# FAQs Guide

## Helpful Links:

1. Universal Enrollment Guide (Duo Mobile enrollments):
https://guide.duo.com/universal-prompt#enrollment
2. Website MFA Faq page:
https://www.linnbenton.edu/student-services/email/mfa.php
3. Promoting Duo Push link:
https://help.duo.com/s/article/promoting-push?language=en_US
4. Phone Versions that work with Duo: IOS and Android

## How frequently are you asked to authenticate on your default device?

varies, depending upon:
- The website you're accessing (for added security, some sites always require a MFA)
- Your individual browser settings (whether or not you clear cookies)
- Whether or not you use more than one computer and web browser (MFA is requested every 8 hours for each computer and each browser you use to access protected website)
- If you are prompted with a screen that asks if you want to trust the browser. You'll have the option to select "Yes, trust browser." This takes the place of the "Remember Me" screen. If you click "Yes, trust browser" the browser will automatically remember you, and you will not be prompted to authenticate for that application or service for the next 8 hours. It is important to not check this box on shared computers.

## What Duo method is right for me? Additional information from Duo

- **Duo Mobile Push** - secure method, recommended and convenient. Requires a mobile device that supports the app and notifies the user that a login has been attempted. Approve or Deny the action for the safety of your account.
- **Security Key** - secure method, you will have to carry a fiscal device and insert it into the device you are logging in to, plus you have to touch the key to activate authentication.
- **Biometrics** - secure method, but only works on a device that has this feature.
- **SMS Test** - *(Student Only Feature)* This is less secure and has risks being sent by text message. This is an option for students that can not use the Duo app or do not have access to a smartphone. You will be texted a passcode to enter into Duo.
- **Phone Call** - *(Student Only Feature)* less secure, but is an option if nothing else will work for you. This allows you to receive a phone call that provides you with a passcode to enter for authentication into Duo

## What is Duo Mobile and Duo Push?

- **Duo Mobile** is Duo Security's free app that allows you to quickly and easily approve a second-factor authentication request using **Duo Push**. You can download it from the Apple or Android mobile app stores.

- **Duo Mobile and Duo Push**, there is no need to carry a bulky token or waste time manually entering passcodes. Just tap to authenticate right on your smartphone.
- Looking for an example of [Duo Push](#) in action.

## How will Duo change my login experience?

Think of Duo as a second layer of security added to your pre-existing login method. When logging in to an application that Duo protects, you will still enter your username and password, only after that, you will have to verify it is really you. You do this by clicking the green checkmark in the Duo Mobile Push app or plugging in your hardware token. Duo does not replace or require you to change your username and password.

## What is Duo, what is multi-factor authentication, and why do we need it?

Two-step authentication uses two forms of authentication to verify your identity. First, you enter your My LB ID and password. Then you need a physical device such as your mobile phone, tablet, sms, or key to access your account. This is required for compliance and is a best practice for your safety and the security of the college.

## Additional questions contact:

Students: [student.helpdesk@linnbenton.edu](mailto:student.helpdesk@linnbenton.edu) or 541-917-4630
Employees: [staff.heltpdesk@linnbenton.edu](mailto:staff.heltpdesk@linnbenton.edu) or 541-917-4333