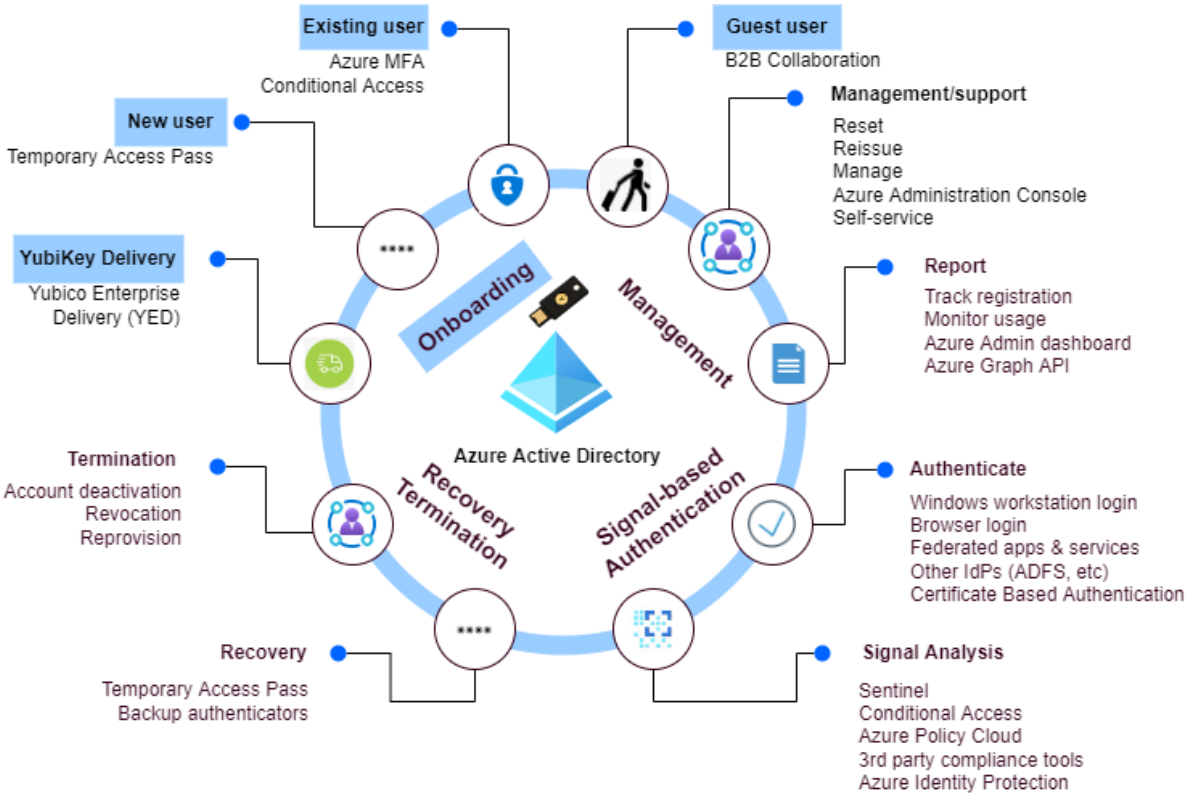
YubiKey Lifecycle Management Best Practices with Microsoft Azure AD Passwordless - Onboarding



YubiKey Delivery

A user's journey starts with receiving a YubiKey, and organizations need to establish a plan for delivering YubiKeys to both their existing and potential new users. For in-office workers, YubiKeys can be picked up via self-service receptacles or distributed during a go-live event. In the case of remote workforces, it will be essential to collect up-to-date end-user addresses for shipping.

Yubico can help support distribution efforts with our turnkey delivery service YubiEnterprise Delivery (YED). The cloud-based service streamlines the distribution of YubiKeys to end users, serving both domestic and international locations including residential addresses. Inventory is stored and ready for request upon entering the desired delivery address.

To further simplify the experience, YubiEnterprise Subscription (YES) provides the flexibility of inventory, additional stock, and access to Yubico technical support all included in an as-a-service model. YES inventory can be managed directly through the YED portal for ease of management and delivery.

Onboarding

Onboarding users to phishing-resistant authentication is the next step in the lifecycle. Organizations typically have to plan for the delivery of YubiKeys to their user groups (based on their locations) and then

establish processes for onboarding both new and existing users and in some cases also for external or "guest" users.

