



Microsoft Entra ID Governance

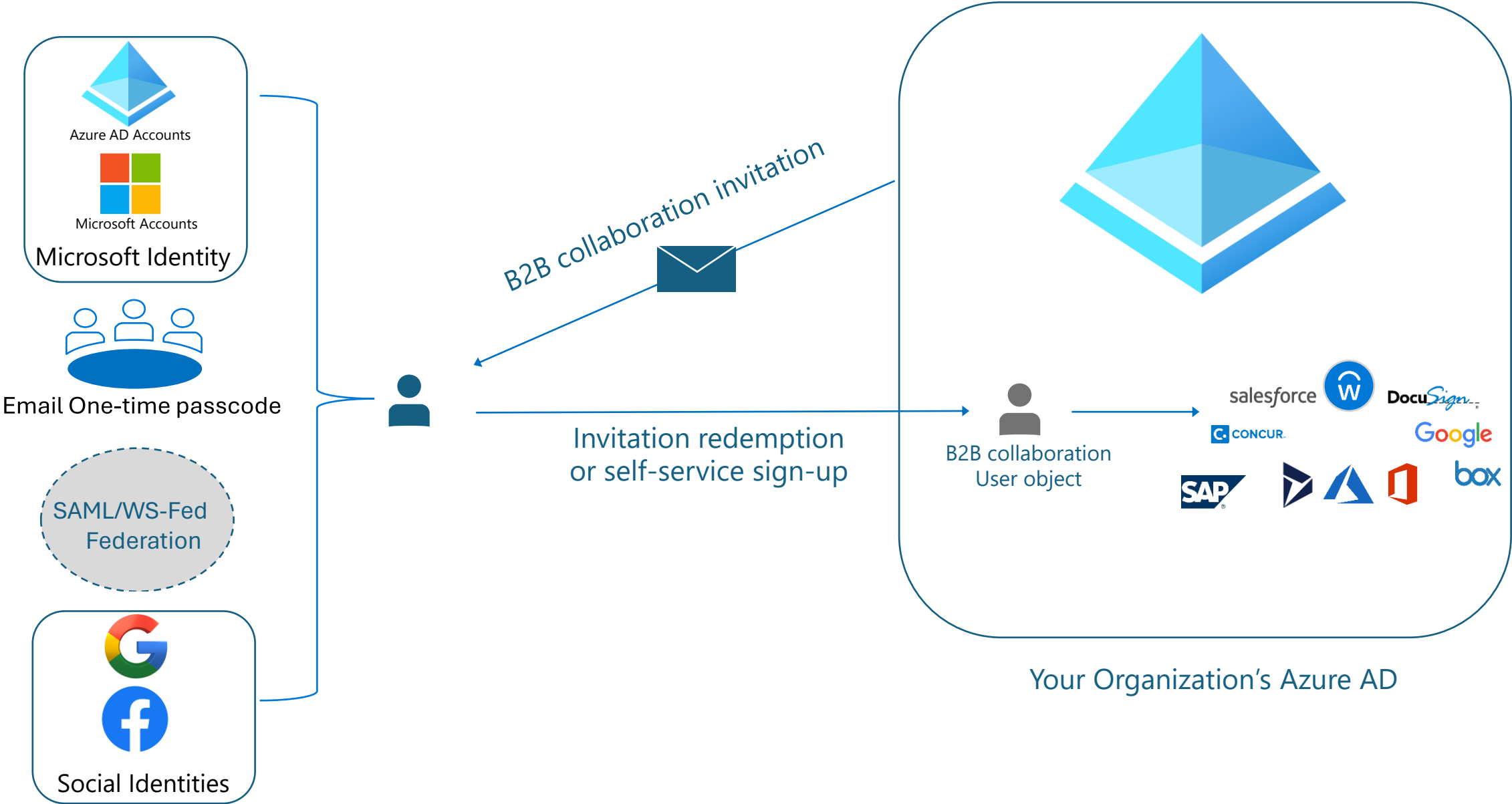
Govern guest and partner access to resources

Proof of concept deployment



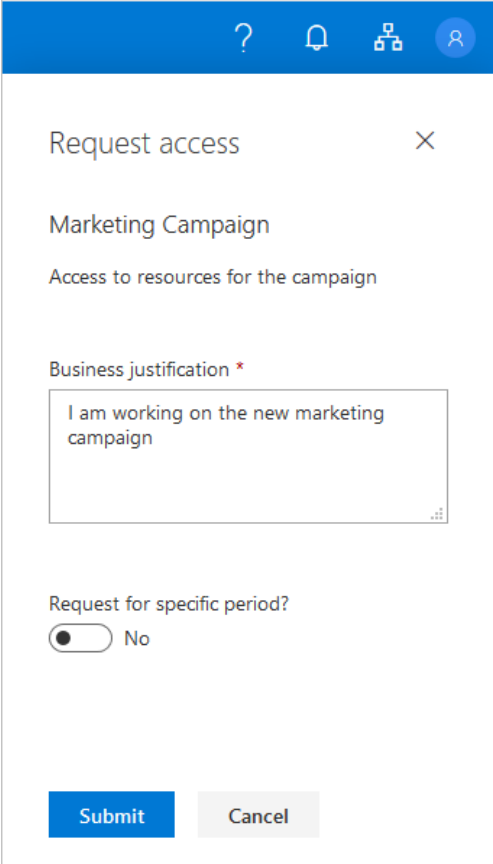
External identities Overview

External User (Partner, Vendor, Supplier)



How to Provision guests into Azure AD

Users can self service
sign-up via Entitlement
Management



The screenshot shows a 'Request access' dialog box with a blue header bar containing icons for help, notifications, and user profile. The dialog title is 'Request access' with a close button (X). The resource being requested is 'Marketing Campaign' with the description 'Access to resources for the campaign'. A 'Business justification' section is marked with a red asterisk and contains a text box with the text 'I am working on the new marketing campaign'. Below this is a toggle switch for 'Request for specific period?' which is currently set to 'No'. At the bottom are 'Submit' and 'Cancel' buttons.

Request access

Marketing Campaign

Access to resources for the campaign

Business justification *

I am working on the new marketing campaign


Request for specific period?

☐ No

Submit Cancel


Users can self service sign-up via External Identities User Flows


How to Provision guests into Entra ID




WOODGROVE


Create account

 Sign up with email

 Sign up with Google

 Sign up with Facebook

Back



WOODGROVE

Add more details

We need more information to set up your account.

