Microsoft Security

SC-900

Learning Path: Ø2

Describe the capabilities of Microsoft Azure Active Directory, part of Microsoft Entra

© Copyright Microsoft Corporation. All rights reserved.

Learning Path Agenda

- Explore the services and identity types of Azure AD.
- Explore the authentication capabilities of Azure AD.
- Explore the access management capabilities of Azure AD.
- Describe identity protection governance capabilities of Azure AD.

PIM

© Copyright Microsoft Corporation. All rights reserved.

Module 1: Explore the services and identity types in Azure AD

© Copyright Microsoft Corporation. All rights reserved.

Module 1 Introduction

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

- Describe Azure AD.
- Describe the identity types that Azure AD supports.

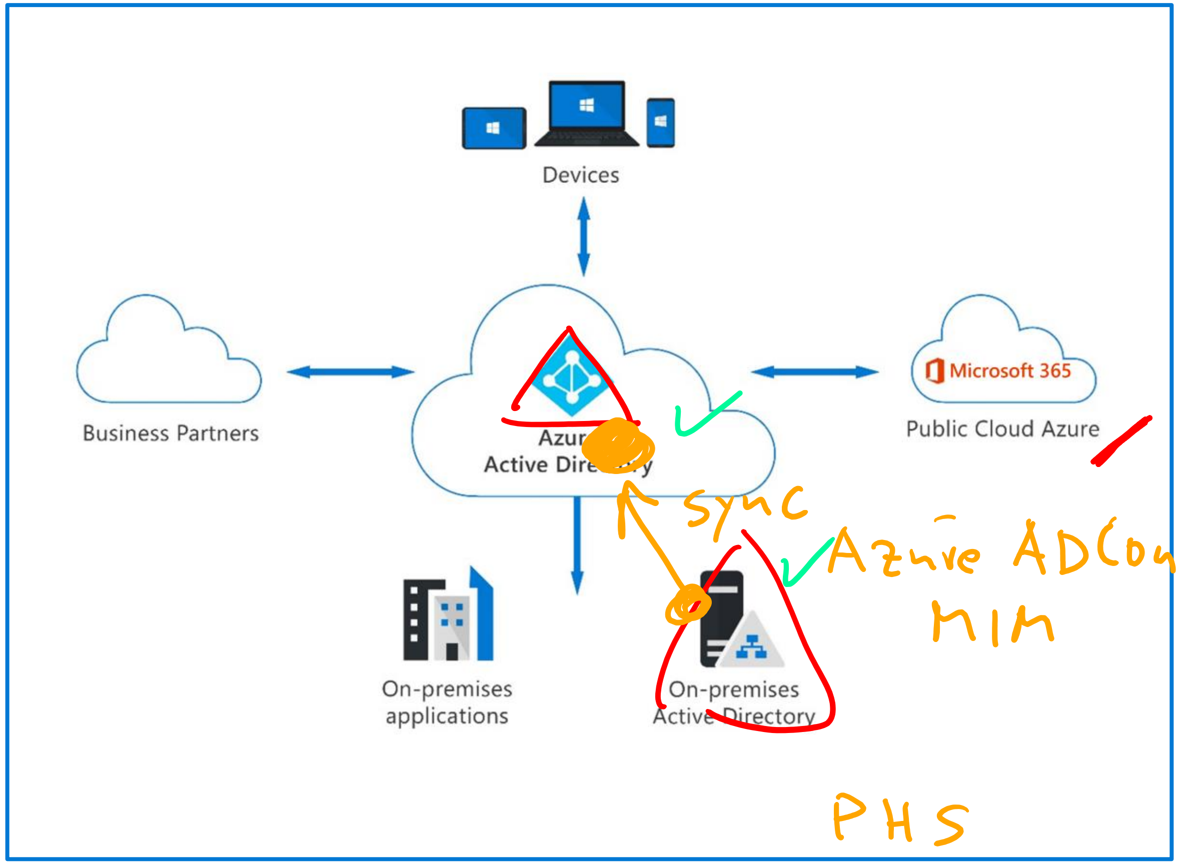
© Copyright Microsoft Corporation. All rights reserved.

Microsoft Azure Active Directory, part of Microsoft Entra

Microsoft Entra is our product family that encompasses all of Microsoft's identity and access capabilities, including Microsoft Azure Active Directory (Azure AD).

Azure AD is Microsoft's cloud-based identity and access management service. Capabilities of Azure AD include:

- 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 and to meet an organization's access governance requirements.
- Each Microsoft 365, Office 365, Azure, and Dynamics 365 Online subscription automatically use an Azure AD tenant.



sync

Azure AD Connect

MIM

PHS

PTA

ws-Fed (SAML)

© Copyright Microsoft Corporation. All rights reserved.

