CISCO DUO

CISCO SECURE

Liftoff: Guide to Duo Deployment Best Practices

Version 3.3 Updated May 2024

Table of Contents

Introduction

Duo is committed to providing you with the best experience possible. We want to be sure you have what you need, whether that be guidance on how to use our product, or where to go for help. 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 a 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 to educate your end-users.
- A quick **overview of how to reach us** for further assistance.

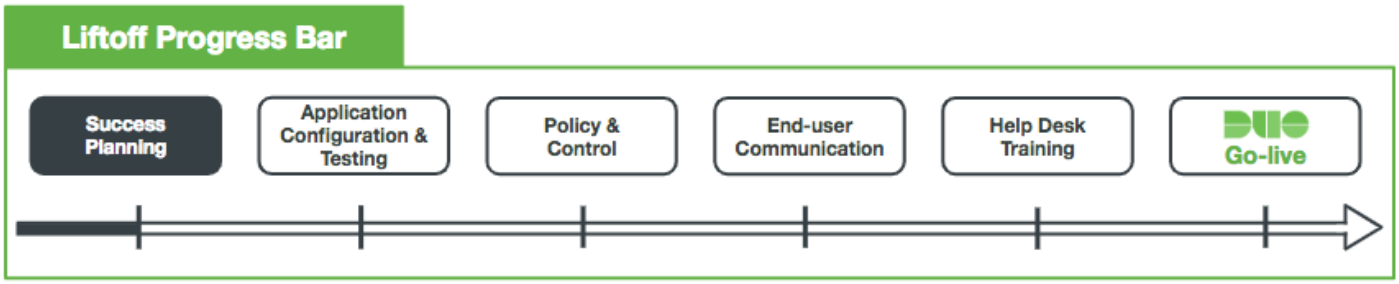
Who is this guide designed for?

- **Anyone responsible for deploying Duo**. This is 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.

Which Duo Edition does this guide apply to?

- The material in this guide **applies to Duo Essentials, Duo Advantage,** and, where relevant, **Duo Premier edition.**
- For more specific information about Duo editions and pricing, see Continuous Identity Security by Cisco Duo.

