Caltech | Center for Technology & Management Education

Designing Infrastructure Solutions on Azure

Powered by simplilearn

Design Authentication Solutions

Learning Objectives

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

- Describe Azure Active Directory
- Recommend a solution for single sign-on (SSO)
- Recommend a solution for authentication
- Recommend a solution for conditional access
- Recommend a solution that includes managed identities

Learning Objectives

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

- Recommend a solution that includes key vault
- 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 for 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 that are connected to your organization’s network.

Along with these, the company has the 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 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.

Azure Active Directory

Azure Active Directory

Azure Active Directory (Azure AD) is Microsoft's cloud-based identity and access management service, which helps employees of an enterprise client to sign in and access resources.

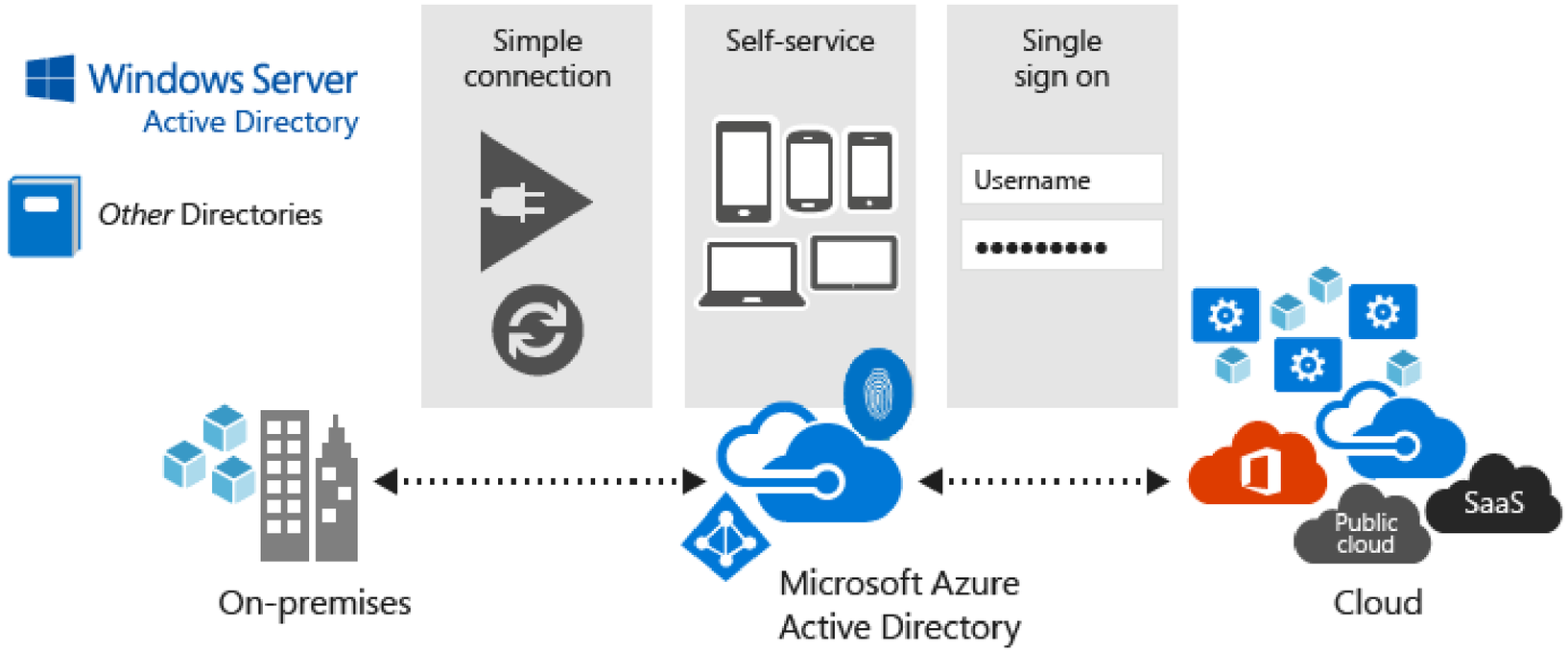
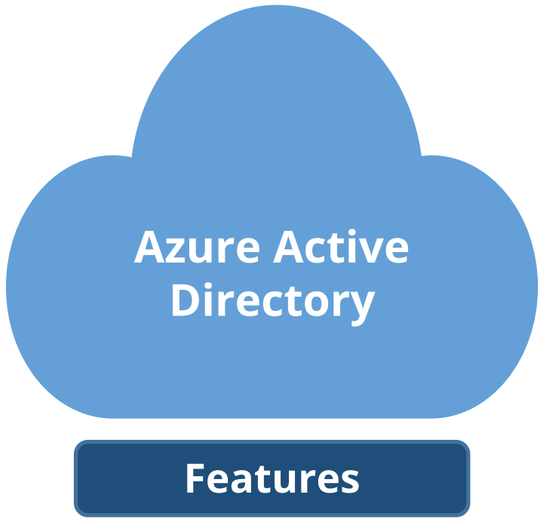


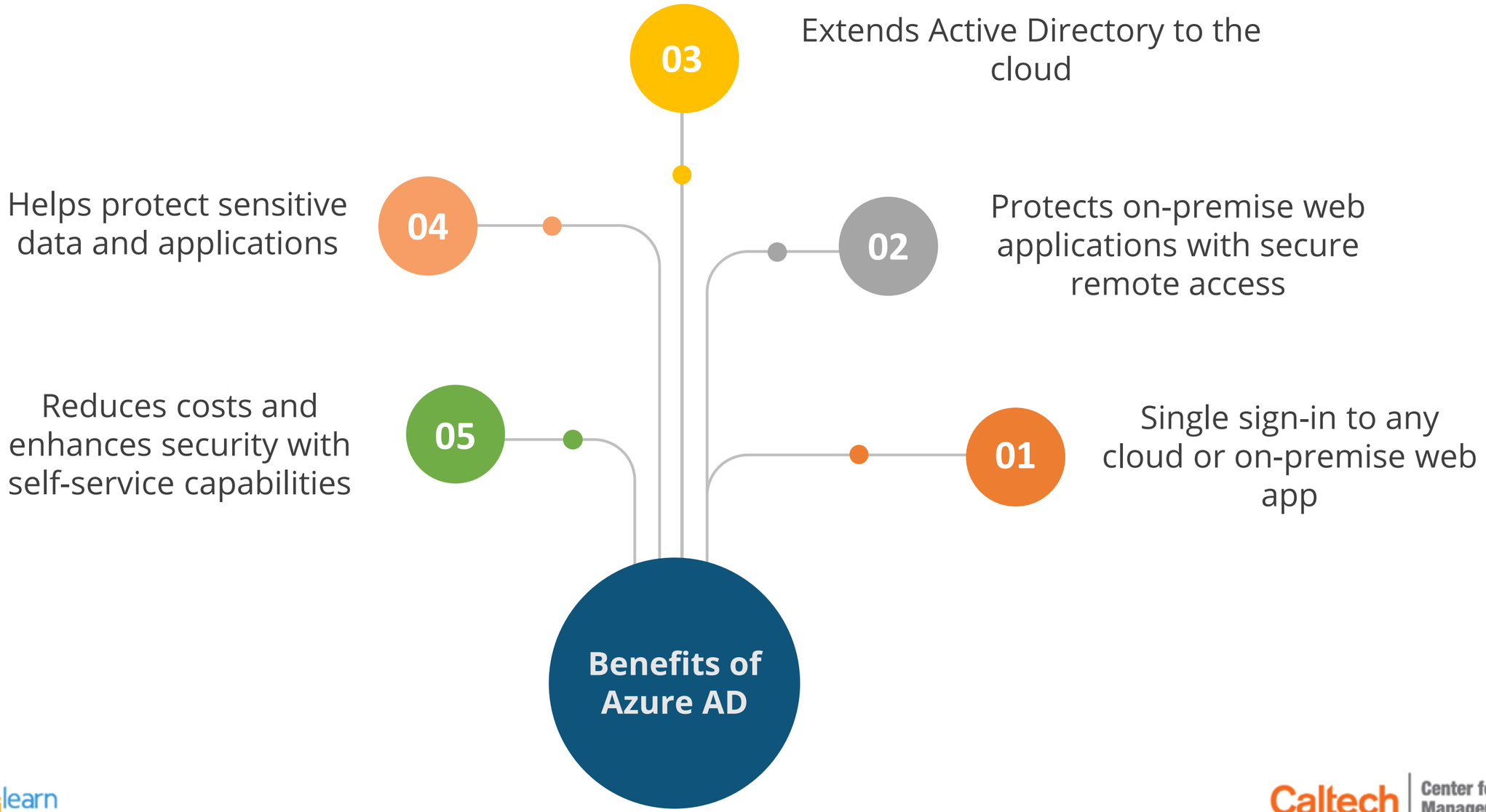
image source: https://docs.microsoft.com/en-in/

Azure Active Directory



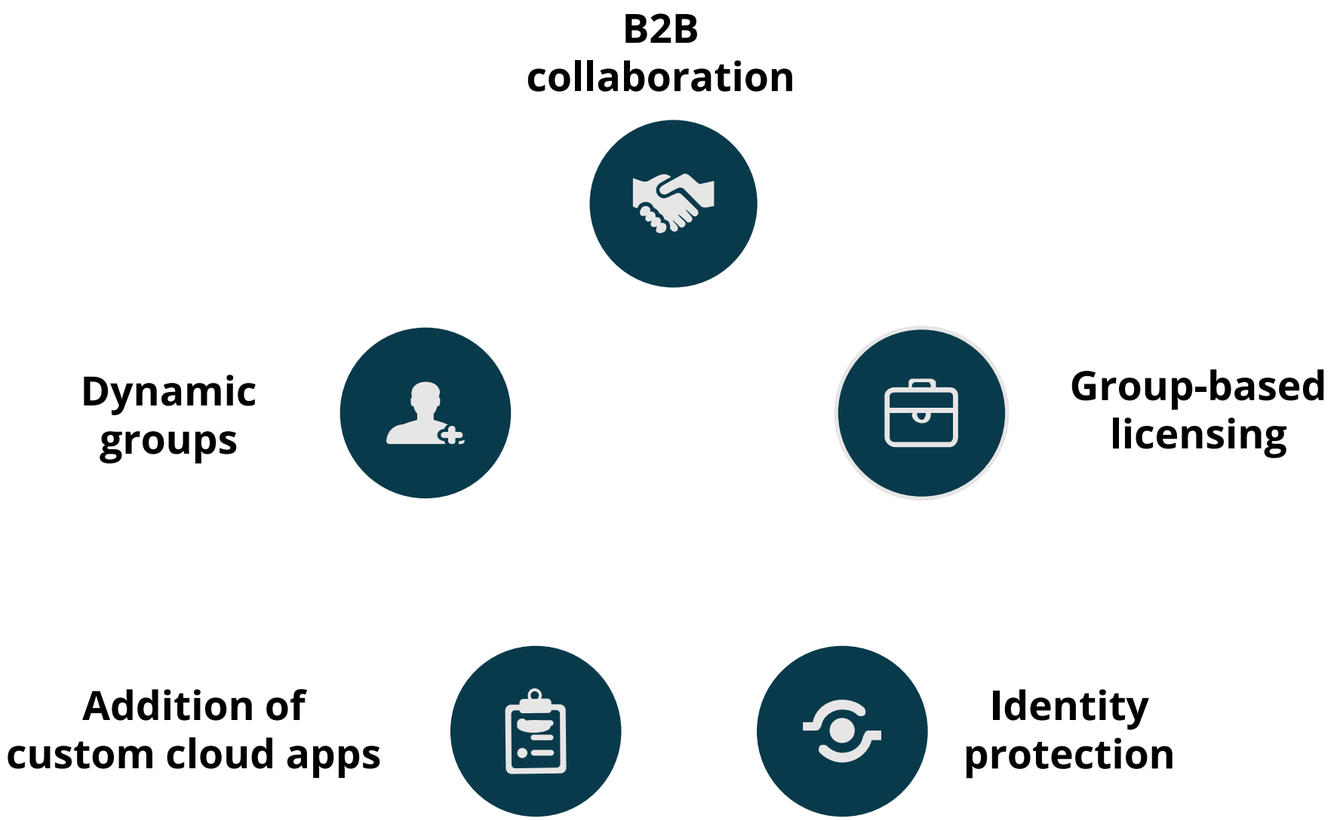
- Single sign-on access to thousands of cloud applications and resources
- Identity management capabilities and integration
- Integration with Windows Server Active Directory
- Facilitates the development of applications with a global scope

Azure Active Directory Benefits



Azure Active Directory Benefits

Some additional benefits include:



Azure Active Directory Concepts

Concepts	Description
Identity	An object that can be authenticated
Account	An identity that has data associated with it
Azure AD Account	An identity created through Azure AD or another Microsoft cloud service
Azure Tenant	A dedicated and trusted instance of Azure AD that is automatically created when an organization signs up for a Microsoft cloud service subscription
Azure AD Directory	Each Azure tenant has a dedicated and trusted Azure AD
Azure Subscription	Used to pay for Azure cloud services

AD Domain Service vs. Azure Active Directory

Azure Active Directory

- Primarily an identity solution, designed for HTTP and HTTPS communications
- Queried using the REST API over HTTP and HTTPS instead of LDAP
- Includes federation services and many third-party services (such as Facebook)

AD Domain Services (AD DS)

- Core functions responsible for managing users and computers
- Allows system administrators to organize data into logical hierarchies
- Includes security certificates, Single sign-on (SSO), LDAP, and rights management

Azure Active Directory Editions

Azure AD Free

It is designed to introduce system administrators to Azure AD.

Microsoft 365

It provides cloud-centric application access and self-service identity management solutions.

Azure AD Premium P2

It has all the features of the other editions, including advanced identity protection and privileged identity management.

Azure AD Premium P1

It is designed to help organizations with demanding identity and access management needs.

Azure Active Directory Editions

Feature	Free	Microsoft 365 Apps	Premium P1	Premium P2
Directory objects	500,000 objects	No object limit	No object limit	No object limit
Single sign-on	Unlimited	Unlimited	Unlimited	Unlimited
Core identity and access	X	X	X	X
B2B collaboration	X	X	X	X
Identity & access for O365		X	X	X
Premium features			X	X
Hybrid identities			X	X
Advanced group access			X	X
Conditional access			X	X
Identity protection				X
Identity governance				X

Recommend a Solution for Single Sign-On (SSO)

Azure Active Directory Seamless Single Sign-On (SSO)

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

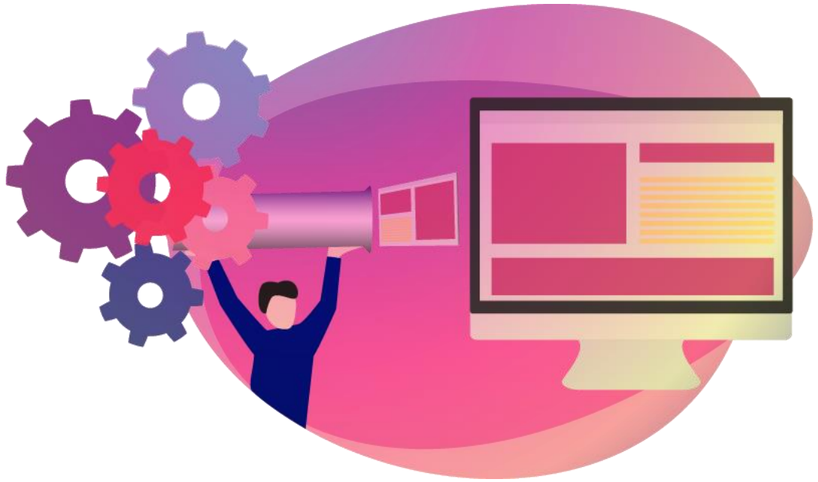
Benefits of Single Sign-On (SSO)

User experience

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

Benefits of Single Sign-On (SSO)

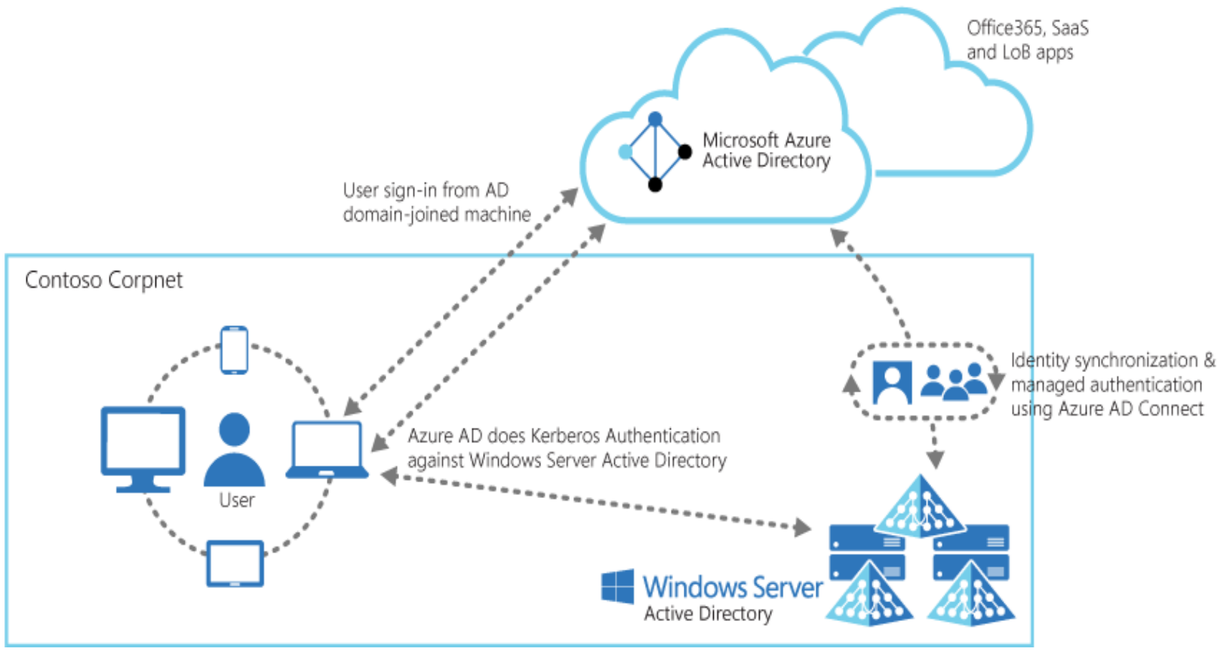
Easy deployment



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

Features of Single Sign-On (SSO)

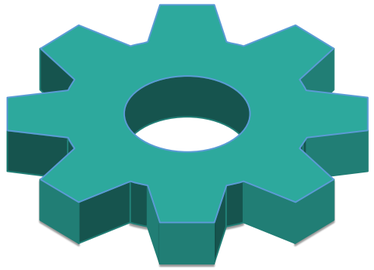
Sign-in username can be the on-premises default username, or another attribute configured in the Azure AD Connect method but cannot be used with ADFS.



