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 yourAppState Username and Password combination.
- **What you have:** This is the 2nd factor. It will take one of three forms: the DUO mobile application on your smartphone, a handy hardware token, or an access code (*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 Self Enrollment
- DUO Two-Factor Authentication Enrollment for Faculty & Staff
- Duo Two-Factor Authentication for Incoming Students
- Duo: Remember Me for 14 Days
- How to Activate Duo Push Notifications to your Smartphone
- How to Get Emergency Bypass Codes for DUO.
- How to Reactivate Duo Mobile on a New Phone
- Logging into Pulse Secure with Duo Token
- What is Duo 2-Factor Authentication (2FA)

For more information including resources for support please visit the DUO - 2-Factor Authentication Service Catalog Page.

**Search Knowledge Base**

**Submit a Service Request**

We value your feedback! Click **HERE** to suggest updates to an existing article, request a new article, or submit an idea.