Two-Factor Authentication

Two-factor authentication (2FA), powered by Duo Security, is available for faculty, staff, special payroll, and student employees. 2FA enhances data security by requiring two forms of identification to gain access to an online resource. On a system that requires 2FA, you would first login with your NetID credentials (something you know) and then verify your identity with a physical device linked to your NetID account (something you have). This additional layer of protection prevents anyone but you from accessing your accounts, even if they have obtained your username and password.

Duo Mobile is an authentication app that works with Duo Security’s two-factor authentication service. Once installed from the app store, the app will send a “push notification” to your smartphone or tablet that allows you to authenticate with one tap.

Related Pages

- Authentication Method Overview
- Setting Up a Landline for 2FA
- Setting Up a Mobile Phone for 2FA
- Setting Up a Tablet for 2FA
- Setting Up a Backup Device for 2FA
- Authenticating via Phone Call
- Authenticating Using an SMS Text Message
- Authenticating via Push Notification (Duo Mobile App)
- Authenticating Using a Passcode
- Purchasing and Registering a Hardware Token for the 2FA Service
- Generating an Alternative Passcode for Forgotten/Lost Devices
- Logging In with 2FA
- 2FA for International Travelers
- Adding 2FA to My Web Application
- Reactivating the Duo Mobile App with New Phone (Same Phone Number)