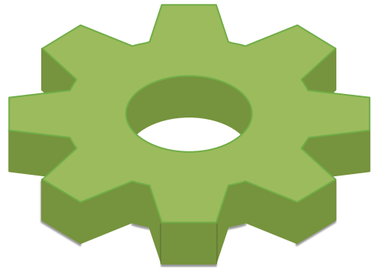
- If SSO fails, use a password at the sign-in page
- Sign in or out of other accounts
- Enabled via Azure AD Connect
- Sample list of applications included with Azure AD

Considerations: Azure AD Seamless Single Sign-On

Some considerations with respect to Azure AD Seamless SSO include:



Can be combined with Password Hash or Pass-through Authentication



Azure AD Join provides SSO for devices registered with Azure AD

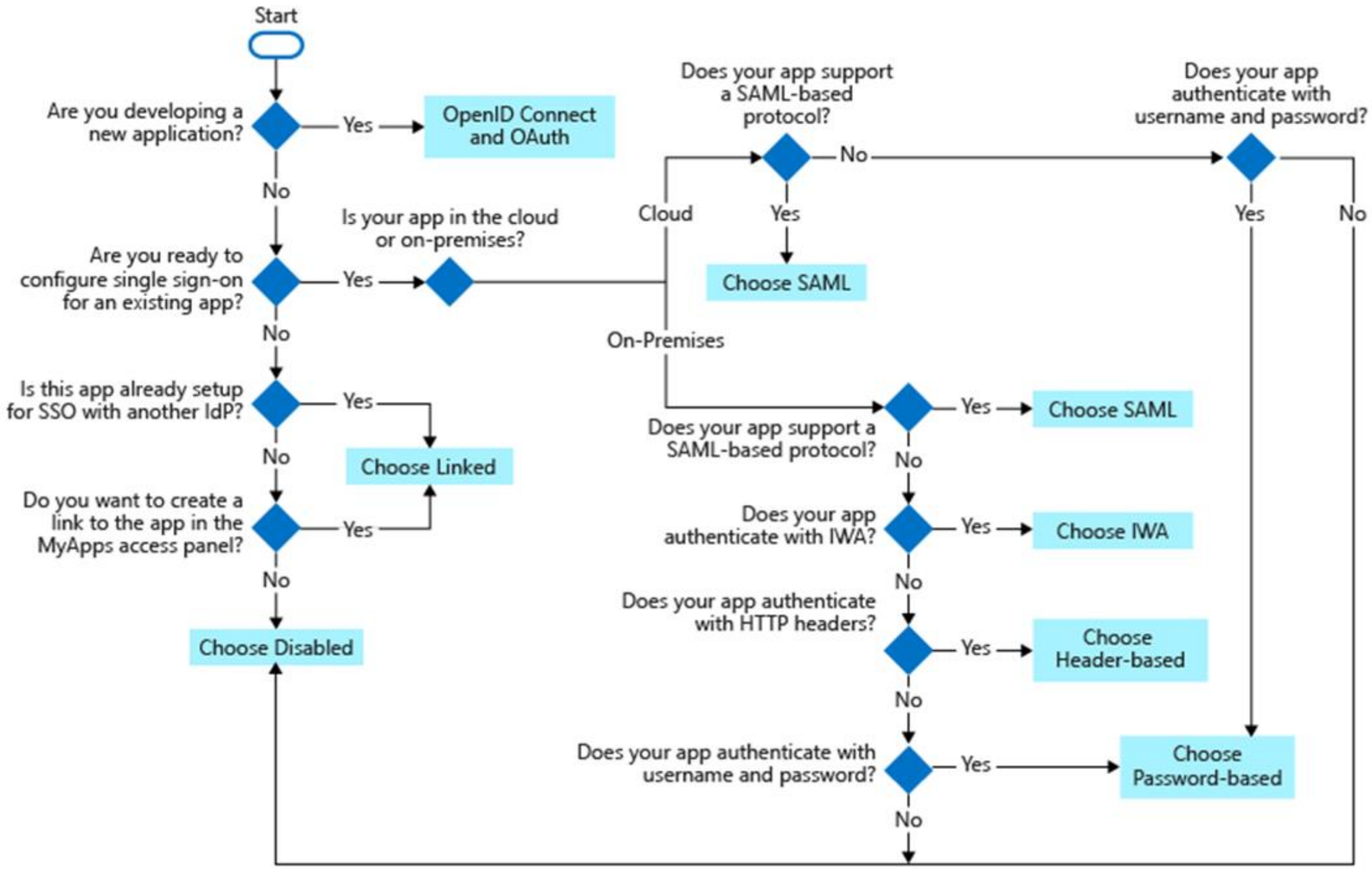
Considerations: Azure AD Seamless Single Sign-On

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

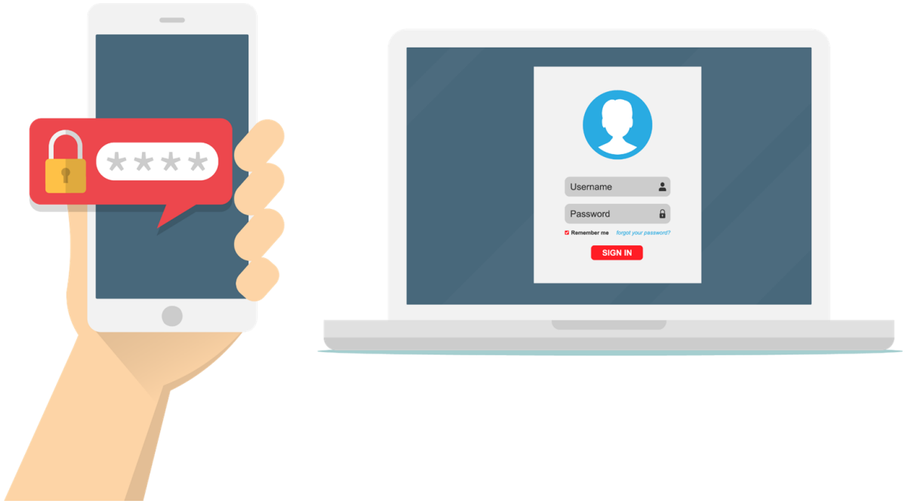
Authentication

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:

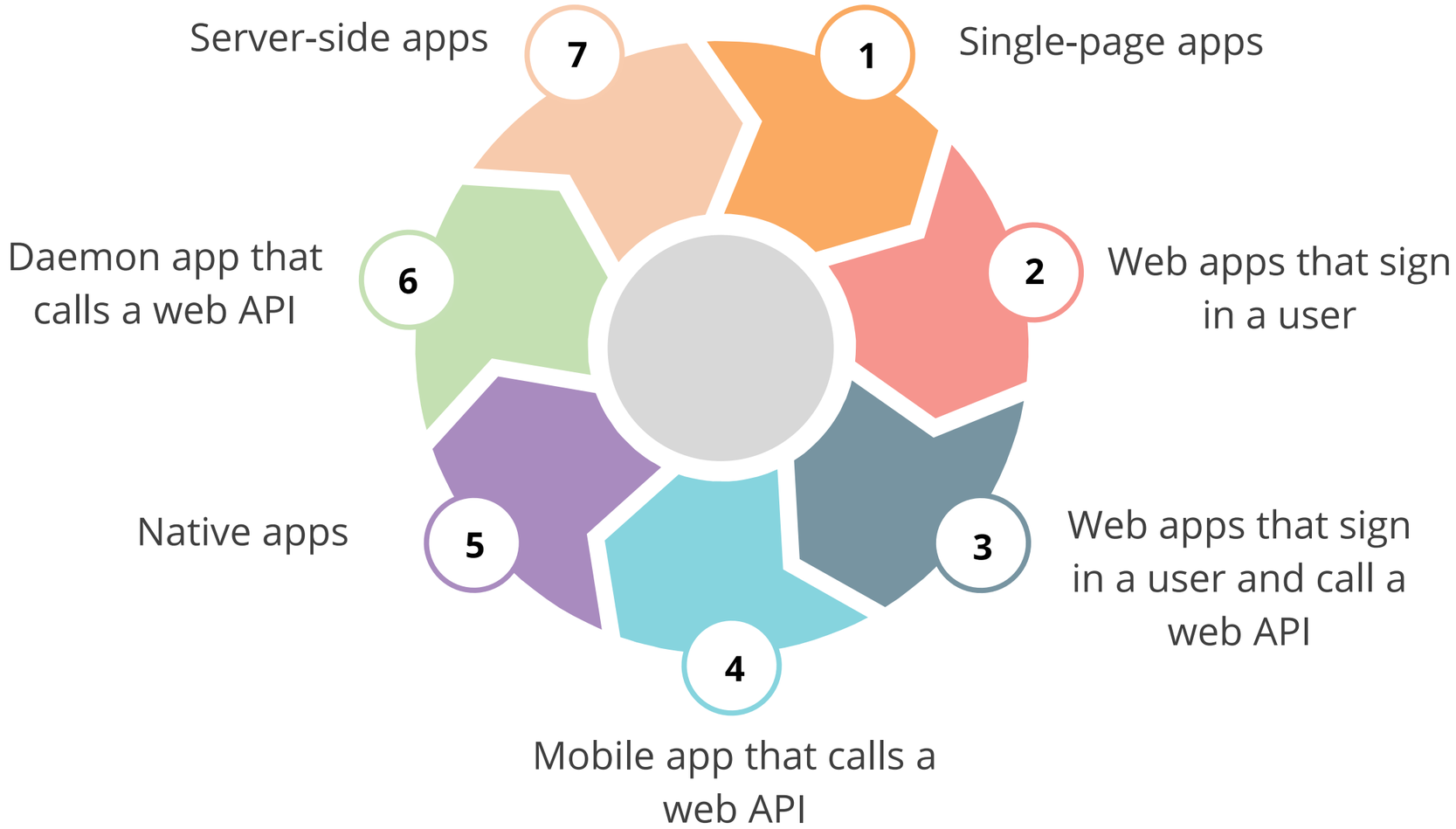
Conditional access policies that require a user to be in a specific location

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:



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.

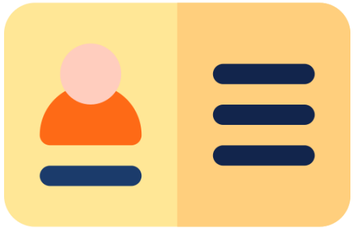
Conditional Access

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.



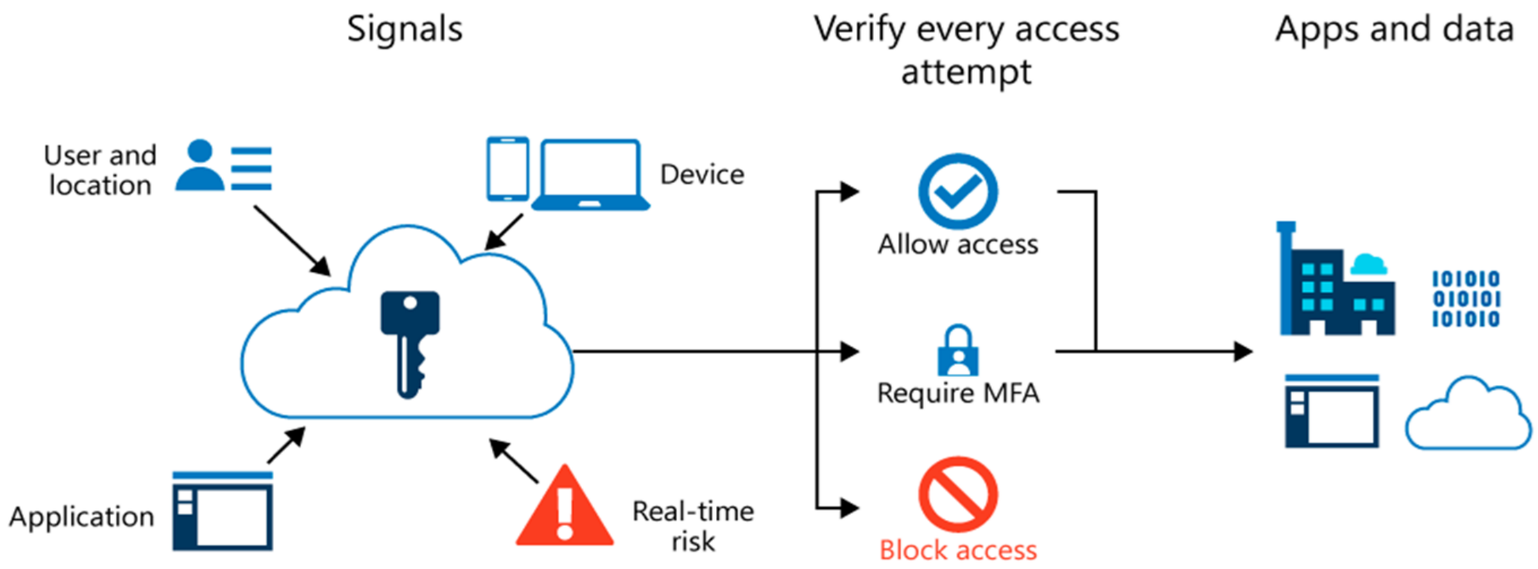
Username or password

Phone or hardware key

Biometrics like fingerprint or face scan

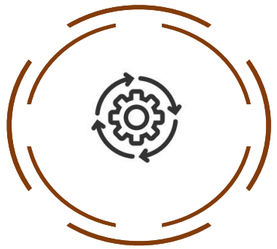
Multi-Factor Authentication (MFA)

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

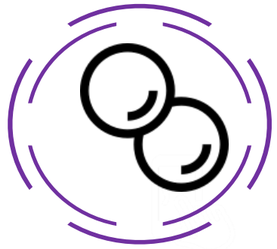


MFA Verification Methods

Verification methods for multi-factor authentication includes:



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

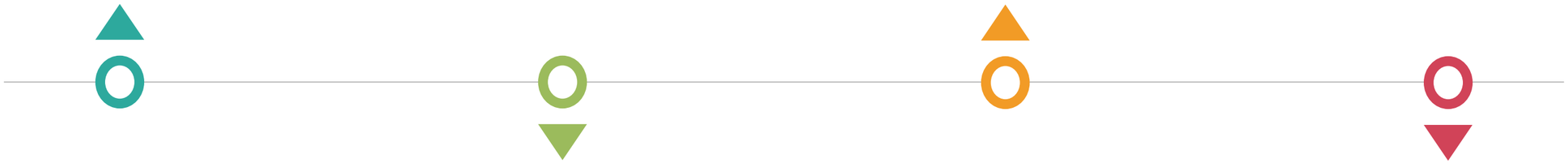
These are the reasons for multi-factor authentication:

Password complexity rules

Password expiration rules

Azure AD identity protection

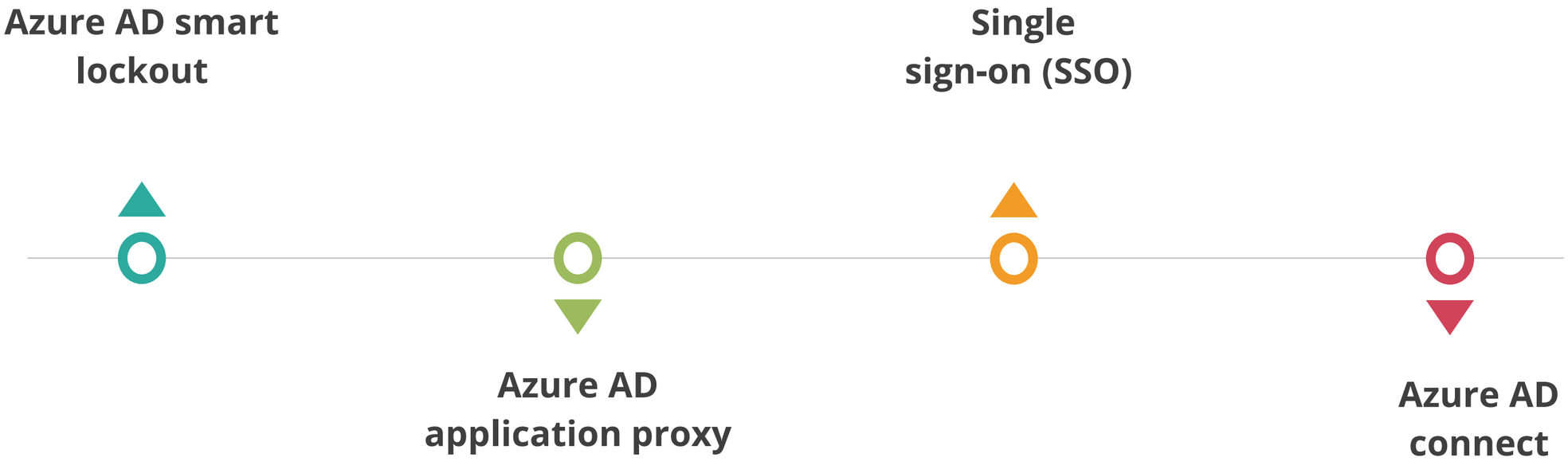
Azure AD password protection



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

Reasons for Multi-Factor Authentication

These are the reasons for multi-factor authentication:



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

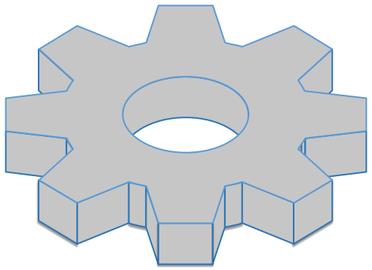
Plan for MFA Deployment

Below are the deployment considerations:

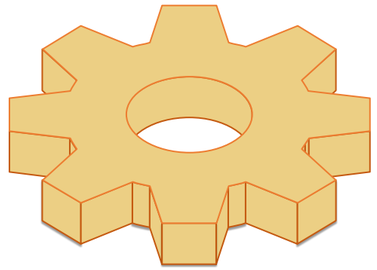
- All users, a specific user, a group member, or a role allocated
- Device platform
- State of the device
- Client applications
- Hybrid Azure AD joined device

Conditional Access and Azure Multi-Factor Authentication

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 additional verification during sign in.



Conditional access policies 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 locks 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	Shows any existing authentication providers that may have associated with an Azure account

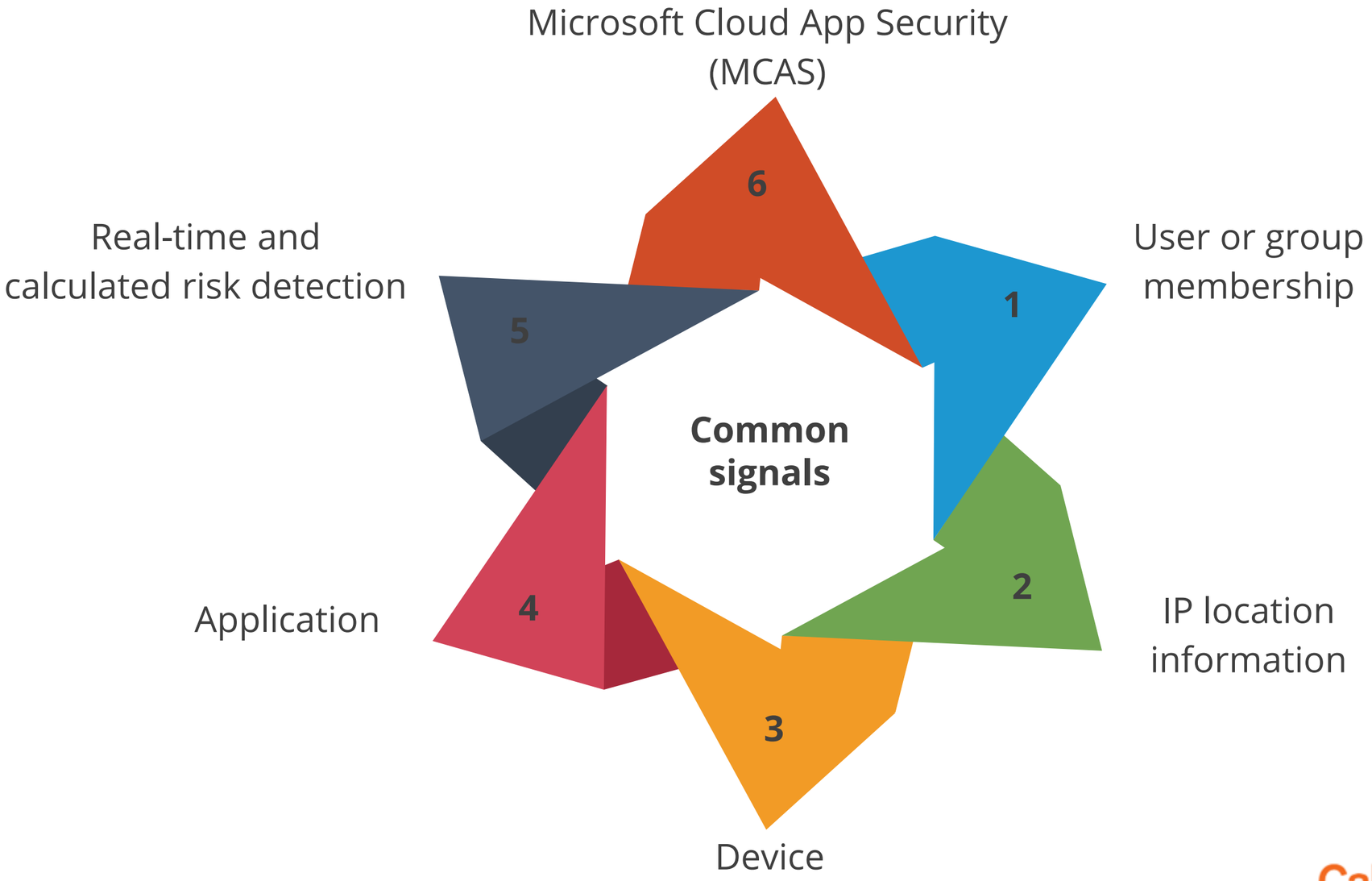
Conditional Access: Signals and Decisions

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

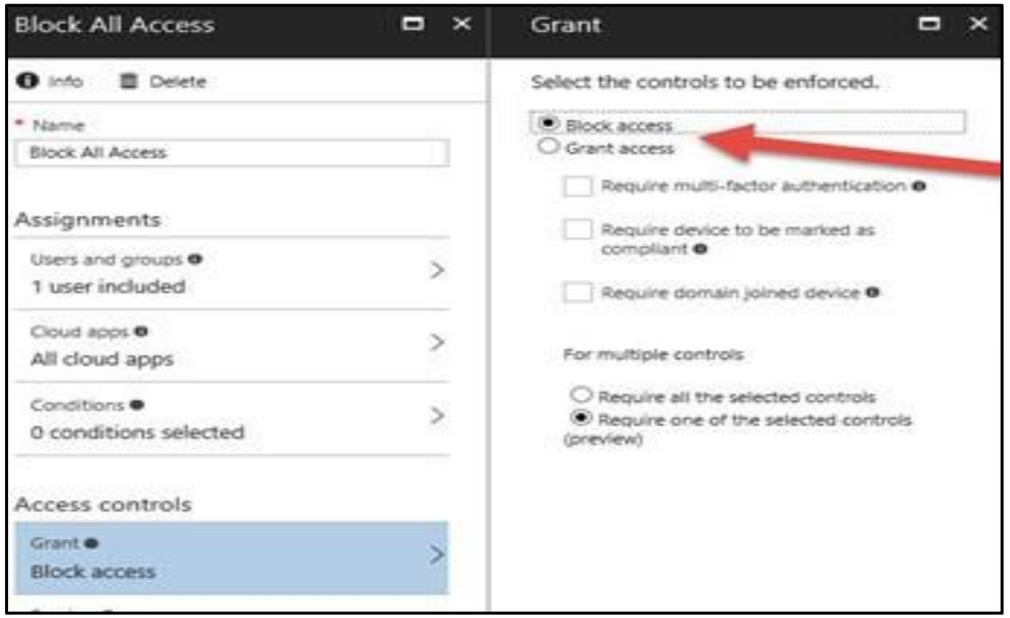
The following are the common decisions that conditional access should consider while making a policy decision:

Block access

Grant access

Block Access

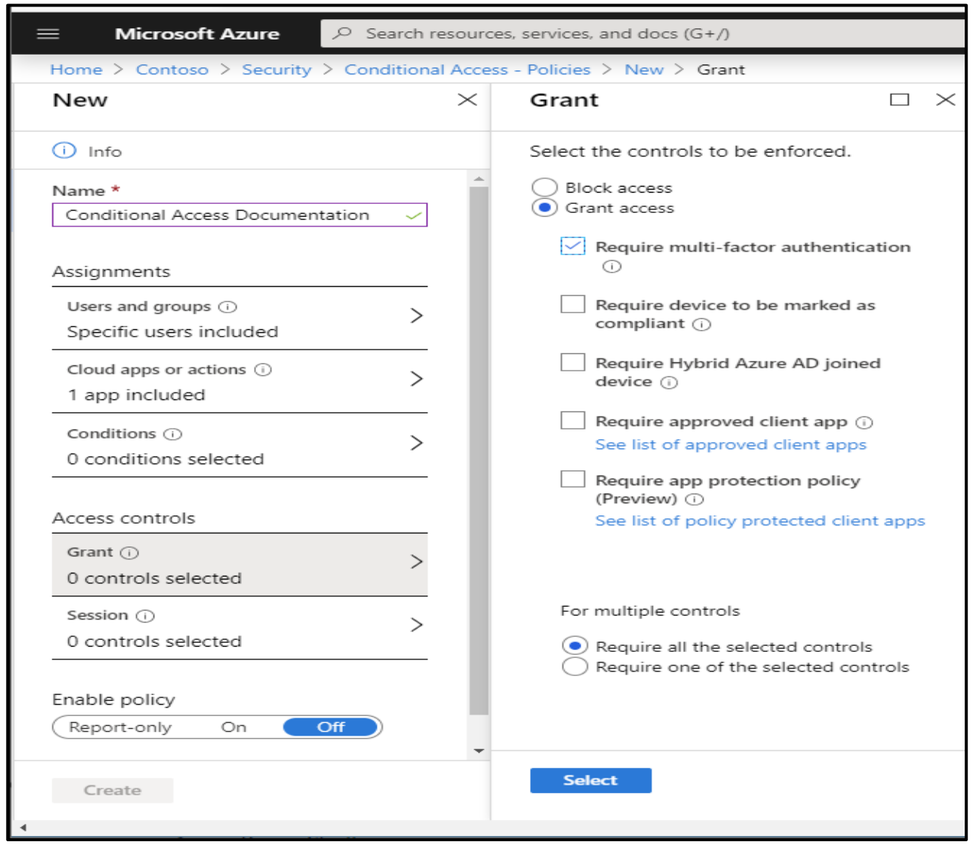
It will block access under the specified assignments.



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

Grant Access

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



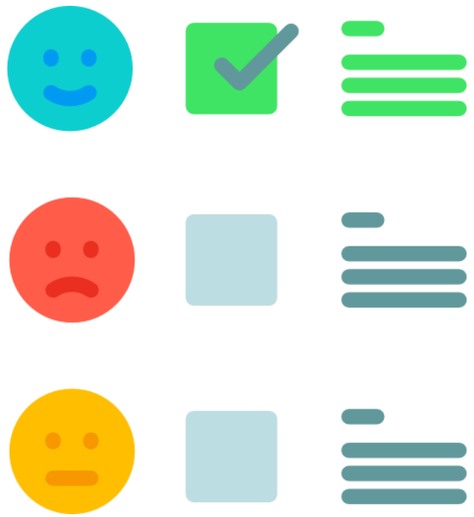
Access Review

Access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments.

The user's access can be reviewed on a regular basis to make sure only the right people have continued access.

Importance of Access Review

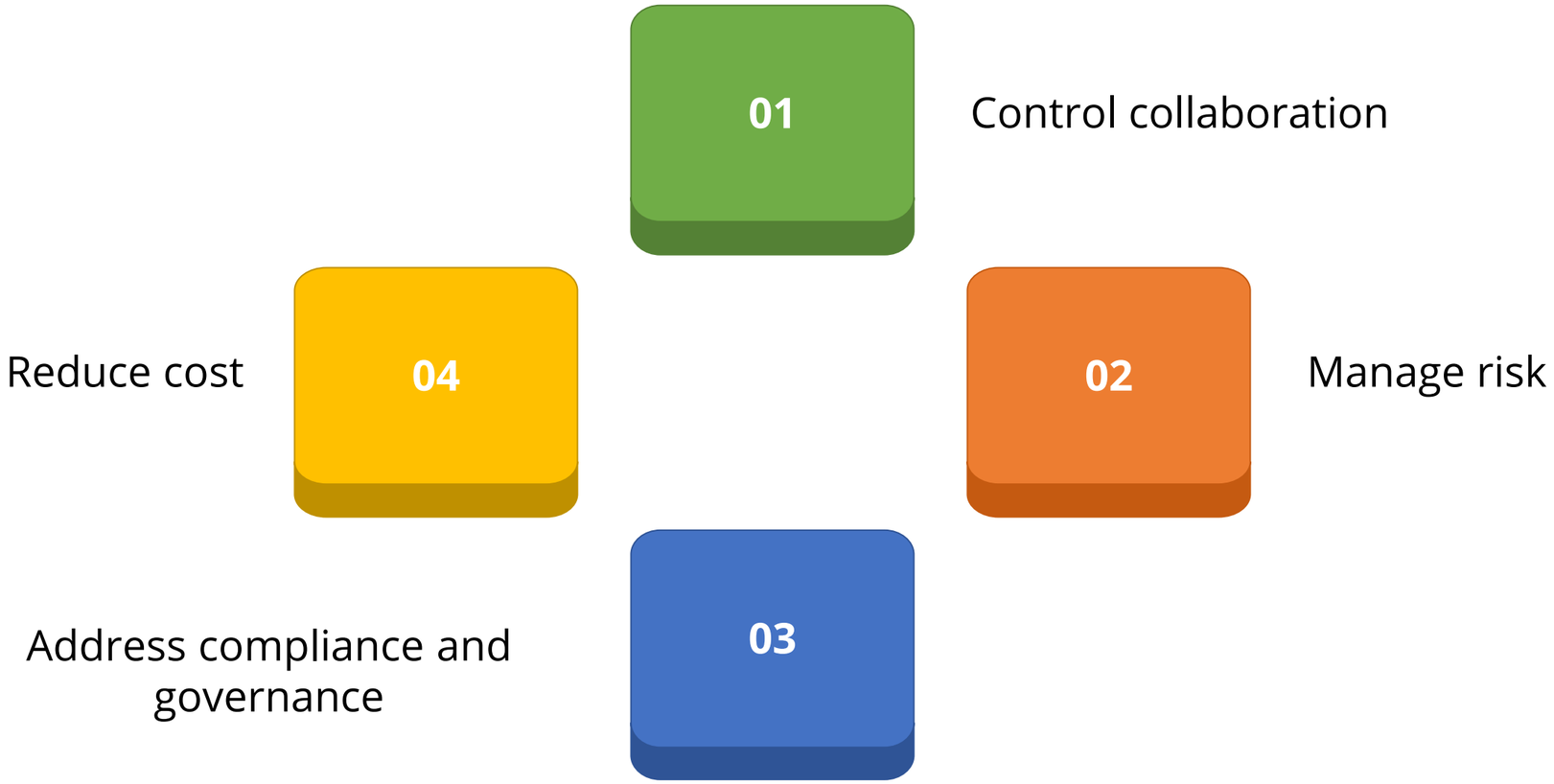
An access review is an Azure AD Identity Governance capability.



