Duo Security: Overview

Last Modified on 10/26/2020 12:19 pm CDT

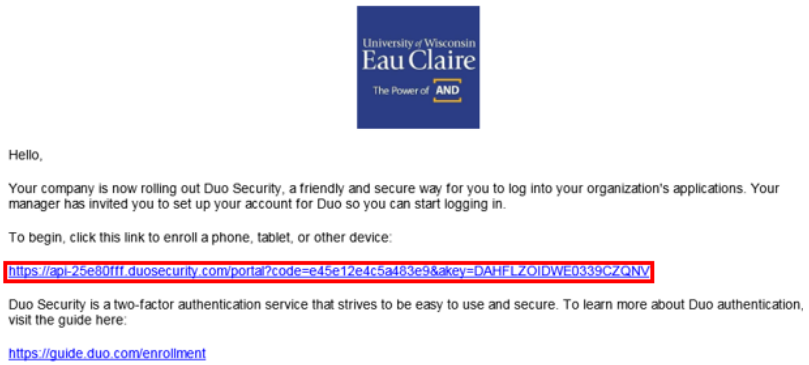
Duo is a multi-factor authentication (MFA) app that adds a layer of protection to your University account. In addition to entering your password, Duo notifies you whenever someone attempts to log into your account, prompting you to either allow the login or deny it.

NOTES:
It is recommended to use a smartphone. If you are using an IOS native email app, you will need to delete and re-add your account in order for Duo to work. For more information on how to do this, read the Email: Configure the Mail App on IOS Devices article.
Duo will not work with the default Gmail mobile app for an Android phone. It is recommended to use the Outlook mobile app.

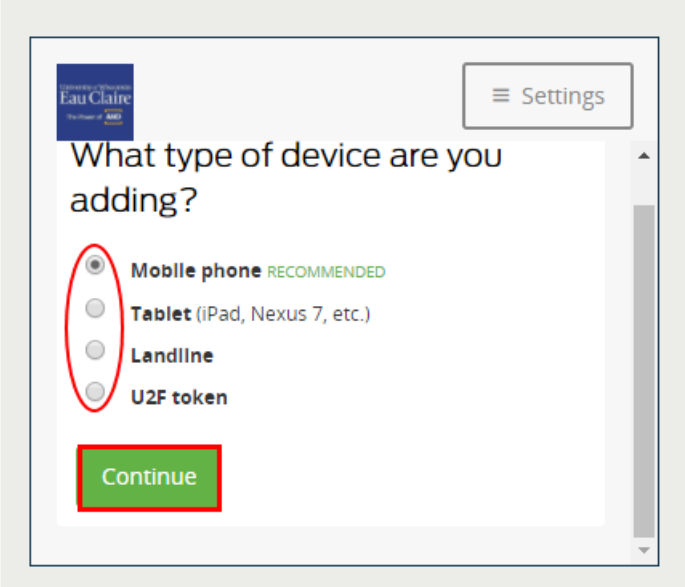
Content

Setting Up Duo Security

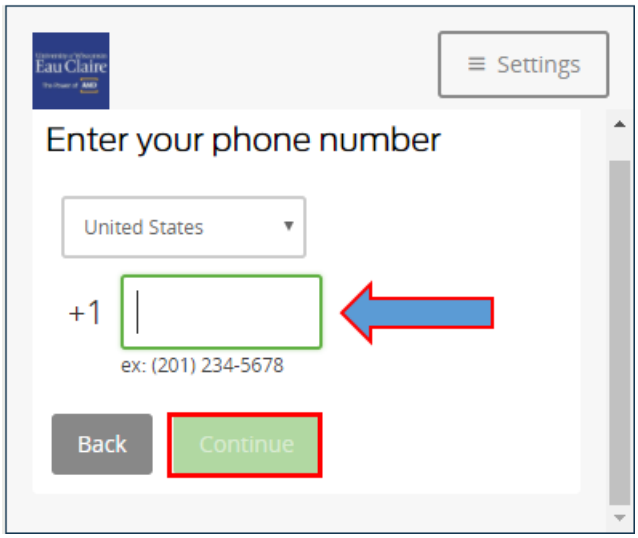
1. Click the link in the Duo Multi-factor email.



