Securing your joiner and leaver process with the provisioning API & Lifecycle Workflows!

13-02-2024

Pim Jacobs

Pim Jacobs

Principal Consultant @ InSpark & Microsoft Security MVP

- Focus on the full Microsoft Entra portfolio
- One of the organisers of the **Dutch Microsoft Entra Community**, join our meetup page!
- Blog: **identity-man.eu**
- Skiing | Soccer | F1 | Family time

MVP Microsoft® Most Valuable Professional

Agenda

1 | Quick Introduction

2 | Account Lifecycle Management

3 | Lifecycle Workflows

4 | Onboarding Workflows

5 | Offboarding Workflows

6 | Takeaways

7 | Lessons Learned

8 | Q & A

Quick Introduction

01 | **Identity Lifecycle Management**
Inbound Provisioning with Joiner Mover Leaver process

02 | **Outbound provisioning to 3rd party apps**
Access and provisioning to 3rd party applications

03 | **Access Lifecycle Management**
Access Packages and Reviews

04 | **Entra Privileged Identity Management**
Just in time just enough access

05 | **Terms of Use**
For employees and guests

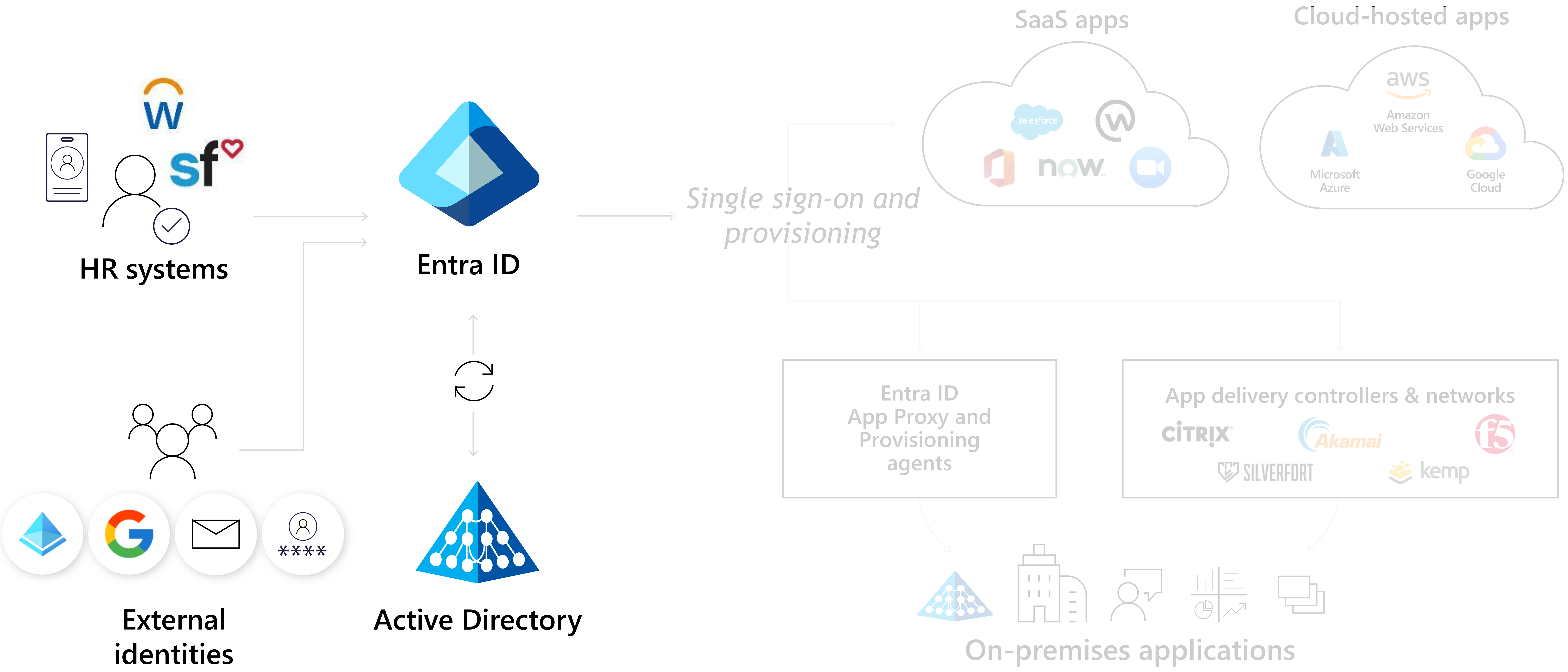
06 | **Reporting**
Improve and fine tuning the current setup

Quick Introduction

01

Identity Lifecycle Management
Inbound Provisioning with Joiner Mover Leaver process

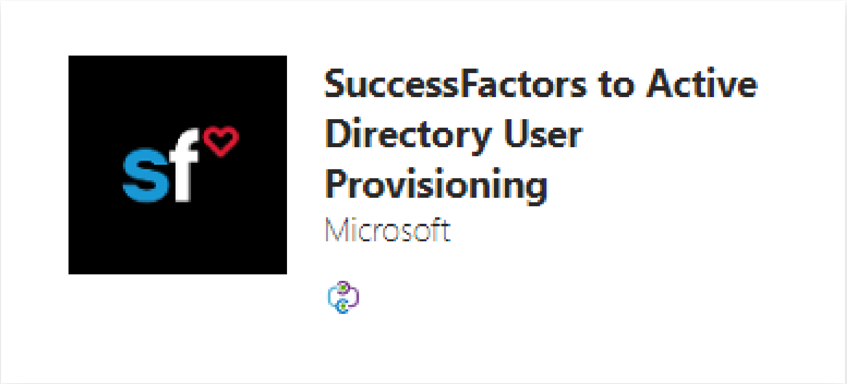
Account Lifecycle Management



Account Lifecycle Management

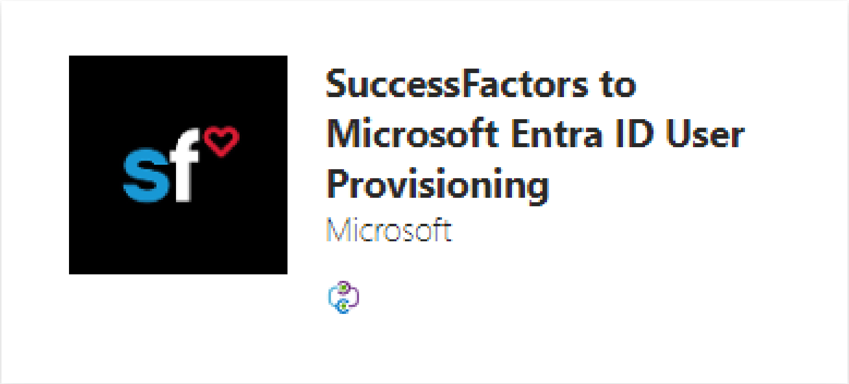
Lifecycle management explained

- Previously only supported with SAP SuccessFactors & Workday.
- Where possible HR data becomes the source of truth!
- HR is responsible for the data and the key for success.
- Accounts are therefore provisioned and expired/disabled on time in AD / Entra ID.
- Lifecycle management is important for all accounts, also admins (LCW) and guests (AR & B2B Sync)!
- **But since august last year extended to ANY HR Source!**



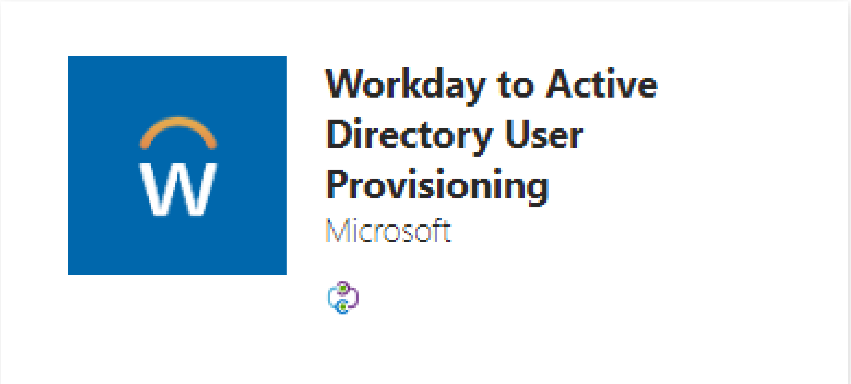
SuccessFactors to Active Directory User Provisioning

Microsoft



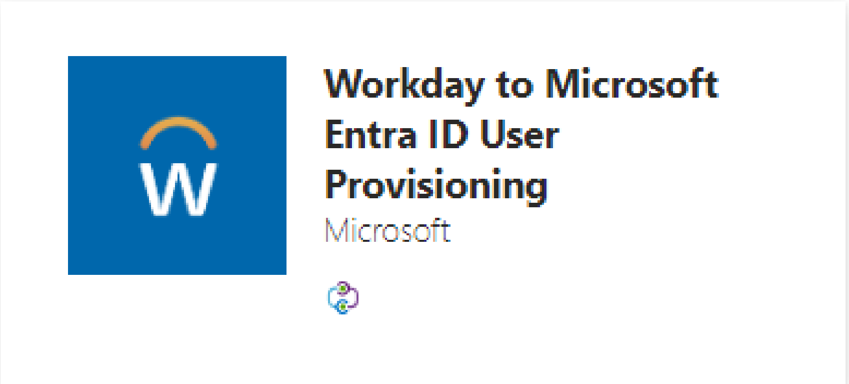
SuccessFactors to Microsoft Entra ID User Provisioning

Microsoft



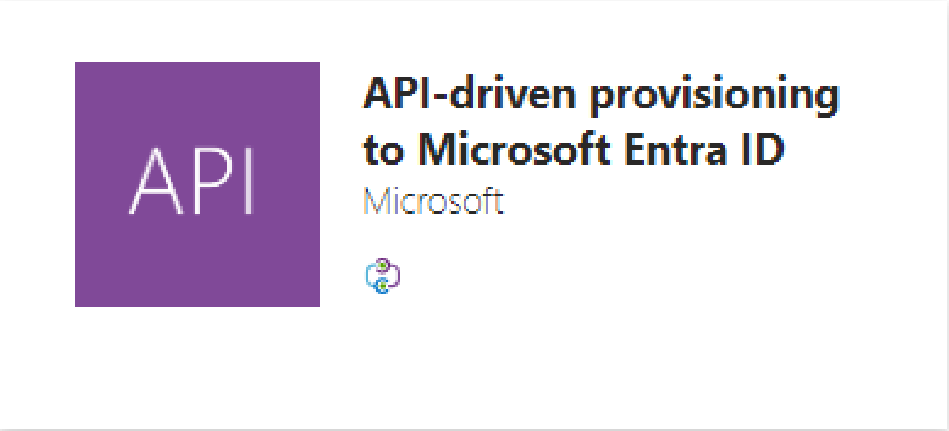
Workday to Active Directory User Provisioning

Microsoft



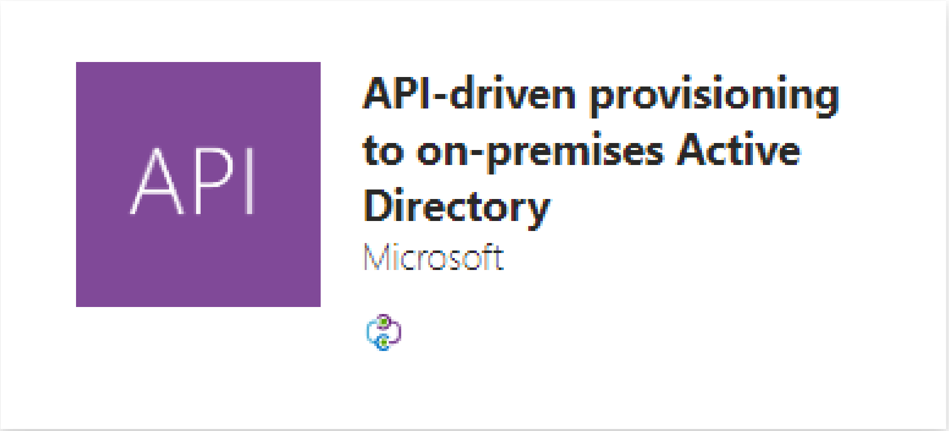
Workday to Microsoft Entra ID User Provisioning

Microsoft



API-driven provisioning to Microsoft Entra ID

Microsoft

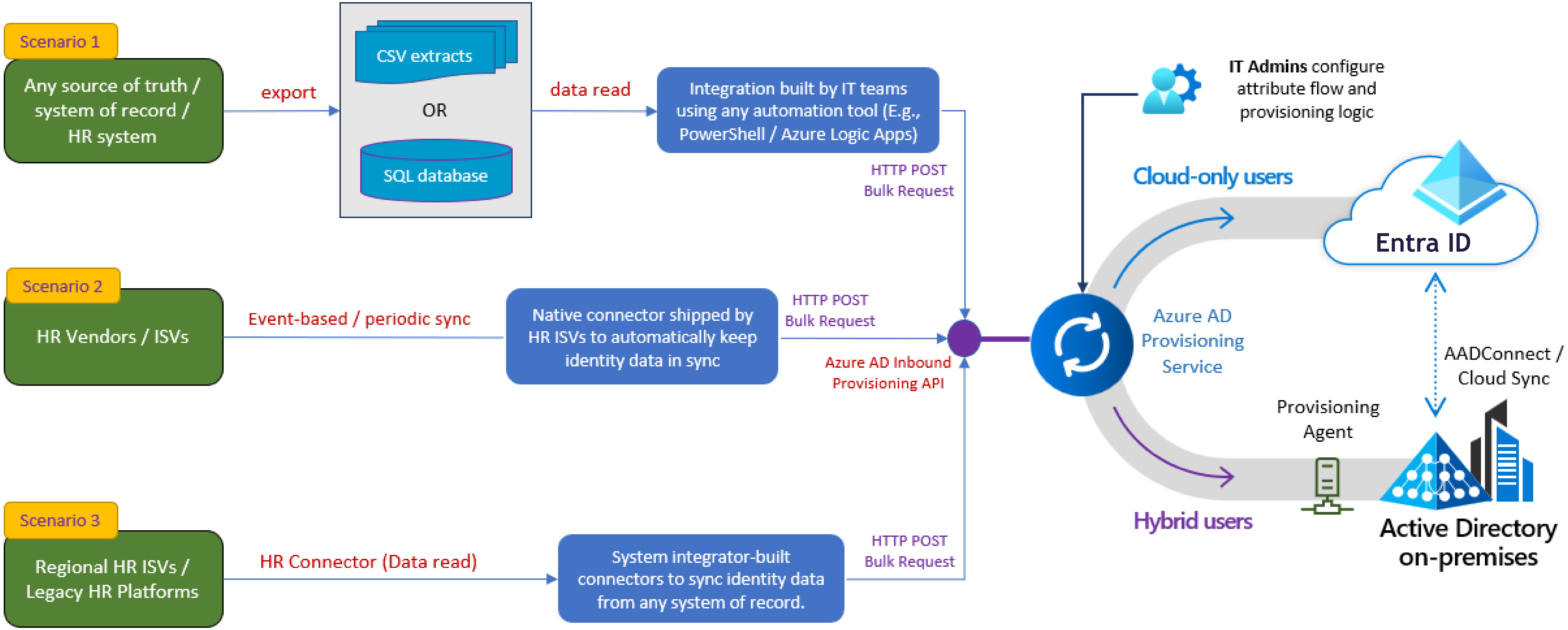


API-driven provisioning to on-premises Active Directory

Microsoft

Manual user creation
Inbound Provisioning API

Inbound Provisioning API



Scenario 1

Any source of truth / system of record / HR system

export

CSV extracts

OR

SQL database

data read

Integration built by IT teams using any automation tool (E.g., PowerShell / Azure Logic Apps)

HTTP POST Bulk Request

Scenario 2

HR Vendors / ISVs

Event-based / periodic sync

Native connector shipped by HR ISVs to automatically keep identity data in sync

HTTP POST Bulk Request

Azure AD Inbound Provisioning API

Scenario 3

Regional HR ISVs / Legacy HR Platforms

HR Connector (Data read)

System integrator-built connectors to sync identity data from any system of record.

