Caltech | Center for Technology & Management Education

Post Graduate Program in Cloud Computing

Powered by simplilearn

Caltech | Center for Technology & Management Education

PG CC - Microsoft Azure Architect Technologies: AZ:303

Powerd by simplilearn

Implement and Manage Hybrid Identities

Learning Objectives

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

- Install and configure Azure Active Directory (AD) connect
- Illustrate Identity synchronization options
- Configure password sync and password writeback
- Configure single sign-on (SSO)
- Use Azure Active Directory (AD) Connect Health

A Day in the Life of an Azure Architect

You have recently joined an organization as a Azure Cloud Architect that runs a hybrid infrastructure that includes both cloud and on-premise application workloads.

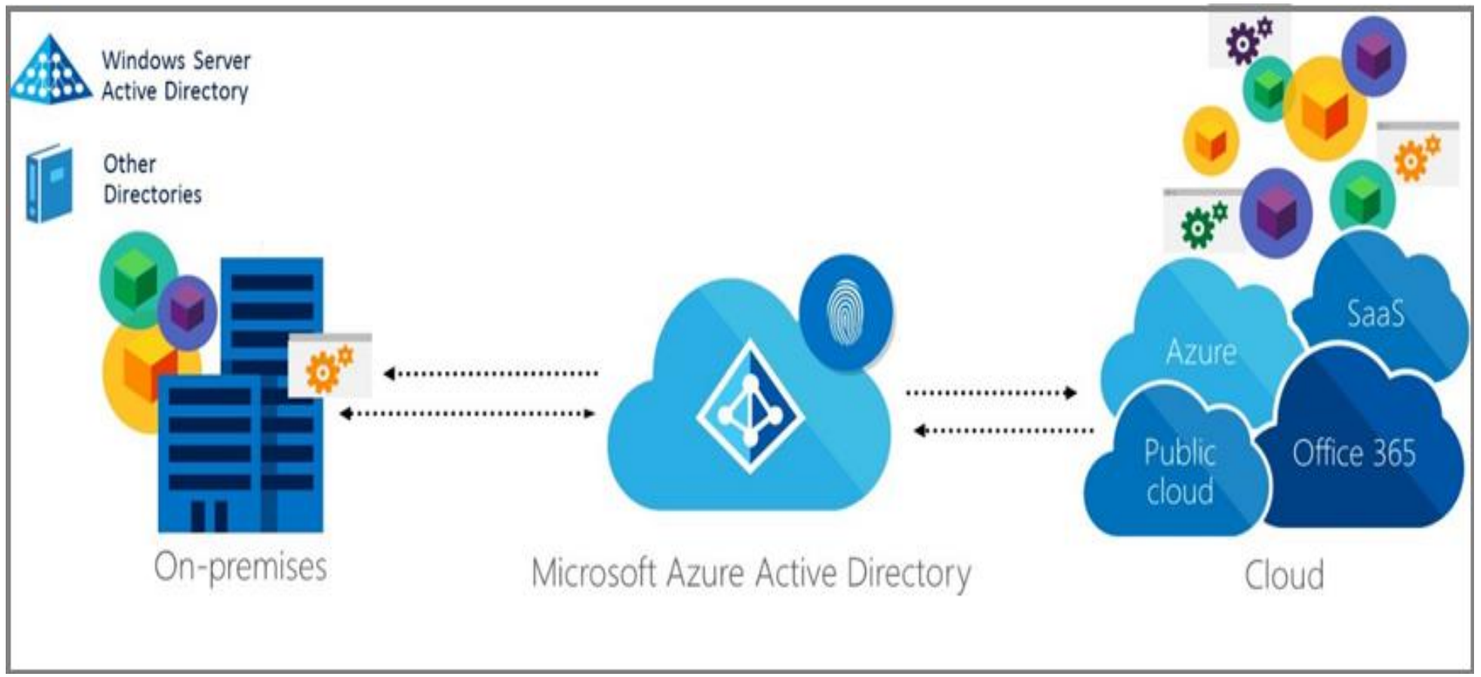
- You have been asked to advise them with a tool that can be used to authenticate and authorize access to all services, regardless of their location (on-premise or cloud).
- Also, the company is also looking for a solution that can enable users to access all software and services they need by logging in only once with a single user account.
- And to keep this entire situation under control, a tool that can help monitor on-premise identity infrastructure.

