

Two – Factor Authentication

Two-factor authentication makes your account more secure by requiring an additional piece of information beyond your username and password. When you log into any service setup with Colorado State University's single sign-on, you will use your mobile device to provide an additional layer of security to your account. This is done by using the Duo Security app or by receiving a phone call.

Setting up Two – Factor Authentication for a Mobile Device or Landline

In order to use the Two-Factor Authentication, a user must have an active eID and will need to enroll by logging into the CSU eID website at <https://eid.colostate.edu> .

In addition to the CSU eID enrollment, activation for the Smart Device will require the download of the Duo Mobile App.

Download the Duo Mobile App from the App store or from the links below for a smartphone.

[iPhone](#)

[Android](#)

[Windows Phone](#)

Enroll using the CSU eID Website:

Click on the Show My Information link in the left navigation.

eIdentity
● YOUR CSU ELECTRONIC ID

Colorado State University

+ Get an eID
Register For Your eID

Modify Your eID
↓ These trigger a login

Show My Information

Change ePassword

Change E-mail Address

Change *Forgotten Password* Help Questions

List My Personal Website

eID: Colorado State University's electronic ID system

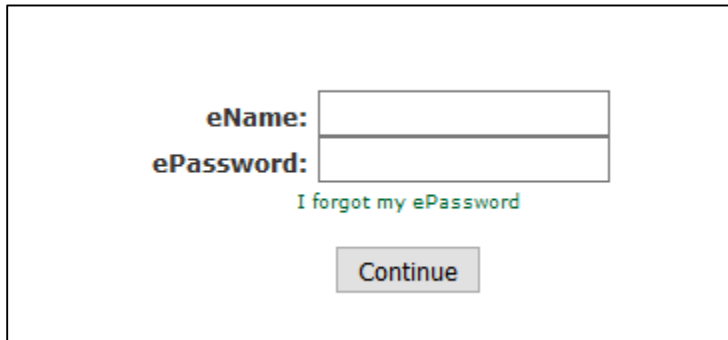
Every CSU student and employee must have an eID

New to the University?

New students, faculty and staff need an eID. Choose [Register for your eID](#) from the navigation area to set one up. The process is simple: first we will ask a few identification questions, then you will pick a password and other details, and your eID will be created.

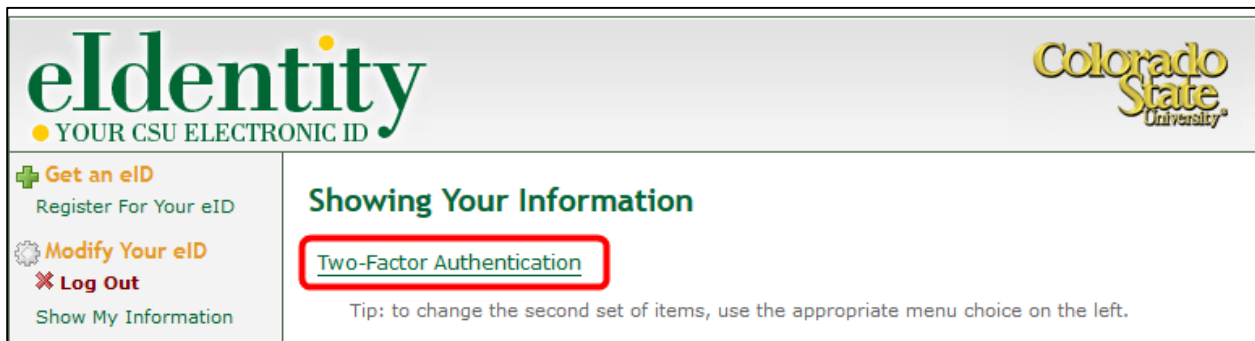
Already have your eID?

Login with the ename and epassword:



A login form with two input fields. The first field is labeled "eName:" and the second is labeled "ePassword:". Below the password field is a link that says "I forgot my ePassword". At the bottom of the form is a button labeled "Continue".

