# 2-Step Verification

## Table of Contents

- **Introduction** ......................................................................................................................... 2
- **Enrolling in 2-Step Verification** ............................................................................................. 2
- **Registering Your Device** ......................................................................................................... 2  
  - Mobile Phone .......................................................................................................................... 3
  - Tablet .......................................................................................................................................... 6
  - Landline ...................................................................................................................................... 8
  - Hardware Token ......................................................................................................................... 9
- **Authenticating with Your Device** .......................................................................................... 9  
  - Push Notification ..................................................................................................................... 10
  - Passcode .................................................................................................................................... 12
  - Phone Call ............................................................................................................................... 13
- **Managing Your Devices** ......................................................................................................... 13  
  - Registering Additional Devices ............................................................................................... 15
  - Deleting Devices ...................................................................................................................... 15
  - Reactivating Duo Mobile ......................................................................................................... 16
- **Getting Help** ........................................................................................................................... 17

For additional training resources, visit [www.calstatela.edu/training](http://www.calstatela.edu/training).
Introduction

2-Step Verification adds an extra layer of security to your MyCalStateLA ID account by using two types of authentication to verify your identity. In addition to your username and password, 2-Step Verification requires a physical device that you control, such as your mobile phone or tablet, to complete the login process. This prevents anyone but you from accessing your account, even if they know your password. This handout covers how to enroll in 2-Step Verification, register and authenticate with your device, manage your devices, and get help.

Enrolling in 2-Step Verification

You can enroll in 2-Step Verification using your MyCalStateLA ID account.

To enroll in 2-Step Verification:
1. Visit the 2-Step Verification website, and then click the Sign Me Up button.
2. Log in with your MyCalStateLA ID account.
3. Once logged in, click the Confirm button. Within 24 hours, you will receive an email message with information on how to complete the enrollment process and register your device.
4. Follow the steps in the Registering Your Device section of this handout.

Registering Your Device

Once you enroll in 2-Step Verification, you need to register at least one device. There are several devices that you can use. Each device has one or more methods that can be used to authenticate (see Table 1).

Table 1 – Supported Devices

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Authentication Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smartphone</td>
<td>• Duo Mobile push notification (recommended)</td>
</tr>
<tr>
<td></td>
<td>• Duo Mobile passcode</td>
</tr>
<tr>
<td></td>
<td>• Text message passcode</td>
</tr>
<tr>
<td></td>
<td>• Phone call</td>
</tr>
<tr>
<td>Tablet</td>
<td>• Duo Mobile push notification</td>
</tr>
<tr>
<td></td>
<td>• Duo Mobile passcode</td>
</tr>
<tr>
<td>Basic mobile phone</td>
<td>• Text message passcode</td>
</tr>
<tr>
<td></td>
<td>• Phone call</td>
</tr>
<tr>
<td>Landline</td>
<td>• Phone call</td>
</tr>
<tr>
<td>Hardware token</td>
<td>• Passcode</td>
</tr>
</tbody>
</table>

To register your device:
1. Log in to the MyCalStateLA Portal with your MyCalStateLA ID account (see Figure 1).
2. The 2-Step Verification Welcome screen appears (see Figure 2). Scroll down and click the Start setup button.
3. The Choose Your Device screen appears. Follow the steps in the Mobile Phone, Tablet, or Landline section of this handout to register your device.

NOTE: You cannot self-register a hardware token. For more information, see the Hardware Token section of this handout.
Mobile Phone
You can use a mobile phone as your authentication device. It lets you authenticate with a phone call or a passcode sent to you via text message. If you have a smartphone, you can install the Duo Mobile app which lets you authenticate with a push notification or a passcode generated by the app.

To register a mobile phone:
1. On the Choose Your Device screen, select the Mobile phone option button, and then click the Continue button (see Figure 3).
2. On the Enter Your Phone Number screen, select United States from the Country drop-down list, type your phone number in the Phone Number box, select the check box to confirm that it is the correct number, and then click the Continue button (see Figure 4).

![Figure 4 – Enter Your Phone Number Screen](image)

3. On the Choose Your Platform screen, do one of the following:
   - If you are registering a smartphone, select the appropriate platform (iPhone, Android, BlackBerry, Windows Phone), and then click the Continue button (see Figure 5).
   - If you are registering a basic mobile phone, select the Other option button, and then click the Continue button (see Figure 6). Skip to step 6.

![Figure 5 – Choose Your Platform Screen with iPhone Selected](image)  ![Figure 6 – Choose Your Platform Screen with Other Selected](image)

4. On the Install Duo Mobile screen, follow the platform-specific instructions to install the Duo Mobile app on your smartphone (see Figure 7). After installing the app, return to the Install Duo Mobile screen, and then click the I have Duo Mobile button.
5. On the Activate Duo Mobile screen, follow the platform-specific instructions to activate the Duo Mobile app on your smartphone (see Figure 8). After an account named California State University, Los Angeles appears in your Duo Mobile app (see Figure 9), return to the Activate Duo Mobile screen, and then click the Continue button.

