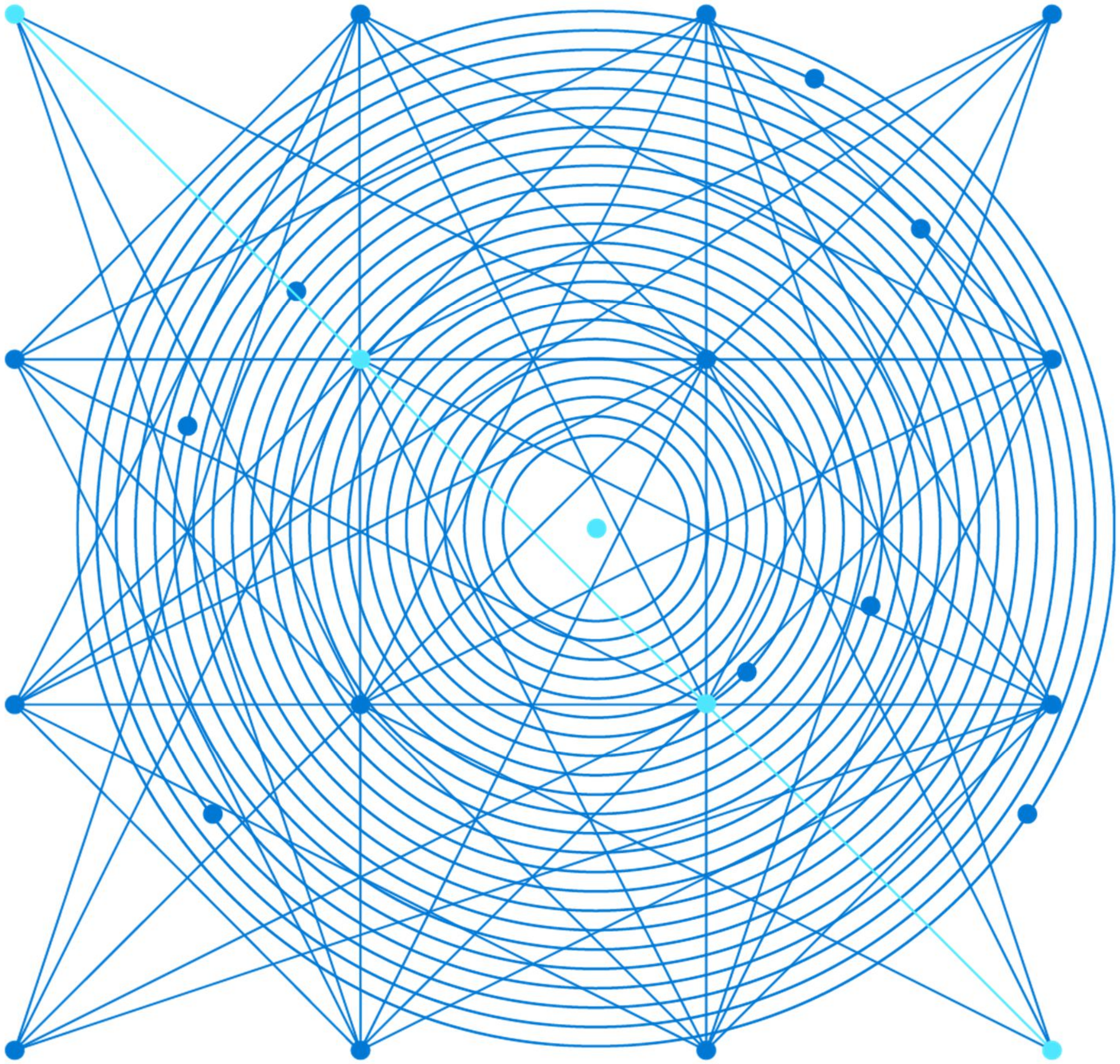
AZ-303: Microsoft Azure Architect Technologies



Module 2: Implement and Manage Hybrid Identities

Azure AD Connect, Password Sync and Password Writeback, and Azure AD Connect Health

Learning Objectives

You will learn the following concepts:

- Hybrid Identity
- Install and configure Azure AD Connect
- Configure password sync and password writeback
- Configure Azure AD Connect Health

Hybrid Identity

Hybrid Identity with Azure Active Directory (1 of 2)

You can use the following authentication methods to implement hybrid identity with Azure AD

