



Meet Wild River!

A new recent hire to the Elven Organization!

Hi, I'm Flow!
Welcome to
the family,
here is your
employment
contract!



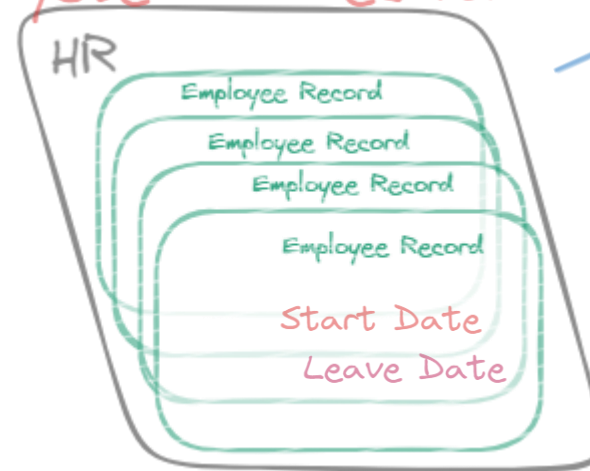
Employment Contract

Person
Org
Role
Sign

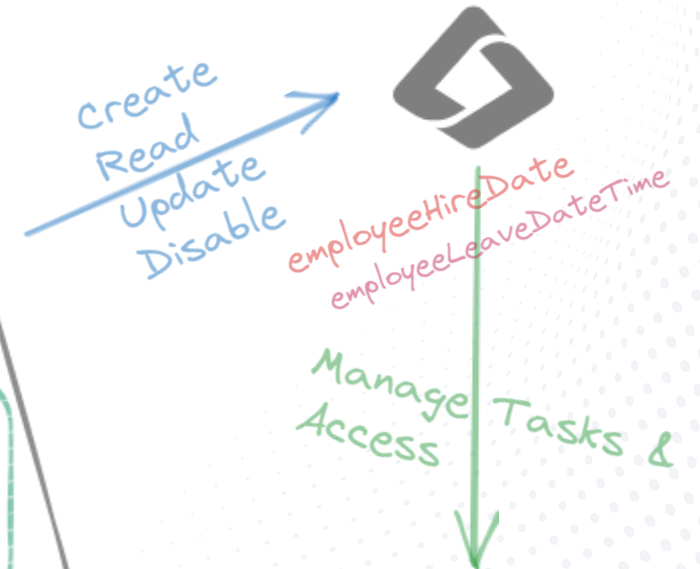


Entra
Verified ID

System of Record

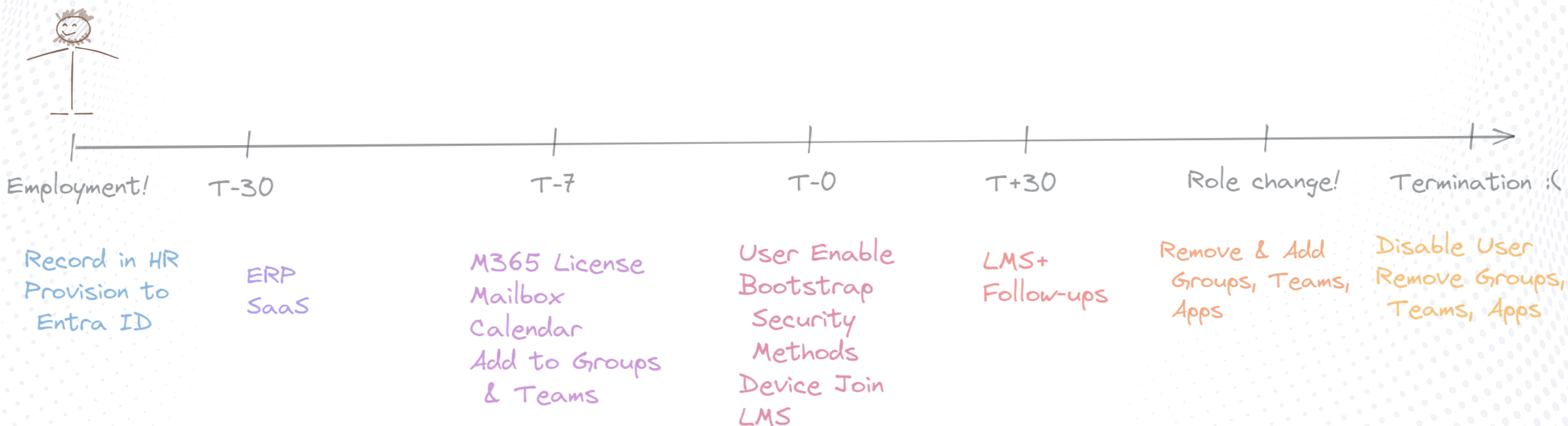


Entra ID Inbound Provisioning



Entra ID Identity Governance

Identity & Access Lifecycle





Knee-Deep Dive into Identity Governance and Lifecycle Workflows with Microsoft Entra ID