Planning the access reviews deployment is essential to make sure that users achieve the desired governance strategy.

Benefits of Access Review

The benefits of enabling access reviews are:



Benefits of Access Review

The benefits of enabling access reviews are:

Control collaboration

Access reviews allow user to manage access to all the resources. When users share and collaborate, one can be assured that the information is among authorized users only.

Manage risk

Access reviews provide a way to review access to data and applications that lowers the risk of data leakage and data spill.

Benefits of Access Review

The benefits of enabling access reviews are:

Address compliance and governance

Access reviews allow user to govern and recertify the access life cycle to groups, apps, and sites. Users can also control and track reviews for compliance or risk-sensitive applications.

Reduce cost

Access reviews are less costly than building the tools or upgrading the existing on-premises tool set.

Recommend a Solution That Includes Managed Identities

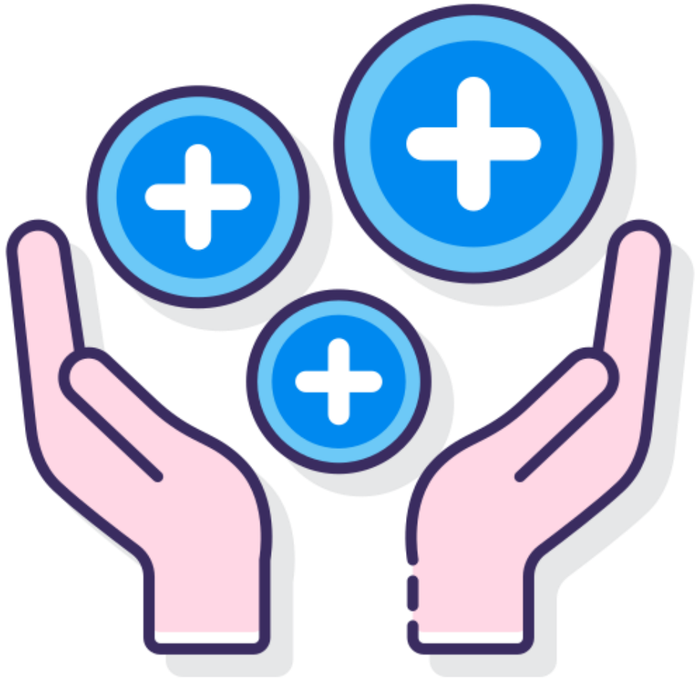
Azure Managed Identity

Azure managed identity provides identity for applications to connect with resources that support Azure AD authentication.

It combines Azure AD authentication and Azure RBAC.

Azure Managed Identity

The benefits of Azure managed identity are:



- No need to manage credentials
- Any resource can be authenticated
- No additional cost
- No need for rotating credentials or certificates

Azure Managed Identity Terminologies

Managed identities involve the use of these terms:

Client ID

A unique ID linked to the Azure AD application and service principal

Object ID

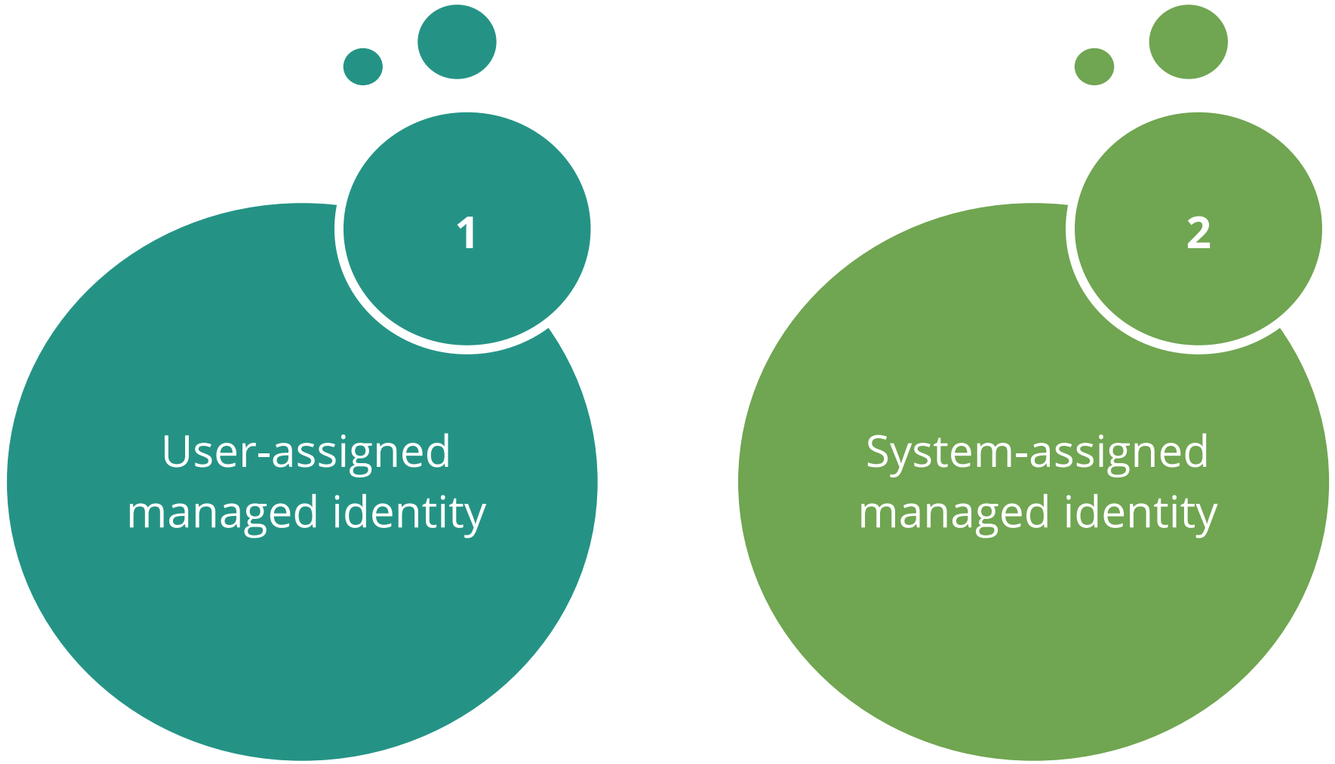
The service principal object of the managed identity

Azure Instance Metadata Service

A REST API that's enabled when Azure Resource Manager provisions a VM.

Types of Managed Identity

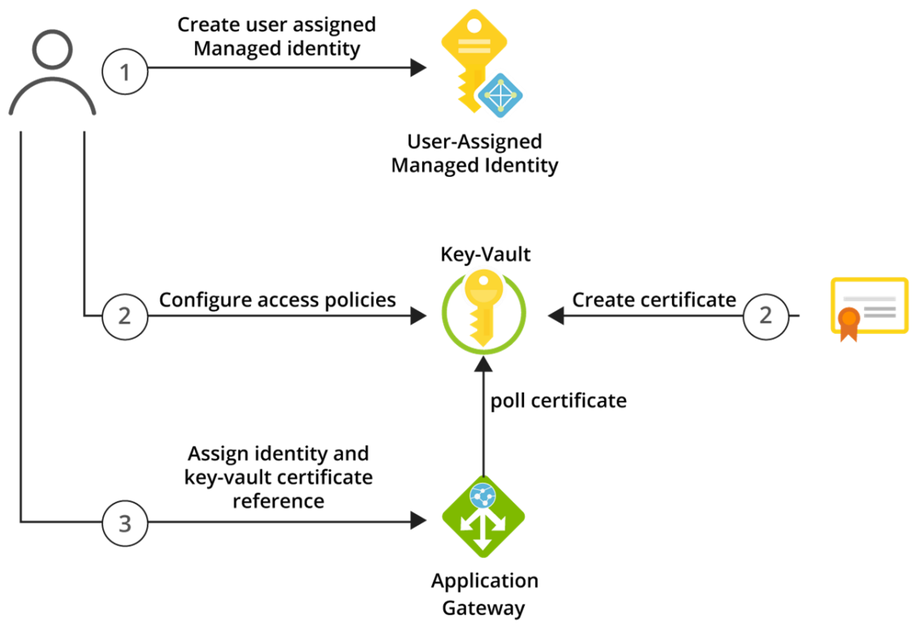
There are two types of managed identities:



User-Assigned Managed Identity

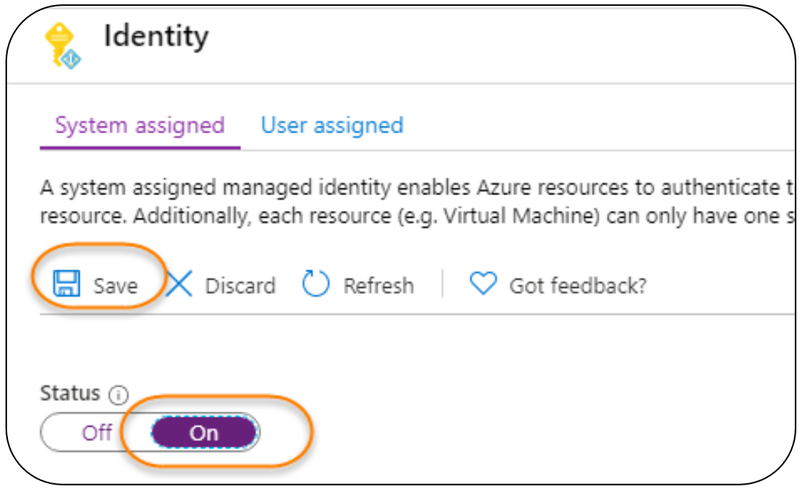
Azure creates a service principal just as it does for a system-assigned identity.

It is created as a standalone Azure resource.



System-Assigned Managed Identity

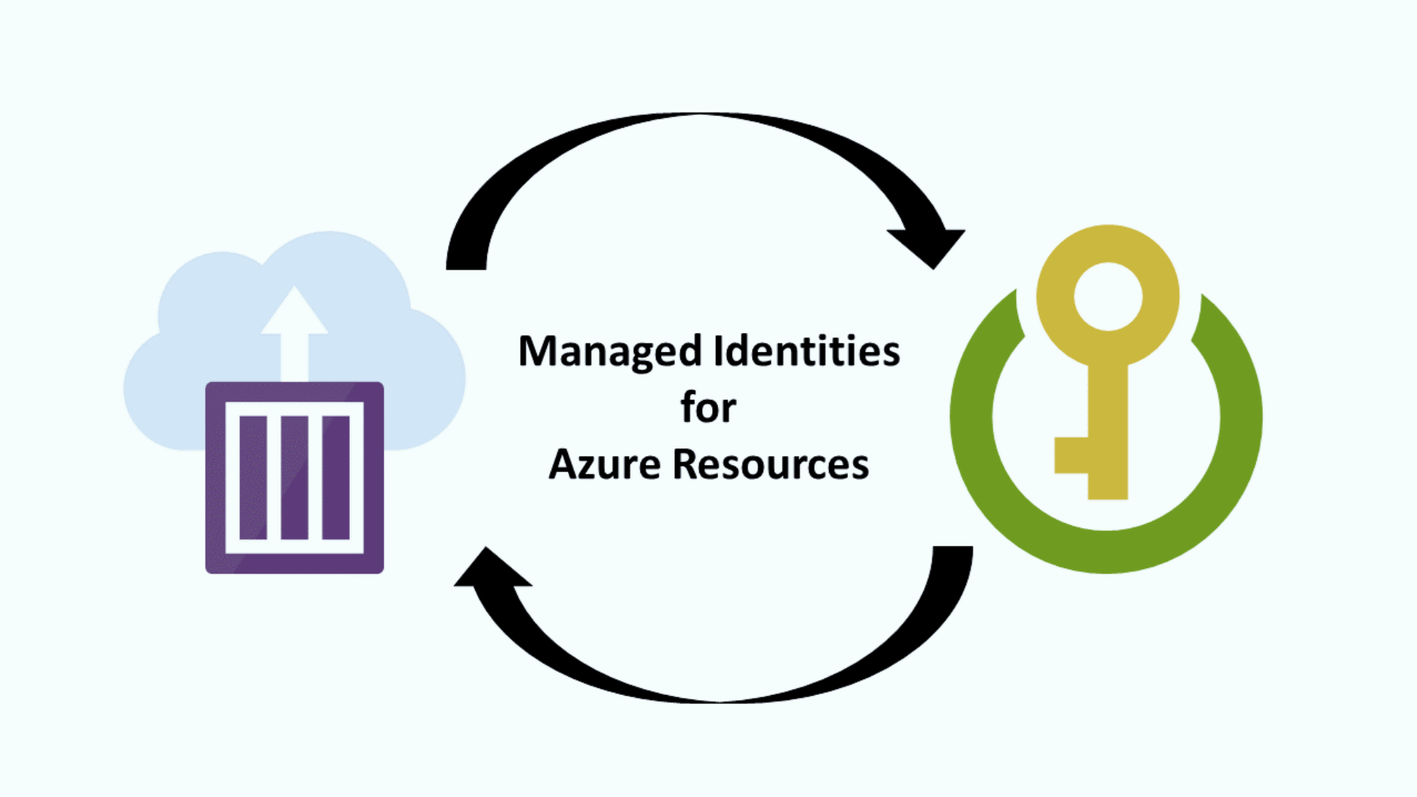
When a user enables the identity, Azure creates a service principal through Azure Resource Manager.



System-assigned managed identity is enabled on an Azure service instance, such as a VM.

Managed Identity for Azure Resources

It manages the credentials to authenticate cloud services when building cloud applications.



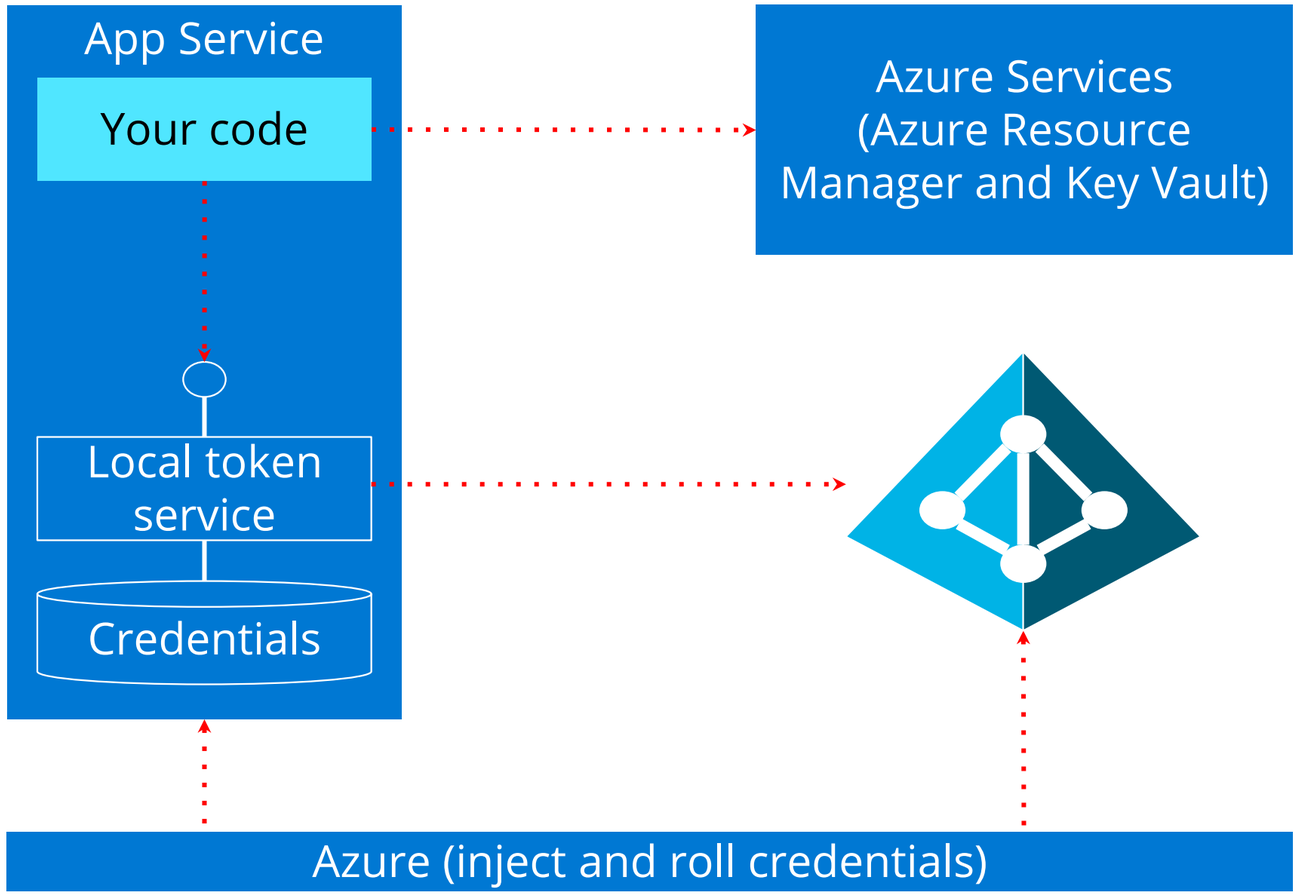
Managed Identity for Azure Resources

These are the advantages of managed identity when used for Azure resources:

- Keeps credentials out of code
- Uses a local MSI endpoint to get access tokens from Azure AD
- Manages the identity in Azure AD for Azure resources automatically
- Offers direct authentication with services or retrieval of credentials from the Azure Key Vault

Workflow of Managed Identity

The following diagram shows the internal workflow of managed identity:

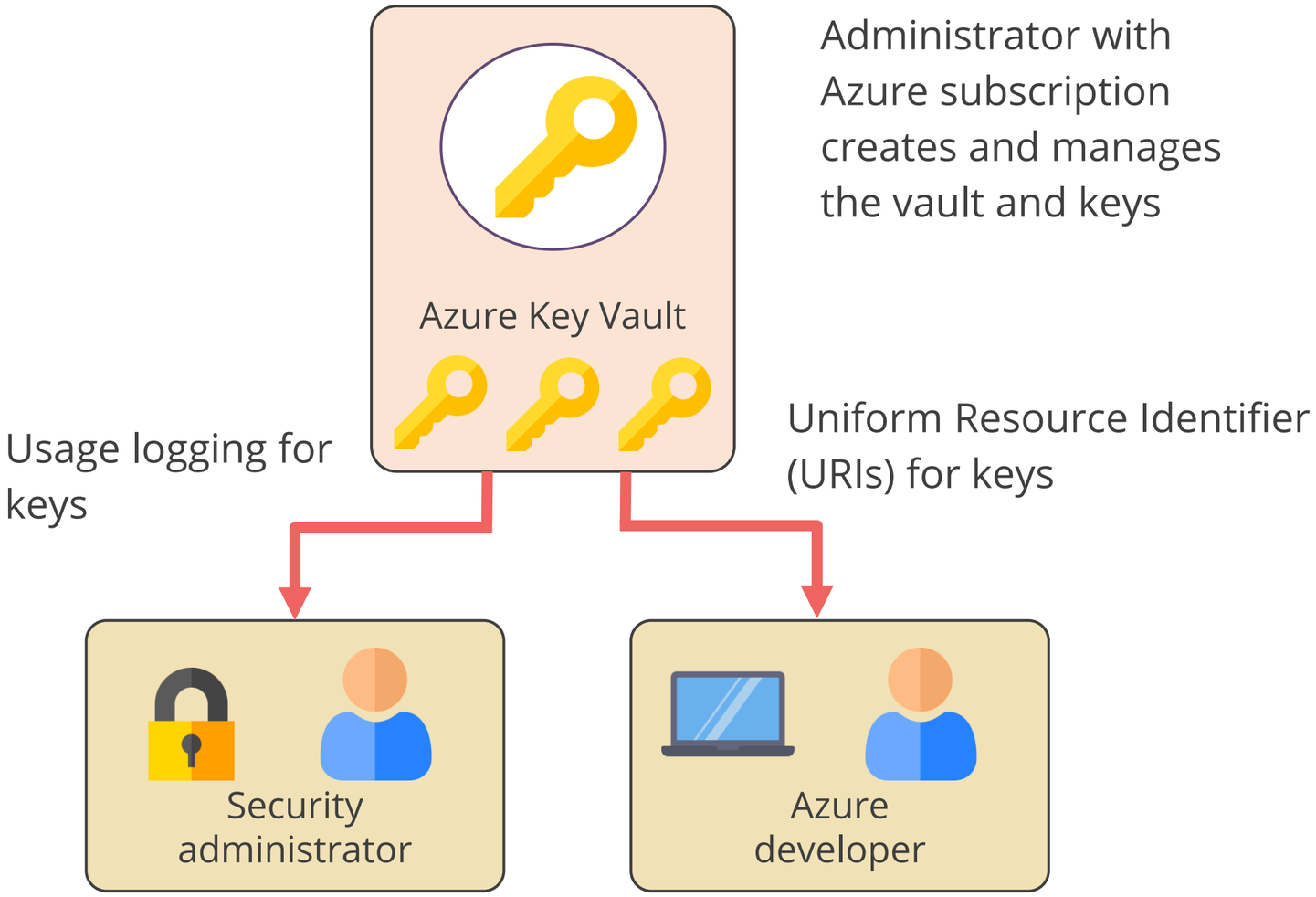


Recommend a Solution That Includes Key Vault

Azure Key Vault

Azure Key Vault is a centralized cloud service for storing application secrets such as encryption keys, certificates, and server-side tokens.

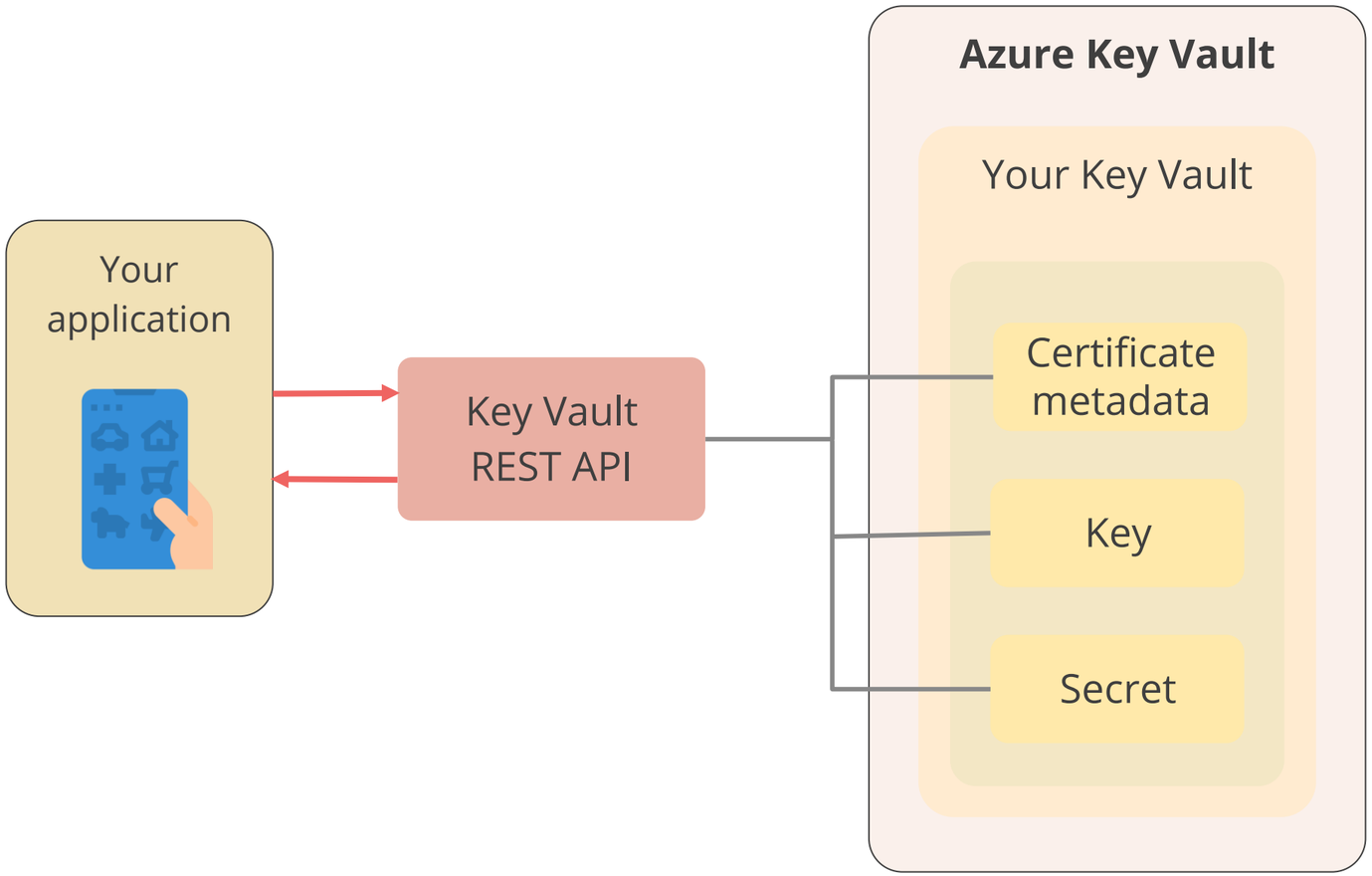
Azure Key Vault



Azure Key Vault offerings:

- Secrets management
- Key management
- Certificate management
- Secrets storage

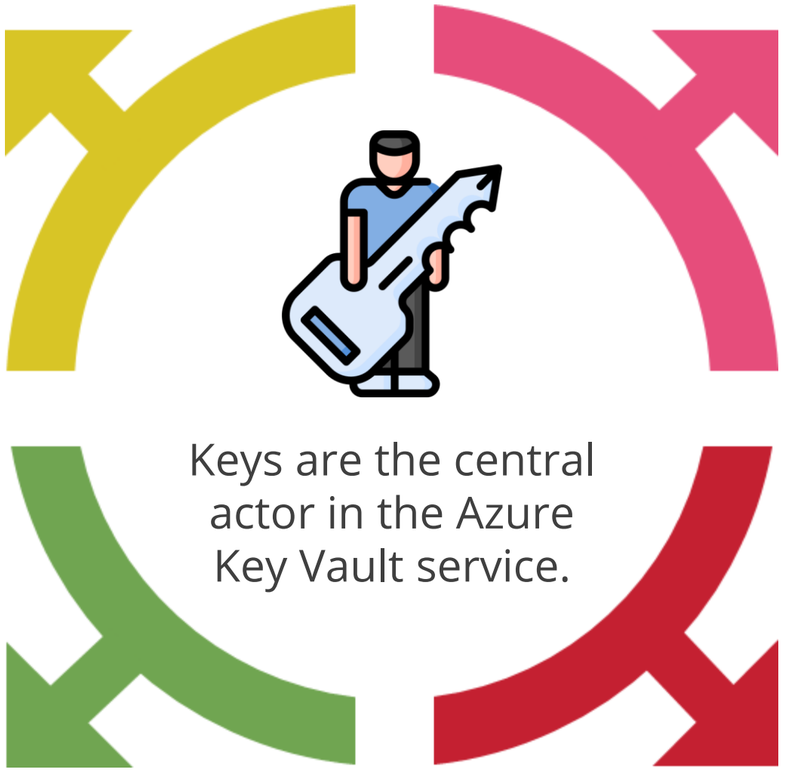
Azure Key Vault Benefits



- Centralize application secrets
- Securely store secrets and keys
- Monitor access and use
- Simplified administration of application secrets
- Integrate with other Azure services

Keys

Keys can be single instanced (only one key exists)



Keys are the central actor in the Azure Key Vault service.

Keys are cryptographic assets that serve a specific purpose

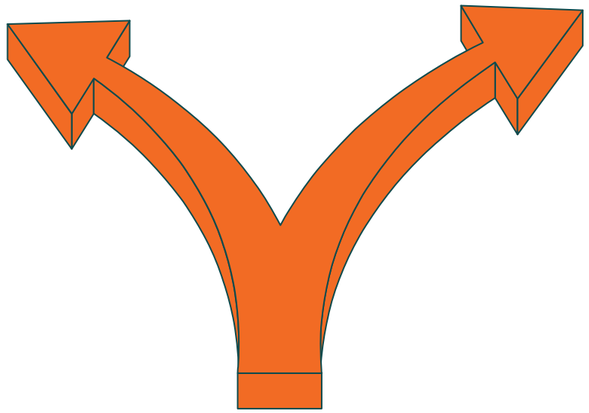
Keys can be versioned (mix of primary and secondary keys)

Keys are never directly accessible to applications

Keys

Hardware Protected Keys

Supports using HSMs that provide a hardened, tamper-resistant environment for cryptographic processing and key generation



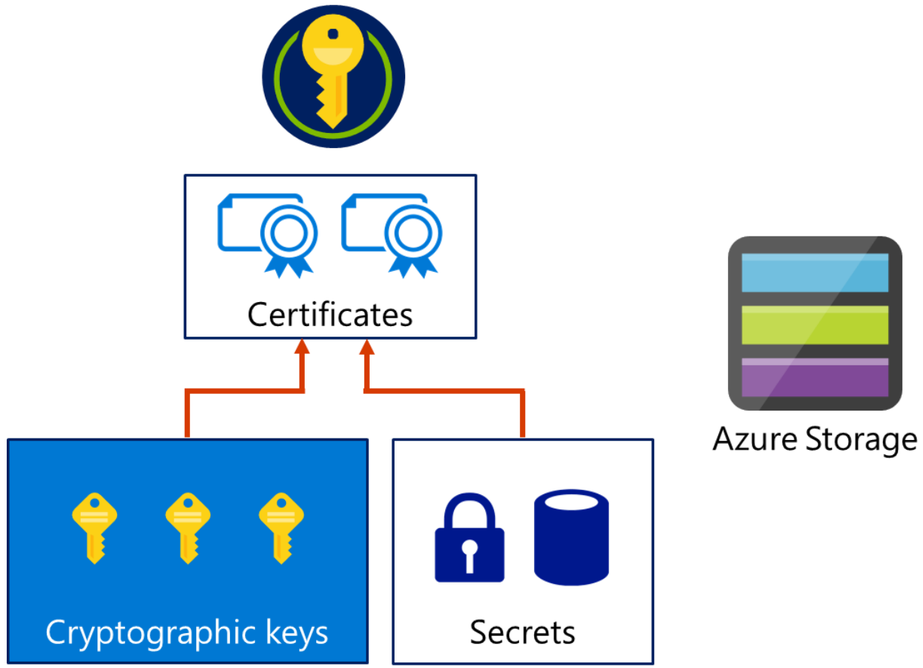
Software Protected Keys

Supports using software-based Rivest–Shamir–Adleman (RSA) and Elliptic curve cryptography (ECC) algorithms

Two types of keys in Key Vault

Secrets

Secrets are small (less than 10K) data blobs protected by HSM-generated key created with the Key Vault.



Types of Keys

Cryptographic keys

Key Vault supports multiple key types and algorithms and using hardware security modules (HSMs) for high-value keys.

Certificates

Key Vault supports certificates, which are built on top of keys and secrets and add an automated renewal feature.

Secrets

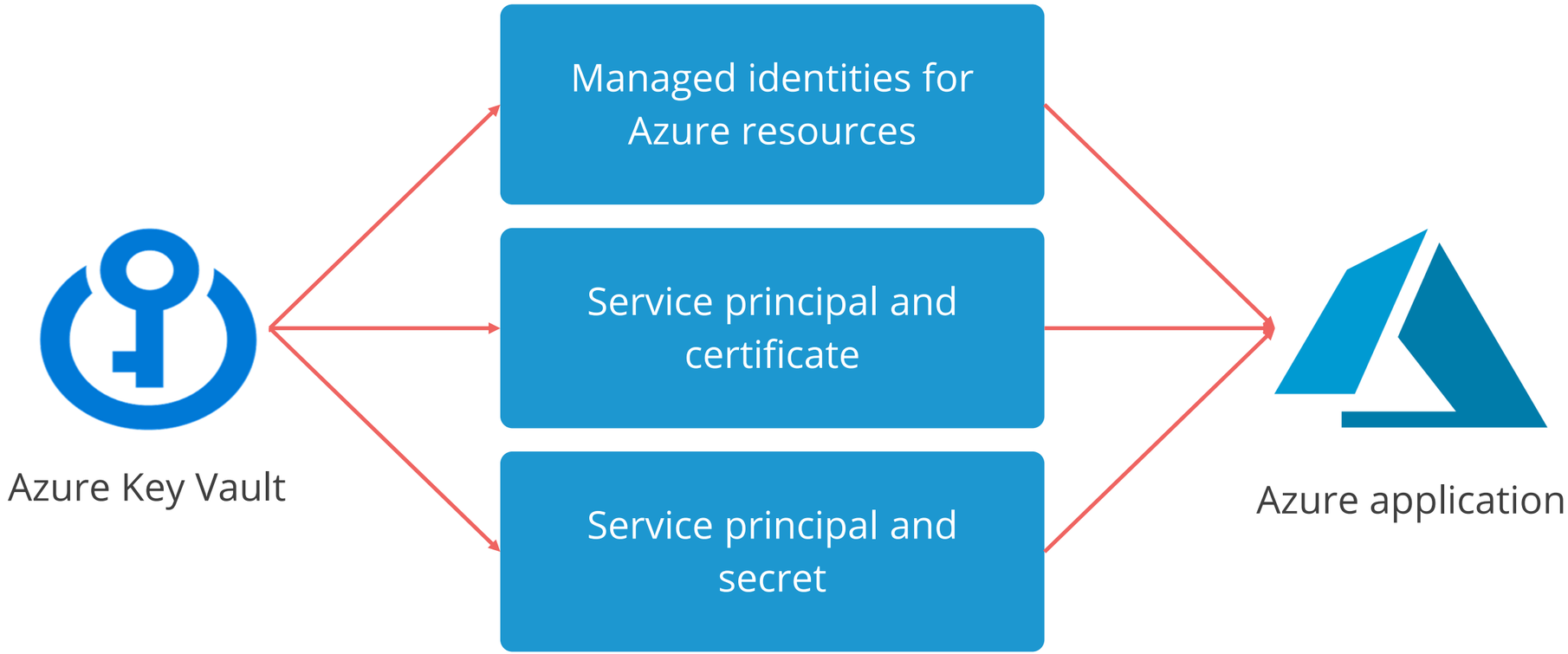
Key Vault provides secure storage of secrets, such as passwords and database connection strings.

