Microsoft Security

Microsoft Entra ID Governance Partner Technical Training

Overview

June 12, 2024

Sumi Venkitaraman
Principal Product Manager, Microsoft Security

Microsoft Security

Training Agenda

Microsoft Entra ID Governance overview

- Feature highlights

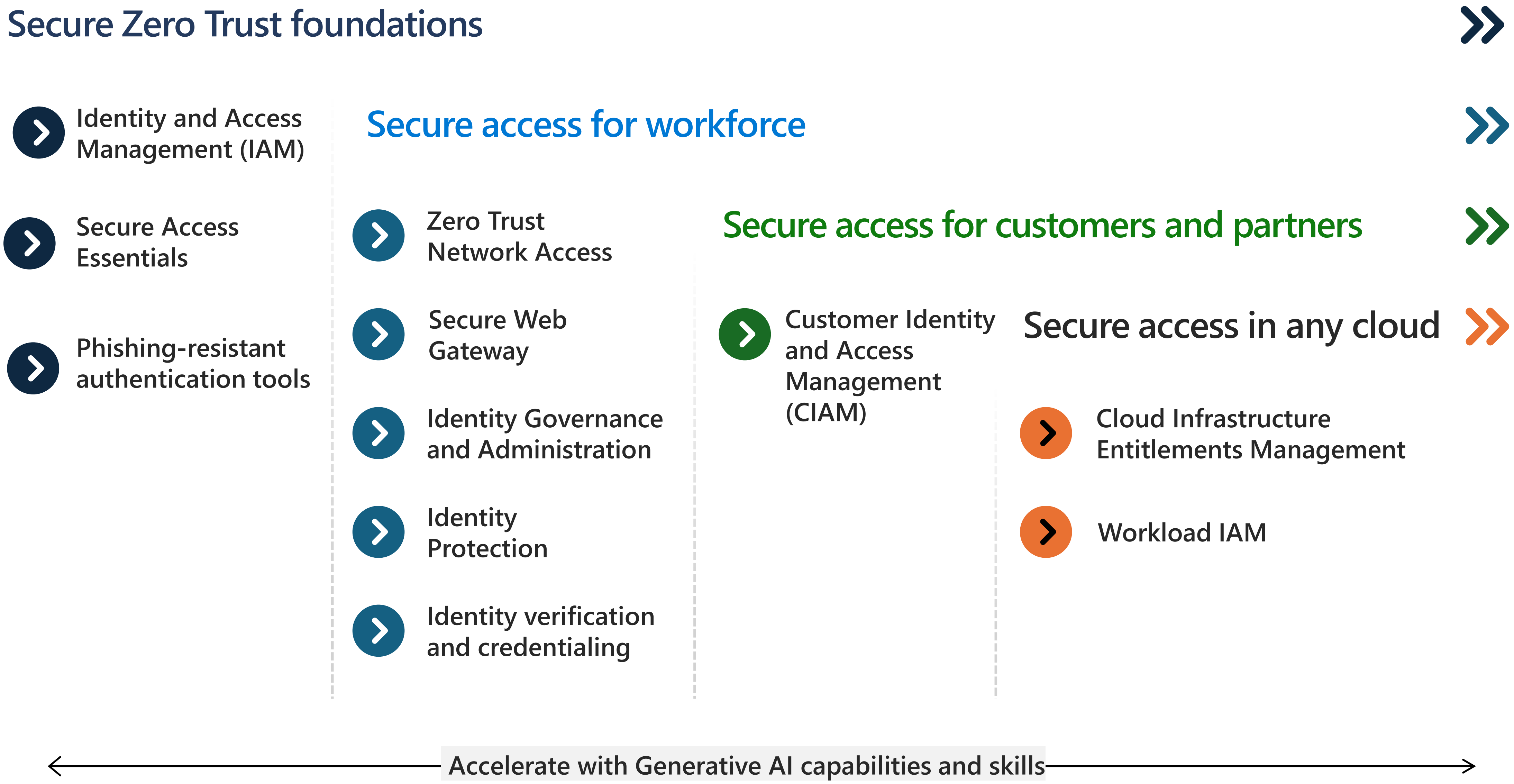
Technical Training

- Scenario Deep Dive

Summary

Microsoft Entra ID Governance Overview

Secure access: maturity stages



Secure Zero Trust foundations

- Identity and Access Management (IAM)
- Secure Access Essentials
- Phishing-resistant authentication tools

Secure access for workforce

- Zero Trust Network Access
- Secure Web Gateway
- Identity Governance and Administration
- Identity Protection
- Identity verification and credentialing

Secure access for customers and partners

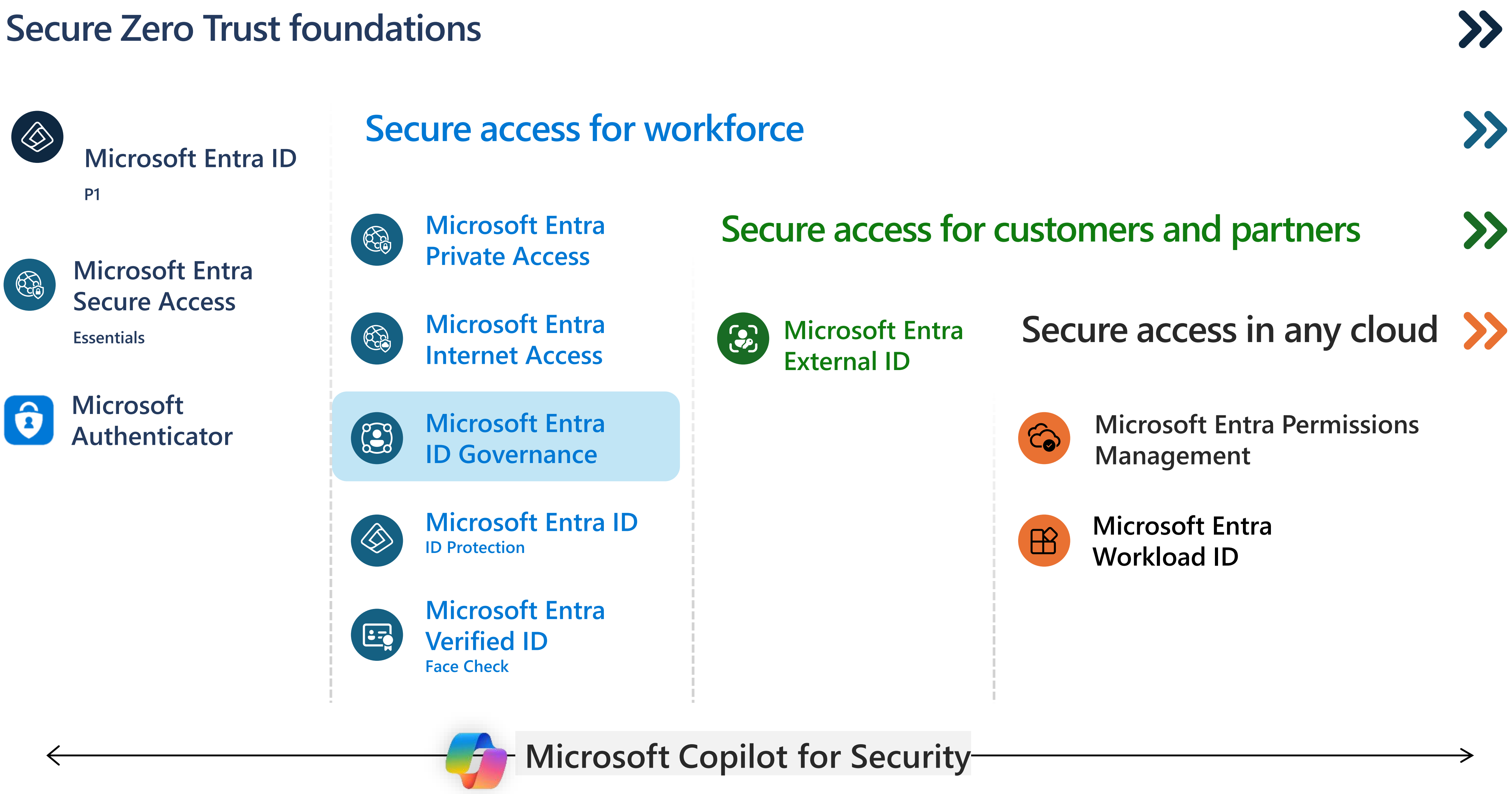
- Customer Identity and Access Management (CIAM)

Secure access in any cloud

- Cloud Infrastructure Entitlements Management
- Workload IAM

Accelerate with Generative AI capabilities and skills

Microsoft Entra



Secure Zero Trust foundations

Microsoft Entra ID
P1

Microsoft Entra Secure Access
Essentials

Microsoft Authenticator

Secure access for workforce

Microsoft Entra Private Access

Microsoft Entra Internet Access

Microsoft Entra ID Governance

Microsoft Entra ID
ID Protection

Microsoft Entra Verified ID
Face Check

Secure access for customers and partners

Microsoft Entra External ID

Secure access in any cloud

Microsoft Entra Permissions Management

Microsoft Entra Workload ID

Microsoft Copilot for Security

Microsoft Entra ID Governance

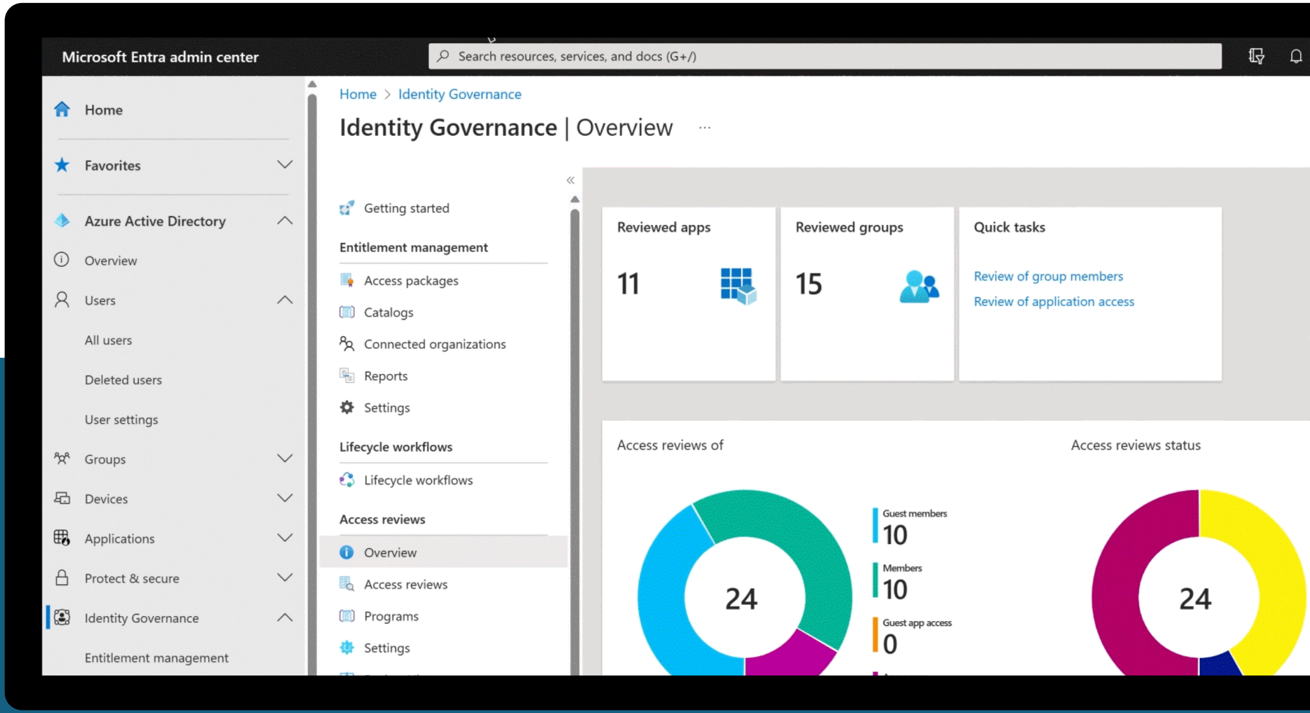
Go to section »

Ensuring that the right people have the right access to the right resources, at the right time

Improve productivity

Strengthen security

Automate routine tasks



Microsoft Entra admin center

Search resources, services, and docs (G+/)

Home

Favorites

Azure Active Directory

Overview

Users

All users

Deleted users

User settings

Groups

Devices

Applications

Protect & secure

Identity Governance

Entitlement management

Home > Identity Governance

Identity Governance | Overview ···

Getting started

Entitlement management

Access packages

Catalogs

Connected organizations

Reports

Settings

Lifecycle workflows

Lifecycle workflows

Access reviews

Overview

Access reviews

Programs

Settings

Reviewed apps	Reviewed groups	Quick tasks
11	15	Review of group members Review of application access

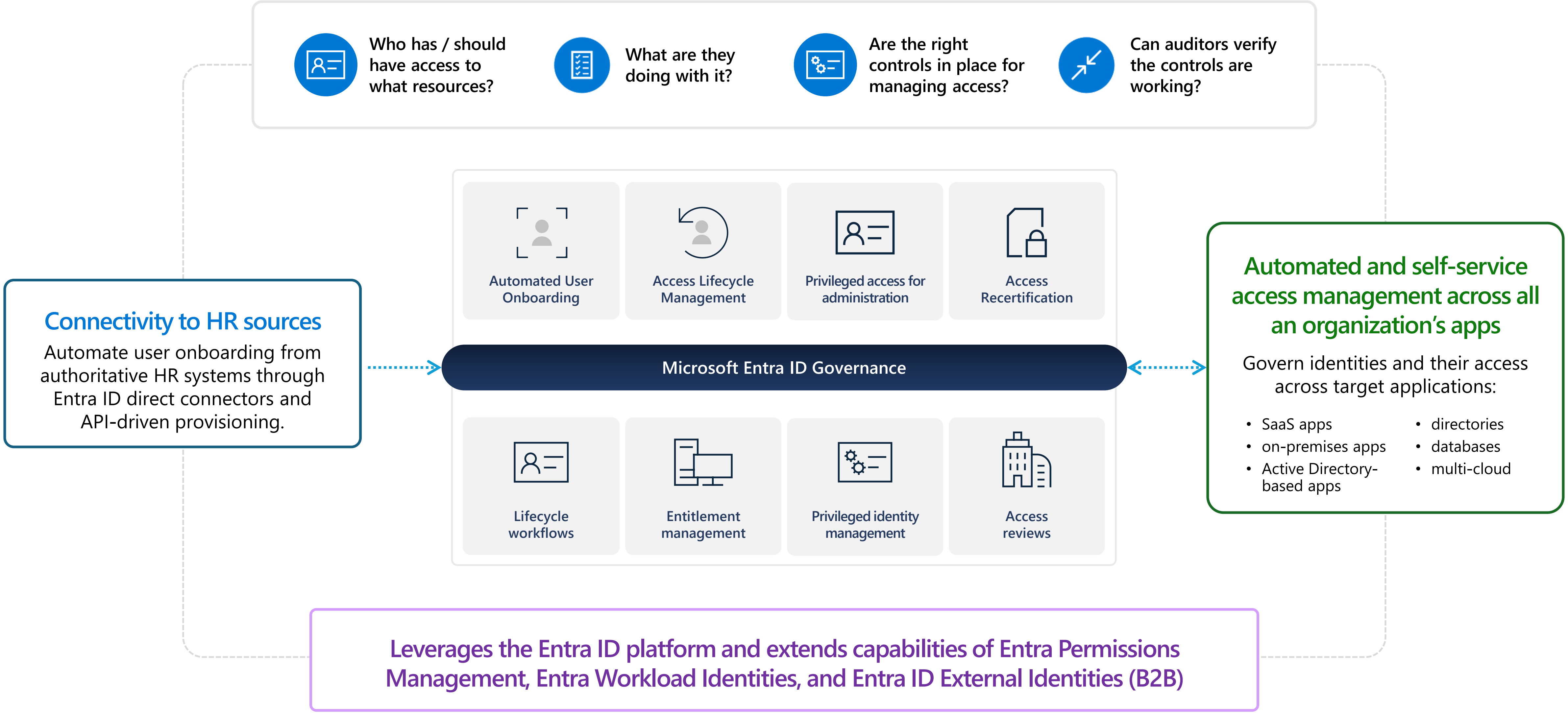
Access reviews of

Access reviews status

Market challenge:

Managing user identities, access rights, and entitlements across IT environments to ensure proper access controls, mitigate risk, and maintain compliance with regulatory requirements

Microsoft Entra ID Governance



Who has / should have access to what resources?

What are they doing with it?

Are the right controls in place for managing access?

Can auditors verify the controls are working?

Automated User Onboarding

Access Lifecycle Management

Privileged access for administration

Access Recertification

Microsoft Entra ID Governance

Lifecycle workflows

Entitlement management

Privileged identity management

Access reviews

Connectivity to HR sources

Automate user onboarding from authoritative HR systems through Entra ID direct connectors and API-driven provisioning.

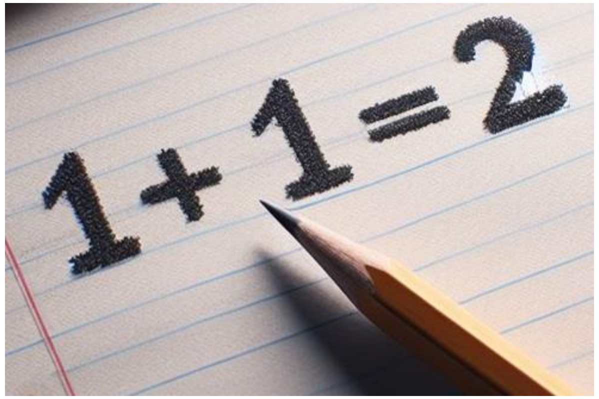
Automated and self-service access management across all an organization's apps

Govern identities and their access across target applications:

- SaaS apps
- on-premises apps
- Active Directory-based apps
- directories
- databases
- multi-cloud

Leverages the Entra ID platform and extends capabilities of Entra Permissions Management, Entra Workload Identities, and Entra ID External Identities (B2B)

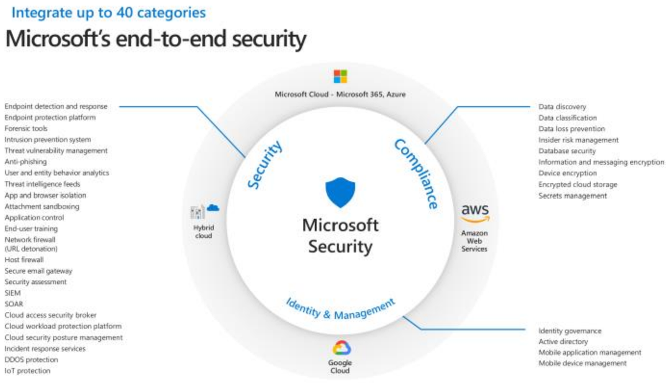
Why Microsoft Entra ID Governance?