6. Your phone is added to the device list on the My Settings & Devices screen and is now ready to approve authentication requests (see Figure 10 and Figure 11). Click the Continue to Login button, and then follow the steps in the Authenticating with Your Device section of this handout to authenticate.
Tablet

You can use a tablet as your authentication device. To do so, you need to install the Duo Mobile app which lets you authenticate with a push notification or a passcode. The app can generate passcodes even when your tablet is offline.

To register a tablet:
1. On the Choose Your Device screen, select the Tablet option button, and then click the Continue button (see Figure 12).
2. On the Choose Your Platform screen, select the appropriate platform, and then click the Continue button (see Figure 13).
3. On the Install Duo Mobile screen, follow the platform-specific instructions to install the Duo Mobile app on your tablet (see Figure 14). After installing the app, return to the Install Duo Mobile screen, and then click the I have Duo Mobile button.

4. On the Activate Duo Mobile screen, follow the platform-specific instructions to activate the Duo Mobile app on your tablet (see Figure 15). After an account named California State University, Los Angeles appears in your Duo Mobile app, return to the Activate Duo Mobile screen, and then click the Continue button.

5. Your tablet is added to the device list on the My Settings & Devices screen and is now ready to approve authentication requests (see Figure 16). Click the Continue to Login button, and then follow the steps in the Authenticating with Your Device section of this handout to authenticate.
**Landline**

You can use a landline, such as your office phone, as your authentication device. When authenticating with a landline, you receive an automated phone call that requires you to press any key on your phone to authenticate.

**To register a landline:**

1. On the **Choose Your Device** screen, select the **Landline** option button, and then click the **Continue** button (see Figure 17).

![Figure 17 – Choose Your Device Screen with Landline Selected](image)

2. On the **Enter Your Phone Number** screen, select **United States** from the **Country** drop-down list, type your phone number in the **Phone Number** box, type your extension (if applicable) in the **Extension** box, select the check box to confirm that it is the correct number, and then click the **Continue** button (see Figure 18).

![Figure 18 – Enter Your Phone Number Screen](image)

3. Your landline is added to the device list on the **My Settings & Devices** screen and is now ready to approve authentication requests (see Figure 19). Click the **Continue to Login** button, and then follow the steps in the **Authenticating with Your Device** section of this handout to authenticate.
Hardware Token

You can use a hardware token as your authentication device. Tokens generate and display a six-digit passcode at the push of a button. Tokens are available at no cost to Cal State LA students, faculty, and staff, and can be requested by visiting the ITS Help Desk in the Library Palmer Wing Lobby. You must present a valid identification to be assigned a pre-registered token.

Authenticating with Your Device

Each time you log in to a system that requires 2-Step Verification, the Authentication screen appears and prompts you to verify your identity using one of the available methods (see Figure 20 and Table 2). If you have more than one device registered in 2-Step Verification, the Authentication screen includes a Device drop-down list which lets you choose the device you want to use before choosing an authentication method (see Figure 21).
Table 2 – Authentication Methods

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send Me a Push</td>
<td>This method is available for smartphones and tablets, and requires you to first install and activate the Duo Mobile app on your device. A push notification is sent to your device and you just tap Approve to authenticate.</td>
</tr>
<tr>
<td>Call Me</td>
<td>This method is available for all mobile phones and landlines. You receive an automated phone call that requires you to press or tap any key on your phone to authenticate.</td>
</tr>
<tr>
<td>Enter a Passcode</td>
<td>This method is available for mobile phones, tablets, and hardware tokens. You authenticate using a passcode generated by the Duo Mobile app or a hardware token, or sent via text message.</td>
</tr>
</tbody>
</table>

**Push Notification**

If you are authenticating with a smartphone or tablet, **Send Me a Push** is the recommended method because it is the easiest and quickest way to authenticate. A push notification is sent to your device and you just tap **Approve** to authenticate.

To authenticate with a push notification:

1. On the **Authentication** screen, do the following (see Figure 22):
   - If you have more than one device registered in 2-Step Verification, select the device (smartphone or tablet) that you want to use from the **Device** drop-down list.
   - Click the **Send Me a Push** button. A login request is pushed to your device.

   **NOTE:** The status bar located at the bottom of the **Authentication** screen updates at each step of the process.

   ![Figure 22 – Send Me a Push Button on the Authentication Screen](image)

2. Open the **Duo Mobile** app on your smartphone or tablet, and then tap the **Request Waiting** message at the top of the screen (see Figure 23).
3. Review the request, and then tap **Approve** to authenticate (see Figure 24).
NOTE: If you receive a login request that you were not expecting, tap **Deny** to reject the request. You will be given the opportunity to report it as fraudulent, or you can tap **It was a mistake** to deny the request without reporting it.

![Figure 23 – Duo Mobile App with Request Waiting Message (iPhone)](image)

![Figure 24 – Duo Mobile App with Login Request (iPhone)](image)

NOTE: You can also respond to login requests from the iOS lock screen or banner notification starting with Duo Mobile version 3.8. When your screen is locked, swipe left on the Duo Mobile lock screen notification, and then approve or deny the request (see Figure 25). When your screen is unlocked, swipe down on the Duo Mobile banner notification, and then approve or deny the request (see Figure 26).