Once logged in to eID, the Two-Factor Authentication link will display at the top of the Show My Information page. Select the Two-Factor Authentication link to start the enrollment process.



The eIdentity dashboard header includes the "eIdentity" logo and "YOUR CSU ELECTRONIC ID" on the left, and the "Colorado State University" logo on the right. A left sidebar contains menu items: "Get an eID", "Modify Your eID", "Log Out", and "Show My Information". The main content area is titled "Showing Your Information" and features a red-bordered link for "Two-Factor Authentication". A tip below the link reads: "Tip: to change the second set of items, use the appropriate menu choice on the left."

The first step in the enrollment process is to Opt in and Enable the Two Factor Authentication. Opt in by selecting the Enable Two-Factor Authentication check box and clicking on Save.



The eIdentity dashboard header is the same as in the previous image. The left sidebar now includes "Show My Information" and "Change ePassword". The main content area is titled "Two-Factor Authentication" and contains a paragraph explaining the security benefits. Below this is an "Opt In" section with a red-bordered box containing a checked checkbox for "Enable Two-Factor Authentication" and a "Save" button.

The next step in the Two-Factor enrollment process is to add the device that will be used for the authentication. .

Insert a Device Name, a unique name that helps identify the device being used for the authentication. For example, Cam the Ram's iPhone ..

Two-Factor Device Management

Add Device

Device Name: Cam the Ram iPhone

Phone Number: 9999999999

Extension:

Type: Please select a type

Platform: Please select a platform

Save Cancel

The Device Name can be anything.

Devices being added must have a dedicated phone line.

Select the type of device that will be used for the Two-Factor Authentication.

Type: Please select a type

landline

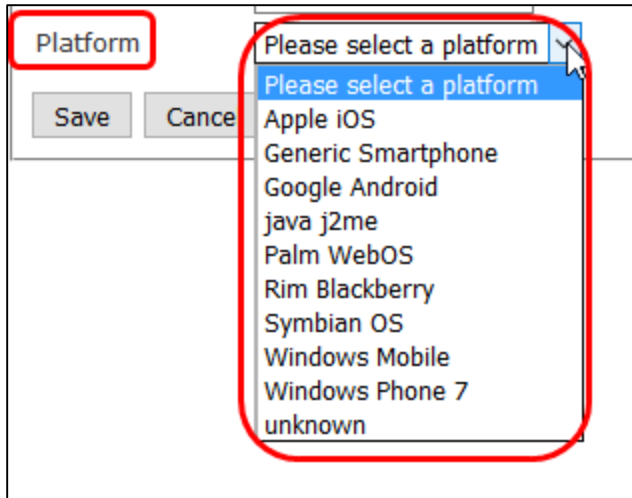
mobile

unknown

Save Cancel

Mobile: iPhone, Android, etc.
Landline: office or home phone
iPads: Not Supported

Select the platform for the device that will be used for the Two-Factor Authentication.



iPhone: select Apple IOS
Android: select Google Android
iPads: Not Supported

Next, click the Save button to save the device information.

A screenshot of a web form titled "Two-Factor Device Management". The form is titled "Add Device" and contains the following fields: "Device Name" with the value "Cam the Ram iPhone", "Phone Number" with the value "9999999999" and a secondary "9999999999" value, "Extension" (empty), "Type" with a dropdown menu set to "mobile", and "Platform" with a dropdown menu set to "Apple iOS". At the bottom of the form, there are "Save" and "Cancel" buttons. The "Save" button is highlighted with a red box.

The Duo Mobile App must be downloaded and installed on the mobile device in order to complete the Two-Factor activation process.

Download the Duo Mobile App from the App store or from the links below:

[iPhone](#)

[Android](#)

[Windows Phone](#)

Note: If using a landline or non-smart device, then the activation is complete.


Final Activation Step from Mobile Device

Once the App has been downloaded to the device, the QR code (the black and white image code) displayed on the Two-Factor Device Activation screen will need to be scanned in order to activate and link the device to your account.

