Azure Active Directory za administratorje Aktivnega imenika

Slavko Kukrika
MVP in prijazen fant

#ntk19

Agenda

- What is (and is NOT) Azure Active Directory?
- Integrating Azure AD with AD DS
- Using some of the Azure AD features
- Azure AD Conditional Access
- Azure Active Directory related Azure services

What Azure Active Directory is NOT

AAD ≠

ADD ≠ DC in Azure VM

AD ⟶ AAD

AD DS

OU, domain, tree, forest

+ additional AD roles
AD Rights Management Services

Singe Sign On in AD forest
Group Policy
Used on LANs and WANs

Kerberos, LDAP

Rich administrative tools

Azure AD

Multi-tenant service

Azure Access Control Service
RMS, PIM, Identity Protection, …
Single Sign On to apps
Can integrate with MDM (no GP)
Used on Internet

REST, SAML-P, WS-Federation,
OAuth, Graph API

Web administration

What is Azure Active Directory?

Cloud service – no on-premises infrastructure needed

- Global scale, reliability and 99,99% SLA availability

Identity store in the cloud

- Can be synchronized with on-premises AD DS
- Used by cloud apps, such as Office 365, Dynamics and Intune

Can be used for device management – Windows, Android and iOS

Control access to apps and resources

Provides additional features, such as:

- Dynamic groups
- Self-service password reset
- Multifactor authentication
- Conditional dynamic access

Azure Active Directory editions

Free

- User and group management
- SSO to 10 apps
- Self-service password change
- Windows 10 Azure AD join
- Sync with on-premises AD DS
- Basic security and usage reports

Basic

- Group-based access management
- Self-service password reset
- Company branding
- Application proxy
- SLA

Premium P1

- Advanced group features
- SSPR with on-premises write-back
- Device write-back
- Multi-factor authentication
- Conditional access based on compliance, location and groups
- MDM auto-enrollment
- Enterprise State Roaming

Premium P2

- Identity protection
- Privileged Identity Management
- Access Reviews

Creating and Managing Azure Active Directory

Azure portal / Azure Active Directory admin center

Microsoft 365 admin center

Azure PowerShell (+ Azure Active Directory module)

Traditional on-premises Active Directory tools

- Only if on-premises Active Directory is synchronized with Azure Active Directory

Synchronizing AD DS with Azure Active Directory

Same Sign-on (Sync identity only)

- Passwords in Azure AD are different then in on-premises AD DS

Synchronize password hashes to Azure AD

- Referred as PHS (Password Hash Sync)
- Passwords in Azure AD and on-premises AD DS are identical
- Recommended option for organizations who do not want any on-premises footprint

