Microsoft and Yubico Part 4 - Enterprise Strong Authentication

Recommended Action Items

This document lists all the references in the series in one easy to find place. Additional informational references are also provided for more details.

Enable security keys as an available passwordless authentication method

- Enable FIDO2 Security Keys as a sign-in option in Azure AD
  - [Enable passwordless security key sign in](#)

Secure the admins by enforcing MFA

- Require MFA for Azure AD Admins using baseline policies or Conditional Access Policies
  - [Before you begin: Protect privileged accounts with MFA](#)

Drive more adoption of passwordless using Conditional Access Policies

- Focus on getting users to use passwordless sign-in.
- Create Conditional Access Policies to require MFA for specific applications and groups of users.
  - [Azure AD Conditional Access documentation](#)
  - Leverage Identity Protection to require MFA for Medium and High RIek sign-ins.
    - [Azure AD Conditional Access Policies - Sign-In Risk Conditions](#)

Enable Windows sign-in with FIDO2 security keys

- Enable Windows to use FIDO2 credential provider
  - [Complete a passwordless authentication deployment](#)

Federate your SaaS applications with Azure AD

- Connect to your applications with federated Single Sign On
  - [Single Sign-On to applications](#)

Enable alternate MFA options for applications that don't support passwordless

- Leverage Azure MFA OATH-TOTP capabilities with YubiKeys if passwordless sign-in cannot be leveraged.
  - [Using YubiKeys With Azure MFA](#)
- Leverage SaaS applications' native MFA capabilities with YubiKeys if the SaaS application cannot be federated with Azure AD
● Works With YubiKey Catalog

Synchronize your on-premises users with AAD Connect
  ❏ Synchronize on-premises users with AAD Connect.
    ● What is Azure AD Connect?
  ❏ Setup Password Hash Sync or alternate authentication method
    ● What is password hash sync?
    ● Choose the right authentication method

Migrate on-premises applications federated with AD FS using Azure AD federation
  ❏ Migrate on-premises applications federated with AD FS to Azure AD
    ● Azure AD Migration Resources

Enable on-premises legacy IWA applications to use passwordless sign-in
  ❏ Upgrade the on-premises applications to use modern authentication protocols
    ● Single sign-on to applications in Azure Active Directory
  ❏ Enable Azure AD Hybrid features
    ● Enable passwordless security key sign-in to on-premises resources with Azure Active Directory
  ❏ Enable Azure AD Application Proxies
    ● Remote access to on-premises applications through Azure Active Directory's Application Proxy

Enable MFA for on-premises applications using RADIUS with NPS Server extension
  ❏ Configure on-premises applications using RADIUS to use Azure MFA and YubiKeys
    ● Integrate your existing NPS infrastructure with Azure Multi-Factor Authentication

Certificate based sign-in with smart cards
  ❏ Leverage YubiKey as the physical smart card
    ● YubiKey Smart Card Deployment Guide