

MFA

MULTI-FACTOR AUTHENTICATION

USER GUIDE



FORDHAM UNIVERSITY



Choose an authentication method

- One Push recommended **Send Me a Push**
- Call Me **Call Me**
- Passcode **Enter a Passcode**
- Remember me for 1 hour

Powered by Duo Security

FORDHAM
THE SEVENTH UNIVERSITY OF NEW YORK



User Guide Contents

What is Multi-Factor Authentication (MFA)?	2
Why Does Fordham Use MFA?	2
How Does MFA Work?	3
Supported Devices	4
How to Enroll in MFA	5
Receiving Your First Push Notification	11
Add or Manage Devices	11
Adding a new device	11
Manage existing devices	12
Frequently Asked Questions	13
Will I be prompted by MFA every time I login to Fordham.edu?	13
Can I set up MFA on more than one device?	13
What if the Duo mobile app stops working?	13
Do I need a smartphone to use MFA?	14
What if I forget my phone at home?	14
What if I lose my phone?	14
What if I don't have a cell phone?	14
What if I don't have a data plan on my smartphone or tablet?	14
What if I don't have an Internet connection or cell phone service?	15
What if my browser is set up to clear cache/cookies upon exiting?	15
Who do I contact with questions about required use of MFA?	15
What information is shared with Duo Security?	15
What if I receive an unexpected login alert?	15
Can I use the Duo Mobile App internationally?	16
Why does the MFA screen look different on different devices?	16



This work is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 3.0 United States License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-sa/3.0/us/> or send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.

What is Multi-Factor Authentication (MFA)?

Multi-factor authentication (MFA), also referred to as two-factor authentication, provides an extra layer of security when you login to an account online. You may already be using MFA with your bank, credit card, or Social Security accounts.

All active, online accounts (student, faculty, and staff) at Fordham University are required to enroll in MFA. Duo Security, a trusted company used by many higher education institutions, provides our MFA service.

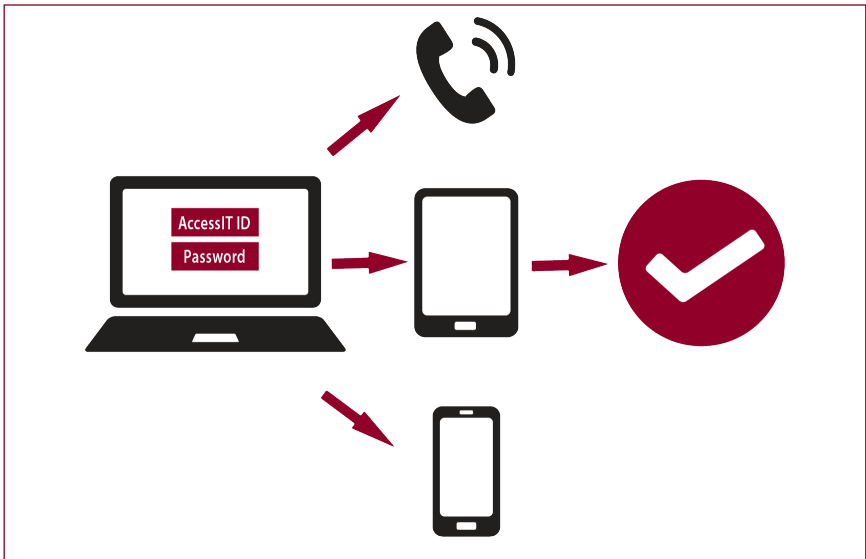
MFA is simple to use: When you login with your password, you will receive an authentication request on a device such as a smartphone, cell phone, tablet, or landline to finish the login process.

In other words, MFA combines something you know (your password) with something you have (a device), to fulfill an authentication request and complete your login process.

Why Does Fordham Use MFA?

Fordham University is committed to protecting the identity and personal information of its community members. We use multi-factor authentication to reduce the risk of unauthorized users gaining access to Fordham accounts.

Data security continues to be a concern in the private and public sectors, including corporations of all sizes, government organizations, and schools. Hackers target higher education institutions for their intellectual property, personally identifiable information, and financial information.



How Does MFA Work?