2. Click **Start setup**.
3. Select the type of device to enroll.
4. Click **Continue**.

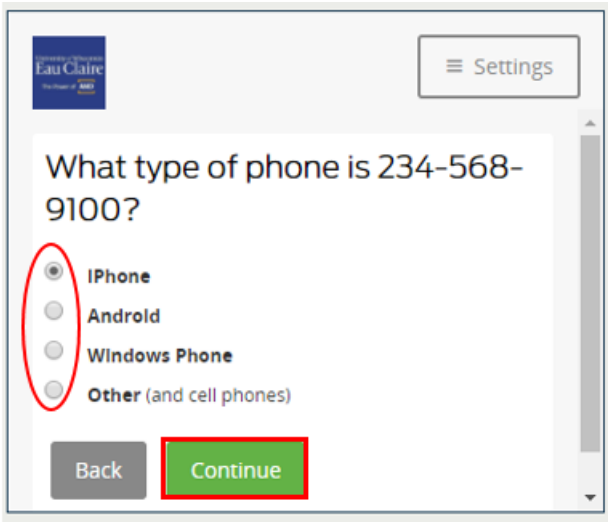


5. Type the number for the device that's enrolled.



6. Click **Continue**.

7. Select the appropriate operating system.



8. Click **Continue**.

Duo Authentication Mechanisms

The primary method of authentication is using the Duo Mobile application. Authentication through Duo token, a SMS message, or phone call is also available, but not preferred. The Duo Mobile application does not require cellular coverage and is more reliable and faster than other options.

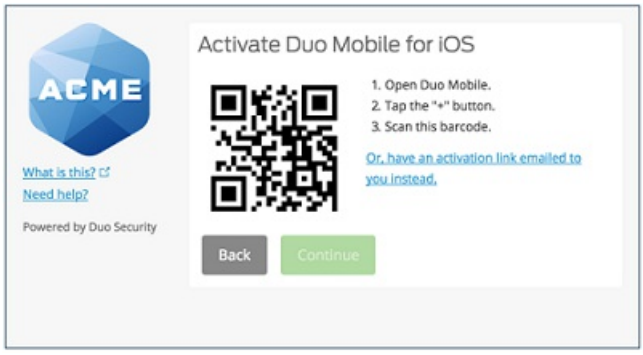
To change your primary Duo authentication mechanism once it's been set, see:Changing Your Default Duo Security Authentication Mechanism.

Duo Mobile Application

The Duo Mobile Application allows you to login by using a push notification or passcode.

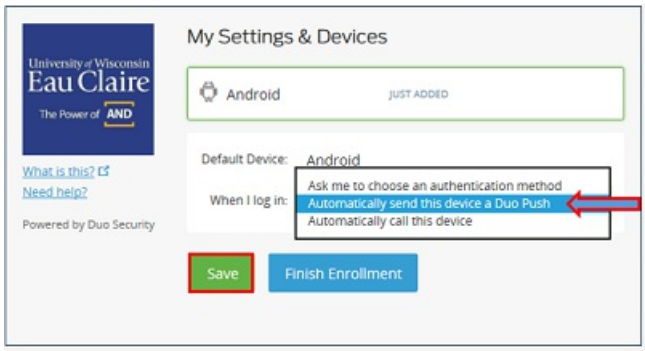
Activate Duo Mobile

1. Install Duo Mobile from your phone's respective app store.
2. Open Duo Mobile.
3. On your phone, tap **GET STARTED**.
4. Using your phone's camera, scan the QR code that appears on the computer screen.



5. Once the QR code is scanned, click **Continue** on the computer.
6. Select an authentication method from the Log In dropdown menu.

   NOTE: You can select any of the methods, but it is recommended that you select ***Automatically send this device a Duo Push****.*



7. Click **Save**.

Using Duo Mobile

Whenever you login using your University account, you will receive a prompt from Duo.

Android

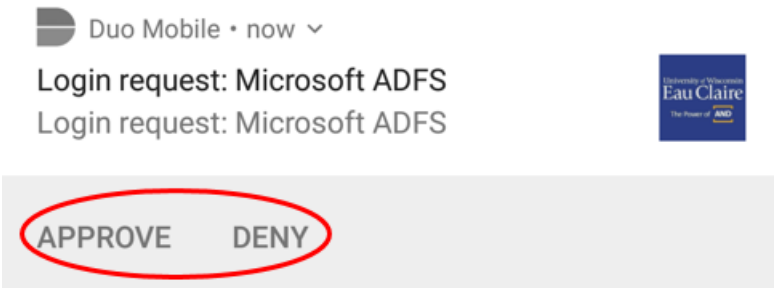
Duo will not work with the default Gmail mobile app on an Android phone. It is recommended to use the Outlook mobile app.

