

Using Duo for Multifactor Authentication



Revision Table			
Date	Version	Description	Author(s)
12/11/17	.1	Initial Draft	John Ruzicka
12/14/17	.2	Revision based on feedback	John Ruzicka
12/19/17	.3	Revision based on feedback	John Ruzicka
12/20/17	.4	Revision based on meeting with Mark Boyce	John Ruzicka
12/21/17	.5	Revisions from User Feedback	John Ruzicka
1/9/18	.6	Revisions from user Feedback	John Ruzicka
1/11/18	.7	Additional Revisions	John Ruzicka
1/18/18	.8	Revisions from Gilbert Loo	John Ruzicka
1/22/18	.9	Revisions from first training class	John Ruzicka
1/22/18	1.0	First release	John Ruzicka
1/23/18	1.1	Changes from Jenn Bejacka	John Ruzicka
1/30/18	1.2	Changes based on general feedback	John Ruzicka
2/1/18	1.3	Changes based on general feedback. FAQ moved to separate document.	John Ruzicka
2/2/18	1.4	Changes based on feedback from Eric Goodman	John Ruzicka
2/9/18	1.5	Change re clarifying when MFA is required	John Ruzicka
3/2/18	1.6	Additional Changes from the MFA team	John Ruzicka
3/20/18	1.7	Changes to link timeout and iOS functionality	John Ruzicka
5/16/18	1.8	Added "Remember Me" information	John Ruzicka
5/23/16	1.9	Additional "Remember Me" information	John Ruzicka

Table of Contents

Introduction	4
What is Multi-Factor Authentication?	4
Why Has UCOP Decided to Use MFA?	4
When is MFA Required?	5
What is Duo?	6
Getting Set Up in Duo	6
Installing the Duo App	6
Activating Duo If You Have a Token (Key FOB)	7
Activating the Duo App on Your Smartphone	7
Reactivating Duo if you Replace Your Mobile Device	10
Adding Another Device in Duo.....	10
Authenticating with Duo	14
Push	14
If “Deny” is Tapped	16
Passcode	17
Travel Code	17
Hardware Tokens	17
Using the “Remember Me” Option.....	19
Duo Settings	21
Modifying An Existing Duo Configuration.....	22
Appendix A – Eight Smart Cybersecurity Habits	23

Introduction

What is Multi-Factor Authentication?

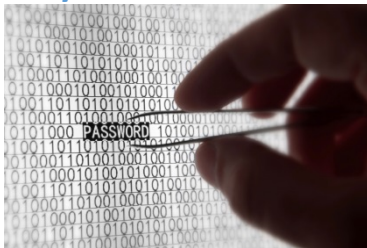


When you use software on your computer you are prompted to login with a user I.D. and password. This is known as “single-factor authentication.” Your password gets you into your computer, or a web site, and verifies your identity.

As security improves, single-factor authentication is being replaced by “multi-factor authentication (MFA),” also known as “two-factor” or “dual-factor authentication.” This involves signing in with your user I.D. and password and then entering an additional code or supplying some type of additional validation indicating that your login attempt is valid.

MFA is already widely used in many areas, including banking, mobile devices, online shopping, etc.

Why Has UCOP Decided to Use MFA?



Hackers are becoming more sophisticated and UCOP is responding to these increased threats. MFA provides an extra layer of security to keep you and the University safer from cyber threats.

For example, if a hacker figures out your email address, and somehow guesses your password, they can go into your account. With MFA, you would receive a notification on another device, usually your smartphone or perhaps a hardware token, that someone is trying to log in to your account. Since it isn't you, you can deny the login and prevent the hacker from gaining access to an application even though they have your I.D. and password.

UCOP realizes that this is an extra step and plans to make MFA as painless as possible. You will only need to authenticate with MFA once per workday (10 hours) unless you use more than one device or browser. For example, if you have a desktop and a laptop computer, you will need to authenticate once for each. If you open one app in Firefox and one in Internet Explorer, you will need to authenticate once in each browser.

Authentication covers multiple apps opened in the same browser window. If you close and reopen your browser, you may have to re-authenticate, depending on browser and cookie settings.

Note that some applications, such as UCPATH, Confluence, etc. have different login timeouts that are shorter. **These are not changing.** For example, you will still be required to sign in to UCPATH each time you use the application.

When is MFA Required?

MFA is being put in place for all apps that use single sign-on and the standard U.C. Applications Login screen (shown below). It is also being put in place for Microsoft Office 365 online (including Outlook email online). Applications that use a different authentication method will not be subject to MFA at this time, including Replicon.

You will be asked to authenticate once during your initial logon to any browser-based application that uses Single Sign-On. You will not be required to re-authenticate for 10 hours *in that browser* provided you keep your browser open (use tabs to open additional applications, or to close the current application without closing the browser). Note: some applications, such as UCPATH, Microsoft Office online applications, and (when off-site) myCloud, require authentication every time they are opened.

MFA is currently only for apps that run on the web (in a browser). **It is not required for applications such as Word, Excel, and the Outlook Desktop client that you open on your desktop.**

See Appendix B of this document for important general information on cybersecurity.

What is Duo?



Duo is the software that UCOP has selected for MFA. It has been used successfully on other U.C. campuses and medical centers. It is a modern, state-of-the-art MFA tool.

Duo allows MFA in multiple ways. These are discussed in detail later in this manual. Briefly, they are:

- **Push:** Duo sends an “Accept/Reject” message to a smartphone or tablet, enabling MFA via a single tap (this option requires the installation of an iOS, Android or Windows Phone app). **This is the easiest method for MFA and the required method if you are using a UCOP-issued smartphone.**
- **Passcode:** Duo generates a passcode to use, even if a mobile device with the Duo app is not connected to the internet. A passcode can be pre-generated for use if you travel overseas and, in a pinch, if you forget your smartphone or token at home.
- **Token:** a physical token is used to display a code for authenticating via Duo. This token is carried on your keychain and is sometimes called a “key FOB.” Pressing the green button on the token displays a code that you use to authenticate.

