yubico

YubiKey

Operational Deployment Guide

Revision Date: 2020-05-01

Copyright

Trademarks

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. Yubico shall have no liability for any error or damages of any kind resulting from the use of this document.

The Yubico Software referenced in this document is licensed to you under the terms and conditions accompanying the software or as otherwise agreed between you or the company that you are representing.

Contact Information

Yubico Inc
530 Lytton Ave., Suite 301
Palo Alto, CA 94301
USA
yubi.co/contact

yubico

Contents:

1. Introduction

Yubico changes the game for strong authentication, providing superior security with unmatched ease-of-use. Our core invention, the YubiKey, is a small USB and NFC device supporting multiple authentication and cryptographic protocols. With a simple touch, it protects access to computers, networks, and online services for the world's largest organizations.

This guide is designed to walk you through the key stages when implementing and deploying YubiKeys, along with our recommended tips for each step of the way. Our aim is to make your YubiKey deployment as easy and as frictionless as possible.

This guide contains:

- Yubico-developed resources based on best-in-class technical and deployment expertise, built specifically to help clients of all industries and sizes successfully deploy our products
- Best practices to follow and pitfalls to avoid, based on hundreds of successful customer deployments
- A quick overview of Yubico's Professional and Support services and how to contact us if you are interested in engaging Yubico for further assistance in your deployment.

Audience:

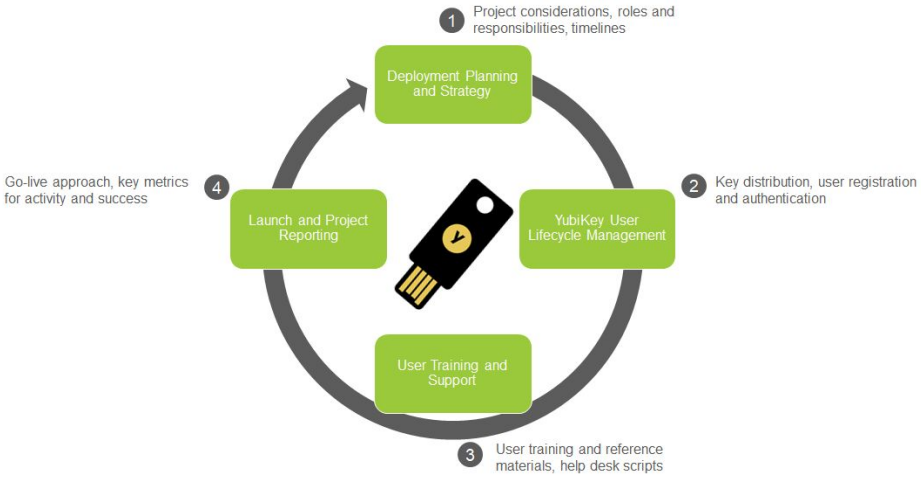
- This document is intended for people who are interested in deploying YubiKeys in their company and are looking for advice and resources on the key decisions for successful deployments. This is traditionally Security Managers, Security Administrators or IT Project Managers. This document is not intended to provide technical implementation steps, but it will link to specific deployment guides or other Yubico resources where appropriate.

Which Yubico Products Does This Guide Apply To?

- YubiKey 5 Series (YubiKey 5 NFC, YubiKey 5Ci, YubiKey 5C, YubiKey 5 Nano, YubiKey 5C Nano)
- Security Key Series (Security Key by Yubico, Security Key NFC by YubiKey)
- YubiKey FIPS Series (YubiKey FIPS, YubiKey C FIPS, YubiKey Nano FIPS, YubiKey C Nano FIPS)
- For information on other Yubico products such as YubiHSM, please visit https://support.yubico.com

2. Steps for a Successful YubiKey Deployment

The steps and elements in this guide are designed to enable customers to deploy YubiKeys to their users. The steps range from initial planning, through the YubiKey lifecycle management process, through training and supporting users, to the final launch and measurement of the deployment.



3. Project Planning

Project Planning is where you will begin designing your overall YubiKey deployment project and individual tasks.

Project Considerations

There are a number of project-based considerations that need to be addressed early in the planning cycle. The following questions should be considered in order to ensure a successful deployment and optimal user experience are delivered:

- **Which services will be affected from this project?**
  The specific use cases defined after reviewing the Technical Deployment Guide will affect the overall project timelines and affected groups.
- **What are the key deliverables dates for your project?**
  In preparing for your project, start with your end date: when is the date that the migration of all of your users must be complete? That end date will affect many of your decisions, such as key fulfillment and deployment, and knowing it in advance will make your project planning easier and more effective.

