Microsoft and Yubico Part 3 - On-premises and Cloud Organizations

On-premises + Cloud Organization Components

Context

In this scenario an On-premises and Cloud Organization:

- Leverages Azure AD as a primary identity provider and for federation.
- Use different MFA controls, sometimes using smart phones with TOTP, push notifications, or SMS. Generally using multiple MFA providers such as Azure MFA, application specific MFA, or third party solutions.
- Utilize SaaS applications for productivity (Office 365), HR, scheduling, CRM, and other Line of Business Applications. Some of these applications are not federated with Azure AD.
- Leverages Active Directory(AD) and Active Directory Federation Services(AD FS) infrastructure for authentication of users, applications, and systems for on-premises and external users.
- Federated some of their on-premises applications with AD FS using WS-Federation and SAML or OpenIDConnect
- Have not synchronized the on-premises users to the Azure AD tenant.
- Have not synchronized computer objects to the Azure AD tenant.
- Some on-premises applications use RADIUS authentication and require MFA controls.
- Some on-premises applications require physical smart cards to authenticate.
Transition to Passwordless

The On-premises and Cloud Organization already has guidance and a strategy from the Cloud Native Organization that addresses cloud based SaaS applications and system sign-in. The on-premises components and system interactions add a new layer of additional complexity that need a passwordless and MFA strategy. The organization realizes that the traditional network perimeter is no longer sufficient and a zero trust architecture is needed. Strong identity is one of the cornerstones of this architecture and requires strong authentication for their users to establish identity as the new control plane. The On-Premises + Cloud Organization have investigated Microsoft's zero-trust maturity model and will start moving towards more advanced capabilities knowing they cannot solely rely on the network and the firewalls.

Synchronize your on-premises users with AAD Connect

A key part to unlocking the most secure, and best experience for your users is to make sure that your organization has begun a migration to start leveraging and managing identities in the cloud. Make sure you are creating an environment that is seamless for the users, and make sure you don't create complexity for the users by creating 2 identities for the same user. You need to ensure your on-premises identities in AD are the same identities that are in Azure AD by synchronizing them using Azure AD Connect. Evaluate all your options for setting up AAD Connect. Decide which objects to synchronize, and understand which authentication options are available for your applications and services. You may have reservations about enabling Azure AD authentication using Password Hash Sync, but you should research the advantages it provides for your organization and understand how Microsoft can claim that it is secure. If Password Hash Sync is not suitable for your organization, then other options to support authentication are available.

Migrate on-premises applications federated with AD FS using Azure AD federation

The goals for on-premises federation are similar for the Cloud Native Organization where the focus was to federate your SaaS applications with Azure AD.

Organizations often choose to migrate to Azure AD to simplify the administrative duties, gain the efficiencies and scalability of the cloud, and to leverage the rich set of features and controls like Azure AD Identity Protection, and passwordless sign-in. Microsoft has provided tools and resources specifically for assisting in the migration of applications from AD FS to Azure AD. This will help you reduce the effort to analyze which applications can easily migrate.
Enable on-premises legacy IWA applications to use passwordless sign-in

For organizations that have an on-premises footprint with AD, you will likely have a catalog of applications that don't participate in federated Single Sign-On. For on-premises applications that use IWA (Integrated Windows Authentication) with Kerberos or NTLM there are three main options for enabling passwordless sign-in.

- **Upgrade the on-premises applications to use modern authentication protocols**

  Your organization may have efforts underway to migrate applications to the cloud. If your applications use IWA, it is going to be difficult to lift and shift them to the cloud. Your organization should consider upgrading relevant applications to use more modern authentication protocols like OpenID Connect, SAML, or WS-Federation and federate your on-premises application with Azure AD. This establishes the application on a path that is more portable across platforms and is one aspect that will make the application more suitable for moving to the cloud when the time comes to migrate the app. Certainly any new development or new applications should first strive to use OpenID Connect instead of using IWA. Similar to the SaaS applications described for the Cloud Native Organization, on-premises applications that are federated with Azure AD will be capable of passwordless sign-in.

Upgrading your applications isn't a hard requirement to support passwordless sign-in, however, if you don't upgrade your applications you will need additional infrastructure components deployed to support integrating the front-end using passwordless sign-in with the backend legacy authentication. The two different options exist for providing legacy IWA applications with a passwordless sign-in experience are described below.

