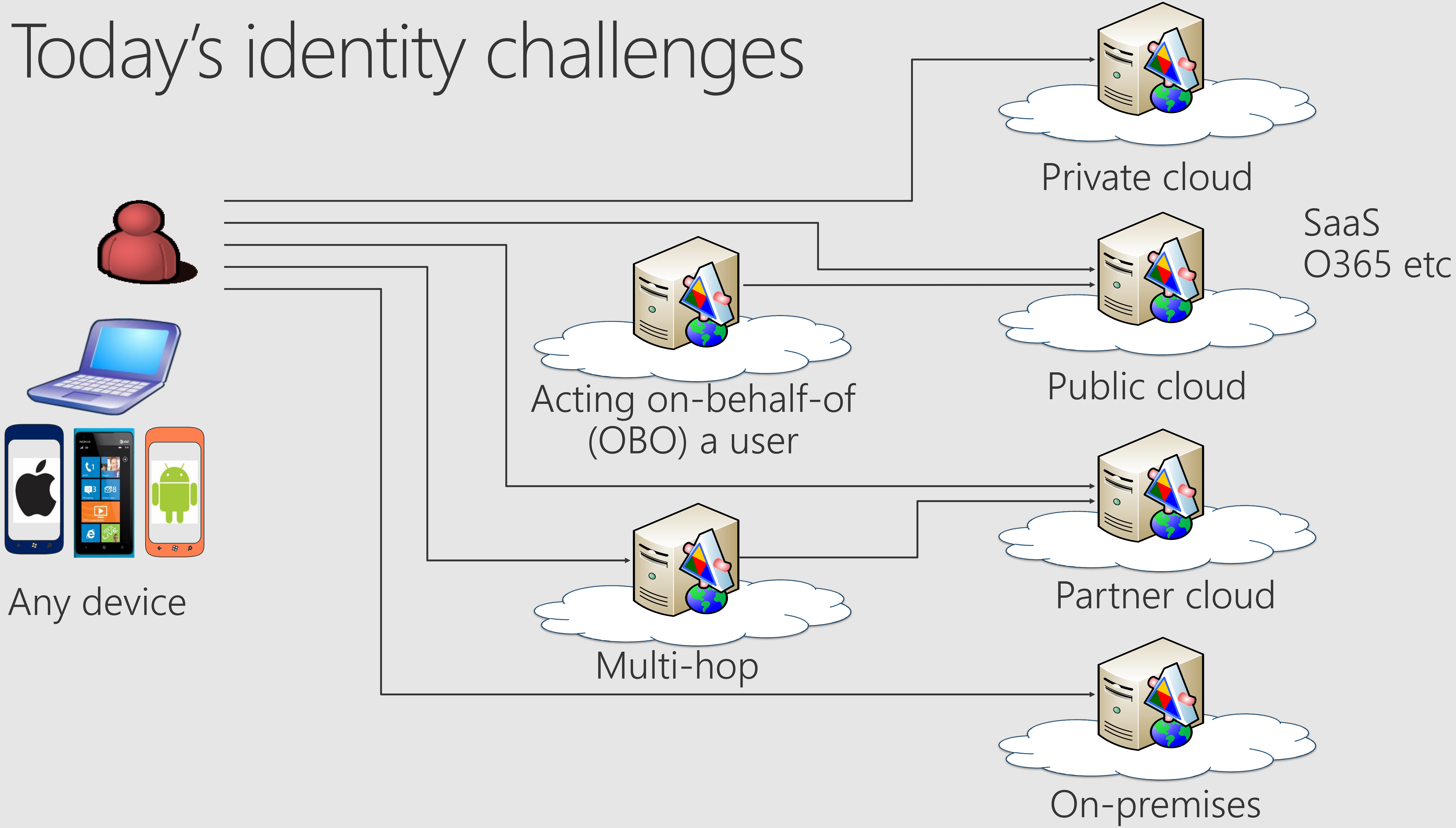
What happens with our passwords in hybrid (and what we can do about it)?

Damir Dizdarević
Logosoft d.o.o. Sarajevo
Microsoft MVP
Microsoft Regional Director

2019
NT KONFERENCA
21. - 23. MAJ 2019

#ntk19

Today's identity challenges



Private cloud

SaaS
O365 etc

Public cloud

Acting on-behalf-of
(OBO) a user

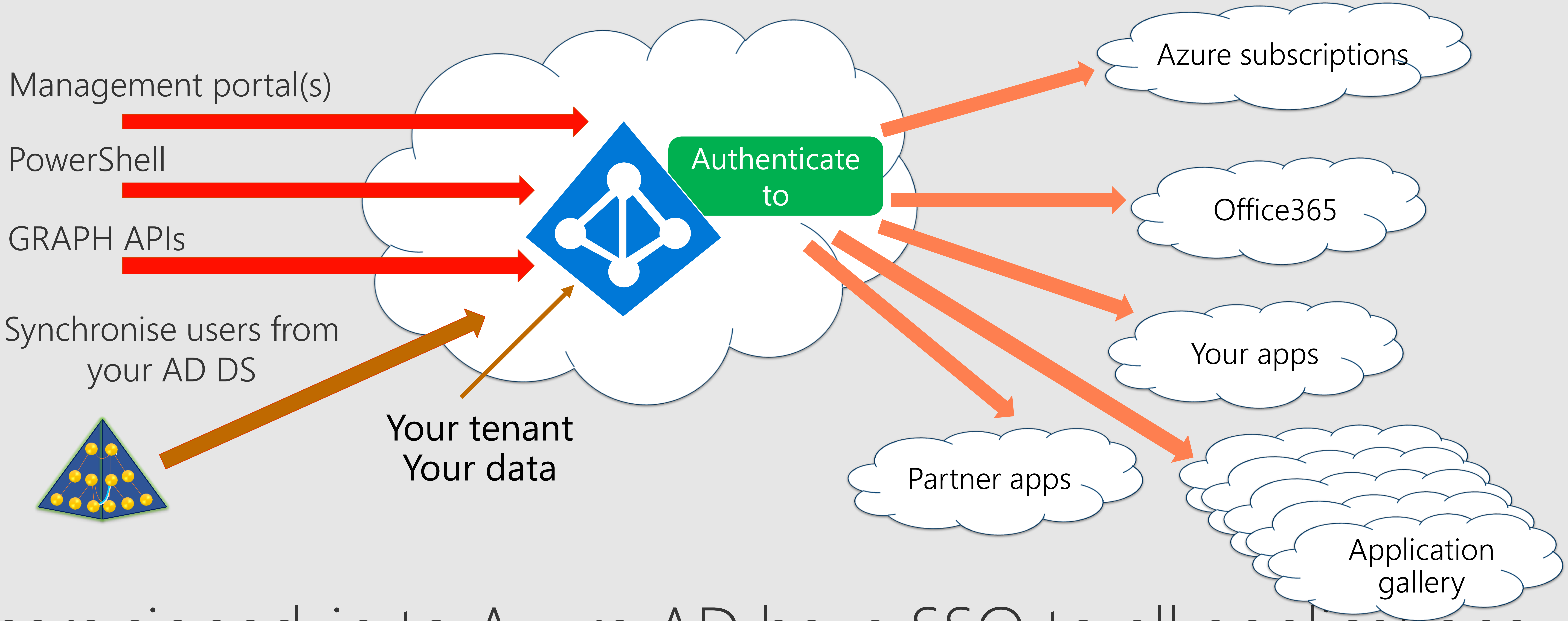
Partner cloud

Multi-hop

On-premises

Any device

Microsoft Azure AD to the rescue

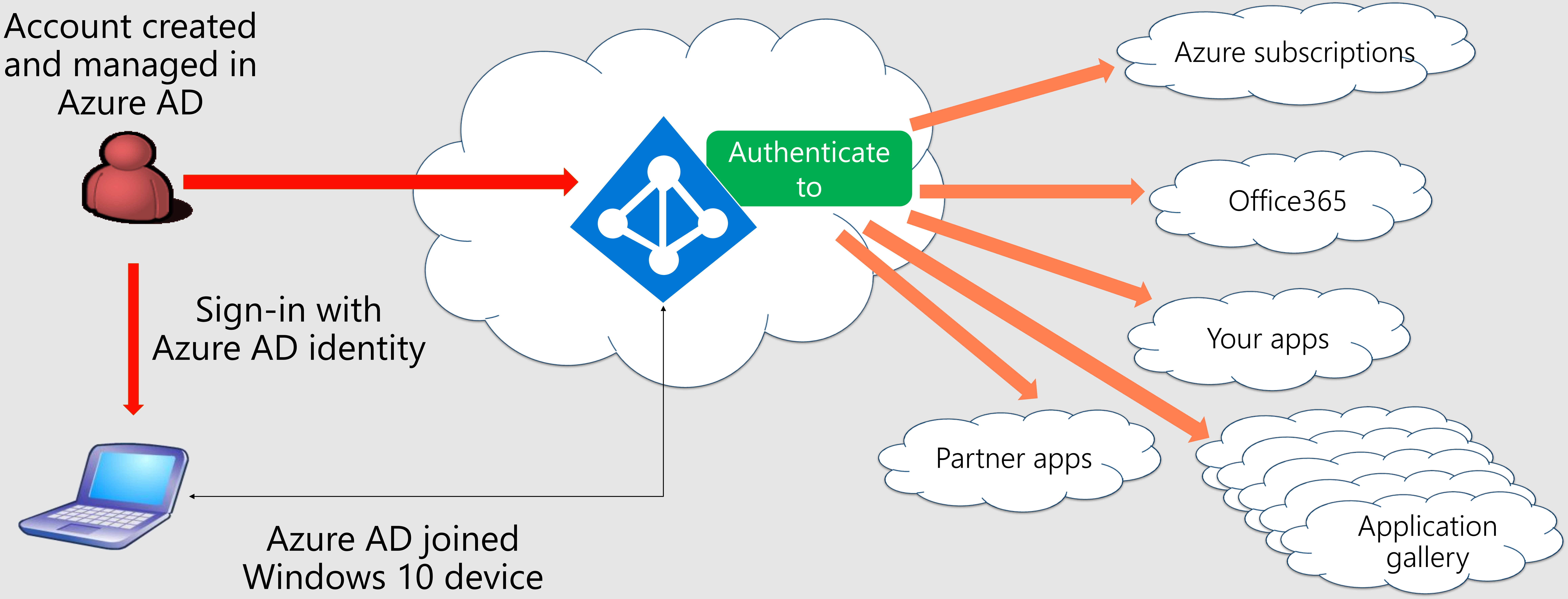


- Users signed-in to Azure AD have SSO to all applications

Azure AD benefits

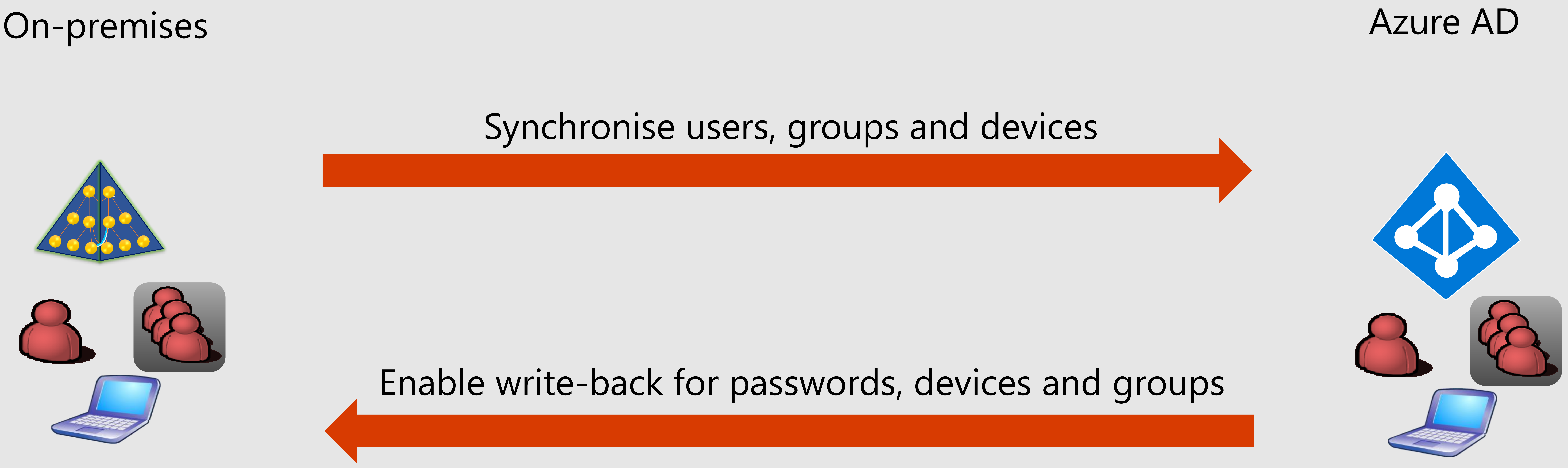
- Authentication to applications via
  - OpenID Connect / Oauth 2.0
  - WS-Federation and SAML
  - Windows Kerberos Authentication via the Azure AD Application Proxy
- Self-service for:
  - Password resets, application and group management
- MFA
- Conditional access
- Identity protection
- And more…