Ease of adoption

Simple extensibility

Time to value



Integrate up to 40 categories

Microsoft's end-to-end security

Endpoint detection and response
Endpoint protection platform
Forensic tools
Intrusion prevention system
Threat vulnerability management
Anti-phishing
User and entity behavior analytics
Threat intelligence feeds
App and browser isolation
Attachment sandboxing
Application control
End-user training
Network firewall
(URL detonation)
Host firewall
Secure email gateway
Security assessment
SIEM
SOAR
Cloud access security broker
Cloud workload protection platform
Cloud security posture management
Incident response services
DDOS protection
IoT protection

Data discovery
Data classification
Data loss prevention
Insider risk management
Database security
Information and messaging encryption
Device encryption
Encrypted cloud storage
Secrets management

Identity governance
Active directory
Mobile application management
Mobile device management

Integrated and Holistic

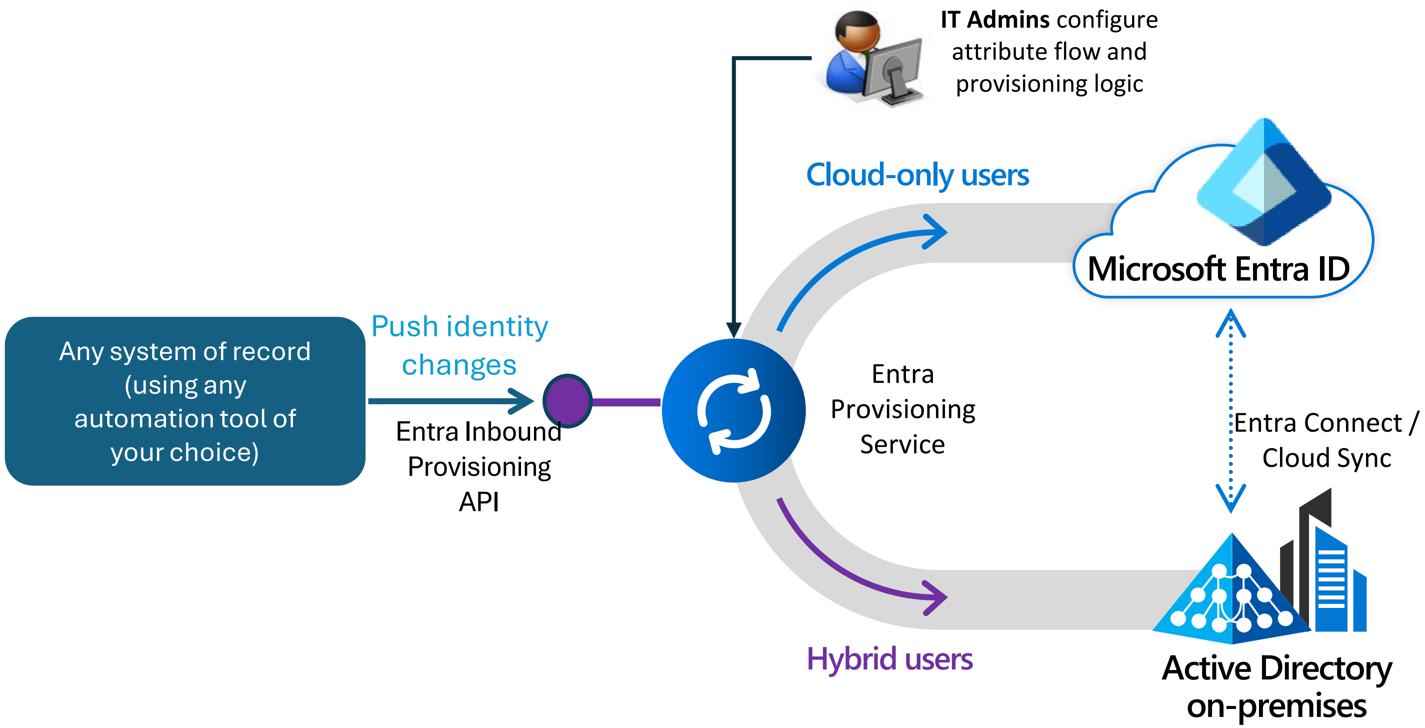
Inbound Provisioning HR API

Connect *any* authoritative system of record for inbound identity provisioning

Connect HR app like UltiPro, a payroll app like ADP, a spreadsheet in Google Cloud or an on-premises Oracle database

Decouples HR data export from how data is cleansed before import into Microsoft Entra ID.

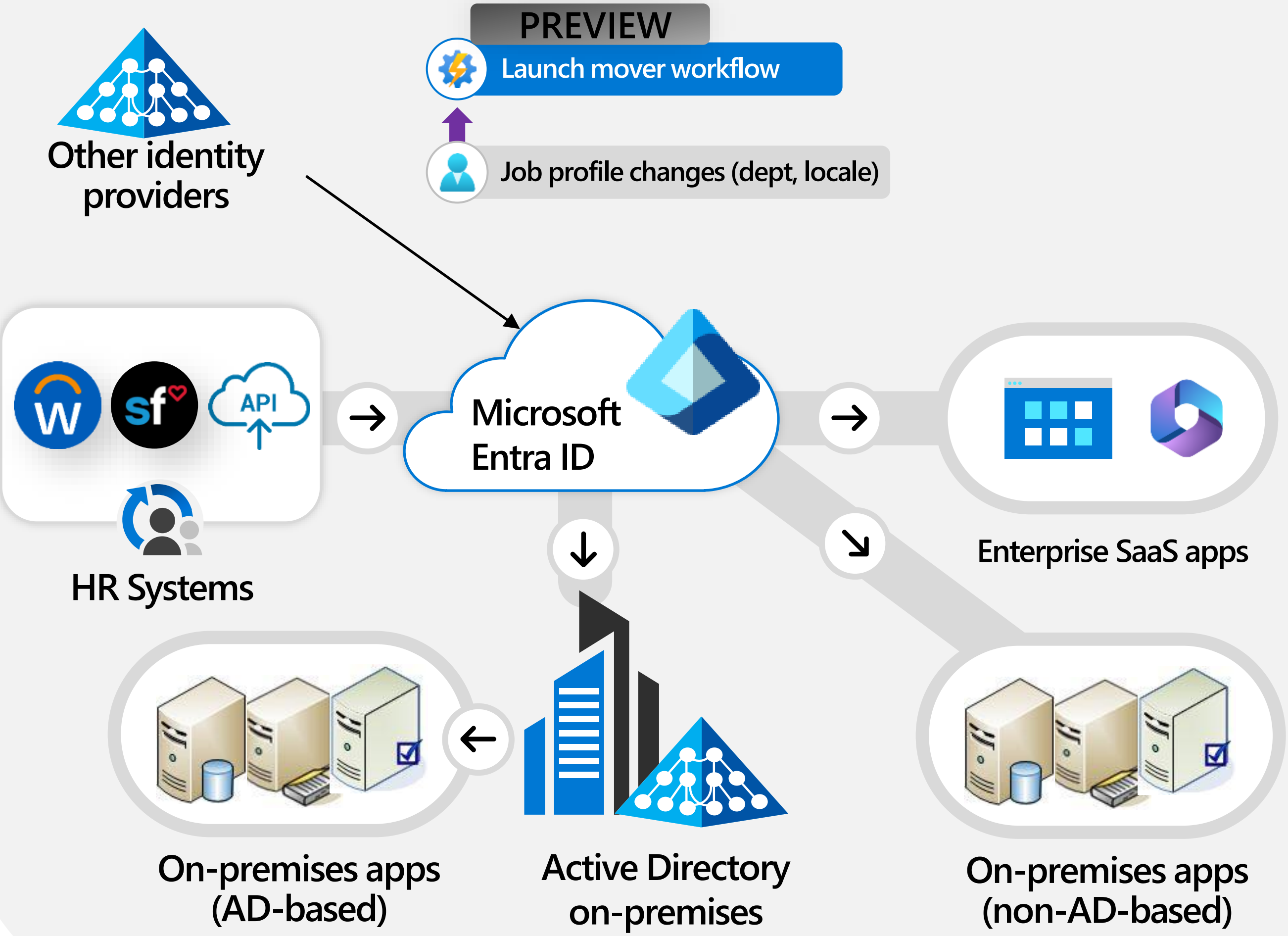
IT admins retain control on identity data flow, transformations and mapping


IT Admins configure attribute flow and provisioning logic
Cloud-only users
Microsoft Entra ID
Any system of record (using any automation tool of your choice)
Push identity changes
Entra Inbound Provisioning API
Entra Provisioning Service
Entra Connect / Cloud Sync
Hybrid users
Active Directory on-premises

Lifecycle Workflows

Automate join / move / leave employee lifecycle events

- You can schedule tasks to occur before, at or after a join or leave date.
- Built-in tasks include generating temporary credentials, sending emails, and updating user attributes, licenses, memberships, and access package assignments.
- You can extend lifecycle workflows with additional tasks via Azure Logic Apps.


PREVIEW
Launch mover workflow
Job profile changes (dept, locale)
Other identity providers
API
HR Systems
Microsoft Entra ID
Enterprise SaaS apps
On-premises apps (AD-based)
Active Directory on-premises
On-premises apps (non-AD-based)

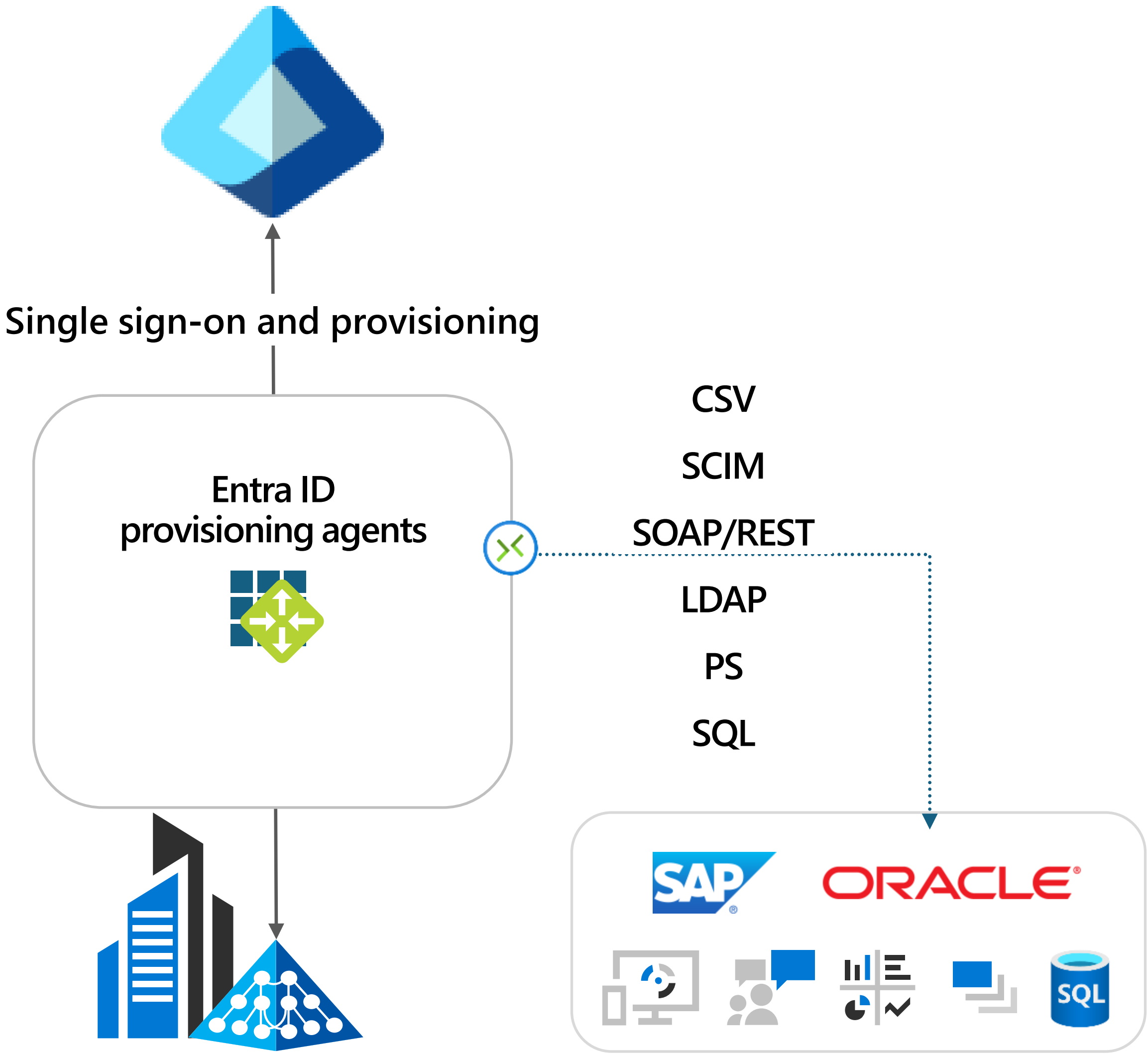
Provisioning to on-premises applications

Users and schema defined in the cloud

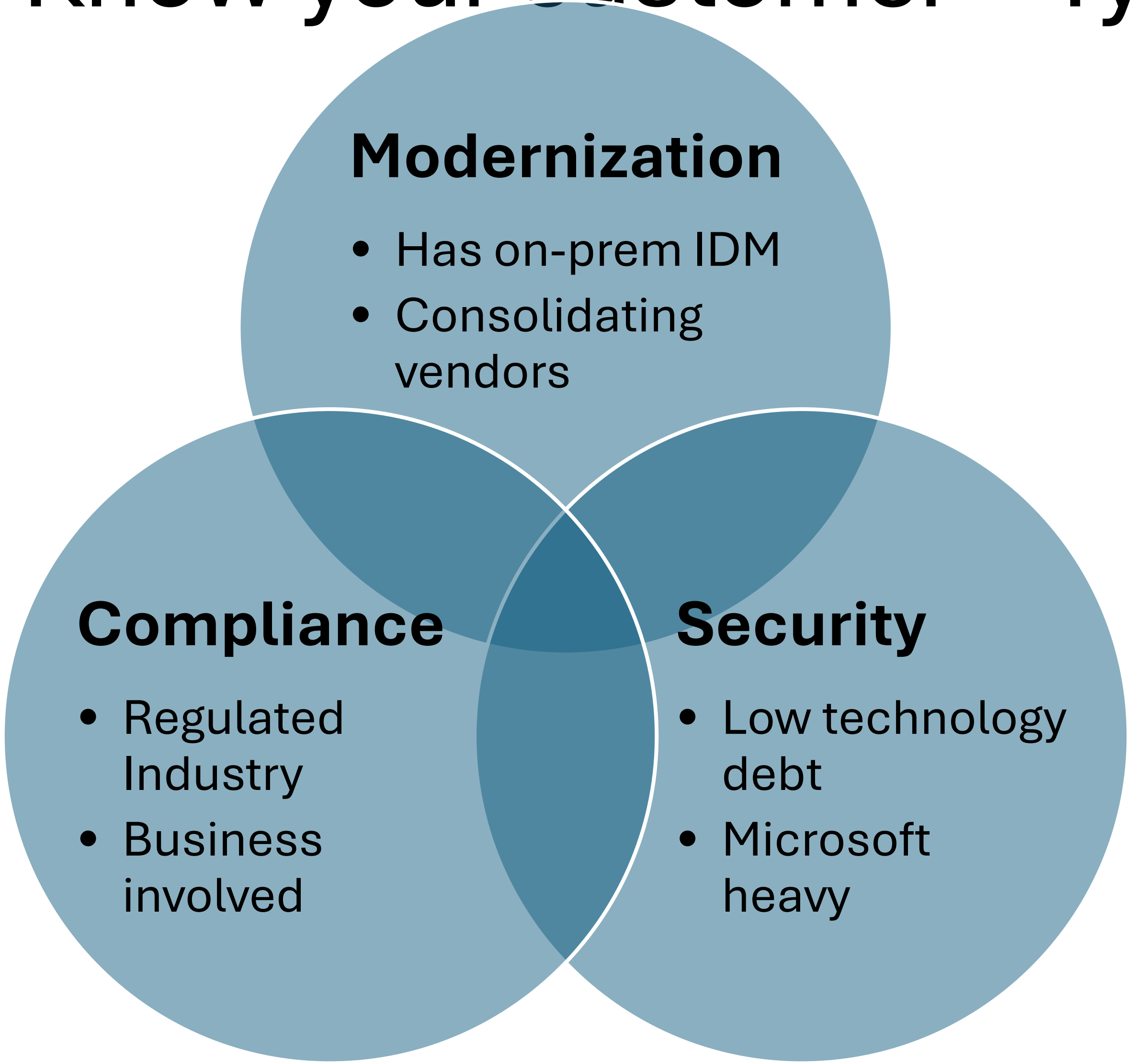
- Supports provisioning from custom schema extensions to app-specific properties.

Translation to the provisioning protocols expected by apps

- Microsoft-delivered connectors: LDAP, SQL, etc.
- Ecosystem of third-party connectors for other apps requiring custom API integrations
- Customers can re-use their existing MIM configuration



Know your customer – Typical themes



Modernization

- Has on-prem IDM
- Consolidating vendors

Compliance

- Regulated Industry
- Business involved

Security

- Low technology debt
- Microsoft heavy

Unlock more value for your customers

1. Migrating to Microsoft Entra ID from Microsoft Identity Manager - Migrating to Microsoft Entra ID from Microsoft Identity Manager | Microsoft Learn
2. Partner-driven integrations - Use partner driven integrations to provision accounts into all your applications - Microsoft Entra ID | Microsoft Learn
3. Github samples - entra-id-inbound-provisioning/LogicApps/CSV2SCIMBulkUpload at main · AzureAD/entra-id-inbound-provisioning · GitHub

SAP Partnership

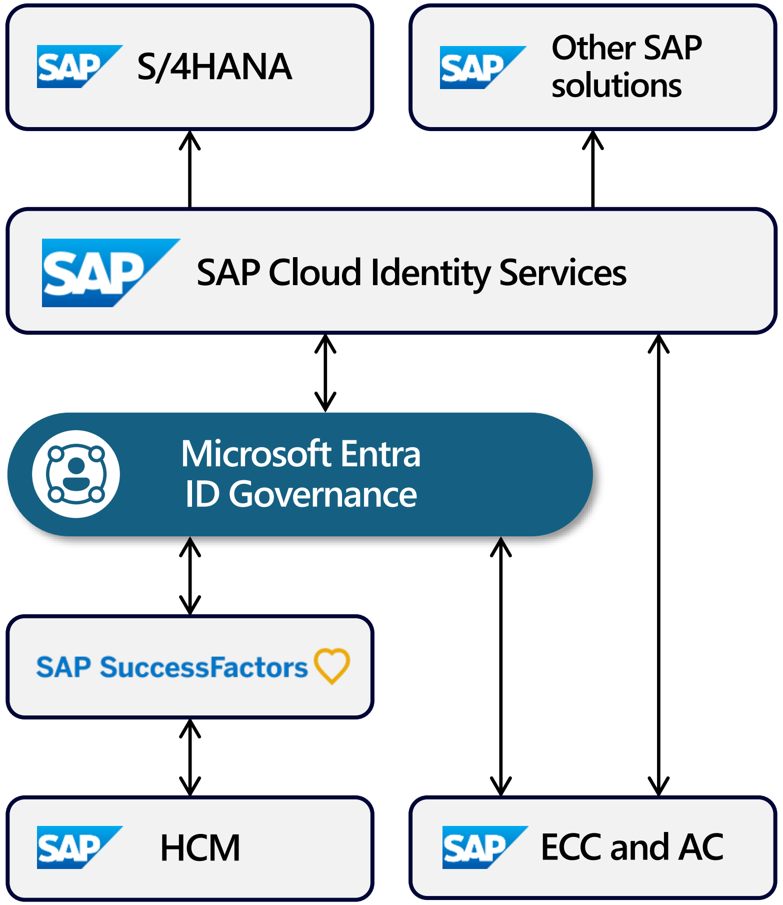
Consistent identity governance for business applications

- ✓ Microsoft Entra provides Single Sign-On and provisioning to SAP cloud and on-premises apps

- ✓ SAP IDM customers migrate their IAM scenarios to Microsoft Entra

SAP IDM to Microsoft Entra migration guidance
https://aka.ms/migratefromsapidm

- ✓ Deeper Microsoft + SAP integration for consistent Identity & Access Governance across apps



Training Hub

- Partner-ready content hosted on Github

https://aka.ms/EntraIDGovernancetraining

- What’s available:

1. Use cases, scenarios and demos
2. PoC-in-a-box guidance and demos

Microsoft Entra Identity Governance

Capability	Scenario	Feature
Identity lifecycle (employees)	Admins can enable user account provisioning from Workday or SuccessFactors cloud HR, or on-premises HR.	Cloud HR to Azure AD user provisioning
Identity lifecycle (guests)	Admins can enable self-service guest user onboarding from another Microsoft Entra tenant, direct federation, One Time Passcode (OTP) or Google accounts. Guest users are automatically provisioned and deprovisioned subject to lifecycle policies.	Entitlement management using B2B
Entitlement management	Resource owners can create access packages containing apps, Teams, Microsoft Entra, and Microsoft 365 groups, and SharePoint Online sites.	Entitlement management
Lifecycle Workflows	Admins can enable the automation of the lifecycle process based on user conditions.	Lifecycle Workflows
Access requests	End users can request group membership or application access. End users, including guests from other organizations, can request access to access packages.	Entitlement management
Workflow	Resource owners can define the approvers and escalation approvers for access requests and approvers for role activation requests.	Entitlement management and PIM
Policy and role management	Admin can define conditional access policies for run-time access to applications. Resource owners can define policies for user's access via access packages.	Conditional access and Entitlement management policies
Access certification	Admins can enable recurring access recertification for: SaaS apps, on-premises apps, cloud group memberships, Microsoft Entra, or Azure Resource role assignments. Automatically remove resource access, block guest access and delete guest accounts.	Access reviews, also surfaced in PIM
Fulfillment and provisioning	Automatic provisioning and deprovisioning into Microsoft Entra connected apps, including via SCIM, LDAP, SQL and into SharePoint Online sites.	User provisioning
Reporting and analytics	Admins can retrieve audit logs of recent user provisioning and sign on activity. Integration with Azure Monitor and 'who has access' via access packages.	Azure AD reports and monitoring
Privileged access	Just-in-time and scheduled access, alerting, approval workflows for Microsoft Entra roles (including custom roles) and Azure Resource roles.	Azure AD PIM
Auditing	Admins can be alerted of creation of admin accounts.	Azure AD PIM alerts

http://aka.ms/IdentityGovernanceOverview

Resources

- Microsoft Entra ID Governance training hub
  aka.ms/EntraIDGovernanceTraining

- Microsoft Entra identity blog
  aka.ms/IdentityBlog

- Microsoft Entra product page
  aka.ms/entra/identitygovernance

- Microsoft Identity solution page
  microsoft.com/Identity

- Microsoft Entra technical documentation
  aka.ms/Entra/IDGovDocs

- Try Microsoft Entra ID Governance free
  aka.ms/EntraIDGovTrial

- Entra ID Governance Licensing Fundamentals
  https://aka.ms/EntraIG/LicDocs

Microsoft Security

Microsoft Entra ID Governance

Scenarios Deep Dive

Agenda

- Overview of Microsoft Entra ID Governance SKU
- Scenario deep dive
  - Employee Lifecycle
  - Govern Access to Resources
  - Govern External Identities

Session Format

We will go through Entra ID Governance as end to end scenarios :

- What scenario is about?
- What features of Entra ID Governance enable the scenario
- How you can do a demo each scenario with your own customers

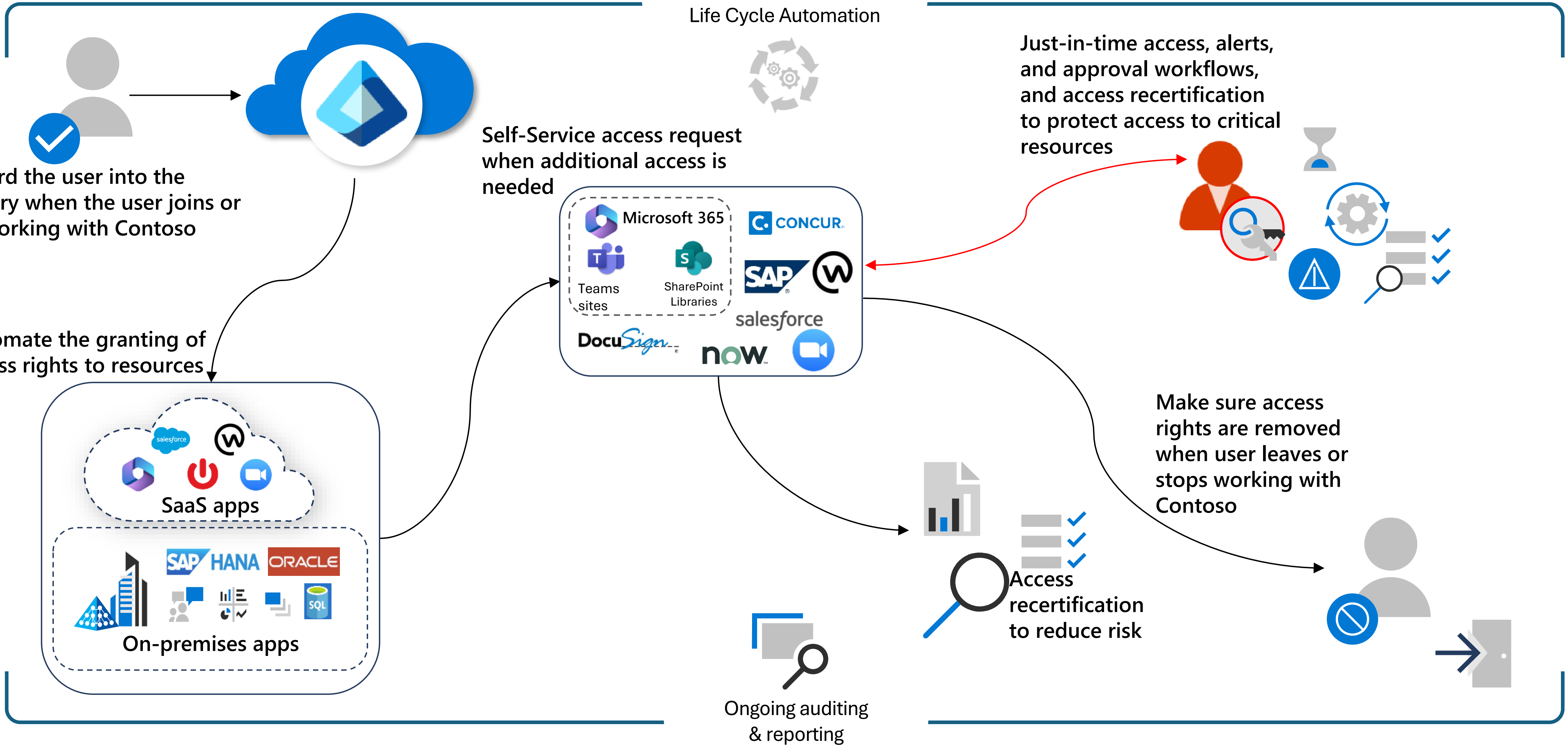
POC in a box

- Look at our POC in a Box developments at:

aka.ms/EntraIDGovernanceTraining

Employee Lifecycle Automation

Contoso's user journey



Life Cycle Automation

Onboard the user into the directory when the user joins or start working with Contoso

Automate the granting of access rights to resources

Self-Service access request when additional access is needed

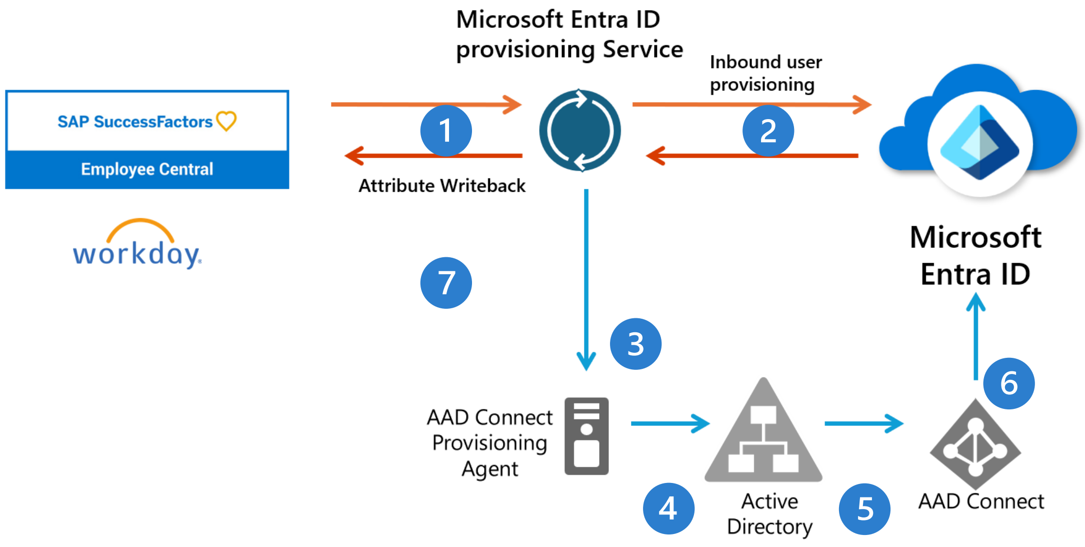
Just-in-time access, alerts, and approval workflows, and access recertification to protect access to critical resources

Make sure access rights are removed when user leaves or stops working with Contoso

Access recertification to reduce risk

Ongoing auditing & reporting

Cloud HR to Active Directory

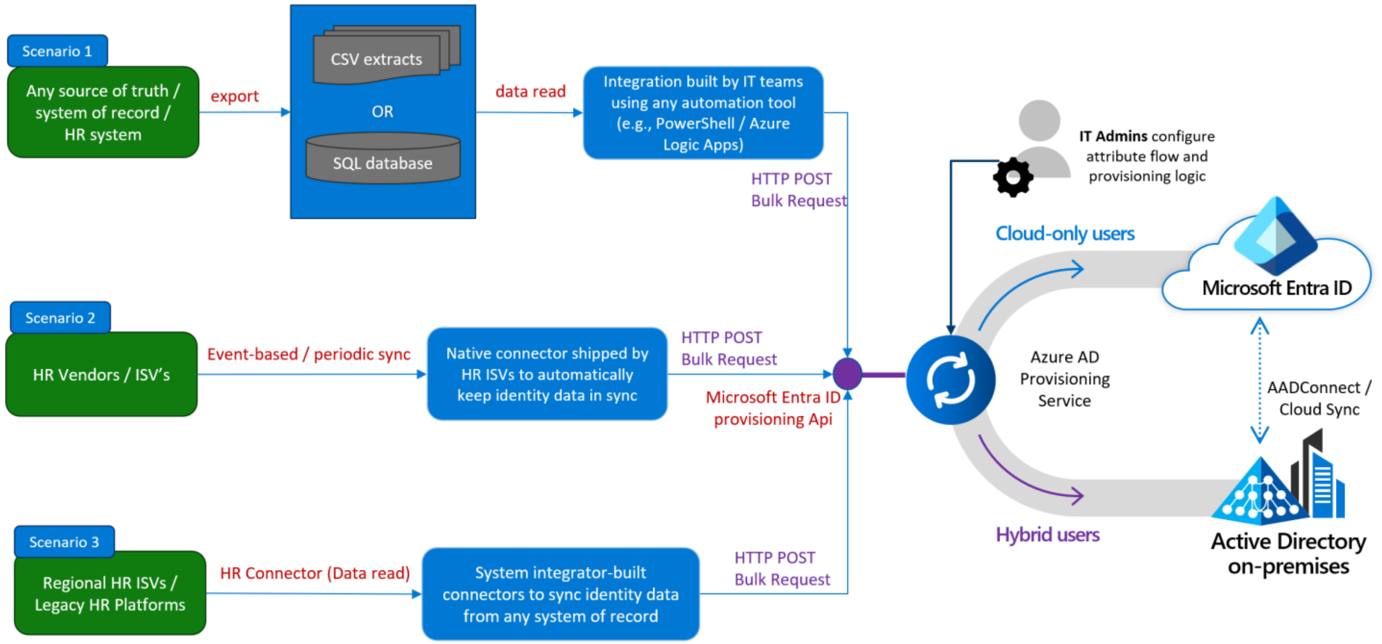


User data Flow:

1. The HR team performs worker transactions (Joiners/Movers/Leavers or New Hires/Transfers/Terminations) in Cloud HR
2. The Microsoft Entra ID Provisioning Service runs scheduled synchronizations of identities from CloudHR and identifies changes that need to be processed for sync with on-premises Active Directory.
3. The Microsoft Entra ID Provisioning Service invokes the on-premises Microsoft Entra ID Connect Provisioning Agent with a request payload containing AD account create/update/enable/disable operations.
4. The Microsoft Entra ID Connect Provisioning Agent uses a service account to add/update AD account data.
5. The Microsoft Entra ID Connect / AD Sync engine runs delta sync to pull updates in AD.
6. The Active Directory updates are synced with Microsoft Entra ID
7. If the CloudHR Writeback app is configured, it writes back attributes such as email, username and phone number to CloudHR.

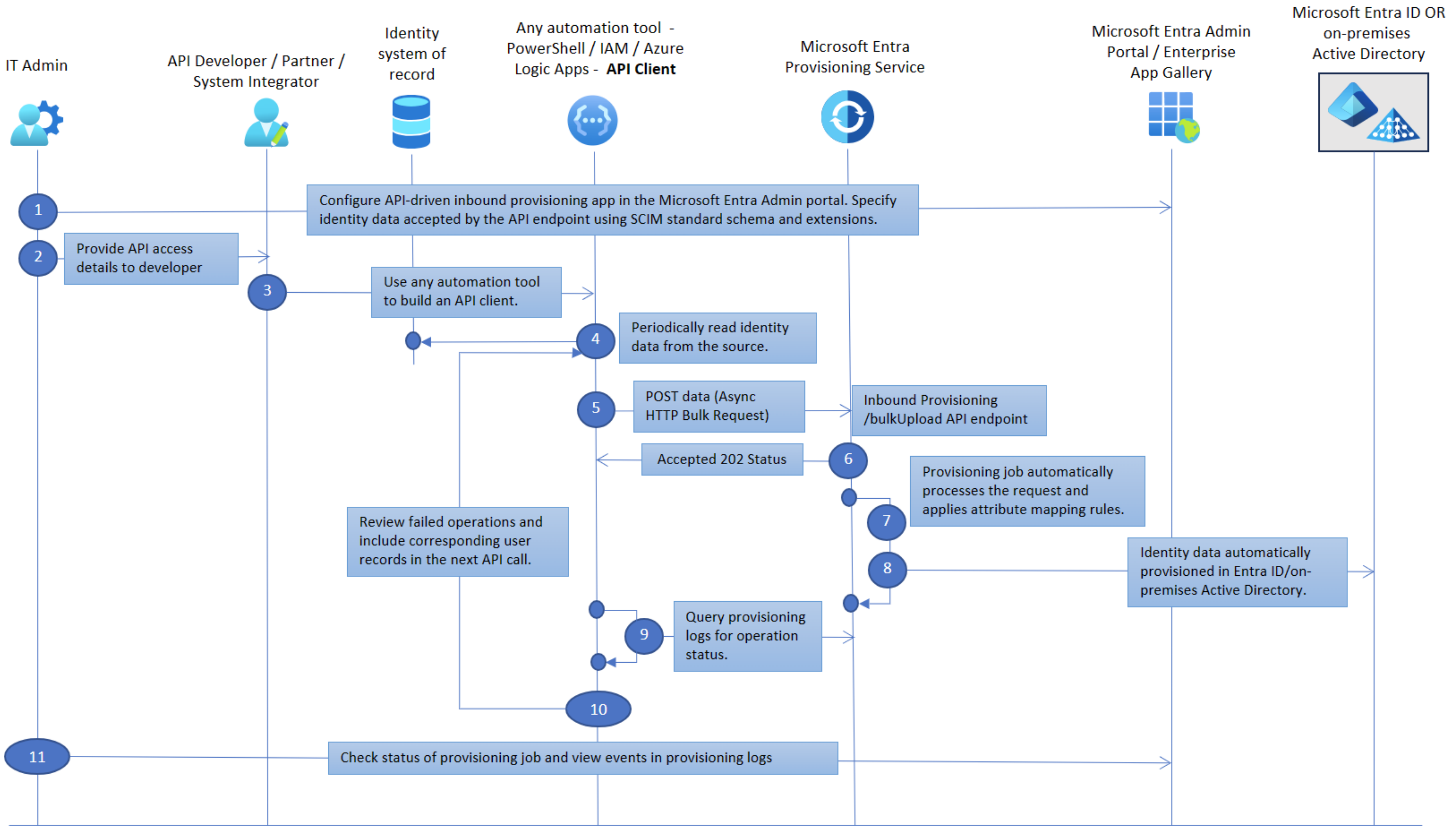
What if my organization doesn’t use Workday or SuccessFactors?

You can use Microsoft Entra ID API-driven provisioning



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 / ISV’s
Event-based / periodic sync
Native connector shipped by HR ISVs to automatically keep identity data in sync
HTTP POST
Bulk Request
Microsoft Entra ID 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
Microsoft Entra ID
Azure AD Provisioning Service
AADConnect / Cloud Sync
Hybrid users
Active Directory on-premises

End to End flow


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

Walkthrough / Demo

Cloud HR Provisioning

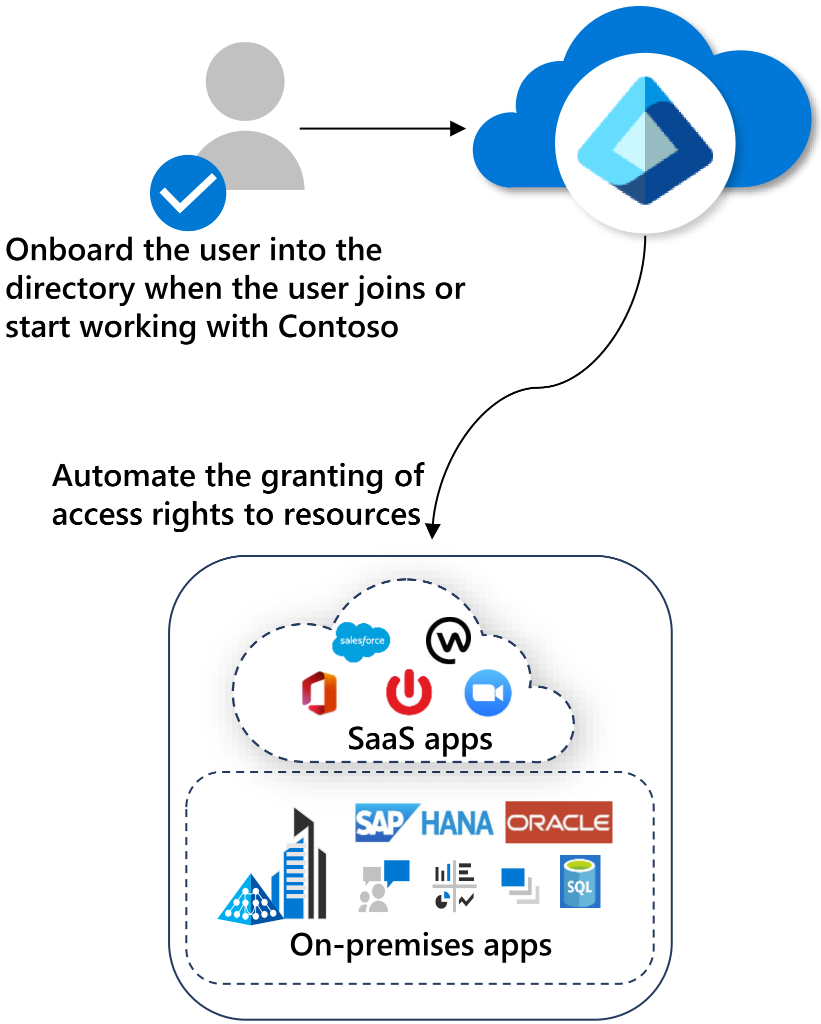
API-Driven Provisioning

Useful Links

aka.ms/EIGAProvisioningAPI

aka.ms/ProvisioningAPIQuickStart

Provisioning user to Apps



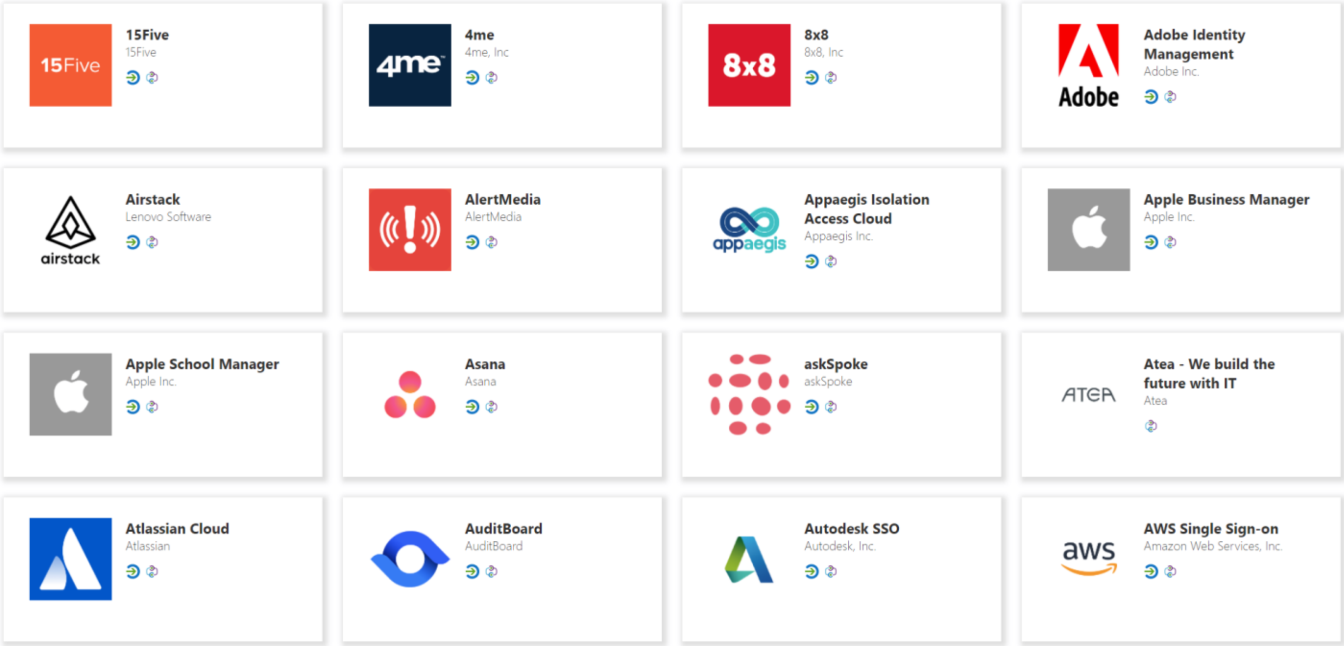
Onboard the user into the directory when the user joins or start working with Contoso

Automate the granting of access rights to resources

SaaS apps

On-premises apps

Provisioning to SaaS apps using SCIM



15Five
15Five

4me
4me, Inc

8x8
8x8, Inc

Adobe Identity Management
Adobe Inc.

