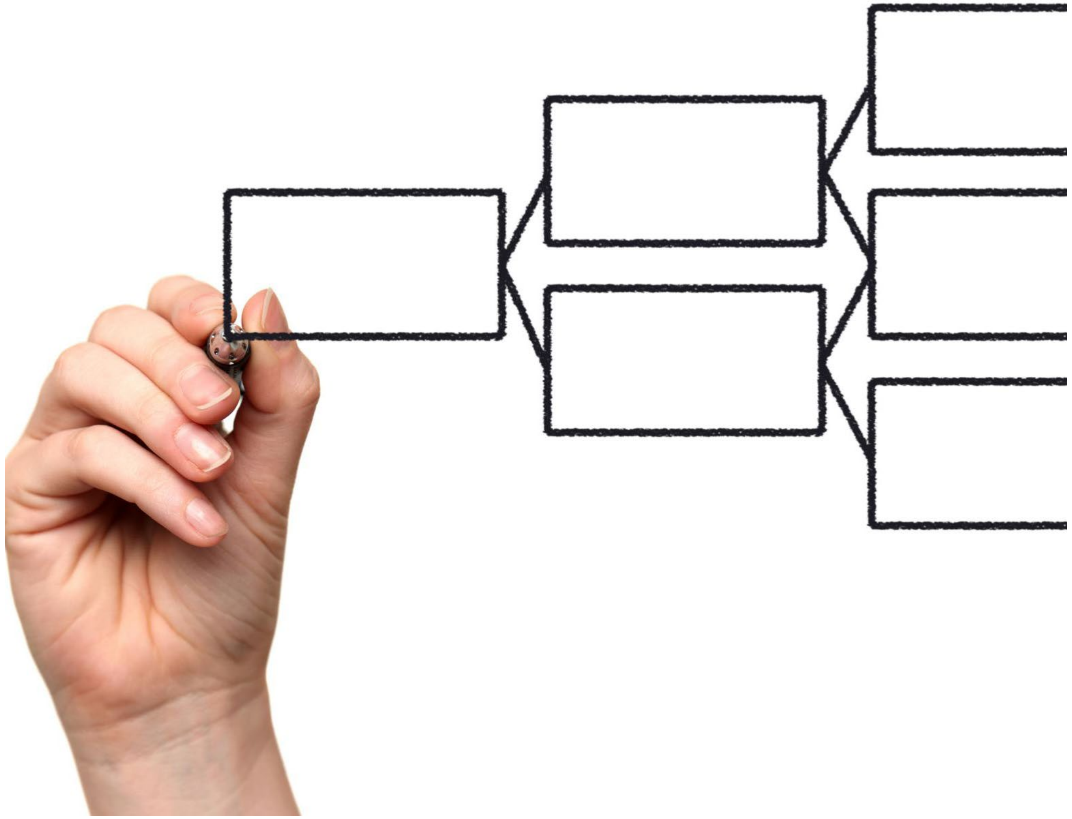
4 Core components that sits on top of Microsoft's flagship identity and access management (IDAM) platform:

1. Lifecycle Workflows
   - enables organizations to manage **Microsoft Entra users** by automating these **three basic lifecycle processes**
2. Entitlement Management
   - process of **requesting**, **approving** and **expiration** of access is automated and self-service by using so called **access packages**.
3. Access Reviews
   - **user's access** can be **reviewed regularly** to make sure **only the right people have continued access**
4. Privileged Identity Management
   - provides **time-based** and **approval-based role activation** to mitigate the risks of excessive, unnecessary, or misused access permissions

Deployment Approach Overview

Understanding Lifecycle Workflows

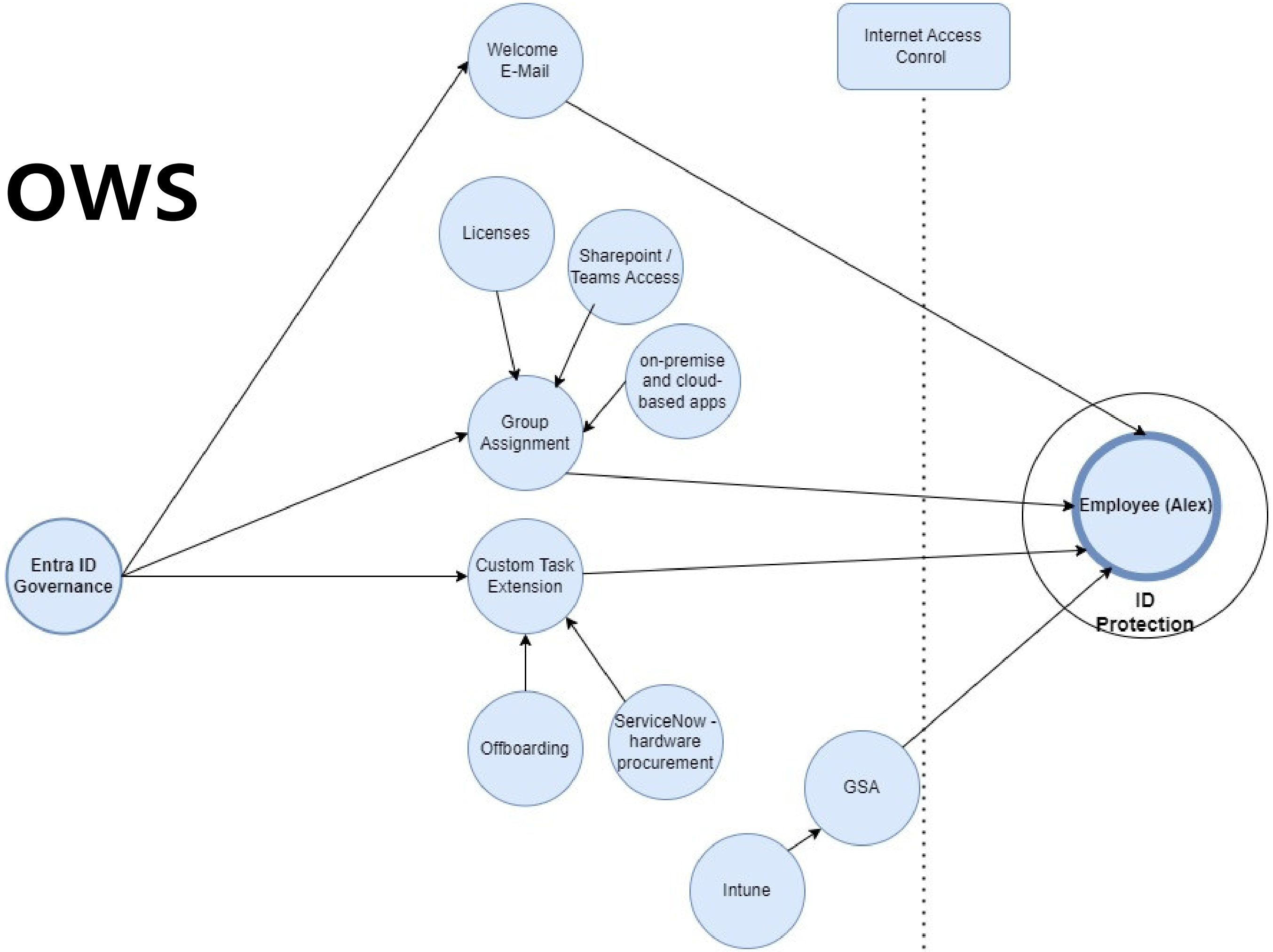
Key phases align with the identity lifecycle



Lifecycle Workflows

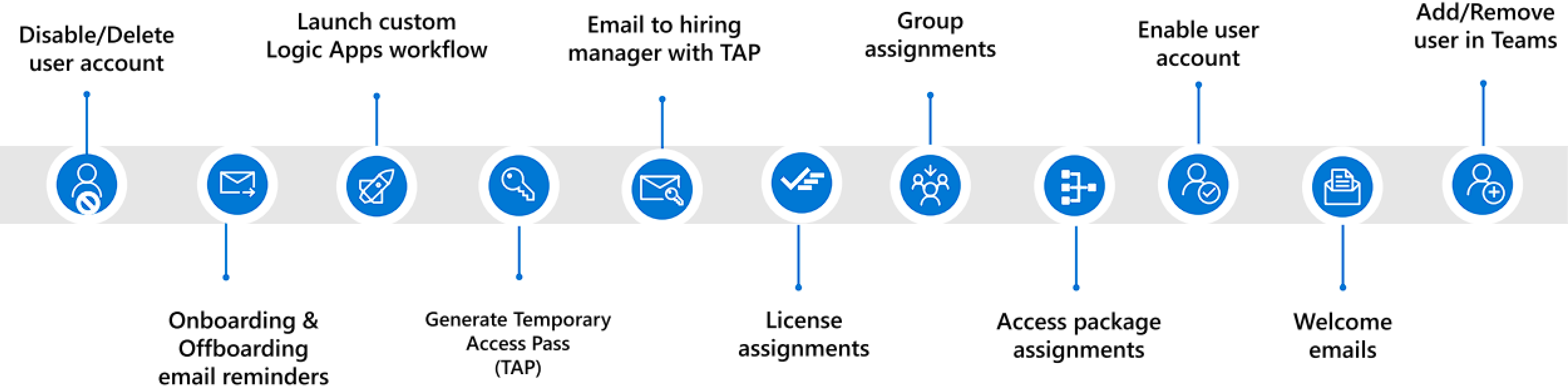
Workflows won't manage the creation or deletion of accounts but will manage what happens to them!

Detailing your onboarding and offboarding process is an important step prior to configuration.



- Which users should have access to which resources?
- What are those users doing with that access?
- Is there effective organizational control for managing access?
- Can auditors verify that the controls are working?
- Are users ready to go on day one or do they have access removed in a timely manner?

Key Phases of the Identity Lifecycle



Disable/Delete user account

Onboarding & Offboarding email reminders

Launch custom Logic Apps workflow

Generate Temporary Access Pass (TAP)

Email to hiring manager with TAP

License assignments

Group assignments

Access package assignments

Enable user account

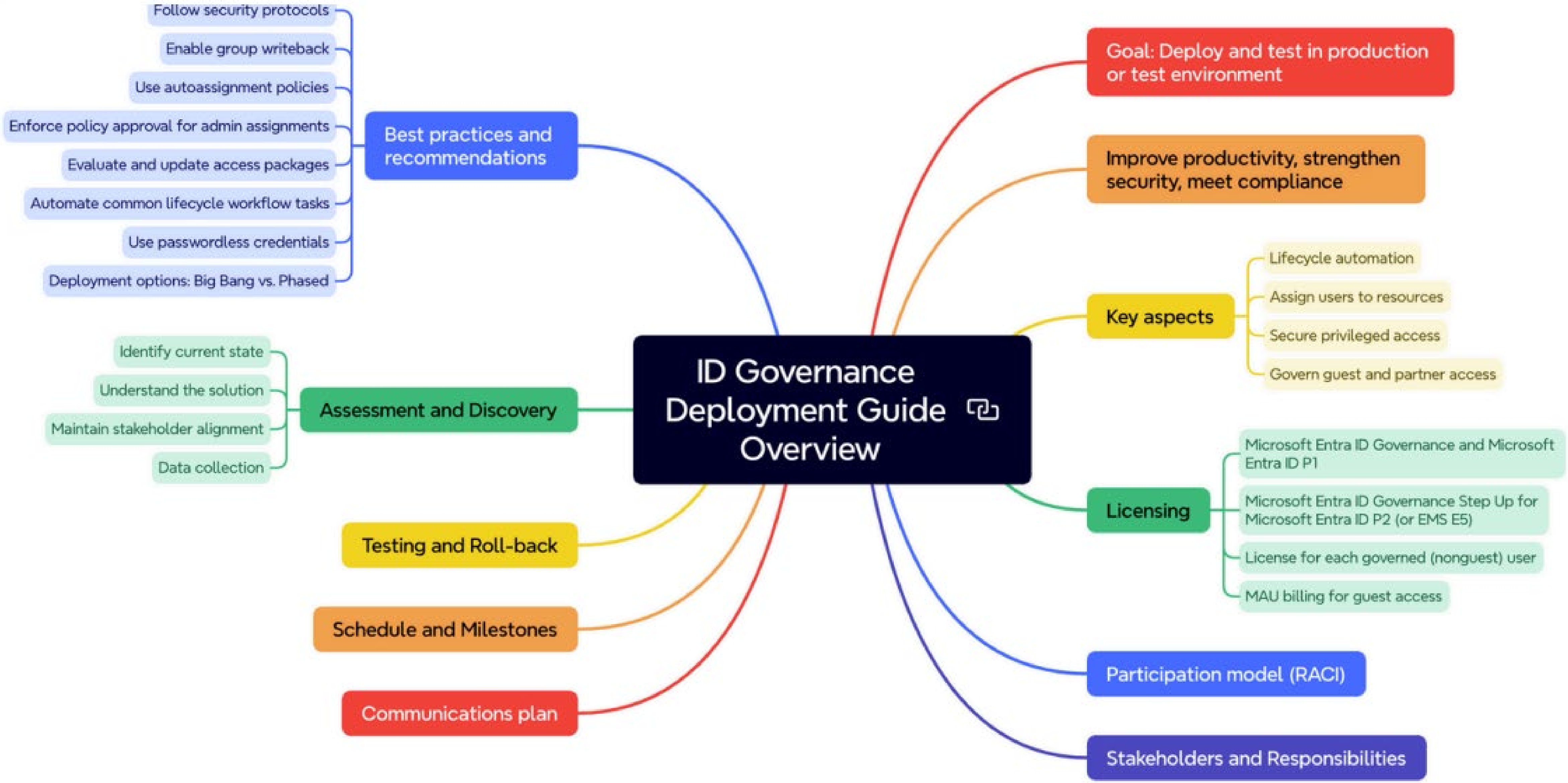
Welcome emails

Add/Remove user in Teams

Entra ID Governance Deployment

1. Automating Employee Lifecycles
2. Assigning Resource Access
3. Managing Guest and Partner Access
4. Govern Privileged Identity