Two-Factor Device Activation

Device Name	Number	Platform
Cam the Ram iPhone	9999999999	Apple iOS

Once created, devices need to be linked to your account. Launch the Duo Mobile App on your device, click the "+" icon at the top right, then scan the image below.



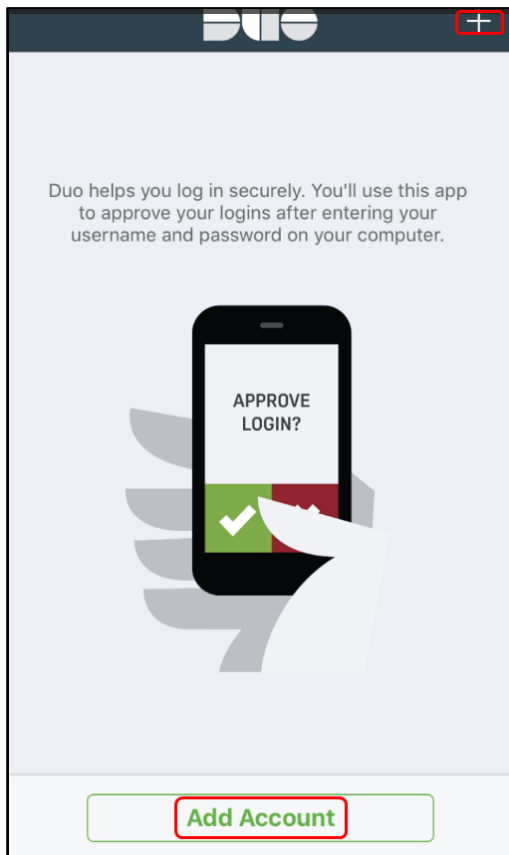
Final screen if using a Smart Device.

[Return](#)

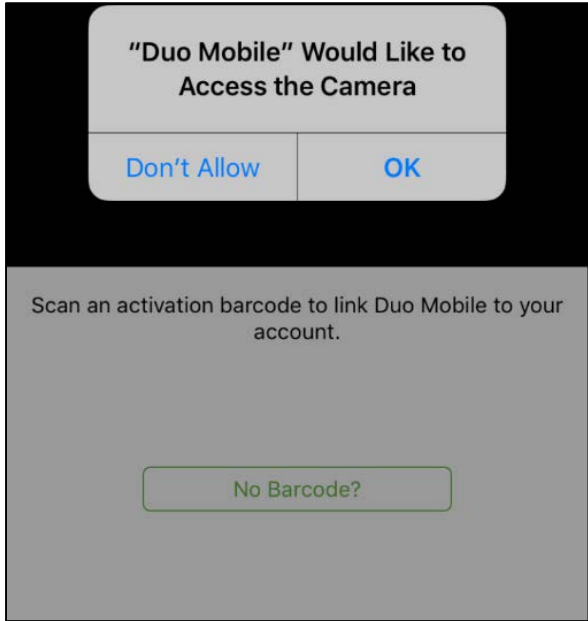
After installing the Duo Mobile App, launch the app on the device in order to complete the final activation.

The Duo Mobile App will display a message asking to allow notifications to be sent to the device. Select OK to allow notifications.

Once notifications have been allowed, an account will need to be added. Click on the Plus sign (+) located in the upper right corner or the Add Account button at the base of the screen to add an account.



