Cloud Computing

Caltech | Center for Technology & Management Education

Post Graduate Program in Cloud Computing

Powerd by simplilearn

Cloud Computing

Caltech | Center for Technology & Management Education

PG CC - Microsoft Azure Architect Design: AZ:304

Powerd by simplilearn

Design Authentication

Learning Objectives

By the end of this lesson, you will be able to:

- Recommend a solution for single sign-on (SSO)
- Recommend a solution for authentication
- Recommend a solution for conditional access
- Recommend a solution for network access authentication

Learning Objectives

By the end of this lesson, you will be able to:

- Recommend a solution for a hybrid identity
- Recommend a solution for user self-service
- Recommend and implement a solution for B2B integration

A Day in the Life of an Azure Architect

You are advising an organization in which you are working as an Architect. The company has an existing hybrid deployment of Azure AD. You have been asked to recommend a solution that ensures that the Azure AD tenant can only be managed from the machines that are within the on-premises network.

Also, users should be able to automatically sign in when they are on devices which are connected to your organization's network.

Along with these, the company has following requirements:

- A solution that can help manage the users.
- A solution that will allow external users to collaborate with your company.

A Day in the Life of an Azure Architect

- A solution for managing member and computer access to shared resources for a group of users.
- A solution to authorize requests to Blob and Queue storage.
- An authentication solution that allows access to both cloud and on-premises apps and resources.

To achieve all of the above, along with some additional features, we would be learning a few concepts in this lesson that will help you find a solution for the above scenario.

Recommend a Solution for Single Sign-On (SSO)

Azure Active Directory Seamless Single Sign-On (SSO)

Azure AD Seamless SSO automatically signs users in when they are on their corporate devices connected to a corporate network.

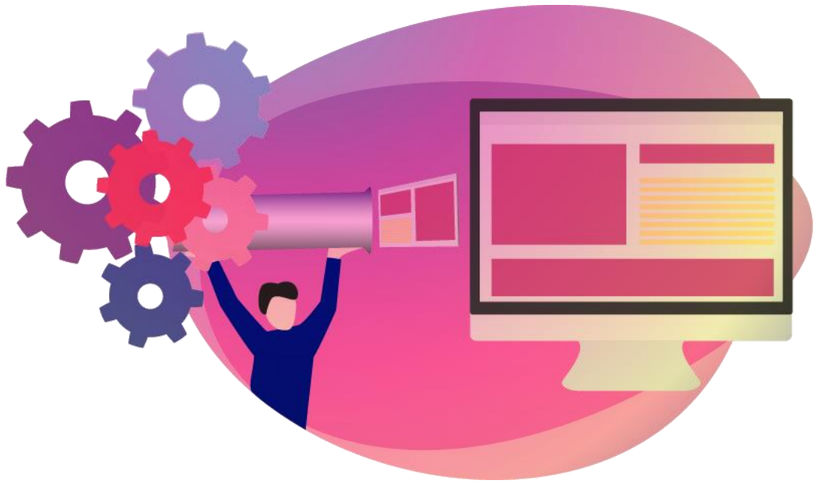
Benefits of Single Sign-On (SSO)

User Experience

- Automatic sign in for both on-premises, cloud-based applications
- Users don't have to enter their passwords repeatedly

Benefits of Single Sign-On (SSO)

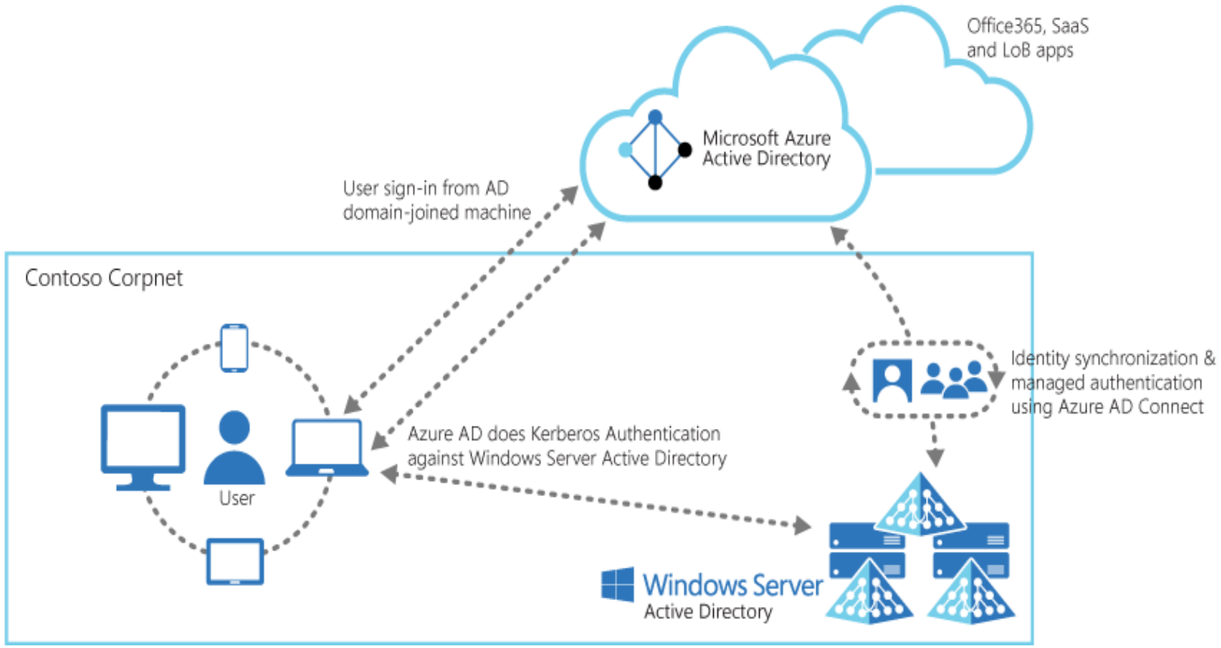
Easy Deployment



- Needs no additional on-premises components
- Works with any method of cloud authentication
- Can be rolled out to some or all the users
- Register non-Windows 10 devices with Azure AD without the need for AD FS infrastructure

Features of Single Sign-On (SSO)

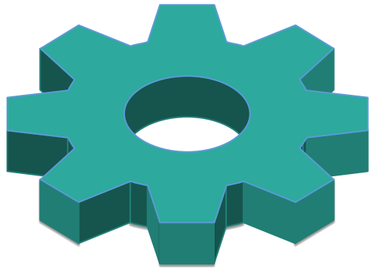
Sign-in username can be the on-premises default username or another attribute configured in the Azure AD Connect method but cannot be used with ADFS.



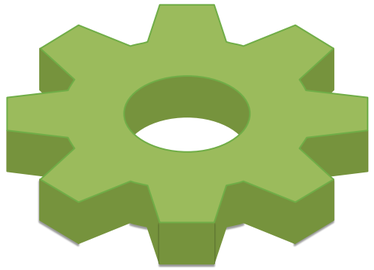
- If SSO fails, use a password at the sign-in page
- Sign in or out of other accounts
- Enabled via Azure AD Connect
- Sample list of applications included with Azure AD

Considerations: Azure AD Seamless Single Sign-On

Some considerations with respect to Azure AD Seamless Single Sign-On include:



Can be combined with Password Hash or Pass-through Authentication



Azure AD Join provides SSO for devices registered with Azure AD

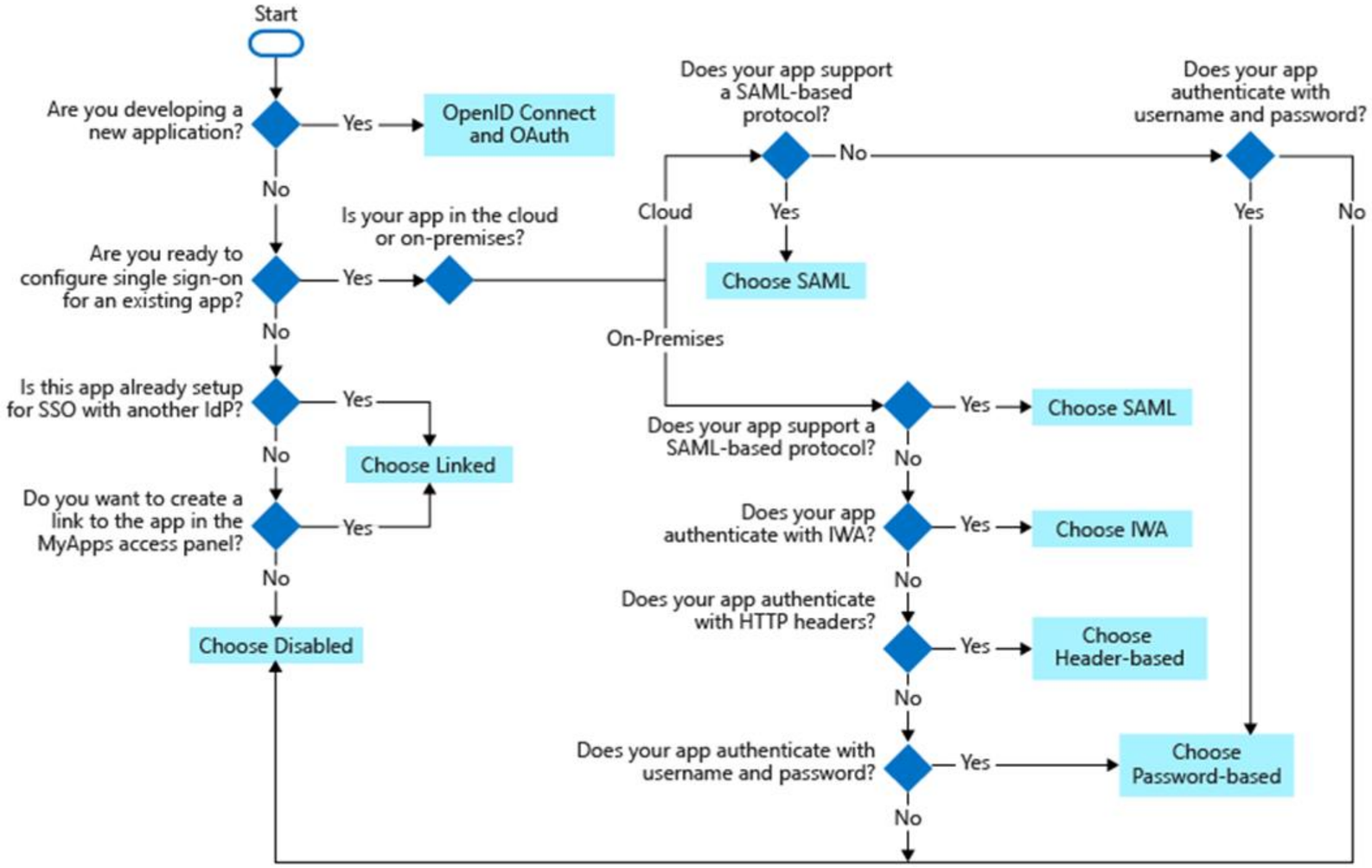
Considerations: Azure AD Seamless Single Sign-On