https://microsoft.github.io/EntraIDGovernance-Training/



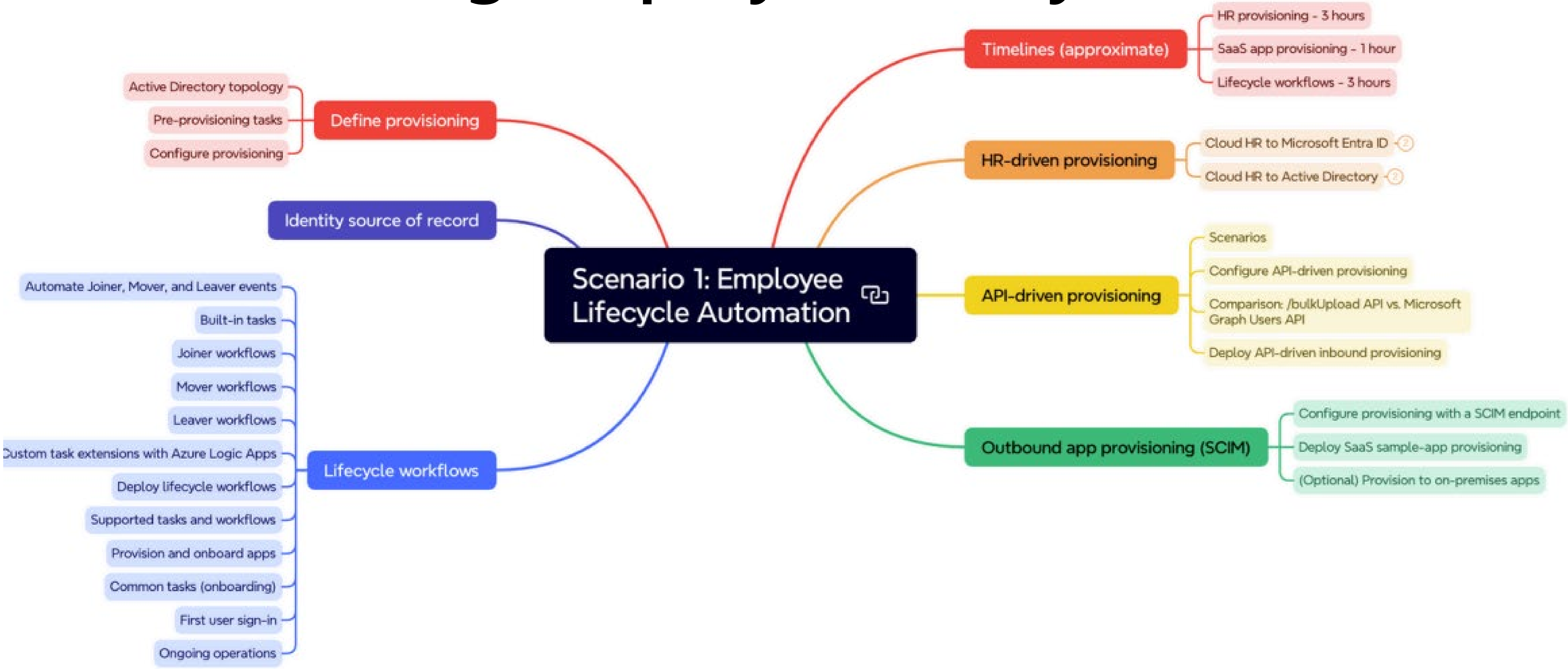
ID Governance Deployment Guide Overview

- Best practices and recommendations
  - Follow security protocols
  - Enable group writeback
  - Use autoassignment policies
  - Enforce policy approval for admin assignments
  - Evaluate and update access packages
  - Automate common lifecycle workflow tasks
  - Use passwordless credentials
  - Deployment options: Big Bang vs. Phased
- Assessment and Discovery
  - Identify current state
  - Understand the solution
  - Maintain stakeholder alignment
  - Data collection
- Testing and Roll-back
- Schedule and Milestones
- Communications plan
- Goal: Deploy and test in production or test environment
- Improve productivity, strengthen security, meet compliance
- Key aspects
  - Lifecycle automation
  - Assign users to resources
  - Secure privileged access
  - Govern guest and partner access
- Licensing
  - Microsoft Entra ID Governance and Microsoft Entra ID P1
  - Microsoft Entra ID Governance Step Up for Microsoft Entra ID P2 (or EMS E5)
  - License for each governed (nonguest) user
  - MAU billing for guest access
- Participation model (RACI)
- Stakeholders and Responsibilities

Automating Employee Lifecycles

- Key Phases
- Workflows, Triggers & Tasks
- Notifications
- Reporting

Automating Employee Lifecycle



Scenario 1: Employee Lifecycle Automation

- Define provisioning
  - Active Directory topology
  - Pre-provisioning tasks
  - Configure provisioning
- Identity source of record
- Lifecycle workflows
  - Automate Joiner, Mover, and Leaver events
  - Built-in tasks
  - Joiner workflows
  - Mover workflows
  - Leaver workflows
  - ustom task extensions with Azure Logic Apps
  - Deploy lifecycle workflows
  - Supported tasks and workflows
  - Provision and onboard apps
  - Common tasks (onboarding)
  - First user sign-in
  - Ongoing operations
- Timelines (approximate)
  - HR provisioning - 3 hours
  - SaaS app provisioning - 1 hour
  - Lifecycle workflows - 3 hours
- HR-driven provisioning
  - Cloud HR to Microsoft Entra ID
  - Cloud HR to Active Directory
- API-driven provisioning
  - Scenarios
  - Configure API-driven provisioning
  - Comparison: /bulkUpload API vs. Microsoft Graph Users API
  - Deploy API-driven inbound provisioning
- Outbound app provisioning (SCIM)
  - Configure provisioning with a SCIM endpoint
  - Deploy SaaS sample-app provisioning
  - (Optional) Provision to on-premises apps

Key Phases of the Identity Lifecycle

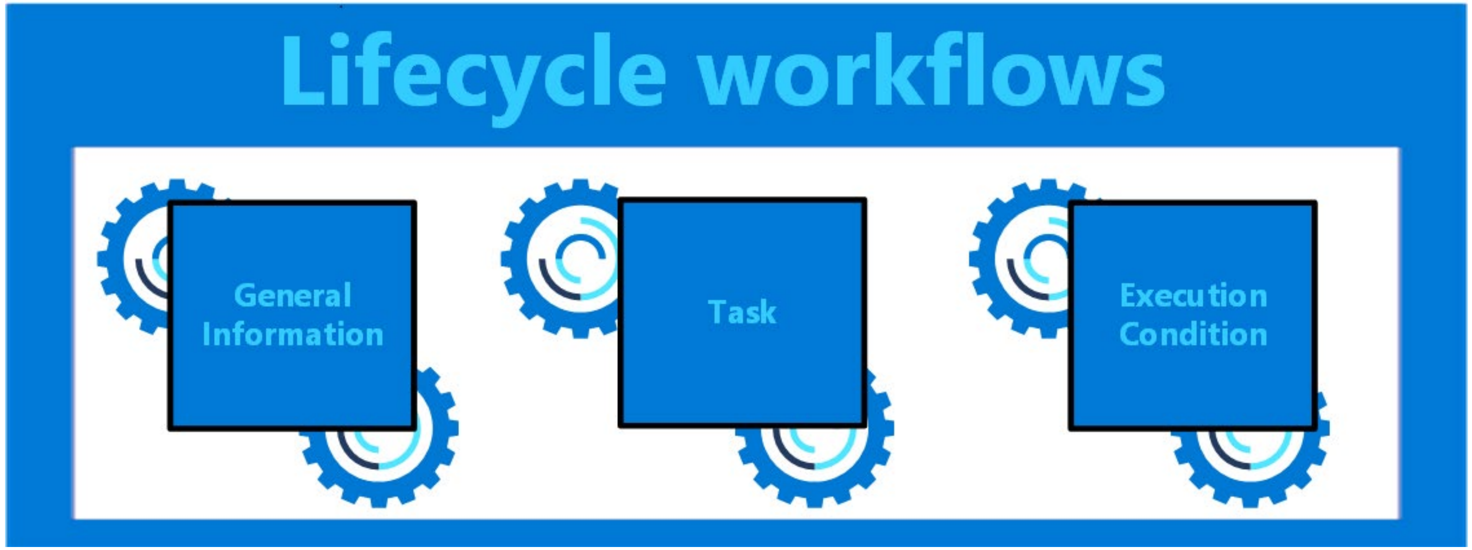
Before building a Lifecycle Workflow in the portal, you should determine which scenario or scenarios you wish to deploy.

Scenario	Predefined Tasks
Onboard prehire employee	Generate TAP and Send Email
Onboard new hire employee	Enable User Account Send Welcome Email Add User To Groups
Real-time employee termination	Remove user from all groups Remove user from all Teams Delete User Account
Pre-Offboarding of an employee	Remove user from selected groups Remove user from selected Teams
Offboard an employee	Disable User Account Remove user from all groups Remove user from all Teams
Post-Offboarding of an employee	Remove all licenses for user Remove user from all Teams Delete User Account
Real-time employee change	Run a Custom Task Extension
Employee group membership changes	Remove access package assignment for user Remove user from selected Teams Send email to notify manager of user move
Employee job profile change	Send email to notify manager of user move Remove user from selected groups Remove user from selected Teams Request user access package assignment

Workflows

Workflows automate tasks based on the joiner-mover-leaver(JML) cycle of lifecycle management, and split tasks for users into categories of where they fall in the lifecycle of an organization.

These categories extend into templates, where they can be quickly customized to suit the needs of users in your organization.



Workflow part	Description
General information	This portion of a workflow covers basic information such as display name, and a description of what the workflow does.
Tasks	Tasks are the actions that are taken when a workflow is executed.
Execution conditions	Defines when(trigger), and for who(scope), a scheduled workflow runs.

Trigger

The supported scheduled triggers are:

- Attribute Changes
- Group Membership change
- Time based

2

The scope depends on the trigger that you use:

- For **Attribute changes**, the trigger is rule based and triggered when the attribute you defined is changed for a user.
- For **Group membership change**, the trigger is group-based and triggered if a user is added or removed from a specific group.
- For Time based attribute, the trigger is rule based and triggered when the time value you defined is met by a user.

1

By default, workflows are scheduled to run every 3 hours.
You can set the interval to be as frequent as 1 hour or as infrequent as 24 hours.

3

Predefined tasks are generally sufficient for most tasks. When you need extra tasks Custom tasks can be triggered via an extension to Azure Logic Apps. This can be used to extend the capabilities of Lifecycle Workflow beyond the built-in tasks.
The steps for triggering a Logic App based on a custom task extension are as follows:

- Create a custom task extension.
- Select which behavior you want the custom task extension to take.
- Link your custom task extension to a new or existing Azure Logic App.
- Add the custom task to a workflow.

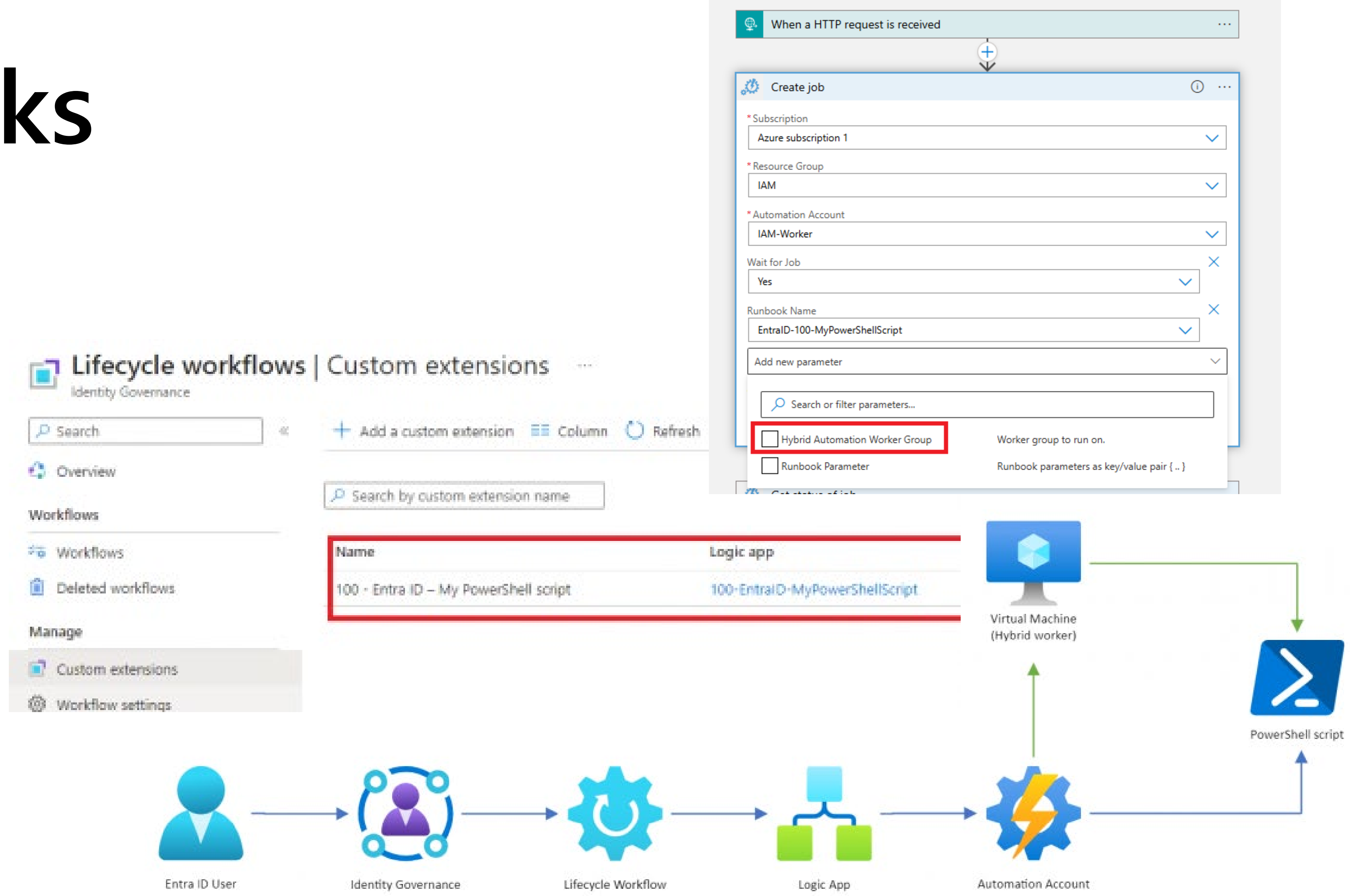
Supported Tasks

Lifecycle Workflow's built-in tasks and can be used to create either new workflows from scratch or inserted into workflow templates so that they fit the needs of your organization.

Task	Description	Relevant Scenarios
Add user to groups	Add user to selected groups	Joiner - Leaver - Mover
Add user to selected teams	Add user to Teams	Joiner - Leaver - Mover
Assign licenses to users	Assign licenses to user	Joiner - Mover
Delete User Account	Delete user account in Microsoft Entra ID	Leaver
Disable User Account	Disable user account in the directory	Joiner - Leaver
Enable User Account	Enable user account in the directory	Joiner - Leaver
Generate TAP and Send Email	Generate Temporary Access Pass and send via email to user's manager	Joiner
Remove all licenses of user	Remove all licenses assigned to the user	Leaver
Remove user from all groups	Remove user from all Microsoft Entra group memberships	Leaver
Remove user from all Teams	Remove user from all Teams memberships	Leaver
Remove user from selected groups	Remove user from membership of selected Microsoft Entra groups	Joiner - Leaver - Mover
Remove user from selected Teams	Remove user from membership of selected Teams	Joiner - Leaver - Mover
Run a Custom Task Extension	Run a Custom Task Extension to callout to an external system	Joiner - Leaver - Mover
Send email after user's last day	Send offboarding email to user's manager after the last day of work	Leaver
Send email before user's last day	Send offboarding email to user's manager before the last day of work	Leaver
Send email on user's last day	Send offboarding email to user's manager on the last day of work	Leaver
Send Welcome Email	Send welcome email to new hire	Joiner
Send onboarding reminder email	Send onboarding reminder email to user’s manager	Joiner
Request user access package assignment	Request user assignment to selected access packages	Joiner - Mover
Remove access package assignment for user	Remove user assignment from selected access packages	Leaver - Mover
Remove all access package assignments for user	Remove all access packages assigned to the user	Leaver
Remove selected license assignments from user	Remove select license assignment from user	Leaver - Mover
Cancel all pending access package assignment requests for users	Cancel all pending access package assignment requests for users	Leaver

Custom Tasks

The Lifecycle Workflows in Entra ID Governance comes with great default tasks options out-of-the-box, but it becomes so much more **powerful** when you start to use the **Custom extension** tasks in your Lifecycle Workflows.



When a HTTP request is received

Create job

* Subscription: Azure subscription 1

* Resource Group: IAM

* Automation Account: IAM-Worker

Wait for Job: Yes

Runbook Name: EntraID-100-MyPowerShellScript

Add new parameter

Search or filter parameters...

□ Hybrid Automation Worker Group — Worker group to run on.