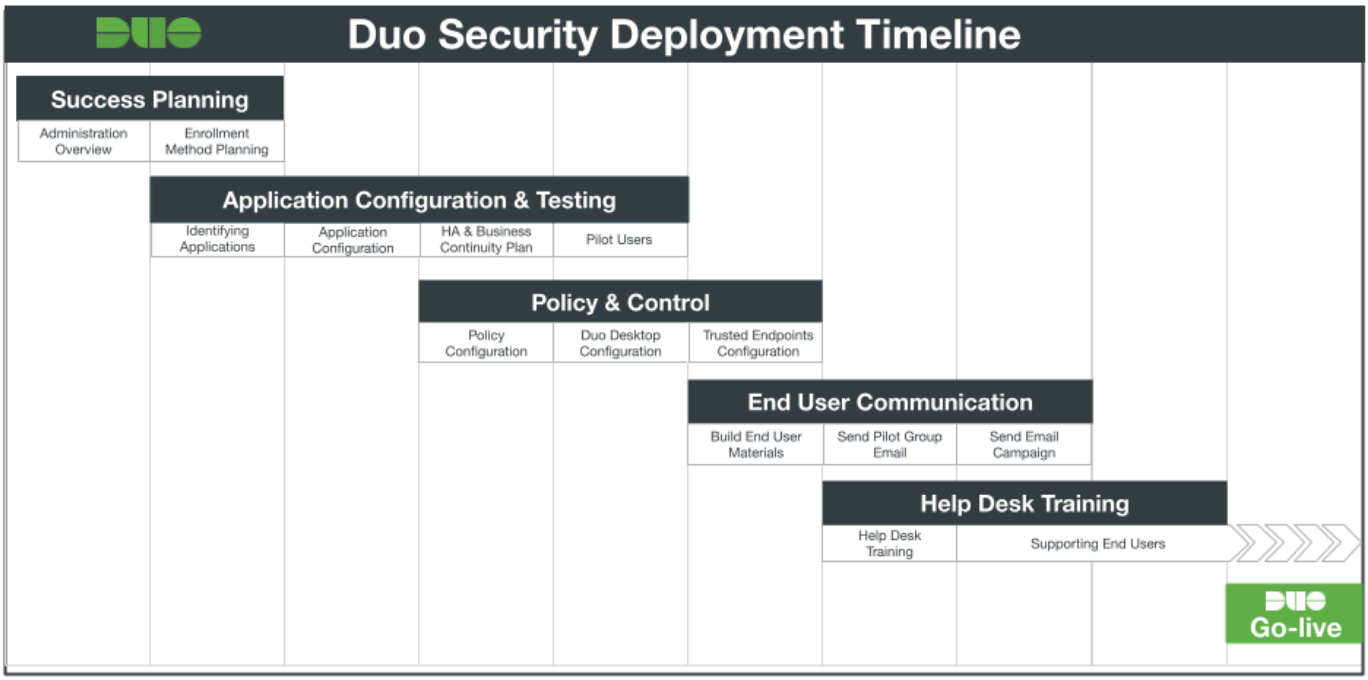
Success Planning: Charting Your Course



Overview of Success Planning

Begin with Success Planning to strategically design your Duo deployment. Reference our Getting Started with Duo documentation followed by the Duo Admin Panel Overview documentation to learn how your Duo subscription will be managed, along with advice for which enrollment method(s) may best suit your needs.

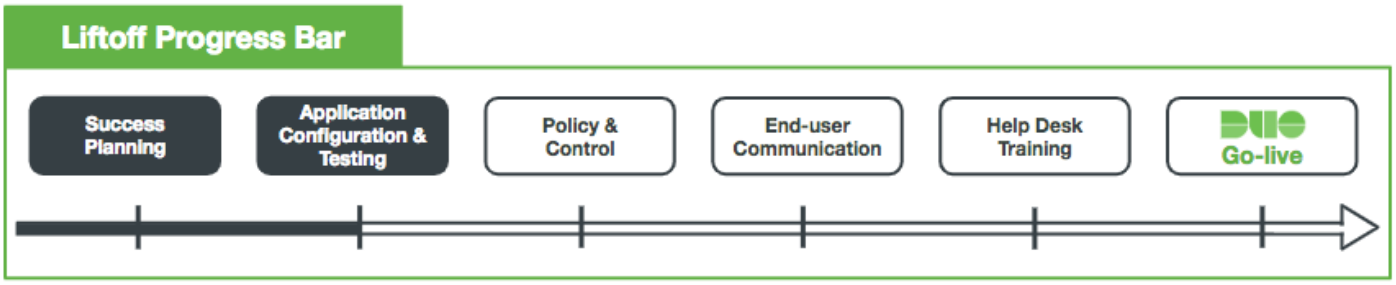
- We developed a **deployment timeline** (see below) based on successful Duo deployments. This can serve as a blueprint for your Duo rollout.
- Each key **Duo Deployment Stage** is emphasized in black, accompanied by **key tasks** to be completed during the stage.



- **Administration Overview**
  Assign Duo administrators roles to manage users, policy settings, applications, and more. Configure alerts and messaging to prevent snags in the deployment process.
    - **Key Resources**
      - Admin Panel Settings Overview
      - Managing Duo Administrators
      - Duo Administrative Roles
      - Help Desk Guide
      - Telephony Credits: Low Credit Alert
      - How-to: Custom Duo Universal Prompt and Duo Desktop Help Messaging
      - Lockout & Fraud Reporting
    - **Best Practices**
      - **Make sure at least 2 Duo administrators have the "Owner" role for your account.** Only Duo administrators with the "Owner" role can create, update, or delete other Duo admins.
      - Specify a Lockout and Fraud Reporting email address. We recommend a **distribution list** so that multiple people can see 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, **set up the Low Telephony Credit Alert option**.
      - **Leverage Administrative Units** to control how administrators can view and manage groups of Duo users and applications.
      - If you have a SAML 2.0 identity provider, **configure single sign-on (SSO) login to the Duo Admin Panel.**

