Microsoft Entra ID Identity Protection and Governance Capabilities

Vlad Catrinescu

Microsoft MVP | Independent Consultant

@vladcatrinescu | VladTalksTech.com | YouTube.com/@VladTalksTech

Overview

Microsoft Entra ID Governance

Dynamic groups

Entra ID access reviews

Entra ID Entitlement Management

Entra ID Privileged Identity Management

Entra ID Protection

Microsoft Entra Permissions Management

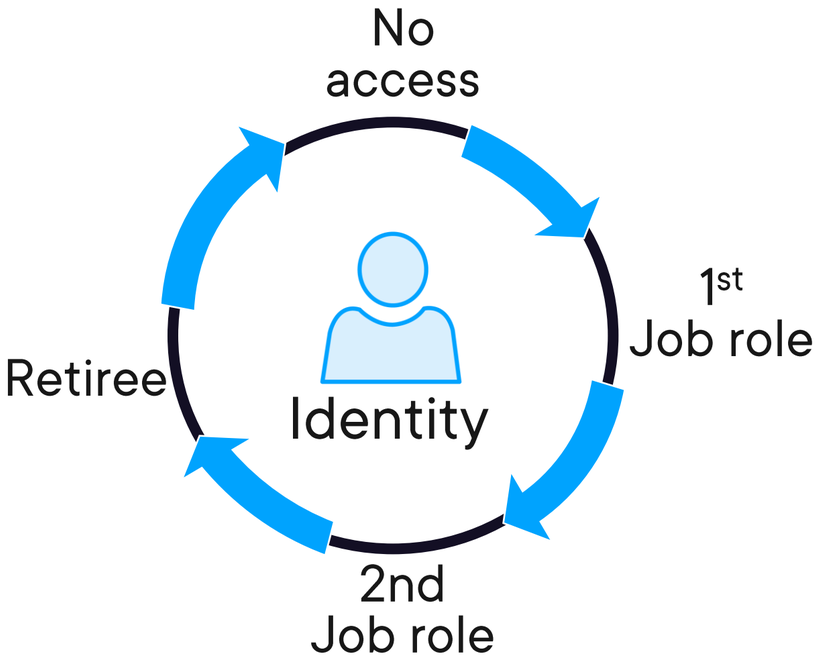
Microsoft Entra ID Governance

Microsoft Entra ID Governance

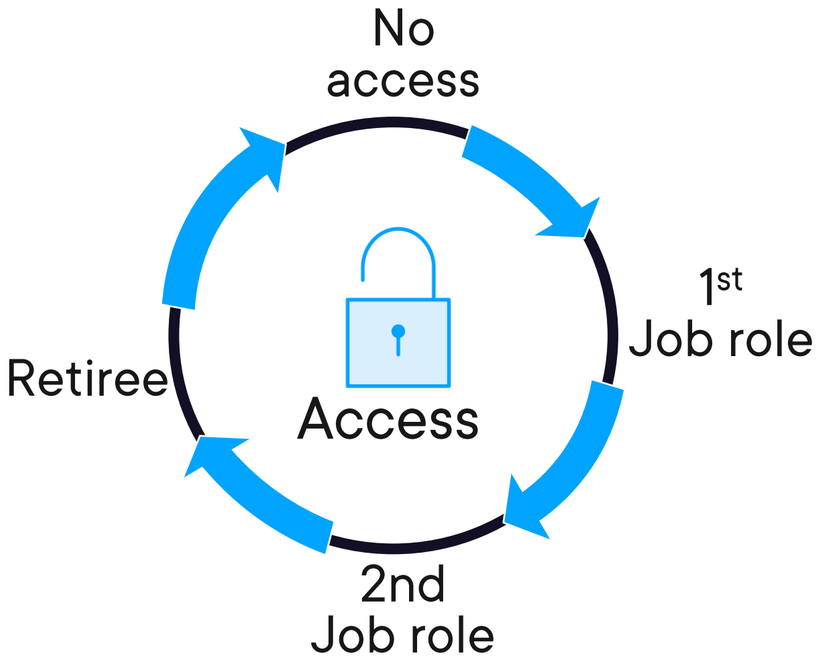
Microsoft Entra ID Governance allows you to balance your organization's need for security and employee productivity with the right processes and visibility. It provides you with capabilities to ensure that the right people have the right access to the right resources.

https://learn.microsoft.com/en-us/entra/id-governance/identity-governance-overview

