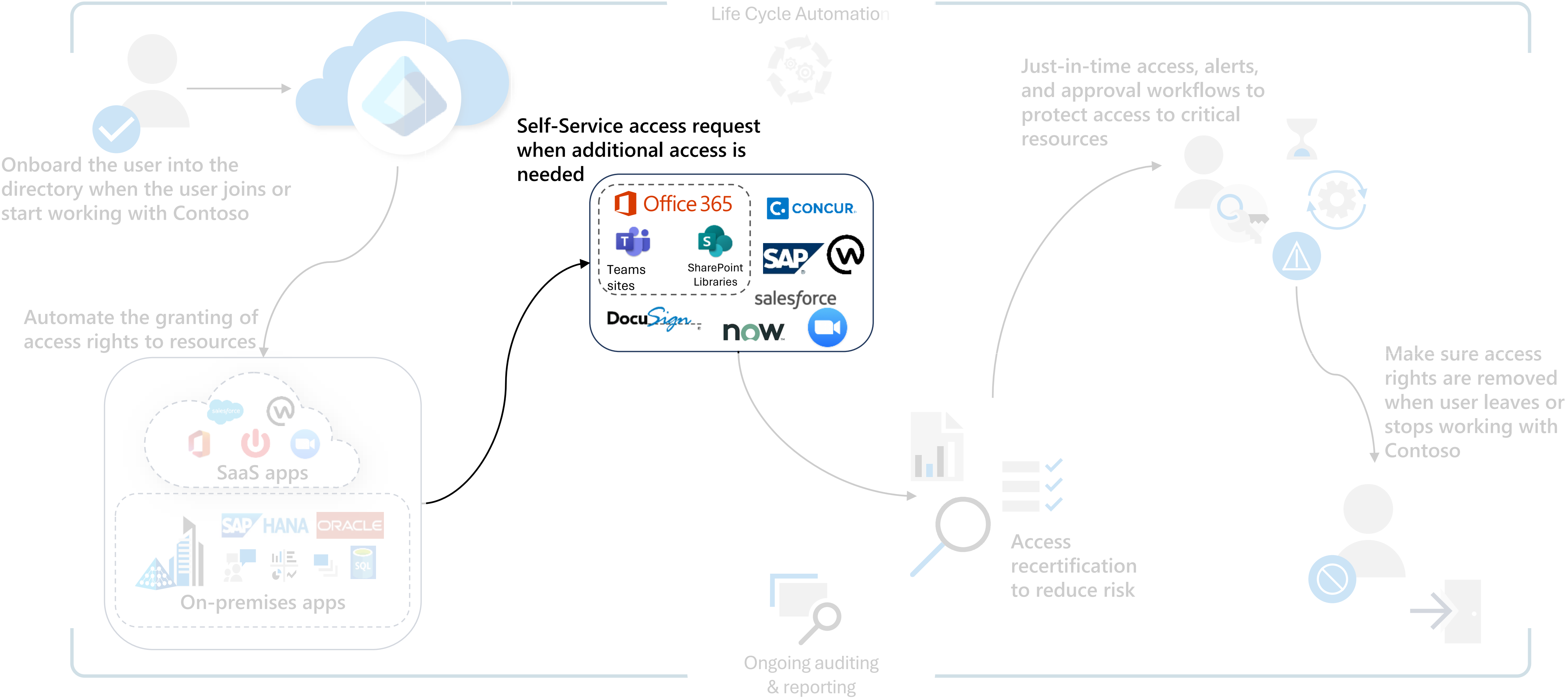
Microsoft Security

Microsoft Entra ID Governance

Assign Employee access to resources

Proof of concept deployment

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 to protect access to critical resources

