Duo Multi-Factor Authentication

Enroll and Authenticate using a Hardware Token

Introduction

In limited circumstances, TU faculty and staff may request a hardware token for Duo Multi-Factor Authentication. A hardware token is a small electronic security device that may be attached to a keychain. These tokens are assigned to users and are used to generate an authentication code (random key code).

Steps to enroll/authenticate a token:

1. Use Case Scenarios - Read through the **use case scenarios** below to make sure you are eligible for a token.
2. Request and Pick up a Hardware Token - Call the Help Center (410-704-5151) or create a TechHelp request (preferred method), to **request and pick up a hardware token**. The Help Center will let you know if you have been approved for the token and will arrange a time for you to pick up the token.
3. **Enroll your token** using the steps below.
4. **Authenticate** using your token.

Use Case Scenarios:

In order to receive a token, one or more of the following scenarios must be true.

- You do not have a mobile device (phone, tablet) that you regularly carry with you, and want a method of authenticating in conference rooms, classrooms, or anywhere else where you don't have a permanent landline phone.
- Your only mobile device is a flip-phone, and you teach in classrooms (or attend meetings in conference rooms) with poor cell reception so phone calls and text messages aren't a reliable option.
- You teach in classrooms with poor cell and Wi-Fi reception, and have had difficulties with mobile devices functioning previously.

Request and Pick Up a Hardware Token

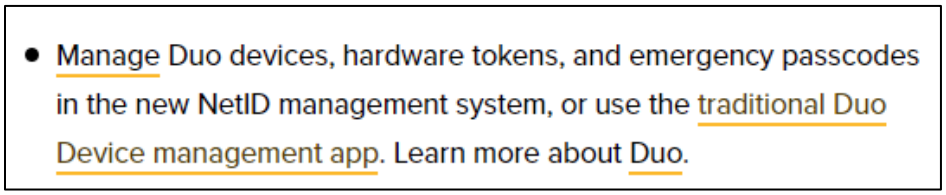
To request a hardware token, you must either call the Help Desk (410-704-5151) or submit a TechHelp request (preferred method). The Help Center will ensure that the client meets the requirements for receiving a token and either approve, deny or escalate the request. If approved, the client will go to the Help Center at a preapproved time to pick up the hardware token.

Use the steps below to fill out a request.

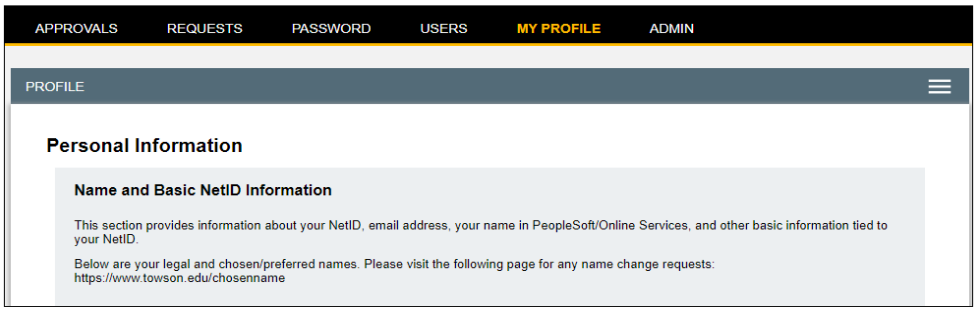
1. From your favorite browser type techhelp.towson.edu in the address bar and press ENTER.
2. Enter your **User Name** (NetID) and **Password**.
3. Request type: **Employee Role**
4. Next drop down: **Accounts, NetID, Passwords, Duo, Sponsored Groups**
5. Next drop down: **Duo Multi-Factor Authentication**
6. Request Detail: **Request a Hardware Token because “use a scenario above”**

Enroll your Token

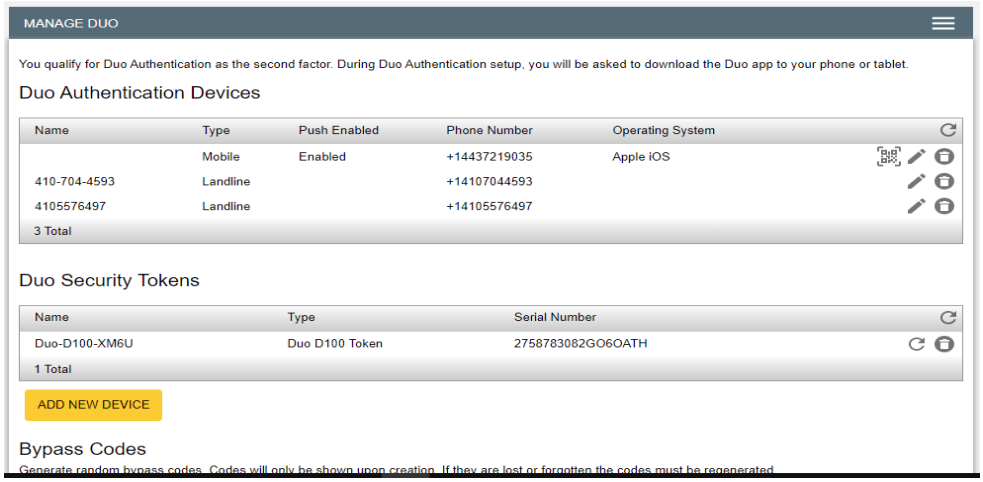
1. Go to Towson.edu/netid
2. Under **Other Faculty/Staff NetID Tools**, choose **Manage Duo Devices**



