



Scopri il gusto delle stelle

Michele Sensalari
MCT, MCSE, MCSA, MCITP
michele@sensalari.com
michele.sensalari@overneteducation.it
[@ilsensa7](#)



Menù



INTRO M365
BUSINESS



MANGE IDENTITY



ROLE BASED ACCESS
CONTROL



AZURE AD FEATURE
IN M365B



WINDOWS 10 HELLO
FOR BUSINESS



MODERN
AUTHENTICATION



AZURE AD P1

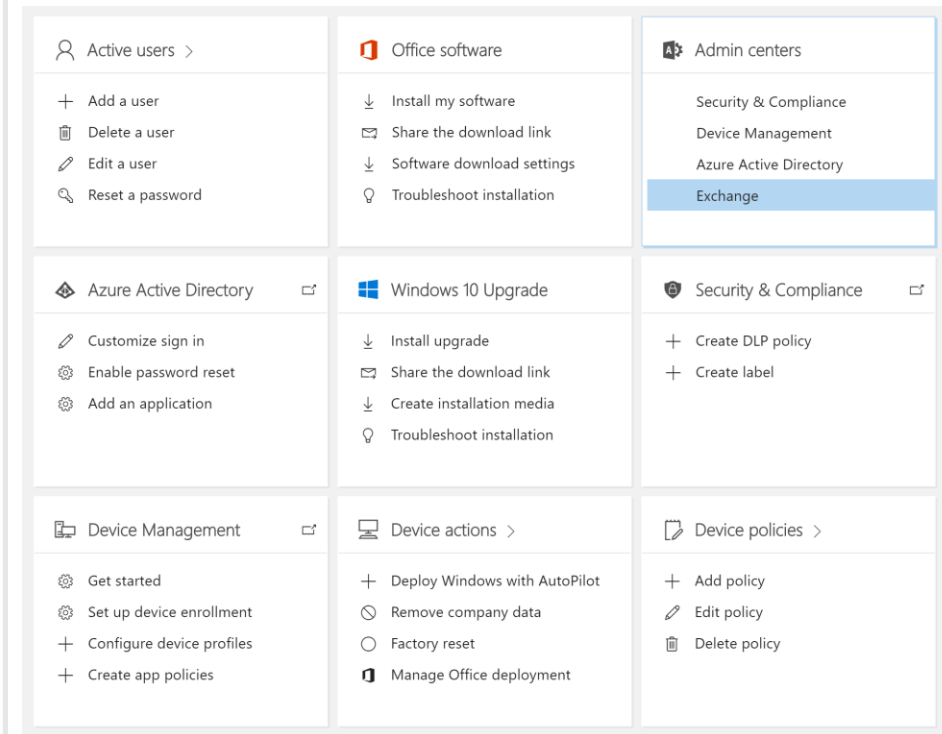


AZURE AD P2

Microsoft 365 Business

Microsoft 365 Business

- M365 Business is an integrated solution bringing together the best-in-class productivity of Office 365 with advanced security and device management capabilities to help safeguard your business.
- You can protect your work files on all of your iOS, Android, and Windows 10 devices with enterprise-grade security that is simple to manage.
- M365 Business is meant for up to 300 licenses.
- Windows devices must be running Windows 7 Professional, Windows 8 Pro, or Windows 8.1 Pro.



M365 Business: functionality

Office 365 Business

Azure AD P1 (only some feature): MFA (Multi Factor Authentication, SSPR (Self Service Password Reset), SSO (Single Sign-on) Third Party Application

Windows 10 Professional (only upgrade from 7, 8.1 Professional)

Office 365 ATP

Data Loss Prevention

Exchange Online Archiving (eDiscovery, Litigation Hold, Retention Policy)

Azure Information Protection

Intune (Windows 10, iOS, Android)

M365 Deployment

Understanding Microsoft 365 Business deployment steps

- Configure users & security policies using Microsoft 365 Business simplified Setup wizard
- Deploy Office 365 Services
- Deploy Windows 10 devices to enable Microsoft 365 Business management and access on-prem resources

Microsoft 365 Business supports On-premises Active Directory

- You can deploy Microsoft 365 Business for customers with on premises Active Directory and local resources. For that, you can configure the Windows device in two ways:
 - **Option A:** Azure AD Joined Device
A configuration where the Windows 10 device is joined to Azure AD while Azure AD Connect is enabled
 - **Option B:** Hybrid Azure AD Joined Device
A configuration where the Windows 10 device is joined to both Azure AD and on-prem AD while Azure AD Connect is enabled

Manage Identity

Identity

- A digital identity is information on an entity used by computer systems to represent an external agent. That agent may be a person, organization, application, or device
- Identity is a "set of attributes related to an entity"
- The identity information makes each entity unique and different from each other
- Identity are usually stored in a repository (ie. a Directory)
- From a security point of view each identity information in the repository represents a Security Principal used to uniquely identify an entity (ie: User Account)

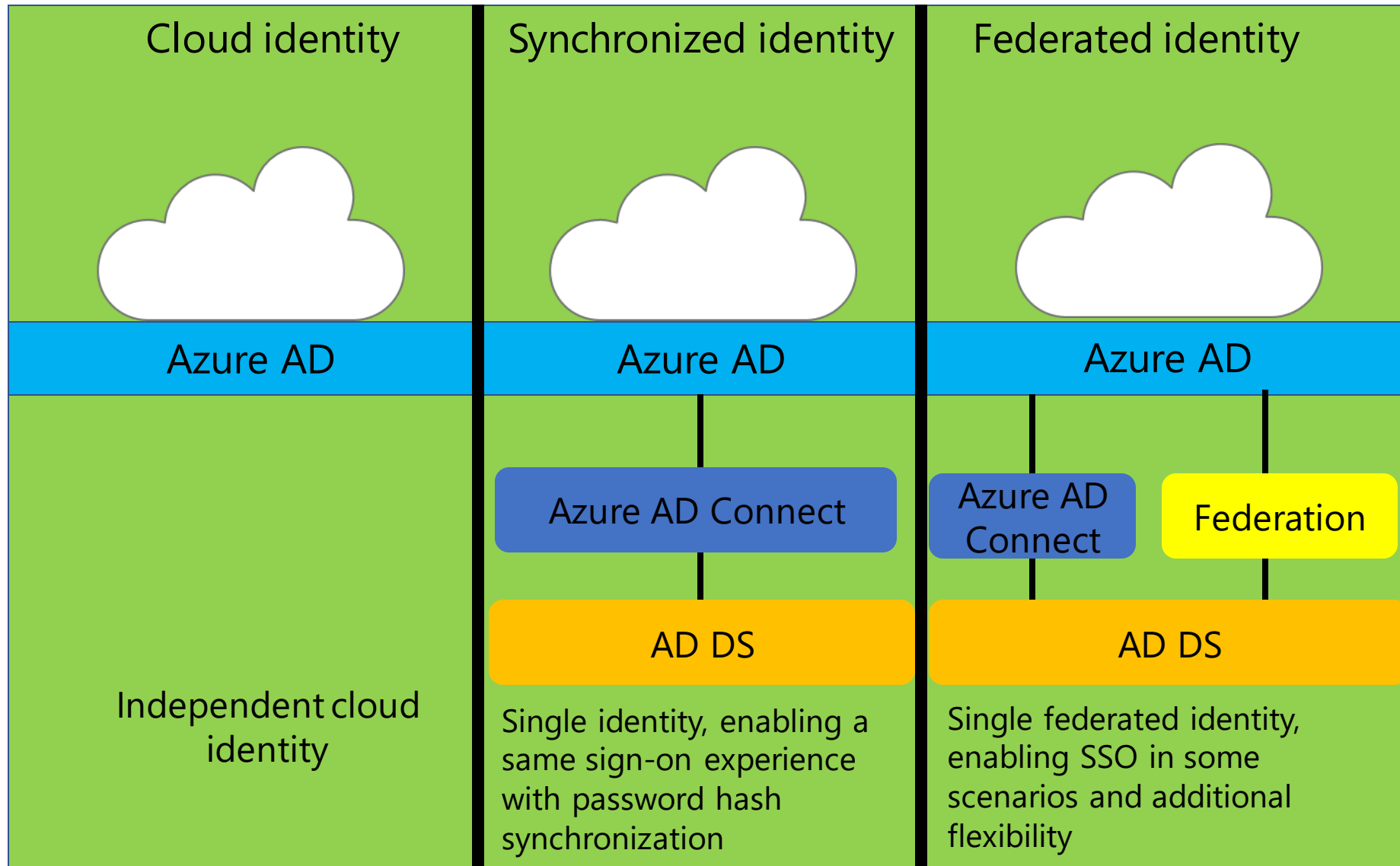
Authentication

- Authentication is a process for verifying the identity of something or someone
- Authentication relies on trust among process components
 - customs, passports, identity card, issuing organizations, people, ...
- And on validity and integrity of credentials

Authorization

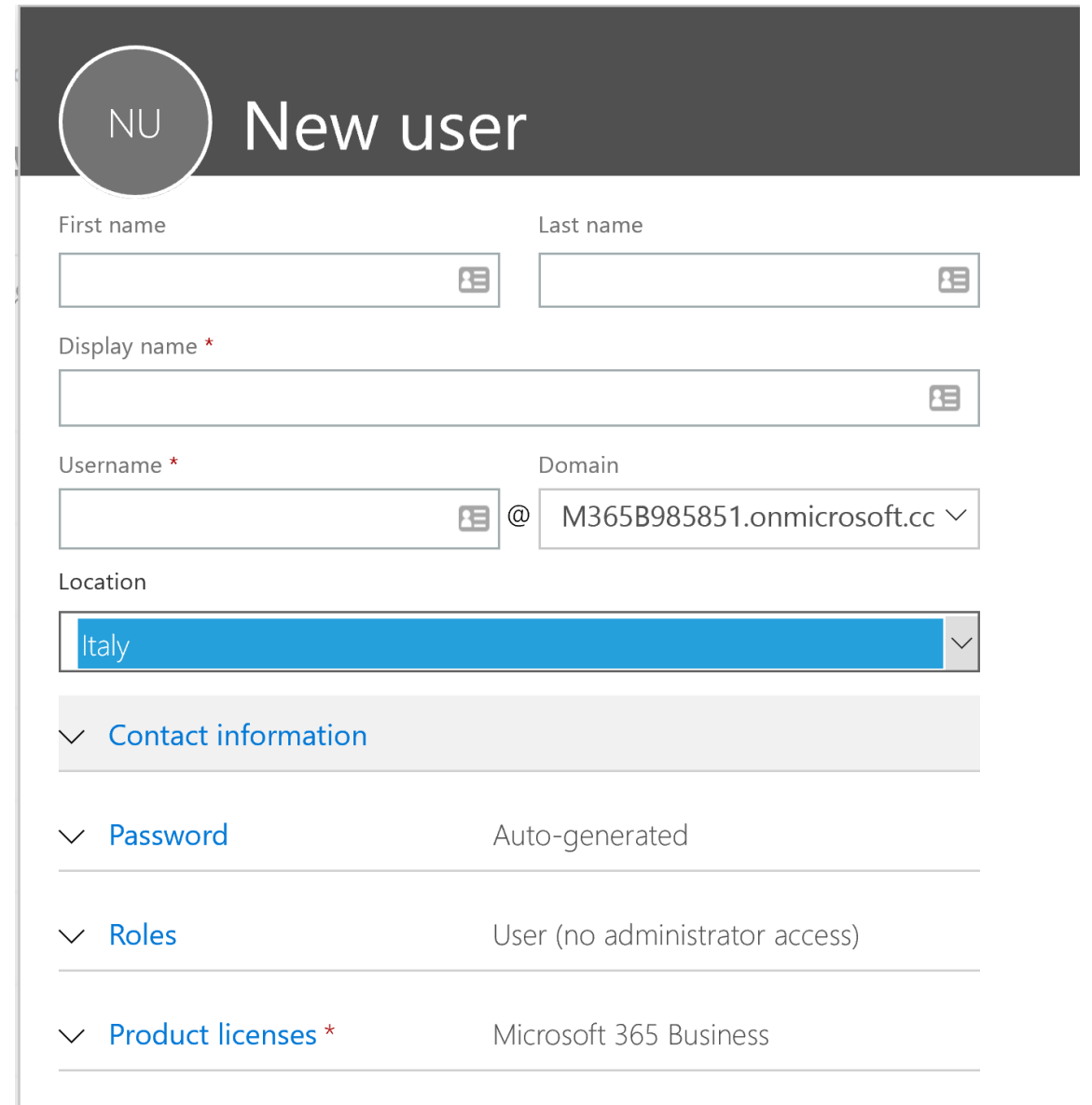
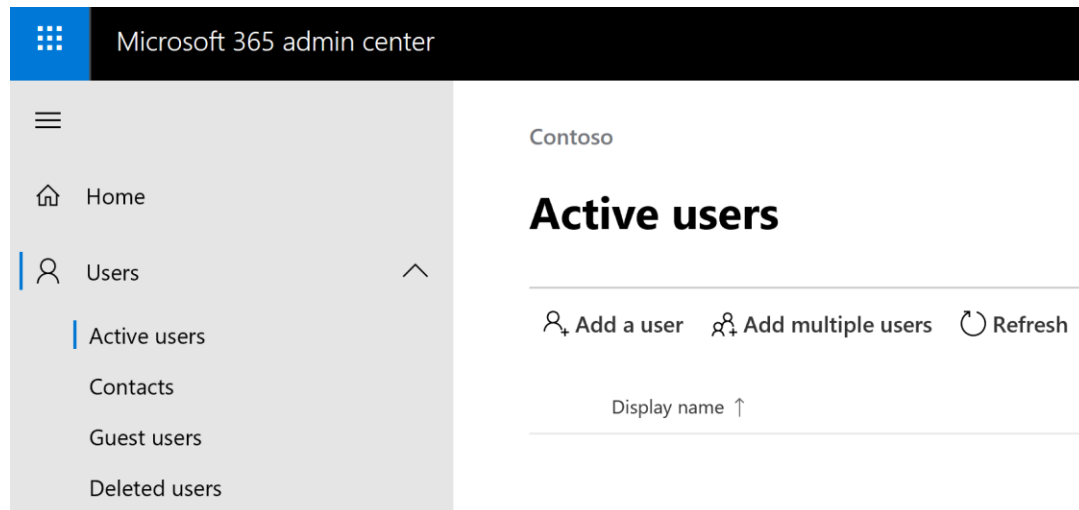
- Is the process to gain access to resources, usually with different rights for different identities
- Identity is verified thru authentication
- Security administrator of resource define what kind of rights a known entity has or what type of actions are permitted