1. To login to a Fordham system, enter your Fordham username and password, as usual.
2. If you login to Fordham.edu or another Fordham system, use your phone or tablet to verify your identity when prompted by Duo.
3. Securely complete the login process.

You may opt to have your authentication remembered for 30 days, if you are using the same browser on the same device.

Phones and devices to verify your identity

A smartphone, landline, cell phone, tablet, or in some situations, a hardware token, may be used to verify your identity for MFA. When you enroll with Duo, our MFA service provider, or anytime thereafter, you can set up one or more devices for authenticating, such as your mobile phone and a landline, two different mobile devices, or a landline and a hardware token when traveling.

We encourage you to enroll multiple phones and devices as a backup in case your preferred device is not available (i.e., left at home, battery depleted).

Ways to verify your identity

Push notifications to smartphones and tablets

With the Duo MFA mobile app, Duo Mobile, a notification is pushed to you in response to the authentication request that you approve or deny.

SMS passcodes

A six-digit passcode in a SMS text message is sent to your registered mobile device. No Internet connection is required. Enter the passcode at the multi-factor prompt during login.

Mobile passcodes

Similar to SMS, the Duo MFA mobile app, Duo Mobile, generates a new, unique six-digit passcode to enter at the multi-factor prompt during login.

Phone callbacks

Your enrolled phone number is called. Answer the phone, listen to the whole message, and press a specific number to complete the login. In addition to the "access number," you will be given another number to press to report a fraudulent call regarding your login. The numbers may change periodically.

Hardware tokens

The hardware token is a small device you carry. Pressing a button on the token generates a new passcode that you type into the multi-factor prompt. No connection to the Internet is required. All requests for hardware tokens must be approved by the Associate Vice President of Fordham's University Information Security Office. A \$20 fee will be charged for lost tokens.

Read more about hardware tokens.

Supported Devices

- Smartphones (Android, iOS, Windows)
- Tablets (iOS, Android)
- Cell phones and landlines
- Hardware tokens

How to Enroll in MFA

You will be asked to enroll in MFA via an email sent from Duo Security or when you first encounter an MFA-enabled application through a browser. You will enroll the phones, tablets, and/or other devices you will use for authentication to Fordham systems. Duo will not ask for your Fordham password.

To enroll, use a browser interface (such as Chrome, Firefox, Safari, Edge, and Internet Explorer) on a desktop or laptop computer. Alternatively, you may use a mobile device or tablet to enroll and request an activation link be sent to a non-Fordham email address that you can access on your mobile device or tablet.

If you need help during the enrollment process, please contact the IT Service Desk at 718-817-3999, HelpIT@fordham.edu, or via the Tech Help page at Fordham.edu.

1. Welcome screen

To begin the enrollment process for MFA, click Start setup.

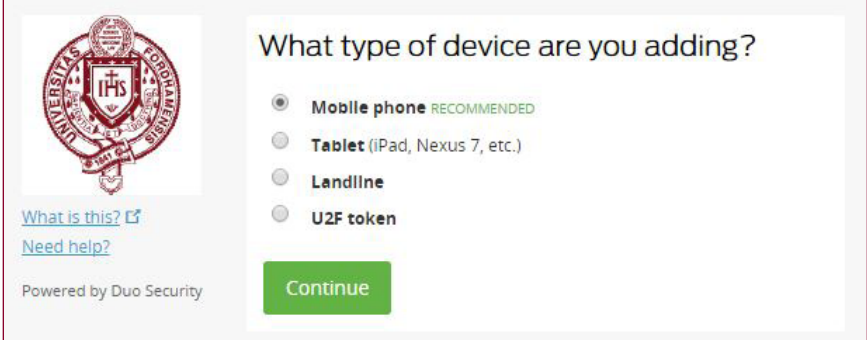


The screenshot shows a web interface for enrolling in Multi-Factor Authentication (MFA) for a Fordham University account. On the left is the Fordham University crest. To its right, the heading reads "Protect Your Fordham University - Account". Below the heading, there are two paragraphs of text explaining that two-factor authentication enhances security by using a secondary device. At the bottom of the text area is a green button labeled "Start setup". On the left side of the screen, there are two links: "What is this?" and "Need help?", and a note stating "Powered by Duo Security".