- Password hash synchronization (PHS)
- Pass-through authentication (PTA)
- Federation (AD FS)

Hybrid Identity with Azure Active Directory (2 of 2)

I need to:	PHS and SSO	PTA and SSO	AD FS
Sync new user, contact, and group accounts created in my on-premises Active Directory to the cloud automatically.	X	X	X
Set up my tenant for Office 365 hybrid scenarios.	X	X	X
Enable my 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 smartcard authentication for my users.[4]			X
Display password expiry notifications in the Office Portal and on the Windows 10 desktop.			X

Install and Configure Azure AD Connect

Azure AD Connect

Password hash synchronization - A sign-in method that synchronizes a hash of a users on-premises AD password with Azure AD.

Pass-through authentication - A sign-in method that allows users to use the same password on-premises and in the cloud but doesn't require the additional infrastructure of a federated environment.

Federation integration - Is used to configure a hybrid environment using an on-premises AD FS infrastructure. It also provides AD FS management capabilities such as certificate renewal and additional AD FS server deployments.

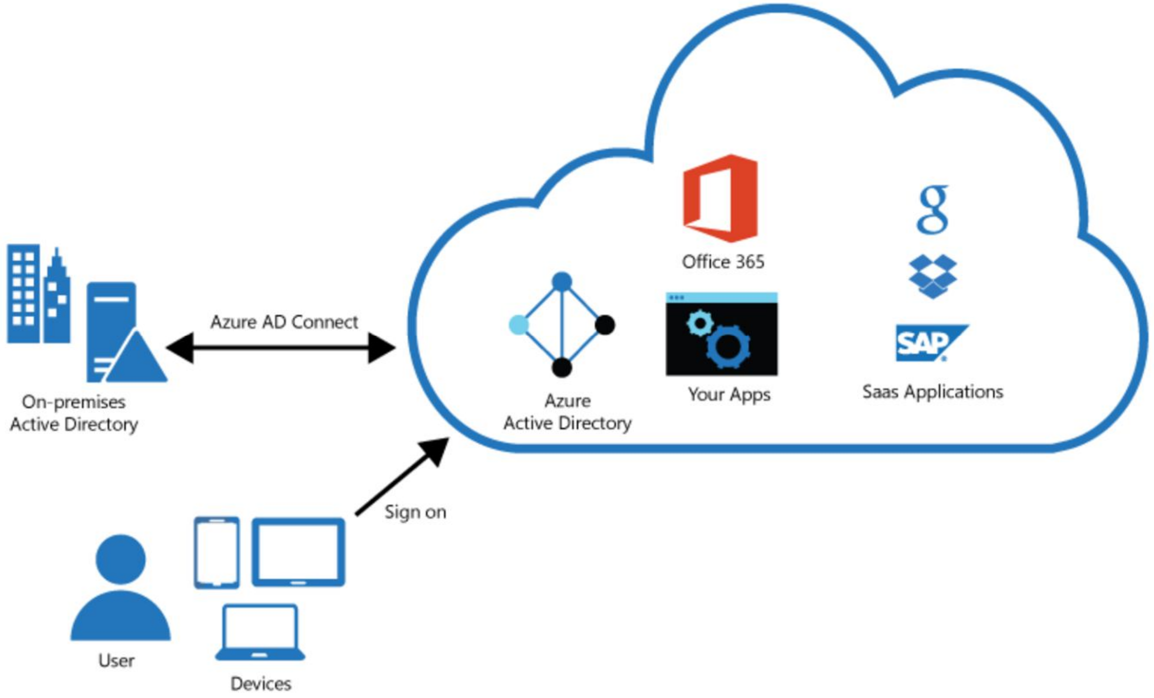
Synchronization - Responsible for creating users, groups, and other objects. As well as, making sure identity information for your on-premises users and groups is matching the cloud.

Health Monitoring - Azure AD Connect Health can provide robust monitoring and provide a central location in the Azure portal to view this activity.

Azure AD Connect (cont.)

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 such as Office 365.
- Single 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.



