NIC

EMPOWER

November 13-15, Oslo Spektrum

Jan Vidar Elven

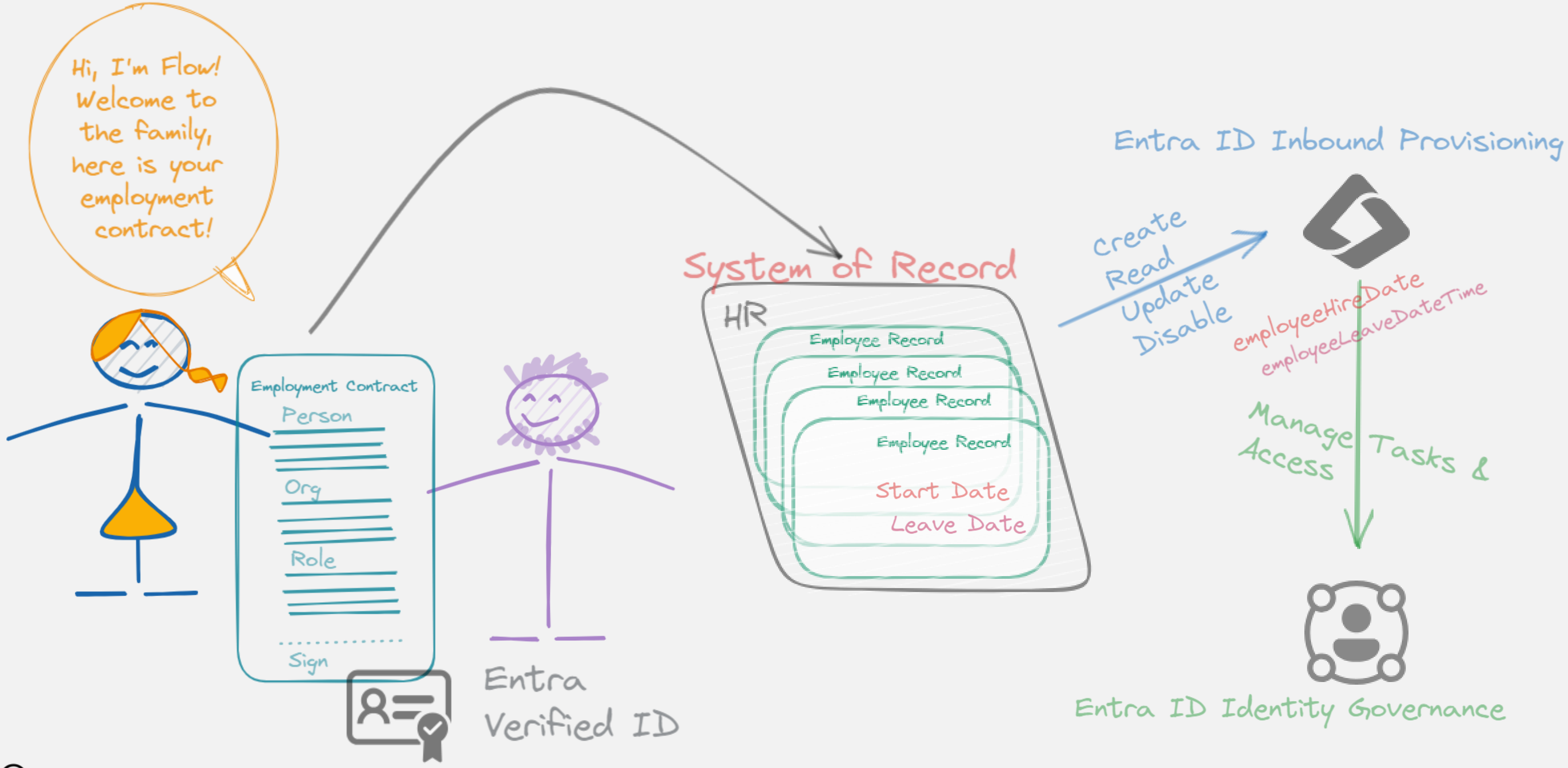
User Lifecycle: Inbound Provisioning and Governance with Microsoft Entra ID Governance and Workflows

Senior Architect @ Evidi | MVP Security | @JanVidarElven

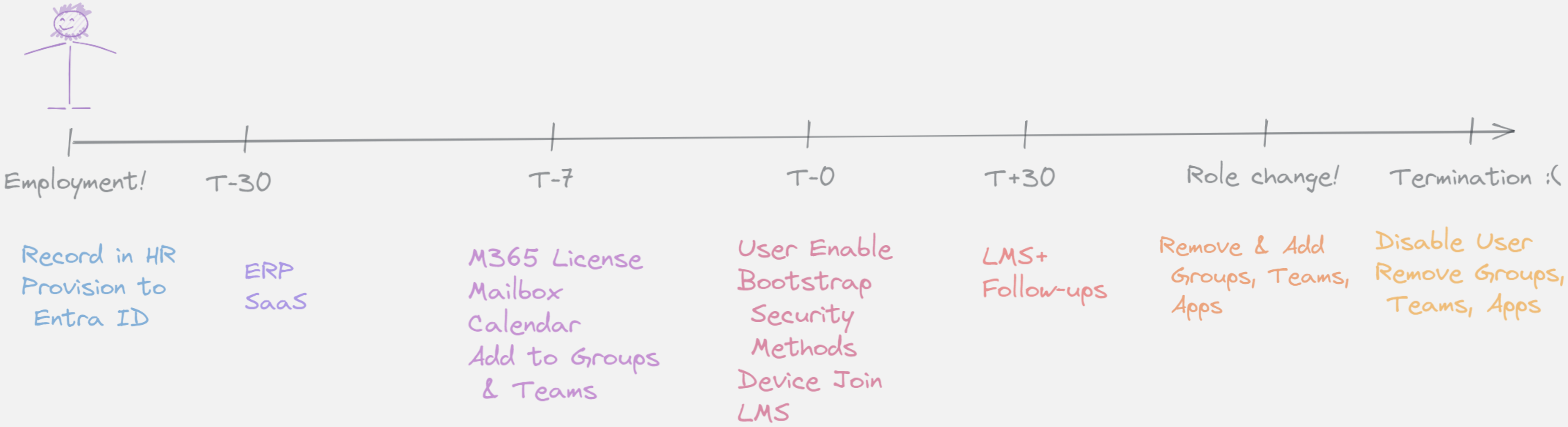
NIC
EMPOWER

Meet Wild River!

A new recent hire to the Elven Organization!


Hi, I'm Flow! Welcome to the family, here is your employment contract!
Employment Contract
Person
Org
Role
Sign
Entra Verified ID
System of Record
HR
Employee Record
Employee Record
Employee Record
Employee Record
Start Date
Leave Date
Create
Read
Update
Disable
Entra ID Inbound Provisioning
employeeHireDate
employeeLeaveDateTime
Manage Tasks & Access
Entra ID Identity Governance

Identity & Access Lifecycle



Employment!