Cloud only user



Account created and managed in Azure AD
Sign-in with Azure AD identity
Authenticate to
Azure subscriptions
Office365
Your apps
Partner apps
Application gallery
Azure AD joined Windows 10 device

Unleash on-premises AD users



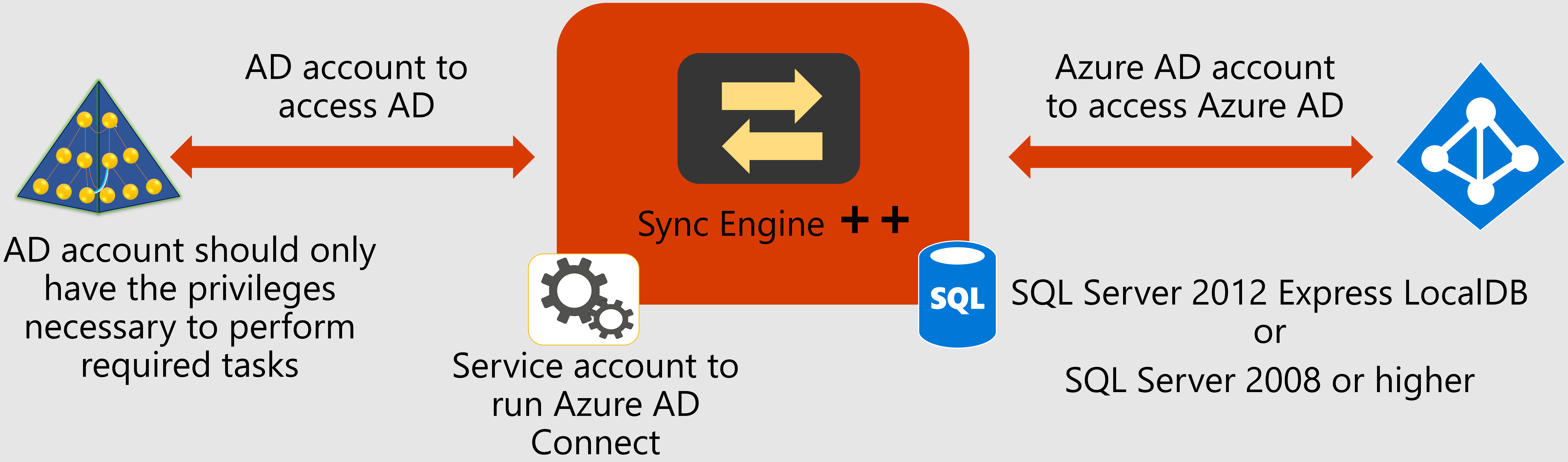
On-premises

Azure AD

Synchronise users, groups and devices

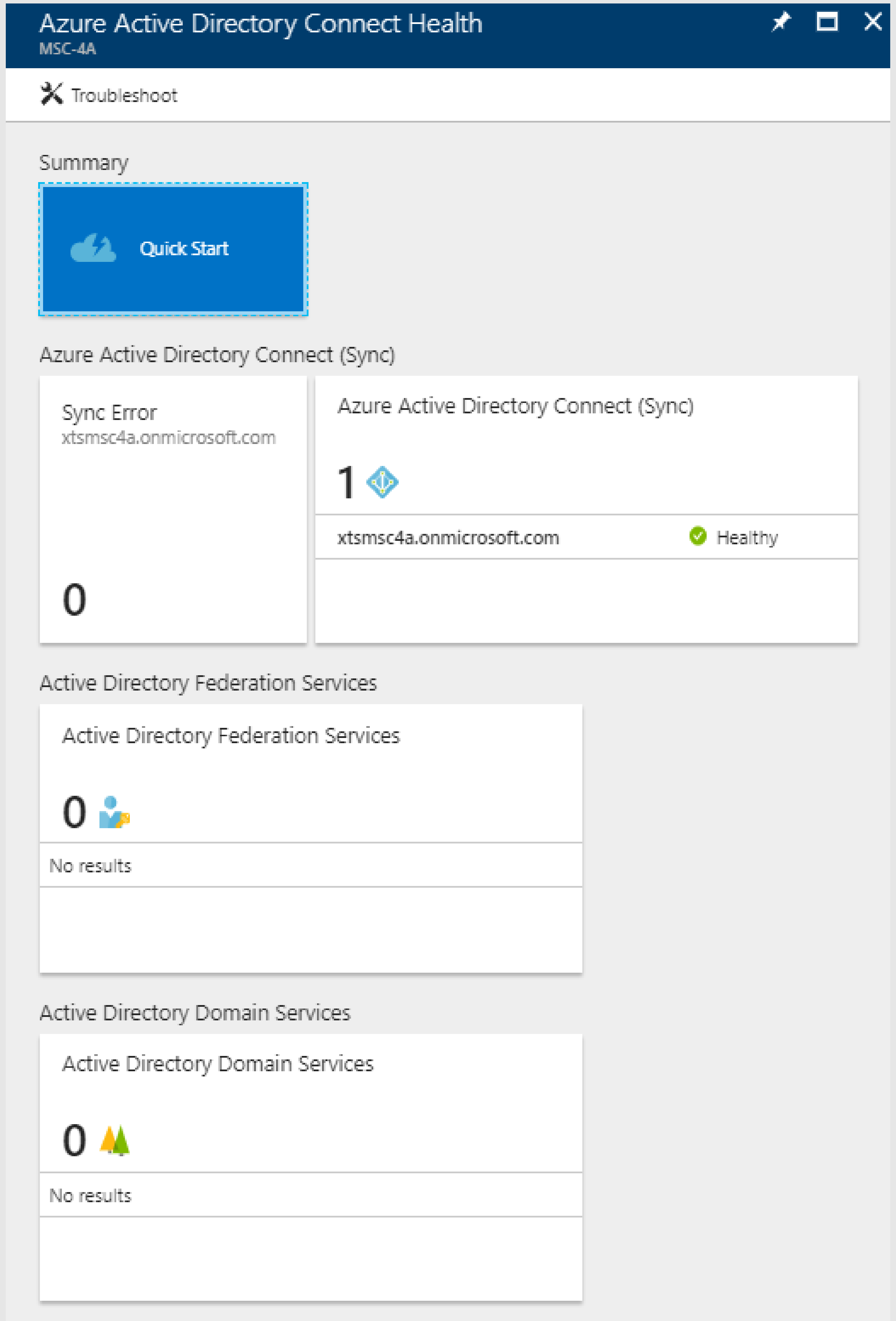
Enable write-back for passwords, devices and groups

Azure AD Connect


AD account to access AD
Sync Engine ++
Azure AD account to access Azure AD
AD account should only have the privileges necessary to perform required tasks
Service account to run Azure AD Connect
SQL
SQL Server 2012 Express LocalDB
or
SQL Server 2008 or higher

- Continuously evolving product
  - Automatic upgrades are possible
    - Set-ADSyncAutoUpgrade

Azure AD Connect Health



Azure Active Directory Connect Health
MSC-4A

Troubleshoot

Summary

Quick Start

Azure Active Directory Connect (Sync)

Sync Error
xtsmsc4a.onmicrosoft.com
0

Azure Active Directory Connect (Sync)
1

xtsmsc4a.onmicrosoft.com ✓ Healthy

Active Directory Federation Services

Active Directory Federation Services
0

No results

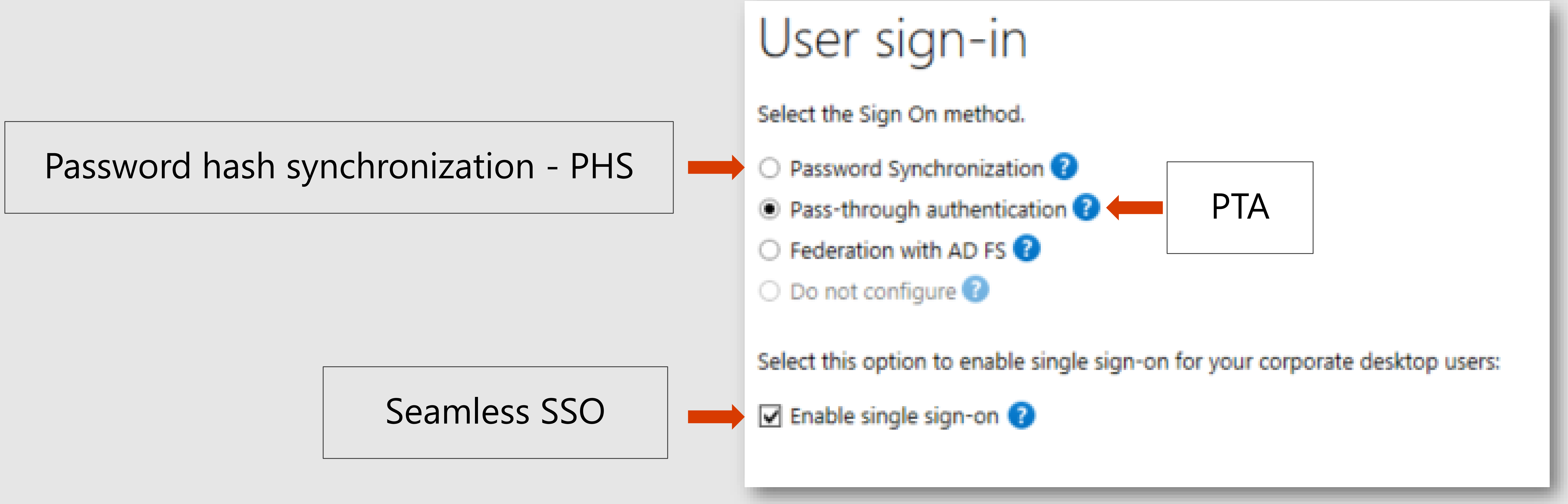
Active Directory Domain Services

Active Directory Domain Services
0

No results

- One-stop shop for viewing the health of your identity infrastructure
  - Azure AD Connect
  - AD FS
  - On-premises AD DS
  - Roles review
- Agents installed on identity infrastructure components
  - Monitoring and alerts
  - Email notification of critical alerts
  - Trends in performance data
  - Usage reports
- Requires a P1 license

Configuring Azure AD password/auth options



Password hash synchronization - PHS

PTA

Seamless SSO

User sign-in

Select the Sign On method.