Azure AD Connect Installation

Install Azure AD Connect:

- Express settings
- Custom settings
- Upgrade from DirSync
- Upgrade from Azure AD Sync or Azure AD Connect

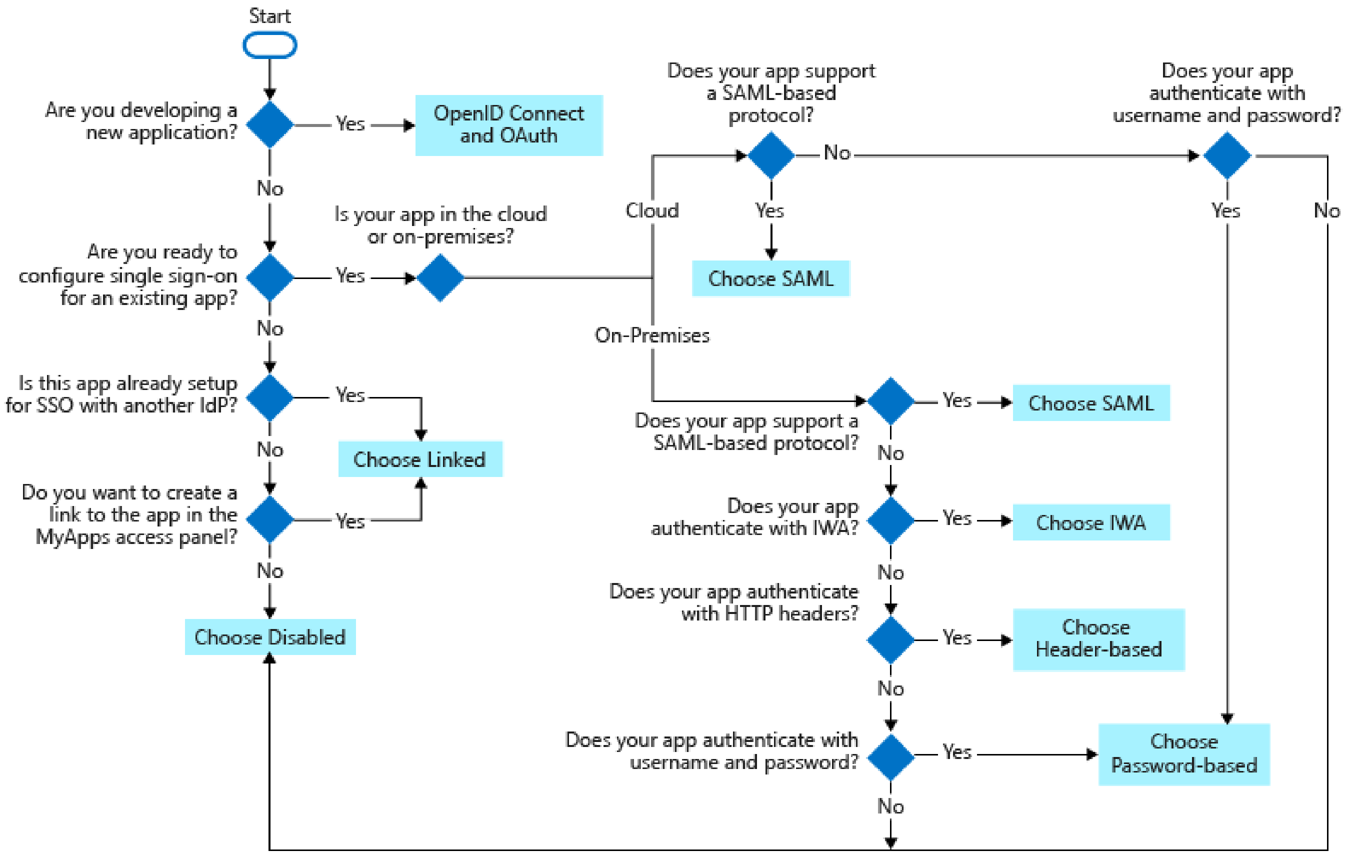
Configure sync features:

- Filtering
- Password hash synchronization
- Password writeback
- Prevent accidental deletes
- Automatic upgrade