Instance Meta Data Service

Azure AD identity types

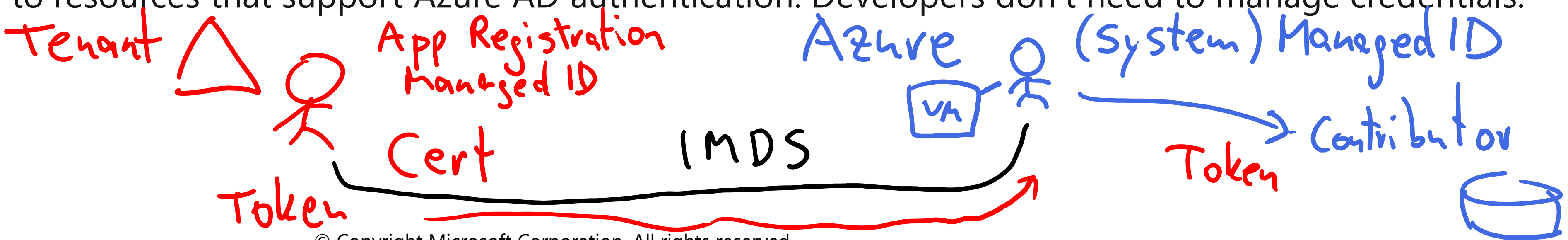
Azure AD manages different types of identities: users, service principals, managed identities, and devices.

User – Generally speaking, a user is a representation of an individual's identity that's managed by Azure AD. Employees and guests are represented as users in Azure AD.

Device - A piece of hardware, such as mobile devices, laptops, servers, or printer. Device identities can be set up in different ways in Azure AD, to determine properties such as who owns the device.

Service principal - You can think of it as an identity for an application. A service principal is created in every tenant the application is used & defines who can access the app, what resources the app can access, and more.

Managed identity – A type of service principal, a managed identity provides an identity for applications to use when connecting to resources that support Azure AD authentication. Developers don't need to manage credentials.



© Copyright Microsoft Corporation. All rights reserved.

Microsoft Security

Demo

Azure AD user settings

© Copyright Microsoft Corporation. All rights reserved.

External identities in Azure AD

Two different Azure AD External Identities:

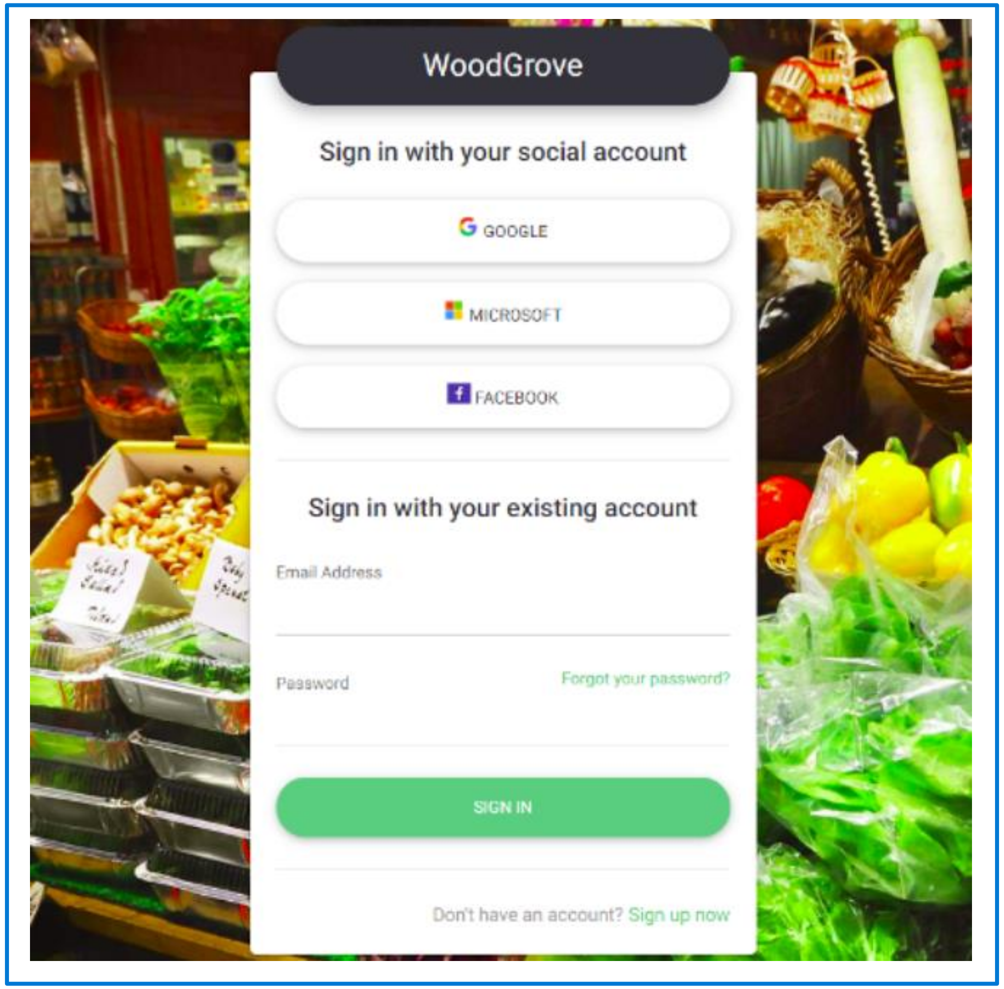
B2B collaboration

B2B collaboration allows you to share your apps and resources with external users.

B2C access management

B2C is an identity management solution for consumer and customer facing apps.

△ App



WoodGrove

Sign in with your social account

GOOGLE

MICROSOFT

FACEBOOK

Sign in with your existing account

Email Address

Password Forgot your password?

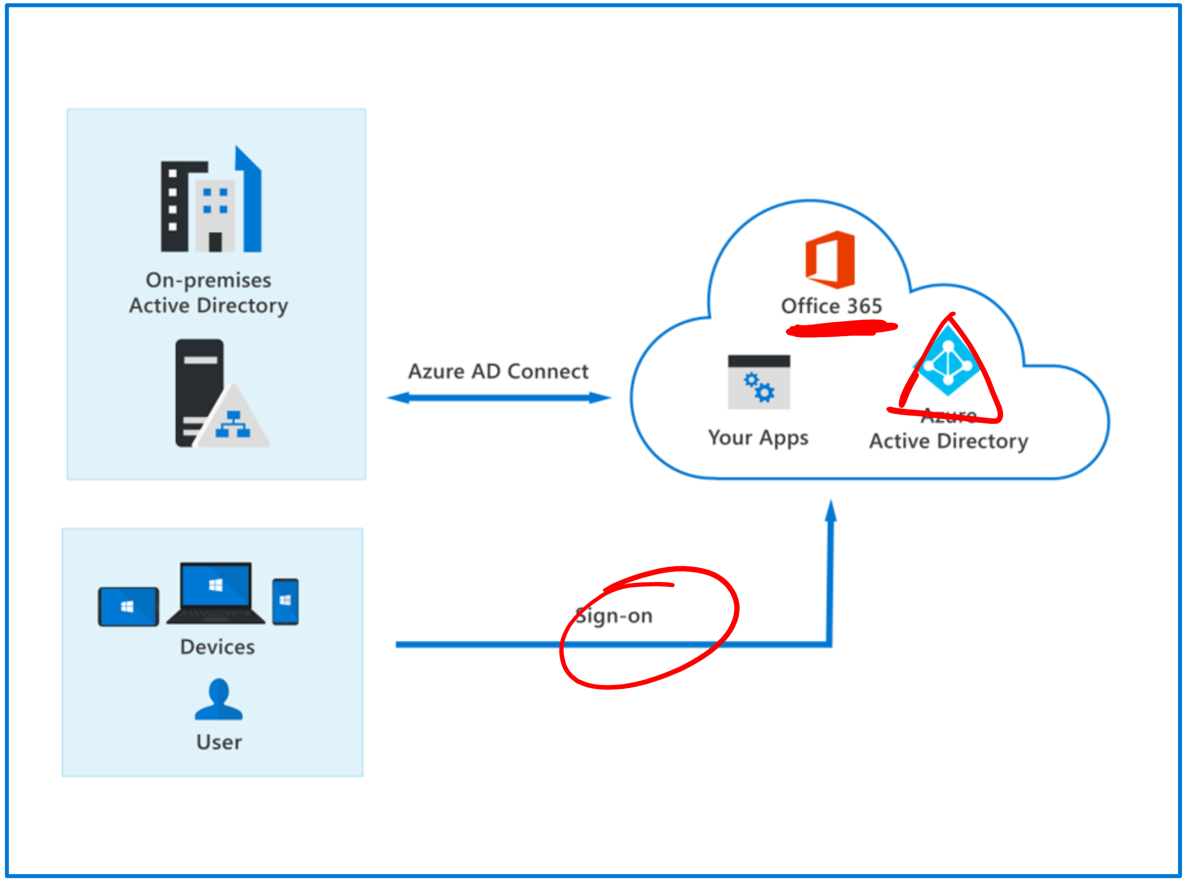
SIGN IN

Don't have an account? Sign up now

© Copyright Microsoft Corporation. All rights reserved.

