Microsoft

SC-900

Learning path 2:

Describe the capabilities of Microsoft Entra ID

SC-900 Course Agenda

Learning Path 1 – Describe the concepts of Security, Compliance, and Identity

Learning Path 2 – Describe the capabilities of Microsoft Entra ID

Learning Path 3 – Describe the capabilities of Microsoft Security Solutions

Learning Path 4 – Describe the capabilities of Microsoft Compliance Solutions

Microsoft

Learning path agenda

- Describe the function and identity types of Microsoft Entra ID.

- Describe the authentication capabilities of Microsoft Entra ID.

- Describe the access management capabilities of Microsoft Entra ID.

- Describe the identity protection and governance capabilities of Microsoft Entra.

Module 1: Describe the function and identity types of Microsoft Entra ID
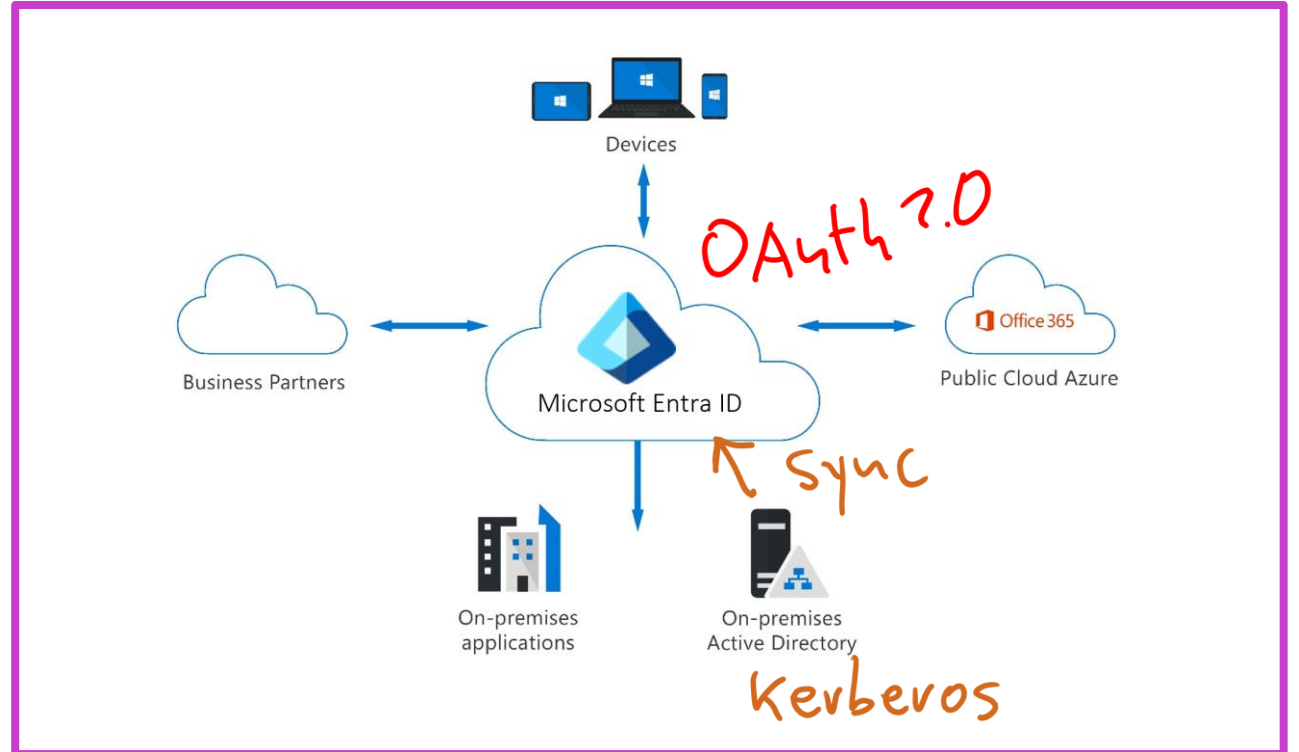
Module 1 introduction

After completing this module, you'll be able to:

1   Describe the core functionality of Microsoft Entra ID.

2   Describe the types of identities supported by Microsoft Entra ID.

3   Describe the concept of hybrid identity as supported by Microsoft Entra ID.

Microsoft Entra ID

Microsoft's cloud-based identity and access management service.

