Duo Mobile and Two-Factor Authentication FAQ

• What is two-factor authentication (2FA)?

Two-factor authentication (2FA) leverages two separate methods of proving a user is who he or she claims to be. Anyone who has ever used a debit card to withdraw money from an ATM has used two-factor authentication. Sliding the debit card into the ATM provides the first factor of authentication: using something you have. Typing in your PIN provides the second factor of authentication: using something you know.

UAB is implementing a similar methodology for logging into select applications and sites, such as uab.box.com. To access those select applications and sites, users will be required to type in their BlazerID and strong password (something you know) and then use Duo Mobile on a smartphone, tablet, cellphone, or token (something you have) to complete the login.

A number of different synonyms and acronyms exist for two-factor authentication, in addition to the 2FA mentioned above. Among the most popular that you might hear are:

- Strong authentication
- Multi-factor authentication (MFA)
- Two-step authentication

• Why is UAB adopting the use of 2FA?

Like many organizations today, UAB, its employees, and its students are prime targets for hackers, online criminal organizations, and ne’er-do-wells in general. Providing this extra layer of security for access to select applications and sites enhances the level of security that UAB provides for all of its stakeholders.

In fact, a number of universities such as Harvard, Stanford, Yale, and Georgia Tech have begun using Duo Mobile 2FA. Outside of the academic arena, common examples of services and products that provide 2FA options include:

- Many mobile and online banking applications
- Popular email services, such as Gmail
- Mobile phones (Androids and iPhones, for example)
- Social media sites, such as Facebook
- Online commerce sites (PayPal and Amazon)

• How does 2FA protect me?

One of the most valuable sets of information that miscreants can steal are our BlazerIDs and strong passwords. If a malicious actor steals those credentials, whether through a successful phishing attack or a password-reuse issue, he/she can impersonate you and access any accounts to which you have access. That can open the door to serious issues, such as changing your direct deposit settings to someone else’s bank account or corrupting/stealing/destroying your research data. Using 2FA raises the bar required to successfully pull off such attacks.

• When will 2FA begin to be used?
UAB will begin integrating Duo Mobile’s 2FA capability soon. Duo 2FA is slated to be incorporated into the login process for select applications and sites during the 2018 fiscal year and beyond. For more information regarding the Duo Mobile app, how to use it, and how to enroll in its 2FA program, please visit http://www.uab.edu/it/home/2-factor.

• Will 2FA be used to login to all UAB applications and associated sites?

Not at this time. UAB initially will integrate Duo Mobile’s 2FA capability with access to uab.box.com in mid-September 2017. Going forward, Duo 2FA will be implemented for use with select applications and sites during the 2018 fiscal year and beyond.

• What’s needed to use Duo Mobile and 2FA?

In general, three things are needed to use Duo Mobile and the 2FA process:

• A Duo Mobile account
• A mobile device, such as a smartphone or tablet
• The Duo Mobile app installed on that smartphone or tablet

If you do not have a smartphone that can run the Duo Mobile app, alternative methods for using Duo and 2FA are available. More information on using hard tokens and cellphones can be found both later in this FAQ.

• How do I get a Duo account?

Duo mobile accounts are created automatically for authorized users who require access to UAB sites and applications protected by Duo security.

• What is the Duo Mobile app and what does it do?

Duo Mobile is an app that generates an out-of-band notification to users when they attempt to login to sites or applications that require Duo 2FA. After typing in a BlazerID and strong password at such a site, Duo can be used on a mobile device to confirm that your login attempt is valid. By simply pushing a button on your mobile device or entering in the PIN that Duo generated, you can confirm that your login is a legitimate session and gain access to the site or application.

If your mobile device, such as an older cell phone, does not support apps, Duo can send passcodes via SMS text that allow you to complete the 2FA process.

• How do I get the Duo Mobile app?

Android users can download the Duo Mobile app from the Google Play store. Simply search for “Duo Mobile,” which is provided by Duo Security. Apple users can download the Duo Mobile App from the App Store by using the same search term.

The app is free, so simply download and install the app.

• What devices can I use with Duo for 2FA?

• Smartphones (iPhone, Android, Microsoft)
• Tablets (iPad and Android)
• Mobile phones that can receive batches of Duo passcodes via text from Duo
• Hard tokens (small devices that generate one-time PINs for Duo)

**Do I need just one mobile device to use Duo for 2FA?**

Yes, but it doesn’t hurt to have more than one device enrolled to use with Duo.