The concept of hybrid identities

- A ***hybrid identity*** is a common user identity for authentication and authorization to all resources, regardless of location (on-prem & cloud).
- With ***Azure AD Connect***, updates to your on-premises AD DS are synchronized to your Azure AD.
- Hybrid identity Authentication methods:
  - Password hash sync PHS
  - Passthrough authentication PTA
  - Federated authentication Fed



© Copyright Microsoft Corporation. All rights reserved.

Module 2: Explore the authentication capabilities of Azure AD

© Copyright Microsoft Corporation. All rights reserved.

Module 2 Introduction

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

- Describe the authentication methods of Azure AD.
- Describe multi-factor authentication in Azure AD.
- Describe the password protection and management capabilities of Azure AD.

© Copyright Microsoft Corporation. All rights reserved.

Authentication methods of Azure AD

Passwords (primary auth)

Phone-based authentication

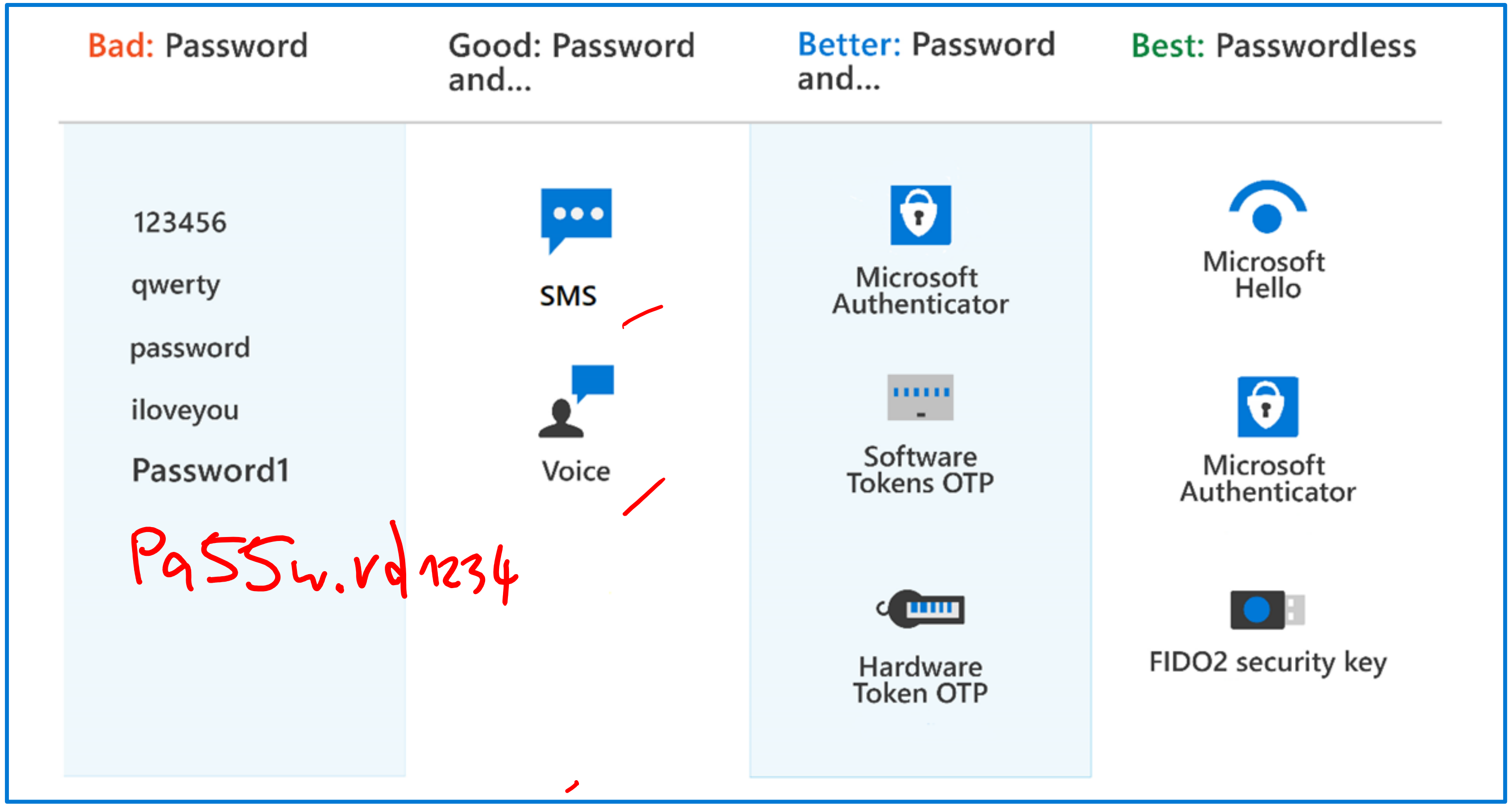
- SMS (primary & secondary auth)
- Voice (secondary auth)