Name

Business name

Business registration code

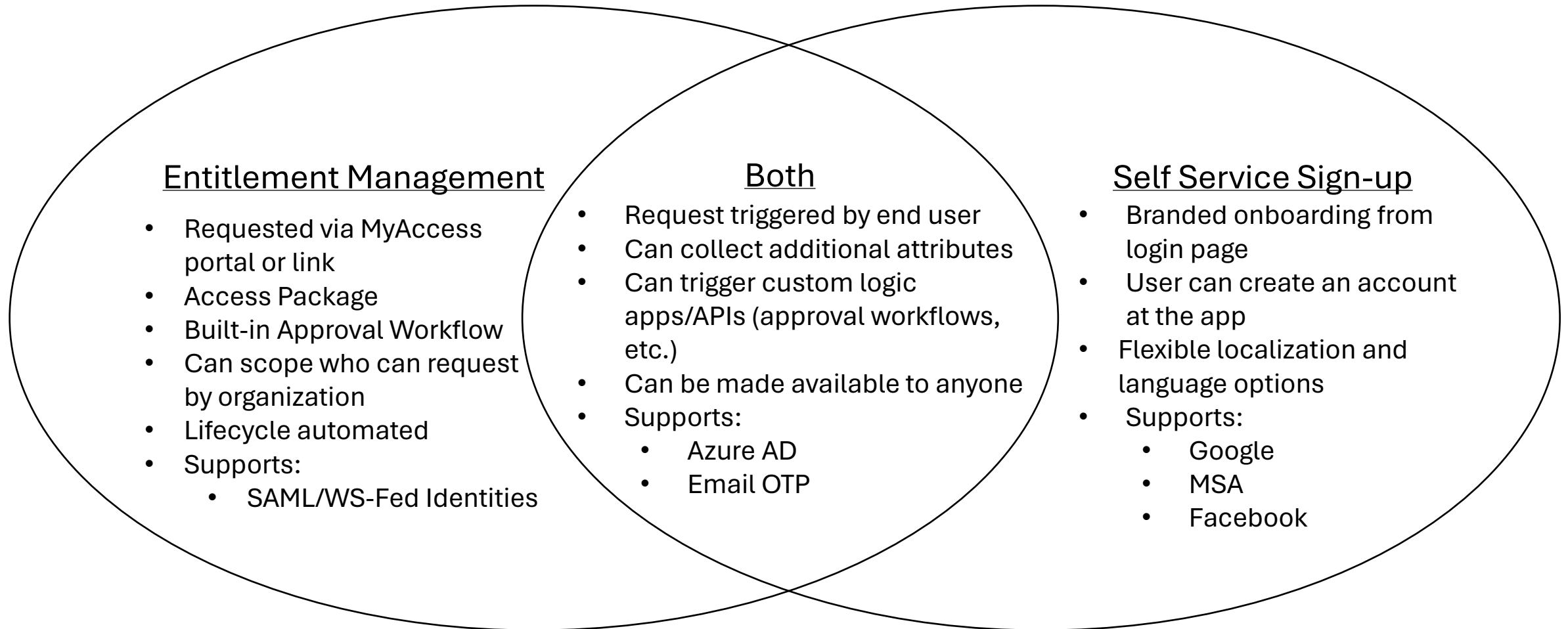
[I don't have a code](#)

Phone number

Back Next

Should I use Entitlement Management or SSSU?

Answer: It depends on what you're looking for.



Onboarding and Discovery

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



One page 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	Lifecycle workflows configured	50
Guests	1,000	Access reviews configured	0
Privileged roles	150	Apps with automated provisioning	30
Groups and teams	200	Policies governed with privileged identities	20
Business applications	250	Access packages for contingent 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 and quickly give the right people the access they need by incorporating Microsoft Entra Verifiable credentials in your access request flows.
- Learn how Standard AAA transforms asset management with unified, cloud-based identity governance**
Standard is a new Microsoft Entra Identity Governance feature that allows you to streamline operations and review processes to simplify identity and access lifecycle management for the users.
- Migrating from MIM? Learn how you can now automate on-premise app provisioning with Microsoft Entra**
Provision identities from Microsoft Entra directly into on-premise applications without any custom coding in three easy steps. You can enable users to access on-premise applications while ensuring the necessary governance processes are in place.

[View all](#)

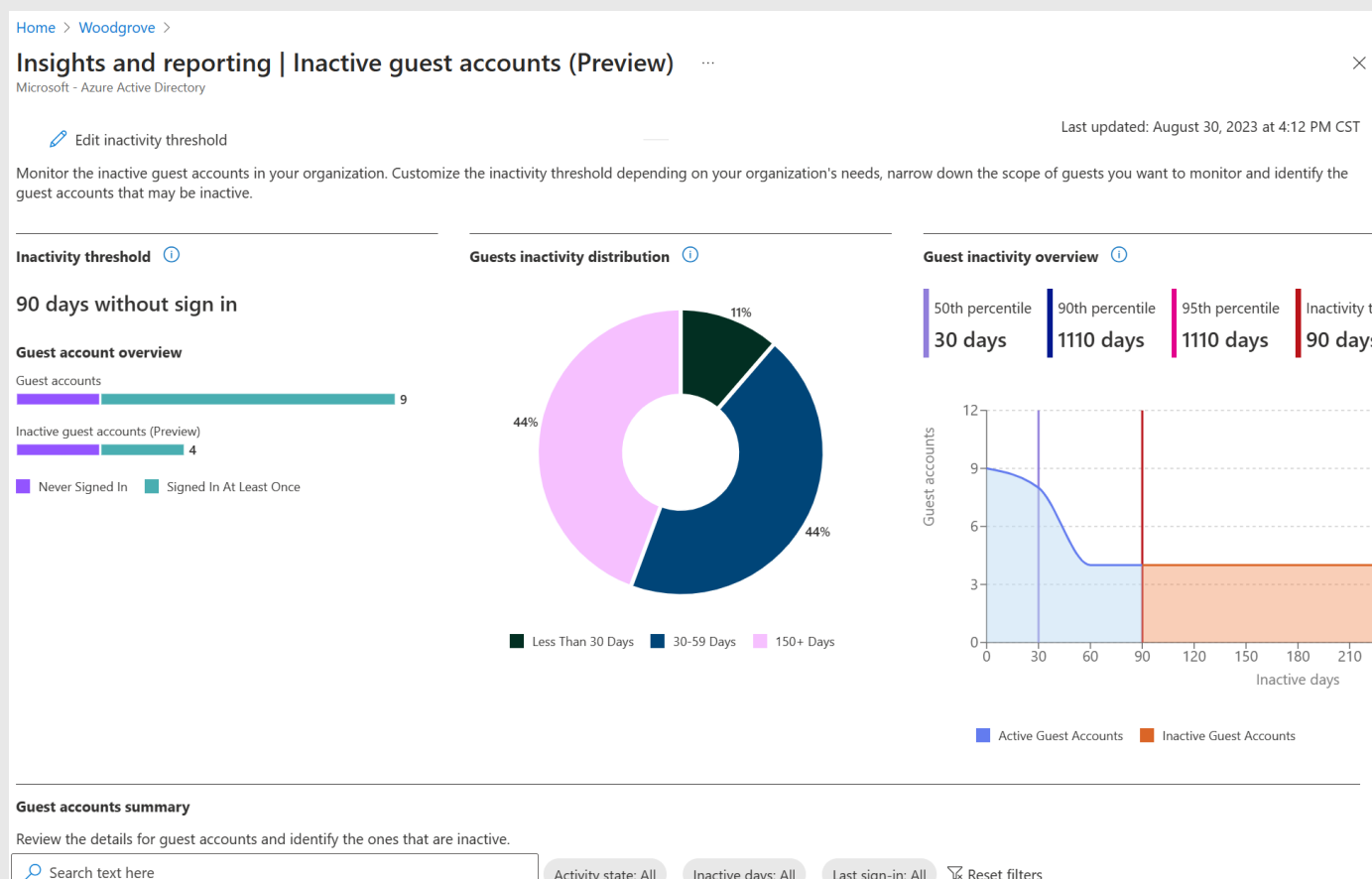
Manage how employees get access to resources
Automatically assign app and resource access based on employee job profile. Ensure that conflicting access (with app administrators and app users, for example) can't occur with Separation of Duties. Delegate access decisions to business groups.
[Learn more](#)

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](#)

