Two-Factor Authentication with Duo Security

> **New Phone?**
> If you have a new phone, you will need to re-activate the Duo Mobile app. Please follow the directions at Duo Security: Managing Your Devices.
> Please remember to choose **My Settings & Devices** prior to logging in.

As part of University Technology's 2014 Security Initiatives, we have partnered with Duo Security to offer additional protection to your uLogin account. This service, known as **Two-Factor Authentication**, protects your uLogin account by adding a second step to the login process. After entering your uLogin ID and password, you will use either your phone or a device known as a hardware token to confirm your identity. This prevents anyone but you from accessing your account, even if they know your password.

This service is not enabled by default. In order to use Duo Two-Factor Authentication, you must first **enroll** in the system using Duo Self-Service Enrollment. New employees who have not self-enrolled will be enrolled automatically approximately two weeks after their hire date (we refer to this as "compulsory enrollment", and you will be unable to log in without contacting UT). Until you are enrolled in the system - either on your own or automatically -, you will continue to log in to Drew University web sites using your uLogin ID and password without the second authentication factor.

Enrollment

Click here to expand...

Am I required to enroll in Duo Two-Factor Authentication?

Drew University requires all **faculty**, **staff**, and **contractors with uLogin accounts** to enroll in the system in order to protect the sensitive University records that employees have access to as part of the course of their work. Please review the Responsible Use of University Data Policy for more information.

Students are not required to be enrolled in the system, although are welcome to do so if they choose. **Student Employees** may be required to enroll depending on the nature of their work and the electronic records they have access to.

What is the schedule for mandatory faculty and staff enrollment?

New employees and contractors must enroll in the system **within two weeks** after their official start date at Drew.

Those not enrolled in the system within that amount of time will have their uLogin accounts disabled. If this applies to you, please contact the UT Service Center at 973-408-4357 to discuss your options.

Completing Self-Service Enrollment

It's easy to enroll yourself in Duo Two-Factor Authentication using our self-service pages. After logging in, Duo Security will walk you through the steps to enroll one or more phone numbers into the system. We recommend enrolling multiple phones, such as your mobile phone and office landline. If you are enrolling multiple phones, enroll your primary cell phone first. Go to the self-service enrollment site (drew.edu/duo) to get started with the process or learn more about the multiple methods Duo supports for logging in.

To learn more about the enrollment process, read the Enrollment Guide on Duo Security's web site.

Please keep in mind that, when enrolling devices/landlines yourself, you will need to have the first one at hand to verify ownership. Also, pay attention to the order in which you add phone numbers, as this will affect how you log in later.

What if I do not have a cell phone?

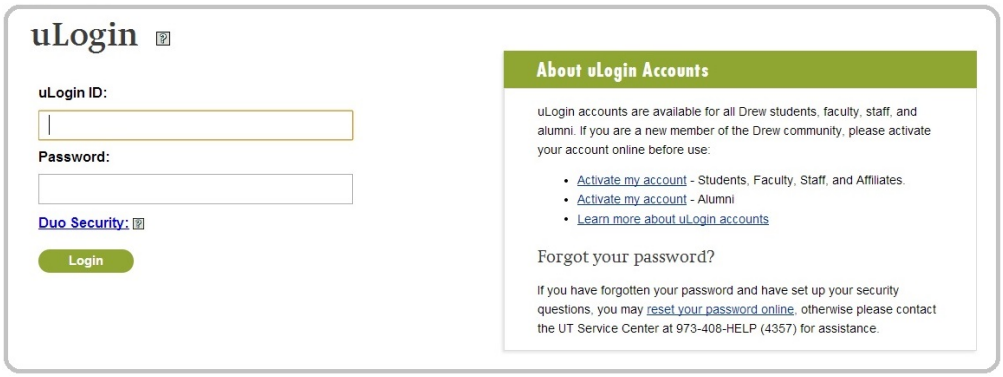
No phone? No problem. Duo supports multiple methods for logging in. If you do not have a cell phone, you may obtain a YubiKey or Classic Hardware Token from University Technology. Tokens are distributed freely to faculty and staff who need to enroll in the two-factor authentication service. Please come to the University Technology Helpdesk with a photo ID to obtain a token. Please note that replacements for damaged or malfunctioning tokens will be provided for free. A $50 charge will apply to replace a missing token.