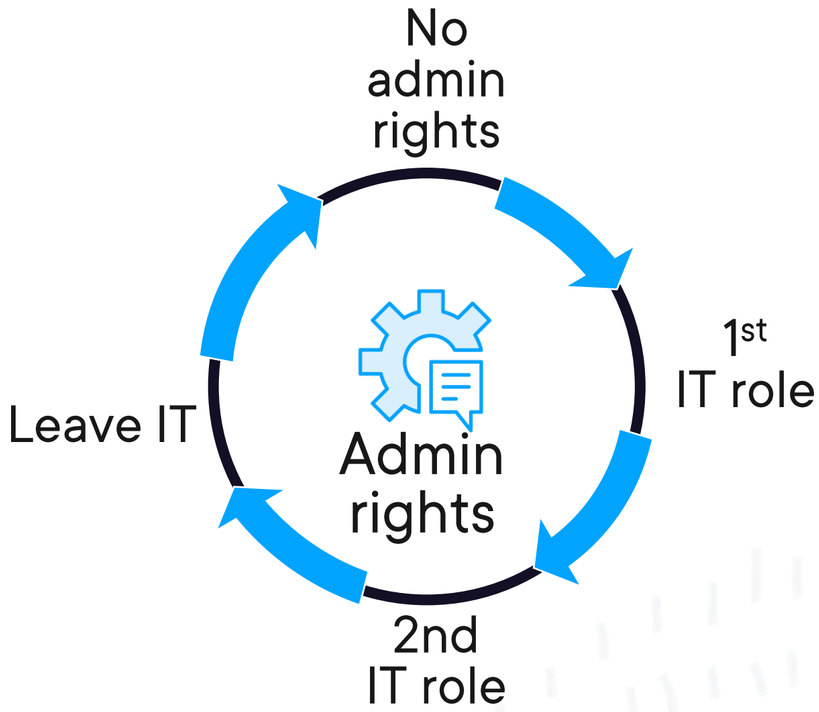
Microsoft Entra ID Governance



Identity Lifecycle

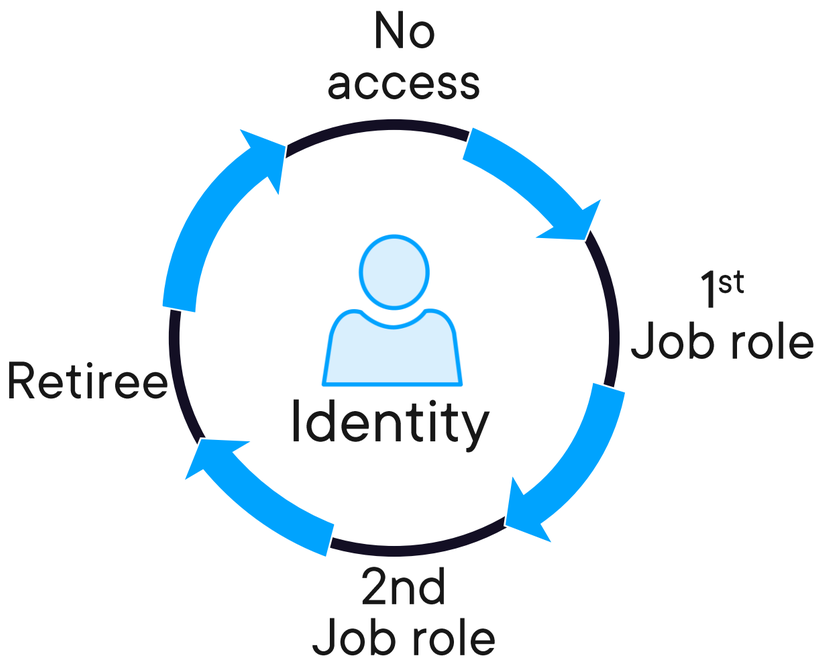


Access Lifecycle



Privileged Access Lifecycle

Identity Lifecycle



Achieve a balance between

- Productivity
  - How quickly can a person have access to the resources they need?
- And security
  - How should their access change over time?

Access Lifecycle

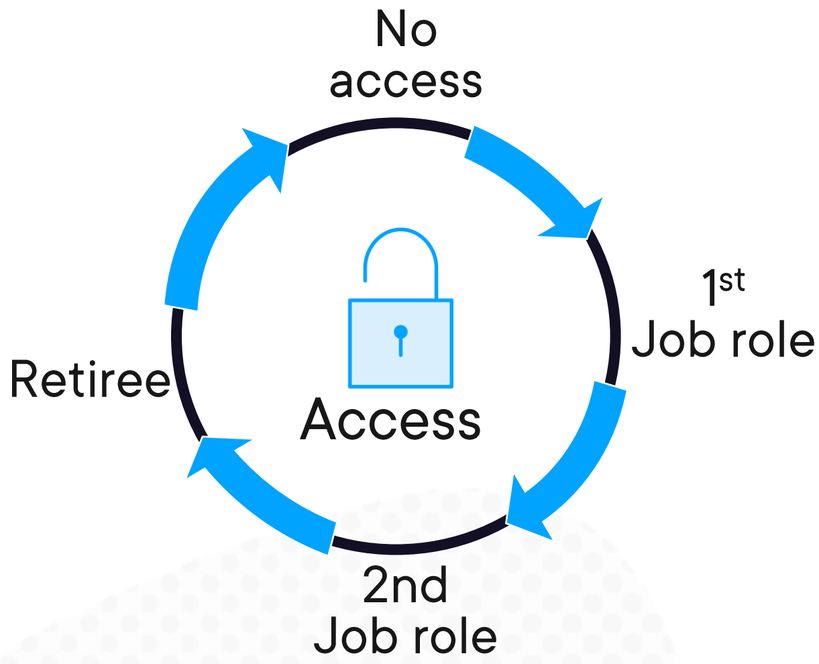
Manage access beyond what was initially provisioned for a user