HTTP POST Bulk Request

IT Admins configure attribute flow and provisioning logic

Cloud-only users

Entra ID

Azure AD Provisioning Service

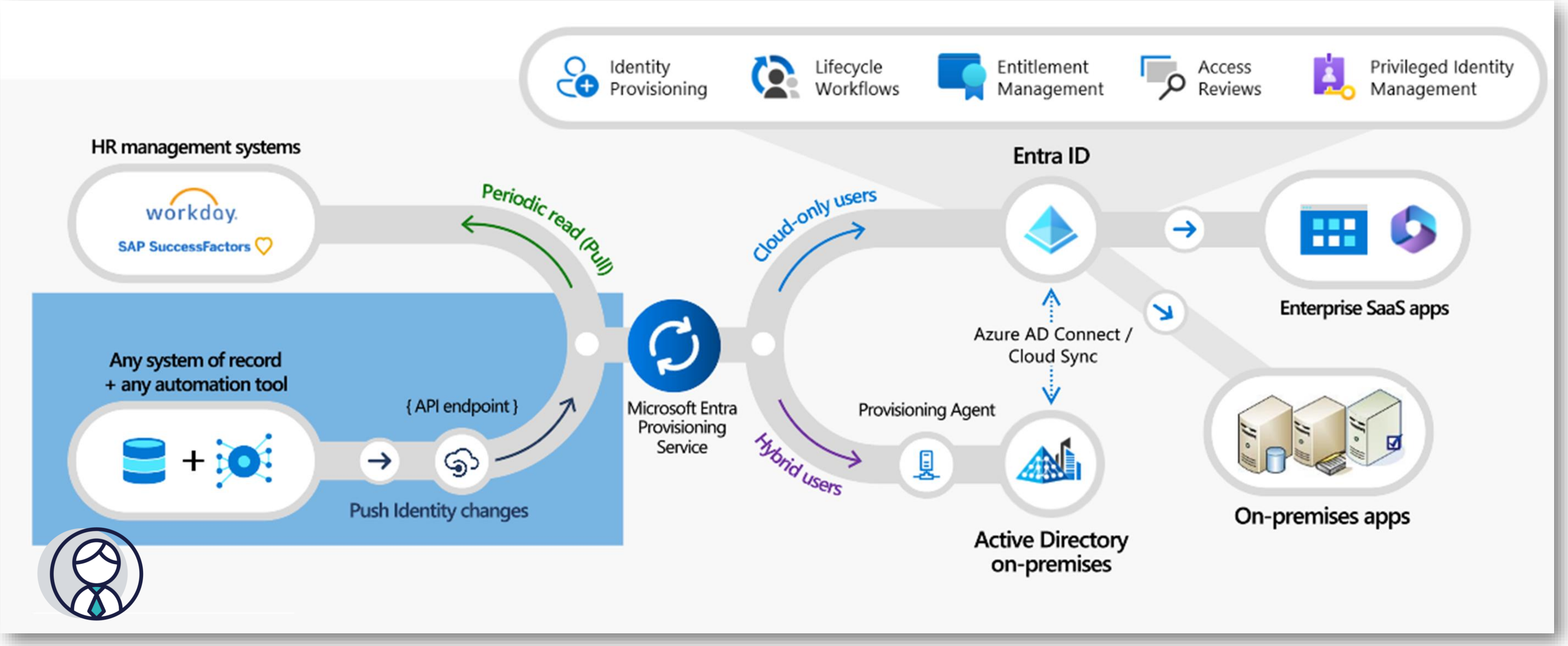
AADConnect / Cloud Sync

Provisioning Agent

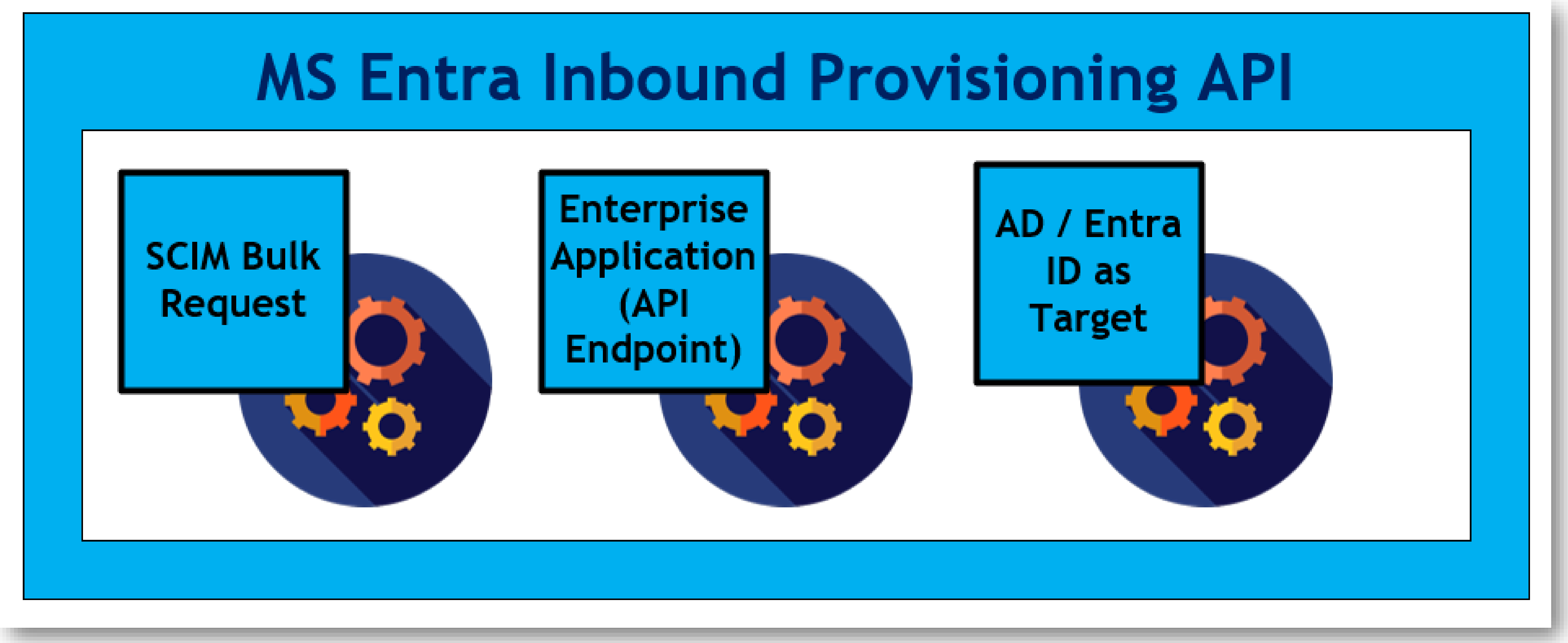
Hybrid users

Active Directory on-premises

Inbound Provisioning API



Understanding the Inbound Provisioning API



MS Entra Inbound Provisioning API

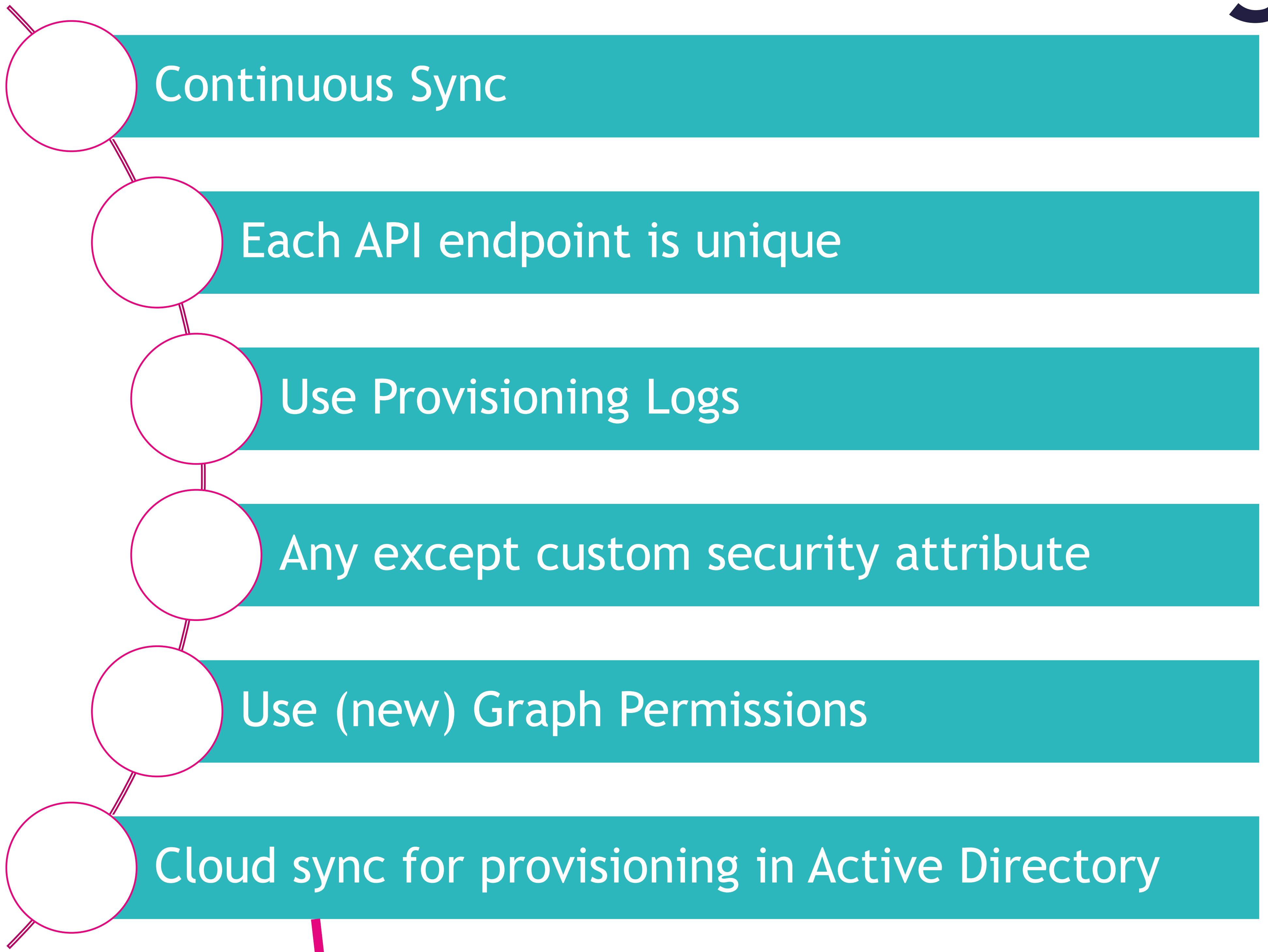
SCIM Bulk Request

Enterprise Application (API Endpoint)

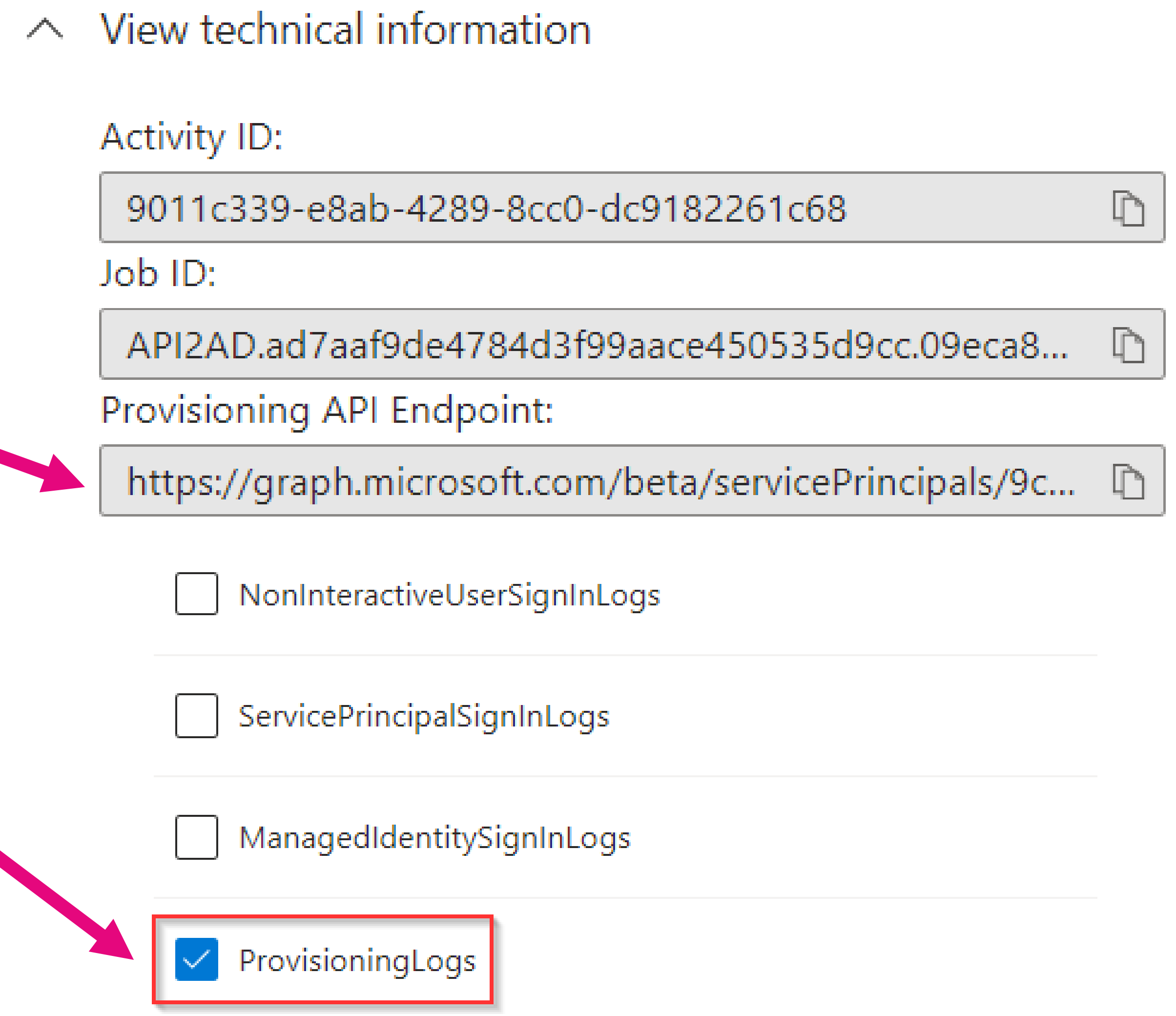
AD / Entra ID as Target

Automate **Lifecycle Management**

Inbound Provisioning API facts



- Continuous Sync
- Each API endpoint is unique
- Use Provisioning Logs
- Any except custom security attribute
- Use (new) Graph Permissions
- Cloud sync for provisioning in Active Directory



View technical information

Activity ID: 9011c339-e8ab-4289-8cc0-dc9182261c68

Job ID: API2AD.ad7aaf9de4784d3f99aace450535d9cc.09eca8...

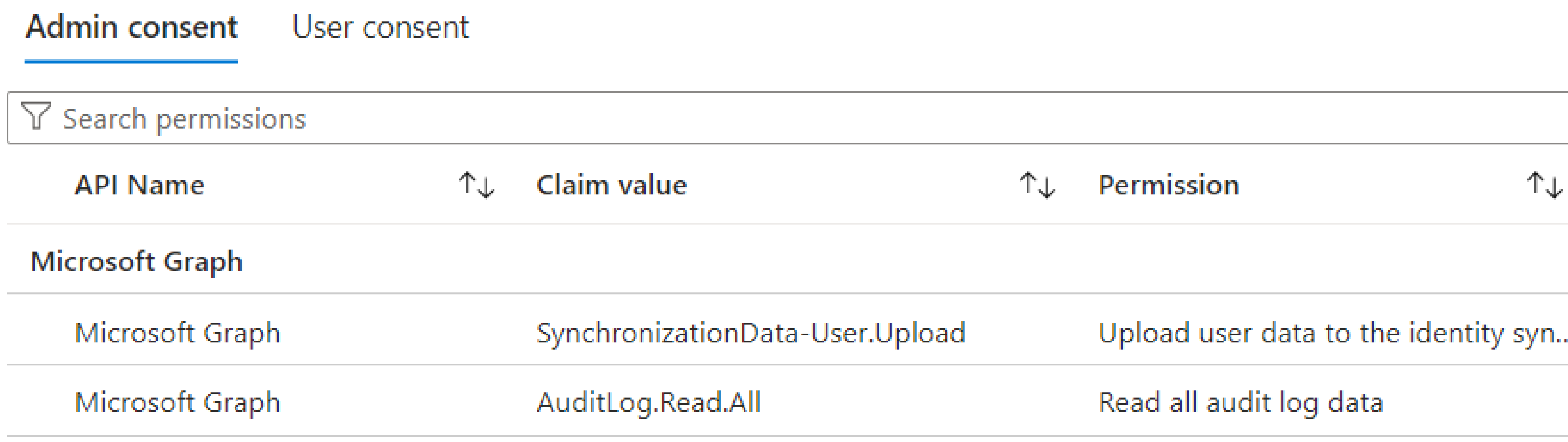
Provisioning API Endpoint: https://graph.microsoft.com/beta/servicePrincipals/9c...

□ NonInteractiveUserSignInLogs

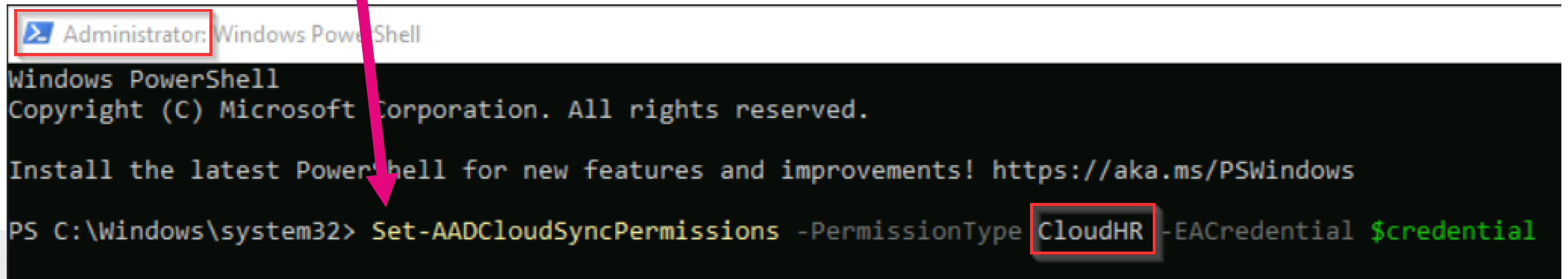
□ ServicePrincipalSignInLogs

□ ManagedIdentitySignInLogs

☑ ProvisioningLogs



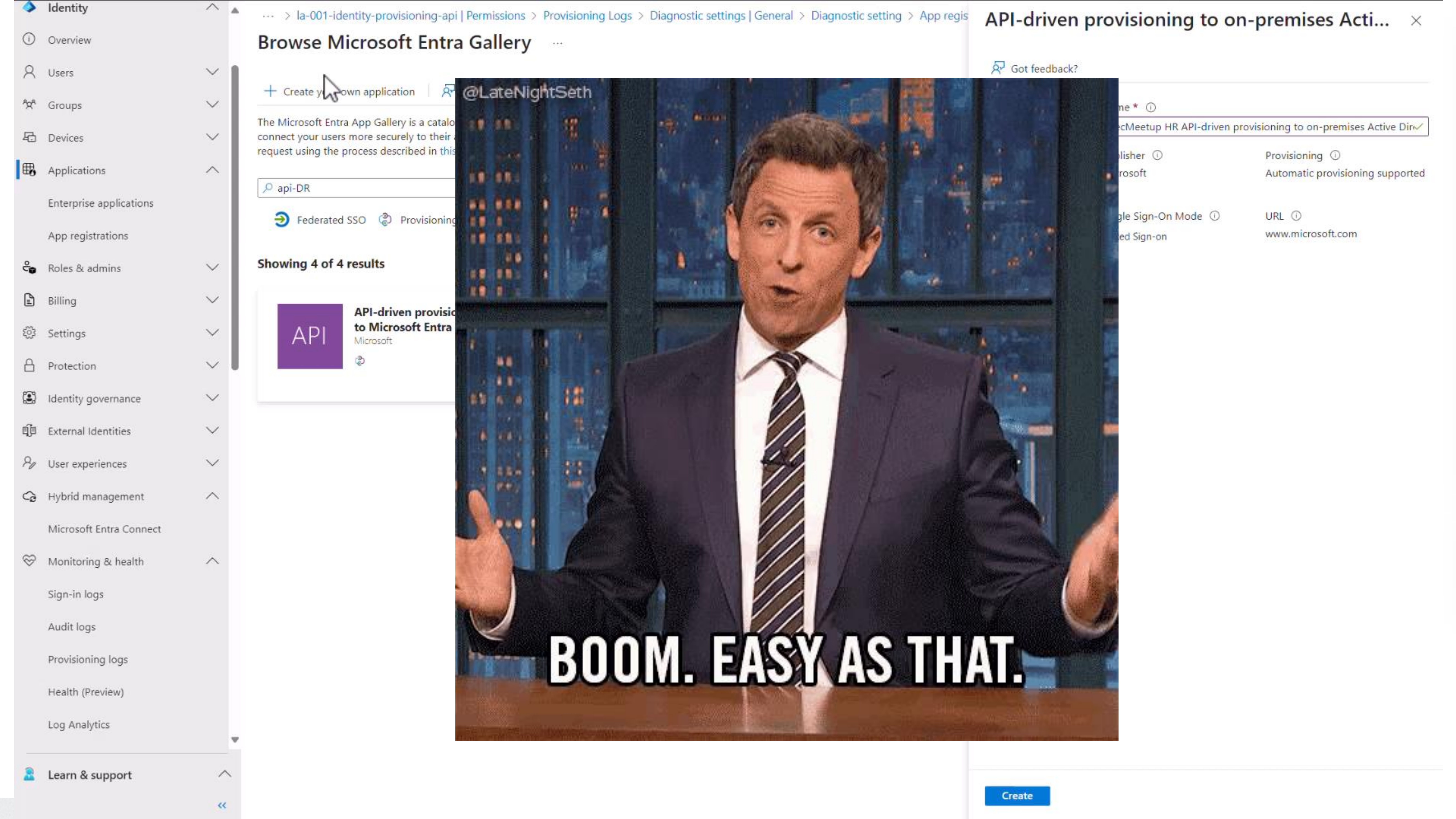
API Name	Claim value	Permission
Microsoft Graph		
Microsoft Graph	SynchronizationData-User.Upload	Upload user data to the identity syn
Microsoft Graph	AuditLog.Read.All	Read all audit log data