○ Password Synchronization
● Pass-through authentication
○ Federation with AD FS
○ Do not configure

Select this option to enable single sign-on for your corporate desktop users:

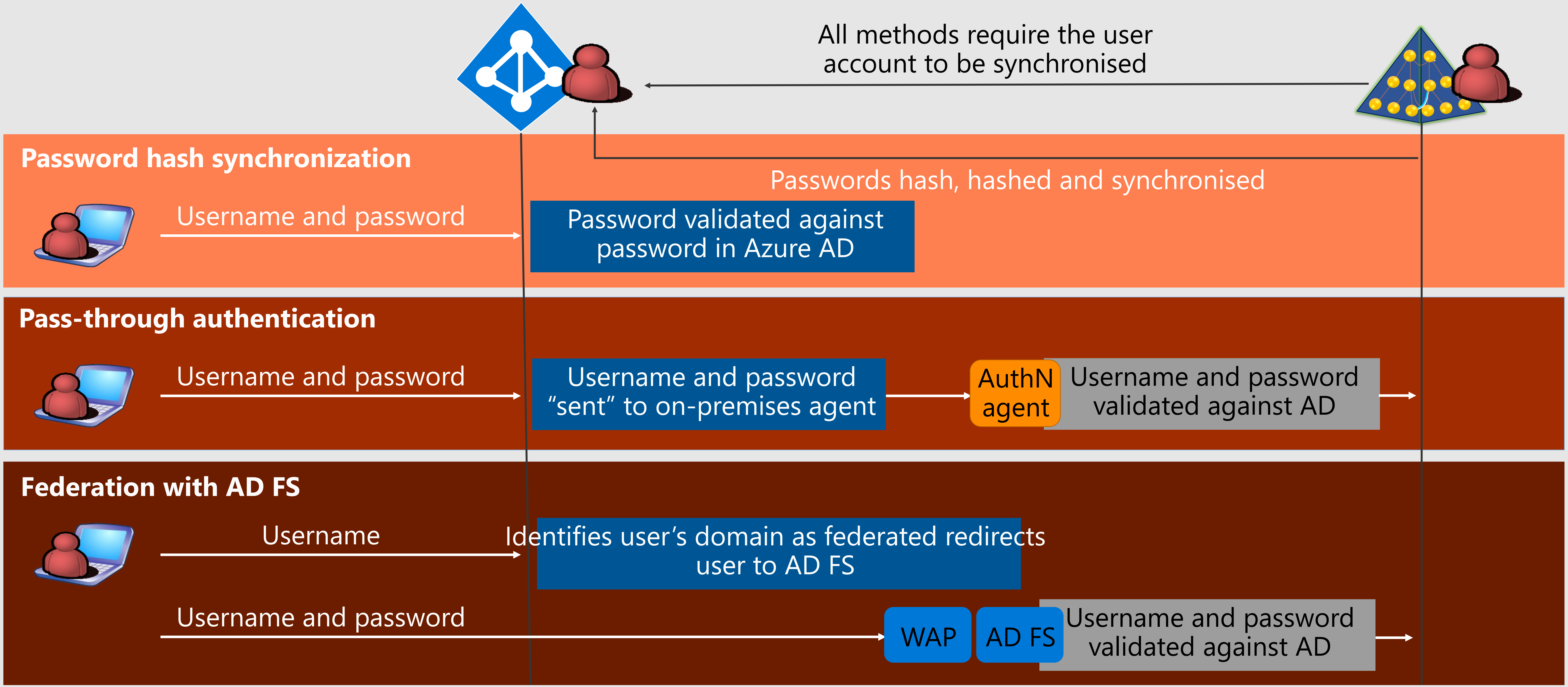
☑ Enable single sign-on

- The options defines how a synchronized on premises user signs in to Azure AD
  - "Do not configure" is used if a 3rd party federated solution is being used
- Seamless SSO works with PHS and PTA

Managing on-premises passwords

- With PHS enabled, on-premises password changes sync to Azure AD **within 2 minutes**
- Password reset for on-premises passwords available via the Azure AD:
  - Requires password writeback
  - Works for passwords reset by the administrator
  - Works for Self-Service Password Resets (SSPR)
  - Synchronous operation
  - Enforces on-premises password policies
  - Passwords for protected on-premises accounts cannot be reset

On-premises user sign-in to Azure AD



All methods require the user account to be synchronised

Password hash synchronization

Username and password

Password validated against password in Azure AD

Passwords hash, hashed and synchronised

Pass-through authentication

Username and password

Username and password "sent" to on-premises agent

AuthN agent

Username and password validated against AD

Federation with AD FS

Username

Identifies user's domain as federated redirects user to AD FS

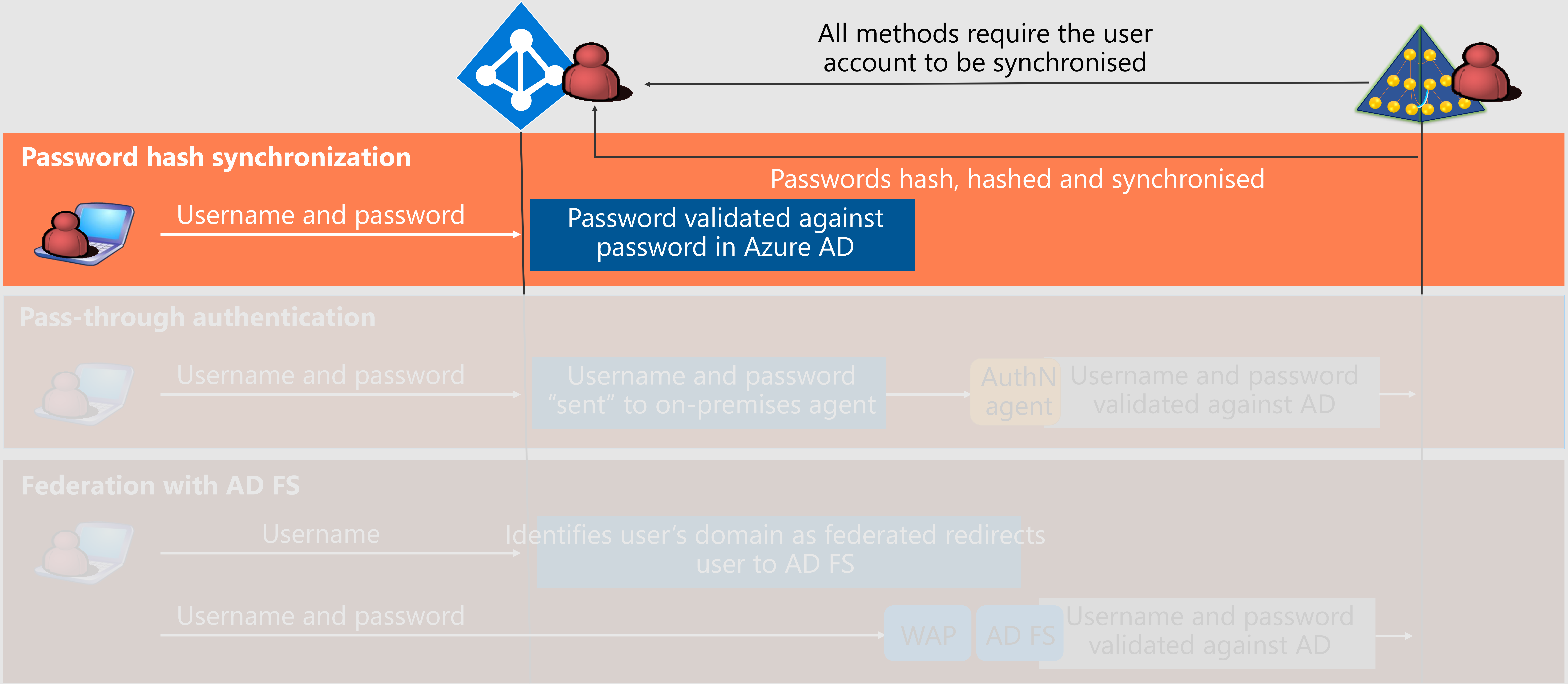
Username and password

WAP

AD FS

Username and password validated against AD

On-premises user sign-in to Azure AD



All methods require the user account to be synchronised

Password hash synchronization

Username and password

Passwords hash, hashed and synchronised

Password validated against password in Azure AD

Pass-through authentication

Username and password

Username and password "sent" to on-premises agent

AuthN agent

Username and password validated against AD

Federation with AD FS

Username

Identifies user's domain as federated redirects user to AD FS

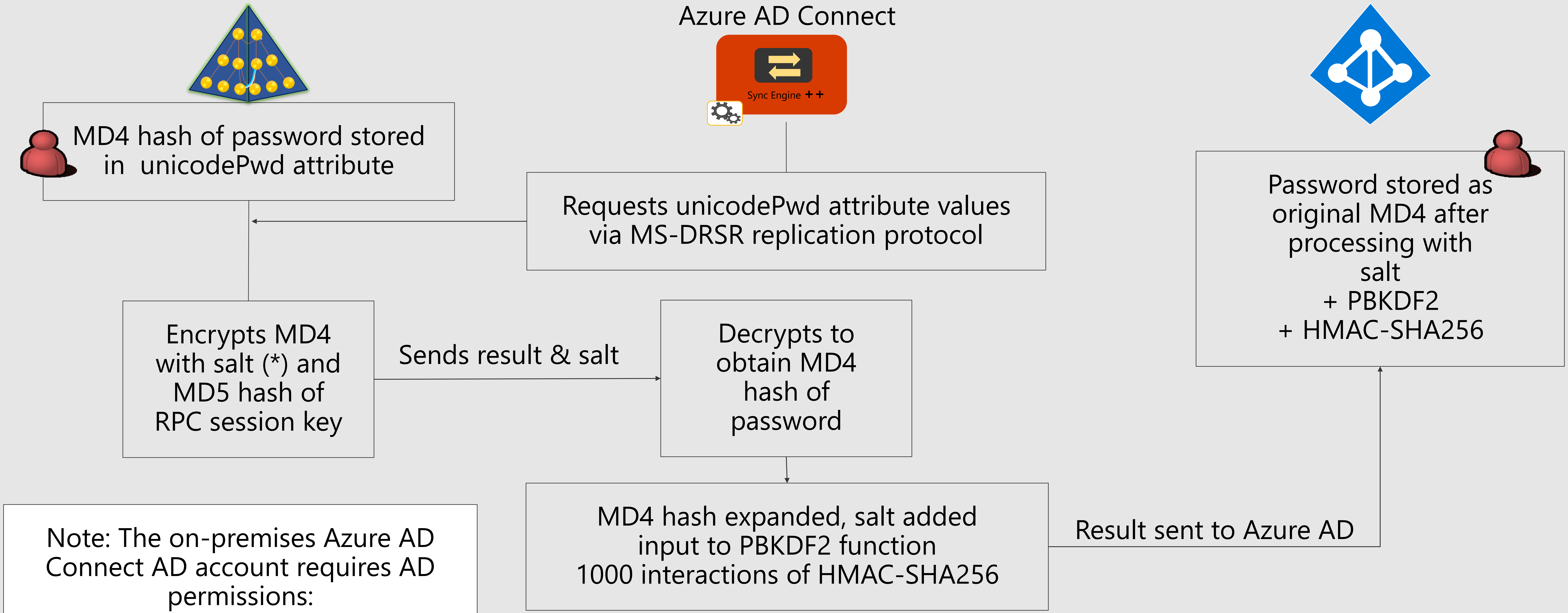
Username and password

WAP

AD FS

Username and password validated against AD

Password synchronization



Azure AD Connect

MD4 hash of password stored in unicodePwd attribute

Requests unicodePwd attribute values via MS-DRSR replication protocol

Encrypts MD4 with salt (*) and MD5 hash of RPC session key

Sends result & salt

Decrypts to obtain MD4 hash of password

MD4 hash expanded, salt added input to PBKDF2 function 1000 interactions of HMAC-SHA256

Result sent to Azure AD

Password stored as original MD4 after processing with salt
+ PBKDF2
+ HMAC-SHA256

Note: The on-premises Azure AD Connect AD account requires AD permissions:

Replicate Directory Changes
Replicate Directory Changes All

Sign in

Does supplied password value, after processing with MD4, with salt, PBKDF2 and HMAC-SHA256, match stored value for user?