Authenticate with ADFS

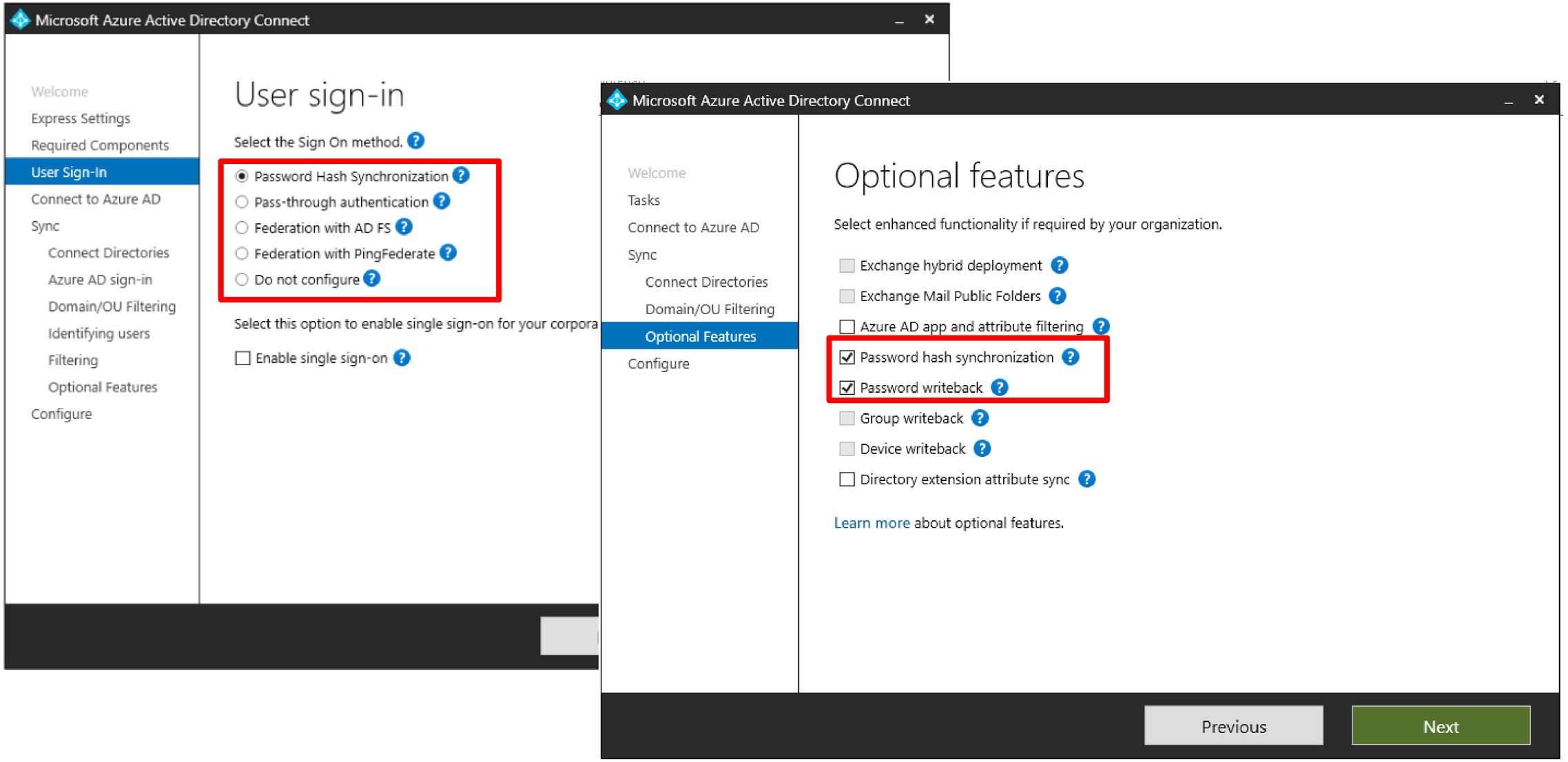
- Passwords are stored only on-premises
- Flexibility and third party interoperability

Authenticate with AD using Pass-through Authentication agent

- Referred to as PTA (Pass-through Authentication)
- Keeps passwords on premise, with on-premises lightweight agent

Azure AD Connect

Azure AD Connect



Groups in Azure Active Directory

Groups are used for managing access to apps and resources

Group can have following membership type:

- Assigned
- Dynamic User
- Dynamic Device

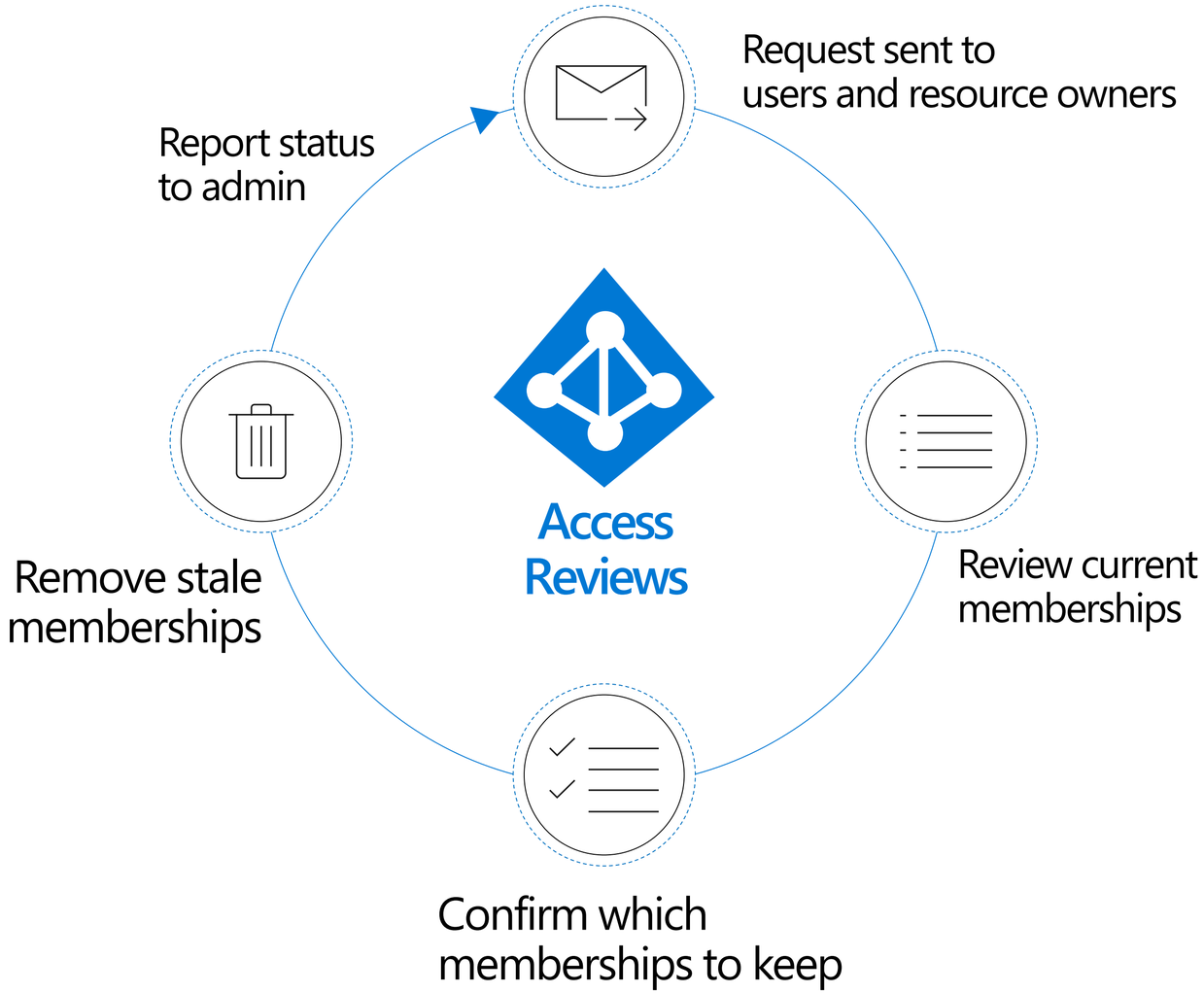
Self-Service Group Management

Group Expiration

Azure Active Directory Access Review

Access reviews

- Manage risk and compliance for employees, guests, business partners, and contractors
- Audit and recertify users' access to applications, resources, and roles
- Configure programs to automatically repeat complex review sequences
- Reviewer can be whoever you want



Self Service Password Reset

User must prove his identity to be able to reset his password

- E-mail, SMS, Authenticator app, security questions

Admins are always enabled for self service password reset

Password write-back to integrate with on-premises AD DS

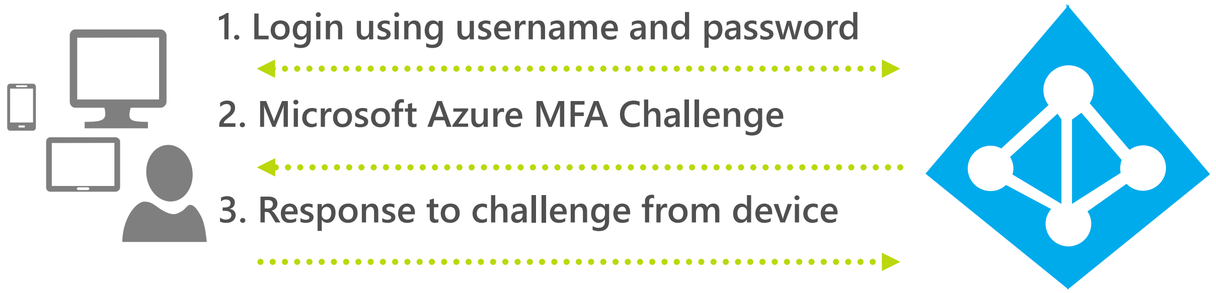
Multi-Factor Authentication

MFA

What is it?

A method of authentication requiring the use of more than one verification method to authenticate a user.

