

Hi 
Ninjas!

SUMMIT
SUMMIT
SUMMIT
SUMMIT
SUMMIT



Halle 36.1
room check-in



Stop the Madness: Eliminating manual user creation with Entra ID Governance



Welcome on stage



Speaker

Nicola Suter

Security Consultant
baseVISION AG



Speaker

Janic Verboon

Endpoint Consultant
baseVISION AG

Session

1. The challenge
2. The solution(s)
3. More Solution(s) and advanced use-cases

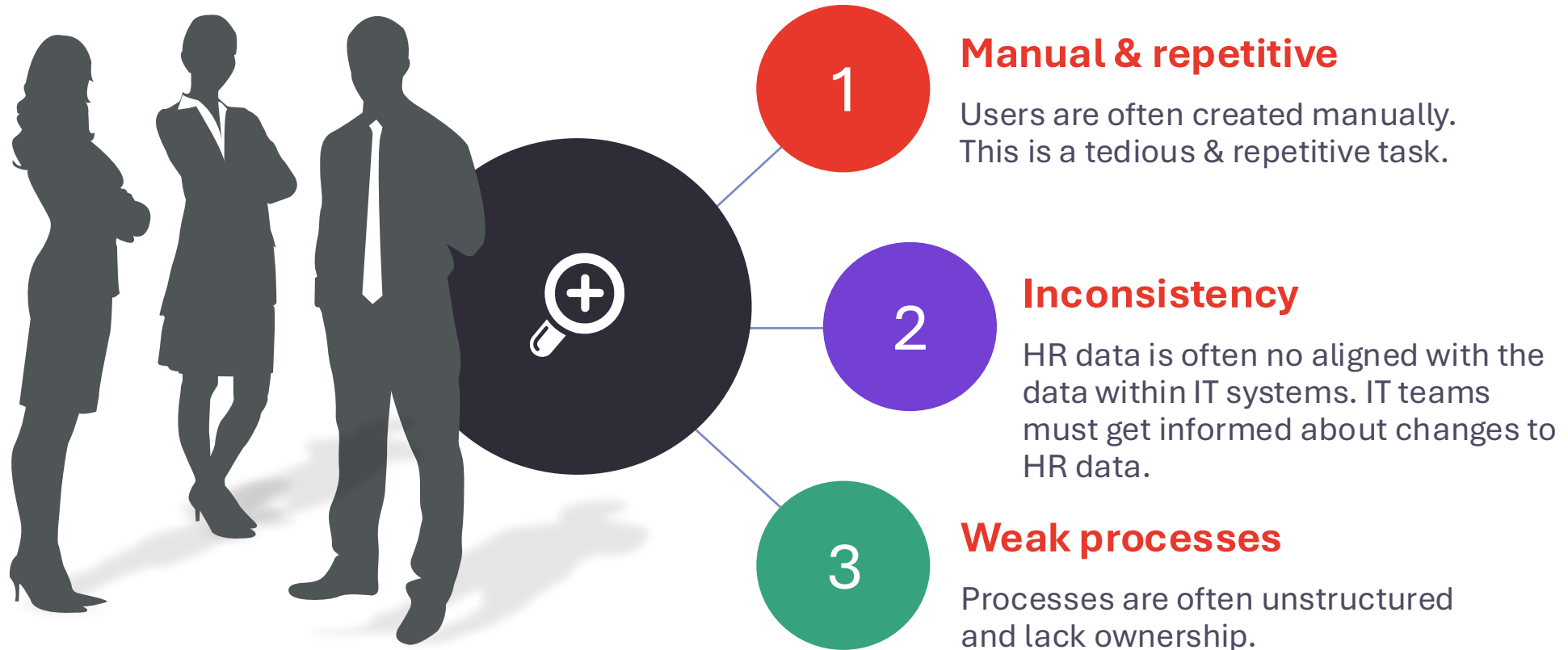
#wpninjas

The Problem Episode I

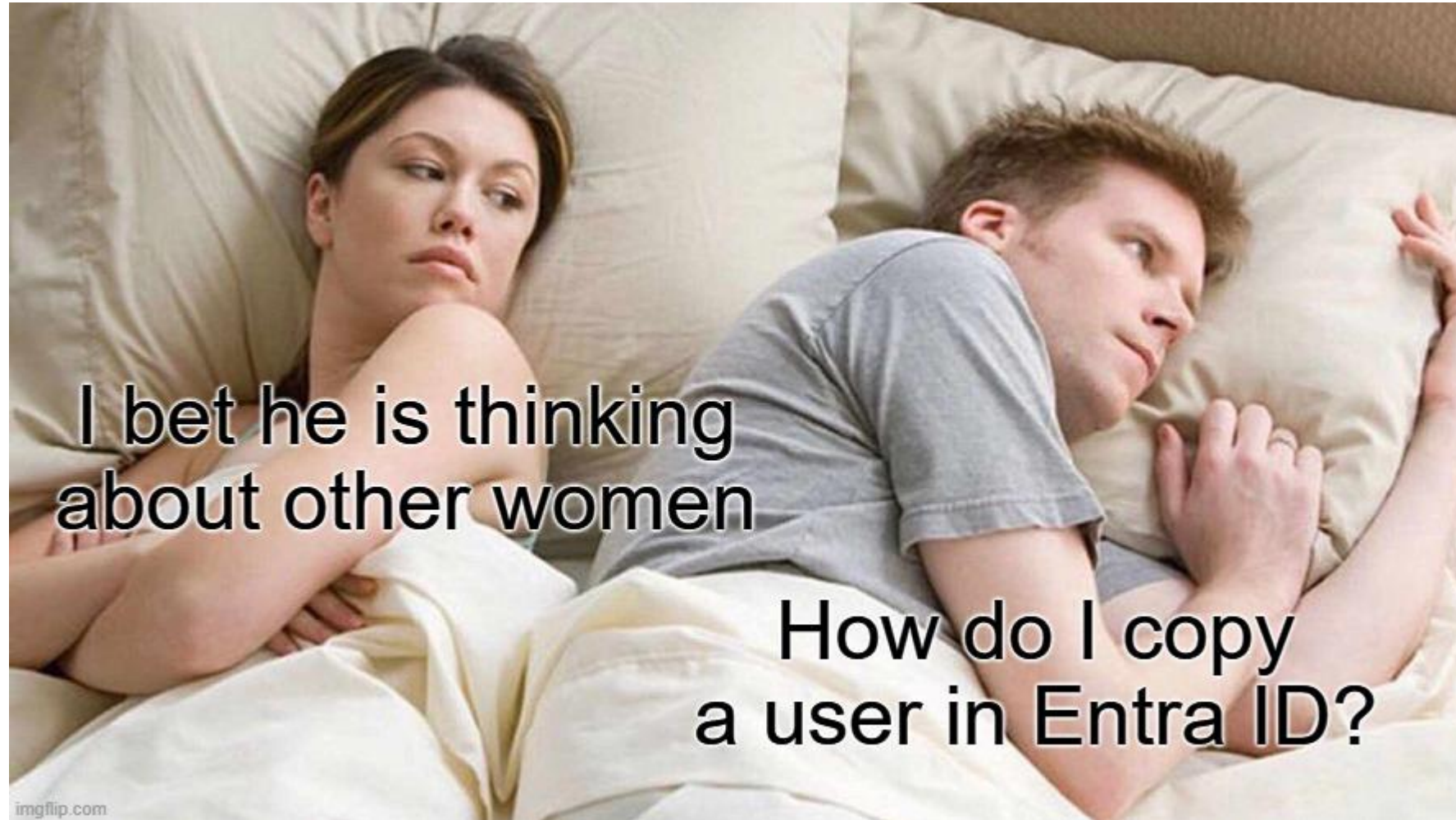
The Phantom Account Creation Menace



The Problem – What we see & experience



The Problem



The Problem

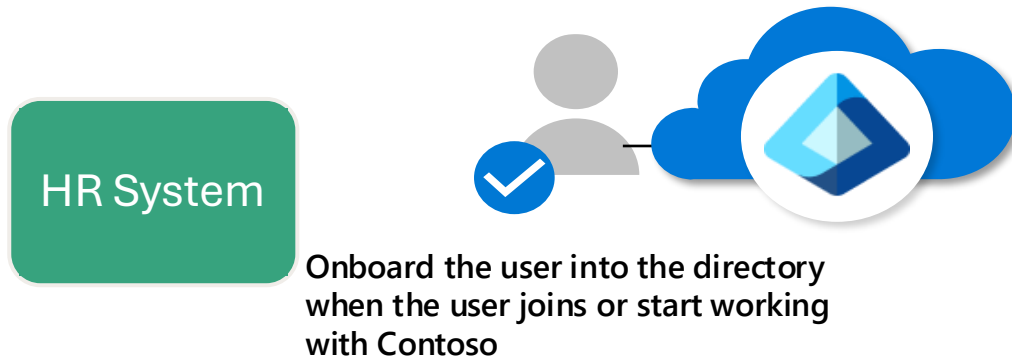


The Solution

Connecting your HR system to your directory



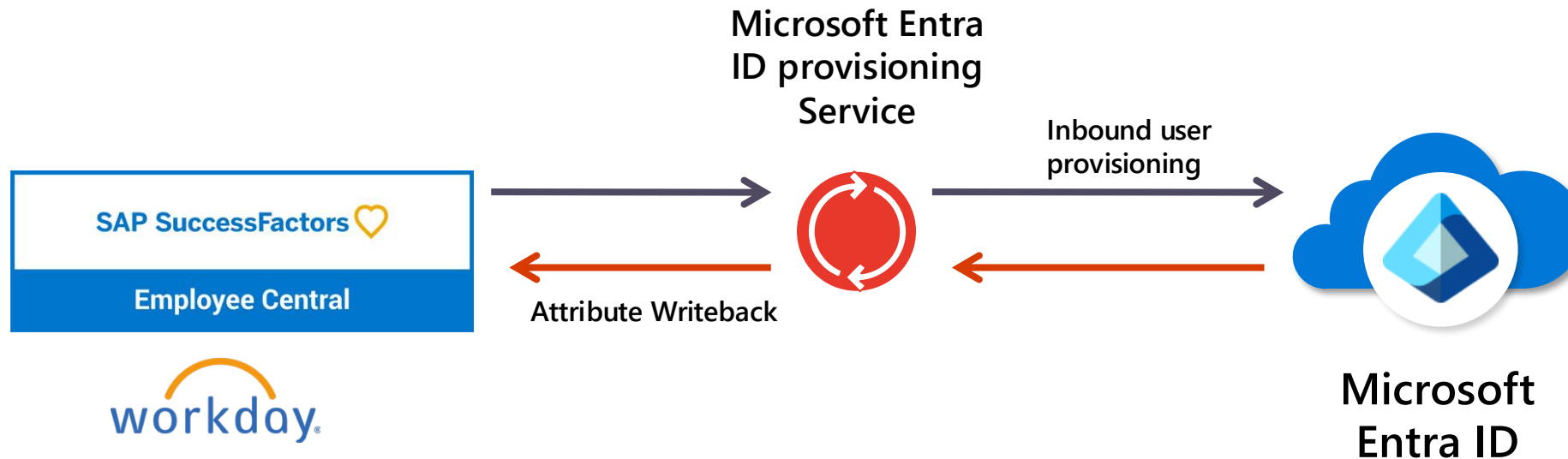
The Solution - Introduction



- By connecting the HR platform to Active Directory / Entra ID, **the HR system becomes the leading system** when it comes to specific user attributes.
- This requires a high involvement of HR during the project phase and the later operation.
- HR data and Active Directory Data must be reviewed and aligned.
- Joiner / Mover / Leaver processes of HR and IT must be aligned and documented.