2. Choose your authenticator

Select the type of device you'd like to enroll and click Continue. The device can be a smartphone, cell phone, landline telephone, or tablet (Apple OS or Android). If none of those devices is suitable, you may request a hardware token from the IT Service Desk. The Associate Vice President of Fordham's University Information Security Office approves requests for hardware tokens.

A \$20 fee will be charged for lost tokens. Learn more about **hardware tokens**.



What type of device are you adding?

- Mobile phone** RECOMMENDED
- Tablet** (iPad, Nexus 7, etc.)
- Landline**
- U2F token**

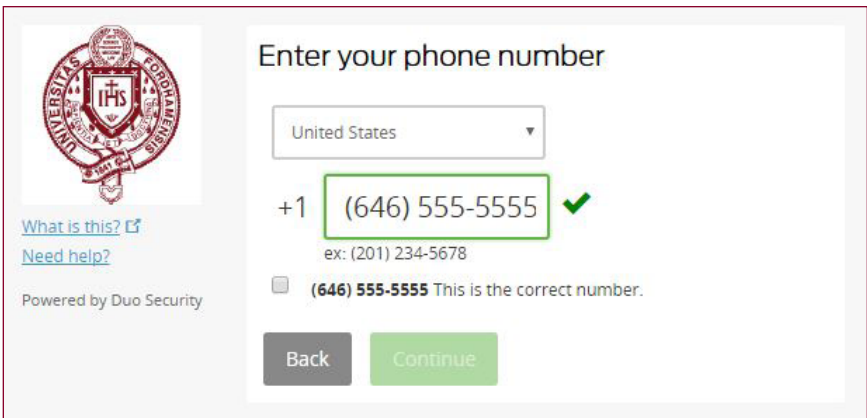
[What is this?](#) [Need help?](#)

Powered by Duo Security

Continue

3. Provide your phone number

Select your country from the drop-down list. Enter your phone number for the device you'll use for authentication when you're logging into a Fordham system. Enter an extension if you chose Landline in the previous step. If you enroll a tablet, you will not be prompted to enter a phone number.



Enter your phone number

United States

+1 (646) 555-5555 ✓

ex: (201) 234-5678

(646) 555-5555 This is the correct number.

Back **Continue**

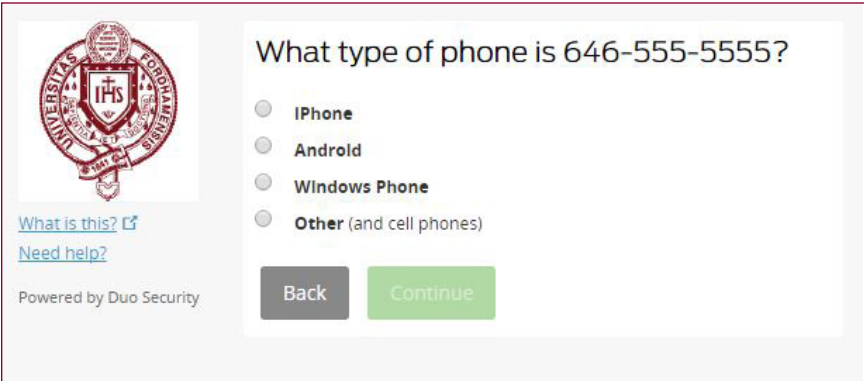
[What is this?](#) [Need help?](#)

Powered by Duo Security

Please double-check that your phone number is entered correctly, check the box, and click Continue.

4. Choose platform

Choose your device's operating system and click Continue.



What type of phone is 646-555-5555?

- iPhone
- Android
- Windows Phone
- Other (and cell phones)

Back Continue

[What is this?](#) [Need help?](#)

Powered by Duo Security

5. Install and use Duo Mobile app

The Duo Mobile app is fast and easy. It works in any country and doesn't require cell service.

Duo Mobile allows you to authenticate quickly and easily on a smartphone or tablet. It's a great alternative to authenticating with a phone call or entering a passcode.