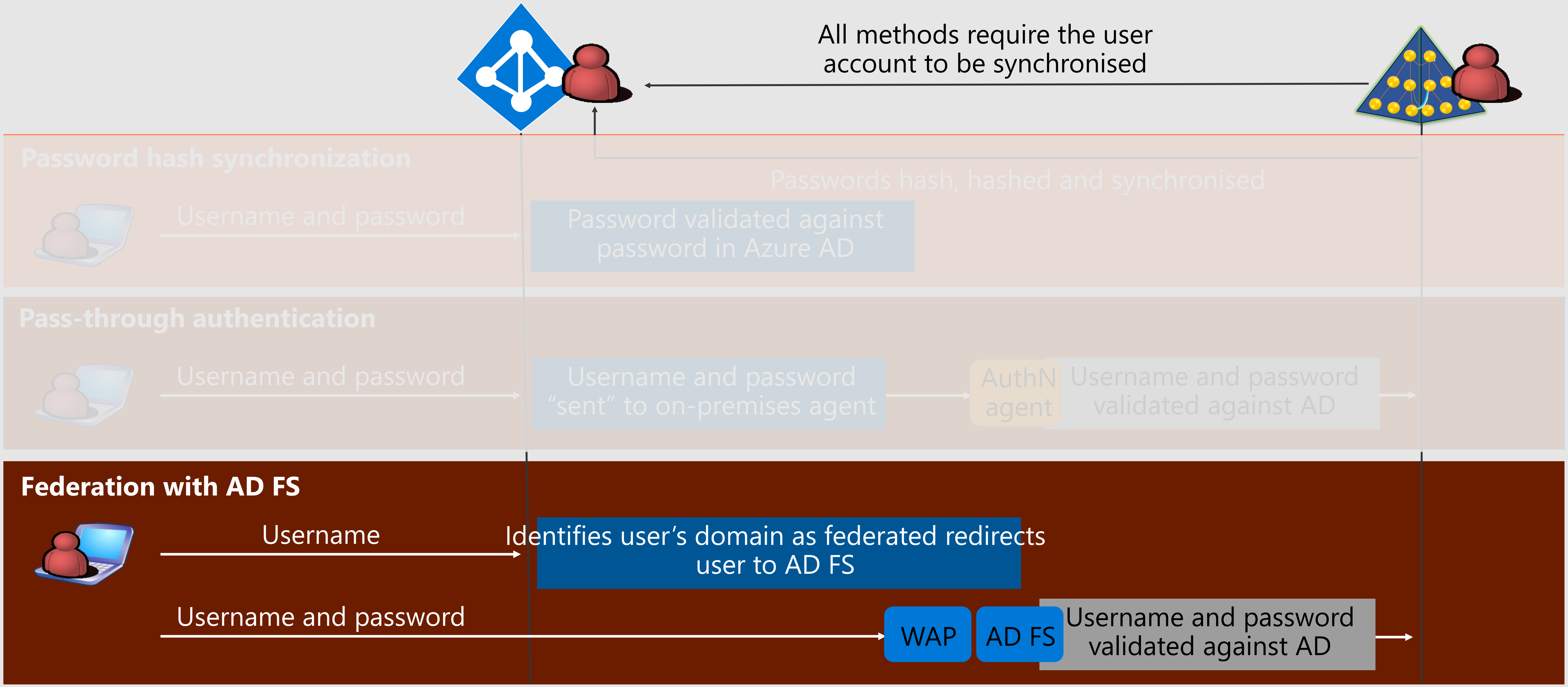
(*) salt is random data that is used as an additional input to a one-way function that "hashes" data

PBKDF = password based Key Derivation Function (RFC 2898)

Password synchronization facts…

- On-premises password complexity applies to synchronized users
  - If an administrator changes the cloud password using PowerShell the Azure AD password policy applies
- accountExpires attribute is not synchronized to Azure AD
- An locked out on-premises AD account can still be active in the cloud
- The cloud password for a PHS user is set to never expire.
- A disabled on-premises AD account will not be reflected in Azure AD until the next sync cycle
  - Potentially 30 mins delay
- PHS can be used in addition to federation and used as a fall-back

On-premises user sign-in to Azure AD



All methods require the user account to be synchronised

Password hash synchronization

Passwords hash, hashed and synchronised

Username and password

Password validated against password in Azure AD

Pass-through authentication

Username and password

Username and password “sent” to on-premises agent

AuthN agent

Username and password validated against AD

Federation with AD FS

Username

Identifies user’s domain as federated redirects user to AD FS

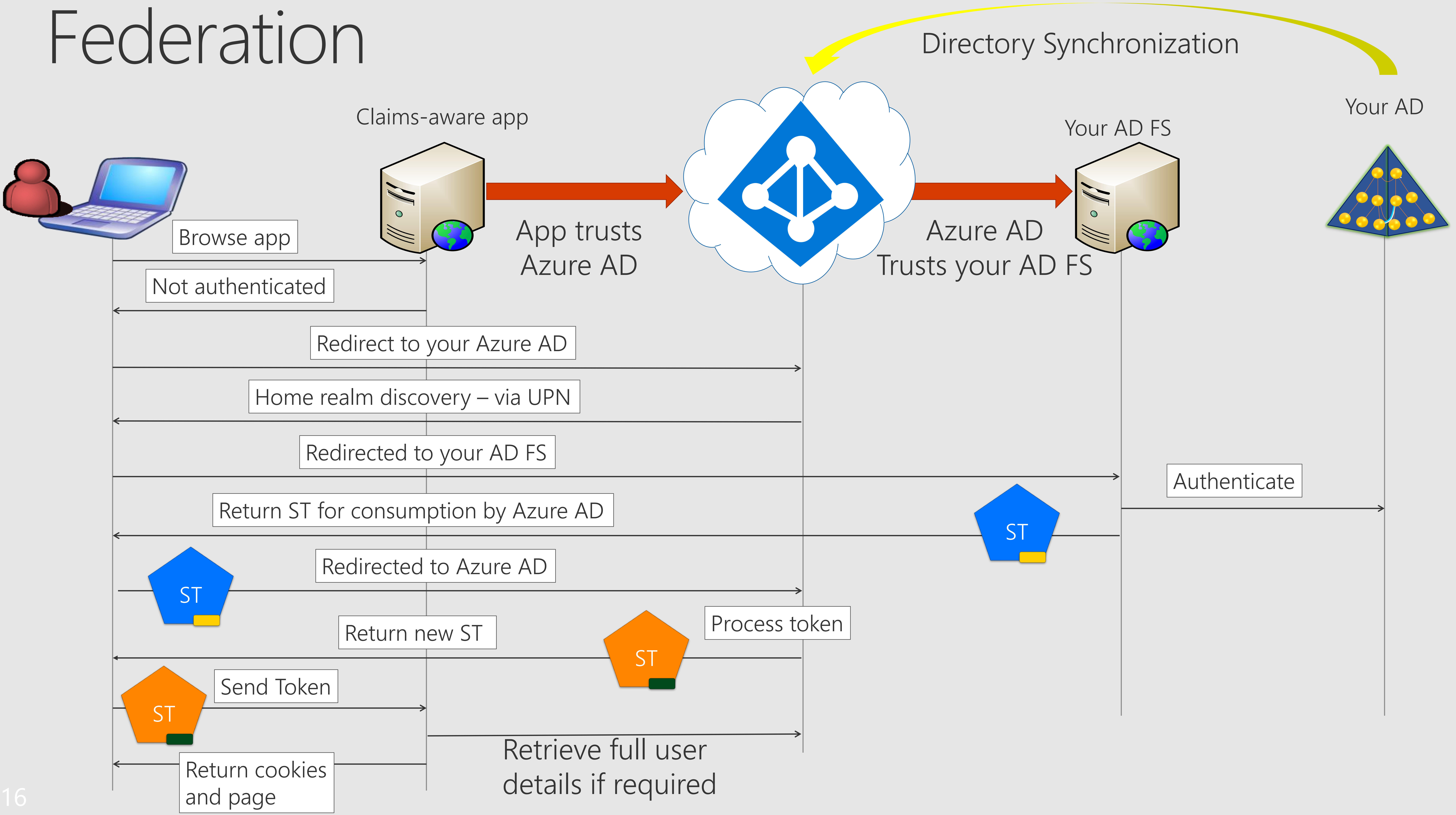
Username and password

WAP

AD FS

Username and password validated against AD

Federation


Directory Synchronization
Claims-aware app
Your AD FS
Your AD
App trusts Azure AD
Azure AD Trusts your AD FS
Browse app
Not authenticated
Redirect to your Azure AD
Home realm discovery – via UPN
Redirected to your AD FS
Authenticate
Return ST for consumption by Azure AD
ST
Redirected to Azure AD
ST
Return new ST
ST
Process token
Send Token
ST
Retrieve full user details if required
Return cookies and page

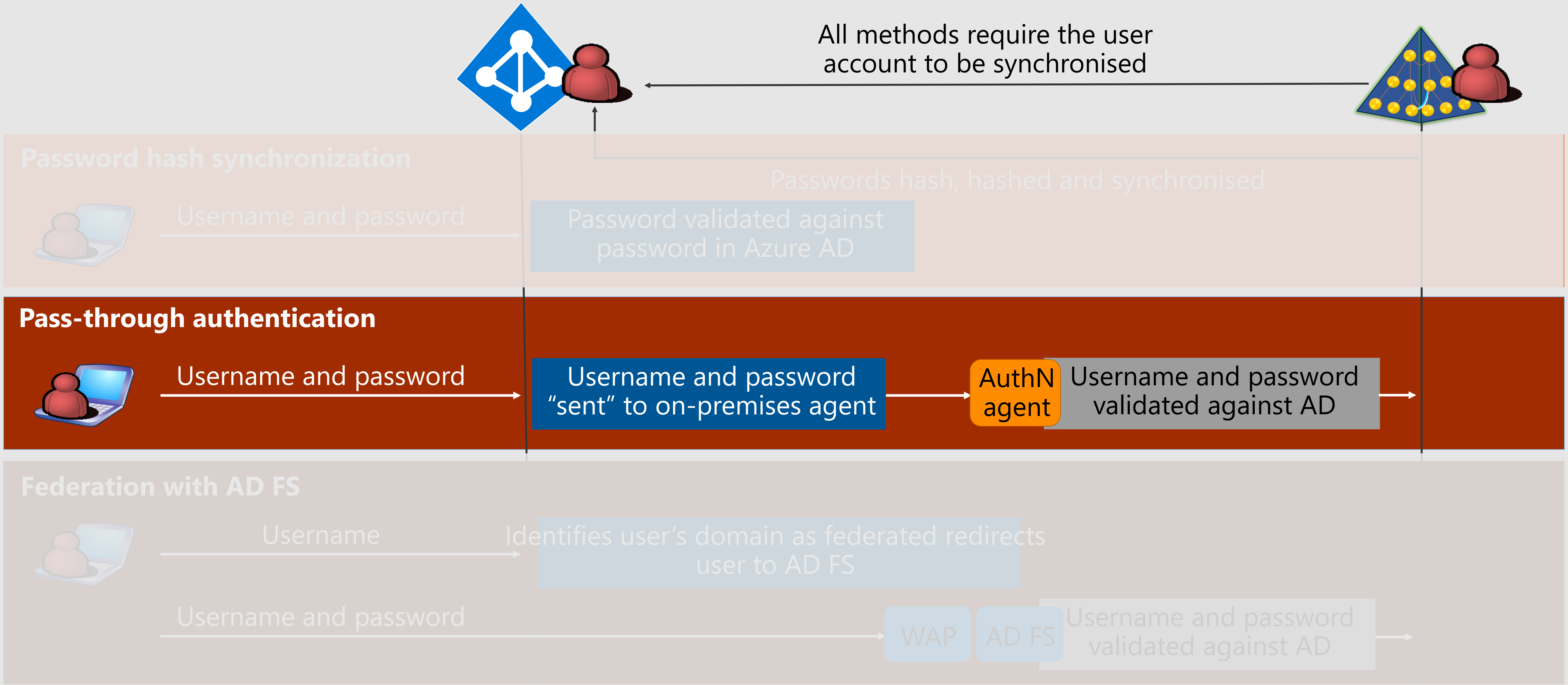
To federate or not? The facts…

- Federation gives you
  - SSO via on premises AD credentials
    - Seamlessly authenticate to AD FS when the client is attached to the corporate network
      - Now supported by Seamless SSO for PHS and PTA
  - Passwords remain on-premises
    - Now supported via PTA
  - On-premises authentication policies
    - Now supported via PTA
  - On-premises authentication methods (multi-factor)
  - Conditional access via AD FS
    - Capabilities++ provided by Azure AD
- Federation requires
  - On-premises AD FS infrastructure with high-availability
  - High-availability for the company’s Internet connection
    - Remote workers will not be able to authenticate to Azure AD If the link is down
  - Planned recovery from the loss of AD FS availability