Automate as much as possible

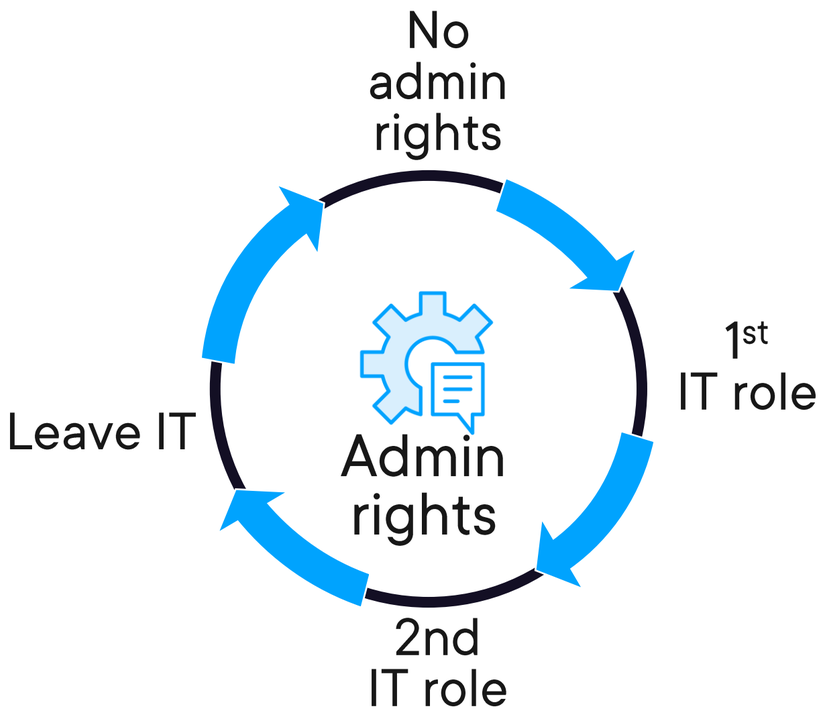
Delegate access to business users

- IT must not become a blocker

Make sure users have the least access needed for their jobs



Privileged Access Lifecycle



Governance process around granting of administrative roles

- Just-in-time access
- Role change alerting capabilities

Microsoft Entra ID Governance Tools

Access Reviews

Entitlement Management

Privileged Identity Management

ID Protection

Microsoft Entra ID Governance Licensing

Feature	Free	Microsoft Entra ID P1	Microsoft Entra ID P2	Microsoft Entra ID Governance
API-driven provisioning		✅	✅	✅
HR-driven provisioning		✅	✅	✅
Automated user provisioning to SaaS apps	✅	✅	✅	✅
Automated group provisioning to SaaS apps		✅	✅	✅
Automated provisioning to on-premises apps		✅	✅	✅
Conditional Access - Terms of use attestation		✅	✅	✅
Entitlement management - Basic entitlement management			✅	✅
Entitlement management - Conditional Access Scoping			✅	✅

Most features require Entra ID Premium P1 or P2

- Entra ID Premium 1 or 2 include the basic functionalities of a certain feature

Advanced functionalities require the Microsoft Entra ID Governance add-on

Many of those features were in preview and usable by P1/P2 users until October 30th, 2023

- Now you need a license to activate them

Guests will also require additional licensing for features to work on their accounts

Licensing References

Microsoft Entra ID Governance licensing for business guests

https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad-blog/microsoft-entra-id-governance-licensing-for-business-guests/ba-p/3575579

Microsoft Entra ID Governance licensing fundamentals

https://learn.microsoft.com/en-us/entra/id-governance/licensing-fundamentals#features-by-license

Dynamic Groups

Dynamic Groups

Groups make it easier for admins to grant permissions to content/applications at scale

Dynamic groups make it easier to automate group membership based on user profile properties