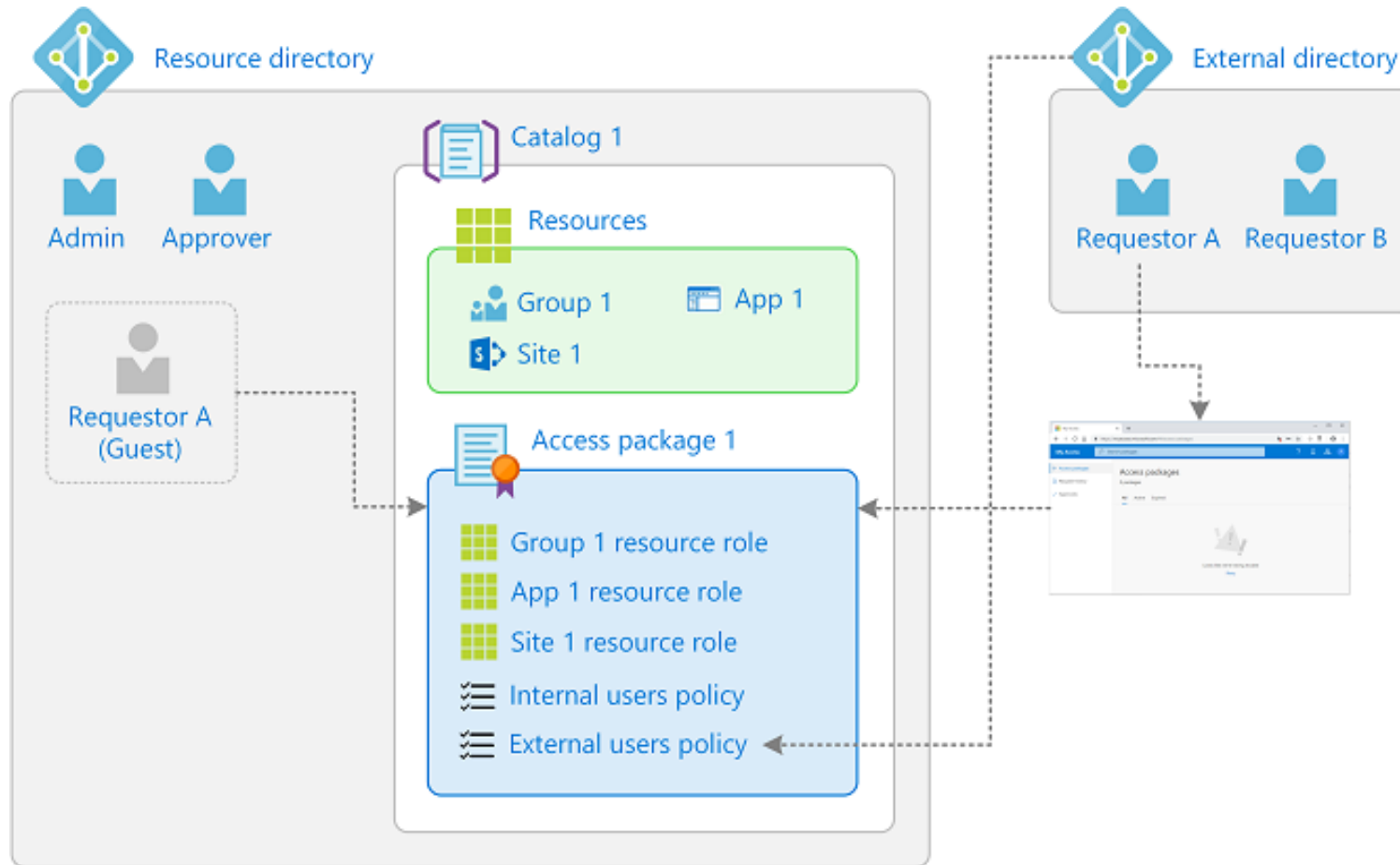
Automate the entire employee identity lifecycle
Design workflows to automatically create or identify via a signal from HR systems. Automatically update access when employee change roles or move. Gracefully remove access when the employee leaves the organization.
[Learn more](#)

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



How access works for external users



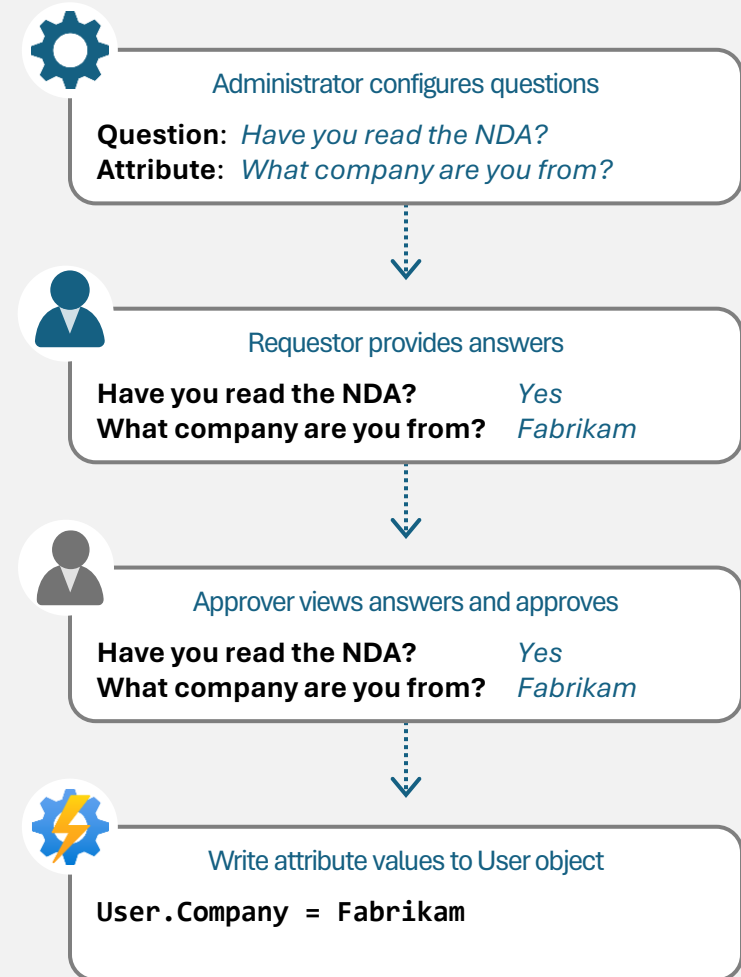
Guest attribute management

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.




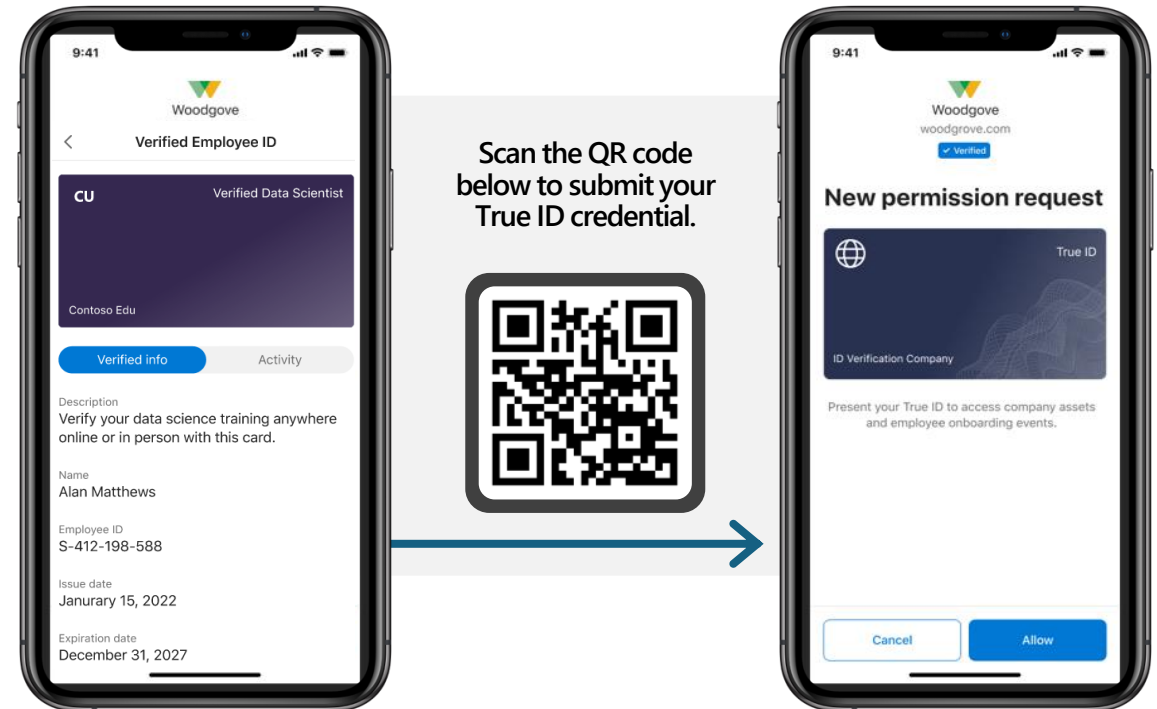
Improving onboarding with decentralized IDs

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



Directly assign any user (Preview)

Entitlement management also allows you to directly assign external users to an access package to make collaborating with partners easier. To do this, the access package must have a policy that allows users not yet in your directory to request access.