Record in HR
Provision to
Entra ID

T-30

ERP
SaaS

T-7

M365 License
Mailbox
Calendar
Add to Groups
& Teams

T-0

User Enable
Bootstrap
Security
Methods
Device Join
LMS

T+30

LMS+
Follow-ups

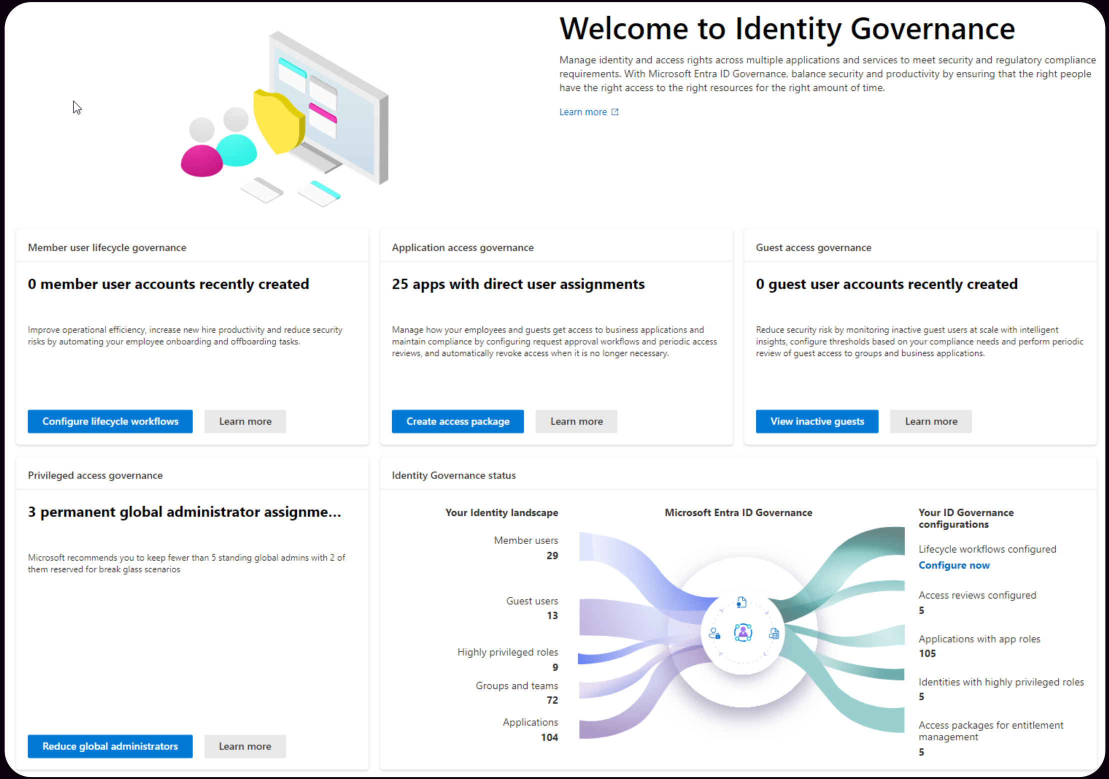
Role change!

Remove & Add
Groups, Teams,
Apps

Termination :(

Disable User
Remove Groups,
Teams, Apps

Introducing Entra ID Governance!



Welcome to Identity Governance

Manage identity and access rights across multiple applications and services to meet security and regulatory compliance requirements. With Microsoft Entra ID Governance, balance security and productivity by ensuring that the right people have the right access to the right resources for the right amount of time.

Learn more

Member user lifecycle governance

0 member user accounts recently created

Improve operational efficiency, increase new hire productivity and reduce security risks by automating your employee onboarding and offboarding tasks.

Configure lifecycle workflows | Learn more

Application access governance

25 apps with direct user assignments

Manage how your employees and guests get access to business applications and maintain compliance by configuring request approval workflows and periodic access reviews, and automatically revoke access when it is no longer necessary.

Create access package | Learn more

Guest access governance

0 guest user accounts recently created

Reduce security risk by monitoring inactive guest users at scale with intelligent insights, configure thresholds based on your compliance needs and perform periodic review of guest access to groups and business applications.

View inactive guests | Learn more

Privileged access governance

3 permanent global administrator assignme...

Microsoft recommends you to keep fewer than 5 standing global admins with 2 of them reserved for break glass scenarios

Reduce global administrators | Learn more

Identity Governance status

Your Identity landscape

Member users 29

Guest users 13

Highly privileged roles 9

Groups and teams 72

Applications 104

Microsoft Entra ID Governance

Your ID Governance configurations

Lifecycle workflows configured
Configure now

Access reviews configured 5

Applications with app roles 105

Identities with highly privileged roles 5

Access packages for entitlement management 5

NIC
EMPOWER

IAM and Identity Governance Core with Entra ID

Service Catalog

- Entitlement Management
- Resource Access Package Requests
- Self Service
- Approvals
- Custom Extensions

Privileged Access

- Entra ID Privileged Identity Management (PIM)
  - Entra ID Roles
  - Entra Groups
  - Azure RBAC
- Endpoint Privilege Management (EPM)
- LAPS
- PAW

