Duo - 2 Factor Authentication

2FA stands for 2-Factor Authentication, meaning a system requires two separate forms of identity verification for access, making it virtually impossible for anyone to compromise your account without having both pieces of the puzzle.

2FA secures your account against threats such as compromises caused by malware and phishing attacks. Even malicious actors who obtain your password will not be able to access your account.

2FA works by combining your two factors:

- **What you know**: In our case, this is your App State username and password combination.
- **What you have**: This is the 2nd factor. It will take one of two forms:
  - the Duo mobile application on your smartphone,
  - a handy hardware token (also called a key or fob)

(You will set this piece up when you are ready to configure 2-Factor for your account).

When both factors have been entered, you are granted access to the system.

**Access Your Duo Settings**

- DUO 2-Factor Authentication
- Duo Enrollment
- Duo Prompt display issue on an iPhone or iPad
- Duo Two-Factor Authentication Enrollment for Faculty & Staff
- Duo Two-Factor Authentication for Incoming Students
- Duo Universal Prompt
- Duo: Manage Devices After Enrollment
- How to Activate Duo Push Notifications to your Smartphone
- Logging into AnyConnect VPN with a Duo Token
- New Phone-How to Reactivate Duo Mobile
- What is Duo 2-Factor Authentication (2FA)

**Search Knowledge Base**

**Submit a Service Request**