Airstack
Lenovo Software

AlertMedia
AlertMedia

Appaegis Isolation Access Cloud
Appaegis Inc.

Apple Business Manager
Apple Inc.

Apple School Manager
Apple Inc.

Asana
Asana

askSpoke
askSpoke

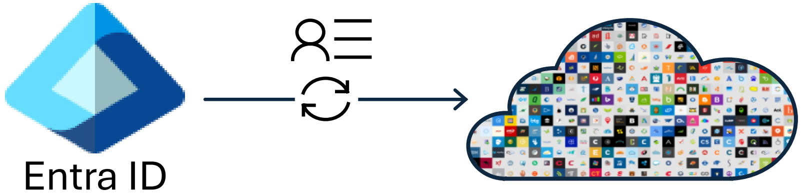
Atea - We build the future with IT
Atea

Atlassian Cloud
Atlassian

AuditBoard
AuditBoard

Autodesk SSO
Autodesk, Inc.

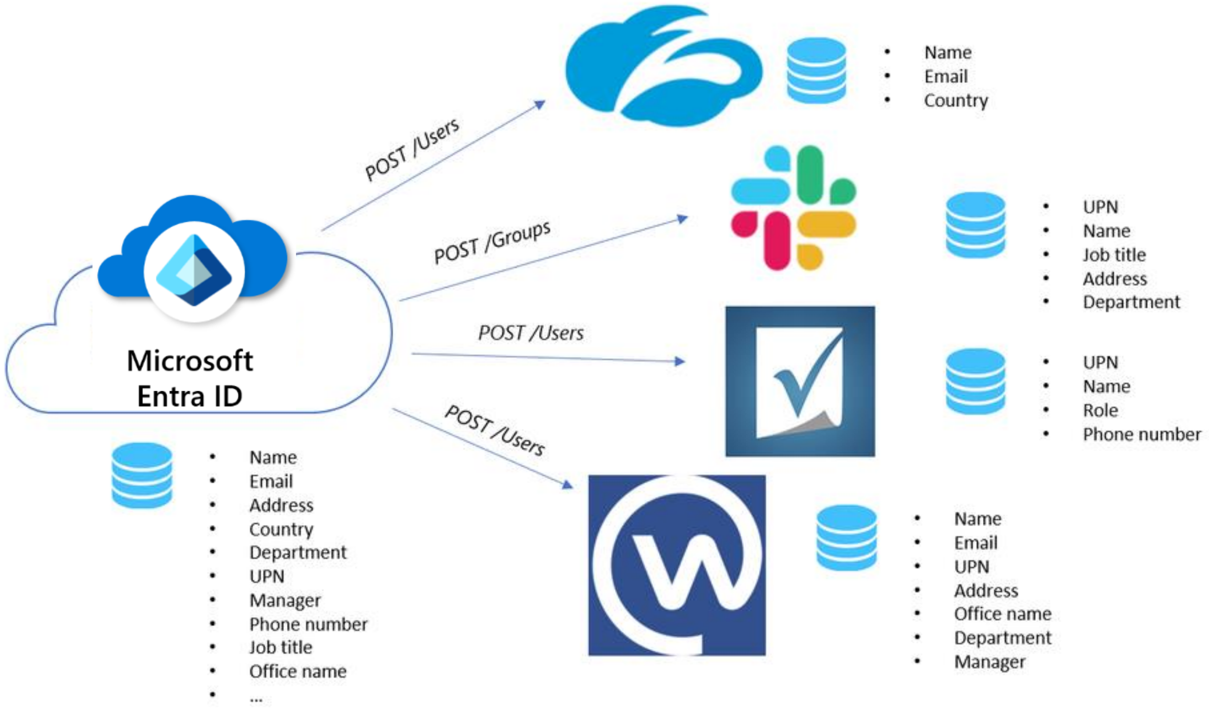
AWS Single Sign-on
Amazon Web Services, Inc.



Entra ID

SaaS applications

Configure provisioning with SCIM endpoint



- SCIM 2.0 is a standardized definition of two endpoints /Users and /Groups
- Uses Rest API endpoints to create, update and delete objects

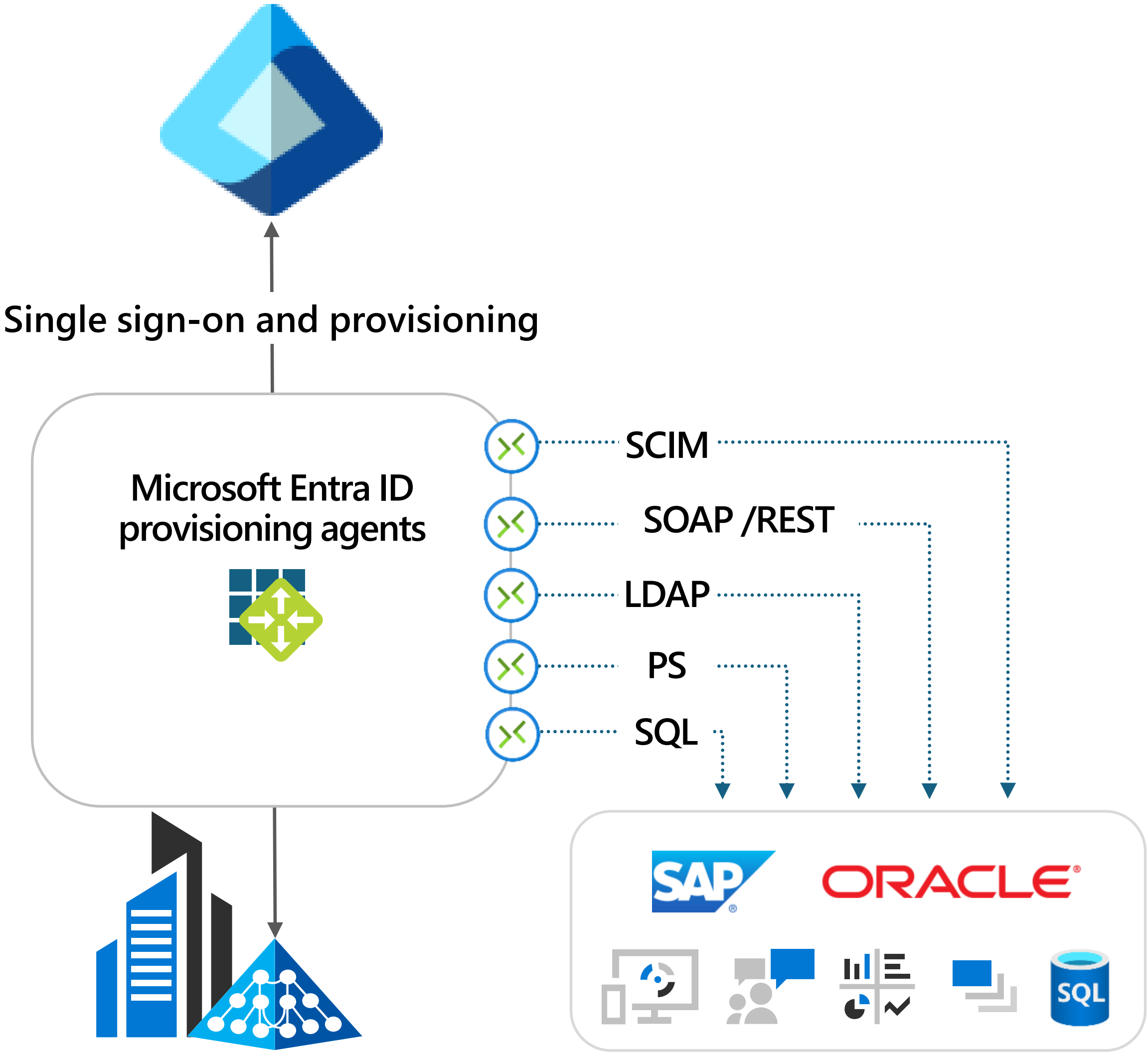
Provisioning to on-premises applications

Users and schema defined in the cloud

- Supports provisioning from custom schema extensions to app-specific properties.

Translation to the provisioning protocols expected by apps

- Microsoft-delivered connectors: LDAP, SQL, etc.
- Ecosystem of third-party connectors for other apps requiring custom API integrations
- Customers can re-use their existing MIM connectors


Single sign-on and provisioning
Microsoft Entra ID provisioning agents
SCIM
SOAP /REST
LDAP
PS
SQL
SAP
ORACLE
SQL

Samples: App provisioning samples for SCIM-enabled apps

Walkthrough / Demo

App provisioning

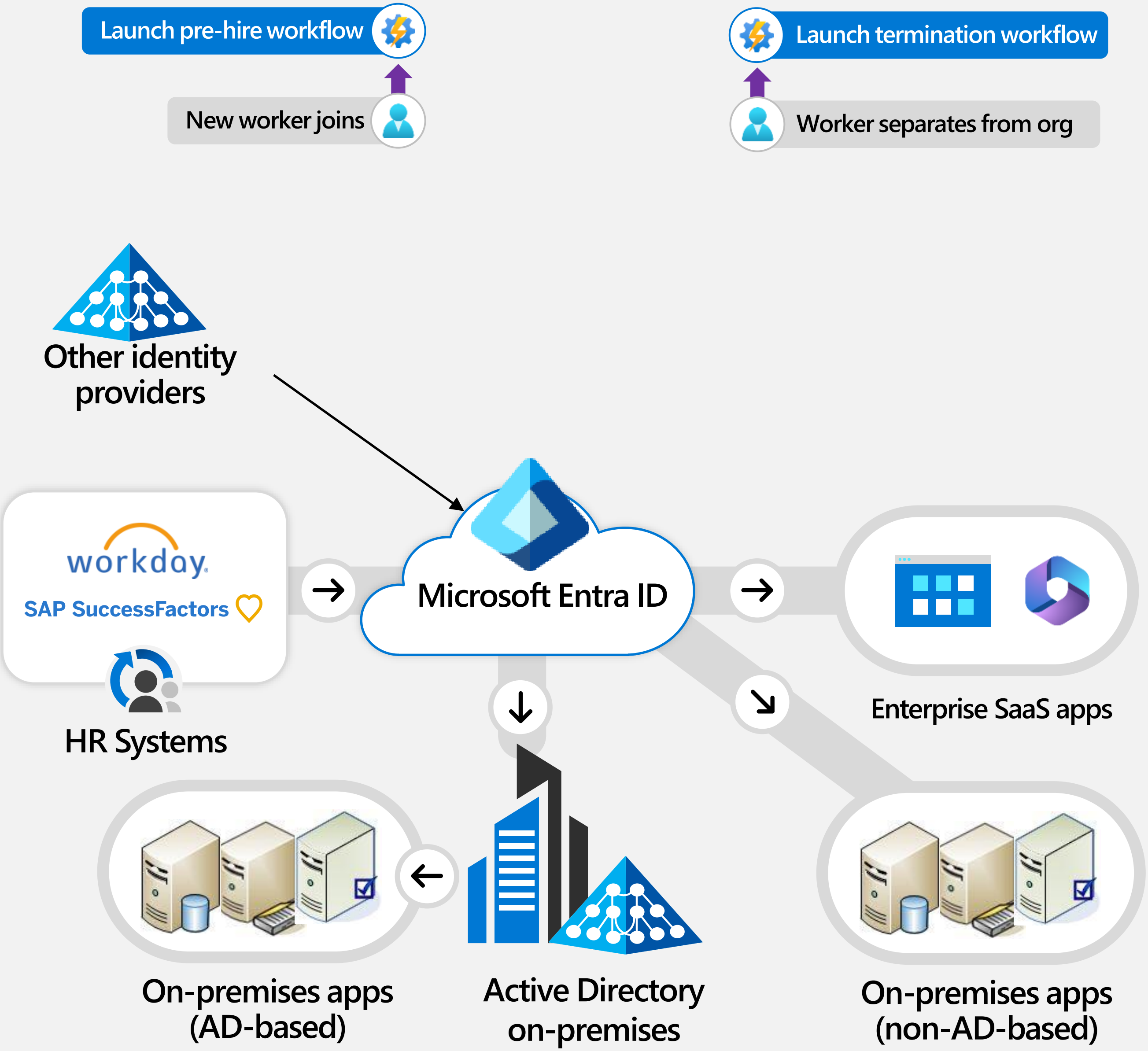
ECMA

Break

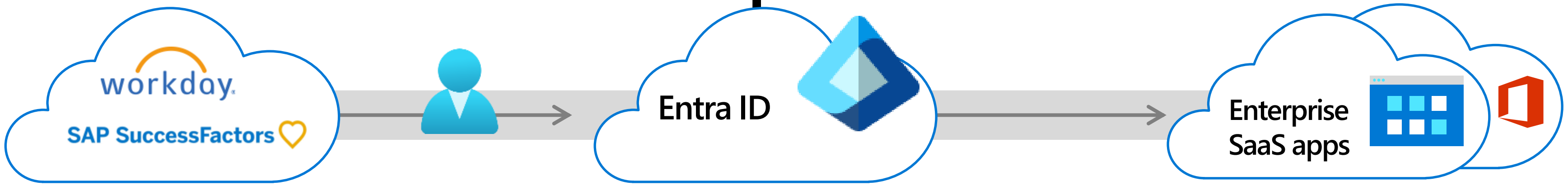
Lifecycle Workflows

Automate join/move/leave employee lifecycle events

- Organizations can schedule tasks to occur before, at or after a join or leave date; these can also be run on-demand.
- Built-in tasks include generating temporary credentials, sending emails, updating user attributes, and memberships, and removing licenses.
- Customers and partners can extend lifecycle workflows with additional tasks via Azure Logic Apps.


Launch pre-hire workflow
New worker joins
Launch termination workflow
Worker separates from org
Other identity providers
workday.
SAP SuccessFactors
HR Systems
Microsoft Entra ID
Enterprise SaaS apps
On-premises apps (AD-based)
Active Directory on-premises
On-premises apps (non-AD-based)

Joiner scenario - Example



workday

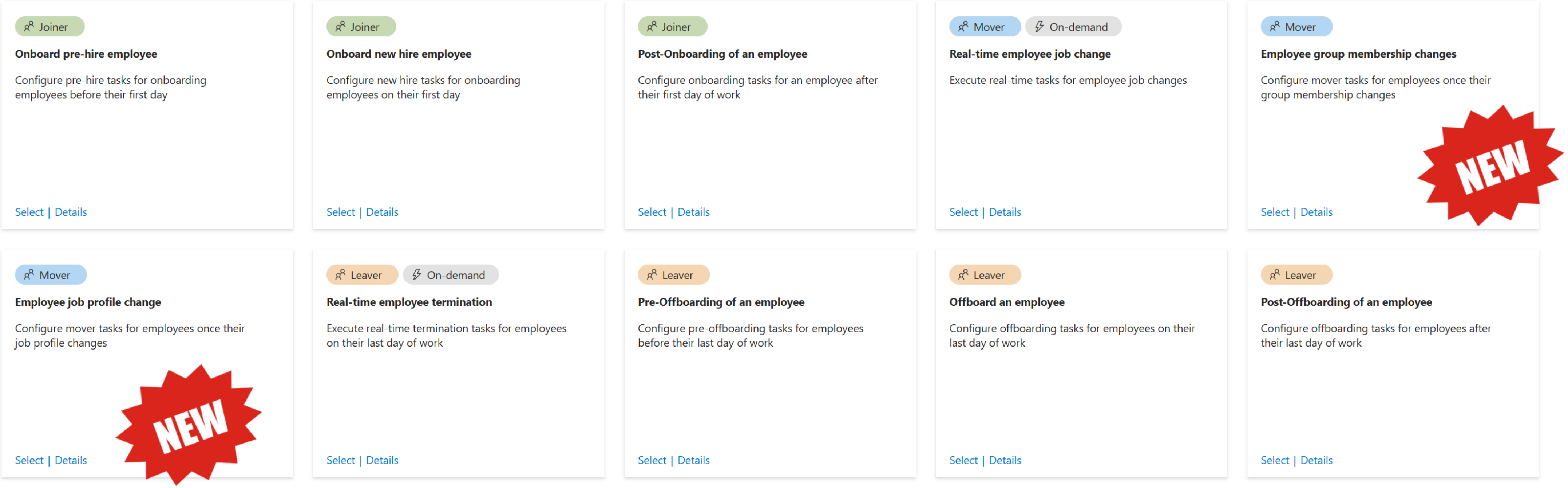
SAP SuccessFactors

Entra ID

Enterprise SaaS apps

Joiner · PRE-HIRE	For pre-hire, "X" days before employee's start date,	Create user account (status=disabled)	'X' days before start	Send email to onboarding DL	Launch custom Logic Apps workflow	Generate Temporary Access Pass (TAP)	Send email to hiring manager with TAP
Joiner · HIRE	On the employee's start date, perform the following tasks.	On start date	On start date	Enable user account	Group assignments	Send welcome email to new hire	Add user to Teams "New Hires" channel
Joiner · WELCOME	Employee's day 1 and Manager shares the temporary access pass.	On start date	On Day 1	Login with temporary access pass	Setup passwordless sign-in Windows Hello / FIDO key	Welcome messages in Teams channel	"Best onboarding experience ever!"