Using Your Account After Enrollment

Click here to expand...

uLogin

Once you have enrolled in Duo Security, you will be required to complete the second step of authentication whenever you see a uLogin form. You can log in from any computer but you will need to approve the login using one of the phones (or hardware token) that you have enrolled in the system.

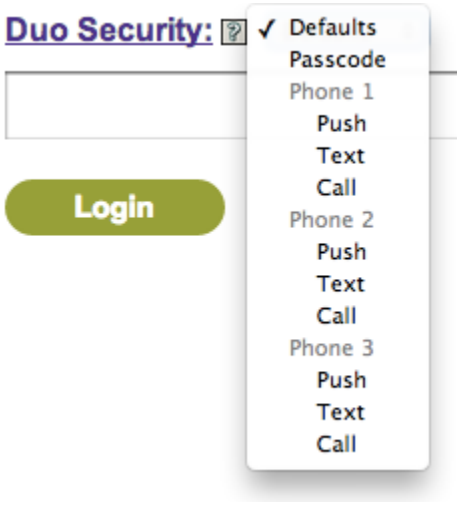


Simply enter your uLogin ID and password as usual and Duo will automatically use the **Default** method to log in. If you have enrolled a smartphone, Duo will send a Push message to the first smartphone listed and prompt you to approve the login using the Duo Mobile app. If you do not have any smartphones on your account, Duo will make a regular telephone call to the first number and you will be prompted to approve the login by pressing any key on your phone.

Using Duo Security options to select another login method

By clicking the Duo Security link on the uLogin form, you can select another method to use to log in. Click the drop-down to view the available options. The phones you have enrolled are designated Phone 1, Phone 2, and Phone 3 in the order in which you registered them during the enrollment process.

Please note: To use these alternate methods, you should still enter your username and password, but do not hit Enter after typing your password!



- **Defaults** - If you do not select any Duo Security options, Duo will automatically use the Default method. If you have enrolled a smartphone, Duo will send a Push message to the first smartphone listed and prompt you to approve the login using the Duo Mobile app. If you do not have any smartphones on your account, Duo will make a regular telephone call to the first number and you will be prompted to approve the login by pressing any key on your phone.
- **Push** (recommended) - If you have registered a smartphone and installed the Duo Mobile app, the Push method of authentication is

recommended. In this mode, Duo will send a notification to your smartphone. Simply accept the pop-up message on your phone and touch **Approve** to authorize the login request.

- **Text** - You may use the Text option with any phone capable of receiving text messages. When you select the Text option, Duo will send a set of 10 one-time passcodes to the phone you have selected. After the text message has been sent, you will be returned to the uLogin form with a login failed message. Once you have the text message, you may use each code in the message to log in once using the **Passcode** option. Once you have exhausted your 10 passcodes, use the Text option again to get more. Whenever you use the Text option to send passcodes, any previously texted passcodes are invalidated immediately, even if unused.
- **Call** - When you select the Call option, Duo will place a voice call to the phone selected. Answer the phone and listen to the voice prompt. Pressing any key on your touch tone phone will approve the login request.
- **Passcode** - You may obtain a 6-digit one-time login passcode from one of several sources. Simply enter the passcode into the box below the drop-down to log in.
    - **Using a YubiKey** - If you have been issued a YubiKey, position the cursor in the third text box and press the button on your YubiKey to enter the passcode.
    - **Using a classic hardware token** - If you have been issued a hardware token, simply press the button to generate a new passcode and enter it into the text box.
    - **From a text message** - If you have used the Text option to send yourself 10 one-time passcodes, enter a passcode you have not used previously. When you have run out of passcodes, you can use the Text option again to send 10 more.
    - **Using the Duo Mobile app on your phone** - If you have registered your smartphone with Duo, you can use the app to generate a passcode as well. Open the Duo Mobile app on your phone and touch the key icon next to the Drew University account to generate a new one-time passcode. Enter this passcode into the third text box.

