NT KONF

25. – 27.
SEPTEMBER
2023
PORTOROŽ

NT KONF
NT KONFERENCA

Entra ID Entitlement Management

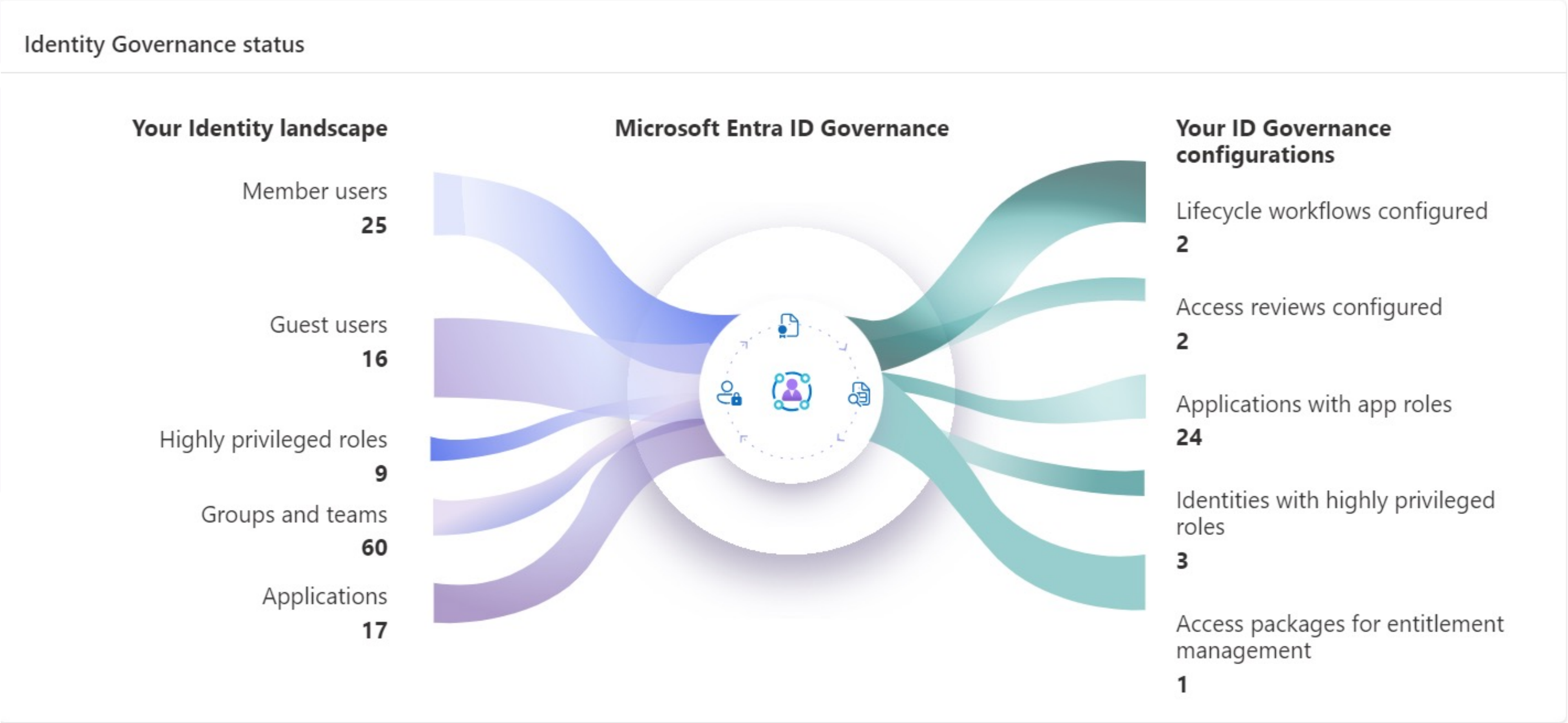
Damir Dizdarević
Logosoft d.o.o. Sarajevo

Microsoft®
Regional Director

Microsoft®
MVP
Most Valuable
Professional

Microsoft Entra Identity Governance

Microsoft Entra ID Governance allows you to balance your organization's need for security and employee productivity with the right processes and visibility.