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Windows\system32> Set-AADCloudSyncPermissions -PermissionType CloudHR -EACredential $credential
```



Browse Microsoft Entra Gallery …

The Microsoft Entra App Gallery is a catalo
connect your users more securely to their
request using the process described in this

api-DR

Showing 4 of 4 results

API-driven provisio
to Microsoft Entra
Microsoft

API-driven provisioning to on-premises Acti… ✕

me * ⓘ
cMeetup HR API-driven provisioning to on-premises Active Dir ✓

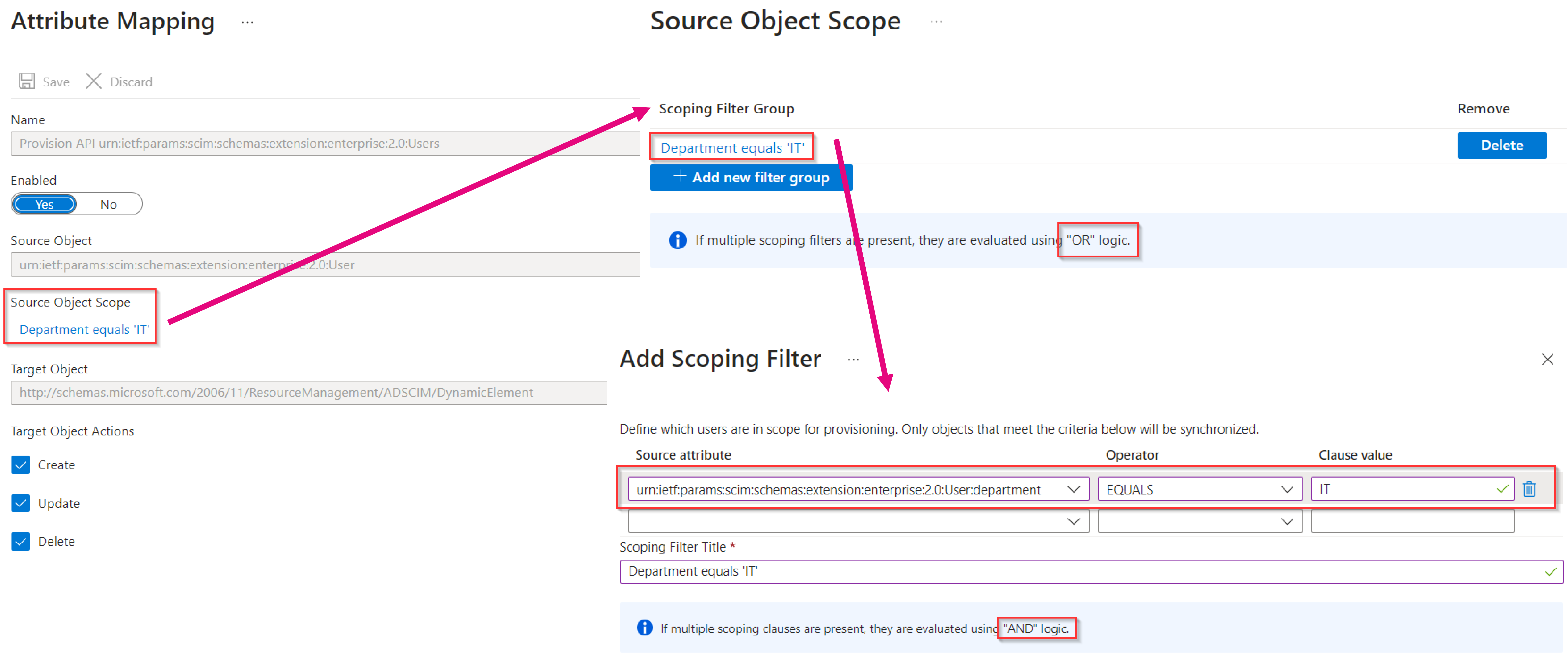
lisher ⓘ
rosoft

Provisioning ⓘ
Automatic provisioning supported

gle Sign-On Mode ⓘ
ed Sign-on

URL ⓘ
www.microsoft.com

Inbound Provisioning API Scoping



Attribute Mapping ···

Save Discard

Name

Provision API urn:ietf:params:scim:schemas:extension:enterprise:2.0:Users

Enabled

[✓ Yes] No

Source Object

urn:ietf:params:scim:schemas:extension:enterprise:2.0:User

Source Object Scope

Department equals 'IT'

Target Object

http://schemas.microsoft.com/2006/11/ResourceManagement/ADSCIM/DynamicElement

Target Object Actions

☑ Create

☑ Update

☑ Delete

Source Object Scope ···

Scoping Filter Group	Remove
Department equals 'IT'	Delete

+ Add new filter group

If multiple scoping filters are present, they are evaluated using "OR" logic.

Add Scoping Filter ···

Define which users are in scope for provisioning. Only objects that meet the criteria below will be synchronized.

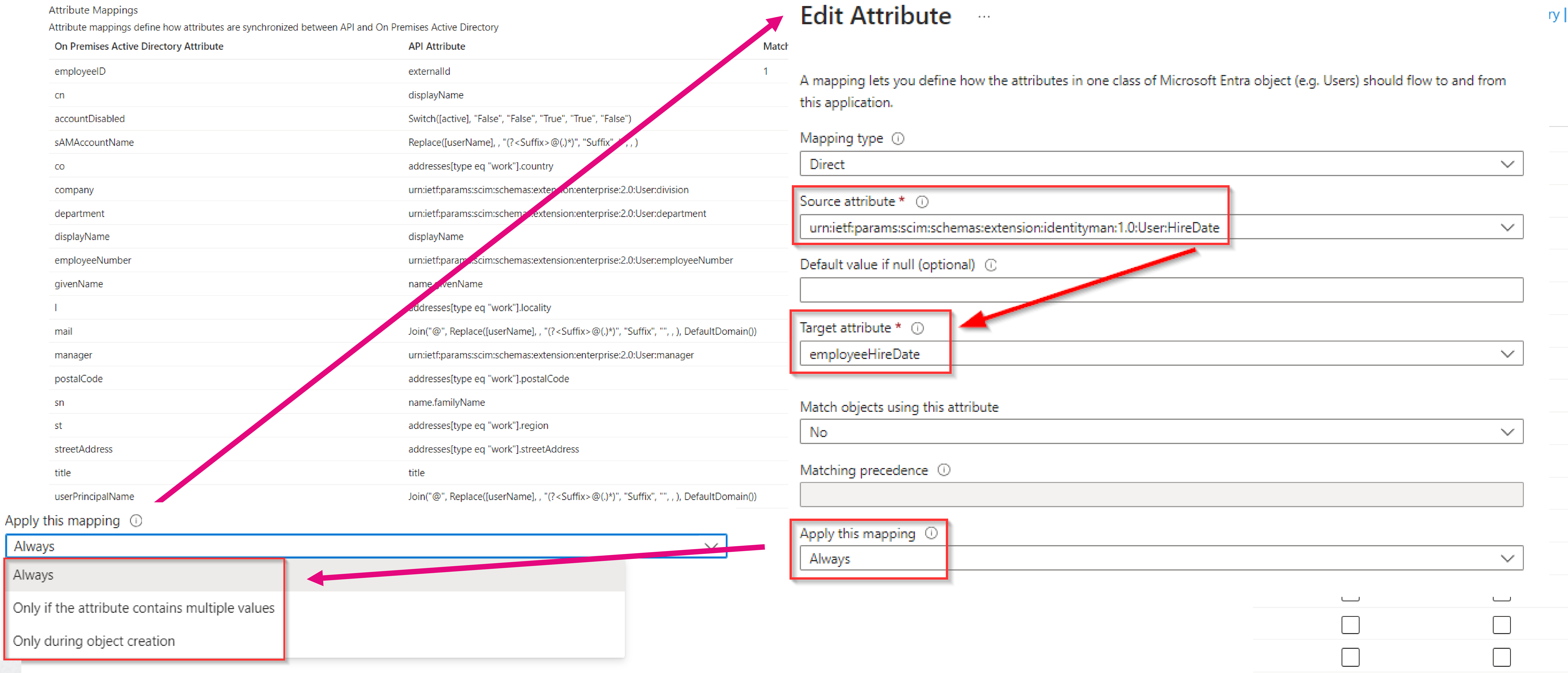
Source attribute	Operator	Clause value
urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:department	EQUALS	IT

Scoping Filter Title *

Department equals 'IT'

If multiple scoping clauses are present, they are evaluated using "AND" logic.

Inbound Provisioning API Schema Extensions



Attribute Mappings

Attribute mappings define how attributes are synchronized between API and On Premises Active Directory

On Premises Active Directory Attribute	API Attribute	Matc
employeeID	externalId	1
cn	displayName	
accountDisabled	Switch([active], "False", "False", "True", "True", "False")	
sAMAccountName	Replace([userName], , "(?<Suffix>@(.)*)", "Suffix", "", ,)	
co	addresses[type eq "work"].country	
company	urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:division	
department	urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:department	
displayName	displayName	
employeeNumber	urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:employeeNumber	
givenName	name.givenName	
l	addresses[type eq "work"].locality	
mail	Join("@", Replace([userName], , "(?<Suffix>@(.)*)", "Suffix", "", ,), DefaultDomain())	
manager	urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:manager	
postalCode	addresses[type eq "work"].postalCode	
sn	name.familyName	
st	addresses[type eq "work"].region	
streetAddress	addresses[type eq "work"].streetAddress	
title	title	
userPrincipalName	Join("@", Replace([userName], , "(?<Suffix>@(.)*)", "Suffix", "", ,), DefaultDomain())	

Apply this mapping: Always

- Always
- Only if the attribute contains multiple values
- Only during object creation

Edit Attribute

A mapping lets you define how the attributes in one class of Microsoft Entra object (e.g. Users) should flow to and from this application.

Mapping type: Direct

Source attribute *: urn:ietf:params:scim:schemas:extension:identityman:1.0:User:HireDate

Default value if null (optional):

Target attribute *: employeeHireDate

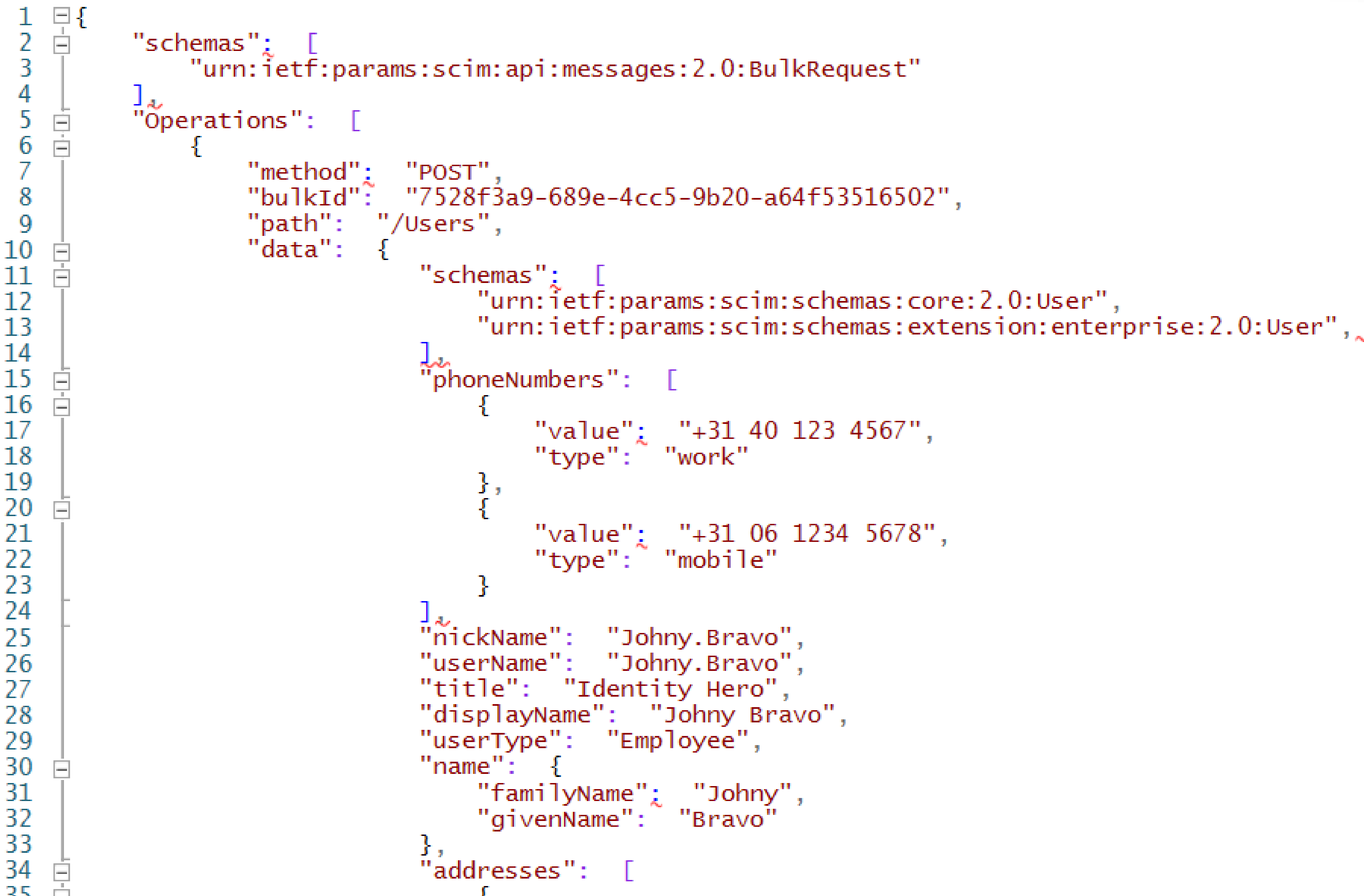
Match objects using this attribute: No

Matching precedence:

Apply this mapping: Always

Bulk Payload Example

- Only for users
- Max 50 users per bulk request
- Can only contain POST as method
- ‘Content-Type: application/scim+json’ is mandatory
- BulkId is generated for reference
- API Endpoint only supports POST
- PowerShell Module available on learn

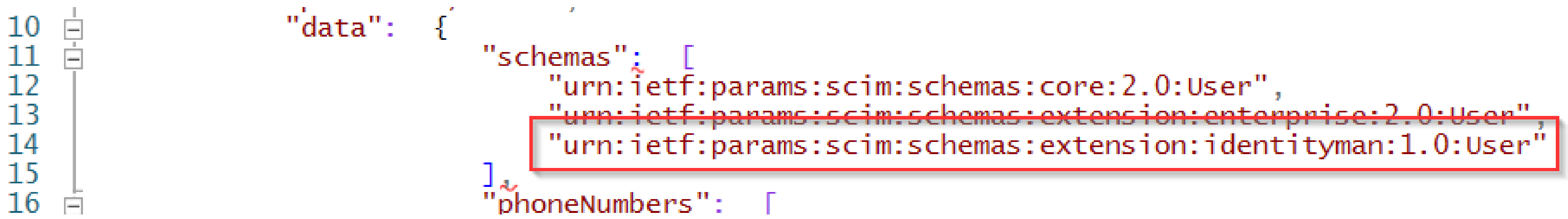


```
{
    "schemas":  [
        "urn:ietf:params:scim:api:messages:2.0:BulkRequest"
    ],
    "Operations":  [
        {
            "method":  "POST",
            "bulkId":  "7528f3a9-689e-4cc5-9b20-a64f53516502",
            "path":  "/Users",
            "data":  {
                "schemas":  [
                    "urn:ietf:params:scim:schemas:core:2.0:User",
                    "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User",
                ],
                "phoneNumbers":  [
                    {
                        "value":  "+31 40 123 4567",
                        "type":  "work"
                    },
                    {
                        "value":  "+31 06 1234 5678",
                        "type":  "mobile"
                    }
                ],
                "nickName":  "Johny.Bravo",
                "userName":  "Johny.Bravo",
                "title":  "Identity Hero",
                "displayName":  "Johny Bravo",
                "userType":  "Employee",
                "name":  {
                    "familyName":  "Johny",
                    "givenName":  "Bravo"
                },
                "addresses":  [
                    {
```

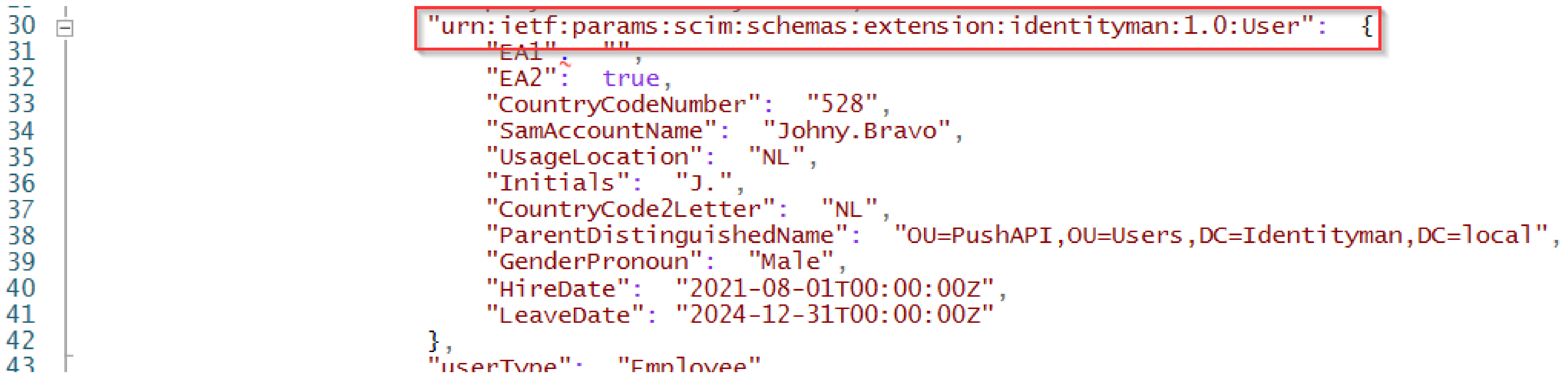
Bulk payload schema extensions

For additional values you want to provision:

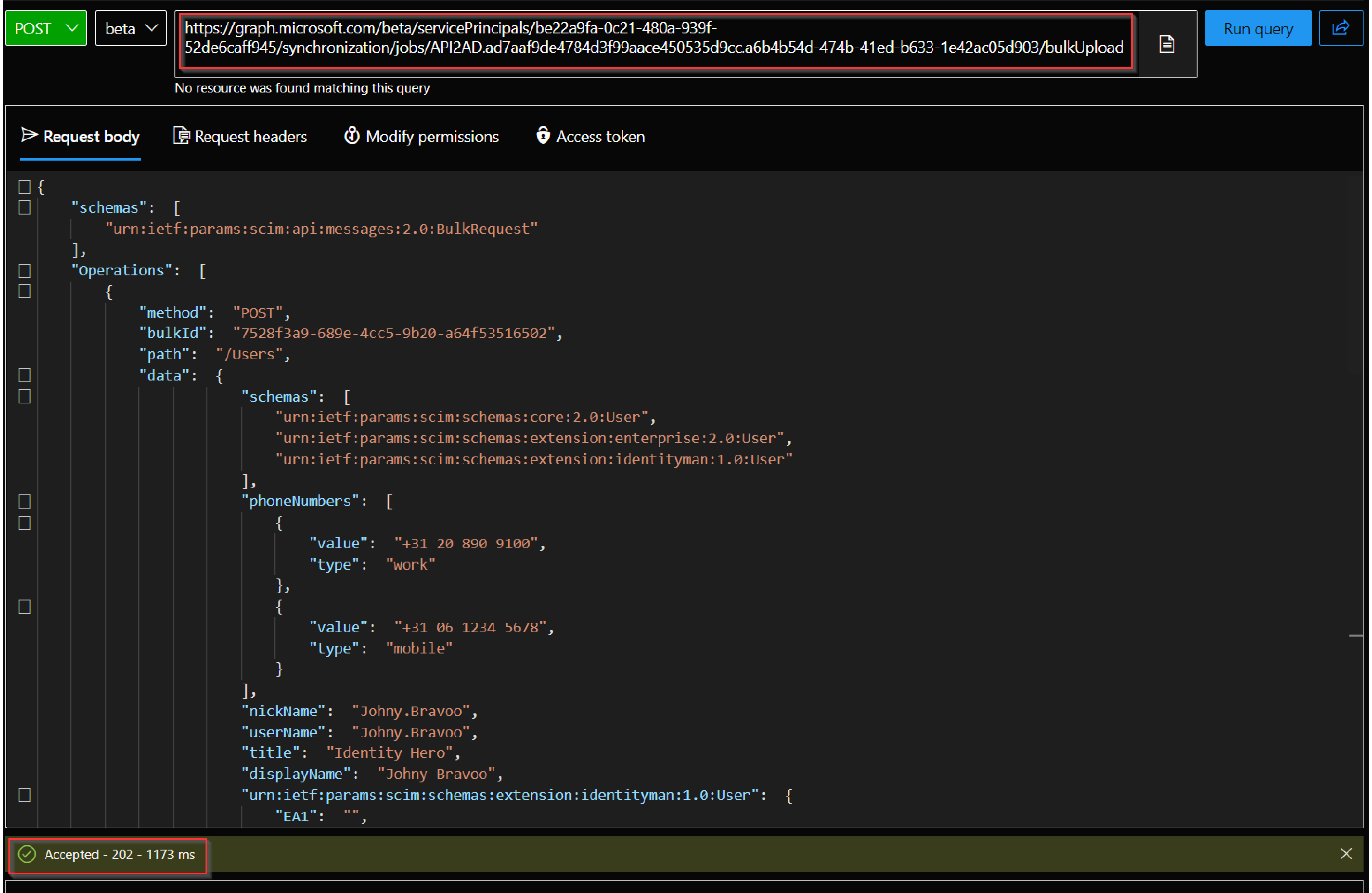
- Make your own schema available in the bulk payload request.
- Add the schema with the attributes you want to provision:
  - ExtensionAttributes
  - UsageLocation
  - Initials
  - OU location
  - **HireDate**
  - **LeaveDate**