Getting Set Up in Duo

Installing the Duo App

Employees with UCOP-issued smartphones are required to use the Duo app. If you have a personal smartphone, you can choose to use the Duo App or request, from your manager, a token (key FOB). The Duo app runs on your smartphone, while the token is a physical device you must carry on your keychain.

Installing the Duo App on your personal smartphone does not track your movements in any way. It does not send any messages, advertising, or spam to your personal smartphone. It only sends notifications when you have attempted to login to an app that requires MFA.

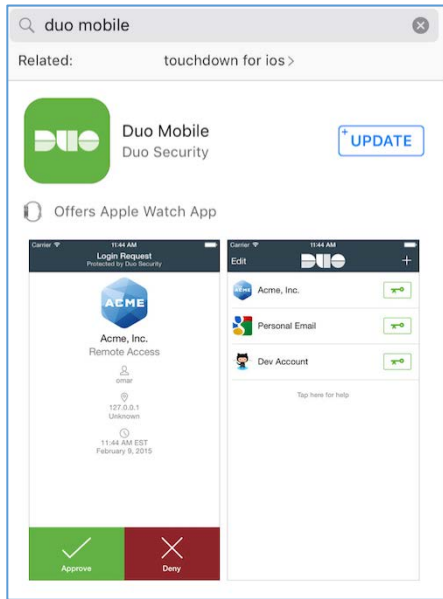
Installing the app lets Duo use the easiest method of authenticating—simply tapping an “Approve” button, as shown in the screen below. Approval can also be done from the lock screen and, in phones that support it, using fingerprint I.D. or facial recognition.

The Duo App is available for iOS, Android, and Windows phones and tablets.

To install the App:

1. Navigate to the App Store for your mobile device, and search for “Duo Mobile.” Install the app using the procedure for your specific phone. Usually, this is simply clicking the “Install” button. For

example, in the iPhone App Store, the Duo app looks like this:



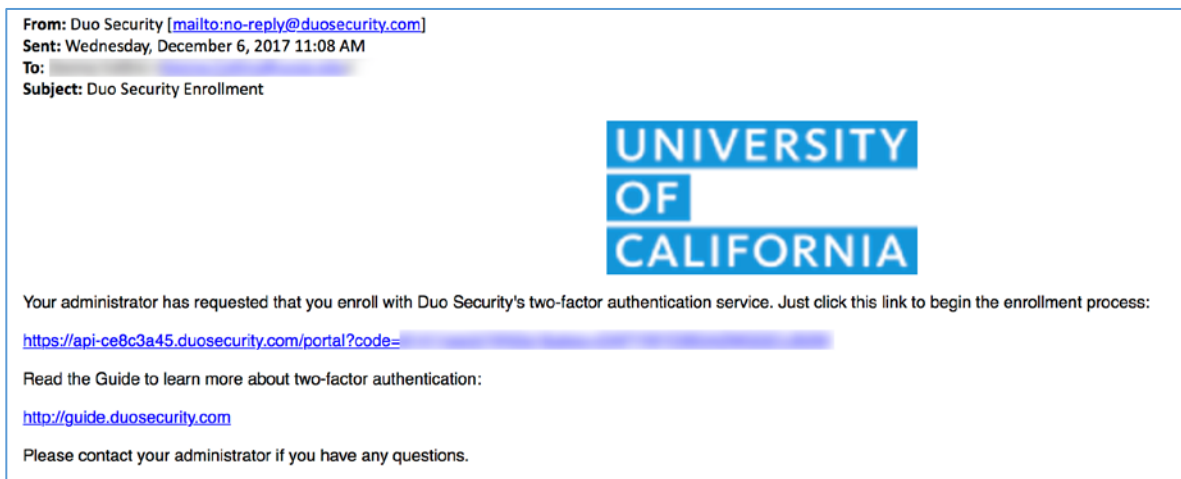
2. You will not initially be able to activate or use the app until you receive an email from Duo Security to start the process. If you are a new employee, you will receive this email on your first or second day of work.

Activating Duo If You Have a Token (Key FOB)

If you are receiving a token (key FOB) instead of using the Duo app on your smartphone, the token will be pre-configured and pre-activated for you by the Service Desk.

Activating the Duo App on Your Smartphone

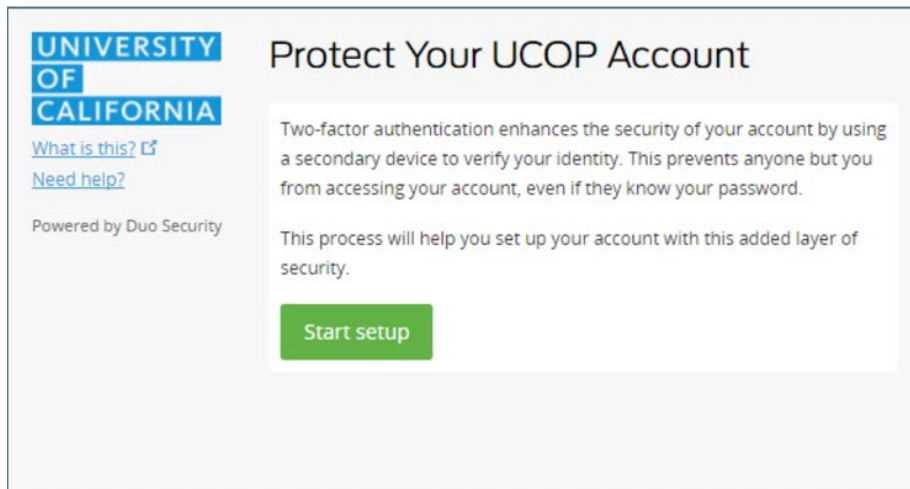
When it is time for you to start using MFA, you will receive an email from Duo Security similar to the following:



Note: as an additional precaution, you will be notified, by UCOP, the day before the Duo activation link is sent. Although you can install the Duo app at any time, it cannot be activated until the activation email is sent.