- Mobile Application
- Automated Phone Call
- Text Message



How it works?

Requiring any two or more verification methods

- Something you know (typically a password)
- Something you have (a trusted device that is not easily duplicated, like a smartphone)

Password protection

Authentication methods

Leverages existing Azure Active Directory passwords capabilities

You can configure custom weak password lists (banned passwords)

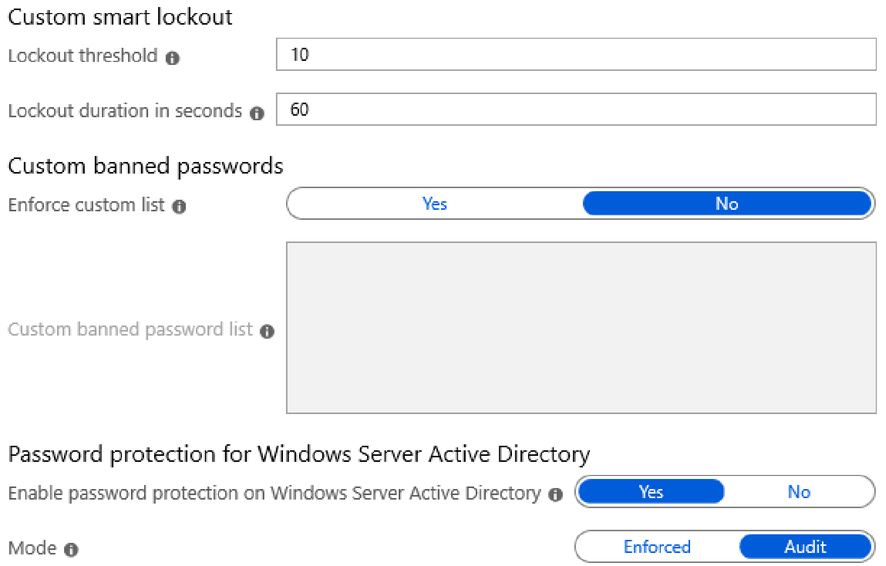
On-premises DCs do NOT require connectivity to the Internet

- Handled via proxy agent on domain member(s)

Substrings within passwords are matched against banned tokens

- Other checks include Levenshtein distances and scoring of weak tokens vs. overall length

Supports Windows Server 2012 R2 and newer domain controllers

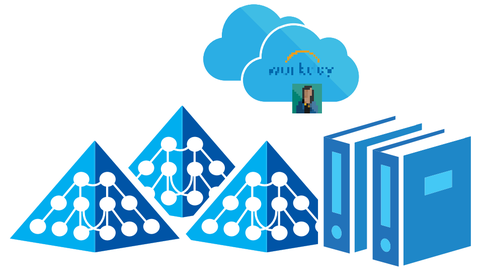


Publishing apps in Azure Active Directory

3100+ preintegrated popular SaaS apps.

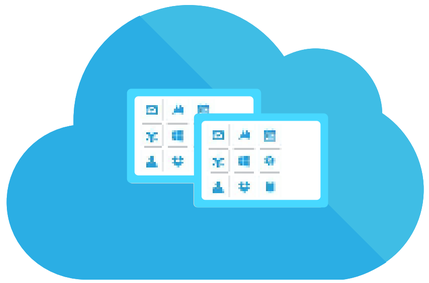
Users can discover available apps at:
http://myapps.microsoft.com

Easily publish on-prem web apps via Application Proxy + Custom apps through a rich standards-based platform.

