Multi-Factor Authentication FAQs

General FAQs

What is Multi-factor Authentication (MFA)?

Multi-factor authentication (MFA) seeks to decrease the likelihood that others can access your data. Specifically, it enhances the security of your NetID by using your phone, tablet or other device to verify your identity when you attempt to access Yale's network and resources from an off-campus location.

It takes two items to access and update your information: “something you know” (like your password) and “something you have” (like your phone). For example, when you visit an ATM, one authentication factor is the ATM card you use to start the transaction - that’s the “something you have.” Next, you enter a PIN, which is the “something you know.” Without both of these factors, your authentication will fail.

Why Do I Need to Use MFA?

Passwords are becoming increasingly easy to compromise. They can be stolen, guessed, and hacked, and new technology and hacking techniques combined with the limited pool of passwords most people use for multiple accounts means information online is increasingly vulnerable. You might not even know who else has your password and is accessing your accounts.

In addition, experience has shown that people are not as good at recognizing malicious email as you might think. Every day, members of the Yale community fall prey to these kinds of scams. We have to take steps to ensure that we are more than just a single click away from having our paycheck stolen or becoming a victim of identity theft.

Multi-Factor Authentication adds a second layer of security to your account to make sure that your account stays safe, even if someone else knows your password. This second factor of authentication is separate and independent from the NetID and password step — MFA never uses or even sees your password.

Who is eligible to use MFA?

The university’s implementation of MFA will include all faculty, staff, and students.

Am I required to use two-factor authentication?

Once your group has been enrolled in MFA, you will be required to use two-factor authentication when logging into the Central Authentication Service (CAS) or YaleConnect Outlook Web Application from an off campus location, or Virtual Private Network (VPN).

Multi-Factor Authentication FAQs

Whom should I contact if I have questions or concerns about the requirement to use Duo?

If you have any questions or concerns about the requirement to use Duo, please contact the ITS helpdesk.

Does MFA see my password?

No, the university system verifies your Internet password with its internal systems as before, and never sends it to MFA. MFA provides only the second factor—the "something you have." In fact, MFA stores very little information—just enough so it can do its job.

What is the definition of "Off-Campus"?

Off-campus is anywhere other than:

- Yale Secure Wireless
- Yale Wireless
- Yale hard wired network
- Some areas of Yale New Haven Hospital

There are a few physically / geographically remote offices (medical) which are connected via Aruba Networks however they are considered on Campus and they will see no change. "Yale Guest" is an off-campus network.

Using MFA - FAQs

How Does Multi-factor Authentication (MFA) Work?

Once you have signed up for MFA, when you attempt to access a protected university application from an off-campus location, you will be prompted to enter your username and password as usual (the first "factor"). You will then be taken to the MFA screen where you will select the device of your choice and the preferred method of verification—push notification, a phone call, or a passcode—you will use to verify that it's you (the second "factor").

What Devices Can I Use?

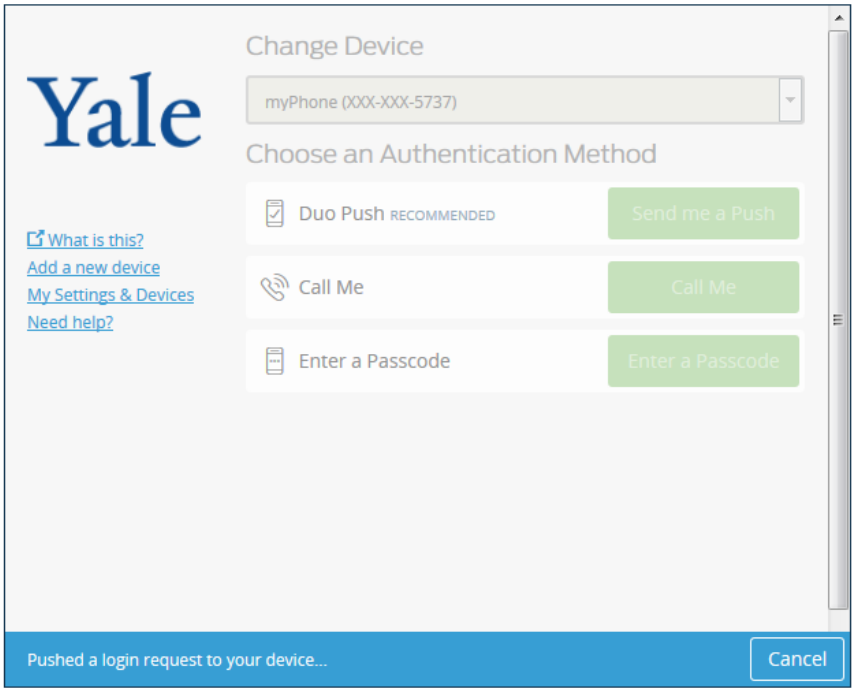
MFA lets you link multiple devices to your account, so you can use your mobile phone, a landline, and a hardware token, as your second factor.