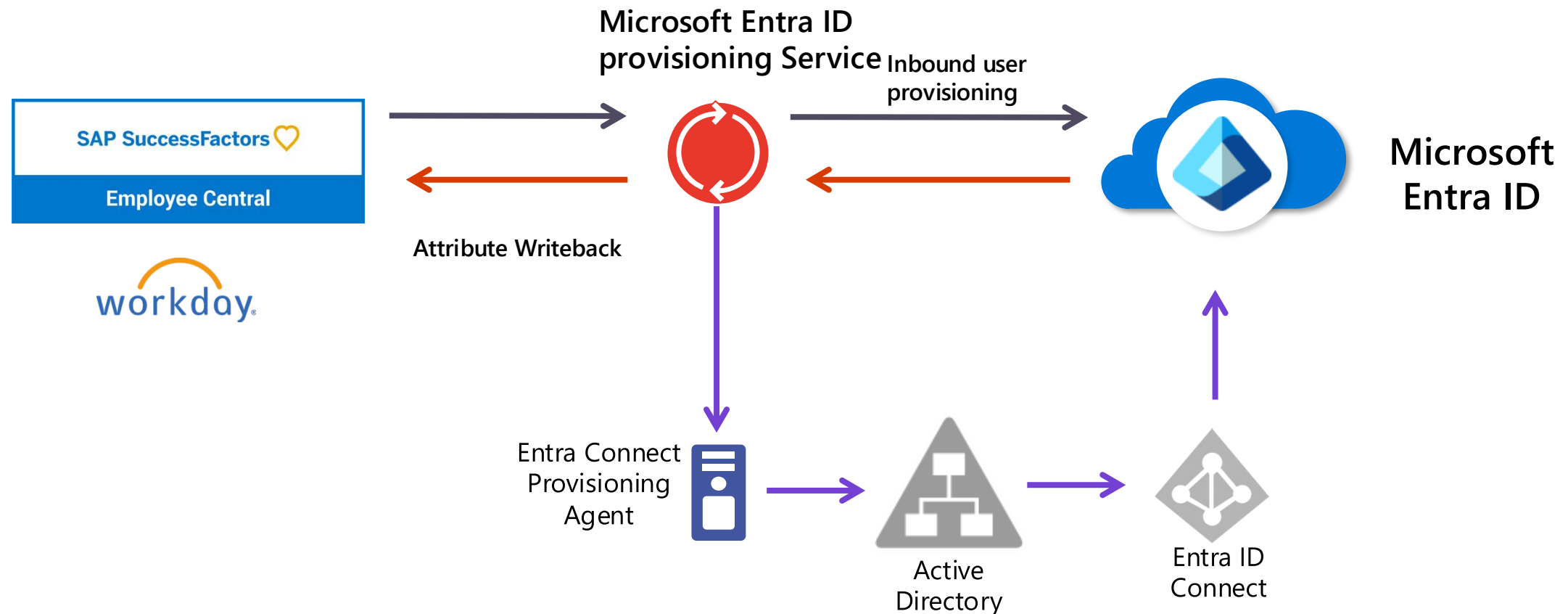
The Solution: Option 1

User Provisioning – Cloud HR to Entra ID

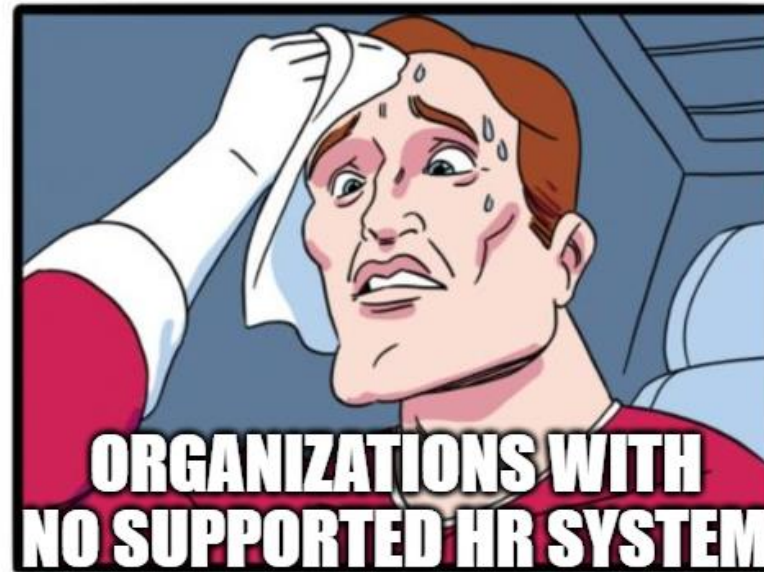


The Solution: Option 2

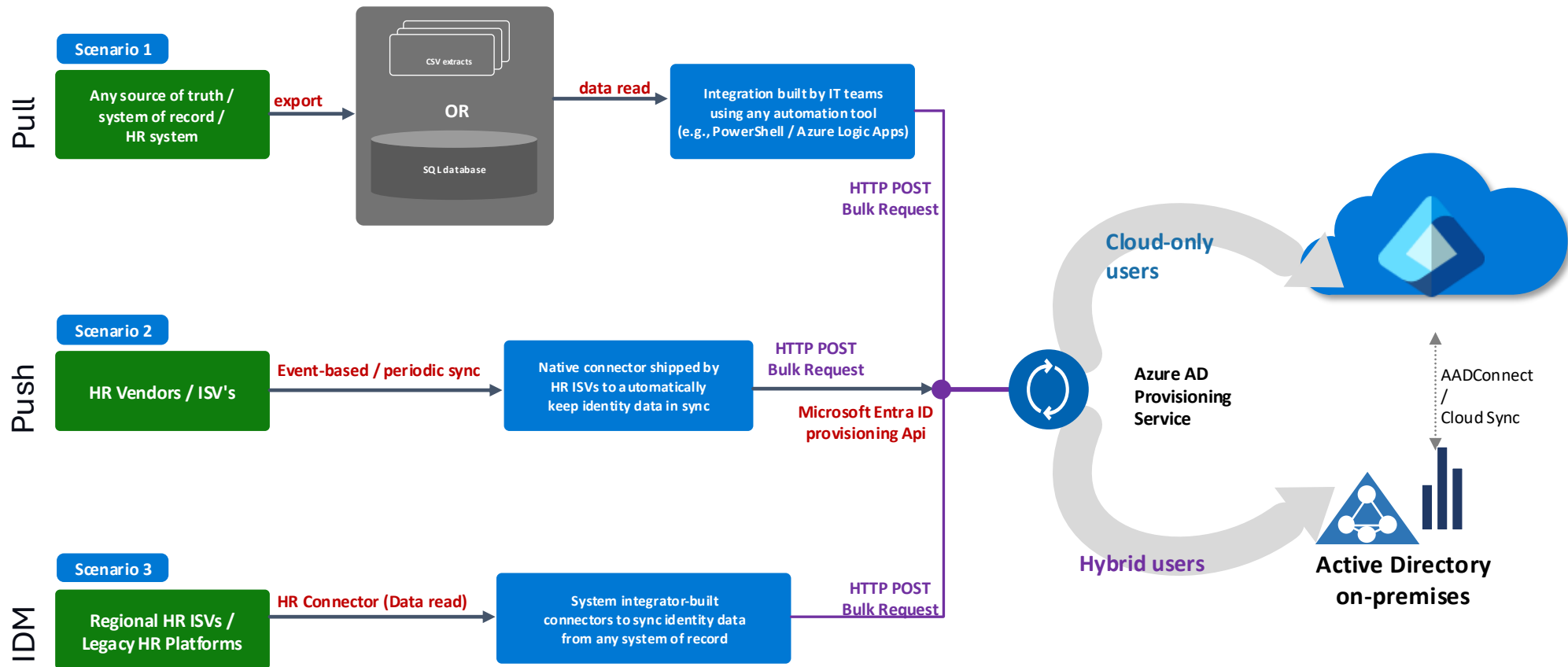
User Provisioning – Cloud HR to Active Directory



The solution: The struggle?



The Solution: API Driven Provisioning



Where Attributes get defined

The screenshot shows the HR Tool interface. On the left is a sidebar with navigation options like Setup, General, Organization, User Access Control, etc. The main area displays a form titled 'Employee' with various fields like EmployeeID, First Name, Last Name, Email ID, Photo, Nick Name, etc. A 'Form Properties' panel on the right shows the 'Form Name' as 'Employee' and the 'Label Name' as 'P_Employee', which is highlighted with a red box.

