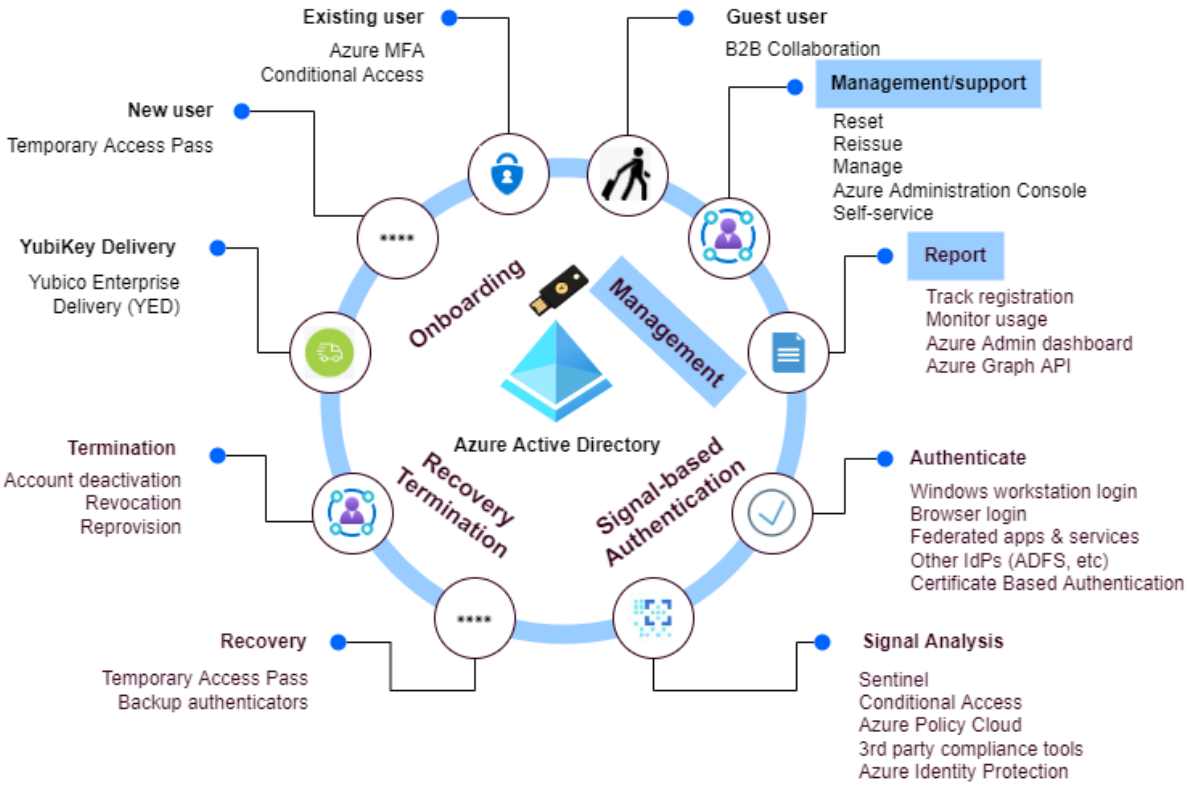
YubiKey Lifecycle Management Best Practices with Microsoft Azure AD Passwordless - Management



The Management component of the deployment process includes providing users with the ability to manage the YubiKeys they are using for authentication purposes. This includes self-service and administrator-based methods for identifying and modifying the YubiKeys that are set against their Azure AD accounts. It also includes providing administrators and managers reporting on the use of YubiKeys to track progress in the deployment process.

Management/support

Empowering end users with the resources to self-support their YubiKey registration and questions will help create a frictionless implementation and reduce the impact on the help desk. Providing a range of support materials such as FAQs, guides, troubleshooting steps, and videos can provide self-directed assistance to a variety of user types. If a user does experience an issue with their YubiKey that they can't resolve, having a trained help desk with support resources of their own can be the second level of support to get the user back up and running as soon as possible.

In a Microsoft Azure AD environment, end users have access to tools that enable them to manage their YubiKeys in a self-service mode. This includes use of the Azure AD user self service portal and the Security Key management tools in Windows 10 and Windows 11. Alternatively, YubiKey management can also be done from the Azure AD administration console by an administrator. Yubico also provides a YubiKey management tool called YubiKey Manager, which is freely available for download and works with several platforms, including Windows, macOS and Linux.

The effort required for this step includes: phishing-resistant authentication configuration, management process planning, deployment of YubiKey Manager where required, creation of guides and user training.

Reporting

Throughout the deployment process, reporting on user registration will help gauge the adoption success and mediate outliers who have not yet registered a YubiKey. These unregistered users can be contacted to take further action until the organization's target adoption rate has been achieved.

Quantitative reporting provides direct evidence of organizations' performance against their deployment goals. Goals can include registration rate, active YubiKey users, reduced help desk tickets, and reduced downtime. Adoption rate is another important goal; it reflects the success of the deployment and the increased security protection across the user base. Cost savings from the reduction of IT support and infrastructure costs should be a valuable benefit of the deployment. These reporting statistics show organizations improve directly from the deployment.

Azure AD provides tools for monitoring YubiKey usage and registration, available from the Azure AD Administration Console. Additional custom reporting can be done using Microsoft Graph API.

The effort required for this step includes: phishing-resistant authentication configuration, Azure AD configuration for access to reports and dashboards, reporting process planning and integration of Microsoft Graph API, if required for custom reports.