Access Governance

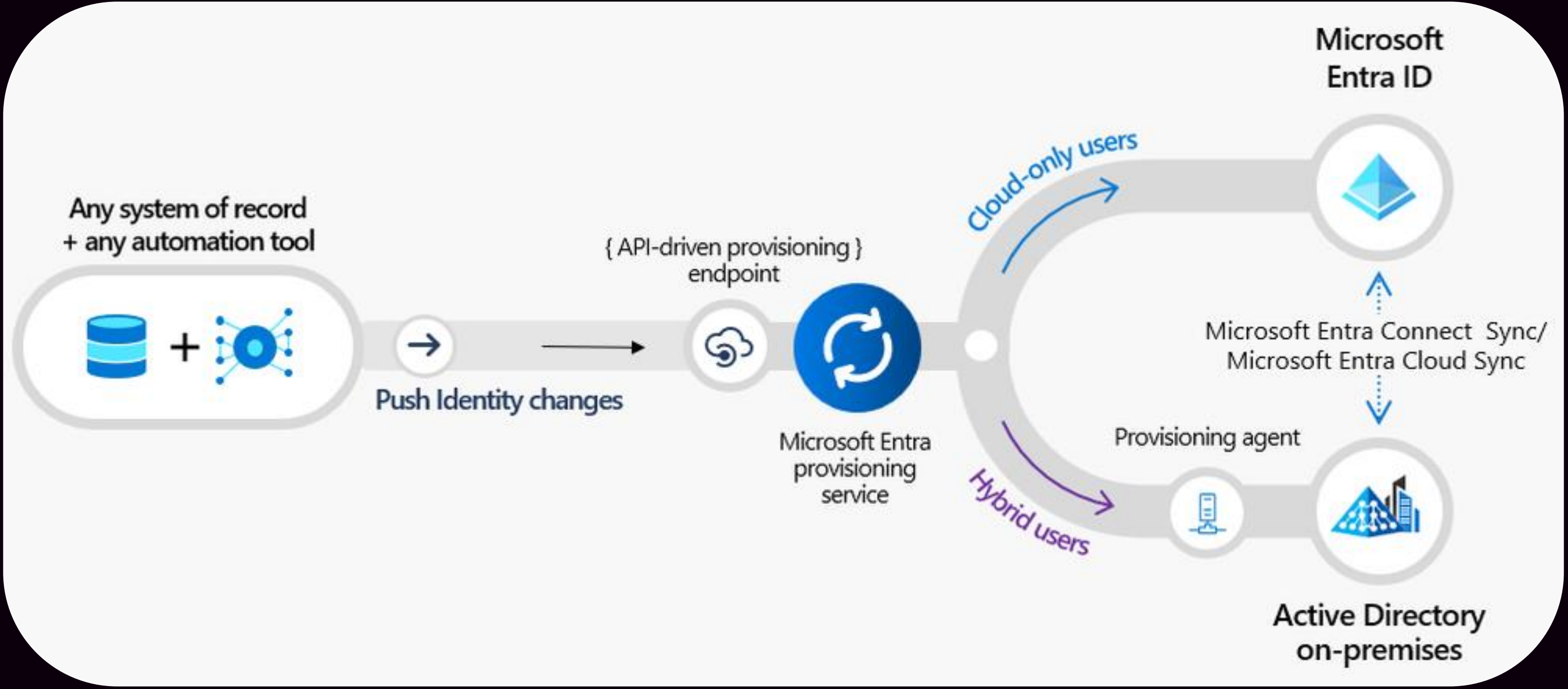
- Access Reviews
- Terms of Use

Lifecycle Workflows

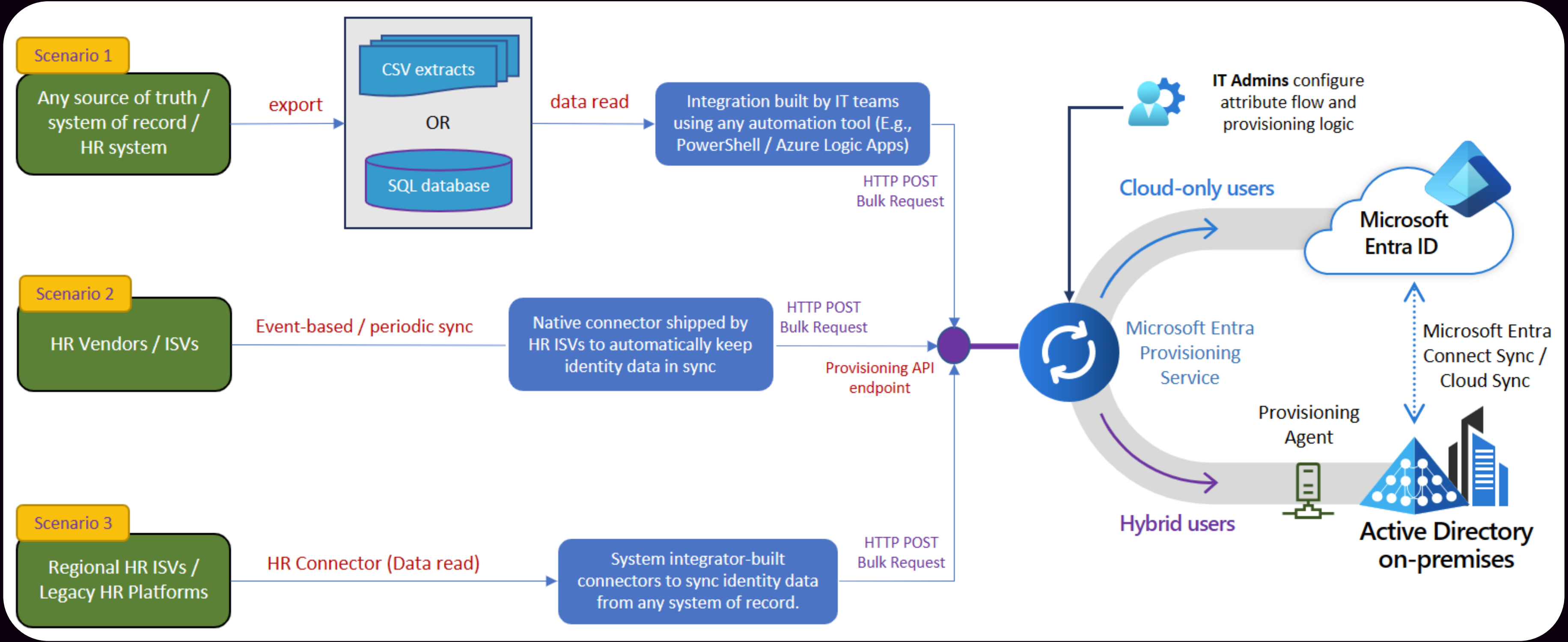
- Inbound Provisioning
- Joiner
- Leaver
- Mover
- Custom Extensions

NIC
EMPOWER

Entra ID Inbound Provisioning API



Inbound Provisioning Scenarios



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

Provisioning API endpoint

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

Microsoft Entra ID

Microsoft Entra Provisioning Service

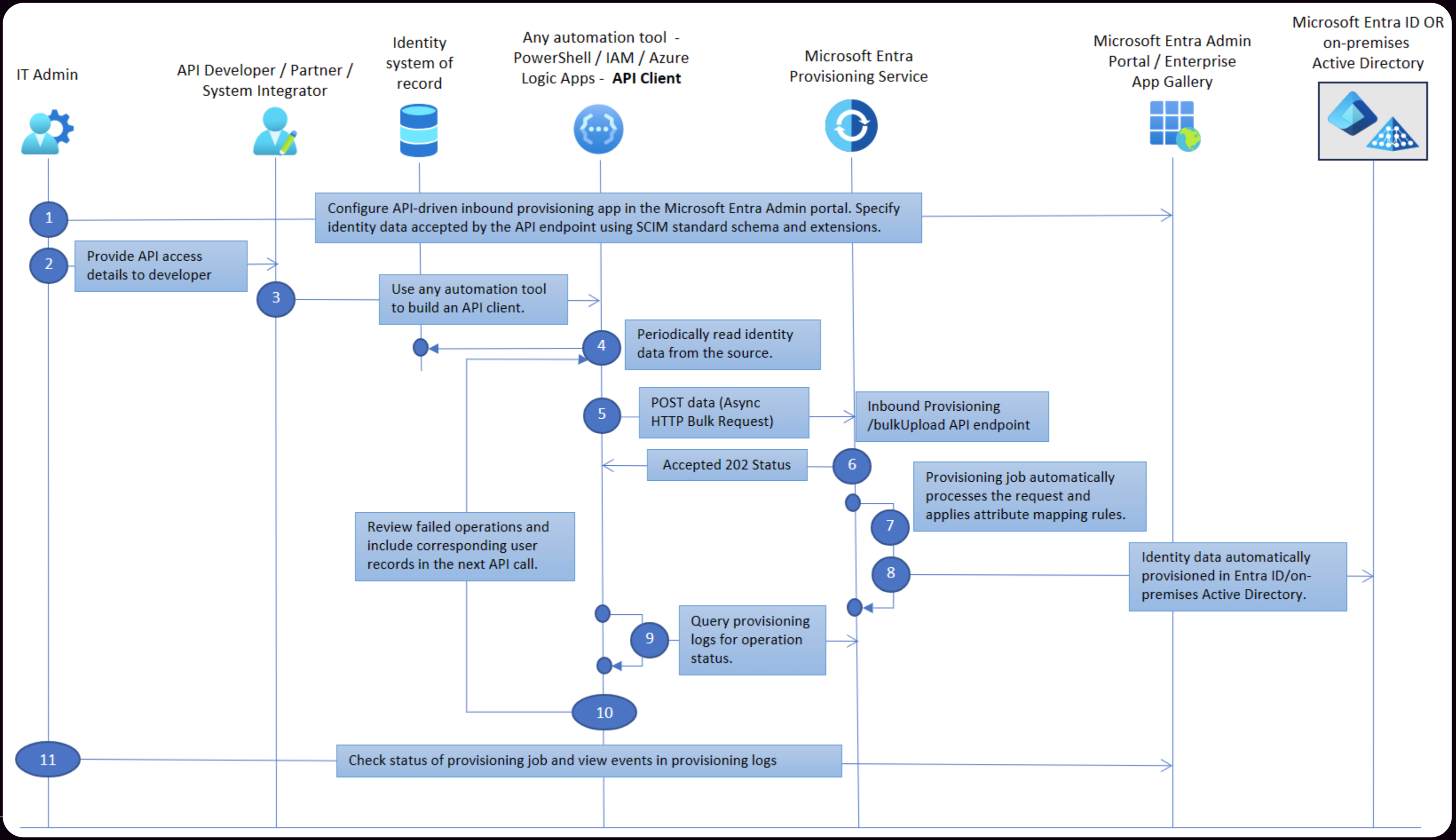
Microsoft Entra Connect Sync / Cloud Sync

Provisioning Agent

Hybrid users

Active Directory on-premises

Inbound Provisioning Deployment Process



IT Admin

API Developer / Partner / System Integrator

Identity system of record

Any automation tool - PowerShell / IAM / Azure Logic Apps - **API Client**

Microsoft Entra Provisioning Service

Microsoft Entra Admin Portal / Enterprise App Gallery

Microsoft Entra ID OR on-premises Active Directory

1 Configure API-driven inbound provisioning app in the Microsoft Entra Admin portal. Specify identity data accepted by the API endpoint using SCIM standard schema and extensions.