- Organizations can enable their employees, guests, and others to sign in and access the resources they need.

- Provide a single identity system for their cloud and on-premises applications.

- Protect user identities and credentials to meet an organization's access governance requirements.

- Subscribers to Azure services, Microsoft 365, or Dynamics 365 automatically have access to Microsoft Entra ID.

- Identity secure score.

Devices

OAuth 2.0

Business Partners

Microsoft Entra ID

Office 365
Public Cloud Azure

Sync

On-premises applications

On-premises Active Directory

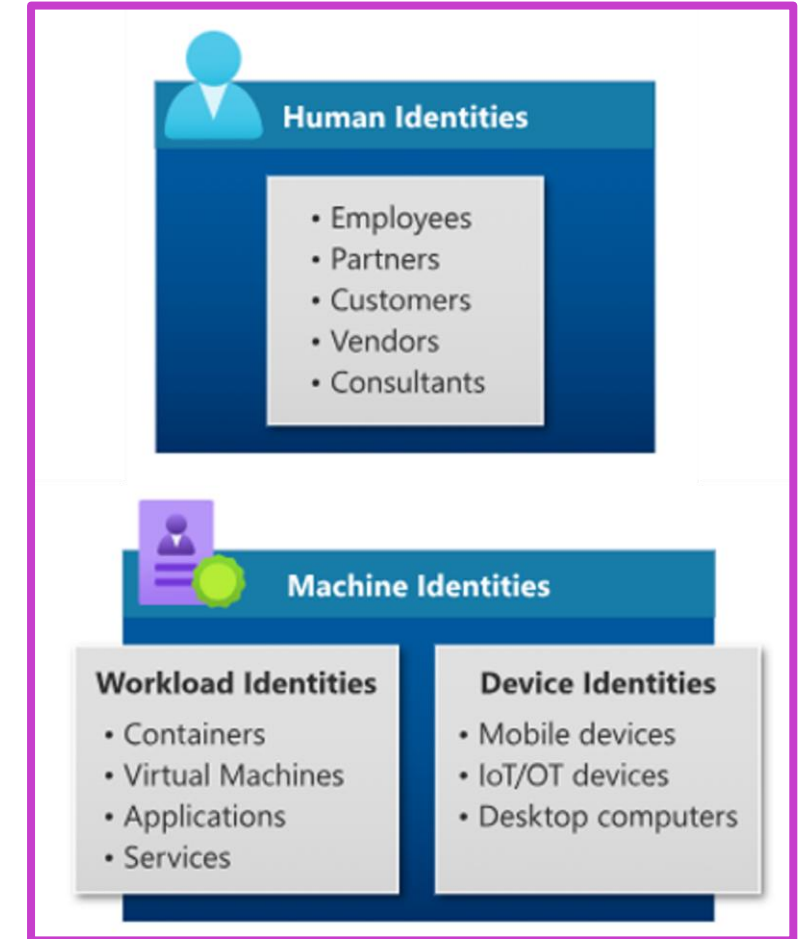Kerberos

Identity types

Human (user) identities

- Internal users – Employees.
- External users – Guests, partners, customers, and so on.

Workload identities (an identity assigned to an application or service)

- Service principal – Uses Microsoft Entra ID for identity and access functions; app developers manage credentials.
- Managed identities – A service principal managed in Microsoft Entra ID that eliminates the need for app developers to manage credentials.

Devices

- Microsoft Entra ID registered – Support for bring your own device.
- Microsoft Entra ID joined – Device joined via an organizational account.
- Hybrid joined – Devices are joined to your on-premises Active Directory and Microsoft Entra ID, requiring organizational account to sign in.