OATH, standard for how codes are generated in one-time passwords, (secondary auth)

- SW tokens
- HW tokens

Passwordless (primary & secondary auth)

- Biometrics (Windows Hello)
- Microsoft Authenticator
- FIDO2



Bad: Password	Good: Password and...	Better: Password and...	Best: Passwordless
123456 qwerty password iloveyou Password1 Pa55w.rd1234	SMS Voice	Microsoft Authenticator Software Tokens OTP Hardware Token OTP	Microsoft Hello Microsoft Authenticator FIDO2 security key

© Copyright Microsoft Corporation. All rights reserved.

Multi-factor authentication (MFA) in Azure AD

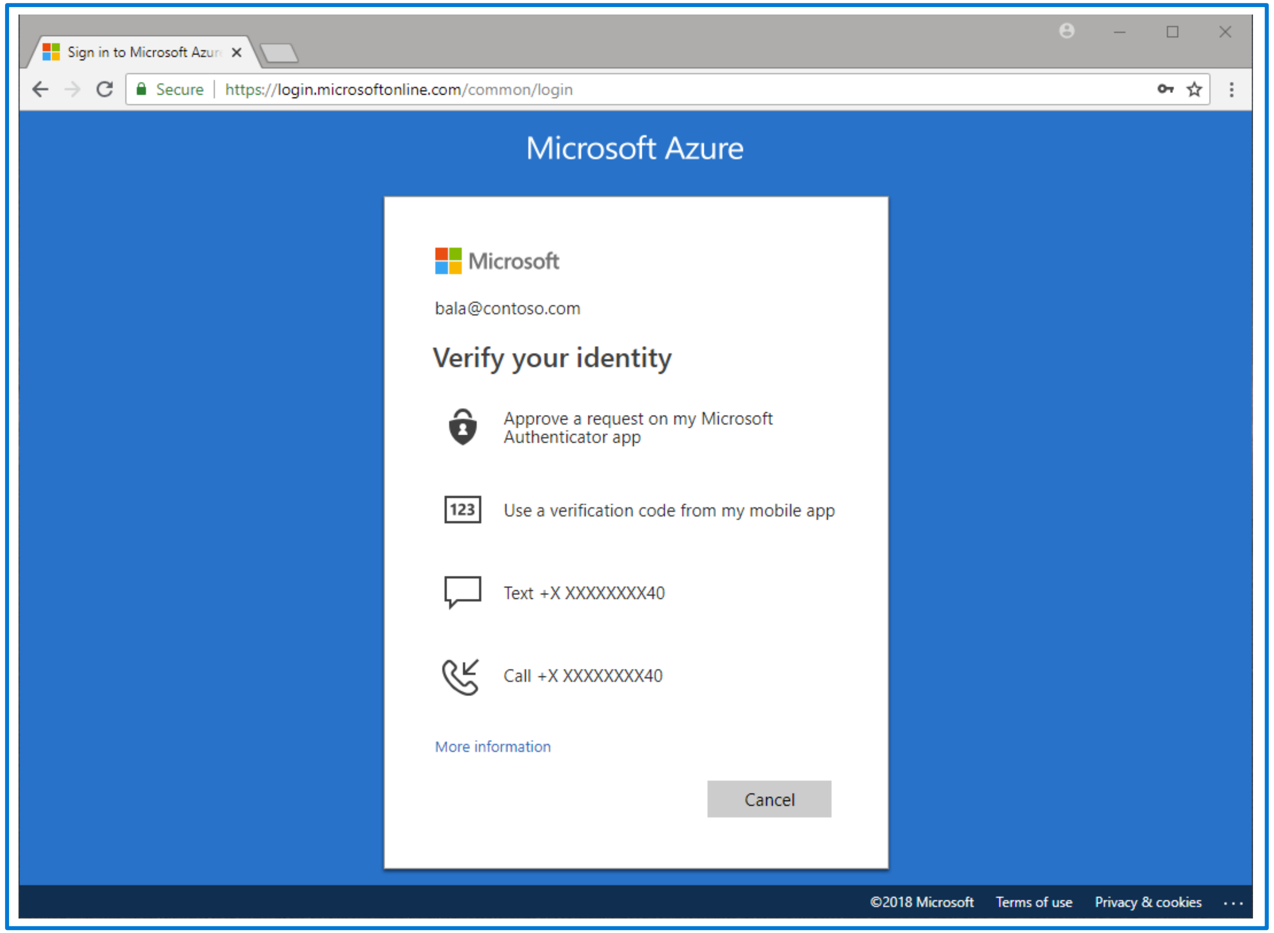
Multifactor authentication (MFA) & Security Defaults