HR Tool

Attributes get defined directly within the HR Tool.

ZohoOne Attribute	Microsoft Entra ID Attribute
externalId	objectId
active	Not([IsSoftDeleted])
displayName	displayName
title	jobTitle
emails[type eq "work"].value	mail
preferredLanguage	preferredLanguage
userName	userPrincipalName

Entra Provisioning API

IT Administrators map the received values from the Provisioning API to AD & Entra Attributes

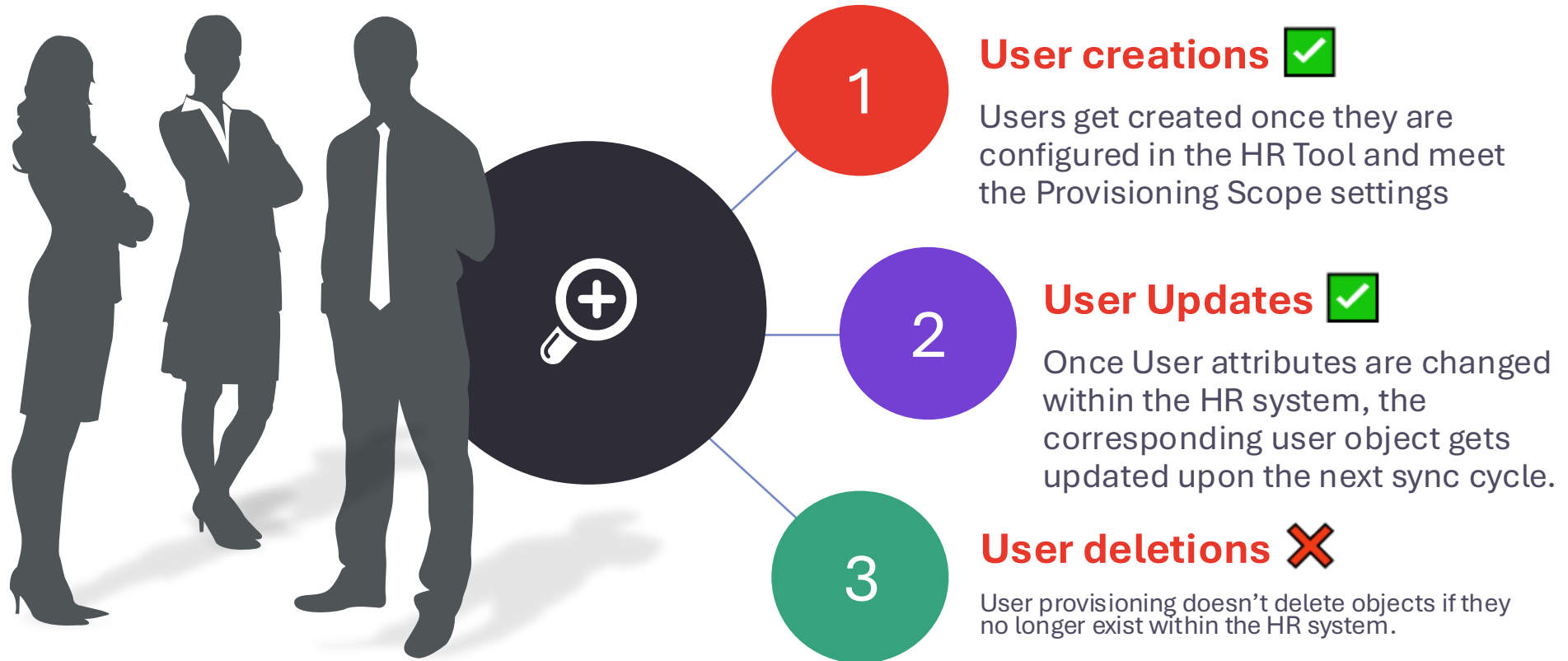
The screenshot shows the 'Attribute mapping' interface in Microsoft Entra ID Connect. It displays a table with columns for 'Target attribute', 'Source attribute', and 'Mapping type'. The 'Users / InetOrgPerson' group is selected, and the 'Add attribute mapping' button is highlighted with a red box.