Getting "Locked Out"

If you attempt, and fail, to log in to your account ten times in a row, you will be locked out of your account. This safety measure is put in place to protect your account (and the data you have access to) from someone who has stolen your password.

A ticket will be logged automatically once you are locked out.

In order to unlock your account, your identity will need to be verified. This can be done in person, at the Helpdesk, with a photo ID, or over the phone with an alternate email address already on file with the University. Alternatively, you can designate an Authorized Proxy to vouch for you (see "Authorized Proxy", in the FAQ). Either way, you will need to have a conversation with a Duo admin (see below) regarding why you were locked out.

Using Your Device with Duo

- uLogin, Your Way! Duo supports a wide-variety of different devices for authentication. Learn more about how to log in using your preferred method.
- **Adding devices, reactivating the Duo Mobile App, or changing the order of devices for authentication**. By logging in to the Two-Factor self-service site (drew.edu/duo) and clicking **My Settings & Devices** (on the left), you can reactivate the Duo Mobile app, remove a device, or choose an automatic push or call for your device (as appropriate). By clicking **Add a new device** on the left, you can enroll a new authentication device. Each of these options will prompt you to confirm that it is really you before allowing you to make changes. Learn more about managing your devices from Duo's documentation.

Syncing Your Drew Email to Your Phone, Tablet, or Other Programs

Please refer to our instructions for Connecting Your Mobile Devices to Google Apps or How to Set Up Your Drew Gmail Account in an Email Client for more information on initial set up with these programs.

For applications that do not support two-factor authentication, you will need to use a new password generated specifically for use with these services known as your **device password**. You can read more about Device Passwords here.

Frequently Asked Questions and Common Issues

Click here to expand...

Many questions are answered at the Duo Security Support Issues page here in U-KNOW.

- **Do I still need to change my uLogin password every 180 days after enrolling in this service?** No. Duo Two-Factor authentication adds additional verification after every login. For this reason, Drew does not require two-factor users to change their regular uLogin passwords every 180 days. Once you have completed Duo enrollment, the password expiration policy will be removed from your uLogin account automatically.
- **Does Duo Security only apply to Drew web sites using uLogin? What about logging into my computer?** At present, Duo Security applies to web-based services protected by Drew's uLogin system. Duo authentication is not required for local logins to your computer.

- **I wish to designate an Authorized Proxy.** If you need to present ID, but are unable to come to campus, you may designate an Authorized Proxy to vouch for your identity. An Authorized Proxy is a supervisor or coworker who can positively identify you by phone call or other means and is able to visit a Duo Administrator in person and sign a proxy authorization form. They are designated in cases of Duo lockout.

  The proxy procedure is as follows:
  - Contact the UT Service Center and explain the issue you are experiencing. Explain that you are unable to come to campus and will be designating a proxy to vouch for your identity. The Service Center will create a ticket and indicate that a proxy will be vouching for your identity.
  - Contact your proxy. Your proxy must be a Drew employee and should be someone you know, a coworker or supervisor, member of the Deans office staff in your school, etc. who is able to positively identify you on the phone call and is able to sign a form accepting responsibility for making such an identification in the presence of one of the Duo Administrators. Note that as part of the internal controls and audit procedures we have established within University Technology for the Authorized Proxy process, Duo Administrators are expressly forbidden from serving as proxies themselves.
  - Your authorized proxy will then contact one of the Duo Admins (listed below) and agree to meet in person to complete a Proxy Authorization form. With Proxy Authorization form in hand, the Duo Admin will perform the required actions on your account and update the ticket. An electronically scanned copy of the form will be attached to the ticket for audit purpose later. We will contact you at the callback number or email address in the ticket to confirm that the required action on your account is complete.

- **I have been designated as an Authorized Proxy by a coworker.** If you have agreed to be a Proxy for someone, please call ahead to the UT Service Center (973-408-4357) to make an appointment with one of the Duo Administrators, who will meet with you to complete a Proxy Authorization form. The Duo Administrators are as follows:

  - Audrey Joubert
  - Betsy Black
  - Paul Coen
  - Scott Wood
  - Vaughn Swanson
  - Verna Holcomb