```
"data": {
        "schemas": [
            "urn:ietf:params:scim:schemas:core:2.0:User",
            "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User",
            "urn:ietf:params:scim:schemas:extension:identityman:1.0:User"
        ],
        "phoneNumbers": [
```



```
"urn:ietf:params:scim:schemas:extension:identityman:1.0:User": {
    "EA1": "",
    "EA2": true,
    "CountryCodeNumber": "528",
    "SamAccountName": "Johny.Bravo",
    "UsageLocation": "NL",
    "Initials": "J.",
    "CountryCode2Letter": "NL",
    "ParentDistinguishedName": "OU=PushAPI,OU=Users,DC=Identityman,DC=local",
    "GenderPronoun": "Male",
    "HireDate": "2021-08-01T00:00:00Z",
    "LeaveDate": "2024-12-31T00:00:00Z"
},
"userType": "Employee"
```



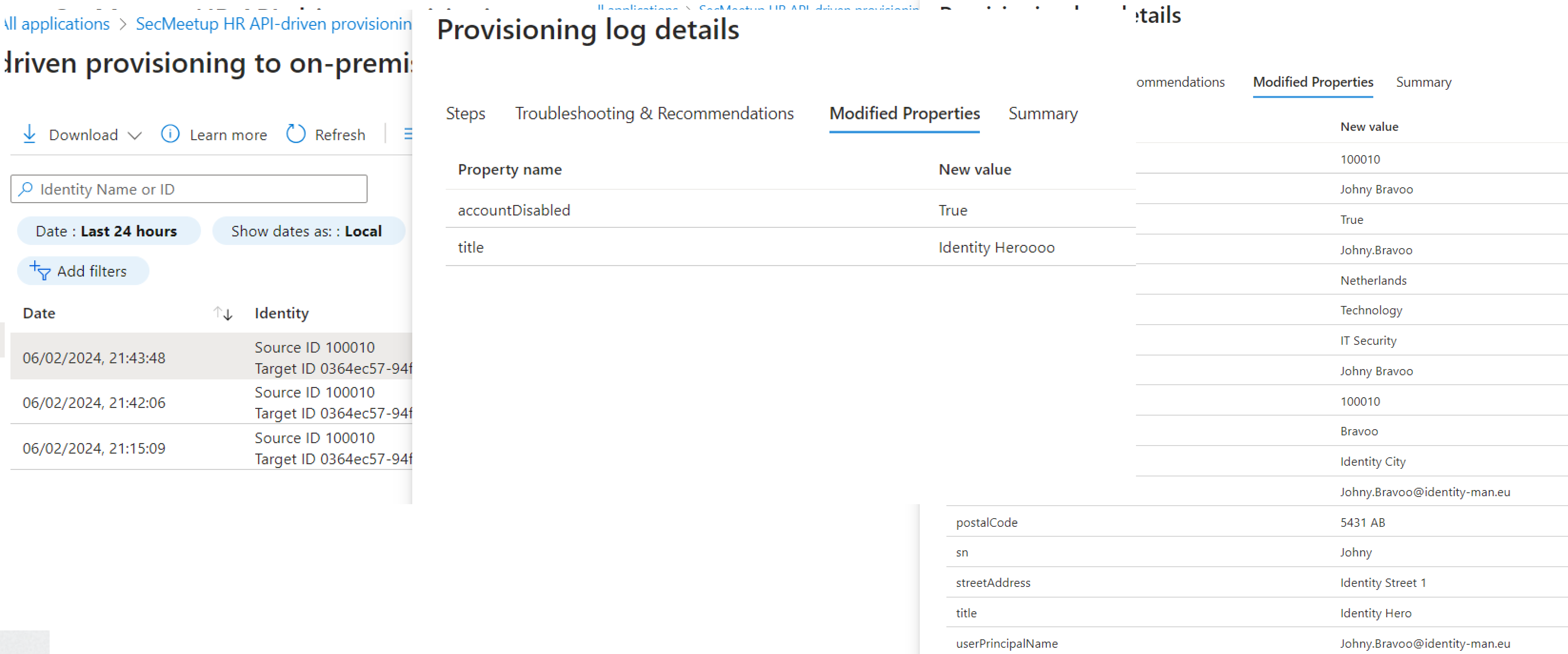
```
https://graph.microsoft.com/beta/servicePrincipals/be22a9fa-0c21-480a-939f-52de6caff945/synchronization/jobs/API2AD.ad7aaf9de4784d3f99aace450535d9cc.a6b4b54d-474b-41ed-b633-1e42ac05d903/bulkUpload
```

No resource was found matching this query