2 Provide API access details to developer

3 Use any automation tool to build an API client.

4 Periodically read identity data from the source.

5 POST data (Async HTTP Bulk Request)

Inbound Provisioning /bulkUpload API endpoint

6 Accepted 202 Status

7 Provisioning job automatically processes the request and applies attribute mapping rules.

8 Identity data automatically provisioned in Entra ID/on-premises Active Directory.

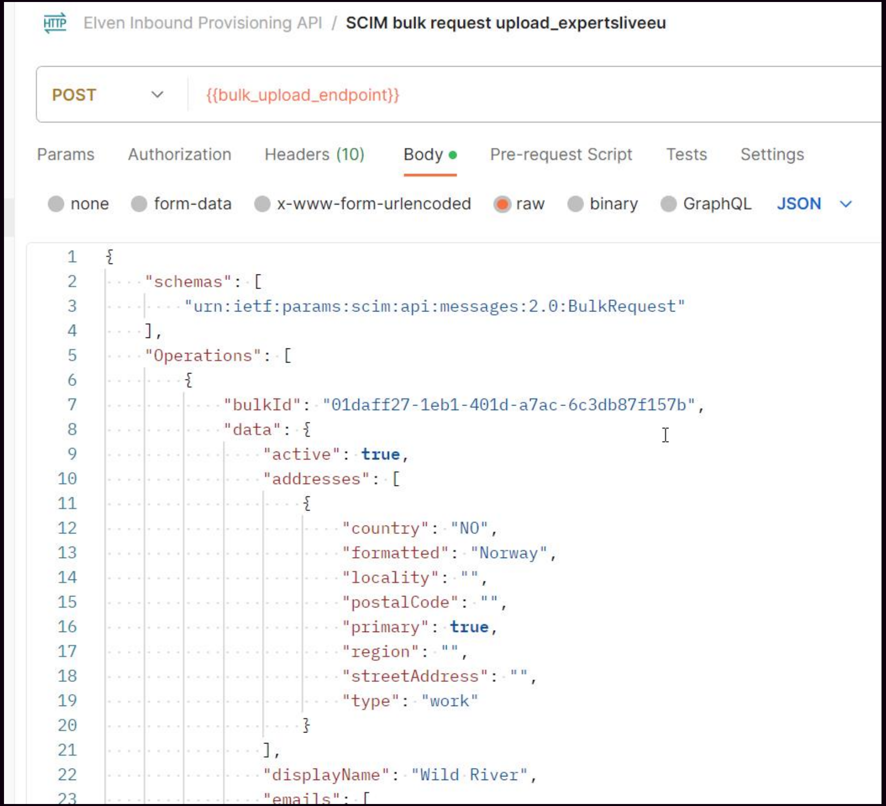
9 Query provisioning logs for operation status.

10 Review failed operations and include corresponding user records in the next API call.

11 Check status of provisioning job and view events in provisioning logs

SCIM

- Graph API
  - Permission Scope & Role
    - SynchronizationData-User.Upload
- POST /bulkUpload
- Schema extensions
- Attribute Mapping



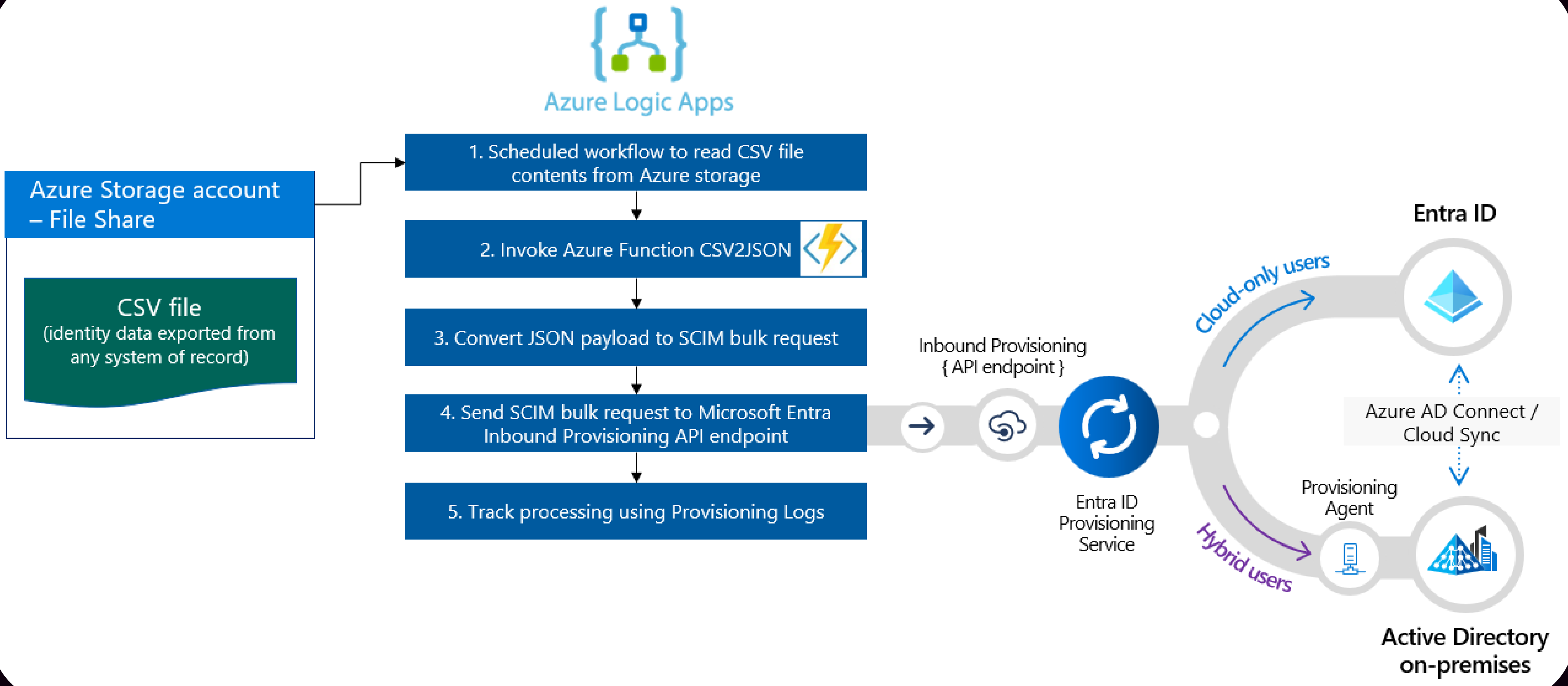
Elven Inbound Provisioning API / **SCIM bulk request upload_expertsliveeu**

POST {{bulk_upload_endpoint}}

○ none ○ form-data ○ x-www-form-urlencoded ● raw ○ binary ○ GraphQL JSON

```json
{
    "schemas": [
        "urn:ietf:params:scim:api:messages:2.0:BulkRequest"
    ],
    "Operations": [
        {
            "bulkId": "01daff27-1eb1-401d-a7ac-6c3db87f157b",
            "data": {
                "active": true,
                "addresses": [
                    {
                        "country": "NO",
                        "formatted": "Norway",
                        "locality": "",
                        "postalCode": "",
                        "primary": true,
                        "region": "",
                        "streetAddress": "",
                        "type": "work"
                    }
                ],
                "displayName": "Wild River",
                "emails": [
```

Start Concept for Inbound Provisioning



Azure Logic Apps

Azure Storage account – File Share

CSV file
(identity data exported from any system of record)

1. Scheduled workflow to read CSV file contents from Azure storage

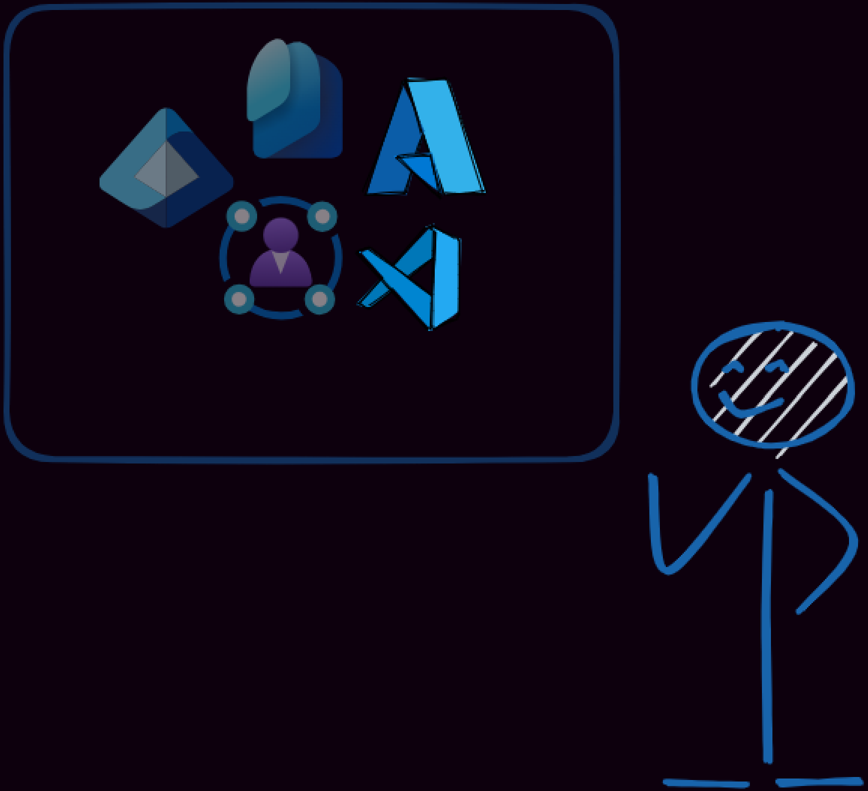
2. Invoke Azure Function CSV2JSON

3. Convert JSON payload to SCIM bulk request

4. Send SCIM bulk request to Microsoft Entra Inbound Provisioning API endpoint

5. Track processing using Provisioning Logs

Demo Inbound Provisioning



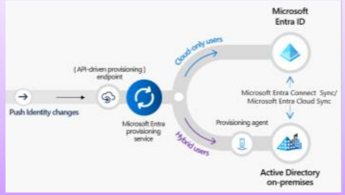
Summarize - Where are we? : 2 phases and need for integration..