□ Runbook Parameter — Runbook parameters as key/value pair { .. }

Lifecycle workflows | Custom extensions

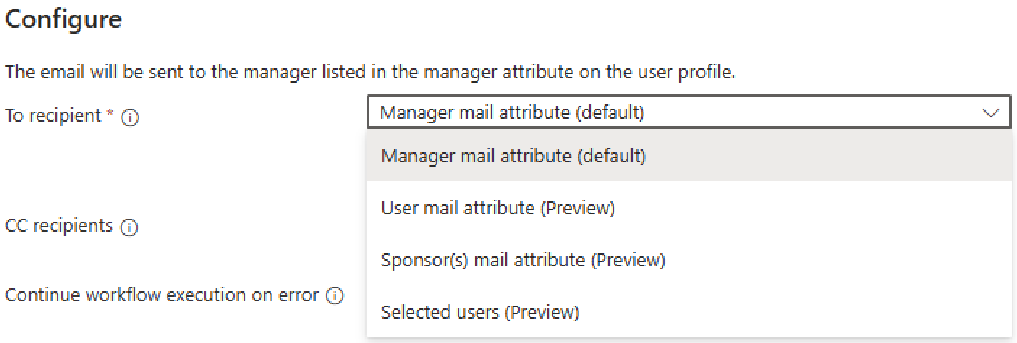
Identity Governance

Search by custom extension name

Name	Logic app
100 - Entra ID – My PowerShell script	100-EntraID-MyPowerShellScript

Notifications

When you're customizing the subject or message body, we recommend that you also enable the custom sender domain and organizational branding. Otherwise, your email will contain an additional security disclaimer.



Configure

The email will be sent to the manager listed in the manager attribute on the user profile.

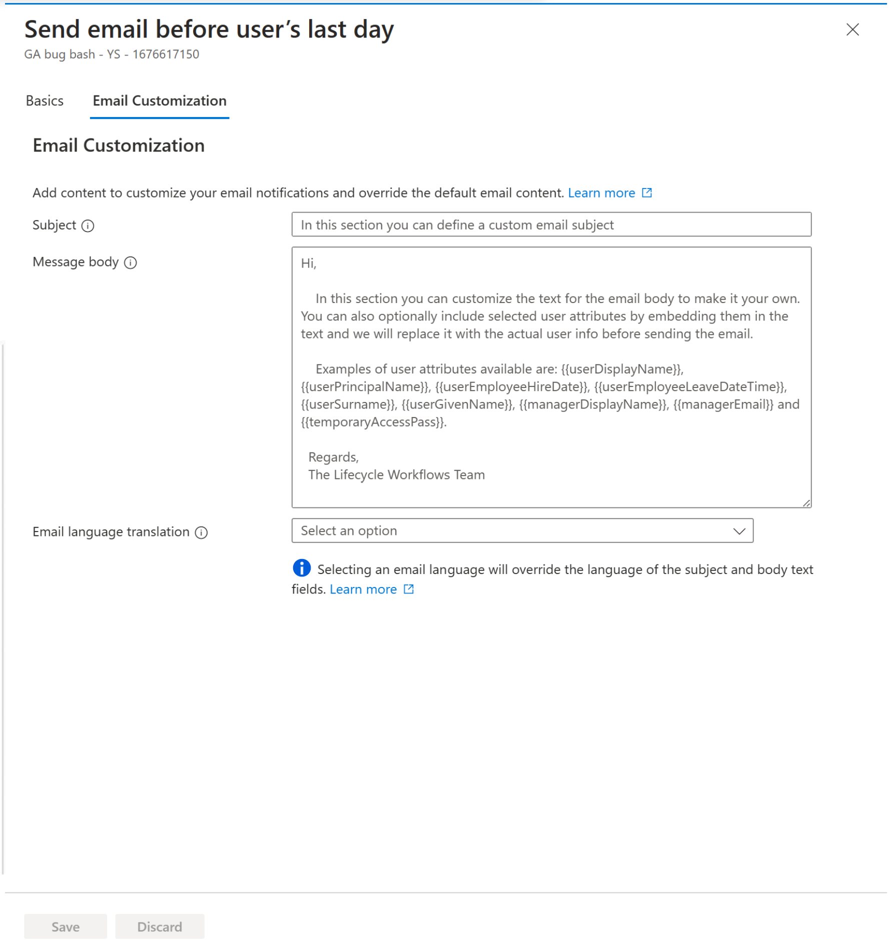
To recipient * ⓘ: Manager mail attribute (default)

- Manager mail attribute (default)
- User mail attribute (Preview)
- Sponsor(s) mail attribute (Preview)
- Selected users (Preview)

CC recipients ⓘ

Continue workflow execution on error ⓘ

Enable task * ⓘ ☑



Send email before user's last day

GA bug bash - YS - 1676617150

Basics | Email Customization

Email Customization

Add content to customize your email notifications and override the default email content. Learn more

Subject ⓘ: In this section you can define a custom email subject

Message body ⓘ:

Hi,

In this section you can customize the text for the email body to make it your own. You can also optionally include selected user attributes by embedding them in the text and we will replace it with the actual user info before sending the email.

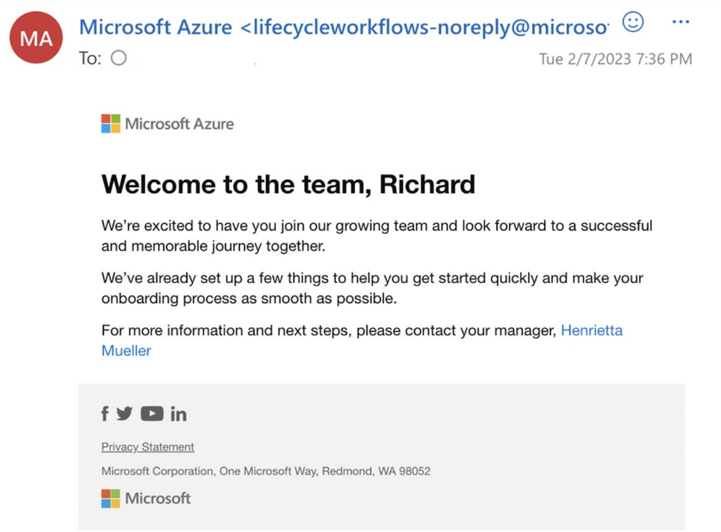
Examples of user attributes available are: {{userDisplayName}}, {{userPrincipalName}}, {{userEmployeeHireDate}}, {{userEmployeeLeaveDateTime}}, {{userSurname}}, {{userGivenName}}, {{managerDisplayName}}, {{managerEmail}} and {{temporaryAccessPass}}.

Regards,
The Lifecycle Workflows Team

Email language translation ⓘ: Select an option

ⓘ Selecting an email language will override the language of the subject and body text fields. Learn more

Save | Discard



MA Microsoft Azure <lifecycleworkflows-noreply@microso

To: ○

Tue 2/7/2023 7:36 PM

Microsoft Azure

Welcome to the team, Richard

We're excited to have you join our growing team and look forward to a successful and memorable journey together.

We've already set up a few things to help you get started quickly and make your onboarding process as smooth as possible.

For more information and next steps, please contact your manager, Henrietta Mueller

f 🐦 ▶ in

Privacy Statement

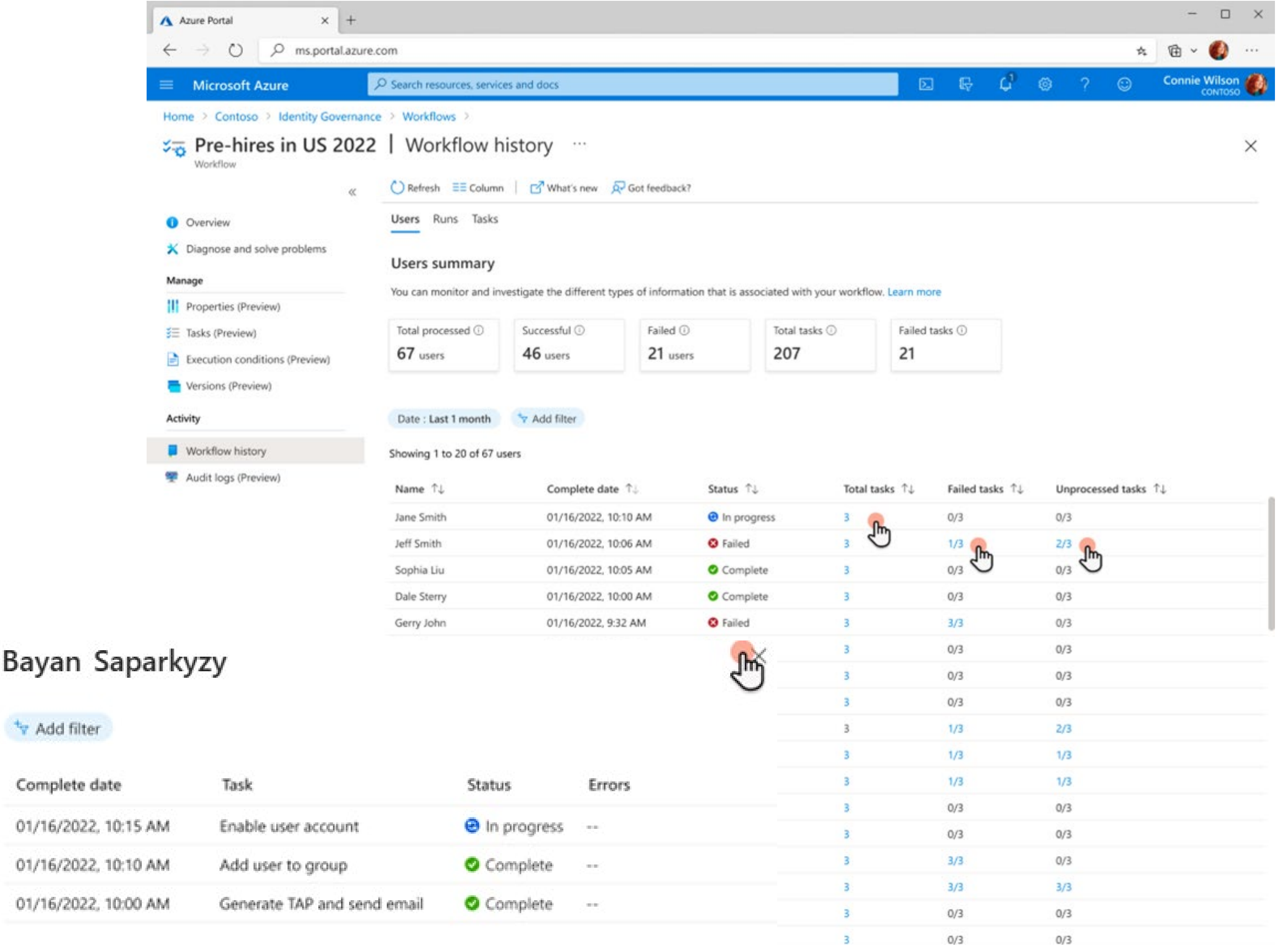
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

Microsoft

Reporting

Lifecycle Workflows provide summaries to see how often a workflow has run, and who it ran successfully for. You're also able to check the status of both the workflow, and its tasks.

Checking the status of workflows and their tasks allows you to troubleshoot potential problems that could come up during their execution.



Home > Contoso > Identity Governance > Workflows >

Pre-hires in US 2022 | Workflow history

Workflow

Users summary

You can monitor and investigate the different types of information that is associated with your workflow. Learn more

Total processed	Successful	Failed	Total tasks	Failed tasks
67 users	46 users	21 users	207	21

Date : Last 1 month | Add filter

Showing 1 to 20 of 67 users

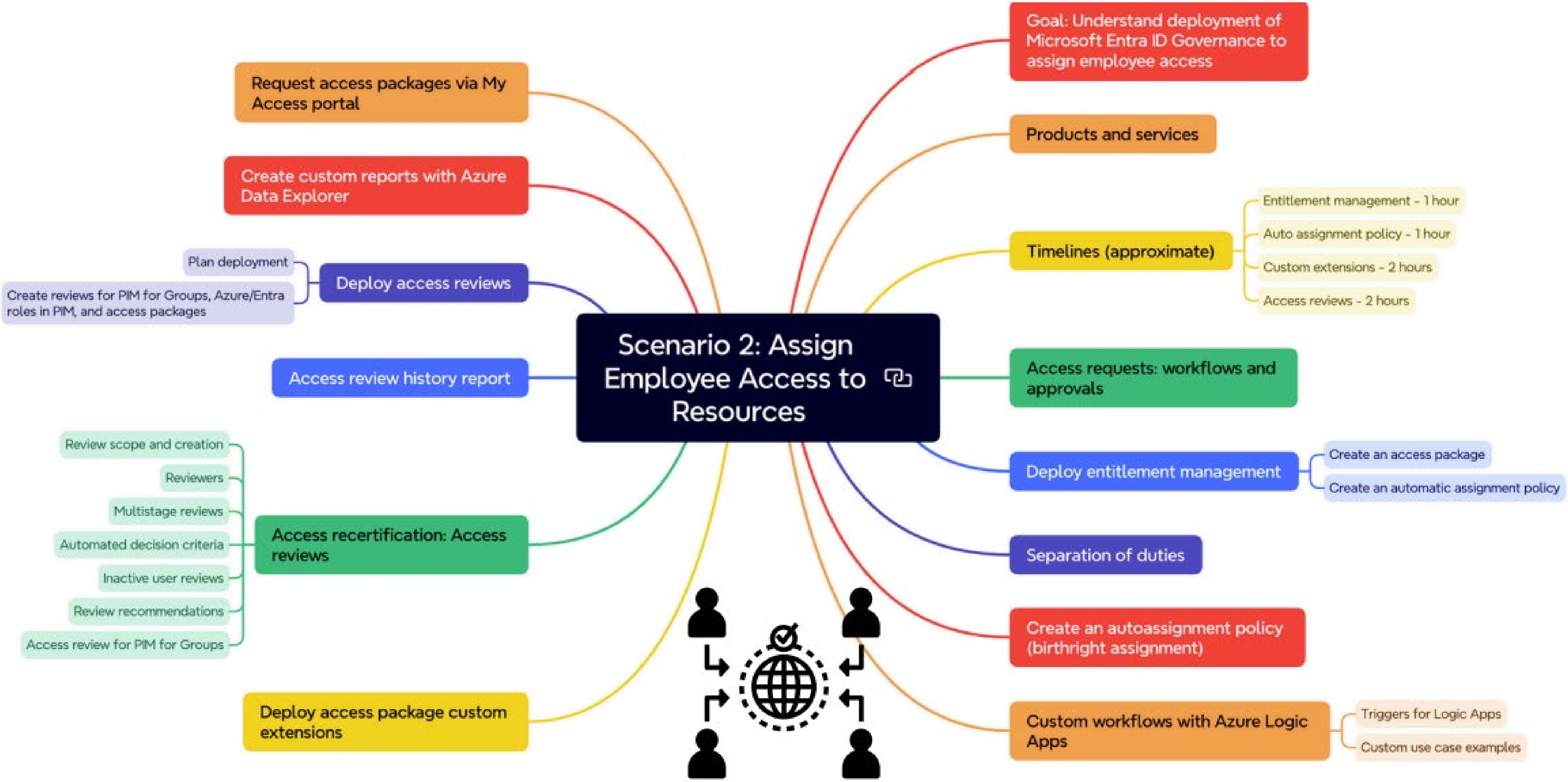
Name	Complete date	Status	Total tasks	Failed tasks	Unprocessed tasks
Jane Smith	01/16/2022, 10:10 AM	In progress	3	0/3	0/3
Jeff Smith	01/16/2022, 10:06 AM	Failed	3	1/3	2/3
Sophia Liu	01/16/2022, 10:05 AM	Complete	3	0/3	0/3
Dale Sterry	01/16/2022, 10:00 AM	Complete	3	0/3	0/3
Gerry John	01/16/2022, 9:32 AM	Failed	3	3/3	0/3
			3	0/3	0/3
			3	0/3	0/3
			3	0/3	0/3
			3	1/3	2/3
			3	1/3	1/3
			3	1/3	1/3
			3	0/3	0/3
			3	0/3	0/3
			3	3/3	0/3
			3	3/3	3/3
			3	0/3	0/3
			3	0/3	0/3