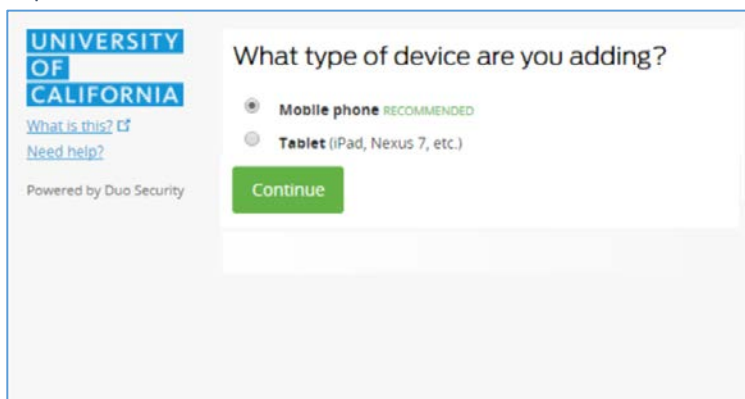
Click the first link in the email to begin the registration process. The link is valid for 30 days. If, for some reason, you do not click the activation link within 30 days, you can get another one by contacting the Service Desk.

The screens below show screens from iOS (iPhone) but the process for Android is similar. After clicking the link to start registration, you will see a screen similar to the following:



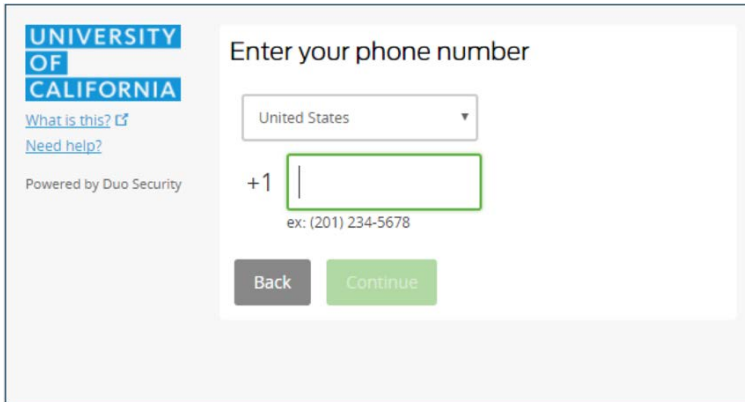
Follow these steps:

1. Tap the "Start setup" button.
2. Select the type of device you are going to use for MFA: Mobile Phone or Tablet, then click "Continue" to proceed.

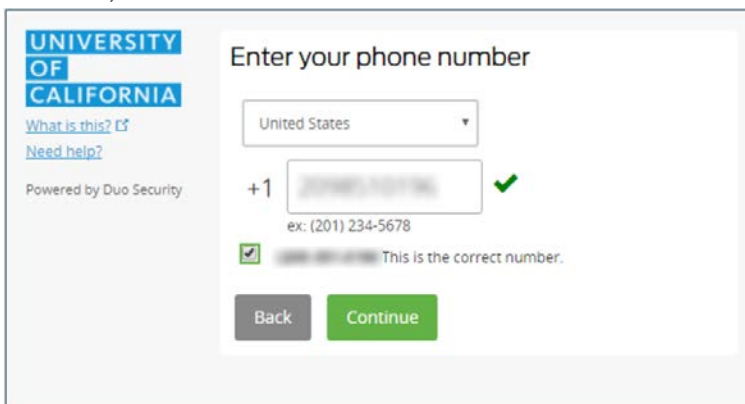


3. If you are registering a tablet, you will be asked to choose whether it is an iOS or Android tablet. After making a selection, skip to step 6. If you are registering a mobile phone, go to step 5.

4. Enter the phone number of the mobile device to use for Duo



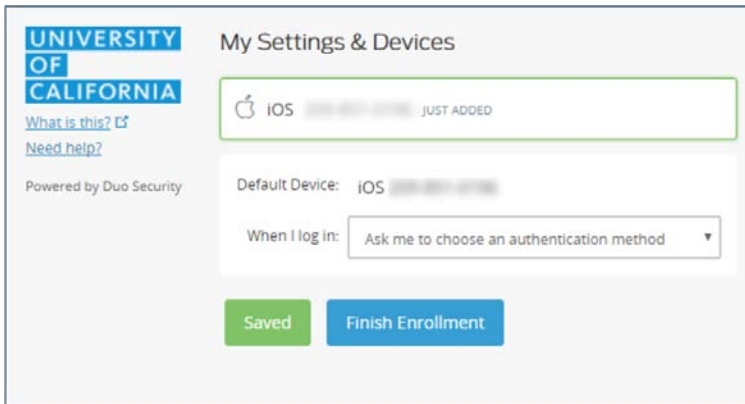
5. Confirm that the phone number you entered is correct by checking the “This is the correct number” checkbox, and then click “Continue”:



6. A QR code will appear on your **computer** screen (not your mobile device). Scan this code using the camera on your mobile device (smartphone or tablet). You may have to give Duo permission to use the camera on your device.

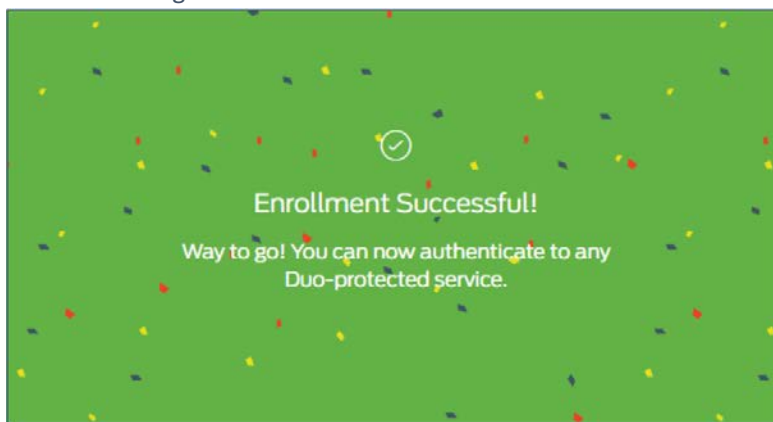


7. You will see a confirmation screen. Click “Finish Enrollment”.



The screenshot shows the 'My Settings & Devices' page for the University of California Duo. On the left, there is a sidebar with the University of California logo, links for 'What is this?' and 'Need help?', and the text 'Powered by Duo Security'. The main content area shows a list of devices with one iOS device listed as 'JUST ADDED'. Below this, there are settings for 'Default Device' (set to the same iOS device) and 'When I log in:' (set to 'Ask me to choose an authentication method'). At the bottom, there are two buttons: 'Saved' and 'Finish Enrollment'.