Identity Governance status

Your Identity landscape

Member users
25

Guest users
16

Highly privileged roles
9

Groups and teams
60

Applications
17

Microsoft Entra ID Governance

Your ID Governance configurations

Lifecycle workflows configured
2

Access reviews configured
2

Applications with app roles
24

Identities with highly privileged roles
3

Access packages for entitlement management
1

What is Entitlement Management?

- Entitlement management is an identity governance feature in Entra ID, that enables organizations to manage identity and access lifecycle at scale, by automating access request workflows, access assignments, reviews, and expiration.

- Entitlement management helps to more efficiently manage access to groups, applications, and SharePoint Online sites for internal users, and also for users outside your organization who need access to those resources.

- To use entitlement management, you must have one of these licenses:
  - Microsoft Entra ID P2 or Microsoft Entra ID Governance
  - Enterprise Mobility + Security (EMS) E5

Why should we use entitlement management?

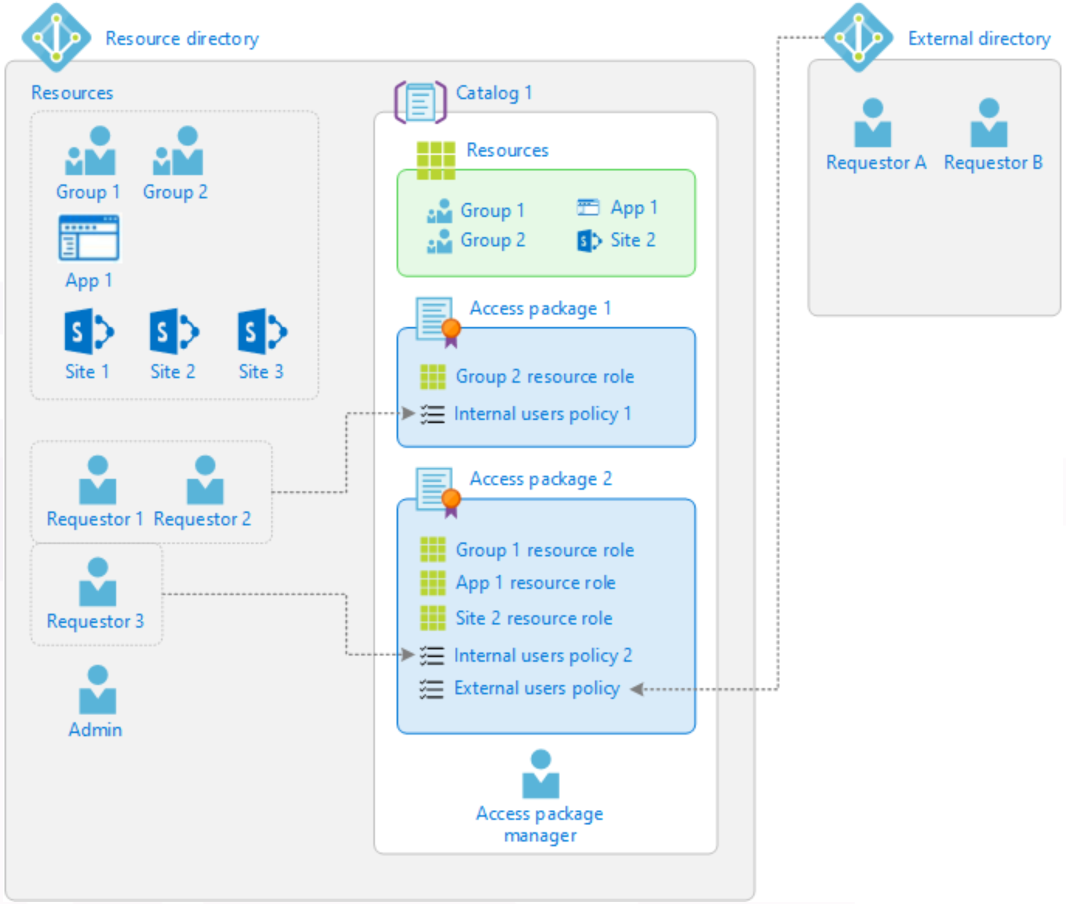
- Enterprise organizations often face challenges when managing employee access to resources such as:
  - Users may not know what access they should have, and even if they do, they may have difficulty locating the right individuals to approve their access
  - Once users find and receive access to a resource, they may hold on to access longer than is required for business purposes
- These problems are compounded for users who need access from another organization, such as external users that are from supply chain organizations or other business partners. For example:
  - No one person may know all of the specific individuals in other organization's directories to be able to invite them
  - Even if they were able to invite these users, no one in that organization may remember to manage all of the users' access consistently

What can I do with entitlement management?