- PHASE 1:
  - Onboarding/offboarding employees
    - Signing, Signicat, Entra Verified ID, ++
  - M&A
  - System of Record/Source of Authority
    - Multiple?
    - Your HR
      - StartDate
      - EndDate
    - + others??

- PHASE 2:
  - User automatic provisioning in Entra ID
  - **CRU**D
  - Lifecycle Workflows:
    - Joiner
    - Mover
    - Leaver
  - employeeHireDate
  - employeeLeaveDateTime

DSP -> Identity Integration

Inbound Provisioning ->

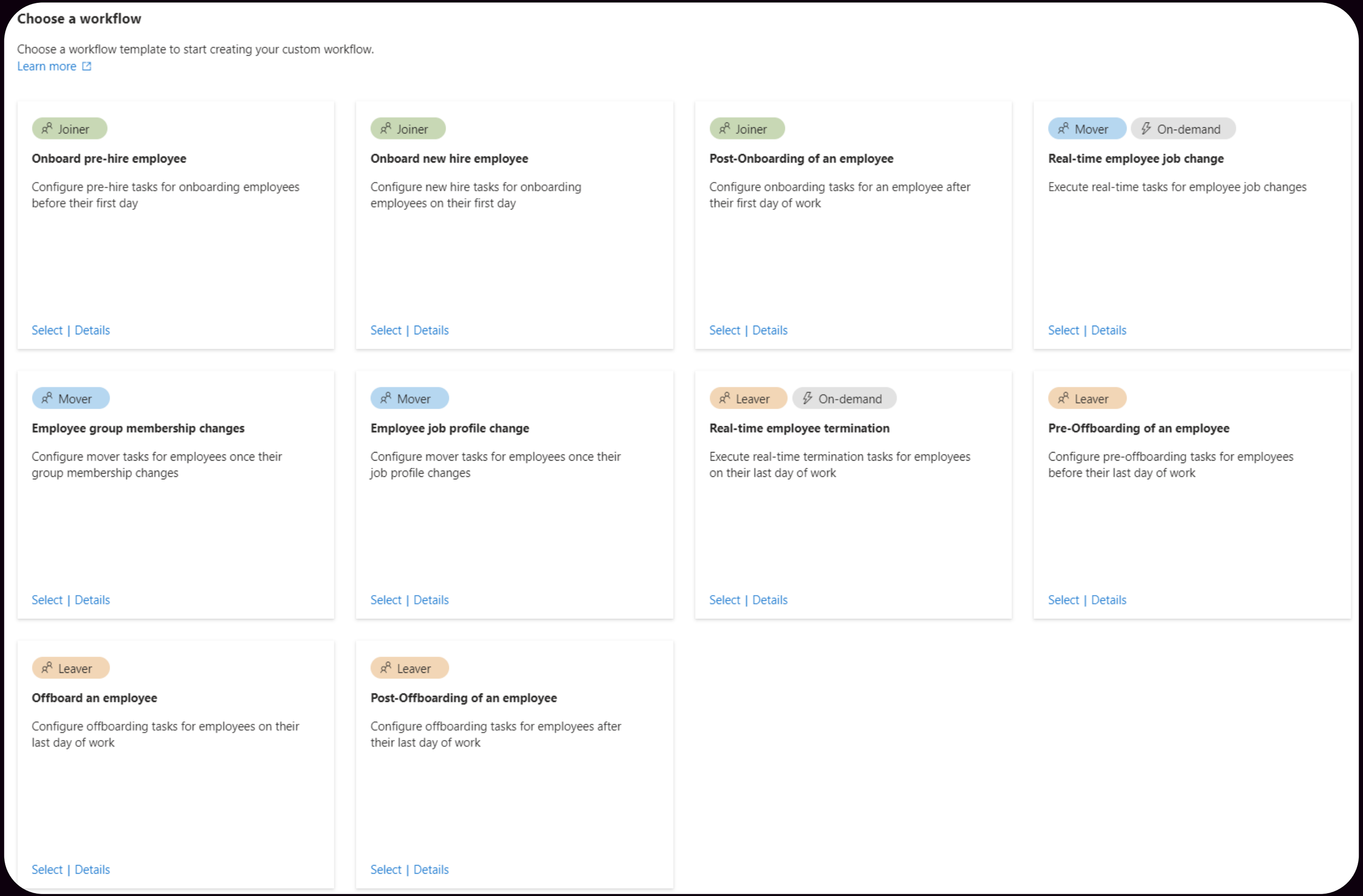

Microsoft Entra ID
Cloud-only users
(API-driven provisioning) endpoint
Push Identity changes
Microsoft Entra provisioning service
Microsoft Entra Connect Sync/ Microsoft Entra Cloud Sync
Provisioning agent
Hybrid users
Active Directory on-premises

Lifecycle Scenarios

Joiner
Hi, I'm new!
Mover
I have a new Title and changed my Role!
Leaver
It's been fun but it's time to go!