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

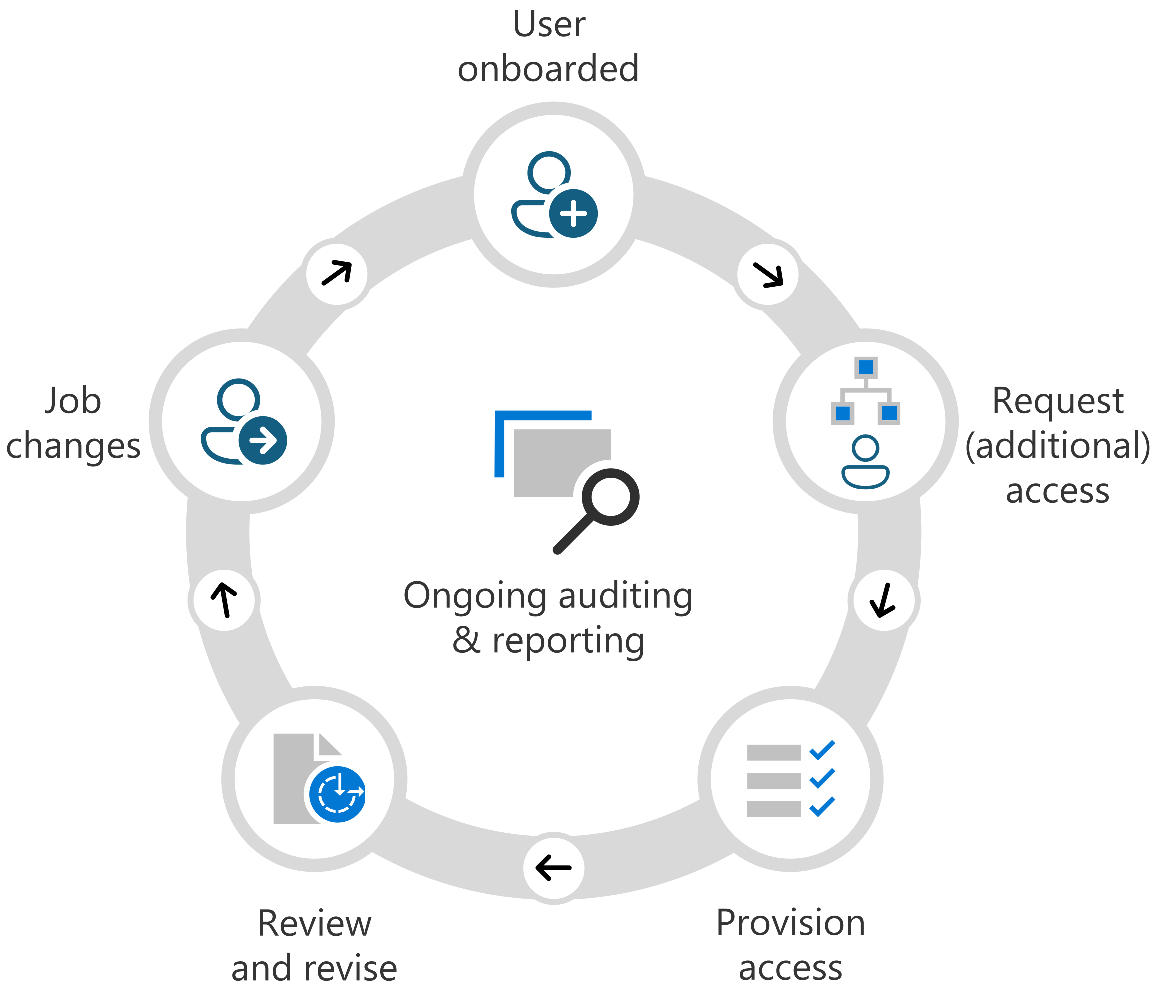
Access recertification to reduce risk

Ongoing auditing & reporting

Access requests, workflow and approvals

Entitlement management

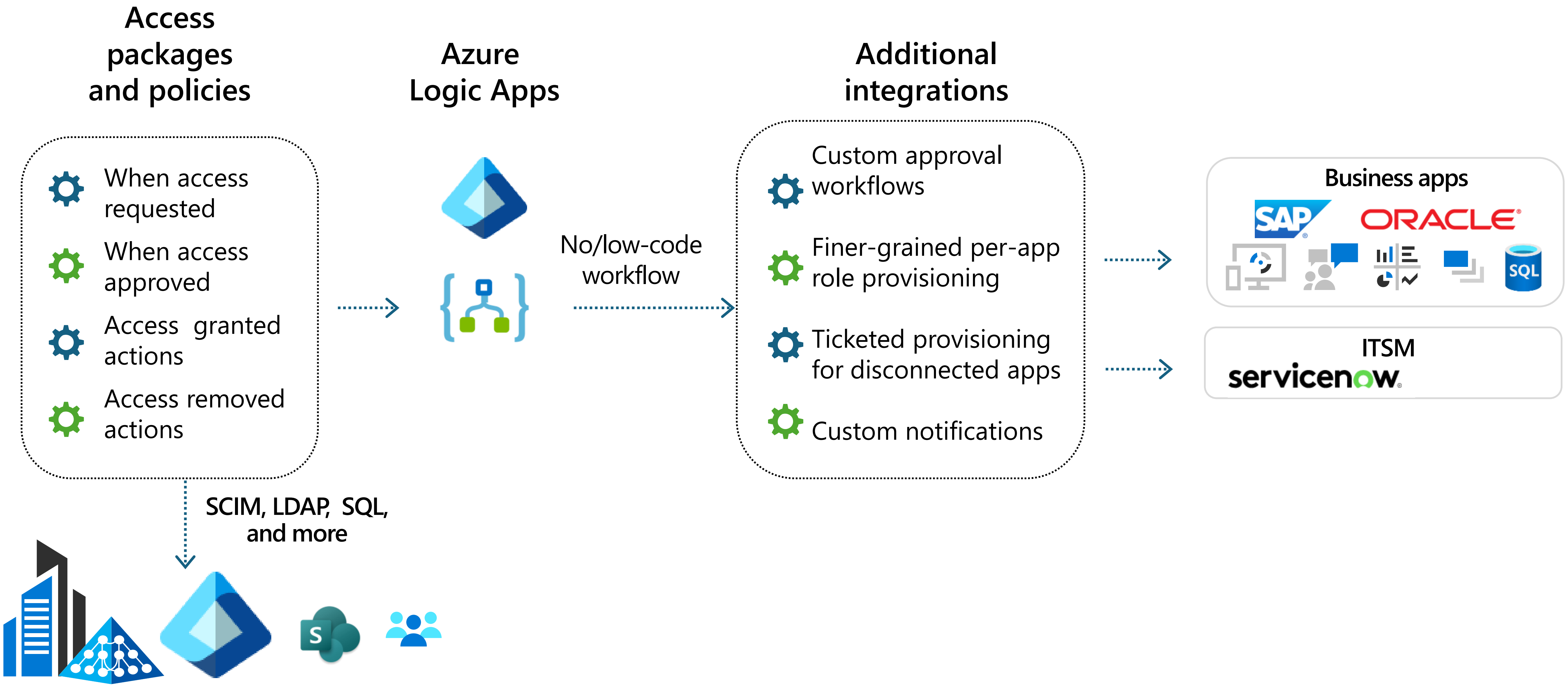
- Give users self-service access requests for resources and automate approval workflows and access assignment, reviews, and expiration for all human identity types (users, guests, etc.)
- Self-service policy and workflow can be defined by app, group or site owners
- Supports multi-stage approval workflows, 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