Lifecycle workflows built-in templates



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

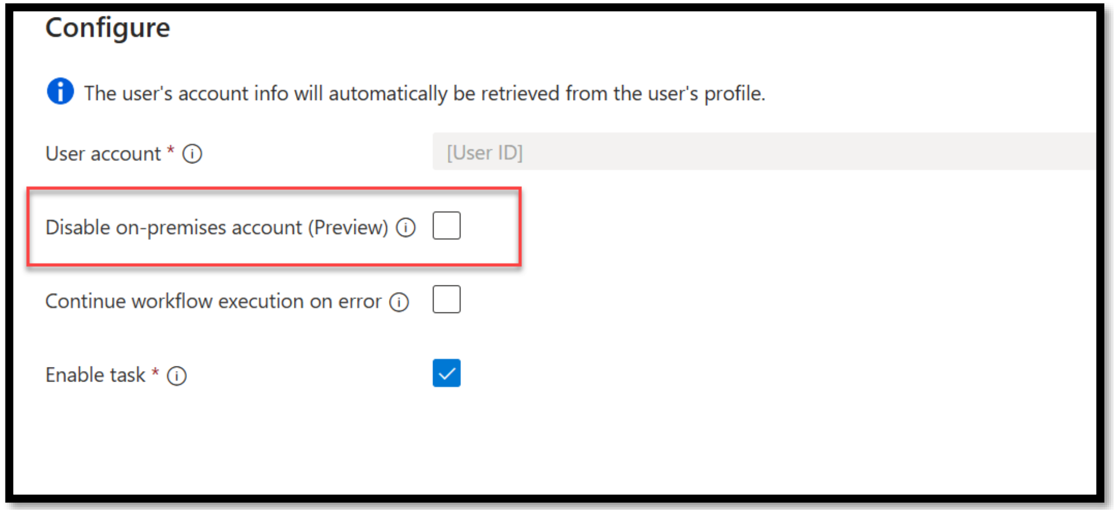
Leaver
Pre-Offboarding of an employee
Configure pre-offboarding tasks for employees before their last day of work
Select | Details

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

New Tasks within Lifecycle Workflows

Disable on-premises account



Configure

ℹ The user's account info will automatically be retrieved from the user's profile.

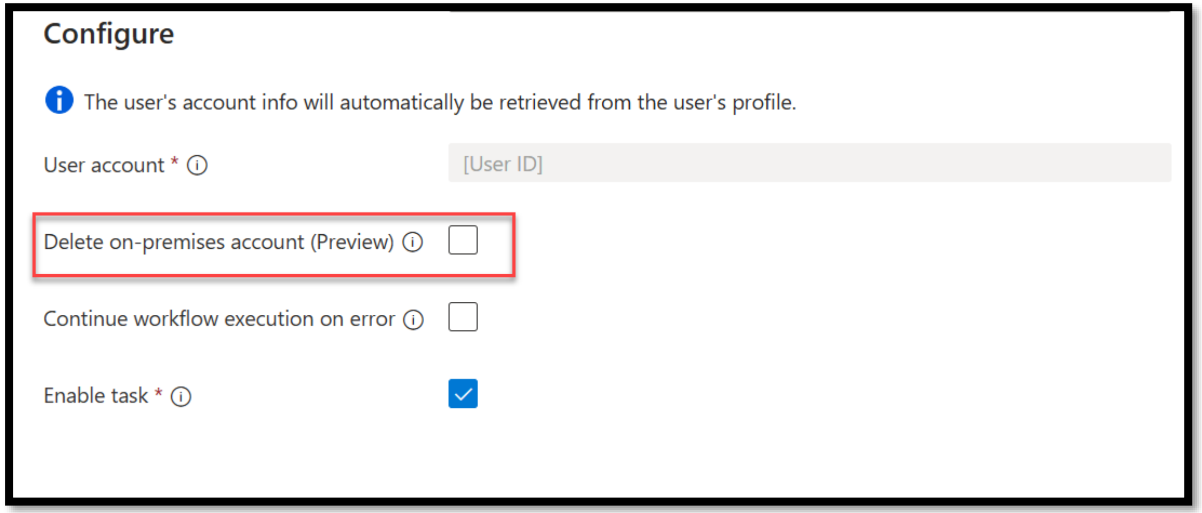
User account * ⓘ [User ID]

Disable on-premises account (Preview) ⓘ □

Continue workflow execution on error ⓘ □

Enable task * ⓘ ☑

Delete on-premises account



Configure

ℹ The user's account info will automatically be retrieved from the user's profile.

User account * ⓘ [User ID]

Delete on-premises account (Preview) ⓘ □

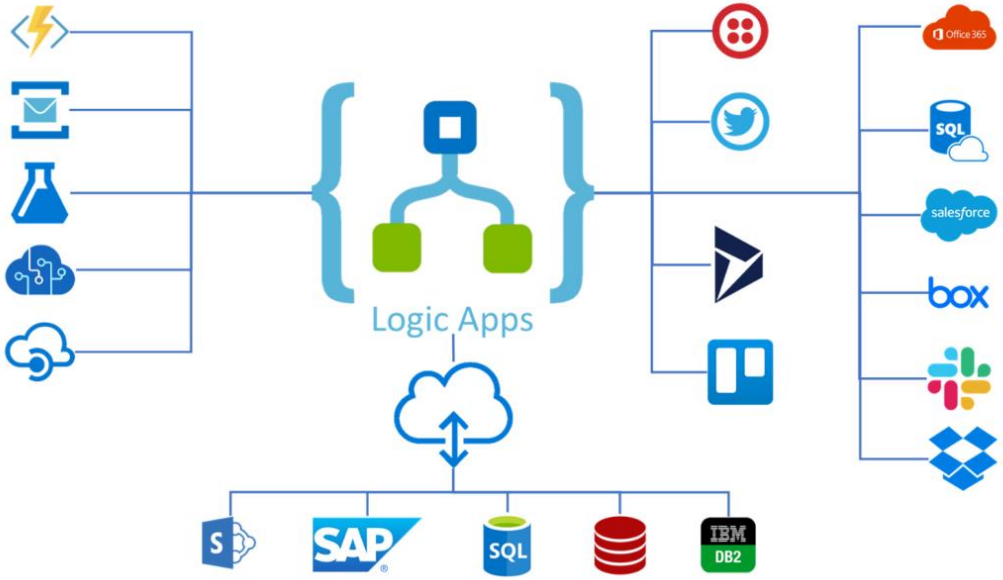
Continue workflow execution on error ⓘ □

Enable task * ⓘ ☑

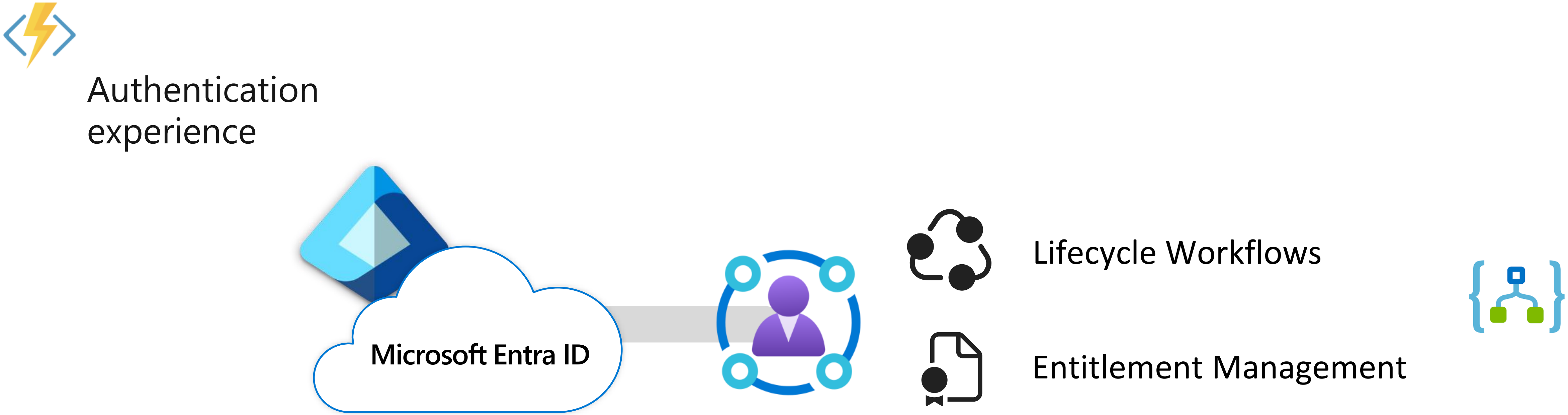
Microsoft Security

What is a Logic App?

Azure Logic Apps is a cloud platform where you can create and run automated workflows with little to no code. By using the visual designer and selecting from prebuilt operations, you can quickly build a workflow that integrates and manages your apps, data, services, and systems.



Which features support custom extensions?



Authentication experience

Microsoft Entra ID

Lifecycle Workflows

Entitlement Management

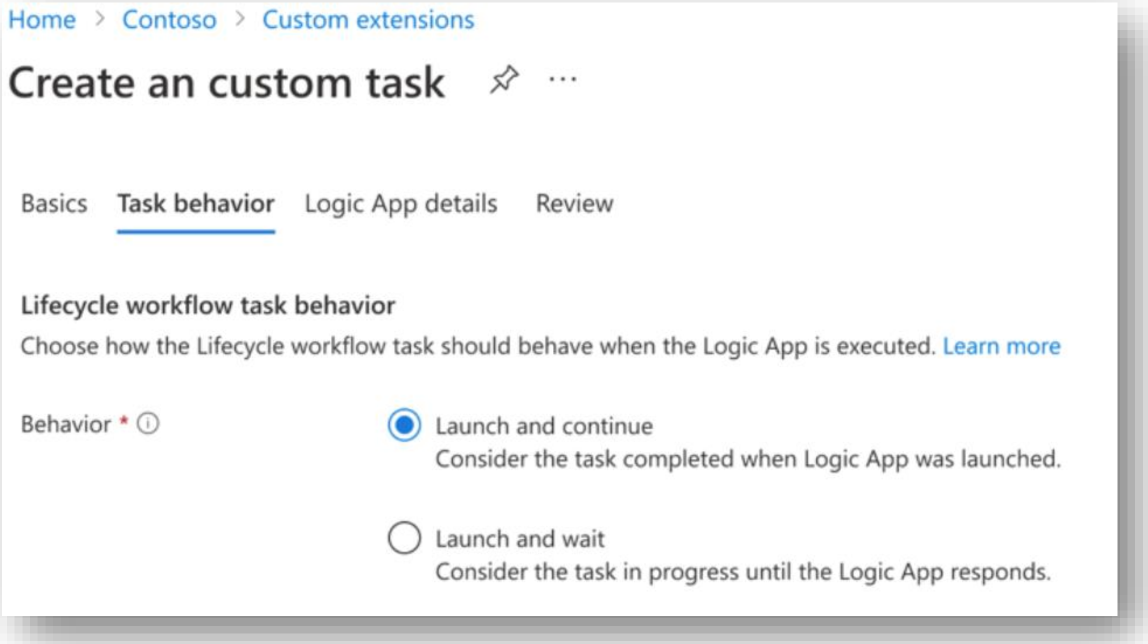
LCW + Custom Extensions (Logic Apps)

General Availability

- With the extensibility feature, Lifecycle Workflows currently support creating custom tasks extensions to call-out to Azure Logic Apps.
- The LCW extensibility feature allows you to utilize the concept of custom task extensions to call-out to external systems as part of a workflow.

Example

An admin could create and link a custom Logic App to a workflow, which ensures the user is also assigned certain characteristics in a third-party SaaS app (like Salesforce) or is sent a custom email.



Create an custom task

Lifecycle workflow task behavior

Choose how the Lifecycle workflow task should behave when the Logic App is executed. Learn more

Behavior *

● Launch and continue
Consider the task completed when Logic App was launched.

○ Launch and wait
Consider the task in progress until the Logic App responds.

Govern Access to Resources

Microsoft Entra ID Governance features used on this scenario

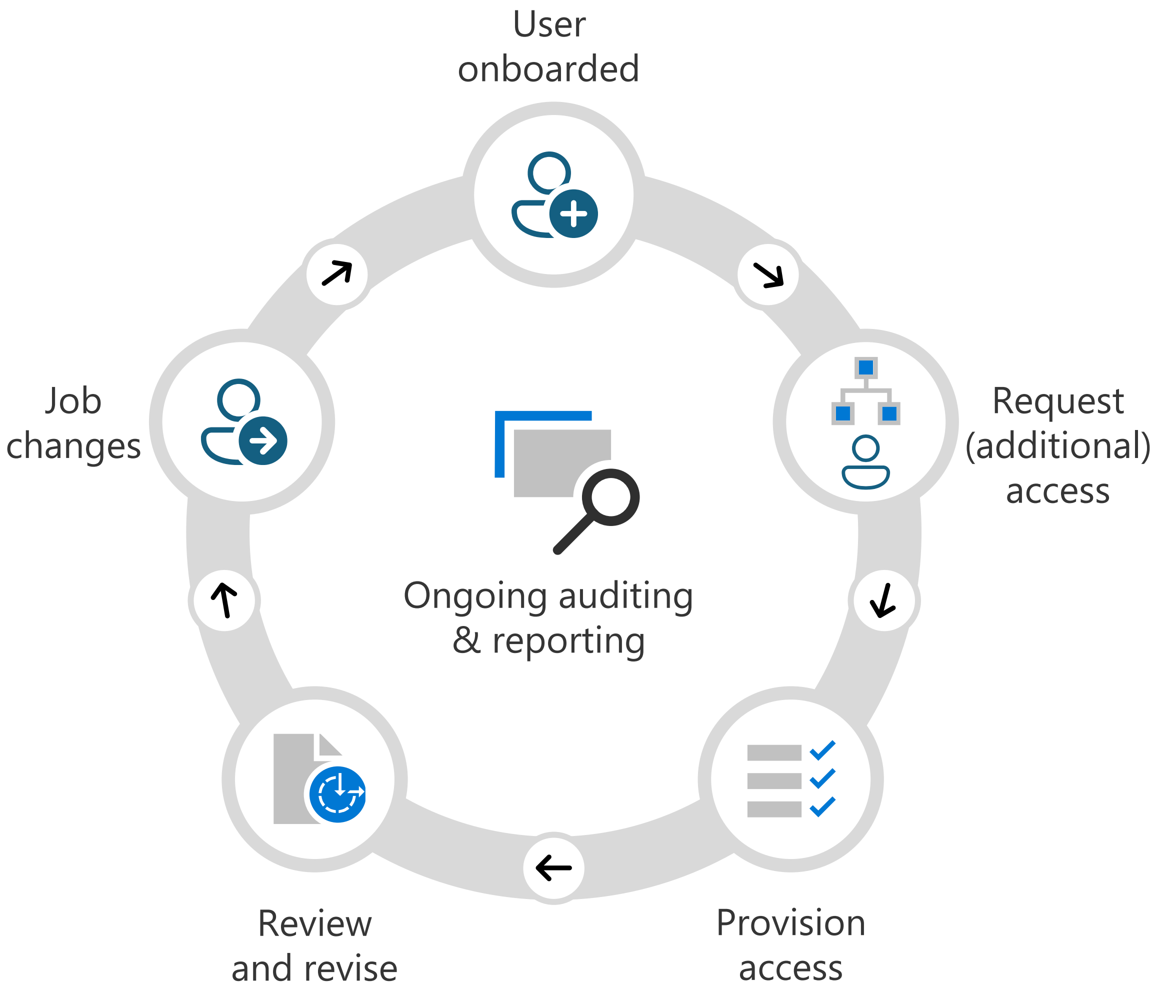
Feature	Description	Stage	Governance SKU
Entitlement Management (EM)	Enables organizations to manage identity and access lifecycle at scale, by automating access request workflows, access assignments, reviews, and expiration.	General Availability	No
EM + Custom Extensions (Logic Apps)	Logic Apps with entitlement management can expand governance workflows beyond the core entitlement management use cases.	General Availability	Yes
EM + Auto assignment policies	Use rules to determine access package assignment based on user properties in Azure Active Directory (Azure AD	General Availability	Yes
AR - Inactive Users	Review and address stale accounts that haven't been active for a specified period on a regular basis.	General Availability	Yes
AR - Machine learning assisted access certifications and reviews	Provides ML-based recommendations to the reviewers of an access review based on the organization's reporting structure.	General Availability	Yes
AR - PIM For Groups	Review access for PIM for Groups on a regular basis.	Public preview	Yes

Source
Microsoft Entra ID Governance licensing fundamentals

Access requests, workflow and approvals

Entitlement management

- Give users self-service access requests for resources and automate approval workflows and access assignment, reviews, and expiration for all human identity types (users, guests, etc.)
- Self-service policy and workflow can be defined by app, group or site owners
- Supports multi-stage approval workflows, separation of duties enforcement, and recurring access recertification
- Supports custom workflows for access lifecycle (through Logic Apps integration)
- Access time-limited, guests removed when last access expires



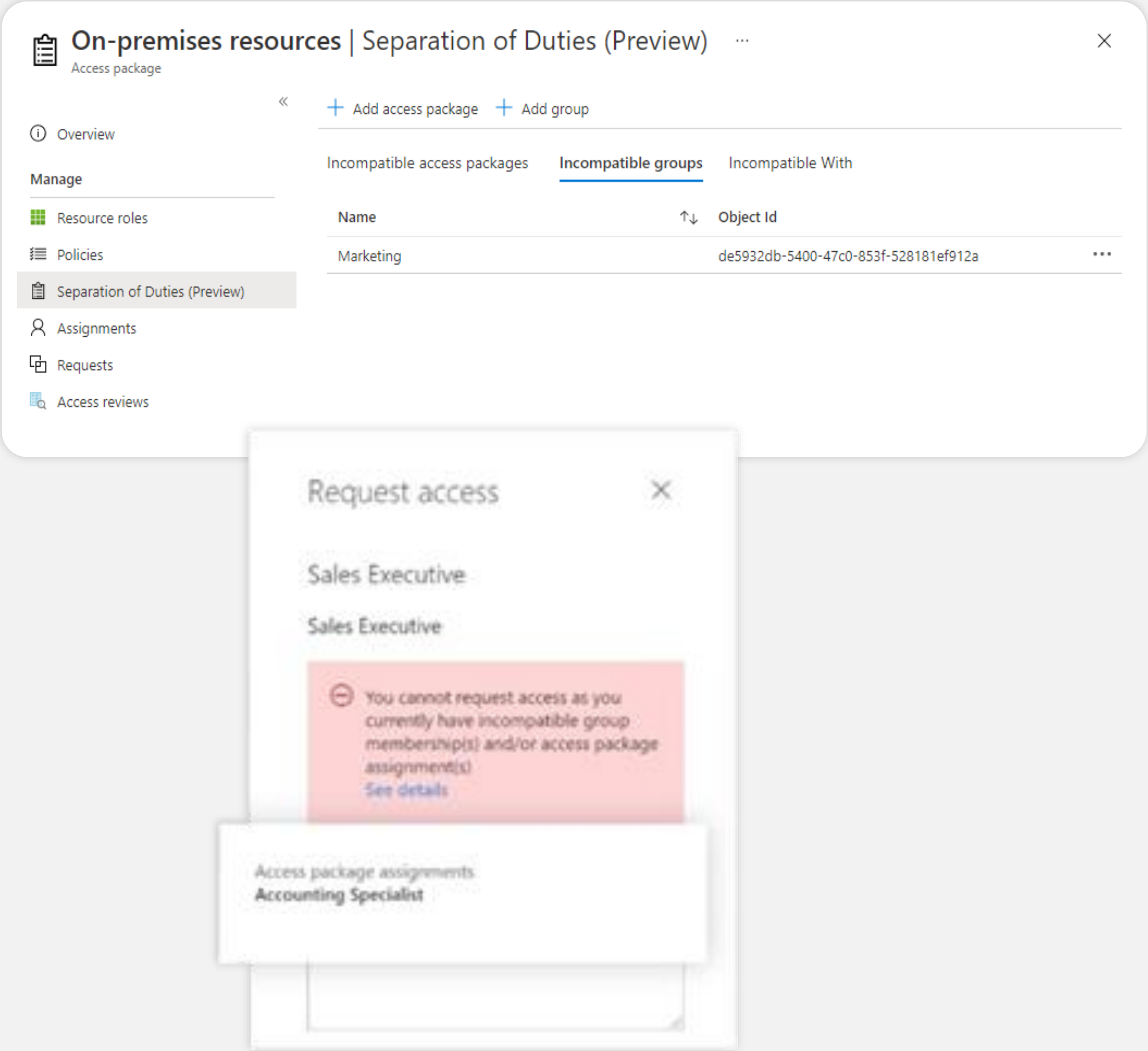
Separation of Duties

Restrict users from requesting an access package

- if they already have an assignment to another access package, or
- if they are a member of a group