Applications using **domain_hint** or **login_hint** parameter capability of Seamless SSO are:

Application name	Application URL to be used
Access panel	https://myapps.microsoft.com/contoso.com
Outlook on Web	https://outlook.office365.com/contoso.com
Office 365 portals	https://portal.office.com?domain_hint=contoso.com, https://www.office.com?domain_hint=contoso.com

Single Sign-On Flowchart

The workflow of Single Sign-On is given below:



Recommend a Solution for Authentication

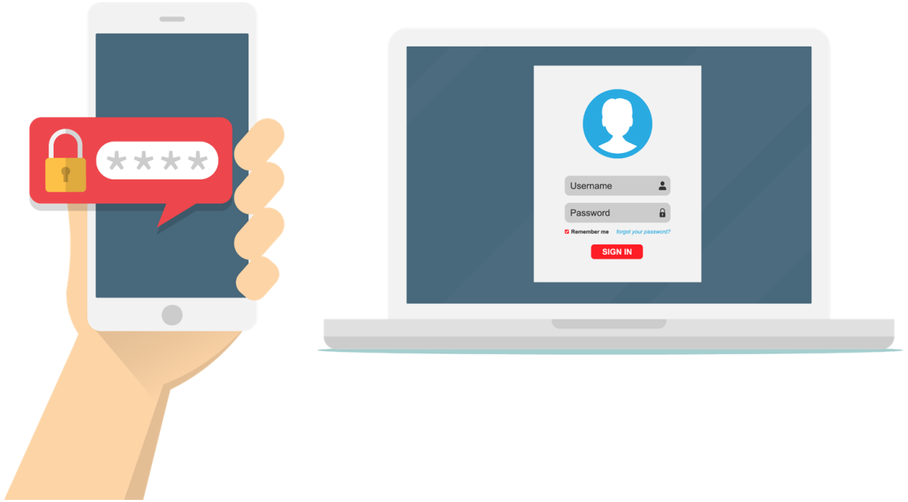
Authentication

Authentication is the process of confirming who the user claims to be.

Microsoft identity platform implements the OpenID Connect protocol for handling authentication.

OAuth vs OpenID Connect

OAuth is used for authorization and OpenID Connect (OIDC) is used for authentication.



OpenID Connect is built on top of OAuth 2.0

It is possible to authenticate a user (using OpenID Connect) and get authorization to access a protected resource that the user owns (using OAuth 2.0) in one request.

Authentication Use Cases

Delegating authentication and authorization to Azure AD enables scenarios such as:

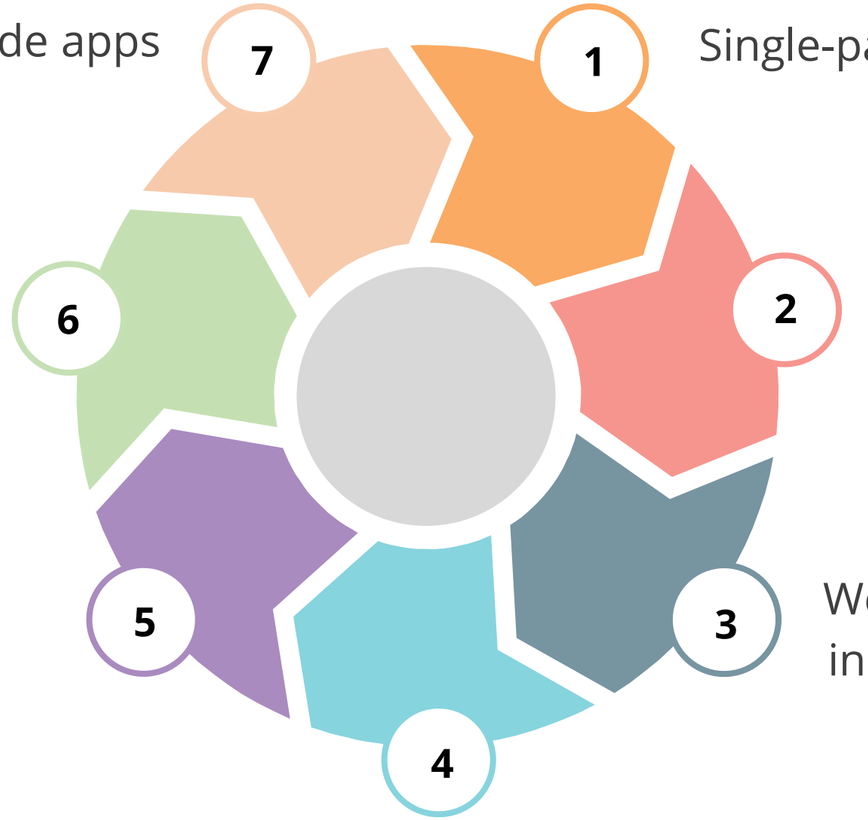
Conditional Access policies that require a user to be in a specific location

The use of multi-factor authentication also called two-factor authentication or 2FA

Single Sign-On enables a user to sign in once and be automatically signed in to all the web apps

Application Scenarios

The Microsoft identity platform supports authentication for these app architectures:



1. Single-page apps
2. Web apps that sign in a user
3. Web apps that sign in a user and call a web API
4. Mobile app that calls a web API
5. Native apps
6. Daemon app that calls a web API
7. Server-side apps

Recommend Solution for Conditional Access

Conditional Access

The policies are if-then statements, which means that if users wish to access a resource, they should first perform an action.

It allows a user to apply the appropriate access controls when not required to keep the organization safe and secure.

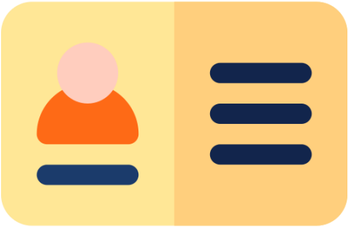
Conditional Access

These are the best practices for Conditional Access:

- Plan your costs
- Communicate with users and IT
- Use the zero trust security model
- Establish the steering committee

Multi-Factor Authentication (MFA)

It is a process where a user is prompted during the sign-in process for an additional form of identification.



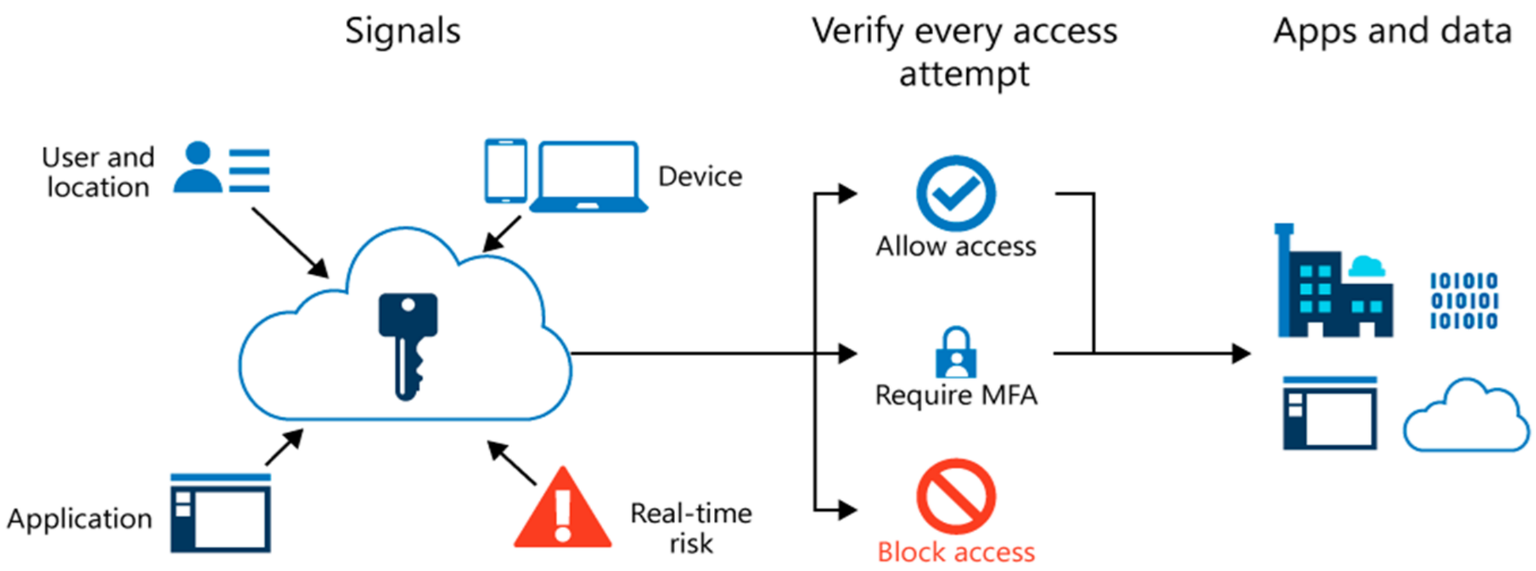
Username or Password

Phone or hardware key

Biometrics like a fingerprint or face scan

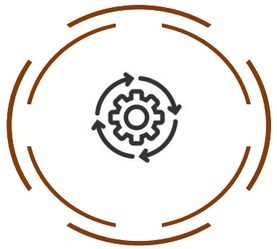
Multi-Factor Authentication

Azure Multi-Factor Authentication provides two-step authentication and verification.