Download Duo Mobile from your app store and follow the installation instructions. After it's installed, return to the enrollment window for installing Duo Mobile and click I have Duo Mobile installed.



[What is this?](#)

[Need help?](#)

Powered by Duo Security

Install Duo Mobile for iOS



1. Launch the App Store app and search for "Duo Mobile".
2. Tap "Get" and then "Install" to download the app.

Tap "OK" when asked if Duo Mobile should be able to send push notifications.

Back

I have Duo Mobile installed

6. Activate Duo Mobile

To use Duo Mobile for authentication, activate and link it to your account. There are two ways to activate the app:

1. On iPhone, Android, and Windows phones, scan the barcode that appears on your computer with the app's built-in barcode scanner. Follow the platform-specific instructions for your device.
2. Alternatively, request an activation link be emailed to you and follow the prompts on your screen. If using a mobile device or tablet to enroll, be sure to request the activation link be sent to a non-Fordham email address that you can access on your mobile device or tablet.



[What is this?](#)

[Need help?](#)

Powered by Duo Security

Activate Duo Mobile for iOS



1. Open Duo Mobile.
2. Tap the "+" button.
3. Scan this barcode.

[Or, have an activation link emailed to you instead.](#)

Back

Continue

The Continue button is clickable after you successfully scan the barcode.

Activate Duo Mobile for iOS

1. Open Duo Mobile.
2. Tap the "+" button.
3. Scan this barcode.

[Or, have an activation link emailed to you instead.](#)

[What is this?](#) [Add a new device](#) [My Settings & Devices](#) [Need help?](#)

Powered by Duo Security

[Back](#) [Continue](#)

7. My Settings & Devices: Configure Device Options

Be sure to add a second phone or other authenticator as a backup device. Click Add another device to repeat the enrollment process. You may give your device a descriptive name by using Device Options in My Settings & Devices.

For the device you'll use most often with Duo, you may want to enable automatic push requests by changing the "When I login" setting from "Ask me to choose an authentication method" to "Automatically send this device a Duo Push," or "Automatically call this device," and click Save. When one of these options is enabled, Duo automatically sends an authentication request via push notification to the Duo Mobile app on your smartphone or a phone call to your device (depending on your selection).

My Settings & Devices

iOS 646-... [Device Options](#)

[+ Add another device](#)

Default Device: iOS 646-...

When I log in: [Ask me to choose an authentication method](#) ▼

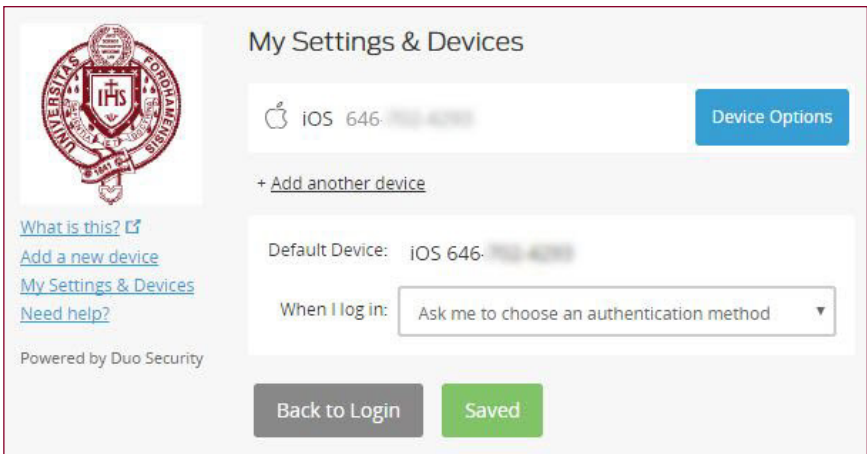
- [Ask me to choose an authentication method](#)
- [Automatically send this device a Duo Push](#)
- [Automatically call this device](#)

[Back to Login](#) [Save](#)

[What is this?](#) [Add a new device](#) [My Settings & Devices](#) [Need help?](#)

Powered by Duo Security

Click Back to Login and proceed to the authentication prompt.