Push

With Duo Push, a notification will be sent to your phone. You may approve this push by accessing it through the notification bar of your phone or on the Duo app.

Push via Notification Bar

1. Tap either **APPROVE** or **DENY**.



2. (Optional) If you tapped APPROVE, tap **CONFIRM** to approve the login

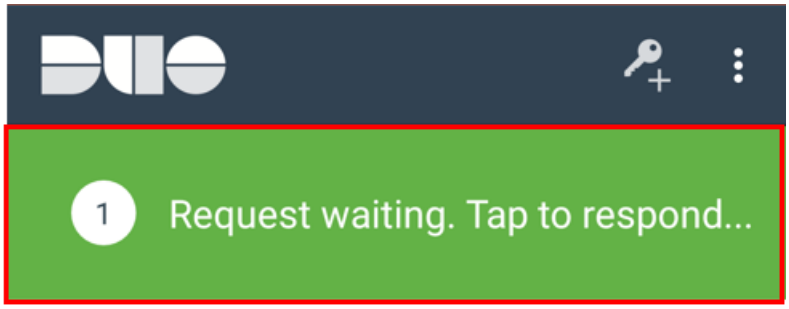
   OR

   tap **CANCEL** if you made a mistake.

3. (Optional) If you tapped DENY, select why the login is being denied.

Push via Duo App

1. Tap the **Request waiting. Tap to respond...** banner.



2. Tap either **Approve** or **Deny**.
3. Select why the login is being denied.

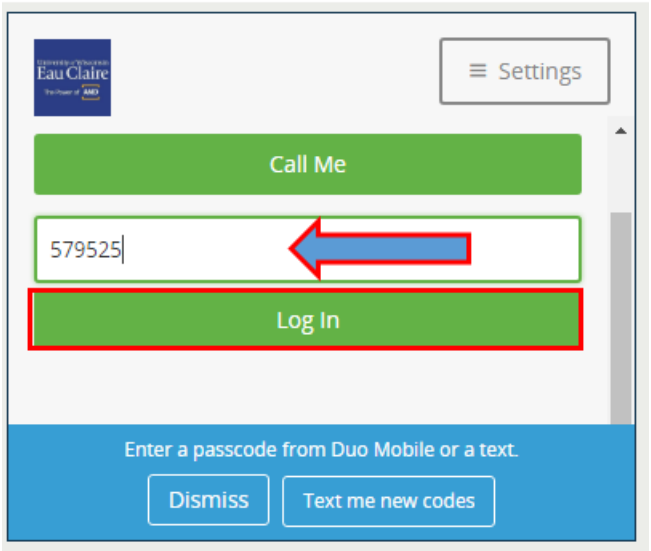
Passcode via Duo App

The Duo Mobile app also allows you to generate a passcode to login.

To enter a passcode:

1. Tap the key icon.

2. Type the given passcode from your phone onto the computer.
3. Click **Log In**.



iPhone

It is recommended that you download the Outlook client for the best experience on your iPhone from the

Apple Store.

Push via Duo App

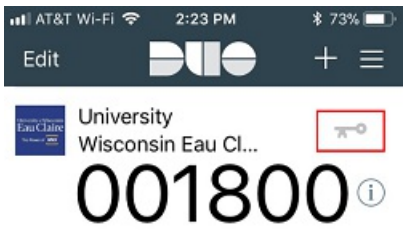
With Duo Push, a notification will be sent to your phone.