Human Identities

- Employees
- Partners
- Customers
- Vendors
- Consultants

Machine Identities

Workload Identities

- Containers
- Virtual Machines
- Applications
- Services

Device Identities

- Mobile devices
- IoT/OT devices
- Desktop computers

Hybrid identity

What is a hybrid identity?

- A common user identity for authentication and authorization to on-premises and cloud resources.

- Hybrid identity is accomplished through:
  - Inter-directory provisioning – A user in Active Directory is provisioned into Microsoft Entra ID.
  - Synchronization – Identity information for your on-premises users and groups matches the cloud.

- Microsoft Entra Cloud Sync – A method for provisioning and synchronization.
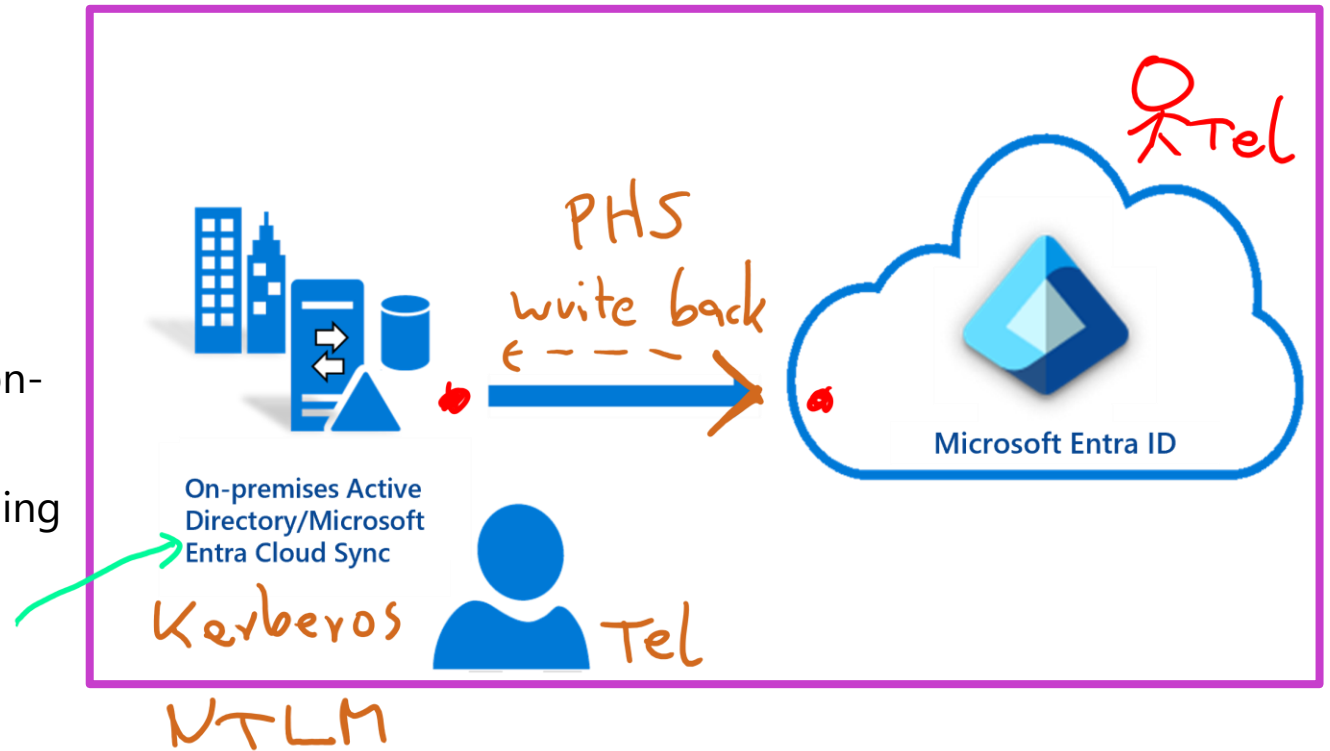
Module 2: Explore the authentication capabilities of Microsoft Entra