[Home](#) > [Sales and Marketing](#) >

Add user to access package

Sales and Marketing

Select policy * ⓘ

▼

[+ Create new policy](#)

☐ User already in my directory

☒ Any user (Preview)

Name ⓘ

Example: 'Chris Green'

Email address * ⓘ

Example: 'chris@contoso.com'

Bypass approval ⓘ

YesNo

Assignment starts on ⓘ

10/05/2021

📅

8:45:51 PM

Assignment ends on ⓘ

MM/DD/YYYY

📅

h:mm:ss A

Business justification ⓘ

Add

Features

- **Request Access for external users:** When a user who isn't yet in your directory requests access, and is approved, they're automatically invited into your directory and assigned access.
- **Grant Access to Resources:** Control who can get access to applications, groups, Teams and SharePoint sites, with multi-stage approval
- **Delegate external users administration:** delegate to access package managers policies definitions with rules for which users can request, who must approve their access, and when access expires.
- **Verified ID:** Require the users to present additional identity proofs during the request process such as a training certification, work authorization, or citizenship status.
- **Create external user during the Access Package assignment**

Planning- Decisions to consider

- Define with which organization(s) you are going to collaborate with.
- Access Package name and description
- Approval levels does the access package will require
- Who will be able to request access?
- Approvers
- What information do the external users need to provide during the request?"
- Access Package expiration time
- Access Reviews requirements
- Verified ID Requirement

Deploy

Step	Instructions
1. Add connected organization in EM	Add connected organization
2. Enable Catalog for External Users	Settings for external users
3. Create an Access Package	Create an access package in entitlement management
4. Check the hidden setting on the access package	Change the Hidden setting
5. Required Verified IDs (Optional Step)	Create an access package with verified ID requirements
6. Onboard users from the access package assignment (Optional Step)	Directly assign any user (Preview)
7. Send a My Access portal link to the external organization contact	Share link to request an access package in entitlement management

Detailed Step by step

<https://learn.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-external-users#enable-catalog-for-external-users>

Auto assignment Rules

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 [Edit](#)

(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

Next >

Features

- **Automatically create assignments:** Add the user when an user properties matches with the policy's membership rule
- **Automatically remove assignments :** Remove the user when an user properties matches with the policy's membership rule

Planning- Decisions to consider

- Access Package name and description
- Define if this Access Package will have approval stages. If it does, define approvers and requestors.
- Attribute(s) for the Business rule definición
- Automatically create assignment
- Automatically remove assignment

Deploy

Step	Instructions
Create an Access Package	Create an access package in entitlement management
Create auto assignment policy	Create an automatic assignment policy

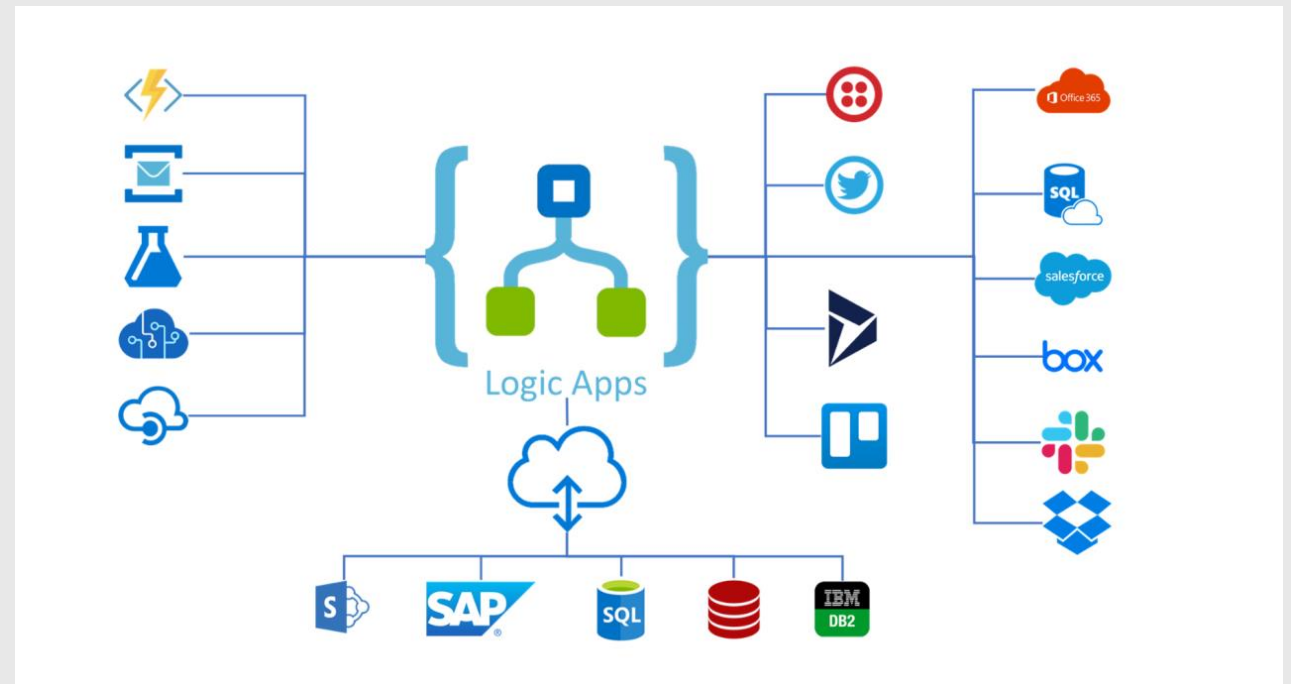
Detailed Step by step

[Configure an automatic assignment policy for an access package in entitlement management - Microsoft Entra | Microsoft Learn](#)

Custom Workflows with Logic Apps

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.



Logic App Integration with Entitlement Management

Used to automate custom workflows and connect apps and services in one place. Users can integrate Logic Apps with entitlement management to broaden their governance workflows beyond the core entitlement management use cases.

- When an access package request is created
- When an access package request is approved
- When an access package assignment is granted
- When an access package assignment is removed
- 14 days before an access package assignment auto expires
- One day before an access package assignment auto expires

Use cases examples

Send custom email Notifications

Send Teams notification

Get user information from other applications

Writeback user information to external systems

Call an External web api to trigger actions on external systems

Creating a set of tasks in Microsoft planner

Generate a TAP

Planning- Decisions to consider

- Processes that you need to automate during the different request stages
- Interfaces available on Target systems
- Request stage where you want to trigger the logic app
- Have Azure Subscription Resources available
- Logic App authentication with target systems

Deploy

Step	Instructions
1. Add custom Extension to a Catalog	Create and add a Logic App workflow to a catalog for use in entitlement management
2. Edit the Custom Extension	Edit a linked Logic App's workflow definition
3. Add custom Extension to an Access Package	Add custom extension to a policy in an access package