Roles and Responsibilities

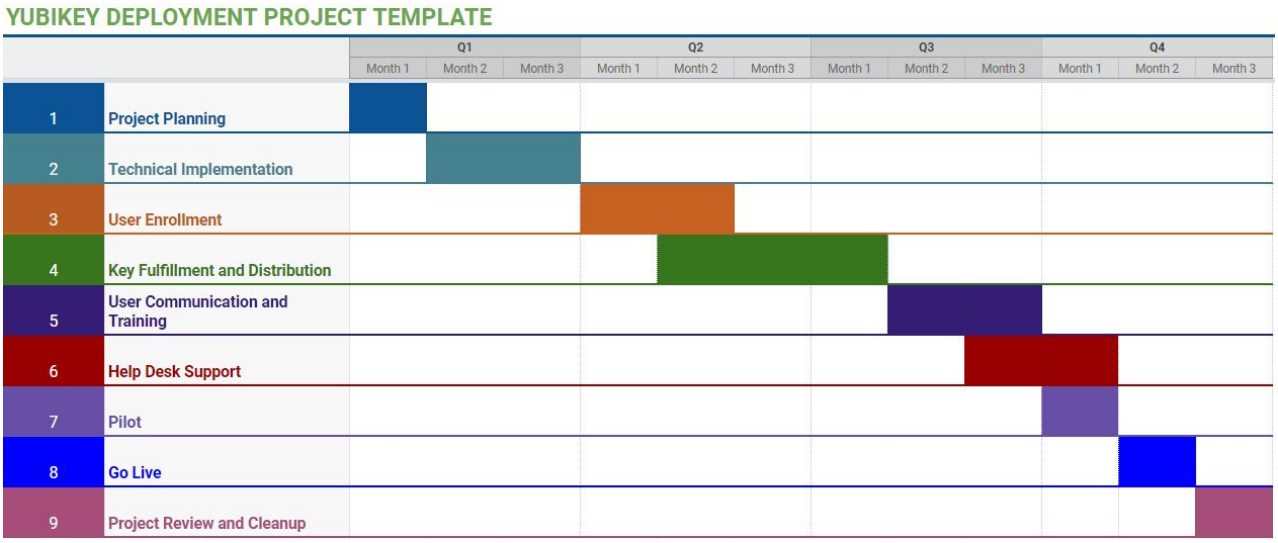
While the number of resources on your project can vary based on the size and breadth of your YubiKey deployment, there are a number of roles that traditionally need to be filled:

Role	Responsibilities
Project Owner	Typically a Vice President and/or Chief Information Security Officer (CISO) who has ultimate decision-making on the project
Project Manager	Traditionally a Security or IT Manager who has day-to-day operational responsibility the project
IAM System Admin	Configures and maintains systems that manage the lifecycle of user accounts and YubiKeys to those accounts.

Identity Management Lead	Leads provisioning team that enables users in systems. This person works with HR to ensure YubiKeys are integrated into the on-boarding process.
Fulfillment Lead	Responsible for YubiKey fulfillment, inventory management during rollout
Application Lead	Responsible for any integrated applications (if necessary, often federated cloud applications)
IT Subject Matter Experts (SMEs)	Often leads or SMEs from desktop, mobile and networking
Security Team	Lead or key personnel from company security
Support /Help Desk Lead	Responsible for first line user support
Training/Communication Lead	Creates user training and outreach materials in support of project

4. Deployment Project Plans and Timelines

We have developed a high-level **sample deployment project plan** (see below) based on previous successful Yubico deployments. This can serve as a blueprint for your YubiKey implementation and rollout. Note that actual timelines will vary widely based on factors such as numbers and types of use cases, users, functions, locations, etc.



The primary components of a YubiKey deployment project are:

- **Project Planning**-- determining the overall project scope and team resources needed
- **Technical Implementation**-- identifying affected applications and legacy systems through installation and testing
- **Key Fulfillment and User Access**-- establish user enrollment processes as well as key fulfillment needs

- **Key Distribution--** creating a key distribution process and plan to distribute keys to end users
- **User Communication and Training**-- includes the overall internal user communications and training plan as well as external/PR communications
- **Help Desk Support**-- creating support materials and scripts for a client's help desk/support group
- **Pilot**-- small group installations to verify processes and gain feedback before larger user deployment
- **Go Live**-- the official production deployment and rollout of YubiKeys to the user population
- **Project Review and Cleanup**-- creating quantifiable reporting to gauge the progress and effectiveness of the rollout

5. Keys to a Successful Deployment

Based on previous successful YubiKey deployments, here are some some key thoughts to remember when planning your project:

- **Communicate, communicate, communicate**: the why/purpose, the overall value (to the organization and end users), and the tasks involved. Be prepared to answer questions from both management and users and provide information throughout the project.
- **Ensure executive buy-in.** Monitoring and enforcement must be supported from the very top of the organization. Any changes made to the user login process will often result in pushback from those users, so executive support is crucial to help offset these concerns and to facilitate the rollout.
- **Make the deployment as 'frictionless' as possible** for all populations. The user experience in particular should be a primary consideration in all aspects of the deployment since it will encourage user adoption.
- **If possible, take a phased approach to secure early successes**. Begin with easy targets with high user impact, and use those early victories to create goodwill in the organization.
- **Create a project SWAT team** to quickly investigate and resolve potential issues. Make sure to factor in additional time during your project plan to manage these issues and make adjustments if necessary.
- **Measure progress and report** at specified intervals.

6. Risk-Based Deployment Strategies

Deployment Security Postures

Before you can decide on how to address each of the various sections of the access lifecycle, you should ensure that you understand the security posture that your company will take. **Depending on the desired security level, multiple deployment plans may need to be put in place.** A company could have multiple security levels depending on the associated risk and criticality of the job different groups or individuals are performing.

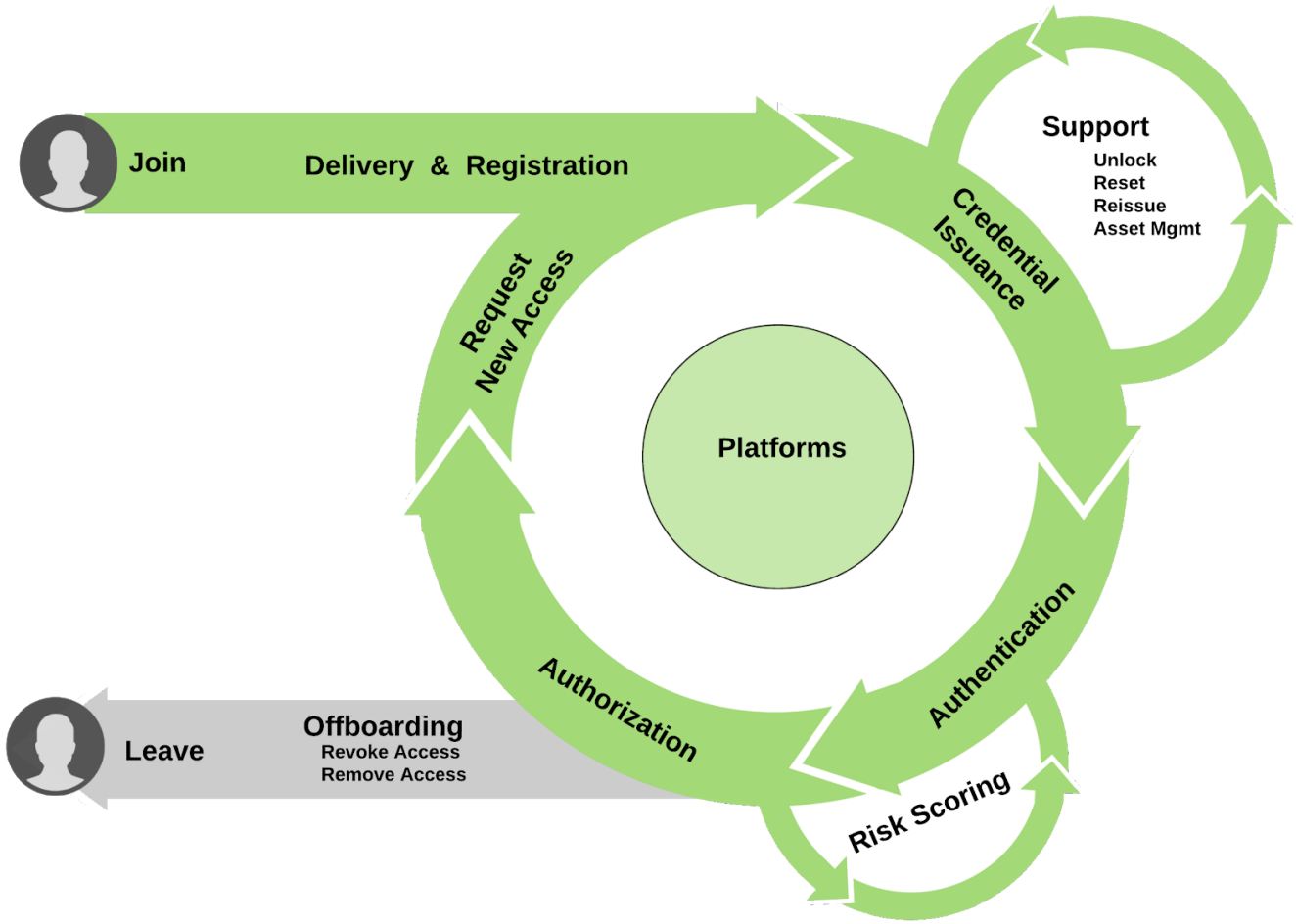
Deciding on the level of security scrutiny that is needed for employees will help direct the appropriate deployment approach. Some environments or jobs require a high level of validation and control to ensure they meet stringent security standards. Many companies don't need the highest level of security to have an effective deployment of YubiKeys. Understanding the User Risk Levels in your organization will optimize your deployment planning.