1. Tap either **APPROVE** or **DENY**.

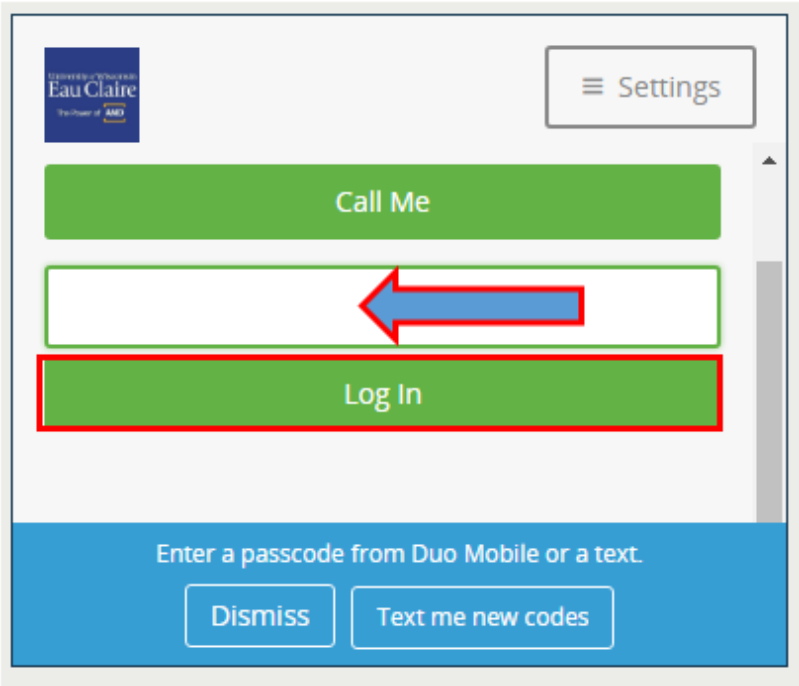
Passcode via Duo App

To enter a passcode:

1. Tap the key icon.



2. Type the given passcode from your phone onto the computer.



3. Click **Log In**.

Using Duo Tokens

A security token is a small hardware device used to authorize access to a network. This physical device resembles a key fob and can prove useful for those without Internet or mobile device access since it does not require cellular data or a WiFi connection. For example, students and faculty studying abroad or international students may want to acquire a Duo token to access applications on the UW-Eau Claire network.

Requesting a Token

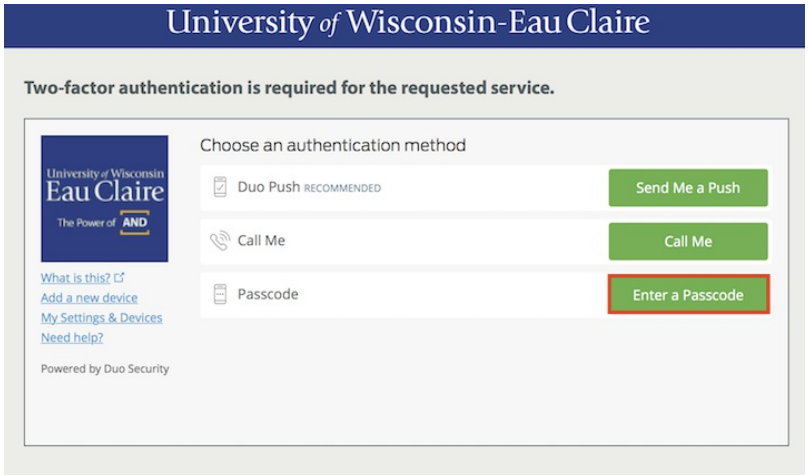
- Complete the Token Request eForm

Note, those filling out the Token Request eForm who do not have a supervisor, can enter UW Eau Claire's Chief Information Security Officer, Steve Ranis, as their supervisor/manager.

SMS/Text Message

A user may login by requesting a SMS/text message to be sent to their phone. This message will contain a passcode.

1. Click **Enter a Passcode.**



2. Click **Text me new codes.**

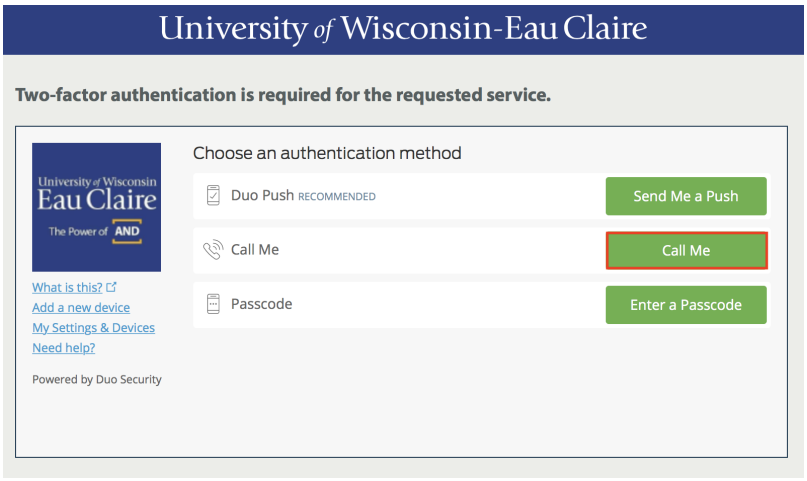
3. You will receive a SMS/text message containing the code.