Detailed Step by step

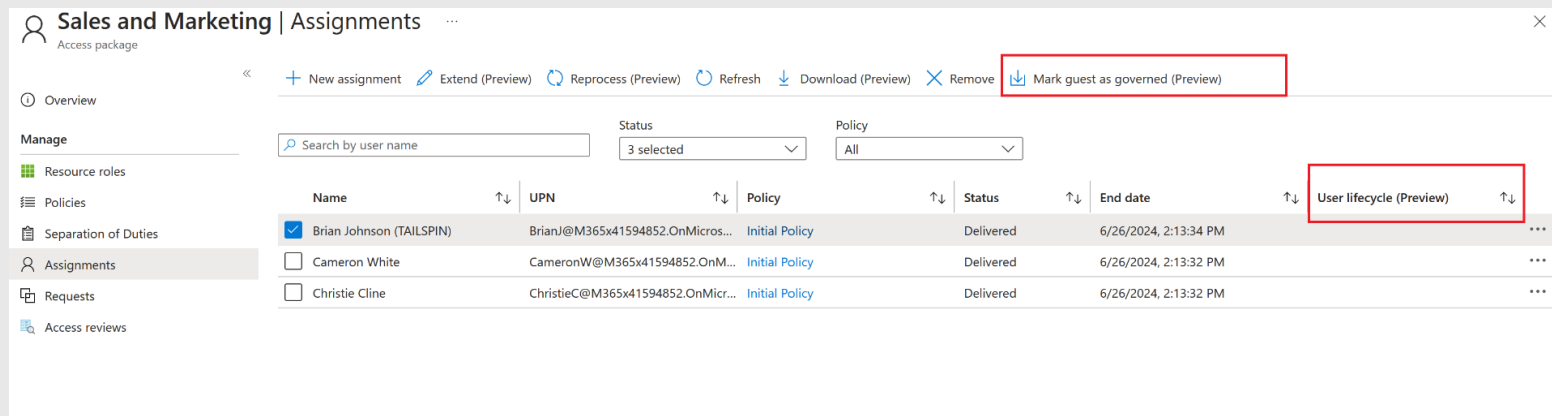
[Trigger Logic Apps with custom extensions in entitlement management - Microsoft Entra | Microsoft Learn](#)

Convert existing external users to be governed

External User states

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.



Sales and Marketing | Assignments

Access package

« + New assignment Extend (Preview) Reprocess (Preview) Refresh Download (Preview) Remove **Mark guest as governed (Preview)**

Overview

Manage

Search by user name

Status: 3 selected Policy: All

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

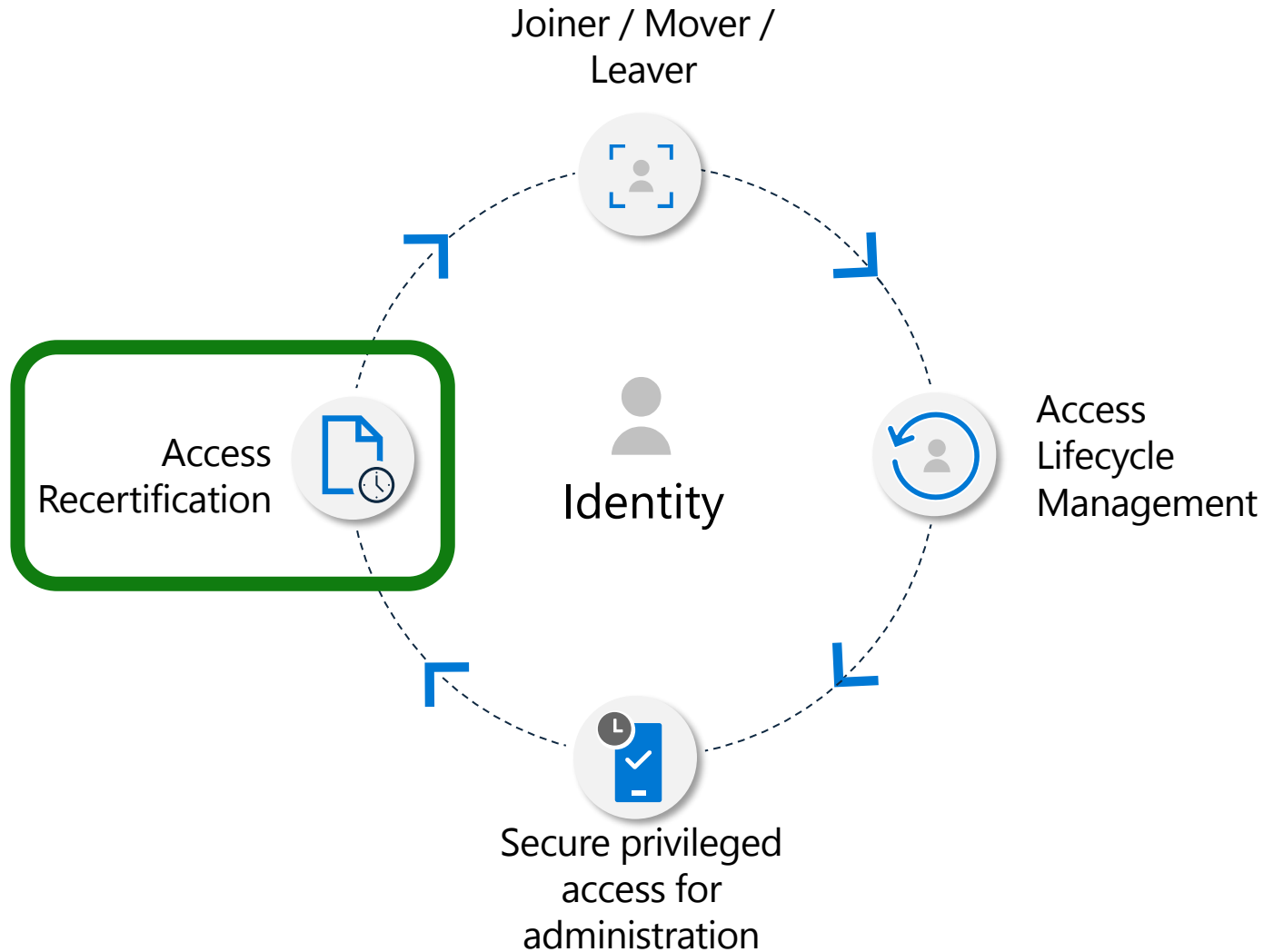
Planning- Decisions to consider

- Create a new access Package or use an existing one
- How assign the existing external users to the access package?
 - Auto Assignment Policy – Define a Rule
 - Self Request – Define approvers and approval levels
 - Direct Assignment

Deploy

Step	Instructions
1. Create and Access Package (optional)	Create an access package in entitlement management
2. Add Auto Assignment Policy (optional)	Create an automatic assignment policy
3. Convert users to governed	Manage guest user lifecycle in the Azure portal

Scenario: Access Recertification



Microsoft Entra ID P2

- Access Reviews - Basic access certifications and reviews

Microsoft Entra ID Governance:

- Access Reviews targeting inactive identities
- Certify PIM for Groups memberships
- Machine Learning assisted recommendations

Access recertification to reduce risk

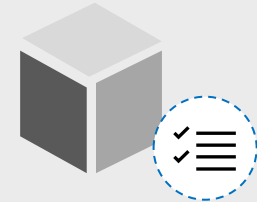
Access Reviews



Natively built-in to
Microsoft Entra



Manage risk and meet
compliance for users,
guests and workload
identities



Ensure access to
sensitive Teams, Groups,
Apps, Roles is reviewed
periodically

How Access Reviews works

Administrator

1. Selects resource



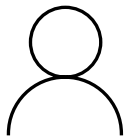
Team/Group
SaaS application
Privileged role
Access Package

2. Selects scope



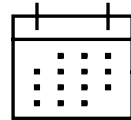
Guests
Employees
Everyone
Workload Identities

3. Selects reviewer



Team/Group owner
Manager
Specific user(s)
Users' self review

4. Selects frequency



Weekly
Monthly
Quarterly
Yearly

[Home](#) > [Identity Governance](#) | [Access reviews](#) >

New access review ...