- Control who can get access to applications, groups, Teams and SharePoint sites, with multi-stage approval, and ensure users don't retain access indefinitely
- Give users access automatically to those resources, based on the user's properties like department or cost center, and remove a user's access when those properties change
- Delegate to non-administrators the ability to create access packages.
- Select connected organizations whose users can request access.

What are access request packages?

- An access package enables you to do a one-time setup of resources and policies that automatically administers access for the life of the access package.
- An access package can be used to assign access to roles of multiple resources that are in the catalog.
- The separation of duties lets you prevent users from requesting an access package if they're already assigned to other access packages or are a member of other groups.



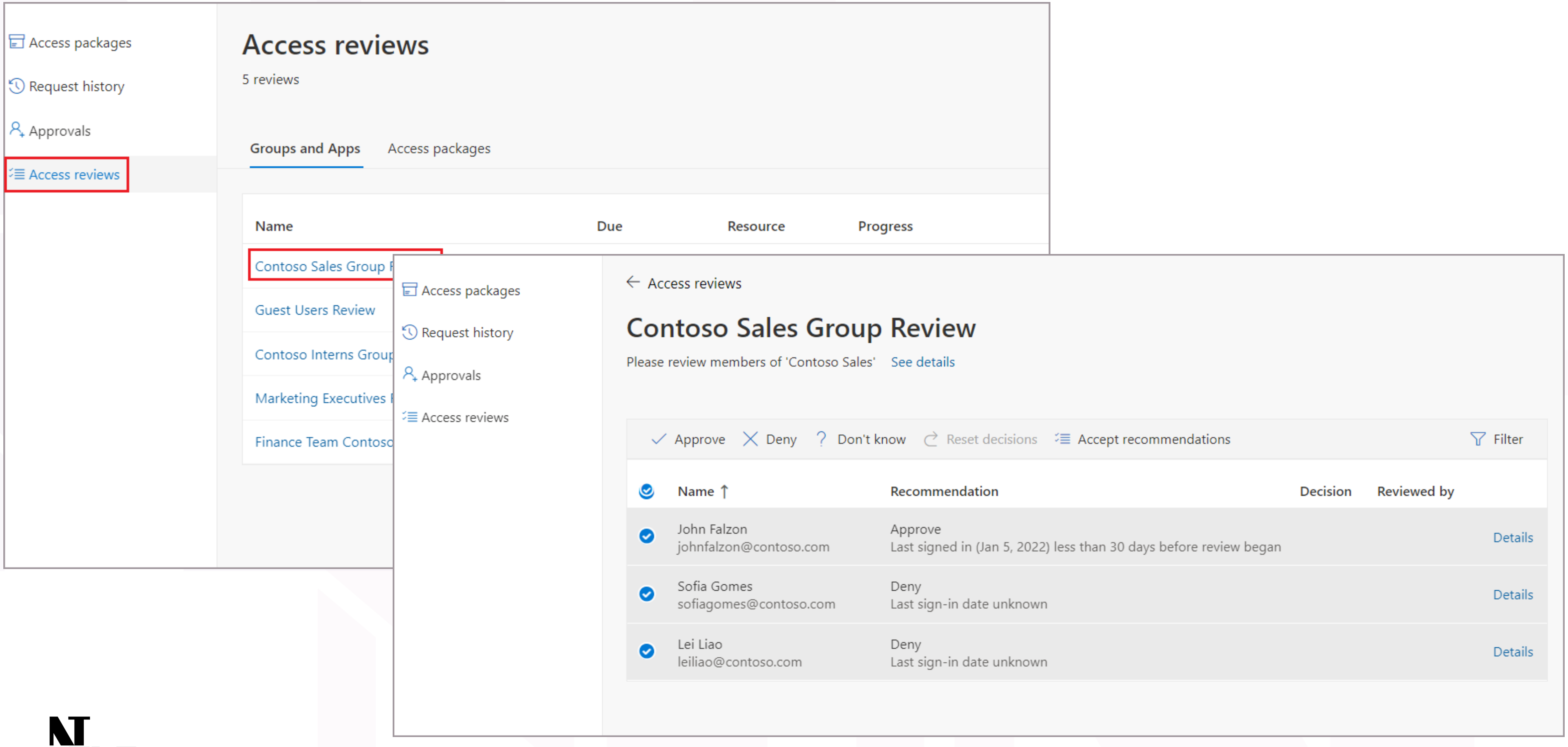
What are access reviews?