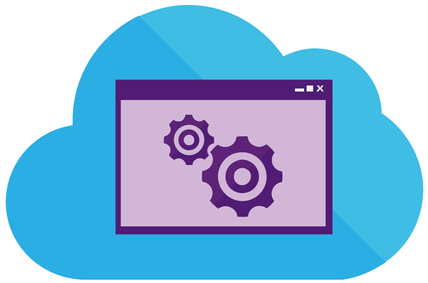


Windows Server
Active Directory
+
Other Directories

Microsoft Azure



SaaS apps

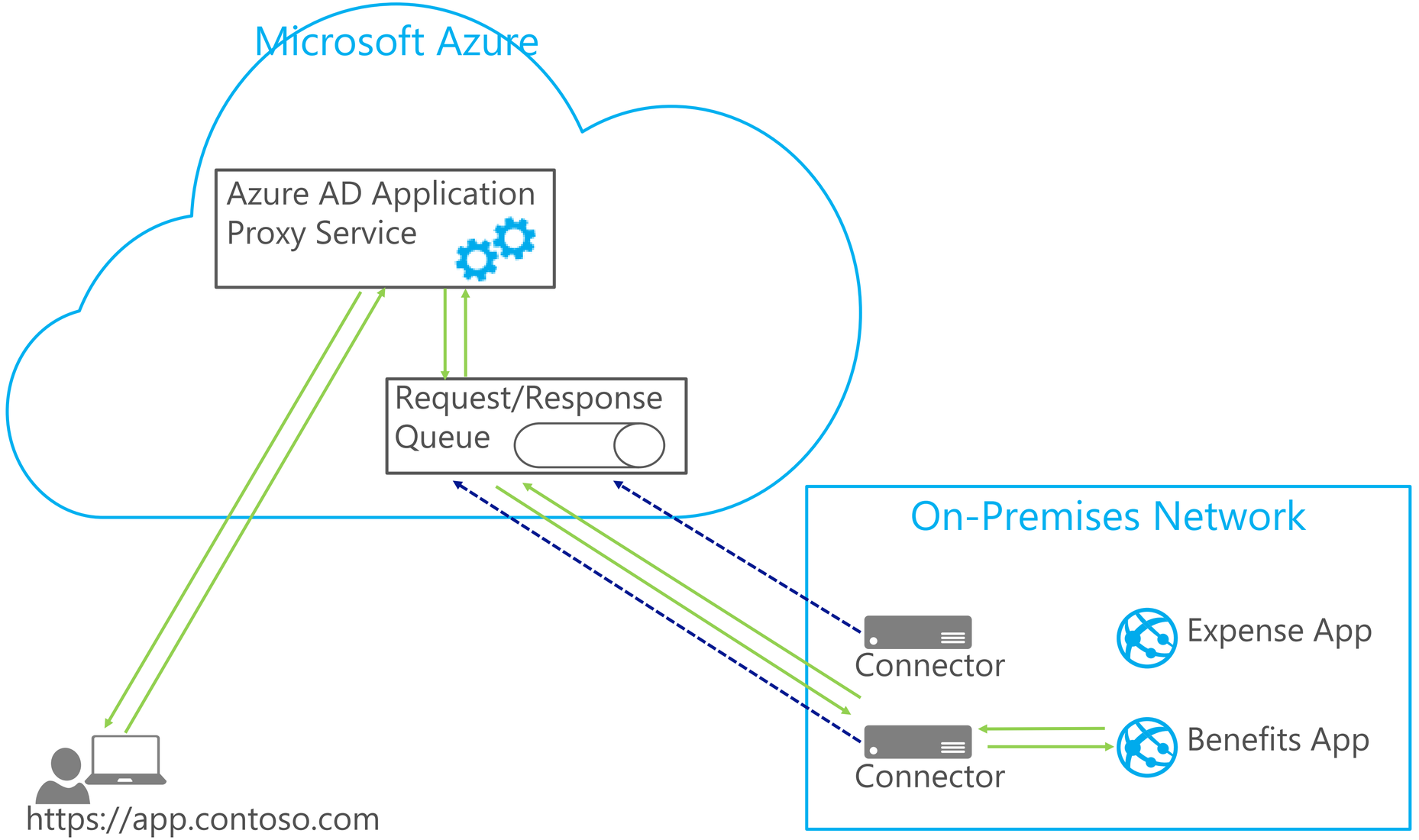


Web Apps
(Azure Active Directory Application Proxy)