Level of Risk	Registration	Key Distribution	Support	Off Boarding
Dedicated	In Building Station	Dedicated YubiKey / In Building	In Person	Revoke / Disable Access Return Key
High	Security Station	In Person	Backup Key In Person	Revoke / Disable Access Return Key
Medium	Delegated Admin (Mgr / Office Mgr)	Delegated Admin	Backup Key Service Desk - Limited Alt Access	Revoke / Disable Access
Low	Self Service	Self Service (Vending Machine)	Backup Key Service Desk - Limited Alt Access	Revoke / Disable Access

The above diagram lists different risk levels. Risk levels are based on your company's number and type of risk factors. The risk levels and security requirements described in the diagram and below are examples and should be tailored to your company's needs. These risk levels will be key drivers in the User Enrollment and Key Distribution discussions.

YubiKeys and the User Access Lifecycle

As the project team prepares to deploy YubiKeys, it is important to understand how YubiKeys are involved in each and every aspect of the user access lifecycle. Your use cases should address all the various scenarios where a user would interact with a YubiKey. It is also important to note that YubiKeys work within an authentication ecosystem. YubiKeys work closely with platforms to provide a secure and easy to use authentication experience.



The access lifecycle has many different phases and understanding where the YubiKeys are involved is important. For more detailed information on each of these phases, please review the YubiKey Technical Deployment Guide.

Delivery & Registration

During the phase, YubiKeys are delivered and assigned to the user. Delivery can be a simple process if everyone is in a central location but if the users are geographically dispersed and/or need to be distributed across partners, formalized processes and procedures need to be developed. Yubico's delivery service (YubiEnterprise) which is discussed later can simplify the process.

During the Registration process, the individual's identity is validated and the YubiKey is registered to the individual. In many companies, identity proofing is accomplished when an employee is hired. Work with your HR department to create processes for registering and validating identities of both employees and contractors.

Credential Issuance

Before the YubiKeys can be used by the individual, credentials need to be issued to the YubiKey. The particular solution and protocol being used will determine the credential issuing process that needs to be followed. Please review the YubiKey Technical Implementation Guide for more information on credential issuing.

Support

Support processes are critical to define, implement, and test during the project. For most companies, it is important to ensure that the support teams have appropriate access to the various systems to resolve any access issues in a timely fashion before going live to production.

Authentication

The YubiKey provides strong authentication and will change the workflow for user login, therefore you should review your authentication processes during your technical deployment work.

Authorization

Once a user authenticates with a YubiKey, platforms and access management systems authorize what the user can access. This is an important part of the authentication / access management workflow, but is outside the scope of what the YubiKey is intended for as the YubiKey is meant for the authentication portion of the process only.

Offboarding

When an individual leaves and is no longer working for the company, their access should be automatically revoked and disabled. Given that the YubiKey cannot authenticate if the credentials are disabled, no real change to the process is needed to ensure access is removed.

7. User Registration

When planning for user enrollment, you need to consider to decide what approach is best for your needs:

User-driven Registration

Creating a central portal for users to self-enroll is a valid option for users with low risk levels as well as scenarios where your use cases are generally limited. In addition, this may be a better option if you have a large number of users and a large number of YubiKeys as this will help minimize the resource impact on your support organization.

Admin-driven Registration

Centralized enrollment is generally a better approach for users with medium, high, and dedicated risk levels. Admin-driven enrollment is generally a great fit for deployments with diverse use cases and/or ones that are technically more complex and require greater control. Since this will place a burden on your IT or support organization, admin-driven enrollment is commonly used in scenarios with fewer users.

8. Key Distribution and Management

Here are some key decision points to consider when preparing to fulfill and distribute YubiKeys to your end users:

Distribution Planning

In preparing your schedule, you will want to consider some key factors:

- How many end users will be receiving the keys?

- How quickly can you enroll them?
- What are their roles?
- Where are they located?
- Do you have telecommuters who don't visit an office?
- How many keys can you effectively deploy each week given your staffing levels?