Module 2 introduction

After completing this module, you'll be able to:

1 Describe the authentication methods of Microsoft Entra ID.

2 Describe multifactor authentication in Microsoft Entra ID.

3 Describe the password protection and management capabilities of Microsoft Entra ID.

Authentication methods of Microsoft Entra

Passwords (primary auth)

Phone-based authentication
- SMS (primary and secondary auth)
- Voice (secondary auth)

OATH (secondary auth)
- Standard for how one-time password codes are generated
- SW tokens
- HW tokens

Passwordless (primary and secondary auth)
- Windows Hello
- Microsoft Authenticator
- FIDO2
- Certificates (primary auth)

| **Bad:** Password	**Good:** Password and...	**Better:** Password and...	**Best:** Passwordless
123456	SMS	Authenticator (Push Notifications)	Authenticator (Phone Sign-in)
qwerty			
password	Voice	Software Tokens OTP	Window Hello
iloveyou			FIDO2 security key
Password1		Hardware Tokens OTP (Preview)	Certificates

Multifactor authentication (MFA)

Dramatically improves the security of an identity, while still being simple for users.

MFA requires more than one form of verification

- Something you know.
- Something you have.
- Something you are.

Security defaults

- Requires all users to complete MFA as needed.
- Forces administrators to use MFA.
- Enforces MFA for all users.
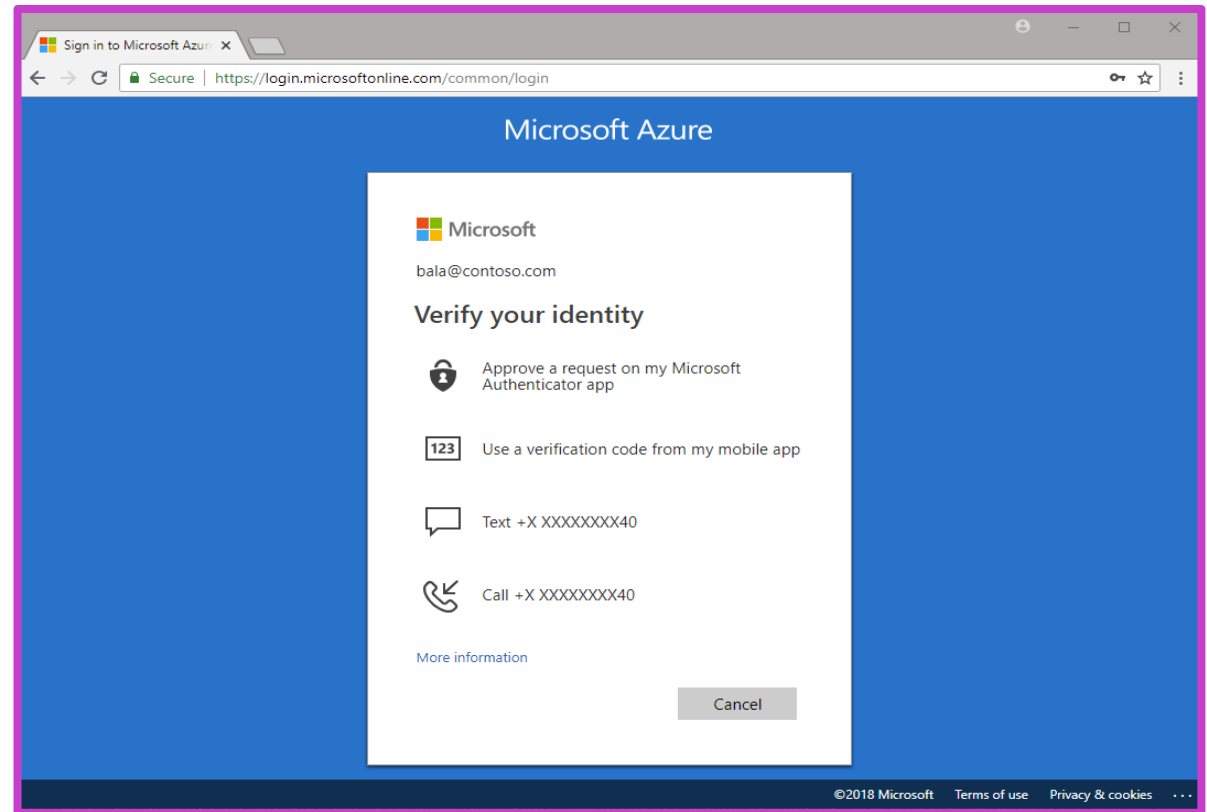
Password protection and management capabilities