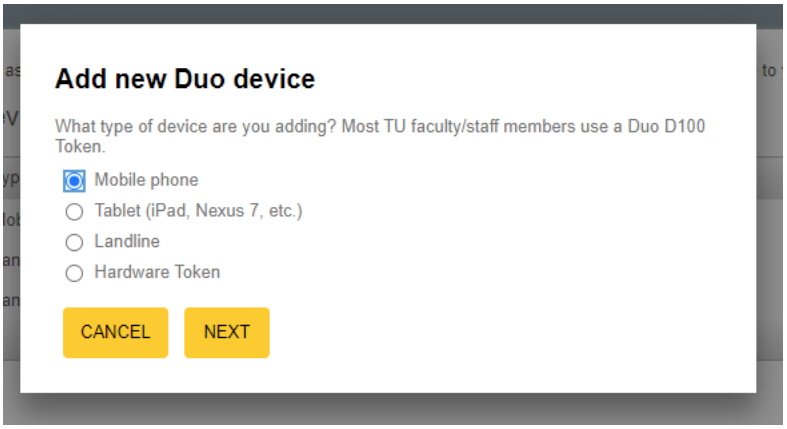
3. After entering your information, your profile will appear:



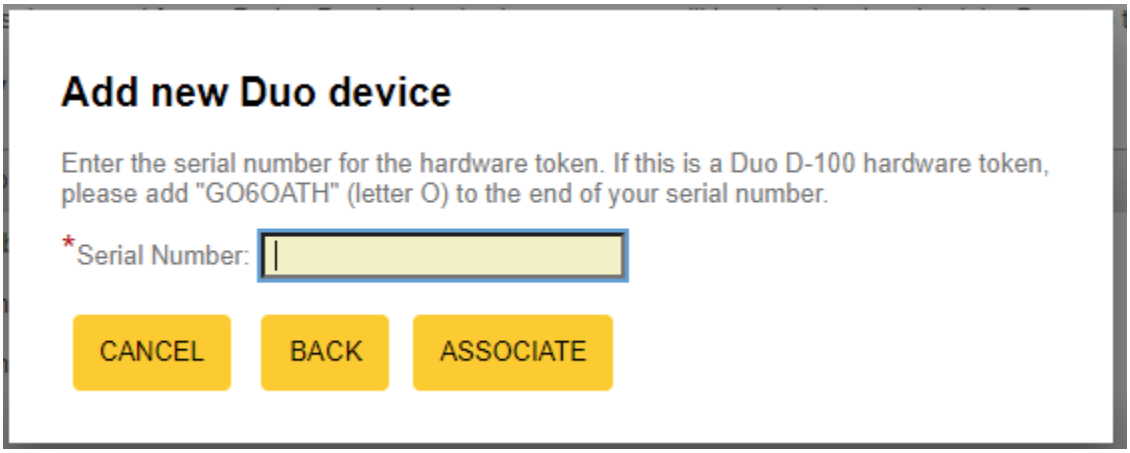
4. Choose **Manage Duo** on the top bar or by clicking the three lines on the right the Manage Duo screen



5. Click **ADD NEW DEVICE**



6. Choose **Hardware Token and click next**
7. Enter the serial number from the back of the Hardware Token (no dashes)



8. Click the **Associate**

Authenticate Using a Hardware Token

1. When the Duo Multi-Factor Authentication window appears, make sure Token is chosen beside device.
9. Press the green button on your hardware token to generate a new passcode. ***Please do not continue to press the green button. It takes a couple seconds for the number to display.***

Figure 1

10. Type the code on the screen in the space provided and press the **Log in** button. You may also select the **Remember me for 30 days** box if available.

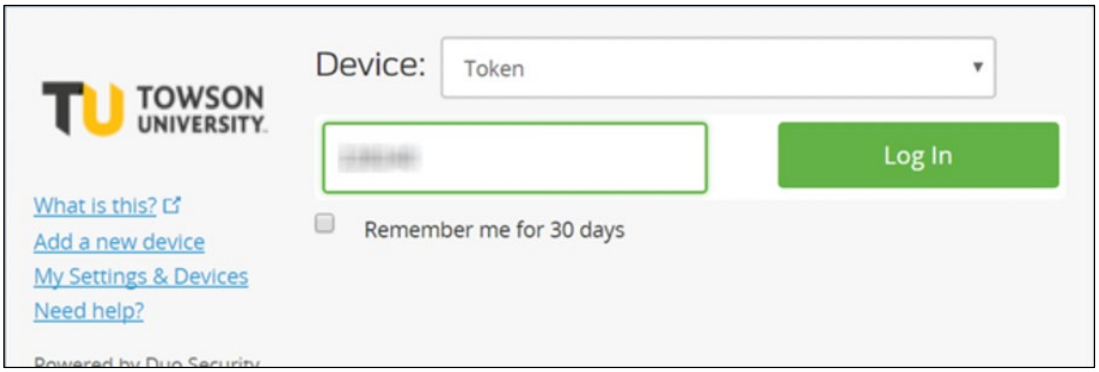


Figure 2

How to Resync your Duo Hardware Token

Tokens can get out of sync if the button is pressed too many times in a row and the generated passcodes aren't used to authenticate with Duo. If this happens, please try authenticating with your hardware token **three** times in a row. The first **two** attempts you will receive the message **Incorrect passcode. Please try again**. On the **third** attempt, you should be granted access.

Figure 3

Note: If this process does not work, contact the OTS Faculty/Staff Help Center by submitting a TechHelp request.