When you are doing your initial setup, you may add as many devices as you like (landline and/or mobile). Subsequently, when you are logging in you can choose which device the

authentication request is sent to and which authentication method you would like (via Duo Mobile App, SMS text message, or phone call).

I've selected to automatically send push notifications to my phone, but I need to authenticate using another device.

If you have checked the box that allows you to send a push to your mobile phone, you will automatically receive push notifications every time you are required to use MFA. The rest of the DUO screen will then be blurred out (as shown below):

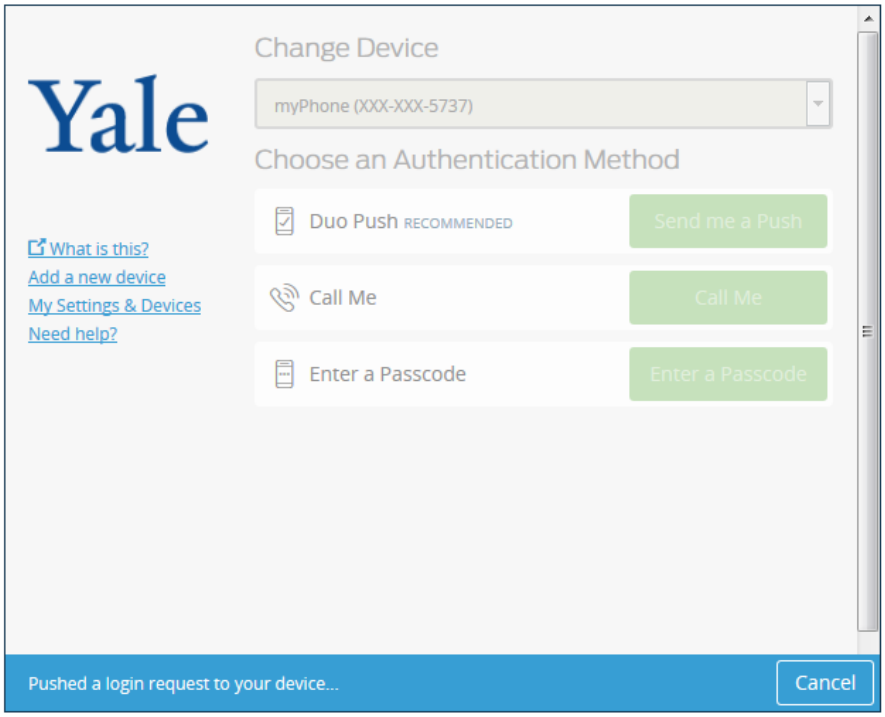


If you need to push the notification to another device, hit CANCEL at the bottom right of the screen. This will allow you to authenticate with another previously-registered device. If you no longer wish to receive automatic push notifications, uncheck the box next to "Automatically send a push". You can then Log In to your desired page or manage your devices.

I've selected to automatically send push notifications to my phone, but I do not have that number anymore.

If you have checked the box that allows you to send a push to your mobile phone, you will automatically receive push notifications every time you are required to use MFA. The rest of the DUO screen will then be blurred out (as shown below):

Multi-Factor Authentication FAQs



If you have a new number and cannot receive the push notification sent to that phone, hit CANCEL at the bottom right of the screen. This will allow you to authenticate with another previously-registered device.

From here, it is recommended that you register another device to ensure that you always have at least two devices to use for Multifactor Authentication.