- **Determine Duo Enrollment Methods**
    - **Key Resources**
      - User Enrollment Options
      - The Duo Policy Guide includes information on how policy configuration can affect user enrollment.
    - **Best Practices**
      - **Import Duo users, groups, and administrators from your existing external directories** to reduce your administrative burden.
      - **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."
      - Understand the **differences between Duo user enrollment states.**

Application Configuration & Testing: Making Duo Work for You



Overview of Application Configuration & Testing

Executing your deployment plan begins with **identifying, configuring, and testing your applications**. You can protect as many applications as you need to and administer each independently. If you have a Duo Premier subscription, you may also want to add the Duo Network Gateway to protect access to your internal web applications and SSH servers. **Testing and piloting your applications and endpoints** before launch is key for a successful deployment.

- **Identify Applications**
  Duo can protect a wide variety of on-premises and cloud-based applications through both pre-configured solutions and generic configurations via SAML, RADIUS, LDAP, and more.
  - **Key Resources**
    - Duo Single Sign-On (SSO) protects access to cloud-based applications and creates a web-based application launcher page for your organization.
    - Many of Duo's application integrations do not require any local components. However, certain functions do require a local Authentication Proxy service. The Authentication Proxy Reference Guide contains a comprehensive reference of configuration options available for the proxy and generic RADIUS and LDAP documentation is also available.
    - **Unique to Duo Premier**: Duo Network Gateway (DNG) provides remote access to on-premises applications with multi-factor authentication and device inspection using the Duo Prompt. You can connect the DNG to Duo SSO or any SAML IdP and add links to on-premises web applications to the application launcher to make them easy for employees to locate.
  - **Best Practices**
    - Review the Duo documentation for applications you have in mind and note any prerequisites, such as the Authentication Proxy, Duo SSO, or a SAML Identity Provider, etc. that could take additional time or resources to prepare.
    - Widely-used and highly-sensitive applications are great starting points:
      - Applications that cover a majority of users will help tie enrollment and implementation together. Microsoft 365 is a great example of this—many people use email, calendaring, and other productivity tools. Starting with a common, shared application will get most of your users enrolled and familiarized with the 2FA experience early on.
      - You can immediately prioritize the security of your systems and applications that contain or have direct access to sensitive data by making them part of your initial Duo roll-out.

- **Considerations**
  - Is there a compliance need?
    - Is there a deadline set by PCI, HIPAA, DEA, etc., or internally by a CISO or other lead?
  - What are your resources for deployment?
    - Are test environments available?
    - If your organization has a small IT staff or staff with limited technical bandwidth, you may want to choose a native or less-complex application integration and then iterate to expand the scope of your Duo project in phases.
    - If you have many resources, you might consider deploying multiple applications at the same time.
  - What will the user experience be like for the application you choose?
    - Consider your users' willingness to adopt 2FA. Select applications that present the Duo Prompt for enrollment and self-service or enroll user groups that will quickly adopt 2FA first.
    - Was there a security incident involving a specific application or user population that is a high-value target?
  - Is there a specific time of year that puts a strain on your organization or IT staff?
    - For example, avoid rolling out new Duo features and functionality at the start of the school year for educational institutions, or November and December for retail organizations. If you're a tax firm, avoid implementing between February and March.
  - After protecting your most commonly-used and at-risk applications, consider protecting:
    - HR portals or payroll systems
    - Privileged access
    - Remote access
    - Stand-alone web applications or cloud identity management solutions

- **Configure Applications**
  - **Key Resources**
    - How-to: Protecting Applications
    - Authentication Proxy Reference Guide
    - Authentication Proxy Best Practice Guide

  - **Best Practices**
    - You can install and configure Duo to protect many of our supported applications in a **variety of ways**. This allows you to build your Duo applications to customize your end-user and administrative experiences.
      - You can find more details about tailoring Duo to your unique environment 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** and Duo Central to help users identify which application they're logging into and 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, "secret key," or "client secret"** like you would a **privileged password**. Do not send the SKEY as a screenshot or plaintext over email,

