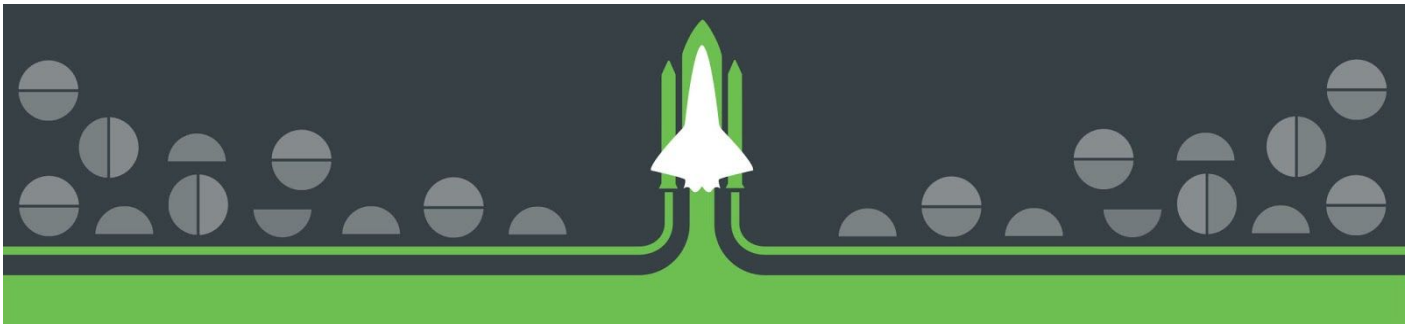


Liftoff: Guide to Duo Deployment Best Practices

Duo is committed to providing you with the best experience possible. From using our product to interacting with our team, we want to be sure you have what you need. By deploying Duo, you will take a big step toward **safeguarding yourself and your organization from data theft and account takeover**.

This guide will walk you through the **key deployment stages** when rolling out Duo, along with our **best practices** and **key resources** for each step of the way. Our aim is to make your Duo deployment as **easy and as successful** as possible.

This guide is the collection of a few things:

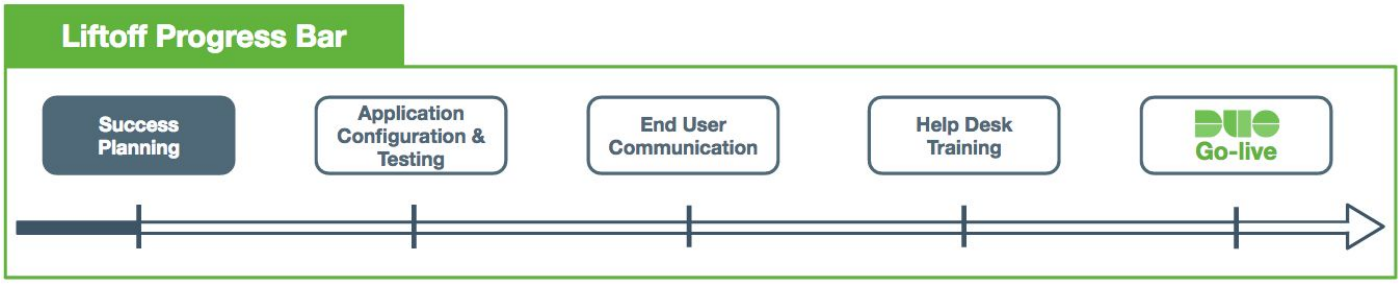
- **Duo-developed resources** based on best-in-class technical expertise, built specifically to help people just like you.
- **Best practices to follow and pitfalls to avoid,** based on thousands of successful customer deployments.
- **Templates and collateral** you can use as to educate your end-users.
- A quick **overview for how to reach us** for further assistance.

Who is this guide designed for?

- **Anyone responsible for deploying Duo**, typically Security Managers, IT Project Managers, or Security Administrators.
- **Note:** This guide is available to highlight deployment best practices. It is not intended as end-to-end documentation for setting up Duo.