8. You are now registered in Duo!



Reactivating Duo if you Replace Your Mobile Device

Duo is “mapped” to a specific mobile device. If you get a new mobile phone, for example, but keep your phone number, Duo will no longer work on the new phone. There are three possible scenarios, listed below. Follow the one that fits your situation:

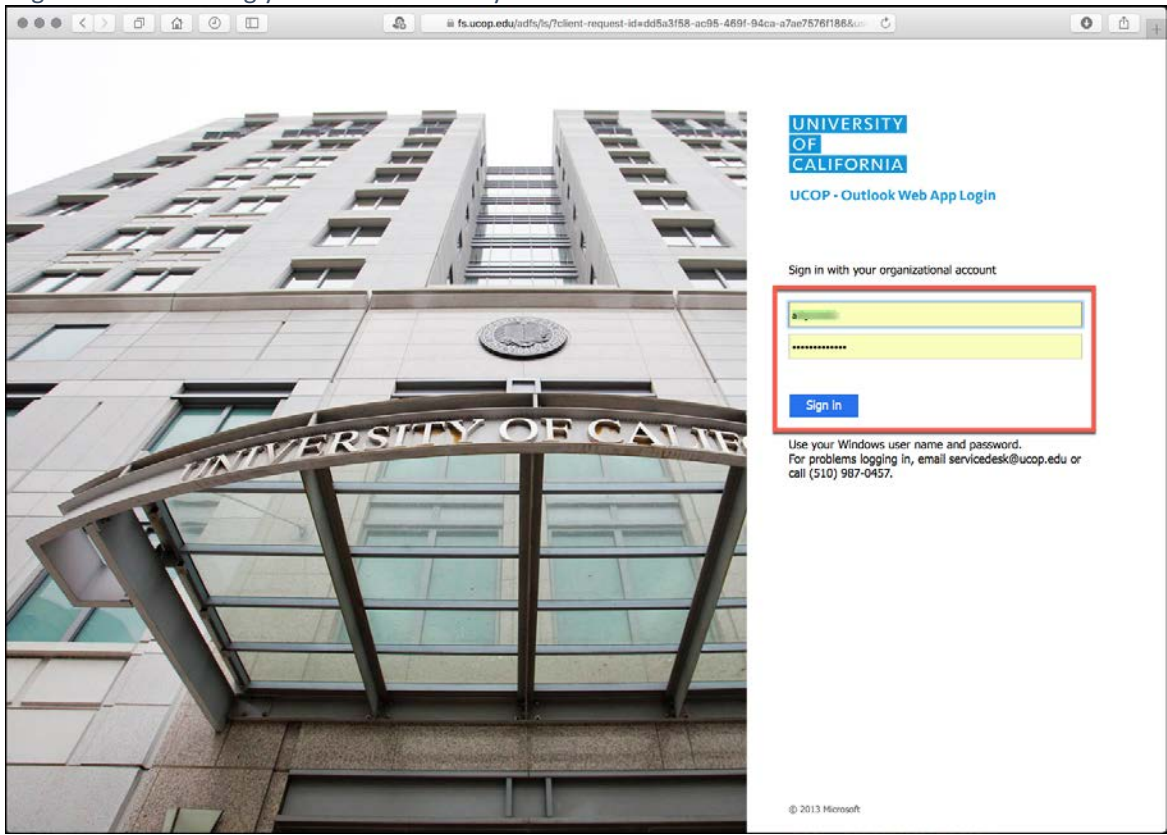
- If your new mobile phone has a different number than your current phone, follow the “Adding Another Device in Duo” instructions below **before** turning in or selling your current phone.
- If your new mobile phone has the same number as your current phone, and you are keeping your current phone (vs. turning it in to, for example, the Verizon store), follow the “Adding Another Device in Duo” instructions **before** turning in or selling your old phone.
- If you turn in your old mobile phone before or at the same time you receive your new phone, you will need to contact the Service Desk to have Duo reactivated. The Service Desk will reactivate Duo for you, and you will receive a text on your phone. Tap the link in the text and then follow the steps in the “Activating the Duo App on Your Smartphone” section of this document.

Adding Another Device in Duo

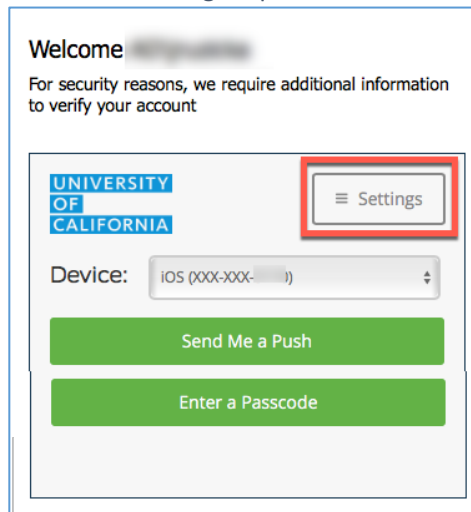
You can self-register a second device in Duo. To add an additional device, such as a second smartphone, follow these steps.