Single Sign-On

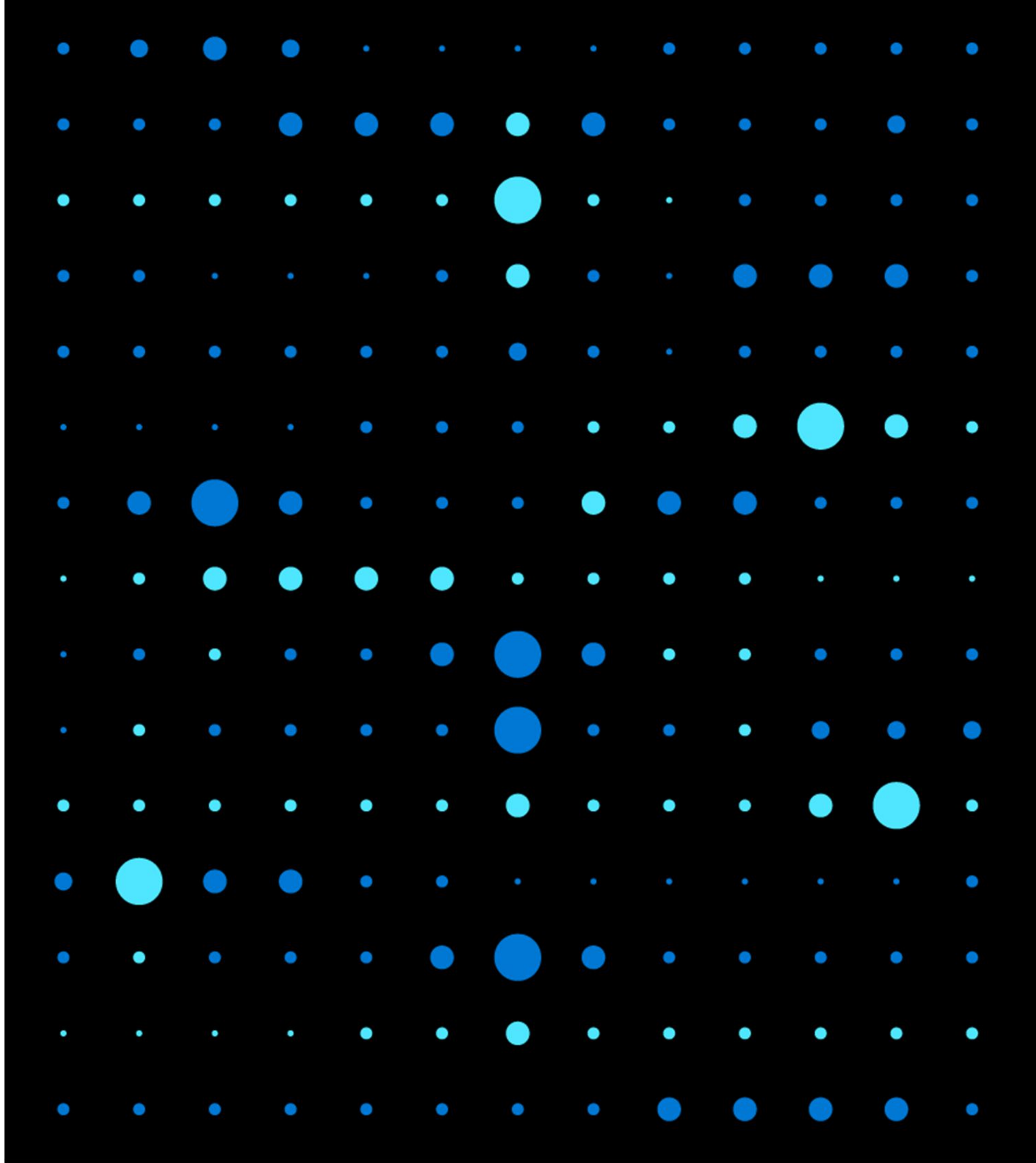
Choosing a single sign-on method depends on how the application is configured for authentication.

- **Cloud applications** can use OpenID Connect, OAuth, SAML, password-based, linked, or disabled methods for single sign-on.
- **On-premises applications** can use password-based, Integrated Windows Authentication, header-based, linked, or disabled methods for single sign-on. The on-premises choices work when applications are configured for Application Proxy.


Start
Are you developing a new application?
Yes
OpenID Connect and OAuth
No
Are you ready to configure single sign-on for an existing app?
Yes
Is your app in the cloud or on-premises?
Cloud
Does your app support a SAML-based protocol?
No
Yes
Choose SAML
Does your app authenticate with username and password?
Yes
No
On-Premises
No
Is this app already setup for SSO with another IdP?
Yes
Choose Linked
No
Do you want to create a link to the app in the MyApps access panel?
Yes
No
Choose Disabled
Does your app support a SAML-based protocol?
Yes
Choose SAML
No
Does your app authenticate with IWA?
Yes
Choose IWA
No
Does your app authenticate with HTTP headers?
Yes
Choose Header-based
No
Does your app authenticate with username and password?
Yes
Choose Password-based
No