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

Hybrid Identity

Hybrid Identity

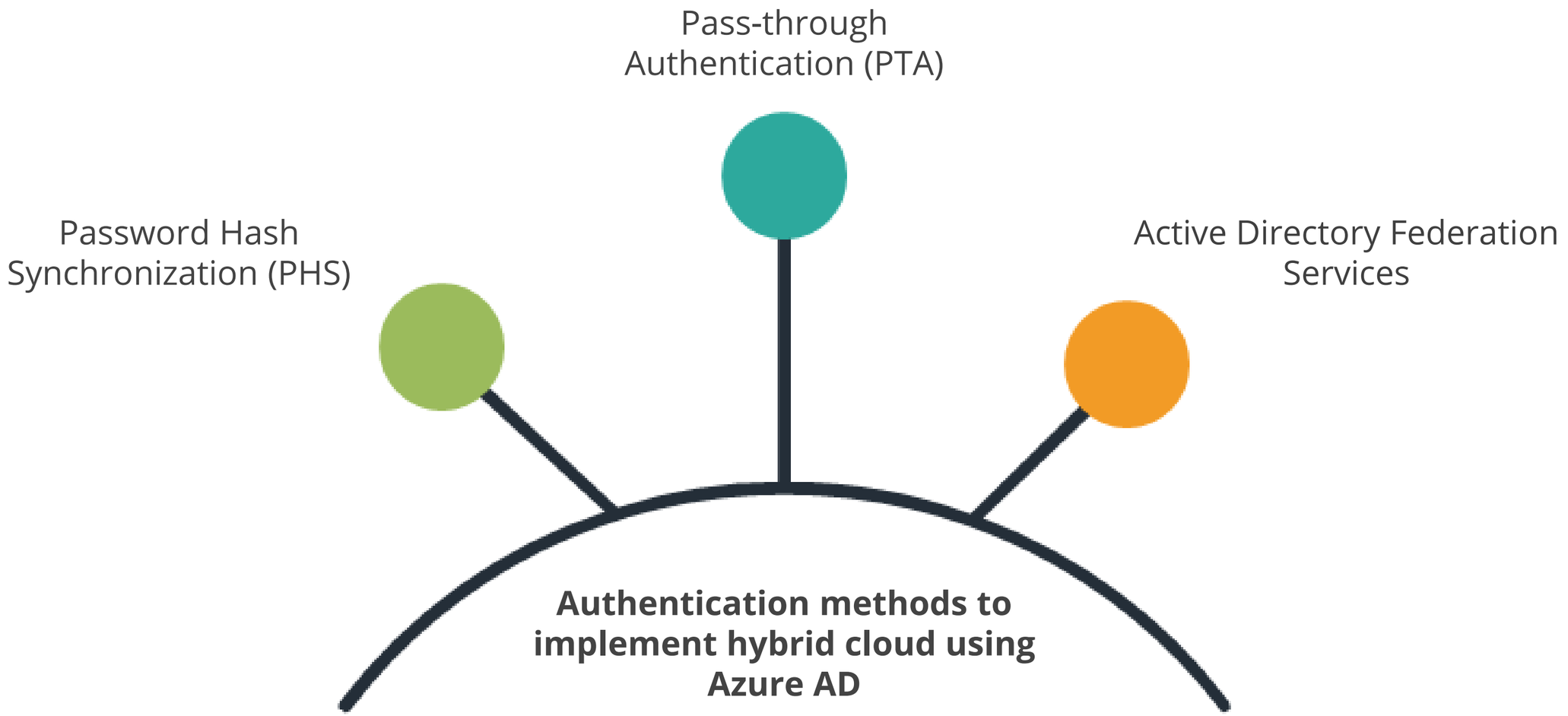
Microsoft's identity management tools provide both on-premise and cloud-based options.



Hybrid Identity is a single user identity that can be used to authenticate and authorize access to all services, regardless of their location.

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

Authentication Method



Common Scenarios

Below are some common scenarios with the recommended hybrid identity option:

Use case	PHS and SSO	PTA and SSO	AD FS
Sync new user, contact, and group accounts created in on-premise Active Directory to the cloud automatically	X	X	X
Setup tenant for Office 365 hybrid scenarios	X	X	X
Enable users to sign in and access cloud services using on-premise 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-premise 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

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

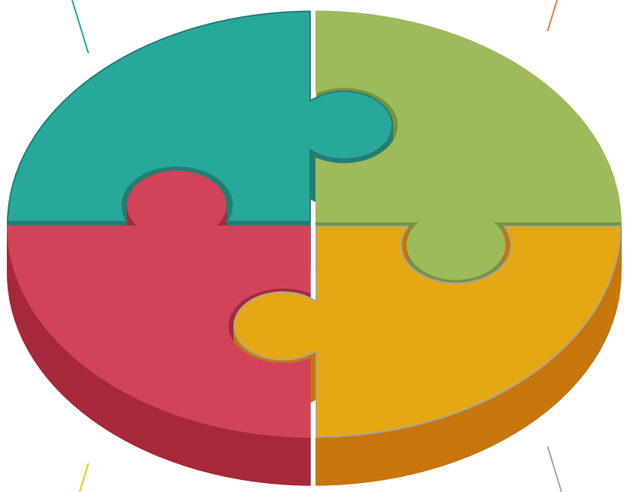
Azure Active Directory (AD) Connect

Azure Active Directory (AD) Connect

Azure AD Connect is a microsoft tool designed to meet and accomplish hybrid identity goals.