- Access reviews in Entra ID, enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments.
- User's access can be reviewed regularly to make sure only the right people have continued access.
- Access reviews address following:
  - As new employees join, how do you ensure they have the access they need to be productive?
  - As people move teams or leave the company, how do you make sure that their old access is removed?
  - Excessive access rights can lead to compromises.
  - Excessive access right may also lead audit findings as they indicate a lack of control over access.
  - You have to proactively engage with resource owners to ensure they regularly review who has access to their resources.

When should you use access reviews?

- Too many users in privileged roles
- When automation is not possible
- When a group is used for a new purpose
- Business critical data access
- Ask group owners to confirm they still need guests in their groups
- Have reviews recur periodically

Review access



Access reviews

5 reviews

Name	Due	Resource	Progress
Contoso Sales Group R			
Guest Users Review			
Contoso Interns Group			
Marketing Executives R			
Finance Team Contoso			

Contoso Sales Group Review

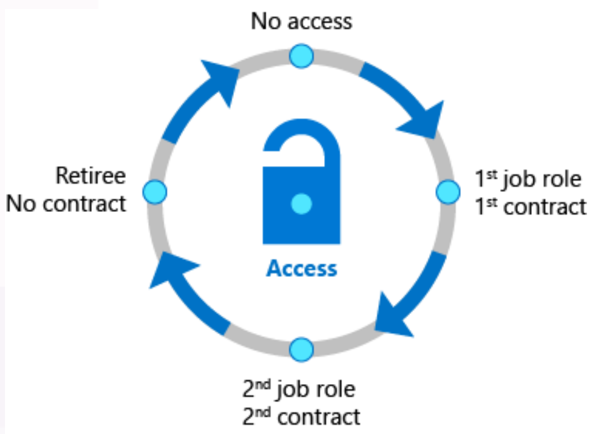
Please review members of 'Contoso Sales' See details

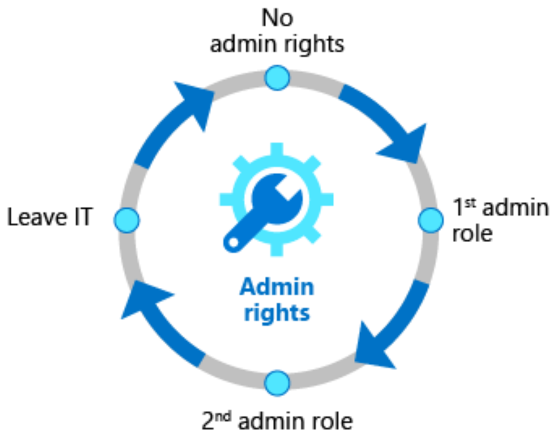
	Name ↑	Recommendation	Decision	Reviewed by	
✓	John Falzon johnfalzon@contoso.com	Approve Last signed in (Jan 5, 2022) less than 30 days before review began			Details
✓	Sofia Gomes sofiagomes@contoso.com	Deny Last sign-in date unknown			Details
✓	Lei Liao leiliao@contoso.com	Deny Last sign-in date unknown			Details