```
{
    "schemas":  [
        "urn:ietf:params:scim:api:messages:2.0:BulkRequest"
    ],
    "Operations":  [
        {
            "method":  "POST",
            "bulkId":  "7528f3a9-689e-4cc5-9b20-a64f53516502",
            "path":  "/Users",
            "data":  {
                "schemas":  [
                    "urn:ietf:params:scim:schemas:core:2.0:User",
                    "urn:ietf:params:scim:schemas:extension:enterprise:2.0:User",
                    "urn:ietf:params:scim:schemas:extension:identityman:1.0:User"
                ],
                "phoneNumbers":  [
                    {
                        "value":  "+31 20 890 9100",
                        "type":  "work"
                    },
                    {
                        "value":  "+31 06 1234 5678",
                        "type":  "mobile"
                    }
                ],
                "nickName":  "Johny.Bravoo",
                "userName":  "Johny.Bravoo",
                "title":  "Identity Hero",
                "displayName":  "Johny Bravoo",
                "urn:ietf:params:scim:schemas:extension:identityman:1.0:User":  {
                    "EA1":  "",
```

Accepted - 202 - 1173 ms

Provisioning Logs



ll applications > SecMeetup HR API-driven provisionin

driven provisioning to on-premi

Download | Learn more | Refresh

Identity Name or ID

Date : **Last 24 hours** | Show dates as: : **Local**

Add filters

Date	Identity
06/02/2024, 21:43:48	Source ID 100010 Target ID 0364ec57-94f
06/02/2024, 21:42:06	Source ID 100010 Target ID 0364ec57-94f
06/02/2024, 21:15:09	Source ID 100010 Target ID 0364ec57-94f

Provisioning log details

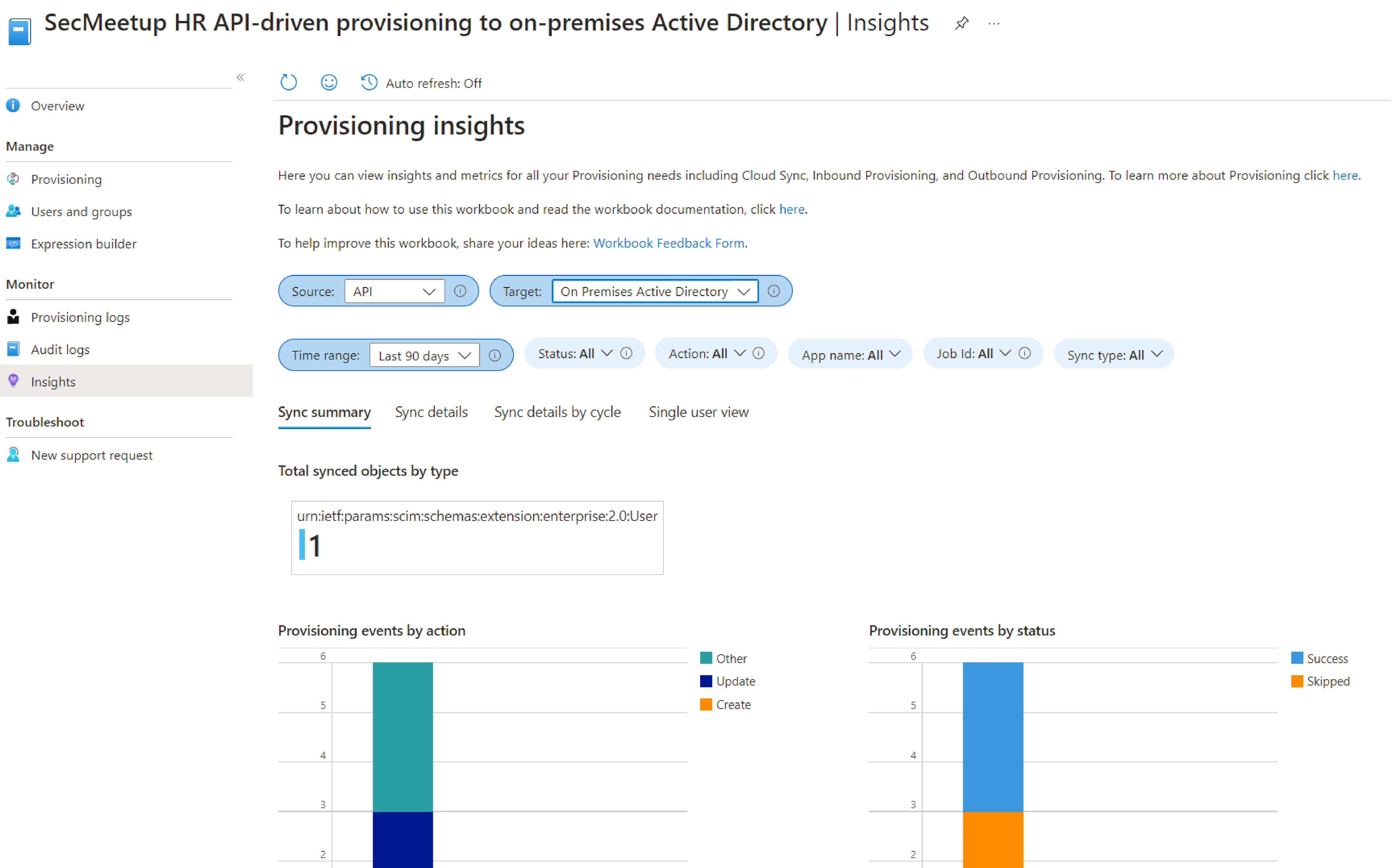
Steps | Troubleshooting & Recommendations | **Modified Properties** | Summary

Property name	New value
accountDisabled	True
title	Identity Heroooo

ommendations | **Modified Properties** | Summary

	New value
	100010
	Johny Bravoo
	True
	Johny.Bravoo
	Netherlands
	Technology
	IT Security
	Johny Bravoo
	100010
	Bravoo
	Identity City
	Johny.Bravoo@identity-man.eu
postalCode	5431 AB
sn	Johny
streetAddress	Identity Street 1
title	Identity Hero
userPrincipalName	Johny.Bravoo@identity-man.eu

Provisioning Insights Workbook



SecMeetup HR API-driven provisioning to on-premises Active Directory | Insights

Overview

Manage

- Provisioning
- Users and groups
- Expression builder

Monitor

- Provisioning logs
- Audit logs
- Insights

Troubleshoot

- New support request

Auto refresh: Off

Provisioning insights

Here you can view insights and metrics for all your Provisioning needs including Cloud Sync, Inbound Provisioning, and Outbound Provisioning. To learn more about Provisioning click here.

To learn about how to use this workbook and read the workbook documentation, click here.

To help improve this workbook, share your ideas here: Workbook Feedback Form.

Source: API

Target: On Premises Active Directory

Time range: Last 90 days

Status: All

Action: All

App name: All

Job Id: All

Sync type: All

Sync summary | Sync details | Sync details by cycle | Single user view

Total synced objects by type

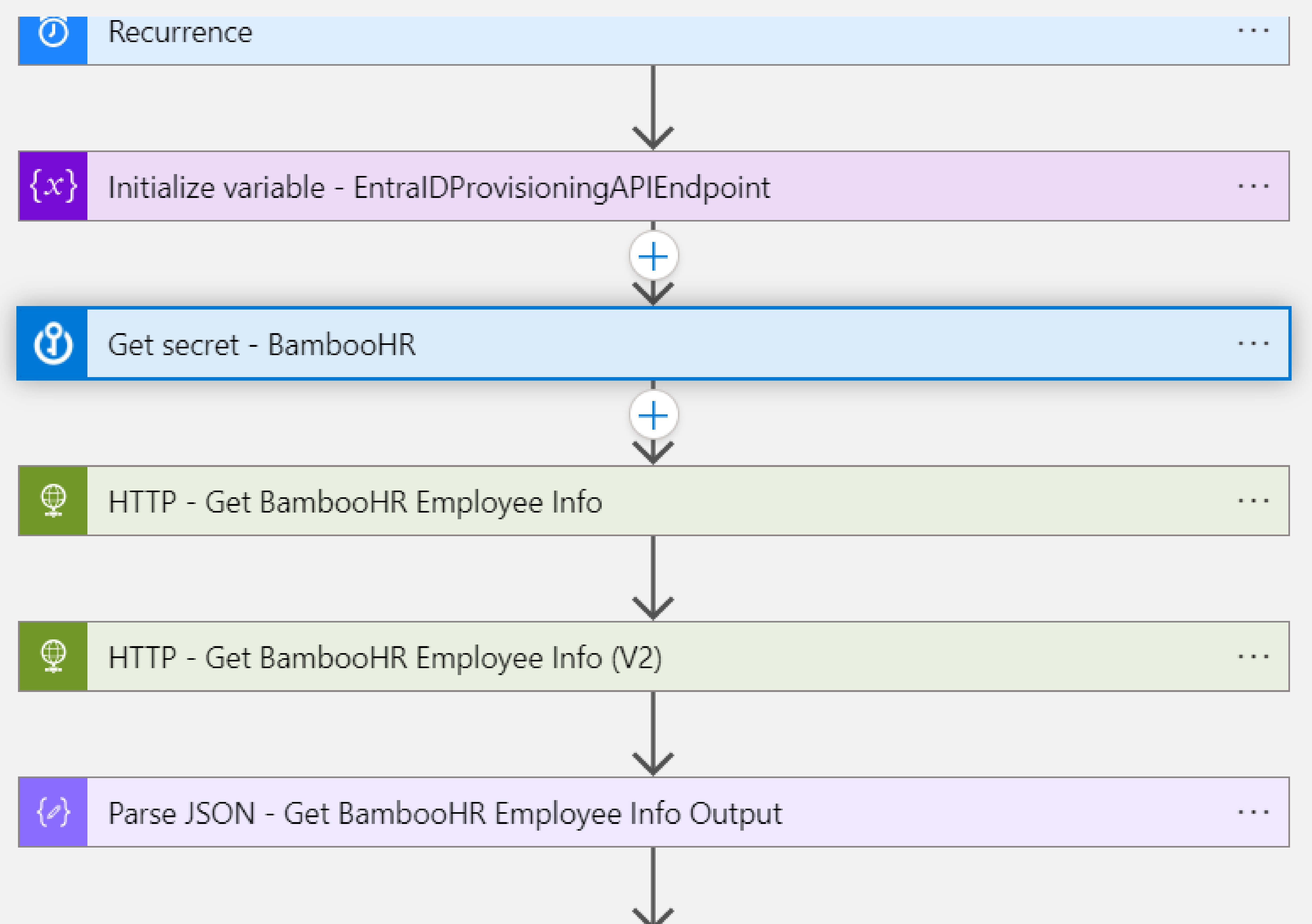
urn:ietf:params:scim:schemas:extension:enterprise:2.0:User
1

Provisioning events by action

Provisioning events by status

Scale out your deployment with automation

Link to my blog below:



Recurrence

Initialize variable - EntraIDProvisioningAPIEndpoint

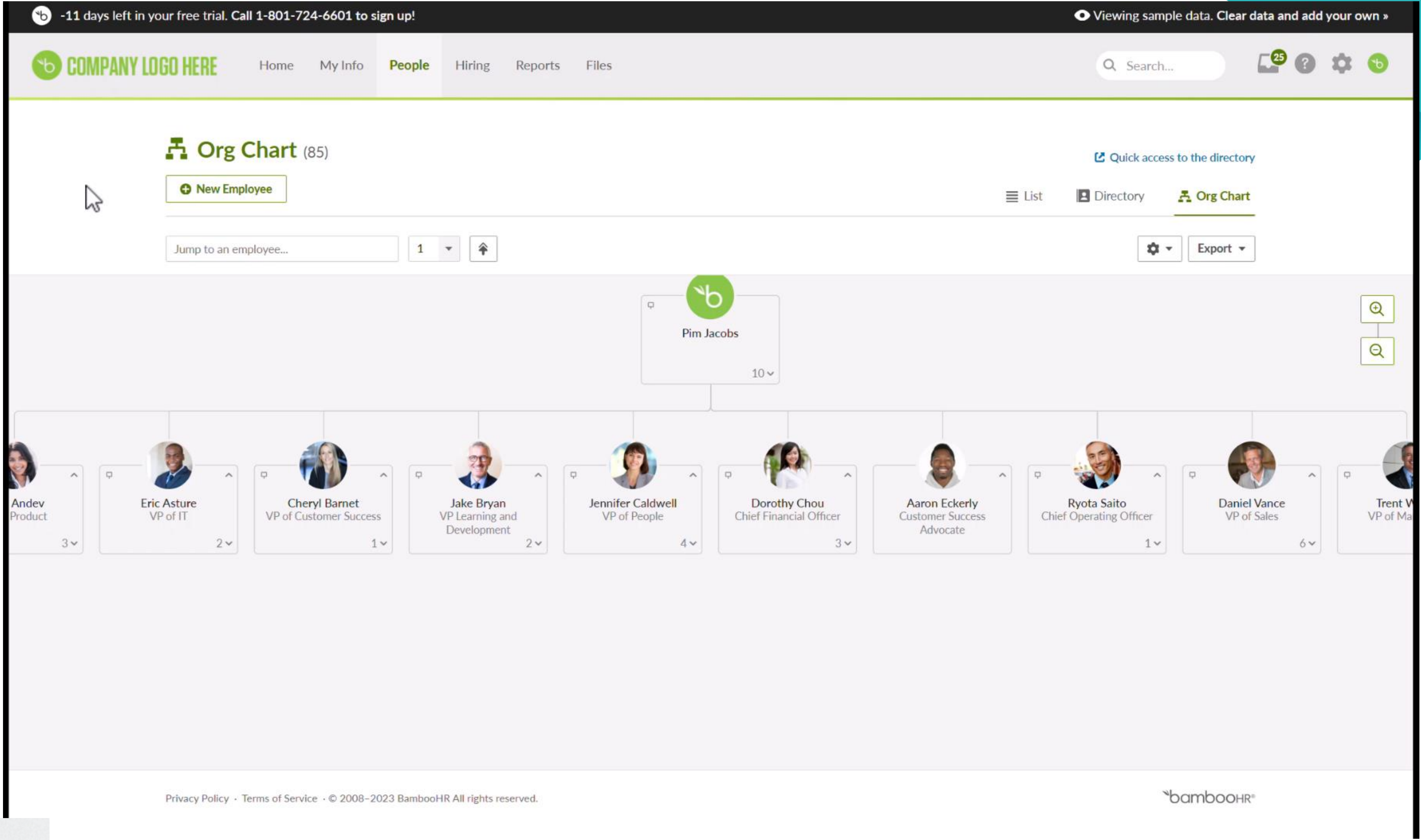
Get secret - BambooHR

HTTP - Get BambooHR Employee Info

HTTP - Get BambooHR Employee Info (V2)

Parse JSON - Get BambooHR Employee Info Output

Demo time!



-11 days left in your free trial. **Call 1-801-724-6601 to sign up!**

Viewing sample data. **Clear data and add your own »**

Org Chart (85)

Pim Jacobs 10

Andev Product 3

Eric Asture VP of IT 2

Cheryl Barnet VP of Customer Success 1

Jake Bryan VP Learning and Development 2

Jennifer Caldwell VP of People 4

Dorothy Chou Chief Financial Officer 3

Aaron Eckerly Customer Success Advocate

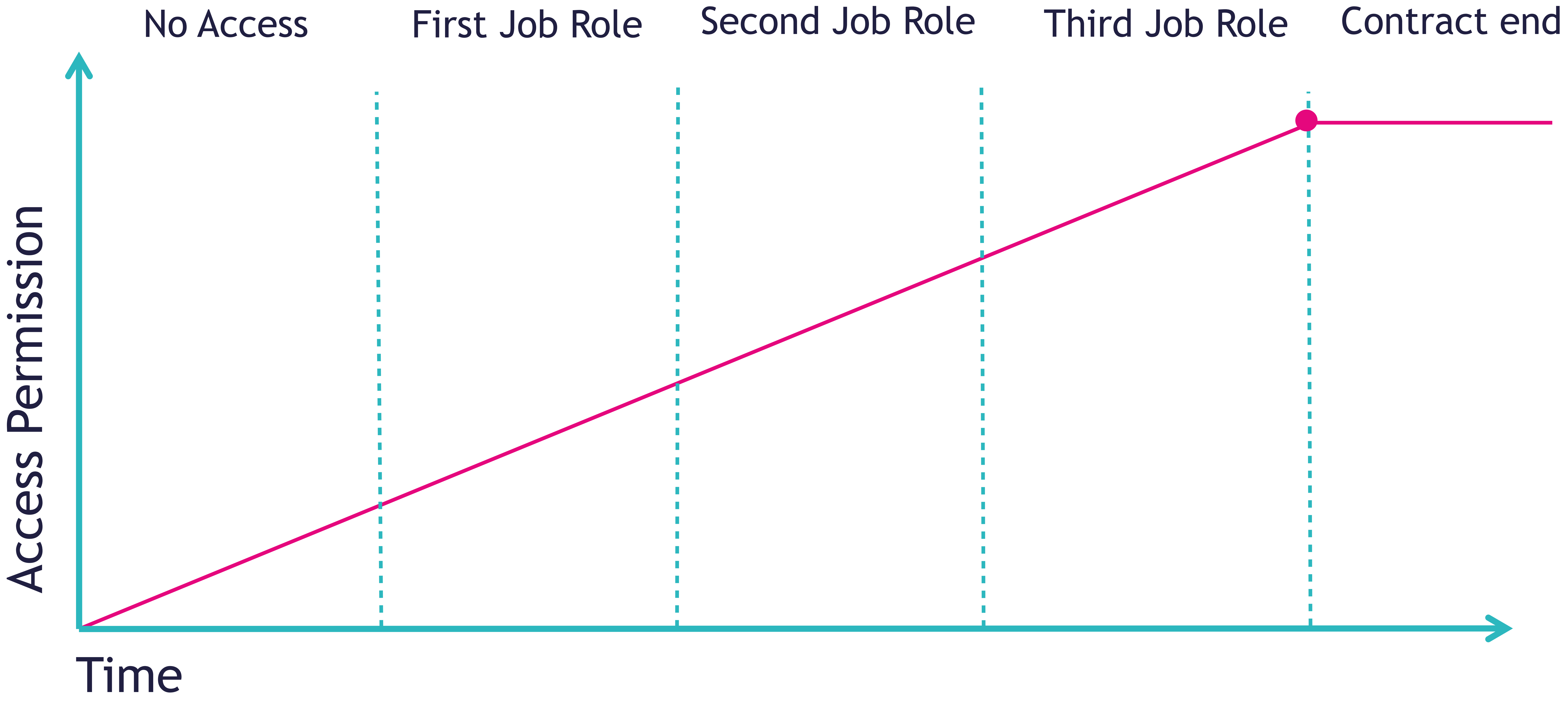
Ryota Saito Chief Operating Officer 1

Daniel Vance VP of Sales 6

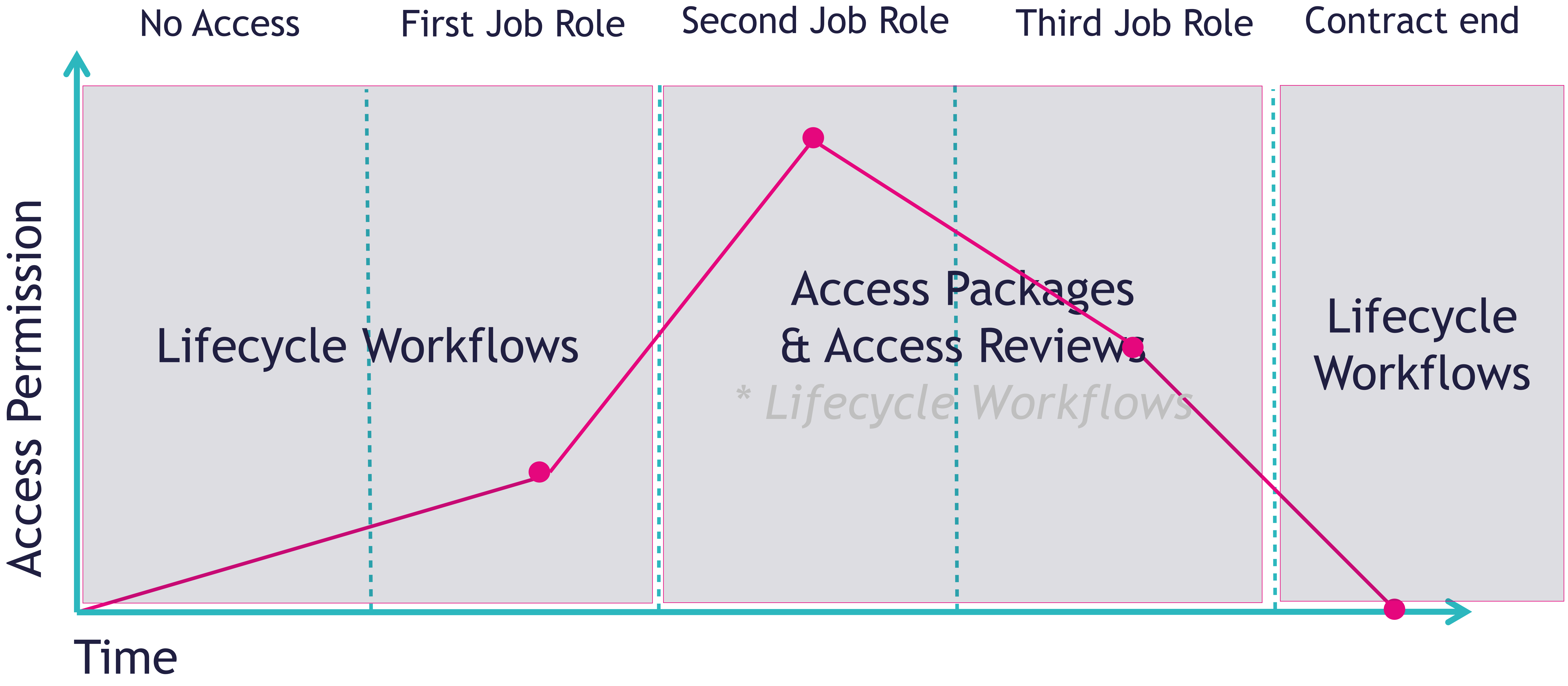
Trent W VP of Ma

Privacy Policy · Terms of Service · © 2008–2023 BambooHR All rights reserved.

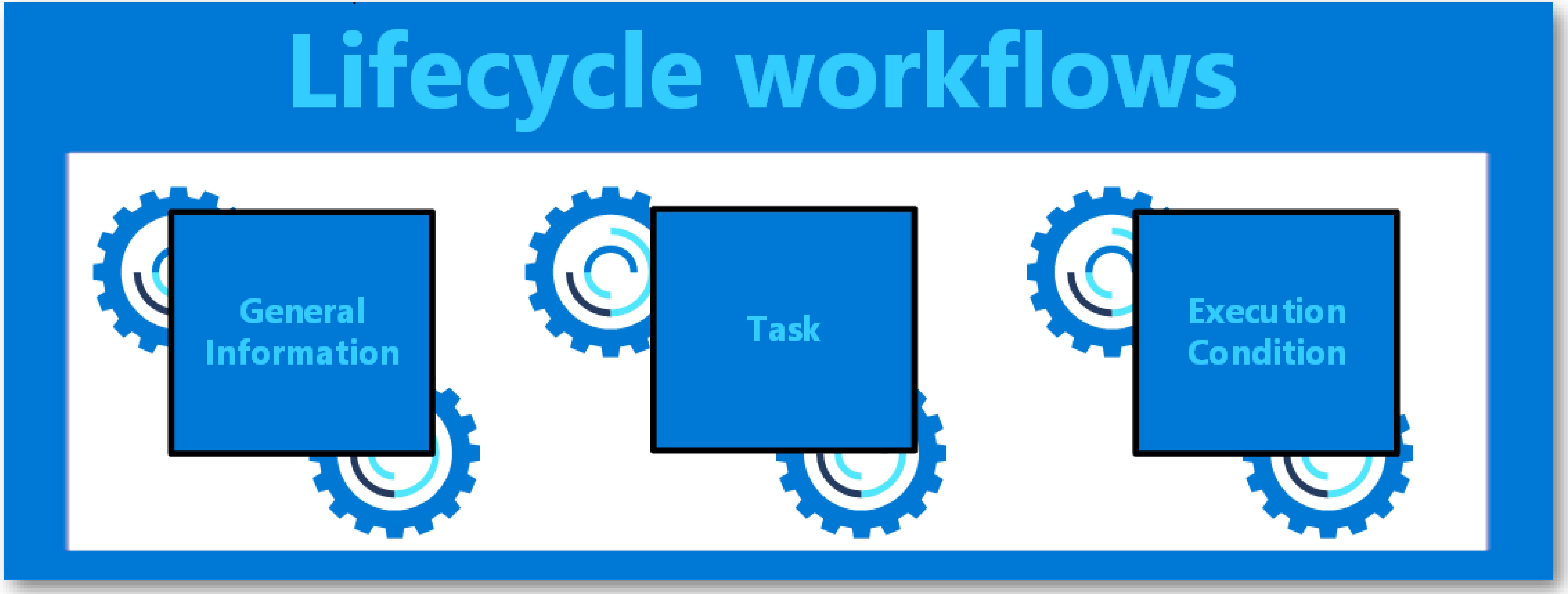
Lifecycle Workflows



Lifecycle Workflows



Understanding Lifecycle Workflows



Lifecycle workflows

General Information

Task

Execution Condition

Automate J(M)L

Execution conditions

Triggers

- On demand
- Scheduled

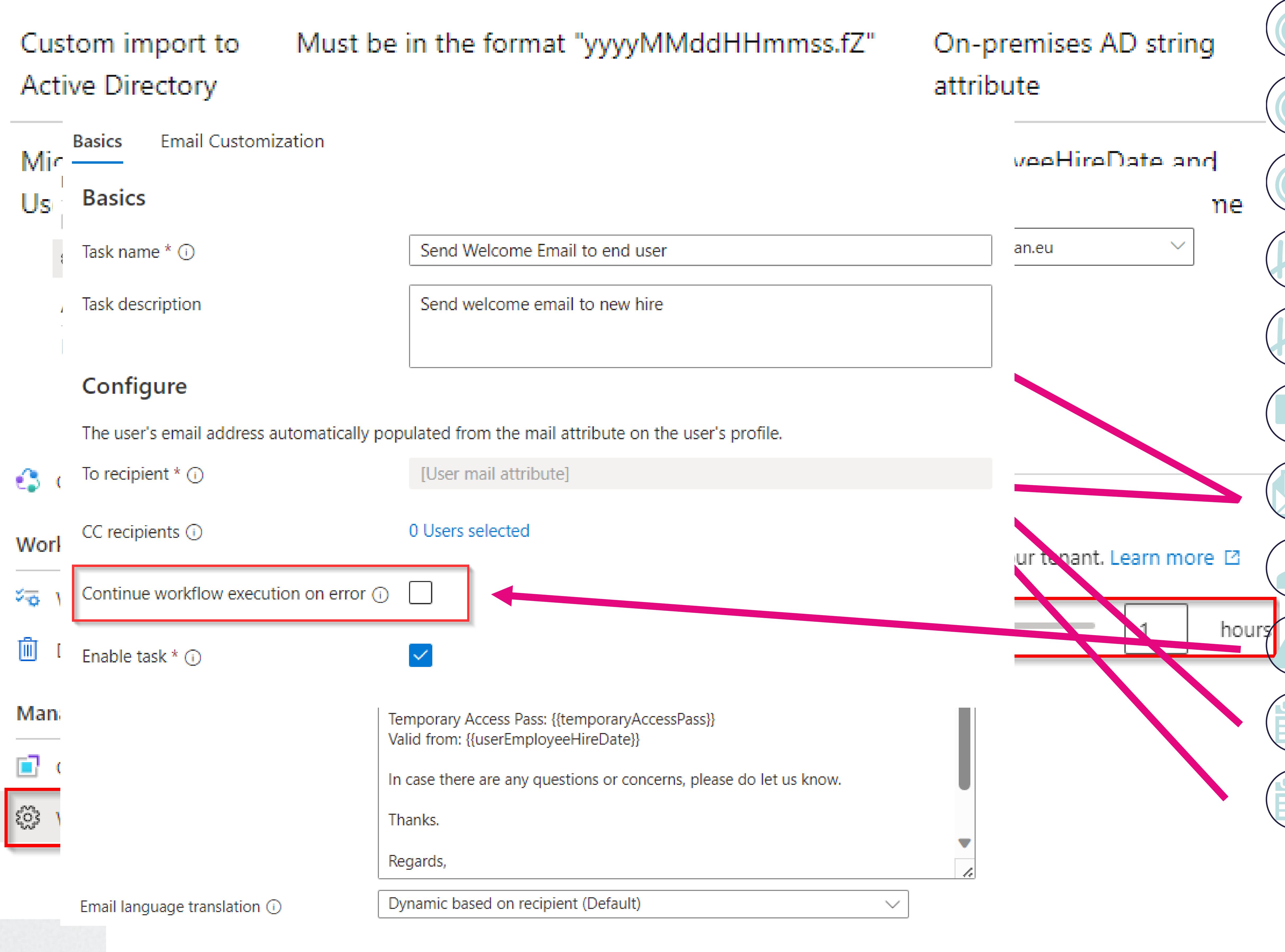
Required Attributes

- EmployeeHireDate
- EmployeeLeaveDateTime
- CreatedDateTime

Scope

- Rule-based
- Manual selected users

Lifecycle Workflows facts



Custom import to Active Directory

Must be in the format "yyyyMMddHHmmss.fZ"

On-premises AD string attribute

Basics

Task name * : Send Welcome Email to end user

Task description: Send welcome email to new hire

Configure

The user's email address automatically populated from the mail attribute on the user's profile.

To recipient * : [User mail attribute]

CC recipients: 0 Users selected

Continue workflow execution on error ☐

Enable task * ☑

Temporary Access Pass: {{temporaryAccessPass}}
Valid from: {{userEmployeeHireDate}}

In case there are any questions or concerns, please do let us know.

Thanks.

Regards,

Email language translation: Dynamic based on recipient (Default)

- Runs each 3 hours
- Interval is customizable (1-24)
- 72 hour window for processing scheduled workflows
- Max 50 Workflows per tenant
- 25 per tasks per workflow
- Preferred Language
- Email customizations (Logo, Domain & Text)
- Today native Entra for standard tasks
- Option to continue workflow on error
- EmployeeHireDate
- EmployeeLeaveDateTime

Custom task extensions

Lifecycle workflows

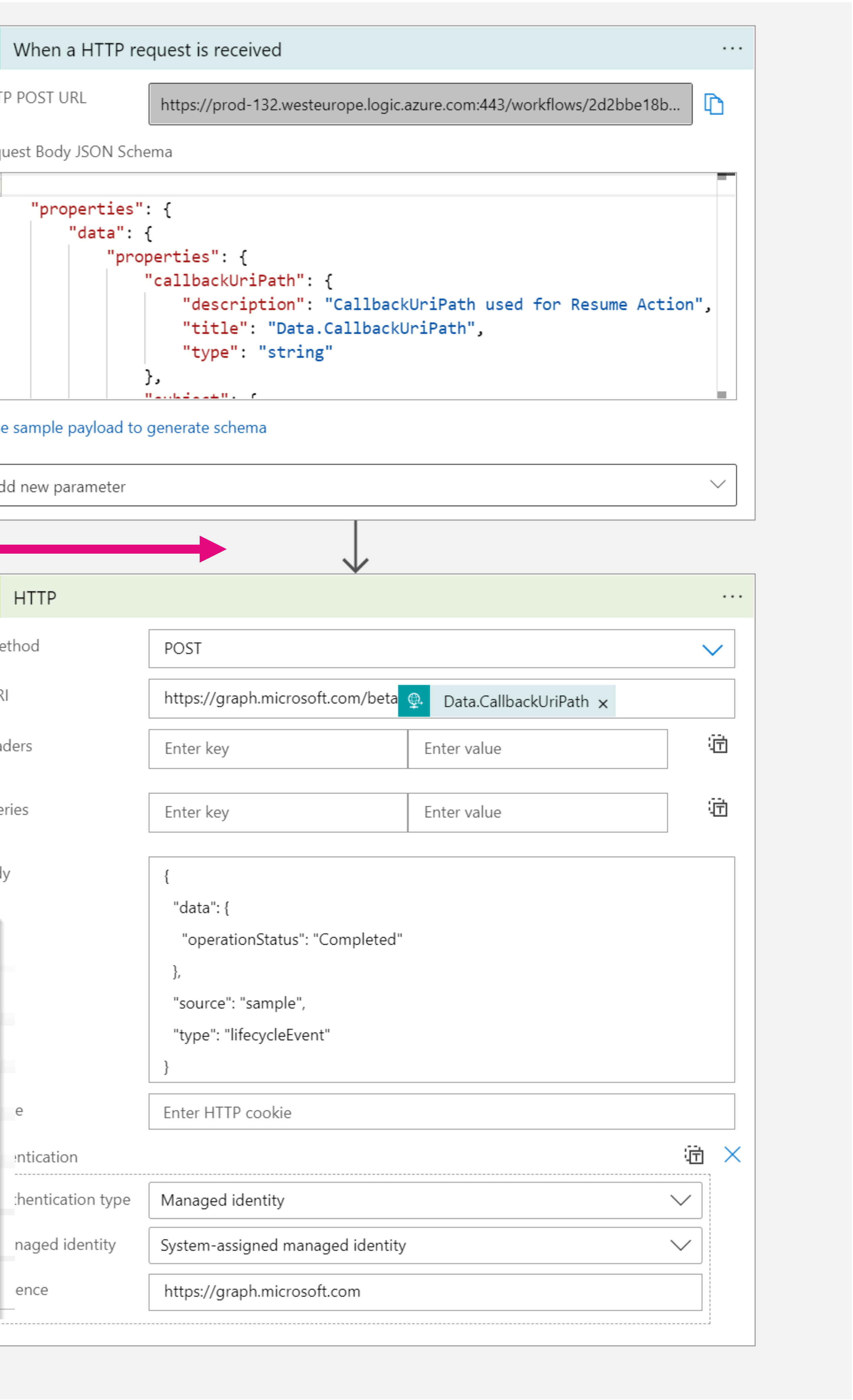
❤

Logic Apps

Prepare Logic Apps for LCW

- Trigger + Callback action
- System assigned managed identity
- Authorization policy

This is where **you** can **build** **your** own **magic**!



When a HTTP request is received

HTTP POST URL: https://prod-132.westeurope.logic.azure.com:443/workflows/2d2bbe18b...

Request Body JSON Schema