How do I add a new device or manage an existing one?

Please refer to the Quick Guides on the main page for instructions on managing devices and enrolling/registering a new phone, tablet, desk phone. Tokens will be added to your profile by an administrator.

How long does it take to enroll/register a device for MFA?

5-10 minutes

How many devices can I add?

There is no limit on the number of devices that can be added. We recommend that all users add at least 2 devices, such as a cellphone/smartphone and a landline/desk phone.

Multi-Factor Authentication FAQs

Do I need to have a smartphone to use MFA?

No, you can use a smartphone, cell phone, landline (such as your office or home phone), tablet, or hardware token. A complete and up-to-date list of authentication methods is available on the MFA website. We recommend that users who have a smartphone choose to use them, since they are the easiest to use with MFA.

What if I forget my smartphone at home?

We encourage users to set up multiple authentication devices with MFA, so that when one method is unavailable, you have others from which to choose. For example, you could set up your smartphone for "push" and also your office phone and home phone to do callback.

What happens if I lose my phone?

Contact the ITS Help Desk immediately if you lose your phone or suspect that it's been stolen. The support specialist will disable it for MFA and help you log in using a one-time bypass code. While it's important that you contact the Help Desk if you lose your phone, remember that your password will still protect your account.

What happens if I upgrade or replace my phone with the same number?

If you have a new phone with the same number, see the Enrolling a New Phone with the Same Phone Number Quick Guide on our MFA Webpage for directions on how to activate DUO mobile and receive push notifications. Push notifications are the simplest and quickest way to authenticate.

Does it cost me money to authenticate with my phone?

"Push" authentication uses a very small amount of Internet data traffic to function (a few kilobytes per login). Text messages and voice calls are sent only when you request them, and would be billed by your carrier like any other text message or inbound voice call. The Duo mobile app also works like a token and will generate a passcode, this functionality will not require any data and works when your smart phone is in "airplane" mode.

What if I don't have a data plan on my phone?

The Duo smart phone app provides options that work without a data plan, a texting plan or even a connection, if necessary. The app can generate the required code without need of either a cell signal or data plan, and it can do so anywhere in the world. If you have a signal and data

plan, the app makes two-factor authentication as easy as a pushing a single button, but if you don't, you can use the app to generate a six digit code and enter that instead.

What if I don't have a connection?

The Duo Mobile App can generate a passcode without a cellular or wireless connection. Alternately, you may use a landline phone if an internet connection is unavailable or request a MFA hardware token.

What is the user experience if you are using your phone or an iPad on a cellular network or on a non-Yale wifi network and need to log in?

You will be prompted to MFA since this is considered an off campus network. If the registered device is the same as the one being used to login, the Duo app will notify & prompt for confirmation and users can confirm access the usual way. Alternatively a secondary device can also be used to confirm the MFA

How would one log into a CAS-protected resource or webmail on an airplane equipped with wifi? What would the experience be in this situation using a laptop, iPad, or phone?

This experience will be the same no matter what off campus location you are trying to log in from. You will be required to authenticate with MFA. In the case where a push or text is not working, your phone will function like a token while in airplane mode generating a passcode every 30 seconds.

How can I get a token?

Tokens will be issued via the walk-in centers. Users can visit a location, provide identification, and a token will be issued to them. In some cases, tokens will also be issued to IT Partners who can distribute to their local community.

Can I use the MFA app internationally?

The MFA smart phone app is designed to work internationally. If you install the app, it can generate the required code without need of either a telephone signal or data plan, and it can do this anywhere in the world. If you have a signal and data plan, the app makes two-factor authentication as easy as a pushing a single button, but if you don't have one of those two things, you can use the app to generate a six digit code and enter that manually.

Multi-Factor Authentication FAQs

Can the system handle international phone numbers?

Yes, MFA can handle international phone numbers. If entering an international phone number, you can leave a space between country code, city code, and the phone number.

How long will my authentication last?

You will be required to MFA every time you log in, when off-campus. This will last for the lesser of your session or 24 hours. You will have the option to remember your device for 1 day with CAS and YaleConnect. This functionality is browser based so you will have to do it in each browser you use.