Users can integrate on-premise directories with Azure Active Directory

Users can access on-premise applications, cloud services using a single identity

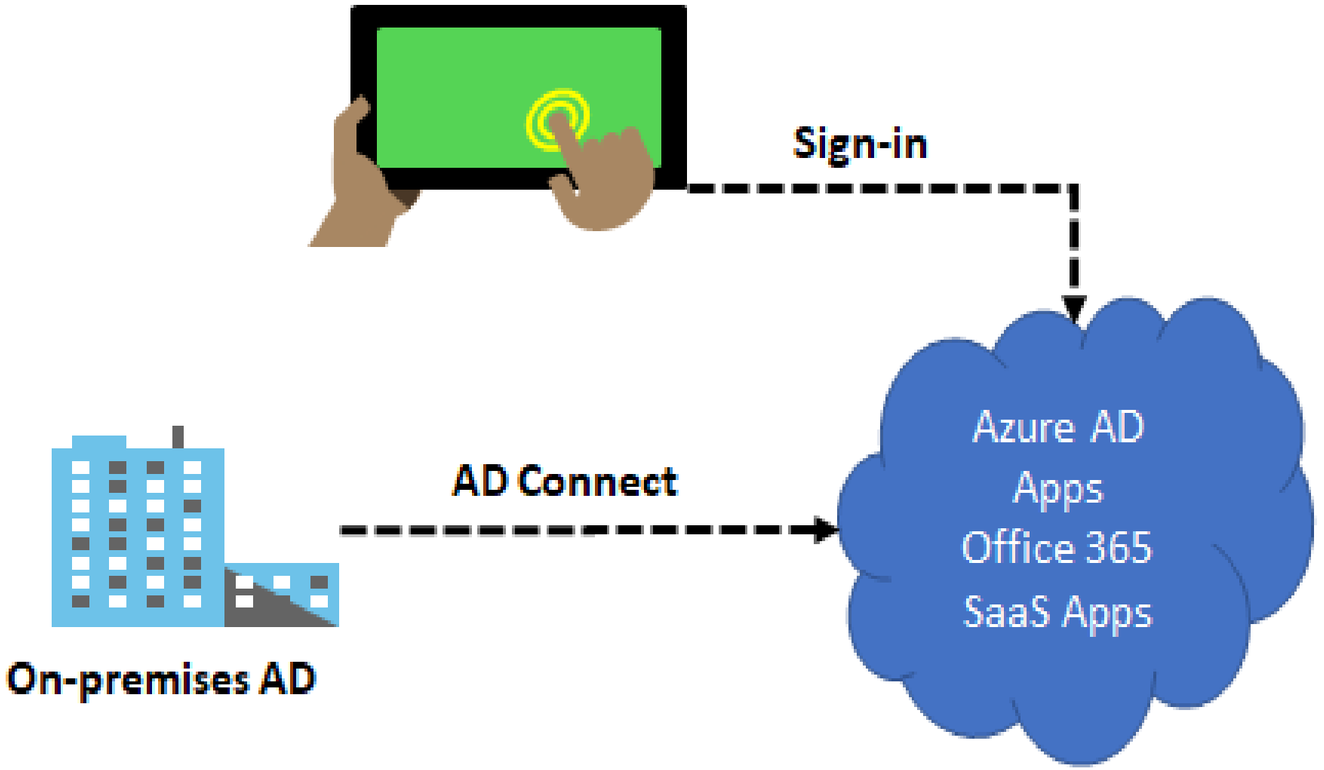


Single tool to provide an easy deployment experience

Replaces older versions of identity integration tools

Azure Active Directory (AD) Connect

Visual representation of Azure AD Connect:



Features of Azure Active Directory (AD)

Below are the features of Azure AD Connect:

- Password hash synchronization
- Pass-through authentication
- Federation integration
- Synchronisation
- Health monitoring

Authentication Options

Azure AD offers the following authentication methods for hybrid identity solutions:

- **Password Hash Synchronization (PHS)** can synchronize an encrypted version of the password hash for user accounts
- **Pass-through authentication (PTA)** helps authenticate the username and password with the on-premise domain controllers
- **Active Directory Federation Service (ADFS)** is the Microsoft implementation of an identity federation solution that uses claims-based authentication

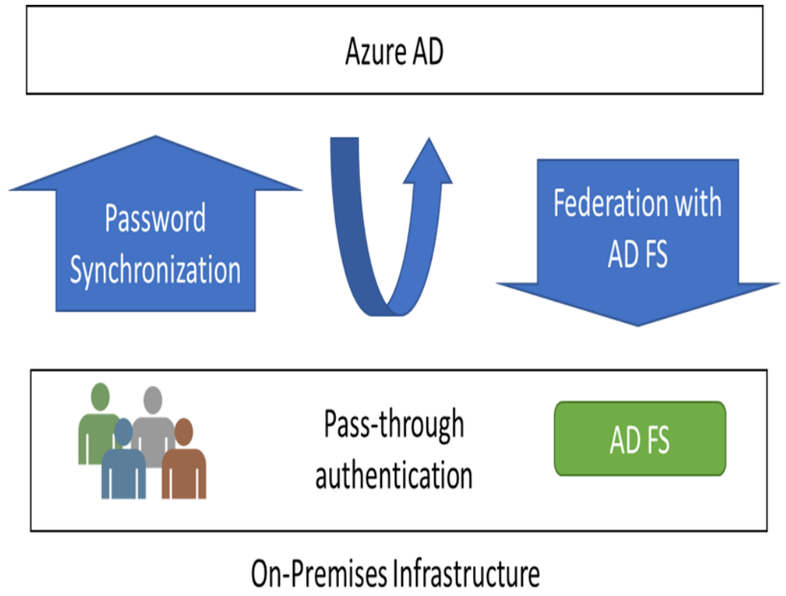


image source: https://docs.microsoft.com/en-in/

Azure AD Connect Installation

Let us look at the below Azure AD Connect solutions:

Express Settings

Custom Settings

Upgrade from Azure AD Sync or DirSync

- Azure AD Connect express settings are used when a user has a single-forest topology and password hash synchronization for authentication.
- Express settings are the default option used for the most commonly deployed scenarios.

Azure AD Connect Installation

Express Settings

Custom Settings

Upgrade from Azure AD Sync or DirSync

- Azure AD Connect custom settings are used when a user wants more options for the installation.
- These settings are used if a user has multiple forests or if a user want to configure optional features not covered in the express installation.
- These settings are used in all cases where the express installation option does not satisfy deployment or topology.

Azure AD Connect Installation

Express Settings

Custom Settings

Upgrade from Azure AD Sync or DirSync

- This option is used when a user has an existing DirSync server already running

Azure AD Connect Installation: Links

Topic	Link
Download Azure AD Connect	Download Azure AD Connect (https://go.microsoft.com/fwlink/?LinkId=615771)
Install using express settings	Express installation of Azure AD Connect (https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-express)
Install using customized settings	Custom installation of Azure AD Connect (https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom)
Upgrade from DirSync	Upgrade from Azure AD sync tool (DirSync) (https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-dirsync-upgrade-get-started)
After installation	Verify the installation and assign licenses (https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-post-installation)

Identity Synchronization Options

Sync Features

Below are some useful sync settings a user sees while configuring AD Connect tool on the on-premise server:

Prevent accidental deletes

This functionality is intended to guard against unintentional configuration changes and changes to your on-premise directory that would affect a large number of users and other artifacts.

Automatic upgrade

This function scans for newer versions of Azure AD Connect on a regular basis. If automatic update is allowed on your server, and a newer version is identified for which your server is qualified, it will upgrade to that newer version automatically.

Sync Features

Filtering

This is the most recommended configuration. With filtering, you can check which objects appear in Azure AD from your on-premise directory.

Password hash organization

It synchronizes the Active Directory password hash with Azure AD.

Password writeback

Users can update and reset their passwords in the cloud while still adhering to their on-premise password policy.

Password Sync and Password Writeback

Password Hash Synchronization (PHS)

It synchronizes the password hash in Active Directory to Azure AD and is the easiest authentication to implement.