MFA requires more than one form of verification:

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

Security defaults:

- A set of basic identity security mechanisms recommended by Microsoft.
- A great option for organizations that want to increase their security posture but don't know where to start, or for organizations using the free tier of Azure AD licensing.



Sign in to Microsoft Azure
Secure
https://login.microsoftonline.com/common/login
Microsoft Azure
Microsoft

bala@contoso.com

Verify your identity

Approve a request on my Microsoft Authenticator app

Use a verification code from my mobile app

Text +X XXXXXXXX40

Call +X XXXXXXXX40

© Copyright Microsoft Corporation. All rights reserved.

Self-service password reset (SSPR) in Azure AD

Benefits of Self-service password reset:

- Administrators can change settings to accommodate new security requirements.
- It saves the organization money by reducing the number of calls and requests to help desk staff.
- It increases productivity, allowing the user to return to work faster.

Self-service password reset works in the following scenarios:

- Password change
- Password reset
- Account unlock

Authentication method of SSPR:

- Mobile app notification
- Mobile app code
- email
- Mobile phone
- Office phone
- Security questions

© Copyright Microsoft Corporation. All rights reserved.

Microsoft Security

Demo

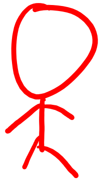
Azure AD
self-service password reset (SSPR)

© Copyright Microsoft Corporation. All rights reserved.

Password protection & management capabilities in Azure AD

- Global banned password list
- Custom banned password lists
- Protecting against password spray
- Hybrid security

© Copyright Microsoft Corporation. All rights reserved.



password

Signin Risk

User Risk

Id Protection

↓ Device compliance

↑

CA Policies

MFA

Allow

Deny

Role

Role

Module 3: Explore the access management capabilities of Azure AD

© Copyright Microsoft Corporation. All rights reserved.

Module 3 Introduction

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

- Describe Conditional Access and its benefits.
- Describe Azure AD roles and role-based access control (RBAC).

© Copyright Microsoft Corporation. All rights reserved.

