Quick Reference Guide

Two-Factor Authentication

Preparing for Two-factor Authentication

To get started with Two-factor Authentication:

- 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) that will be using the Duo app for two-factor authentication. The Duo app is for Apple/iOS, Android, Blackberry, Windows Mobile/Phone smartphones and/or tablets only.
- 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 for an example) instead of or in addition to the Duo mobile app, please request one in advance through your IT support team.

Using Two-Factor Authentication

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

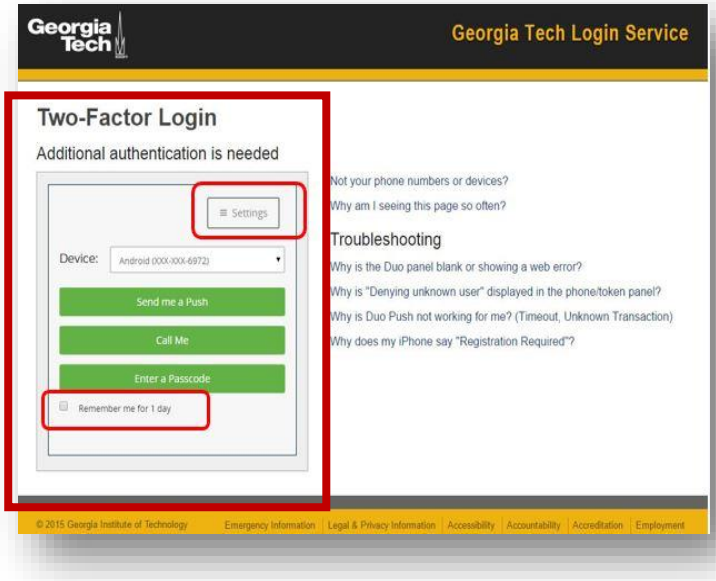
1. **Push** – sends a push request to a laptop, tablet, or smartphone which the user must approve.
2. **Phone call** – sends a call to a mobile or landline phone, which the user must answer.
3. **Passcode (via SMS Text)** – sends a number or series of numbers to a laptop, tablet, or mobile device (non-smartphone) via text message (SMS).
4. **Hardware token** - A single passcode is produced by the Duo app on your smartphone or tablet (iOS or Android only), or by a hardware token *

Denying Unexpected Notifications

If you receive an unexpected 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.

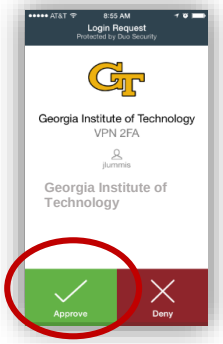
Authorizing Access Using Duo

Once the Duo app is installed, you'll be prompted to enter your second authentication when logging in to many of Tech's secured web applications. After logging in using your regular Tech account credentials (username and password), you will see the following screen:



Using a Push Notification

If using a push notification, you'll receive notification on your smartphone after you click the "Login" button. Open the Duo mobile app, then click "Approve" to access Tech applications.



Georgia Tech Office of Information Technology

Quick Reference Guide

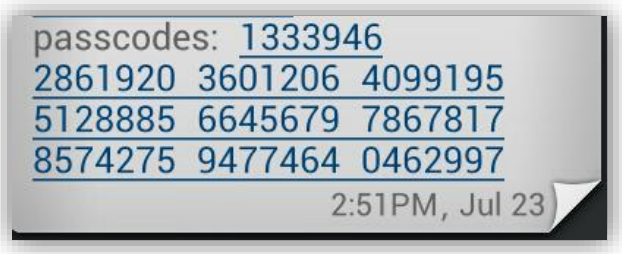
Two-Factor Authentication

Using a Phone Call

If using a phone call to authenticate, you'll receive a call on the phone you've registered. Answer and select "1" to authenticate. **NOTE:** *OIT recommends registering a secondary phone number for your account as a backup.*

Using a Passcode (via SMS Text)

If using a passcode (via SMS Text), choose one number from the set of numbers sent via text or email each time you authenticate. ***NOTE****: OIT recommends printing out at least one set of these numbers as a backup in case your phone is inaccessible.*



Using a Hardware Token*

If you prefer not to use the Duo mobile app, a telephone call, or passcodes sent via text message, you may be issued a hardware token or key fob. These tokens are available in two formats, a random number generator with a small LCD screen (an example is pictured below), or one that connects to a laptop or tablet via a standard USB port. Use the numeric passcode shown on the device's screen when logging in to Georgia Tech's secured sites when on campus using Tech's Central Authentication Service (CAS) or when off-campus using Tech's Virtual Private Network (VPN) to access content remotely.

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

For more information about the Georgia Tech implementation of two-factor authentication, visit the Georgia Tech Two-factor Authentication website at: www.twofactor.oit.gatech.edu.

Georgia Tech Office of Information Technology