Target attribute	Source attribute	Mapping type
AccountEnabled	[!(IsHardDeleted)]	Expression
Alias	mailNickname	Direct
AssignedTo	assignedTo	Direct
AuthnReq	authnReq	Direct
City	city	Expression
CompanyName	companyName	Direct
Country	country	Expression
CountryCode	countryCode	Expression
CountryLetterCode	countryLetterCode	Expression
Department	department	Expression
Description	description	Expression
DisplayName	displayName	Direct
DisplayNameSuffix	displayNameSuffix	Direct
DisplayNameSuffixes	displayNameSuffixes	Direct
DisplayNameSuffixes	displayNameSuffixes	Direct
EmployeeID	employeeID	Direct
EmployeeType	employeeType	Direct
ExtensionAttribute1	extensionAttribute1	Expression
ExtensionAttribute10	extensionAttribute10	Expression

Entra ID Connect

IT Administrators map the attributes from AD to Entra ID fields

What Entra ID User Provisioning takes care of



Actions you should take before implementation

Pilot

Start piloting your implementation

Ownership

Define Ownership over the different processes for and edge cases.

Attributes

Define which attributes you require and where they are coming from.

Data cleansing

Ensure data within your HR System & AD is aligned and cleansed.

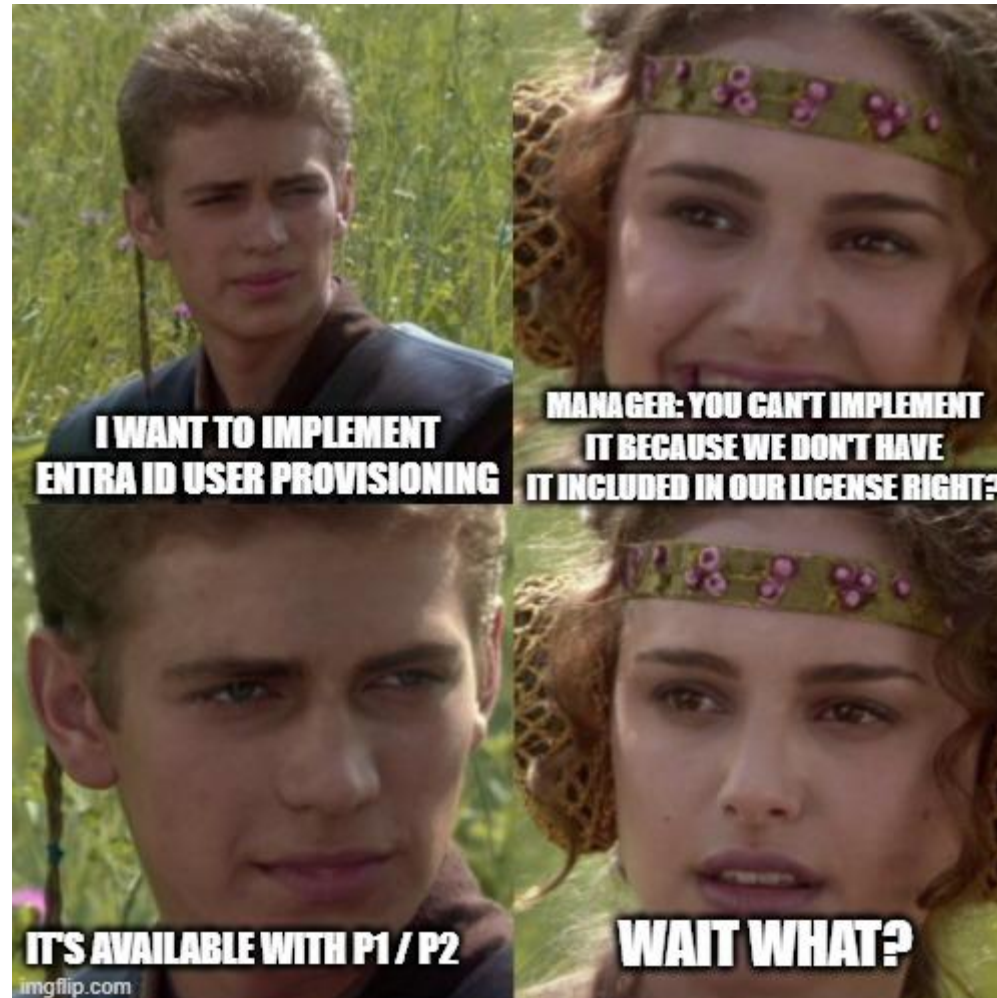


Last but not least?



But what about licensing?