Reduce the risk of users setting weak passwords:

- Global banned password list.

- Custom banned password lists.

- Protecting against password spray.

- Integrates with an on-premises Active Directory environment.

Custom smart lockout

Lockout threshold ⓘ   10

Lockout duration in seconds ⓘ   60

Custom banned passwords

Enforce custom list ⓘ   Yes   No

Custom banned password list ⓘ   contoso
                                  fabrikam
                                  tailwind
                                  michigan
                                  wolverine
                                  harbaugh
                                  howard

Password protection for Windows Server Active Directory

Enable password protection on Windows   Yes   No
Server Active Directory ⓘ

Module 3: Explore the access management capabilities of Microsoft Entra
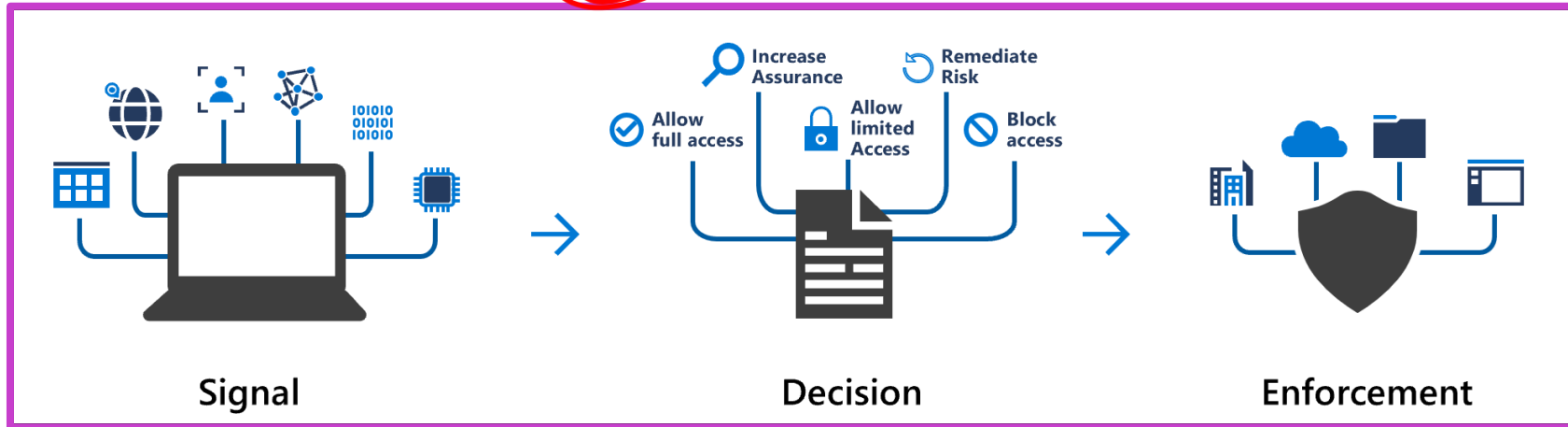
Module 3 introduction

After completing this module, you'll be able to:

1   Describe Conditional Access and its benefits.

2   Describe Microsoft Entra ID roles and role-based access control (RBAC).

Conditional Access

At their simplest, Conditional Access (CA) policies are if-then statements.