Table of Contents

Success Planning: Charting Your Course

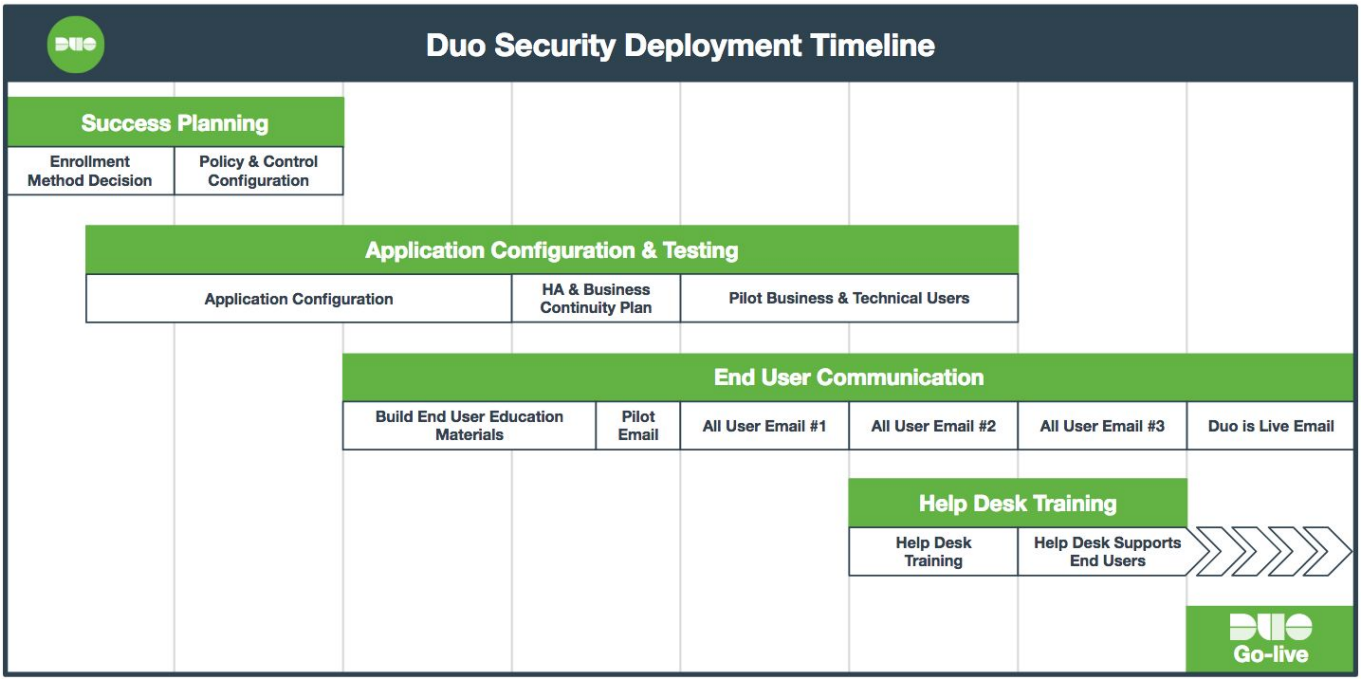


Overview of Success Planning

Success Planning is where you will begin designing your Duo deployment, deciding which **deployment method** best suits your needs, and learning about the **features and policies** of your specific Duo Edition. We have also included **Duo Admin Account settings best practices** to ensure you are taking advantage of the full capabilities of your Duo subscription.

Build Plan For Your Duo Deployment

- **Key Resources**
  - Getting Started with Duo
- **Best Practices**
  - We have developed a **deployment timeline** (see below) based on successful Duo deployments. This can serve as a blueprint for your Duo rollout.
  - Each key **Duo Deployment Stage** is highlighted in green, accompanied by **key tasks** to be completed during the stage.



Configure Duo Admin Account Settings

- **Key Resources**
  - Admin Panel Settings Overview
  - Duo Administrative Roles
  - Telephony Credits: Low Credit Alert
  - How-to: Custom Duo Prompt Help Messaging
  - Lockout & Fraud Reporting
- **Best Practices**
  - Specify a Lockout and Fraud Reporting e-mail address. We recommend a **distribution list** so that multiple people have visibility to those alerts.
  - **Customize the help message** shown to your users in the Duo browser prompt with the Help Desk Message Setting.
  - If your organization consumes a large volume of telephony credits, setup the Low Telephony Credit Alert option.
  - **Only Owners** can create and modify other users, because of this, **we recommend having at least 2 admin users with the Owner role** within the account.