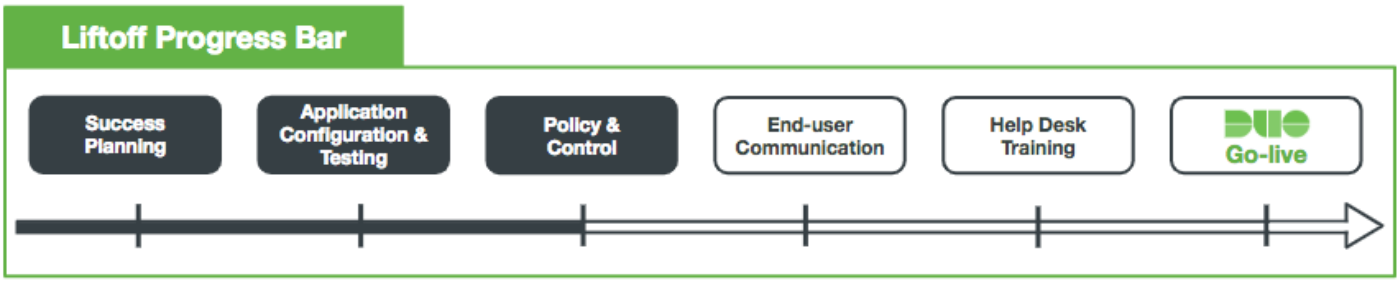
even to Duo support technicians. If you need to transmit your SKEY, we recommend encrypting it prior to sending and transmitting it over an encrypted medium such as HTTPS or secure email.

- **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**.
      - **Unique to Duo Premier:** If you're using the DNG to provide SSH or application access to on-premises applications, we recommend conducting a test that ensures you are able to access those applications from outside your network without using your VPN client.
    - **Label your applications** in the Duo Admin Panel accordingly to reflect how they're used in your test or production environments. This can be edited in the **Settings** section of the application page.
      - Example: *Cisco ASA [TEST]* and *Cisco ASA* are two separate Cisco ASA applications configured the same for testing and production, respectively.

- **High Availability & Disaster Recovery Configurations**
  - **Key Resources**
    - Duo Guide to Business Continuity Preparedness
    - How Duo Security Delivers Service Reliability
    - Setting up the Duo Authentication Proxy for High Availability
    - Setting up the Duo Network Gateway for High Availability
  - **Best Practices**
    - Understand the Duo failmode options and which integrations support them.
      - Authentication workflows that involve the **Duo Authentication Proxy**, as well as most installer-based integrations like Duo Authentication for Windows Logon and RDP and Duo Unix with PAM support (pam_duo), generally allow you to configure a failmode.
    - Create an **emergency plan to remove Duo** from the authentication workflow in the event of a long service disruption.
      - This should be done on a **per-application basis**.

- **Conduct an End-User Pilot**
  - **Key Resources**
    - Deploying a Proof of Concept
  - **Best Practices**
    - We recommend piloting Duo in multiple 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.

Policy & Control: Protecting Access to What Matters



Overview of Policy & Control

Duo Policies provide an easy way to create rules around who can access applications and under what conditions. **Customize** policies globally or per user group or application to allow for powerful and granular control of access within your deployment. User enrollment strategy will also inform your policy configuration.

- **Customize User Access with Duo Policies**
  - **Key Resources**
    - Policy & Control documentation
    - Duo Policy Guide: Configuring Access via Duo Policies
  - **Best Practices**
    - Keep in mind that enrollment, group, and user statuses can impact policy implementations.
    - Some policy implementation scenarios **require both an Application and a Group Policy** to achieve the desired outcomes.
    - As a start, here are some of the most popular policy controls to consider for your rollout:
      - Deny access from anonymous IPs
      - Deny access from non-supported browsers
      - Require users to have the most up-to-date version of Duo Mobile
      - Require that mobile users enable screen lock
      - Require that users are on the latest version of iOS or have the latest security patches on Android
      - Allow access only to devices that have Duo Desktop installed
      - Require that laptops and desktops are on the latest patch level of Windows OS or have the latest version of macOS
      - Require that laptops and desktops have password, firewall and/or disk encryption enabled
      - **Unique to Duo Premier:** Require laptops and desktops to have an antivirus agent installed
      - Allow access to users using only Trusted Endpoints
      - Allow users to choose to remember their devices