*** Review type** * Reviews Settings * Review + Create

Schedule an access review to ensure the right people have the right access to access packages, groups, app
[Learn more](#)

Select what to review *

Teams + Groups

Review scope *

☒ All Microsoft 365 groups with guest users ⓘ

☐ Select Teams + groups

[+ Select group\(s\) to exclude](#)

Group

Scope *

☒ Guest users only

☐ All users ⓘ

How Access Reviews works

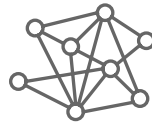
Reviewer

1. Send notification



Email is sent to the reviewer

2. Review



Review current membership with system generated recommendations

3. Confirm



Reviewers confirm which memberships to keep

4. Apply result



Denied users are removed from the resource

My Access

Search users

Access packages

Request history

Approvals

Access reviews

← Access reviews

FY22 Quarterly review

Please review members of 'FY22 Planning' [See details](#)

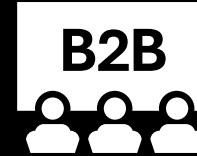
☒ Approve ☒ Deny ☒ Don't know ☒ Reset decisions ☒ Accept recommendations

	Name ↑	Recommendation
<input checked="" type="checkbox"/>	abhijeet sinha absinh@fimdev.net	Approve Last signed in (Jul 1, 2021) less than 30 days before review began
<input checked="" type="checkbox"/>	Barclay Neira barclayn@fimdev.net	Deny Last sign-in date unknown
<input checked="" type="checkbox"/>	Bhaskar Kamasani vikama@microsoft.com	Deny Last signed in (May 6, 2021) more than 30 days before review began
<input type="checkbox"/>	Bhaves Patel bpatel@microsoft.com	Approve Last signed in (Jun 30, 2021) less than 30 days before review began
<input type="checkbox"/>	Blake Nelson Blake.Nelson@microsoft.com	Approve Last signed in (Jun 21, 2021) less than 30 days before review began
<input type="checkbox"/>	Bob Grumpy bobgrumpy@fimdev.net	Deny Last signed in (Apr 5, 2021) more than 30 days before review began



Employees

- Change jobs or leave the company
 - Employee's previous access are not removed.
 - Users accumulate excessive permissions

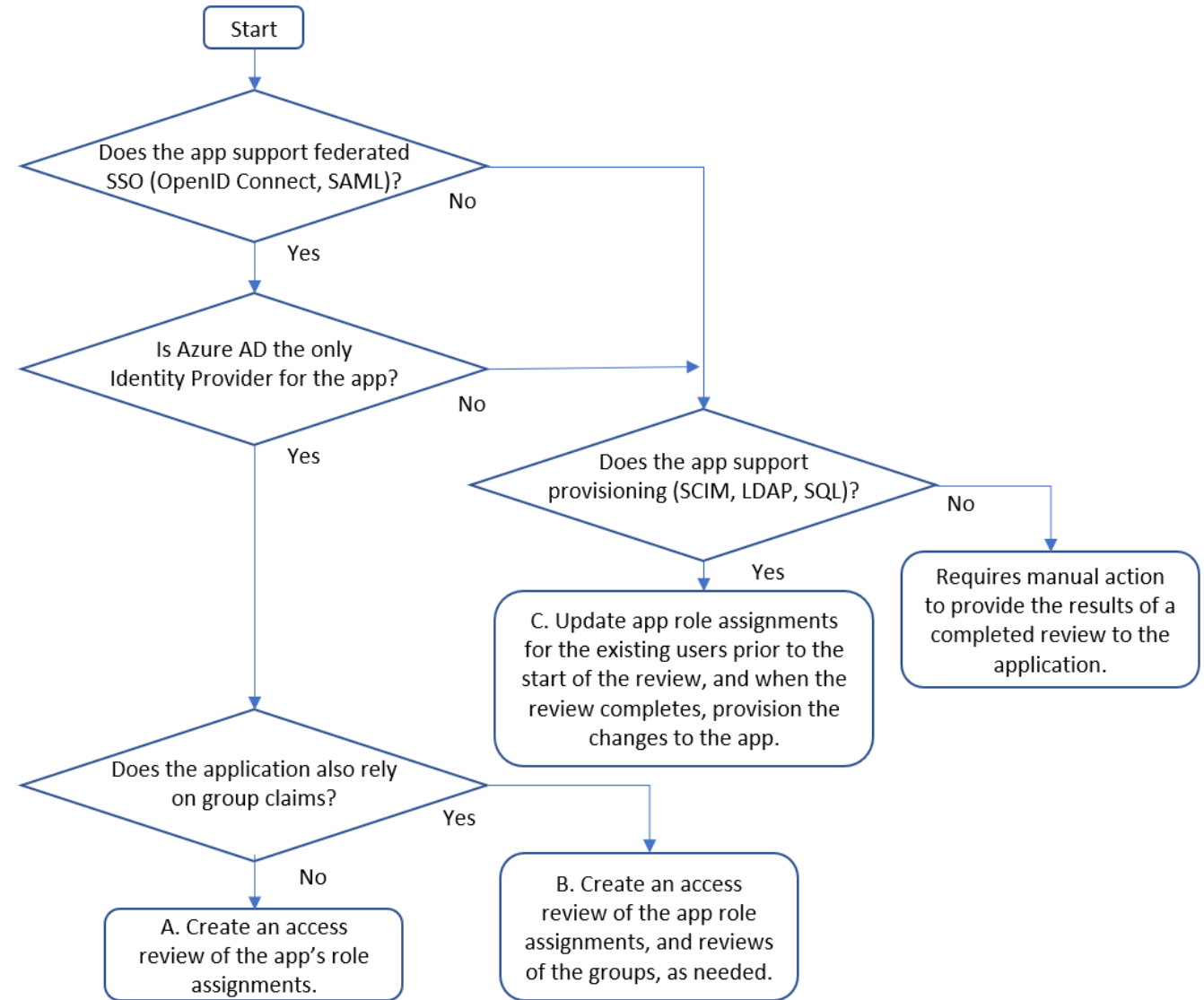


External Users

- Guests invited into the tenant
 - What access should they have?
 - When should they leave?

Planning

- Determine application readiness



Planning- Decisions to consider

1. Who is responsible for the review?

A. Users review their own privilege

- Schedule access review to ask users themselves if they still need access.
- Remove privilege if the user denies or does not respond.

B. Resource owners review privileges assigned to their resources.

- Schedule access review to ask resource owners to review the privileges assigned to their resource.

Possible Reviewers:

- Group Owners
- Specific Users
- Managers of Users

Planning (Contd)

2. How many stages of reviews are needed?

- Reach consensus across multiple sets of reviewers
- Assign alternate reviewers to weigh in on unreviewed decisions
- Reduce burden on later stage reviewers

New access review ...

* Review type * **Reviews** Settings * Review + Create

Determine review stages, reviewers, and timeline below.


Multi-stage review *  ☒

First stage review

Select reviewers * 

Stage duration (in days) * 

Second stage review


 Reviewers in later stage can overwrite decisions from previous stage

Select reviewers * 

Fallback reviewers  [+ Select fallback reviewers](#)

Stage duration (in days) * 

Third stage review

 Reviewers in later stage can overwrite decisions from previous stage

Select reviewers * 

Users or Groups *  [ADM_TENANT_ADMINS](#)

Stage duration (in days) * 

 [Delete](#)

Reveal review results

Show previous stage(s) decisions to later stage reviewers  ☒

Planning (Contd)

3. Decide on criteria for automated decisions

- Response Triggers
- Account Inactivity
- Justification requirements
- Alerting and notifications

New access review ...

* Review type * Reviews Settings * Review + Create

Configure additional settings, including decision helpers and email notifications.