Bayan Saparkyzy

Add filter

Complete date	Task	Status	Errors
01/16/2022, 10:15 AM	Enable user account	In progress	--
01/16/2022, 10:10 AM	Add user to group	Complete	--
01/16/2022, 10:00 AM	Generate TAP and send email	Complete	--

Assigning Resource Access

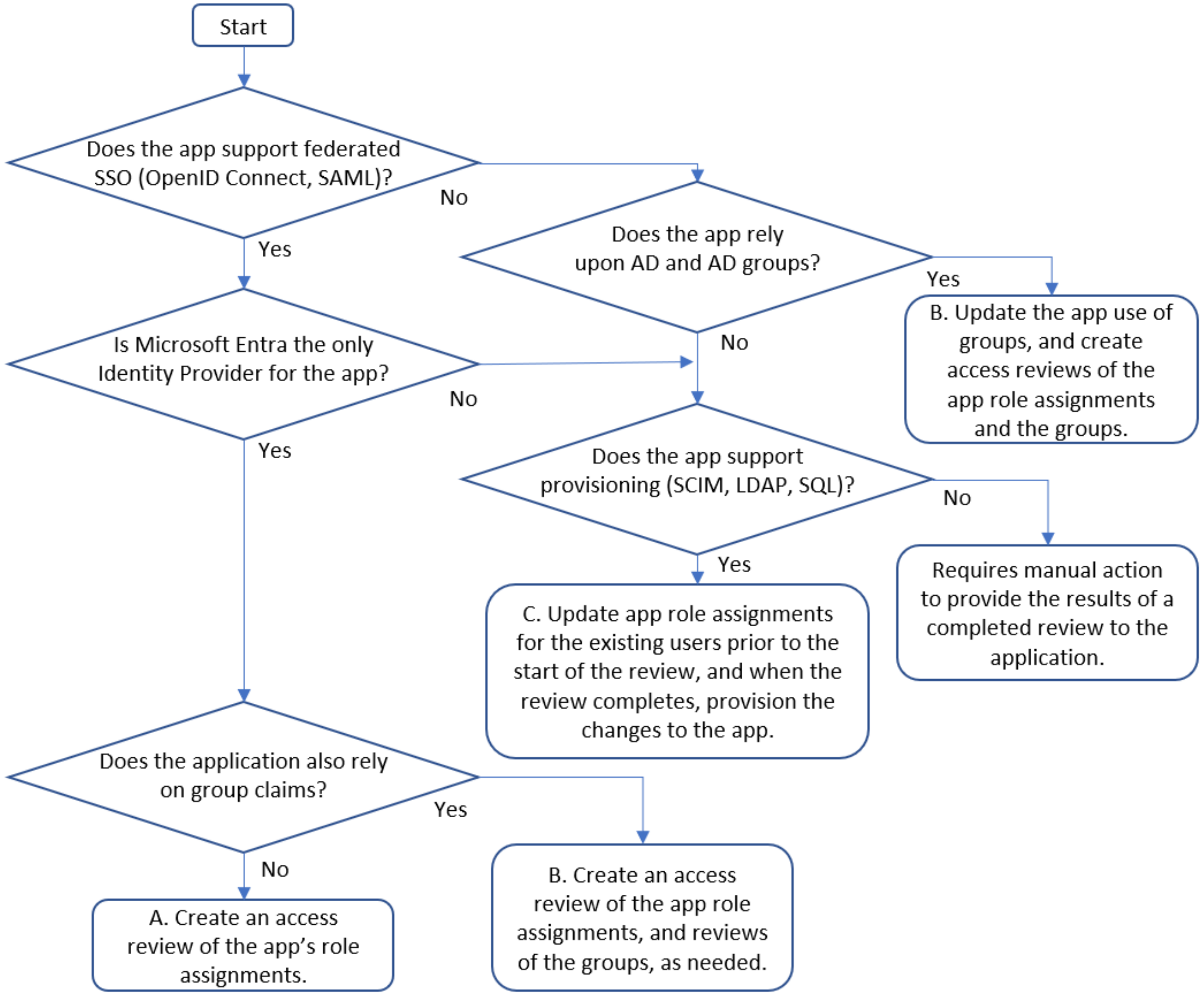


Scenario 2: Assign Employee Access to Resources

- Goal: Understand deployment of Microsoft Entra ID Governance to assign employee access
- Products and services
- Timelines (approximate)
  - Entitlement management - 1 hour
  - Auto assignment policy - 1 hour
  - Custom extensions - 2 hours
  - Access reviews - 2 hours
- Access requests: workflows and approvals
- Deploy entitlement management
  - Create an access package
  - Create an automatic assignment policy
- Separation of duties
- Create an autoassignment policy (birthright assignment)
- Custom workflows with Azure Logic Apps
  - Triggers for Logic Apps
  - Custom use case examples
- Request access packages via My Access portal
- Create custom reports with Azure Data Explorer
- Deploy access reviews
  - Plan deployment
  - Create reviews for PIM for Groups, Azure/Entra roles in PIM, and access packages
- Access review history report
- Access recertification: Access reviews
  - Review scope and creation
  - Reviewers
  - Multistage reviews
  - Automated decision criteria
  - Inactive user reviews
  - Review recommendations
  - Access review for PIM for Groups
- Deploy access package custom extensions

Assigning Resource Access

- Catalog Management
- Using Access Packages
- Why Access Reviews



Start

Does the app support federated SSO (OpenID Connect, SAML)?

Yes

No

Is Microsoft Entra the only Identity Provider for the app?

Yes

No

Does the app rely upon AD and AD groups?

Yes

No

B. Update the app use of groups, and create access reviews of the app role assignments and the groups.

Does the app support provisioning (SCIM, LDAP, SQL)?

Yes

No

C. Update app role assignments for the existing users prior to the start of the review, and when the review completes, provision the changes to the app.

Requires manual action to provide the results of a completed review to the application.

Does the application also rely on group claims?

Yes

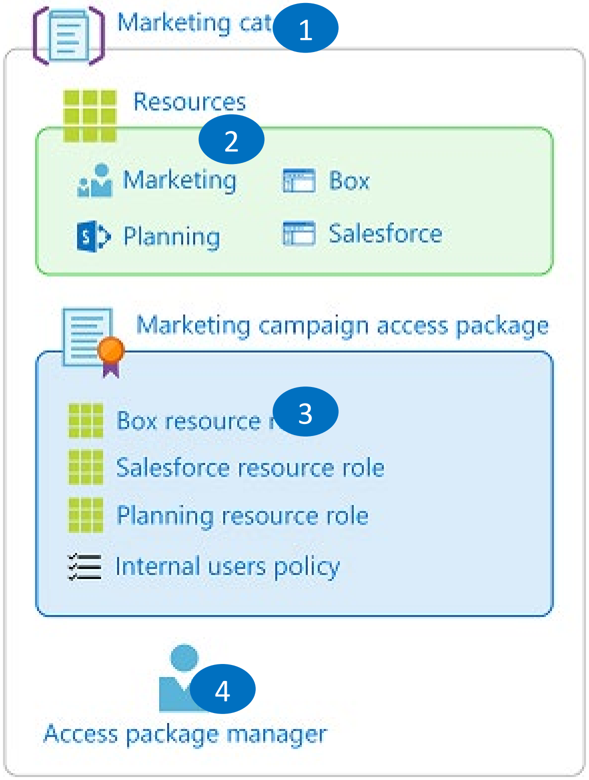
No

A. Create an access review of the app’s role assignments.

B. Create an access review of the app role assignments, and reviews of the groups, as needed.

Catalog Management

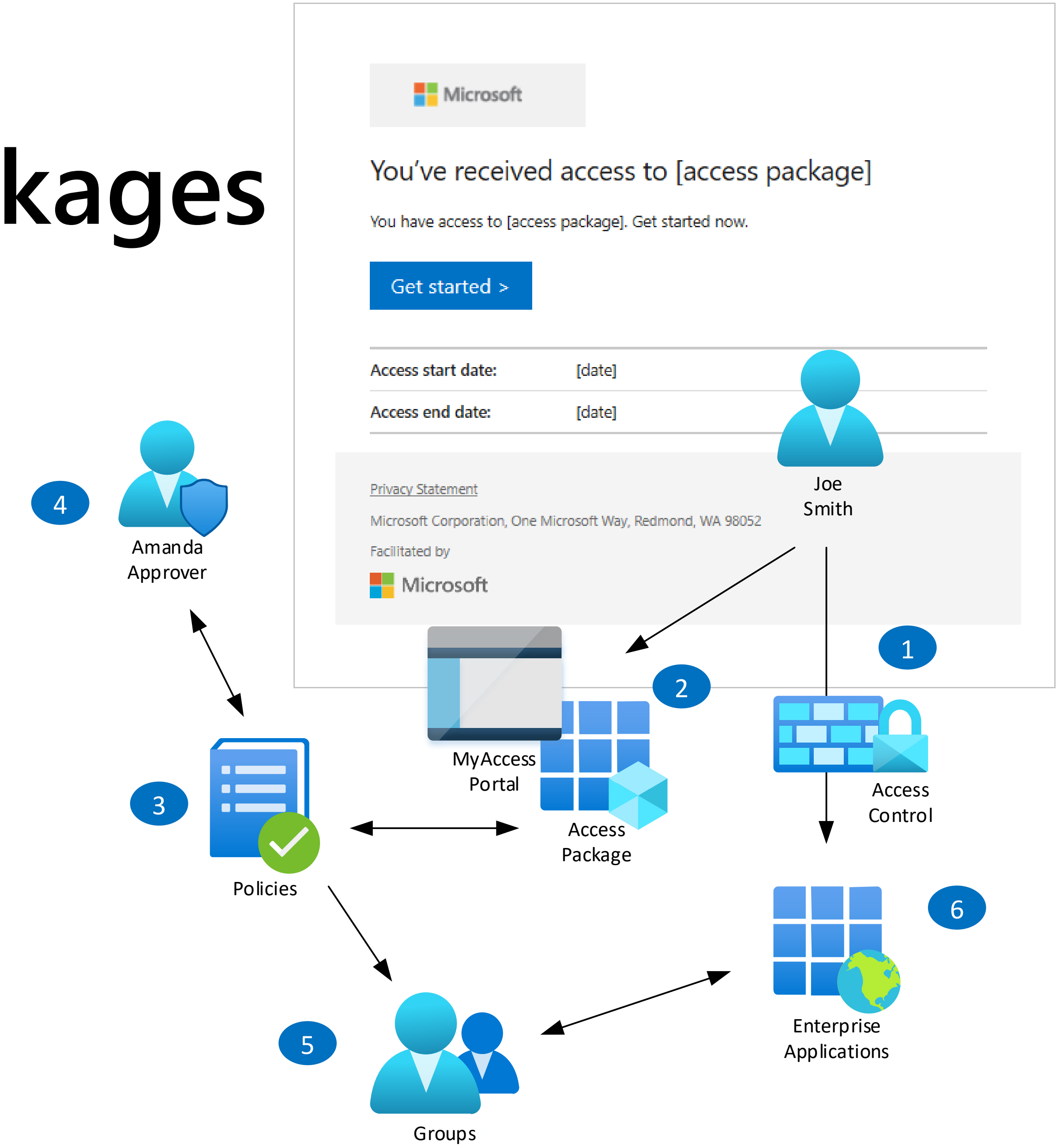
1. Select the catalog where you want to put the access package and ensure that it has the necessary resources.
2. Add resource roles from resources in the catalog to your access package.
3. Specify an initial policy for users who can request access.
4. Specify approval settings and lifecycle settings in that policy.



Scenario	Number of policies
I want all users in my directory to have the same request and approval settings for an access package	One
I want all users in certain connected organizations to be able to request an access package	One
I want to allow users in my directory and also users outside my directory to request an access package	Two
I want to specify different approval settings for some users	One for each group of users
I want some users access package assignments to expire while other users can extend their access	One for each group of users
I want some users to request access and other users to be assigned access by an administrator	Two
I want some users in my organization to receive access automatically, other users in my organization to be able to request, and other users to be assigned access by an administrator	Three

Using Access Packages

1. End user requires access to SSO application. Company policy says that requests must come by way of an access request
2. User goes to MyAccess portal to request application from the catalog
3. Based on the Access Package policy, either the resource is automatically assigned or goes to an approver(s)
4. Approver(s) receive notification to add user
5. User is added to Resource role. This can be a group, application, Sharepoint site, or Entra role.
6. Once added to the resource, the user is allowed access to the application



Microsoft

You've received access to [access package]

You have access to [access package]. Get started now.

Get started >

Access start date: [date]

Access end date: [date]

Privacy Statement

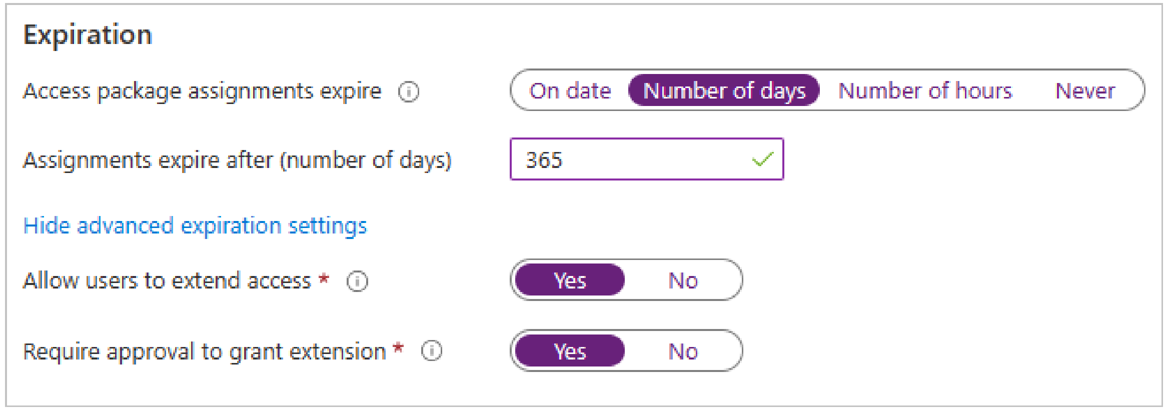
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

Facilitated by

Microsoft

Why Access Reviews

- **Control collaboration**: Access reviews allow you to manage access to all the resources your users need. When users share and collaborate, you can be assured that the information is among authorized users only.
- **Manage risk**: Access reviews provide you with a way to review access to data and applications, which lowers the risk of data leakage and data spill. You gain the capability to regularly review external partners' access to corporate resources.
- **Address compliance and governance**: With access reviews, you can govern and recertify the access lifecycle to groups, apps, and sites. You can control and track reviews for compliance or risk-sensitive applications specific to your organization.
- **Reduce cost**: Access reviews are built in the cloud and natively work with cloud resources such as groups, applications, and access packages. Using access reviews is less costly than building your own tools or otherwise upgrading your on-premises tool set.