NIC EMPOWER

Lifecycle Workflows in Entra ID Governance



Choose a workflow

Choose a workflow template to start creating your custom workflow.
Learn more

Joiner

Onboard pre-hire employee

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

Select | Details

Joiner

Onboard new hire employee

Configure new hire tasks for onboarding employees on their first day

Select | Details

Joiner

Post-Onboarding of an employee

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

Select | Details

Mover On-demand

Real-time employee job change

Execute real-time tasks for employee job changes

Select | Details

Mover

Employee group membership changes

Configure mover tasks for employees once their group membership changes

Select | Details

Mover

Employee job profile change

Configure mover tasks for employees once their job profile changes

Select | Details

Leaver On-demand

Real-time employee termination

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

Select | Details

Leaver

Pre-Offboarding of an employee

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

Select | Details

Leaver

Offboard an employee

Configure offboarding tasks for employees on their last day of work

Select | Details

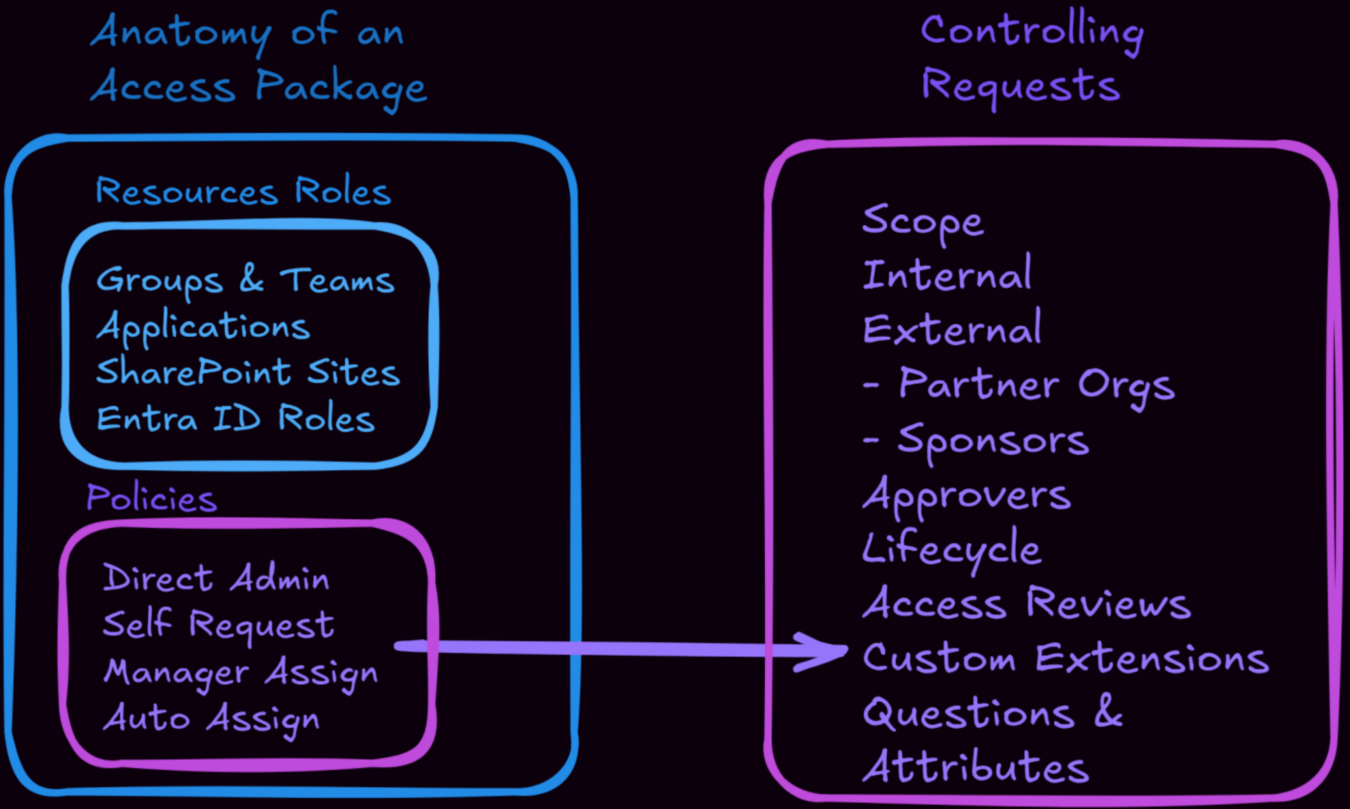
Leaver

Post-Offboarding of an employee

Configure offboarding tasks for employees after their last day of work

Select | Details

Entitlement Management - Access Packages



Anatomy of an Access Package

Resources Roles

- Groups & Teams
- Applications
- SharePoint Sites
- Entra ID Roles

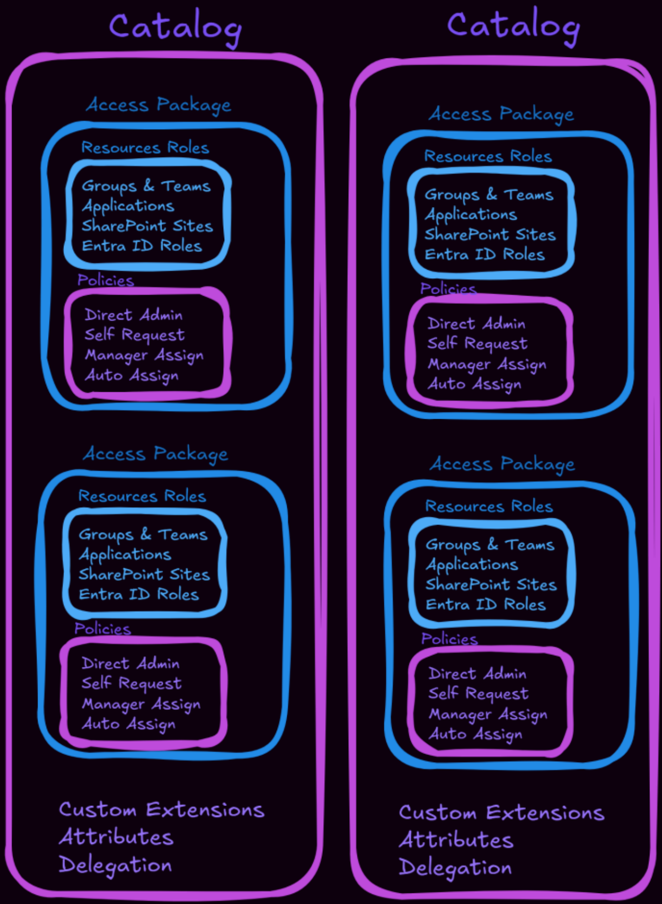
Policies

- Direct Admin
- Self Request
- Manager Assign
- Auto Assign

Controlling Requests

- Scope
- Internal
- External
  - Partner Orgs
  - Sponsors
- Approvers
- Lifecycle
- Access Reviews
- Custom Extensions
- Questions & Attributes

Entitlement Management - Catalogs



Catalog

Access Package

Resources Roles

Groups & Teams
Applications
SharePoint Sites
Entra ID Roles

Policies

Direct Admin
Self Request
Manager Assign
Auto Assign

Access Package

Resources Roles

Groups & Teams
Applications
SharePoint Sites
Entra ID Roles

Policies

Direct Admin
Self Request
Manager Assign
Auto Assign

Custom Extensions
Attributes
Delegation

Catalog

Access Package

Resources Roles

Groups & Teams
Applications
SharePoint Sites
Entra ID Roles

Policies

Direct Admin
Self Request
Manager Assign
Auto Assign

Access Package

Resources Roles

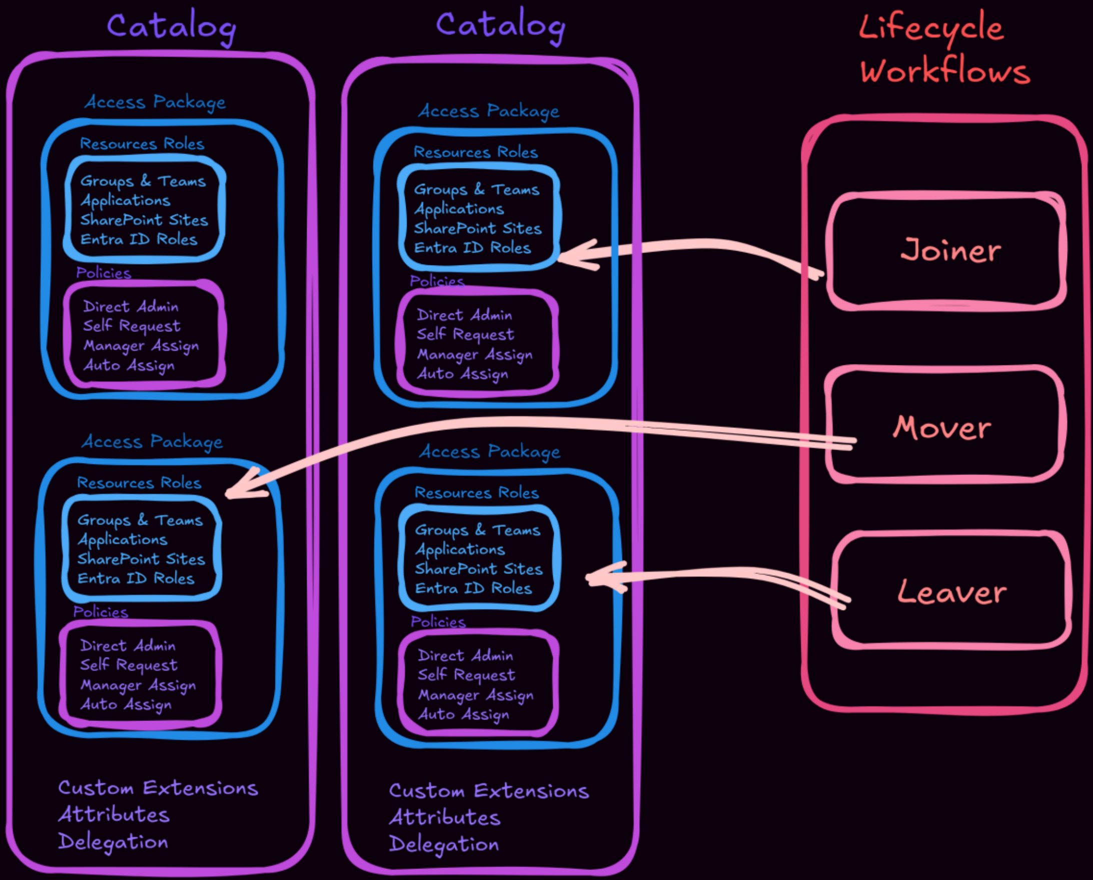
Groups & Teams
Applications
SharePoint Sites
Entra ID Roles