Microsoft 365 authentication options

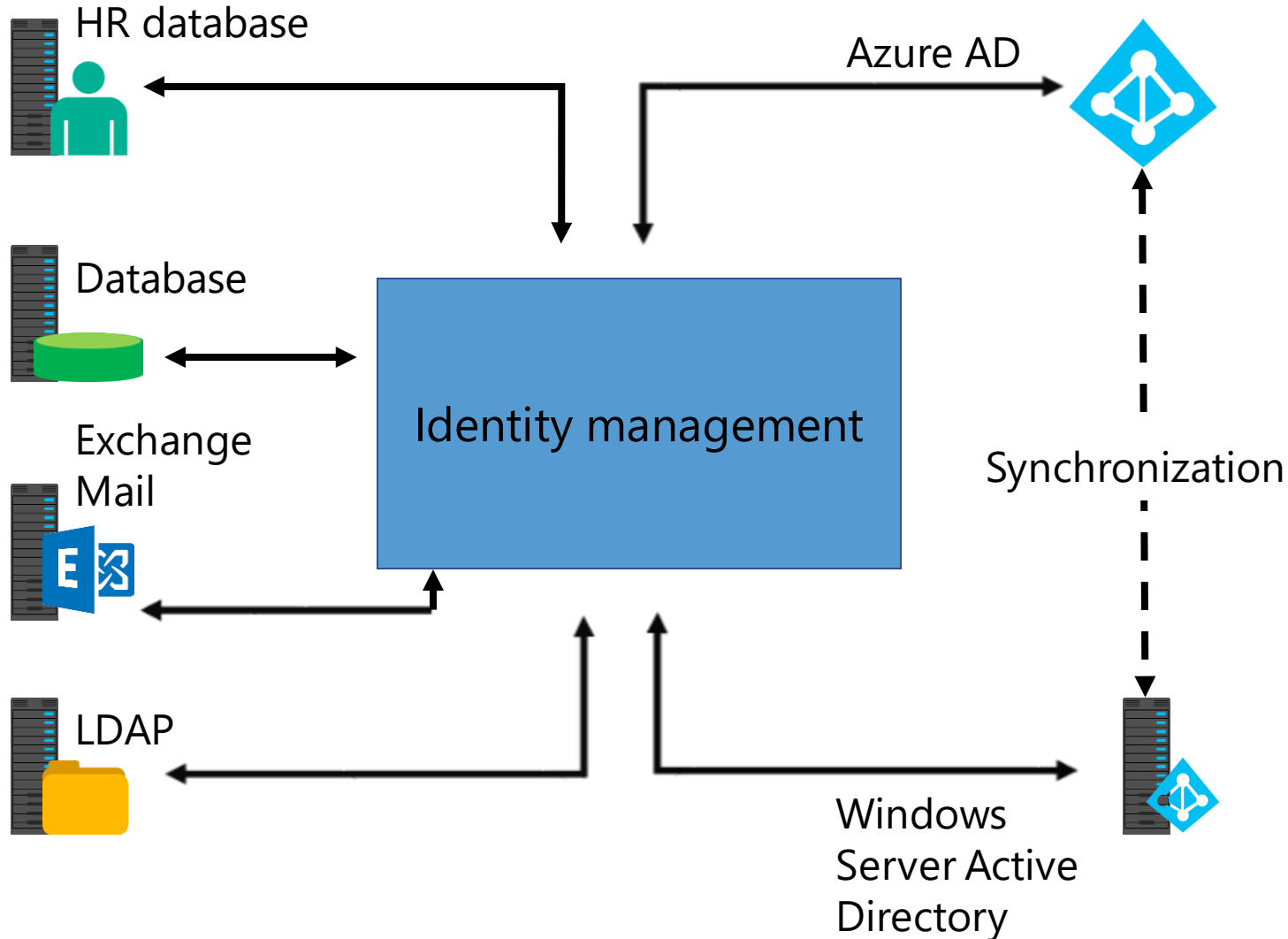


Cloud Identity

With the cloud-only model, you manage your user accounts in Microsoft 365 only. No on-premises servers are required; it's all handled in the cloud by Azure AD. You create and manage users in the Microsoft 365 admin center or by using Windows PowerShell

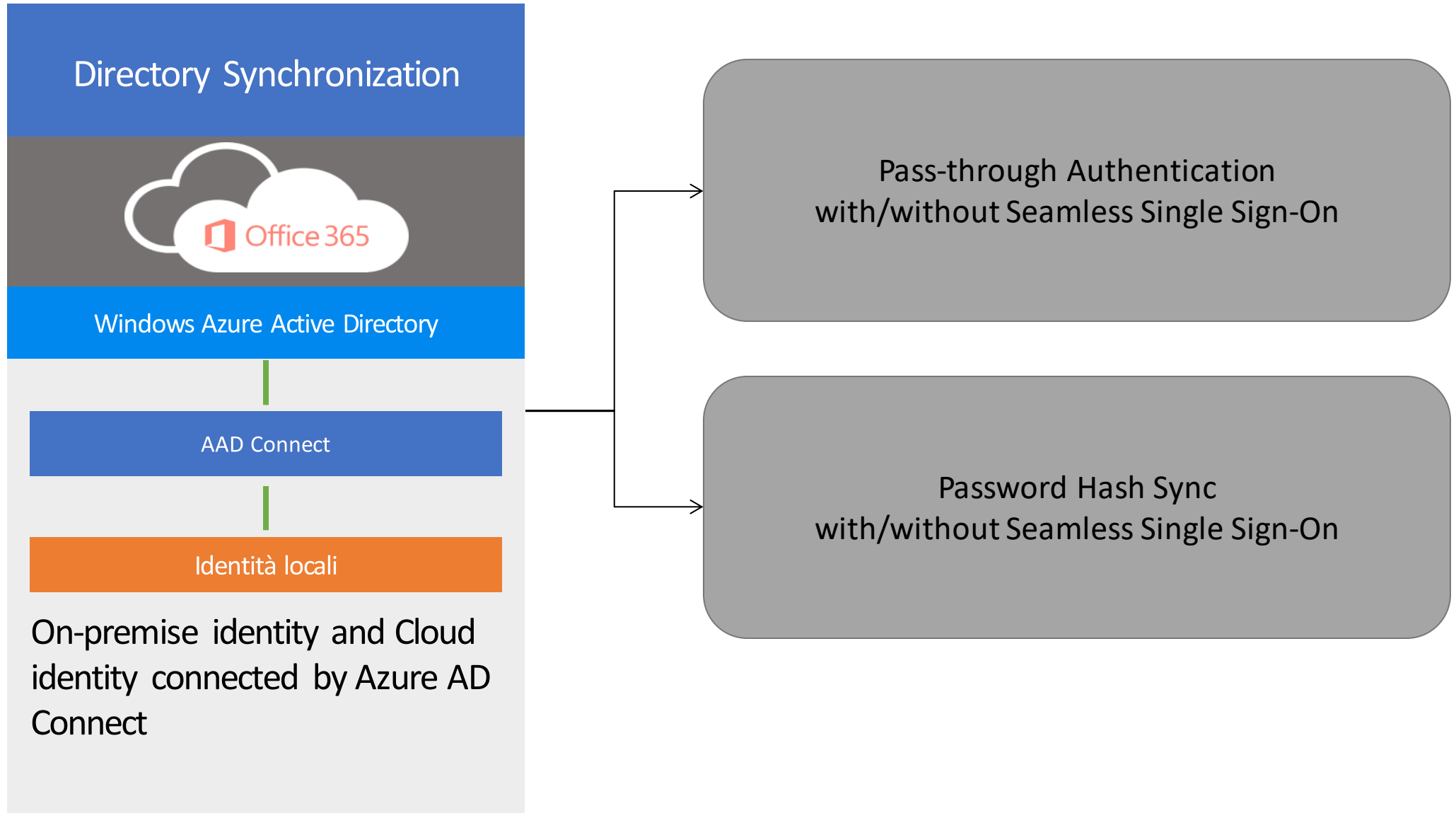
The screenshot shows the 'New user' form in the Microsoft 365 admin center. The form is set against a dark grey header with a circular profile picture placeholder containing the letters 'NU' and the text 'New user'. The form fields are as follows: 'First name' and 'Last name' are text input fields with user icons; 'Display name' is a text input field with a user icon and an asterisk; 'Username' is a text input field with a user icon and an asterisk; 'Domain' is a dropdown menu showing 'M365B985851.onmicrosoft.cc'; 'Location' is a dropdown menu showing 'Italy'; 'Contact information' is a section header with a downward arrow; 'Password' is a section header with a downward arrow, showing 'Auto-generated'; 'Roles' is a section header with a downward arrow, showing 'User (no administrator access)'; and 'Product licenses' is a section header with a downward arrow, showing 'Microsoft 365 Business'.

Directory synchronization and Hybrid Identity



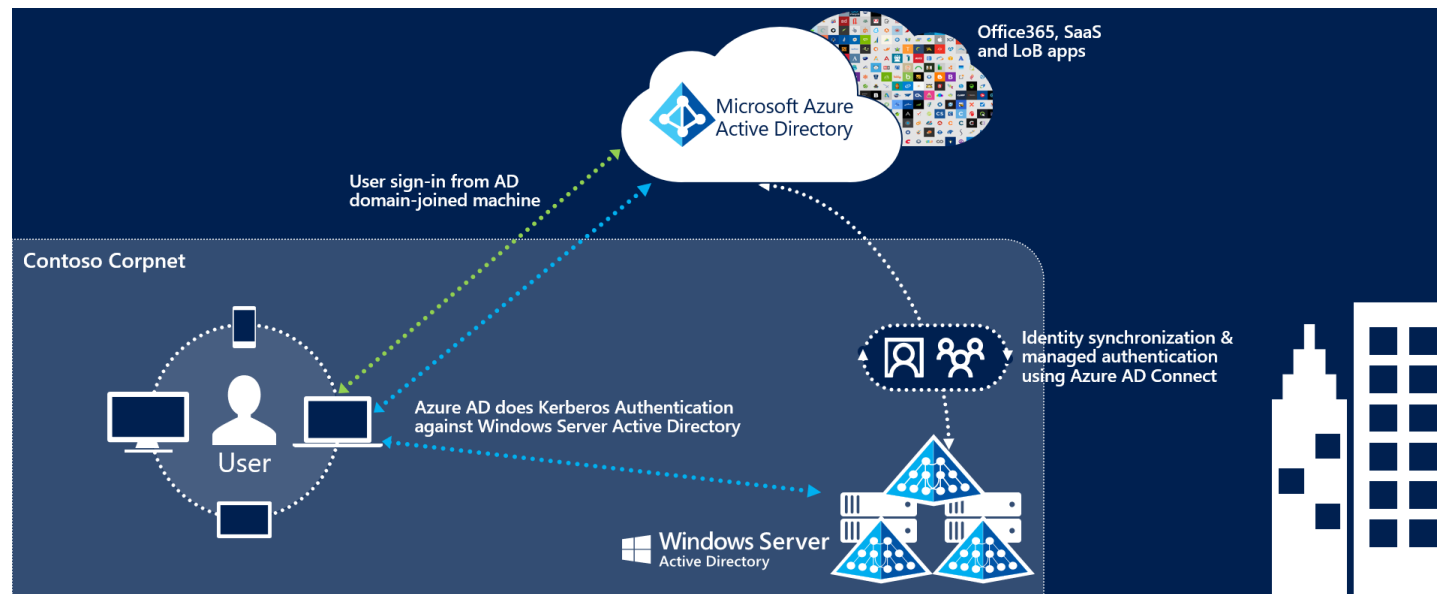
Microsoft's identity solutions span on-premises and cloud-based capabilities. These solutions create a common user identity for authentication and authorization to all resources, regardless of location. We call this **hybrid identity**.

Synchronized Identity



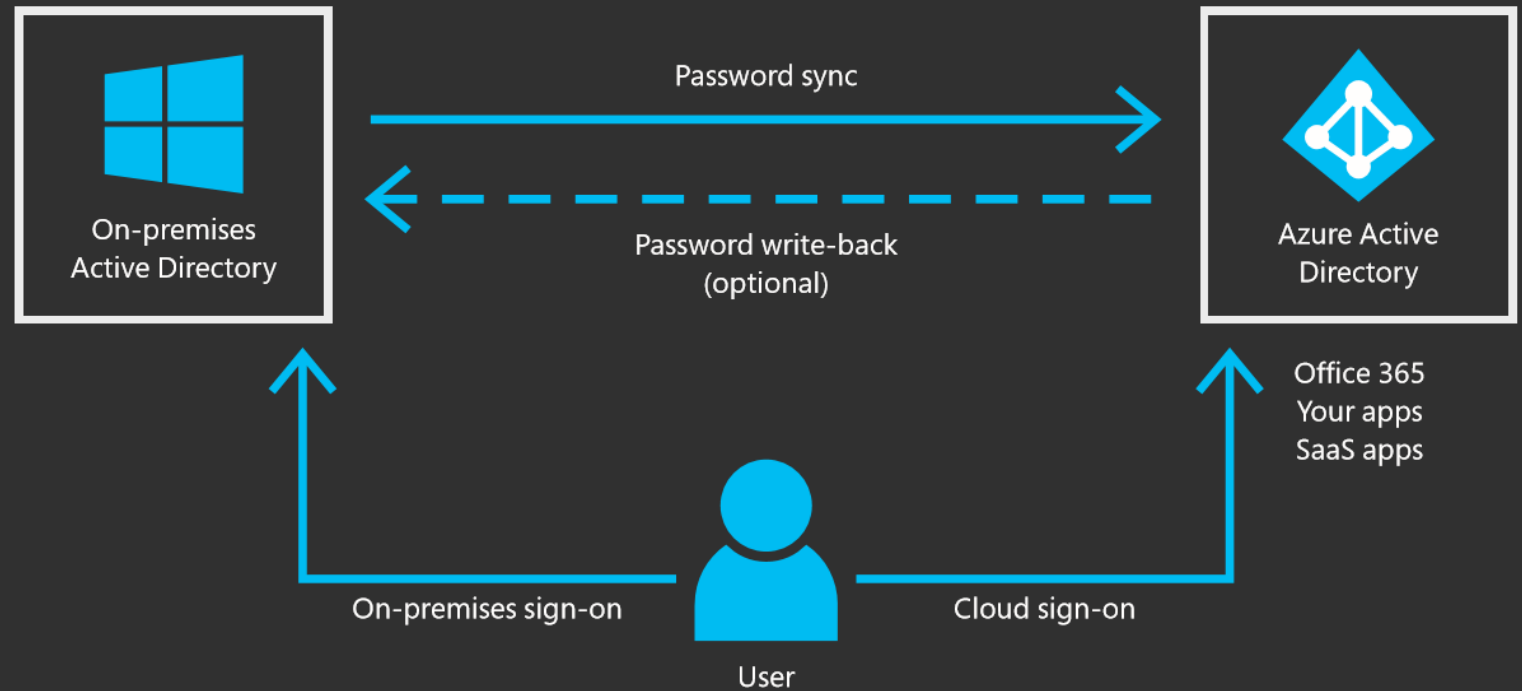
Seamless SSO

- Works in combination with **Password Hash Synchronization** or **Pass-through Authentication**.
- Users are automatically signed into both on-premise and cloud-based applications when on the corporate network.
- Users do not have to enter their passwords repeatedly.
- Users outside the corporate network can sign in using the normal username and password method required with Password Hash Synchronization.
- No additional components/servers are required. AD Connect Wizard with tick in a box (see below) and a GPO.