The Solution: Licensing

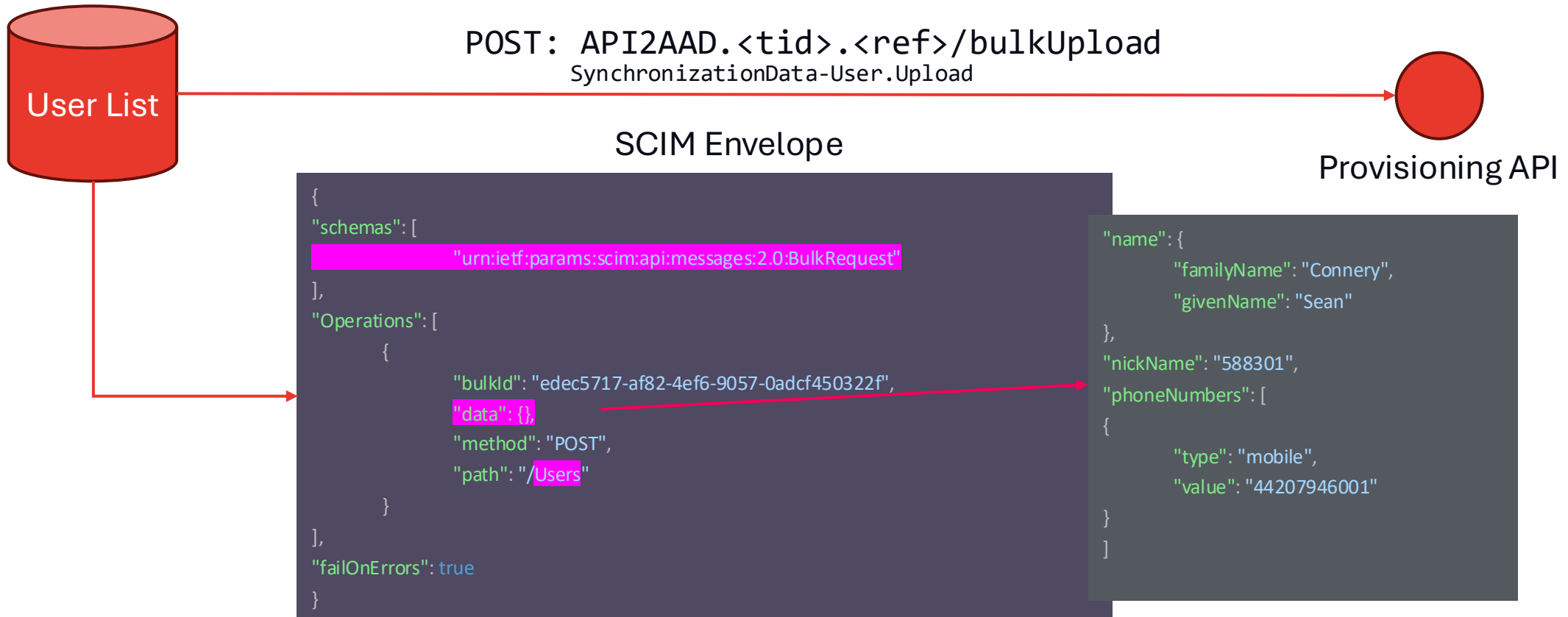


The Solution

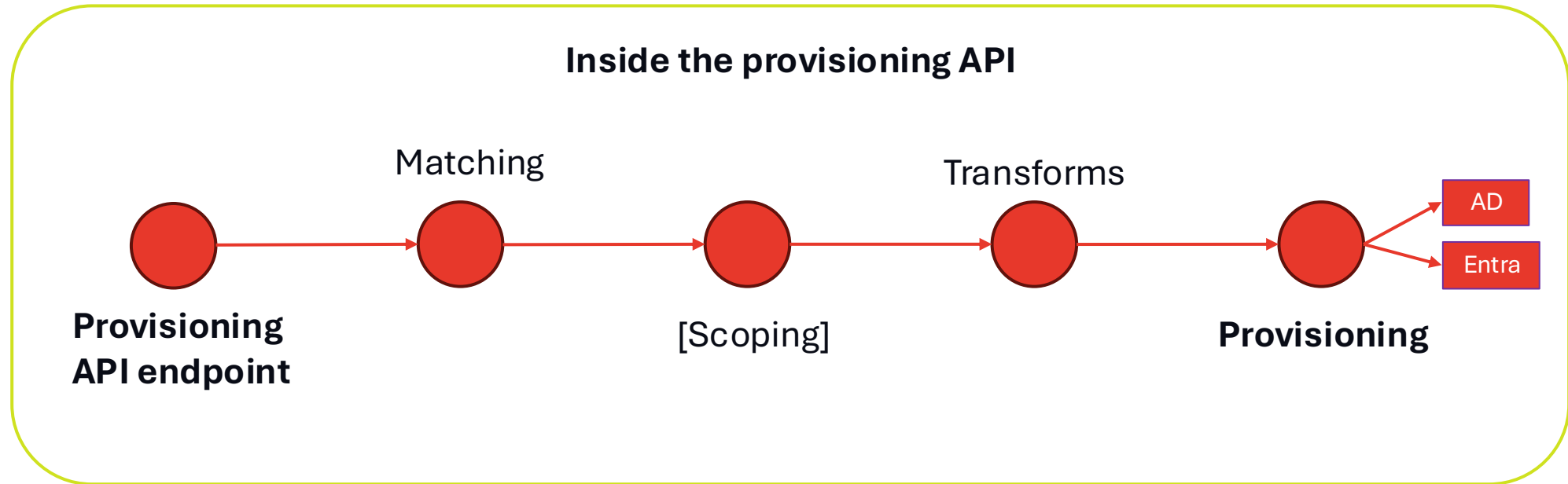


The Solution: SCIM

SCIM: System for Cross-domain Identity Management



The Solution: SCIM + Transforms



Transforms?

```
{
  "schemas": [
    "urn:ietf:params:scim:api:messages:2.0:Error"
  ],
  "detail": "Invalid data!",
  "status": 400,
  "scimType": "invalidSyntax",
  "errors": {
    "urn:ietf:params:scim:schemas:core:2.0:User:userName": [
      "The urn:ietf:params:scim:schemas:core:2.0: user:user name field is required."
    ],
    "urn:ietf:params:scim:schemas:core:2.0:User:emails": [
      "The urn:ietf:params:scim:schemas:core:2.0: user:emails field is required."
    ]
  }
}
```

The Solution: SCIM + Transforms

```
{
  "schemas": [
    "urn:ietf:params:scim:api:messages:2.0:Error"
  ],
  "detail": "Invalid data!",
  "status": 400,
  "scimType": "invalidSyntax",
  "errors": {
    "urn:ietf:params:scim:schemas:core:2.0:User:userName": [
      "The urn:ietf:params:scim:schemas:core:2.0: user:user name field is required."
    ],
    "urn:ietf:params:scim:schemas:core:2.0:User:emails": [
      "The urn:ietf:params:scim:schemas:core:2.0: user:emails field is required."
    ]
  ]
}
```

Source Attribute (API)	Target Attribute (Microsoft Entra ID)	Mapping Type ↓	Matching Precedence
	IsSoftDeleted	None	
Join(" ", [name.givenName], [name.familyName])	displayName	Expression	
Replace([userName], "(?<Suffix>@(.)*", "Suffix", "", ,)	mailNickname	Expression	
ToLower(Join("@", NormalizeDiacritics(StripSpaces(Join(".",	userPrincipalName	Expression	

Transformations

Never ever manage the accountEnabled status



Disable user

[Enable user](#) [Disable user](#)

Disables the user in on prem Active Directory. It might take a few minutes for this change to take effect.

Action details

Submission time
16 Oct 2025 12:11

Submitted by
Attack disruption

Actions status
✓ Completed

Approval ID
968775

Action source
Attack disruption

Transformations

Just provide it while provisioning the user initially.