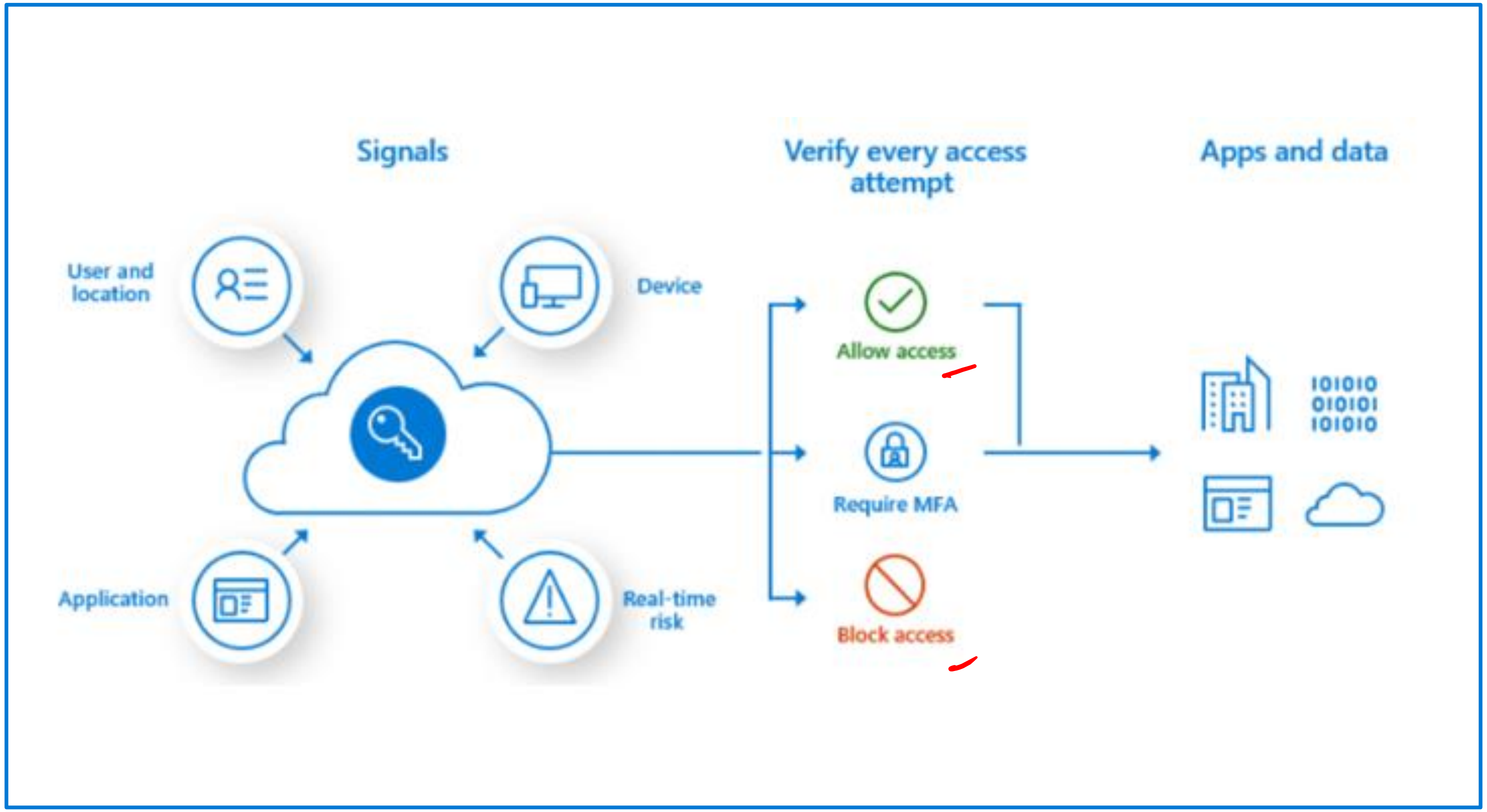
Conditional access CA

Conditional Access signals:

- User or group membership
- Named location information
- Device
- Application
- Real-time sign-in risk detection
- Cloud apps or actions
- User risk

Access controls:

- Block access
- Grant access
- Require one or more conditions to be met before granting access.
- Control user access based on session controls to enable limited experiences within specific cloud applications.



© Copyright Microsoft Corporation. All rights reserved.

Microsoft Security

Demo

Azure AD Conditional Access

© Copyright Microsoft Corporation. All rights reserved.

Azure AD roles & role-based access control (RBAC)

Azure AD roles control permissions to manage Azure AD resources.

- Built-in roles ✓
- Custom roles json
- Categories of Azure AD roles: Azure AD specific, service- specific, cross service
- Only grant the access users need

© Copyright Microsoft Corporation. All rights reserved.

Module 4: Describe the identity protection and governance capabilities of AD

© Copyright Microsoft Corporation. All rights reserved.

Module 4 Introduction

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

- Describe the identity governance capabilities of Azure AD.
- Describe the benefits of Privileged Identity Management (PIM).
- Describe the capabilities of Azure AD Identity Protection.

© Copyright Microsoft Corporation. All rights reserved.

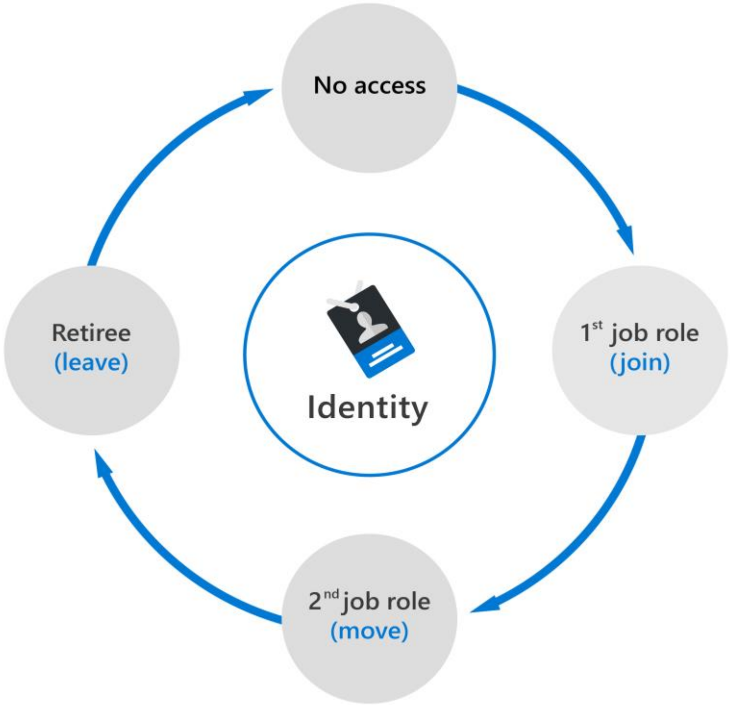
Identity governance in Azure AD

The tasks of Azure AD identity governance

- Govern the identity lifecycle.
- Govern access lifecycle.
- Secure privileged access for administration.