Demonstration: Azure AD Seamless Single Sign-On

- Prerequisites
- Enable Azure AD Connect
- Verify Seamless SSO is enabled



Configure Password Sync and Password Writeback

Enable Azure AD Self-Service Password Reset

Prerequisites:

- A working Azure AD tenant with a license
- A user with the Global Administrator role
- A non-privileged test user
- A group that the test user is a member of

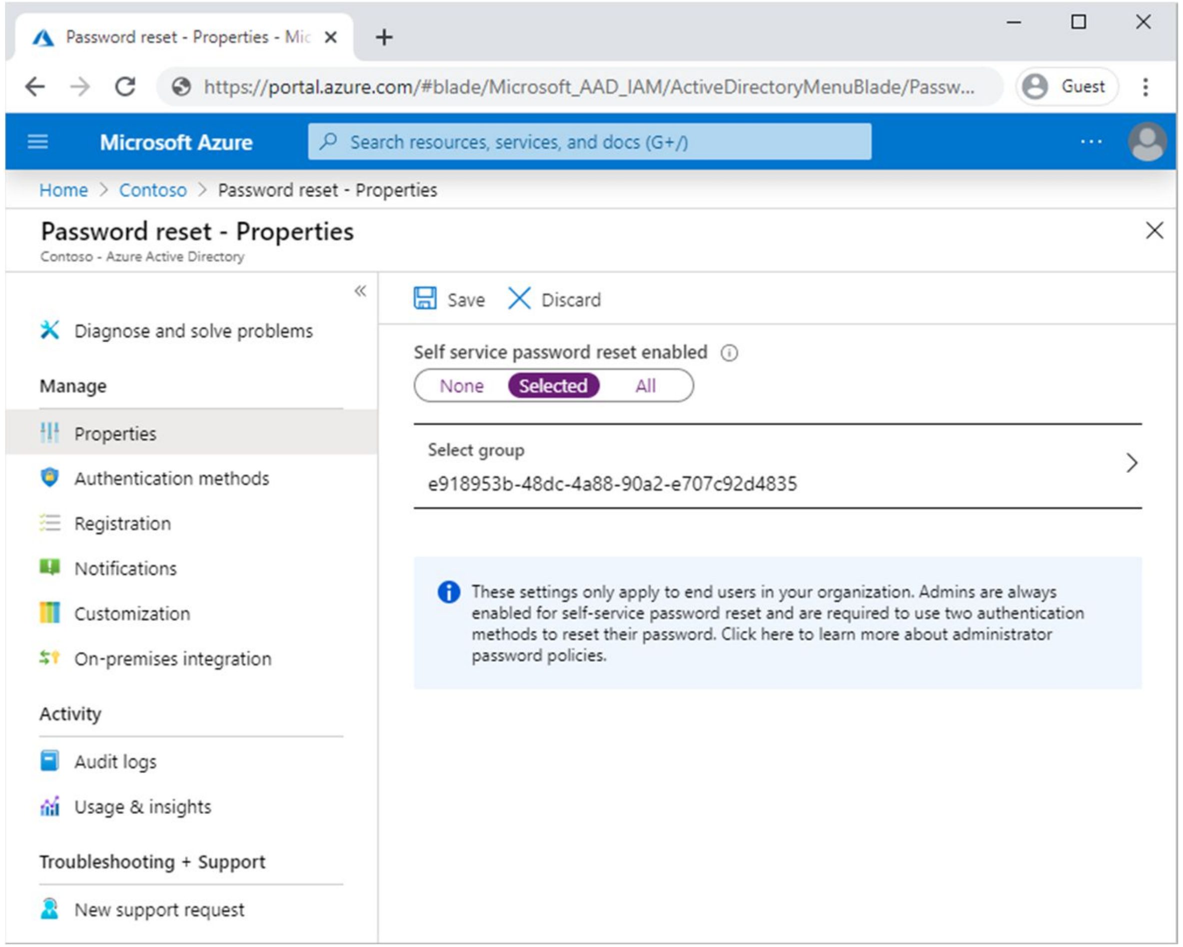
Enable self-service password reset:

- via the Azure Portal

Select authentication methods and registration options:

- Mobile app notification
- Mobile app code
- Email
- Mobile phone
- Office phone