Public preview

Request and provisioning workflow integrations

Custom workflows for access lifecycle



Access packages and policies

- 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

ITSM

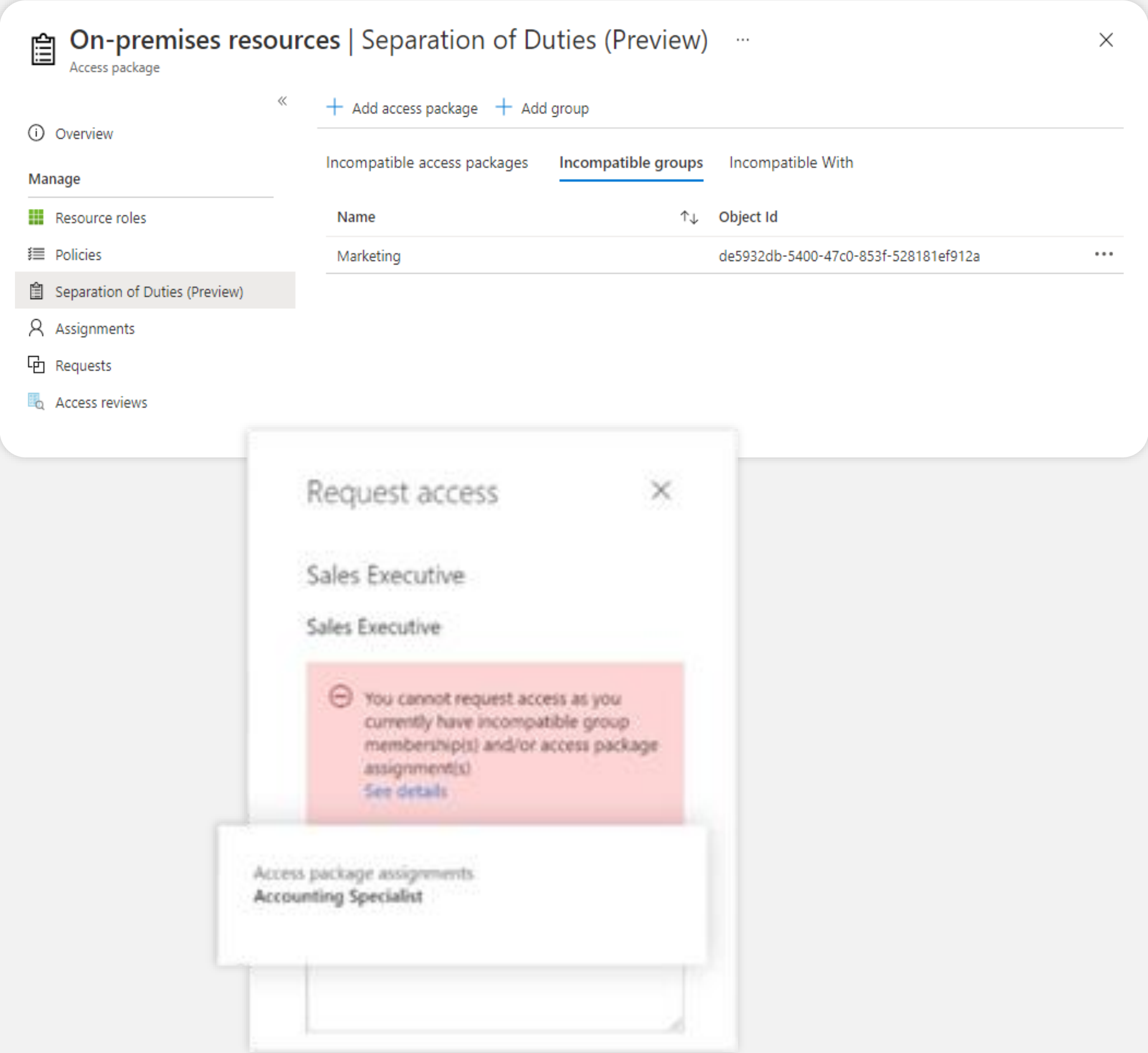
Separation of Duties

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



On-premises resources | Separation of Duties (Preview) ···

Access package

+ Add access package + Add group

Incompatible access packages | **Incompatible groups** | Incompatible With

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

Request access

Sales Executive

Sales Executive

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

Access package assignments
Accounting Specialist

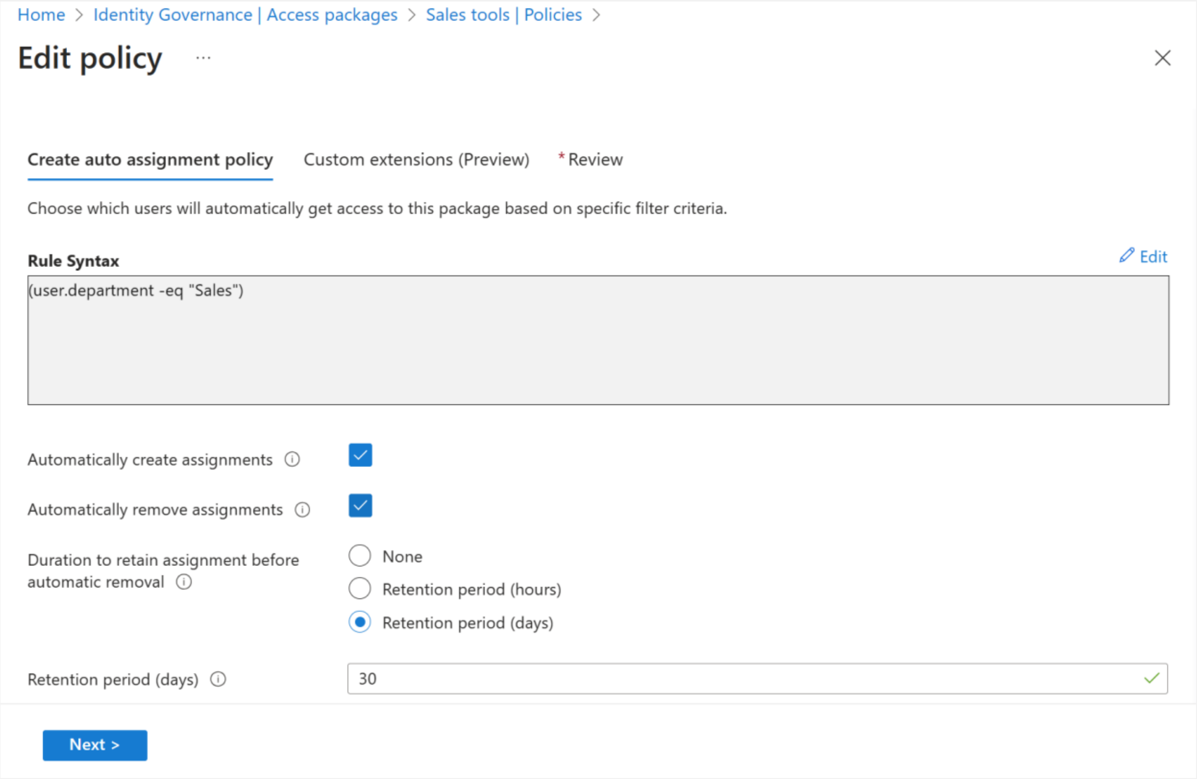
Microsoft Security

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
Edit
Next >

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

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

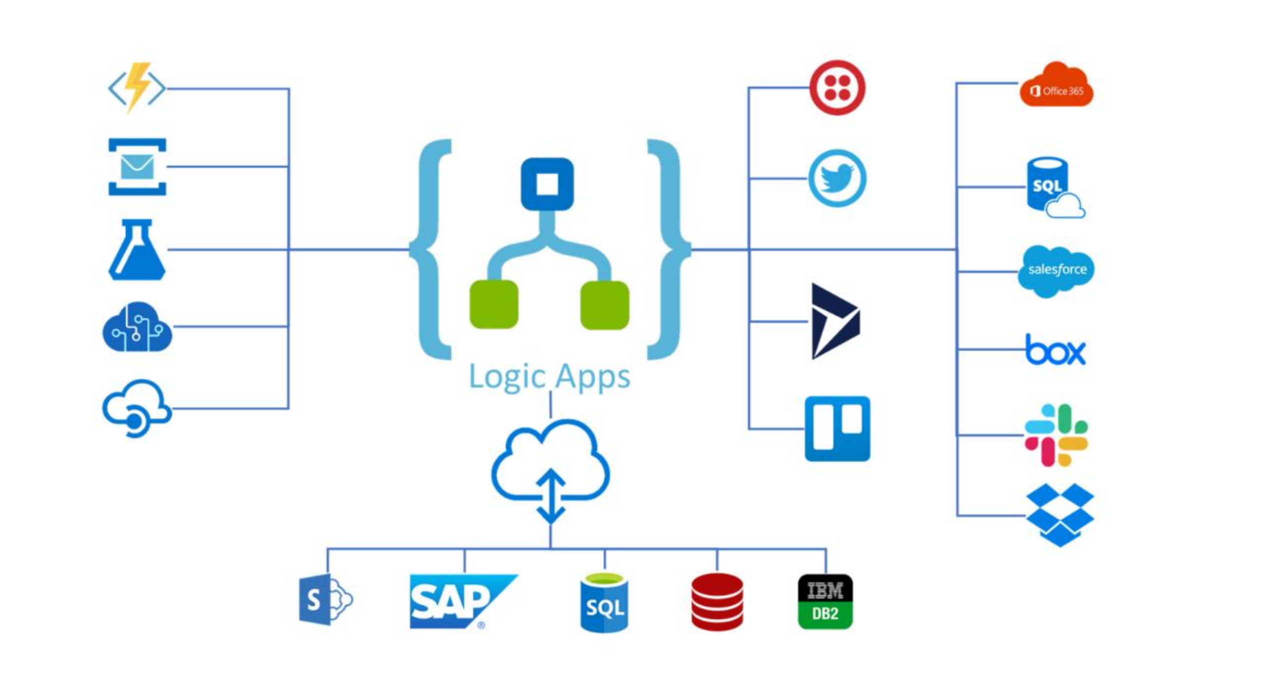
Microsoft Security

Custom Workflows with Logic Apps

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.



Microsoft Security

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

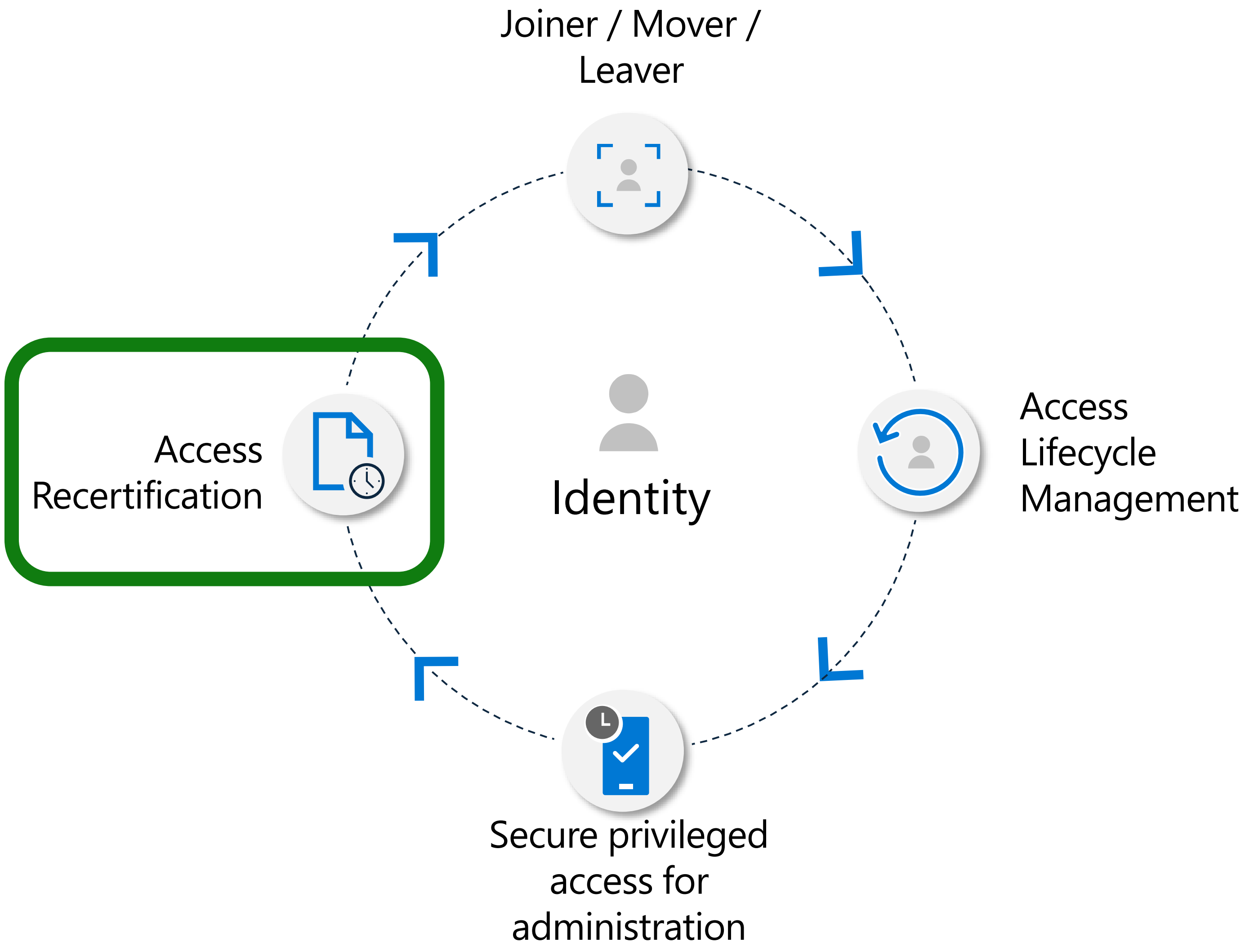
- Processes that you need to automate during the different request stages
- Interfaces available on Target systems
- Request stage where you want to trigger the logic app
- Have Azure Subscription Resources available
- Logic App authentication with target systems

