Two-Factor and Multi-Factor Authentication

Jeff Clark - 2023-07-20 - Accounts and Access

Duo Verified Push at Florida Atlantic University

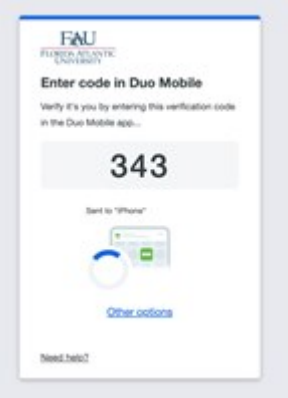
Two-factor and multi-factor authentication add a second or third layer of security to your FAUNet ID. Using a second factor when logging into services such as Banner, Workday, and ePrint helps prevent anyone other than you from logging in even if they know your password.

To better protect University data and to ensure compliance with State of Florida access control polices, the University has begun implementing stricter password policies.

How it works:

Duo Verified Push enhances the security of conventional MFA by requiring you to enter a code on your device to complete login. After July 10th, to approve a login, you will be presented with a code that needs to be entered in the DUO Mobile app. This added layer of security helps prevent potential phishing and other credential-stealing attacks and reduces the likelihood of accidental approval of malicious login attempts.

When you log in to a single-sign on enabled service, such as Canvas, MyFAU, or Outlook, your browser will display a DUO prompt containing a three digit code.



Open the DUO Mobile app on your Android or iOS device and enter the code displayed in your browser (not the code displayed above).

Important: If you are receiving the prompt but you are not logging in, click **"I'm not logging in"** below the "Verify" button.

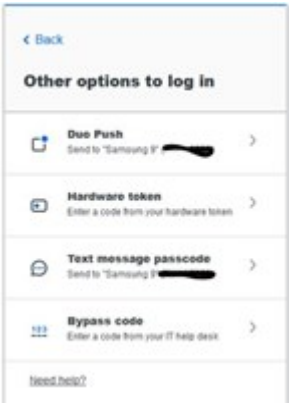
After you have entered the code, you will be asked if you ***Trust this browser?***

If you are using a shared/public computer, we require that you select **"No , do not trust this browser."** This will prevent others from taking over your session after you leave the computer/kiosk.

If you select **"Yes, trust browser"** you will not be prompted for DUO in this browser session for 24 hours.

When you see the prompt, click "Other options"

Select the option you would like to use for the verification.



Users with access to sensitive data through use of their FAUNet ID will have to sign up for a new service called Multi-Factor Authentication (MFA), which will let you keep the same password for 365 days.

MFA is a technology that provides a second method of authenticating you when logging into services with sensitive information. You will be able to choose from a few methods to accomplish this. Users wishing to opt-in may use our **Two-factor and multi-factor authentication enrollment tool.**

Instructions available here.

Advantages of choosing two-factor include:

Users of services such as Workday and other reporting tools will not require VPN to achieve full functionality from home.
Passwords expire in 365 days rather than 60.

If you elect to use MFA you will be required to provide a second method (or factor) of authentication when accessing Workday and other sensitive services. To enroll use the **Two-factor and Multi-Factor Enrollment tool.** The enrollment tool will

allow you to enroll a mobile app (Duo), cell phone, tablet, land line, or special hardware tokens. We recommend that you enroll using both the mobile app and a number as a backup method for authenticating. This backup number will allow you to access Workday if you are unable to use your cell phone. The mobile app works across cellular data and Wireless (WiFi), as well as offline. We highly recommend this method because using this application incurs no data, text (SMS), or other charges when using codes and WiFi.

If you do not have access to a smartphone, we recommend that you request a hardware key fob (FOB) by **submitting a help desk request** . FOBs may be picked up by appointment from the Help Desk in CM22 on the Boca Campus, SR291 on the Jupiter Campus, or LA303 on the Davie Campus.

More information about MFA and the devices supported by FAU can be found by visiting the **Duo Security user documentation** .