- Department
- Country
- City
- Title
- State

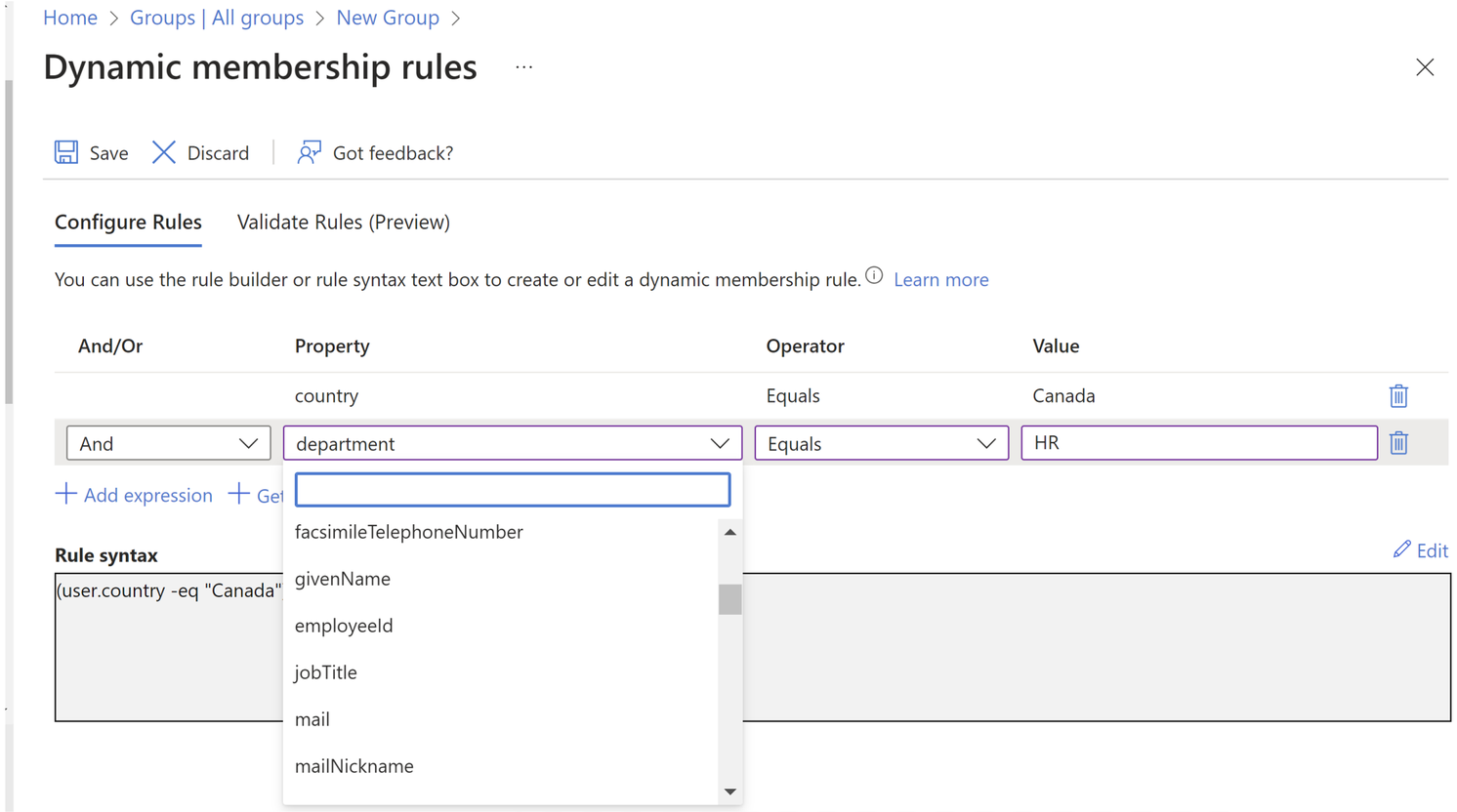
User interface to build rules

- Can also copy paste if you pre-built them in an external editor

Rule validator allows you to try it out before creating the group

- Add users and see if they would be in the group or not!