Approaches to Distributing Keys

Similar to User Enrollment, your approach to distributing keys will be dependent on your user risk levels:

Risk Level: Low

At the lowest level, **we recommend that self-service be utilized to ensure employees can quickly return to work**. With self-service, workers will be able to obtain a YubiKey via methods ranging from a company vending machine or unsupervised basket of keys to an administrative assistant or support staff. Even though this risk level is low, it does not imply that the authentication mechanisms will be low. At this level, authentication is strong with a YubiKey but the identity proofing process is not stringent. Many large corporations work at this level for employees who have standard access.

At this level, **the service desk should have the ability to change the authentication mechanism from a YubiKey to another option**. This could include a mobile app MFA solution, or reversion back to username and password. The alternative access option would only be available for a limited amount of time until the user receives their new YubiKey as this option would degrade the authentication assurance level. Any action to change the authentication mechanism should then send a notification to the user and their manager.

One of the main challenges at this level is how the service desk will validate the caller. Some companies have moved away from standard phone calls to video conferencing techniques which are readily available on desktops and mobile devices. The service desk can then visually inspect the caller (Photo IDs, drivers licenses, etc.) and compare to company records if necessary.

Risk Level: Medium

At the medium level, **we recommend that a person of authority is involved in the registration and key provisioning process**. This could be the individual's manager or an office manager. The user will be required to have a backup key in case they lose their primary key.

The service desk processes will be similar to the lower risk level but could require a manager approval step to change the authentication mechanism from the YubiKey. The alternative access option would be only available for a limited amount of time until the user receives their new YubiKey. At this level, the user would need to get a new YubiKey from their dedicated source such as their manager. Any action to change the authentication mechanism will prompt a notification to the user and their manager.

Risk Level: High

At the high level, we recommend that a security station be used to register the user and distribute YubiKeys. The security station will allow for in-person identity proofing processes. A high level risk YubiKey could be used for specific IT production data access. We highly recommend that YubiKeys be physically labeled to clearly identify that it is used for accessing production systems. The user should be required to have a backup key in case they lose their primary key. For support, the user will need to go to a security station to resolve any issues. This will reduce the chance of the service desk being fooled into sending out a YubiKey to the wrong party.

Risk Level: Dedicated

The dedicated level is a special case that would be **reserved for departments that deal with sensitive production data**. A call center or an HR department could fall into this category. Often, the YubiKey will be checked in and out upon entering and exiting the physical location where the job function is performed. In these cases, **we recommend that dedicated YubiKeys are issued which are only used for these particular job functions**. We highly recommend that YubiKeys be physically labeled for this purpose in order to delineate access privileges. We also recommend that a security station within the department register the user and distribute YubiKeys. The security station should allow for in-person identity-proofing processes. The user would not have a backup key as they will only be able to access systems from the dedicated location. For support, the user will need to go to the security station to resolve any issues. This will reduce the chance that the services can be fooled into sending out a YubiKey to the wrong party.

Deployment Enforcement and Escalation

As part of your deployment plan, you will want to have enforcement and escalation policies established such as:

- Who are the defined resources in charge of site deployment?
- Who is the primary point of contact in each site/group to handle issues?
- How will enforcement be handled?

Backup Keys

We recommend that all users be required to have a backup key in case they lose their primary key. Having a backup key will reduce calls to your service desk and not degrade the authentication assurance level. If a backup key is not an option, your service desk could issue temporary or new YubiKeys if necessary. This would require additional processes, controls and potentially tooling to ensure the assurance level is not degraded.

Revoking/Retrieving YubiKeys

As part of the deployment process, you will need to create a process for handling revoking and retrieval of YubiKeys. When an individual leaves and is no longer working for the company, their access should be automatically revoked and disabled. Given that the YubiKey cannot authenticate if the credentials are disabled, no real change to the process is needed to ensure access is removed. Any tracking system should be updated to state that the YubiKey is no longer in use.

Risk Level: Low

When offboarding a worker, the user's credentials will be revoked but the YubiKey will not be required to be returned. When the user's credentials are disabled, the YubiKey cannot be used for authentication.

Risk Level: Medium

When offboarding, the user's credentials will be revoked but the YubiKey will not be required to be returned. When the user's credentials are disabled, the YubiKey cannot be used for authentication.

Risk Level: High

On offboarding, the user's credentials will be revoked, and the YubiKey will be returned.

Risk Level: Dedicated

On offboarding, the user's credentials will be revoked and their YubiKey must be returned.

Handling Lost YubiKeys

A procedure for handling lost devices should already be part of your IT help desk playbook, and it should be extended to include the new YubiKeys. In addition, when YubiKeys are reported lost, we recommend that you:

- Expire any current sessions and request the user re-authenticate
- Disassociate the YubiKey from the user's account and access rights
- Ensure there is an alternate method (backup YubiKey or other) so the user is not inconvenienced
- It's also important to audit the user account's activity prior to the point in time when the device was lost to note any unusual activity. If there is anything suspicious, consider the possibility of a breach and escalate accordingly.
- Determine a process to provide replacement YubiKeys to users
- How will you dispose of previously lost YubiKeys which are found?