Users

Mapping type * ⓘ

Constant

Constant attribute (API) * ⓘ

true

Target attribute (Microsoft Entra ID) * ⓘ

accountEnabled

Flow null values ⓘ (Preview)

☐ Flow null values

Apply this mapping ⓘ

Only during object creation

Match objects using this attribute ⓘ

☐ Yes

Provisioning logs

Trace details via provisioning logs

Steps Troubleshooting & Recommendations Modified Properties Summary

- ✓ 1. Import User from API ✓
- ✓ 2. Match User between API and Microsoft Entra ID ✓
- ✓ 3. Determine if User is in scope ✓
- ^ 4. Provision User in Microsoft Entra ID ⓘ

EntrySynchronizationSkip

Result	Skipped
Description	The state of the entry in both the source and target systems already matches the urn:ietf:params:scim:schemas:extension:enterprise:2.0:User '588302' cannot be made.
SkipReason	RedundantExport
ReportableIdentifier	588302

^ 4. Provision User in Microsoft Entra ID ✓

EntryExportAdd

Result	Success
Description	Urn:ietf:params:scim:schemas:extension:enterprise:2.0:User 'baden.ninja@itdrlab.onmicrosoft.com' was created in Microsoft Entra ID
AccountEnabled	true
StreetAddress	Strand 45
City	London
State	London
PostalCode	WC2N 5DU
Country	United Kingdom
Department	Double-0 Section
EmployeeId	588308
DisplayName	Baden Ninja
GivenName	Baden
JobTitle	Field Agent
MailNickname	588308
Manager	ad6b0844-0e84-4c38-915f-bd6ce4ad757b
Mobile	44207946007
PreferredLanguage	en-GB

Demo inbound provisioning

Seeing the magic at work and behind the curtain

<https://github.com/nicolonsky/Entra.IDGOV.PoC>



01

Matching Attribute

No match: duplicates, deletes and chaos

02

Special Characters

Ä,Ö,Ü must be replaced with custom logic.

03

Uniqueness

Unique e-mails and UPNs must be taken care of

04

Uniqueness with multiple instances

Multiple instances of the provisioning APIs do not handle conflicts and provisioning will fail!

05

Multi Divisions & Domains

Different cases are difficult to cover and maintain with if, else and the expression logic.

06

User Provisioning != Lifecycle

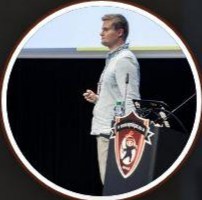
Access Management, Outbound Provisioning, Credential Provisioning, Lifecycle Management are not covered.

Want to learn more about Lifecycle management?



SECURITY IDENTITY

**Better Together:
Enhancing Endpoint &
Security Management
with Entra ID
Governance**



Janic Verboon
Microsoft MVP



Loris Ambrozzo
Security Specialist

14 – 17 Sept 2026
Trafo Baden, Switzerland
[#WPNinjaSummit](#) [summit.wpninjas.global](#)



Wednesday 16.09
09:50 – 10:50
Halle 36.3

The Problem Episode II

Attack of the Cloned Permissions



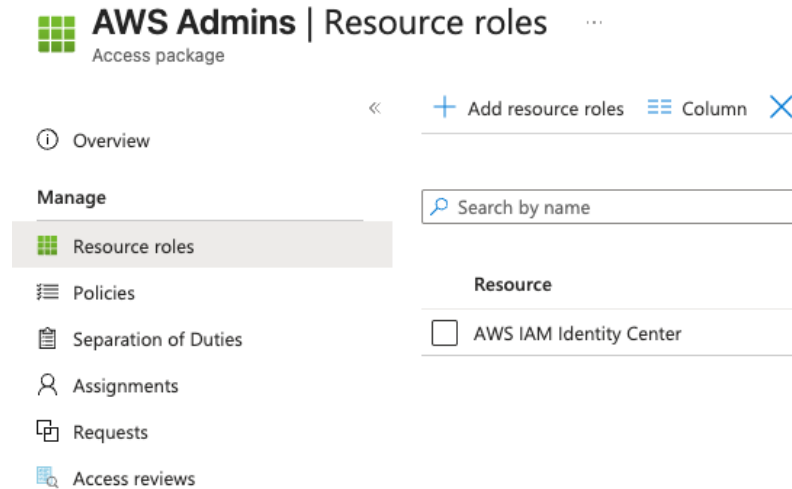
The Problem Part II



The Problem Part II – What we see



The Solution – Outbound Provisioning

A screenshot of the AWS IAM console's 'Provisioning' configuration page for an application. The page contains several input fields: 'Homepage URL' (https://aws.amazon.com/), 'Logo' (AWS logo), 'User access URL' (https://launcher.myapps.microsoft.com/api/signin/fac27507-afc4-46d1...), 'Application ID' (fac27507-afc4-46d1-8973-7de0746fe148), 'Object ID' (f18b7486-0f2f-47af-934e-25be201c90b4), 'Terms of Service Url' (Publisher did not provide this information), 'Privacy Statement Url' (Publisher did not provide this information), and 'Reply URL' (https://eu-central-1.sso.signin.aws/platform/saml/acs/e8788859-dc9a-...). At the bottom, the 'Assignment required?' toggle is set to 'Yes' and is highlighted with a red rectangular border.

Configure Provisioning

If the application supports outbound provisioning, you can automatically create User / Groups within 3rd party apps

Require User assignment

Assign users and groups to the Enterprise app to govern Access

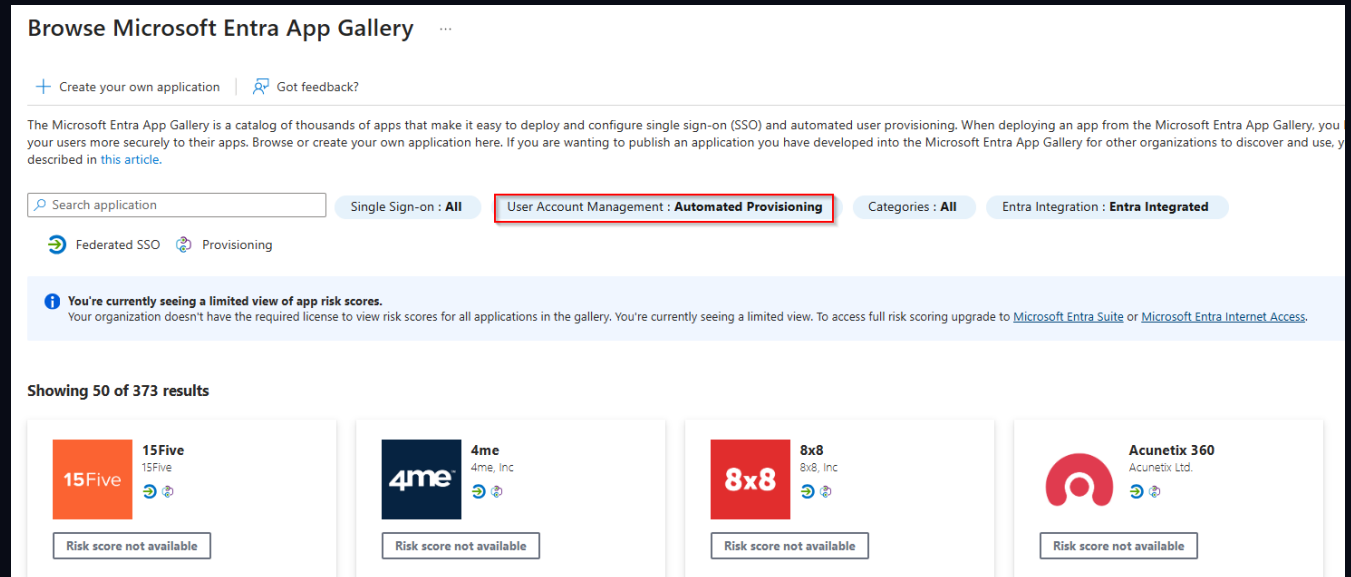
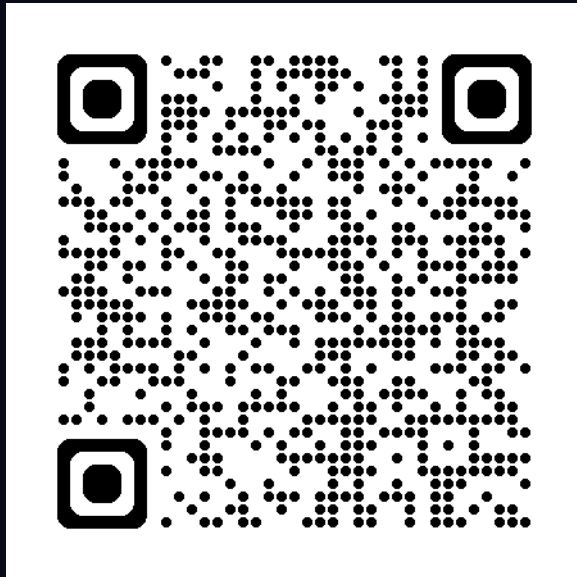
Manage Group Membership

Build Access Packages for users to get added to the Enterprise Apps.

