Help Desk Guide

Originally released June 22, 2016
Revised July 24, 2017

Table of Contents

Commonly-used terms

Some terms you may encounter in Duo documentation, among your internal IT team, or from end users:

2FA (two-factor authentication): an additional layer of authentication beyond a username/password. 2FA implies something you know (password) and something you have with you (like Duo Mobile on your smartphone) to prevent somebody from simply "knowing" your password and accessing your data. When Duo's 2FA is enabled, you still enter your username and password; Duo does *not* replace your username and password. It is simply an added layer of security on top of your existing credentials.

Duo Admin Panel: the login-protected interface where Duo administrators can manage their users, devices, integrations, roles, logs, billing information, and so on.

Duo Authentication Prompt: this lets users choose how to verify their identity each time they log in (e.g. "Duo Push" or "Call") to a web-based application. The prompt allows for inline enrollment and authentication.

Passcode: these can be generated either via the Duo Mobile app, SMS (text message), or a user's hardware token.

Platform: a user's device type (iPhone, Android, etc).

Push Notification (Duo Push): this is an out-of-band authentication request that is sent to the Duo Mobile App on an enrolled device. Push notifications include information like user location, the IP address, and the application that the user is trying to access.

Self-service portal: if this has been enabled in the admin panel, that means that a user can add additional devices, or update their authentication method settings, right from the Authentication Prompt. Available to all paying editions of Duo.

Part 1: Overview

Why do I need this guide?

Rolling out two-factor authentication (often referred to as 2FA) to your company can produce questions from your end-users. While Duo prides itself on its ease of setup and friendly interface, we understand that the Duo authentication experience can initially be confusing for some individuals—especially if they have never used two-factor before. This document is designed to provide you with quick answers to address issues that your end-users may encounter when using Duo.

This guide is intended for use by administrators listed with specific administrative roles to help end-users complete common tasks and resolve issues. You can read more about the difference between Duo accounts for administrators and end-users here.

Duo recommends having at least two Duo Owners for any given account. Likewise, it is important to regularly update your list of administrators as Owners may enter or leave your organization. Having two owners provides redundant access to the Duo Admin Panel and ensures a more consistent level of access should an owner be unavailable. We find that having multiple owners saves customers time by letting them self-serve their administrative needs.

Here's a quick overview of the roles and their access to complete tasks within the Duo Admin Panel:

Action	Administrative Role: Owner	Admin	Application Manager	User Manager	Help Desk	Billing	Read-only
View Logs	✓	✓	✓	✓	✓	✗	✓
Modify phones, tokens, & bypass codes	✓	✓	✗	✓	✓	✗	✗
Modify users & groups	✓	✓	✗	✓	✗	✗	✗
Modify applications	✓	✓	✓	✗	✗	✗	✗
Modify settings	✓	✓	✗	✗	✗	✗	✗
View & modify billing	✓	✗	✗	✗	✗	✓	✗
View & modify administrators	✓	✗	✗	✗	✗	✗	✗

Part 2: Enrollment and activation

What will the enrollment experience be like for end-users?

Users have two options: to start the enrollment process from a device other than what they plan to authenticate with (such as a laptop or desktop they will use to access Duo-protected services) **or** with what will eventually be their authentication device (such as their mobile phone).

Enrolling from a laptop, desktop, or other non-authentication device

Users will begin with the link provided in their enrollment email. When using the enrollment prompt, users can scan a QR code with their authentication device:

If a user says that they cannot scan the QR code, ask them to verify that they have allowed the app access to the phone's camera; otherwise they will not be able to scan the code. More information on this process is available in our Enrollment Guide: https://guide.duo.com/enrollment

Enrolling from their authentication device

With this method, users will begin setup from the enrollment email on their mobile device, proceed through enrollment, and finally install Duo Mobile if needed. More details are available in this Knowledge Base article: https://help.duo.com/s/article/3890

How do I resend enrollment emails?

Emails can be re-sent to users who have been created using bulk enrollment or Active Directory Sync and have yet to complete enrollment. Follow the process detailed in Step 5 of Bulk Self-enrollment here to resend enrollment emails: https://duo.com/docs/enrolling_users#bulk-self-enrollment

Part 3: Authentication and authentication methods

How do I add or activate a new authentication device?

This process explains how to add and/or activate a new authentication device (such as a mobile phone, landline, tablet, or U2F token) for a user. If the self-service portal within the Authentication Prompt is enabled (available only for paying editions of Duo), then users can add new devices themselves. If the portal is not enabled, then devices may only be added by administrators.

Note that users may only add a new device via the self-service portal if they have access to another previously-activated authentication device or a bypass code. If they do not have access to either, then an administrator must assist them in adding a new device.

If self-service portal enabled: https://guide.duo.com/add-device
Manually via Duo Admin Panel: https://duo.com/docs/administration-devices

What should I do if a user forgets their device?

Have a user who left their phone or hardware token at home? Check out this Knowledge Base article for ways you can help: https://help.duo.com/s/article/3302

What should I do if my device is lost or stolen?

Always stress to users that they should contact an administrator immediately if their 2FA authentication device is lost or stolen.

If the self-service portal is enabled and a user has a second authentication device, then they should immediately access the “My Settings & Devices” menu in the Authentication Prompt and delete the lost or stolen device. If the user does not have self-service enabled or a second authentication device, then an administrator must delete the device from Duo after ensuring a new authentication method has been added.

If self-service portal enabled: https://guide.duo.com/common-issues#lost-phone
Manually via Duo Admin Panel:
https://duo.com/docs/administration-devices#dealing-with-lost-or-stolen-phones

Why am I not receiving Duo Push notifications?