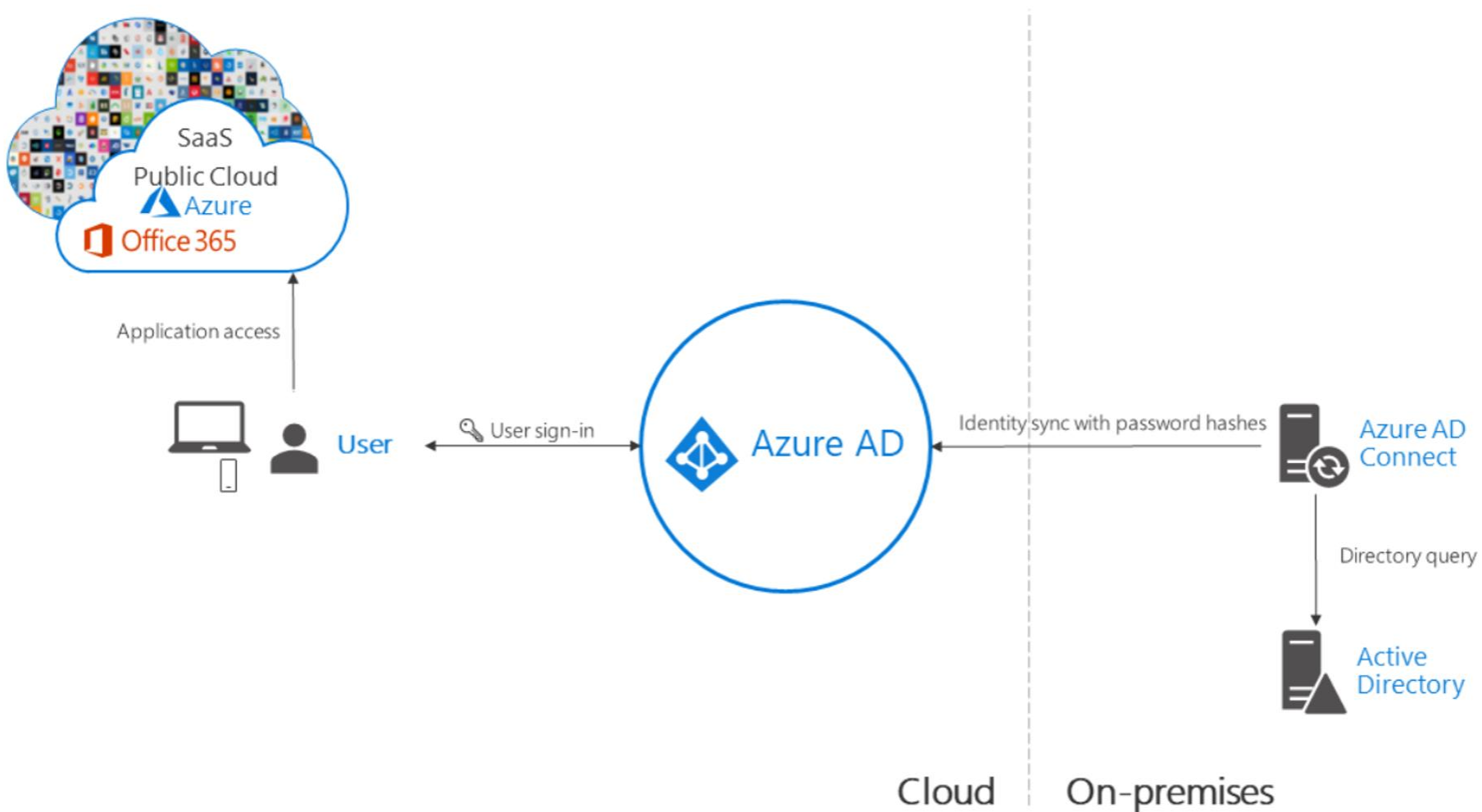


Password hash sync authentication

The simplest way to maintain a single authoritative identity database, Azure AD Connect can check for changes to the on-premises Active Directory and automatically update Azure AD. While users will still need to maintain separate passwords for cloud resources, this can be remedied by synchronizing password hashes as well.

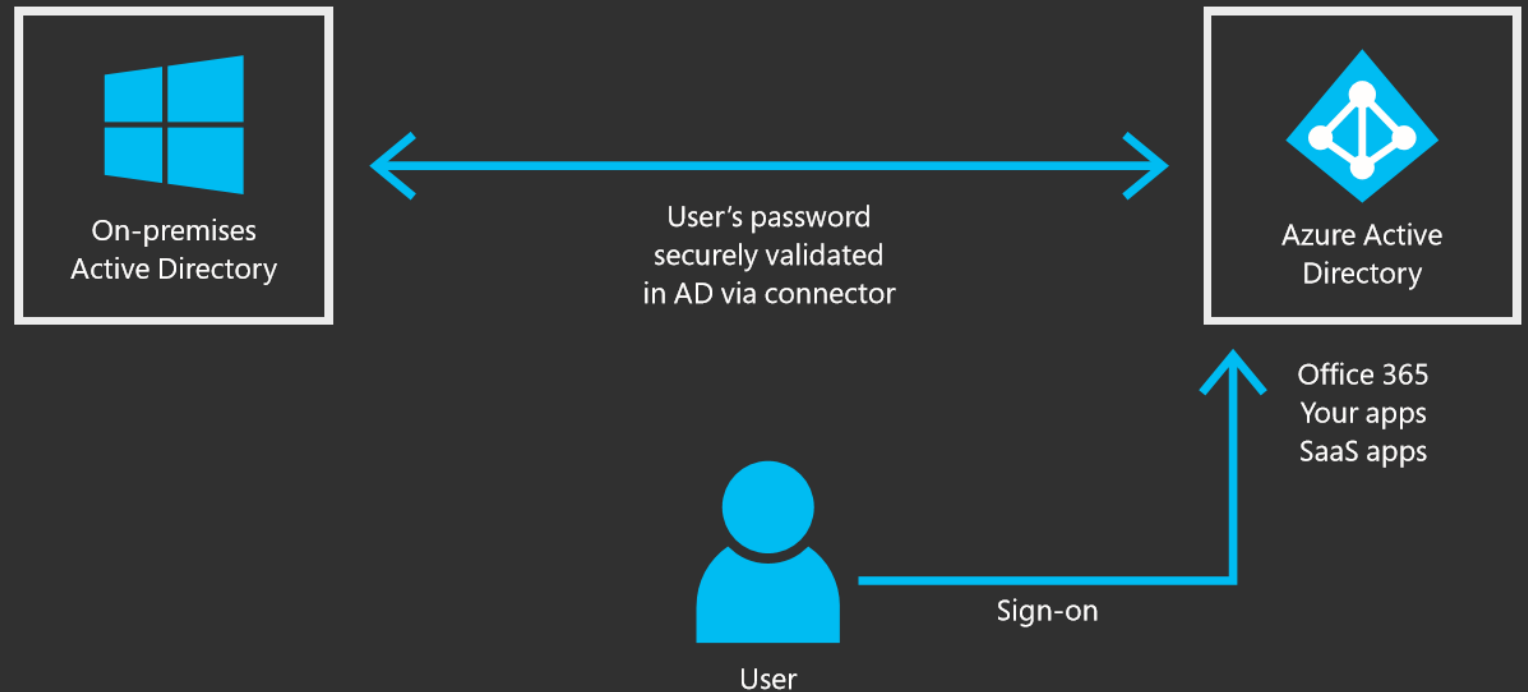


Azure AD Hybrid Identity with Password Hash Sync

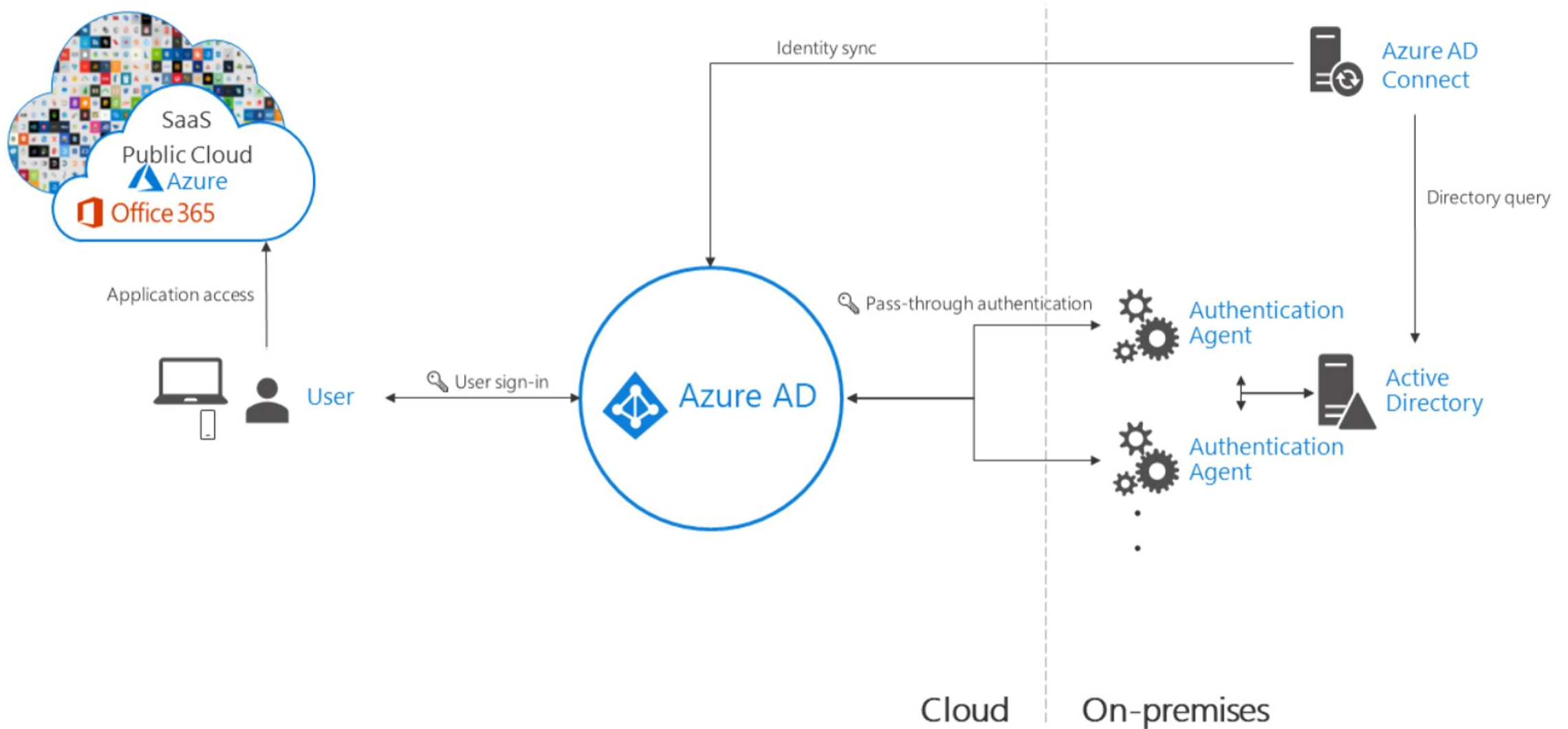


Pass-through authentication

This password validation solution allows on-premises devices to connect to cloud resources using their corporate credentials, solving many of the compliance issues of identity synchronization. Azure AD passes credentials back to the on-premises Active Directory server to validate the user. Unlike federated authentication, the company does not have to maintain servers in a perimeter zone.