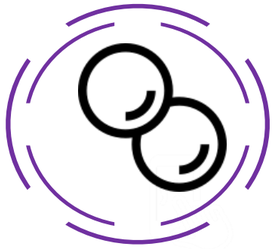


MFA Verification Methods

Verification methods for multi-factor authentication:



Microsoft Authenticator App



OAUTH Hardware Token

SMS

MFA Authentication Methods

These are the authentication methods of MFA:

- Call to phone
- Verification code from mobile app
- Text message to phone
- Notification on mobile app

Reasons for Multi-Factor Authentication

These are the reasons for multi-factor authentication:

Password complexity rules

Password expiration rules

Azure AD identity protection

Azure AD password protection

Source: https://docs.microsoft.com/

Reasons for Multi-Factor Authentication

These are the reasons for multi-factor authentication:

Azure AD smart lockout

Azure AD application proxy

Single sign-on (SSO)

Azure AD connect

Source: https://docs.microsoft.com/

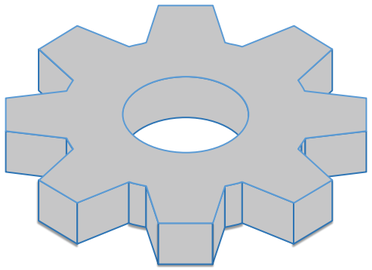
Plan for MFA Deployment

Below are the deployment considerations:

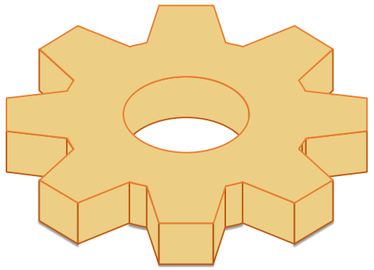
- All users, a specific user, a group member, or a role allocated
- Device platform
- State of the device
- Client applications
- Hybrid Azure AD joined device

Conditional Access and Azure Multi-Factor Authentication (MFA)

Azure MFA allows a user to impose restrictions on app access depending on the conditions listed below:



MFA can be set for users and groups to prompt for additional verification during sign-in.



Conditional Access policies, on the other hand, can be used to establish MFA-required events or applications.

Configure MFA Settings

The MFA settings are given in the table below:

Feature	Description
Account lockout	Temporarily lock accounts if there are too many denied authentication attempts in a row.
Block/unblock users	Used to block specific users from being able to receive MFA requests.
Fraud alert	Configure settings related to user's ability to report fraudulent verification requests
Notifications	Enable notifications of events from the MFA server.
OAUTH tokens	Used in cloud-based Azure MFA environments to manage OAUTH tokens for users.
Phone call settings	Configure settings related to phone calls and greetings for cloud and on-premises environments.
Providers	This will show any existing authentication providers that may have associated with an Azure account.

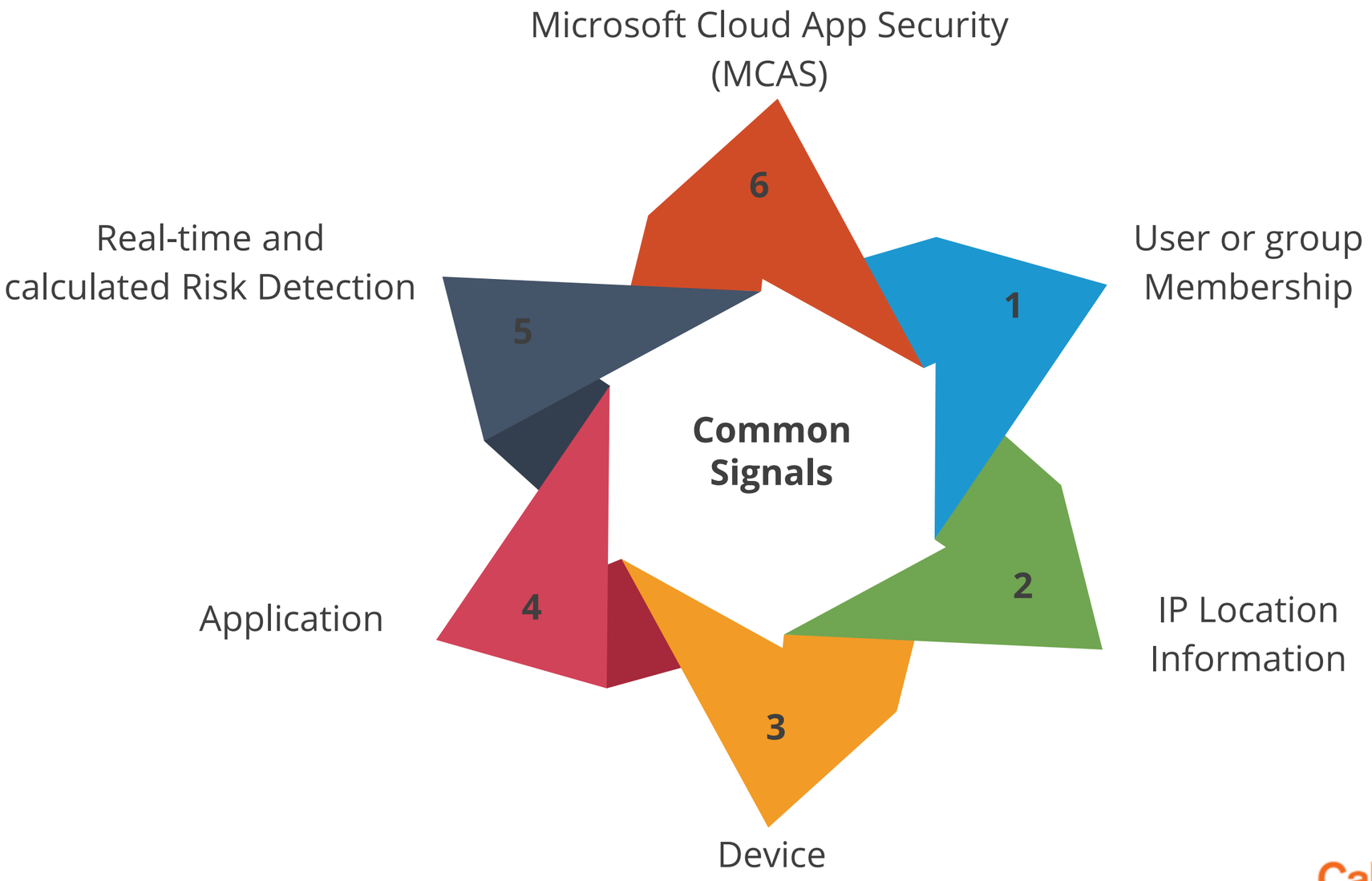
Conditional Access: Signals and Decisions

These are the commonly applied policies:

- Requires MFA for management tasks
- Requires MFA for users with administrative roles
- Blocks or grants access from specific location
- Requires trusted locations for Azure MFA registration
- Blocks sign-in for users attempting to use legacy authentication protocols
- Requires organization-managed devices for specific applications
- Blocks risky sign-in behaviors

Conditional Access: Signals

These are the common signals:



Conditional Access: Decisions

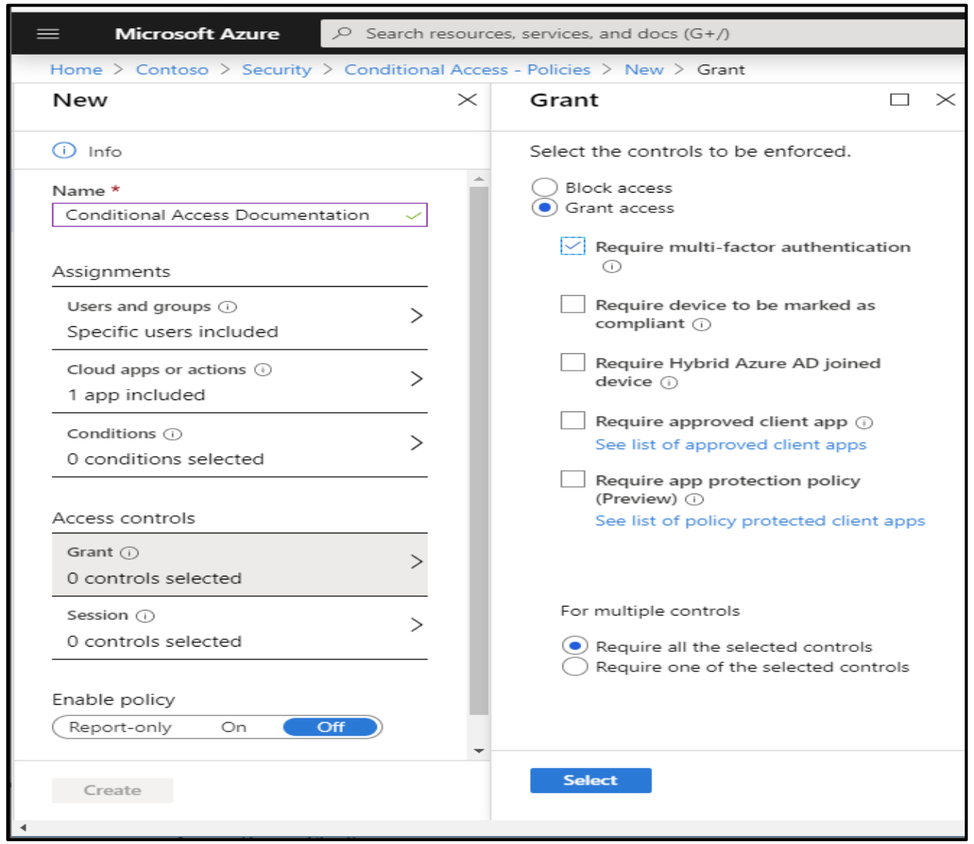
The following are the common decisions that Conditional Access should consider while making a policy decision:

Block Access

Grant Access

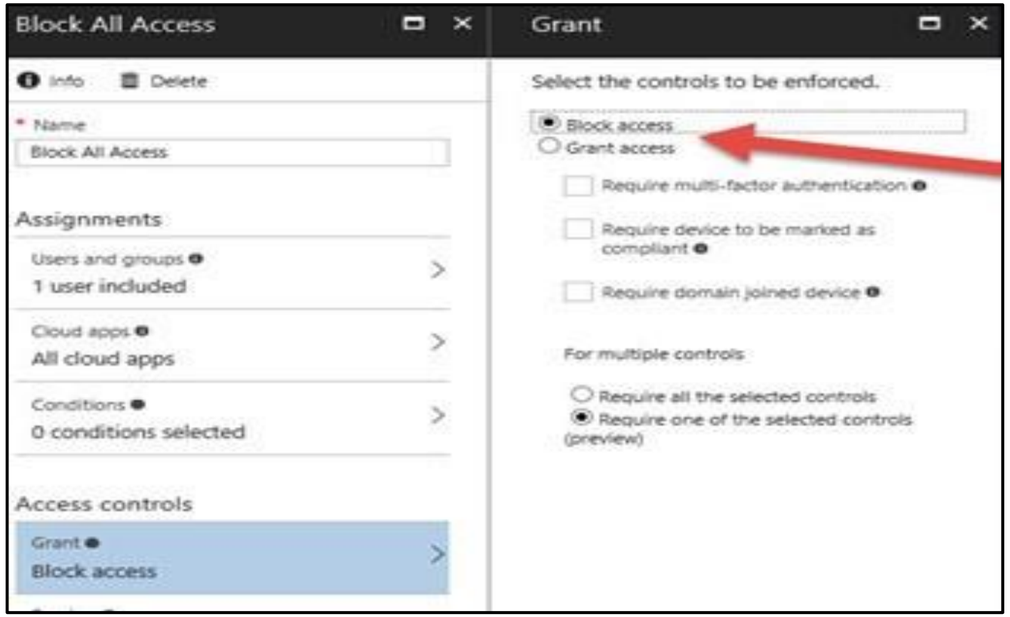
Grant Access

Grant provides administrators with a means of policy enforcement where they can block or grant access.