4. Type the passcode into the *Login* field.

Phone Call

A user may login by requesting a phone call from Duo.

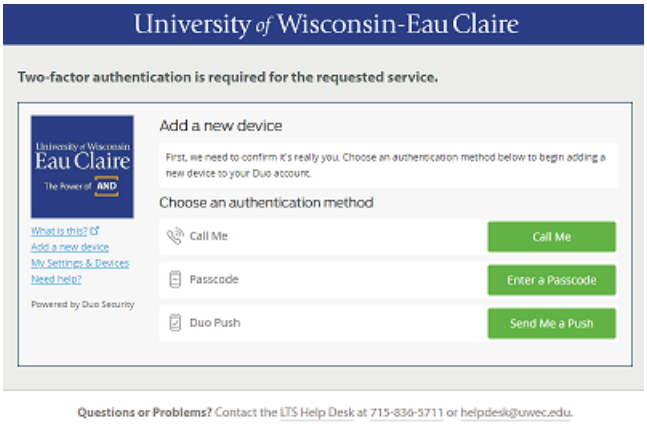
1. Click **Call Me.**



2. Answer the call.
3. Touch any button on your phone keypad to login.

Adding a New Device

1. Navigate to your Duo protected app (i.e. CampS, Office 365, etc.)
2. Login using your university credentials.
3. Click **Add a new device**.



4. Confirm your identity by choosing one of the two-factor authentication methods.

5. Once authenticated, select the type of device you are adding.

   NOTE: It is recommended to add a mobile device.

6. Click **Continue**

7. Type the number of the new device.
8. Click **Continue**.

9. Select the type of phone.
10. Click **Continue**.

11. Activate the new device by following the steps in theActivate Duo Mobile section.

Duo Security FAQ

What is Duo Security and How Will it Affect Users?

What is Duo Security?

- Duo Security uses multi-factor authentication to act as an additional layer of protection when logging into University of Wisconsin-Eau Claire online programs.

What is Multi-Factor Authentication?

- Multi-factor authentication (MFA) matches your login credentials with a personal device, providing two forms of login verification. Once a user provides their login credentials, a notification will be sent to your designated personal device asking for login approval.

What University Platforms Use Duo Security?

- The University of Wisconsin-Eau Claire requires Duo Security on CampS for all users.
- Staff members are required to use Duo Security for Office365.
- In the future, Duo Security will be implemented on other University operating systems and databases.

Who is Eligible for Duo Security?

- Multi-factor authentication through Duo Security is available for all faculty and staff.

How Does Duo Security Affect Me?

- When MFA is required, a user must provide:
    - Their UWEC username and password

      A designated device to confirm your Duo Security notification.

Will Wisconsin's Public Records Law Apply to Personal Content on my Device?

- No, using Duo Security on your personal device will not subject your personal communication to Wisconsin's Public Records Law. However, communication on your personal device regarding the University of Wisconsin-Eau Claire is subjected to Wisconsin's Public Records Law.

What If a Mail Client Does Not Support Duo Security?

- If a client has mail protocols such as Post Office Protocol (POP) or Internet Message Access Protocol (IMAP), they will still be allowed to function without Duo Security.

Which applications have Multi-Factor Authentication implemented?

- Amp+
- *Blackboard
- CampS
- CampusCall
- Canvas

- Cashnet
- Campus Loan Manager (CLM)
- Cherwell
- Cloud Lock+
- D2L
- EAB
- Easy Morph
- eForms
- Financial's Edge (NXT)
- Financial's Edge web portal (NXT)
- GlobalProtect VPN
- HRS Software+
- Interface to US Bank (Formerly Pennybags)
- Maxient
- Mayo Health App (Admin Only)
- Mercury (RMS)
- Nelnet
- Next Gen
- Office 365
- Oracle BI Project
- Orchard
- P2PEManager
- Perceptive Content
- PointNClick: GUI
- PointNClick: Web Portal
- ProCare
- Qualtrics (Anonymous surveys, Individual users)
- **Qualtrics (Shared Acounts)
- Raiser's Edge (NXT)
- Sever Management Console
- Shared Financial System (SFS)+
- SilverCloud+
- Slate
- Stealth Watch+StudentAccess
- StudentAccess
- Telefunds (Ruffalo-Cody)
- Terra Dotta ISSS (CIE)
- Terra Dotta Study Abroad (CIE)

- Titanium
- Toolbox
- Tutor Track (Red Rock)
- Umbrella+
- UW System Portal (my.wisc)
- Valt
- WISDM

*NOTE: + - Indicates UW System hosted application, * - Scheduled for Fall 2020, **- Scheduled for Winter Break 2021*

How Should I Start Using Duo Security?