1. Go to any application that requires MFA, such as Microsoft Outlook Online (owa.ucop.edu).

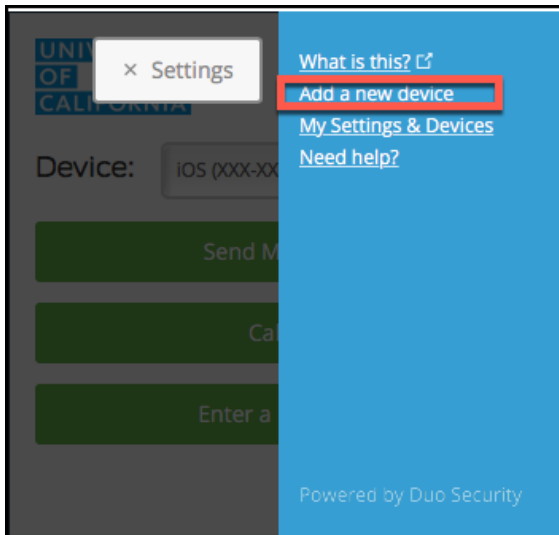
2. Log in as normal using your Active Directory User ID and Password



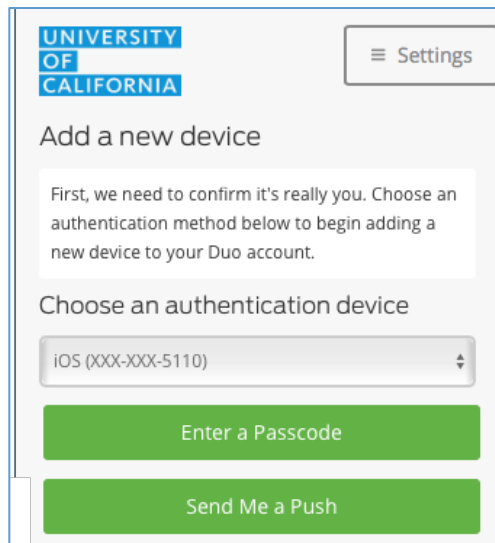
3. Select the "Settings" option:



4. Select “Add a new device”



5. You will be asked to authenticate using your current device. Select “Enter a Passcode” or “Send me a Push.”



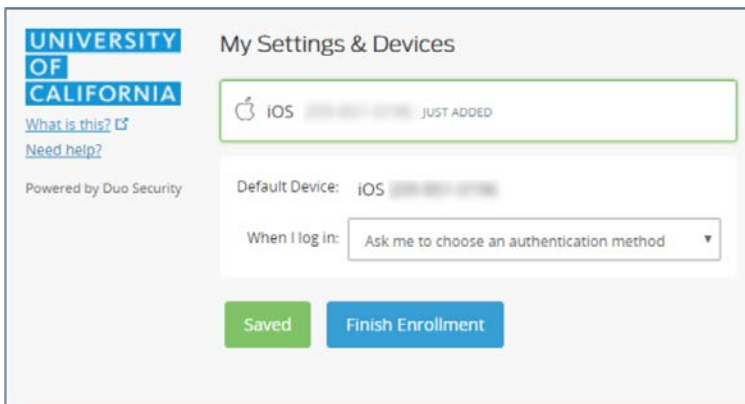
6. Respond to the Push on your **original** mobile device or enter the passcode.
7. Select “Tablet,” regardless of whether the second device you are adding is a phone or a tablet, then click “Continue” to proceed.



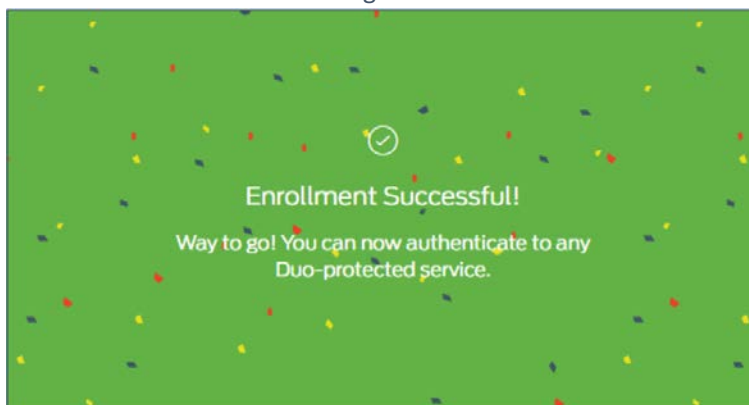
8. A QR code will appear **on your computer screen** (not on your mobile device). Scan this code using the camera on your mobile device (smartphone or tablet). You may have to give Duo permission to use the camera on your device.



9. You will see a confirmation screen. Click “Finish Enrollment”.



10. Your additional device is now registered in Duo!



Authenticating with Duo

Duo offers multiple ways to authenticate. Options available depend on the device used for authentication. They are:

- **Push:** Duo sends a “push” to the Duo app. You approve the MFA request by tapping “Approve” from the Duo app or from the home screen. iOS users can also approve using a fingerprint scan or facial recognition, if your iPhone supports it.
- **Passcode:** the Duo app, or a hardware token, shows a passcode. This code is entered on the login screen to approve the MFA login.
- **Bypass Code:** if you forget your mobile device, you can call the Service Desk and request a temporary passcode. You will need to verify your identity with the Service Desk by answering some security questions before they will issue you the code.
- **Travel Code:** if you are going to be travelling overseas and do not wish to incur international roaming charges, you can receive a travel code to use while abroad. This code should be requested, via ServiceNow, **at least** three business days before your planned travel. If you are going to be traveling abroad for a week or more, the Service Desk can temporarily issue you a hardware token to use while you travel.

Push

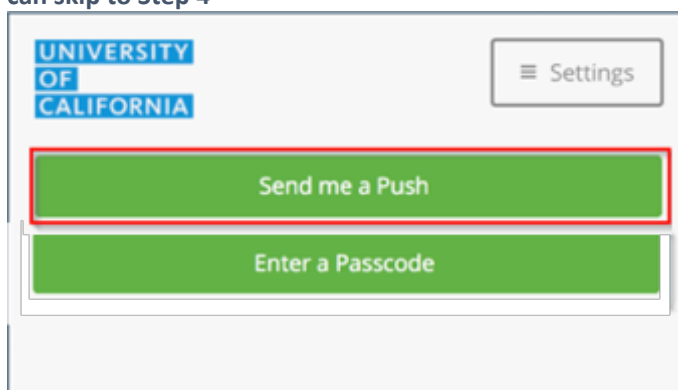
Push authentication is the easiest method to use and is the required method if you have a UCOP-issued mobile device. After entering your user ID and password, a message is sent to the Duo app that you are trying to login/authenticate.

The app makes a sound or vibrates, then you simply tap the “Approve” button on your smart device. **If you get this message and you are NOT trying to log in to an application, you should contact the Service Desk immediately as this means someone may be trying to fraudulently access a UCOP application!**

“Push” can be set up as the automatic default. See “Duo Settings” for more information.