```
{
    "properties": {
        "data": {
            "properties": {
                "callbackUriPath": {
                    "description": "CallbackUriPath used for Resume Action",
                    "title": "Data.CallbackUriPath",
                    "type": "string"
                },
                "subject": {
```

HTTP

*Method: POST

*URI: https://graph.microsoft.com/beta Data.CallbackUriPath ×

Headers: Enter key | Enter value

Queries: Enter key | Enter value

Body:

```
{
  "data": {
    "operationStatus": "Completed"
  },
  "source": "sample",
  "type": "lifecycleEvent"
}
```

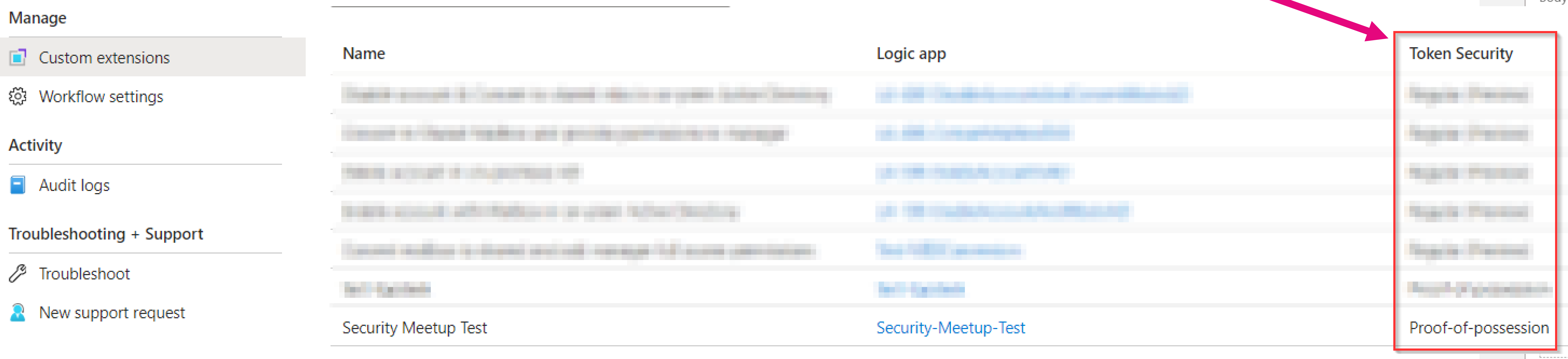
e: Enter HTTP cookie

ntication

hentication type: Managed identity

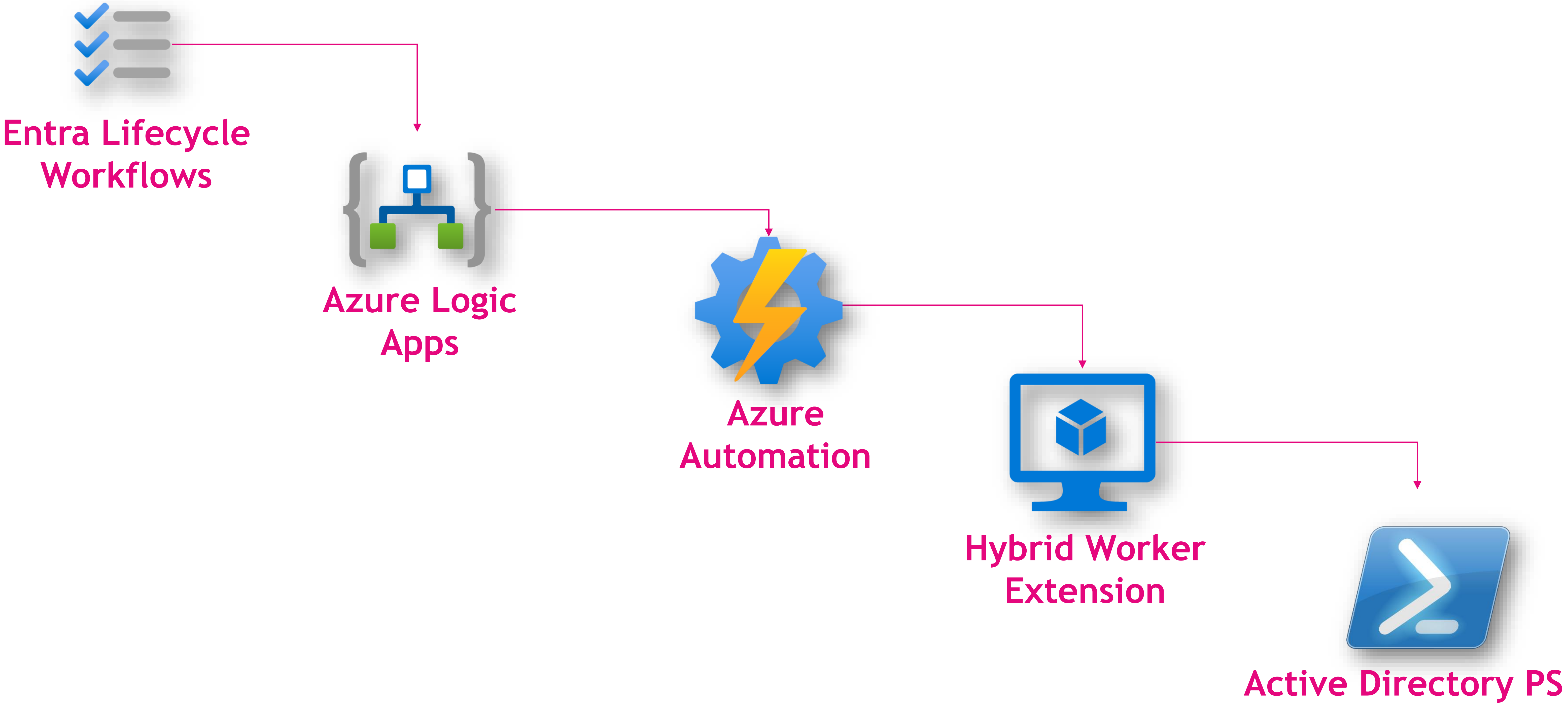
naged identity: System-assigned managed identity

ence: https://graph.microsoft.com



Name	Logic app	Token Security
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
Security Meetup Test	Security-Meetup-Test	Proof-of-possession

What about Hybrid Identities?



Entra Lifecycle Workflows

Azure Logic Apps

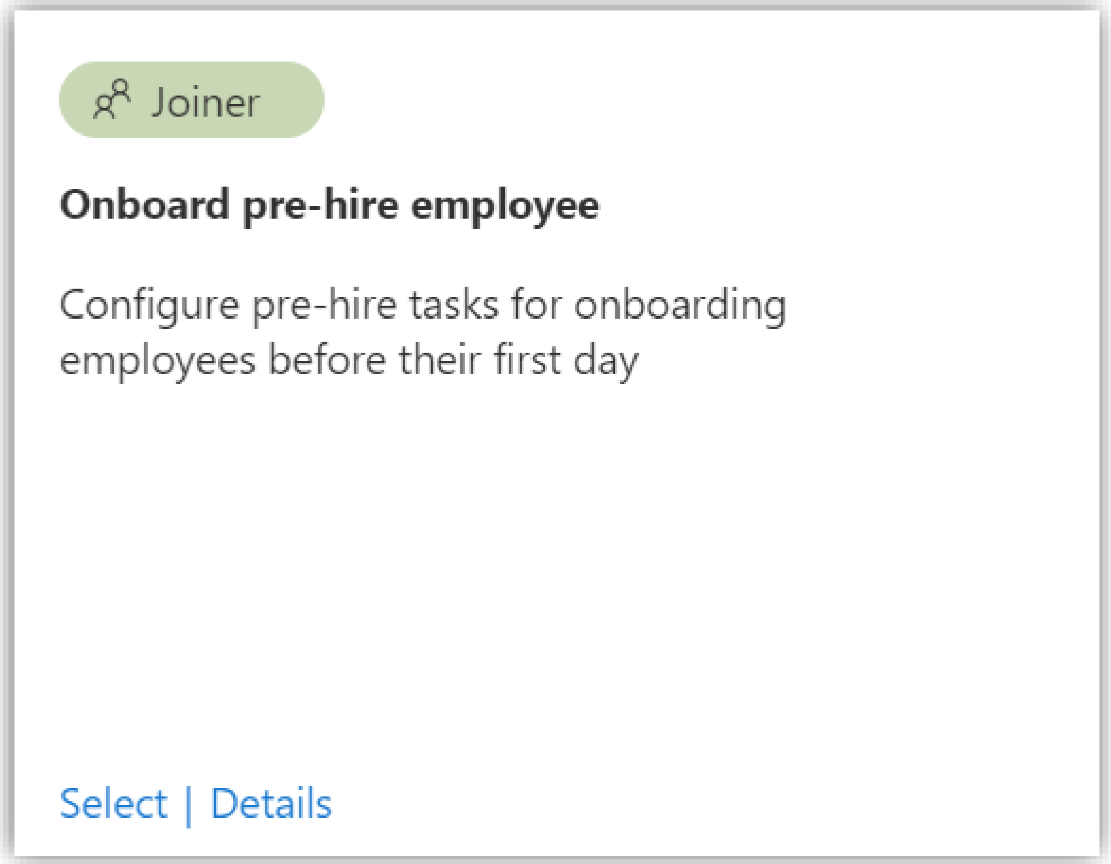
Azure Automation

Hybrid Worker Extension

Active Directory PS

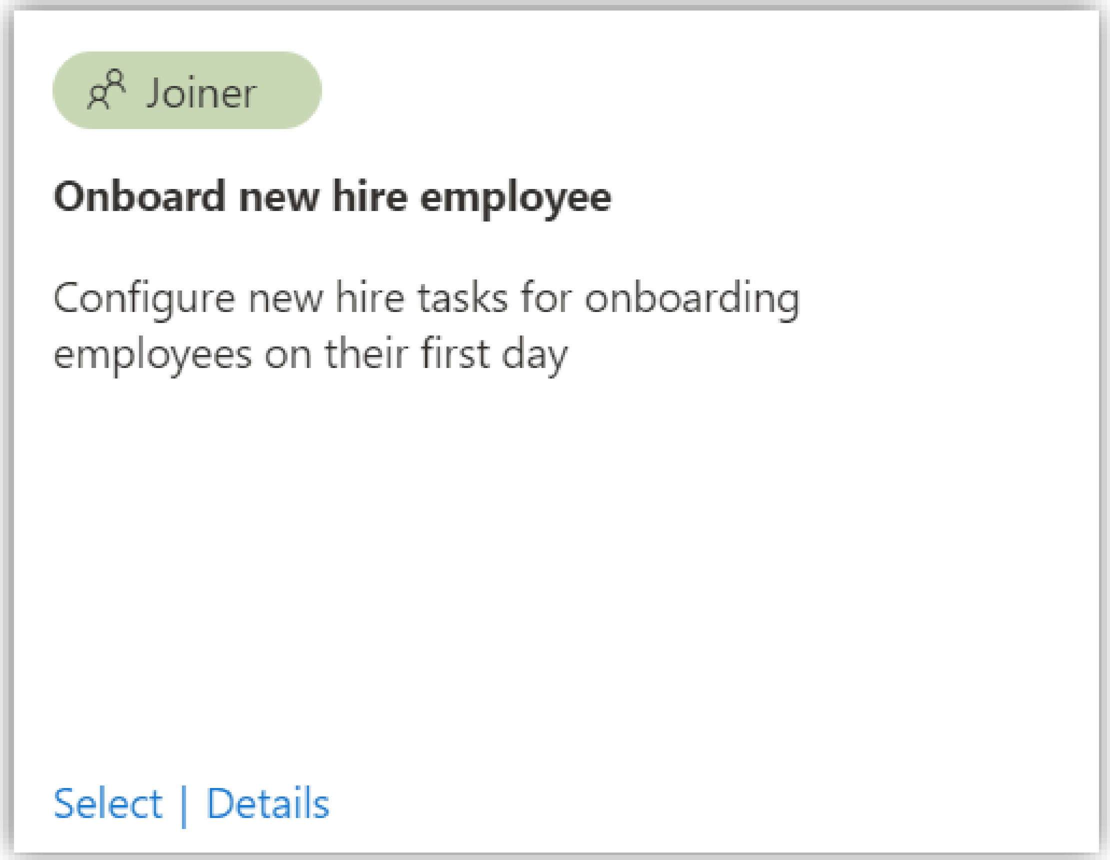
Lifecycle Workflows

Available workflow templates for joiners:



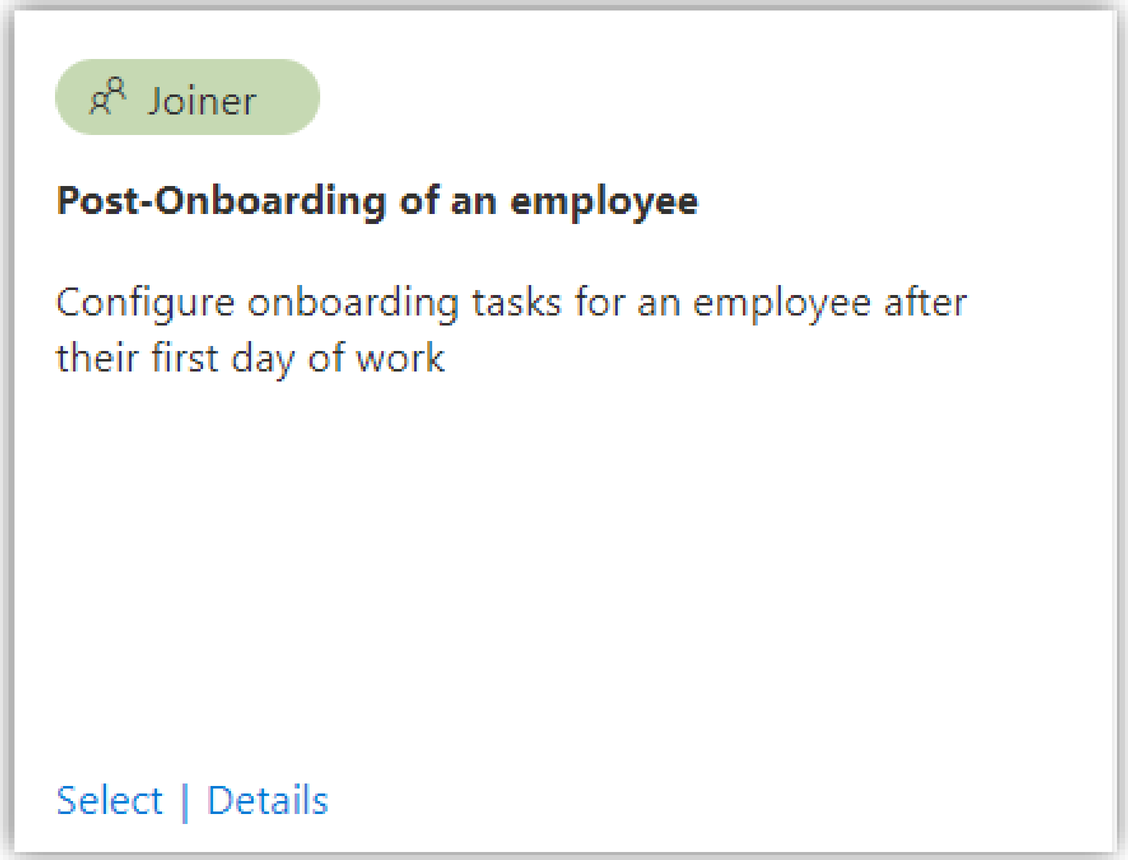
Onboard pre-hire employee

Configure pre-hire tasks for onboarding employees before their first day



Onboard new hire employee

Configure new hire tasks for onboarding employees on their first day

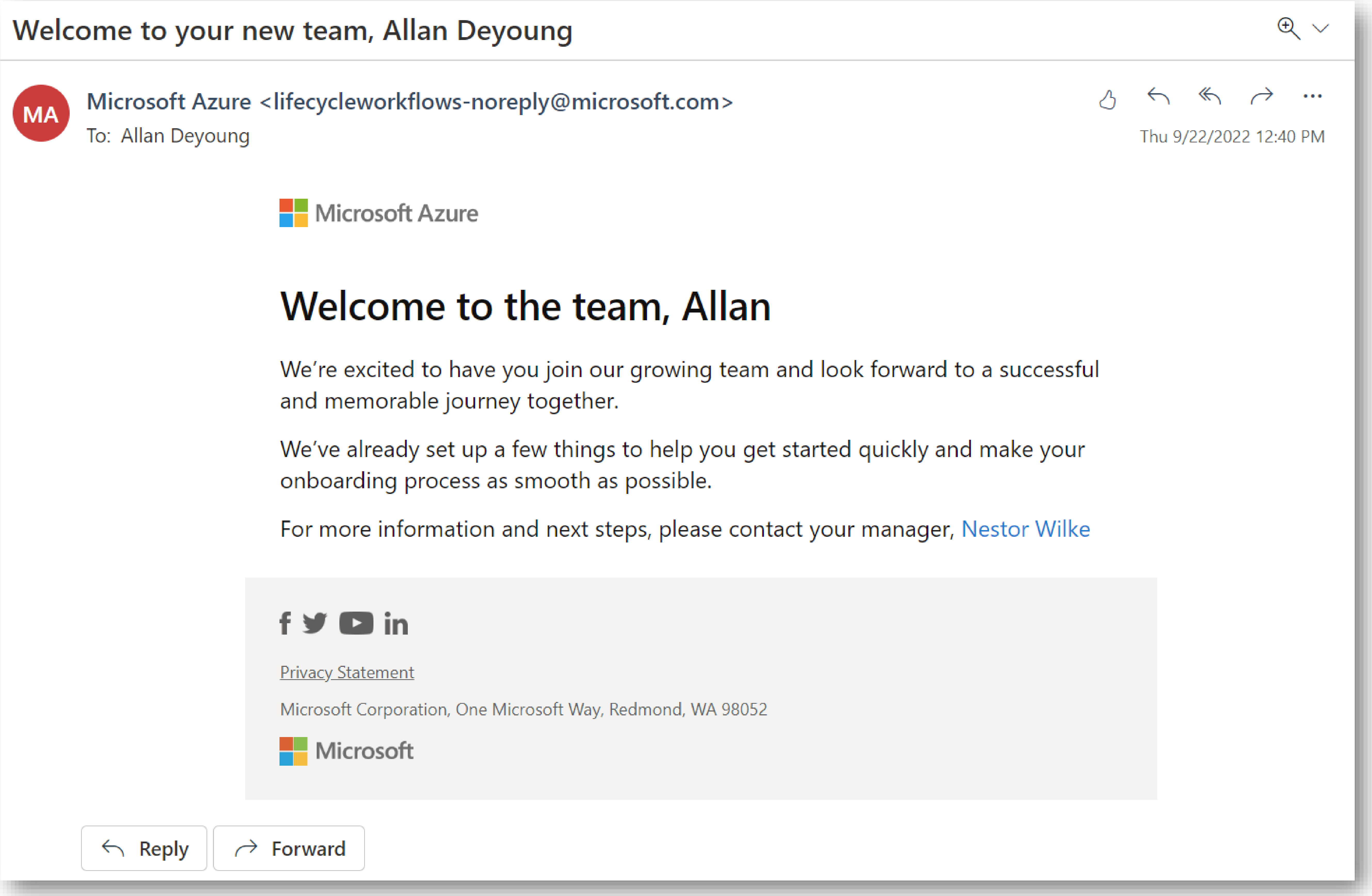


Post-Onboarding of an employee

Configure onboarding tasks for an employee after their first day of work

Onboarding Tasks

- Add or Remove user to group
- Enable or disable User Account
- Generate TAP and send to manager
- Send welcome mail
- Add or Remove user from selected Teams
- Send onboarding reminder email
- Run custom task extension
- Request user access package assignment



Welcome to your new team, Allan Deyoung

Microsoft Azure <lifecycleworkflows-noreply@microsoft.com>

To: Allan Deyoung

Thu 9/22/2022 12:40 PM

Microsoft Azure

Welcome to the team, Allan

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

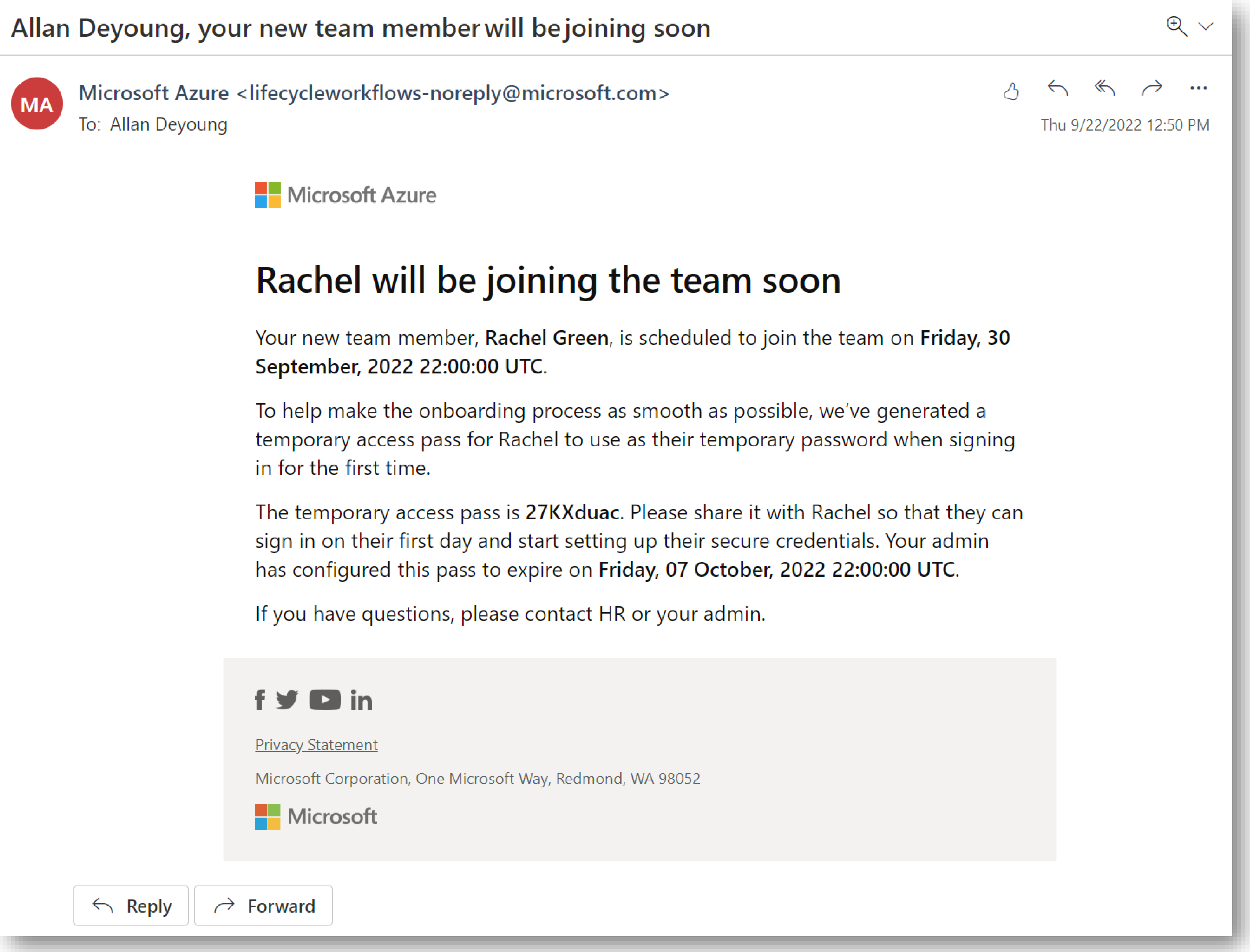
We've already set up a few things to help you get started quickly and make your onboarding process as smooth as possible.

For more information and next steps, please contact your manager, Nestor Wilke

Privacy Statement

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

Microsoft



Allan Deyoung, your new team member will be joining soon

Microsoft Azure <lifecycleworkflows-noreply@microsoft.com>

To: Allan Deyoung

Thu 9/22/2022 12:50 PM

Microsoft Azure

Rachel will be joining the team soon

Your new team member, **Rachel Green**, is scheduled to join the team on **Friday, 30 September, 2022 22:00:00 UTC**.

To help make the onboarding process as smooth as possible, we've generated a temporary access pass for Rachel to use as their temporary password when signing in for the first time.

The temporary access pass is **27KXduac**. Please share it with Rachel so that they can sign in on their first day and start setting up their secure credentials. Your admin has configured this pass to expire on **Friday, 07 October, 2022 22:00:00 UTC**.

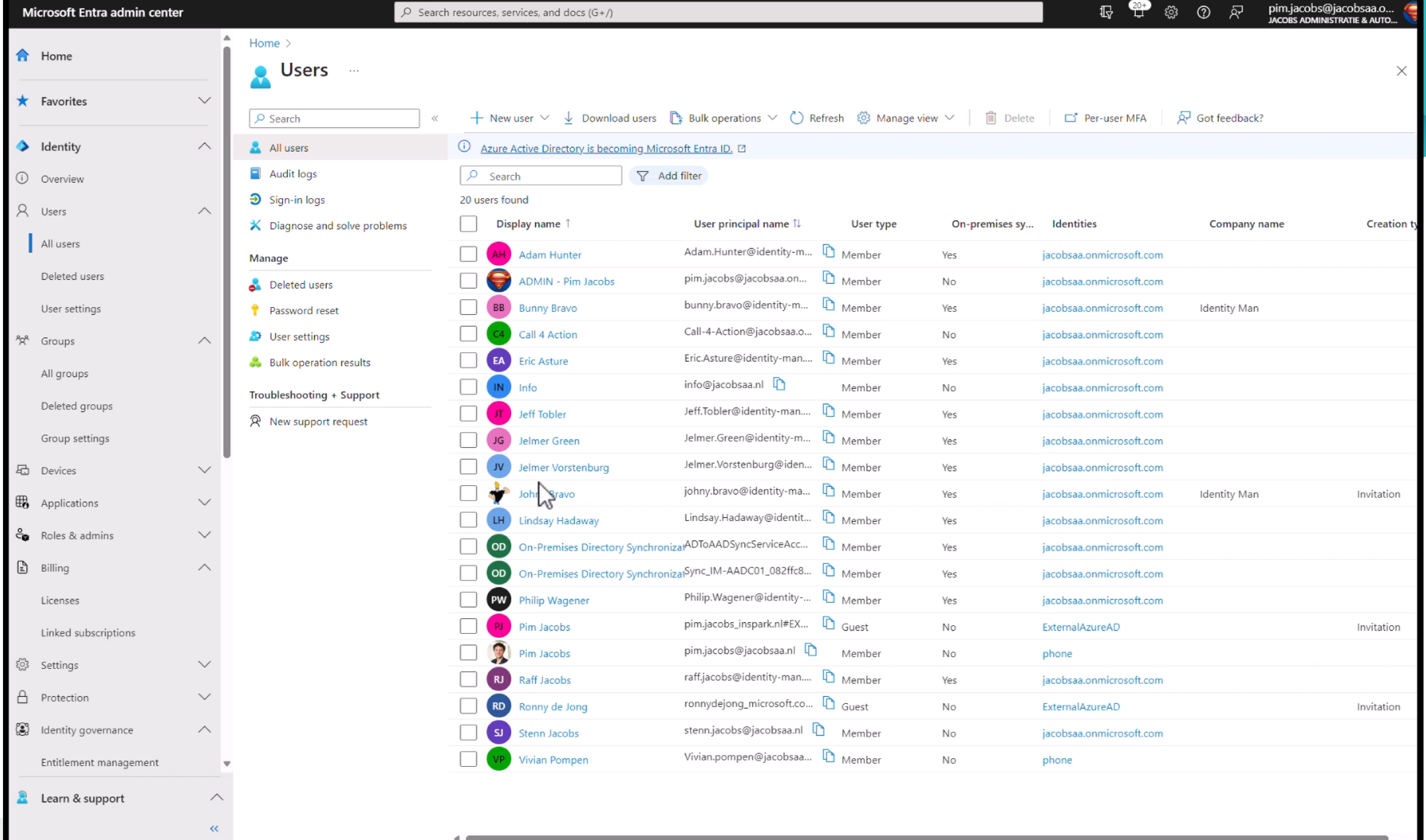
If you have questions, please contact HR or your admin.

Privacy Statement

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

Microsoft

Demo time!



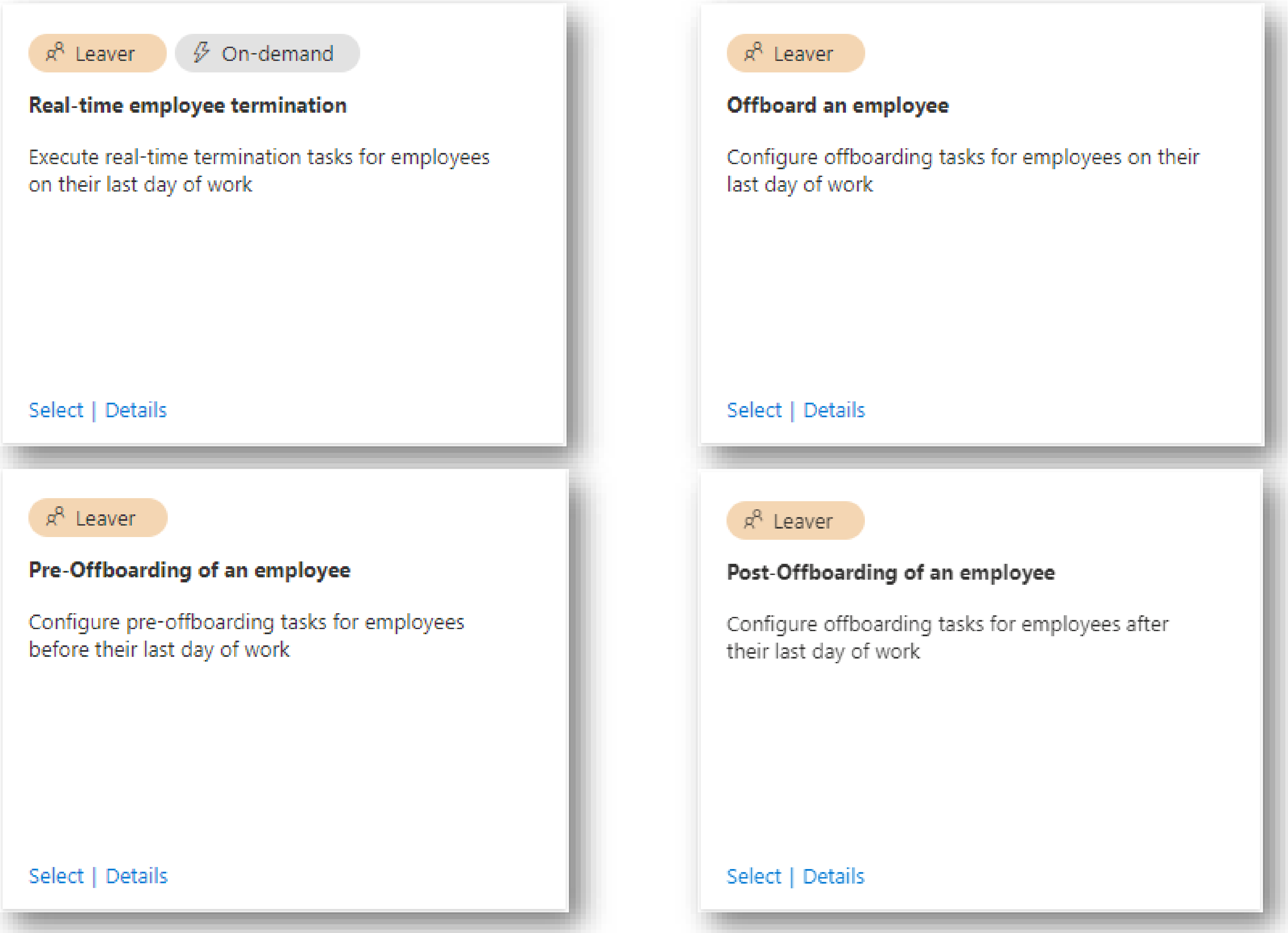
Azure Active Directory is becoming Microsoft Entra ID.

20 users found

Display name ↑	User principal name ↑↓	User type	On-premises sy...	Identities	Company name	Creation ty