Find apps that support outbound provisioning



```
pwsh ./Invoke-SCIMGalleryAppReport.ps1
```



DisplayName	AppId	ObjectId	ProvisioningState	TargetDirectory	SupportsUserProvisioning	SupportedUserAction	SupportsGroupProvisioning	SupportedGroupActions
Zoho One (DA)	bdac29e8-971804537a-4		Enabled	ZohoOne	TRUE	Add,Update,Delete	TRUE	Add,Update,Delete
Meta Work Accounts	8b7ac83d-21321163bd-e		Disabled	N/A	FALSE	N/A	FALSE	N/A
Zoho One	e0c58779-2fc40d1ceca-6		Enabled	ZohoOne	TRUE	Add,Update,Delete	TRUE	Add,Update,Delete
Meta Work Accounts	1e833a1f-4a471fb8637-43		Enabled	FacebookWorkAccounts	TRUE	Add,Update	FALSE	Add,Update,Delete
API-driven provisioning to on-premises Active Directory	c3f6f100-3b2c4db33ce-8		Enabled	On Premises Active Directory	FALSE	Add,Update	FALSE	Add,Update,Delete
Meta Work Accounts	8f2ec480-b84f6fc7dfc-ea2		Enabled	FacebookWorkAccounts	TRUE	Add,Update	FALSE	Add,Update,Delete
Zoho People: API-driven provisioning to Microsoft Entra ID	5f6f498c-1b0fd2f861d-c9		Enabled	Microsoft Entra ID	FALSE	Add,Update	FALSE	Add,Update,Delete

The Solution – Access Packages



Govern the whole access lifecycle for groups, apps, directory roles via Access Packages.

A screenshot of the Microsoft My Access portal. The browser address bar shows the URL "https://myaccess.microsoft.com/@itdrlab.onmicrosoft.com/#/access-packages". The page title is "Access packages". Below the title, there is a search bar and a list of packages. The "Available (1)" tab is selected, showing a table with one package: "AWS Admins". The table has columns for Name, Description, Resources, and Actions. The "AWS Admins" package has a description of "Grant AWS Admin Permissions" and a "Request" button in the Actions column. The left sidebar shows the user's profile (Sean Connery) and navigation links for Home, My Account, My Apps, My Groups, My Access, Overview, and Access packages.

A screenshot of the "AWS Admins" access package details modal. The modal has a title bar with "AWS Admins" and a close button. Below the title bar, there is a message: "You already have access to 'AWS Admins'. View access package". The modal has two tabs: "Request details" and "Resources", with "Resources" selected. Below the tabs, there is a "View by:" dropdown menu showing "All resources (1)". At the bottom, there is a section titled "AWS IAM Identity Center" with the text "Application - Role: User".

Access Package recommended approach



Auto Assign Access Packages*

Automatically assign Access packages based on Entra User attributes

Let Managers request Access for users*

Let Managers request access for their reporters.

Let Users request Access Packages

Let users request dedicated access using the MyAccess portal.

Define Access packages

Define which Access Packages you require within your environment.



* Requires an Entra Identity Governance licensing

Demo outbound provisioning

Seeing the magic at work and behind the curtain



Pitfalls Episode II



01

SaaS App Penalty

SSO / Provisioning features are often behind a pay wall: <https://sso.tax/>

04

Group Claims

Use immutable identifiers and not display names.

02

Sync Scope

Ensure that the sync scope is configured to only assigned users and groups

05

SCIM Token

Ensure that SCIM Tokens / Credentials are monitored and renewed on time.

03

Nested Groups

Members of a nested group are not provisioned to the third party app.

06

SCIM ≠ SCIM

There are different SCIM standards and the implementation might not be the same for every third-party application.

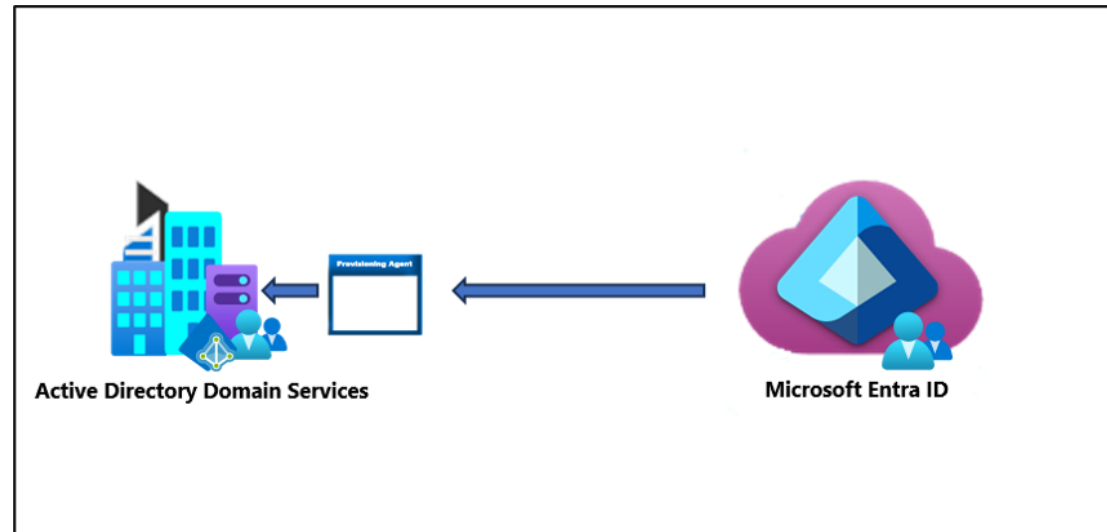
Troubleshooting can be challenging.



Cool but what about On-premise groups?

Entitlement Management

The Entra ID Provisioning Agent can be used to write-back groups from Entra ID to on-premise Active Directory. Entra ID becomes the master for managing those groups.