To federate or not? More facts…

- Federation may require manual certificate rollover
  - Auto renewal possible for most configurations (AD FS auto certificate rollover enabled)
- Federation **doesn’t** give you
  - Cloud authentication scalability
  - Identity Protection
    - Requires P2 license
- PHS & PTA
  - Cloud authentication
  - Cloud scalability
  - Identity protect
- PTA
  - Simple deployment of agents
  - Automatic update of on-premises agents
  - Automatic rollover of certificates
  - Requires high-availability for the company’s Internet connection

On-premises user sign-in to Azure AD



All methods require the user account to be synchronised

Password hash synchronization

Passwords hash, hashed and synchronised

Username and password

Password validated against password in Azure AD

Pass-through authentication

Username and password

Username and password “sent” to on-premises agent

AuthN agent

Username and password validated against AD

Federation with AD FS

Username

Identifies user’s domain as federated redirects user to AD FS

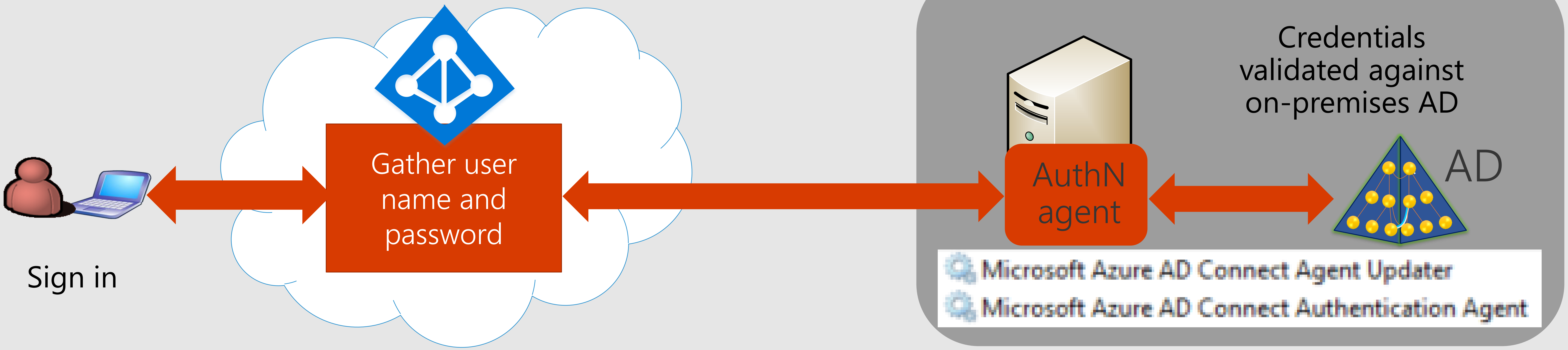
Username and password

WAP

AD FS

Username and password validated against AD

Pass-through authentication

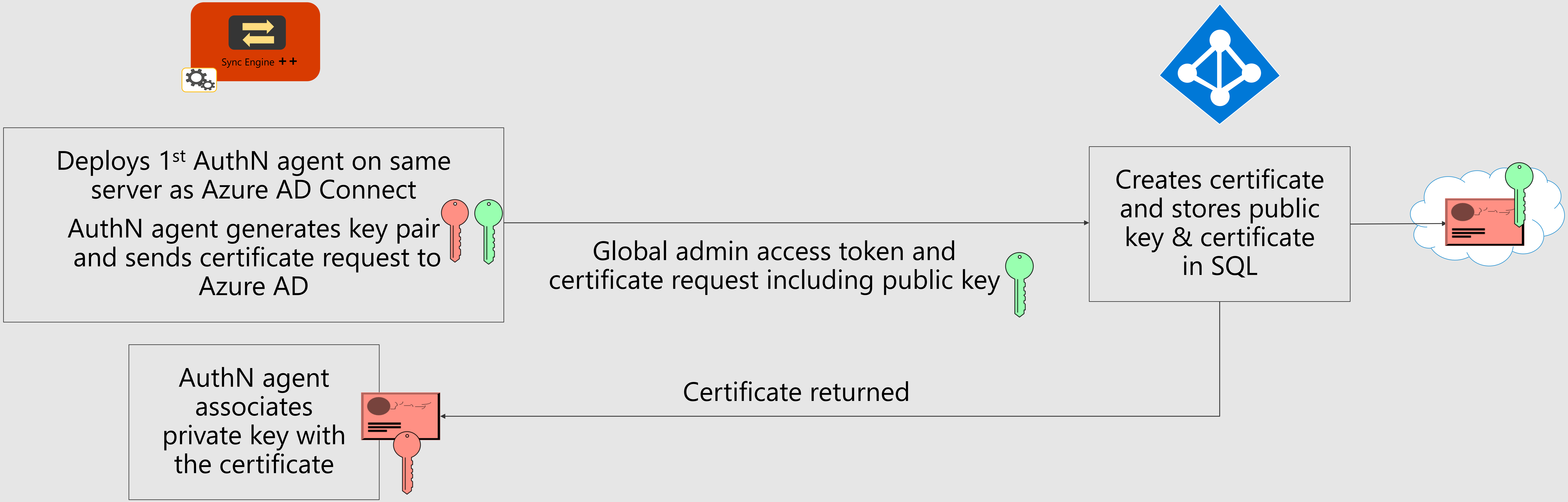

Gather user name and password
Sign in
Credentials validated against on-premises AD
AuthN agent
AD

Microsoft Azure AD Connect Agent Updater

Microsoft Azure AD Connect Authentication Agent

- The pass-through authentication agent (AuthN agent) only requires outbound firewall ports
  - Port 80 and 443
- Multiple agents should be deployed for fault tolerance and performance
  - Three agents should provide required performance
- All communications via mutually authenticated HTTPS

Pass-through authentication installation



Deploys 1st AuthN agent on same server as Azure AD Connect

AuthN agent generates key pair and sends certificate request to Azure AD

Global admin access token and certificate request including public key

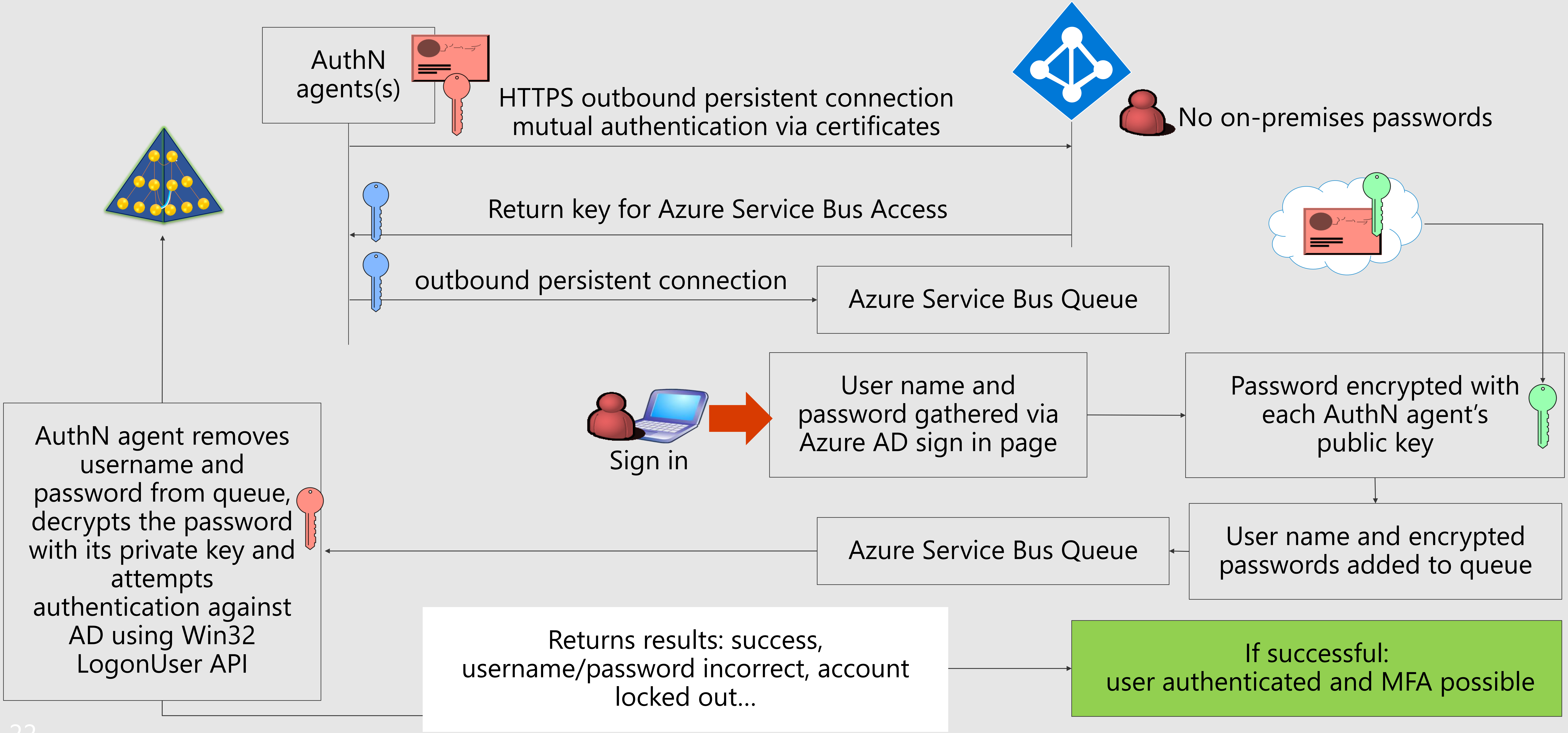
Creates certificate and stores public key & certificate in SQL

Certificate returned

AuthN agent associates private key with the certificate

- Each agent has its own unique certificate and private key
  - Azure AD periodically triggers the renewal of certificates and keys

Pass-through authentication in action



AuthN agents(s)

HTTPS outbound persistent connection mutual authentication via certificates

No on-premises passwords

Return key for Azure Service Bus Access

outbound persistent connection

Azure Service Bus Queue

Sign in

User name and password gathered via Azure AD sign in page

Password encrypted with each AuthN agent’s public key

User name and encrypted passwords added to queue

Azure Service Bus Queue

AuthN agent removes username and password from queue, decrypts the password with its private key and attempts authentication against AD using Win32 LogonUser API