Policies

Direct Admin
Self Request
Manager Assign
Auto Assign

Custom Extensions
Attributes
Delegation

Access Packages – Lifecycle Workflows



Catalog

Access Package

Resources Roles

Groups & Teams
Applications
SharePoint Sites
Entra ID Roles

Policies

Direct Admin
Self Request
Manager Assign
Auto Assign

Access Package

Resources Roles

Groups & Teams
Applications
SharePoint Sites
Entra ID Roles

Policies

Direct Admin
Self Request
Manager Assign
Auto Assign

Custom Extensions
Attributes
Delegation

Catalog

Access Package

Resources Roles

Groups & Teams
Applications
SharePoint Sites
Entra ID Roles

Policies

Direct Admin
Self Request
Manager Assign
Auto Assign

Access Package

Resources Roles

Groups & Teams
Applications
SharePoint Sites
Entra ID Roles

Policies

Direct Admin
Self Request
Manager Assign
Auto Assign

Custom Extensions
Attributes
Delegation

Lifecycle Workflows

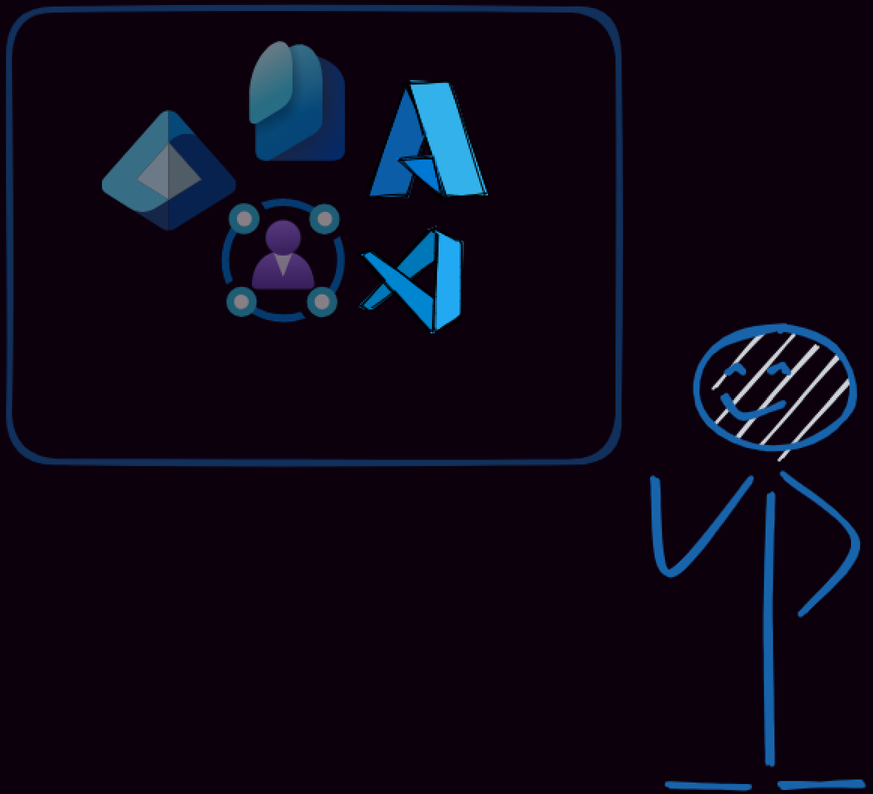
Joiner

Mover

Leaver

NIC
EMPOWER

Demo Lifecycle Workflows



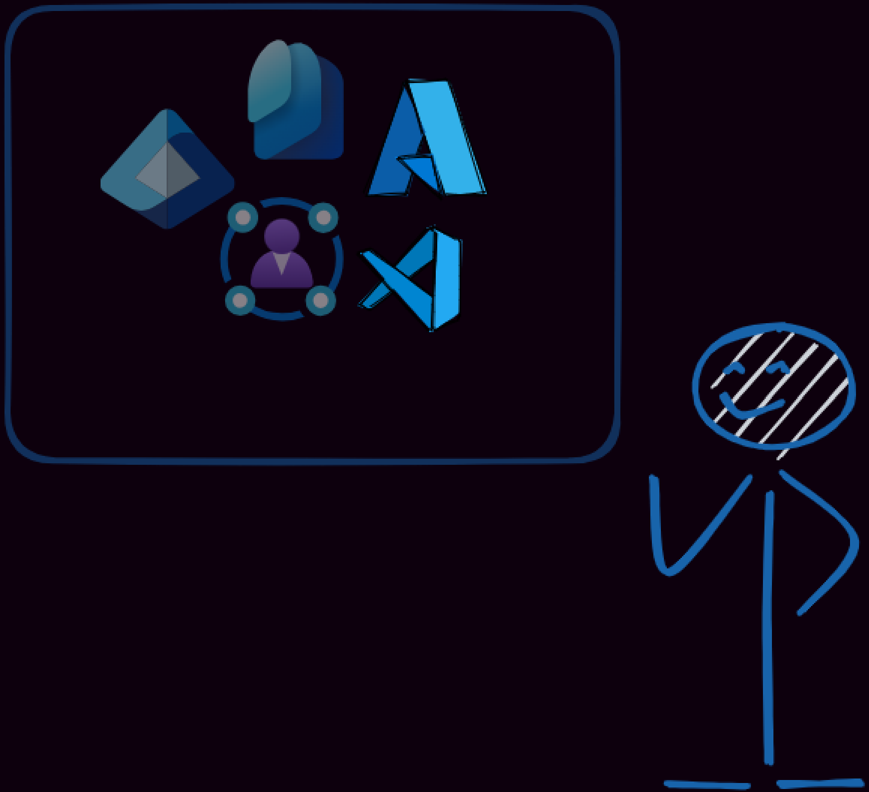
NIC
EMPOWER

Lifecycle Workflows – Custom Extensions

- Logic Apps
- Can send requests to other API's, for example:
  - Azure Functions
  - APIM
  - App Services
  - External API
    - (SMS Gateways)
    - …

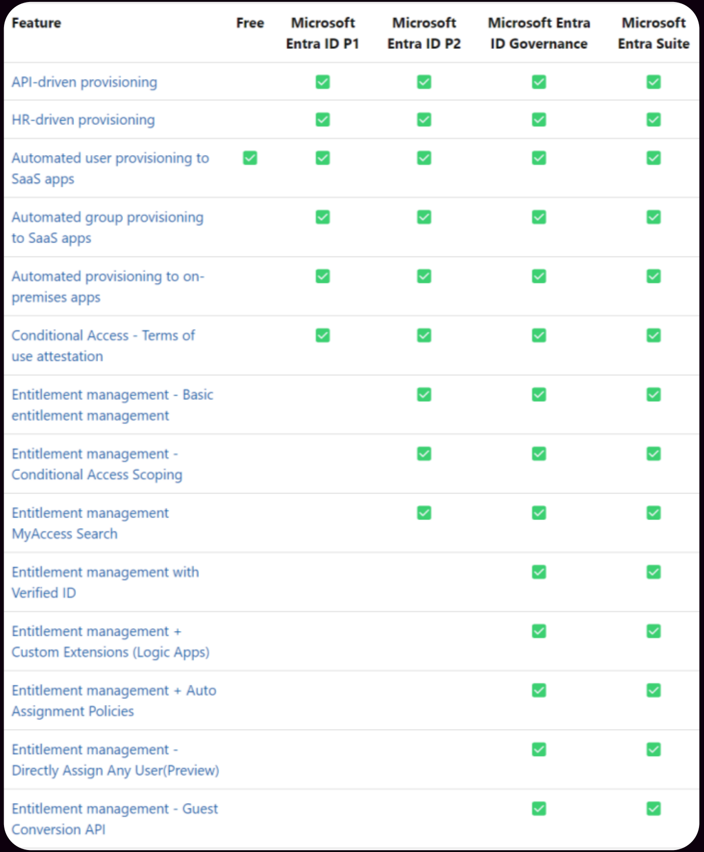
- Magic wand of automation for Lifecycle scenarios 🪄

Demo Custom Extensions



Entra ID Governance Licenses

- API-driven Provisioning
  - Entra ID P1 | P2 | Entra ID Governance | Step Up | **Entra Suite**
- Lifecycle Worklows
  - LCW + Custom Extensions (Logic Apps)
  - Entra ID Governance | Step Up | **Entra Suite**
- **PS! Entra Suite has a free 90-days / 25 user trial now.**