Integrated custom apps

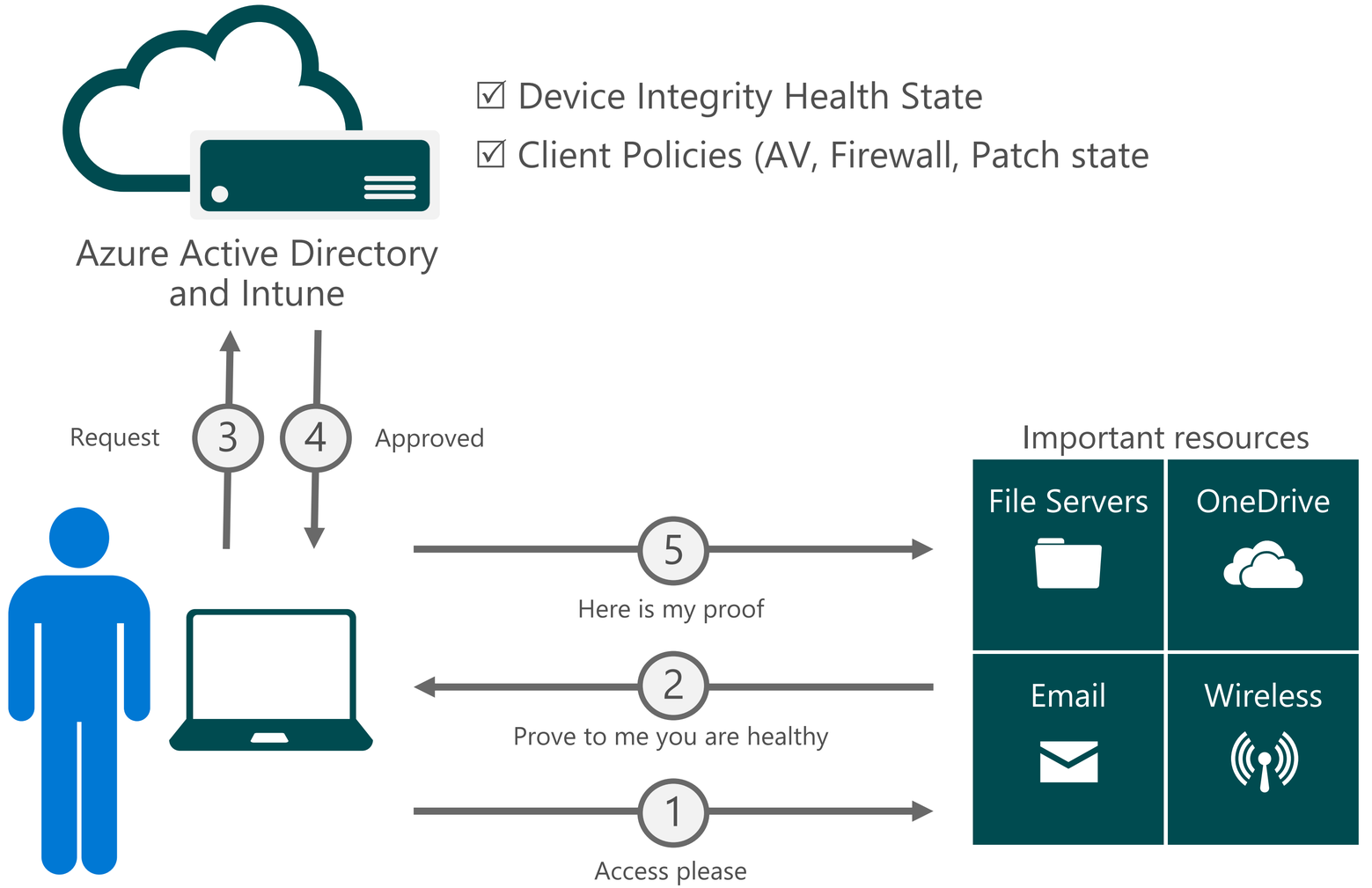
1000s of Applications, single password with SSO experience

Azure AD Application Proxy



Device compliance

1. MDM evaluates policy compliance
2. Health Attestation service reports device compliance
3. MDM reports to Azure AD device compliance
4. Compliance information is used by Conditional Access to grant or deny access



Conditional Access

Conditional Access

Policy Conditions

Azure AD Identity Protection Service

User
- User identity
- Group membership
- Session Risk

Windows Defender
Lookout
Skycure

Device
- OS Platform
- Is Compliant / Domain joined
- Is lost or stolen
- Device Risk

App
- Mobile or Cloud app
- Per app policy

Location
- IP range
- Country / Region

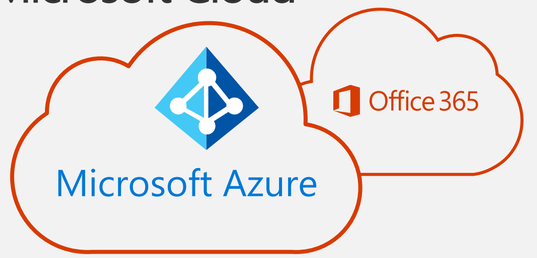
Policy Controls

Access Control
- Allow sign-in
- Block sign-in
- Enforce MFA
- Terms of Use
- Partners