Identity lifecycle

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



© Copyright Microsoft Corporation. All rights reserved.

Entitlement management and access reviews

Entitlement management

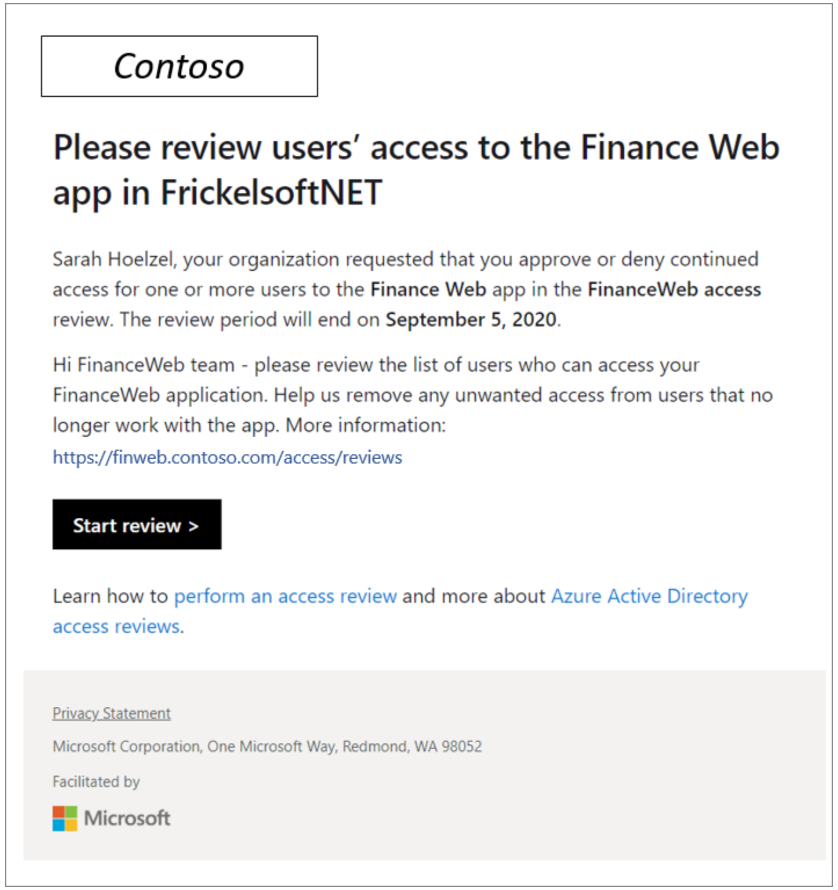
- It is an identity governance feature that enables organizations to manage identity and access lifecycle at scale.
- It automates access request workflows, access assignments, reviews, and expiration.

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.

Terms of use

- Allow information to be presented to users, before they access data or an application.
- Ensure users read relevant disclaimers for legal or compliance requirements.



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

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

© Copyright Microsoft Corporation. All rights reserved.

Privileged Identity Management (PIM)

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

- Just in time, providing privileged access only when needed, and not before.
- Time-bound, by assigning start and end dates that indicate when a user can access resources.
- Approval-based, requiring specific approval to activate privileges.
- Visible, sending notifications when privileged roles are activated.
- Auditable, allowing a full access history to be downloaded.

© Copyright Microsoft Corporation. All rights reserved.

Azure Identity Protection

Enables organizations to accomplish three key tasks:

- 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.

It can categorize and calculate risk:

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

It provides organizations with three reports:

- Risky users
- Risky sign-ins
- Risk detections

© Copyright Microsoft Corporation. All rights reserved.

Learning Path Summary

In this learning path, you have:

- Learned about Azure AD and services and identity types Azure AD supports.
- Explore the authentication capabilities of Azure AD and MFA.
- Explore the access management capabilities of Azure AD with Conditional Access and Azure AD RBAC.
- Describe identity protection and governance capabilities of Azure AD, including PIM, entitlement management, and access reviews.
- Learned about the capabilities of Azure AD Identity Protection.

© Copyright Microsoft Corporation. All rights reserved.

Microsoft Security

© Copyright Microsoft Corporation. All rights reserved.