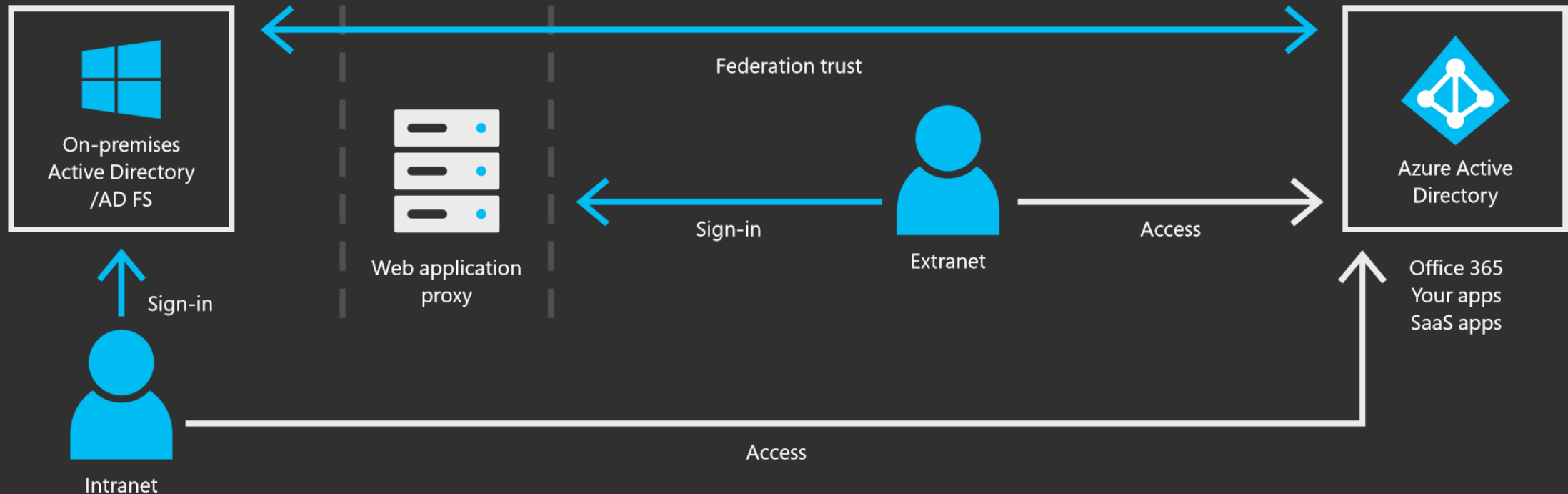


Azure AD Hybrid Identity with Pass-through authentication

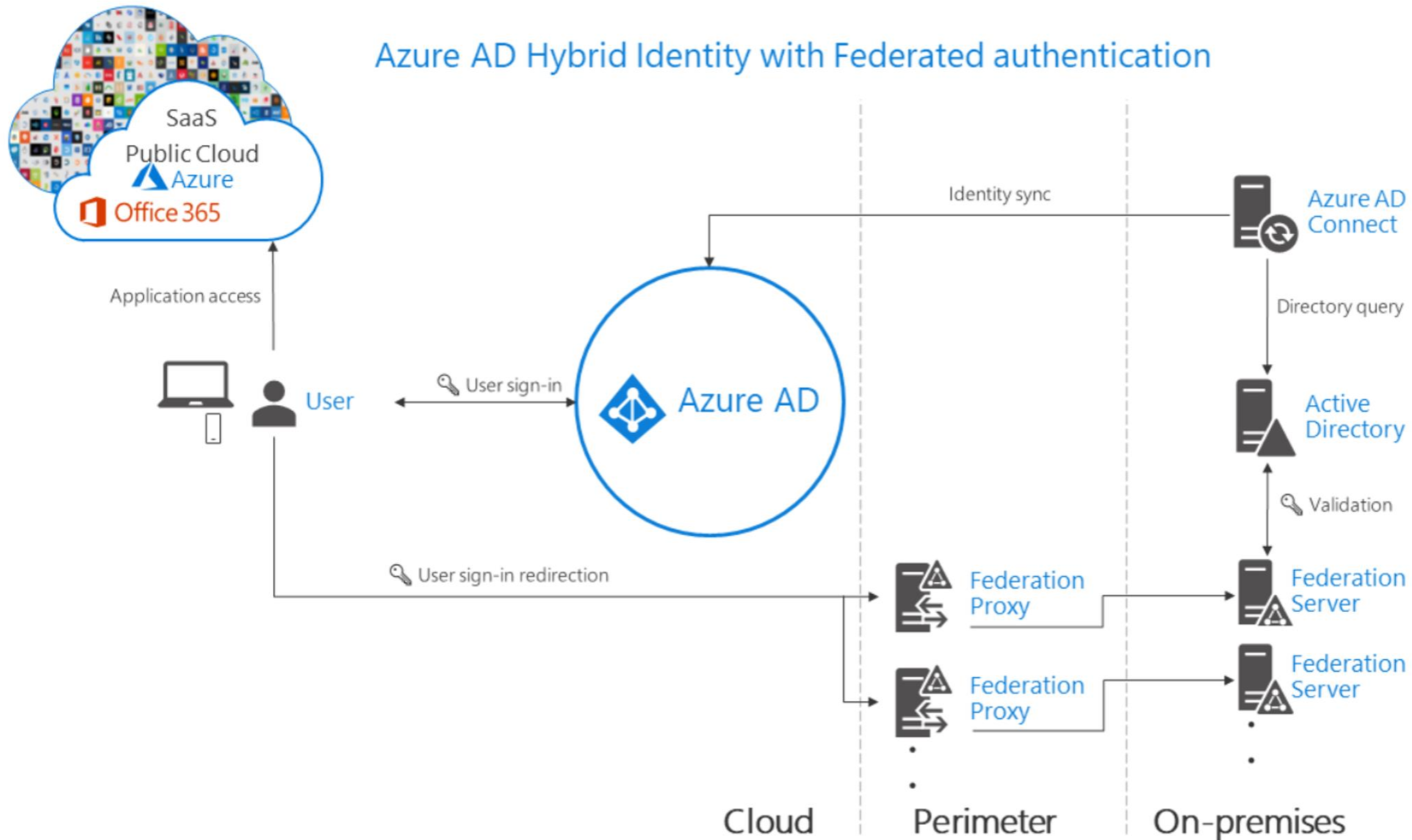


Federated authentication

With this method of authentication, the business commits to providing an identity service for employees. An on-premises identity service provides single sign-on capabilities through Active Directory Federation Services (AD FS). Federated authentication allows custom and more rigorous levels of access control. However, availability of the federated infrastructure becomes extremely important—if users cannot connect to the Internet, domain controller, or federated servers, then they cannot log into cloud services.



Azure AD Hybrid Identity with Federated authentication



RBAC

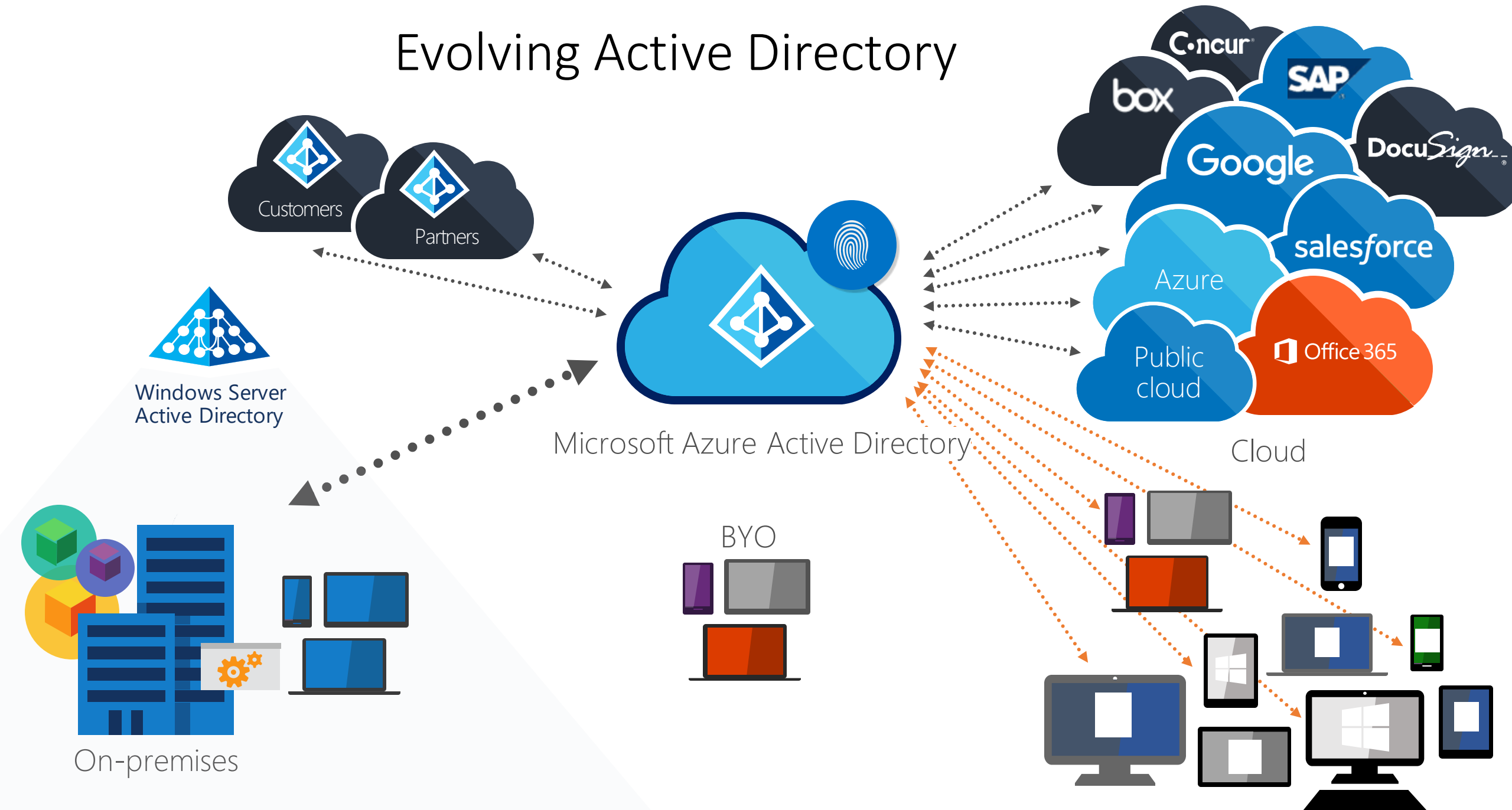
Using Admin Roles In Microsoft 365

- In Microsoft 365 you use administrator roles to assign specific administrative functions to users
- Each admin role maps to common business functions and gives permissions to do specific tasks in the Microsoft 365 admin center
- You can manage admin roles in Microsoft 365 using the Microsoft 365 admin center or Windows PowerShell. Roles include:
 - Global administrator
 - Billing administrator
 - Dynamics 365 service administrator
 - Exchange administrator
 - Password administrator
 - Skype for Business administrator
 - Power BI administrator
 - Service administrator
 - SharePoint administrator
 - User management administrator

- ☐ User (no administrator access)
This user won't have permissions to the Office 365 admin center or any admin tasks.
- ☐ Global administrator
This user will have access to all features in the admin center and can perform all tasks in the Office 365 admin center.
- ☒ Customized administrator
You can assign this user one or many roles so they can manage specific areas of Office 365.
 - ☐ Billing administrator
 - ☐ Dynamics 365 service administrator
 - ☐ Customer Lockbox access approver
 - ☐ Exchange administrator
 - ☐ Helpdesk (Password) administrator
 - ☐ License administrator
 - ☐ Skype for Business administrator
 - ☐ Message Center reader
 - ☐ Power BI service administrator
 - ☐ Reports reader
 - ☐ Service administrator
 - ☐ SharePoint administrator
 - ☐ Teams Communications Administrator
 - ☐ Teams Communications Support Engineer
 - ☐ Teams Communications Support Specialist
 - ☐ Teams Service Administrator
 - ☐ User management administrator

Azure Active Directory: Feature

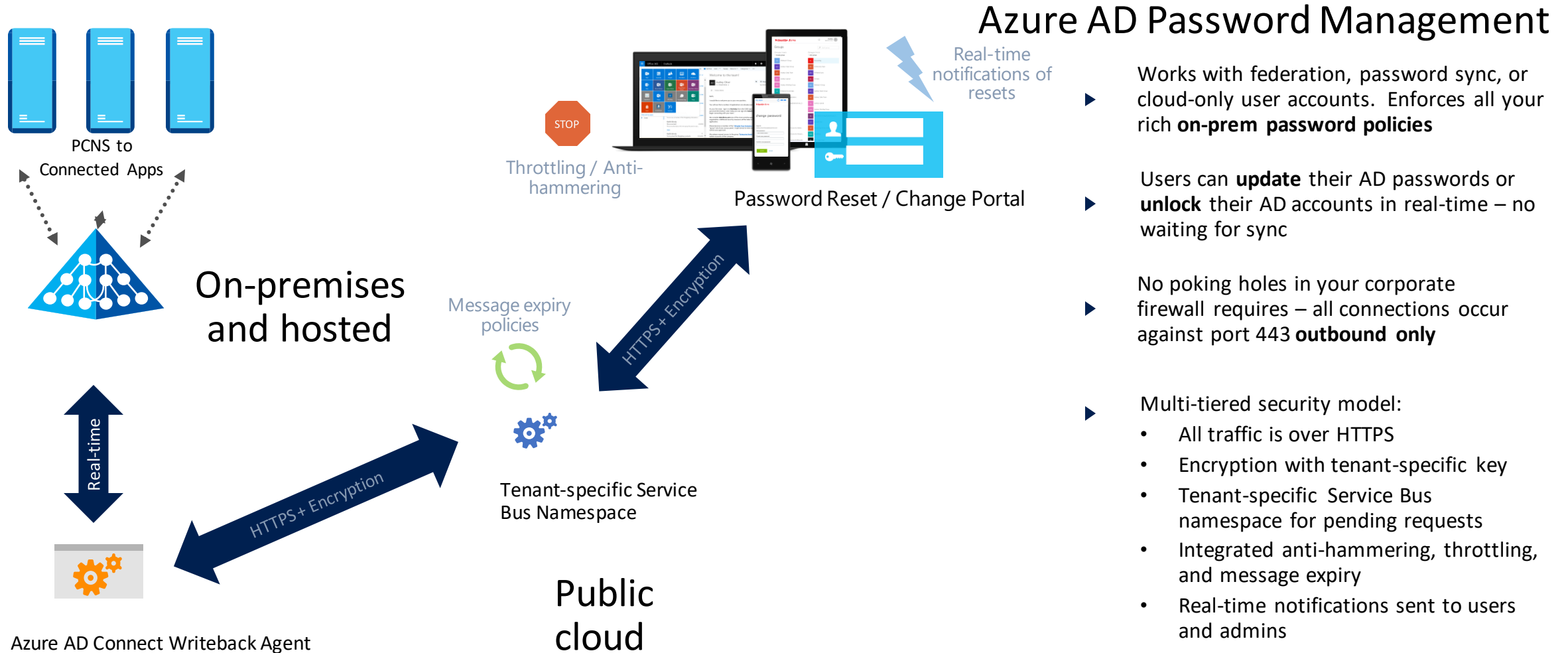
Evolving Active Directory



Plan and Implement Self-Service Password Management

- Self-service password reset (SSPR) allows users to reset their own password without requiring intervention by an administrator
- SSPR is not enabled by default
- To reset a password, users must authenticate their identity first
- If an administrator wants to use SSPR, they must use two verification methods, and they are not able to use security questions
- If you purchase Azure AD Premium, it includes the ability to write back passwords. This enables you to implement self-service password reset for synchronized identities and federated identities

Self-Service Password Management



Azure AD Password Management

- ▶ Works with federation, password sync, or cloud-only user accounts. Enforces all your rich **on-prem password policies**
- ▶ Users can **update** their AD passwords or **unlock** their AD accounts in real-time – no waiting for sync
- ▶ No poking holes in your corporate firewall requires – all connections occur against port 443 **outbound only**
- ▶ Multi-tiered security model:
 - All traffic is over HTTPS
 - Encryption with tenant-specific key
 - Tenant-specific Service Bus namespace for pending requests
 - Integrated anti-hammering, throttling, and message expiry
 - Real-time notifications sent to users and admins

Compromised Credential: BIG ISSUE

81% of hacking breach involve credential theft



Compromised Credentials: The Primary Point of Attack for Data Breaches

By [Torsten George](#) on January 24, 2018



Share



Tweet



Consiglia 12



Organizations Should Move to an Identity-centric Approach Based on a Zero Trust Model

Recent [headlines](#) of Russia-linked hackers harvesting access credentials to infiltrate the U.S. Senate and stage lateral attacks illustrate a common tactic used by cyber criminals and state-sponsored attackers. According to the Verizon 2017 Data Breach Investigation Report, [a whopping 81%](#) of hacking-related breaches leverage either stolen, default, or weak passwords. So why are so many organizations still focusing on securing the network perimeter, instead of rethinking their core defenses by maturing their identity and access management strategies to secure applications, devices, data, and infrastructure – both on-premises and in the cloud.