Adam Hunter	Adam.Hunter@identity-m...	Member	Yes	jacobsaa.onmicrosoft.com		
ADMIN - Pim Jacobs	pim.jacobs@jacobsaa.on...	Member	No	jacobsaa.onmicrosoft.com		
Bunny Bravo	bunny.bravo@identity-m...	Member	Yes	jacobsaa.onmicrosoft.com	Identity Man	
Call 4 Action	Call-4-Action@jacobsaa.o...	Member	No	jacobsaa.onmicrosoft.com		
Eric Asture	Eric.Asture@identity-man...	Member	Yes	jacobsaa.onmicrosoft.com		
Info	info@jacobsaa.nl	Member	No	jacobsaa.onmicrosoft.com		
Jeff Tobler	Jeff.Tobler@identity-man...	Member	Yes	jacobsaa.onmicrosoft.com		
Jelmer Green	Jelmer.Green@identity-m...	Member	Yes	jacobsaa.onmicrosoft.com		
Jelmer Vorstenburg	Jelmer.Vorstenburg@iden...	Member	Yes	jacobsaa.onmicrosoft.com		
Johny Bravo	johny.bravo@identity-ma...	Member	Yes	jacobsaa.onmicrosoft.com	Identity Man	Invitation
Lindsay Hadaway	Lindsay.Hadaway@identit...	Member	Yes	jacobsaa.onmicrosoft.com		
On-Premises Directory Synchroniza	ADToAADSyncServiceAcc...	Member	Yes	jacobsaa.onmicrosoft.com		
On-Premises Directory Synchroniza	Sync_IM-AADC01_082ffc8...	Member	Yes	jacobsaa.onmicrosoft.com		
Philip Wagener	Philip.Wagener@identity-...	Member	Yes	jacobsaa.onmicrosoft.com		
Pim Jacobs	pim.jacobs_inspark.nl#EX...	Guest	No	ExternalAzureAD		Invitation
Pim Jacobs	pim.jacobs@jacobsaa.nl	Member	No	phone		
Raff Jacobs	raff.jacobs@identity-man...	Member	Yes	jacobsaa.onmicrosoft.com		
Ronny de Jong	ronnydejong_microsoft.co...	Guest	No	ExternalAzureAD		Invitation
Stenn Jacobs	stenn.jacobs@jacobsaa.nl	Member	No	jacobsaa.onmicrosoft.com		
Vivian Pompen	Vivian.pompen@jacobsaa...	Member	No	phone		

Lifecycle Workflows

Available workflow templates for leavers:



Real-time employee termination

Execute real-time termination tasks for employees on their last day of work

Offboard an employee

Configure offboarding tasks for employees on their last day of work

Pre-Offboarding of an employee

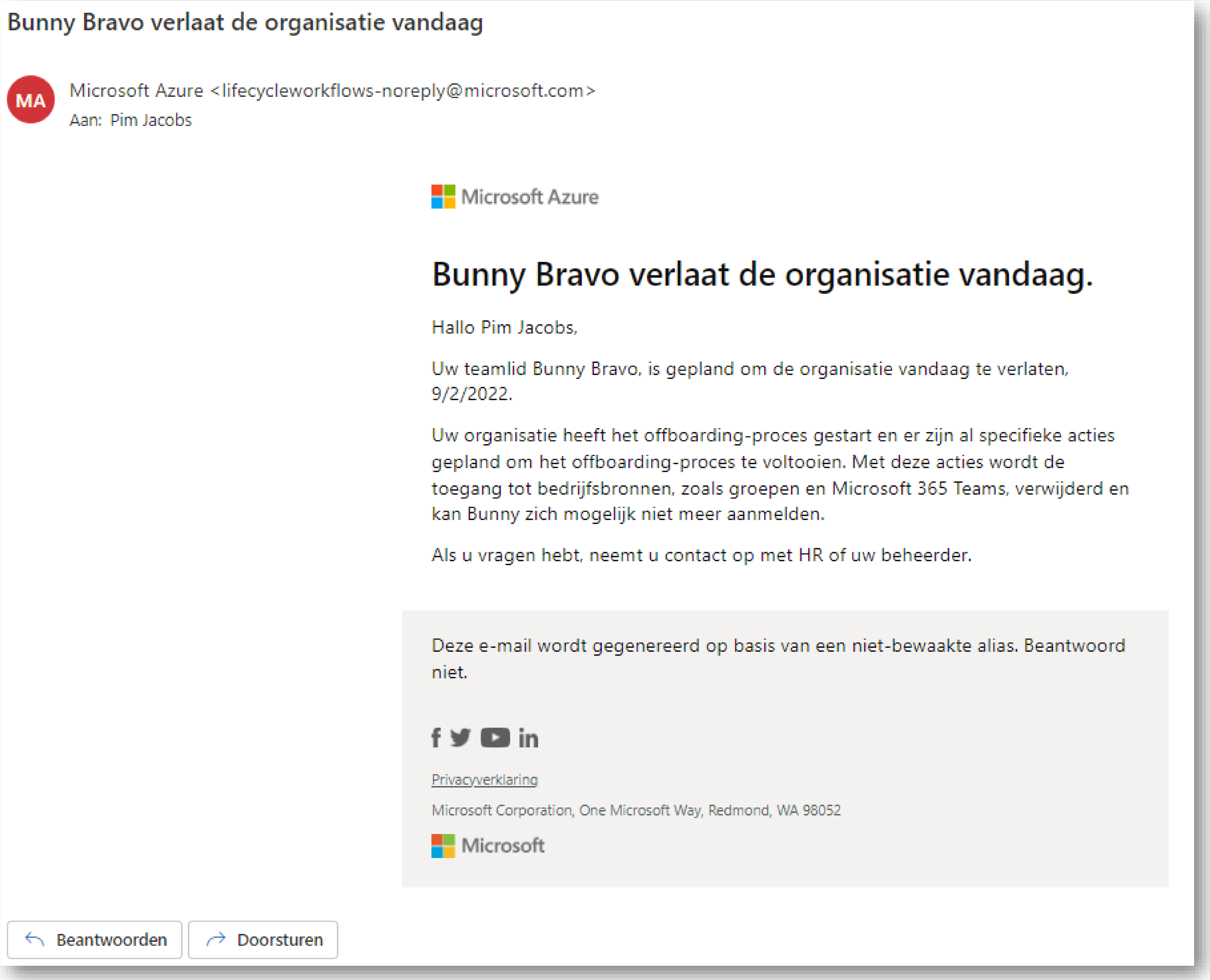
Configure pre-offboarding tasks for employees before their last day of work

Post-Offboarding of an employee

Configure offboarding tasks for employees after their last day of work

Offboarding Tasks

- Send email before user’s last day
- Send email on user’s last day
- Send email after user’s last day
- Disable / Delete User Account
- Remove all licenses for user
- Remove user from all / selected teams
- Remove user from all / selected groups
- Remove (all) access package assignment for user
- Cancel all pending access package assignment requests for user
- Run custom task extension



Bunny Bravo verlaat de organisatie vandaag

Microsoft Azure <lifecycleworkflows-noreply@microsoft.com>
Aan: Pim Jacobs

Bunny Bravo verlaat de organisatie vandaag.

Hallo Pim Jacobs,

Uw teamlid Bunny Bravo, is gepland om de organisatie vandaag te verlaten, 9/2/2022.

Uw organisatie heeft het offboarding-proces gestart en er zijn al specifieke acties gepland om het offboarding-proces te voltooien. Met deze acties wordt de toegang tot bedrijfsbronnen, zoals groepen en Microsoft 365 Teams, verwijderd en kan Bunny zich mogelijk niet meer aanmelden.

Als u vragen hebt, neemt u contact op met HR of uw beheerder.

Deze e-mail wordt gegenereerd op basis van een niet-bewaakte alias. Beantwoord niet.

Privacyverklaring

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

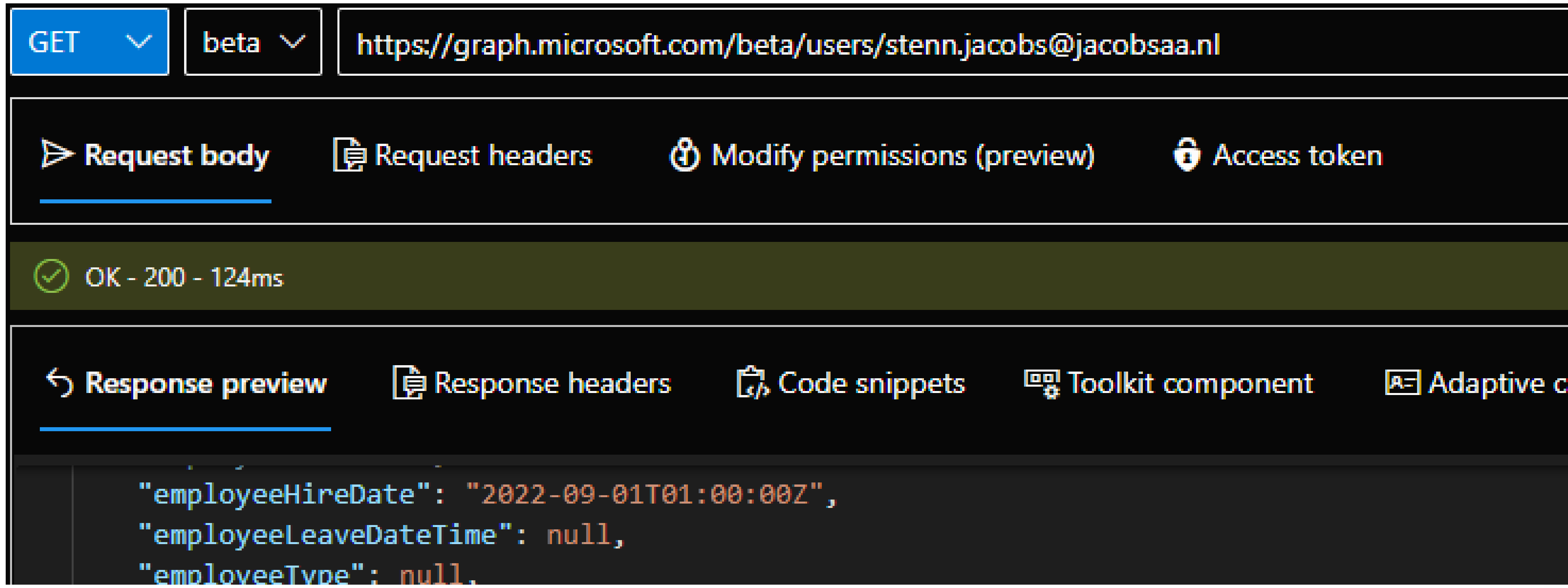
Is leaver data exposed?

Not by default, required application permissions:

- User.Read.All & User-LifeCycleInfo.Read(Write).All

For delegated permissions:

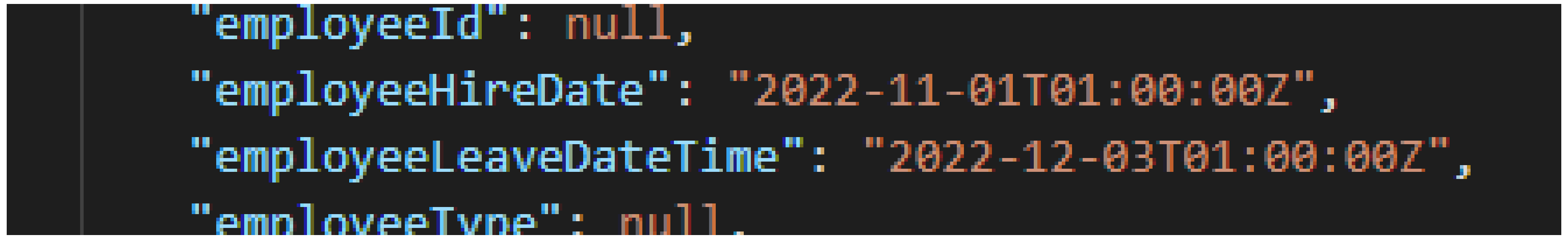
- User.Read.All
- User-LifeCycleInfo.Read(Write).All
- <u>AND, Global Admin permissions</u>



https://graph.microsoft.com/beta/users/stenn.jacobs@jacobsaa.nl

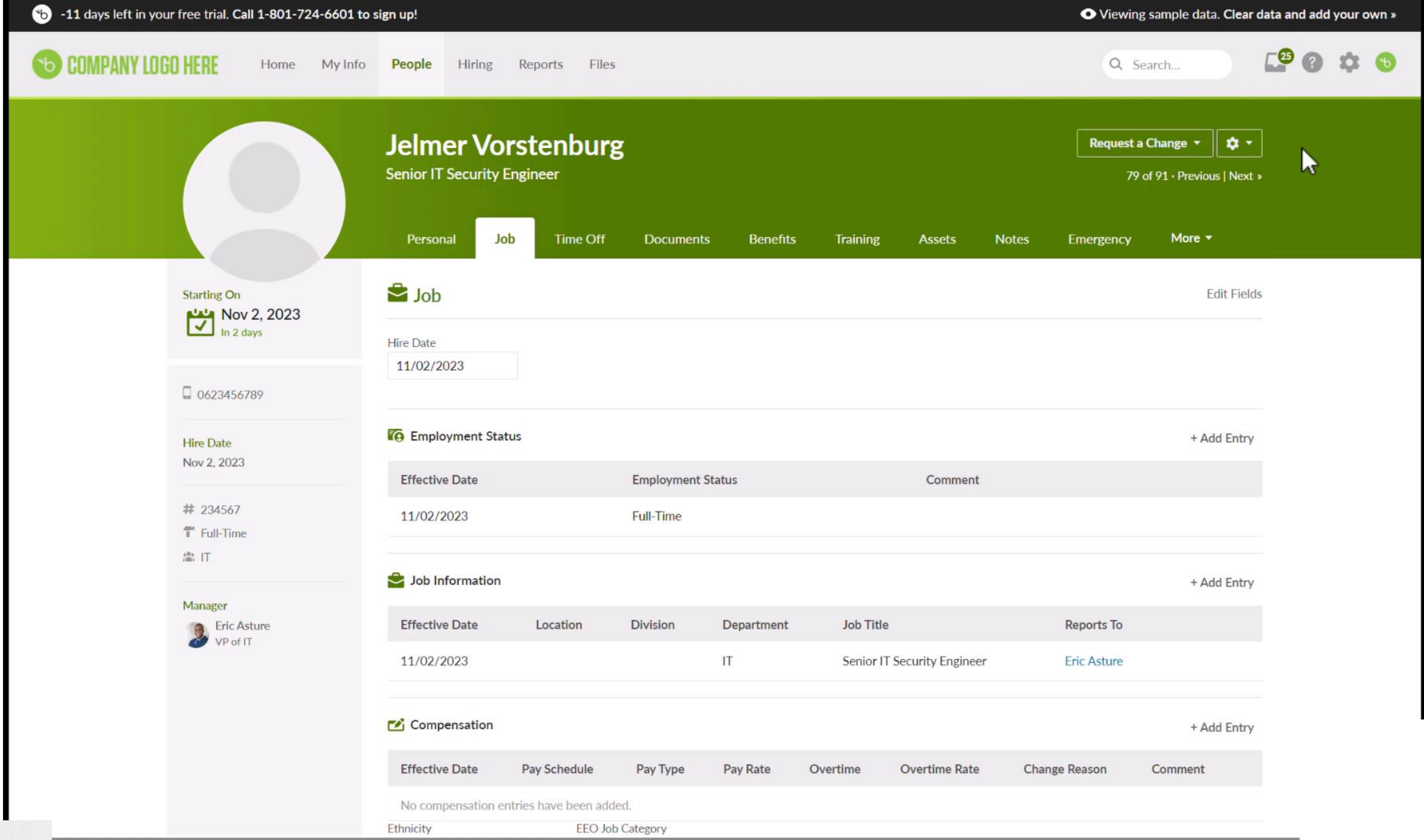
OK - 200 - 124ms