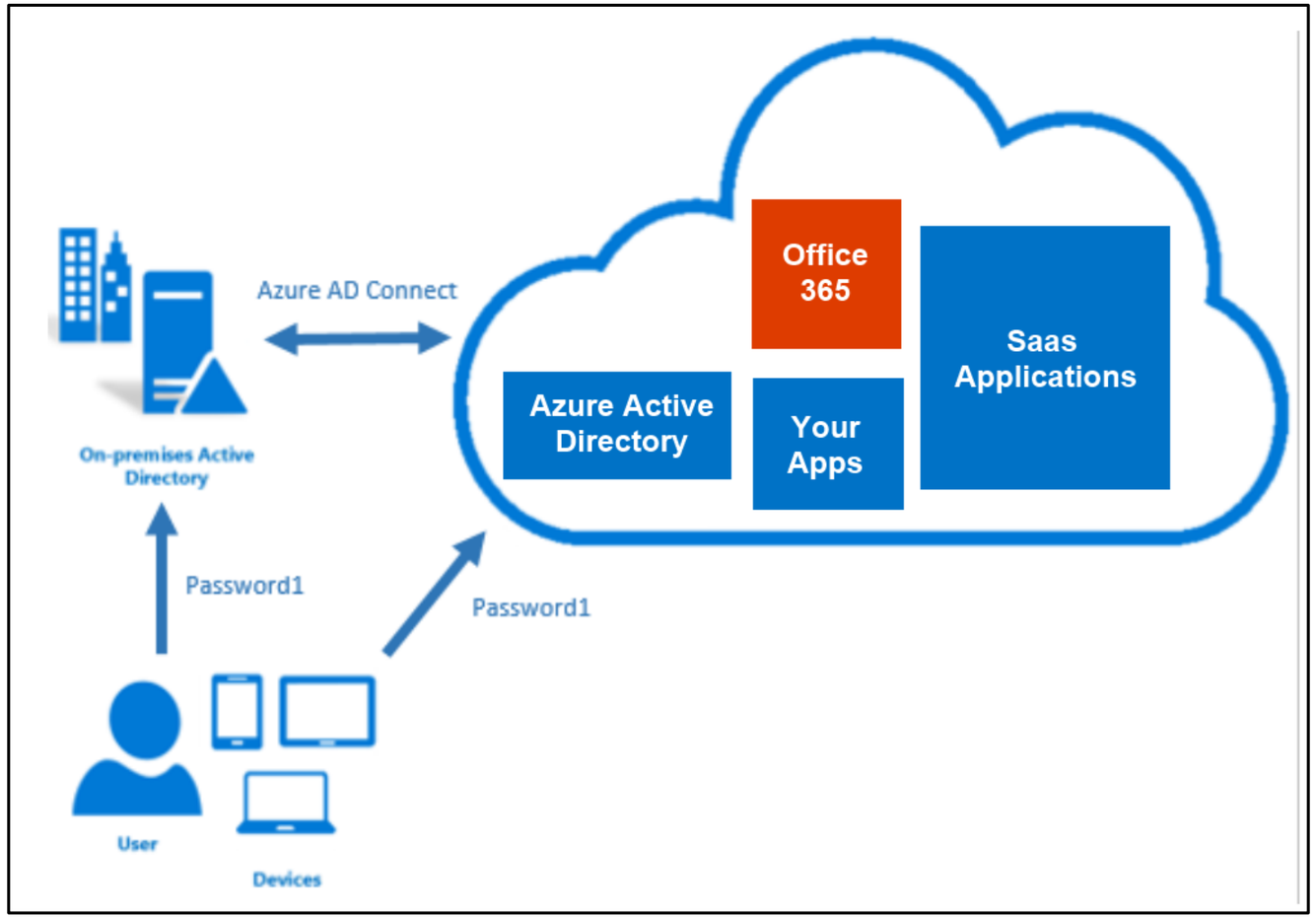
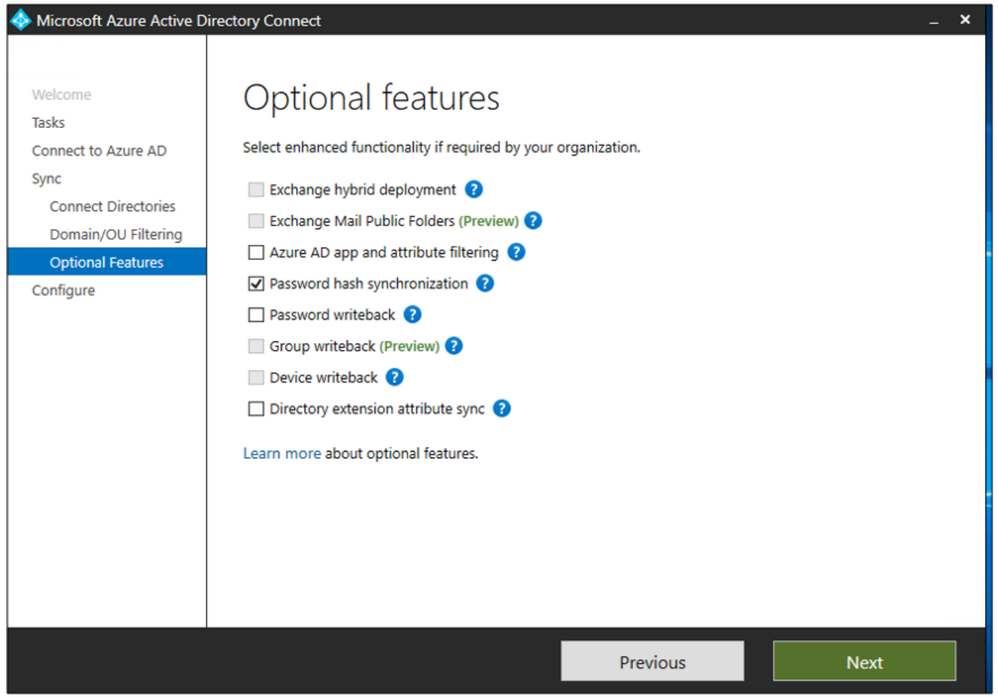