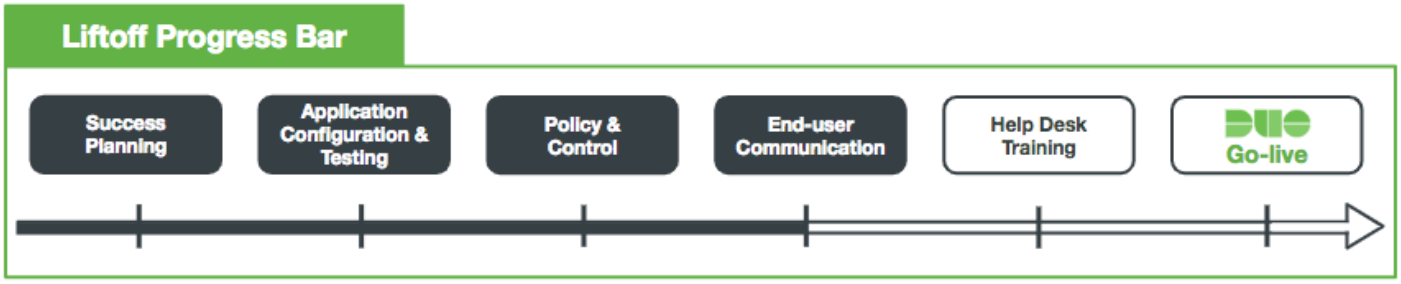
- **Deploy and Test Duo Desktop Overview**
  - **Key Resources**
    - Duo Desktop documentation

        - Duo Desktop FAQ
        - Duo Desktop Release Notes
        - Duo Desktop Knowledge Base articles
    - **Best Practices**
        - To start collecting device information without blocking users, we recommend targeting a test group of users and a pilot application. As part of the Duo Desktop deployment, consider:
            - Configure the Duo Desktop policy to require installation of Duo Desktopwithout selecting the "Block access" options below it.
            - See how the deployment of both the application and policy would affect a sample population of your user base.
            - Review the states of devices accessing Duo-protected applications in the Admin Panel, then assess which policy will best protectyour users.
        - To distribute and install Duo Desktop, we recommend applying the Duo Desktop policy to a web-based application that features Duo's inline authentication prompt. This installation requires administrator privileges and allows users to self-install the client when prompted during Duo authentication.
        - Consider combining Duo Desktop policy with other Duo policies including Browsers, Plugins, and Operating Systems policies. For example, a custom policy may enforce access based on the following checks:
            - Has an encrypted drive (using FileVault for macOS or BitLocker for Windows 10)
            - Has the host firewall enabled (using Application Firewall for macOS or Windows Defender Firewall)
            - Is protected by a password
            - Is accessing the application using a Chrome browser
        - We recommend combining the existing OS policy with the Duo Desktop policy. By doing so, Duo Desktop will be the preferred and more trusted source of information about the endpoint OS over a user agent.
            - The application additionally provides the security patch version for Windows devices. For the Operating Systems policy, under the “Allow Windows devices” header, open the dropdown under the “Encourage users to update” or “Block versions” label, and you’ll see new Windows 10 and 11 version options. When you select these options, additional information appears on the right side of the policy screen with details about activating an Operating Systems policy with this setting.
        - **Unique to Duo Premier: Agent Verification**- You can configure Duo Desktop to block access to a device if an antivirus agent is not running at the time of application access. See a list of supported antivirus/anti-malware agents.
        - **Troubleshooting:** Reference the Duo Desktop Knowledge Base articles for a list of common questions and issues.