Returns results: success, username/password incorrect, account locked out…

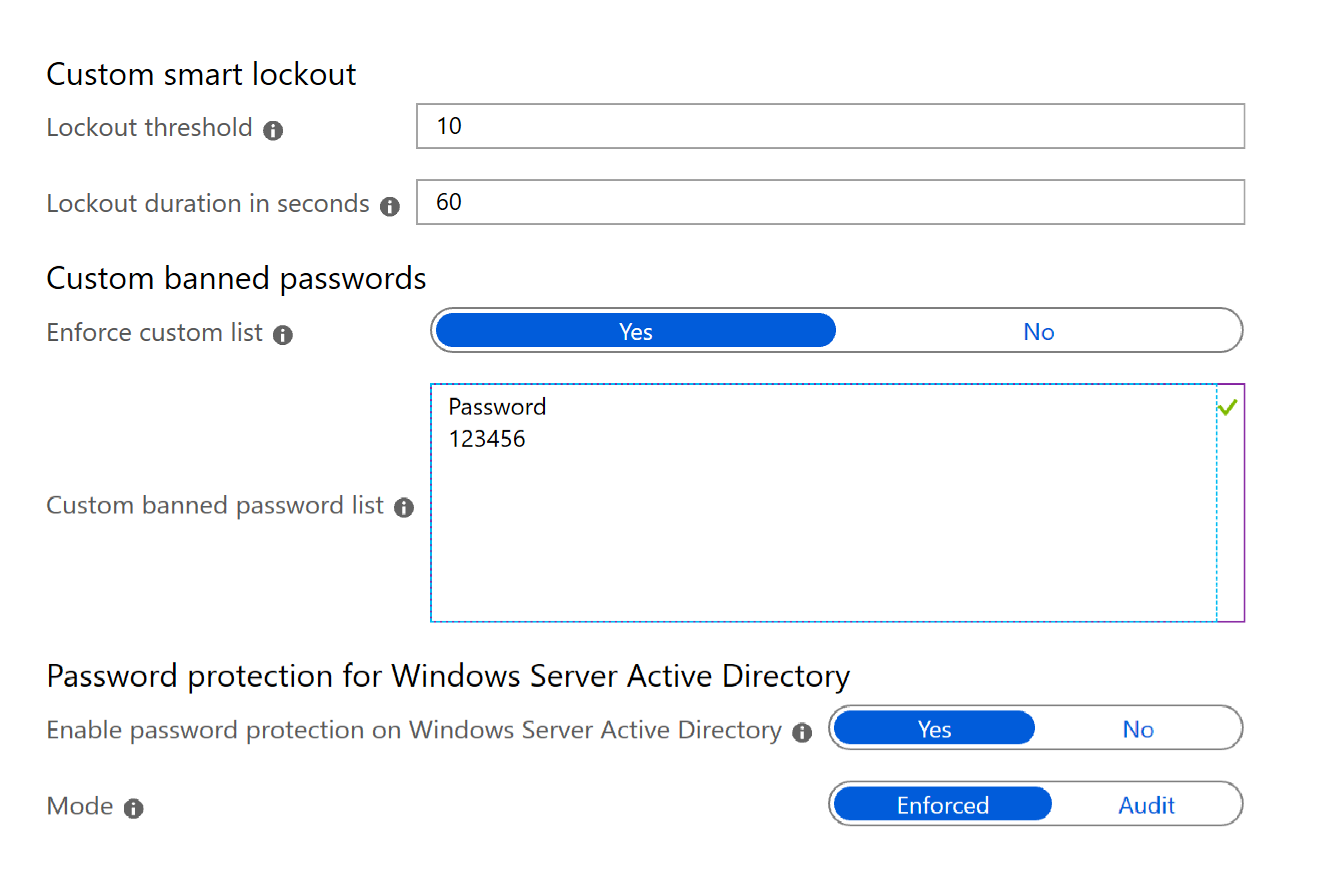
If successful:
user authenticated and MFA possible

Pass-through authentication the facts…

- No on premises passwords in the cloud
- All on-premises password policies operational
- Account lockout/disabled operational
- Does not support on-premises MFA
  - Azure AD MFA supported
- Works with Alternate ID
- Does not provide SSO for on-premises credentials
  - Requires Seamless SSO
- Requires high-availability for the company's Internet connection
  - Remote workers will not be able to authenticate to Azure AD If the link is down
- Currently does not support legacy auth
  - Example Office 2010

Account lockout and password protection

- Azure AD Smart Lockout protects against brute-force attacks and on-premises account lockout
- Locks account in Azure AD
  - Lockout Threshold – default 10 failed attempts
  - Lockout Duration – default 60 seconds
    - Automatically increases with a continuing attack
- Machine intelligence algorithms attempt to distinguish between genuine users and attackers
  - Factors include past sign-in behaviour, user's devices and browsers
  - Lockout Threshold automatically adjusted



Custom smart lockout

Lockout threshold: 10

Lockout duration in seconds: 60

Custom banned passwords

Enforce custom list: [✓ Yes] No

Custom banned password list:

Password
123456

Password protection for Windows Server Active Directory

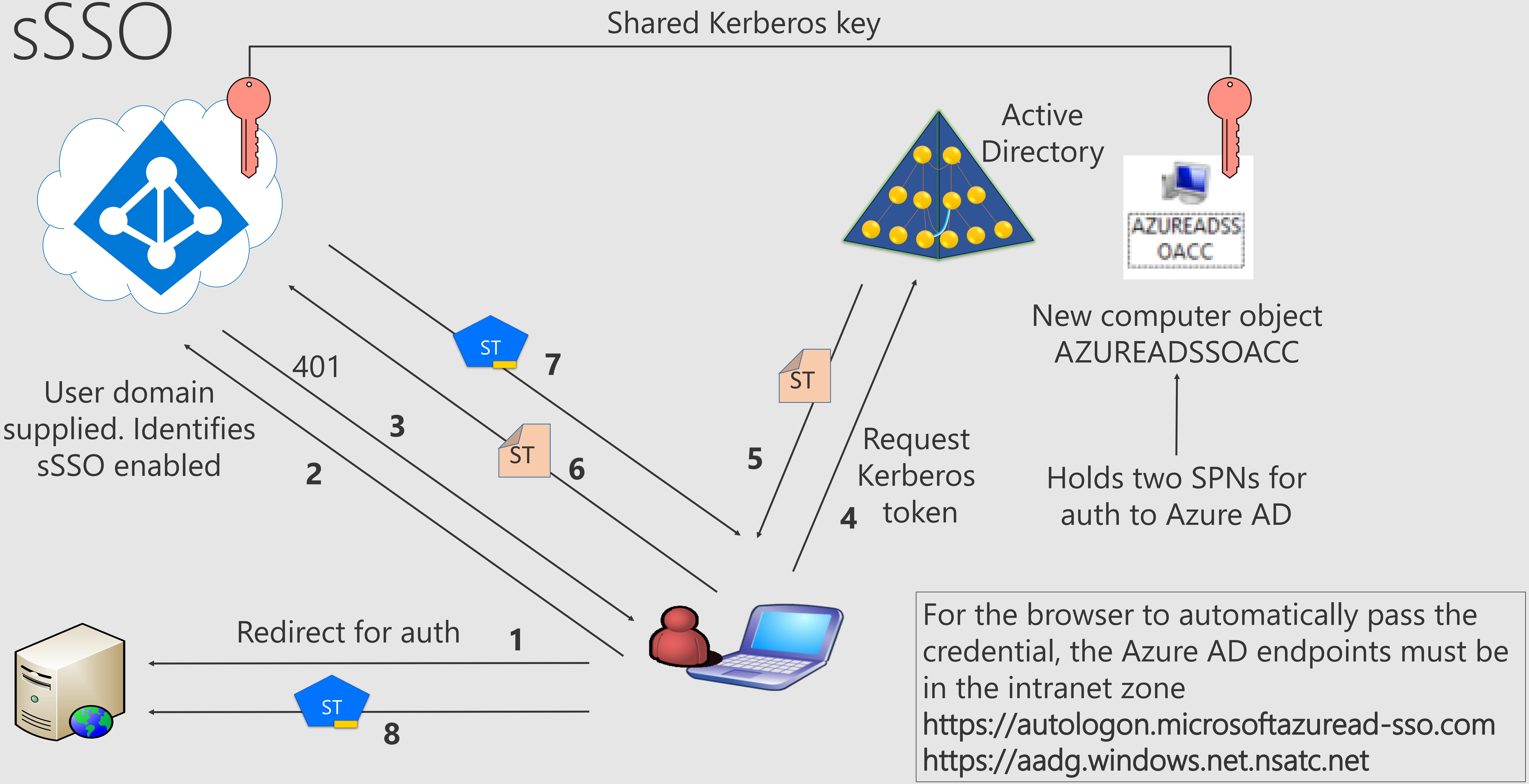
Enable password protection on Windows Server Active Directory: [✓ Yes] No

Mode: [✓ Enforced] Audit

Seamless SSO, the facts…

- Works with pass-through authentication or password hash sync
- Users only need to type their username to authenticate to Azure AD
  - It is possible for applications to pass a domain_hint for seamless SSO
  - Supports Windows 7 and above
  - Machine must be domain joined or hybrid domain joined and have access to a DC
    - On corporate network or via remote access technology
  - Authenticates to Azure AD with a Kerberos token
  - Available with all versions of Azure AD
  - Supports Alternate ID
  - Support for multiple browsers and OSs
    - Including Safari and Mac

sSSO


Shared Kerberos key
Active Directory
AZUREADSS OACC
New computer object AZUREADSSOACC
Holds two SPNs for auth to Azure AD
User domain supplied. Identifies sSSO enabled
401
Redirect for auth
1
2
3
4
Request Kerberos token
5
ST
6
ST
7
ST
8
ST

For the browser to automatically pass the credential, the Azure AD endpoints must be in the intranet zone
https://autologon.microsoftazuread-sso.com
https://aadg.windows.net.nsatc.net

Demo

- PTA with Seamless SSO

Kerberos authentication

- Seamless SSO can be configured with PTA or PHS
- If the user is connected to the corporate AD domain and sSSO succeeds, the authentication to Azure AD is Kerberos
- If the user is not connected to the corporate AD domain, authentication will fall-back to select authentication method (PTA or PHS)
- If an incompatible or mis-configured browser is detected, authentication will fall-back to select authentication method (PTA or PHS)

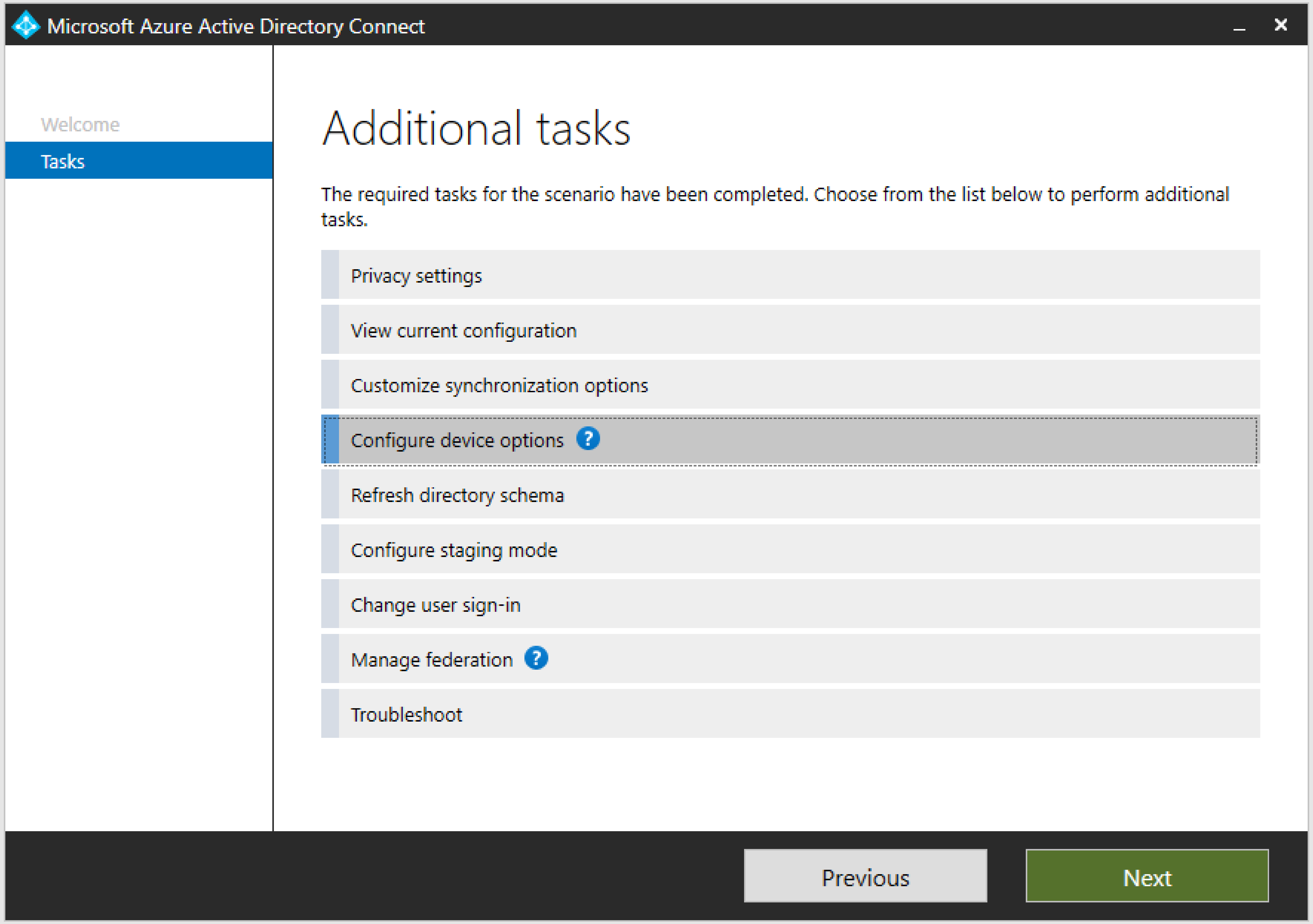
Kerberos Key

- The security of your on-premises authentication relies on the integrity of the Kerberos key
  - Recommended to roll the key every 30 days
- For details of managing key rolling see:
  - https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-sso-faq
- Automatic key rollover is on the roadmap!