Issuing YubiKeys to New Employees

- **Work with your Human Resources group to integrate providing YubiKeys into your new employee implementation process**
    - As covered in the Registration paragraph in Section 5

9. User Communication and Training

Notifying and training end users are crucial elements of a successful deployment. Here are some important best practices to consider:

User Communication

Preparing your users for the upcoming migration is key to the success of your project. There are a variety of methods you can take to notify your users, including emails, standalone marketing materials, videos and usage of your company's intranet page. Here are some keys to successful communications:

- **Notify your users early and often**. Users will be far more likely to support the change and begin using their YubiKeys if they receive notification about the project ahead of time (and usually with multiple touch points).
- Make sure you **provide a rationale for the change and explain the benefits**. People are more likely to adopt the changes and begin using their new YubiKeys if they understand how they benefit from the changes.
- **Make your instructional materials very clear** and make any call to actions very specific. Don't assume that your users will know what to do-- tell them directly what is needed from them.
- Try to **make your communications engaging and fun** if possible. Keep the tone simple and avoid IT jargon as much as possible.
- Anticipate that some users will be on high alert for **phishing** (i.e. they might think Yubico emails are a phishing attempt). If your company uses email filters, make sure to whitelist any appropriate email address
- Determine if any **additional languages** are needed for your user communications

User Training

Written communications by themselves may not be enough to prepare your users and communicate the rollout to them. An additional possibility is to conduct user training sessions which can consist of:

- **Classroom-like sessions**, either in-person or webinar. These sessions should generally should cover at least these three topics:
  - How to setup and activate your key
  - What to do if you lose your key or if it fails
  - Contact details for your help desk/support staff

  Another possibility in these classroom sessions is to have your users attend with their YubiKeys and to activate them during the session. This will lengthen the training session, but it's the best option to get as many users activated and operational at the same time.
- **One-on-one sessions**-- for high-risk employees or executives, one-on-one training sessions are a great approach to ensure they are operational with as little friction as possible
- **Client support office hours** (defined time periods where users can drop in for training)
- **Town Halls**-- one option here is to piggyback with other training group's training sessions
- **Videos** (how-to tutorials)
- Create a temporary "**Genius bar**" for large sites featuring hands-on training and assistance

10. Help Desk Support

Your Help Desk employees or IT support staff will generally be the first line of support for your users, and preparing them with appropriate training is a key success factor in your deployment. Here are some best practices from successful deployments:

- **Determine a support plan.** What will help desk support look like for your sites? Do you want one global group or multiple groups?
- **Create a training plan** for your support groups and help desk personnel. Training them upfront is essential (how to use and how to troubleshoot).
- **Build out help desk scripts** to assist support personnel in triaging and escalations.
- **Other Notes**
  - If your support staff is unfamiliar with **two-factor authentication,** provide them background materials to help them understand the larger concepts.
- **Overview of Yubico Support**
  - For more information, and to get assistance with your YubiKeys, see:
    - Yubico Support home page
    - YubiKey Documentation and FAQs
    - Open a Yubico Support ticket

11. Conducting a User Pilot

As a general rule, rolling out YubiKeys in a phased approach allows for lessons to be learned, and in many cases a faster and more successful project. In a phased approach, it is strategic to show quick wins with a key population to further encourage positive sentiment and build advocacy.

Big Bang approaches however are sometimes necessary. This can be due to regulatory requirements, sensitivity to a recent breach, or even something as simple as the cultural approach of a company. Big Bang projects require

an increased amount of up-front planning and executive sponsorship. Project scopes can be reduced but if they impact all users, training and user experience become critical from the beginning.

Other considerations in deciding on a User Pilot v. Big Bang Approach

- Will users be migrated one at a time or in groups?
- How many groups will be migrated? Do different groups need to be migrated separately? Do they have different needs?
- How many geographic locations will be migrated?
- What are the various functions that are being migrated? Do they have different requirements?
- Where will your support groups be? Will they be all virtual (via a help desk) or at locations or both?

