

## Introduction

As a community provider with Medical Staff privileges at UCSF Saint Francis and UCSF St. Mary's, you have the option to opt in to using a UCSF Outlook Web network email account. You will receive an email on Monday, August 19, with the subject line **Activate Your UCSF Network Email Account**. This document will assist you with activating your Okta secure access account, setting up a device in Duo Multi-Factor Authentication (MFA), creating your UCSF email password, and accessing your Outlook Web network email account.

**NOTE:** If you plan to opt in to using your UCSF network email account, please complete this process within **seven days** of receiving the email as the Okta account activation link will expire at that time.

## Activating Your Okta Account and Setting Up Duo Multi-Factor Authentication (MFA)

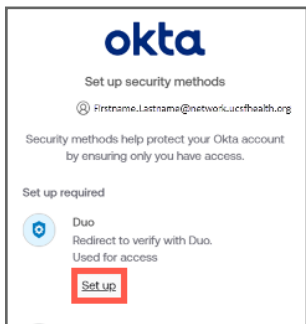
**NOTE:** If you already have Duo Mobile installed on your mobile device, complete steps 1-9 below and then skip to **Enrolling a New Device in Duo with Duo Already Installed** in the next section.

1. Open the **Your UCSF Email Account** email and click the **Activate Okta Account** within **seven days** of receiving the email.

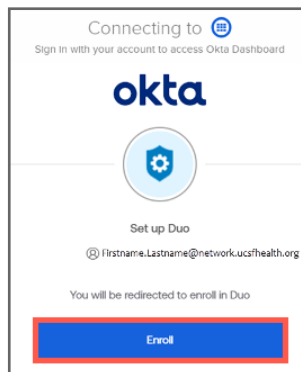
**NOTE:** It is recommended you start this process on a desktop workstation to easily facilitate scanning of the on-screen QR code within the Duo Mobile app.

2. On the **Okta Set up security methods** screen, you will see two **Set Up** buttons (for **Duo** and **Password**).

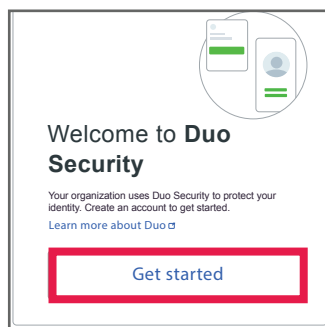
3. Select the **Set up** option for **Duo**.



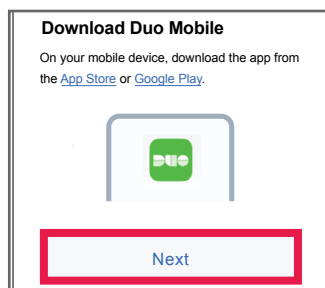
4. On the **Set up Duo** screen, click the **Enroll** button.



5. The **Welcome to Duo Security** screen will load, select the **Get started** button to set-up an account in Duo.

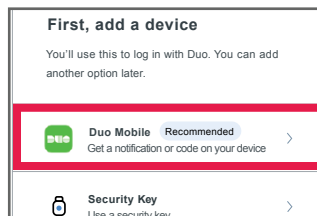


6. Before clicking the **Next** button on the **Download Duo Mobile** screen, you will need to download the **Duo Mobile app** from the **App Store** or **Google Play**.



7. Select the **Duo Mobile** option.

**NOTE:** The UCSF Duo tenant supports two authentication methods: **Duo Mobile** and **Security Key**. **Duo Mobile** is highly recommended.



(Continued on the next page)

## Enrolling in Duo on a New Device (continued)

8. Enter your **Mobile Phone Number** before clicking the **Continue** button.

9. Click the **Yes, It's correct** button to confirm your mobile phone number.

10. Scan the on-screen QR code to register your device with Duo in the Duo Mobile app.

**NOTE:** You will be presented with a Duo prompt on your mobile device.

## Enrolling a New Device in Duo with Duo Mobile Already Installed

**NOTE:** The following steps will pick up after **step 9** in the previous section.

1. Open the **Duo Mobile app** on your device before selecting the **Add +** button.

2. Select the **Use QR code** option.

3. **Scan** the *QR code* using your device's camera.

4. The **Added Duo Mobile** confirmation screen will load, select the **Continue** button.

5. On the **Add another way to log in?** screen, select the **Skip for Now** link to complete the process.

## Setting up your UCSF Network Email Account Password

1. Return to the **Okta – Set up security methods** screen.

2. Under the **Password** section, select the **Set up** option.

3. On the **Set up password screen**, enter a **password** that fits the password requirements on screen.

(Continued on the next page)

## Setting up your UCSF Network Email Account Password (continued)

4. Confirm your password by entering it in the **Re-enter password** field.

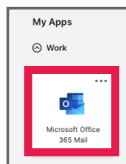
5. Select the **Next** button to complete the process.

## Logging Into Your UCSF Email Account

1. Navigate to <https://netlogin.ucsfhealth.org>.
2. On the **Okta login** screen, enter your **UCSF email address** and **Password**.

3. Click the **Sign in** button.

4. Under **My Apps** heading, select the tile.




5. **Microsoft Outlook Web Email** loads successfully.

6. Congratulations! You have successfully accessed your UCSF email account!

## Creating and Sending Emails Securely


There may be times where you need to send UCSF patient Protected Health Information (PHI), Restricted (P4) data, or Sensitive (P3) data to recipients either internally or externally. See UCSF's data classification policy [here](#).

**NOTE:** Recipients will need to register with the UCSF secure email service to view the message securely.

1. From Microsoft Outlook Web Email, select the  button.
2. Enter the **recipient(s)** in the To: and Cc: fields.

3. Include **Secure:** at the beginning of your subject line to encrypt emails that contain **sensitive** or **restricted** information, followed by a **subject** for the email that provides context to the recipient(s).

4. Enter the **message** information into the **body** section of the email.

5. Click the  button to send your email to the recipients

6. Congratulations! You have successfully created and sent a secure message using Microsoft Outlook Web email.