Membership processing is not instant

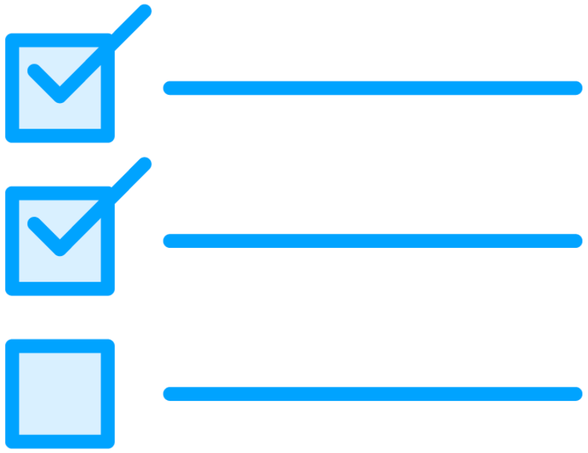


Demo

Dynamic groups

Entra ID Access Reviews

Entra ID Access Reviews



Access reviews help you proactively engage owners to verify permissions

Remove permissions of users who no longer need access to a resource

Settings You Can Configure

Review M365 Groups or Applications

All Users or Guests Only

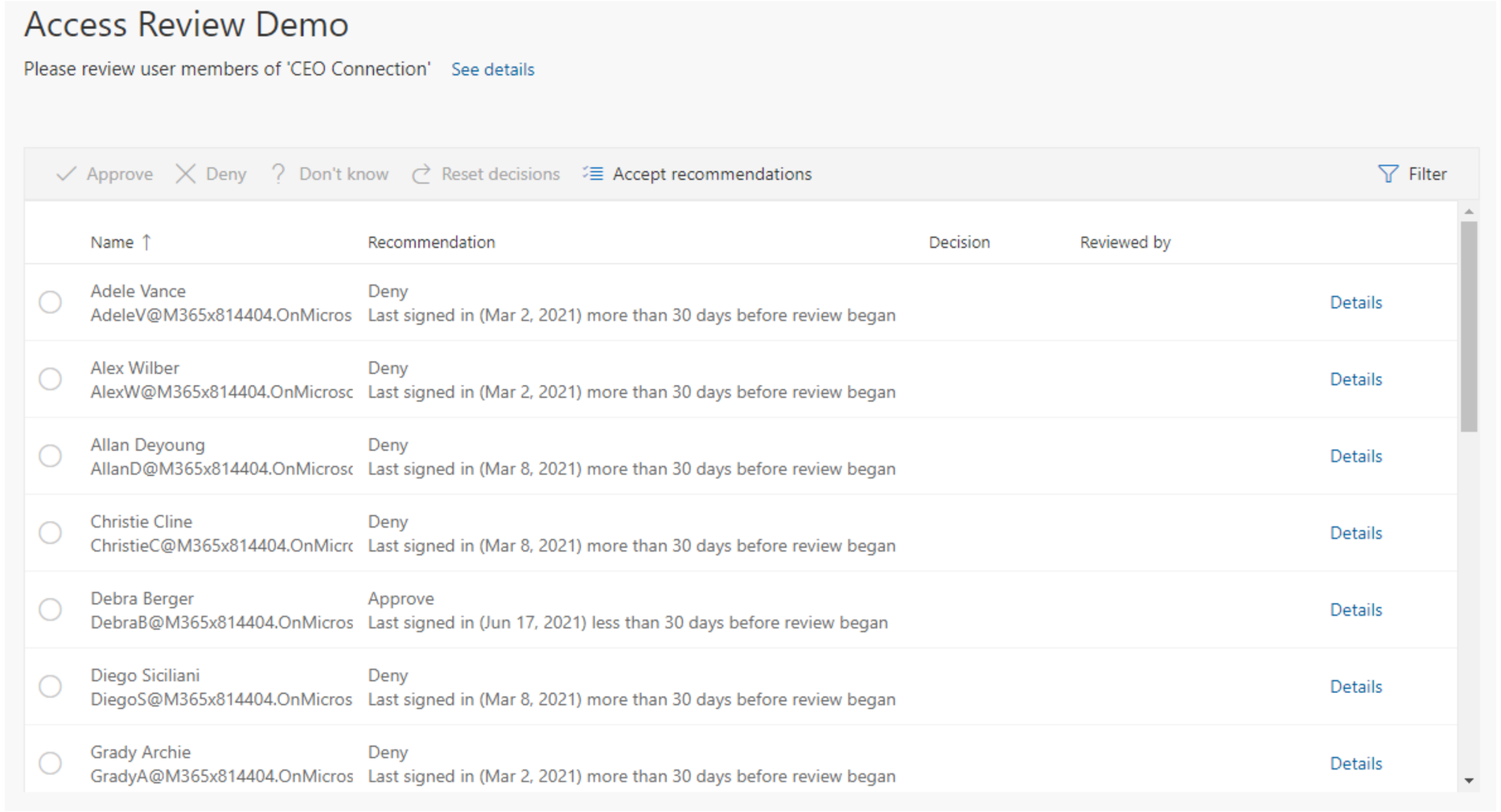
Single Stage or Multi-stage

Reviewers (Group Owners, or Selected People, etc)