How do I Set-Up Duo Security?

- To set-up multi-factor authentication, you must download the Duo Security Mobile application on a personal device, such as a smartphone or tablet. If you do not want to download the Duo Security Mobile application, you may request a token that will create a six-digit passcode to validate your identity.

Can I Still Login if I do not Have My Login Device?

- You may receive a temporary password by calling the Learning Technology Services HelpDesk at 715-836-5711.

What Are Tokens?

- A token is a small portable device that a user can use to authorize their desired login through Duo Security. The token creates a six-digit passcode that the enables the user to successfully login to any UW-Eau Claire platforms that requires Duo Security.

How Should I Use My Token?

- Press the green button on the token. This will create a six-digit passcode.
- Type this passcode into the Duo Security login portal.
- Click **Enter a Passcode**.

Where Do I Receive My Token?

- Complete the Token Request eForm

NOTES: those filling out the Token Request eForm who do not have a supervisor, can enter UW Eau Claire's Chief Information Officer, Chip Eckardt, as their supervisor/manager.

How Much Does a Token Cost?

- Any current faculty, staff, or student will be initially be given a token upon request.

Is There Anywhere I Can Go on Campus for Help?

- You may contact the University of Wisconsin-Eau Claire's Learning Technology and Services department.
  - Phone: (715)-836-5711
  - Email: helpdesk@uwec.edu
  - Location: Vicki Lord Larson Hall 1106

How Do I Use Duo Security?

Can I Still Login If I do not Have My Phone/Token?

- There are three options to solve this problem.
  - You may receive a temporary passcode by calling UWEC helpdesk at (715)-836-5711. Your identity will be verified after answering multiple security questions.
  - You may also generate a password that will be used as a backup code.

What Should I do If My Password Created by My Token is not Working?

- Check if the token is right side up, making sure you are not entering the numbers upside down.

Will My Account Get Locked After A Certain Number of Failed Login Attempts?

- Yes, your account will be locked for 30 minutes if there are 100 consecutive failed login attempts.

Why Am I Not Receiving Duo Security Push Notifications on my iPhone or Android?

- If your push notifications are not showing up, pull down your notification tab from the top of your phone to check all recent notifications.

How Should I Login If My Device does not Have Service or is on Airplane Mode?

- The Duo Security Mobile application can give you a one-time use password even if your device does not have service.
  - To access this, open the Duo Security Mobile application
  - Then, navigate to the upper-left hand corner of your screen
  - Click the **Key Icon** or **Down Arrow**
  - Type in the six-digit generate password into the Duo Security Mobile application portal.

How Should I Login If My Device does not Have WiFi?

- The Duo Security Mobile application can give you a one-time use password even if your device does not have service.
  - To access this, open the Duo Security Mobile application
  - Then, navigate to the upper-left hand corner of your screen

    - Click the **Key Icon** or **Down Arrow**
    - Type in the six-digit generate password into the Duo Security Mobile application portal.

Is Duo Security Authentication Needed Every Time I Login?

- There is a "Remember Me" option you may select on the Duo Security screen while logging in. This option will ensure login for 12 hours without needing to use Duo Security.

What Should I do if the "Remember Me" Option is Unavailable?

- This option will need to be turned on if you have previously selected the default option for Duo Security to automatically send a push notification to your device.
- In order to turn "Remember Me" on, follow the below steps.
    - Click **Cancel** on your current login
    - Click the **"Remember me for 12 Hours"** box
    - Login by clicking the down arrow to create a six-digit passcode, using your token to login, or clicking **Send Me a Push**.

In Order to Login into my Workstation, Do I Need to Use Duo Security?

- No, users do not have to use Duo Security in order to login to your workstation.

How does Multi-Factor Authentication (MFA) work if I am traveling or studying abroad?

- For those traveling or studying abroad, phone service may be a challenge depending on your phone carrier's service level and may even depend on the specific plan you have. An easy way to avoid issues is to use a hardware token or fob that will provide the MFA response. Using a hardware token does not require cellular phone access or wireless network access. It is completely stand-alone and works independently of your phone.

- See the Requesting a Token section above for detail on getting your own token.

Contact

For questions or support in using Duo Mobile, contact theLTS Help Desk (836-5711)