Duo for International Travel

How to use Duo while traveling internationally

Duo keeps your Swarthmore account secure anywhere in the world, but not all of your second factor devices may be available to you during your travels abroad. The most common issues people run into relate to phone service, which means you may not have access to receive the Push, Call Me, or SMS Text Message options on your app enabled smartphone or mobile phone. However, there are still other options for you using the devices you already may have registered as well as some other devices you can add before leaving for your trip.

NOTE: in Duo, a “Passcode” is numerical and is NOT the same as your password

App Enabled Smartphones (and Tablets)

Many people may have a smartphone with the Duo Mobile app setup as one of their devices to access account through Duo. While this is great, international travel with a US phone can be costly, but you can still use the passcode generation option on the app (with your phone set on Airplane Mode to keep from getting charged for any calls, texts, or internet service) to generate any passcodes needed to log into your account. You can do the same with any app enabled tablet devices. As long as the app on the tablet was set up and registered before traveling abroad you will still be able to generate passcodes without needing wifi or data service. Just remember to put it on Airplane Mode to make sure to avoid any accidental data charges.

If you purchase an international SIM card to use while traveling, please be aware that it will change the phone number of your phone, so it will no longer be considered a registered device with Duo. You will have to add the new number (and re-pair the app, if you wish to use those features) to your Duo account. To add the new number requires adding it as a new device, which requires you to authenticate with a device already registered with Duo, so please keep this in mind.

If you have a separate phone that you use for international travel you can add it to you Duo account as an additional device at any time. Adding or editing devices requires that you authenticate with a device that is already registered with your account.

SMS Texted Passcodes

Unless you have a phone that is both set up to receive text messages internationally and is registered with Duo, you will not be able to do this once you are already abroad. It is highly suggested that you text yourself a set of passcodes before you leave just in case you need them, should one of your other device options fail while you are abroad. You will receive a set of 10 codes. They can each only be used once, but will stay active until you either use them or text yourself a new set of passcodes. Please see below for instructions on how to send yourself SMS Texted passcodes.

1. After you have logged into a Swarthmore service with your username and password, you will see the Swarthmore Duo Authentication screen. a. If you do not see this screen you may have it set to "Remember me for 15 days." If so, please follow these steps in a Private/Incognito window or from a different browser than the one you chose the "remember me" setting.
2. Once on the Duo Authentication Screen, you will see your device listed near the top of the screen. Make sure the device listed can receive text messages, or is the one you wish to currently send a text to. To change the device, click anywhere on the device field and choose the desired device from the dropdown menu.
3. Chose either "Passcode" or "Bypass Code" as your authentication method.
4. A blue bar will show up across the bottom of the window informing you that you can enter codes from various code generating locations in this field. After this message, click the button that says "Text me new codes." This will send a text message with 10 passcodes to the device chosen in step 2.
5. From here, you can choose any device or method to continue your login. You do not have to continue with the passcode login option.

Once you have your set of passcodes, save them somewhere you will have access to them without internet service, and potentially still be able to access them if your phone dies, breaks, or is simply not available to you.

Hardware Tokens

There are two types of hardware tokens currently available at Swarthmore. A hardware token is a small device made to be carried on a keyring so you can keep it with you at all times. Depending on the what types of computers you will be working with and what you may be working on while traveling, you may prefer one device over another. Below is a description of each type of hardware token we offer. Please note that we are asking you to choose only one of these hardware token options, if you feel you need one. They are available at the Help Desk in Beardsley Hall Rm 110.

U2F Token

Duo allows you to register a U2F Token as a second factor device. This token is a small device designed to carry on a keychain that plugs into a USB port on your computer. We use a U2F token called a YubiKey, but all U2F tokens require the use of the Chrome web browser and access to a USB port to function. If you have a newer Macbook, you may be required to use a USB-C to USB adaptor to use this option. While on the Duo screen, you will plug in your YubiKey to an available USB port on your computer. The key symbol on the token will begin to blink, and once it does you will touch the key symbol. Once Duo has recognized that the YubiKey has been touched you will be authenticated and given access to your account.
Passcode Generator

There is another hardware token option available called a passcode generator or a digipass token. This is a small device designed to carry on a keychain that generates a 6-digit one-time use passcode when you push the green button on the device. These tokens need to be registered to you by the Help Desk. While on the Duo screen during login, you can click on the "Enter a Passcode" button - even if you did not select the token from the device dropdown menu. Anywhere that offers the "Enter a Passcode" option will accept a passcode from any registered device of yours that generates a passcode, including your digipass token. Once you enter the passcode, click the "log in" button and you will be given access to your account.

NOTE: in Duo, a "Passcode" is numerical and is NOT the same as your password