What is Duo?

Duo is a multi-factor authentication system we use to add an extra layer of security to your account. It adds an additional step during login to help keep you safe while being online. USF utilizes Duo for securely logging in to your PC, access to GEMS, GEMS Self Service, FAST and select other databases hosted by IT.

This document explains how to:

- Set up your NetID account to utilize Duo, and initialize your first device
- Use one of the authentication options, including install of the mobile app
- Set up additional devices
- Get additional help, including installation of the desktop client

Refer to the end of this document for some frequently asked questions.

First-time Setup of Duo Authentication

1. Navigate to [http://netid.usf.edu/duo](http://netid.usf.edu/duo).
2. Select Start setup, then select the type of device you wish to add. We recommend adding your mobile phone, your office phone, or a U2F token.
   Select Continue.
3. a. If you chose either your mobile or office phone, enter your phone number, select the check box to verify that this is the correct phone number.
   b. If using a U2F token follow the onscreen instructions. Full U2F setup instructions can be found at [https://guide.duo.com/u2f](https://guide.duo.com/u2f).
   Select Continue.
4. You will have to verify your phone number. Select to have the system call or text.

![Verification Code](image)

5. Enter the verification code, select Verify and then Continue. Your default device is now set up, and from the dropdown menu you may select if you would like to get an automatic push, call or request to select your authentication method at the time you log in.

![Authentication Methods](image)

6. Select Continue to Login.
You will now be on the main Duo page. Whenever you find yourself here, you may select one of the options to authenticate your identity and log in.

A) Duo Push

This method will send a push notification to the Duo app on your mobile device (Apple or Android phones, as well as tablets of the same types) that allows you to confirm that you are actually trying to log in to your account.

First-time app setup:

1. To install the app on your phone, go to the App Store or Google Play store as appropriate and follow the prompts.
2. With the app installed, click on My Settings & Devices on the Duo homepage on your computer. You will be asked to authenticate, use one of the other two available methods. Then, click on the Device Options button next to your phone number, select the type of device and then the I have Duo Mobile installed button.
3. Attempting to open the app for the first time on your device will bring up the camera, which can be used to scan the authentication barcode, which will now be displayed in your computer’s browser. Alternatively, you may use the link provided to have an activation email sent to you instead.
4. With the barcode successfully scanned the image on your computer will gain a green check and you may click Continue.

B) Call Me

This method will call your phone (mobile or land line). The recording will ask you to press any key on your phone to log in.
C) Enter a Passcode

This method will allow you to use a passcode which the system will send you via text. After clicking the Enter a Passcode button, another button will appear at the bottom of the frame that you can use to send yourself new codes if needed.

Now, we recommend adding an additional device, such as your office phone. This ensures that if your mobile device is unusable for some reason, you can still get into your computer.

Adding additional devices

1. From the main Duo page at http://netid.usf.edu/duo, select Add a new device. You will need to authenticate with one of the methods above.
2. Select the type of device you would like to add and follow the instructions above for installation. Adding your office phone as a landline simply requires entry of the number and then checking the box that reads This is the correct number.

Authenticating for GEMS, FAST, or GEMS Self Service

1. When accessing GEMS, FAST, or GEMS Self Service you will be redirected to the Two-Factor Authentication page to perform the second form of identity authentication.
2. Select the type of device you would like to use to authenticate. The example below has a cell phone, a landline, and a U2F token as the authentication options. Depending on which method is chosen will vary the next actions needed.

Where do I get help?

1. DUO has excellent information in their guide which can be accessed at https://guide.duo.com/
2. Contact the USF IT Service Desk at (813) 974-1222 or help@usf.edu