Configure notifications and customizations


Password reset - Properties - Mic
https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Passw...
Guest
Microsoft Azure
Search resources, services, and docs (G+/)
Home > Contoso > Password reset - Properties
Password reset - Properties
Contoso - Azure Active Directory
Diagnose and solve problems
Manage
Properties
Authentication methods
Registration
Notifications
Customization
On-premises integration
Activity
Audit logs
Usage & insights
Troubleshooting + Support
New support request
Save
Discard

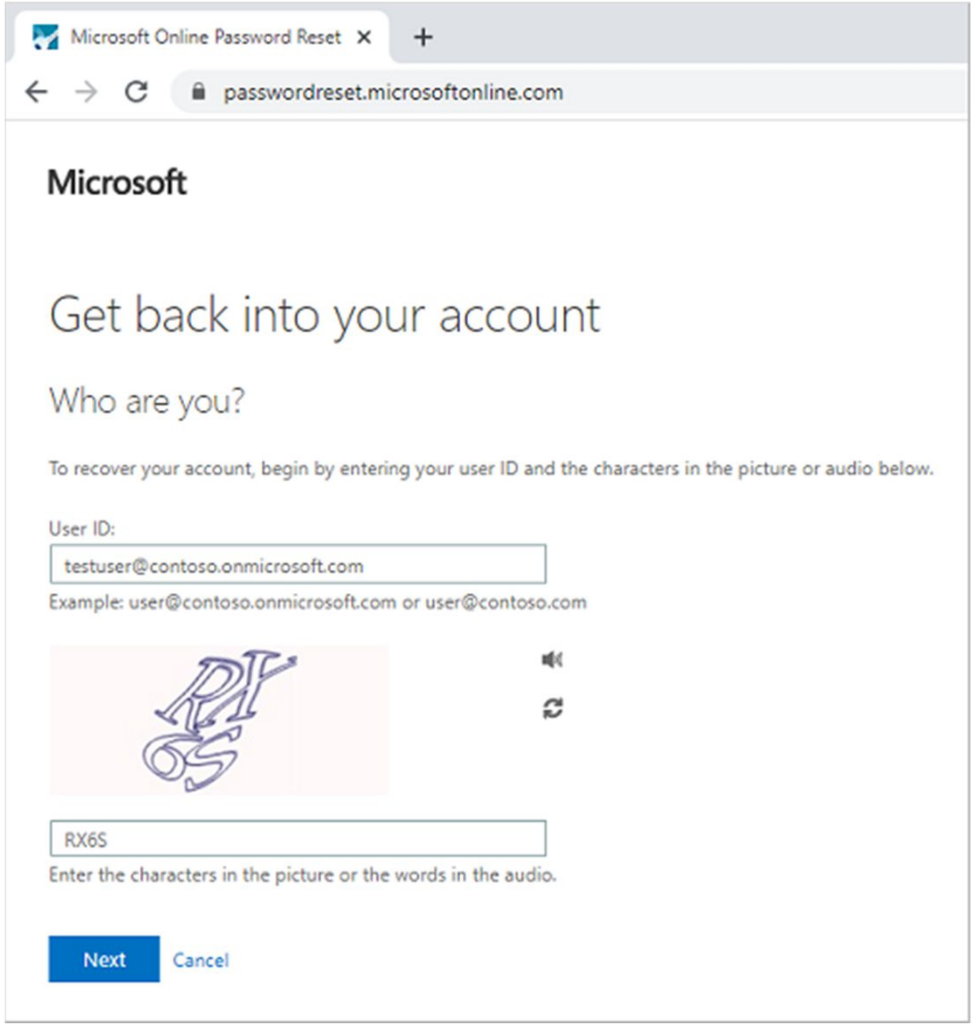
Self service password reset enabled: None [✓ Selected] All

Select group: e918953b-48dc-4a88-90a2-e707c92d4835

These settings only apply to end users in your organization. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password. Click here to learn more about administrator password policies.

Test Self-Service Password Reset

With SSPR enabled and configured, test the SSPR process as the test user



Microsoft Online Password Reset
passwordreset.microsoftonline.com
Microsoft

Get back into your account

Who are you?

To recover your account, begin by entering your user ID and the characters in the picture or audio below.

User ID: testuser@contoso.onmicrosoft.com

Example: user@contoso.onmicrosoft.com or user@contoso.com

RX6S

Enter the characters in the picture or the words in the audio.