image source: https://docs.microsoft.com/en-in/

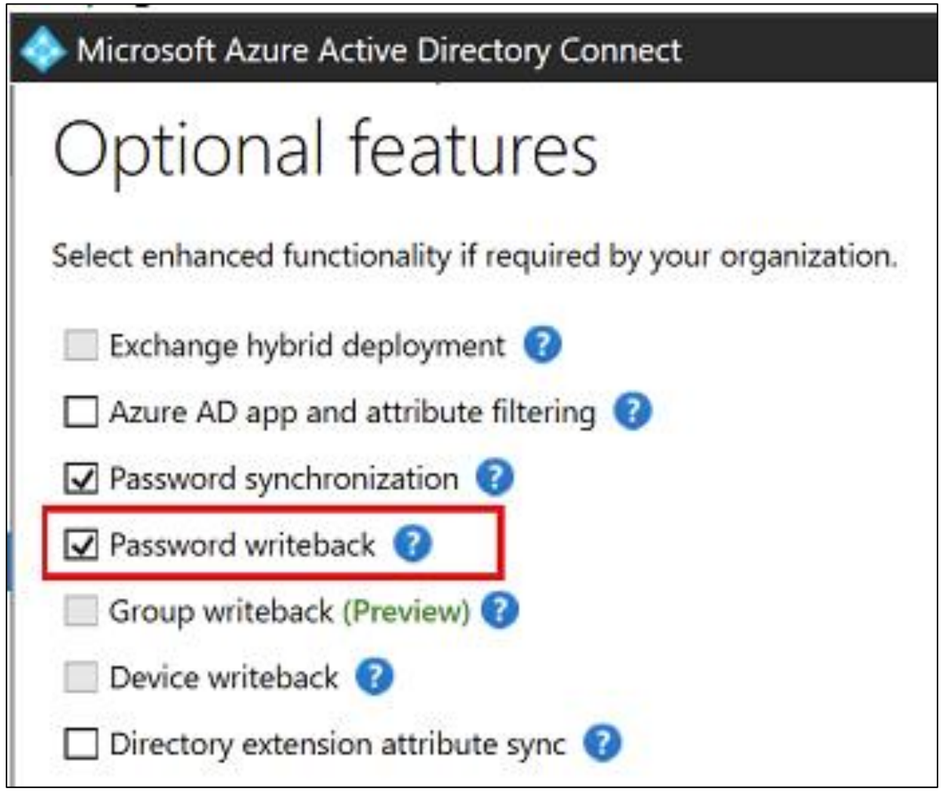
Benefits of Password Hash Synchronization (PHS)

- It aids in the reduction of passwords.
- It has the potential to improve your users' productivity.
- It has the potential to lower your help desk costs.



Password Writeback

Password writeback is an Azure AD Connect function that allows password changes in the cloud to be written back in real time to an existing on-premise directory.

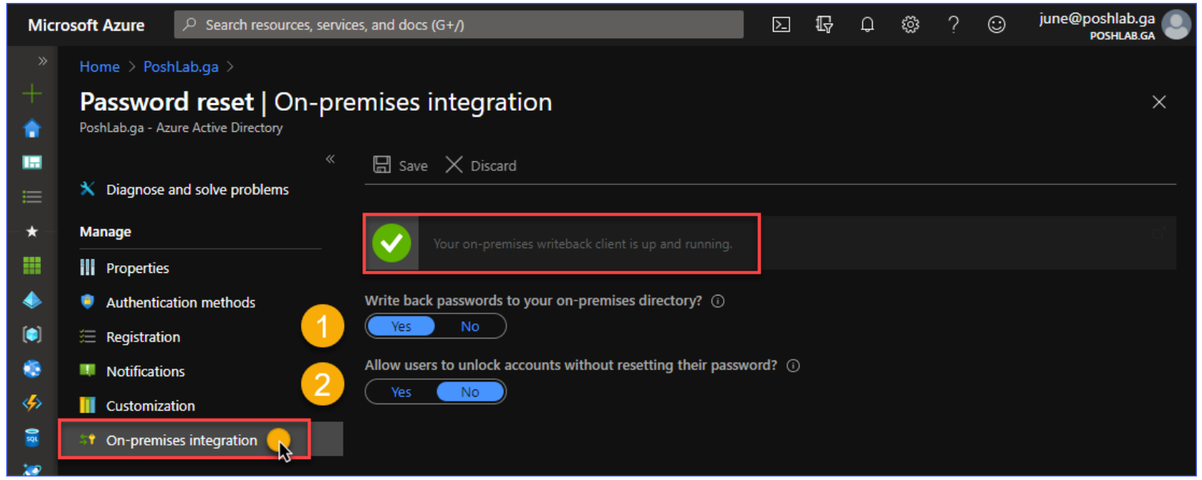


It is possible to allow it using Password Hash Organization (PHS).

Integration on the Premises

Password writeback provides following features:

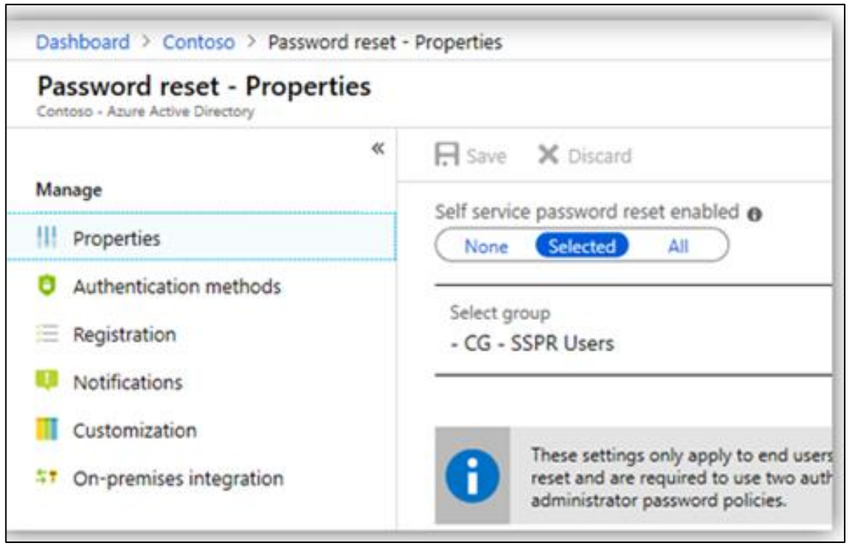
- Password policies for Active Directory Domain Services (AD DS) on-premise are enforced.
- The user can get a quick feedback.
- Password changes and writebacks are supported.
- No inbound firewall rules needed.



Self-Service Password Reset Writeback (SSPR)

Self-service password reset (SSPR) in Azure Active Directory allows users to alter or reset their passwords.