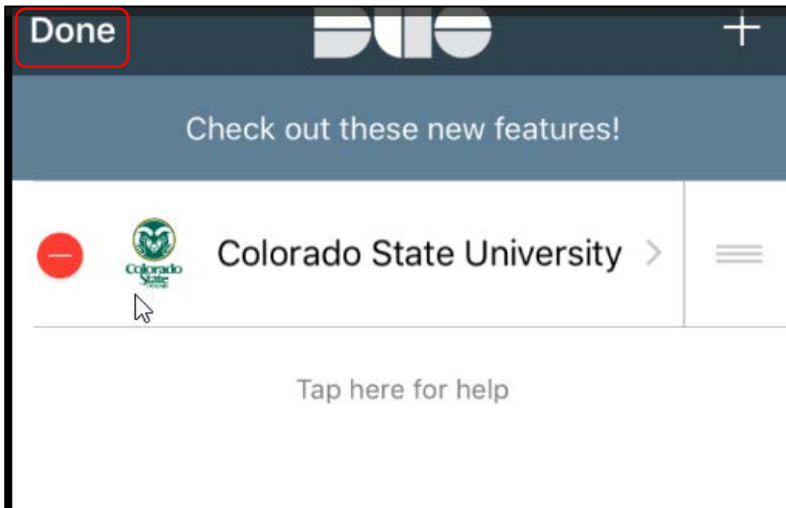
Allow Duo Mobile to Access the Camera by clicking on the OK button.



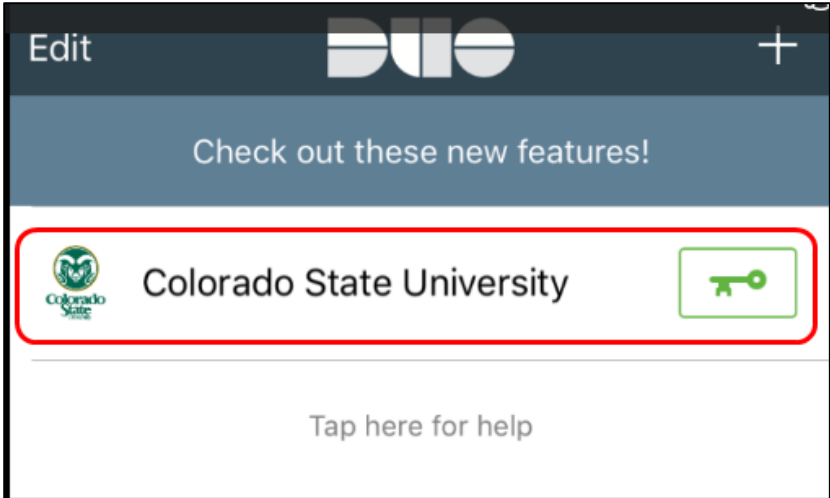
Note: depending on the smart device, the message on the app can vary, slightly.

Next, hold the smart device up to the QR code so the camera can scan the QR code displayed on the Two-Factor Device Activation screen.

Select the Done button in the upper left corner of the mobile device to close the Add Duo Account.



Once the account has been created on the Duo Mobile App, a key should be displayed next to the institution name on the screen.



After scanning the QR code and setting up the account on the Duo Mobile app, click on the Return link at the bottom left of the screen to return to the Two-Factor Authentication screen.

The Two-Factor Authentication screen will display the registered devices.

Two-Factor Authentication

Two-factor authentication makes your account more secure by requiring an additional piece of information beyond your username and password. When you log into any service setup with Colorado State University's single sign-on, you will use your mobile device to provide an additional layer of security to your account. This is done by using the Duo Security app, receiving a phone call, or text message.

Opt In
 Enable Two-Factor Authentication

Registered Devices [+ Register Device](#)

Device Name	Number	Extension	Platform	Activated	Action
Cam the Ram	1999999999		Apple iOS	True	reactivate delete modify