Azure storage

Key Vault can manage the keys of an Azure Storage account. Internally, Key Vault can list (sync) keys with an Azure Storage Account and regenerate (rotate) the keys periodically.

Key Vault Authentication and Authorization

Illustration of authentication and authorization between the Azure Key Vault and Azure application:



Key Vault Authentication and Authorization

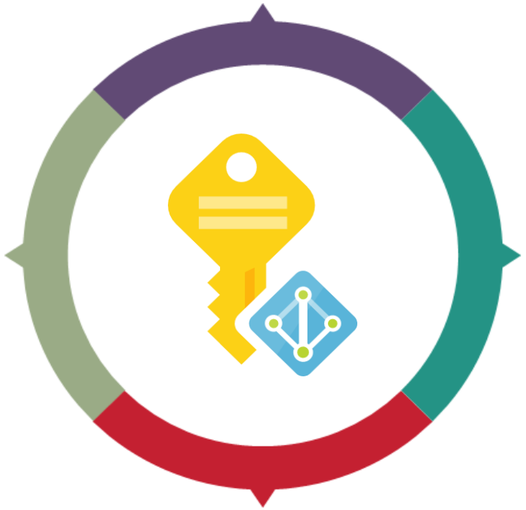
The procedure for accessing the Key Vault:

Authenticate

Azure Active Directory to authenticate users and applications

Read and write data in the Azure Key Vault

Uses a separate Key Vault access policy



Restrict network access

Services in the network can access the vault

Authorize

Role-based access control (RBAC)

Key Vault Availability and Redundancy

Availability and redundancy are distinct features in Azure Key Vault:

01 Key vault features multiple layers of redundancy

02 Contents of the Key Vault are replicated within the region and to a secondary region at least 150 miles away

03 If components within the Key Vault service fail, alternate components within the region step in

Key Vault Best Practices

The best practices of the Key Vault:

- Control what users can access
- Store certificates in the Key Vault

- Grant access to a specific scope
- Ensure that you can recover a deleted Key Vault or Key Vault objects

Assisted Practice

Azure Key Vault

Duration: 10 Min.

Problem Statement:

As an Azure Architect, you've been asked to provide your organization with an Azure security solution for storing application secrets such as tokens, passwords, certificates, API keys, and other secrets such as certificates, keys, and secret management.

Assisted Practice: Guidelines

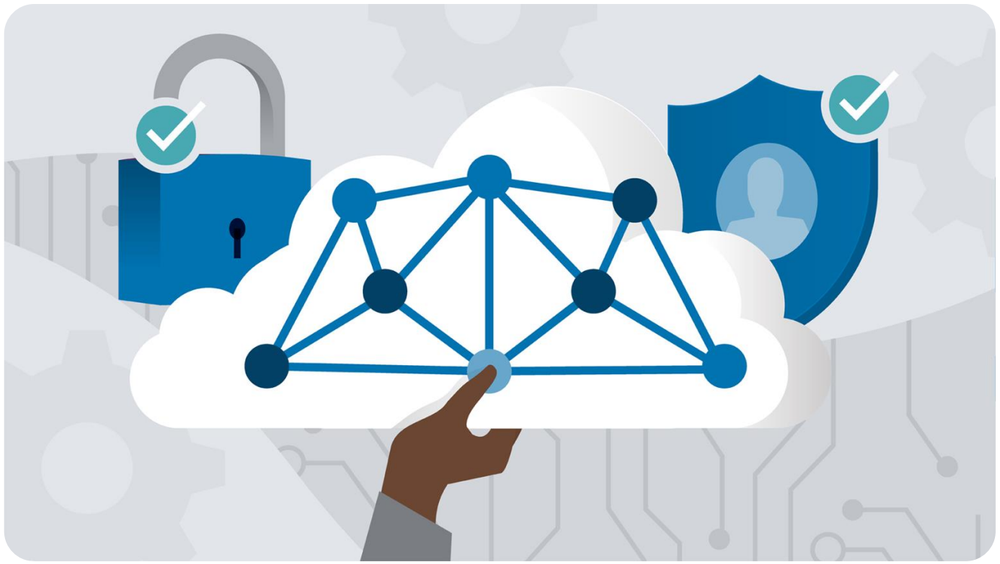
Steps to create an Azure key vault are:

1. Login to your Azure portal
2. Search for and select Key Vault
3. Select Create on key vault page
4. Provide the details and create an Azure key vault

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:

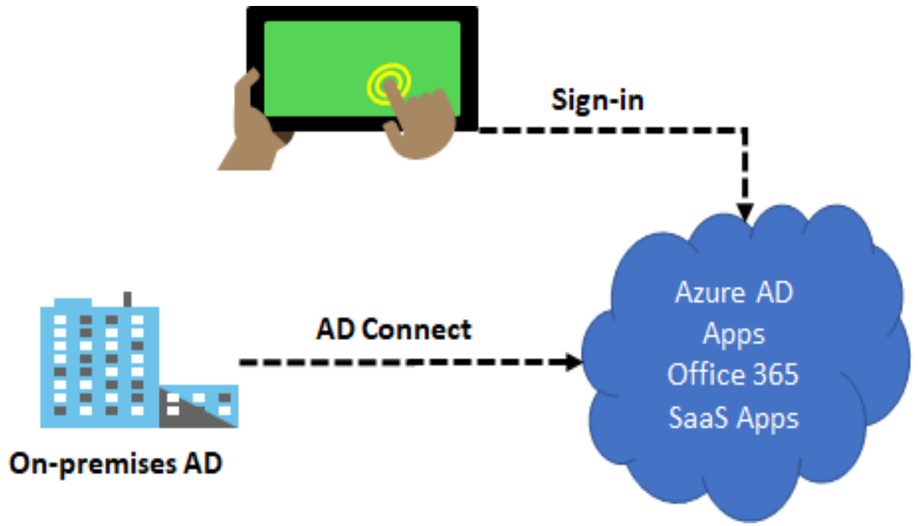
Password hash synchronization (PHS)

Pass-through authentication (PTA)

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.

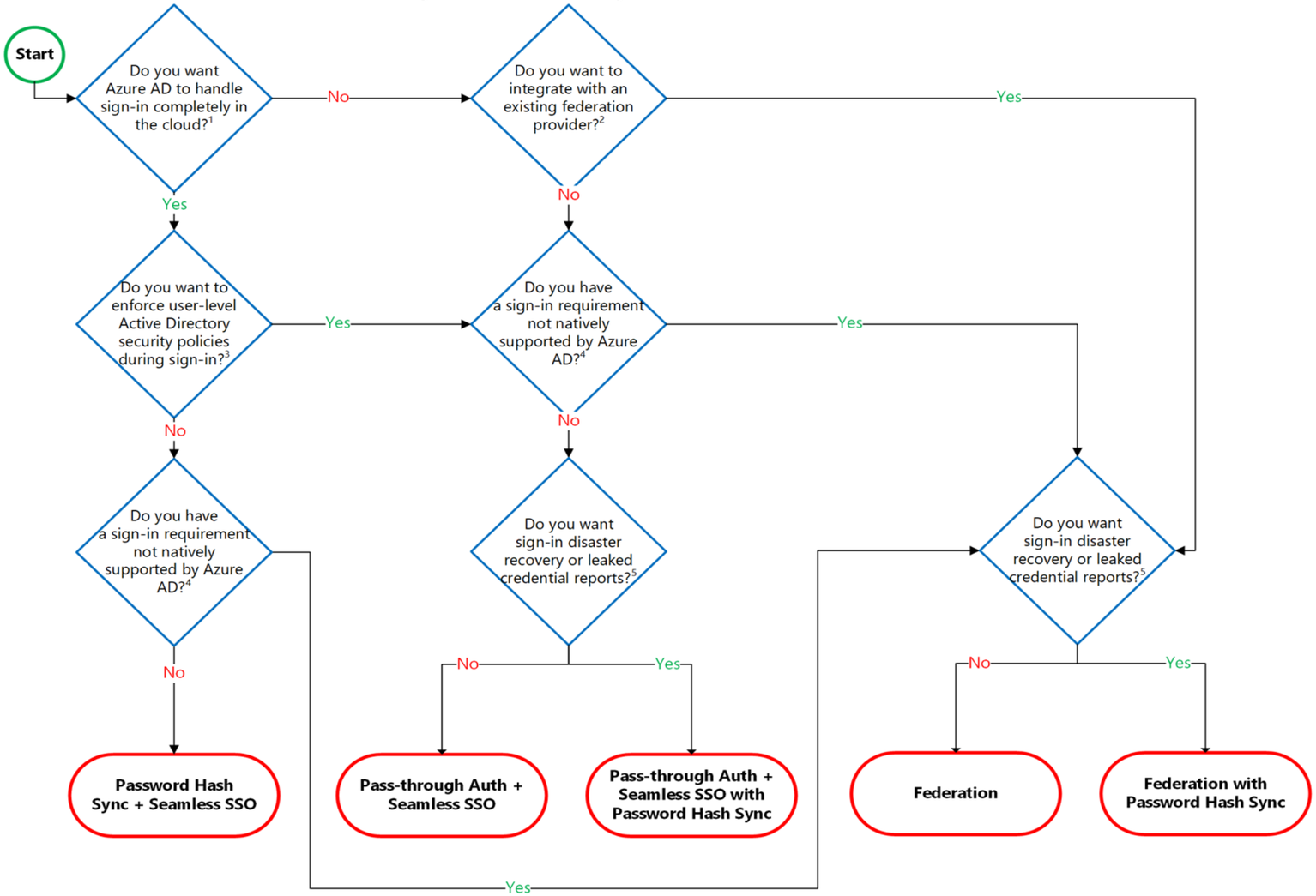
Common Scenarios

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:

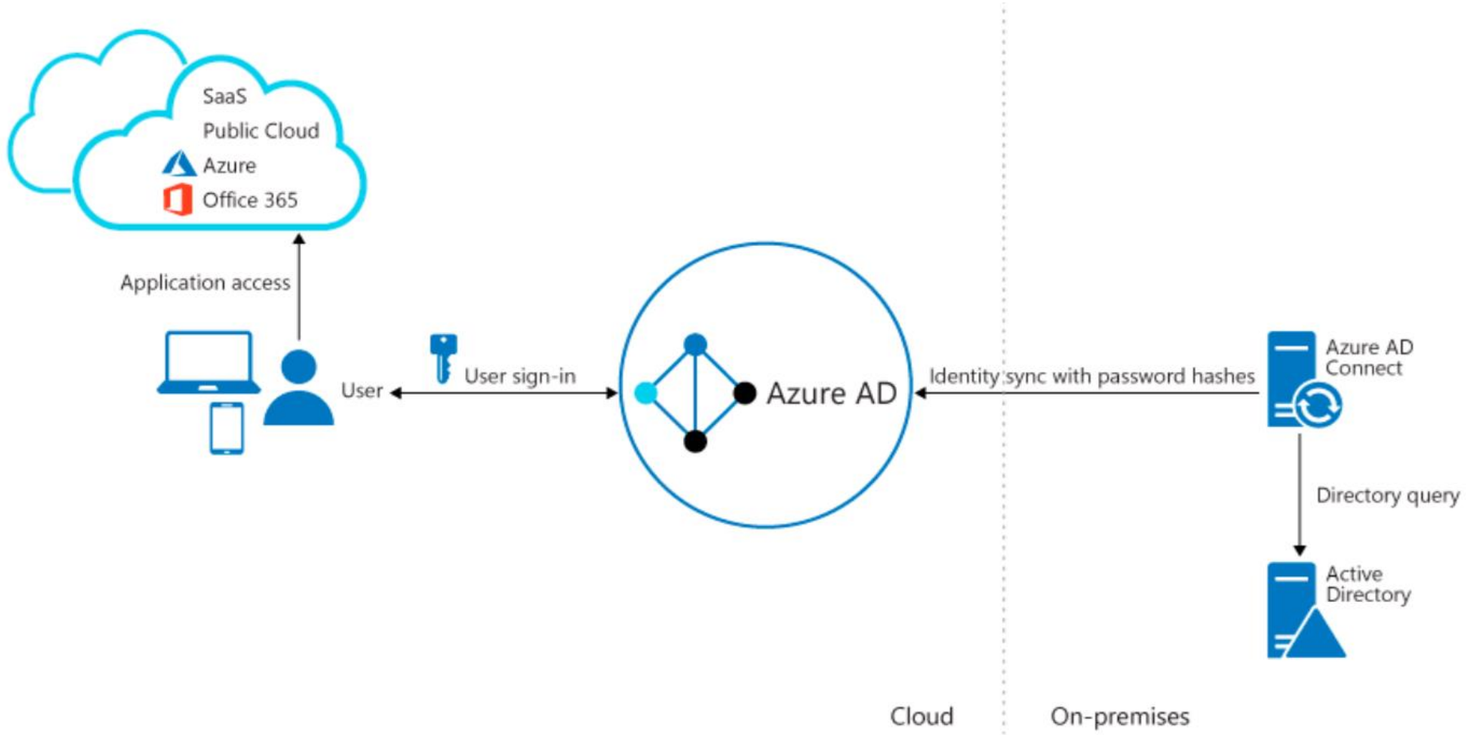


Source: https://docs.microsoft.com/

Authentication Architecture

Azure AD Hybrid identity with password hash sync

Simplicity of a password hash synchronization solution

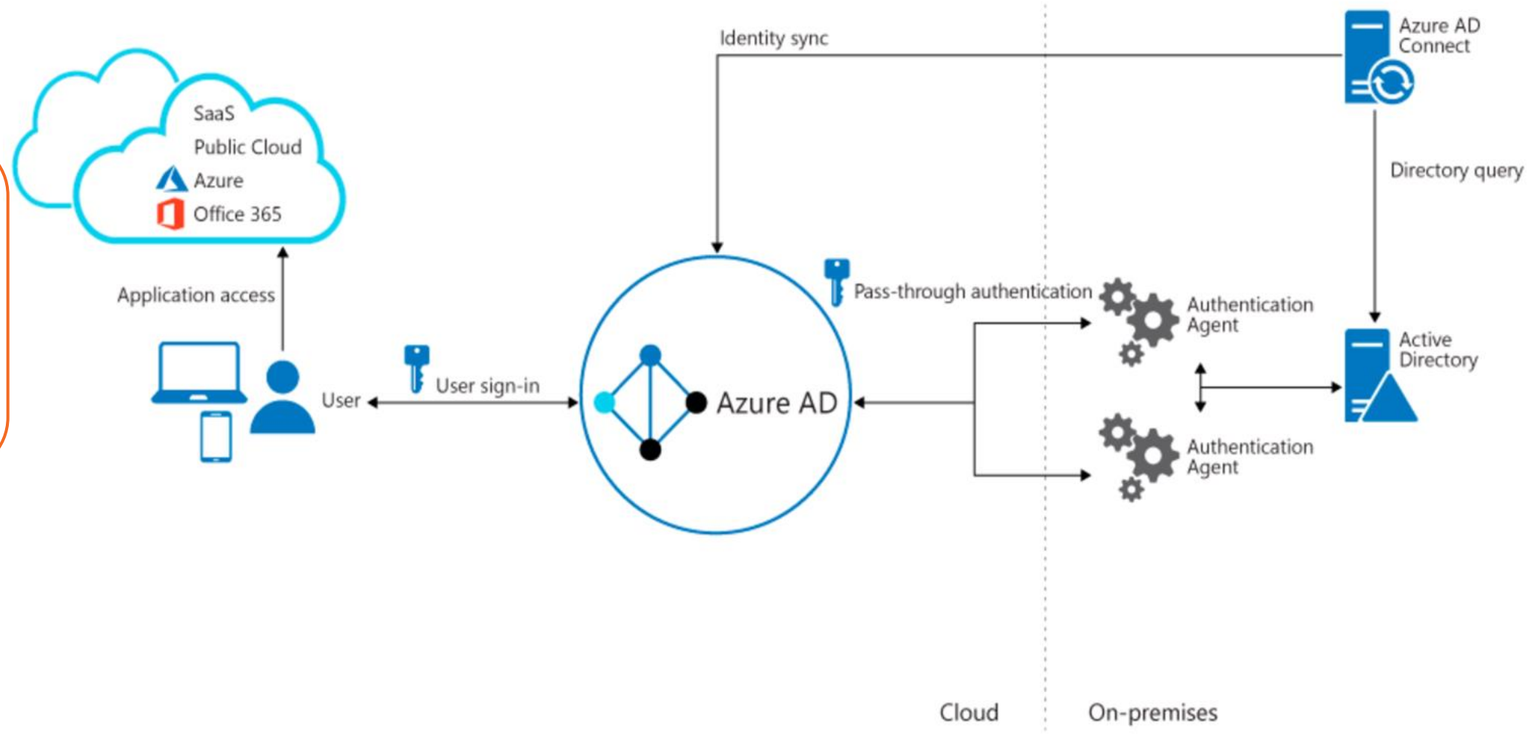


Source: https://docs.microsoft.com/

Authentication Architecture

Azure AD Hybrid identity with Pass-through authentication

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



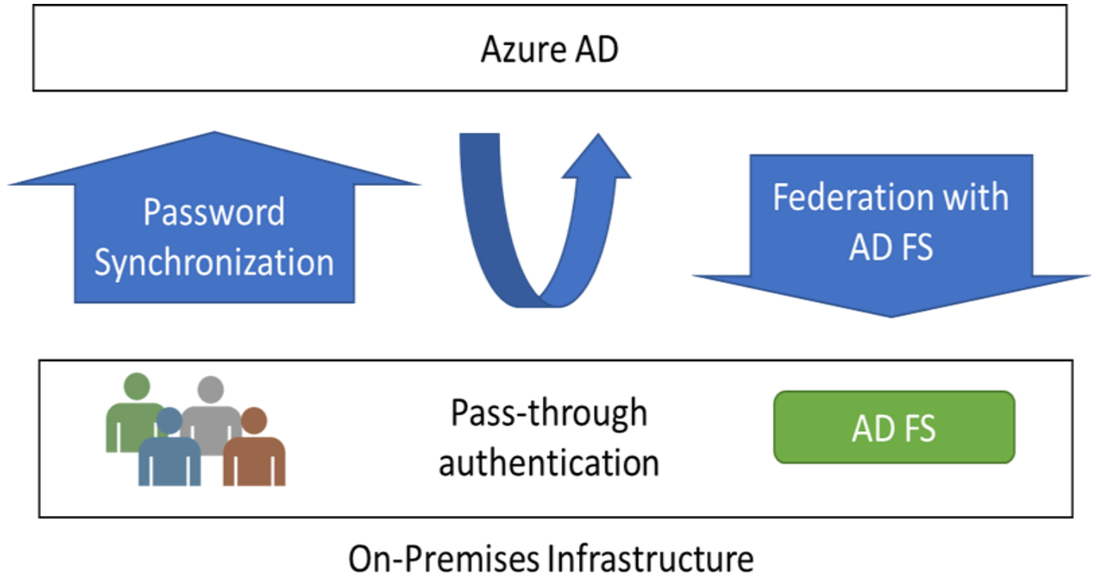
Source: https://docs.microsoft.com/

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

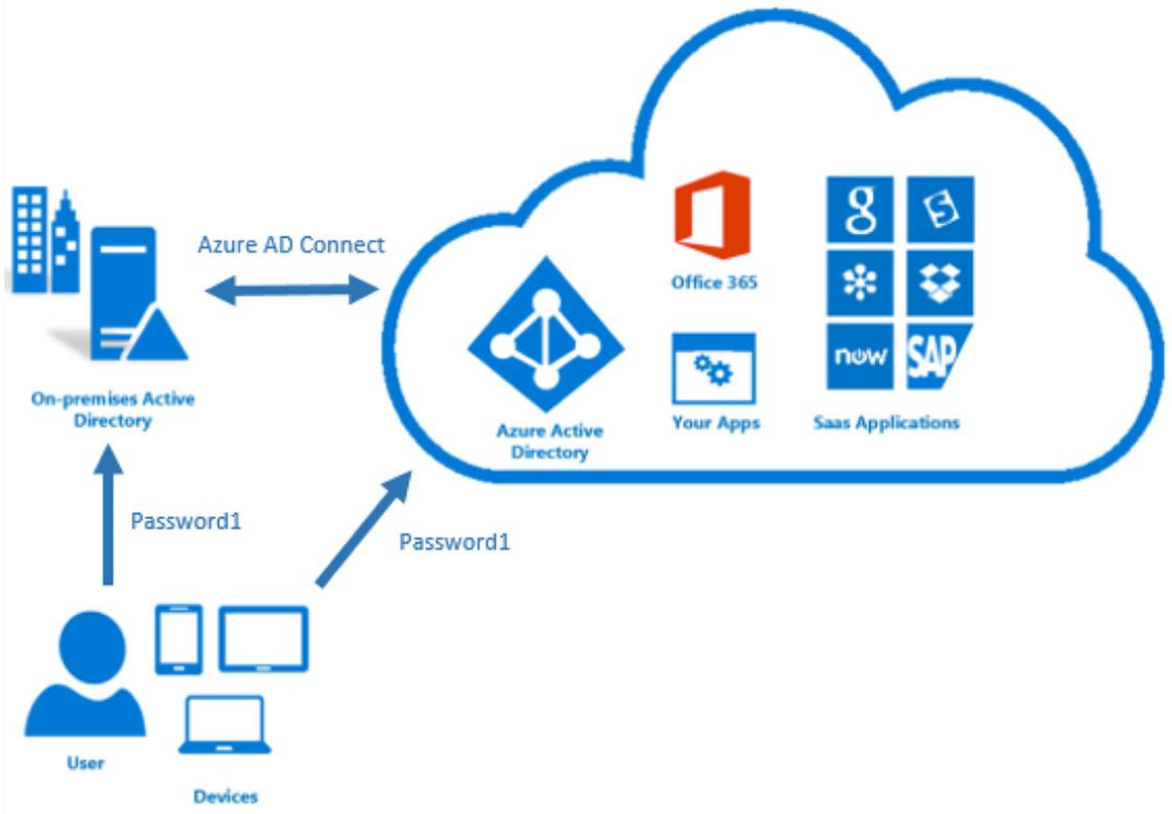


Authentication Options

The second option organizations can choose to authenticate is:

Pass-through authentication

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



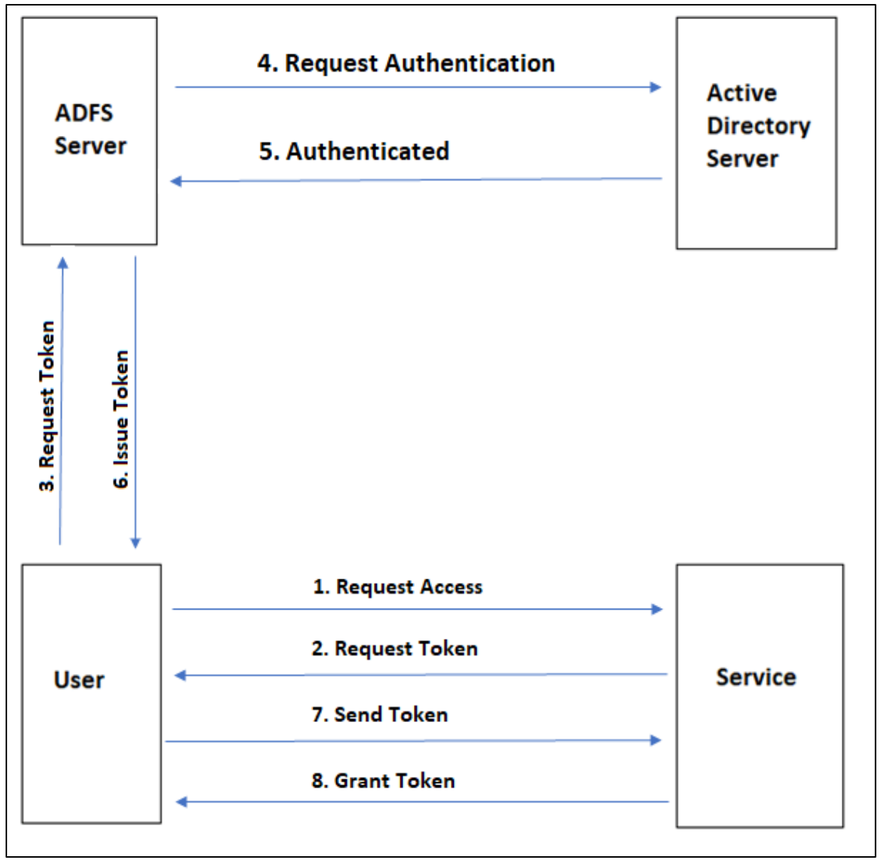
Source: https://docs.microsoft.com/

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	Azure Active Directory admin center provides agent status

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

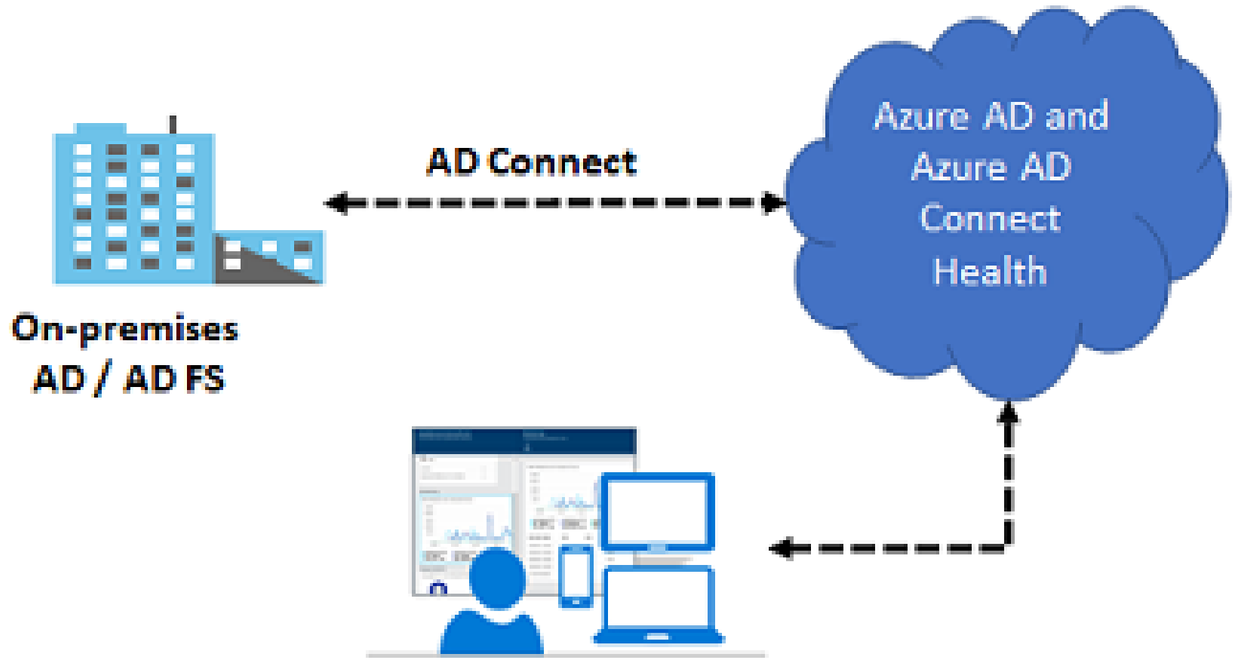
Comparing Authentication Methods

Consideration	Password hash synchronization + Seamless SSO	Pass-through authentication + Seamless SSO
Do users get a 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 multi-factor 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

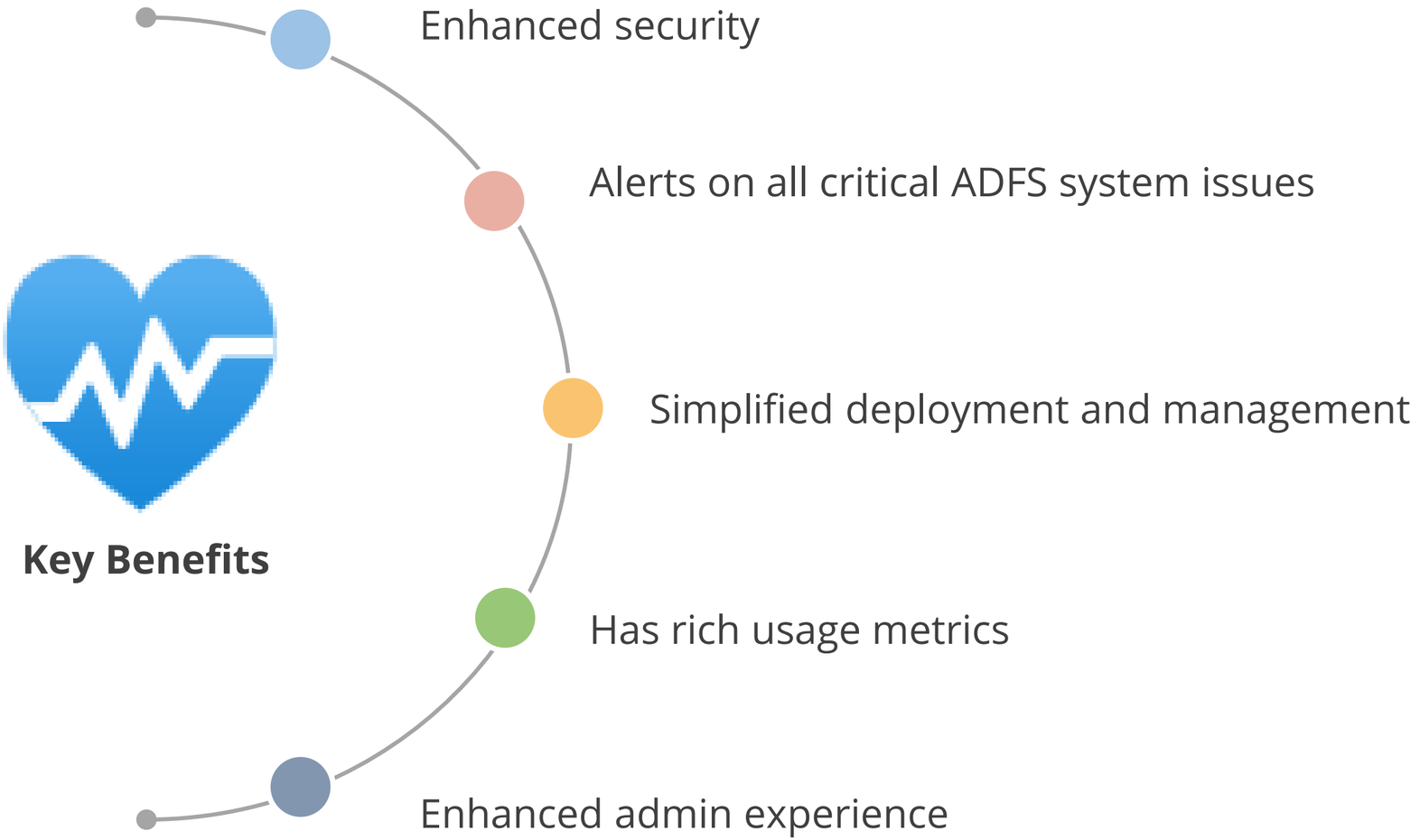
Source: https://docs.microsoft.com/

Azure AD Connect Health

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



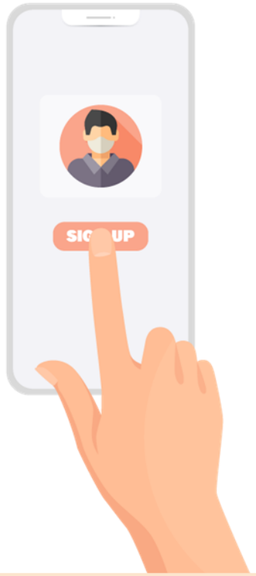
Why Use Azure AD Connect Health?