Block Access

It will block access under the specified assignments.



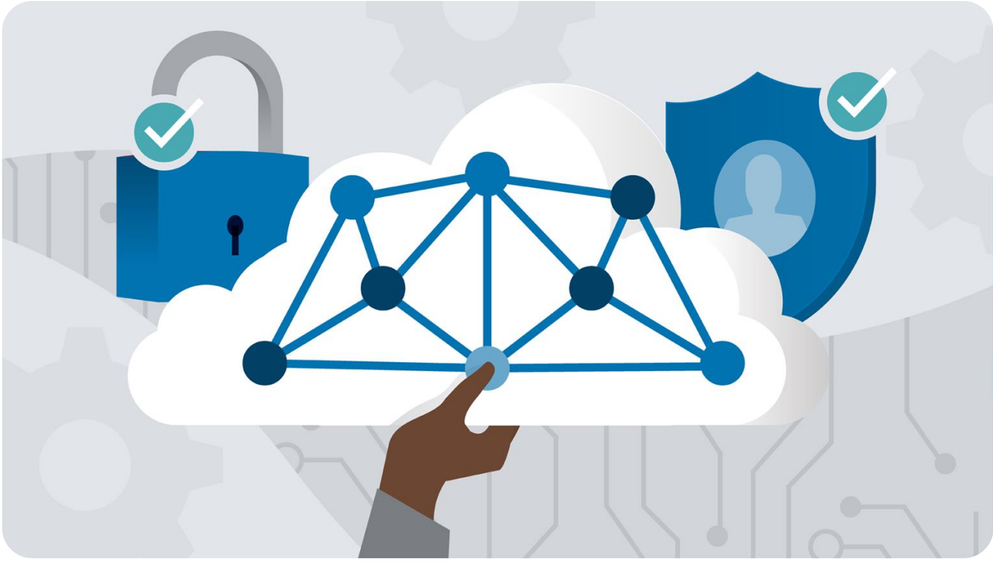
Block control is a powerful tool that should be used only by those who have the necessary knowledge.

Recommend a Solution for Hybrid Identity

Hybrid Identity

Microsoft's identity solutions span on-premises and cloud-based capabilities.

These solutions create a common user identity for authentication and authorization to all resources, regardless of location.



Hybrid Identity

The following authentication methods can be used to implement hybrid identity with Azure AD:

1

Password hash synchronization (PHS)

2

Pass-through authentication (PTA)

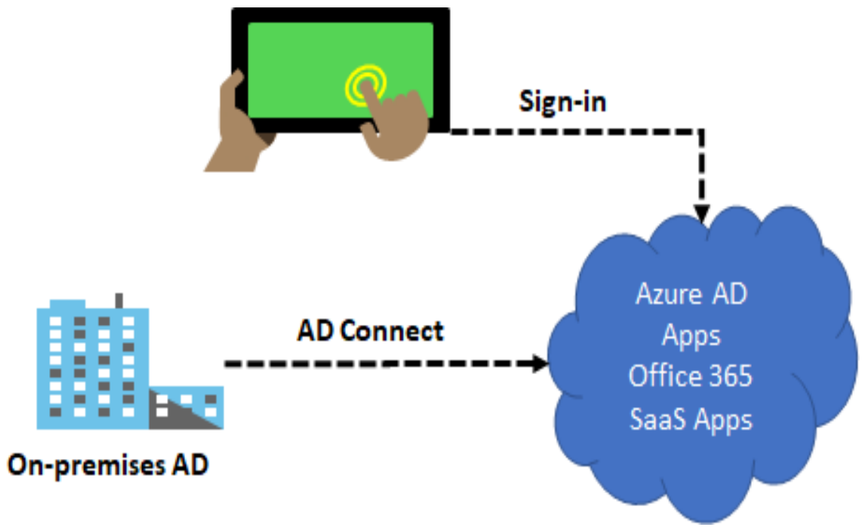
3

Federation (AD FS)

Azure AD Connect

Integrating on-premises directories with Azure AD provides a common identity for accessing both cloud and on-premises resources.

- Users can use a single identity to access on-premises applications and cloud services.
- It is a tool to provide an easy deployment experience for synchronization and sign-in.



Azure AD Connect replaces older versions of identity integration tools such as DirSync and Azure AD Sync.

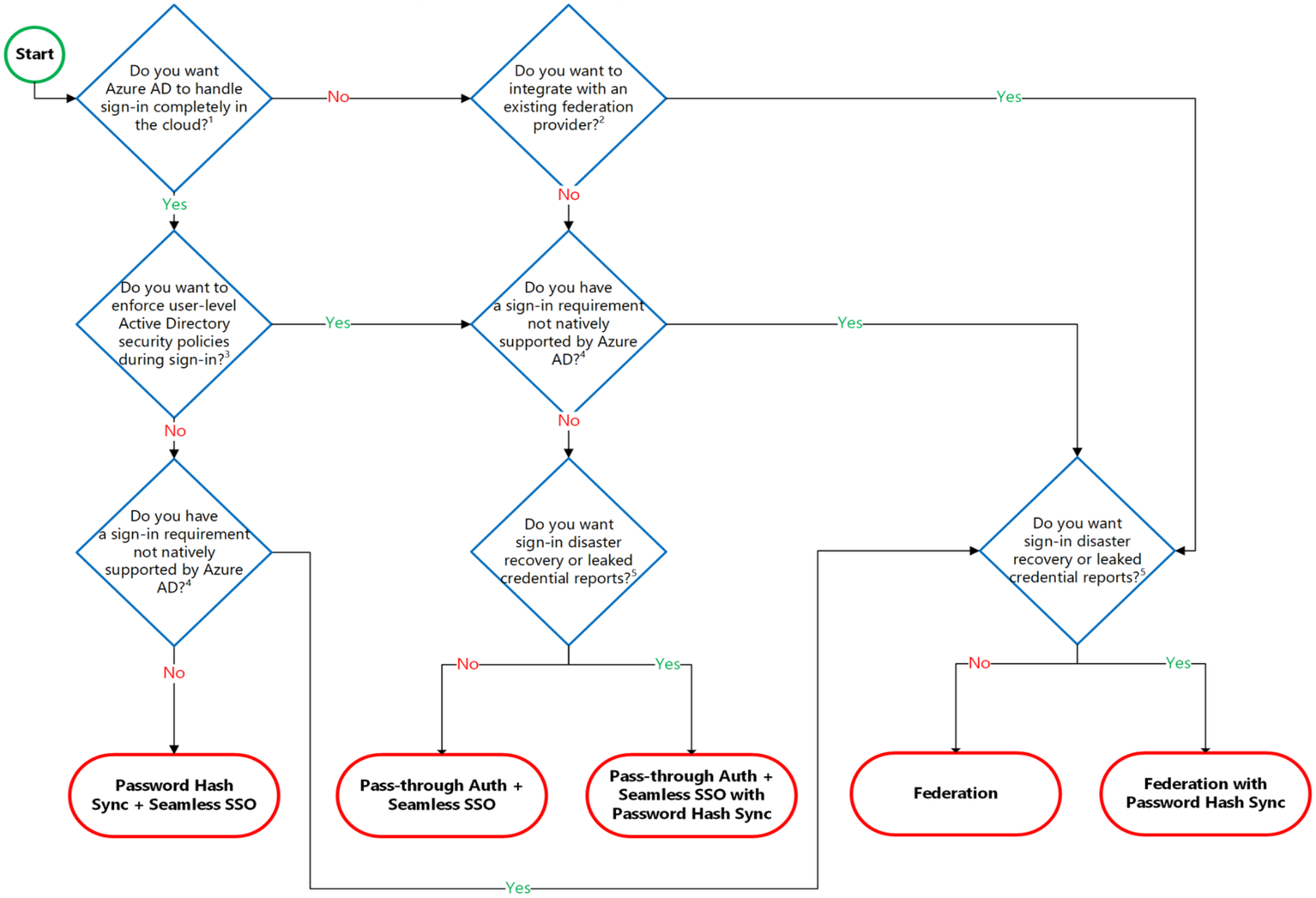
Common Scenarios

Below are common scenarios with recommended hybrid identity option:

User needs to:	PHS and SSO	PTA and SSO	AD FS
Sync new user, contact, and group accounts created in their on-premises Active Directory to the cloud automatically	X	X	X
Set up tenant for Office 365 hybrid scenarios	X	X	X
Enable users to sign in and access cloud services using their on-premises password	X	X	X
Implement single sign-on using corporate credentials	X	X	X
Ensure no password hashes are stored in the cloud		X	X
Enable cloud-based multi-factor authentication solutions	X	X	X
Enable on-premises multi-factor authentication solutions			X
Support smart card authentication for users			X
Display password expiry notifications in the Office Portal and on the Windows 10 desktop			X

Hybrid Identity Decision Tree

Workflow of hybrid identity decision tree is shown below:

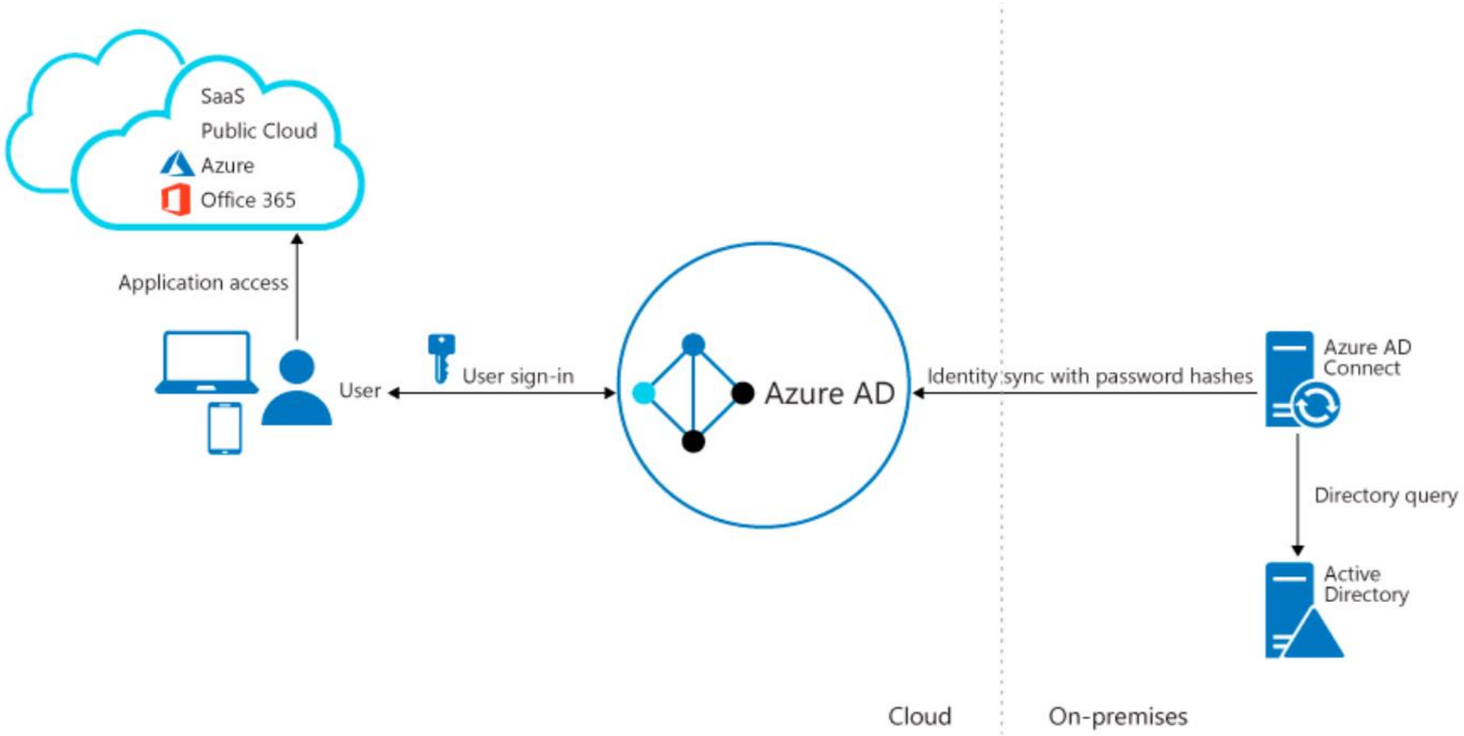


Source: https://docs.microsoft.com/

Authentication Architecture

Azure AD Hybrid identity with password hash sync

Simplicity of a password hash synchronization solution

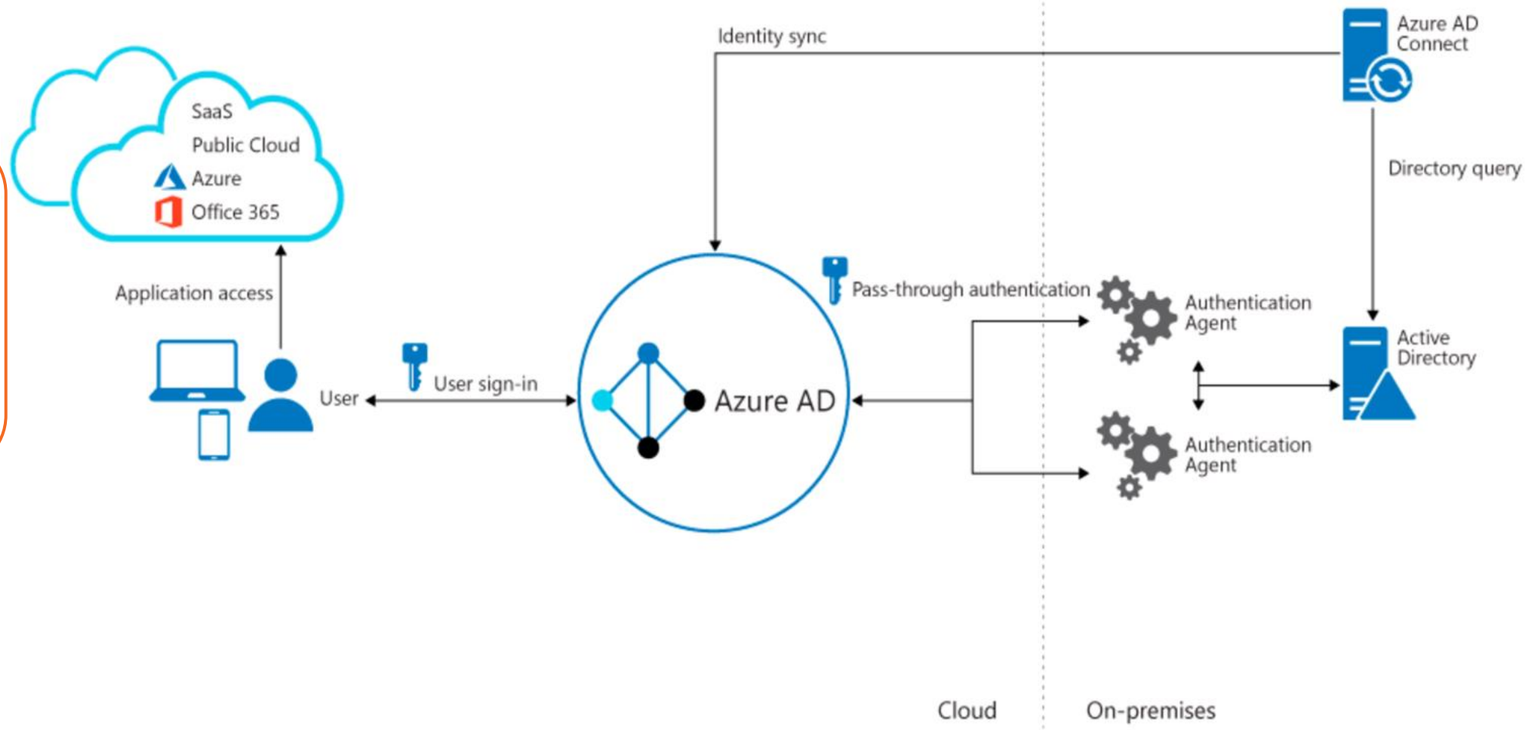


Source: https://docs.microsoft.com/

Authentication Architecture

Azure AD Hybrid identity with Pass-through authentication

Agent requirements of pass-through authentication, using two agents for redundancy



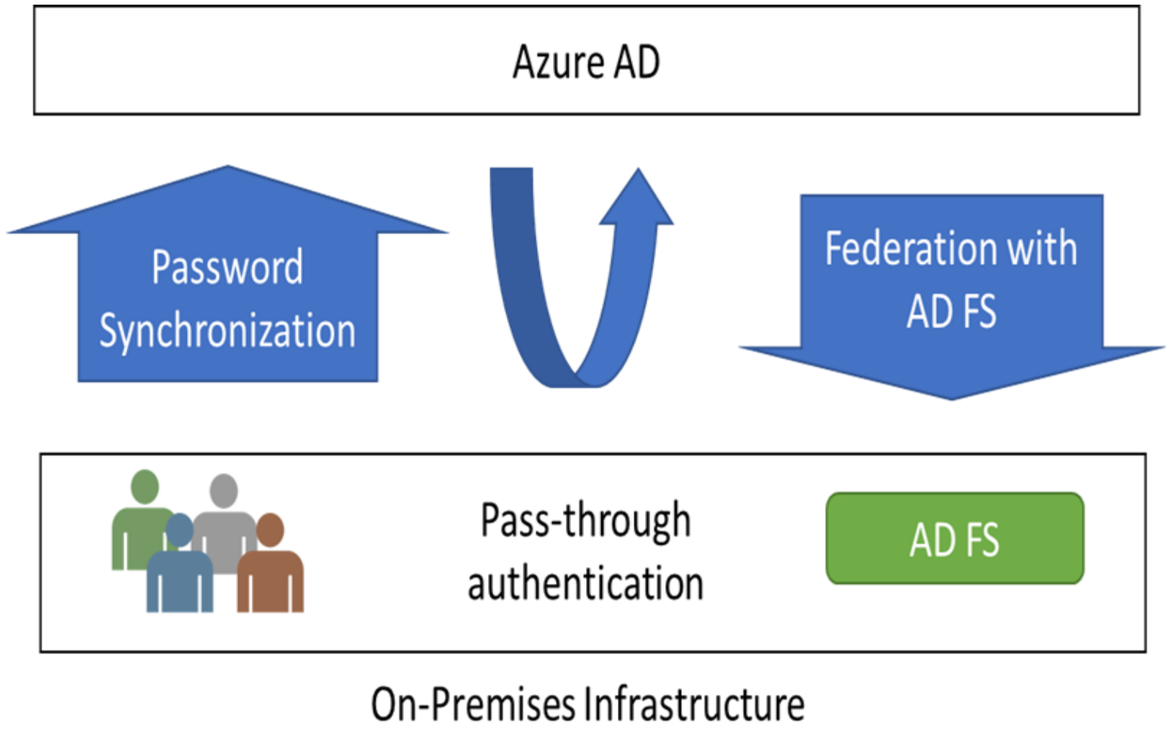
Source: https://docs.microsoft.com/

Authentication Options

The first option organizations can choose to authenticate is:

Password Hash Synchronization

PHS can synchronize an encrypted version of the password hash for user accounts

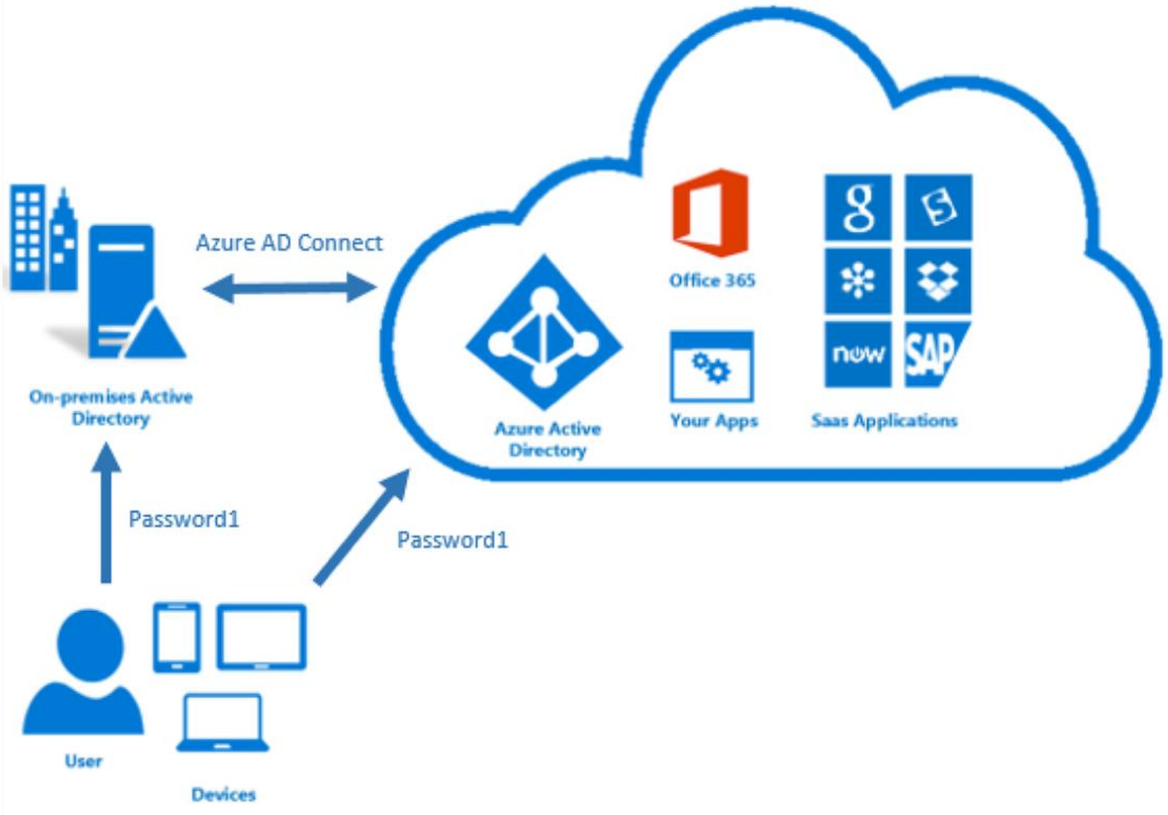


Authentication Options

The second option organizations can choose to authenticate is:

Pass-through authentication

PTA authenticates the username and password with the on-premises domain controllers



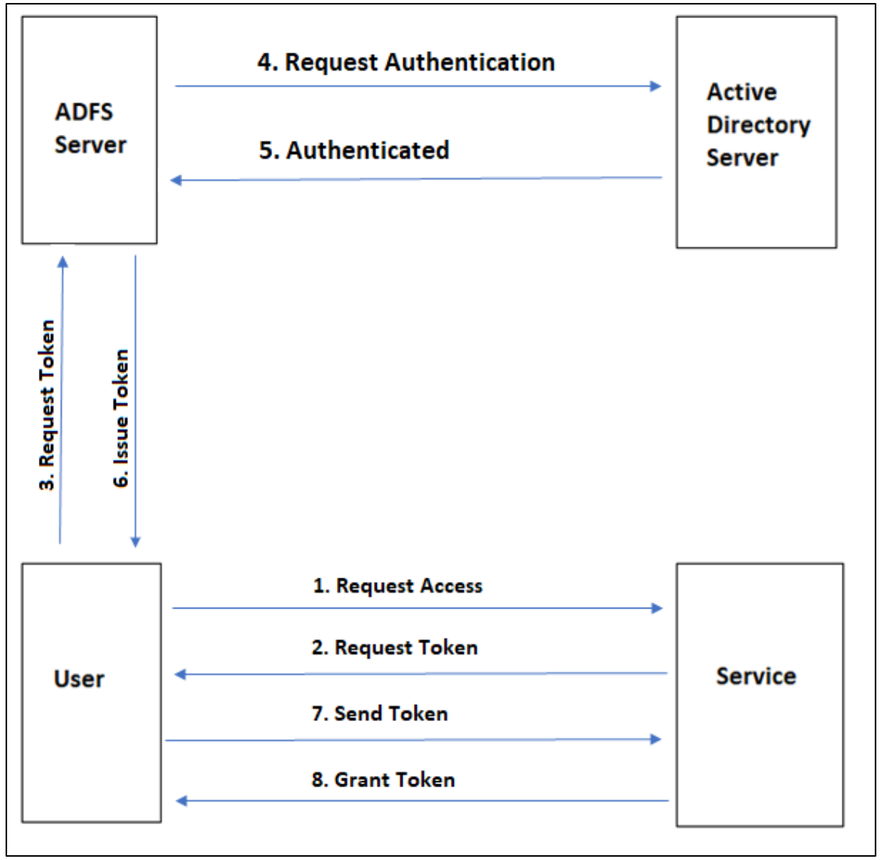
Source: https://docs.microsoft.com/

Authentication Options

The third option organizations can choose to authenticate is:

Active Directory Federation Services

AD FS is the Microsoft implementation of an identity federation solution that uses claims-based authentication



Comparing Authentication Methods

Consideration	Password hash synchronization + Seamless SSO	Pass-through Authentication + Seamless SSO
Where does authentication happen?	In the cloud	In the cloud after a secure password verification exchange with the on-premises authentication agent
What are the on-premises server requirements beyond the provisioning system: Azure AD Connect?	None	One server for each additional authentication agent
What are the requirements for on-premises internet and networking beyond the provisioning system?	None	Outbound internet access from the servers running authentication agents
Is there a TLS/SSL certificate requirement?	No	No
Is there a health monitoring solution?	Not required	Agent status provided by Azure Active Directory admin center

Source: https://docs.microsoft.com/

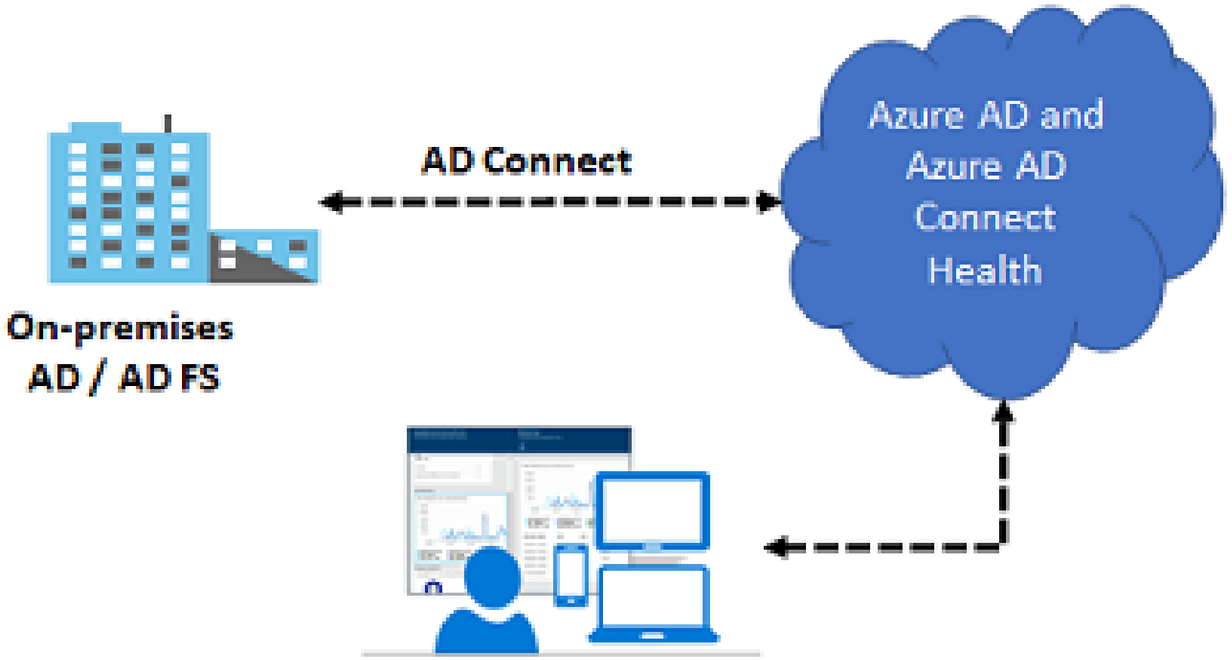
Comparing Authentication Methods

Consideration	Password hash synchronization + Seamless SSO	Pass-through Authentication + Seamless SSO
Do users get single sign-on to cloud resources from domain-joined devices within the company network?	Yes with Seamless SSO	Yes with Seamless SSO
What sign-in types are supported?	UserPrincipalName + password Windows-Integrated authentication by using Seamless SSO Alternate login ID	UserPrincipalName + password Windows-Integrated authentication by using Seamless SSO Alternate login ID
What are the multifactor authentication options?	Azure AD MFA Custom Controls with Conditional Access*	Azure AD MFA Custom Controls with Conditional Access*
What are the Conditional Access options?	Azure AD Conditional Access, with Azure AD Premium	Azure AD Conditional Access, with Azure AD Premium

Source: https://docs.microsoft.com/

Azure AD Connect Health

Azure AD Connect Health helps monitor on-premises identity infrastructure thus ensuring the reliability of the environment.