First, ensure that the user allows notifications on their phone.

You may have trouble receiving push requests if there are network issues between your phone and our service. Many phones have trouble determining whether to use the WiFi or cellular data channel when checking for push requests, and simply turning the phone to airplane mode and back to normal

operating mode again often resolves these sort of issues, if there is a reliable internet connection available. Similarly, the issue may be resolved by turning off the WiFi connection on your device and using the cellular data connection. A Duo Push notification is only 2 KB.

Check the time and date on your phone and make sure they are correct. If the date and time on your phone are manually set, try changing your device's configuration to sync date and time automatically with the network.

We have also created in-depth troubleshooting guides for Duo Push delivery for iOS: https://help.duo.com/s/article/2051 and Android: https://help.duo.com/s/article/2050. Note that an IT administrator with ability to modify port access may be required depending on the specific issue being encountered.

How do I assign tokens to users?

Tokens purchased from Duo are automatically imported into your account. Admins need to manually import third-party OTP token information into Duo. When importing tokens, keep in mind that tokens should be unique between Duo accounts.

Duo supports FIDO U2F tokens, but U2F tokens cannot be imported or assigned to users from the Admin Panel. Instead, users self-enroll the U2F token via the Duo enrollment prompt or self-service portal. See our documentation about enabling U2F authentication and the U2F enrollment process for end users to learn more.

To assign a token to an end user:
https://duo.com/docs/administration-devices#assigning-a-token-to-an-end-user

How do I generate bypass codes?

A bypass code is a temporary passcode created by an administrator for a specific user. These are generally used as “backup codes,” so that users who are having problems with their mobile devices (e.g., mobile service is disrupted, the device is lost or stolen, etc.) can still access their Duo-protected systems. Bypass codes can also be used to allow a temporary user access to applications that do not support self-enrollment without having enrolled a device. Bypass codes expire after being used the allowed number of times, or after an administrator-defined amount of time. By default, bypass codes expire after a single use or in one hour, whichever happens first.

Follow the process here to generate them:
https://duo.com/docs/administration-users#generating-a-bypass-code

Part 4: Pro tips

Users may be on high alert for phishing

If you have just rolled out Duo education internally, users may be highly suspect of communications they receive like the Duo enrollment and activations email. You may receive concerns from users that they are being phished through this email. If you would like to check the communications that were sent, you can see the email or SMS copy in the admin panel, and/or ask the user to forward you a copy of the messaging they have received so that you can verify that it is a secure message and they can proceed with enrollment/authentication.

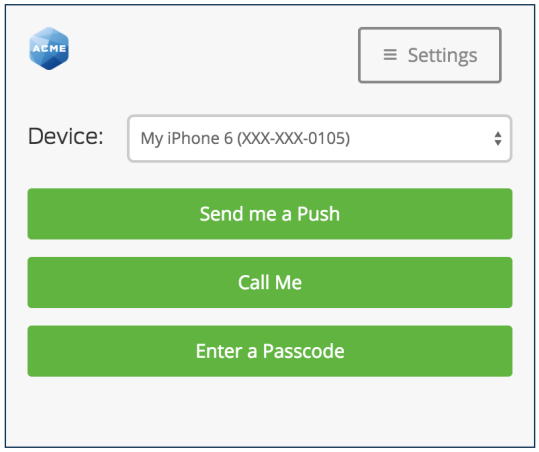
Encourage users to use Duo Push

Always encourage your users to use Duo Push, if possible. Duo Push is the best option: it is convenient, secure, and the cheapest (there are no telephony charges for Push authentication). Users can also Push if they do not have cell service, and it works in any country.

We have also created a guide to help promote Duo Push with users:
https://help.duo.com/s/article/promoting-push

A user's Authentication Prompt may be formatted differently than they expect

If a user is logging in from a smaller device (like a tablet) or a small browser window, the authentication prompt may look slightly different than what they have seen in end-user documentation. They still have the same functionalities as other users with the same rights.



Whitelist no-reply@duosecurity.com

If your organization uses email filtering, whitelist this address or users may not receive enrollment or activation emails.

Activation links and enrollment links have different expiration dates

An enrollment link expires in 30 days. If you resend an enrollment email, that will not reset the enroll-by date.

An activation link expires, by default, after 24 hours. Users who have recently been sent activation links from the Duo Admin Panel cannot be sent a new link until the existing link expires.

Additional information on activation & enrollment messaging is located at https://duo.com/docs/enrolling_users.

Part 5: Troubleshooting and support

Troubleshooting resources

All Duo Admin Panel processes and application configuration recommendations are available on Duo's exhaustive documentation home at duo.com/docs.

help.duo.com is the home of Duo's Knowledge Base: a searchable repository of troubleshooting resources and self-service content.

Having issues with authentication or accessing the Duo Admin Panel? Our Support Team updates Duo's Status Page at https://status.duo.com in real time to reflect any service issues. We highly recommend subscribing!

Getting the best possible support from Duo

If you did not find the information you needed, here is what you will need to contact Duo's Support Team:

- Make sure the person contacting support is listed is a listed administrator in the Duo Admin Panel.
    - If they have an administrative role other than Owner, support will only be able to help them complete relative to their level of access.
- If appliances or applications outside of Duo are involved (ex: Active Directory), make sure an administrator with access to them is available.
- Make sure to provide screenshots and log files whenever possible.
- Your Account ID.
- If including your authentication proxy .cfg or other sensitive files, make sure to **never** share a secret key (SKEY) via plain text. We recommend GPG encryption.
- If you've previously contacted Duo Support, include the ticket number regarding this issue.

Determine how and when to contact Duo Support based on your edition and urgency:
https://help.duo.com/s/article/1441