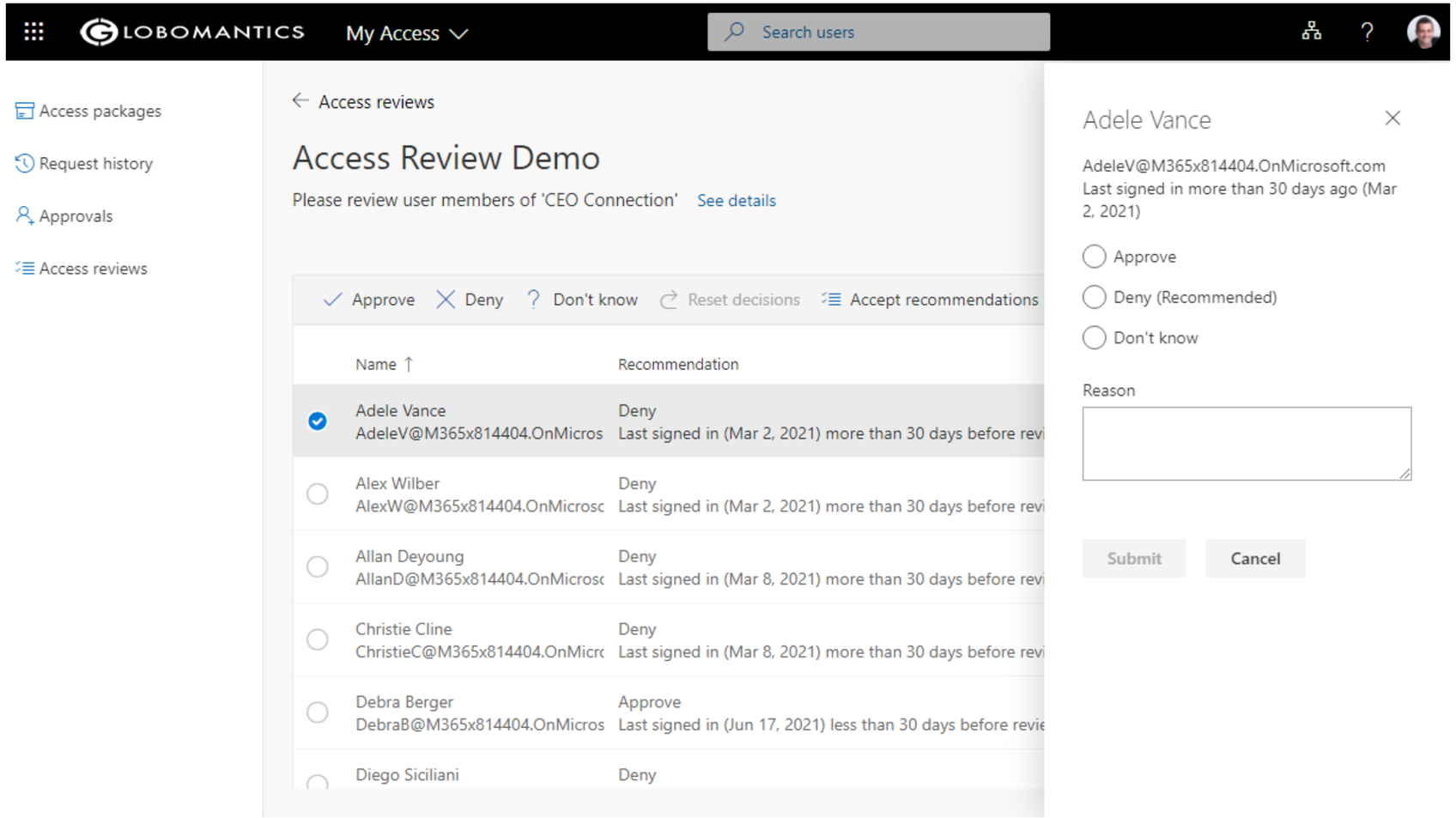
Review Recurrence

Action to apply

Access Review: Reviewer Point of View



Access Info and Reason

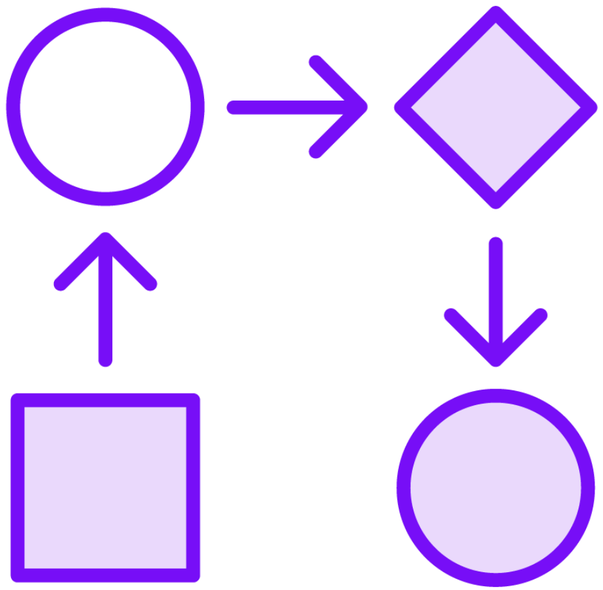


Demo

Access reviews

Entra ID Entitlement Management

Entitlement Management



Entitlement Management allows organizations to manage identity and access lifecycle at scale

- Implement access automation
- Offload access management to business stakeholders

The Problems Its Built to Solve

When users start working on a project or a new team – they don’t know all the accesses they need

Each resource might have its different owners, taking different times to give the user their permissions

User Productivity

How Entitlement Management Helps

Designated users (admin and non-admin) can create access packages

Access packages contain a collection of permissions across M365 and external apps

- Groups/Teams
- SharePoint sites
- Entra ID connected external apps
  - Salesforce/Box/Custom LOB/etc.