Self-Service Password Reset (SSPR) Writeback

Password writeback offers the following benefits:

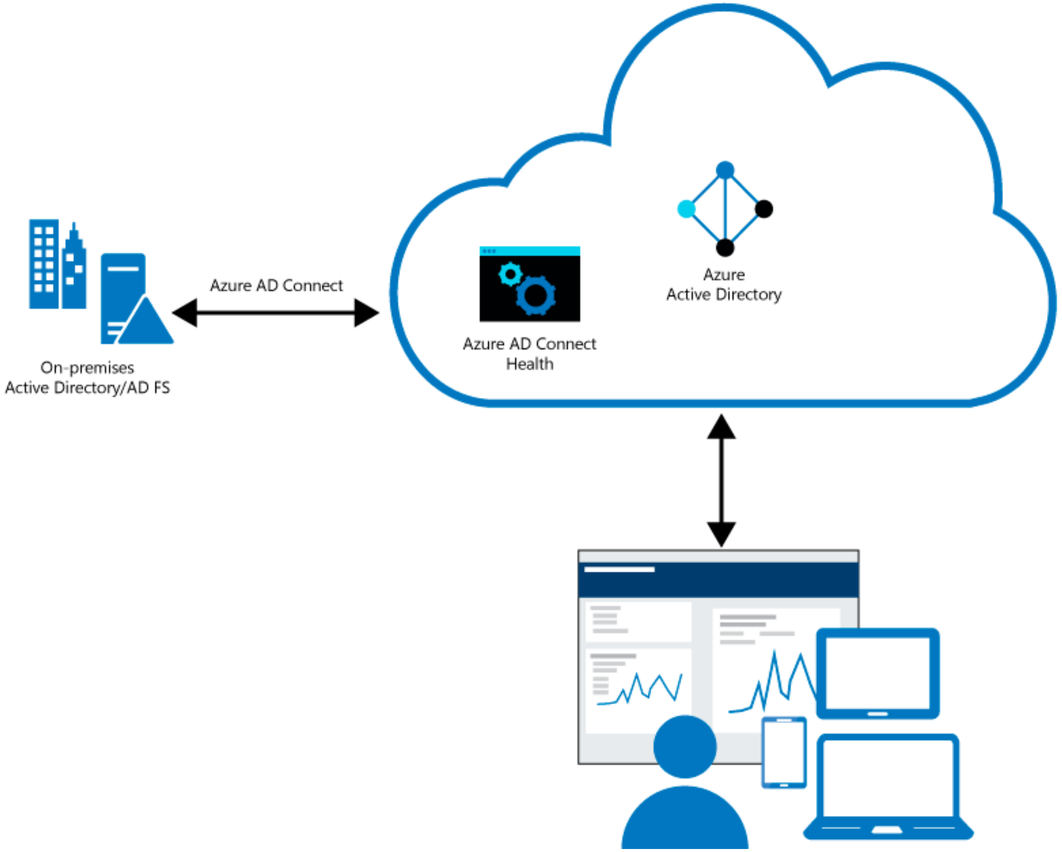
- Enforcement of Active Directory Domain Services (AD DS) password policies
- Zero-delay feedback
- Support for password changes from the Access Panel and Office 365
- Support for password writeback when an admin reset the password from the Azure portal
- No need for opening inbound ports on the edge firewall