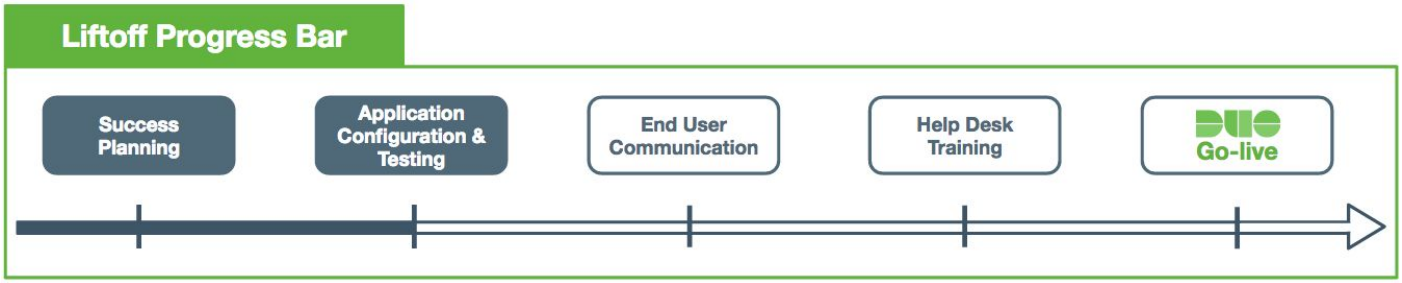
Determine Duo Enrollment Methods

- **Key Resources**
  - User Enrollment Options
- **Best Practices**
  - Duo recommends using Active Directory Sync to reduce the administrative burden for provisioning and deprovisioning users.
  - **Customize the email sent to your synchronized users** by enabling the Send enrollment email to synced users **option**. You can choose to include your company logo in the Enrollment Email.

Customize User Access with Duo Policies

- **Key Resources**
  - Duo Docs: Policy & Control
  - Duo Policy Guide: Configuring Access via Duo's Policy Engine
- **Best Practices**
  - Keep in mind that enrollment, group, and user statuses can impact policy implementations.
  - Some policy implementation scenarios will **require both an Application and a Group Policy** to achieve the desired outcomes.

Application Configuration & Testing: Making Duo Work for You



Overview of Application Configuration & Testing

Executing the plan begins with **configuring applications** and continues with **testing**. You can protect as many applications as you need, and administer each independently. **Testing and piloting your applications** before launch is also key for a successful deployment.

Configure Applications

- **Key Resources**
  - How-to: Protecting Applications
  - Application Configuration Documentation
  - How-to Videos: Application Integrations
  - Authentication Proxy Reference Guide
  - Authentication Proxy Best Practice Guide
- **Best Practices**
  - Duo can be installed and configured to protect many of our supported applications in a **variety of ways**. This allows you to build your Duo applications to give you the desired end-user and administrative experiences.
    - You can find more details in our Application Documentation and Knowledge Base.
  - Give your applications **meaningful names** in the Duo Admin Panel.
    - The application name is **displayed prominently in Duo Push requests** to end users. This helps users identify which application is initiating the 2FA request.
    - Descriptive application names make it easier to find applications in the Duo Admin Panel and filter the **authentication log** results.
  - Treat your **application SKEY** like you would a **privileged password**. Do not ever send the SKEY as a screenshot or plaintext over email, even to Duo support technicians! If you do need to transmit your SKEY, we recommend a SHA-256 hash.

Test Your Duo Applications

- **Best Practices**
  - Test your Duo Applications in a **non-production environment**. This allows you to identify potential issues before your end-users encounter them.
    - There is no limit to the number of Duo Applications you can set up. We recommend building a Duo integration in a **lab environment or virtual machine before deploying to end-users**.
  - **Label your applications** in the Duo Admin Panel accordingly to reflect their usage in your test or production environments.

- Example: *Eng-SSH-TEST* and *Eng-SSH-PROD* are two separate Duo Unix Applications configured the same for testing and production, respectively.