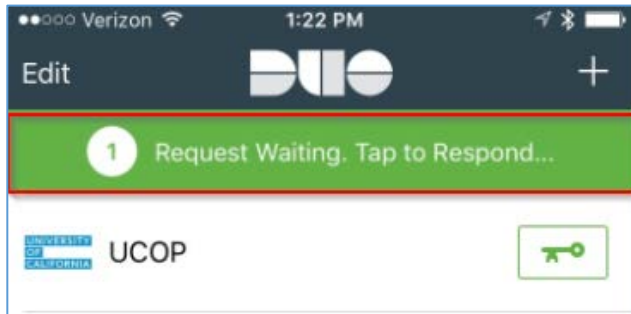
To use Push Authentication:

1. Log into a web application using your UCOP Active Directory ID and password
2. The Duo Authentication Method screen appears. **Note: if “Push” is set as the automatic default, you can skip to Step 4**

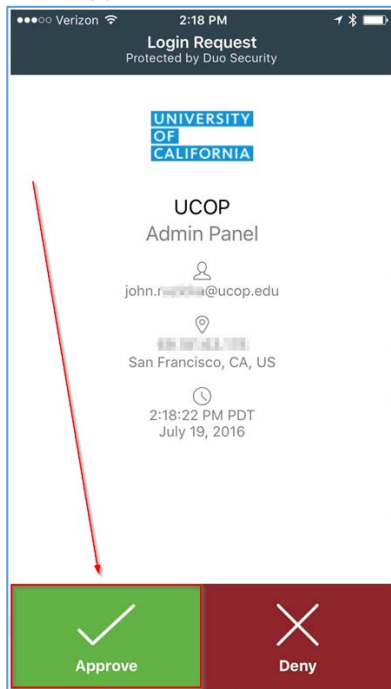


3. Click “Send me a Push.” Your phone will beep or vibrate, depending on how you have set up notifications.

4. Open the Duo App on your mobile phone or tablet or tap the notification that appears on the lock screen of your smartphone. Note: on most iOS and Android phones, you can authenticate directly from the home screen by swiping left when the Duo message appears.
5. In the Duo app, a green bar at the top of the app indicates that you have a request waiting. Tap on the green bar. **Note: the Push times out after one minute. If more than one minute passes between the time you login and when you open the Duo app, you will have to select “Send Me a Push” a second time.**



6. Click “Approve.”



7. You may see a message similar to the following from certain systems, such as TRS. If so, check “Do not ask me again for this site” and then click “Permit Use”:



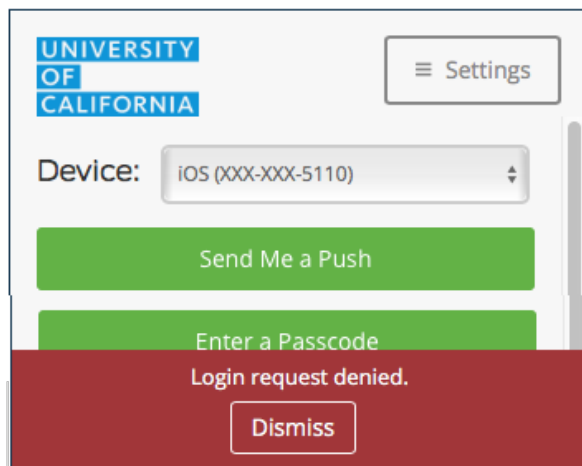
If “Deny” is Tapped

Note: if you tap “Deny,” the login will be cancelled, and the Duo mobile app will ask for a reason you chose Deny. The choices are:

- It seems fraudulent
- It was a mistake

At this time, there is no difference between the two selections. Both cancel the login. However, **if you suspect a fraudulent attempt to access an application, call the Service Desk immediately!**

You will see a screen similar to the following:

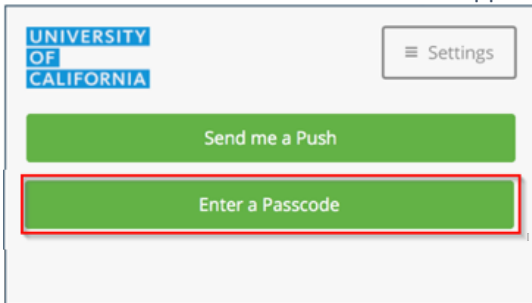


Tap dismiss to try again. There is no limit to the number of attempts to use MFA, i.e. your Duo MFA account will not be locked or disabled after any number of failed attempts.

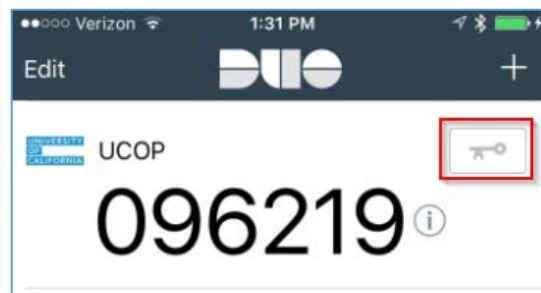
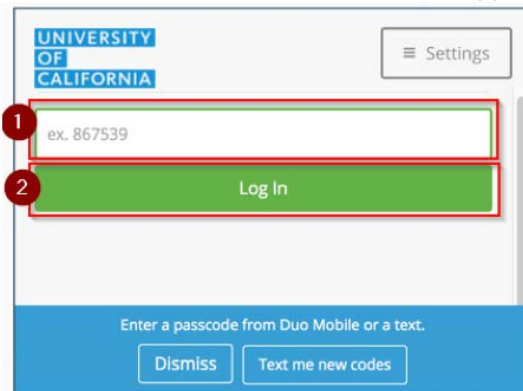
Passcode

If your smart device is not connected to the internet, you can still use Duo by selecting the “Enter a Passcode” method. **Note: “Send Me a Push” is the preferred, and easiest, method for users with internet-connected smart devices.**

1. Log into a web application using your UCOP Active Directory ID and password
2. The Duo Authentication Method screen appears



3. Select “Enter a passcode”
4. An input box appears on the computer screen. Open the Duo app on your smartphone or tablet and tap on the key icon to reveal the one-time use passcode, or press the green button your token to reveal the code. Enter the code from the app into this screen and then click “Log In.”