In order to ensure a successful YubiKey deployment, we recommend conducting a predefined user pilot. Attached are some of our key recommendations:

- **Initially test with a pilot group of IT or technical users** to ensure that the end-to-end technology fully works, and that the login experience matches user expectations. This pilot should generally last from 15-30 days.
- After the initial pilot of the IT and/or technical users, **deploy to a small subset of non-technical business users** to determine user education gaps and what to expect when deploying at scale.
- Overall, the size and structure of this pilot group is dependent on your organization size, but a good rule of thumb is to make the combined pilots are **no more than 10% of your total user population**.
- User pilots should include **full functionality**.
- By definition, pilots involve limited risk, but you need to **maintain the ability to roll back** to the previous authentication method.
- Make sure you stay actively engaged with the pilot groups and make sure you **meet with them on a regular basis** throughout in order to gain feedback. Ensure that all pilot feedback is documented and reviewed with the larger project group.

12. Go Live

Once you have executed a successful pilot, you are now ready for the official go-live date and start of the production deployment. Here are some key steps to consider in planning your final Go-Live process.

- Confirm **Help Desk readiness** and the Help Desk team's **escalation plan**
- **Notify your organization** (end-users, help desk, and IT admins) via email that Yubico is going live
- **Internally market** the deployment kickoff
    - Post YubiKey announcements on your **intranet or employee community webpage**
    - Display rollout posters at all company locations. Common & lunch areas often work best.

13. Deployment Reporting

Rollout reporting is often overlooked, but it's a crucial part of any deployment project since it allows you to track and understand the rate and effectiveness of the deployment as well as the usage of your new YubiKeys. Some important considerations for effective reporting and monitoring are:

- **Define mutually agreed upon metrics**:
    - Number of applications enabled

  - Number of YubiKeys distributed
  - % of YubiKeys distributed
  - Number of users activated
  - % of active users
  - Number of authentication failures
  - % of authentication failures
  - Help desk call reduction volume (ideal but not always easy to measure)
- Create and produce **executive dashboards and reports** to publicize the project progress

YubiKey Deployment Project Sample Report

	Current Week	Project to Date	Total Projected
Number of applications enabled	0	5	5
Number of YubiKeys distributed	500	1500	2000
% of YubiKeys distributed	25%	75%	100%
Number of users activated	250	750	1000
% of active users*	19%	58%	100%
Number of authentication failures	37	181	NA
% of authentication failures	1.09%	1.71%	NA

* Active users = users using YubiKeys >2x in past 7 days

- If possible, **create an audit trail** to give you visibility into the impact of the YubiKeys. Did they give up? Problems like this could indicate a misconfiguration, a gap in user education, or simply a scenario that wasn't considered in the initial rollout plan.
- **Collect user feedback** through surveys. We also recommend collecting customer feedback through post-deployment surveys. These surveys should focus on:
  - Activation/registration process
  - Ease of use of YubiKey
  - Perceived security of YubiKey
  - Training gaps
  - Issues with YubiKeys
  - Areas for improvement

  We also recommend integrating key metrics listed above to confirm them or gain additional information on them.

14. Ongoing Support Considerations

YubiKey Refresh

Periodically, Yubico comes out with new versions of the YubiKey that may include new features (e.g. security protocols, form factor, etc.). The deployment plan should keep this in mind. **As a general rule, the introduction of a new YubiKey should follow a similar process of when an employee receives a new YubiKey after a**

key has been lost. The new YubiKey will most likely be backwards compatible so existing functionality should not be broken. As a result, new YubiKeys can be rolled out before new functionality is given to the end-users which will help in rolling out new functionality. It will be important to implement an asset management system to more easily know what version of YubiKey that the employee has.