 Jan Vidar Elven | Senior Architect & Evidi | MVP Security |
@janvidarelven

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

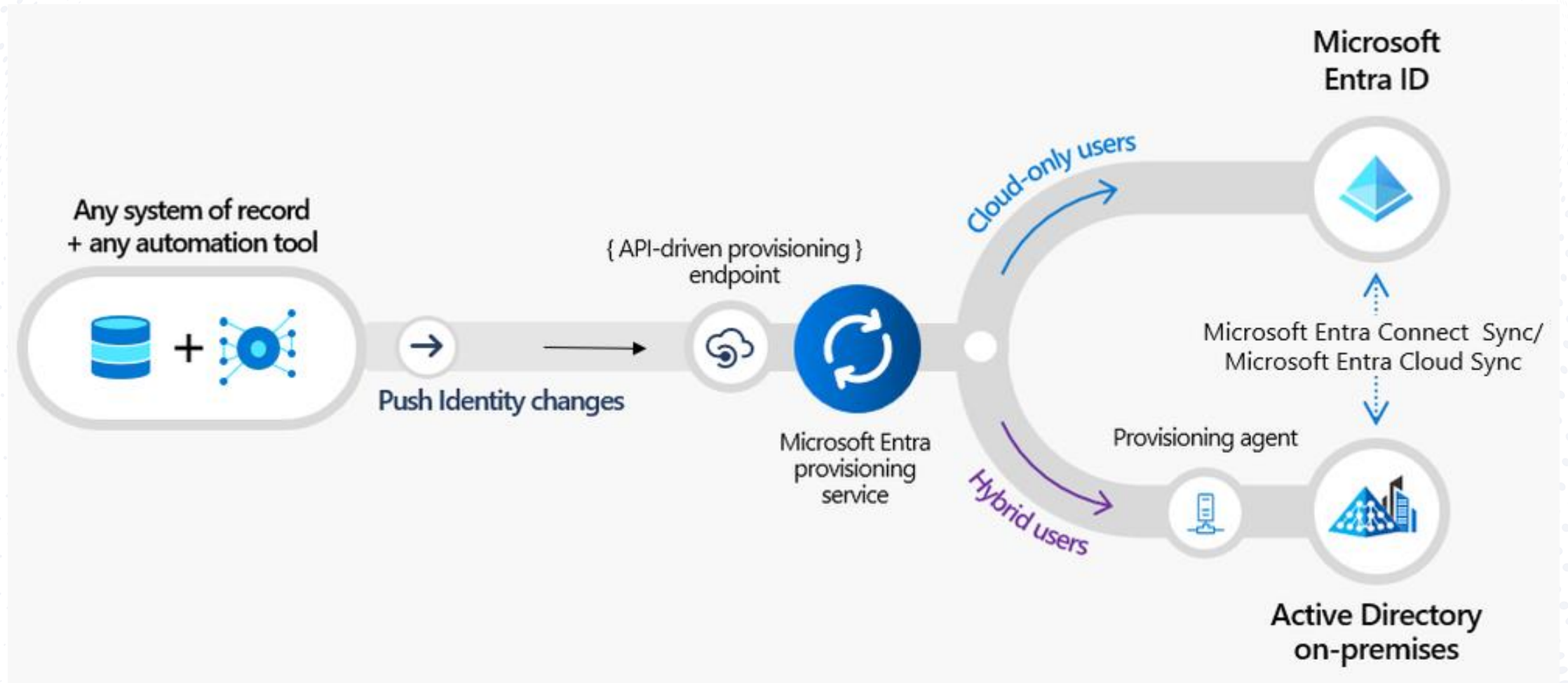
Access reviews configured
5

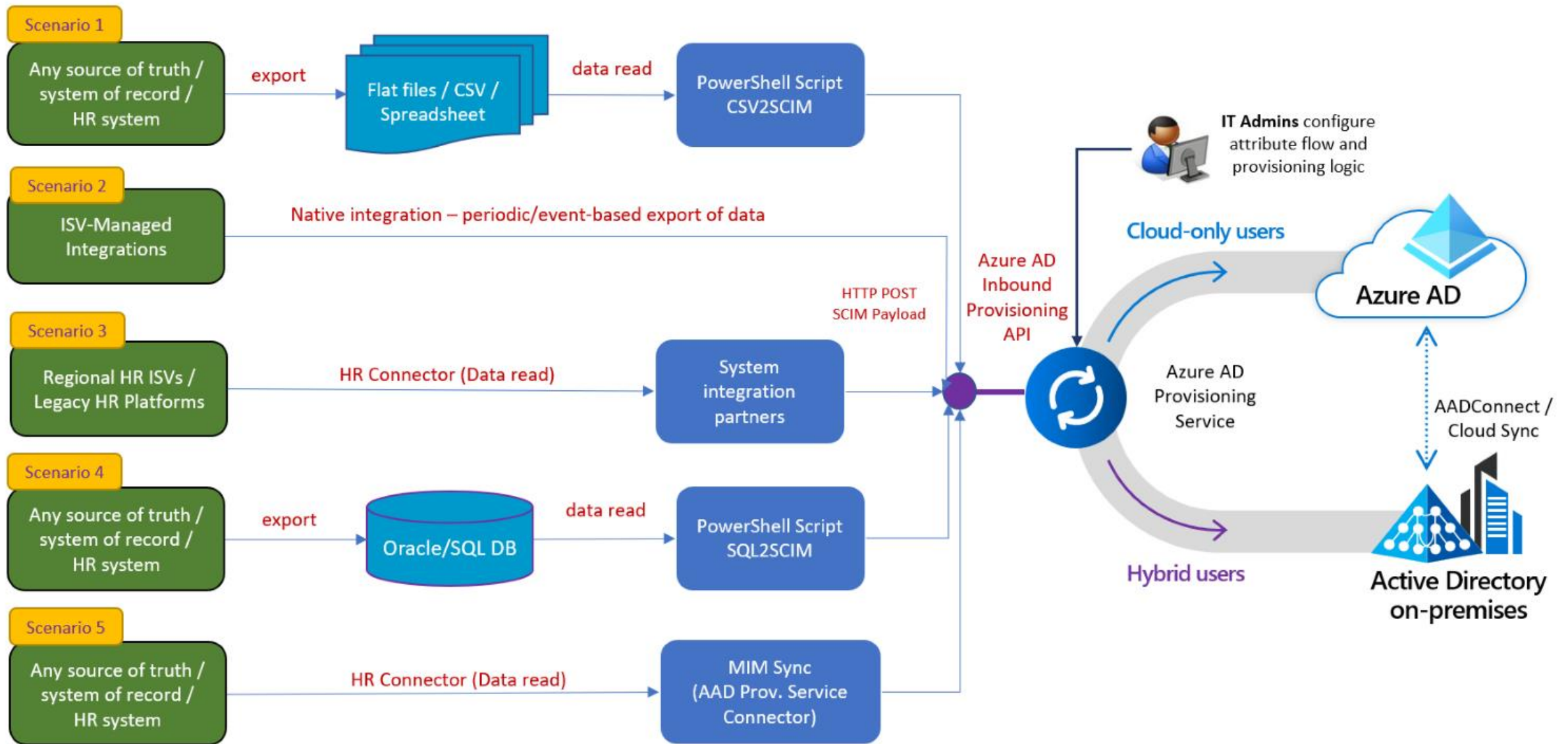
Applications with app roles
105

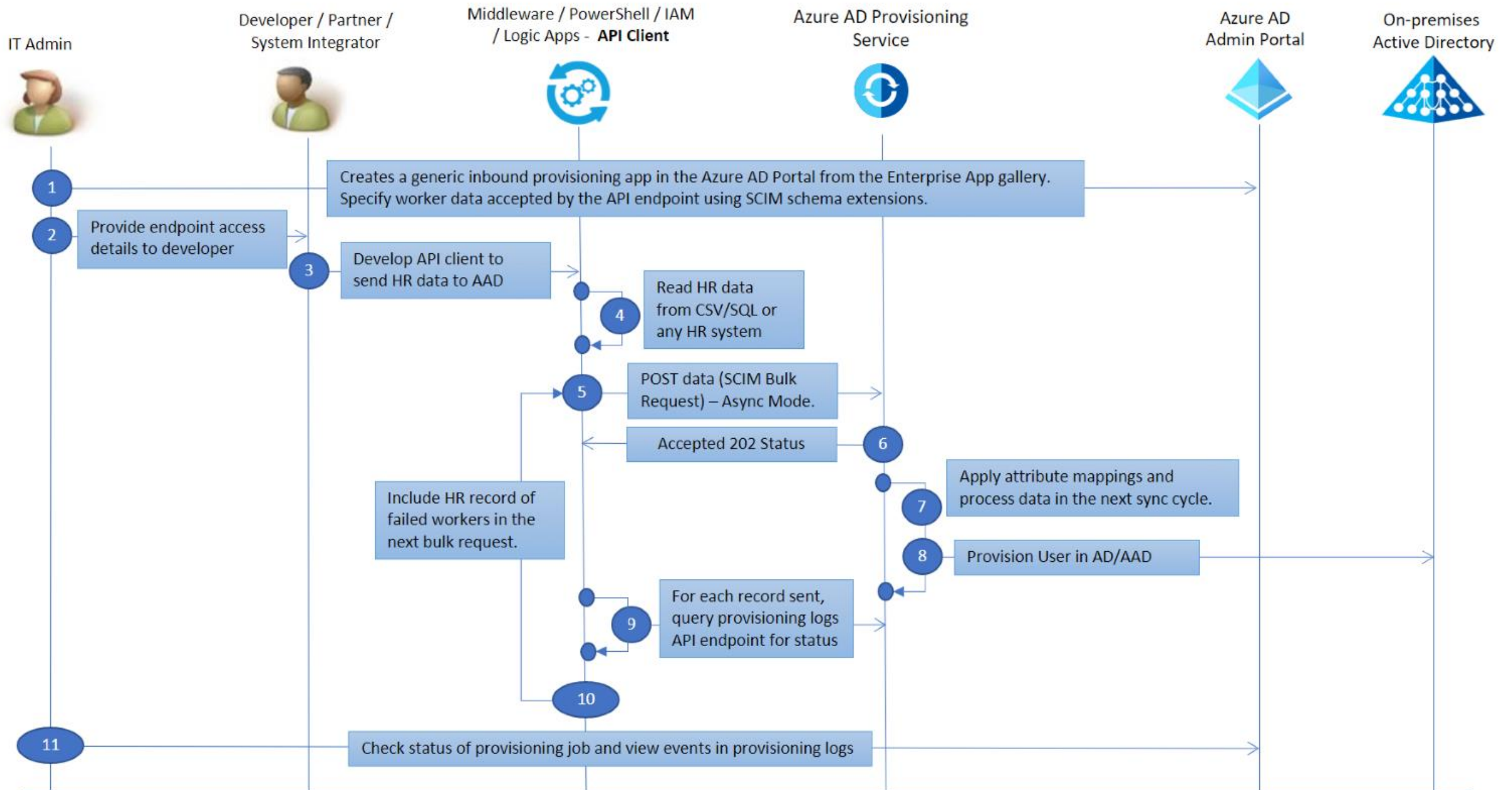
Identities with highly privileged roles
5

Access packages for entitlement management
5

Introducing Entra ID Provisioning API







SCIM requests

HTTP Elven Inbound Provisioning API / SCIM bulk request upload_expertsliveeu

POST {{bulk_upload_endpoint}}

Params Authorization Headers (10) **Body** Pre-request Script Tests Settings

☐ none ☐ form-data ☐ x-www-form-urlencoded ☒ raw ☐ binary ☐ GraphQL **JSON** ▾

```

1  {
2    "schemas": [
3      "urn:ietf:params:scim:api:messages:2.0:BulkRequest"
4    ],
