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 hardware tokens are assigned to users and are used to generate a random bypass 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. Submit a TechHelp to request a hardware token.
3. Enroll your hardware token using the steps below.
4. Authenticate using your token.

Use Case Scenarios

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 a Hardware Token

1. From your favorite browser type techhelp.towson.edu.
2. Enter your Username (NetID) and Password on the Tech-Help Authenticated Login screen and click Login.

Figure 1
NetID Management: Duo – Enroll and Authenticate Using a Hardware Token – Faculty/Staff

3. Request type: **Employee Role (Faculty, Staff, Student Workers, etc.)**


5. Next drop down: **Duo Multi-Factor Authentication**

6. Request Detail: Request a Hardware Token because “use a scenario above”

![Figure 2](image1.png)

7. Click the **SAVE** button at the bottom of the page.

![Figure 3](image2.png)

**Note:** The Faculty Staff Help Center will ensure that the client meets the requirements for receiving a hardware token and either approve, deny, or escalate the request. If approved, The Faculty Staff Help Center will arrange a pickup time.

**Enroll your Hardware Token**

1. From your favorite browser type [towson.edu/netid](http://towson.edu/netid).

2. Under the **Manage NetID** section, click the **Manage** link.

![Figure 4](image3.png)

3. Enter your **Username (NetID)** and **Password** on the **Towson University Authenticated Login** screen and click **Login**.

![Figure 5](image4.png)
4. Make sure the **MY PROFILE** tab is chosen at the top of the screen and then click the **MANAGE DUO** tab at the top. You will be able to see **DUO authenticated devices** and **security tokens** linked to your NetID account.

![Duo Authentication Devices](image)

**Figure 6**

5. Scroll down and click on the **ADD NEW DEVICE** button under the **Duo Security Tokens** section.

![ADD NEW DEVICE](image)

**Figure 7**

6. The **Add new Duo device** window will appear.

7. Select **Hardware Token** from the list of devices.

![Device Selection](image)

**Figure 8**

8. Click **NEXT** button after selecting the type of device.

![Next Button](image)

**Figure 9**

9. The **Add new Duo device** window will appear.

10. Enter the **serial number** of the hardware token without the dashes into the required field.

![Serial Number](image)

**Figure 10**

Note: the **serial number** is 10 digits long and is listed on the back side of your **hardware token**.

![Hardware Token](image)

**Figure 11**

11. In the same field, type **GO6OATH** at end of serial number.
12. Click the **ASSOCIATE** button.

![Figure 12]

13. The **successfully added hardware token** window will appear automatically.

![Figure 13]

14. Click the **DONE** button.

![Figure 14]

### Logout

Click the **Logout** button in the upper right-hand corner of the screen when finished.

![Figure 15]

### Authenticate Using a Hardware Token

1. When the **Duo Multi-Factor Authentication** window appears after logging in with your **netid** and **password**, select **Token** from the **Device** dropdown menu.

![Figure 16]

2. Click the **Enter a Passcode** button in the window.

**Note:** The **Enter a Passcode** button will change to **Login**.

![Figure 17]
3. On your **hardware token**, press the green button once and wait a couple seconds for the passcode to be generated and displayed.

![Figure 18](image)

4. Type the displayed passcode into the field on the **Duo Multi-Factor Authentication** window and press the **Log In** button. You may also check the **Remember me for 30 days** box if available.

![Figure 19](image)

**How to Resync your Duo Hardware Token**

**Note:** Hardware Tokens can get out of sync if the button is pressed too many times in a row and the generated passcodes aren't entered into the **Duo Multi-Factor Authentication** window. If this happens, please try authenticating with your hardware token **three** times in a row. On the first **two** attempts, you will receive **Incorrect passcode. Please try again.** On the **third** attempt, you should be granted access.

![Figure 20](image)

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