Expiration

Access package assignments expire ⓘ: On date [✓ Number of days] Number of hours Never

Assignments expire after (number of days): 365 ✓

Hide advanced expiration settings

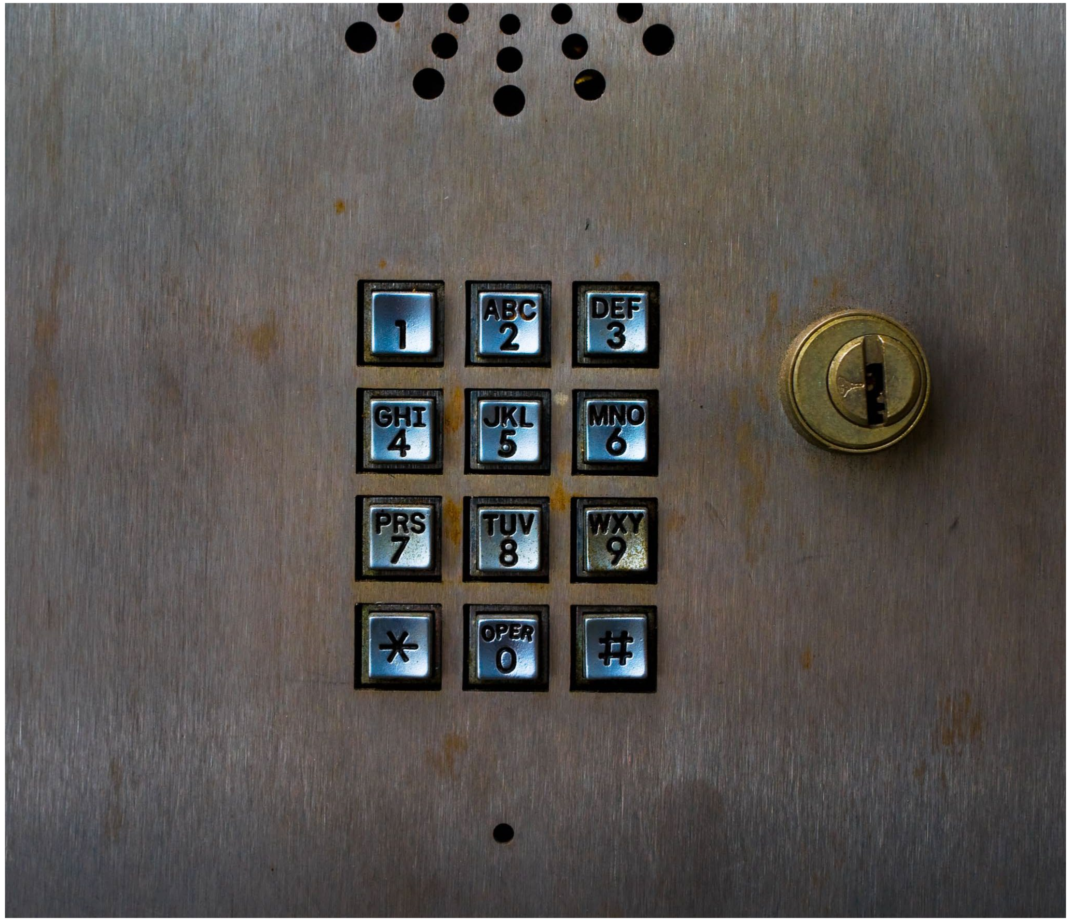
Allow users to extend access * ⓘ: [✓ Yes] No

Require approval to grant extension * ⓘ: [✓ Yes] No

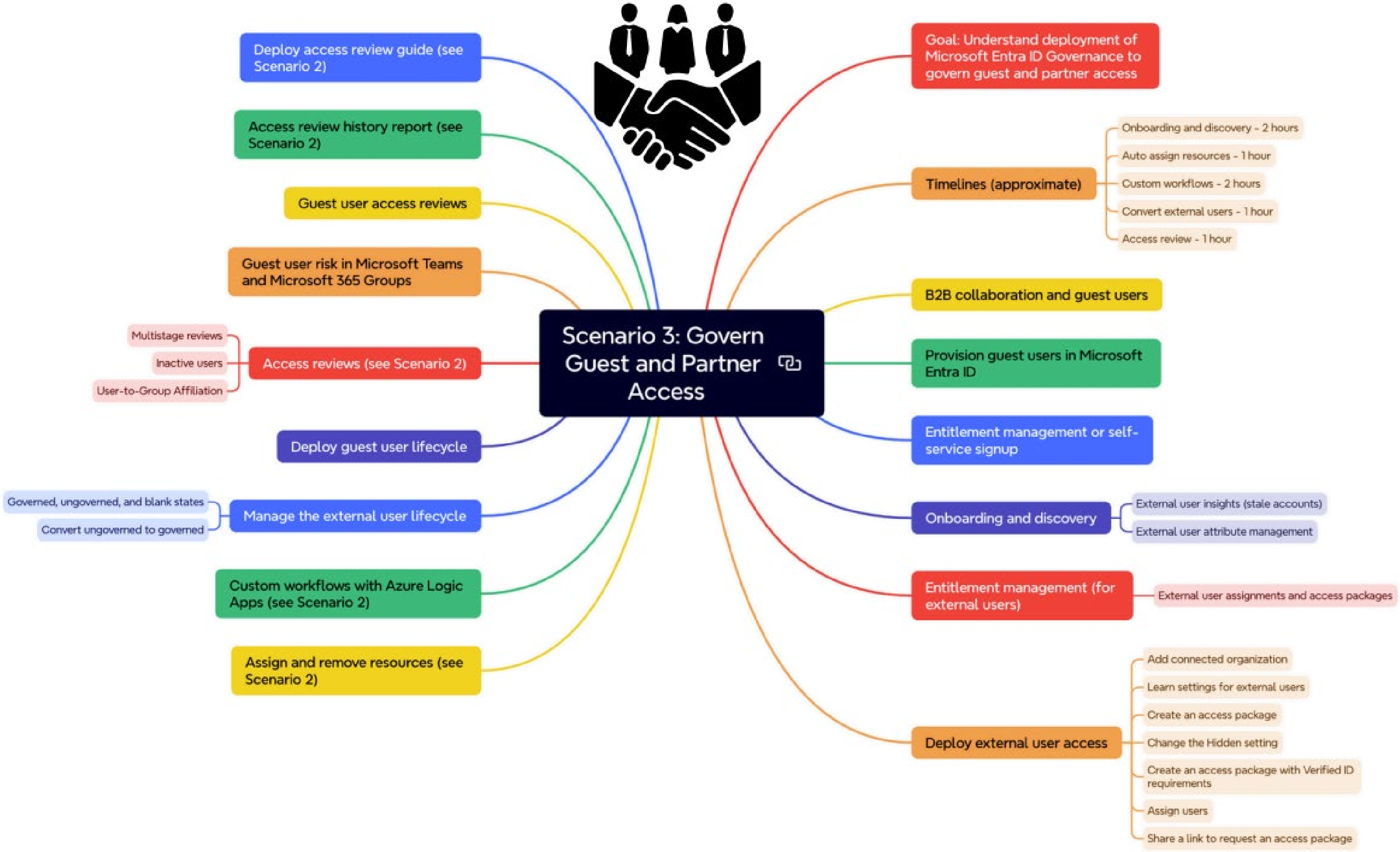
Component	Value
Resources to review	Access to Microsoft Dynamics.
Review frequency	Monthly.
Who does the review	Dynamics business group Program Managers.
Notification	Email is sent at the start of a review to the alias Dynamics-Pms.Include an encouraging custom message to reviewers to secure their buy-in.
Timeline	48 hours from notification.
Automatic actions	Remove access from any account that has no interactive sign-in within 90 days by removing the user from the Security group dynamics-access.Perform actions if not reviewed within timeline.
Manual actions	Reviewers can do removals approval prior to automated action if desired.

Managing Guest and Partner Access

- Onboarding
- Options for Review
- Using Access Packages



Managing Guest and Partner Access

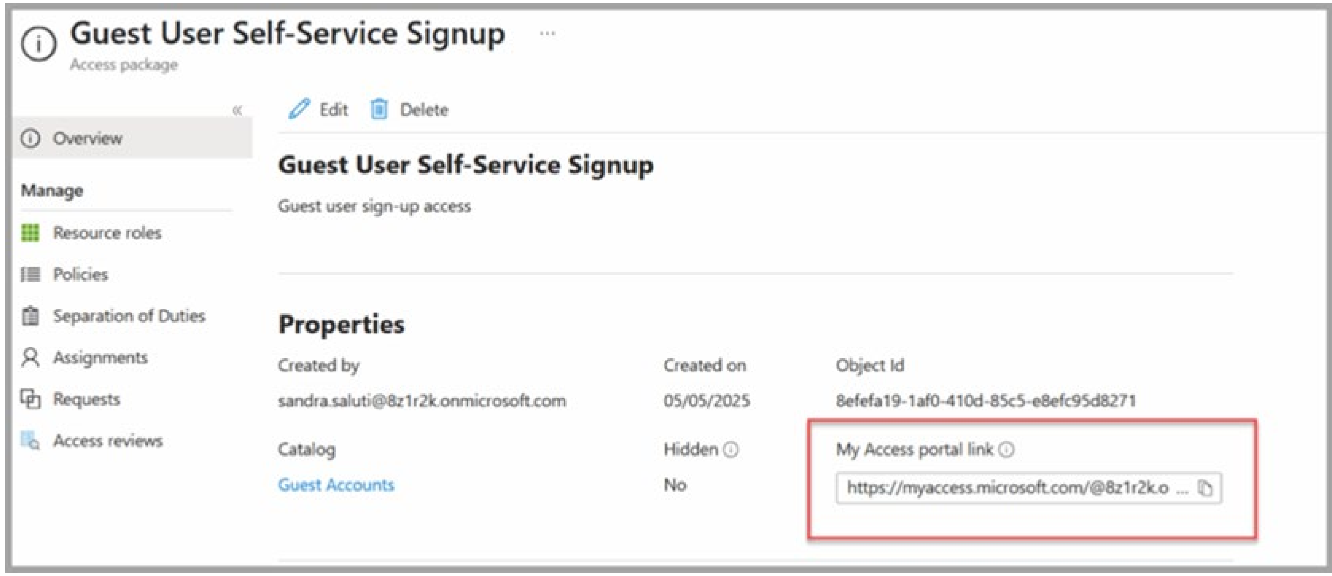


Scenario 3: Govern Guest and Partner Access

- Goal: Understand deployment of Microsoft Entra ID Governance to govern guest and partner access
- Timelines (approximate)
  - Onboarding and discovery - 2 hours
  - Auto assign resources - 1 hour
  - Custom workflows - 2 hours
  - Convert external users - 1 hour
  - Access review - 1 hour
- B2B collaboration and guest users
- Provision guest users in Microsoft Entra ID
- Entitlement management or self-service signup
- Onboarding and discovery
  - External user insights (stale accounts)
  - External user attribute management
- Entitlement management (for external users)
  - External user assignments and access packages
- Deploy external user access
  - Add connected organization
  - Learn settings for external users
  - Create an access package
  - Change the Hidden setting
  - Create an access package with Verified ID requirements
  - Assign users
  - Share a link to request an access package
- Deploy access review guide (see Scenario 2)
- Access review history report (see Scenario 2)
- Guest user access reviews
- Guest user risk in Microsoft Teams and Microsoft 365 Groups
- Access reviews (see Scenario 2)
  - Multistage reviews
  - Inactive users
  - User-to-Group Affiliation
- Deploy guest user lifecycle
- Manage the external user lifecycle
  - Governed, ungoverned, and blank states
  - Convert ungoverned to governed
- Custom workflows with Azure Logic Apps (see Scenario 2)
- Assign and remove resources (see Scenario 2)

Managing Guest - Onboarding

1. **Scope:** Set this to **All users (connected organizations + new external users)**.
   Note: While it's best practice to limit access to known (managed) organizations, using this broader setting simplifies the process.
2. **Approval:** Since we're dealing with **external users**, approval is **required**.
   1. **Select Approvers:**
      Choose at least **two approvers**, so there's a backup if the primary approver is unavailable.
3. **Lifecycle**: Expiration might differ based on users, but for this purpose, lets just add a never expire
   1. Access package Assignment expire : Never
   2. User can request specific timeline: No
   3. Access Review: No



Guest User Self-Service Signup

Access package

Guest User Self-Service Signup

Guest user sign-up access

Properties

Created by: sandra.saluti@8z1r2k.onmicrosoft.com

Created on: 05/05/2025

Object Id: 8efefa19-1af0-410d-85c5-e8efc95d8271

Catalog: Guest Accounts

Hidden: No

My Access portal link: https://myaccess.microsoft.com/@8z1r2k.o ...

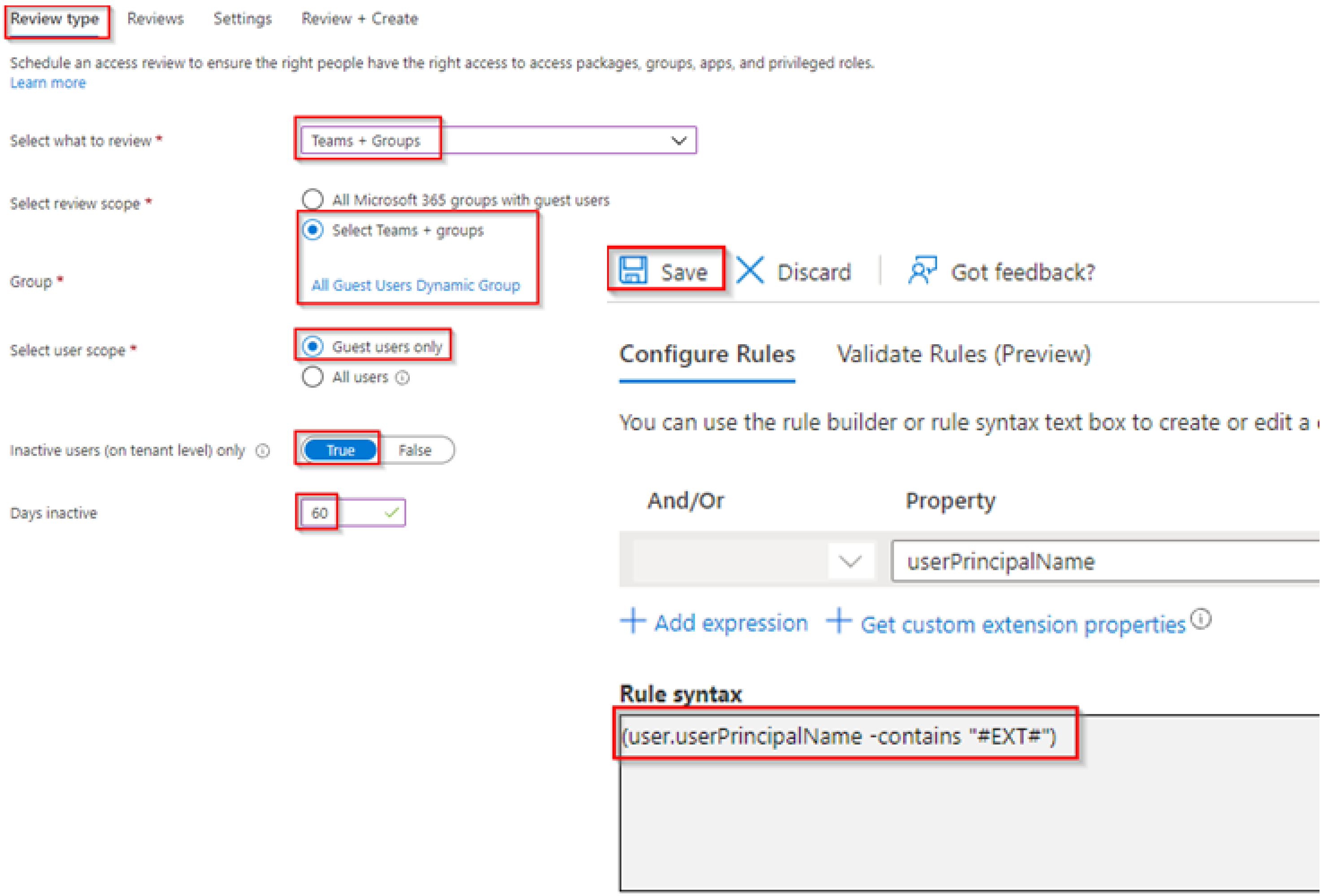
Managing Guest - Options

1. **Let the lifecycle of guest accounts be managed via Identity Governance** – Whereby an access package will manage the provisioning and deprovisioning process of the guest users.
2. **Use Azure Automation and scripting logic to clean-up guest accounts** **–** Whereby a global access review will be used for your guest users and a script will be placed within Azure Automation which will disable and eventually clean-up ‘inactive’ guest users from your tenant.
3. **Use Access Reviews to clean-up Guest Accounts –** Whereby an access review is created for guest users which can and eventually will disable and clean-up ‘inactive’ guest accounts from your tenant.

