Self-Assessment for Technical Readiness

yubico

This document is designed to help you assess your current identity management and security environment so that you can determine where the YubiKey fits, as well as create a vision for where you would like to end up.

1. What Identity Provider are you using?

If you're looking for your provider's instructions on how to integrate with the YubiKey, try visiting our Works With YubiKey catalog! You can search by security protocol, category of service provider, your YubiKey version, or the name of your provider.

2. Do you have multiple Identity Providers that need to be consolidated? Do you have a plan for handling this with the YubiKey?

Since the YubiKey is multiprotocol this will allow you flexibility in working with multiple identity providers. However, it is recommended to consolidate and use one source of truth for identity management.

3. Are you compliant with all requirements for your Identity Provider's solution? (Example: Smartcard requires a PKI and YubiKey minidriver, Azure passwordless requires specific versions of Windows 10, etc)

Be sure to document these requirements and how you will address them.

4. Have you assessed compatibility of YubiKey protocols with those of your Identity Provider? Which protocols will you employ?

If you're not sure of the entire span of protocols available on your purchased YubiKeys, check your device listing here.

5. Based on the above research, will you have to use multiple protocols to handle your environment? Which will be needed? (Example: FIDO2 for Workstation login and web apps combined with smartcard for server access for administrators and OTP for VPN.)

6. If using OTP, some Identity Providers require secrets to be uploaded prior to being assigned to a user. Does your Identity Provider require this? (Examples: Okta, Duo) Will Yubico be providing this programming or will you do this yourself?

Custom programming is available for order quantities of 500 or more. For more information on custom programming, check here. For your specific service, check with their support guides on how to program your YubiKeys.

7. Is your technology estate on-premise, cloud, or hybrid? Do you have federated apps? Are your user accounts held in AD or is your source of truth HR software?

Getting an accurate picture of your connection points and resources is important in setting up your YubiKeys to ensure the best user experience.

8. Have you evaluated all your entry points that need to be secured by YubiKeys? Such as, VPN, cloud apps, contract workers, or other special cases. What are your top 3 use cases?
Click here for a comprehensive list of use cases and their solutions.
9. What legacy applications do you have and what authentication methods do they support?
YubiKeys have options for holding a static password or you may want to look at leveraging the smart card capabilities if your legacy applications don’t work with modern authentication such as FIDO2.
10. Do your users access applications via single sign-on, or do they access the applications from the service provider?
Note this may be useful if a legacy application doesn't support a modern authentication protocol such as FIDO2 but does support SSO.

11. Do you have different MFA requirements for users and privileged accounts? Have you created policies around the requirements for issuing and receiving a privileged account and how that will be provisioned to a YubiKey?
The consideration here is to create policies around the requirements for issuing and receiving a privileged account and how that will be provisioned to a YubiKey.
12. Are you planning on your users doing a self-registration or will an administrator register the YubiKeys?
In the next week you will receive an operational deployment guide that will walk you through this decision and the associated process.
13. Have you identified a pilot group of users and a pilot rollout plan?
Be sure to expand the testing across your use cases and user groups for a more realistic deployment simulation. Identify user groups that may need more assistance and adjust your deployment materials to handle those use cases.
14. Have you identified your different user groups and the access requirements of each group?

Identifying these different user groups is important in planning the distribution of YubiKeys and the registration methods required. You may have users that will be using FIDO2 only, or there may be users that need both TOTP and FIDO2 which may require admin registration before you can give the YubiKey to the user to self register their FIDO2 credentials. This is also beneficial if you are using different form factor YubiKeys, such as nanos, ensuring that users get the YubiKey that fits their needs best.

15. Have you begun planning for the lifecycle of the Yubikey, including registration, loss, recovery, and decommissioning?

If this feels a little overwhelming, don’t worry! Over the next couple of weeks, we will provide resources to guide you through this process.