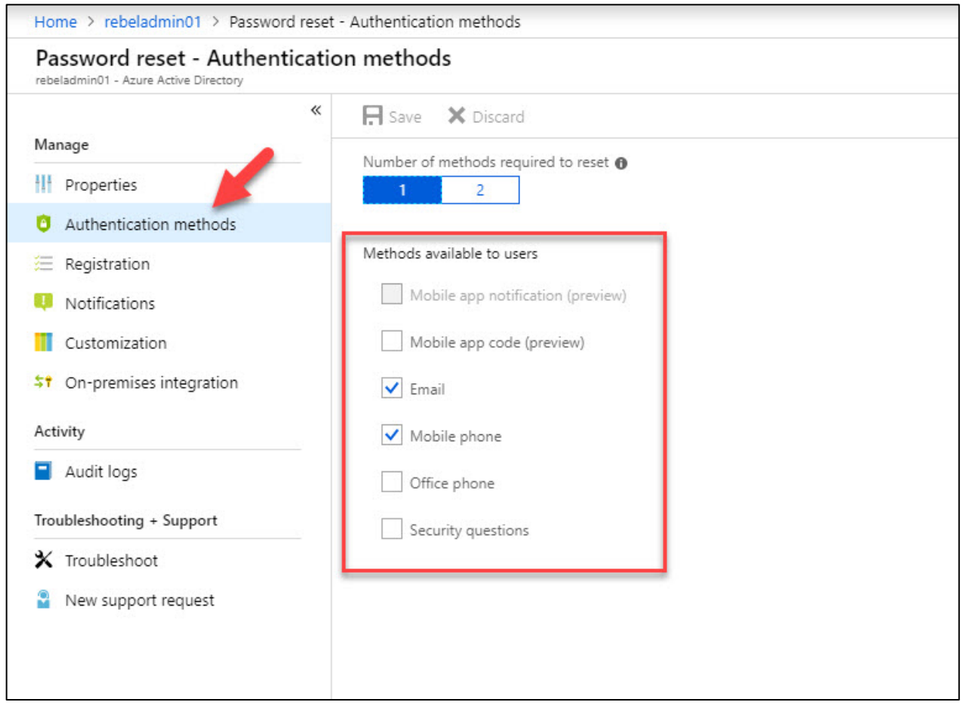
- If a user's account is locked or they forget their password, they will unblock themselves and get back to work by following the prompts.
- If a user can't sign in to their computer or an application, SSPR eliminates help desk calls and productivity loss.



Enabling Self-Service Password Reset Writeback (SSPR)

SSPR can be done via the Azure Active Admin Portal, and the SSPR settings can be found under the ‘Password Reset’ section.

- The user may specify how many alternative forms of identification a user must have in order to reset their password.
- Mobile phone, Email, and Security Questions are some of the methods available.



Azure Single Sign-On (SSO)

Azure Single Sign-On (SSO)

Single Sign-On (SSO) refers to a user's ability to access all software and services they need by logging in only once with a single user account.

SSO allows users to access all required applications without having to validate again.

Benefits of Single Sign-On

There are various benefits of using Single Sign-On:

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

Benefits of Single Sign-On

Without Single Sign-On, user will have to:

- Recall domain-specific passwords and sign in to each program without single sign-on
- Create and update each program, such as Office 365, Box, and Salesforce. IT workers build and upgrade user accounts
- Recall their codes and log in to each program separately

Single Sign-On Method

Selection of a Single Sign-On process depends on how the application is configured for authentication.

Benefits

- For Single Sign-On, cloud applications can use OpenID Connect, OAuth, SAML, password-based methods, and connected or disabled modes.
- Users can access on-premise applications as well as cloud services like Office 365 using a single identity.

Single Sign-On Flowchart

The workflow of Single Sign-On is given below:

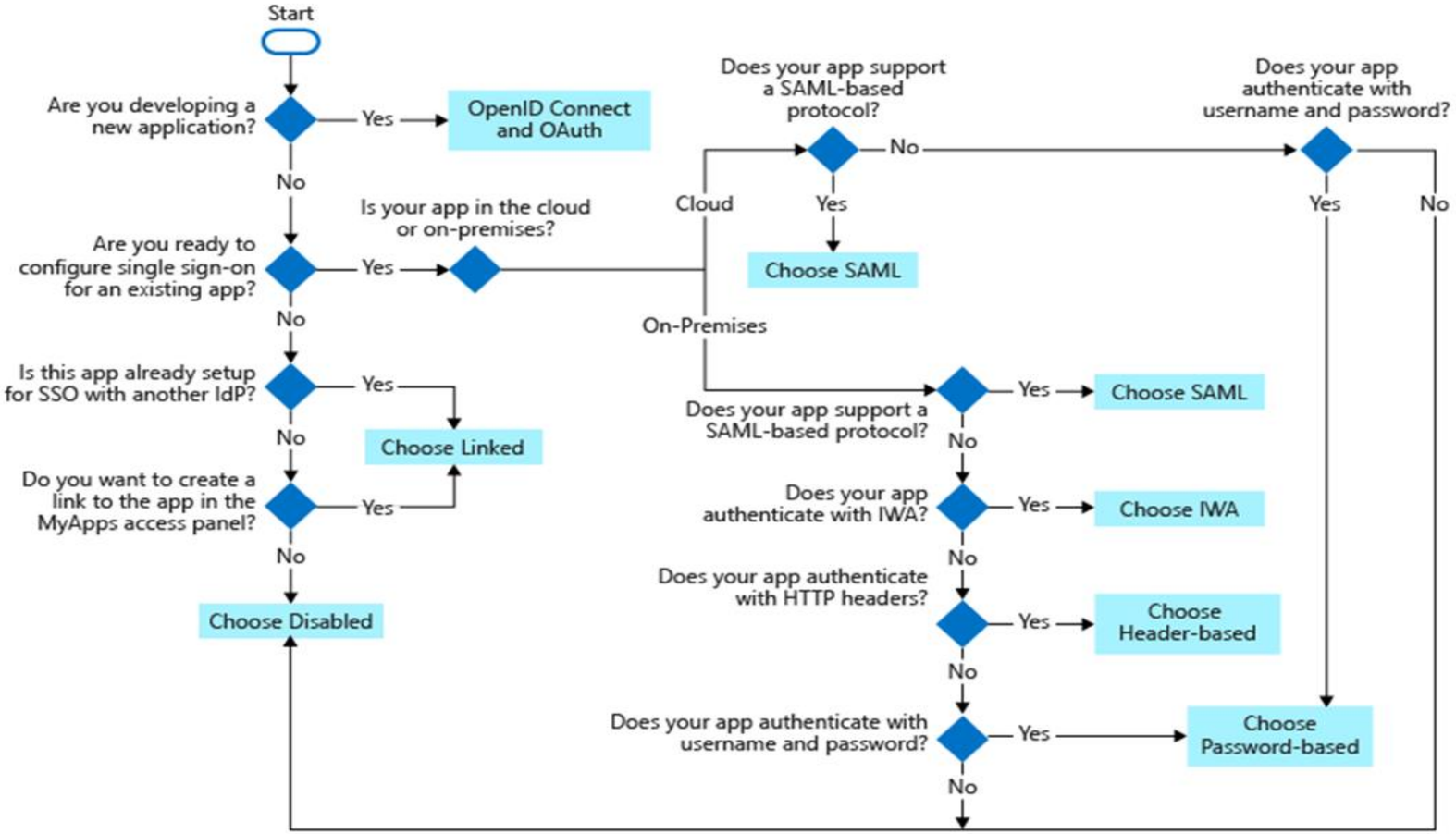
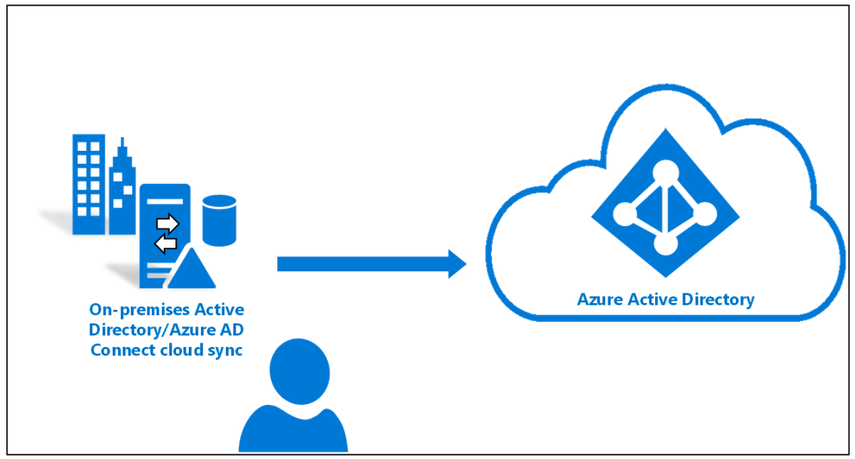