Why Use Azure AD Connect Health?

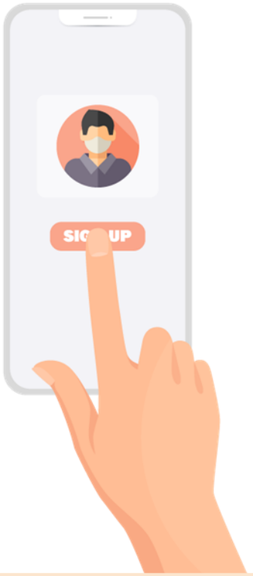
Key Benefits

- Enhanced security
- Alerts on all critical ADFS system issues
- Simplified deployment and management
- Rich usage metrics
- Enhanced admin experience

Recommend a Solution for User Self Service

Self Service Sign-Up

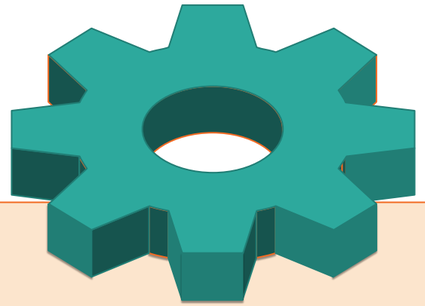
With a self-service sign-up user flow, one can create a sign-up experience for external users who want to access apps.



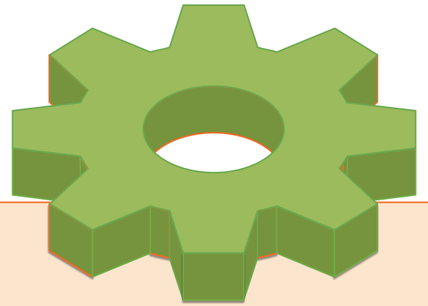
The user signs up for a cloud service and has an identity automatically created for them in Azure AD based on their email domain.

Self Service Sign-Up

As part of the sign-up flow:



Provide options for different social or enterprise identity providers

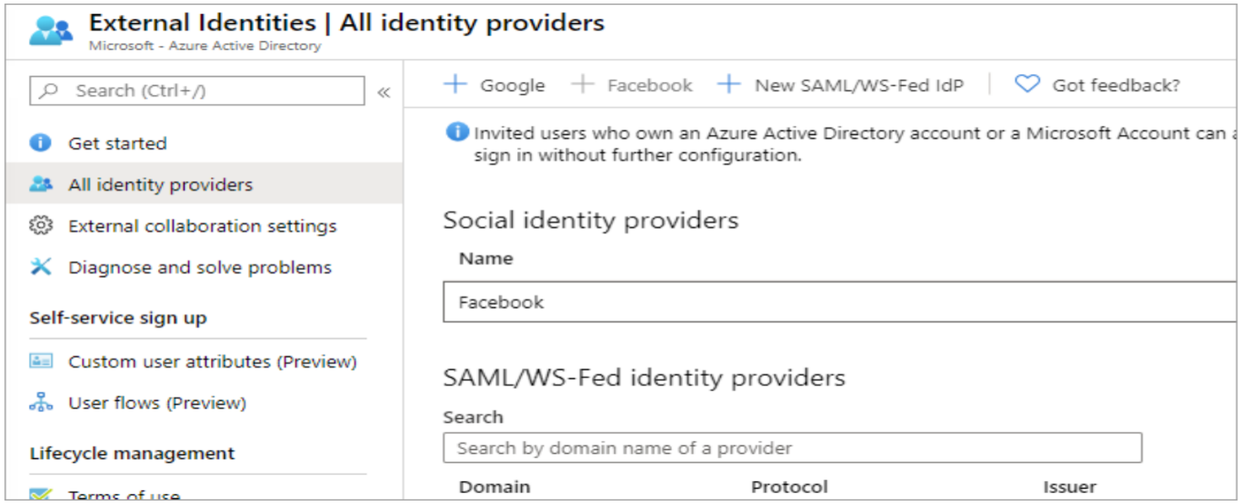


Collect information about the user

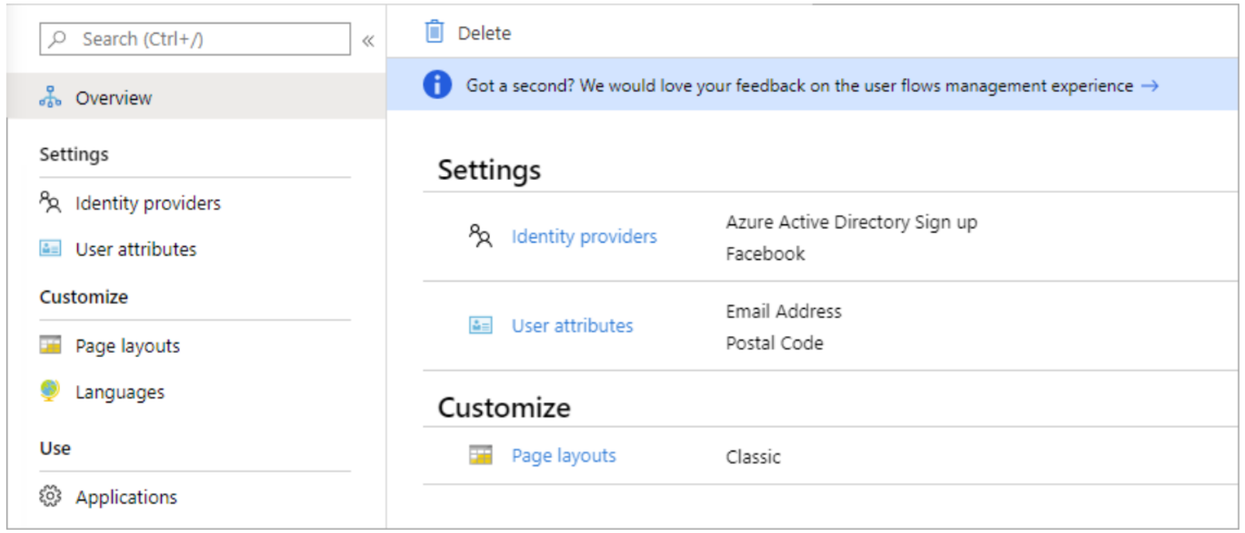
Self-Service Sign-Up Use Cases

Self-Service Sign-Up User Flow

Set up federation with Identity Providers



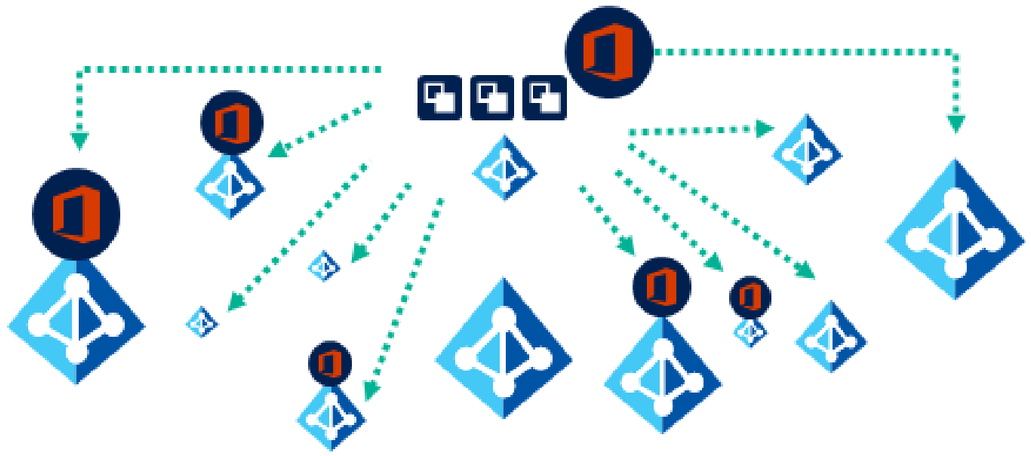
Create a Self-Service Sign-Up User Flow



Recommend and Implement a Solution for B2B Integration

Azure AD B2B

With Azure AD B2B (business-to-business):



- There are no external operating costs for user's business.
- Azure AD is not needed since the partner uses their own identities and credentials.
- The user does not have to worry about passwords or external accounts.
- The user does not need to sync accounts or manage account lifecycles.

Guest Users

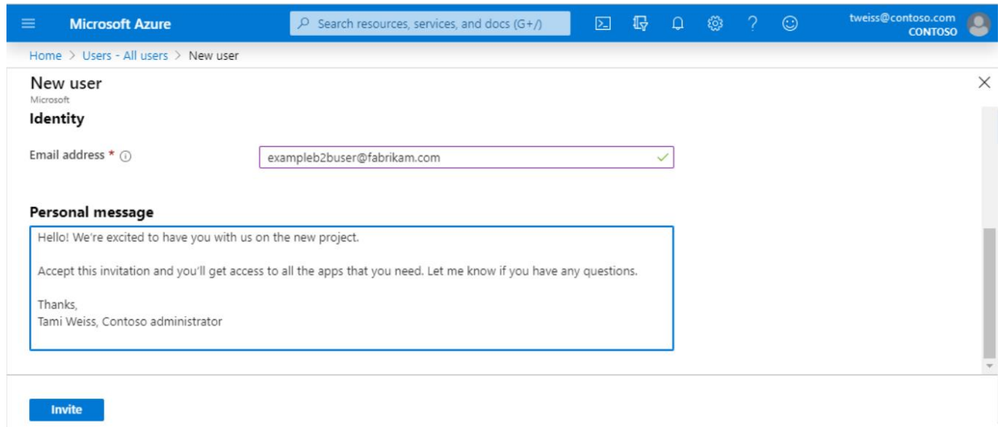
Guest users are those who are not considered as an internal entity, such as an external partner, stakeholder, or a customer.

Prerequisites

- Anyone can be asked to work for a company by adding them as a guest user.
- Guest users can use their own work, education, or social identity to log in.
- A user should have the ability to create user accounts.
- A user should have a working email address.

Adding Guest Users

Anyone can work with a company by being added to a directory as a guest user.