As long as you have an active Duo account and at least one enrolled mobile device, you can use that mobile device to complete the 2FA process. However, a best practice is to enroll two devices and use one as a primary authentication device and the other as a backup. For example, if you have an iPhone and an iPad, you can install the Duo Mobile app on each and enroll them for use with your Duo account.

Use the iPhone as your primary device for 2FA authentication. If you lose your phone or it’s stolen, you can still use your iPad for 2FA authentication until you purchase a new phone and enroll it for use with your Duo account. If you lose or break your phone, be sure to delete it from your account as soon as possible.

**What if I want to add a new mobile phone or device to my Duo Mobile account?**

If you already have enrolled a primary mobile device for use with your Duo account and want to add a second device, visit [https://www.uab.edu/it/home/images/2FA/Documents/Duo-User-Guide---Add-Device_Manage-Settings.pdf](https://www.uab.edu/it/home/images/2FA/Documents/Duo-User-Guide---Add-Device_Manage-Settings.pdf) for instructions on how to add another device.

**How do I enroll my first authentication device?**

If you’ve never enrolled a mobile device for use with Duo, launch a browser on your computer and visit a website that UAB protects with Duo security, such as uab.box.com. Login to that site by typing your BlazerID and strong password. Once you have authenticated, you will land on Duo’s Start Setup landing page. Then visit one of the following sites for specific instructions on how to enroll your desired mobile device:

- [http://www.uab.edu/it/home/2fa-android](http://www.uab.edu/it/home/2fa-android) for Android phones and tablets
- [http://www.uab.edu/it/home/2fa-ios](http://www.uab.edu/it/home/2fa-ios) for iPhones and iPads
- [http://www.uab.edu/it/home/2fa-nonsmart](http://www.uab.edu/it/home/2fa-nonsmart) for non-smart phones

**How does Duo and 2FA work?**

Once a mobile device is linked to your Duo Mobile account, that device can use multiple methods to help you login to a site that requires Duo 2FA. The two most common ways are via a Duo Push or a randomly-generated passcode. Duo Push is the recommended way to complete the 2FA process, but generating passcodes via the Duo Mobile app is the best way to complete the 2FA process if your phone has no signal and cannot receive a Push.

**How does Duo Push work?**

When you login from your computer to an application or site that requires Duo 2FA with your BlazerID, you first enter your BlazerID and strong password, like usual. You will then see a screen asking you to choose a Duo authentication method (usually Duo Push or Passcode).
When you click the “Send Me a Push” button on your computer screen, you will be asked to open the Duo Mobile app on your device (phone, tablet, etc.) and check for a request. A “Request waiting” banner will appear in the Duo app on your device (Sometimes you have to swipe down to make the banner appear). Tap the banner to pull up the confirmation screen. Click the big green “Accept” check mark in the bottom-left corner of the device to complete the login. Click the big red “Deny” X to decline and cancel the login.

If you click on the “Accept” button and return to your computer screen, you will notice that your login session has been completed. If you wait too long to choose “Accept” or “Deny,” the Duo Push request will expire.

**Note:** If you receive a Duo Push notification and you ARE NOT trying to log in, DO NOT hit the “Accept” button. An unsolicited Push notification likely is a sign that your BlazerID credentials have been compromised and a malicious actor is trying to login as you. In such a scenario, click the “Deny” button, immediately go to [BlazerID Central](http://www.uab.edu/it/home/2fa), and change your strong password.

- **What if I receive an unexpected Duo login attempt notification on my mobile device?**

That is a sign that your UAB credentials likely have been compromised and an attacker is trying to login with your BlazerID. Click the red “Deny” button in the Duo Mobile app. Since the attacker doesn’t have access to your mobile device, he/she can’t complete the login via Duo. The login attempt will fail. However, you should immediately visit BlazerID Central and change your strong password.

- **How do Passcodes work when authenticating?**

When you login from your computer to an application or site that requires Duo 2FA with your BlazerID, you first enter your BlazerID and strong password, like usual. You will then see a screen asking you to choose a Duo authentication method (usually Duo Push or Passcode).

When you click the “Enter a Passcode” button on your computer screen, go to your device, open the Duo Mobile app, and click the green key next to your UAB-BlazerID account. The Duo app will generate a six-digit number. Return to your computer screen, type in the six-digit number and hit the Enter key. If you typed in a valid passcode, your login session will be completed successfully.