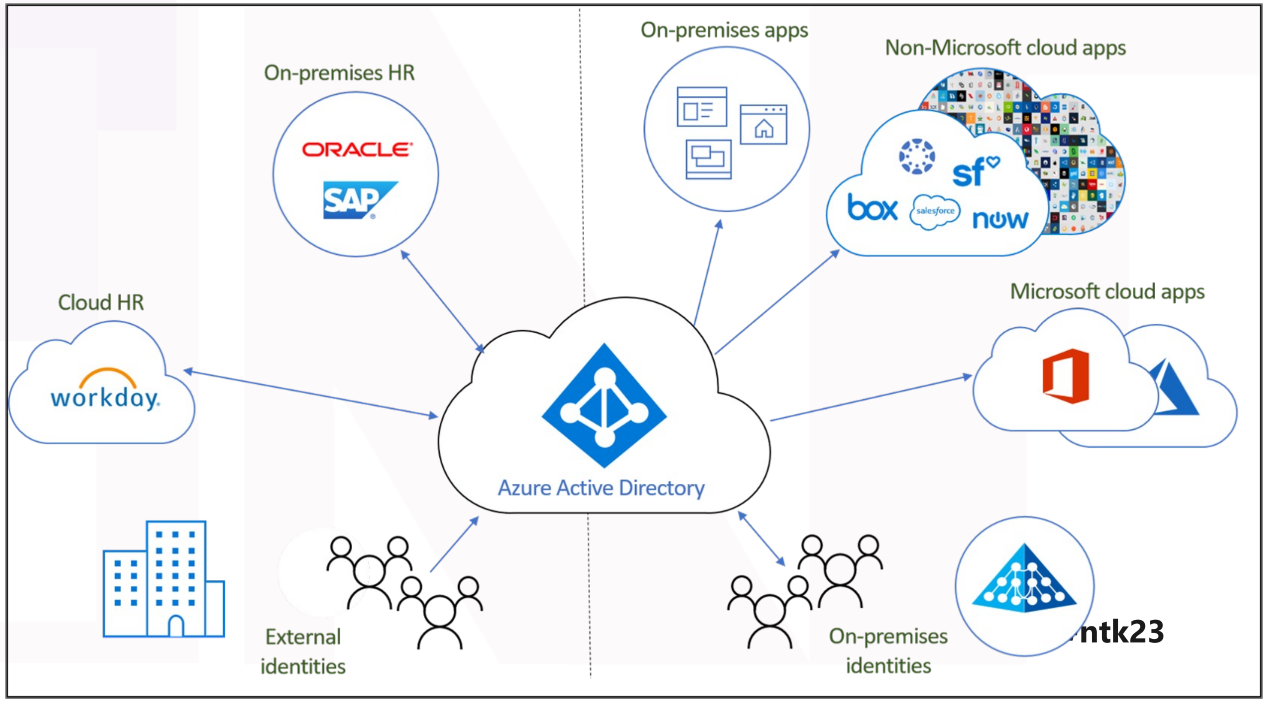
What is identity lifecycle management?

- Identity lifecycle management is the foundation for Identity Governance, and effective governance at scale requires modernizing the identity lifecycle management infrastructure for applications.

- Identity Lifecycle Management aims to automate and manage the entire digital identity lifecycle process.