- **Configure and Test Trusted Endpoints Overview**
    - **Key Resources**
        - Trusted Endpoints documentation
        - Trusted Endpoints Best Practices
        - How Duo Establishes Device Trust
        - Trusted Endpoints Knowledge Base articles
        - Integration with Cisco Secure Endpoint

- **Certificate-based Trusted Endpoint Verification End of Support**
  - As part of the shift away from certificates for identifying trusted endpoints, we will end support for management integrations based on issuing Duo Device Trust certificates in a future release. Learn more in the Duo Trusted Endpoints Certificate Migration Guide.
- **Best Practices**
  - The Trusted Endpoints Global Policy defaults to checking devices for trust but never blocks access if the device is untrusted. We recommend leaving the default global setting and configuring additional policies applied to applications or user groups to allow or disallow based on their trust status.
  - Consider using the Trusted Endpoints with Duo Mobile integration to ensure that end-users' mobile devices are checked for security posture every time they are used to access a secured application. Note that once enabled, the user will be prompted to open Duo Mobile to perform a device health check prior to authentication.
  - **Unique to Duo Premier:** If you use Cisco Secure Endpoint as your endpoint security agent, you can integrate Duo with the agent using a connector application. This enables Duo and Cisco Secure Endpoint to have shared visibility into a Windows or macOS endpoint, and Duo can block access to protected applications by Duo from devices deemed as compromised by Cisco Secure Endpoint.
- **Testing and Troubleshooting Trusted Endpoints**
  - Every organization is different, which can affect how you roll out and enforce Trusted Endpoints. Common deployment scenarios are documented in our Deployment Setup Tips.
  - We recommend testing to understand the end-user experience:
    - Will users encounter any additional prompts during authentication?
    - Are users blocked when attempting access from an untrusted device when a blocking policy is configured?
  - As part of a comprehensive test plan, consider testing application access with:
    - Multiple OSes, including mobile OSes like Android and iOS
    - Thick applications on both desktops and mobile devices (if applicable)
    - A variety of browsers, including mobile browsers
  - If using the Manual Enrollment integration for testing, note that downloading and installing a certificate for manual enrollment on the test device does not mean that the device will be checked for trust.
    - Be sure to add the user associated with that test device to a test user group, then associate that test group with the Manual Enrollment integration.
    - Also note that a Manual Enrollment certificate is only associated with the user who first uses it. However, multiple certificates for separate user logins on one machine are supported.
  - **Troubleshooting:** Reference our Trusted Endpoints Knowledge Base articles for a list of common questions and issues related to Trusted Endpoints.

End-user Communication: What Everyone Needs to Know

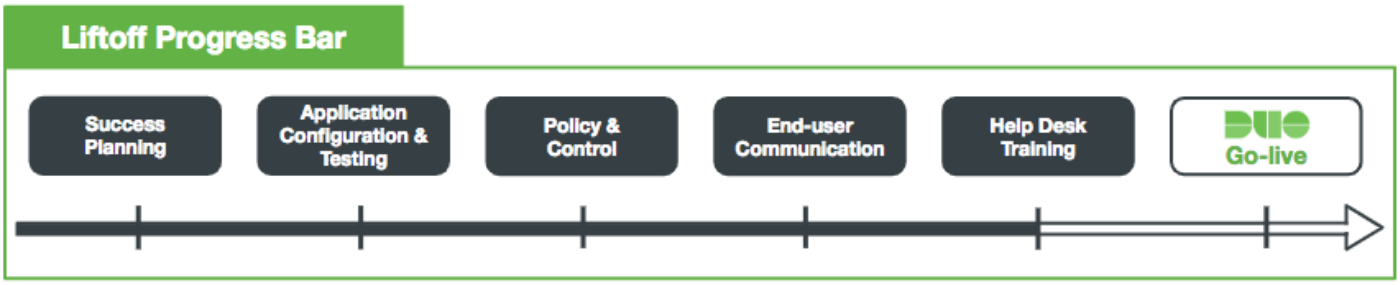


Overview of End-user Communication

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
    - Duo Demo Website
    - Duo Privacy Data Sheet
  - **Templates**
    - End-User Education Email Communication Templates
      - These include templates for communicating with end-users about a new Duo deployment, enforcing Trusted Endpoints, Duo Desktop, Verified Duo Push, and more.
    - Customizable Duo Deployment Signage Templates
  - **Best Practices**
    - Encourage users to use Verified Push. It is a cheap, safe, and simple way to authenticate. Verified Push works on either WiFi or cellular service with data and can be used in any country.
    - **Be aware that 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**, add **no-reply@duosecurity.com** to your allow list.
    - If applicable, inform users about the data collected by Duo Desktop.
      - The Duo Desktop application collects information from a user's laptop or desktop device at the time of authentication to ensure that the device's security health is congruent with the Duo administrator's security policies.
      - For more information, see: What data does Duo Desktop collect?