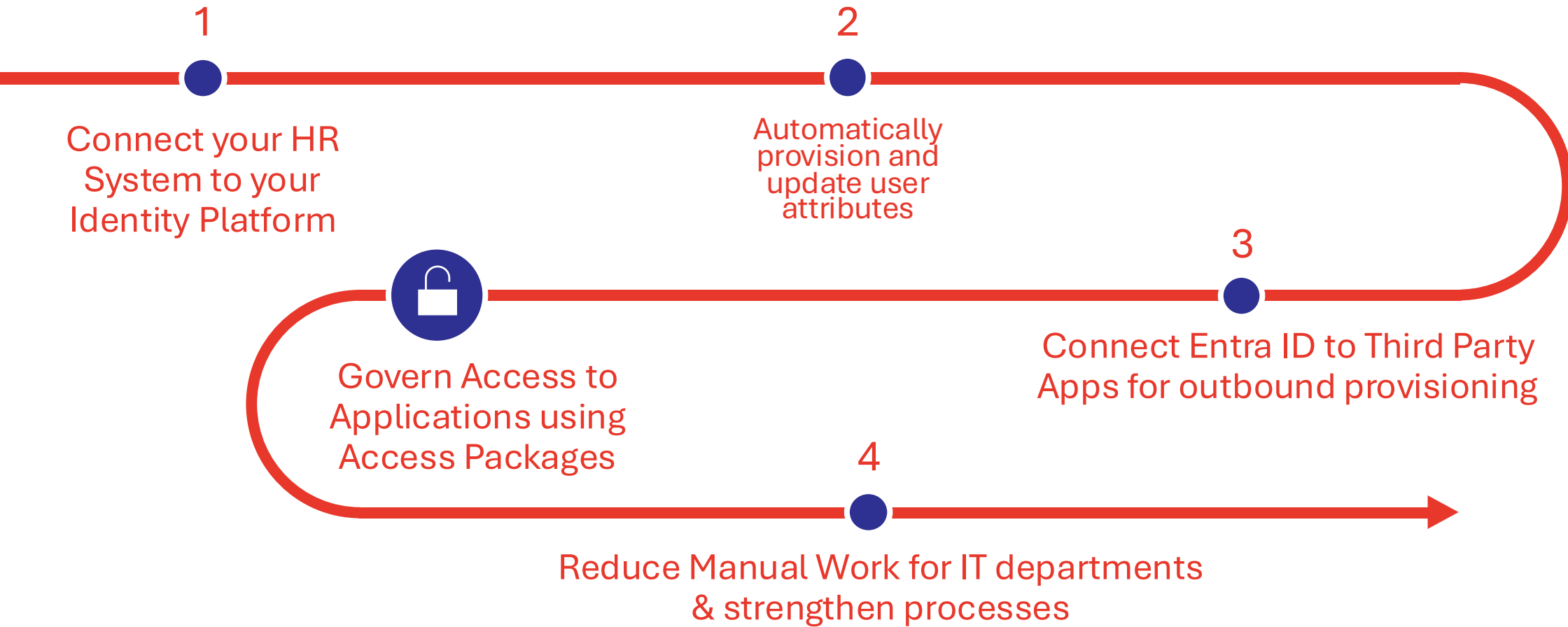


Important: Only 1 target OU is supported at the moment!

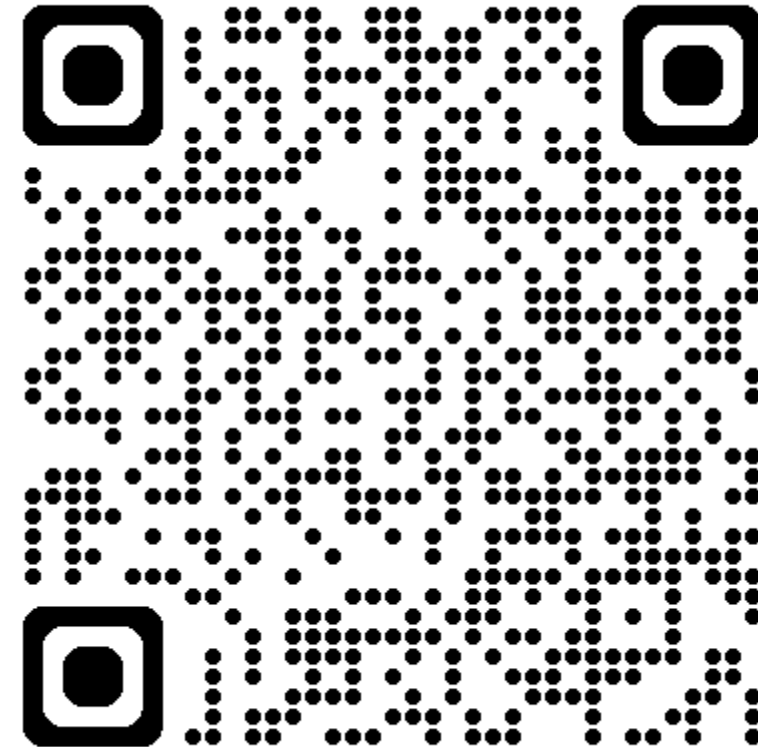
Summary



Summary



Call to action



[nicolonsky/Entra.IDGOV.PoC:](https://nicolonsky/Entra.IDGOV.PoC:Microsoft%20Entra%20Identity%20Governance%20PoC)
Microsoft Entra Identity
Governance PoC

Thank you to our sponsors!



PLATINUM SPONSORS

glueck■kanja



Recast

2Pint



GOLD SPONSORS

control up



eido

THREATLOCKER®
ZERO TRUST PLATFORM

inforcer

baseVISION
Trusted Swiss Cybersecurity



nerdio

SILVER SPONSORS



Apento



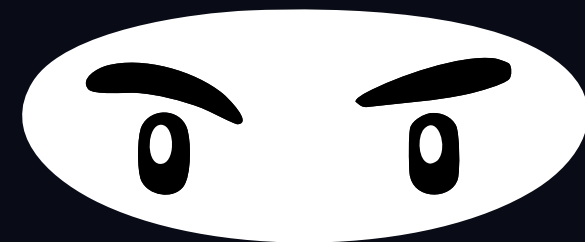
ugurlabs

Thank You, Ninjas!

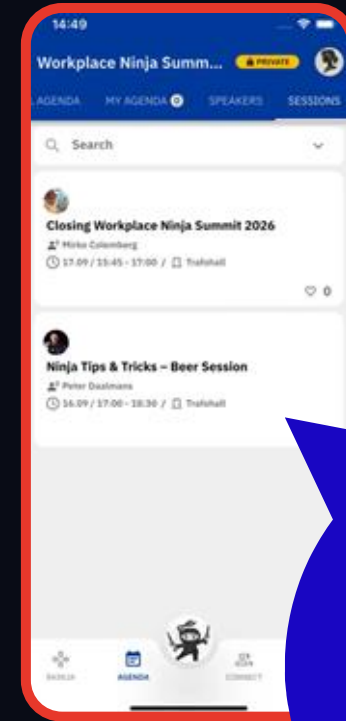
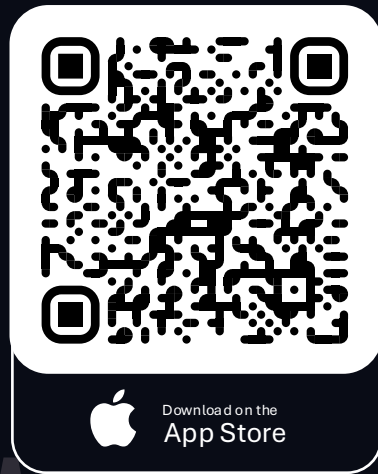
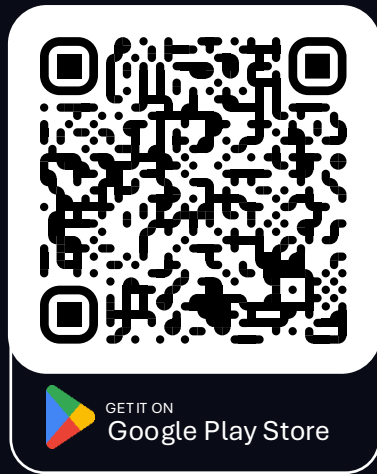


See You
Next Year!

SUMMIT
SUMMIT
SUMMIT
SUMMIT
SUMMIT



Download the app and never miss any updates



We appreciate
your feedback!