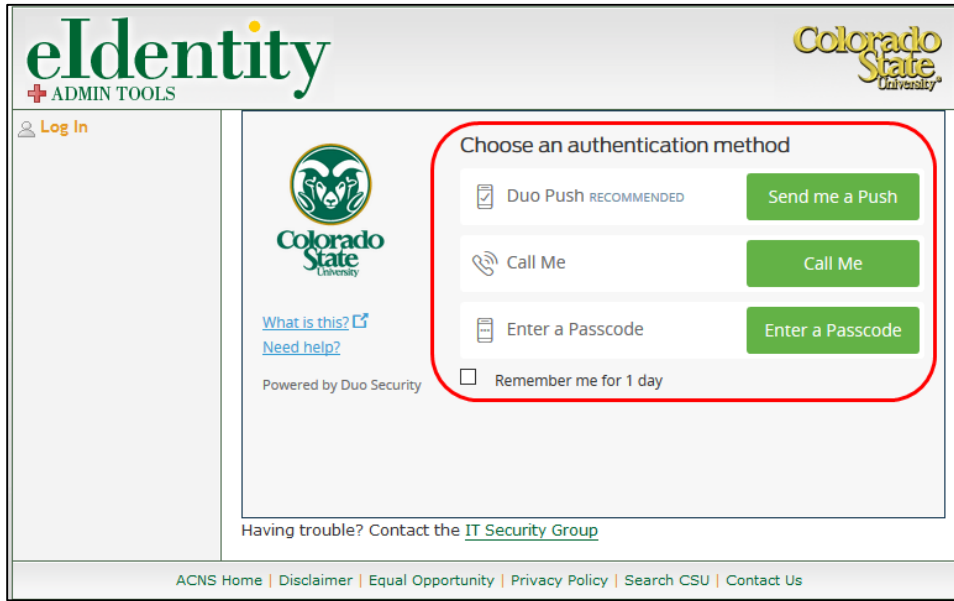
Reactivate, Edit or delete a device by selecting the link to the right of the Device Name.

Tip: If you remove your active device from the Duo Mobile App, go to <http://eid.colostate.edu>, Show My Information screen to access the Two-Factor information and Reactivate your account.

How to Login After Enabling Two-Factor Authentication

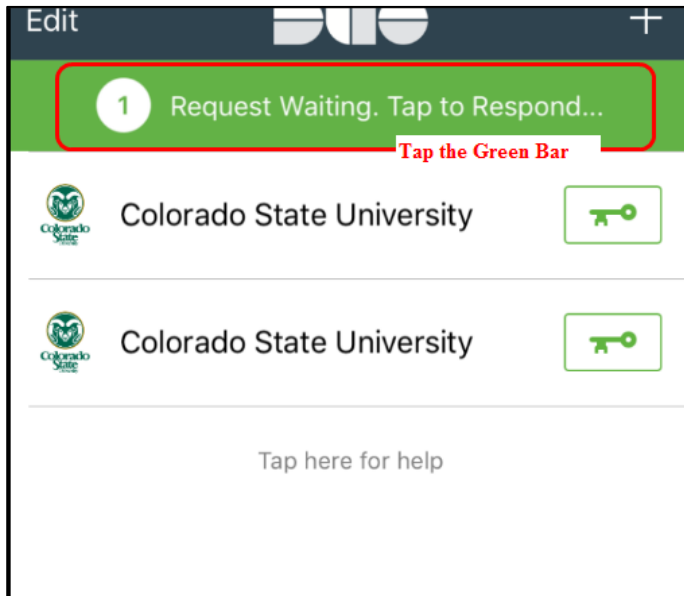
Accessing a service web page that requires the Two-Factor authentication will display a screen showing a selection of authentication methods.

Supported Browsers: Chrome, Firefox, Safari, Internet Explorer 8 or later, and Opera.