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 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 the 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**.
      - **Demonstrate Duo Push** by either presenting your smartphone or using the Push Notification Demo.
      - If applicable, demonstrate the user experience for the Duo Desktop using our Demo.
    - Remind Duo administrators that their administrator 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**, they should contact Duo Support **via phone rather than email** to ensure immediate action.
      - Issues that halt your business operations and have no procedural workaround are considered to be of **critical severity**.

Duo Support & Helpful Resources

Overview of Duo Support

If you need additional help, **contact our** Support team! Our Customer Ticket Portal is the best way to create a case–it is the easiest and most secure way to share technical information such as logs, configurations, or screenshots with Duo Support. You can also always drop us a line at support@duosecurity.com.

For **more immediate or emergency assistance,** please call us at **(866) 760-4247**. If you are located outside of the US, find your country's phone number here.

Our Support team is available **Monday through Friday from 9 a.m. to 5 p.m. local time**. Outside of those hours, you can call Duo Support to report a Critical Severity issue with our service. Critical Severity issues are defined as **"Duo's service halts your business operations and no procedural workaround exists."** Note that new setups or general deployment questions are not considered Critical Severity issues.

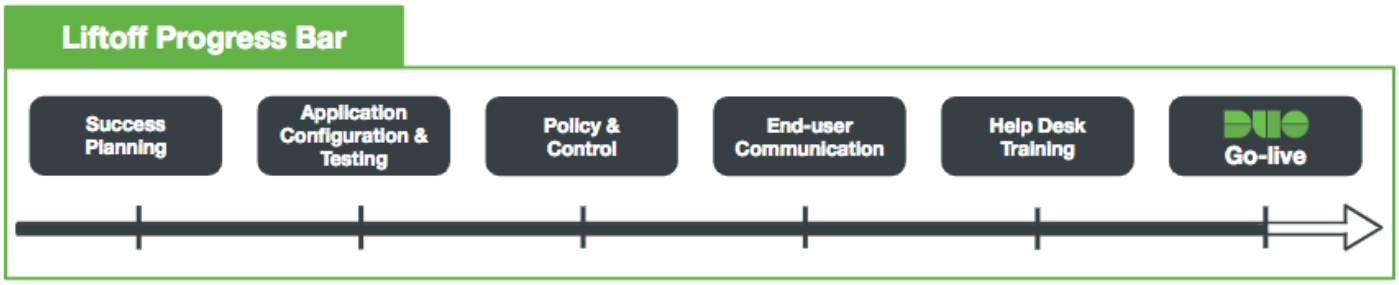
Duo requires that only administrators listed in the Duo Admin Panel contact Duo Support. Be ready to verify your identity through a Duo Push authentication (or another method) and provide your 10-digit account ID to ensure prompt service.

Overview of Helpful Resources

We are committed to providing you with the best possible experience. Below is a collection of **key Duo resources to assist you in getting the most out of your Duo subscription.**

- Duo Knowledge Base - Search our extensive knowledge base articles for quick answers on our most common customer issues.
- Duo Documentation - Detailed deployment documentation, installation, and configuration information for a wide range of devices and apps.
- Cisco Community: Duo Security - Connect with and learn from Duo users and security professionals in our public forum.
- Status Page - Check the current status of Duo's systems.
- Customer Ticket Portal - Create new cases, review previous requests, or leave CSAT feedback.
- Product Release Notes - Subscribe to receive an email as soon as new Release Notes are posted.
- Duo Blog - The official Duo blog. Great for product & security industry updates.
- Upcoming Duo Events & Webinars - Keep up-to-date with our latest webinars and upcoming events.
- Additional Resources - Guides, How-Tos, and Infographics

Duo Go-live: Ensuring a Seamless Deployment



Overview of Duo Go-live

Congratulations! You successfully completed the steps to 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 promote** your Duo deployment:
  - ❑ Post Duo announcements on **intranet or your employee community webpage**.
  - ❑ Include Duo in **company events** and **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.