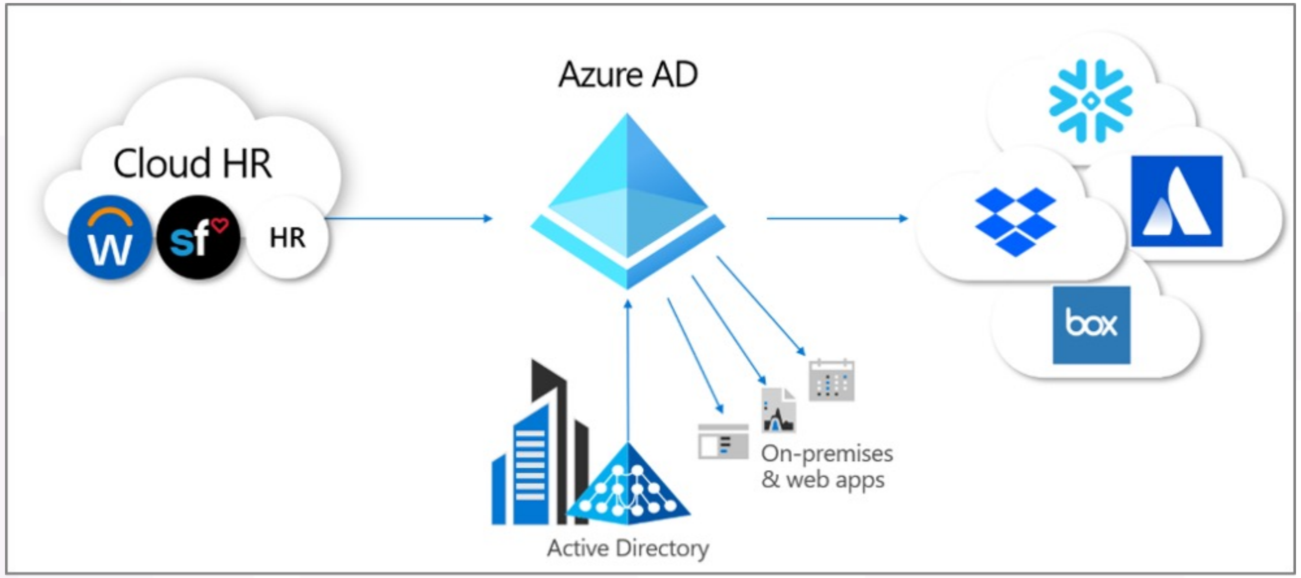




ntk23

Typical identity lifecycle tasks

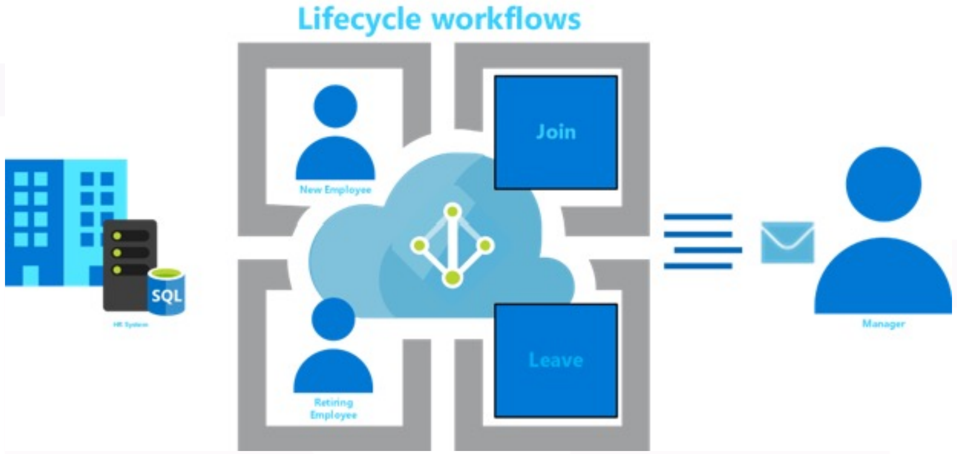
- Join - when an individual comes into scope of needing access, an identity is needed by those applications, so a new digital identity may need to be created if one isn't already available
- Move - when an individual moves between boundaries that require additional access authorizations to be added or removed to their digital identity
- Leave - when an individual leaves the scope of needing access, access may need to be removed, and subsequently the identity may no longer be required by applications other than for audit or forensics purposes