Signal → Decision → Enforcement

Assignments determine which signals to use

- Users, groups, workload identities, directory roles.
- Cloud apps or actions.
- Sign-in and user risk detection.
- Device or device platform.
- IP location.
- More...

**Access controls determine how a policy is enforced**

- Block access.
- Grant access – Require one or more conditions to be met before granting access.
- Session control – Enable a limited experience.

Microsoft Entra roles and role-based access control (RBAC)

Microsoft Entra ID roles control permissions to manage Microsoft Entra resources.

- Built-in roles.

- Custom roles.

- Categories of Microsoft Entra roles:
  - Microsoft Entra specific
  - Service-specific
  - Cross service

- Only grant the access users need.
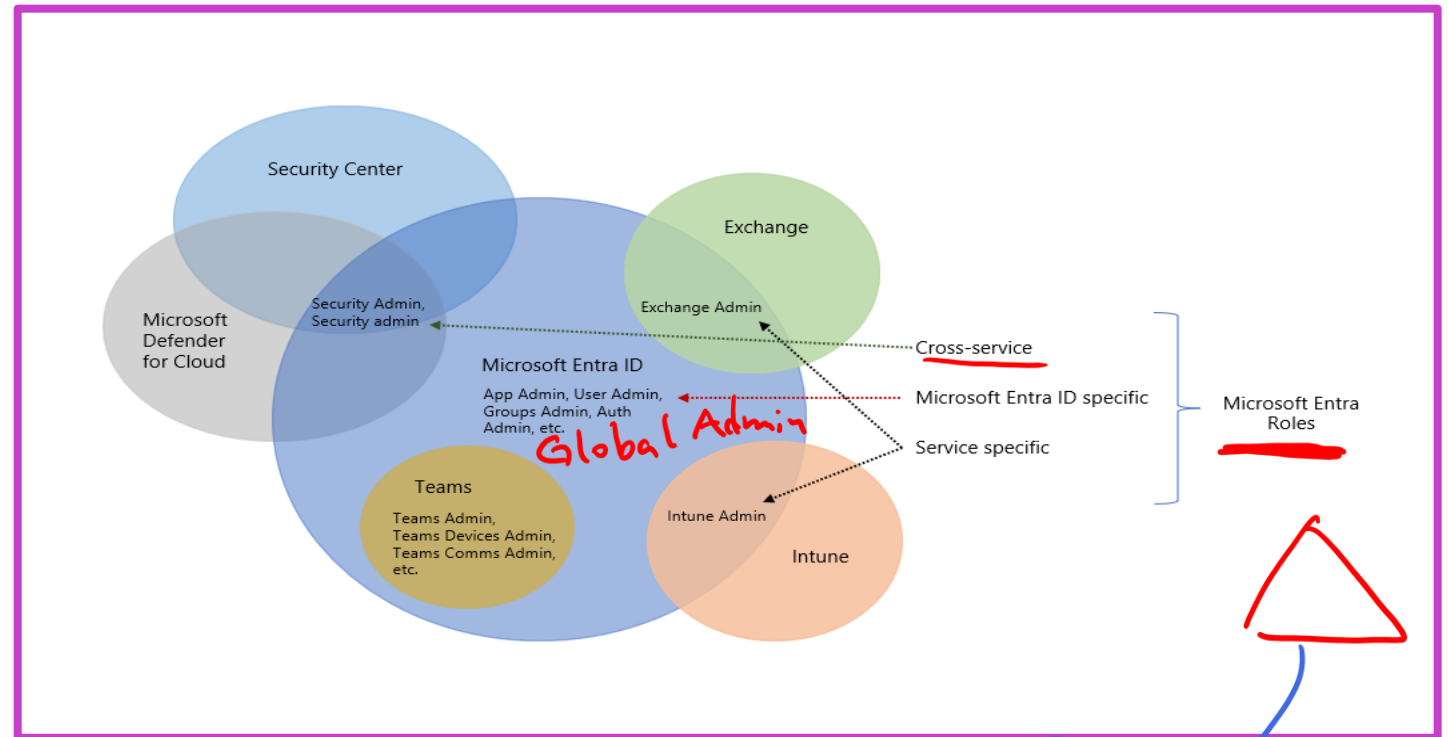
Module 4: Describe the identity protection and governance capabilities of Microsoft Entra

