yubico

Accelerate YubiKey adoption at scale
Deployment best practices to enhance security with phishing-resistant MFA

Security is only as strong as your weakest link

Depending on how diligently your users put authentication workflows into daily practice indicates how secure you really are. While identifying an effective authentication solution is the right first step, putting deployment best practices into place that accelerate and encourage user adoption is critical to enhancing the security posture of an organization.

Best practices to accelerate your YubiKey deployment

To protect against modern cyberthreats, Yubico offers the YubiKey, a hardware security key for phishing-resistant two-factor (2FA), multi-factor (MFA), and passwordless authentication at scale. Organizations worldwide are deploying YubiKeys to ensure secure user access to business networks, data, applications, and to reduce operating costs. YubiKeys help organizations across industries and the government secure their employees, customers, and supply chains against cyberthreats, enabling them to drive regulatory compliance.

Yubico's Professional Services team can provide technical and operational guidance to help streamline your YubiKey implementation and rollout with services mapped to your needs.

Below are some of the key best practices we recommend to help you accelerate your organization's deployment of phishing-resistant MFA.

1. Planning
Project considerations, roles/responsibilities, and timelines

2. Lifecycle Management
Key distribution, user registration, and authentication

3. Training & Support
User training materials, help desk processes, and scripts

4. Launch & Reporting
Go-live planning, key activity, and success metrics

1. Planning: Covering all angles

As a first step, it's best to develop a phased approach to ensure a frictionless deployment of YubiKeys. A holistic plan that clearly identifies all users and use cases for phishing-resistant MFA across your entire organization and supply chain is a must. A successful deployment also involves a variety of roles and responsibilities such as technical implementation tasks, lifecycle management, and operational components such as training, support, launch and reporting. Examples of key process questions include:

- What are your users' needs, behaviors and risk profiles?
- Have you included all appropriate departments in planning meetings for your YubiKey deployment journey?
- Do you have cross-functional alignment?

2. Lifecycle Management: Empowering users with YubiKeys

Yubico makes it very convenient to get phishing-resistant MFA directly into the hands of your employees and supply chain vendors to increase security and improve productivity. Through services such as YubiEnterprise Subscription which provides a service-based and affordable model for purchasing YubiKeys, and YubiEnterprise Delivery which provides a turnkey distribution service, Yubico can help you get YubiKeys to anywhere you need them. Key questions to ask as you prepare to distribute and manage your YubiKeys:

- Where are most of your users located—in-office, remote or hybrid?
- How will users, especially remote users, receive the YubiKey?
- How will you manage lost keys?

Once your users have their YubiKeys, the next step involves registering the keys with the applications and devices they will use. We recommend that each user has a second YubiKey as a backup, and if users cannot locate a YubiKey, revoking and replacing keys is the recommended next step. If a user leaves the organization, some organizations retrieve YubiKeys prior to their departure while others prefer to allow departing users to keep their YubiKeys and continue using it for their own personal accounts.

3. Training & Support: Spreading awareness

The next important step is effective education and awareness, in order to showcase to your user community why the company invested in the YubiKey, and the direct benefits to users. The YubiKey's simple user experience requires minimal training and on-going support for users. However, should users require additional guidance, there are a variety of training approaches, including in-person and virtual webinars, and how-to videos that can be utilized. Key questions to ask:

- How will you train and support users?
- Do you have a communication plan with accessible assets that will help support users?

4. Reporting & Launch: Evaluate for lift-off

After a comprehensive plan is created, it's also important to map out the various metrics that will be beneficial to capture to show success, such as:

- Number of keys distributed
- Number of users activated
- Applications enabled
- Security threats mitigated
- Reduction in password reset-related IT support calls
- Productivity related to user log-in times

Having clear visibility through reports, or even by conducting user surveys can provide extra clarity back to the business. Key questions to ask:

- How will you measure the progress and success of your deployment?
- What specific metrics make sense for your organization?

Best practices for success

Raise the bar for security for all users with access to sensitive data and move beyond passwords, SMS or mobile authentication.

Develop a deployment plan for the organization that is inclusive of key stakeholders beyond IT.

Ensure all users have a primary and a backup YubiKey for highest security and productivity.

If a user cannot locate a YubiKey, revoke and replace keys to enable seamless continuity.

Ensure that communication and training materials are created for both your users and your help desk.

Share lessons learned and best practices with the community to encourage effective security hygiene.

> " The initial rollout has been quite seamless and we have been able to quickly onboard our users. With a strong infrastructure in place and easy access to documentation and support, we are confident that we have taken back security and control.

Martin Joy, Director, Information & Communications Technology, Government of Nunavut

---

Yubico is ready to help

The Yubico Professional Services team is composed of knowledgeable security professionals with experience gained from hundreds of customer implementations across a wide range of industries. From standard implementations to complex enterprise rollouts, Yubico Professional Services has the skills and expertise to help guide you through all technical and operational facets of a YubiKey implementation and deployment. You can embrace the YubiKey with confidence, knowing that you have a solution and the right experts in place to prevent account takeovers and empower your users. Get started today!

Contact the Yubico sales team today to be a cyber security leader with the YubiKey.

The YubiKey Family
The YubiKey is available in multiple form factors for desktop, laptops, mobile devices and tablets.