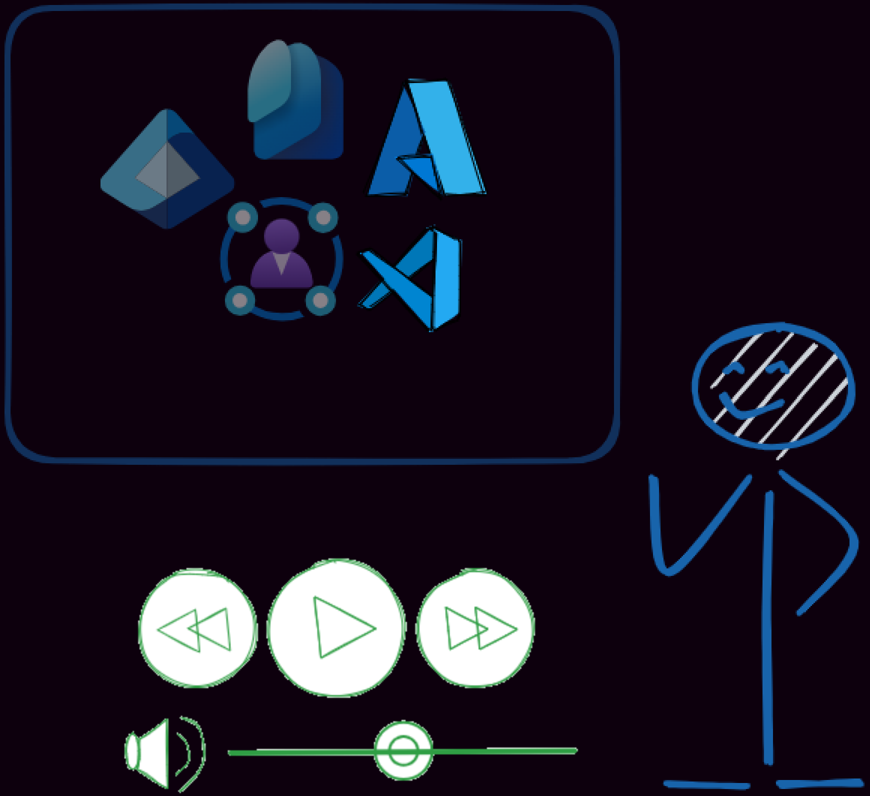


Feature	Free	Microsoft Entra ID P1	Microsoft Entra ID P2	Microsoft Entra ID Governance	Microsoft Entra Suite
API-driven provisioning		✓	✓	✓	✓
HR-driven provisioning		✓	✓	✓	✓
Automated user provisioning to SaaS apps	✓	✓	✓	✓	✓
Automated group provisioning to SaaS apps		✓	✓	✓	✓
Automated provisioning to on-premises apps		✓	✓	✓	✓
Conditional Access - Terms of use attestation		✓	✓	✓	✓
Entitlement management - Basic entitlement management			✓	✓	✓
Entitlement management - Conditional Access Scoping			✓	✓	✓
Entitlement management MyAccess Search			✓	✓	✓
Entitlement management with Verified ID				✓	✓
Entitlement management + Custom Extensions (Logic Apps)				✓	✓
Entitlement management + Auto Assignment Policies				✓	✓
Entitlement management - Directly Assign Any User(Preview)				✓	✓
Entitlement management - Guest Conversion API				✓	✓

NIC EMPOWER

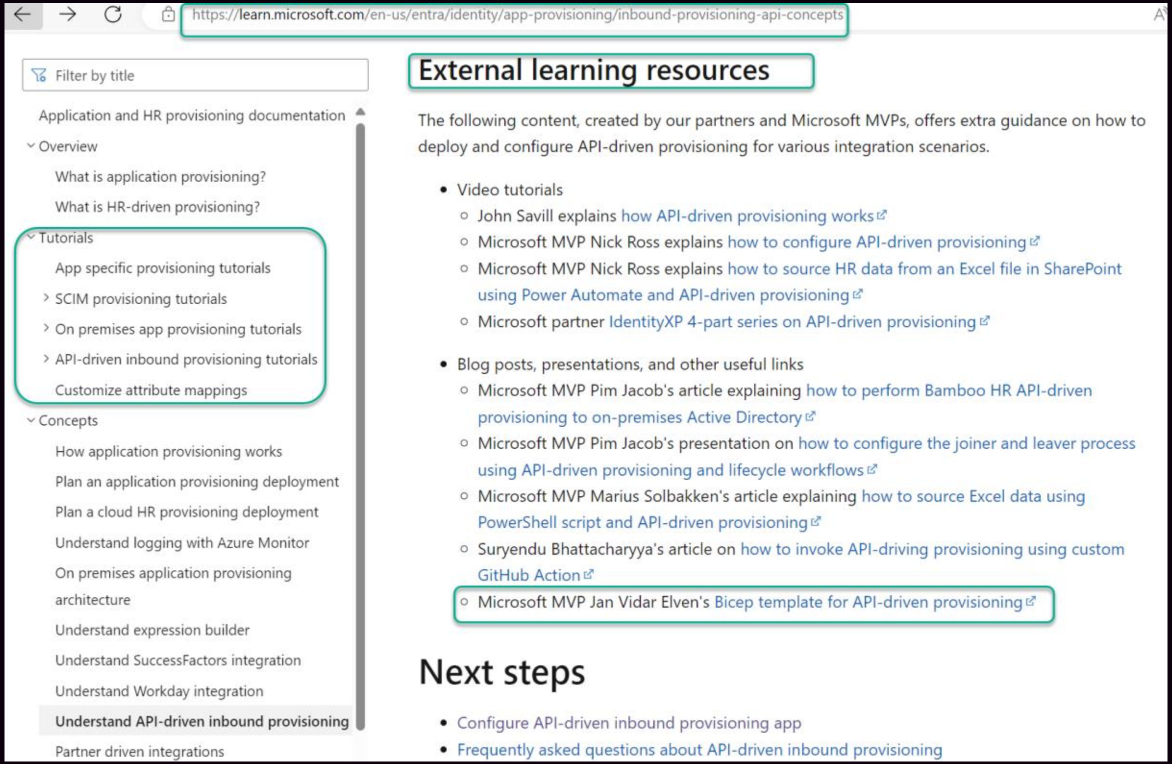
https://learn.microsoft.com/en-us/entra/id-governance/licensing-fundamentals

Demo



Welcome,
Ola Nordmann!

Presentation & Demo Source :/>



https://learn.microsoft.com/en-us/entra/identity/app-provisioning/inbound-provisioning-api-concepts

Filter by title

- Application and HR provisioning documentation
- Overview
  - What is application provisioning?
  - What is HR-driven provisioning?
- Tutorials
  - App specific provisioning tutorials
  - SCIM provisioning tutorials
  - On premises app provisioning tutorials
  - API-driven inbound provisioning tutorials
  - Customize attribute mappings
- Concepts
  - How application provisioning works
  - Plan an application provisioning deployment
  - Plan a cloud HR provisioning deployment
  - Understand logging with Azure Monitor
  - On premises application provisioning architecture
  - Understand expression builder
  - Understand SuccessFactors integration
  - Understand Workday integration
  - Understand API-driven inbound provisioning
  - Partner driven integrations

External learning resources

The following content, created by our partners and Microsoft MVPs, offers extra guidance on how to deploy and configure API-driven provisioning for various integration scenarios.

- Video tutorials
  - John Savill explains how API-driven provisioning works
  - Microsoft MVP Nick Ross explains how to configure API-driven provisioning
  - Microsoft MVP Nick Ross explains how to source HR data from an Excel file in SharePoint using Power Automate and API-driven provisioning
  - Microsoft partner IdentityXP 4-part series on API-driven provisioning
- Blog posts, presentations, and other useful links
  - Microsoft MVP Pim Jacob's article explaining how to perform Bamboo HR API-driven provisioning to on-premises Active Directory
  - Microsoft MVP Pim Jacob's presentation on how to configure the joiner and leaver process using API-driven provisioning and lifecycle workflows
  - Microsoft MVP Marius Solbakken's article explaining how to source Excel data using PowerShell script and API-driven provisioning
  - Suryendu Bhattacharyya's article on how to invoke API-driving provisioning using custom GitHub Action
  - Microsoft MVP Jan Vidar Elven's Bicep template for API-driven provisioning

Next steps

- Configure API-driven inbound provisioning app
- Frequently asked questions about API-driven inbound provisioning

NIC EMPOWER

https://github.com/JanVidarElven/ExpertsLiveEurope2023 @JanVidarElven