Configure Azure AD Connect Health

Azure AD health Overview

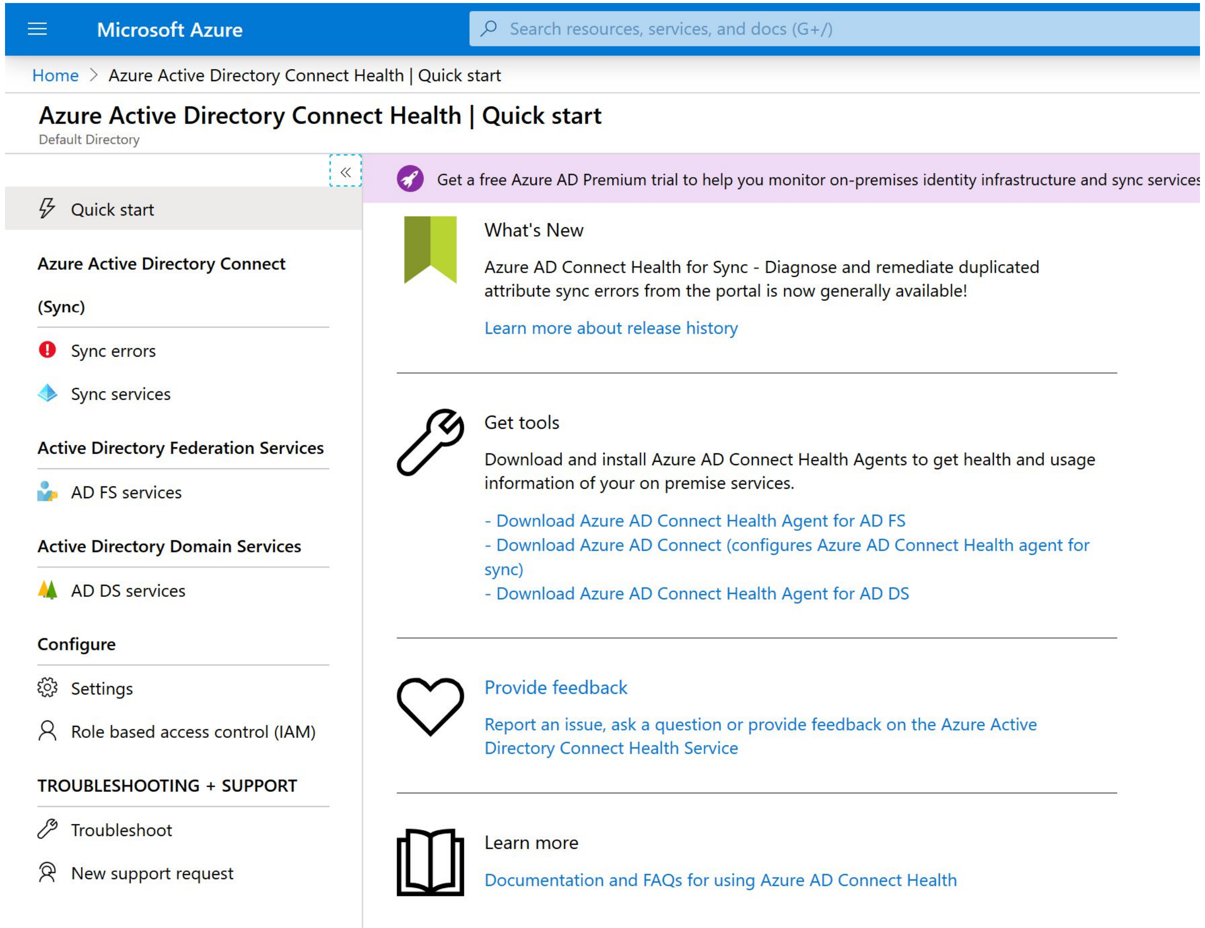
Azure AD Connect Health helps monitor on-premises identity infrastructure thus ensuring the reliability of the environment

- Key benefits:
    - Enhanced security
    - Alerts on all critical AD FS system issues
    - Simplified deployment and management
    - Rich usage metrics
    - Enhanced admin experience



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



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Azure Active Directory Connect Health | Quick start

Azure Active Directory Connect Health | Quick start

Default Directory

Quick start
Azure Active Directory Connect (Sync)
Sync errors
Sync services
Active Directory Federation Services
AD FS services
Active Directory Domain Services
AD DS services
Configure
Settings
Role based access control (IAM)
TROUBLESHOOTING + SUPPORT
Troubleshoot
New support request

Get a free Azure AD Premium trial to help you monitor on-premises identity infrastructure and sync services

What's New

Azure AD Connect Health for Sync - Diagnose and remediate duplicated attribute sync errors from the portal is now generally available!

Learn more about release history

Get tools

Download and install Azure AD Connect Health Agents to get health and usage information of your on premise services.

- Download Azure AD Connect Health Agent for AD FS
- Download Azure AD Connect (configures Azure AD Connect Health agent for sync)
- Download Azure AD Connect Health Agent for AD DS

Provide feedback

Report an issue, ask a question or provide feedback on the Azure Active Directory Connect Health Service

Learn more

Documentation and FAQs for using Azure AD Connect Health

Module Review Questions

Microsoft Azure

Online Role-based training resources:

Microsoft Learn

https://docs.microsoft.com/en-us/learn/

Microsoft Azure

Thank you.