Best Approach ←

Managing Guests - Reviews

Use Access Reviews to clean-up Guest Accounts – Whereby an access review is created for guest users which can and eventually will disable and clean-up 'inactive' guest accounts from your tenant.



Review type | Reviews | Settings | Review + Create

Schedule an access review to ensure the right people have the right access to access packages, groups, apps, and privileged roles.
Learn more

Select what to review *: Teams + Groups

Select review scope *:
○ All Microsoft 365 groups with guest users
● Select Teams + groups

Group *: All Guest Users Dynamic Group

Select user scope *:
● Guest users only
○ All users

Inactive users (on tenant level) only: [✓ True] False

Days inactive: 60

Save | Discard | Got feedback?

Configure Rules | Validate Rules (Preview)

You can use the rule builder or rule syntax text box to create or edit a

And/Or	Property
	userPrincipalName

+ Add expression + Get custom extension properties

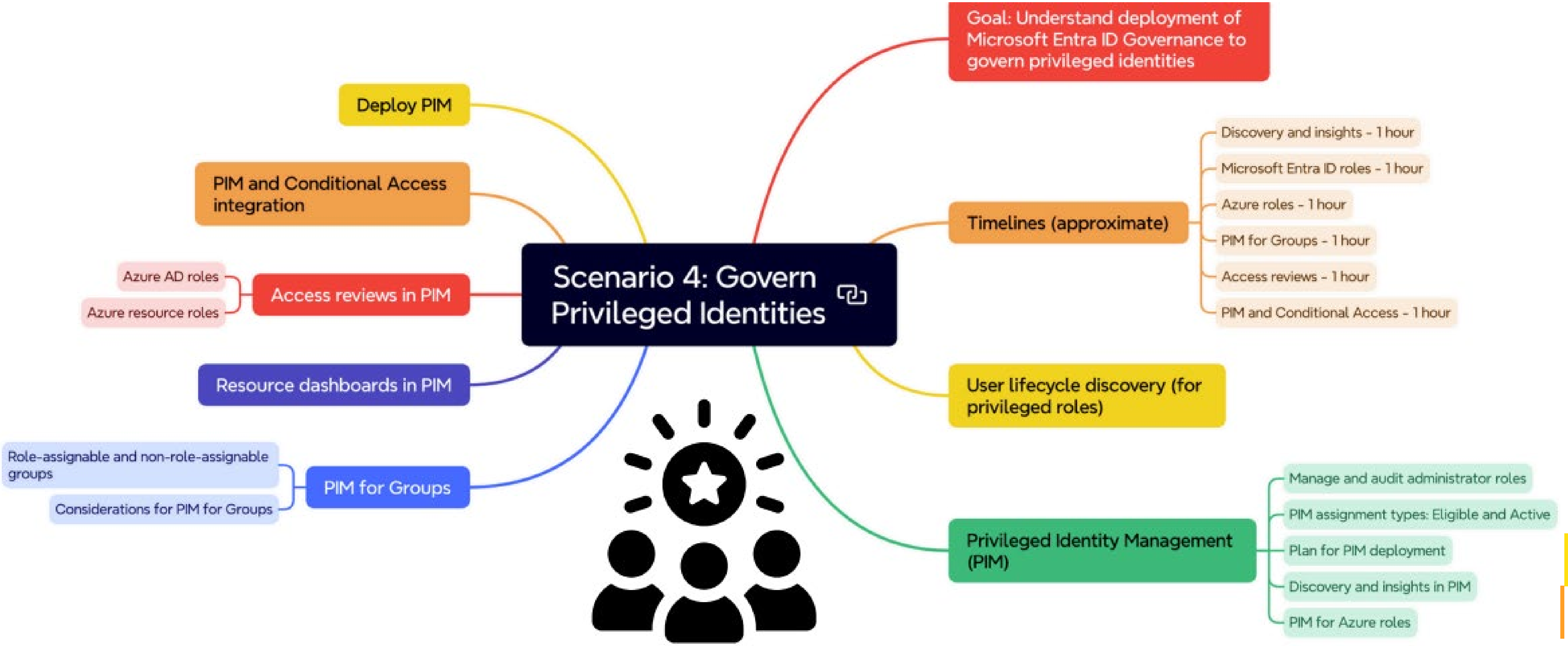
Rule syntax

```
(user.userPrincipalName -contains "#EXT#")
```

Govern Privileged Identities

- Protecting privileged accounts
- Implementing effective access controls
- Monitoring account activities

Govern Privileged Identities



Scenario 4: Govern Privileged Identities

- Goal: Understand deployment of Microsoft Entra ID Governance to govern privileged identities
- Timelines (approximate)
  - Discovery and insights - 1 hour
  - Microsoft Entra ID roles - 1 hour
  - Azure roles - 1 hour
  - PIM for Groups - 1 hour
  - Access reviews - 1 hour
  - PIM and Conditional Access - 1 hour
- User lifecycle discovery (for privileged roles)
- Privileged Identity Management (PIM)
  - Manage and audit administrator roles
  - PIM assignment types: Eligible and Active
  - Plan for PIM deployment
  - Discovery and insights in PIM
  - PIM for Azure roles
- Deploy PIM
- PIM and Conditional Access integration
- Access reviews in PIM
  - Azure AD roles
  - Azure resource roles
- Resource dashboards in PIM
- PIM for Groups
  - Role-assignable and non-role-assignable groups
  - Considerations for PIM for Groups

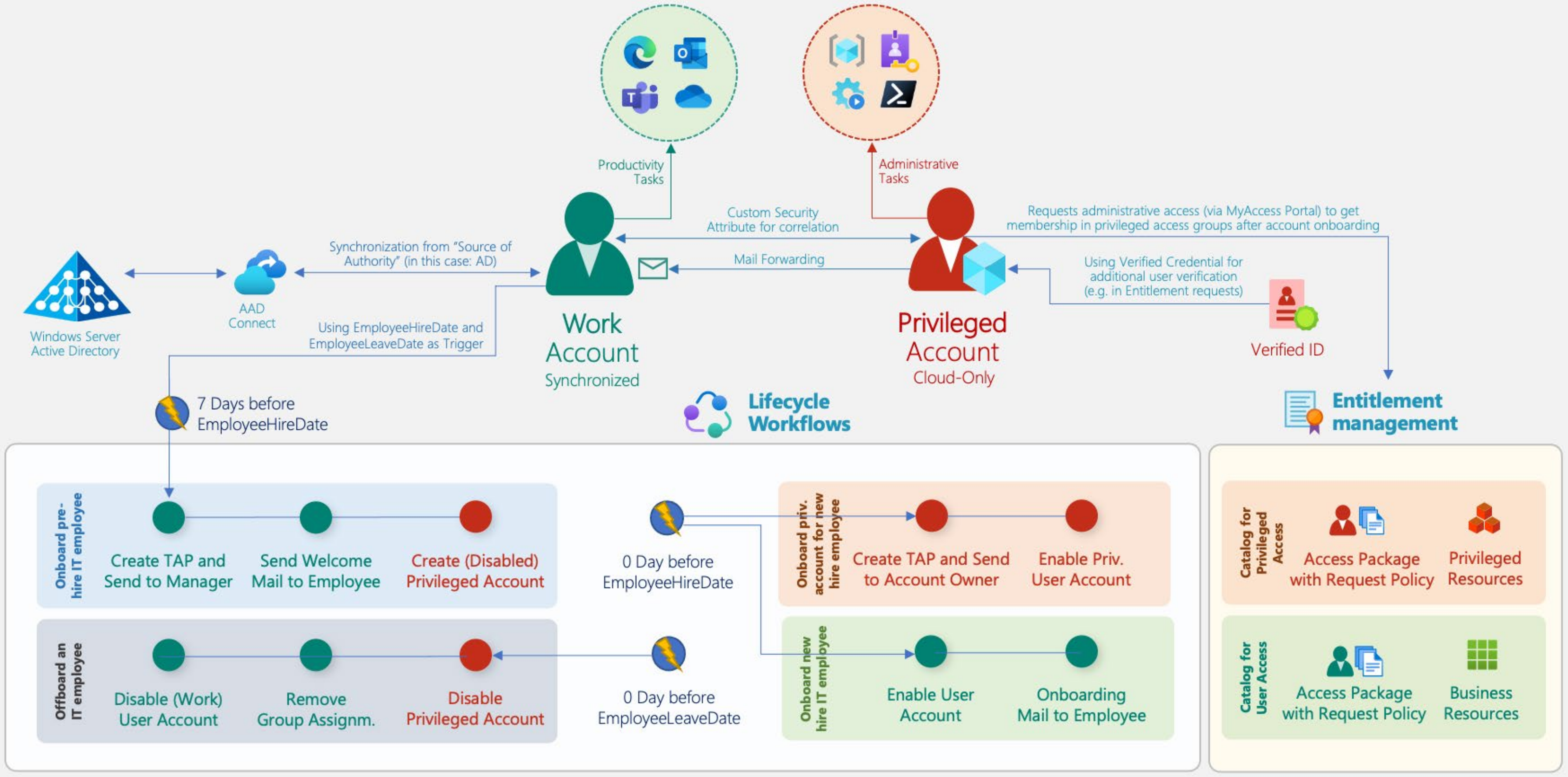
Govern Privileged Identities

Use access reviews to:

- Govern access to critical app, Microsoft Teams, and Office 365 groups
- Reduce access risk of Azure AD B2B guests
- Ensure users in privileged roles require permissions
- Review machine accounts with excessive access
- Manage Conditional Access policy exception lists

In PIM, use access reviews to:

- Automate discovery of stale roles assignments
- Review Azure and Microsoft Entra ID roles
- Remove users from a role after the access review



Productivity Tasks
Administrative Tasks
Windows Server Active Directory
AAD Connect
Synchronization from "Source of Authority" (in this case: AD)
Using EmployeeHireDate and EmployeeLeaveDate as Trigger
Work Account Synchronized
Custom Security Attribute for correlation
Mail Forwarding
Privileged Account Cloud-Only
Requests administrative access (via MyAccess Portal) to get membership in privileged access groups after account onboarding
Using Verified Credential for additional user verification (e.g. in Entitlement requests)
Verified ID
7 Days before EmployeeHireDate
Lifecycle Workflows
Entitlement management
Onboard pre-hire IT employee
Create TAP and Send to Manager
Send Welcome Mail to Employee
Create (Disabled) Privileged Account
0 Day before EmployeeHireDate
Onboard priv. account for new hire employee
Create TAP and Send to Account Owner
Enable Priv. User Account
Catalog for Privileged Access
Access Package with Request Policy
Privileged Resources
Offboard an IT employee
Disable (Work) User Account
Remove Group Assignm.
Disable Privileged Account
0 Day before EmployeeLeaveDate
Onboard new hire IT employee
Enable User Account
Onboarding Mail to Employee
Catalog for User Access
Access Package with Request Policy
Business Resources

https://www.cloud-architekt.net/assets/images/2022-11-15-manage-privileged-identities-with-azuread-identity-governance/OverviewPrivUserIdentityWorkflow.png

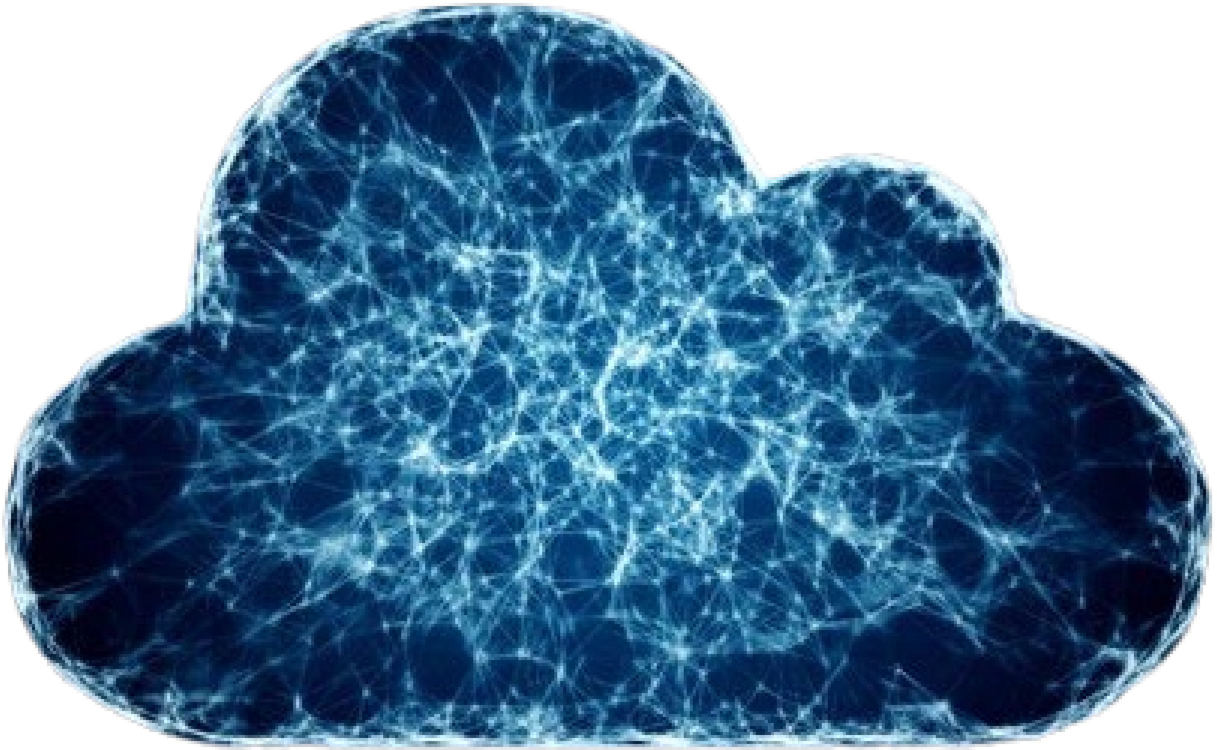
Thomas Naunheim | www.cloud-architekt.net

Making the Shift

Explore the journey of transitioning from traditional platforms like MIM to Entra and some important steps you'll want to take now to be successful.