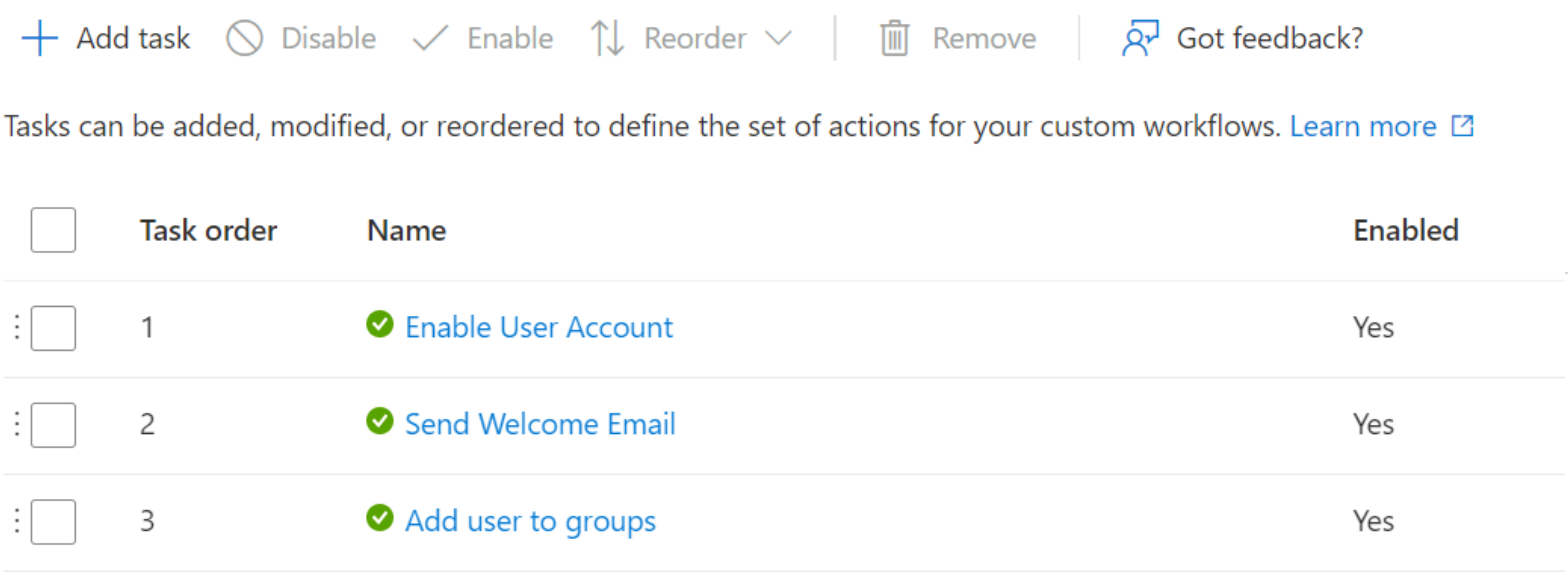
What are lifecycle workflows?

Lifecycle workflows are a new identity governance feature that enables organizations to manage Azure Active Directory (Azure AD) users by automating these three basic lifecycle processes:

- **Joiner:** When an individual enters the scope of needing access. An example is a new employee joining a company or organization.
- **Mover:** When an individual moves between boundaries within an organization. This movement might require more access or authorization. An example is a user who was in marketing and is now a member of the sales organization.
- **Leaver:** When an individual leaves the scope of needing access. This movement might require the removal of access. Examples are an employee who's retiring or an employee who's terminated.

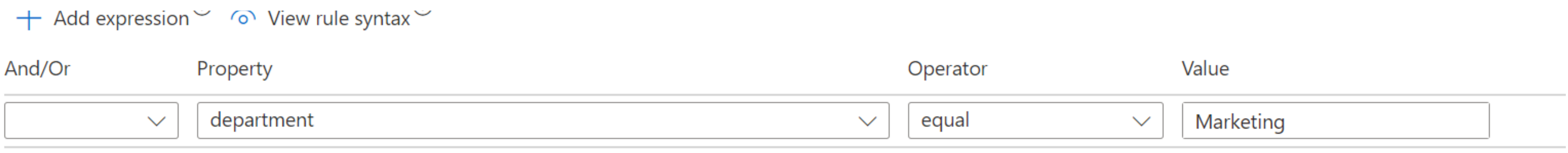


Lifecycle workflows



Tasks can be added, modified, or reordered to define the set of actions for your custom workflows. Learn more

□	Task order	Name	Enabled
□	1	✓ Enable User Account	Yes
□	2	✓ Send Welcome Email	Yes
□	3	✓ Add user to groups	Yes



And/Or	Property	Operator	Value
	department	equal	Marketing

Entra ID Entitlement management - DEMO

NT KONF

NT KONFERENCA

25. – 27.
SEPTEMBER
2023
PORTOROŽ

This is not school, but we love to get grades.
Please fill out our questoineers and leave us your feedback.
You may even win some cool rewards.

NT
KONF

NT KONFERENCA

25. – 27.
SEPTEMBER
2023
PORTOROŽ