Quick Reference Guide - Two-Factor Authentication with Duo

Preparing for Two-factor Authentication with Duo

To get started using two-factor authentication with Duo:

- Contact your local IT support team to arrange a time to set up the app on your smartphone and receive training.
- Bring the device(s) you wish to enroll with the Duo app. The app can be used on Apple/iOS, Android, Blackberry, Windows Mobile, phone smartphones and/or tablets.
- If you don't have a smartphone, bring your telephone number or your mobile phone (non-smartphone).
- If you would prefer to use a hardware token (see page 2) instead of or in addition to the Duo mobile app, please request one in advance through your IT support team.

Using Two-Factor Authentication with Duo

There are four methods for authenticating using two-factor authentication. It is advised that you set up and test at least two methods.

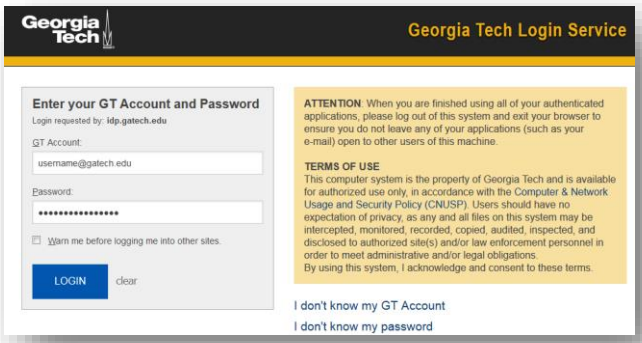
1. **Push** – sends a push request to a laptop, tablet, or smartphone which the user must approve.
2. **Phone call** – sends a call to a mobile or landline phone which the user must answer.
3. **Hardware token** – produces a single passcode each time the token is activated**. ***
4. **Passcode** – delivers a one-time six-digit code each time you need to authenticate. This method is recommended if internet access is not available or when using VPN.

Denying Unexpected Notifications

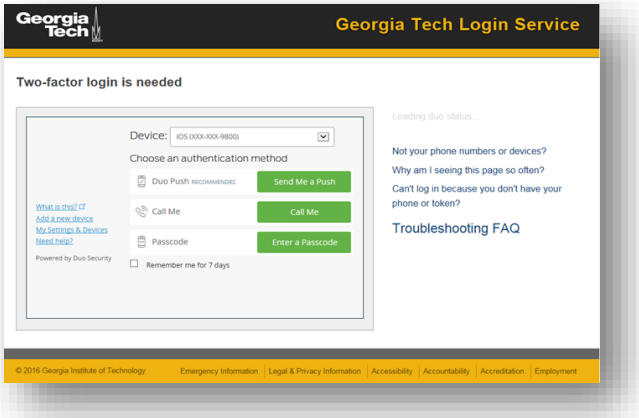
If you receive an unexpected Duo login request via your Duo app or a phone call, select 'Deny' and contact your local IT support team immediately. This activity may represent an unauthorized attempt to use your Tech credentials.

Authorizing Access Using Duo

From the CAS login page below, you'll use your Tech account credentials (username and password) as you normally do. Once you've entered your username and password, you'll see the Duo screen which will authenticate you depending on what method you chose as a second factor.



CAS Login page



Duo prompt page

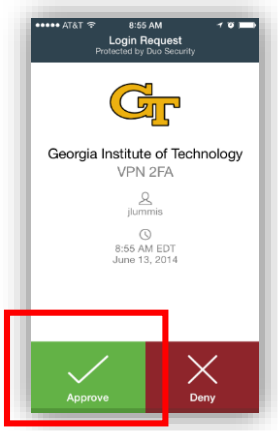
Using Duo Push

If you're using Duo Push, you'll receive a notification on your device (smartphone, tablet, etc.) after you've entered your username and password from the CAS login page. Open the Duo Mobile app, then click "Approve" to access Tech systems.

Georgia Tech Office of Information Technology

Quick Reference Guide - Two-Factor Authentication with Duo

Duo push screen



Using Duo Phone Call

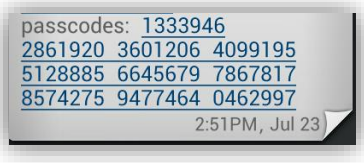
If using Duo Phone Call, you'll receive a phone call on the phone you've registered. Please make sure to select a phone that is secure and not accessible by the general campus. Answer and select "1" to authenticate. **NOTE:** *OIT recommends registering a secondary phone number for your account as a backup.*

Using a Hardware Token*

If you prefer not to use the Duo mobile app you may be issued a hardware token or key fob. Use the numeric passcode shown on the device's screen when logging into Georgia Tech's sites using CAS login screen.

** Note: Using a token is not the preferred method. A cost is associated with the purchase of token devices.*

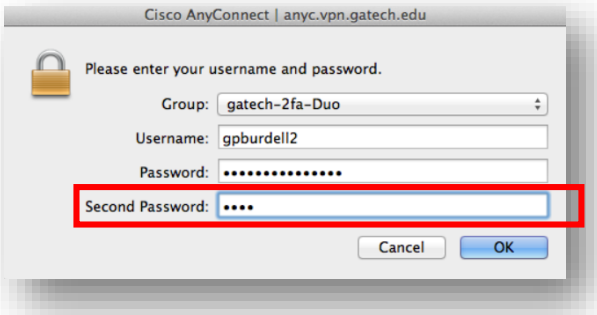
Using Duo Passcodes



If you are using printed passcodes available from Passport (www.passport.gatech.edu), choose one number from the set of numbers each time you authenticate. ***NOTE**: OIT recommends printing out at least one set of these numbers as a backup.*

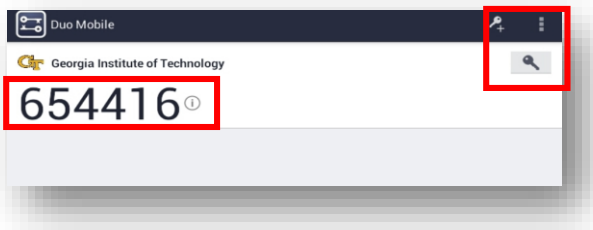
Using Duo Passcode with Virtual Private Network

If you're accessing Tech systems off-campus using Cisco Virtual Private Network (VPN), you'll need to authenticate using your username and password first before clicking on the Duo app for your second authentication.



Enter a code or type "Push" or "Phone" on the second line.

To generate a one-time passcode as the second authenticaion, open the Duo app and click the Key icon located at the top right next to the Georgia Tech logo (see below). Type the code on the "Second Password" line. Or, to generate a push or phone authentication, enter the word "*push*" or "*phone*" on the second line. Approve the push or press 1 on your phone to authenticate.



For more information about two-factor authentication, go to the Two-factor website (***https://twofactor.oit.gatech.edu***).

Georgia Tech Office of Information Technology