```
    "employeeHireDate": "2022-09-01T01:00:00Z",
    "employeeLeaveDateTime": null,
    "employeeType": null,
```



```
    "employeeId": null,
    "employeeHireDate": "2022-11-01T01:00:00Z",
    "employeeLeaveDateTime": "2022-12-03T01:00:00Z",
    "employeeType": null,
```

Demo time!



Jelmer Vorstenburg

Senior IT Security Engineer

Starting On
Nov 2, 2023
In 2 days

0623456789

Hire Date
Nov 2, 2023

234567
Full-Time
IT

Manager
Eric Asture
VP of IT

Job

Hire Date: 11/02/2023

Employment Status

Effective Date	Employment Status	Comment
11/02/2023	Full-Time	

Job Information

Effective Date	Location	Division	Department	Job Title	Reports To
11/02/2023			IT	Senior IT Security Engineer	Eric Asture

Compensation

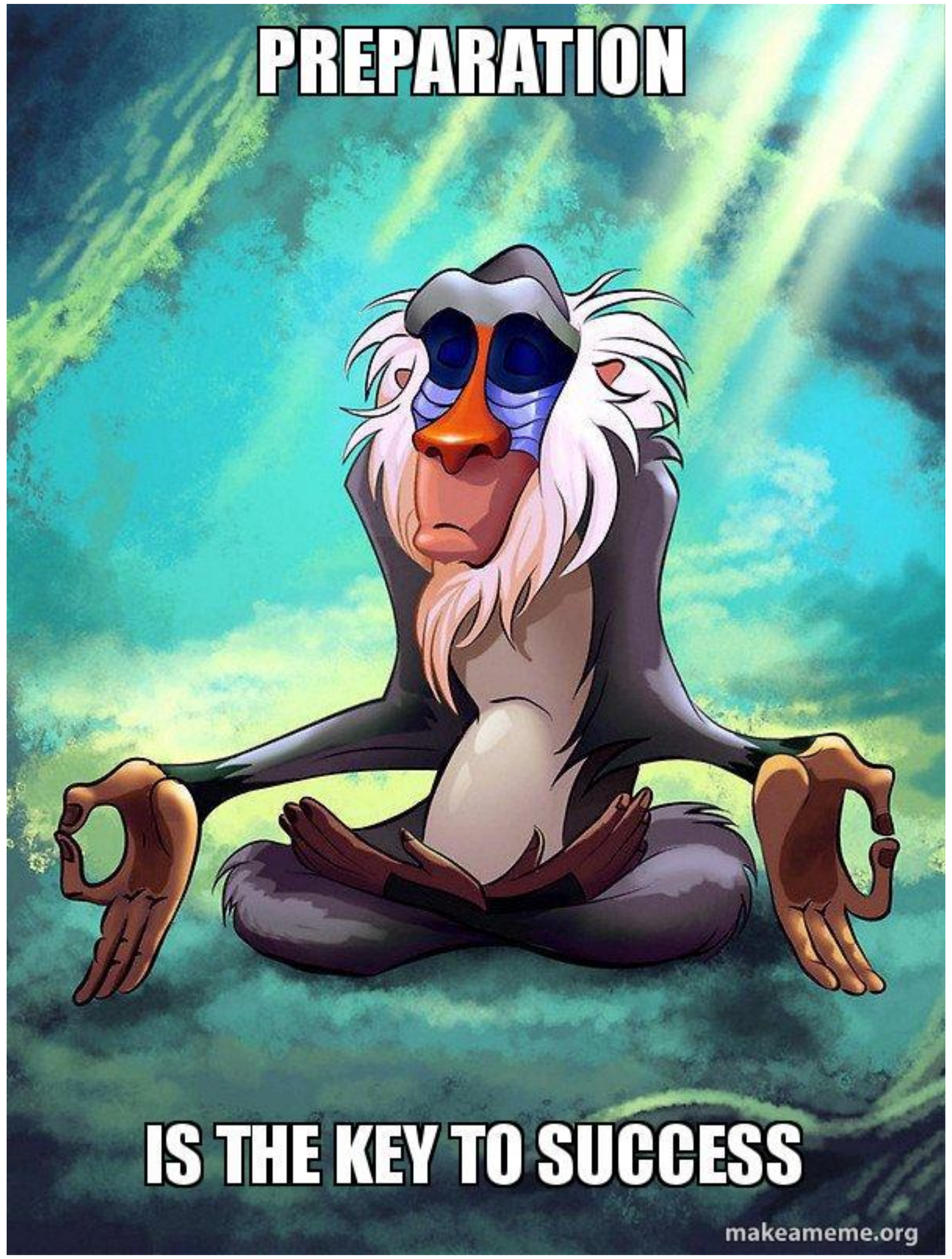
Effective Date	Pay Schedule	Pay Type	Pay Rate	Overtime	Overtime Rate	Change Reason	Comment

No compensation entries have been added.

Ethnicity
EEO Job Category

Takeaways

Inbound Provisioning API preparations



Make sure that:

- HR is involved as they are a key stakeholder
- EmployeeID is stamped on existing users
- Define a small pilot group for scoping on single department or company

Inbound Provisioning API implementation

Keep in mind that:

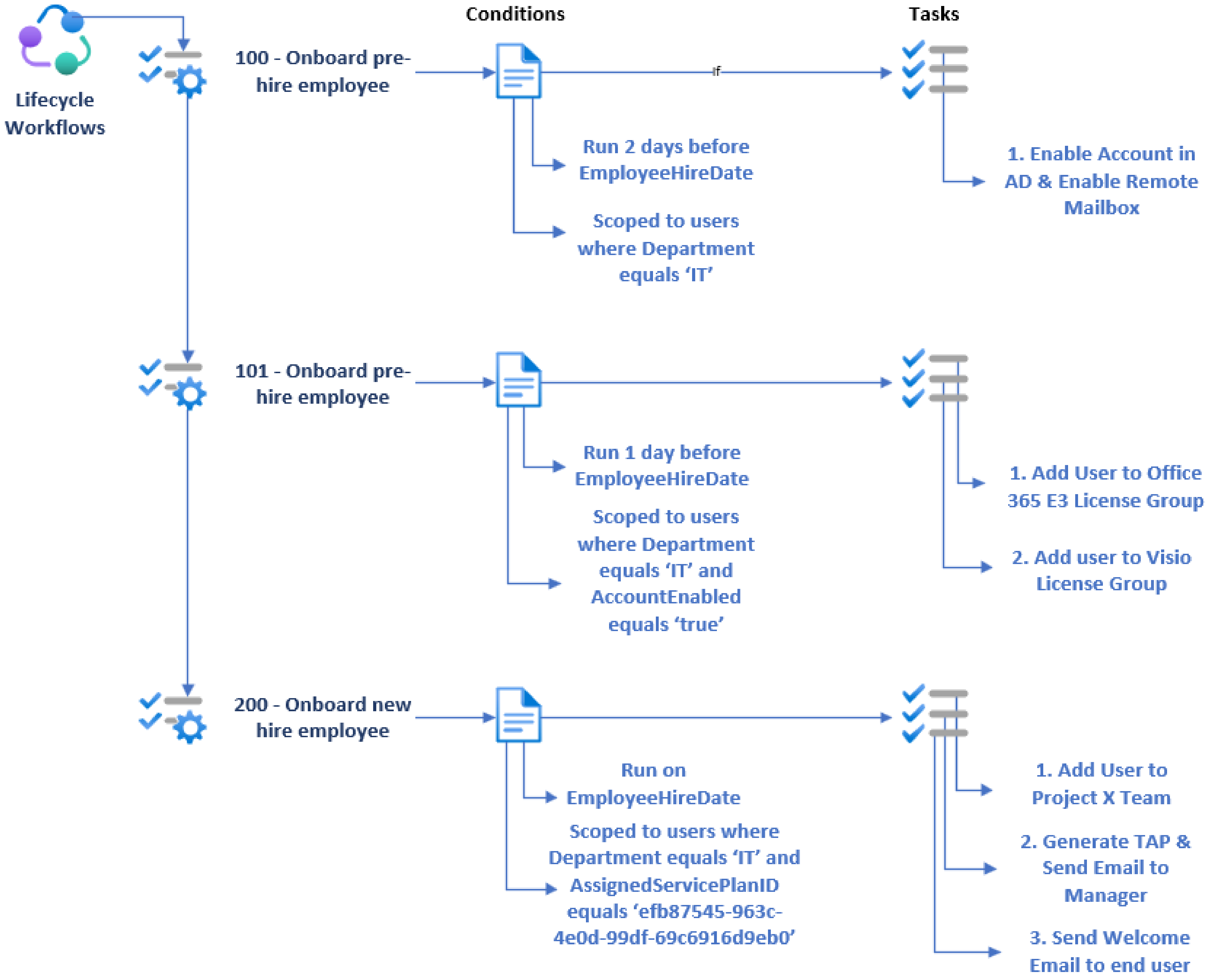
- **With conflicting UPNs the user won't be provisioned.**
- **If you set the same EmployeeID on two or more objects the provisioning will throw a failure.**
- **Don't update UPN, SamAccountname and AccountEnabled (Only during object creation)**

Inbound Provisioning API implementation

Keep in mind that:

- **The manager is mapped based on the EmployeeID and must be in scope for provisioning to be set.**
- **The CN in Active Directory won't be updated even if set to always.**
- **An empty value received from the API won't overwrite an attribute value which has a value.**

Plan 4 Lifecycle Workflows



Lifecycle Workflows

Conditions

Tasks

100 - Onboard pre-hire employee

If

Run 2 days before EmployeeHireDate

Scoped to users where Department equals 'IT'

1. Enable Account in AD & Enable Remote Mailbox

101 - Onboard pre-hire employee

Run 1 day before EmployeeHireDate

Scoped to users where Department equals 'IT' and AccountEnabled equals 'true'

1. Add User to Office 365 E3 License Group

2. Add user to Visio License Group

200 - Onboard new hire employee

Run on EmployeeHireDate

Scoped to users where Department equals 'IT' and AssignedServicePlanID equals 'efb87545-963c-4e0d-99df-69c6916d9eb0'

1. Add User to Project X Team

2. Generate TAP & Send Email to Manager

3. Send Welcome Email to end user

Start simple and basic, **<u>but with a plan!</u>**

Fill the gaps with Azure Logic Apps to provide hybrid support and custom/complex tasks.

Least privilege

Lifecycle Workflows Administrator

Users in this role can create and manage all aspects of workflows and tasks associated with Lifecycle Workflows in Microsoft Entra. This role also grants the ability to check the execution of scheduled workflows, launch on-demand workflow runs, and inspect workflow execution log.

(Cloud) Application Administrator

Users in this role can add, manage, and configure enterprise applications, app registrations but will not be able to configure or manage on-premises like app proxy.

Lessons Learned

- The Inbound Provisioning API is extremely powerful so extend the user scope slowly and get HR involved.
- Preferably use an API of HR where possible!
- Configure dependencies on previous Lifecycle Workflows (like we also recommend in MIM).
- If the 1st of the month is a Saturday, we do require a Temporary Access Pass which is valid for 3 days (using built-in example).
  - When you want to go Passwordless Lifecycle Workflows can be extremely helpful (for onboarding and restrictions!)
  - Multi-use Temporary access passes are required
- Reboots during Out-of-the-Box experience are killing when providing temporary access passes with Lifecycle Workflows!

Q & A

Thank you!