Introduction

Passwords can be problematic. They can be relatively easy to steal or accidentally give away, and hard to remember, and requirements change from one site to another. If they fall into the wrong hands, important information and systems are vulnerable. One of the simplest and most powerful tools to stop account abuse while reducing the need for ever-more-complicated passwords is called two-factor authentication. At Carleton we use Duo for managing two-factor authentication.

What is Two Factor Authentication?

In its most common form, two-factor authentication means logging in with a username and password combination (factor one), followed by verification via a text message, phone call, or smartphone app, to name a few (factor two). Most services offer a “remember me on this device” option so that you aren’t prompted for the second factor every time. For our purposes this option is available for the span of 60 days. Don’t have a mobile phone? You can also use your desk phone, tablet, or a key-fob sized device that generates short codes. You may already have encountered two-factor authentication in some other web services that you use. It has also been branded as 2-step verification (Google), login verification (Twitter), and login approvals (Facebook). If you used TurboTax this year, you probably used your phone as a second factor.

Carleton uses Duo to provide two-factor authentication, along with many other universities and colleges, and click here to see Duo’s explanation of Two-Factor Authentication.

For more information take the annual InfoSec 101 security awareness training course.
Setting up Duo

- To access the enrollment page at Carleton go to: login.carleton.edu
- Until March 30th when Duo becomes mandatory, you can choose the "Turn Two-Factor on (or off)"
- If you currently or have previously configured Duo, you can choose "Manage your phones and devices"
- Then, follow Duo's instructions for how to enroll: https://guide.duo.com/enrollment

Receive Backup Codes

After doing this, you can also request a list of one-time-use codes that you could keep with you in case you do not have your authentication device on hand. We recommend all Duo users do this if possible, and that you keep the codes available somewhere you can access if your phone or primary Duo device is not working. Follow the instructions here: Duo Codes for Backup

Create a Backup Option

We HIGHLY recommend that you configure at least one backup option:

- For Faculty & Staff we recommend using at least two different devices - a cell phone and an office landline, for example.
- For Students, Faculty or Staff (particularly those with only one device) we recommend requesting and storing 5 one-time use passcodes that you can keep with you.

This will help make sure you can independently make changes to duo even when you have changes in phone numbers.

Re-configure Duo on a New Phone

1. Access the Duo management page at Carleton: login.carleton.edu
2. Choose "Manage your phones and devices" - you will see the following page:

Duo Two-Factor Devices

New Duo user? Please see the Duo section of infoSec 101 (abbreviated 2-minute help video here). If you get stuck, select One-Factor Authentication (Password Only) and call the ITS helpdesk at 507-222-5999.

We strongly recommend that you configure a backup phone number or tablet. To do so, verify your identity again below (why again? because these are sensitive operations for which "remember me for 60 days" is insufficient) and select "Add another device."

If your phone number did not change, the easiest option is to choose "Call me" and then answer the phone and follow the prompts.

Find your cell phone number in your list of devices and choose Device Options, and choose to reconfigure Duo Mobile. It should step you through the rest of the instructions.

For more information you can continue to Duo's device management guide to edit your device: https://guide.duo.com/manage-devices#manage-existing-devices

If your device number changed, and if you have no other devices configured for duo, you will need to contact the ITS helpdesk for assistance.

3. You will need to complete the Duo authentication process again to verify that you are authorized to manage your devices.

4. Find your cell phone number in your list of devices and choose Device Options, and choose to reconfigure Duo Mobile. It should step you through the rest of the instructions.

For more information you can continue to Duo's device management guide to edit your device: https://guide.duo.com/manage-devices#manage-existing-devices

If your device number changed, and if you have no other devices configured for duo, you will need to contact the ITS helpdesk for assistance.

Using Passcodes: Duo while Traveling or without Cellular or Wireless Coverage

You will use the "Enter a Passcode" option and get a passcode by opening the app. Specific directions for each phone platform can be found at guide.duo.com by selecting your device OS from the list on the left and looking for the passcode section.

If you do not have a smartphone or tablet, please contact the ITS helpdesk at least one week before departure to arrange for an alternate authentication option.

Alternate Authentication Options

If you do not have a mobile phone, have a limited phone plan, or would like to discuss any issues with using your phone we can meet with you about authentication options. There are small devices called security tokens or key fobs that Carleton community members can request for free (and keep) that generate codes that are synchronized with your account. At any point, in any location, you can use one of those codes to authenticate. The codes refresh every few seconds.

To request one of these security tokens, sign up for Duo as described above and configure at least one phone, then call or email the ITS helpdesk.
We need at least 1 week's notice to make sure we have an available device and can properly link it to your account.

Systems that Trigger a Duo Prompt

Everything URL beginning with login.carleton.edu or apps.carleton.edu uses two factor authentication, and we're adding more sites to the list as we can. Some examples include: Google, Reason, Symplicity, Terradotta, search committee access to jobs.carleton.edu, Slate Admissions, this Wiki, Lynda.com, blogs.carleton.edu, and about 50 off-campus services.

For faculty, staff, and students, because the risk is low, ITS-managed public labs are exempt from Duo for many sites commonly used for standard academic purposes, but services that contain sensitive, protected information will still prompt for Duo Authentication in labs. If you are repeatedly prompted for Duo confirmation on a public lab computer, let the ITS helpdesk know.

FAQs about Duo (redirects to another page)

Troubleshooting

For questions not answered below, check guide.duo.com for common instructions and step-by-step guides; or duo.com/support for more specific problems or questions, or contact the ITS Helpdesk.

"Remember me for 60 Days" box is greyed out

If you configured Duo to "Automatically send a push" notification, then anytime you are re-prompted, Duo will send you a push before allowing you to choose the Remember Me option. There are two ways to address this issue.

Option 1: Keep Automatic Push, Cancel, and Re-Push

If you like the Automatic Push, you can keep that turned on and still have devices remember you.

1. When you are at a duo prompt where you'd like to set the "Remember me" option, press the blue "cancel" button on the Duo prompt.
2. Ignore the prompt that is sent to your device
3. The duo screen should still be visible, and now you should be able to check the "Remember me" box
4. Click "Send me a Push" again. This will send a new Duo push to your phone, and once accepted, that device will remember you for 60 days.

Option 2: Turn off Automatic Push

If you don't want to do the process described in Option 1 each time you need to remember a device, you can turn Automatic Pushes off. To do this:

1. Click Cancel on the push that came up
2. In the left side of the Duo window, click "My Settings & Devices"
3. Approve the Duo prompt that comes, to ensure Duo that you are you (you still will not be able to choose a remember me option)
4. In the window that opens, you should see menus for "Default Device:" and "When I log in:"
5. Change the "When I log in:" setting to "Ask me to choose an authentication method"

After this, you will need to click the "Send me a Push" button each time you are prompted, but it will be easier to get to the "Remember me for 60 days" box

I chose "Remember me" and it hasn't been 60 days, but I am being prompted again

If you have cleared your browser's cookies and cache, this will reset the token that Duo uses to track your device. Simply check the box again and you should be good for the next 60 days or until the next clearing of cookies and cache.

Codes from my Security Token (Key Fob) are not working
If the button on the security token (key fob) gets pressed too many times (for example: the token is in your bag or pocket and may have been pressed by other items) the codes can get unsynchronized from your account. These can be resynchronized, but require phone assistance from the ITS Helpdesk. Call them at 507-222-5999 for help. For ITS staff, read this duo support article for guidance.

Who to Contact

Two-factor authentication is supported by the ITS helpdesk:

Phone: 507-222-5999

Email: helpdesk@carleton.edu (do NOT use for urgent issues)