Upon completion settings

Auto apply results to resource ⓘ

☐

If reviewers don't respond ⓘ

Take recommendations ▼

Action to apply on denied guest users ⓘ

Remove user's membership from t... ▼

At end of review, send notification to

[Account Admin](#)

Enable reviewer decision helpers

No sign-in within 30 days ⓘ

☒

User-to-Group Affiliation ⓘ

☒

Advanced settings

Justification required ⓘ

☒

Email notifications ⓘ

☒

Reminders ⓘ

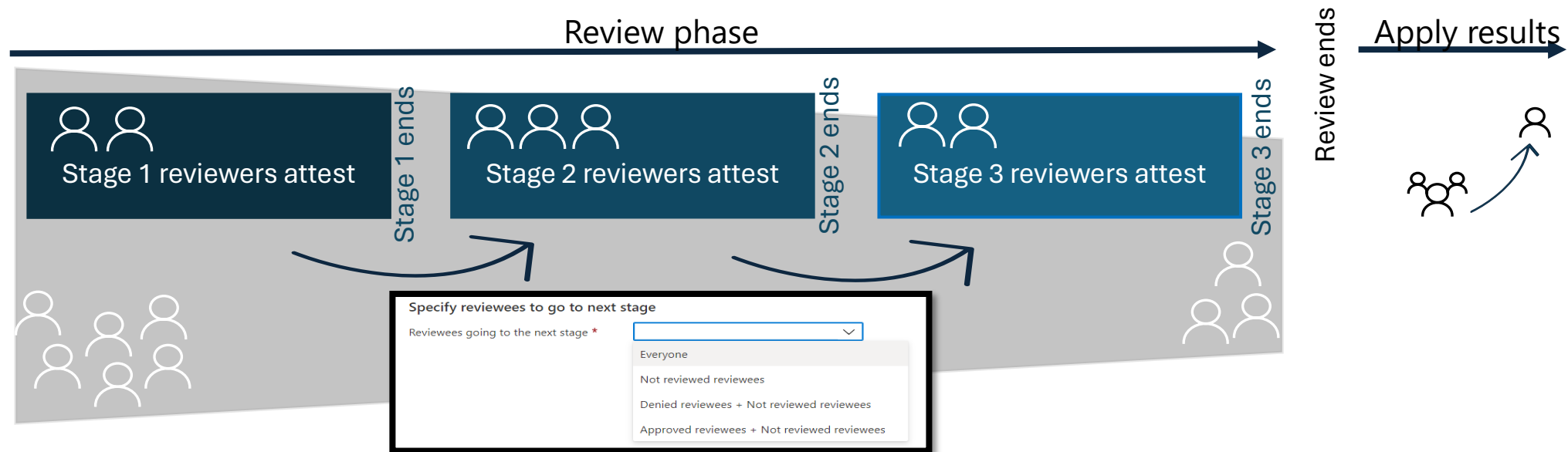
☒

Additional content for reviewer email ⓘ

Multi-stage Access Reviews

Meet complex audit and recertification requirements through multiple stages of reviews

- **Reach consensus across multiple sets of reviewers.** Requires agreement from independent reviewers at every stage before access is recertified.
- **Assign alternate reviewers to weigh in on unreviewed decisions.** Ensure accounts left unreviewed by unresponsive or out-of-office reviewers are sent to the next appropriate reviewer, such as the user's manager or the resource owner.
- **Reduce burden on later-stage reviewers.** Filter down the number of decisions for your later-stage reviewers by excluding accounts denied in previous stages. For example, have users attest to their own needs for access before asking the resource owners to attest.



Multi-Stage Reviews Decisions

First stage reviewers?

Select user(s) or group(s) – the owner(s) of the applications

Second stage reviewers?

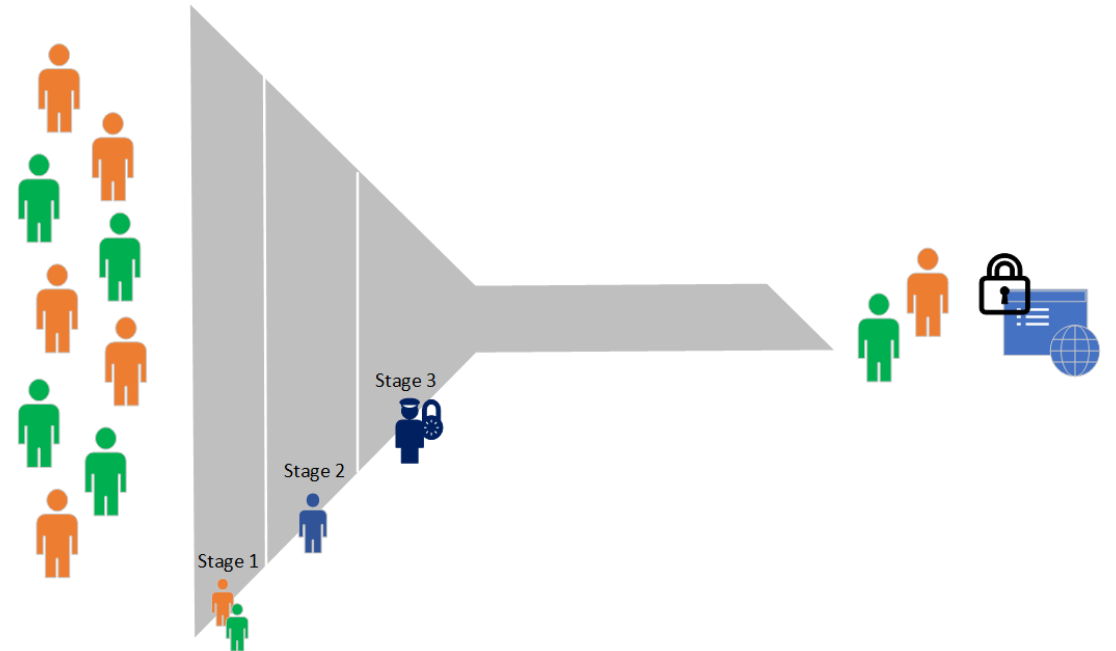
Managers of users

Show previous stage(s) decisions to later stage reviewers?

Which reviewees go to the next stage?

Expected action on non-response?

Approve/Deny



AR – Inactive Users

General Availability

Review inactive users

- Review and address stale accounts that haven't been active for a specified period
- Includes interactive and non-interactive sign-ins
- You define what inactive means
- Automatically remove stale accounts

New access review ...

[* Review type](#) [* Reviews](#) [Settings](#) [* Review + Create](#)

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 * [2nd level support](#)

i The selected group is managed in Azure AD Privileged Identity Management (Azure AD PIM). Access Reviews on this group include both eligible and active member assignments.

Scope *
☐ Guest users only
☒ All users ⓘ

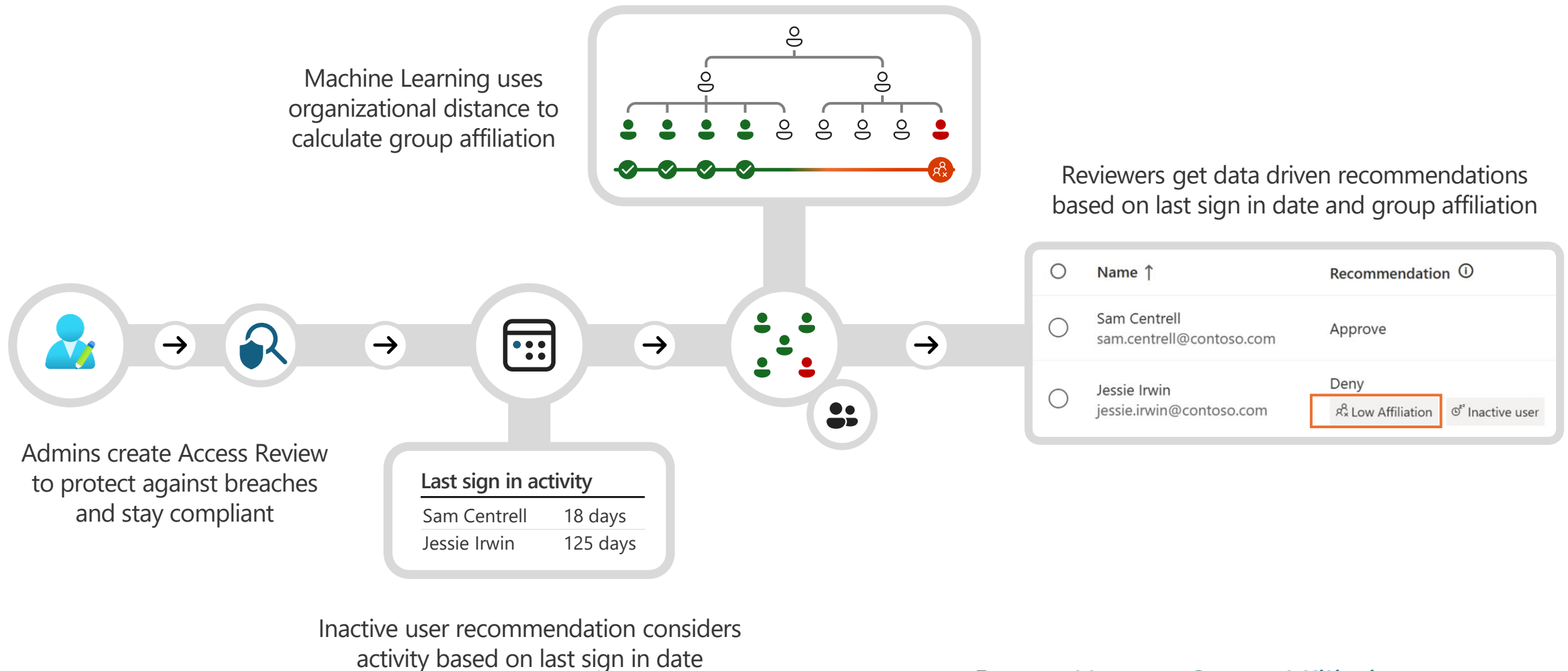
i In public preview, B2B direct connect users and teams in shared channels are included in access reviews. B2B direct connect users and teams are not supported in reviews of 'All Microsoft 365 groups with guest users', as well as reviews scoped to inactive users. Click here to learn more.