Windows 10 and AD users

- Hybrid Azure AD Join
  - AD Domain Join with automatic Azure AD registration
  - All the benefits of Group Policy / SCCM / Intune
- When users sign-in to their device they get a Kerberos token for on-premises AD and Primary Refresh Token (PRT) for Azure AD access
- Single sign on to all Azure AD authenticated resources
  - No requirement to have access to a DC
- Conditional access policies can be based on the users device
- Windows Hello for Business can be used for authentication

Hybrid Azure AD Join configuration



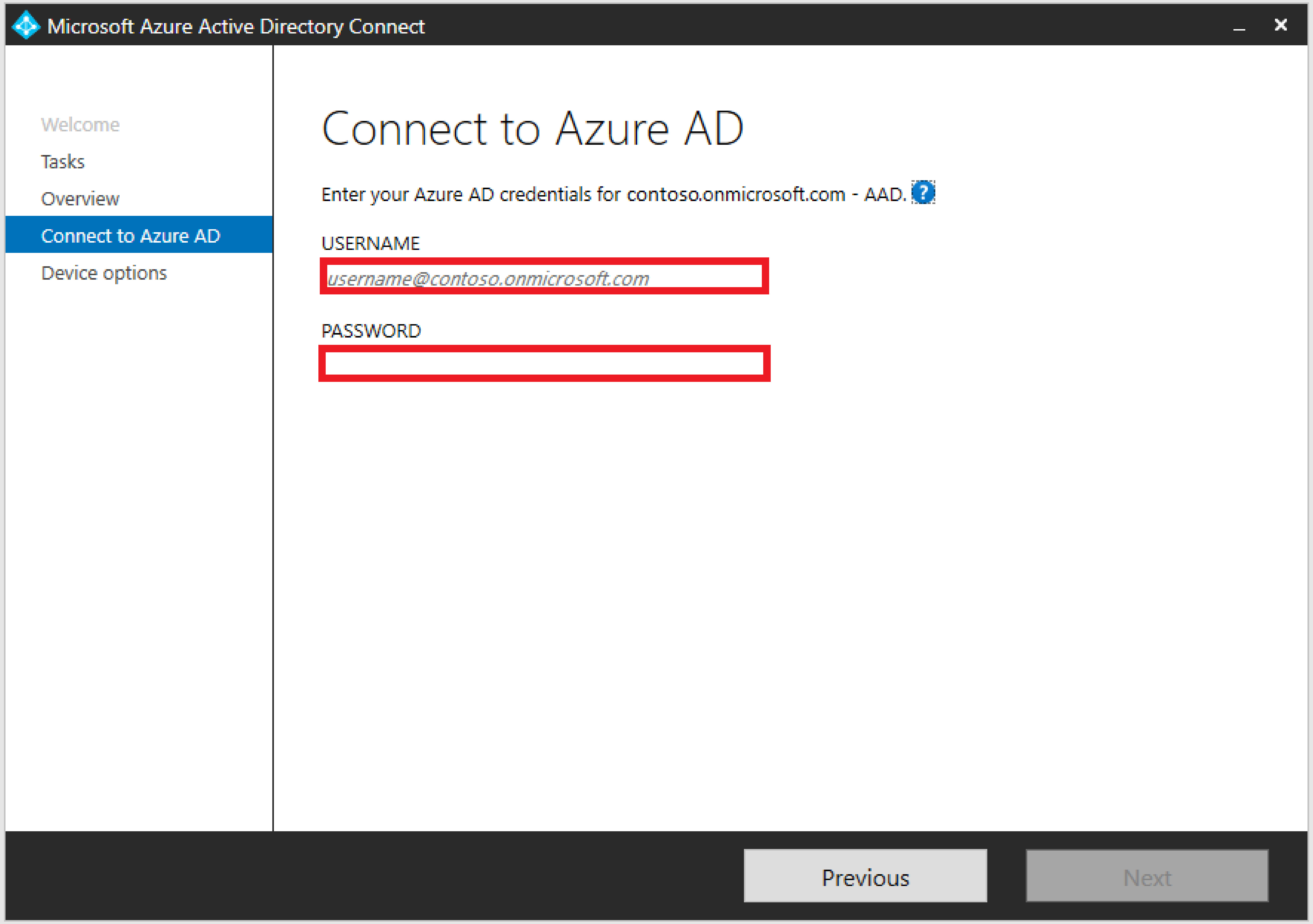
Microsoft Azure Active Directory Connect

Additional tasks

The required tasks for the scenario have been completed. Choose from the list below to perform additional tasks.

- Privacy settings
- View current configuration
- Customize synchronization options
- Configure device options ?
- Refresh directory schema
- Configure staging mode
- Change user sign-in
- Manage federation ?
- Troubleshoot

Hybrid Azure AD Join configuration



Connect to Azure AD

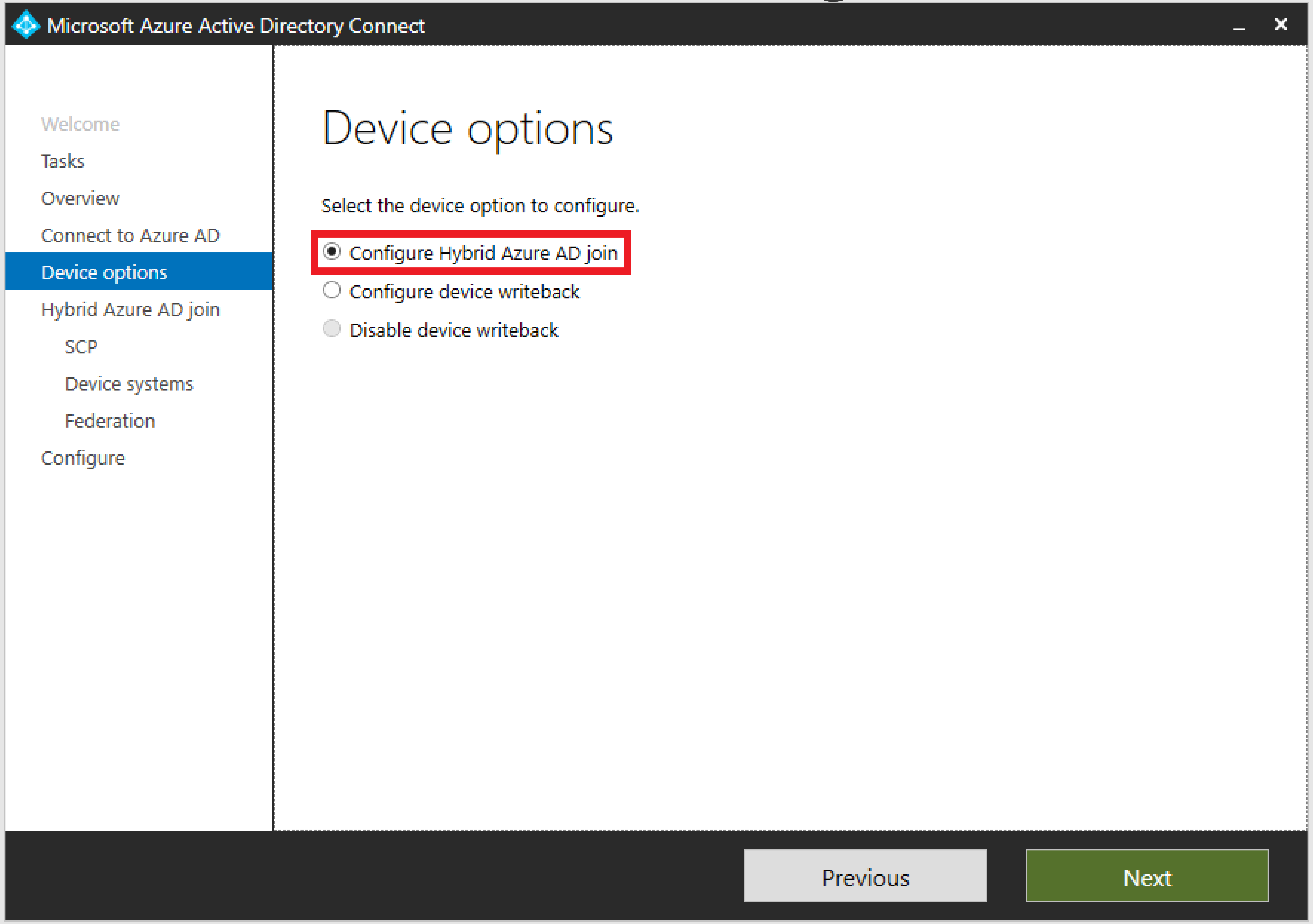
Enter your Azure AD credentials for contoso.onmicrosoft.com - AAD.

USERNAME

username@contoso.onmicrosoft.com

PASSWORD

Hybrid Azure AD Join configuration



Device options

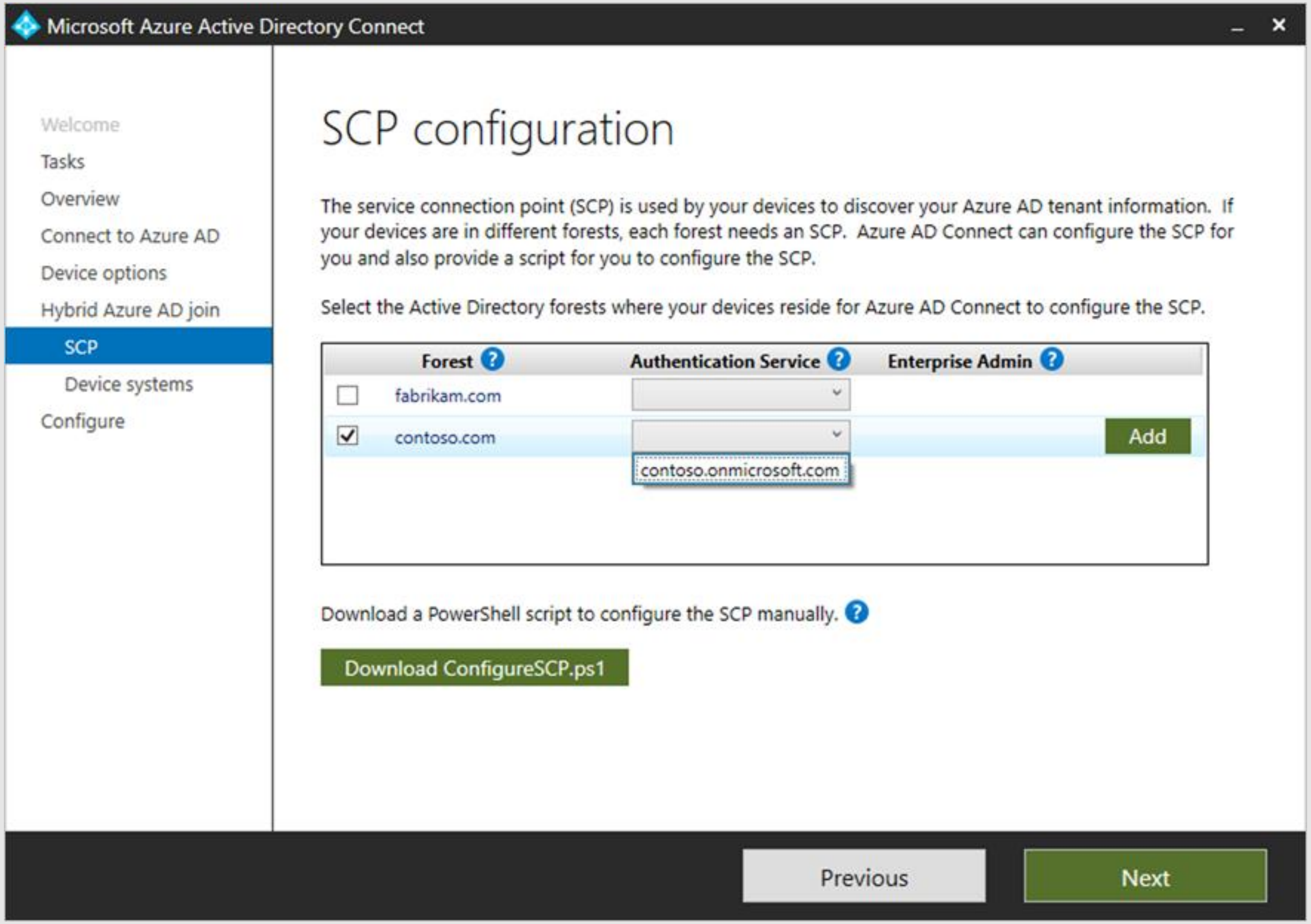
Select the device option to configure.