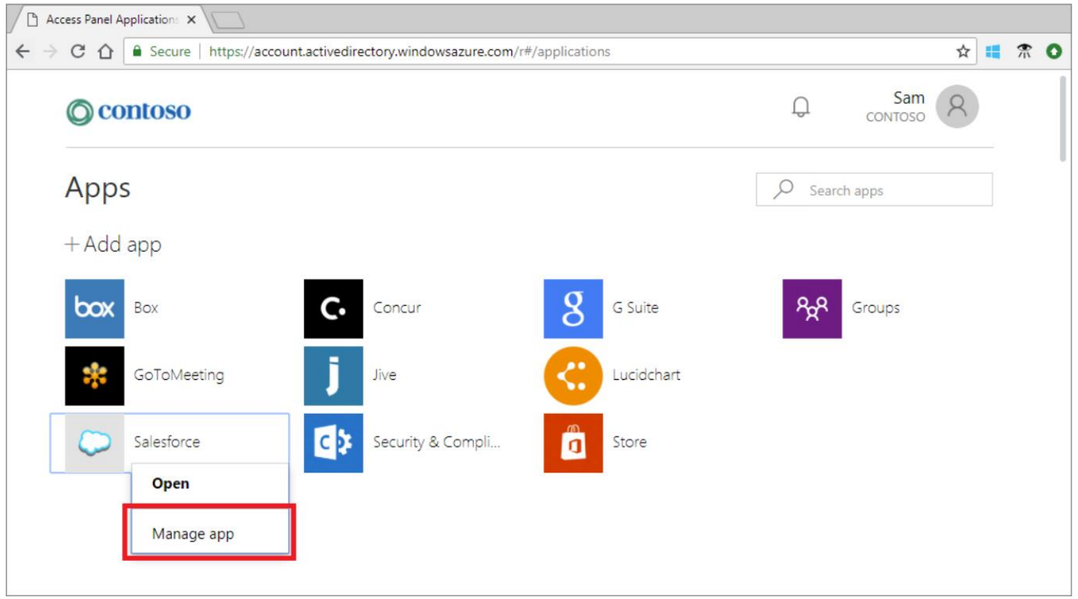


Follow the instructions given below to add a new guest user:

- Log in as an administrator to the Microsoft Azure portal
- Create a **New guest user**
- The user will receive the invitation as a guest
- After accepting the invite, guest users can be assigned to any app or group

Adding Guest Users

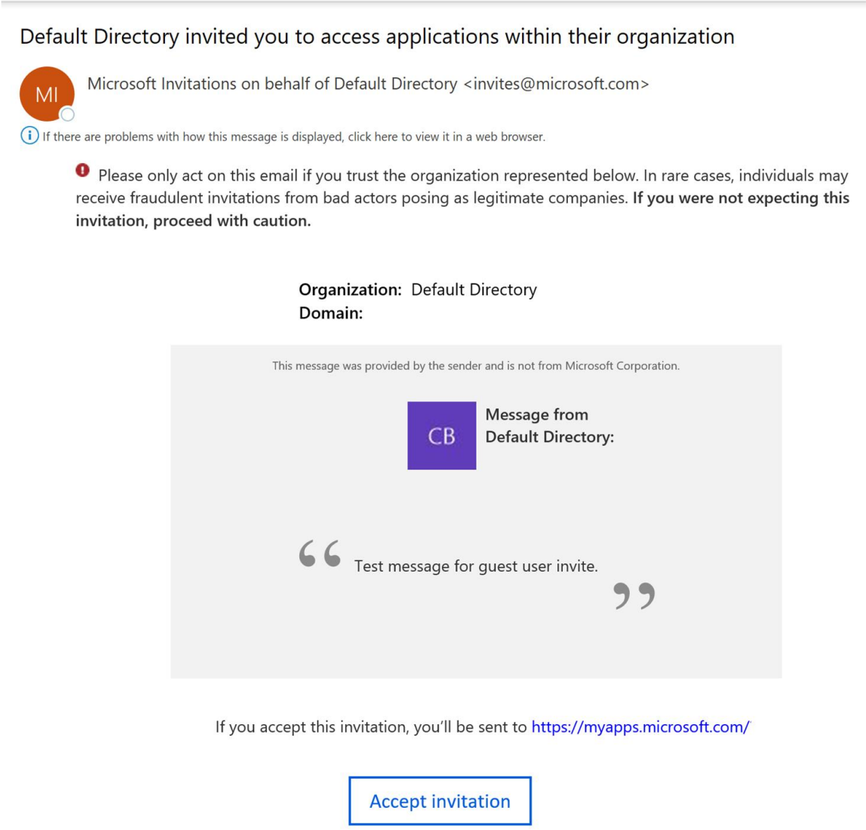
Allow application or group owners to manage their guest users



- Administrators: Self-service app and group management
- Non-administrators: Use Access Panel to add guest users

Accept the Guest User Invite

Follow the instructions to accept a new user invite:



- Log in to your guest user's email account
- In the inbox, locate the mail with the subject **You're invited**
- Open the email and click on **Get started**
- Select **Accept Invitation**

Assisted Practice

Azure AD Join

Duration: 10 Min.

Problem Statement:

You've asked an Azure Architect to assist your company with an Azure authentication solution that allows access to both cloud and on-premises apps and resources.

Assisted Practice: Guidelines

Steps to create Azure AD Join:

1. Sign in to the Azure portal as an administrator
2. Under Azure services, select Azure Active Directory
3. Select Devices on the left of the Azure AD page
4. Click on Device Settings
5. Users may join devices to Azure AD

Assisted Practice

Azure AD: User Creation

Duration: 10 Min.

Problem Statement:

As an Azure Architect, you have been asked to help your organization with an azure authentication solution that can help manage the users.

Assisted Practice: Guidelines

Steps to create a user in Azure AD:

1. Sign in to the Azure portal as an administrator
2. Under Azure services, select Azure Active Directory
3. Under Manage, select Users
4. Select New user
5. Fill in the required fields and create

Assisted Practice

Azure AD Guest User Creation

Duration: 10 Min.

Problem Statement:

As an Azure Architect, you've been asked to assist your company with an azure authentication solution that will allow external users to collaborate with your company.

Assisted Practice: Guidelines

Steps to create a guest user in Azure AD:

1. Sign in to the Azure portal as an administrator
2. Under Azure services, select Azure Active Directory
3. Under Manage, select New guest user
4. On the New user page, select Invite user, then add the guest user's information and then click on the Invite button

Assisted Practice

Azure AD: Group Creation

Duration: 10 Min.

Problem Statement:

As an Azure Architect, you've been asked to provide your company with an azure authentication solution for managing members and computer access to shared resources for a group of users. For example, creating a security group for a certain security policy.

Assisted Practice: Guidelines

Steps to create a user group:

1. Sign in to the Azure portal as an Azure AD
2. Under Azure services, select Azure Active Directory
3. On the Active Directory page, select Groups and then select New group
4. Your group will be created and ready for you to add members

Assisted Practice

Add Azure AD Authentication for Storage

Duration: 10 Min.

Problem Statement:

As an Azure Architect, you have been asked to help your organization with an azure authentication solution to authorize requests to Blob and Queue storage.

Assisted Practice: Guidelines

Steps to create a guest user in Azure AD:

1. Log in to the Azure portal at https://portal.azure.com
2. Search using the keyword Storage account and open it
3. Create a Container under your storage account where you wish to upload a blob
4. In the Authentication Type field, select Azure AD account to indicate you want to authorize the upload operation by using your Azure AD account

Assisted Practice

Azure AD: Custom Domain Creation **Duration: 10 Min.**

Problem Statement:

As an Azure Architect, you have been asked to help your organization with an azure authentication solution to create a custom domain name that will help you to create user names familiar to your users.

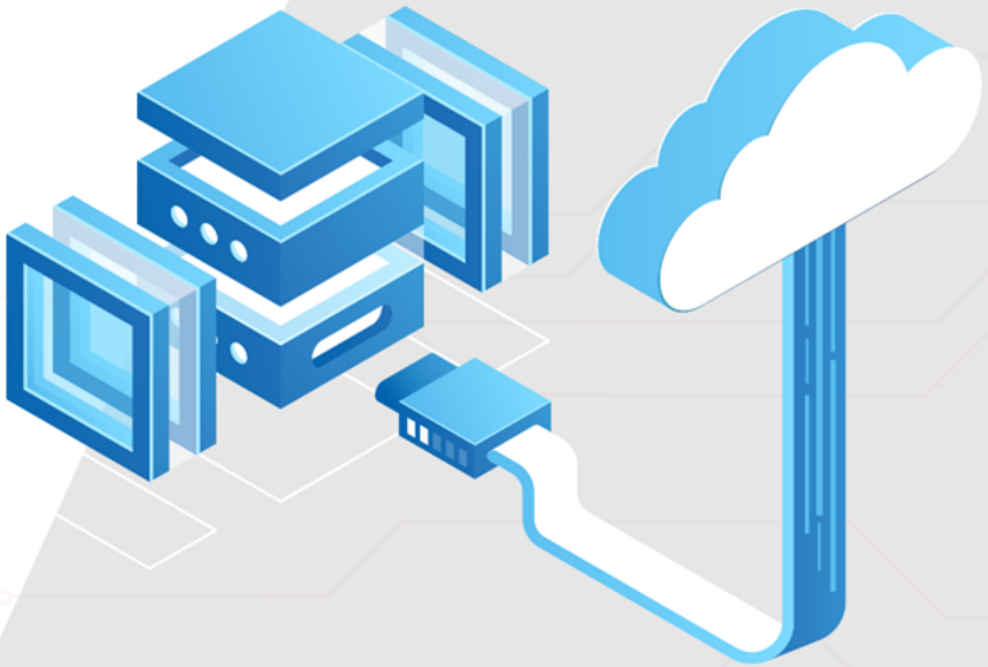
Assisted Practice: Guidelines

Steps to create a custom domain:

1. Sign in to the Azure portal as an administrator
2. Under Azure services, select Azure Active Directory
3. Add a custom domain name, then click on Add domain
4. The unverified domain is added , and a page appears showing DNS information

Key Takeaways

- In Conditional Access policies if users want to access a resource, then they must complete an action.
- Multi-factor authentication is a process where a user is prompted during the sign-in process for an additional form of identification.
- Azure AD Seamless SSO automatically signs users in when they are on their corporate devices connected to a corporate network.
- Guest users are not expected to receive an internal invitation from the CEO or to receive any company benefits.



Thank you