![Figure 25 – Duo Mobile Lock Screen Notification (iPhone)](image)
If you select **Enter a Passcode** as your authentication method, you can authenticate using a passcode generated by the Duo Mobile app or a hardware token, or sent via text message. Each passcode can be used only once.

### To authenticate with a passcode:

1. On the **Authentication** screen, do the following (see Figure 27):
   - If you have more than one device registered in 2-Step Verification, select the device (mobile phone, tablet, or hardware token) that you want to use from the **Device** drop-down list.
   - Click the **Enter a Passcode** button. The **Passcode** box appears (see Figure 28).

   **NOTE:** The status bar located at the bottom of the **Authentication** screen updates at each step of the process.

2. Do one of the following:
   - To use a passcode from **Duo Mobile**, open the **Duo Mobile** app on your smartphone or tablet, and then tap the key icon to generate a new passcode (see Figure 29).
   - To use a passcode from a text message, click the **Text me new codes** button at the bottom of the **Authentication** screen to get a list of passcodes texted to your mobile phone (see Figure 28).
   - To use a passcode from a hardware token, press the button on your hardware token to generate a new passcode (see Figure 30).
NOTE: Tokens can get out of sync if the button is pressed too many times in a row and the generated passcodes are not used for login. If your token stops working, contact the ITS Help Desk at 323-343-6170 for assistance. They will ask you to generate three passcodes in a row so they can attempt to resynchronize your token.

3. On the Authentication screen, enter the passcode from the Duo Mobile app, hardware token, or text message in the Passcode box, and the click the Log In button (see Figure 28).

Figure 29 – Key Icon in the Duo Mobile App (iPhone)

Phone Call

2-Step Verification works with all mobile phones and landlines by supporting authentication via phone call. If you select Call Me as your authentication method, you receive an automated phone call that requires you to press or tap any key on your phone to authenticate.

To authenticate with a phone call:

1. On the Authentication screen, do the following (see Figure 31):
   - If you have more than one device registered in 2-Step Verification, select the device (mobile phone or landline) that you want to use from the Device drop-down list.
   - Click the Call Me button. A call is placed to the selected phone.
   
   NOTE: The status bar located at the bottom of the Authentication screen updates at each step of the process.

2. Answer the phone, listen to the instructions, and then press or tap any key on the phone to authenticate.

Figure 31 – Call Me Button on the Authentication Screen

Managing Your Devices

2-Step Verification includes a self-service portal that allows you to manage your authentication devices. You can use it to register additional devices as well as edit or delete your registered devices.
To manage your devices:

1. Log in to the MyCalStateLA Portal with your MyCalStateLA ID account, and then click the Settings button in the upper-right corner of the Authentication screen (see Figure 32).
2. On the Settings menu, click the My Settings & Devices link (see Figure 33).
3. On the My Settings and Devices Authentication screen, select the desired authentication device and method, and then approve the authentication request using your device (see Figure 34). The My Settings & Devices screen appears (see Figure 35). Follow the steps in the Registering Additional Devices, Deleting Devices, or Reactivating Duo Mobile section of this handout to manage your devices.
Registering Additional Devices

It is recommended to register at least two devices in 2-Step Verification as a backup in case the device you normally use to authenticate is lost or unavailable.

To register additional devices:
1. On the My Settings & Devices screen, click the Add another device link located below the device list (see Figure 36).
2. On the Choose Your Device screen, select the desired option, and then follow the on-screen prompts to register your new device (see Figure 37). For step-by-step instructions, see the Mobile Phone, Tablet, or Landline section of this handout.

Deleting Devices

If needed, you can delete a device that you registered in 2-Step Verification.

NOTE: If you only have one device registered in 2-Step Verification, you cannot delete it. If you want to delete your last device, first add another device, and then delete the original.

To delete a device:
1. On the My Settings & Devices screen, click the Device Options button next to the device that you want to delete, and then click the Delete Device button on the menu that appears (see Figure 38).
2. The Delete Device pop-up window opens asking you to confirm. Click the Remove button (see Figure 39).
3. A message appears at the bottom of the **My Settings & Devices** screen indicating that the device was successfully deleted. Click the **Dismiss** button (see Figure 40).

### Reactivating Duo Mobile

If you delete the Duo Mobile app from your smartphone or tablet, or you get a new smartphone but keep the same phone number, you need to reactivate Duo Mobile on your device.
To reactivate Duo Mobile:

1. On the My Settings & Devices screen, click the Device Options button next to the device that you want to reactivate, and then click the Reactivate Duo Mobile button on the menu that appears (see Figure 41).
2. On the Choose Your Platform screen, select the appropriate platform, and then follow the on-screen prompts to reactivate Duo Mobile (see Figure 42). For step-by-step instructions, see the Mobile Phone or Tablet section of this handout.

Getting Help

If you need assistance with enrolling in 2-Step Verification or managing your devices, please contact the ITS Help Desk at 323-343-6170 or helpdesk@calstatela.edu.