Asset Management

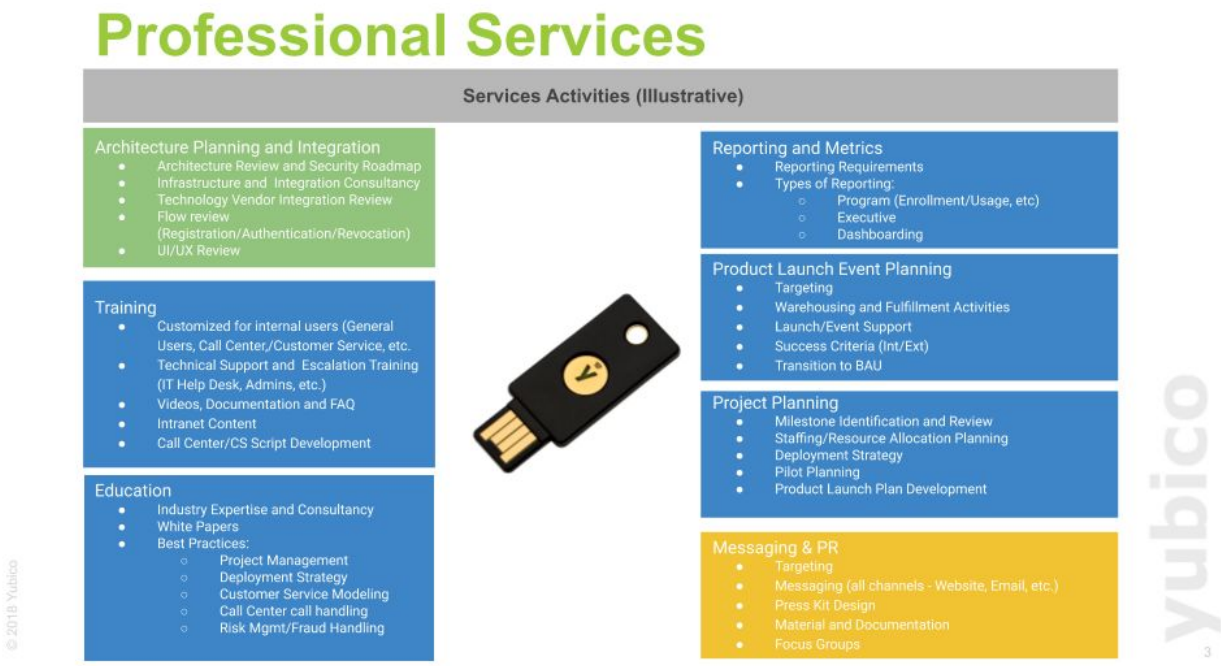
The deployment plan should also include how the company wants to track the YubiKeys as an asset. Some companies do not see the need to individually track the YubiKeys. It can be useful to track YubiKeys to understand how many YubiKeys are associated with an individual or department, what models of YubiKeys are in circulation, and how the YubiKeys are being used. Each YubiKey has a unique serial number which can be read by using the free Yubico tools. The YubiKey model and supported protocols can be programmatically read as well from the YubiKeys. Further, the YubiKey can be configured to allow the serial number to be read when it is inserted. The YubiKey information could then be read into a company's asset management system for analysis.

15. Additional Yubico Services

Professional Services

Yubico's Professional Services group is available to offer you additional assistance in your project including:

- **Services Workshops** which are education- and assessment-focused. These can be held on-site and feature thorough architecture reviews as well as other topics of your choice. These can also include customized guides for integration/implementation/deployment
- **Services Projects** focusing on Technical and/or Business/Operational areas based on agreed upon customer needs and requirements.



Support Services

Yubico Support Services offer:

- 24x7 global priority support desk for problem resolution
- Technical deployment services
- Technical integration services with third party systems
- Support for YubiCloud hosted service

Support Services Tiers

	Bronze	Silver	Gold	Platinum
24x7 Support Desk	YubiKey, Security Key, YubiHSM, YubiHSM KSP, YubiKey Smart Card Minidriver, Yubico PIV Tool, YubiKey Manager, Yubico Authenticator			
Integration Type	None	Basic	Intermediate	Advanced
Technical Integration Services Hours	None	**35 total:** 30 virtual 5 remote live	**55 total:** 45 virtual 10 remote live	**70 total:** 55 virtual 15 remote live
Hours Add-on	X	✓	✓	✓
YubiCloud Add-on	✓	✓	✓	✓

Yubico offers support services in four tiers, enabling customers to find the right offering for their unique needs. All tiers include 24x7 problem reporting for named Yubico products. Higher tiers offer increasing levels of technical integration services by providing additional allocation of services hours.

Technical integration services provide advisory and consultative assistance to customers to integrate Yubico solutions with third party platforms and solutions. Services are provided via a combination of virtual messaging and live remote sessions.

Support for YubiCloud can be added to any tier. In addition, customers may also purchase additional bundles of tech- nical integration services hours.

YubiEnterprise

YubiEnterprise is Yubico's first service-based offering which is designed to transform the way that organizations purchase, deploy and manage YubiKeys. With various subscription, delivery, and management self-service options, YubiEnterprise equips organizations with a simple and efficient way to deploy strong authentication at scale.

The first two YubiEnterprise service offerings available to Yubico customers are YubiEnterprise Subscription and YubiEnterprise Delivery.

- **YubiEnterprise Subscription** is an annual per-user pricing model that allows customers to purchase YubiKeys based on how many users they have to support versus how many keys they need. This supports predictable spending, with access to the latest product versions and lowers the cost to entry for

the industry-leading authentication solution. YubiEnterprise Subscription is available today for businesses with 750 users or more.

- **YubiEnterprise Delivery** is a cloud-based service that allows customers to streamline the YubiKey deployment process with the ability to self-select and oversee inventory management, shipping locations and timeframes, delivery status, and returns or replacement processing. All of these features are accessible through an administrator console hosted by Yubico, or can be integrated directly into existing IT software using public APIs. YubiEnterprise Delivery is expected to be available in Q2 2020.