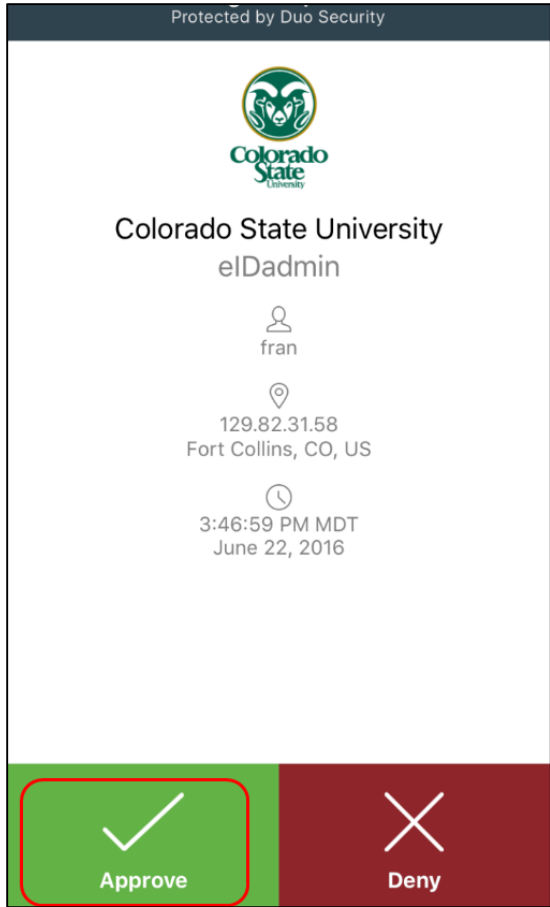


Duo Push Method:

Selecting the Duo Push authentication method will send a Duo Mobile push notification, a text message, to the registered device.

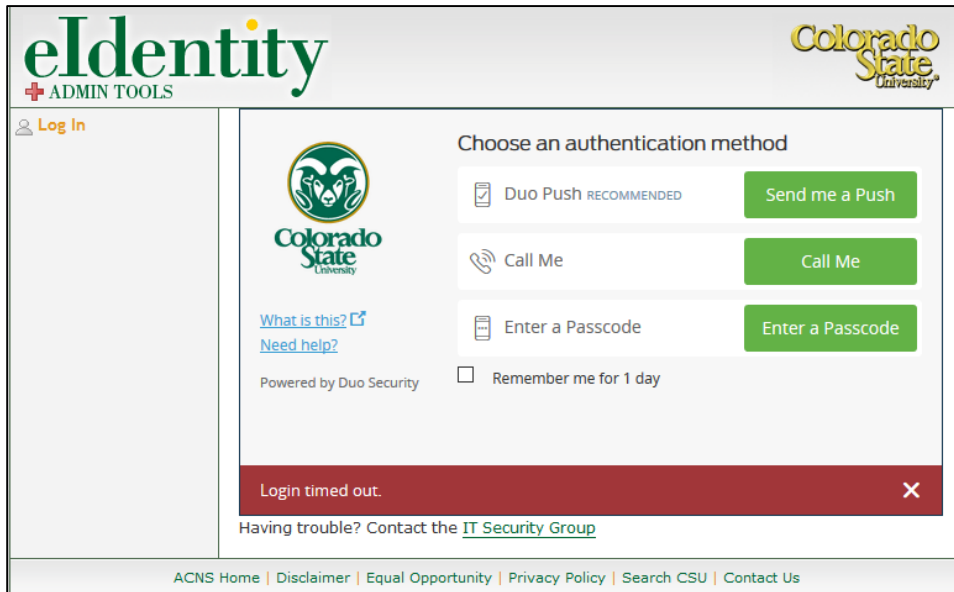


From the Duo Mobile App, tap the green bar at the top of the screen.



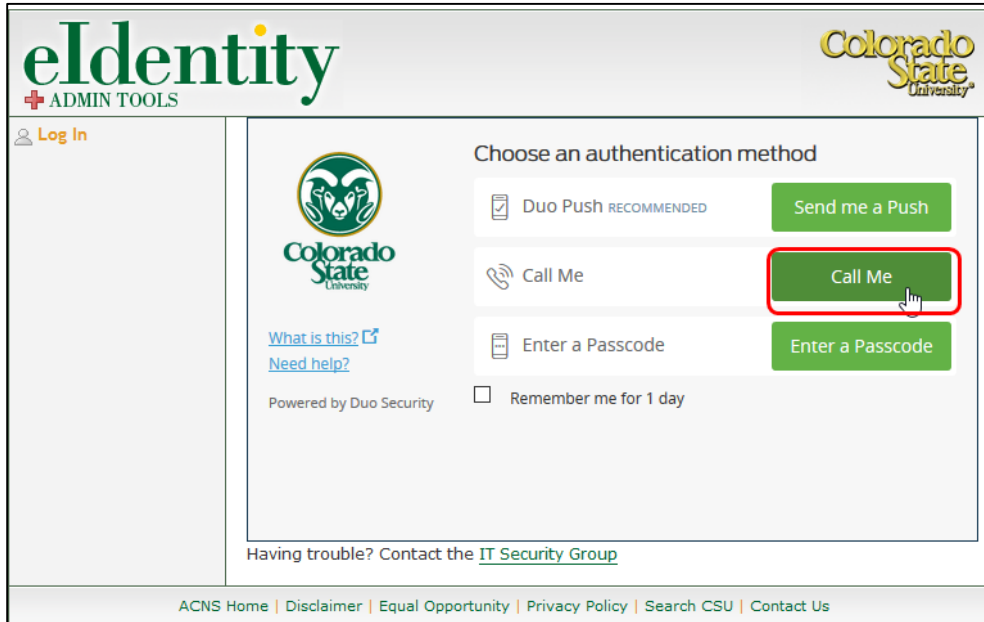
Approve the push by selecting the Approve button. Once the Push has been approved, you will have access to the service page.