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

Scenario: Access Recertification


Joiner / Mover / Leaver
Access Lifecycle Management
Secure privileged access for administration
Access Recertification
Identity

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

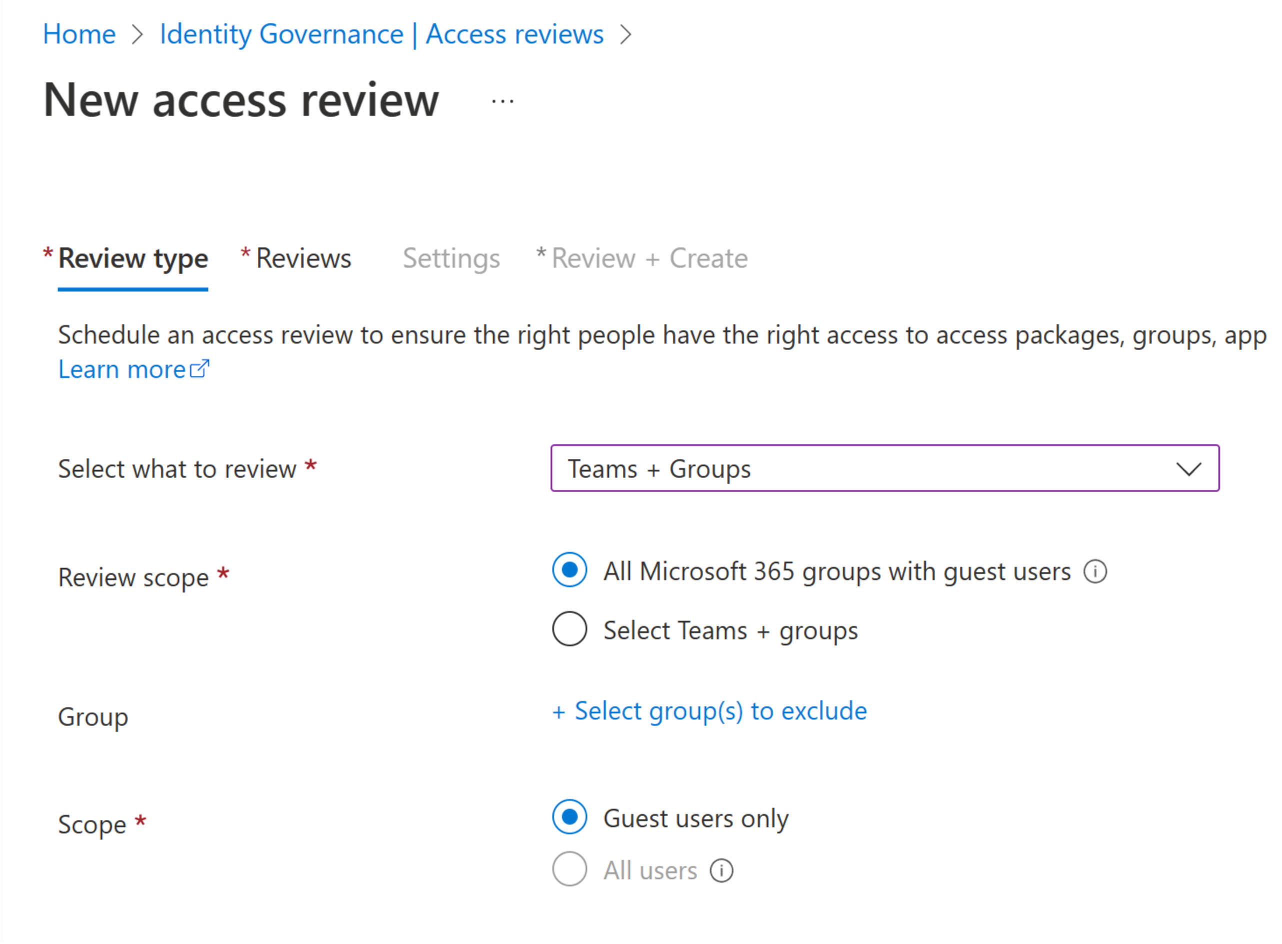
Guests
Employees
Everyone
Workload Identities

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

Group: + Select group(s) to exclude

Scope *:
● Guest users only
○ All users ⓘ

How Access Reviews works

Reviewer

1. Send notification

Email is sent to the reviewer

2. Review

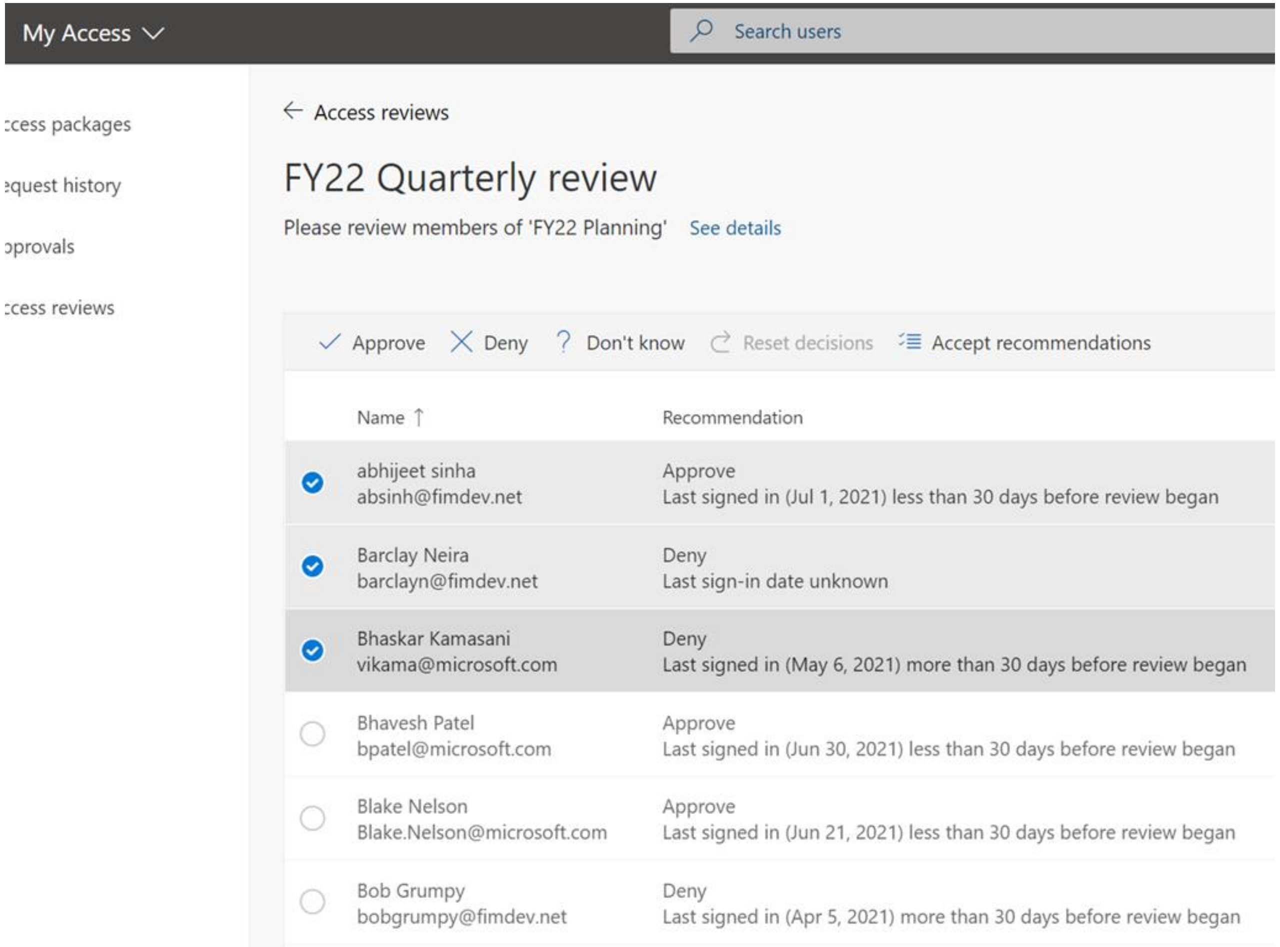
Review current membership with system generated recommendations

