Using ArchPass Two-Step Login (CAS, web-based applications)

There are multiple options for using ArchPass two-step login, powered by the Duo Mobile App. You can choose from:

- Push notification using the Duo Mobile app
- Phone call
- Passcodes generated by the Duo Mobile app
- Passcodes sent via text message

You may also use ArchPass’s Remember me for 14 days option when logging in.

Consider This First

- Before you can use ArchPass, you must first enroll a device (phone or tablet) in the Duo Mobile App.
- To log in to an ArchPass-protected system you will first enter your UGA MyID and password. Click Log in. Then you will see the Duo authentication screen.

Use "Remember Me"

To bypass the Duo prompt for 14 days when using the same device and web browser, check the Remember me for 14 Days checkbox at the bottom of the Duo window. (This feature requires browser cookies.)

Checkbox grayed out? If you set Duo to automatically send you a push notification, the Remember me for 14 days checkbox may be grayed out.

Cancel the push by clicking the blue Cancel button on the Duo authentication screen. You will then be able to click the checkbox. Then you will need to choose another option to authenticate.

Push Notification—Duo Mobile App

Click Send Me a Push. To bypass the two-factor prompt for 14 days when using the same device and web browser, first check Remember me for 14 days.
Duo will immediately send a push notification to your mobile device. On your device, tap **Approve** to approve the login.

Important! If you receive a push notification that you did not initiate, tap **Deny**, then tap **It seemed fraudulent on the “Why are you denying this request?” screen.**

If you want to cancel the push (because you want to switch to a different device or authentication method), click the blue **Cancel** button that appears on the login screen when the push is being sent.
Phone Call—Call Me

Click **Call Me**. To bypass the two-factor prompt for 14 days when using the same device and web browser, first check **Remember me for 14 days**. This feature requires browser cookies.

Duo will immediately phone the number you enrolled. Answer the call on your phone, and press 1 immediately to approve the login. If you have enrolled more than one phone, select the phone you want Duo to call from the Device drop-down menu.

**Important!** If you receive a Duo authentication phone call that you did not initiate, press 9 to report fraud.

If you want to cancel the phone call (because you want to switch to a different device or authentication method), click the blue **Cancel** button that appears on the login screen when the call is being made.

**Enter a Passcode**

Click **Enter a Passcode**. To bypass the two-factor prompt for 14 days when using the same device and web browser, first check **Remember me for 14 days**. This feature requires browser cookies.
You can get a passcode to enter in two ways. Instructions for each option are below.

- Generate a passcode with the Duo Mobile app
- Get passcodes via text message

**Generate a Passcode with the Duo Mobile App**

You don't need WiFi or a cellular connection to generate a passcode with the Duo Mobile app.

You can even generate a passcode with the Duo Mobile app if your device is in Airplane mode.

1. Open the **Duo Mobile** app on your device.
2. In the app, tap the **down arrow**.
3. A six-digit passcode displays in the app. Pressing the circle of arrows will generate a new code.
To log in on your computer, click the **Enter a Passcode** button, then enter the passcode in the passcode field, and click **Log In**.
Get Passcodes Via Text Message

1. On the authentication screen, click the **Enter a Passcode** button.
2. Click **Text me new codes** at the bottom of the window.

Duo will immediately send a text message with 10 passcodes to the device you enrolled.
To log in on your computer, enter the first six-digit passcode in the authentication window on your computer, and click Log In. Use the remaining passcodes in order as needed until they expire.

Note: Each passcode can be used only once. Passcodes expire after 30 days.