You Can Also Configure

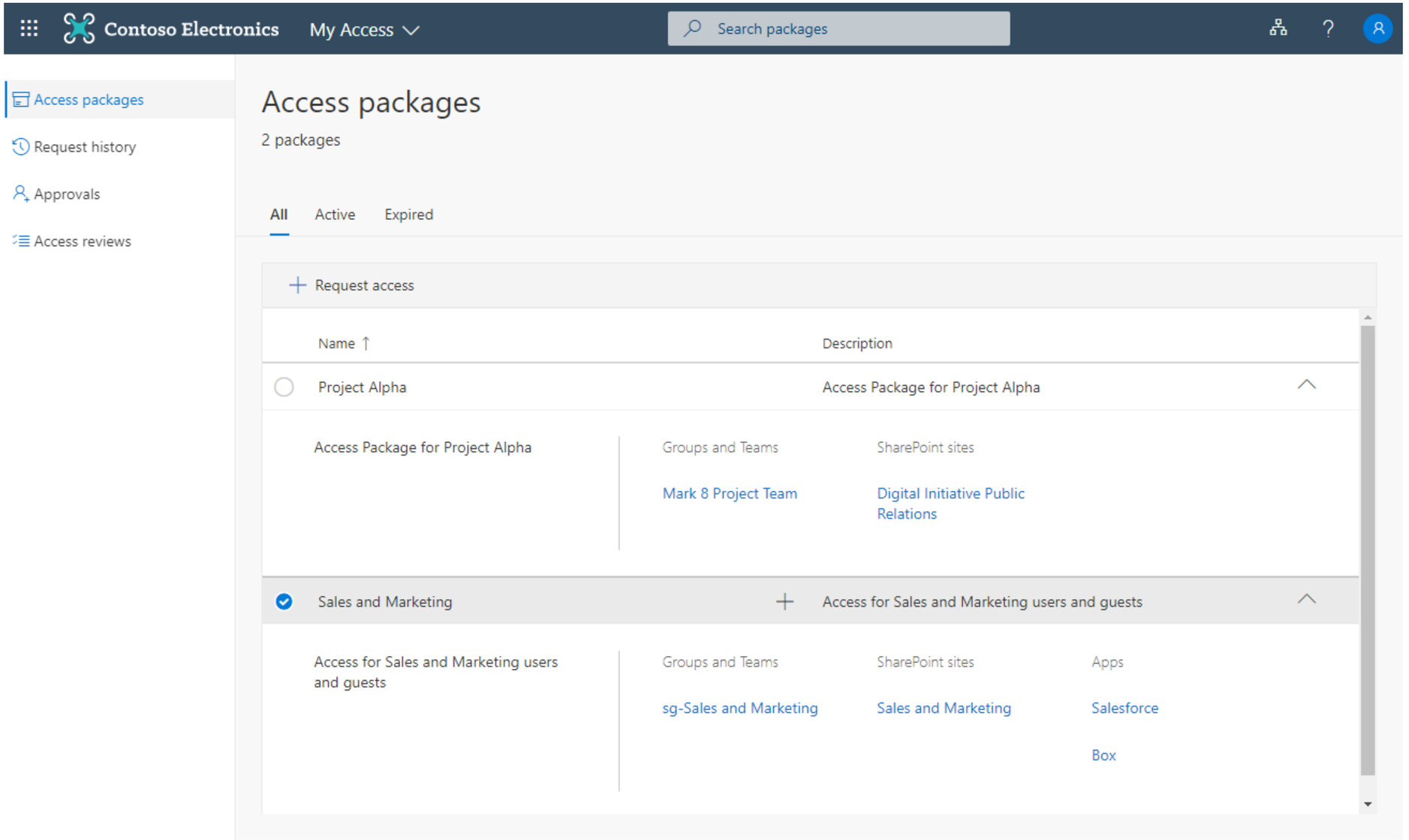
Who can request access?

Does it need an approval?

Does access automatically expire?

Are access reviews needed?

From an End User Perspective



Catalogs

Access packages are grouped in catalogs

- Tenant > Catalogs > Access Packages

Administrators can delegate access to catalogs

- Catalog Owners
- Catalog Reader
- Access Package Manager
- Access Package Assignment Manager

Demo

Entra ID Entitlement Management

Microsoft Entra Privileged Identity Management

Privileged Identity Management (PIM)

An administrator role is more valuable to a hacker than a user role

PIM allows you to provide just-in-time (JIT) privileged access to Entra ID roles and Azure resources

How Does It Work?

Administrators decide which users are eligible for certain roles

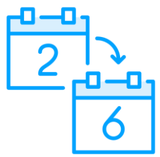
- Roles are not automatically assigned

When an admin needs admin permissions

- They request the role
- You can have an approval process
- You can send e-mails to a list notifying everyone
  - Increase visibility

Privileged Identity Management Benefits

Provide just-in-time privileged access to Entra ID and Azure resources



Assign time-bound access to resources using start and end dates

Require approval to activate privileged roles

Enforce multi-factor authentication to activate any role

Demo

Microsoft Entra Privileged Identity Management

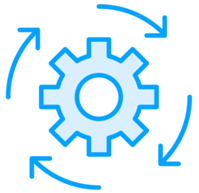
Microsoft Entra ID Protection

Microsoft Entra ID Protection

Microsoft Entra ID Protection helps organizations detect, investigate, and remediate identity-based risks. These identity-based risks can be further fed into tools like Conditional Access to make access decisions or fed back to a security information and event management (SIEM) tool for further investigation and correlation.