● Configure Hybrid Azure AD join

○ Configure device writeback

○ Disable device writeback

Hybrid Azure AD Join configuration



SCP configuration

The service connection point (SCP) is used by your devices to discover your Azure AD tenant information. If your devices are in different forests, each forest needs an SCP. Azure AD Connect can configure the SCP for you and also provide a script for you to configure the SCP.

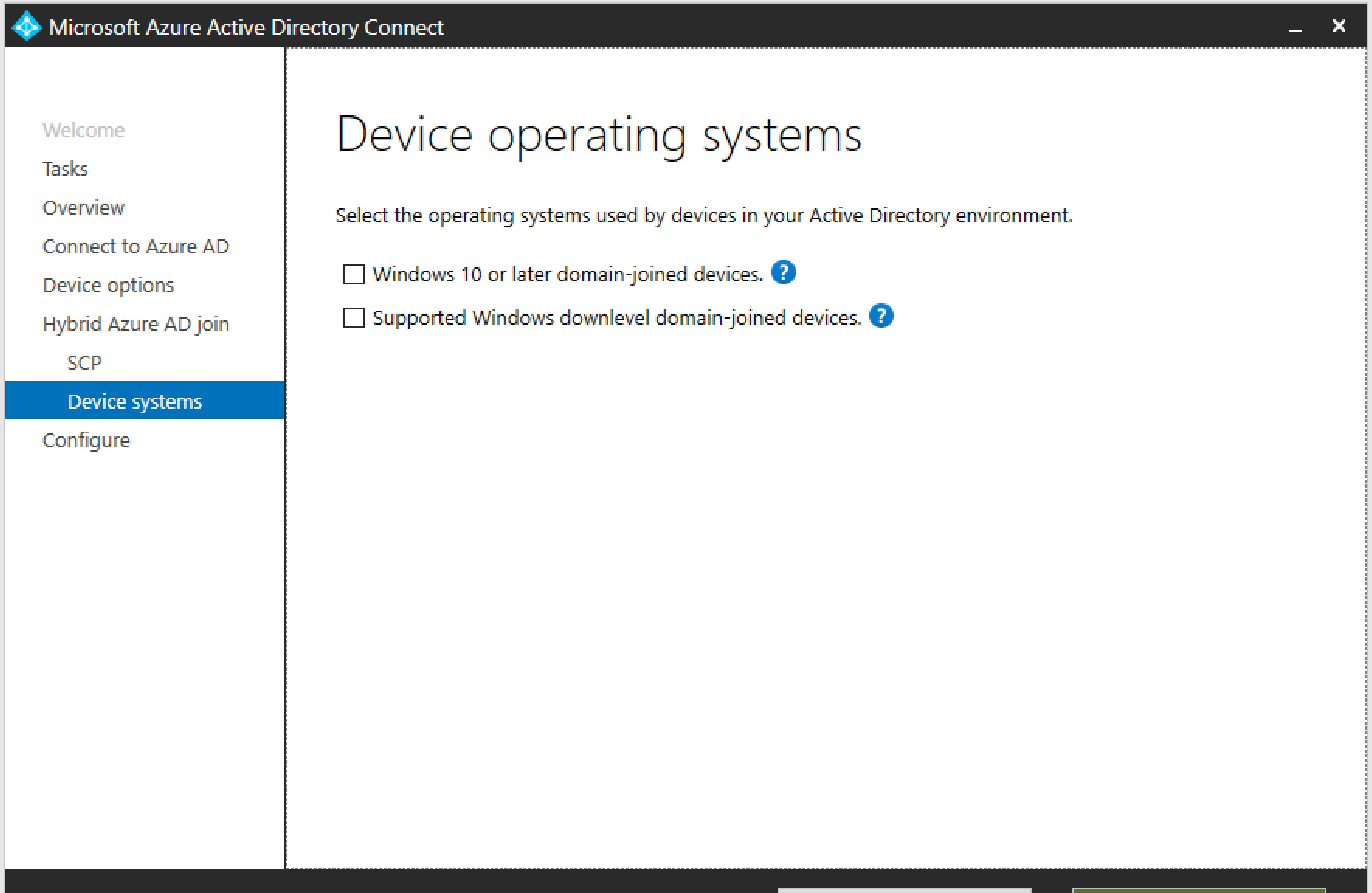
Select the Active Directory forests where your devices reside for Azure AD Connect to configure the SCP.

	Forest	Authentication Service	Enterprise Admin
☐	fabrikam.com		
☑	contoso.com	contoso.onmicrosoft.com	Add

Download a PowerShell script to configure the SCP manually.

Download ConfigureSCP.ps1

Hybrid Azure AD Join configuration



Microsoft Azure Active Directory Connect

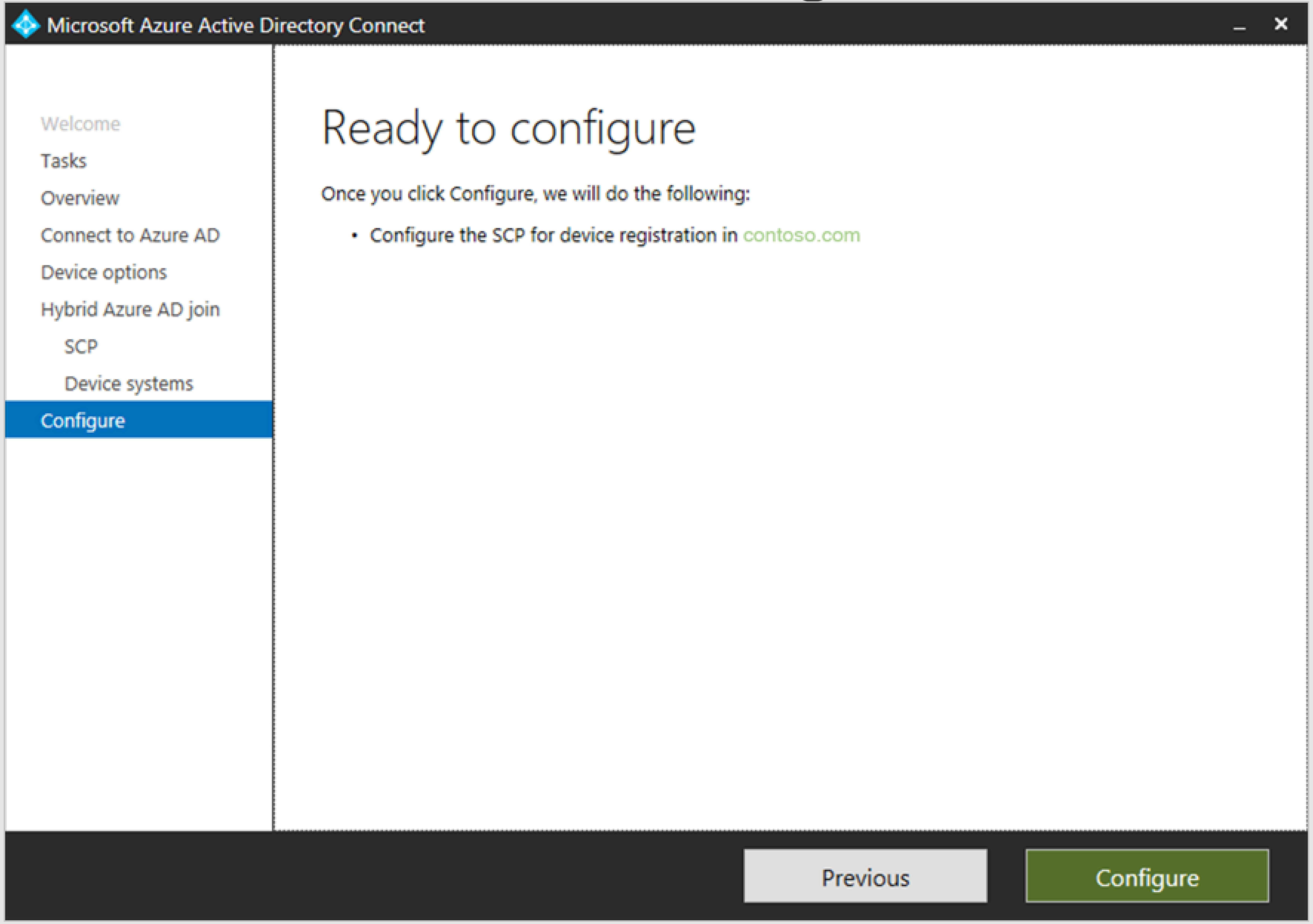
Device operating systems

Select the operating systems used by devices in your Active Directory environment.

□ Windows 10 or later domain-joined devices. ?

□ Supported Windows downlevel domain-joined devices. ?

Hybrid Azure AD Join configuration



Ready to configure

Once you click Configure, we will do the following:

- Configure the SCP for device registration in contoso.com

Hybrid Azure AD Join – downlevel devices

1. The following policy must be set to All: **Users may register their devices with Azure AD**
2. Add the following URLs to the Local Intranet zone in Internet Explorer:
    - https://device.login.microsoftonline.com
    - https://autologon.microsoftazuread-sso.com
3. Enable **Allow updates to status bar via script** in the user's local intranet zone
4. Configure Seamless SSO
5. Download and install **Microsoft Workplace Join for non-Windows 10 computers**

Recommendations

- New customers:
  - Use cloud authentication (PTA or PHS)
    - Leverage conditional access and Azure AD MFA
  - Existing customers with AD FS
    - Keep AD FS for authentication if it meets all your requirements
    - If using AD FS for authentication to apps, switch to Azure AD for authentication to apps
- Enable Seamless SSO if your using PTA or PHS
  - Simple to deploy
  - Immediately enhances the sign-in experience for your users
- Also consider passwordless authentication (yet to come)

Feature summary	PTA + sSSO	PHS + sSSO	ADFS
Authentication against credentials held on-premises	Yes	No	Yes
Single-Sign-On	Yes	Yes	Yes
Passwords remain on premises	Yes	Salted hash synced	Yes
On-premises MFA solution	No	No	Yes
Azure AD MFA	Yes	Yes	Yes
On-premises password policies	Yes	Partial	Yes
On-premises account enable/disable	Yes	Delayed (30 mins)	Yes
On-premises password lockout	Yes	No	Yes
Conditional access	Yes++	Yes++	Yes
Credentials captured from user via Azure AD UI	Yes	Yes	No
Protection against on-premise account lockout	Smart Lockout	N/A	Extranet Lockout
Cost of implementation	Medium	Low	High
Scalability/fault tolerance	Cloud scalability	Cloud scalability	Complex
AuthN **fails** for remote workers if the on-premises Internet connection is down. Requires HA solution.	Yes	No	Yes
On-going maintenance for authentication	Automated	None	SSL certificate management
Azure AD Connect Health monitoring	Not integrated	Limited	Yes
Azure AD Identity Protection (requires P2 license)	Yes	Yes	No

Q&A