Recommend a Solution for User Self-Service

Self-Service Sign-Up

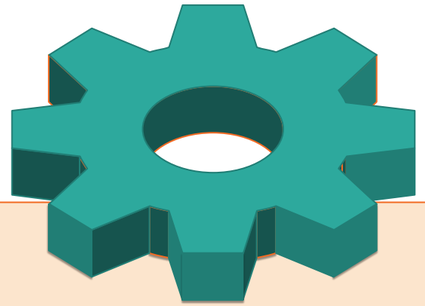
With a self-service sign-up user flow, one can create a sign-up experience for external users who want to access apps.



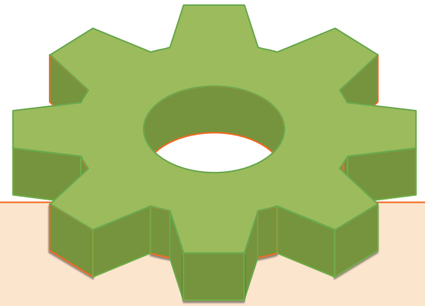
The user signs up for a cloud service and has an identity automatically created for them in Azure AD based on their email domain.

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

Getting customers to services they want faster

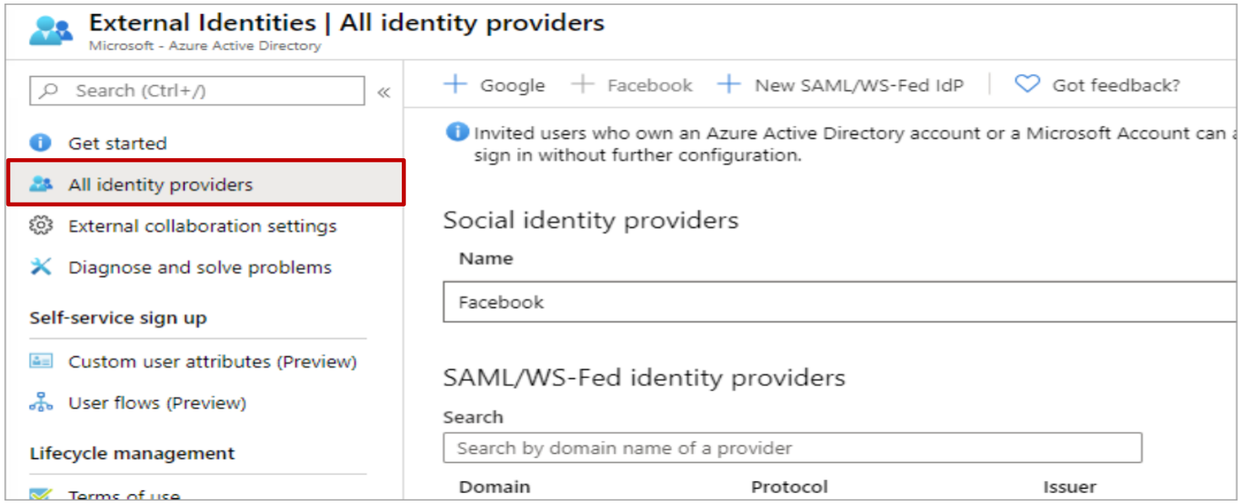
Creating email-based offers for a service

Turning self-service-created Azure AD tenant into a managed tenant

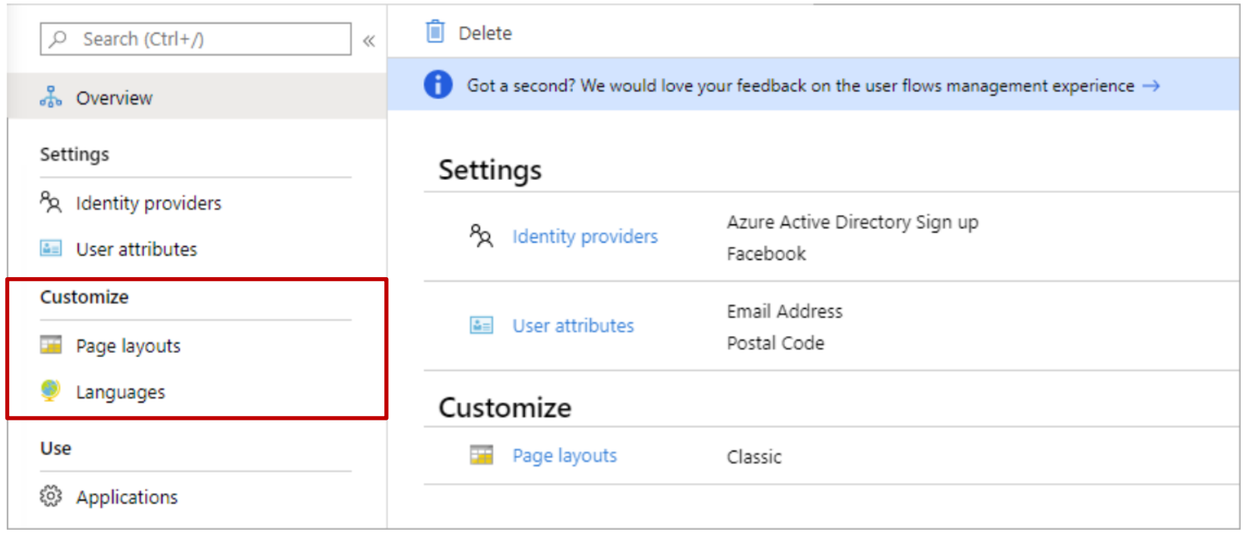
Creating email-based sign-up flows

Self-Service Sign-Up User Flow

Set up federation with identity providers

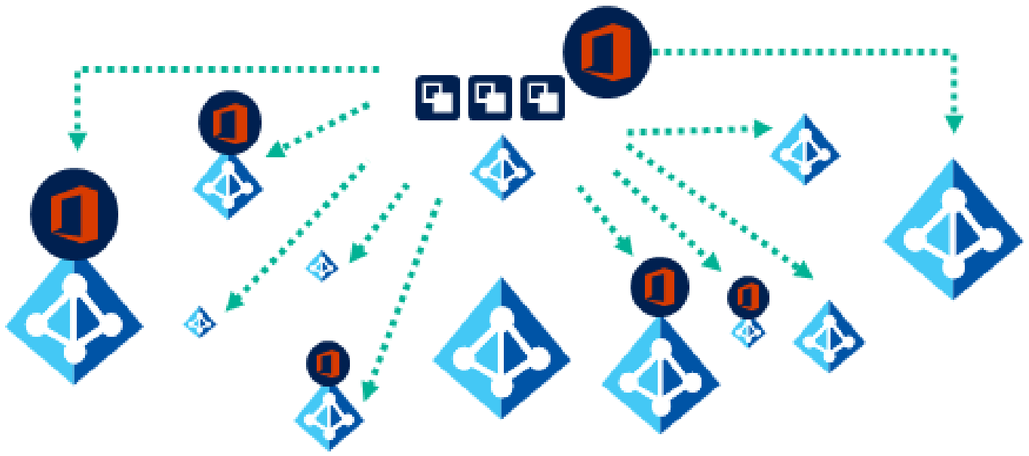


Create a self-service sign-up user flow



Recommend and Implement a Solution for B2B Integration

Azure AD B2B



- There are no external operating costs for the 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

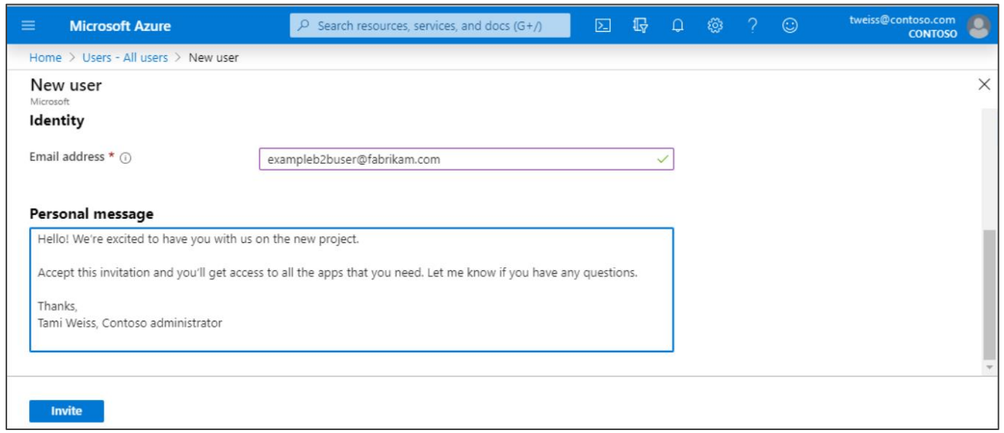
Guest users are those who are not considered an internal entity, such as an external partner, stakeholder, or customer.

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.

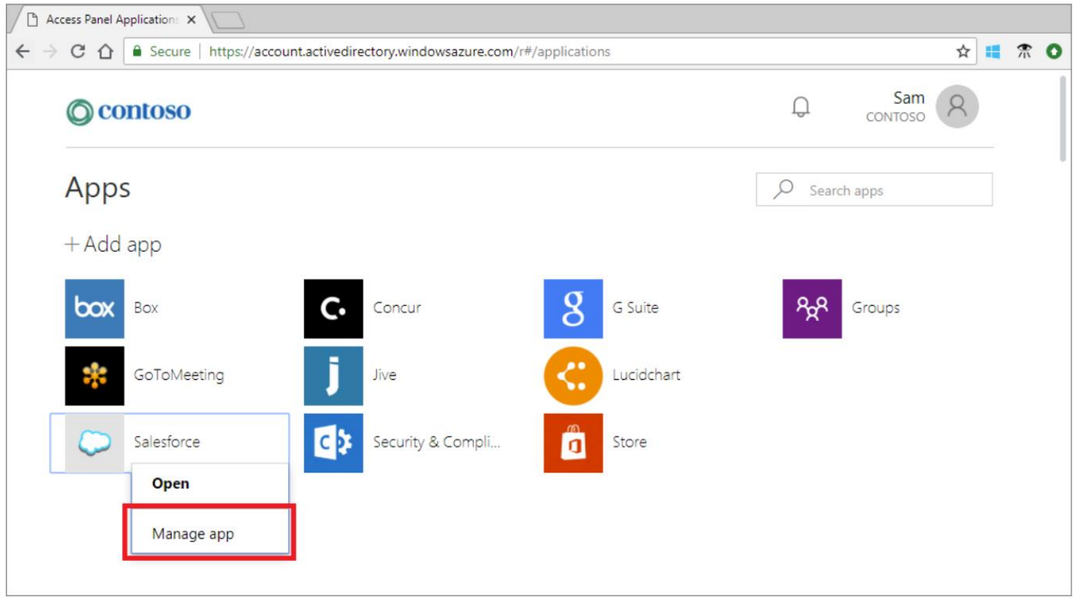


Follow the instructions given below to add a new guest user:

- 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

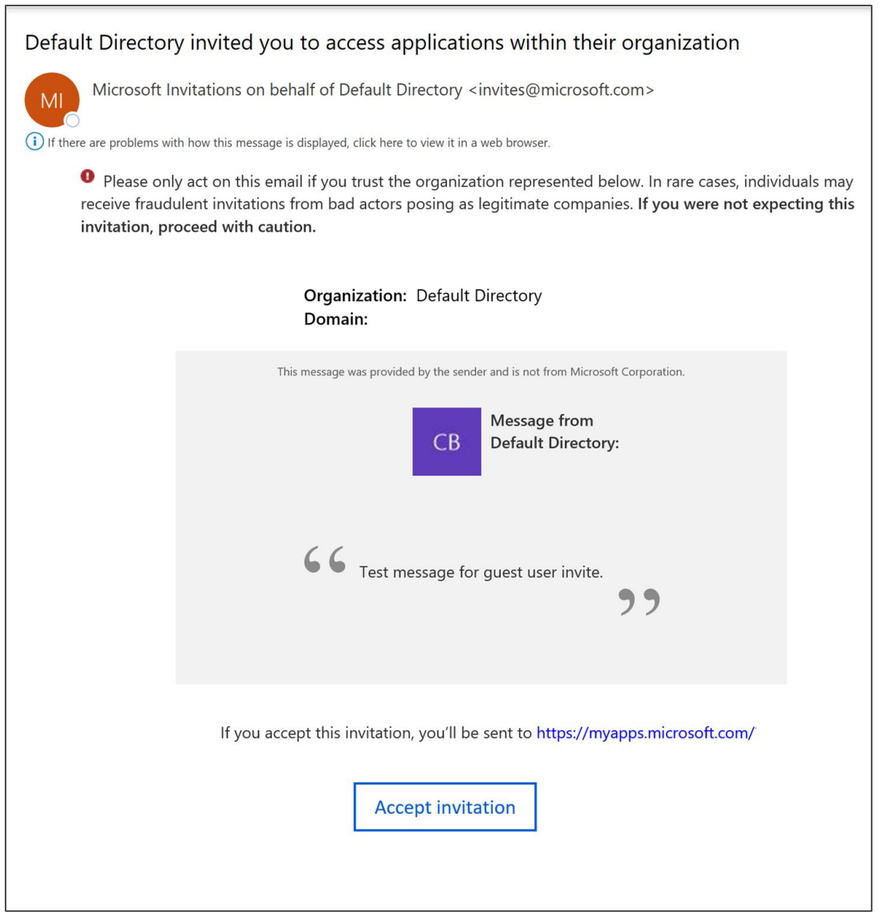
Allow application or group owners to manage their guest users.



- 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 the 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 an Azure AD Join:

1. Sign into the Azure portal as an administrator
2. Create an Azure AD Join
3. Create a virtual machine
4. RDP to the virtual machine to join the machine to Azure AD domain

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 into 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 into 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.

Assisted Practice: Guidelines

Steps to create a user group:

1. Sign into 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 into 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 usernames familiar to your users.

Assisted Practice: Guidelines

Steps to create a custom domain:

1. Sign into 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.

Setting Up Azure Active Directory

Duration: 25 min.

Project Agenda: To set up Azure Active Directory for your organization

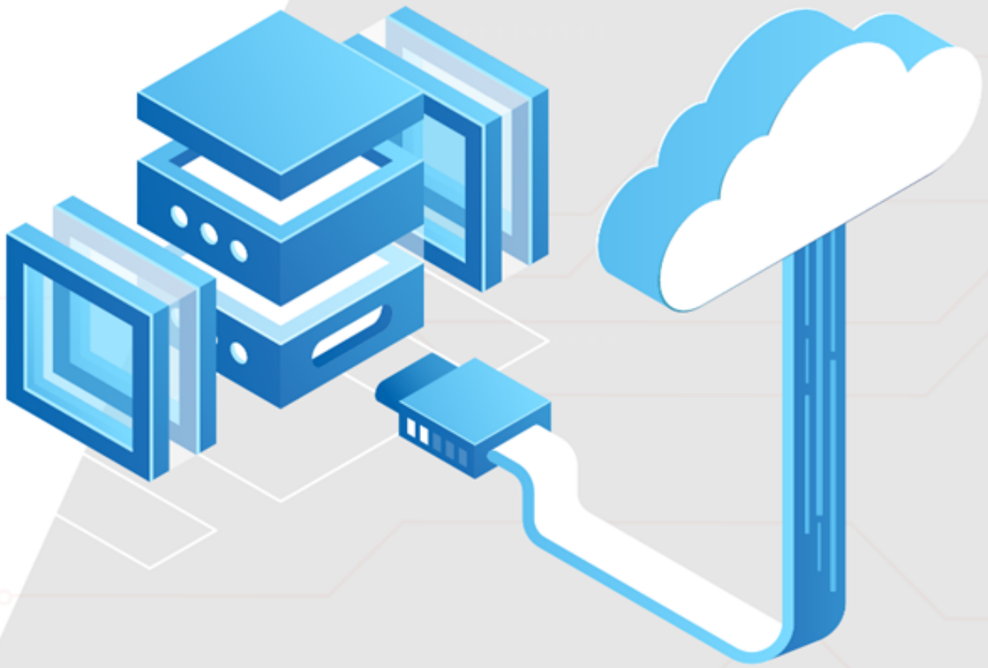
Description: Sim-Edu is a global firm with their headquarters in US and branch offices in multiple other locations in UK, Asia Pacific, etc. As part of their initial setup, they want to understand how Azure AD works and how they can leverage the Azure AD's capabilities. Their main requirements are as follows:

- Buying a third-party domain name
- Setting up an AD and a custom domain
- Implementing Sync between on prem AD and Azure AD

Perform the following:

1. Buy a domain name
2. Set up an Azure AD
3. Create a custom domain in the Azure AD
4. Prepare the sync

LESSON-END PROJECT



Thank you