Module 4 introduction

After completing this module, you'll be able to:

1 Describe the identity governance capabilities of Microsoft Entra.

2 Describe Privileged Identity Management (PIM).

3 Describe the capabilities of Microsoft Entra Identity Protection.

4 Describe permissions management.

Identity governance in Microsoft Entra

The right people have the right access to the right resources.

Access Packages

The tasks of Microsoft Entra identity governance

- Govern the identity life cycle.
- Govern access life cycle.
- Secure privileged access for administration.

Identity life cycle

- Join: A new digital identity is created.
- Move: Update access authorizations.
- Leave: Access may need to be removed.
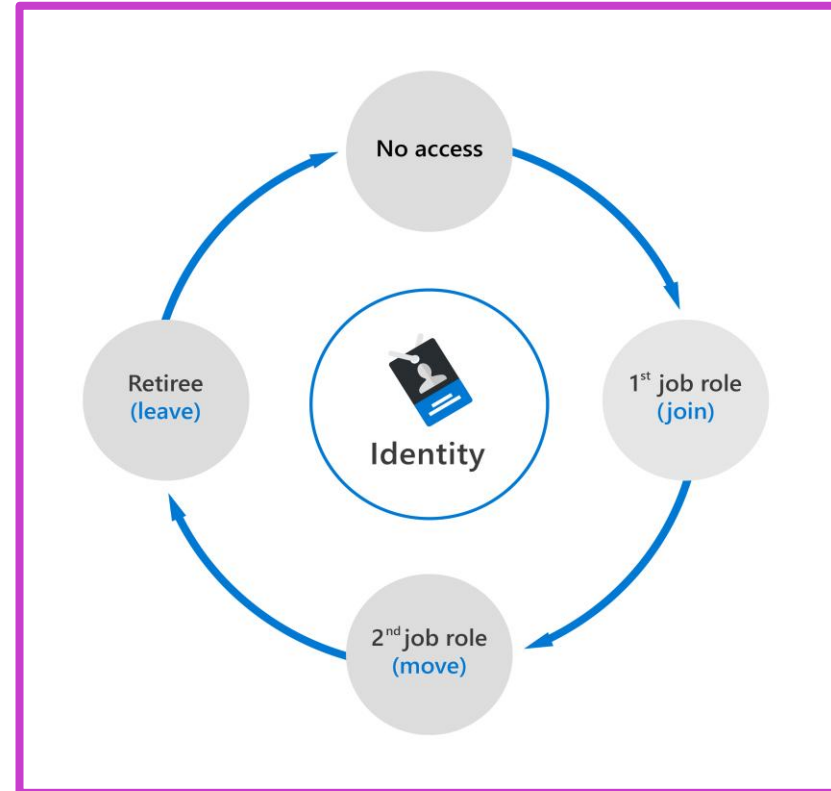
Access reviews

Access reviews

- Enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignment.

- Ensure that only the right people have access to resources.

- Used to review and manage access for both users and guests.

Multistage access reviews

- Support up to three review stages.

- Support workflows to meet recertification and audit requirements calling for multiple reviewers.

- Reduce the number of decisions each reviewer is accountable for.

Contoso

Please review users' access to the Finance Web app in FrickelsoftNET

Sarah Hoelzel, your organization requested that you approve or deny continued access for one or more users to the **Finance Web** app in the **FinanceWeb** access review. The review period will end on **September 5, 2020**.