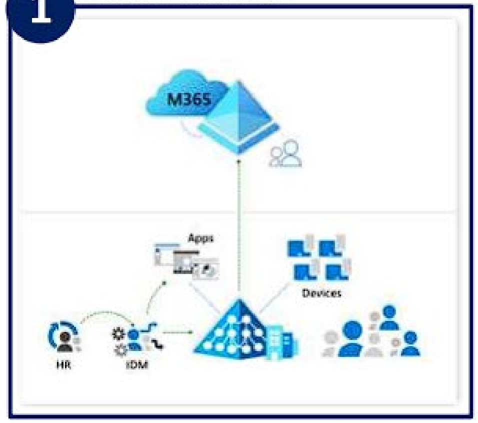
Journey to Cloud First

- Stages of Transformation
- Legacy Workflows
- Why Migrate from MIM
- Moving to a Cloud-First Hybrid Model
- Considerations

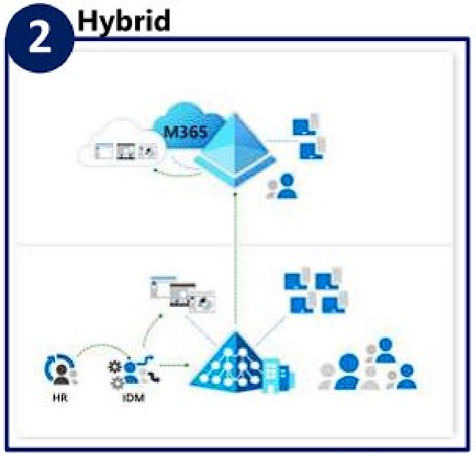


Stages of Transformation

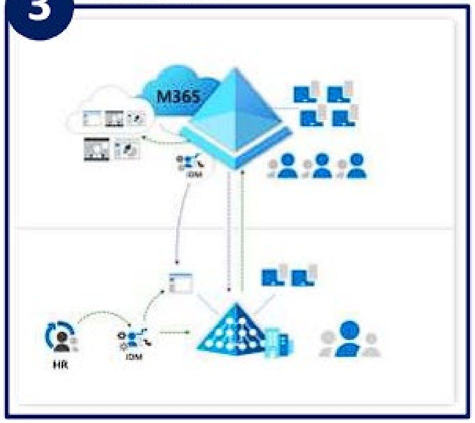
1 Cloud Attached



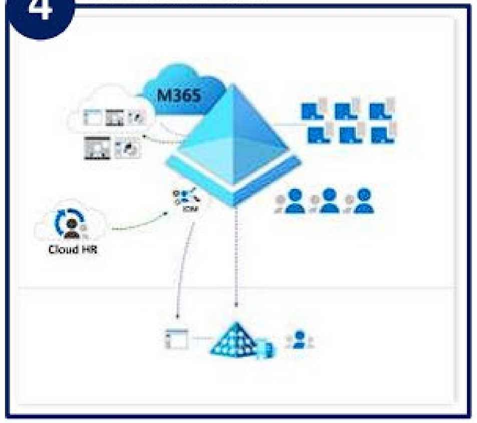
2 Hybrid



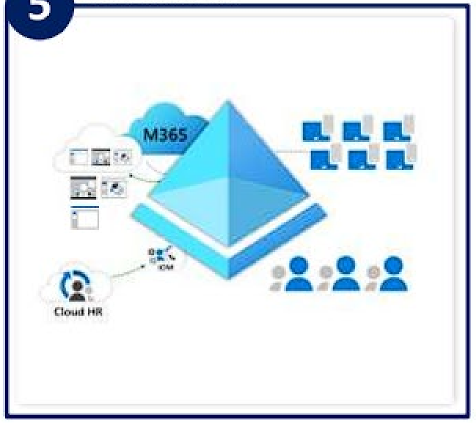
3 Cloud First



4 AD minimized



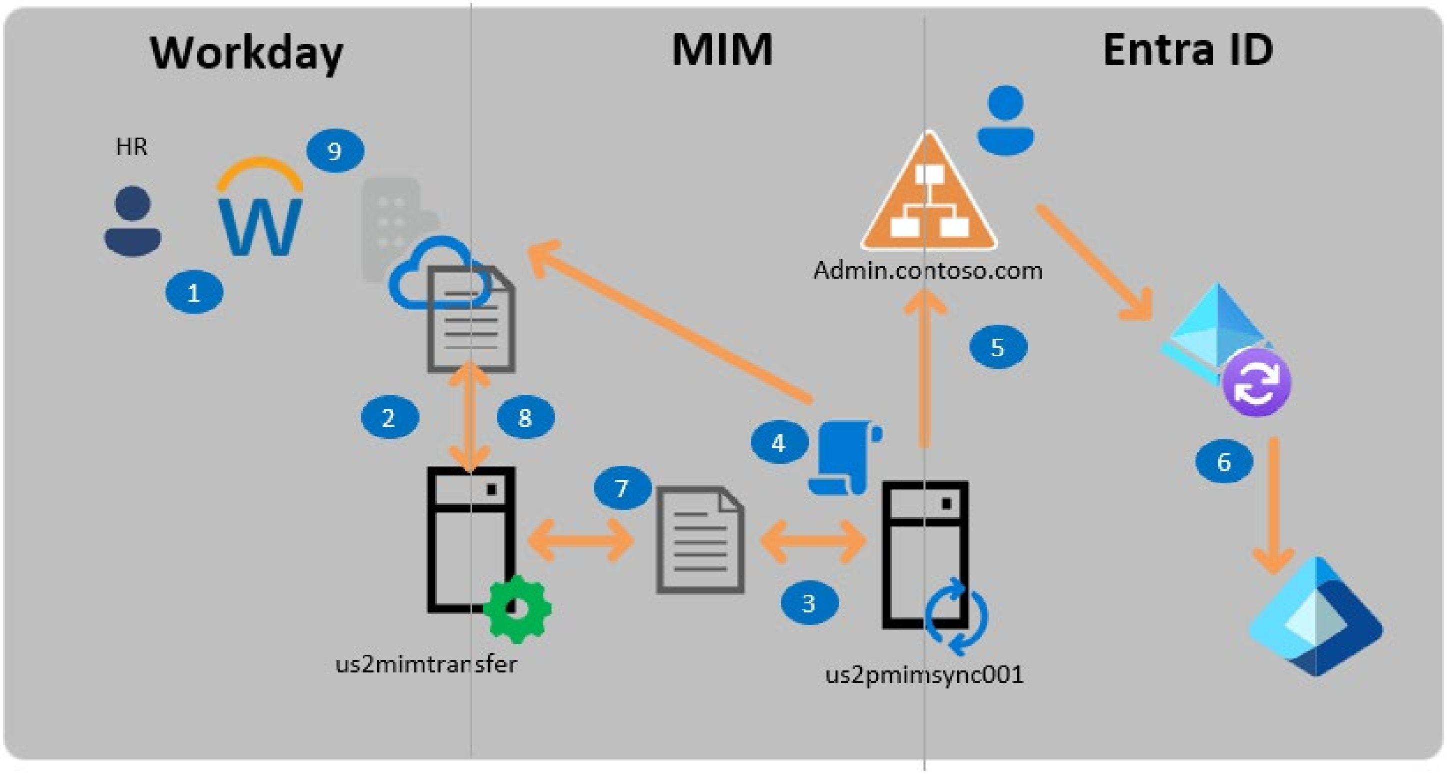
5 100% Cloud



- Cost reduction and consolidation
- Risk reduction and efficiency improvements
- Application modernization challenges
  - Applications with dependencies on password sign-in
  - Applications with local user stores, lost accounts, or Shadow IT
  - Manual processes for on/off boarding and access control
  - Non-standard access rights assignments
  - Isolation of applications that can’t or won’t be modernized

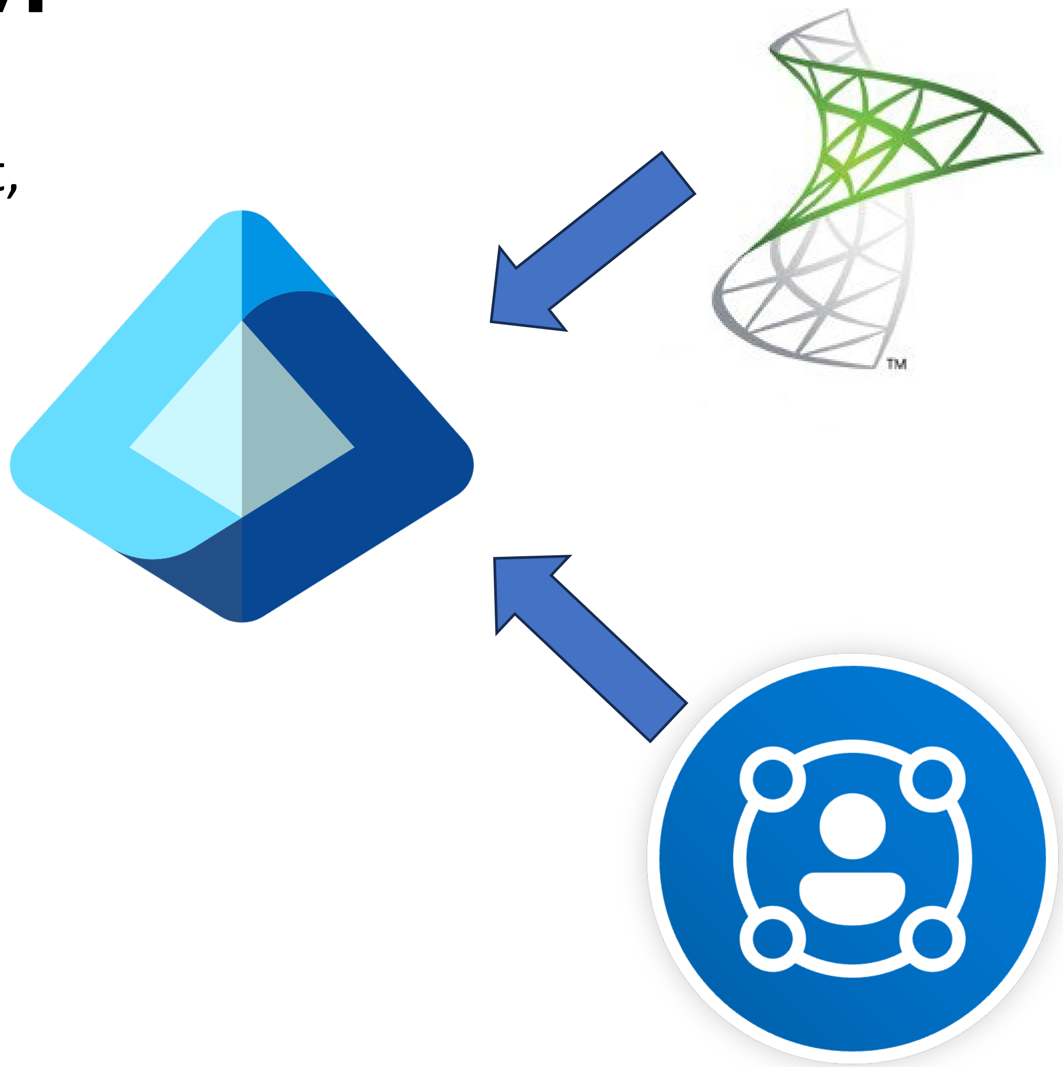
Legacy Workflows

1. The HR team performs worker transactions (Joiners/Movers/Leavers or New Hires/Transfers/Terminations) in Workday HCM
2. Workday sends a CSV file via WINSCP to us2mimtransfer (Azure Container)
3. CSV File is dropped into us2pmimsync001.admin.contoso.com --- C:\MIM\Workday\in\encrypted /ToMIM/MIM_
4. MIM picks this file up, transforms to what MIM needs to send back to Workday (Email address)
5. MIM creates AD Account and Exchange attributes
6. Entra ID Connect Service syncs the AD object to Microsoft Cloud
7. CSV File is updated into us2pmimsync001.admin.contoso.com --- C:\MIM\Workday\out\enc\W_* /ToWorkday
8. WINSCP picks up the file from MIM
9. Workday receives the email address and updates workday configurations with the email address.



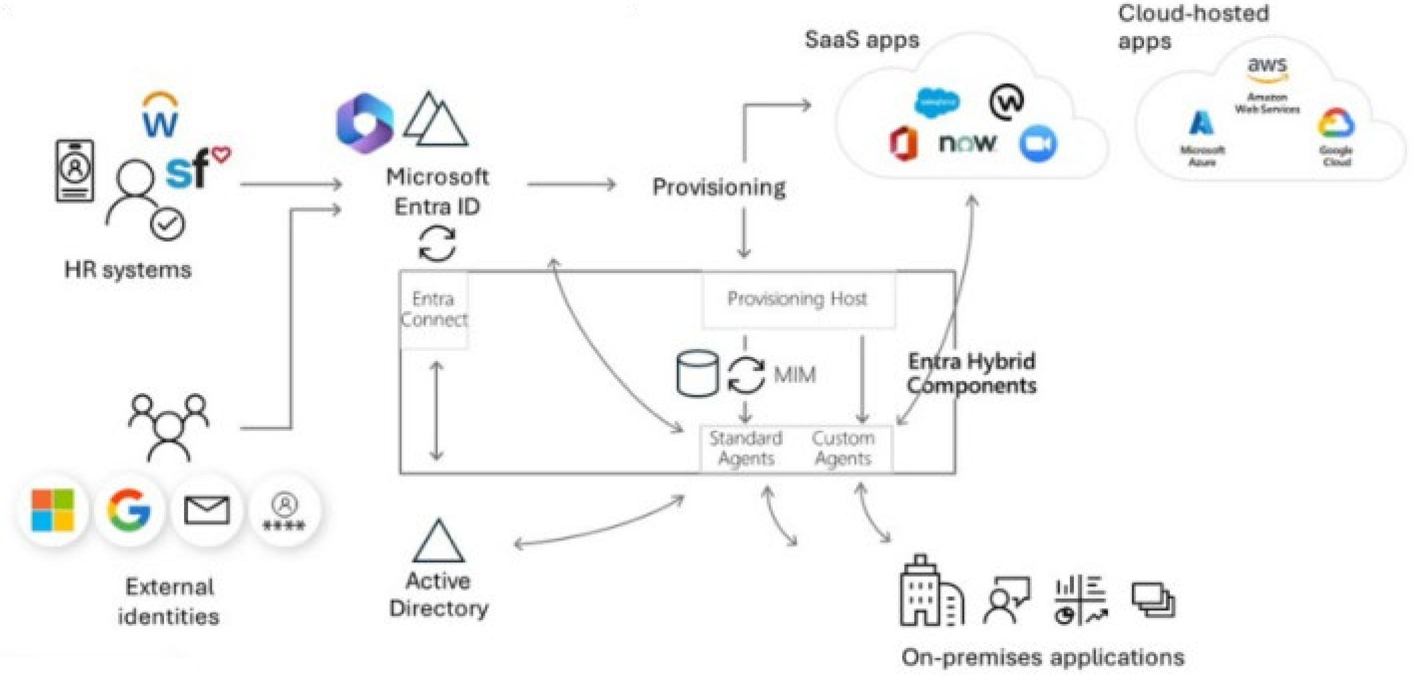
Why Migrate From MIM

- **Complete Configuration & High Maintenance:** Requires significant customization for deployment, time intensive configuration, resource to support are hard to come by
- **Scalability & Flexibility Limitations:** Large scale deployments are hard to support, not very adaptable to change
- **Limited Cloud Integration:** Build to support on-prem environments and lacks native cloud compatibility
- **Limited Governance & Reporting Features:** Using existing cloud first tooling in Entra is very limited
- **Cumbersome User Experience:** User interface is outdated & less intuitive for users
- **End of Life Concerns:** Microsoft is putting their efforts into the Cloud



Moving to a Cloud-First Hybrid Model

- MIM receives provisioning instructions and attribute changes from Microsoft Entra ID – replacing the upstream HR agents that were previously in MIM (hence “cloud-first”).
- The provisioning instructions are simply carried out by the provisioning host’s own agents
- In complex scenarios the HR → Microsoft Entra ID flows may need to be customized, providing pre-import consolidation
- This architecture allows the progressive migration of MIM to Microsoft Entra ID, without the cost, risk, and pressure of a big-bang project
- The business logic will be consolidated in Microsoft Entra ID – decisions on provisioning, licensing, approvals, and governance are made by Microsoft Entra ID.



Considerations - Objects

Going to cloud-only is a big shift and you'll have to move ALL aspects of your identity there…..

1. Group management
   - Distribution Groups
   - Security
2. ACLs
   - File Shares
   - SharePoint
   - 3rd party systems
3. User management & provisioning
   - Shared / Resource mailboxes
   - Service accounts

Considerations - Objects

Going to cloud-only is a big shift and you'll have to move ALL aspects of your identity there…..

1. Group management
   - Distribution lists should be the first to go, along with shared / resource mailboxes
   - Security groups tie back to ACLs
2. ACLs
   - This is generally the most painful without a service catalog or well documented dependency matrix
3. User management & provisioning
   - Shared / Resource mailboxes should be there with distribution groups
   - Service accounts tie back to ACLs

Considerations - Entra ID Cloud Sync

Still need to sync to an on-prem AD? Move to Entra ID Cloud Sync!!