Forbes

[Billionaires](#) [Innovation](#) [Leadership](#) [Money](#) [Consumer](#) [Industry](#) [Lifestyle](#) [Features](#)

Forbes CommunityVoice Connecting expert communities to the Forbes audience. What is This?

469 views | Oct 12, 2018, 09:00am

The Growing Issue Of Compromised Credentials



Steve Tout CommunityVoice
Forbes Technology Council CommunityVoice ⓘ

POST WRITTEN BY

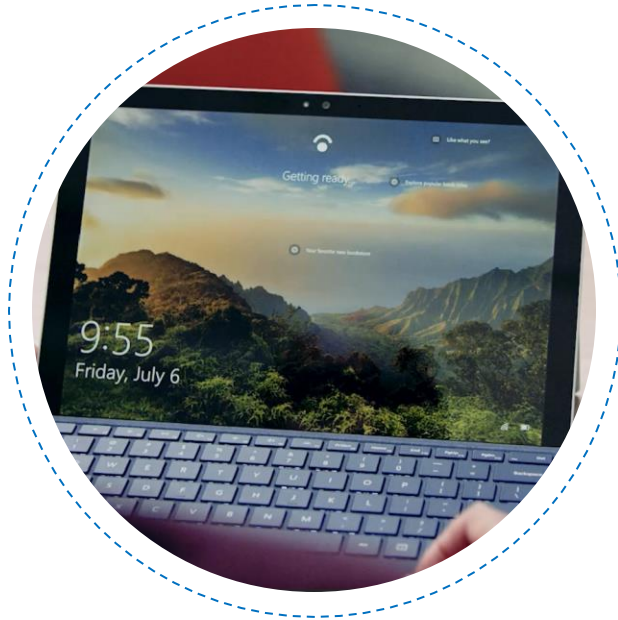
Steve Tout

CEO of [VeriClouds](#). I write about the identity and cloud security space as well as my interests in leadership, strategy and business.

73% of people re-use password across multiple account

Why Azure AD: **Strong authentication**

High security, convenient methods



Windows Hello




Microsoft Authenticator



OATH Security Tokens

Implementing Multi-Factor Authentication

- Multi-factor Authentication (MFA) in Microsoft 365 helps increase security by requesting users to provide a user name and a password while signing in and then use a second authentication method.
- The second authentication method might be acknowledging a phone call, text message, or an app notification on their smartphone
- You can also enable users who authenticate from a federated, on-premises directory for multi-factor authentication.
- The tenant administrator enables MFA in the Microsoft 365 admin center

 Microsoft

multi-factor authentication

users service settings

app passwords

☒ Allow users to create app passwords to sign in to non-browser apps

☐ Do not allow users to create app passwords to sign in to non-browser apps

verification options

Methods available to users:

☒ Call to phone

☒ Text message to phone

☒ Notification through mobile app

☒ Verification code from mobile app or hardware token

remember multi-factor authentication

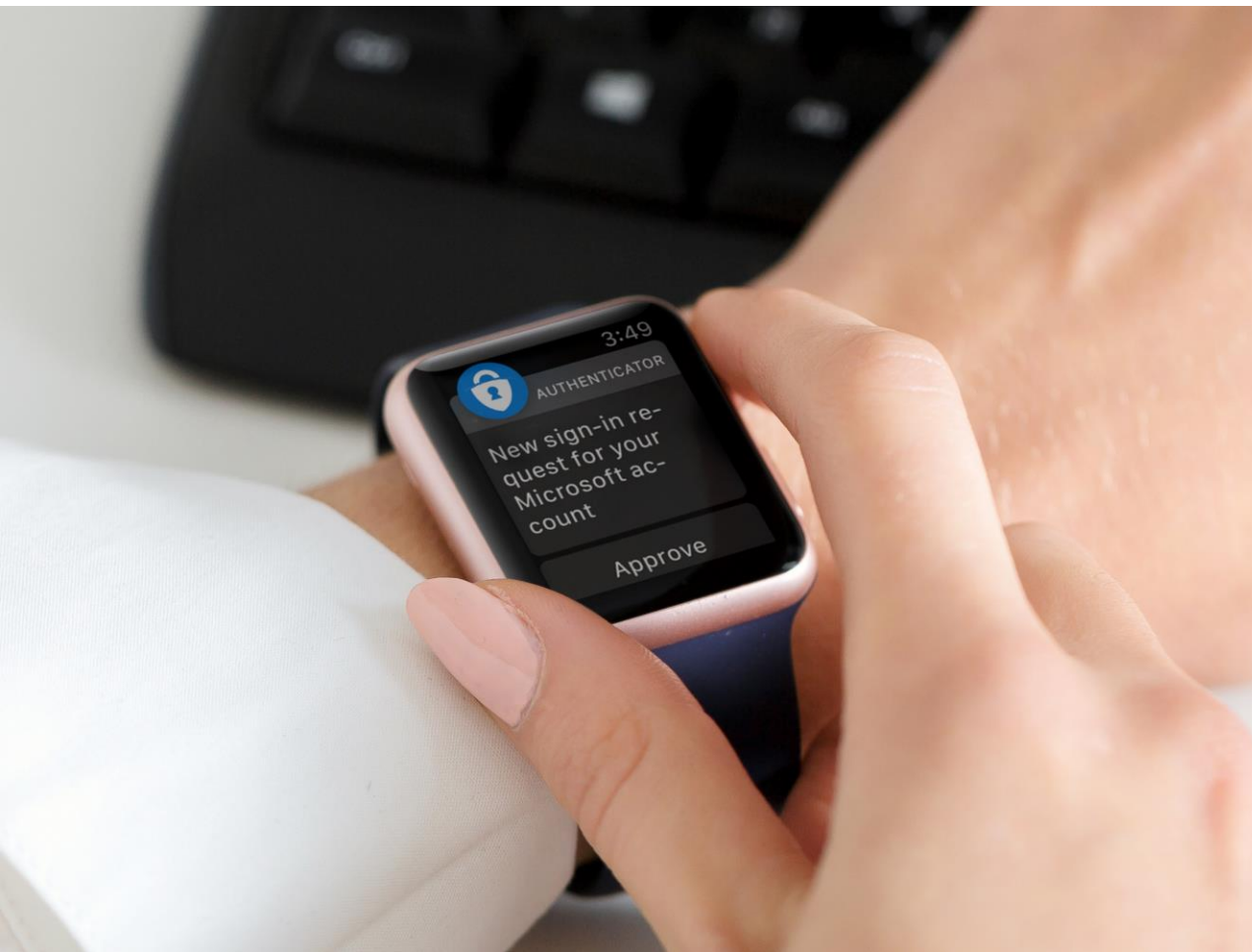
☐ Allow users to remember multi-factor authentication on devices they trust

Days before a device must re-authenticate (1-60):

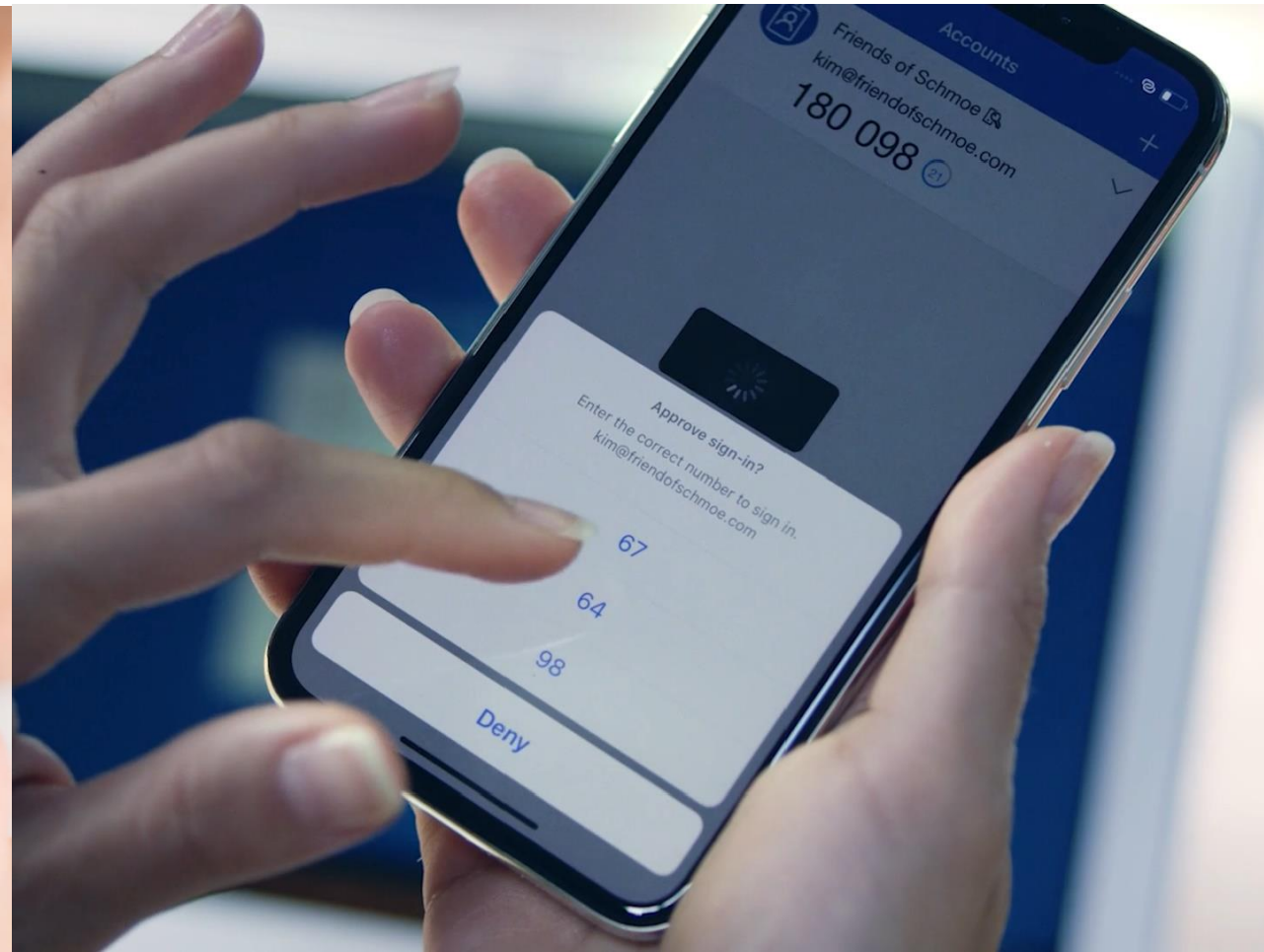
save

Microsoft Authenticator for Azure AD

User-friendly experience



Password-less authentication

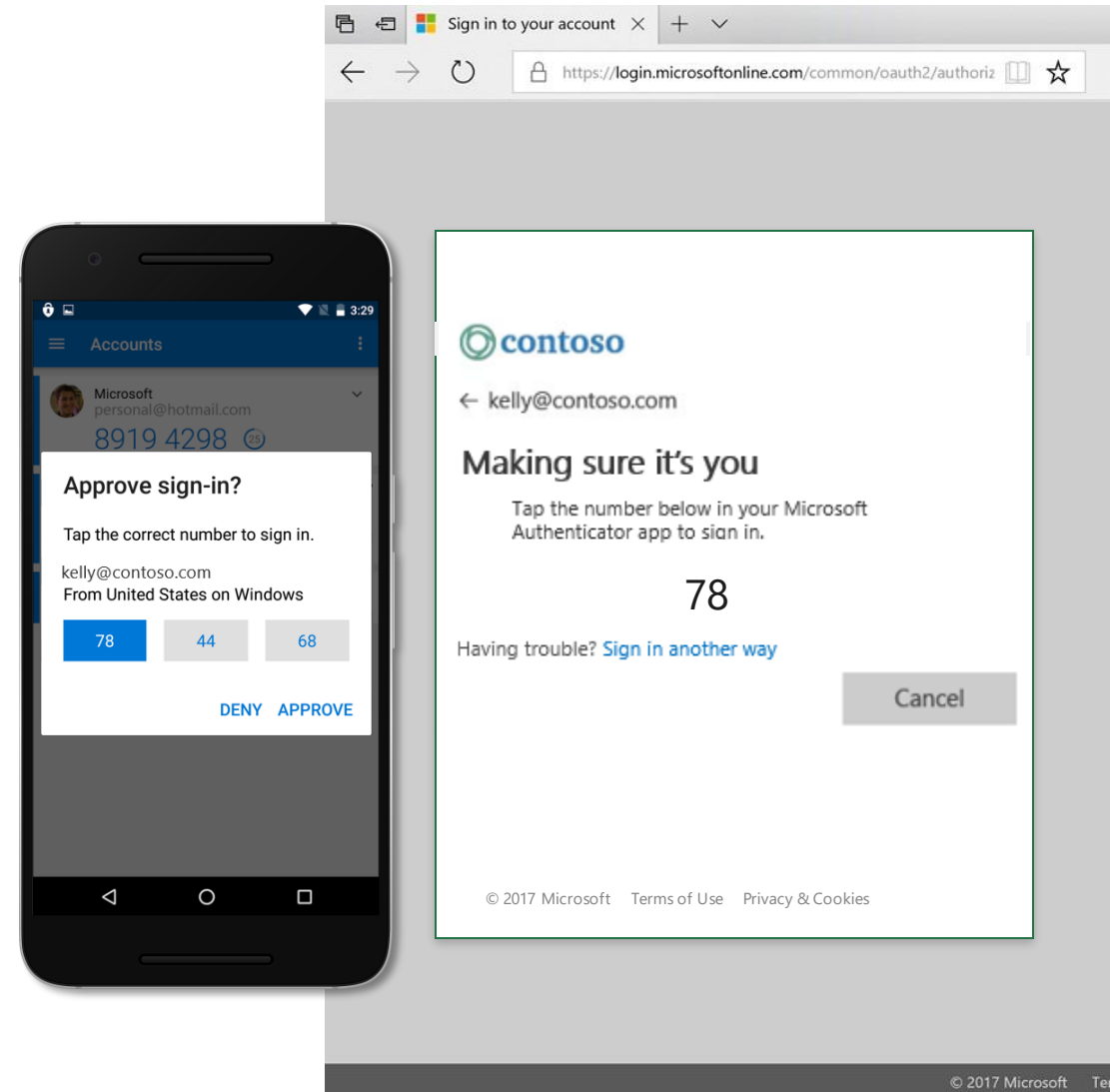


Seamless, secure and productive experience for users Microsoft Authenticator for Azure AD