3. Confirm

Reviewers confirm which memberships to keep

4. Apply result

Denied users are removed from the resource



FY22 Quarterly review

Please review members of 'FY22 Planning' See details

	Name ↑	Recommendation
●	abhijeet sinha absinh@fimdev.net	Approve Last signed in (Jul 1, 2021) less than 30 days before review began
●	Barclay Neira barclayn@fimdev.net	Deny Last sign-in date unknown
●	Bhaskar Kamasani vikama@microsoft.com	Deny Last signed in (May 6, 2021) more than 30 days before review began
○	Bhavesh Patel bpatel@microsoft.com	Approve Last signed in (Jun 30, 2021) less than 30 days before review began
○	Blake Nelson Blake.Nelson@microsoft.com	Approve Last signed in (Jun 21, 2021) less than 30 days before review began
○	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

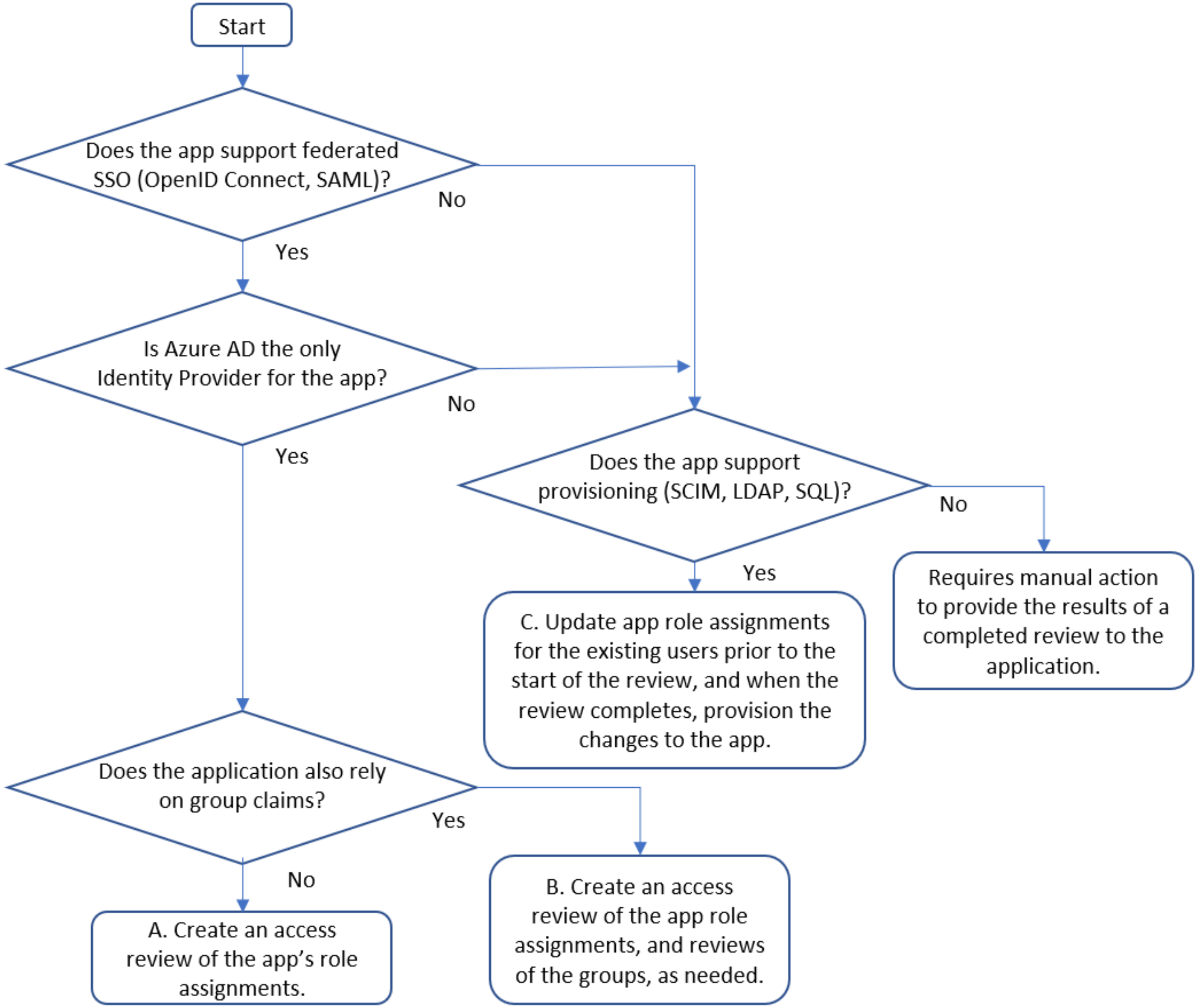
B2B

External Users

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

Planning

- Determine application readiness


Start
Does the app support federated SSO (OpenID Connect, SAML)?
No
Yes
Is Azure AD the only Identity Provider for the app?
No
Yes
Does the app support provisioning (SCIM, LDAP, SQL)?
No
Yes
C. Update app role assignments for the existing users prior to the start of the review, and when the review completes, provision the changes to the app.
Requires manual action to provide the results of a completed review to the application.
Does the application also rely on group claims?
Yes
No
A. Create an access review of the app's role assignments.
B. Create an access review of the app role assignments, and reviews of the groups, as needed.

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.

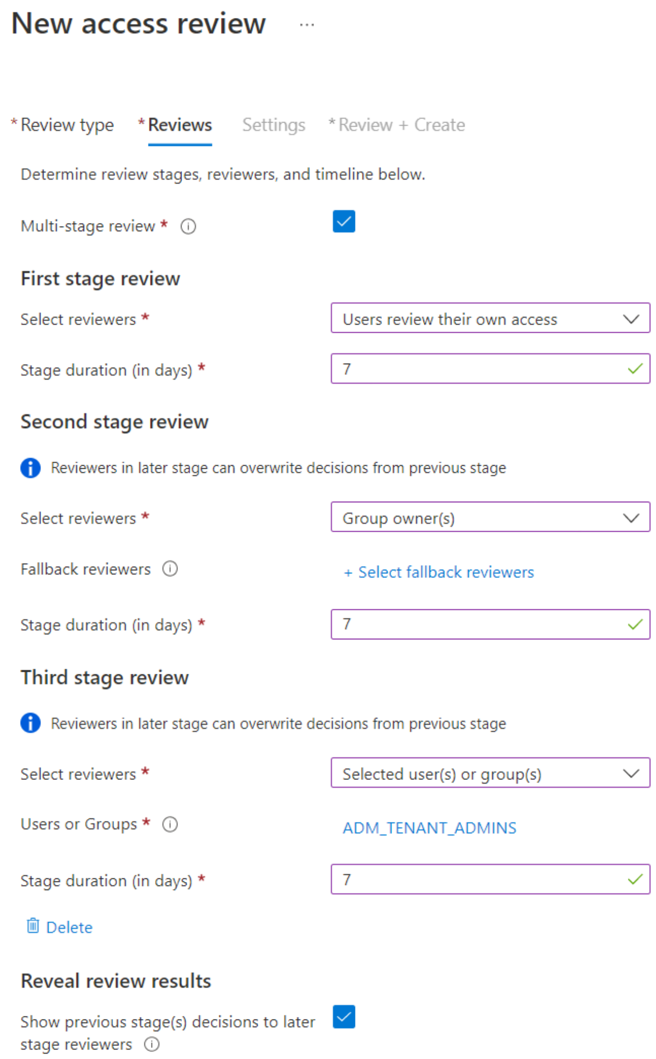
Possible Reviewers:

- 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



Determine review stages, reviewers, and timeline below.