- **Simplified Setup and Management:** Cloud Sync uses a lightweight provisioning agent and manages all sync configurations in the cloud, making it easier to install, configure, and manage than Entra Connect Sync.
- **Support for Disconnected Forests:** Cloud Sync can connect to multiple, disconnected on-premises Active Directory forests, making it ideal for mergers and acquisitions or organizations with legacy forest structures.
- **High Availability:** Multiple active agents can be used for Cloud Sync, providing high availability and ensuring that synchronization continues uninterrupted even if one agent fails.
- **Group Writeback:** Cloud Sync supports group writeback, allowing changes to groups in Microsoft Entra ID to be written back to your on-premises Active Directory.
- **Cloud-Managed Configuration:** All sync configurations are managed in the cloud, simplifying management and reducing the need for on-premises administration.
- **Support for Large Groups:** Cloud Sync supports synchronizing large groups with up to 50,000 members.
- **Easy Deployment and Maintenance:** The lightweight agent and cloud-managed configurations lead to a simpler deployment and maintenance experience.

Considerations - Entra ID Cloud Sync

There are still some scenarios where you can’t use Cloud Sync:

- You need to sync device objects
- Groups with more than 50,000 members
- Merging user attributes from multiple domains
- Using Pass-Through Authentication

Full feature matrix: https://learn.microsoft.com/en-us/entra/identity/hybrid/cloud-sync/what-is-cloud-sync#how-is-microsoft-entra-cloud-sync-different-from-microsoft-entra-connect-sync

Improving Identity Efficiency

Learn how to continue the journey of modernizing identity & access management in Entra to streamline other IT processes, reduce administrative overhead, and improve overall operational efficiency.

Key Takeaways

Piloting Success

EIDG Considerations

Piloting Success

Scenario / Phase	Task / Features	Success Criteria
Employee Lifecycle Automation	HR Provisioning	Configure or Demo Workday or API Driven provisioning with Basic mapping
	SaaS Apps provisioning Sample	Optional- Setup provisioning for 1 SaaS app with basic mapping
	Lifecycle Workflows	At least one workflow per J/M/L scenario
Assign Employee Access to resources	Entitlement Management	At least one basic Access Package
	Entitlement Management	Create one Auto-assignment Policy
	EM + Custom Extensions	Describe (or Demo) the use case and create an empty logic app
	Access Recertification	Create at least one access review (Weekly , follow up after results)
Govern Guest and partner access to resources	Onboarding and Discovery	Navigate the Guests report and IGA dashboard
	Auto-assignment	Create an Access Package for guests, add an aut-assignment policy
	EM + Custom Extensions	Describe (or Demo) the use case and create an empty logic app
	Convert existing guests to Governed	Take a guest user , and assign it to an Access Package
	Access Recertification	Create at least one access review (Weekly , follow up after results)
Govern Privileged Identities and their access	Discovery and insights	Navigate through PIM portal Discovery
	Microsoft Entra ID Roles	Setup and test PIM for at least one Entra ID Roles
	Azure Roles	Setup and test PIM for at least one Azure role
	PIM for Groups	Discover Groups to be used with PIM , Configure and test at least one group
	Access Reviews + PIM	Create at least one access review (Weekly , follow up after results)
	PIM + CA	Setup and PIM authentication Context and add one CA policy for PIM , Test result

EIDG - Workflow Considerations

- Scheduling limits: A Lifecycle Workflow runs by default (if it's scheduled) each 3 hours.
  - This can be customized on tenant level between 1-24 hours, which enables organizations to run each workflow each hour (but do remember this applies to all workflows).
- Max Workflows: Per tenant you can have up to 50 workflows today.
- Max Tasks: Per workflow you're able to configure 25 tasks today.
  - If you want more custom scenarios use Logic Apps
- Setting language per user: With the default tasks available we can send emails, the language of these mails is based on the preferredlanguage value set on the user account in Entra. If not set, the preferredLanguage set on the tenant level will be used.
- User Managers: When using email templates, **it's mandatory for the user to already have a mailbox and the manager field of the user to be configured correctly** (remember that the manager needs a mailbox as well).
- Time-based triggers: The scheduled triggers for onboarding and offboarding are based on the EmployeeHireDate and EmployeeLeaveDateTime values on the user account.
- Timing is important: For workflows, when a user joins your organization set the EmployeeHireDate at the beginning of the day, for EmployeeLeaveDateTime set the value to the end of the day.

EIDG - Entitlement Considerations

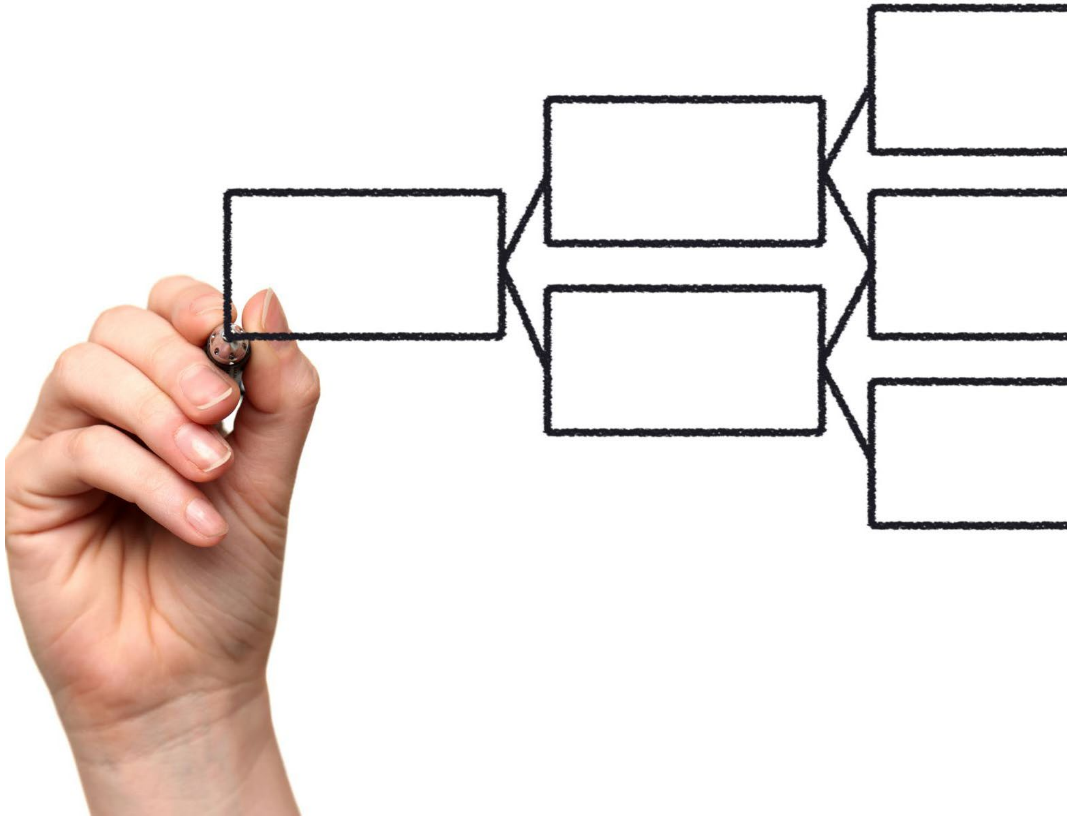
- Synced Groups: Directory-synced groups (like AD groups) cannot be directly added to access packages – you'll need Group Writeback
- Request Processing: Access package requests can sometimes take an extended amount of time to process (even hours).
- My Access Portal: If a user is both a requestor and an approver, they won't see their own request on the Approvals page in My Access.
- User Roles and Permissions: To create & manage access packages, you need specific roles / permissions in Entitlement Management.
- Automatic Assignment Policies: Only administrators can create automatic assignment policies for access packages.
- Access Reviews: Ensure that the access package has the necessary approvers configured, as users cannot approve their own requests.
- Resource Types: Access packages primarily manage access to Microsoft Entra resources, including groups, apps, & SharePoint sites.
- External Users: When managing external users, consider implementing a two-step approval process with shorter access periods.
- Catalog Management: All access packages must be created within a catalog.
- Requestor Information: You can configure access packages to include requestor information, such as their business justification.
- Request Policies: You can create multiple policies for an access package to control who can request it and for what duration.
- Monitoring and Reporting: Utilize Azure Monitor workbooks to monitor access package activity and changes to application role assignments.
- Incompatible Roles: Be aware of separation of duties and avoid assigning roles that are incompatible with the resources in the access package.
- Programmatic Creation: Access packages can only be created and managed programmatically using Microsoft Graph.

EIDG - PIM Considerations

- Assignment: Once a group, management group or subscription is managed, it can't be unmanaged. This prevents another resource administrator from removing Privileged Identity Management settings.
- Role assignments per subscription limited: Azure supports up to 4000 role assignments per subscription or remove redundant role assignments
- Role assignments at the role scope limits: Azure supports up to 500 role assignments per management group
- Custom Roles limits: Azure supports up to 5000 custom roles in a directory.
- Azure role assignments: Check that you're currently signed in with a user that is assigned a role that has the Microsoft.Authorization/roleAssignments/write permission such as Role Based Access Control Administrator at the scope you're trying to assign the role.
- Custom roles - Define one management group in AssignableScopes of your custom role, or try to remove and readd roles again.
- Access denied or permission errors: Ensure you're signed in with a role in the write scope, role included in a Microsoft.Storage data action, or a role assignment included an ABAC condition that uses a GUID comparison operators
- Azure features are disabled: Assign the Contributor or another Azure built-in role with write permissions to the selected scope
- Transferring a subscription to a different directory: Recreate role assignments in the new directory
- Classic subscription administrators: This is retired and no longer supported.
- Custom Security attributes: If custom security attributes have been defined, assign the Attribute role at tenant scope or attribute set scope. By default, Global Administrator and other administrator roles do not have permissions.

EIDG - PIM Considerations

- Harden the Microsoft Entra provisioning agent server as a Control Plane (formerly Tier 0) asset by following the guidance provided in Secure Privileged Access and Active Directory administrative tier model.
- Restrict administrative access to the Microsoft Entra provisioning agent server to only domain administrators or other tightly controlled security groups.
- Create a dedicated account for all personnel with privileged access. Administrators shouldn't be browsing the web, checking their email, and doing day-to-day productivity tasks with highly privileged accounts.
- Enable multifactor authentication (MFA) for all users that have privileged access in Microsoft Entra ID or in AD.
- Follow the guidance provided in Securing privileged access.

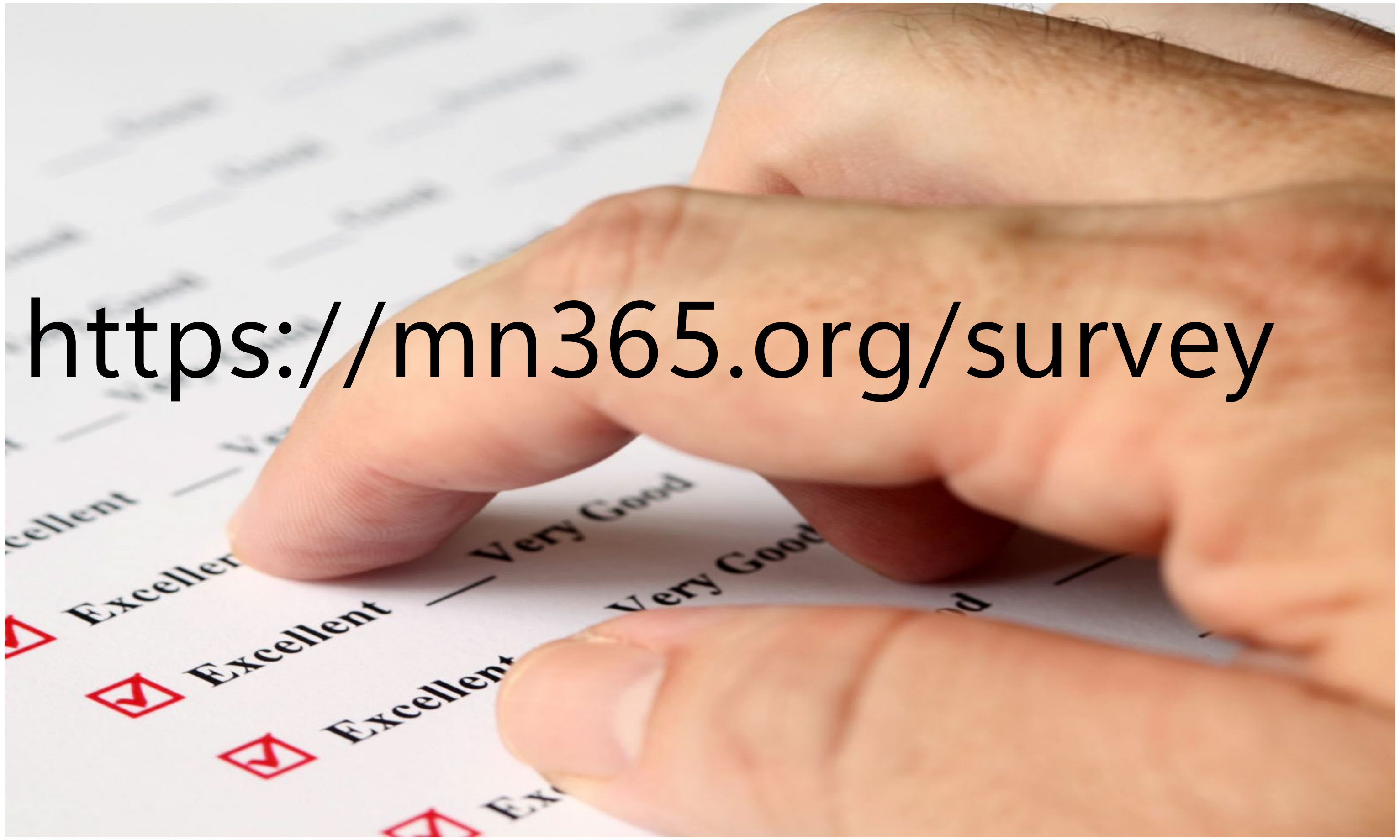


Resources

Community support and documentation

IAM scenario in MIM	Link for more information on IAM scenario in Microsoft Entra
Provisioning from SAP HR sources	bring identities from SAP HR into Microsoft Entra ID
Provisioning from Workday and other cloud HR sources	provisioning from cloud HR systems into Microsoft Entra ID with join/leave lifecycle workflows
Provisioning from other on-premises HR sources	provisioning from on-premises HR systems with join/leave lifecycle workflows
Provisioning to non-AD-based on-premises applications	provisioning users from Microsoft Entra ID to on-premises apps
Global address list (GAL) management for distributed organizations	synchronization of users from one Microsoft Entra ID tenant to another
AD security groups	govern on-premises Active Directory based apps (Kerberos) using Microsoft Entra ID Governance
Dynamic groups	rule-based Microsoft Entra ID security group and Microsoft 365 group memberships
Self-service group management	self-service Microsoft Entra ID security group, Microsoft 365 groups and Teams creation and membership management
Self-service password management	self-service password reset with writeback to AD
Strong credential management	passwordless authentication for Microsoft Entra ID
Historical audit and reporting	archive logs for reporting on Microsoft Entra ID and Microsoft Entra ID Governance activities with Azure Monitor
Privileged access management	securing privileged access for hybrid and cloud deployments in Microsoft Entra ID
Business role-based access management	govern access by migrating an organizational role model to Microsoft Entra ID Governance
Attestation	access reviews for group memberships, application assignments, access packages and roles

Workshop Survey



https://mn365.org/survey

Thank You