image source: https://docs.microsoft.com/en-in/

Configure Azure AD Connect Cloud Sync

Configure Azure AD Connect Cloud Sync

It helps to meet and accomplish hybrid identity goals for synchronization of users, groups, and contacts to Azure AD.



It makes use of the Azure AD cloud provisioning agent to accomplish this.

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

Azure AD Connect Cloud Sync Benefits

Multiple provisioning agents can be used to simplify high availability deployments

Support for synchronizing to an Azure AD tenant from a multi-forest disconnected Active Directory forest environment

Simplified installation with light-weight provisioning agents

Support for large groups with up to 50K members

Azure Active Directory (AD) Connect Health

Azure AD Connect Health

Azure AD Connect Health monitors on-premise identity infrastructure, ensuring the environmental stability.

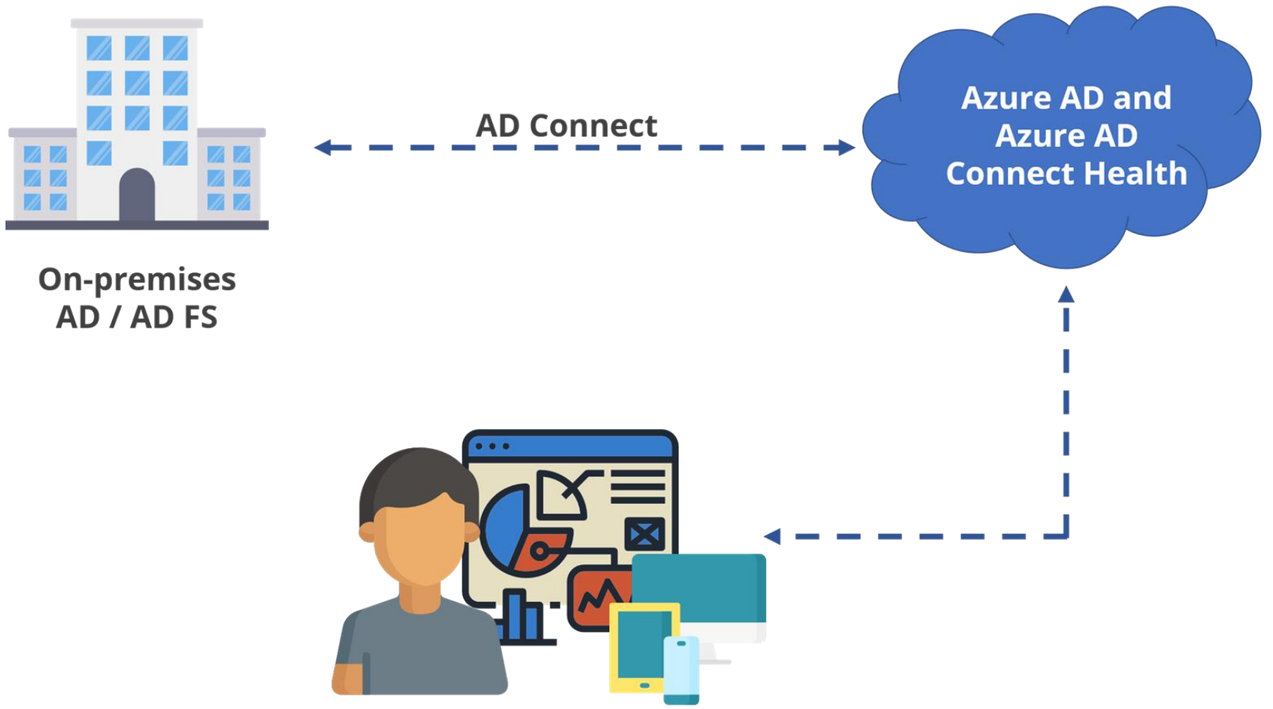


image source: https://docs.microsoft.com/en-in/

Azure AD Connect Health Benefits

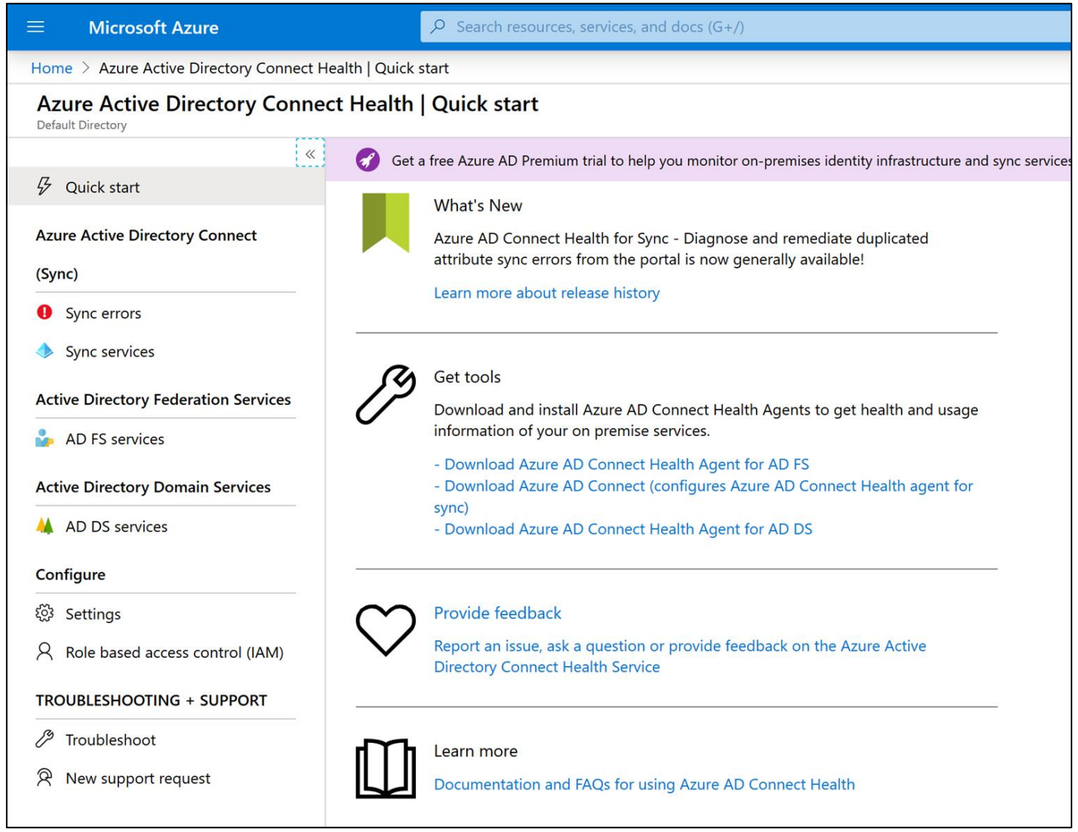