Report on users who have incompatible access rights

Alert on users receiving access directly to applications



Name	Object Id
Marketing	de5932db-5400-47c0-853f-528181ef912a

Sales Executive

Sales Executive

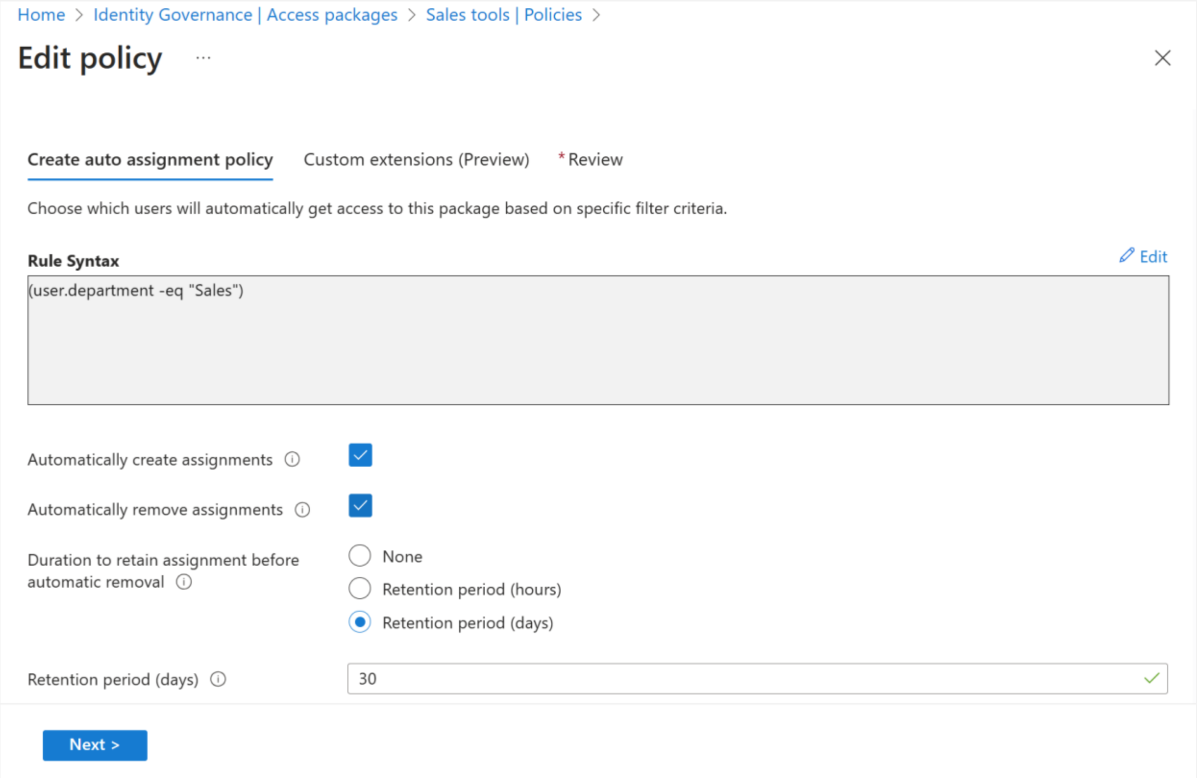
You cannot request access as you currently have incompatible group membership(s) and/or access package assignment(s)

Access package assignments
Accounting Specialist

Assign and remove resources automatically

Birthright assignment

- Use rules to determine access package assignment based on user properties, similar to dynamic groups.
- Assignments to users are added or removed depending on whether they meet the rule criteria.



Home > Identity Governance | Access packages > Sales tools | Policies >

Edit policy

Create auto assignment policy | Custom extensions (Preview) | * Review

Choose which users will automatically get access to this package based on specific filter criteria.

Rule Syntax

```
(user.department -eq "Sales")
```

Automatically create assignments ☑

Automatically remove assignments ☑

Duration to retain assignment before automatic removal: ○ None ○ Retention period (hours) ● Retention period (days)

Retention period (days): 30

Walkthrough / Demo

Lifecycle Workflows

Access Packages

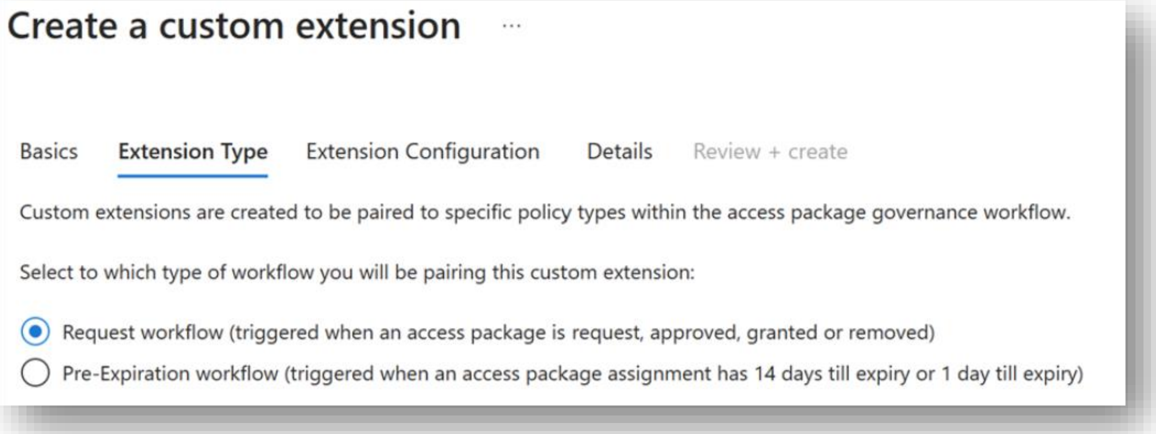
EM + Custom Extensions (Logic Apps)

General Availability

- Use Azure Logic Apps to automate custom workflows and connect apps and services in one place.
- Broaden your governance workflows beyond the core entitlement management use cases.

Example

An admin could create and link a custom Logic App to entitlement management, so that when a user requests an access package, a Logic App is triggered that ensures the user is also assigned certain characteristics in a third-party SaaS app (like Salesforce) or is sent a custom email.



Create a custom extension ...

Custom extensions are created to be paired to specific policy types within the access package governance workflow.

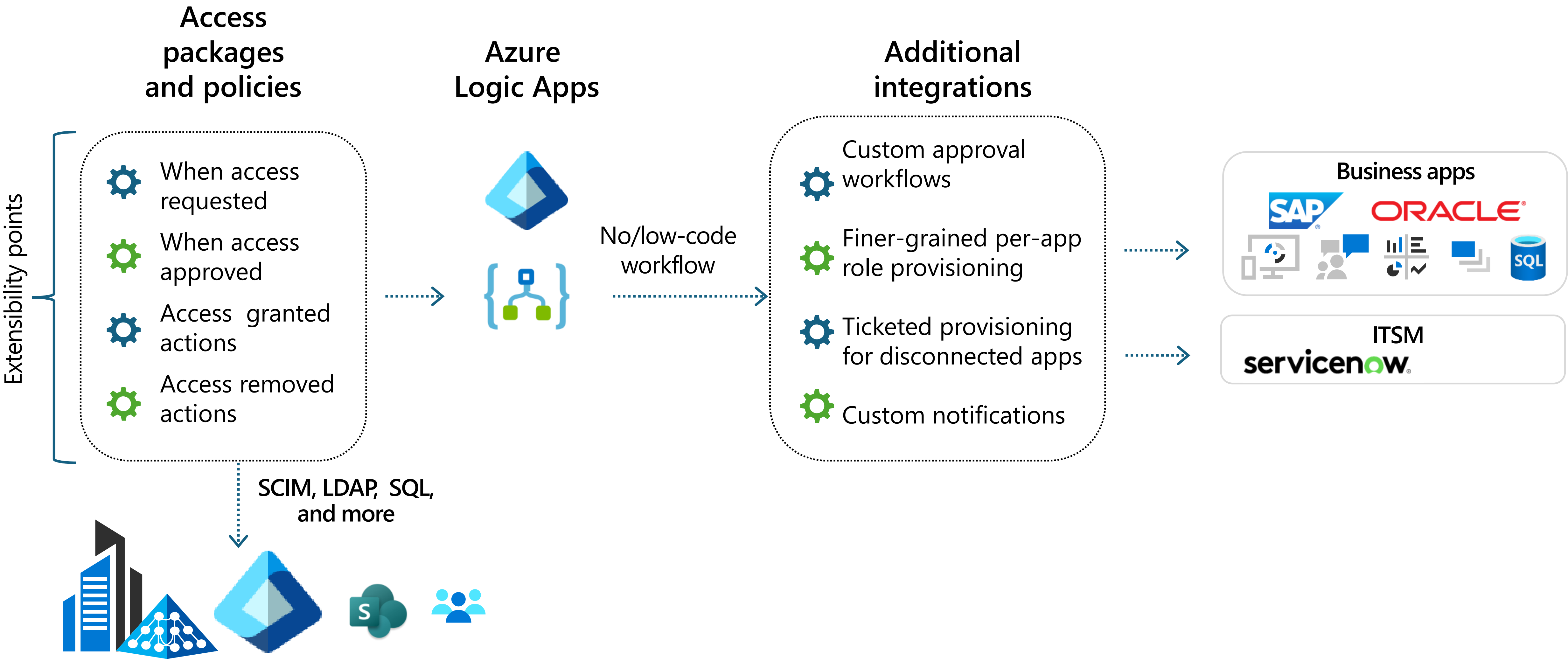
Select to which type of workflow you will be pairing this custom extension:

● Request workflow (triggered when an access package is request, approved, granted or removed)

○ Pre-Expiration workflow (triggered when an access package assignment has 14 days till expiry or 1 day till expiry)

Request and provisioning workflow integrations

Custom workflows for access lifecycle



Access packages and policies

Extensibility points

- When access requested
- When access approved
- Access granted actions
- Access removed actions

SCIM, LDAP, SQL, and more

Azure Logic Apps

No/low-code workflow

Additional integrations

- Custom approval workflows
- Finer-grained per-app role provisioning
- Ticketed provisioning for disconnected apps
- Custom notifications

Business apps

SAP ORACLE SQL

ITSM

servicenow

Walkthrough / Demo

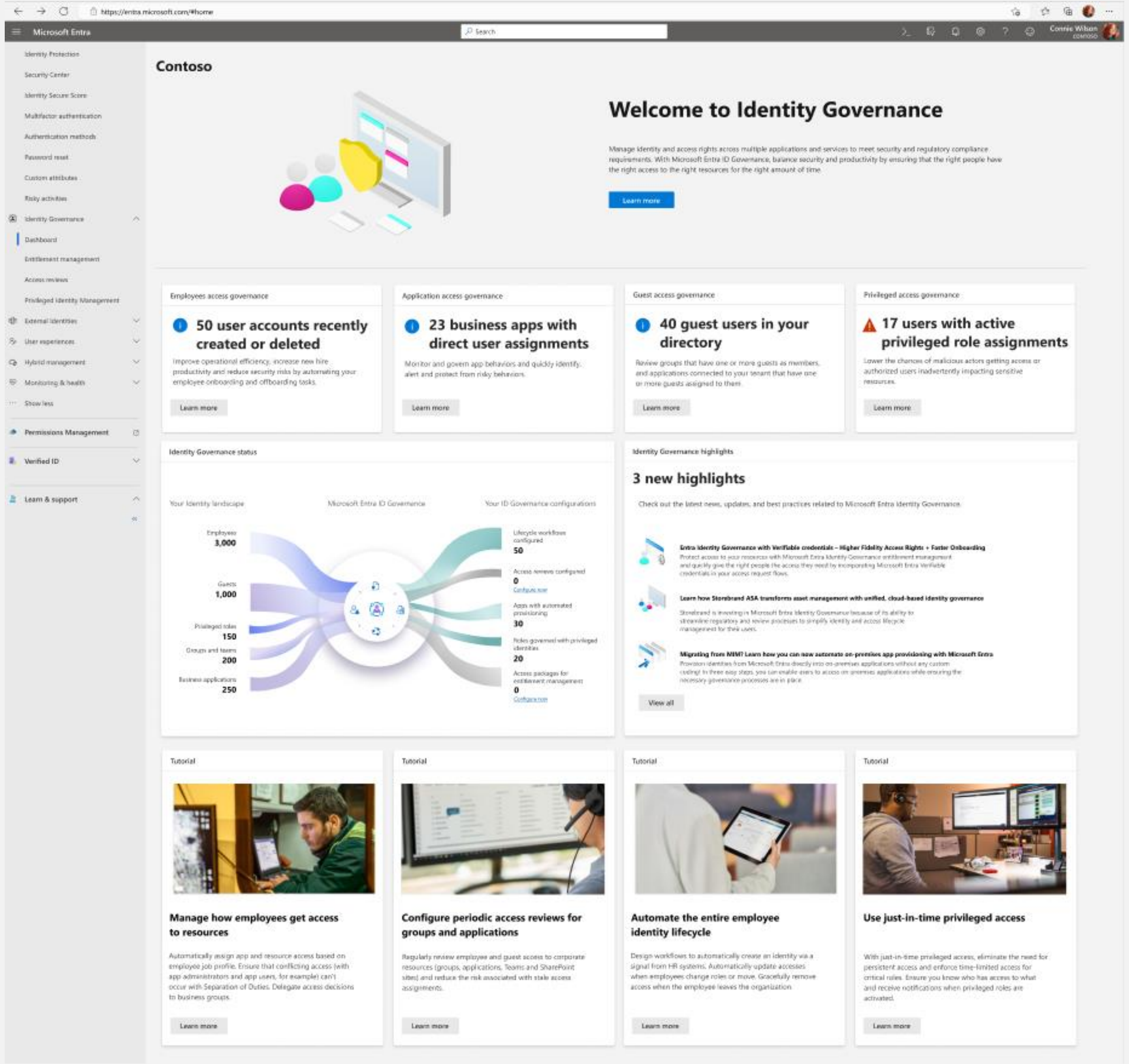
Access Packages + Custom Extensions

Break

Govern External Identities

Discover new insights and actions that will improve your ID Governance posture

- One page to to track your ID Governance journey
- Action oriented activity insights
- Assess whether and how you need to respond to potential issues
- Intelligent recommendations to optimize your environment



Contoso

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

Employees access governance

50 user accounts recently created or deleted

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

Learn more

Application access governance

23 business apps with direct user assignments

Monitor and govern app behaviors and quickly identify, alert and protect from risky behaviors.

Learn more

Guest access governance

40 guest users in your directory

Review groups that have one or more guests as members, and applications connected to your tenant that have one or more guests assigned to them.

Learn more

Privileged access governance

17 users with active privileged role assignments

Lower the chances of malicious actors getting access or authorized users inadvertently impacting sensitive resources.

Learn more

Identity Governance status

Your Identity landscape
Microsoft Entra ID Governance
Your ID Governance configurations
Employees
3,000
Guests
1,000
Privileged roles
150
Groups and teams
200
Business applications
250
Lifecycle workflows configured
50
Access reviews configured
0
Configure now
Apps with automated provisioning
30
Roles governed with privileged identities
20
Access packages for entitlement management
0
Configure now

Identity Governance highlights

3 new highlights

Check out the latest news, updates, and best practices related to Microsoft Entra Identity Governance.

Entra Identity Governance with Verifiable credentials – Higher Fidelity Access Rights + Faster Onboarding
Protect access to your resources with Microsoft Entra Identity Governance entitlement management and quickly give the right people the access they need by incorporating Microsoft Entra Verifiable credentials in your access request flows.

Learn how Storebrand ASA transforms asset management with unified, cloud-based identity governance
Storebrand is investing in Microsoft Entra Identity Governance because of its ability to streamline regulatory and review processes to simplify identity and access lifecycle management for their users.

Migrating from MIM? Learn how you can now automate on-premises app provisioning with Microsoft Entra
Provision identities from Microsoft Entra directly into on-premises applications without any custom coding! In three easy steps, you can enable users to access on-premises applications while ensuring the necessary governance processes are in place.

View all

Tutorial

Manage how employees get access to resources

Automatically assign app and resource access based on employee job profile. Ensure that conflicting access (with app administrators and app users, for example) can't occur with Separation of Duties. Delegate access decisions to business groups.

Learn more

Tutorial

Configure periodic access reviews for groups and applications

Regularly review employee and guest access to corporate resources (groups, applications, Teams and SharePoint sites) and reduce the risk associated with stale access assignments.

Learn more

Tutorial

Automate the entire employee identity lifecycle

Design workflows to automatically create an identity via a signal from HR systems. Automatically update accesses when employees change roles or move. Gracefully remove access when the employee leaves the organization.

Learn more

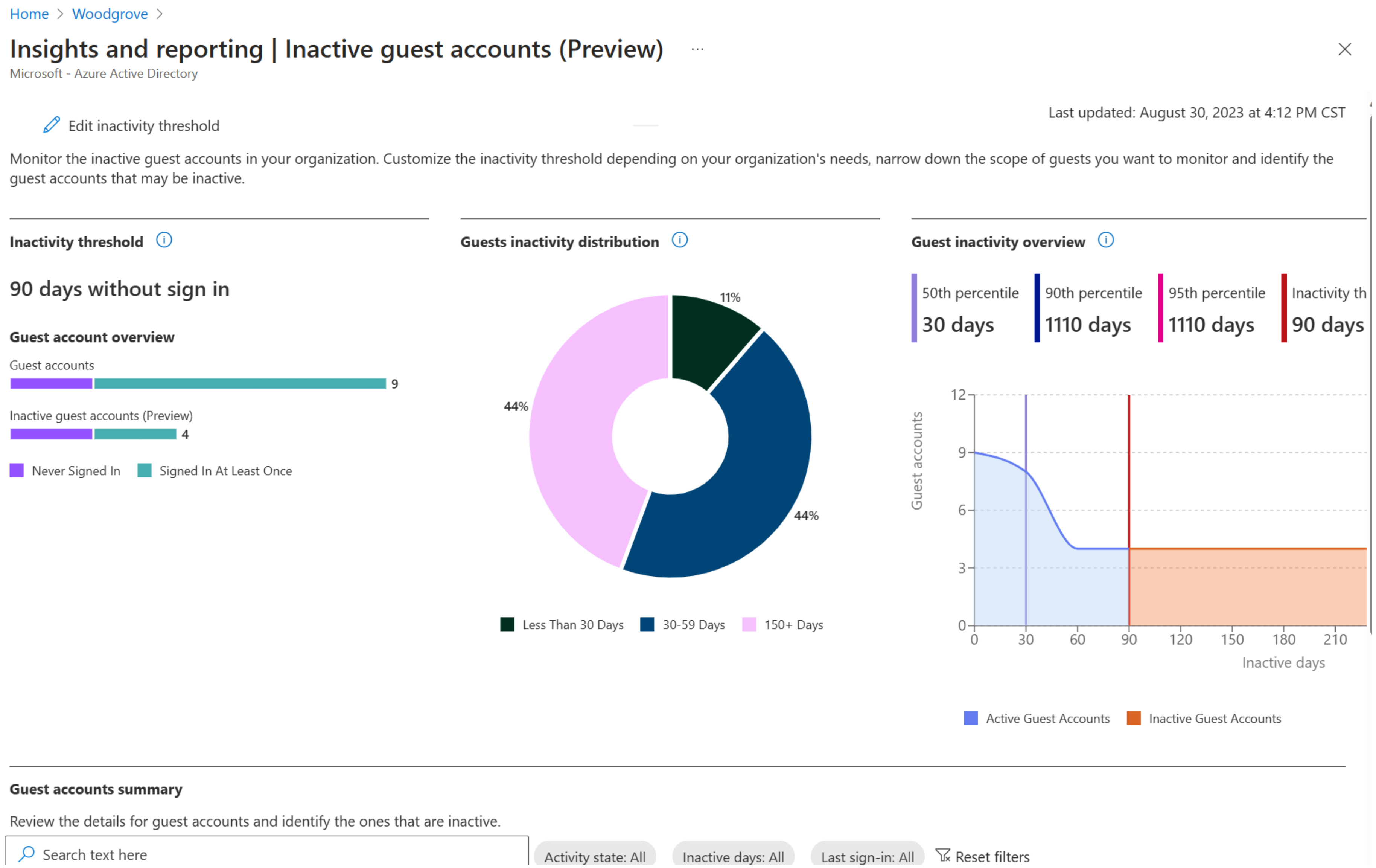
Tutorial

Use just-in-time privileged access

With just-in-time privileged access, eliminate the need for persistent access and enforce time-limited access for critical roles. Ensure you know who has access to what and receive notifications when privileged roles are activated.