Multi-stage review * ☑

First stage review

Select reviewers * Users review their own access

Stage duration (in days) * 7

Second stage review

Reviewers in later stage can overwrite decisions from previous stage

Select reviewers * Group owner(s)

Fallback reviewers + Select fallback reviewers

Stage duration (in days) * 7

Third stage review

Reviewers in later stage can overwrite decisions from previous stage

Select reviewers * Selected user(s) or group(s)

Users or Groups * ADM_TENANT_ADMINS

Stage duration (in days) * 7

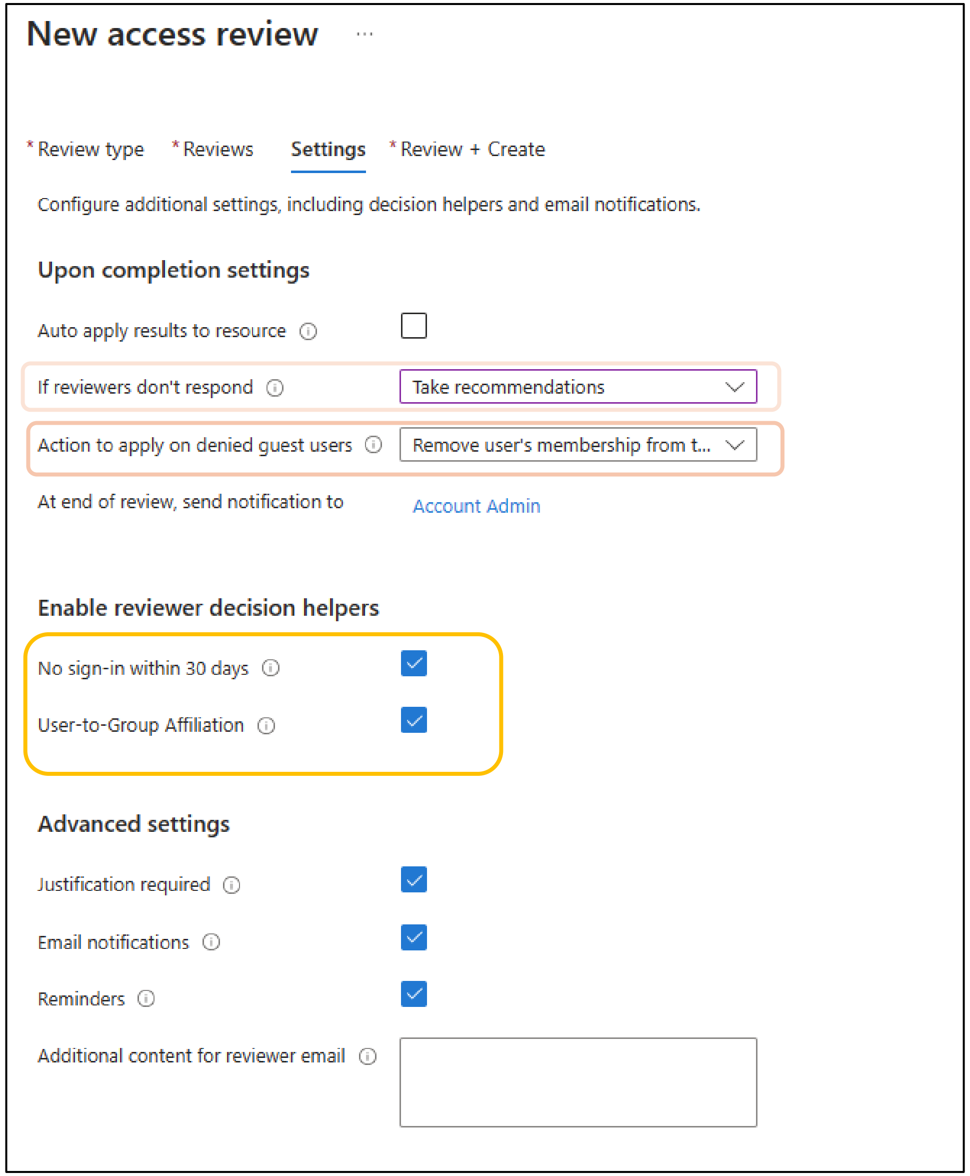
Reveal review results

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



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 Reviews Decisions

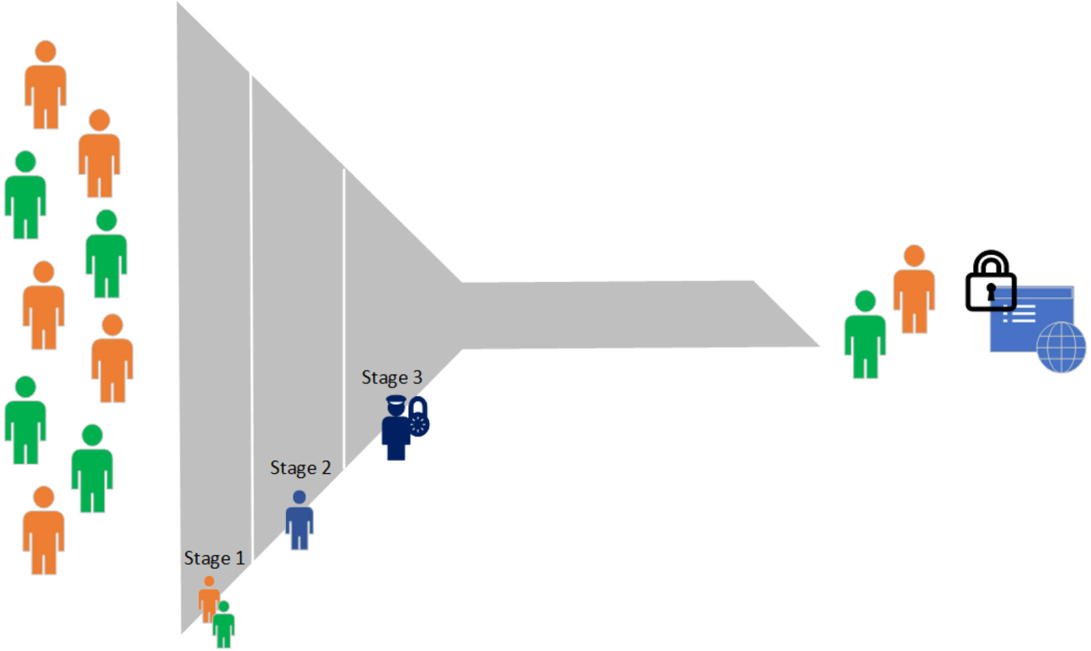
First stage reviewers?
Select user(s) or group(s) – the owner(s) of the applications