Note, the notification push is only valid for a few seconds. If you don't approve the Push, it will time out and expire.



Call Me Push Method:

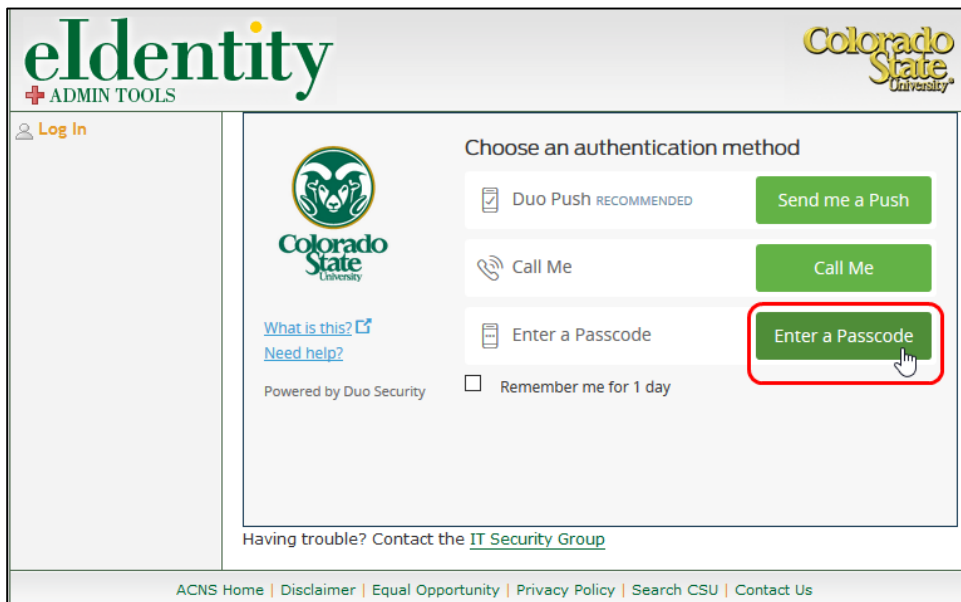
Selecting the Call Me method will initiate a call to the phone number listed for the registered device. Complete the steps per the automated call from Duo to access the service page.



The screenshot shows the eIdentity login interface for Colorado State University. The page title is "eIdentity ADMIN TOOLS" and the Colorado State University logo is in the top right. On the left, there is a "Log In" link. The main content area is titled "Choose an authentication method" and features three options: "Duo Push RECOMMENDED" with a "Send me a Push" button, "Call Me" with a "Call Me" button (highlighted by a red box), and "Enter a Passcode" with an "Enter a Passcode" button. There is also a "Remember me for 1 day" checkbox. Below the options, it says "Powered by Duo Security" and "Having trouble? Contact the IT Security Group". The footer contains links for "ACNS Home", "Disclaimer", "Equal Opportunity", "Privacy Policy", "Search CSU", and "Contact Us".