My Settings & Devices

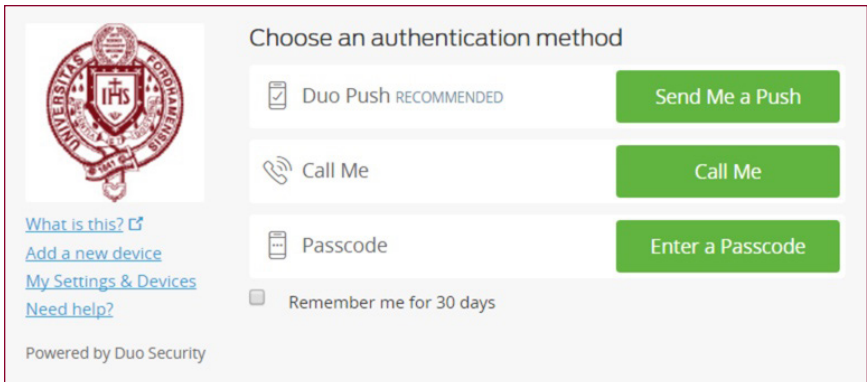
What is this? [Add a new device](#) [My Settings & Devices](#) [Need help?](#)

Powered by Duo Security

Back to Login Saved

Receiving Your First Push Notification

Click Send me a Push to give MFA a try. All you need to do is tap Approve on the Duo login request received at your phone.



Choose an authentication method

What is this? [Add a new device](#) [My Settings & Devices](#) [Need help?](#)

Powered by Duo Security

Duo Push **RECOMMENDED** [Send Me a Push](#)

Call Me [Call Me](#)

Passcode [Enter a Passcode](#)

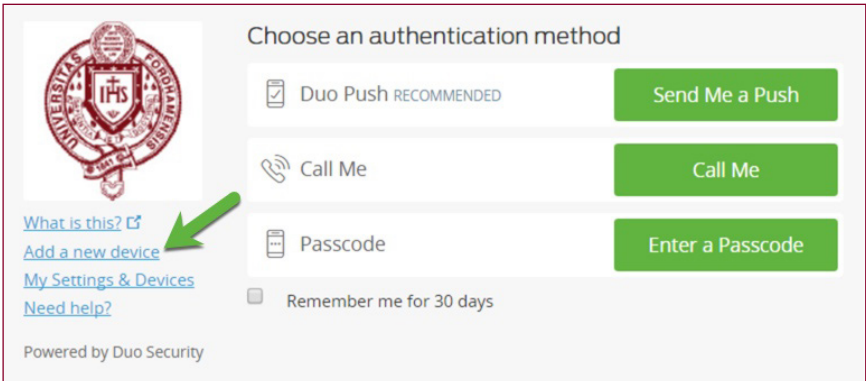
Remember me for 30 days

Select “Remember me for 30 days” so you won’t have to authenticate for a month. Choose this option when using the same browser on your device.

Add or Manage Devices

Adding a new device

You can easily add new devices right from the Duo authentication prompt. To enroll a new device, select Add a New Device. If using a smaller screen, click the Settings button at the top right of the Duo authentication prompt.



To add your new device, choose an authentication method and complete the multi-factor authentication process described above.

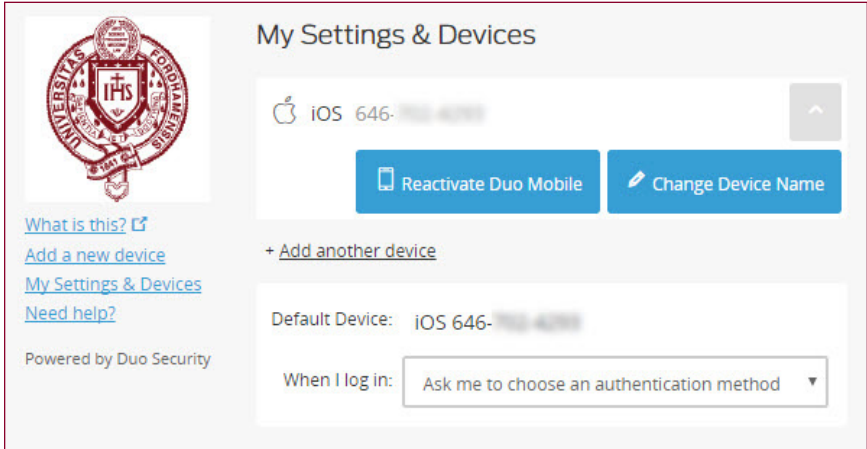
If you've checked the "Remember me for 30 days" option for authentication, you won't get the authentication prompt when using the same browser on your device until the 30-day period has expired. You can get a new prompt now by logging into the Fordham.edu portal with a different browser.