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

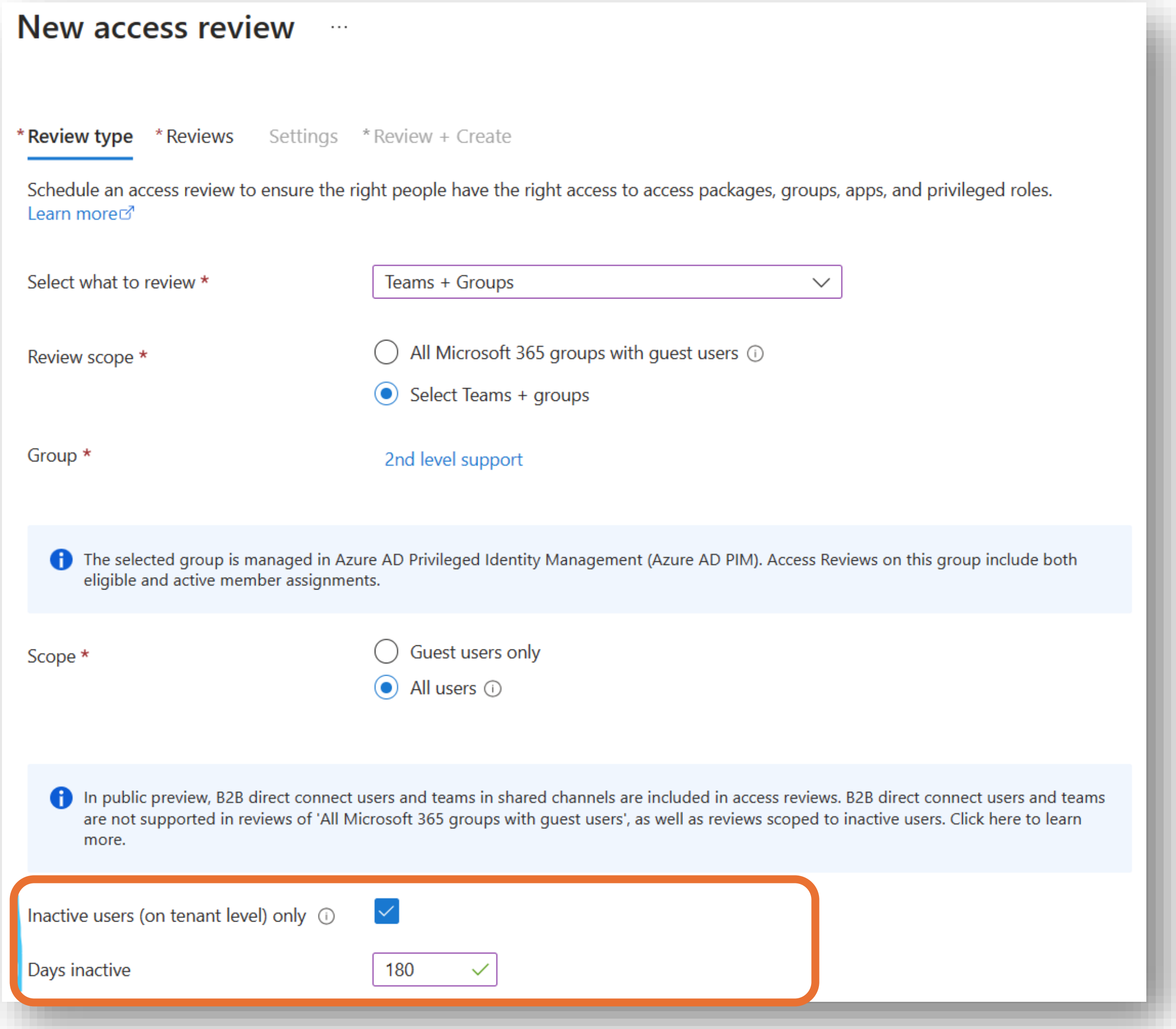


AR – Inactive Users

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 ···

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

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

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.