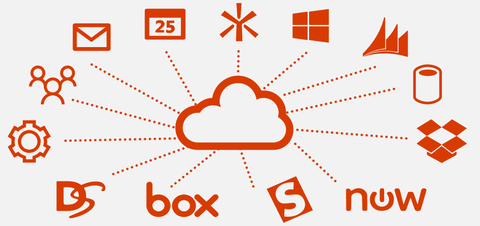
Session Restrictions
- Restrict download
- Disable print
- Prevent data leak

Applications

Microsoft Cloud



3rd Party SaaS Apps

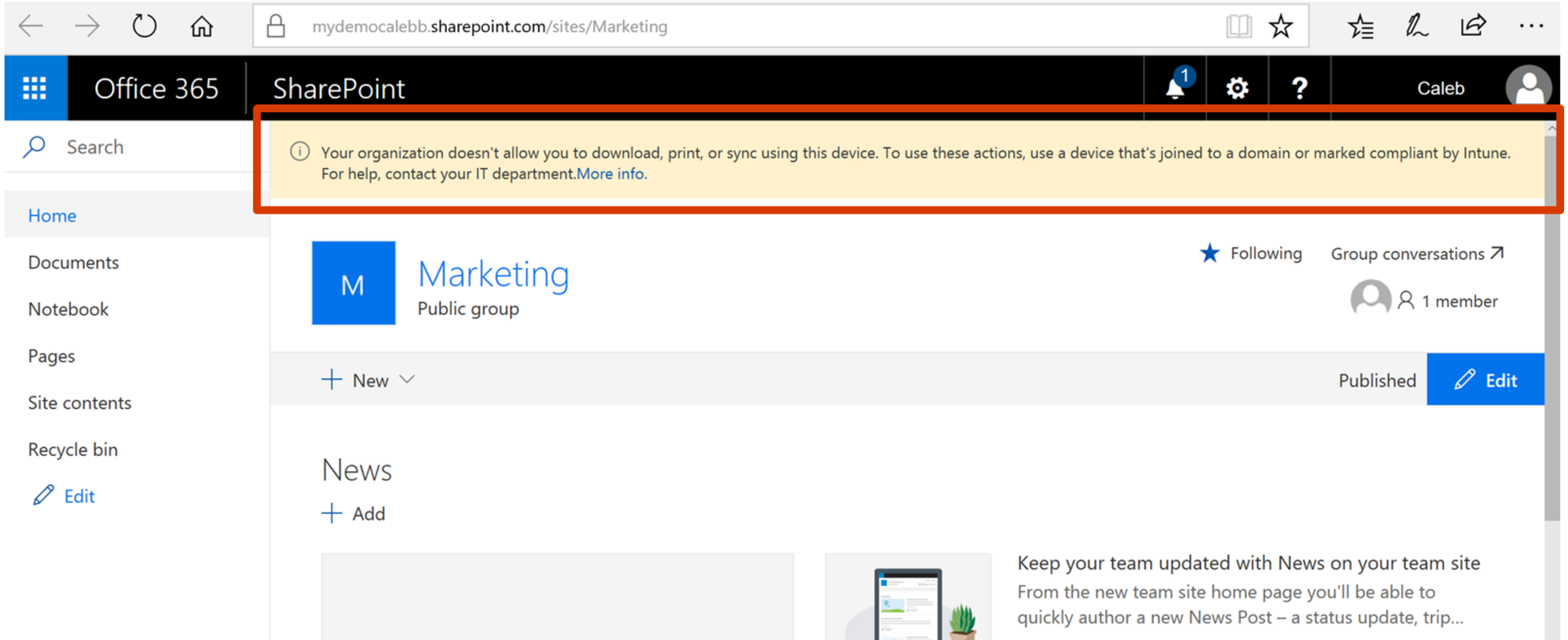


On Premises Apps

Session control

Conditional access isn’t just a binary allow / block

Different levels of access in a session enable better security and productivity



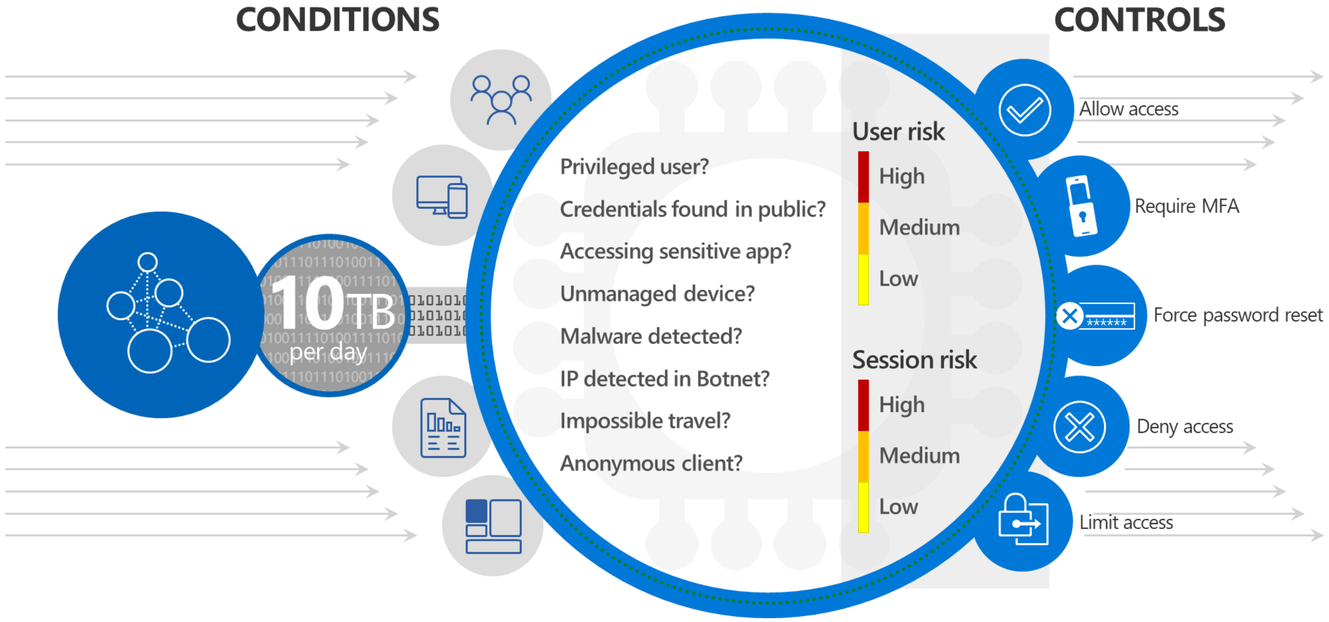
Azure Active Directory related services

Azure AD Privileged Identity Management

- Discover, restrict and monitor privileged identities and their access to resources
- Enforce on-demand, just in time administrative access when needed
- Set up approval flows for privilege activation.
- Ensure policies are met with alerts, audit reports and access reviews

Azure AD Identity Protection

- Detects anomalies in individual sign-ins
  - Sign-ins from unfamiliar locations
  - Impossible travel from unfamiliar locations
  - Sign-ins from malware-infected devices
  - Sign-ins from anonymous IP addresses
  - Sign-ins from suspicious IP addresses
- Users flagged for risk: Low, Middle, High
- User risk policy and Sign-in risk policy



Summary

Azure Active Directory stores identities and provides access control

- It can be integrated with Microsoft Intune (MDM device management)

Azure Active Directory has four editions

- Azure Active Directory licenses are assigned to users or groups

Different options for synchronization with on-premises AD DS

- Sync identities only, Password Hash Sync, federation, Pass-through Authentication

Groups management, access review and password protection

Self service password reset, Multi-factor authentication

Conditional access

Additional information

What is Azure Active Directory?

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis

What is hybrid identity?

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-hybrid-identity

Azure AD Connect sync: Understand and customize synchronization

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-whatis

How it works: Azure AD self-service password reset

https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks

What is conditional access in Azure Active Directory?

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

Azure Active Directory: Introduction

https://social.technet.microsoft.com/wiki/contents/articles/51495.azure-active-directory-introduction.aspx