If you're adding a new device to replace one that you previously activated for Duo Push, don't select the Duo Push authentication method on this page unless you still have the original device. If you don't have the original device, but you have a new device with the same phone number, then you can authenticate with a phone call or SMS passcode.

You can't add a new device from this page if you do not have access to any of your previously enrolled authentication devices; you'll need to contact the IT Service Desk for help.

Manage existing devices

Click the Device Options button next to any of your enrolled devices to view the actions available for that type of device. Here you can Reactivate Duo Mobile for an enrolled smartphone, Change Device Name for any type of phone, or delete any authentication device.



My Settings & Devices

[What is this?](#) [Add a new device](#) [My Settings & Devices](#) [Need help?](#)

Powered by Duo Security

Default Device: iOS 646-780-4288

When I log in: Ask me to choose an authentication method

Frequently Asked Questions

Will I be prompted by MFA every time I login to Fordham.edu?

You *will not* be prompted to verify your identity with MFA for a month if you have opted to have your authentication remembered for 30 days when using the same device and browser.

You *will not* be prompted to verify your identity with MFA when using a wired device (desktop or laptop) on campus in administrative and faculty offices.

You *will not* be prompted to verify your identity with MFA when using the *wireless network* at the Health Center and Counseling and Psychological Services.

You *will* be prompted to verify your identify with MFA when you're using a *wired* computer in a public area, such as the labs, libraries, any residence hall, or at a smart podium.

You *will* be prompted to verify your identify with MFA when accessing Fordham systems *wirelessly* (via a laptop, tablet, or smartphone) and when logging in with VPN or Mydesktop.

Can I set up MFA on more than one device?

Yes! You should set up MFA on more than one device as a backup in case your preferred device is not available (i.e., left at home, battery depleted). During the initial set up or anytime you go to your Duo Security account, you may add as many phones/devices as you like (landline and/or mobile). Login to Duo Security to choose which device Duo will send the authentication request to (via Duo Mobile app, SMS text message, or phone call).

What if the Duo Mobile app stops working?

When you get a new phone, it will lose its association with your Duo account, even if you install Duo Mobile on the new device. If the phone number of your new phone is the same, you can still authenticate using the phone call or SMS option, but the push option will not work until re-activated.

Re-activate your new phone with the Manage devices option.

1. Ensure that you still have access to any of the phone numbers enrolled in Duo.

-
2. Set the authentication option to Phone call and select Manage device. When the selected phone rings, answer and hit any key to authenticate.
 3. From here, you can select the phone number of your new phone (assuming it's the same phone number) and under Actions, select Activate Duo Mobile. This will prompt you to scan in a new QR code from the Duo app. If you have difficulties with this process, you can submit a service request to the IT Service Desk via Fordham.edu > Tech Help page or call 718-817-3999 for immediate assistance.

Do I need a smartphone to use MFA?

No. Duo provides a great deal of flexibility and there are other options in lieu of a smartphone. Duo can send a text message to a regular cell phone or place a voice call to your office/home landline. In some situations, a hardware token can be provided to use in verifying your identity (the token does not require an Internet connection).

What if I forget my phone at home?

Contact the IT Service Desk. They will verify your identity and provide a temporary passcode. We encourage you to then go into Manage devices and add an additional device. Please refer to Adding a new device.

What if I lose my phone?

Contact the IT Service Desk immediately. They will verify your identity, delete your lost phone from your Duo account to prevent malicious activity, and provide a temporary passcode. Please refer to Adding a new device.

What if I don't have a cell phone?

