DUO - Two-Factor Authentication

This information only applies to accounts manually enrolled into two-factor authentication.

Questions, comments, or feedback? Please email duo-group@brandeis.edu

Introduction

Two-factor authentication (2FA) strengthens access security by requiring two methods (also referred to as factors) to verify your identity. These factors can include something you know - like a username and password, plus something you have - like a smartphone app to approve authentication requests.

2FA protects against phishing, social engineering, and password brute-force attacks. It secures your logins from attackers exploiting weak or stolen credentials.

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

Getting Started

1. Enroll two devices (primary and backup) into the DUO Two Factor portal on Brandeis' Identity Management site.
   a. We recommend using the smartphone app as your primary device.
   b. We recommend using a landline (desk phone) as your backup device.
2. Download the DUO Mobile app from the App Store or Google Play on to your smartphone. See DUO's Documentation for detailed guides.

Things to Expect with DUO

Logging into specific services will prompt account holders to authorize the login attempt with a second factor. The following authentication methods are available as a second factor:

- Smartphone app (recommended)
- SMS
- Phone Call (desk phone/cellphone for call back)
- Hardware token*

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.

For those users desiring greater convenience, the Duo login page has a "Remember this device" checkbox. 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 asked to confirm with Duo. The current trust period is 30 days. This will allow you to connect to your Brandeis Account from the same computer using the same browser.

* 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)

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

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

- Remote Desktop (RDC)
- Set Up RDC for Windows 7
- Set Up RDC for Windows 10
- Set Up RDC for Windows XP
- Upload feedback files for assignments