Introduction

Saint Francis and St. Mary's employees accessing UCSF-hosted applications are required to set upuse Duo Multi-Factor Authentication (MFA) to authenticate their identity.

Duo MFA FAQs

FAQs

What is multi-factor authentication (MFA)?

MFA is essential to web security because it quickly neutralizes the risks associated with compromised passwords. If a password is hacked, guessed, or even phished, that's no longer enough to give an intruder access: without approval at the second factor, a password alone is useless.

Is there a cost for using DUO MFA?

No, Duo MFA is provided at no cost to keep you, your data, and UCSF safe.

If I use Duo on my personal smartphone, will this interfere with my personal business?

In today's world of phishing and scamming, most companies are requiring MFA. Have you ever been asked to receive a code via text on your phone when logging into a website? That is a form of MFA. Cell phones are the most efficient and secure method to provide MFA.

Having Duo on your personal phone won't interfere or interact with any personal data. Duo only sends you a push notification when you are logging into accounts that require it.

Why have I never had to use Duo before?

All hospitals have an MFA process in place. If not Duo, one that is like Duo. Duo MFA is a well-established workflow at UCSF. Most of our staff currently have Duo on their phones. Anytime you access the UCSF network from home, Duo is required.

Duo MFA Device Options and Instructions

Duo MFA is available to UCSF Health Saint Francis and St. Mary's employees on the following devices:
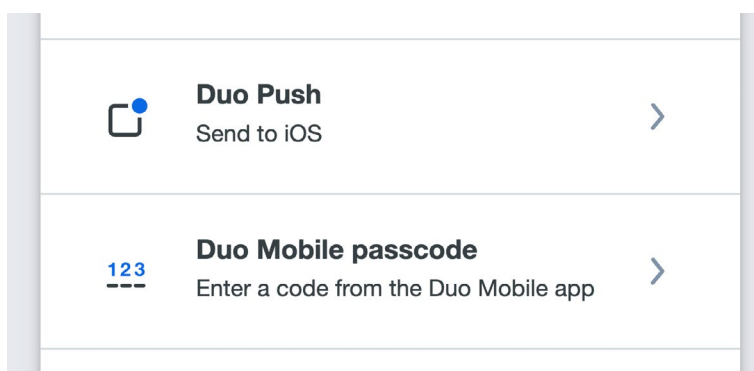
1. Duo Push

This is the default verification method for Duo users with a smart device, and UCSF IT's recommended method for multi-factor authentication. This requires a smartphone or tablet running Android or iOS with the Duo Mobile application installed and enrolled to your Active Directory account, and an internet connection.

- To enroll your smart device in Duo, visit Enrolling a Smart Device (Smartphone or Tablet) in Duo.
- To learn how to use Duo Push, visit Duo MFA Push.

2. Duo Mobile Passcode

This is an alternate option for MFA verification; this also requires the Duo Mobile application installed to a smart device (smartphone or tablet running Android or iOS) but does not require an internet connection.

- To enroll your smart device in Duo, visit Enrolling a Smart Device (Smartphone or Tablet) in Duo.
- To learn how to use Duo Mobile Passcode, visit Duo MFA Passcode.

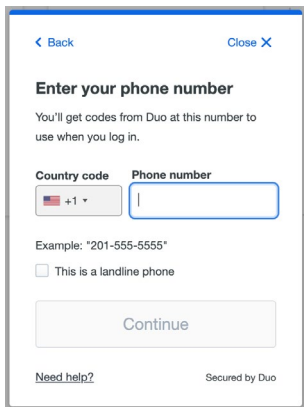|	Duo Push Send to iOS	>
123 ---	Duo Mobile passcode Enter a code from the Duo Mobile app	>

3. Token

Tokens are only available to users for whom Duo Push or Mobile Passcode are not viable options. Users will need to carry a physical token that will generate a unique passcode for each login that the user will manually enter at the Duo prompt.

Duo tokens will be provided by request by visiting UCSF IT's onsite team Monday, July 22 through Friday, August 9. After August 9, Duo tokens can be requested by filling out a form available on the UCSF IT Service Desk portal, which will be accessible via the UCSF Health Saint Francis and St. Mary's Hospital and Clinics intranet portal at https://sfch.ucsfhealth.org/.

- To learn how to use the Duo Token option, visit Multi-Factor (Duo) Authentication Methods | UCSF IT.

4. Phone Call (Mobile and Landline)

Alternate option for verification that does not require a smart device. Warning: This is a less secure option, as most phones by default allow anyone to answer calls without unlocking the device.
NOTE: In the future, UCSF IT will no longer offer this authentication option.

- To enroll in a phone to receive a Duo MFA phone call, visit Enrolling a Mobile (Non-Smartphone) or Landline Phone in Duo.
- To learn how to use the Phone Call option, visit Duo MFA Phone Call.