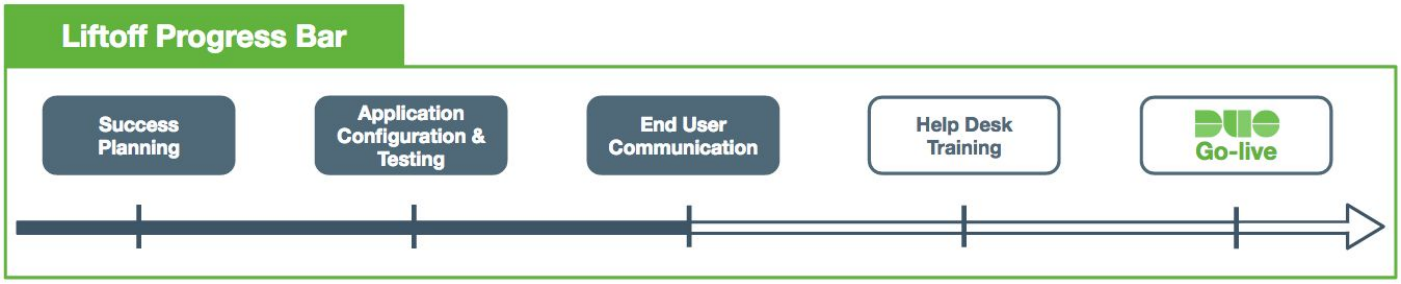
Conduct an End-User Pilot

- **Key Resources**
  - Deploying a Proof of Concept
- **Best Practices**
  - We recommend piloting Duo in two phases to ensure a successful and smooth deployment.
    - **PHASE 1:** Test with a pilot group of IT or technical users to ensure that the technology works and the login experience matches what you're looking for.
    - **PHASE 2:** Once you have worked out the login experience with your IT group, deploy to a small subset of non-technical business users to determine user education gaps and what to expect when deploying at scale.

High Availability & Disaster Recovery Configurations

- **Key Resources**
  - Duo Guide to Business Continuity Preparedness
  - Setting up the Duo Authentication Proxy for High Availability and Disaster Recovery
- **Best Practices**
  - Understand the Duo failmode options and which integrations can support them.
    - Primarily, authentication workflows that involve the **Duo Authentication Proxy** as well as most installer-based integrations like Winlogon/RDP, UNIX PAM, etc.
  - Have an **emergency plan for how to remove Duo** from the authentication workflow in the event of a long-duration local network outage or Duo outage.
    - This should be done on a **per-application basis**.

End-user Communication: What Everyone Needs to Know



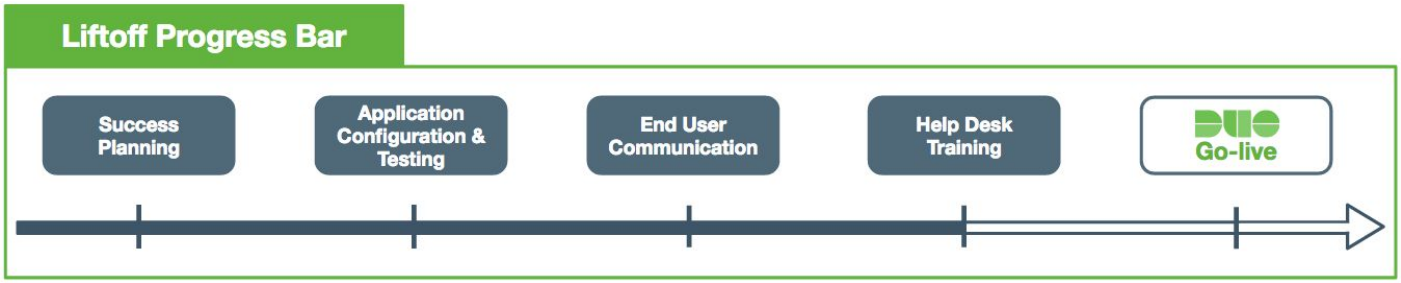
Overview of End-user Communication

Chances are you have a lot of **end users** that need to know what Duo is, how Duo will impact them, and how to get enrolled. Below you will find **user-friendly templates and resources.** Strong end-user communication plans encourage adoption and greatly reduce the deployment burden on your help desk.