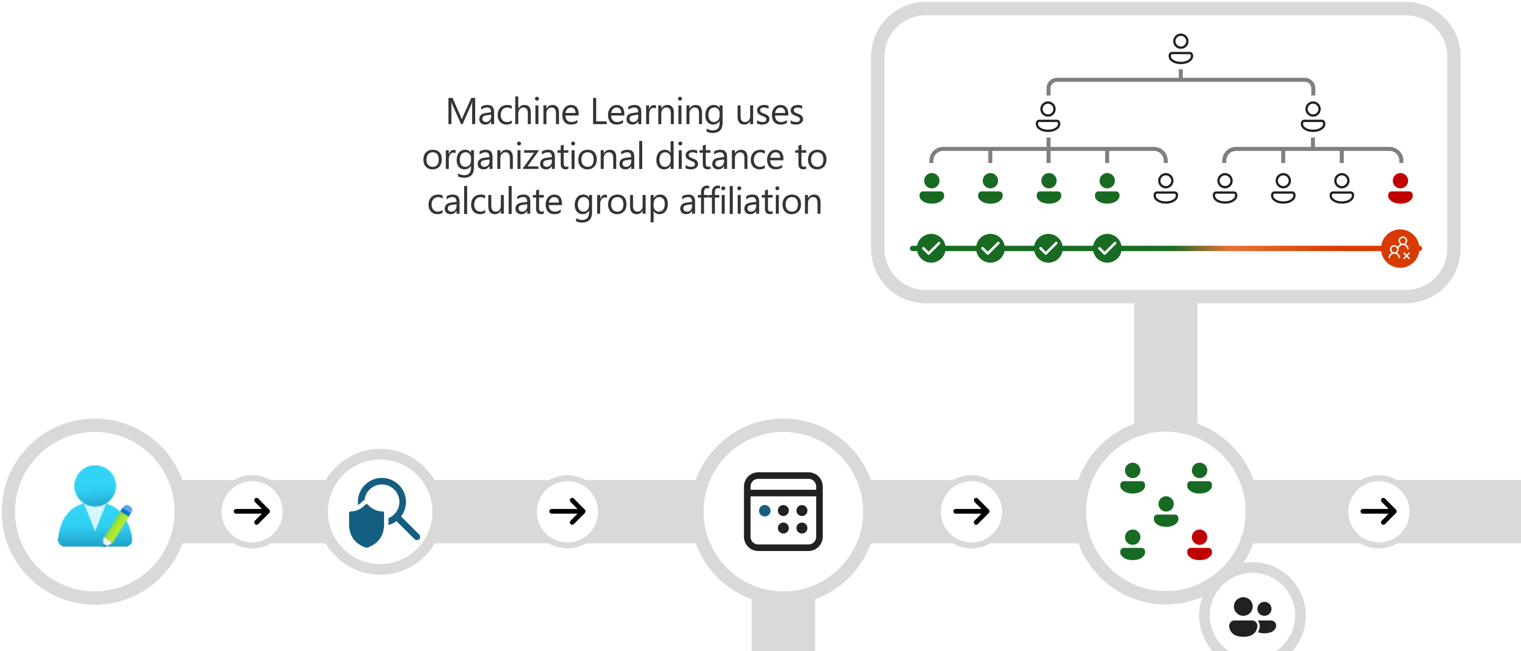
Inactive users (on tenant level) only ☑

Days inactive 180

Machine Learning based recommendations in Access Reviews

User-to-Group Affiliation

Machine Learning uses organizational distance to calculate group affiliation

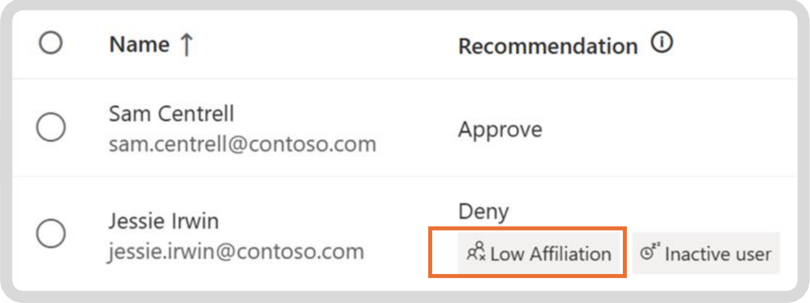


Admins create Access Review to protect against breaches and stay compliant

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

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



○	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

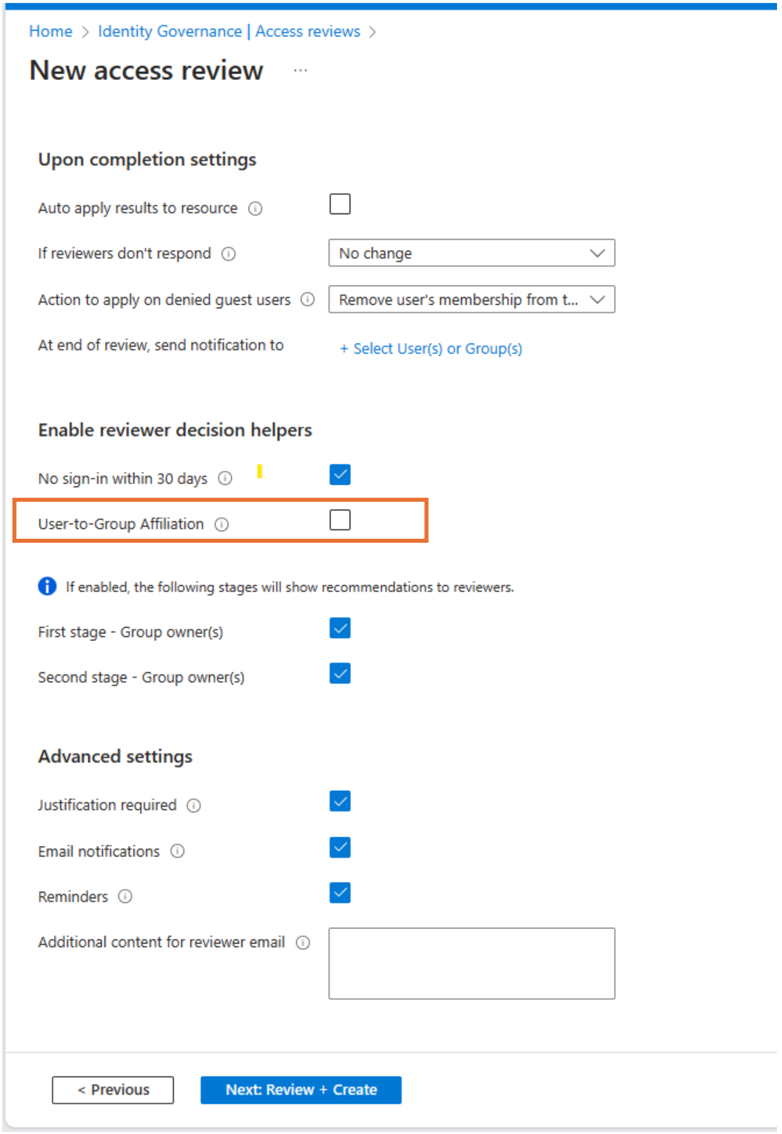
User to Group Affiliation

- 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



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 ⓘ ☑

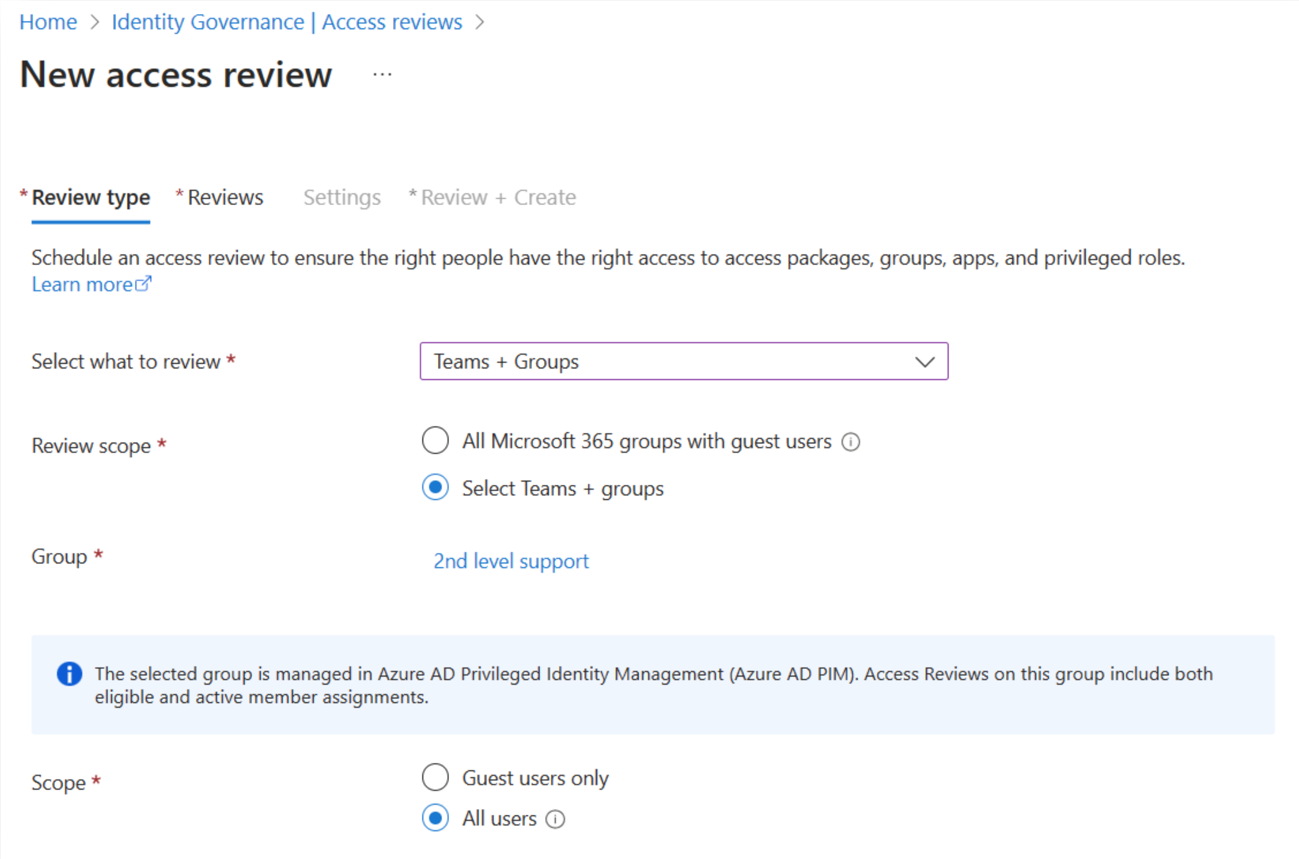
Additional content for reviewer email ⓘ

AR – PIM for Groups

Public preview

Review access for PIM for Groups

- Includes active members of the group and eligible members
- Only active owners can be assigned as reviewers
- Inactivity of users up to 2 years



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

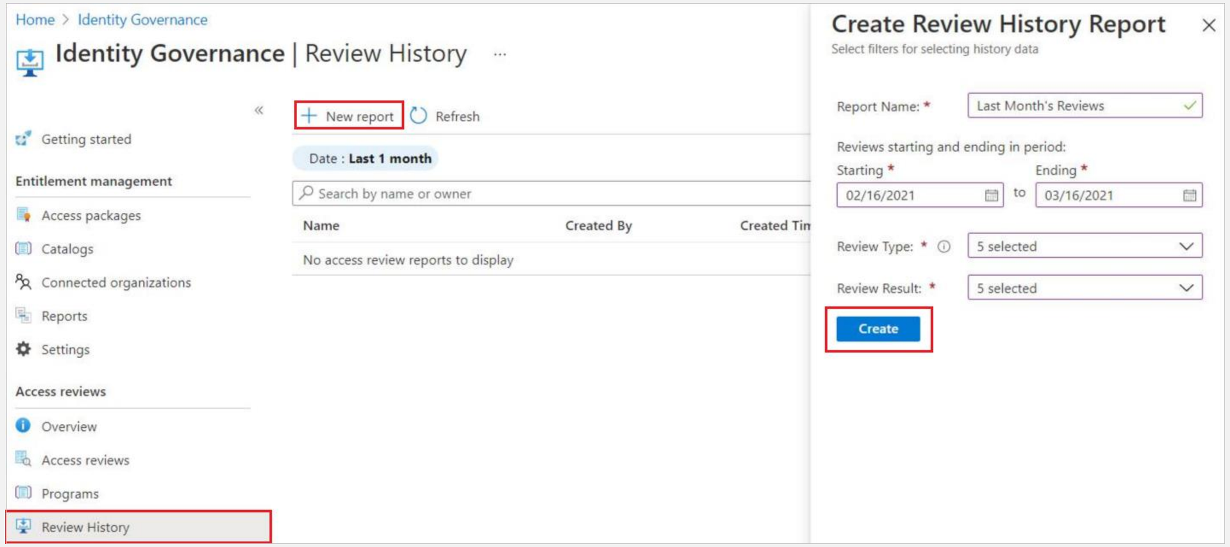
Group * 2nd level support

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

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 Tim
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

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?

Microsoft Secu

Thank you