- **Enable Azure AD Hybrid features**

  Upgrading your applications is not always a possibility or may not be a top priority for an organization. Additionally, not all clients will support modern authentication protocols and must use IWA. Microsoft has added support to Windows and Azure AD allowing an organization to use passwordless authentication to sign into Windows and still use IWA for Hybrid Azure AD Joined Windows 10 machines. Hybrid Azure AD Join is when the machine is simultaneously joined to the on-premises AD controllers in addition to being joined to Azure AD. Once this feature is enabled, and other Azure AD Hybrid components are deployed and configured, then passwordless sign-in is available to the on-premises IWA applications. A user will now seamlessly be able to sign-in to the Windows machine using the YubiKey and then gain access to the on-premises applications that leverage both modern authentication and IWA.

- **Enable Azure AD Application Proxies**

  Microsoft offers Azure AD Application Proxies that can support integrating the authentication protocols used by the front-end client and the backend legacy application. The Azure AD Application proxy is made up of public cloud facing endpoints and on-premises connectors that can bridge the authentication protocols and offer another method for your applications to support passwordless sign-in. A user accessing an IWA application via an Azure AD Application proxy can now seamlessly use passwordless sign-in with a YubiKey for accessing the application.
Enable MFA for on-premises applications using RADIUS with NPS Server extension

RADIUS is a standard protocol used by many on-premises applications. Azure AD alone will not support the protocol but Microsoft has provided support using a Network Policy Server (NPS) extension to provide a RADIUS adapter. By enabling the NPS server extension your organization will be able to leverage Azure MFA for authentication requests on applications that rely on RADIUS. Passwordless sign-in will not be available for these applications, however your organization can enable Azure MFA for these applications and leverage the same YubiKey hardware as TOTP tokens.

Certificate based sign-in with smart cards

Organizations that are using certificate based authentication using smart cards to secure access to applications already have the benefit of being passwordless. These users are in the habit of using physical cards protected with a convenient PIN for various use-cases. The physical smart cards provide users a secure, convenient way to sign-in using certificates. While the user experience is relatively simple, the infrastructure to support smart card sign-in can be complex. Enterprises with smart card deployments may have to enlist the help of different vendors to supply the physical smart cards, peripherals like smart card readers, Credential Management systems, and PKI infrastructure.

For some organizations FIDO2 will support their requirements and may simplify a lot of the complexity that smart cards bring to an organization. However, FIDO2 may not be able to be used in all scenarios that are needed by organizations, especially government organizations that must meet specific compliance standards.

Additionally, smart cards have the advantage of years of growing support and can support many more common use-cases like Windows Remote Desktop, sign-in to MacOS, administrative credential enrollment, or various other scenarios. These organizations will likely want to take advantage of FIDO2 but not yet migrate away from smart card. These organizations may find that they can leverage FIDO2 passwordless for some scenarios but not all and will take advantage of it where possible as an additional convenient and secure certificate based sign-in for systems.

Leverage YubiKey as the physical smart card

Organizations with smart cards should standardize and use YubiKeys as smart cards which are already being used to access other systems using FIDO2, U2F, TOTP, and HOTP. By leveraging the YubiKeys for smart card authentication, then the organization will simplify the environment by removing the need for separate smart cards and readers. The organizations will likely be able to reduce costs by reducing hardware and licensing requirements. The users will also benefit and be able to use the same security key to access all their systems.

Summary

At this stage in the On-Premises + Cloud Organization's journey to passwordless they are gaining some traction in their zero-trust maturity. They are focusing on migrating applications federated with AD FS to Azure AD where possible. They are continuing a shift to the cloud by synchronizing their on-premises identities and moving authentications from AD and AD FS to Azure AD. Legacy applications using Integrated Windows Authentication are now
participating and honoring passwordless sign-in as well. Other on-premises applications leveraging RADIUS will not be able to leverage passwordless sign-in yet until they are upgraded. However the organization is beginning to transition the users, allowing them to leverage the same YubiKeys as OTP tokens to support RADIUS based applications which require MFA. The organization can also simplify their deployment and leverage the YubiKey as a smart card. The organization is on a good path securing applications by enabling MFA while simultaneously positioning the organization to take advantage of passwordless once the capabilities are available.