Phone sign-in using Microsoft Authenticator

Two factor, password-less authentication

Public / Private key exchange



Azure AD support for any OATH-certified hardware tokens

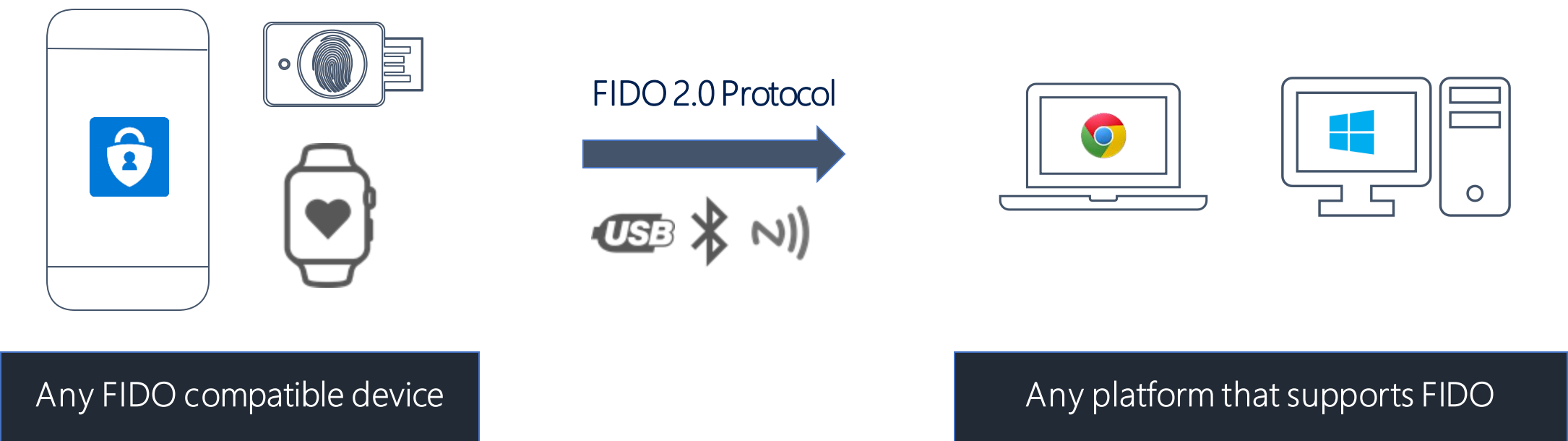
MFA without smartphones

Use up to 5 authenticator devices
per user



Seamless, secure and productive experience for users

FIDO2 for Azure AD Join (in private preview)



FIDO 2.0 creates an open ecosystem of authentication devices

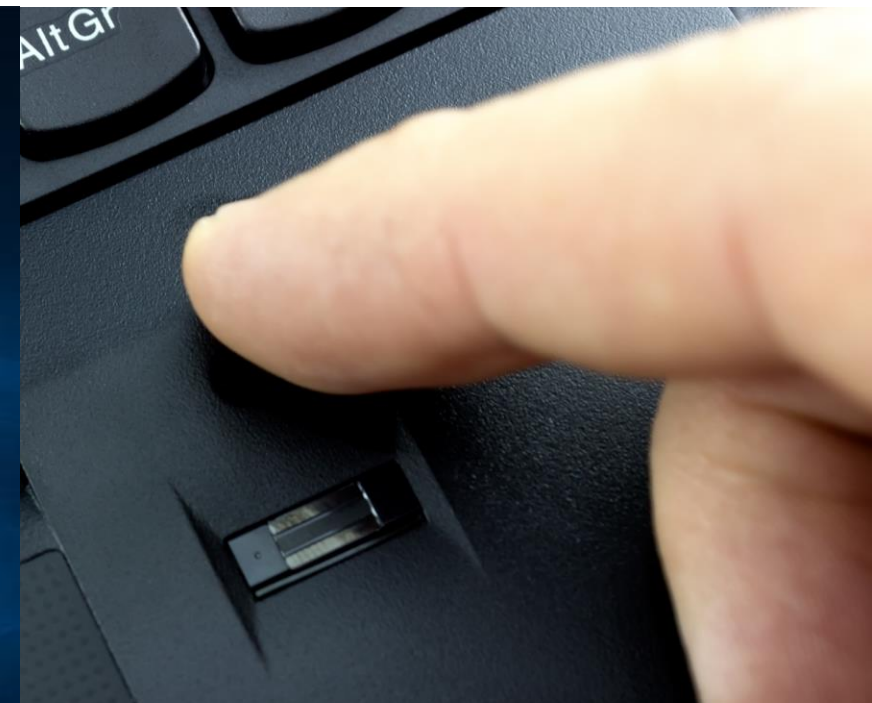
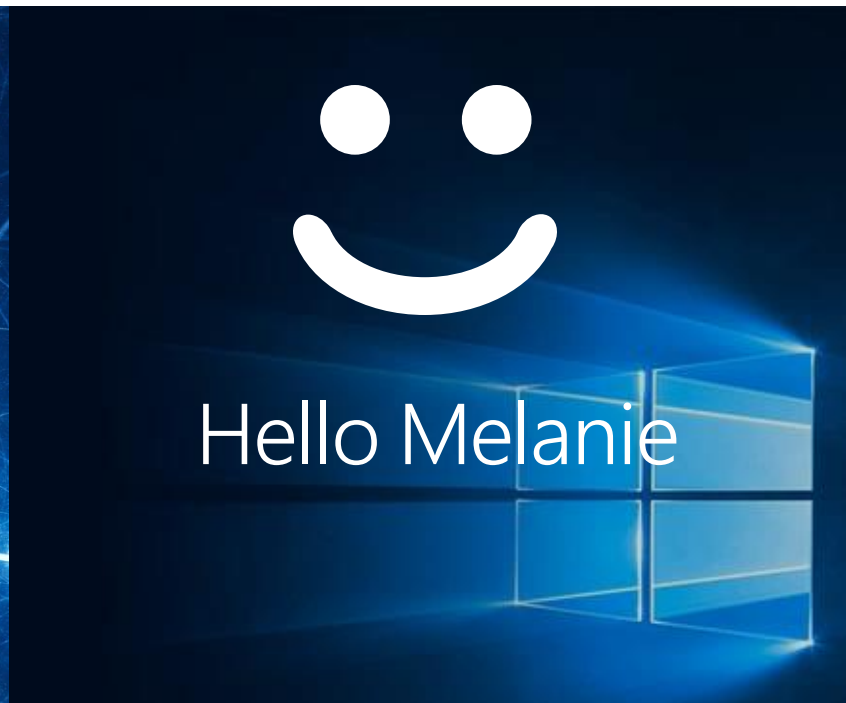
Windows 10 MFA

Password-less with Windows 10 Hello

Enterprise-grade security

User-friendly experience

Password-less authentication



47M

active Windows
Hello users

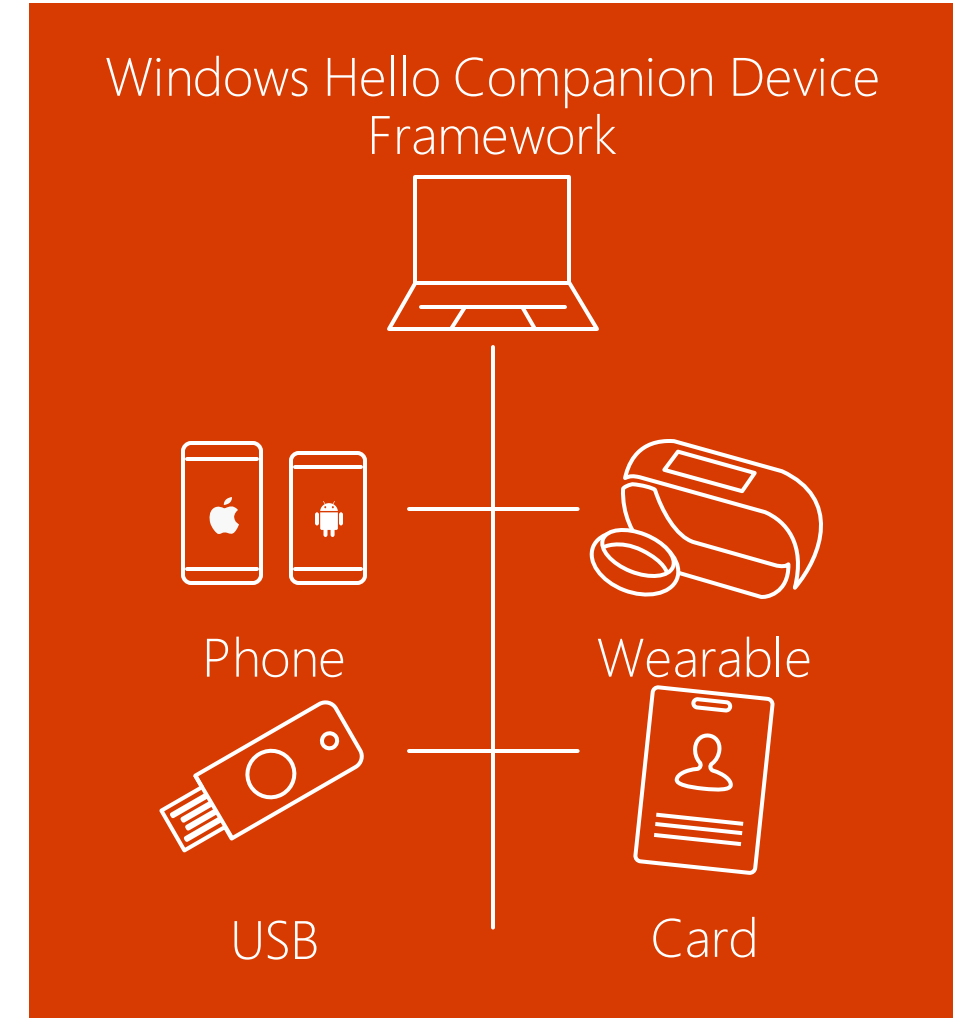


6.5k

enterprises have deployed
Windows Hello for Business

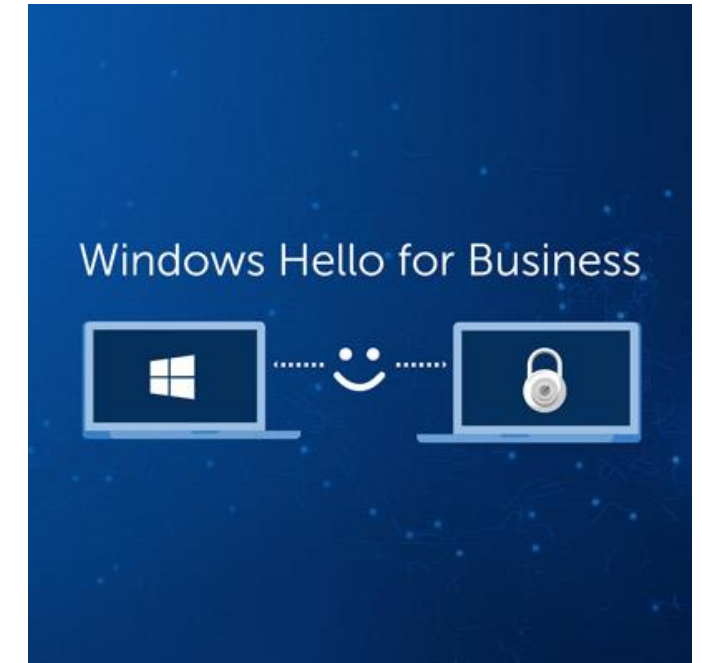
Windows Hello for Business

- **No passwords!**
 - Password-less, strong authentication
 - On devices with TPM, multi-factor authentication
- **Available for Windows 10**
- **Secure**
 - Credentials are protected by hardware
- **Extensible**
 - The Windows Hello Companion Device Framework
 - Possibilities for a wide array of devices



WHFB Authentication Methods

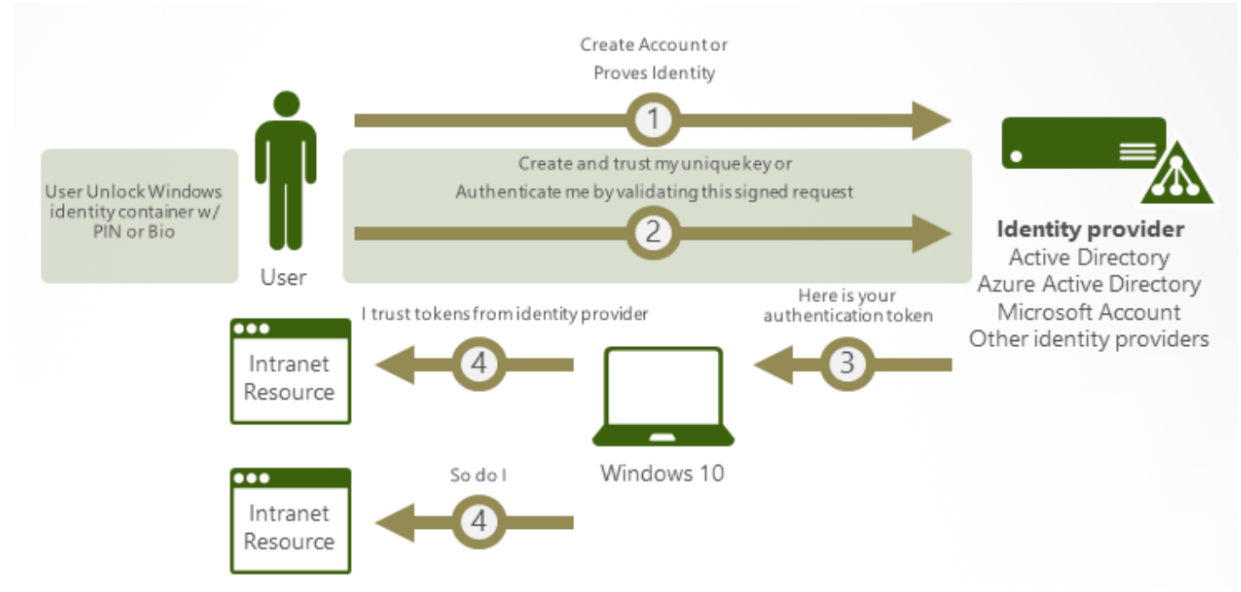
- Windows Hello for Business offers these methods:
 - Log in with your username and password
 - Log in with a PIN
 - Log in with facial recognition
 - Log in with a fingerprint
 - Log in with the Microsoft Authenticator app
 - Log in with a FIDO 2.0 key* (like [Yubikeys](#))



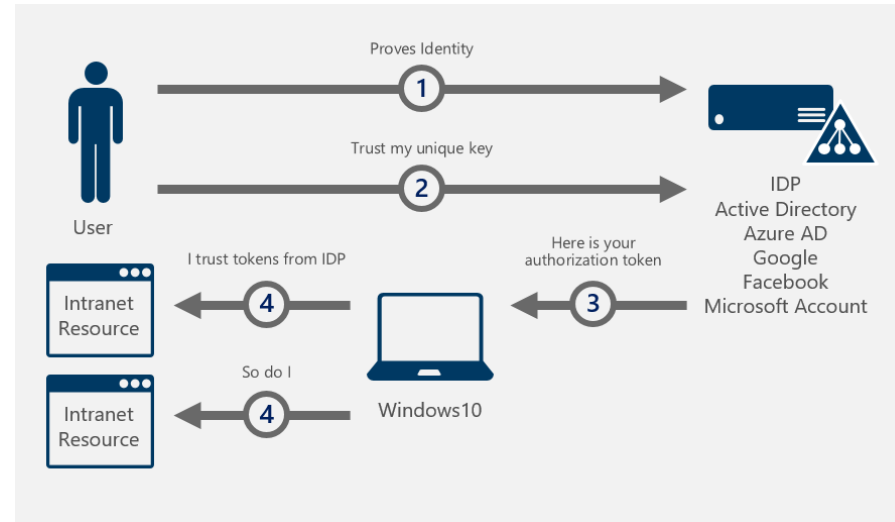
* In private preview only for non-Hybrid Azure AD joined devices running Windows 10 version 1809, and up

Windows Hello for Business: Workflow

Registration



Access



Windows 10 Hello for Business: Intune

Device Enrollment

Home > Microsoft Intune > Device enrollment - Windows enrollment > Windows Hello for Business - Properties > Settings

Windows Hello for Business - Properties

Windows enrollment

Search (Ctrl+/)

Overview

Manage

Properties

Name: All users and all devices

Description: This is the default Windows Hello for Business configuration applied with the lowest priority to all users regardless of group membership.

