DUO - Two-Factor Authentication

Introduction

DUO Security is a two-factor authentication (2FA) system that adds an extra layer of security to your Brandeis account. When it comes to account security, it's best to protect it with both something you know (your password) and something you have (your phone or mobile app).

After DUO is enabled on your account, you will be asked to authenticate with DUO when you log in to Brandeis online resources or Google Apps. This prevents unauthorized access to your account even if your password is compromised because you will get prompted by DUO when you aren't trying to log in yourself. If you get prompted for DUO when you aren't trying to log in, contact the Help Desk immediately to let them know of a suspicious login attempt.

More details about two-factor authentication are available on DUO Security's website.

Getting Started

1. Choose which devices you would like as second factors.
   a. ITS recommends using the smartphone app as your primary device.
      Tip: Download the DUO Mobile app from the App Store or Google Play on to your smartphone BEFORE you enroll the device on the Two Factor portal.
   b. ITS recommends using a landline (desk phone) as your backup device.
2. Enroll two devices (primary and backup) into the DUO Two Factor portal on Brandeis' Identity Management site.
   a. ITS strongly recommends setting up at least two devices with DUO in case you are not near the original device you set up. As mentioned above, ITS recommends the smartphone app or mobile phone for its convenience when off-campus, abroad, or traveling.
   b. The following authentication methods are available as a second factor:
      i. Smartphone app (recommended)
      ii. SMS (text messages)
      iii. Phone Call (rings to desk phone/cellphone for)
      iv. Hardware token*

Need more detailed instructions? Go to our Setting up DUO page for a step-by-step guide through the process.

* When/If choosing to use your hardware token, ensure that the green button is on the left side of the device and the word 'DUO' can be read properly (pictured at 'Hardware token' link above). Also note that Hardware Tokens are available to Faculty/Staff only at this time.

If none of these methods will reliably work for you, please contact the Technology Help Desk (x6HELP, 781-736-4357) for possible solutions.

Things to Expect with DUO

Logging into specific services will prompt account holders to authorize the login attempt with a second factor.

By default, every time you want to log into your Brandeis Account, you will also be prompted via Duo to confirm the login. This is generally once per login. This default behavior is the most secure option available.

Tip: For users desiring greater convenience, the Duo login page has a "Remember me for 30 days" checkbox. This is a per-device, per-application setting. For example, if you use both Chrome and Firefox on the same computer, you will have to check the box in both Chrome and Firefox separately. If this option is checked, your device will be treated as a trusted device. The trusted device can go longer periods between the times that you are typically asked to confirm with Duo.
Please note: you may not see the “Remember me for 30 days” checkbox until you’ve successfully enrolled and logged into Duo at least once. To enable this, deny the prompt from your second factor to log in, and the checkbox should be available shortly.

Brandeis websites/services that currently support 2FA include:

- Google Suite
- LATTE
- Zoom
- webedit.brandeis.edu (Cascade Server)
- Echo360
- Box
- And more

Have Questions? Need Help? Please see our DUO 2FA FAQ.

Related articles

- Using the Gradebook
- Text Editing
- Adding TAs and Guests
- Google Groups
- Create Online Assignments