- **I don’t have a smartphone. How can I use Duo and 2FA?**

Any mobile phone that can receive an SMS text message can work with Duo Mobile. In such cases, Duo will send a batch of 10 passcodes via a text. You can use each of those passcodes to complete the 2FA sign-on once until you run out of passcodes. Also, a “hard token” that generates PIN passcodes can be acquired for a monthly fee. If you have a cell phone that can receive SMS text messages, visit the following page to learn how to enroll and use that device during the two-factor authentication process:

[http://www.uab.edu/it/home/2fa-nonsmart](http://www.uab.edu/it/home/2fa-nonsmart)

If you need to use a hard token, you must fill out an Exception Request Form and submit it to AskIT via a ServiceNow ticket. If the request is approved by the Enterprise Information Security Office, AskIT will work with you to configure and assign a token to you. All tokens must be picked up by the requesting individual at the AskIT office in Cudworth Hall (CEC 225), and proper identification must be provided to the AskIT staff in order to receive the token. [http://www.uab.edu/it/home/2fa-token](http://www.uab.edu/it/home/2fa-token)
• Can I still use Duo Mobile for 2FA even if my smartphone/tablet can’t get a signal or connect to the Internet?

Yes. When you login from your computer to an application or site that requires Duo 2FA with your BlazerID, you first enter your BlazerID and strong password, like usual. You will then see a screen asking you to choose a Duo authentication method (usually Duo Push or Passcode).

When you click the “Enter a Passcode” button on your computer screen, go to your device, open the Duo Mobile app, and click the green key next to your UAB-BlazerID account. The Duo app will generate a six-digit number. Return to your computer screen, type in the six-digit number and hit the Enter key. If you typed in a valid passcode, your login session will be completed successfully.

• What if my Duo-registered phone or device is lost or stolen?

If you have a second device enrolled for use with Duo Mobile, use the second device to and the following instructions to access your Duo account and delete the lost or stolen device from your account:


If you do not have a second enrolled device, contact AskIT and ask them to delete the lost or stolen device from your account. You can contact AskIT by calling 996-5555, emailing askit@uab.edu, or visiting the Contact AskIT web page.

• What if I don’t have a mobile phone that receives texts, a smartphone, or a tablet? How do I use Duo to sign in via 2FA?

A Duo “hard token” that generates PIN passcodes can be acquired for a monthly fee paid by the requesting party’s department. If you need to use a hard token, you must fill out and submit an Exception Request Form and submit it to AskIT via a ServiceNow ticket. If the request is approved by the Enterprise Information Security Office, AskIT will work with you to configure and assign a token to you. All tokens must be picked up by the requesting individual at the AskIT office in Cudworth Hall (CEC 225), and proper identification must be provided to the AskIT staff in order to receive the token.

• Do I have to complete the 2FA process every time?

You can if you like, but you don’t have to receive a push notification or type in a passcode every single time you perform a Duo-enabled login. During the login process, when you choose an authentication method, there’s a “Remember me” checkbox that appears below the login choices. By placing a check in that box, Duo will remember that you successfully logged in using 2FA from that particular device. During the defined “Remember me” period, Duo will not require 2FA from that particular device.

However, you still will be required to use 2FA during that “Remember me” period if you log in from a different device. For example, at 8 a.m. you log in from your desktop computer to a site or application that UAB protects with Duo, and you check the “Remember me” box during the 2FA process. During the “Remember me” period, you will not have to repeat the 2FA process for that site/application while using your computer. However, if at 10 a.m., you log in to that same site/application with a laptop, Duo will
require you to complete the 2FA process because this is the first time today that it has seen you log in to the site/application with the laptop. You can again check the “Remember me” box for your laptop and Duo also will remember that you logged in from it. At that point, you will not have to repeat the 2FA process on either your desktop computer or laptop until the “Remember me” grace period expires.

• Does Duo 2FA work with the Box app on Apple and Android mobile devices?

Yes. The two-factor login authentication process you use to login to uab.box.com is the same when you use the Box app on a mobile device. Due to their larger screens, tablets are ideal for using the Box app with the Duo 2FA login process. Due to the small size of many mobile phone screens, UAB IT recommends that you use a tablet instead of a mobile phone when using the Box app with Duo 2FA.