Travel Code

If you plan to travel, Duo Mobile is still the preferred method for authenticating. If you are going to be overseas and don't want to incur roaming charges, call the Service Desk or open a ticket in ServiceNow **at least** three business days before your planned travel.

The Service Desk will generate a travel code for use during your trip. If your trip is a week or more they will arrange for you to receive a hardware token to use during your trip.

Hardware Tokens

If you have a UCOP-issued smartphone, you are required to use the Duo Mobile app. If you do not wish to use the Duo app on a personal mobile device, you can ask your manager to obtain a hardware token for you.

Note: before choosing the token option, keep in mind that the Duo App is easier to use. The Duo app does not track your movements in any way. It does not send any messages, advertising, or spam to your personal smartphone. It only sends notifications when you have attempted to login to an app that requires MFA.

Your manager should create a ServiceNow request for a token. Once your request is approved, you can pick up your hardware token at the Service Desk at 1111 Franklin Street or make alternative arrangements for pickup with the Service Desk.

Important: do not press the green button multiple times, or the hardware token can become out-of-sync. Do not store the token in a place where the green button may be repeatedly pressed multiple times by accident, such as in a backpack. If your token becomes out-of-sync, contact the Service Desk and they will help you to re-sync it.

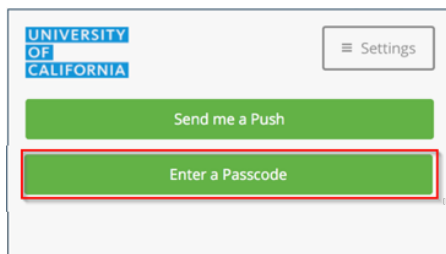
The Service Desk will register and activate the token for you.

Hardware tokens look like this:

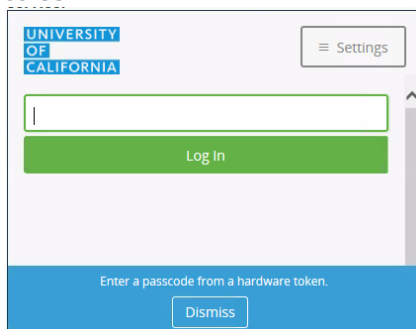


To use the token:

1. Log into a web application using your UCOP Active Directory ID and password.
2. The Duo authentication method screen appears:



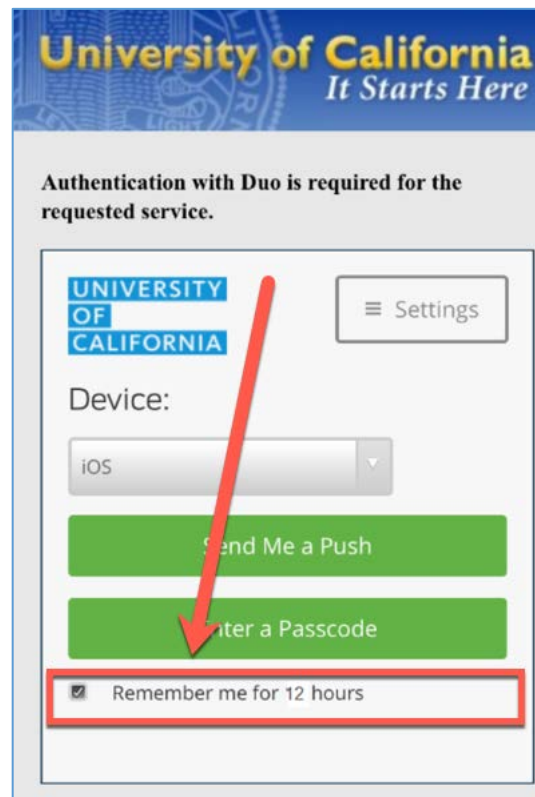
3. Select "Enter a passcode." Press the green button on the token and enter the code on the login screen:



Note: the code on the hardware token changes frequently. If you wait too long to enter the code, it may have already expired. In that case, simply push the green button on the token to get another code.

Using the “Remember Me” Option

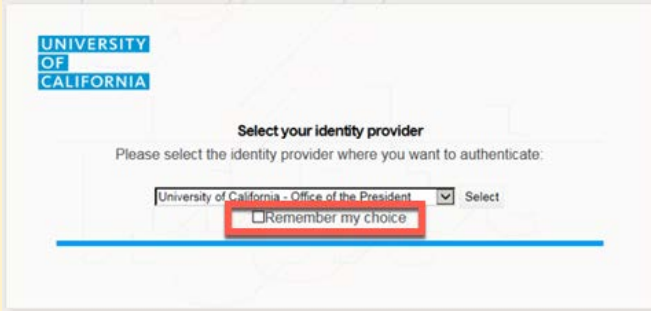


After using Duo for a while, you will probably notice that, if you close your browser, you have to reauthenticate again the next time you open it, even if a full workday has not passed. To have Duo remember you for a full 12 hours, check the “Remember me for 12 hours” box **before** you choose “Send Me a Push” or “Enter a Passcode.”



“Remember me” is a setting unique to each browser. If, for example, you switch from Internet Explorer to Firefox in the middle of the day, you will need to re-authenticate with Duo. **Note: some applications, such as UCPATH, require Single Sign-On credentials each time you log in to them. “Remember me” does NOT override these application-specific settings.**

Also, “Remember me” is specific to you. If another person uses your computer to log in, they will have to authenticate with Duo even if you previously selected “Remember me for 12 hours.”