The first type of user onboarding will be for new employees in the organization. Deploying and registering YubiKeys along with other new hire technology will streamline the onboarding process and acclimate users to YubiKeys from the start. The second is existing users who will begin using YubiKeys in their existing authentication workflows. For these users, communicating the value and improved experience will encourage existing user acceptance of YubiKeys. After communicating the change, providing clear and easy-to-follow instructions will reduce any registration friction.

After preparing the environment for YubiKeys' technical use cases, end users will receive and register their YubiKeys for use. Like other technology, it's important to have policies and plans for YubiKey usage from how to store the key, what happens if a key is lost, what department supports questions or concerns, and the eventual offboarding of an employee. Planning for lifecycle management of YubiKeys will prepare an organization for the journey ahead.

New User

With new users, companies have the advantage of having a clean slate where configurations and security policies can be set up correctly from the beginning. Typically, the new user account is created which triggers a number of processes that have the goal of provisioning equipment, setting up access to systems, and defining access rules, including authentication and authorization. This means that for authentication purposes, phishing resistant and MFA devices can be distributed and registered as part of the onboarding process. As a result, new users can begin using those methods for authentication without having to go through any migration processes.

When onboarding a new employee, organizations can leverage several of Microsoft's solutions with the intention of eliminating friction: Autopilot to simplify the provisioning of new hardware, Intune to designate and setup the applications the employee will need, and finally Temporary Access Pass (TAP) to provide an initial login, which will enable the user to subsequently self-register their YubiKey. Using TAP to bootstrap user authentication makes it possible to provide a passwordless experience from the beginning for new users. It is also possible and recommended to register an additional backup YubiKey, especially for high privilege user accounts.

New user onboarding can be automated using different tools, ranging from human resource management applications to identity governance systems that integrate with Azure AD (for example using SCIM). These types of integrations provide a streamlined process that allows organizations to enforce their desired security policies.

The effort required for this step includes: YubiEnterprise Delivery integration, user provisioning automation, onboarding process planning, creation of onboarding guides and user training.

Existing User

For existing users who are migrating to YubiKeys, an Azure AD account is already set up for them. This account is usually synchronized with an Active Directory account, and an MFA method may be already configured (in most cases it's required for Conditional Access). For these users what is required is a combination of system configurations (enabling passwordless authentication in Azure AD, setting up required policies in AD groups and Azure AD Connect for cloud and on-prem environments, etc.) as well

as user training on how to register and use YubiKeys for phishing-resistant authentication. It is also quite common to plan deployment in waves or phases, where groups of users are designated on each phase, provided with YubiKeys and trained/educated in their use. These users proceed to register their YubiKeys for phishing-resistant authentication and start using them during a predefined period of time where feedback is collected and used to improve provisioning and training processes and materials. Similarly this phased approach can be used to identify or refine system configurations and any required updates.

The main challenge for existing users is to migrate them to phishing-resistant authentication and stop using passwords and other MFA methods. Breaking old habits is hard, but with proper communication that emphasizes the advantages (stronger security, ease of use and cost effectiveness) and a frictionless process, it is possible to achieve a successful deployment.

Start with communicating with end users about the coming change by explaining what a YubiKey is and its value, both for security and user benefits. Educating users about the importance of the security initiative can help establish user buy-in.

Once users have been informed of the upcoming authentication change, providing users with clear and easy-to-follow instructions on registering and using the YubiKey will help create a frictionless experience. Be sure to create materials that meet different user groups at their technology acumen to reduce confusion.

The effort required for this step includes: YubiEnterprise Delivery integration, phishing-resistant configuration, deployment phases process planning, creation of guides and user training.

Guest User

Users from outside the organization can be provided with access to resources in the organization using the capabilities in Azure Active Directory B2B to collaborate with external guest users, which include the ability to grant the required permissions that guest users need. Using Conditional Access it is possible to implement a policy that requires phishing-resistant authentication and MFA for guest user access. In a similar way to new user onboarding, it is best to define the corresponding processes for onboarding guest users as well as the communications and user training materials to ensure a seamless deployment.

The effort required for this step includes: YubiEnterprise Delivery integration, phishing-resistant configuration, deployment phases process planning, creation of guides and user training.