Below are the key benefits of using Azure AD Connect Health:

- Enhances Security
- Triggers alert on all critical ADFS system issue
- Is easily deployed and managed
- Maintains rich usage metrics
- Provides great user experience

Azure AD Connect Health Implementation

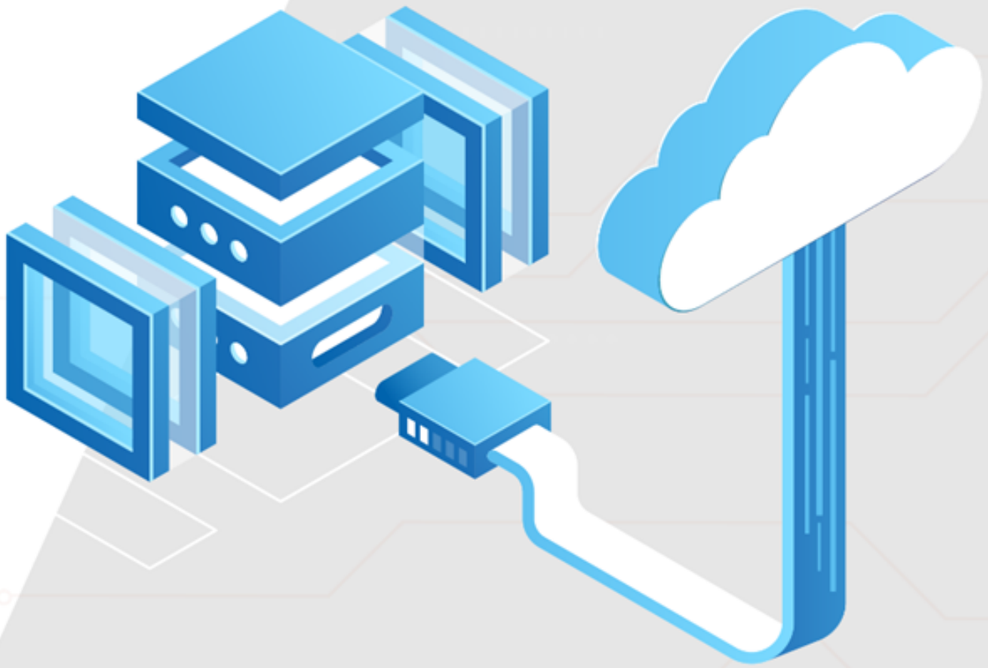
Follow the below steps to implement Azure AD Connect Health.

- Install the Azure AD Connect Health agent
- Install the latest version of Azure AD Connect (includes Azure AD Connect Health for sync)
- Monitor Azure AD Connect Health portal
  - Views of alerts
  - Performance monitoring
  - Usage analytics



Key Takeaways

- A hybrid Identity is a single user identity used to authenticate and authorize access to all services, regardless of their location.
- Azure AD offers PHS, PTA, and ADFS authentication methods for hybrid identity solutions.
- Azure Single Sign-On refers to a user's ability to access all software and services.
- Azure AD Connect Health monitors on-premise identity infrastructure, ensuring environmental stability.



Thank you