Build End User Communication Materials

- **Key Resources**
  - Duo User Guide
  - Promoting Duo Push Guide
  - Video: Welcome to Duo (for End Users)
  - Video: Getting Started with Duo - Enrolling in Duo Mobile & using Duo Push
  - Video: Two-Factor Authentication with Duo Push
  - Duo Demo Website
- **Templates**
  - Email Communication Templates
  - Customizable Duo Deployment Signage Templates
- **Best Practices**
  - Encourage users to use Duo Push. It is the safest and cheapest way to authenticate. Duo Push works on either WiFi or cellular service with data, and can be used in any country.
  - **Enrollment links and activation links have different expiration dates**. Enrollment links expire after 30 days (resending does not restart the clock), while activation links are set to expire by default after 24 hours.
  - Anticipate that some users will be on high alert for **phishing** (i.e. they might think Duo emails are a phishing attempt).
  - If your company uses **email filters**, whitelist no-reply@duosecurity.com.

Help Desk Training: Readying Your Team



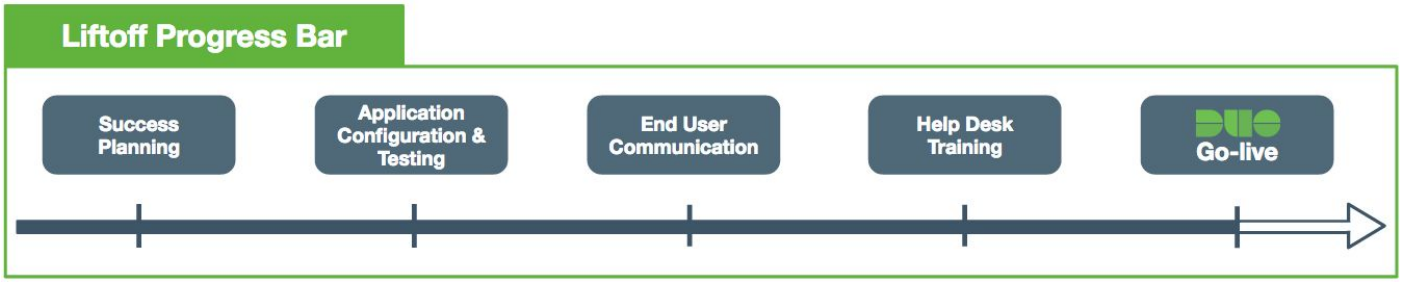
Overview of Help Desk Training

Help Desk employees are your first line of support. To help them be successful, we have created a **handy guide** (linked below) just for them. You will also find tips on **how to educate your Help Desk** team about Duo and importance of securing Trusted Access for your organization.

Enable Your Help Desk Team

- **Key Resources**
  - Help Desk Guide
  - Duo Knowledge Base
  - Duo System Status Page
  - Duo Admin Panel
- **Best Practices**
  - Assume that the Help Desk staff is **brand new to Duo and two-factor authentication**.
    - Show the "What is Two-Factor Authentication" video if you have the ability to do so to provide a high-level overview of 2FA.
    - **Demonstrate Duo Push** by either presenting your smartphone or using the Push Notification Demo.
  - Remind Duo administrators that their admin account is not a user account, and they will require both to access the Admin Panel and protected applications.
  - Be sure your Help Desk team is aware that **if a Critical Severity issue occurs**, contact Duo Support **via phone rather than email** to ensure immediate action.
    - Critical Severity are issues that halt your business operations and have no procedural workaround exists.

Duo Go-live: Ensuring a Seamless Deployment



Overview of Duo Go-live

Congratulations! You have successfully completed the steps to help ensure a smooth and seamless deployment. Below is a **checklist for the final days** leading up to your Duo go-live to ensure a successful launch day.

Duo Go-live Checklist:

- **Internally market** the deployment of Duo:
  - Post Duo announcements on **intranet or employee community webpage**.
  - Include Duo in **company events** or **presentations**.
  - Display Duo posters at all company locations - common & lunch areas work best.
- Confirm **Help Desk readiness** and the Help Desk team's **Duo escalation plan**.
- **Notify your organization** (end-users, help desk, and IT admins) via email that Duo is going live with effective dates.