Enter a Passcode Method:

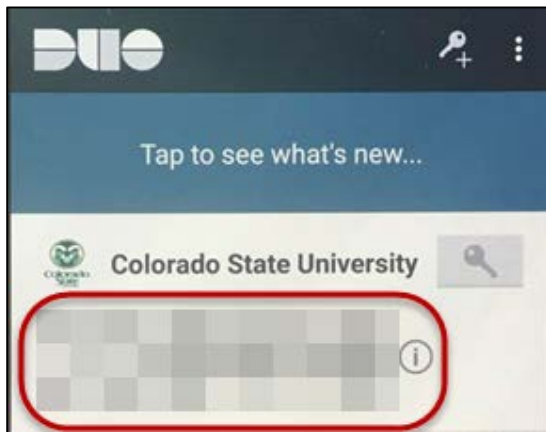
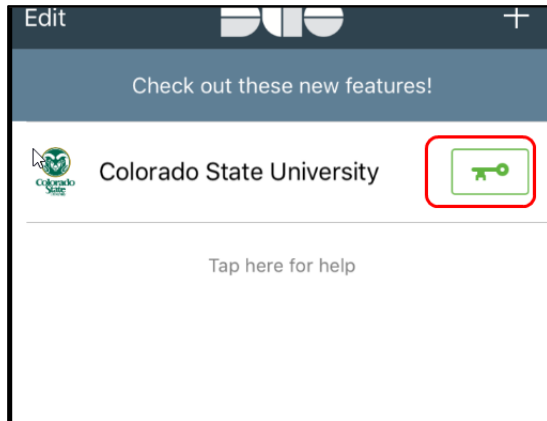
Selecting the Enter Passcode button will require a user to generate a passcode using the Duo Mobile App and entering it in the Enter a Passcode field on the Choose an Authentication Method screen.



This screenshot is identical to the one above, showing the "Choose an authentication method" screen. In this instance, the "Enter a Passcode" button is highlighted with a red box, indicating the selection of this method.

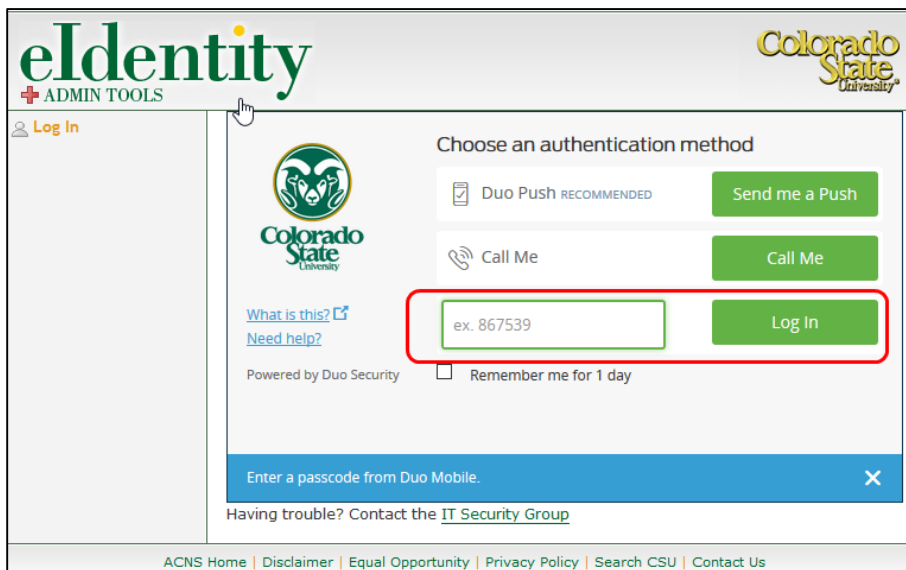
From the Choose an Authentication Method Screen, select the Enter a Passcode button.

Next, open the Duo Mobile App on your Smart Device and click on the key next to the institution name.



Duo will generate a 6-digit passcode.

Type the passcode generated by the Duo Mobile App in the Login field of the Choose an Authentication Method screen.



Once the Passcode has been entered, you will have access to the service page.