5    "Operations": [
6      {
7        "bulkId": "01daff27-1eb1-401d-a7ac-6c3db87f157b",
8        "data": {
9          "active": true,
10         "addresses": [
11           {
12             "country": "NO",
13             "formatted": "Norway",
14             "locality": "",
15             "postalCode": "",
16             "primary": true,
17             "region": "",
18             "streetAddress": "",
19             "type": "work"
20           }
21         ],
22         "displayName": "Wild River",
23         "emails": [

```



Azure Storage account
– File Share

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

2. Invoke Azure Function CSV2JSON



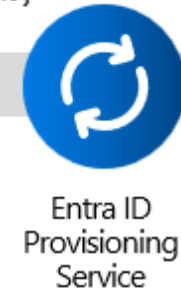
3. Convert JSON payload to SCIM bulk request

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

5. Track processing using Provisioning Logs

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

Inbound Provisioning
{ API endpoint }



Cloud-only users

Hybrid users

Entra ID



Azure AD Connect /
Cloud Sync

Provisioning
Agent



Active Directory
on-premises

Demo Inbound Provisioning



Lifecycle Scenarios

Joiner



Mover



Leaver



Lifecycle Workflows in Entra ID Governance

[Choose a template](#) Basics Configure scope Review tasks Review + create

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 change

Execute real-time tasks for employee job 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](#)

Demo Lifecycle Workflows



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



Presentation & Demo Source : \>

<https://github.com/JanVidarElven/ExpertsLiveEurope2023>

@JanVidarElven

Thank you to our Sponsors