Learn more

Get Insights on existing External Users



Home > Woodgrove >

Insights and reporting | Inactive guest accounts (Preview) ···

Microsoft - Azure Active Directory

Edit inactivity threshold

Last updated: August 30, 2023 at 4:12 PM CST

Monitor the inactive guest accounts in your organization. Customize the inactivity threshold depending on your organization's needs, narrow down the scope of guests you want to monitor and identify the guest accounts that may be inactive.

Inactivity threshold ⓘ

90 days without sign in

Guest account overview

Guest accounts 9

Inactive guest accounts (Preview) 4

🟪 Never Signed In 🟦 Signed In At Least Once

Guests inactivity distribution ⓘ

Guest inactivity overview ⓘ

50th percentile	90th percentile	95th percentile	Inactivity th
30 days	1110 days	1110 days	90 days

Guest accounts summary

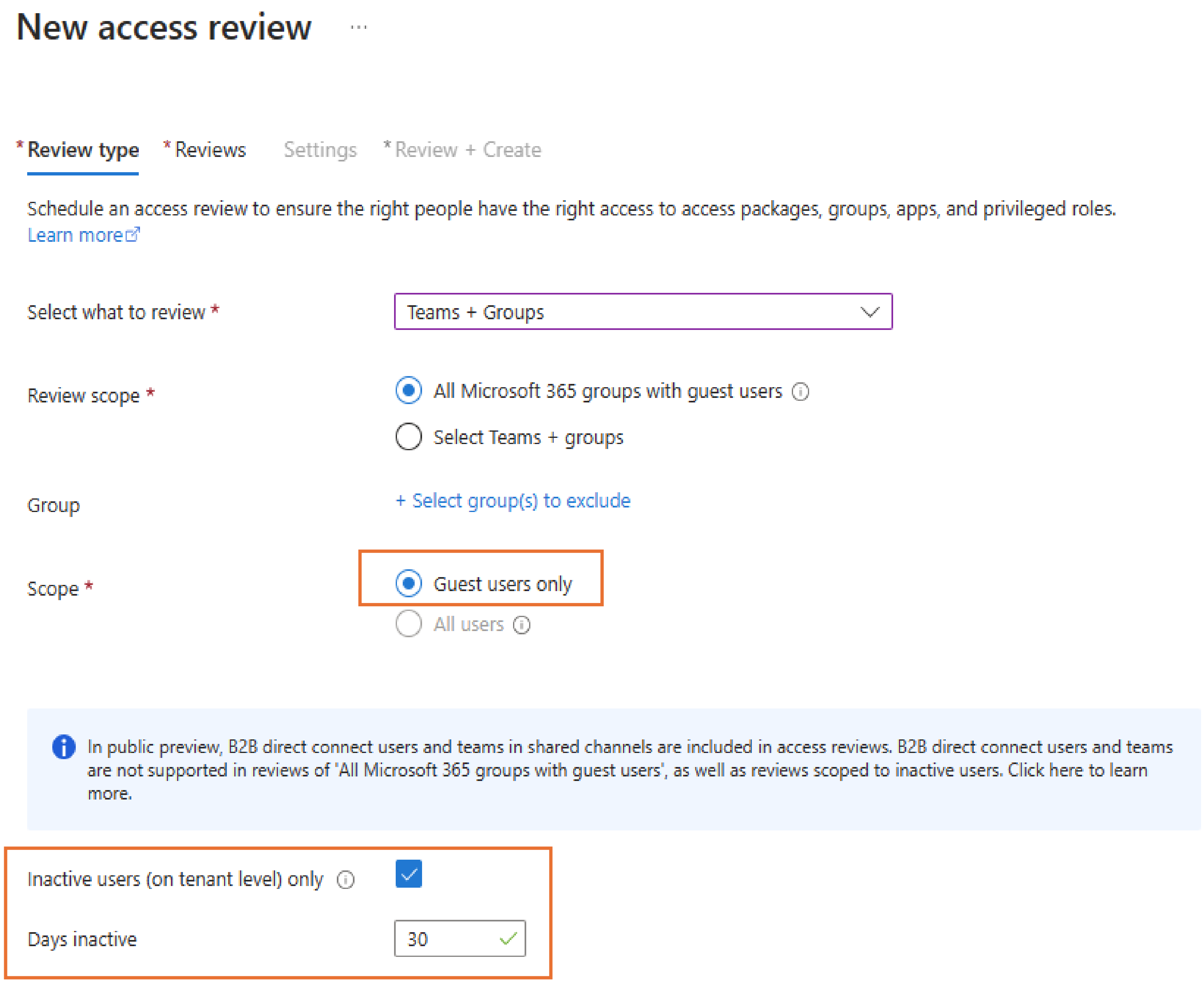
Review the details for guest accounts and identify the ones that are inactive.

Access Certification for Guests

You can review either:

- A group in Entra ID that has one or more guests as members.
- An application connected to Entra ID that has one or more guest users assigned to it.

- A guest is “inactive” if a sign in event isn’t recorded in 30 days



New access review ···

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

Review scope *
● All Microsoft 365 groups with guest users ⓘ
○ Select Teams + groups

Group
+ Select group(s) to exclude

Scope *
● Guest users only
○ All users ⓘ

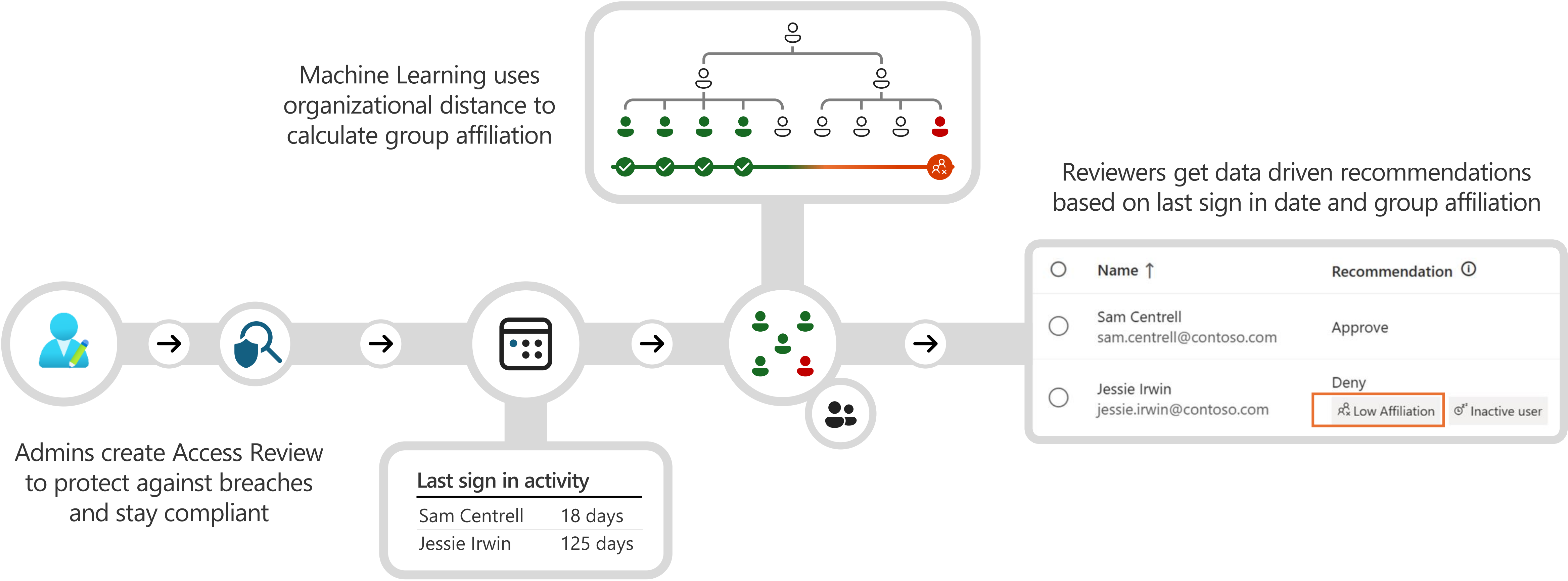
In public preview, B2B direct connect users and teams in shared channels are included in access reviews. B2B direct connect users and teams are not supported in reviews of 'All Microsoft 365 groups with guest users', as well as reviews scoped to inactive users. Click here to learn more.

Inactive users (on tenant level) only ⓘ ☑

Days inactive 30 ✓

Machine Learning based recommendations in Access Reviews

User-to-Group Affiliation



Admins create Access Review to protect against breaches and stay compliant

Machine Learning uses organizational distance to calculate group affiliation

Inactive user recommendation considers activity based on last sign in date

Reviewers get data driven recommendations based on last sign in date and group affiliation

Last sign in activity	
Sam Centrell	18 days
Jessie Irwin	125 days

○	Name ↑	Recommendation ⓘ
○	Sam Centrell sam.centrell@contoso.com	Approve
○	Jessie Irwin jessie.irwin@contoso.com	Deny Low Affiliation Inactive user

Demo: User-to-Group Affiliation

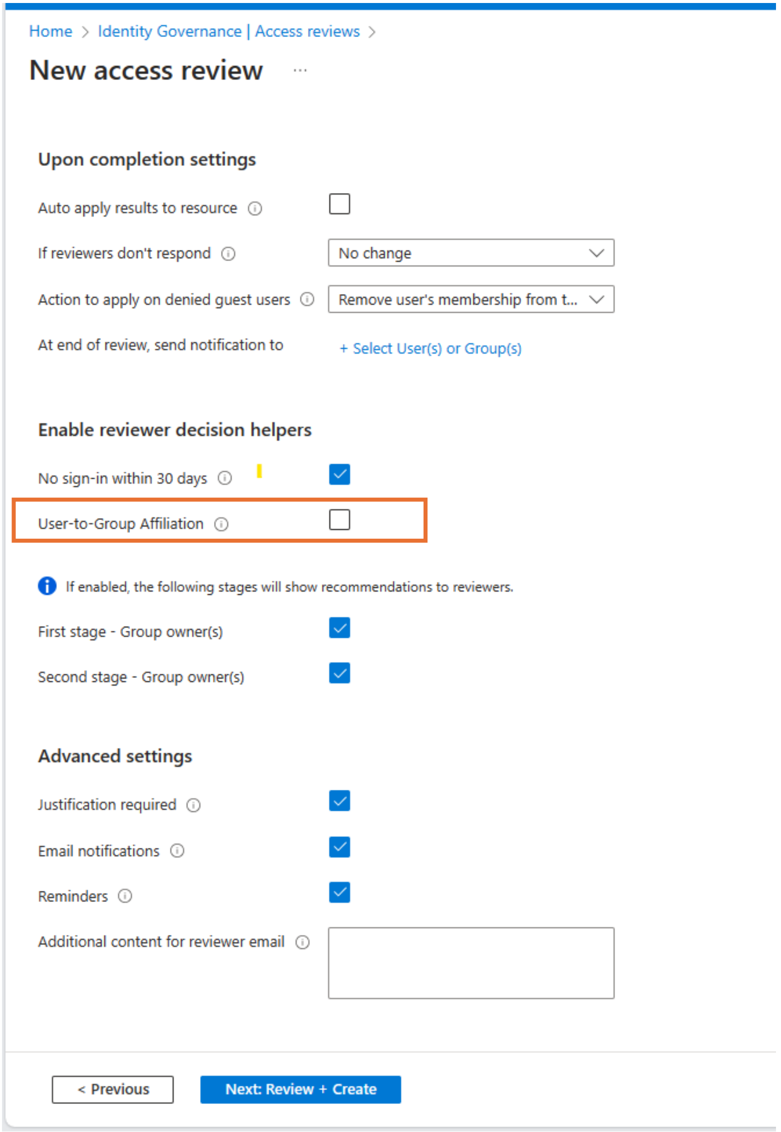
User to Group Affiliation

- Detects user affiliation with other users within the group, based on organization's reporting-structure similarity.

- Users who are distant from all the other group members based on their organization's chart, are considered to have "low affiliation" within the group.

*** Only available for users in your directory.*
*** A user should have a manager attribute*
***Groups with more than 600 users are not supported.*

Demo



Home > Identity Governance | Access reviews >

New access review ···

Upon completion settings

Auto apply results to resource ⓘ □

If reviewers don't respond ⓘ No change

Action to apply on denied guest users ⓘ Remove user's membership from t...

At end of review, send notification to + Select User(s) or Group(s)

Enable reviewer decision helpers

No sign-in within 30 days ⓘ ☑

User-to-Group Affiliation ⓘ □

ⓘ If enabled, the following stages will show recommendations to reviewers.

First stage - Group owner(s) ☑

Second stage - Group owner(s) ☑

Advanced settings

Justification required ⓘ ☑

Email notifications ⓘ ☑

Reminders ⓘ ☑

Additional content for reviewer email ⓘ

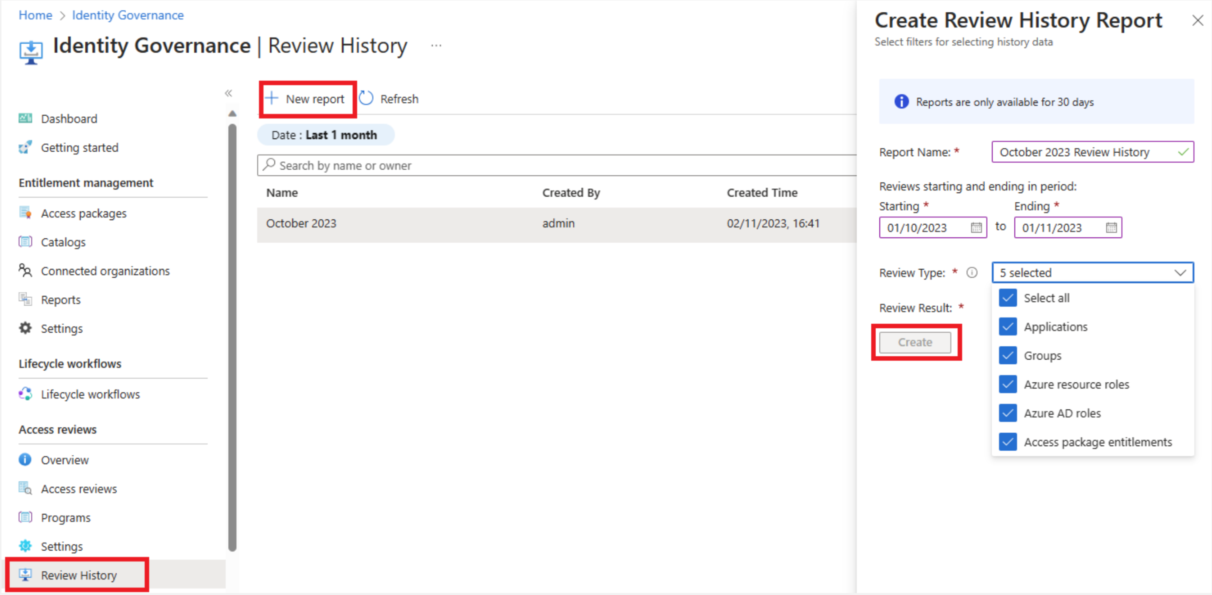
< Previous | Next: Review + Create

Access Review history report

- Downloadable review history to gain more insight on Access Reviews.

- Download results for audit and compliance needs, or to integrate with other solutions.

- Reports can be constructed to include specific access reviews, for a specific time frame, and can be filtered to include different review types and review result.



Date : **Last 1 month**

Name	Created By	Created Time
October 2023	admin	02/11/2023, 16:41

Create Review History Report

Select filters for selecting history data

Reports are only available for 30 days

Report Name: * October 2023 Review History

Reviews starting and ending in period:

Starting * 01/10/2023 to Ending * 01/11/2023

Review Type: * 5 selected

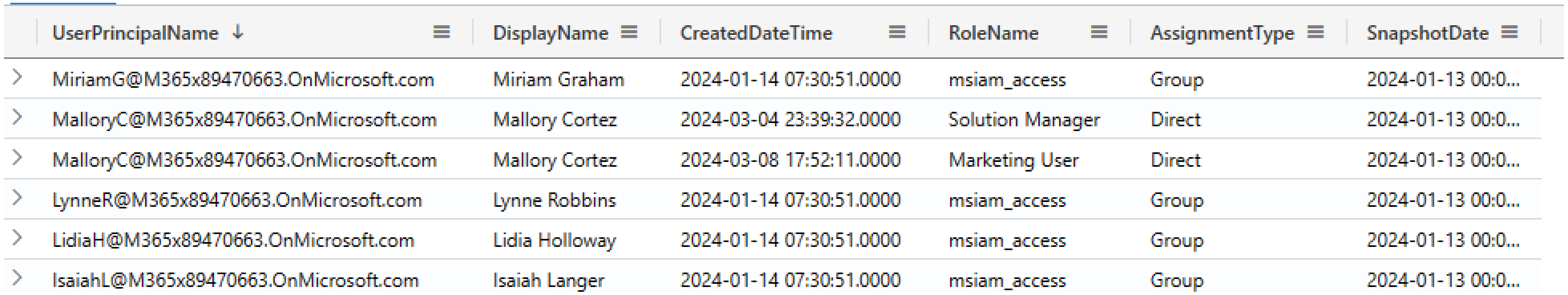
- ☑ Select all
- ☑ Applications
- ☑ Groups
- ☑ Azure resource roles
- ☑ Azure AD roles
- ☑ Access package entitlements

Review Result: *

Custom Reports

Customers need an approach to report on end-to-end access across Entra and key apps, including who had access at a given time in the past, how that access has changed, and who has access today.

- Setup Azure Data Explorer in an Azure Subscription
- Extracting data from Microsoft Entra and third-party applications using PowerShell scripts and MS Graph
- Ingesting the data into Azure Data Explorer
- Building custom queries using Kusto Query Language.