Settings: **Enabled**

Settings

Save Discard

Configure Windows Hello for Business: Enabled

Use a Trusted Platform Module (TPM): Required Preferred

Minimum PIN length: 6

Maximum PIN length: 127

Lowercase letters in PIN: Not allowed

Uppercase letters in PIN: Not allowed

Special characters in PIN: Not allowed

PIN expiration (days): 41

Remember PIN history: 5

Allow biometric authentication: Yes No

Use enhanced anti-spoofing, when available: Yes

Allow phone sign-in: Yes No

Device Configuration

Home > Microsoft Intune > Device configuration - Profiles > Create profile > Windows Hello for Business

Create profile

Name: Enter a name...

Description: Enter a description...

Platform: Windows 10 and later

Profile type: Identity protection

Settings: **Configure**

Scope (Tags): 0 scope(s) selected

Windows Hello for Business

Windows 10 and later

Configure Windows Hello for Business: Enable

Minimum PIN length: Not configured

Maximum PIN length: Not configured

Lowercase letters in PIN: Not allowed

Uppercase letters in PIN: Not allowed

Special characters in PIN: Not allowed

PIN expiration (days): Not configured

Remember PIN history: Not configured

Enable PIN recovery: Enable Not configured

Use a Trusted Platform Module (TPM): Enable Not configured

Allow biometric authentication: Enable Not configured

Use enhanced anti-spoofing, when available: Enable Not configured

Certificate for on-premise resources: Enable Not configured

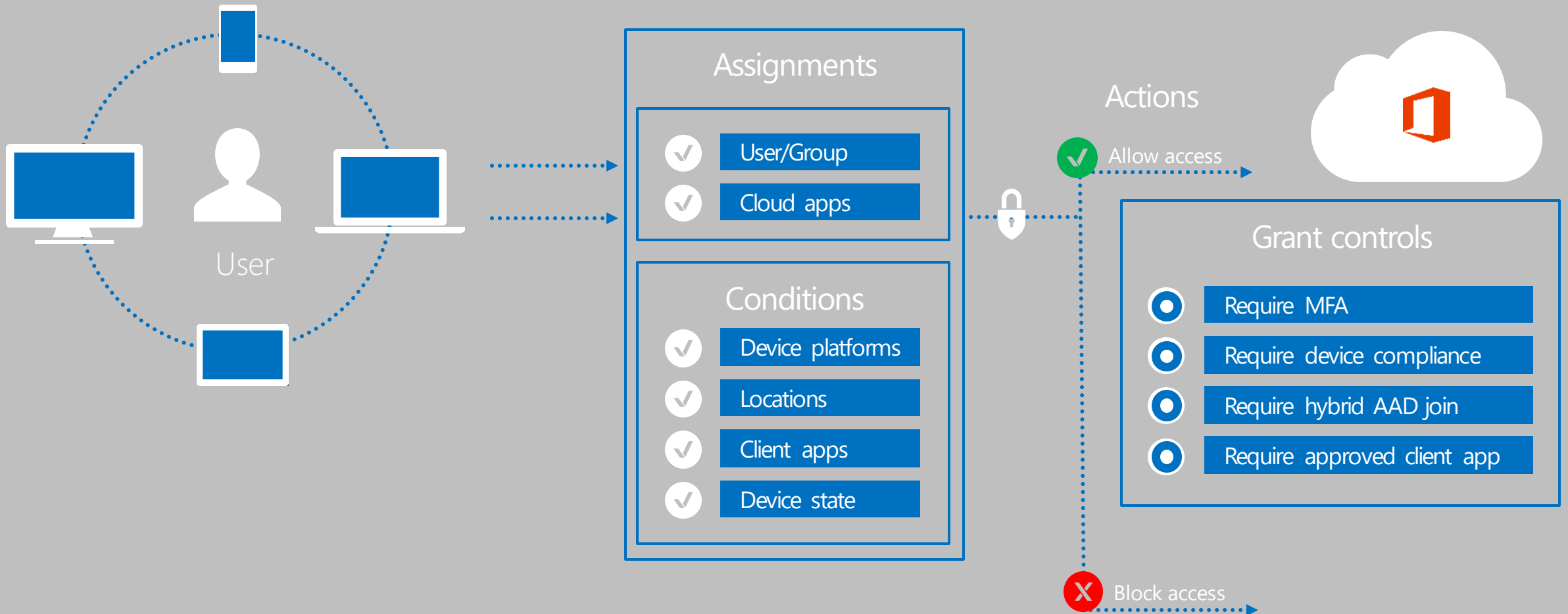
Modern Authentication in M365

Modern Authentication

- Modern Authentication in Microsoft 365 is based on ADAL (Active Directory Authentication Library) and OAuth 2.0 and supports some of the newer features that are available in Microsoft 365. These security features provide enhanced authentication to users. Examples include:
- Multi-factor Authentication (MFA) using smart cards
- Certificate-based Authentication (CBA)
- Third-party SAML identity providers
- By default Exchange Online, SharePoint Online, and Skype for Business Online automatically use Modern Authentication.
- Office 2013 must be enable; Office 2016/2019 default enable

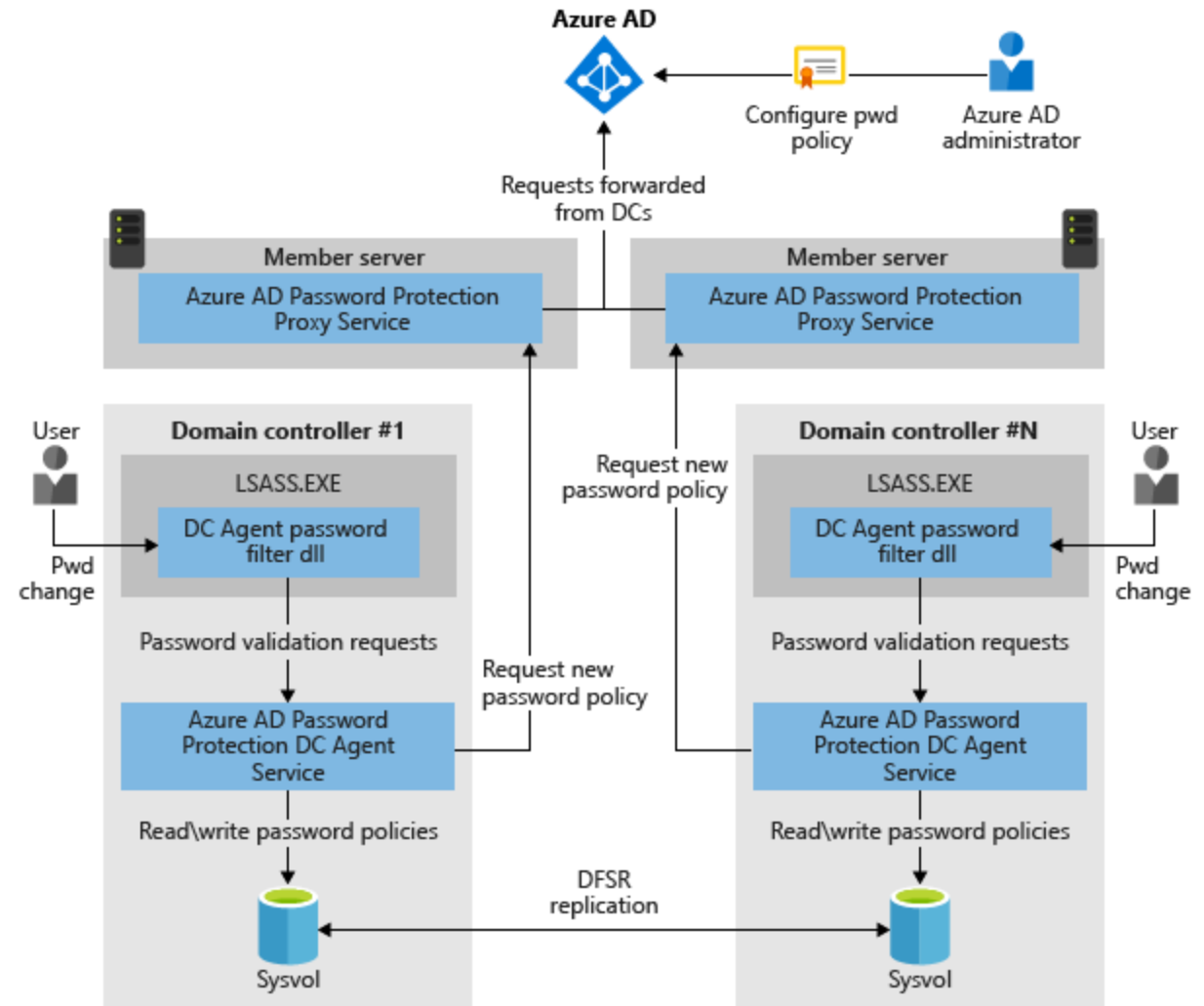
Azure Active Directory P1 Plan

Conditional Access

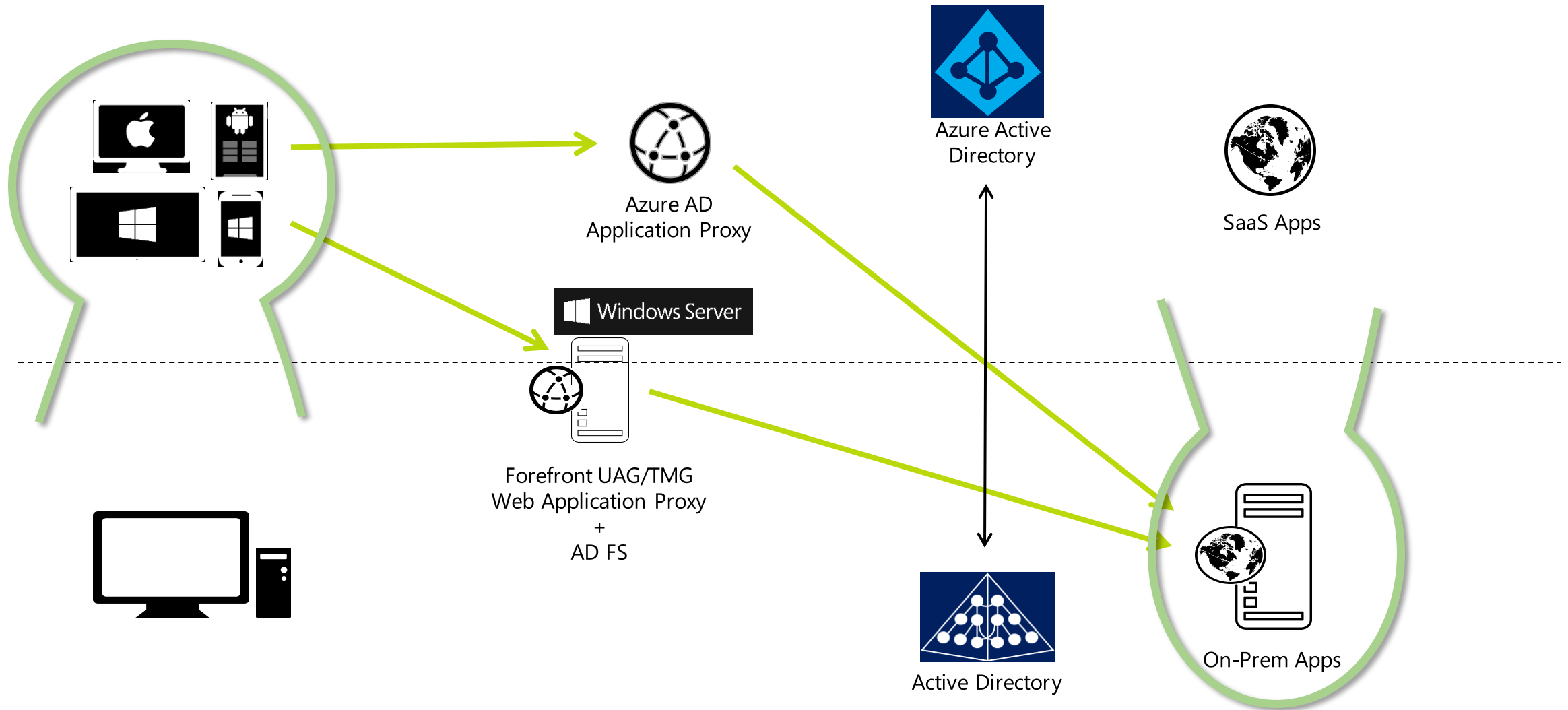


Azure AD Password Protection

- Hackers use brute force techniques like password spray attacks to discover and compromise accounts with common passwords.
- Azure AD Password Protection helps you eliminate easily guessed passwords from your environment, which can dramatically lower the risk of being compromised by a password spray attack
- Azure AD Password Protection also provides an integrated admin experience to control checks for passwords in your organization, in Azure and on-premises.
- Azure AD Premium Password Protection is an Azure AD Premium 1 feature
- Required: Azure AD password protection for Windows Server Active Directory (preview)