https://learn.microsoft.com/en-us/entra/id-protection/overview-identity-protection

Microsoft Entra ID Protection Features



Automate the detection and remediation of identity-based risks

Investigate risks using data in the portal

Export risk detection data to third-party utilities for further analysis

Microsoft Entra ID Protection: Analysis

Microsoft Entra ID Protection analyses trillion of signals per day

Uses signals to calculate sign-in risk and user risk

- Sign-in risk is the probability that the sign-in wasn't performed by the user
- User risk is a probability that the user identity has been compromised

Categorizes risks in three levels

- Low
- Medium
- High

Sign-in Risk Detections (Six Examples of Many)

- Atypical travel
- Suspicious browser
- Password spray
- New country
- Activity from anonymous IP address
- Mass access to sensitive files

https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-risks#sign-in-risk-detections

User Risk Signals

Possible attempt to access Primary Refresh Token (PRT)

Anomalous user activity

User reported suspicious activity

Additional risk detected

Leaked credentials

Microsoft Entra threat intelligence

https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-risks#user-risk-detections

Entra ID Protection: Actions

Provides three key reports for admins

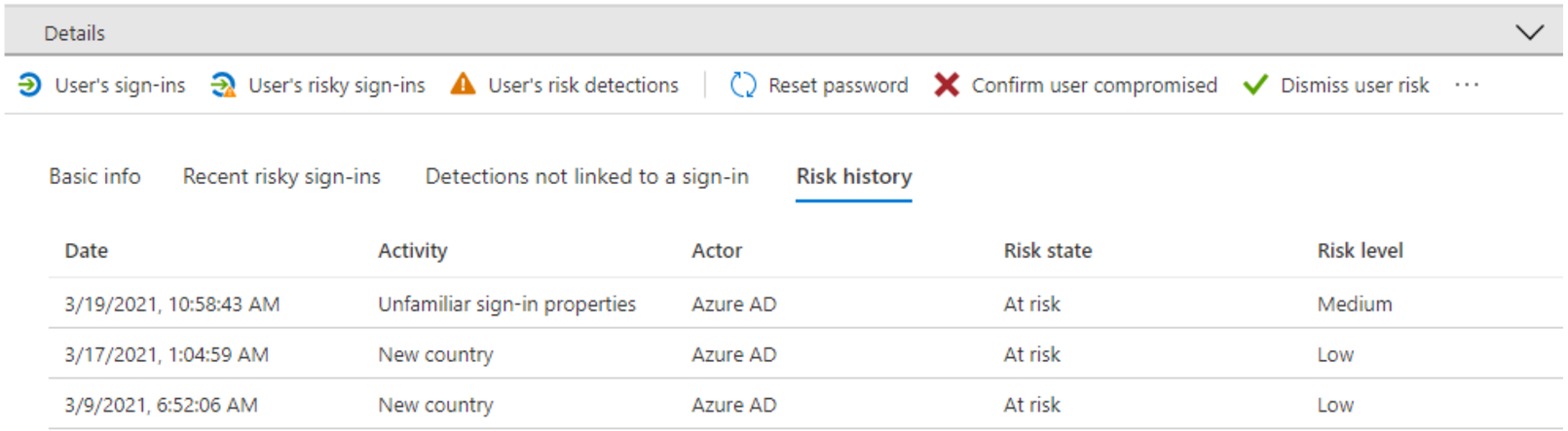
- Risky users
- Risky sign-ins
- Risk detections

Risk levels are used by Conditional Access to trigger certain actions

Risk signals can trigger remediation efforts

- Perform MFA
- Reset password
- Block account

Risky User Sample Report



Microsoft Entra Permissions Management

Microsoft Entra Permissions Management

Microsoft Entra Permissions Management is a cloud infrastructure entitlement management (CIEM) solution that provides comprehensive visibility into permissions assigned to all identities. For example, over-privileged workload and user identities, actions, and resources across multicloud infrastructures in Microsoft Azure, Amazon Web Services (AWS), and Google Cloud Platform (GCP).

https://learn.microsoft.com/en-us/entra/permissions-management/overview

Permissions Management Pillars

Discover

Asses permission risks by evaluating the gap between permissions granted and permissions used

Remediate

Right-size permissions based on usage, grant new permissions on-demand, and automate just-in-time access for cloud resources

Monitor

Detect anomalous activities with machine learning-powered alerts and generate detailed forensic reports

Permission Management Sample Actions

Cross-cloud permissions discovery

Permission Creep Index (PCI)

Automated deletion of permissions unused for the past 90 days

Permissions on-demand

ML-powered anomaly detections

Context-rich forensic reports

Module Conclusion

- Microsoft Entra ID Governance
- Dynamic groups
- Entra ID access reviews
- Entra ID Entitlement Management
- Entra ID Privileged Identity Management
- Microsoft Entra ID Protection
- Microsoft Entra Permissions Management

Up Next:

Course Conclusion