UserPrincipalName ↓	DisplayName	CreatedDateTime	RoleName	AssignmentType	SnapshotDate
MiriamG@M365x89470663.OnMicrosoft.com	Miriam Graham	2024-01-14 07:30:51.0000	msiam_access	Group	2024-01-13 00:0...
MalloryC@M365x89470663.OnMicrosoft.com	Mallory Cortez	2024-03-04 23:39:32.0000	Solution Manager	Direct	2024-01-13 00:0...
MalloryC@M365x89470663.OnMicrosoft.com	Mallory Cortez	2024-03-08 17:52:11.0000	Marketing User	Direct	2024-01-13 00:0...
LynneR@M365x89470663.OnMicrosoft.com	Lynne Robbins	2024-01-14 07:30:51.0000	msiam_access	Group	2024-01-13 00:0...
LidiaH@M365x89470663.OnMicrosoft.com	Lidia Holloway	2024-01-14 07:30:51.0000	msiam_access	Group	2024-01-13 00:0...
IsaiahL@M365x89470663.OnMicrosoft.com	Isaiah Langer	2024-01-14 07:30:51.0000	msiam_access	Group	2024-01-13 00:0...

To read the tutorial, visit: Custom reports using Microsoft Entra and application data - Microsoft Entra ID Governance | Microsoft Learn

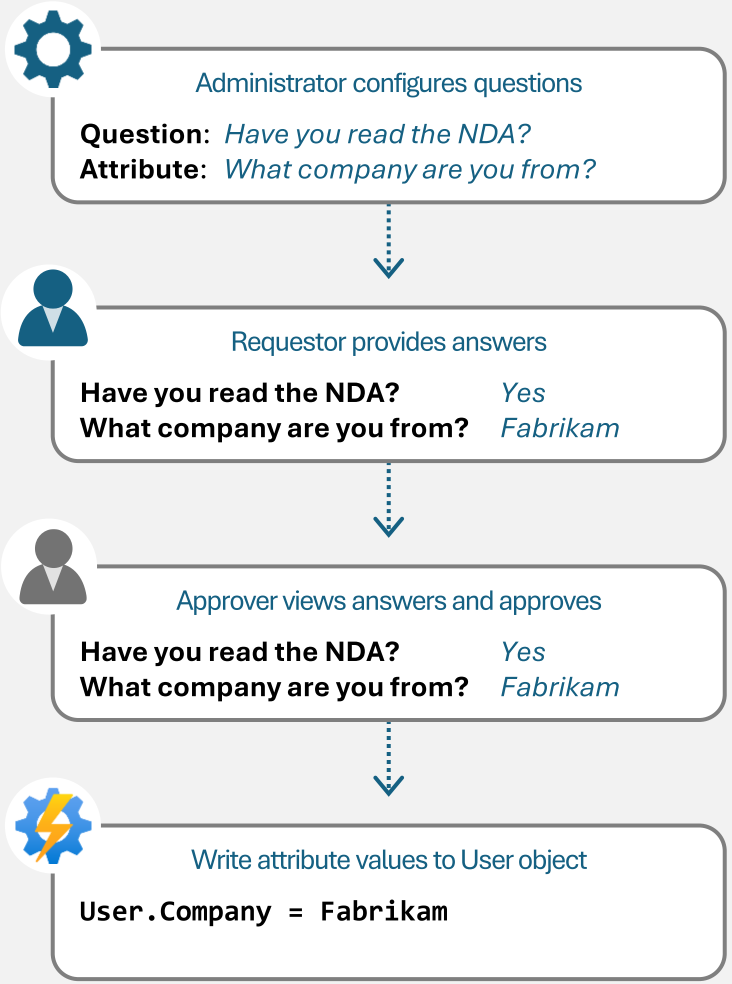
Guest attribute management

Collect additional information from requestors

- Include custom questions that are surfaced within the request flow.
- Approvers are shown the information as part of the request so they can make better decisions.

Store provided information in User attributes

- If your apps or processes need to reference it later, you can also store requestor information in attributes automatically.
- Especially useful for onboarding external users.



Administrator configures questions

Question: *Have you read the NDA?*
Attribute: *What company are you from?*

Requestor provides answers

Have you read the NDA? *Yes*
What company are you from? *Fabrikam*

Approver views answers and approves

Have you read the NDA? *Yes*
What company are you from? *Fabrikam*

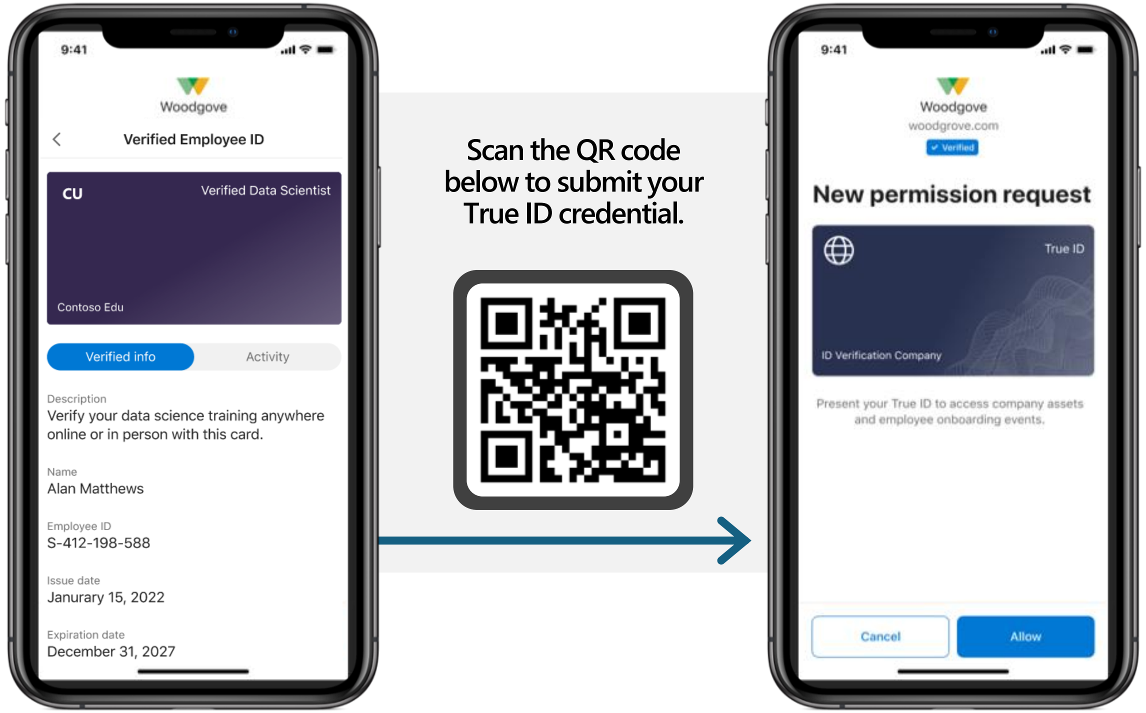
Write attribute values to User object

```
User.Company = Fabrikam
```

Improving onboarding with decentralized IDs

Microsoft Entra Verified ID in entitlement management

- Reduces need for self-attestation by new employees or business partners. Users requesting access will be able to obtain identity attributes from a wide set of issuers.
- Simplifies approval processes, as approvers do not need to personally vet requestor’s authenticity of claims
- Simplifies compliance posture with increased consistency and reduced need for manual intervention



Description
Verify your data science training anywhere online or in person with this card.

Name
Alan Matthews

Employee ID
S-412-198-588

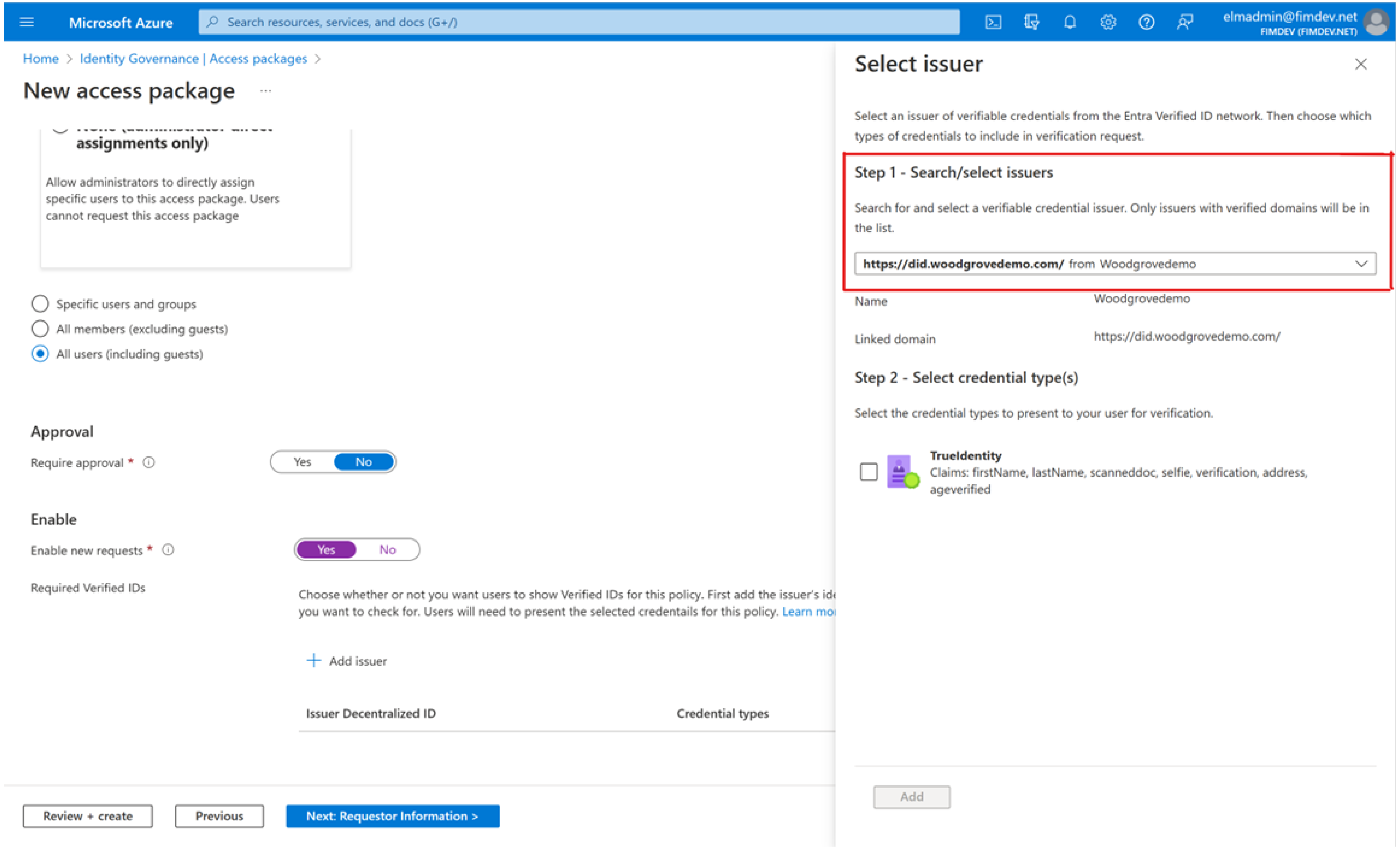
Issue date
Janurary 15, 2022

Expiration date
December 31, 2027

Scan the QR code below to submit your True ID credential.

Present your True ID to access company assets and employee onboarding events.

Adding a Verified ID requirement to an access package


Microsoft Azure
Search resources, services, and docs (G+/)
elmadmin@fimdev.net
FIMDEV (FIMDEV.NET)
Home > Identity Governance | Access packages >
Review + create
Previous
Next: Requestor Information >
Add

New access package ···

assignments only)

Allow administrators to directly assign specific users to this access package. Users cannot request this access package

○ Specific users and groups
○ All members (excluding guests)
● All users (including guests)

Approval

Require approval * ⓘ Yes [✓ No]

Enable

Enable new requests * ⓘ [✓ Yes] No

Required Verified IDs

Choose whether or not you want users to show Verified IDs for this policy. First add the issuer's ide
you want to check for. Users will need to present the selected credentails for this policy. Learn mo

+ Add issuer

Issuer Decentralized ID	Credential types

Select issuer

Select an issuer of verifiable credentials from the Entra Verified ID network. Then choose which types of credentials to include in verification request.

Step 1 - Search/select issuers

Search for and select a verifiable credential issuer. Only issuers with verified domains will be in the list.

https://did.woodgrovedemo.com/ from Woodgrovedemo

Name	Woodgrovedemo
Linked domain	https://did.woodgrovedemo.com/

Step 2 - Select credential type(s)

Select the credential types to present to your user for verification.

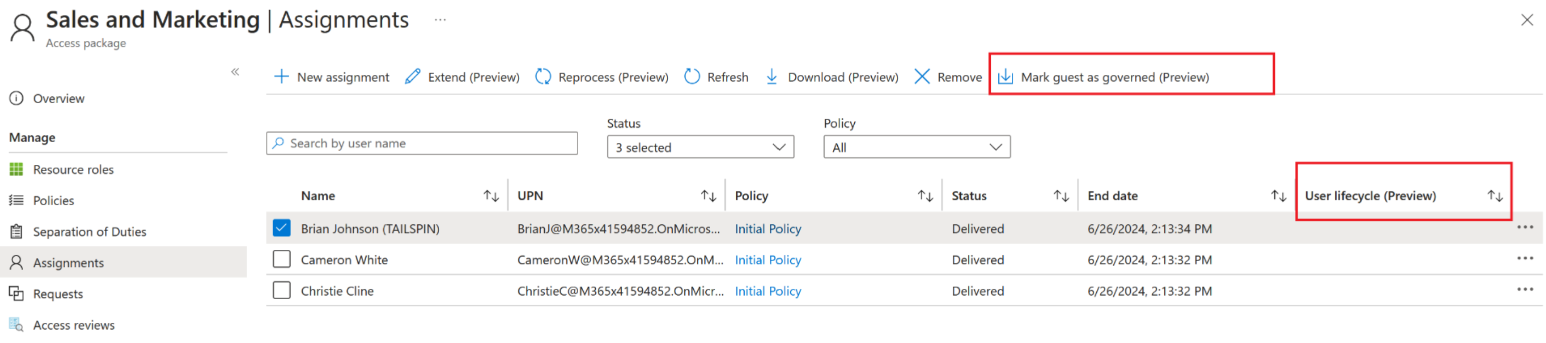
□ **TrueIdentity**
Claims: firstName, lastName, scanneddoc, selfie, verification, address, ageverified

Microsoft Security

“Governed” guest state (managing external user lifecycle)

Entitlement management allows you to gain visibility into the state of a guest user's lifecycle through the following viewpoints:

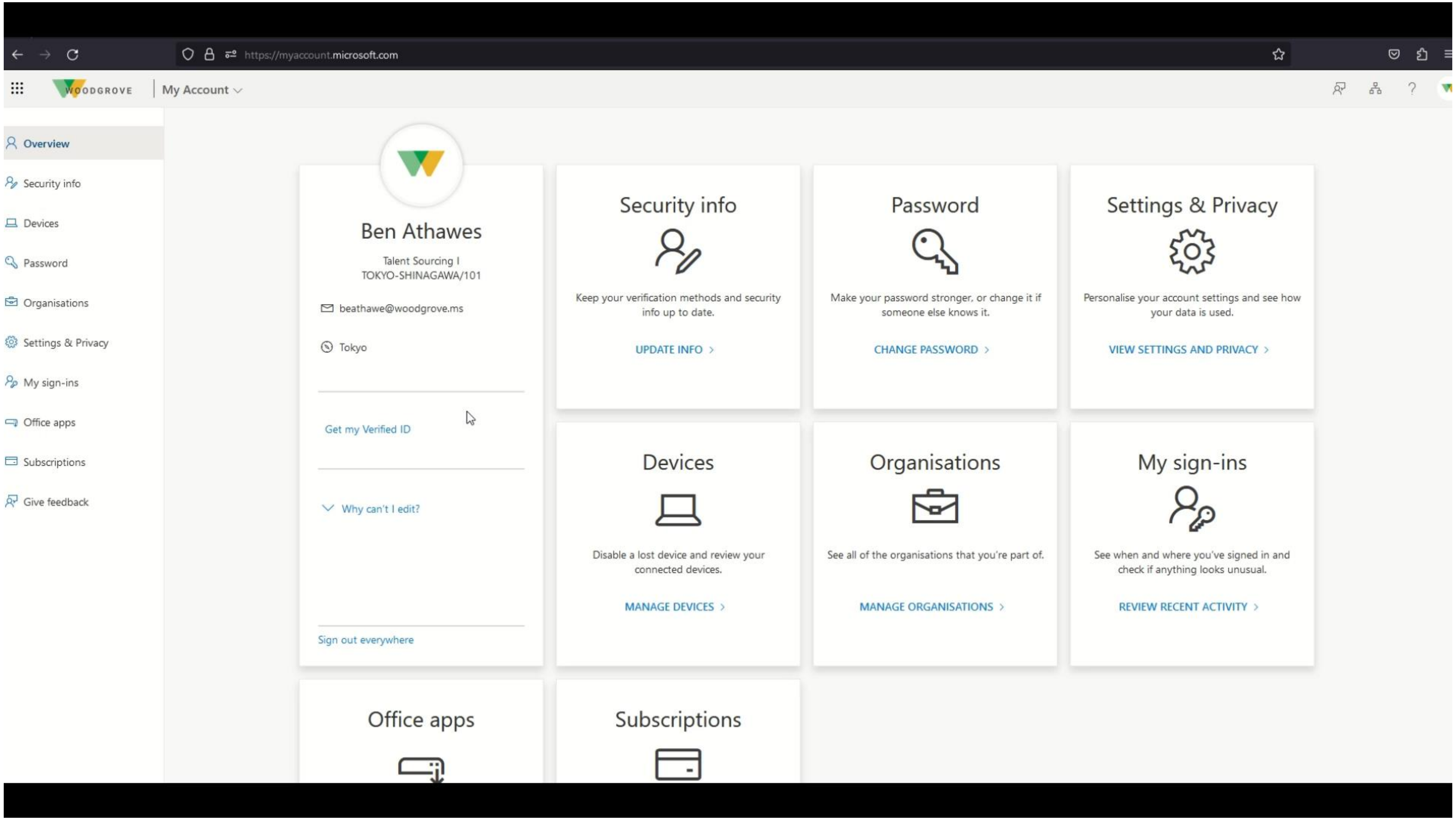
- **Governed** - The guest user is set to be governed.
- **Ungoverned** - The guest user is set to not be governed.
- **Blank** - The lifecycle for the guest user isn't determined. This happens when the guest user had an access package assigned before managing user lifecycle was possible.



	Name	UPN	Policy	Status	End date	User lifecycle (Preview)
☑	Brian Johnson (TAILSPIN)	BrianJ@M365x41594852.OnMicros...	Initial Policy	Delivered	6/26/2024, 2:13:34 PM	
□	Cameron White	CameronW@M365x41594852.OnM...	Initial Policy	Delivered	6/26/2024, 2:13:32 PM	
□	Christie Cline	ChristieC@M365x41594852.OnMicr...	Initial Policy	Delivered	6/26/2024, 2:13:32 PM	

Demo: getting and using a Verified employee credential to request an access package

Can be used for internal and external user verification



https://myaccount.microsoft.com

WOODGROVE | My Account

- Overview
- Security info
- Devices
- Password
- Organisations
- Settings & Privacy
- My sign-ins
- Office apps
- Subscriptions
- Give feedback

Ben Athawes

Talent Sourcing I
TOKYO-SHINAGAWA/101

beathawe@woodgrove.ms

Tokyo

Get my Verified ID

Why can't I edit?

Sign out everywhere

Security info

Keep your verification methods and security info up to date.

UPDATE INFO >

Password

Make your password stronger, or change it if someone else knows it.

CHANGE PASSWORD >

Settings & Privacy

Personalise your account settings and see how your data is used.

VIEW SETTINGS AND PRIVACY >

Devices

Disable a lost device and review your connected devices.

MANAGE DEVICES >

Organisations

See all of the organisations that you're part of.

MANAGE ORGANISATIONS >

My sign-ins

See when and where you've signed in and check if anything looks unusual.

REVIEW RECENT ACTIVITY >

Office apps

Subscriptions

Walkthrough/Demo

Guest Insights

Convert Guests to governed

Onboard guests with Verified ID

Microsoft Security

Thank you

Go to https://aka.ms/EntraIDGovernancetraining for more information!