If you don't have a cell phone, Duo allows you to use your landline phone. You'll receive an automated phone call that requires you to hit any button to confirm your identity. In some situations, a hardware token will be distributed for use in verifying your identity.

What if I don't have a data plan on my smartphone or tablet?

Open the Duo Mobile app on your smartphone/tablet and select the key icon in the bar labeled "Fordham University" to generate a six digit passcode for one-time use to login. This method does not use data nor incur any charges.

What if I don't have an Internet connection or cell phone service?

Open the Duo Mobile app and generate a single passcode by tapping the key icon in the bar labeled "Fordham University." This method works anywhere, even in places where you don't have an Internet connection or can't get cell service.

Alternatively, if you anticipate not having a connection, you can request an SMS passcode in advance. Enter the pre-generated passcode at the MFA prompt during login. Batches of 10 SMS passcodes can be requested by choosing the "Enter a passcode" option on the authentication window and clicking "Text me new codes" in the blue bar at the bottom of the window. Each batch is valid for 30 days. A passcode, once used, cannot be used again.

What if my browser is set up to clear cache/cookies upon exiting?

The "Remember your device for 30 days" option uses a persistent cookie. If you clear cookies after you log off the browser, the device will not be remembered. You will have to confirm your identity when you login again.

Whom should I contact with questions about the requirement to use MFA?

We encourage you to contact the Associate Vice President of Fordham's University Information Security Office with feedback or questions about MFA. The AVP can be reached directly at infosec@fordham.edu.

What information is shared with Duo Security?

Duo only stores your Fordham username, email address, and authentication device information, such as your phone number. Duo does not have access to your Fordham password.

What if I receive an unexpected login alert?

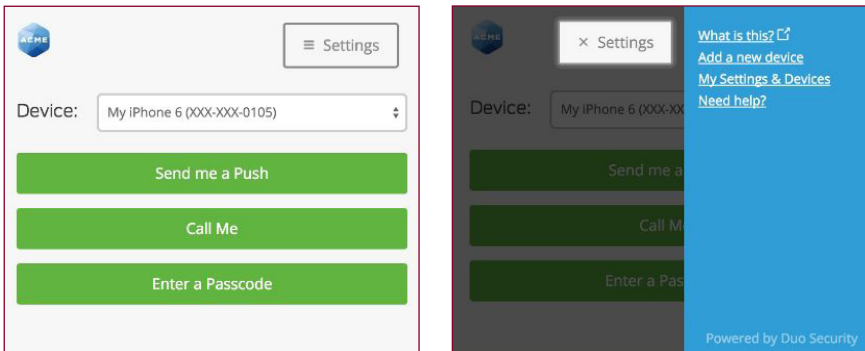
If you receive a notification (a login alert on the Duo Mobile app, a phone call from the authentication system, or a passcode via text message) that you did not initiate via the login process, your Fordham username and password may have been compromised. Reject the login and change your password as soon as possible. Go to [Fordham.edu](https://fordham.edu), select Log In, select Change password below the Login button, and follow the instructions.

Can I use the Duo Mobile App internationally?

The Duo Mobile App is designed to work internationally. If you use the app, tap the key icon in the bar labeled “Fordham University” to generate the required six-digit passcode without need of either a telephone signal or data plan. You can do this anywhere in the world.

Why does the MFA screen look different on different devices?

If you’re logging in with Duo from a device with a smaller screen (like a tablet) or small browser window, your authentication prompt may look slightly different. Don’t worry! All the devices and options shown in the full-size prompt are available for use, and you can enroll and manage devices by following the same steps.



Access Add a new device or My Settings & Devices by clicking the Settings button at the top. Click the X on the Settings button to return to the authentication prompt.



Choose an authentication method

- Duo Push recommended Send Me a Push
- Call Me Call Me
- Passcode Enter a Passcode

Remember me for 1 hour

Powered by Duo Security

FORDHAM
THE SEASIDE UNIVERSITY OF NEW YORK



USER GUIDE



Fordham IT

718-817-3999 | HelpIT@fordham.edu

[@FordhamIT](https://twitter.com/FordhamIT) | fordham.edu/IT

Providing high quality technology support and resources for teaching, learning, research, and campus life at Fordham University.