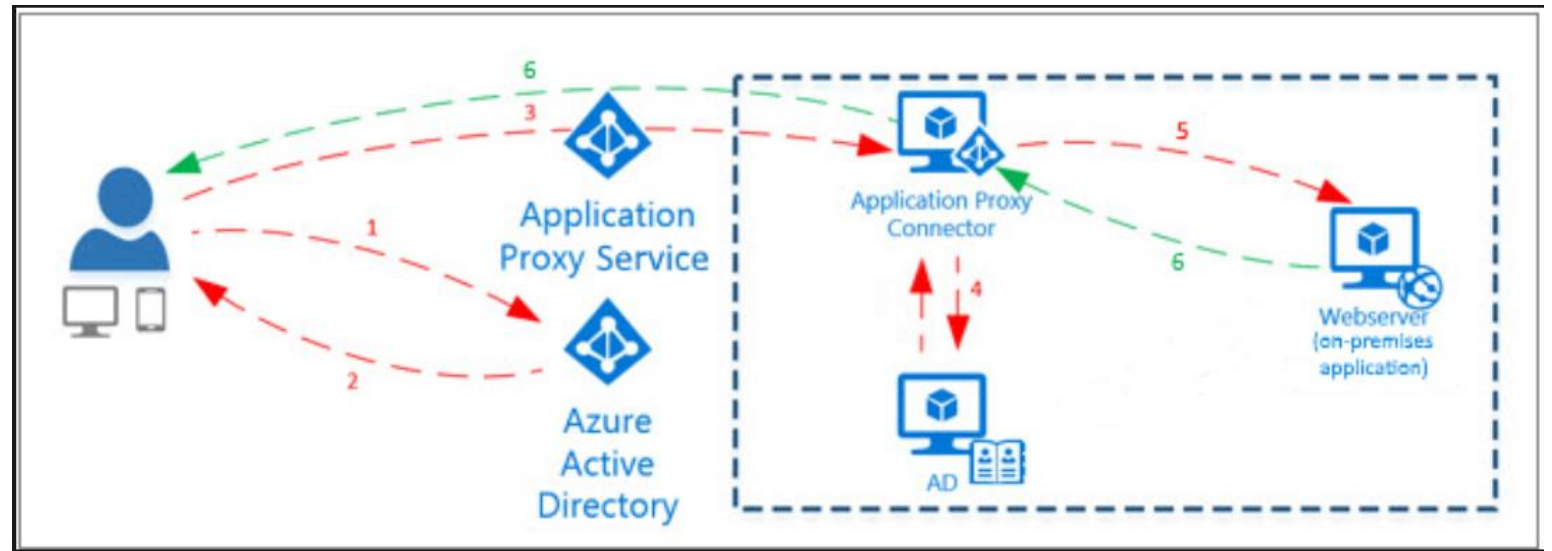


Azure AD Proxy Apps: Application Access scenario



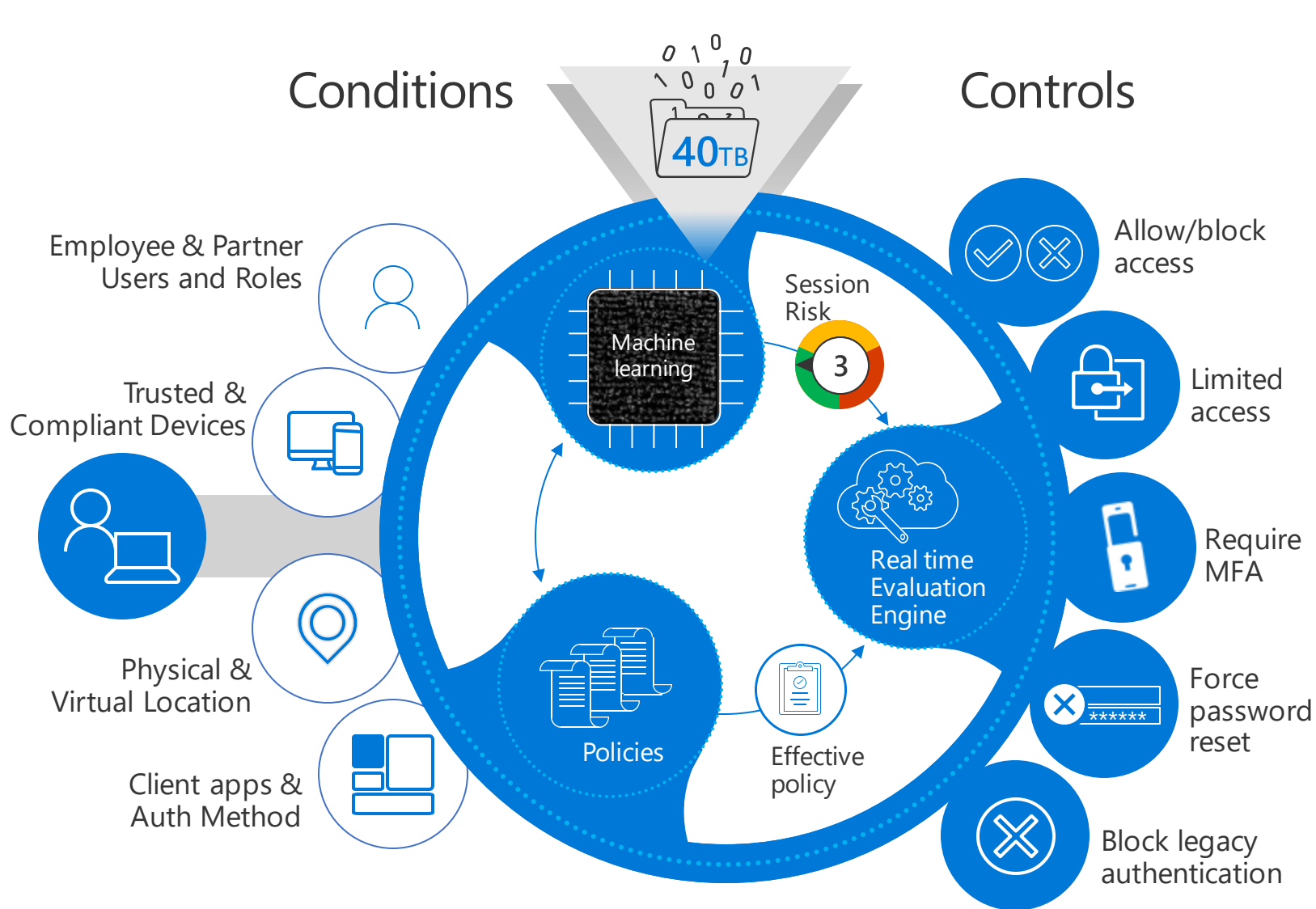
How Application Proxy Service works

- Connectors are deployed on local network
- Multiple connectors can be deployed for redundancy and scale
- The connector auto connects to the cloud service
- User connects to the cloud service that routes their traffic to the resources via the connectors



Azure Active Directory P2 Plan

Azure AD Identity Protection



Azure AD
ADFS
MSA
Google ID

Android
iOS
MacOS
Windows
Windows Defender ATP

Geo-location
Corporate Network

Browser apps
Client apps



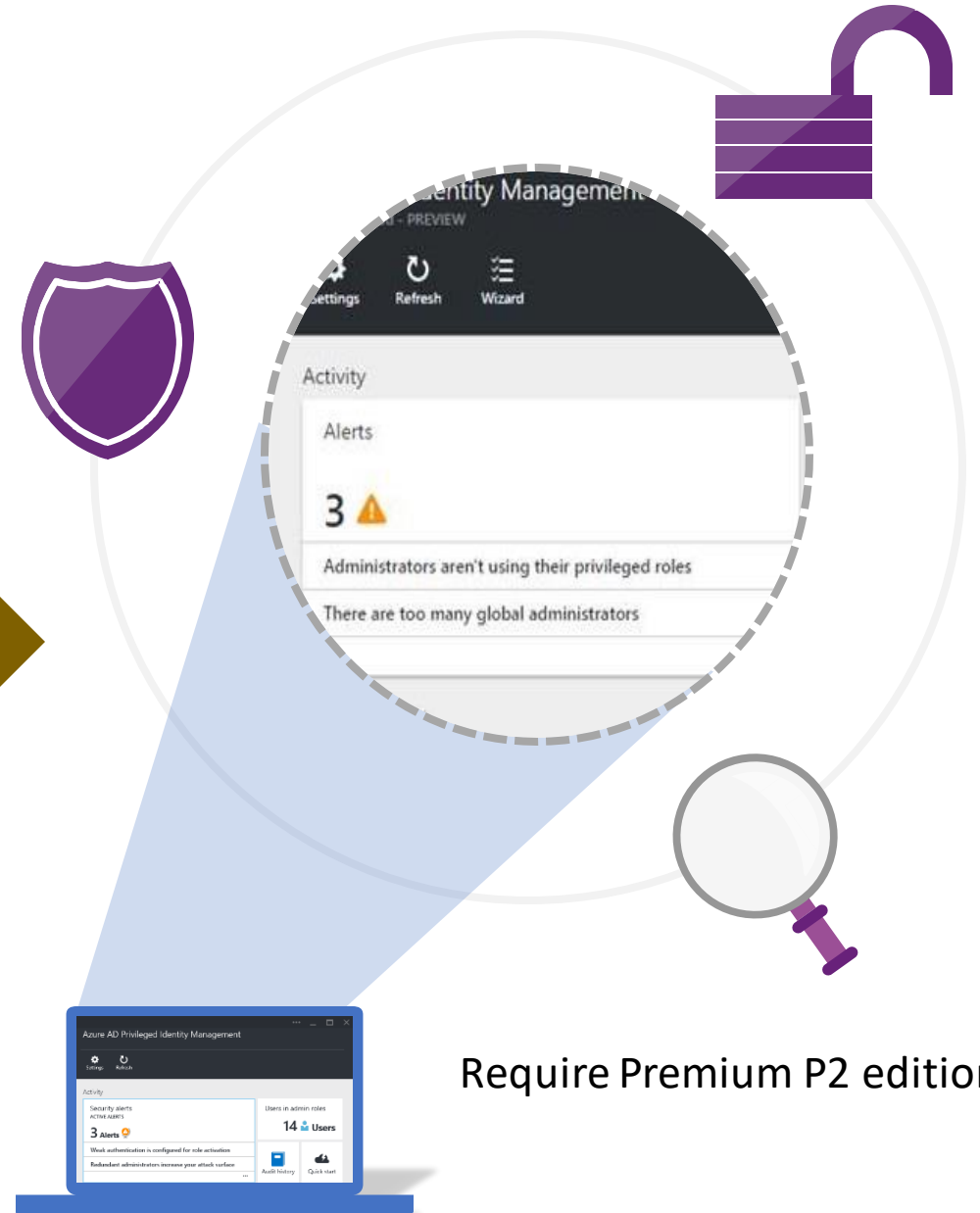
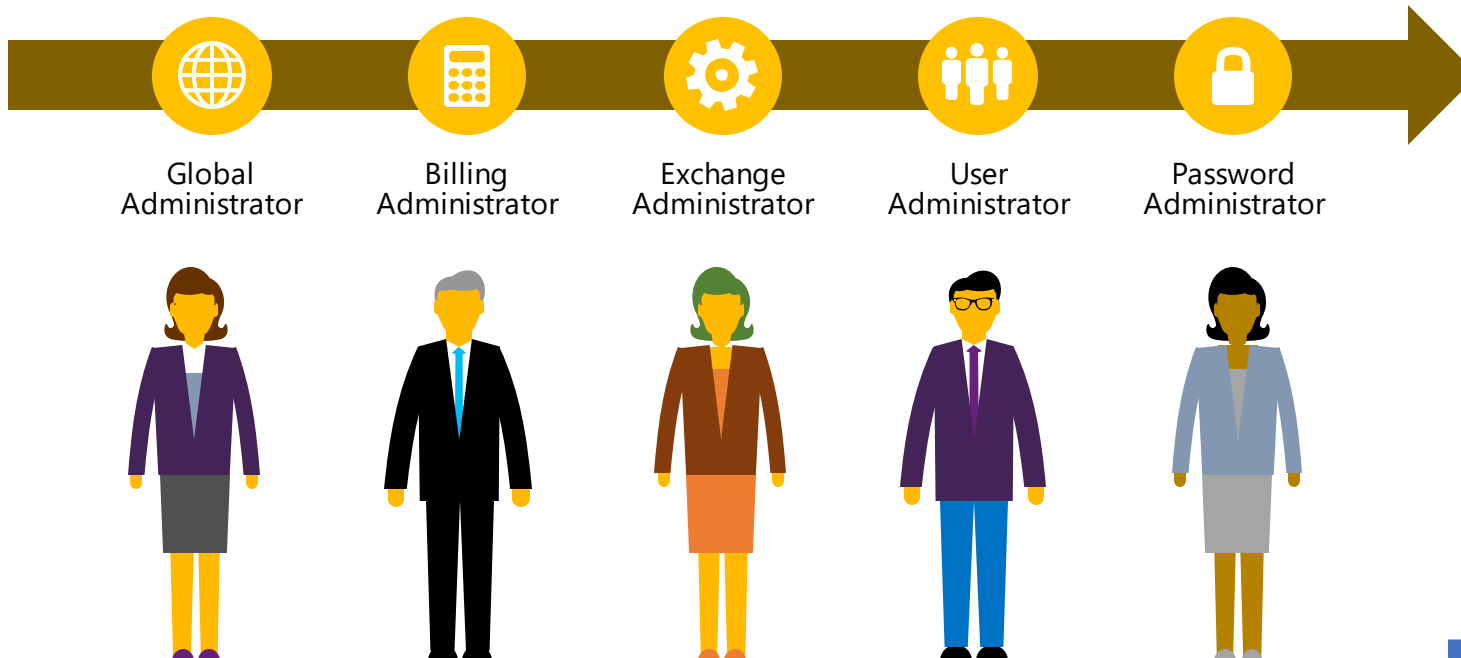
Privileged Identity Management

Discover, restrict, and monitor privileged identities

Enforce on-demand, just-in-time administrative access when needed

Manage access to resources in Azure AD, Azure Resources (Preview), and other Microsoft Online Services like Office 365 or Microsoft Intune

Provides more visibility through alerts, audit reports and access reviews



Privileged Identity Management benefits

Reduces exposure
to attacks
targeting admins

Removes unneeded permanent
admin role assignments

Limits the time a user has admin
privileges

Ensures MFA validation prior to
admin role activation

Simplifies
delegation

Separates role administration
from other tasks

Adds roles for read-only views
of reports and history

Asks users to review and justify
continued need for admin role

Increases visibility
and finer-grained
control

Enables least privilege role
assignments

Alerts on users who haven't
used their role assignments

Simplifies reporting on admin
activity

Grazie