Hi FinanceWeb team - please review the list of users who can access your FinanceWeb application. Help us remove any unwanted access from users that no longer work with the app. More information: https://finweb.contoso.com/access/reviews

Start review >

Learn how to perform an access review and more about Azure Active Directory access reviews.

Privacy Statement

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

Facilitated by

Microsoft

Privileged Identity Management (PIM)

PIM enables you to manage, control, and monitor access to important resources in your organization.

1   Just in time, providing privileged access only when needed, and not before.

2   Time-bound, by assigning start and end dates that indicate when a user can access resources.

3   Approval-based, requiring specific approval to activate privileges.

4   Visible, sending notifications when privileged roles are activated.

5   Auditable, allowing a full access history to be downloaded.

Microsoft Entra Identity Protection

Detect
- Categorize risk into three tiers: Low, medium, and high.
- Calculate the sign-in risk and user risk.

Investigate
- Risk detections report.
- Risky sign-ins report.
- Risky users report.
- Risky workload identities report.

Remediate
- Automated remediation.
- Manual remediation.

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

Risky User Details ✕

⮕ User's sign-ins   🔁 User's risky sign-ins   ⚠ User's risk detections   ⋯

Basic info   Recent risky sign-ins   ⋯

User	Vjekoslav Vlasic
Roles	Limited admin
Username	vvlasic@woodgrove.ms
User ID	abcdefgh-xxxx-zzzz-1111-xxxxxxxxxxxx
Risk state	At risk
Risk level	Low
Details	-
Risk last updated	12/16/2021, 10:25:59 AM
Office location	
Department	
Mobile phone	

Permissions management

Comprehensive visibility and control over permissions for any identity and any resource in Microsoft Azure, Amazon Web Services (AWS) and Google Cloud Platform (GCP).

[Handwritten annotations: "ARC", "AWS", "On Prem", "ARC VM", "VM", "Agent"]

Discover → Remediate → Monitor

Discover
Assess permission risks by evaluating the gap between permissions granted and permissions used.
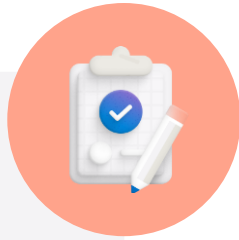
Remediate
Right-size permissions based on usage, grant permissions on-demand.

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

Learning path summary

Describe the capabilities of Microsoft Entra.

In this learning path, you have:

- Learned about Microsoft Entra ID and the services and identity types it supports.

- Explored the authentication capabilities of Microsoft Entra and MFA.

- Explored the access management capabilities of Microsoft Entra, with Conditional Access and Microsoft Entra RBAC.

- Described identity protection and governance capabilities of Microsoft Entra, including PIM and access reviews.

- Learned about the capabilities of Microsoft Entra Identity Protection.

Knowledge check

An organization has completed a full migration to the cloud and has purchased devices for all its employees. All employees sign in to the device through an organizational account configured in Microsoft Entra ID. Select the option that best describes how these devices are set up in Microsoft Entra ID.

A. These devices are set up as Microsoft Entra ID registered.
B. These devices are set up as Microsoft Entra ID joined.
C. These devices are set up as Hybrid Microsoft Entra ID joined.

After hearing of a breach at a competitor, the security team wants to improve identity security within their organization. What should they implement to provide the greatest protection to user identities?

A. Multifactor authentication.
B. Require security questions for all sign-ins.
C. Require strong passwords for all identities.

Knowledge check continued

An organization plans to implement Conditional Access. What do admins need to do?

A. Create policies that enforce organizational rules.
B. Check that all users have multi-factor authentication enabled.
C. Amend your apps to allow Conditional Access.

Your IT organization is looking for a solution that provides comprehensive visibility and control over permissions for any identity and any resource in their multi-vendor cloud environment. Which Microsoft solution is best suited to address these needs?

A. Identity Protection.
B. Privileged Identity Management.
C. Permissions Management.