Two-Factor Authentication with DUO

What is two-factor authentication?

Two-factor authentication adds a second layer of security to your online accounts. Verifying your identity using a second factor (like your phone or other mobile device) prevents anyone but you from logging in, even if they know your password.

This second factor of authentication is separate and independent from your username and password — Duo never sees your password.

How It Works

1. Enter username and password as usual
2. Use your phone to verify your identity
3. Securely logged in

Why do I need this?

Passwords are increasingly easy to compromise. They can often be stolen, guessed, or hacked — you might not even know someone is accessing your account. Two-factor authentication helps keep your account secure even if your password is compromised. With Duo Push, you'll be alerted right away (on your phone) if someone is trying to log in as you.

Browse All Articles

All Faculty members will be required to use Duo by 11/19/19. This will apply to any online UMBC service requiring a login, except for current, "self-service" functions such as timesheets, etravel requests, etc. Click here for more information.

News

- Best Practices for Duo Two-Factor Authentication
- All Faculty Required to Use Duo 2-factor Authentication
- How Undergraduate Admissions Migrated to Duo
- Employees with PS Access Required to Use 2 Factor Login

DoIT strongly encourages Duo users to enroll a backup authentication device to avoid being locked out of your account should you be without your default device!

Recommended Articles

- How do I opt in Duo two-factor authentication for my UMBC account?
- How do I add/enroll a device in Duo?
- Now that I've set up Duo on my device(s), how do I use it to log in to my account?
- Best Practices for Using Duo

For more information on two-factor authentication as provided by Duo Security, go to http://guide.duosecurity.com