Inactive users (on tenant level) only ⓘ ☒

Days inactive 180 ✓

Machine Learning based recommendations in Access Reviews

User-to-Group Affiliation



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

Action to apply on denied guest users

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 ☐

Advanced settings

Justification required ☒

Email notifications ☒

Reminders ☒

Additional content for reviewer email

[< Previous](#) [Next: Review + Create](#)

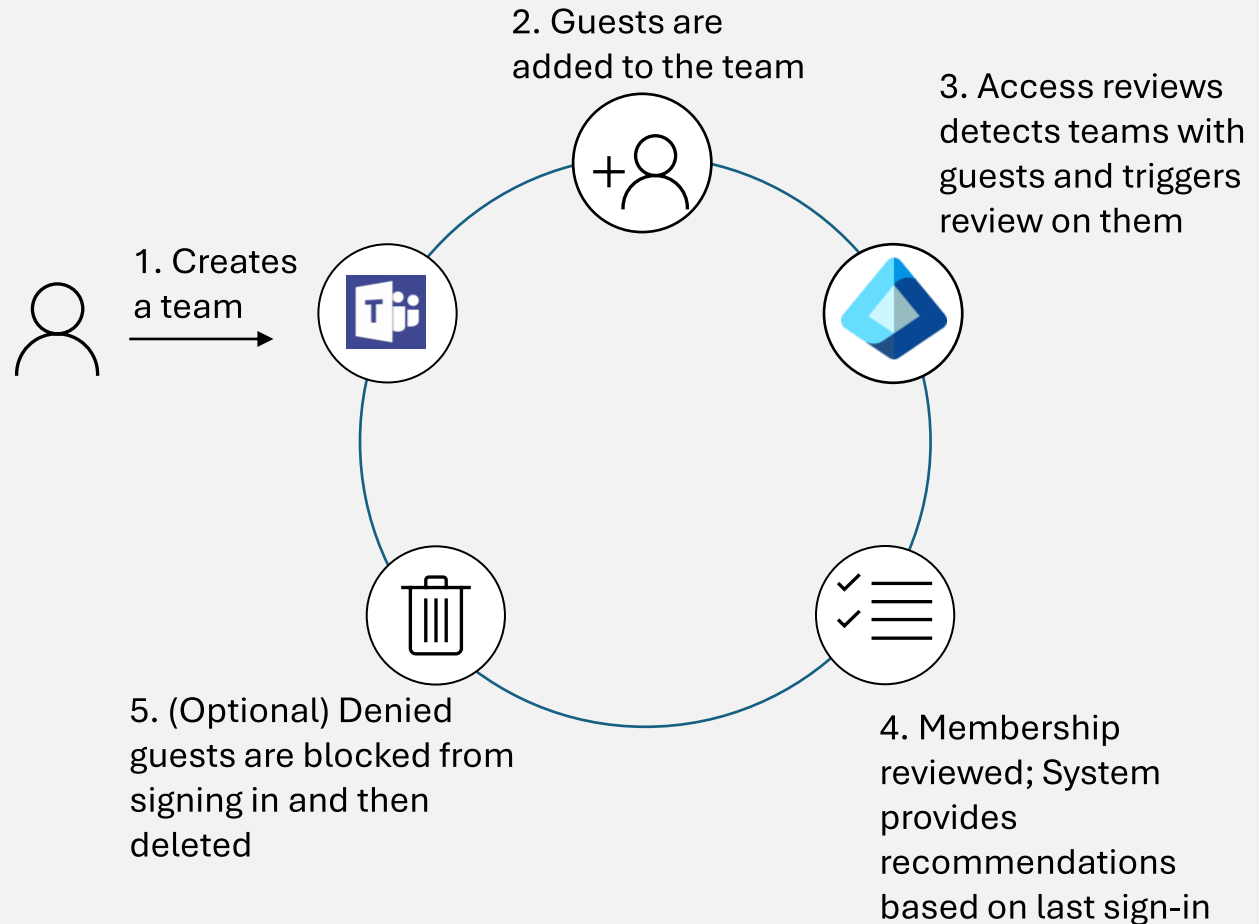
Access Reviews for Guests

Reduce risk of guest users in Teams and Microsoft 365 groups

Newly created groups that have guests, and **existing groups** that have newly added guests are automatically included in the review

Designate **group owners** or **guests themselves** to be the reviewer

Ensure that guest users retain only the **access they need** to Teams and Microsoft 365 groups



Access Certification for Guests

You can review either:

- A group in Azure AD that has one or more guests as members.
- An application connected to Azure AD 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 ...

[* Review type](#) [* Reviews](#) [Settings](#) [* Review + Create](#)

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 ⓘ

i 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



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.

Home > Identity Governance

Identity Governance | Review History ...

« **+ New report** Refresh

Date: **Last 1 month**

Search by name or owner

Name	Created By	Created Time
No access review reports to display		

Create Review History Report ×

Select filters for selecting history data

Report Name: * Last Month's Reviews ✓

Reviews starting and ending in period:

Starting * 02/16/2021 to Ending * 03/16/2021

Review Type: * ⓘ 5 selected

Review Result: * 5 selected

Create

Deploying Access Reviews Guide

Scenario	Instructions
Planning an Access Reviews Deployment	Plan a Microsoft Entra access reviews deployment
Access review of PIM for Groups	Create an access review of PIM for Groups (preview)
Access review of Azure resource and Azure AD roles in PIM	Complete an access review of Azure resource and Azure AD roles in PIM
Access review of an access package	Create an access review of an access package in entitlement management

Join Entra ID Governance Advisors - Customer Community

What is Entra ID Governance Advisors

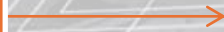
- Entra ID Governance Advisors is a community that consists of selected customers and partners who collaborate via virtual small/large group discussions, content reviews, digital forum and more

Benefits of Joining the Entra ID Governance Advisors:

- Members benefit by participating in the following ways:
 - Direct engagement with Microsoft Product Groups
 - Dedicated sessions focused on upcoming features and deep-dives
 - Early access to Private Preview and Roadmap access
 - Valuable inputs from Microsoft and other customers all under NDA
 - Learn and interact with other customers across verticals, sizes, and segments\
-
- Please fill out the survey here if interested in joining: <https://aka.ms/MicrosoftEntraAdvisors/>

Next Steps

Give us feedback, let us know
your comments:
aka.ms/idnacat/igapocsurvey



Are you ready for deployment?

Thank you