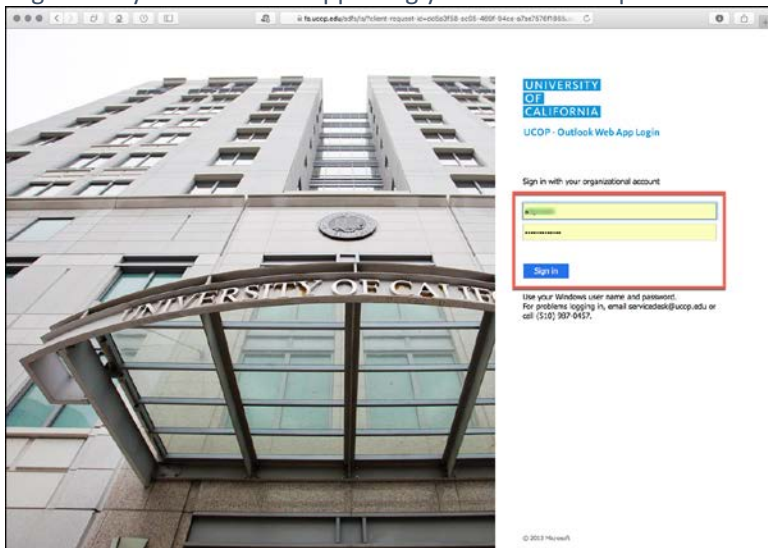
Note: “Remember me for 12 hours” is unique to Duo. Selecting any of the other “Remember me” options, such as a location setting or browser password, does not affect this setting for Duo. The chart below explains various options when logging in and what they mean:

Item	What it means
	<p>Select Your identity provider</p> <p>Selecting “Remember my choice” on this screen tells your browser to remember your physical location—such as UCOP or a specific campus—so you won’t have to enter it the next time you log in.</p> <p>This option does not remember your ID or password and does not affect Duo.</p>
	<p>Would you like to store your password for ucop.edu?</p> <p>Selecting “Yes” to this prompt tells your browser to remember your password when you visit the same web site again.</p> <p>This option does not affect Duo.</p>
	<p>Remember me for 12 hours</p> <p>Checking this box after the Duo MFA prompt appears tells Duo to remember you for 12 hours, even if you close and reopen your browser. Note that some applications, such as UCPath, require your UCOP credentials every time you log in regardless of whether you have checked this box.</p>

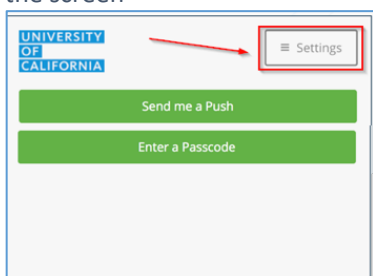
Duo Settings

When logging into an application that uses Duo, it is possible to change your settings. **Note that there is no way to access settings without initiating a Duo login request, i.e. you must go to application that requires MFA to see the “Settings” button.**

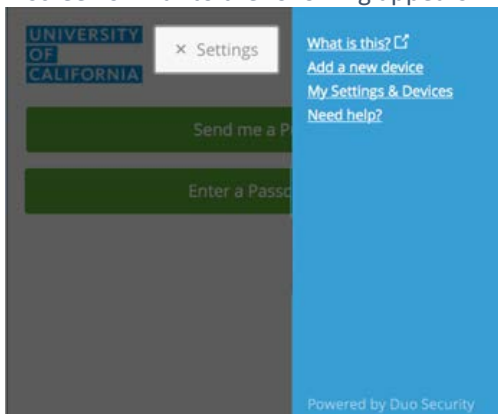
1. Log into any MFA-enabled app using your user ID and password:



2. When the Duo authentication choice screen appears, click the “Settings” button in the upper right of the screen



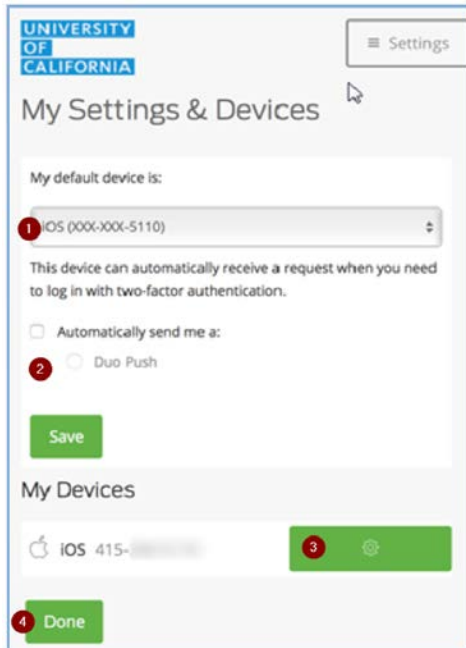
3. A screen similar to the following appears:



4. To add a new device, click the “Add a new device” link. See the instructions earlier in this manual to add a second device. To view or modify current settings, click “My Settings & Devices.” The “What is this?” and “Need help?” links take you to Duo’s web site where additional help is available

Modifying An Existing Duo Configuration

1. After clicking the “My Settings & Device” link, a screen similar to the following appears:











2. If you have more than one device configured to use Duo, the default device can be selected from the dropdown labeled “1” in the screenshot above.
3. To use automatic authentication, click “Automatically send me Duo Push.” Once this option is selected, it will no longer be necessary to choose an authentication method each time authentication is required. Click “Save” to save the changes (see number “2” above).
4. To edit information about a current device, click the “Gear” icon next to that device (see number “3” above).
5. Click “Done” (see number “4” above) when finished to save any changes (see number 4 above).


Appendix A – Eight Smart Cybersecurity Habits

MFA is one piece of UCOP's cybersecurity initiative. The guide below shows smart cybersecurity habits to use at UCOP, and in daily life.

8 SMART CYBERSECURITY HABITS

Learn more at:
<https://security.ucop.edu/resources/security-awareness/habits.html>

1		Think twice before clicking on links or opening attachments.	5		Keep your devices, browsers and apps up to date.
2		Verify requests for private information.	6		Back up critical files.
3		Protect your passwords.	7		Delete sensitive information when it's no longer needed.
4		Protect your stuff. Lock it up or take it with you.	8		If it's suspicious, report it!



GETTING HELP

IT Service Desk
ucop.service-now.com
ServiceDesk@ucop.edu
510-987-0457

BUILDING SECURITY

Franklin
510-987-9700

Kaiser
510-271-6131

20th St.
510-987-0020

Broadway
510-267-1124

UNIVERSITY
OF
CALIFORNIA

Information
Security
Awareness