Two-Factor Authentication with Duo

November 2023: Upcoming Changes in Duo

Attackers continue to develop more sophisticated methods into manipulating users to bypass the protections of passwords and insecure two-factor authentication. Lehigh is responding by increasing the security required to access your account.

Beginning on December 1, 2023, new Lehigh users will have the following secure options for 2FA in Duo:

- Duo Mobile app with Push (Lehigh preferred method)
- Physical USB FIDO2 compatible security key (works when your phone has no connection)
  - USB-C (link to Amazon)
  - USB-A (link to Amazon)
- Printable backup codes

Beginning on March 4, 2024, insecure authentication methods will no longer function. The following options will be removed:

- SMS (text)
- Phone call
- Duo mobile app passcode generation
- Duo token number generator

You can add and remove authentication methods/devices at https://account.lehigh.edu/duo

All other second factor options (other than your default) are under the 'Other options' link.

For full information, see Duo's documentation.

Two-factor authentication, also referred to as 2FA, protects users from unauthorized access to Lehigh accounts in the event that a password is compromised. 2FA is currently only licensed and required for faculty and staff. You may already be familiar with 2FA if you've accessed sites that require it, such as for online banking. Two-factor authentication uses two pieces of information to establish your identity when you are trying to access a site or service:

- The first factor is something only you know, such as your password.
- The second factor is something only you have, such as your mobile phone (recommended).

If your password is compromised through a phishing attack or other malicious means, a cyber criminal would also need your second factor to access your account.

Lehigh has contracted services from Duo Security to enable two-factor authentication on your Lehigh computing account. Duo's services allow you to choose the type of authentication method that works best for you: a push notification sent to your mobile device through the Duo Security app, a generated code each time you log in to a site or service, or another device such as a telephone to call you when two-factor authentication is needed.

Get Started

Ready to enroll? Begin by completing the Lehigh Duo Security device enrollment options and adding your second factor device(s). Enroll as many additional factors as practical - it's good to have. For more information, refer to Two-Factor Authentication with Duo Enrollment Process.

Duo's instructions for using your devices:

Duo Mobile (Push Notifications or Passcodes): Apple iPhone, Apple Watch, Android Phone, and Windows Phone

Other Devices: Cell Phones and Landlines for SMS/Text or Voice Callback, Hardware Tokens and U2F Authenticators.

How-to Articles and FAQ

Twofactor Authentication with Duo Prompt (SSO): How to provide your second factor when using Lehigh SSO.

Duo: Adding and removing New Devices: How to add and remove devices, sometimes referred to as "authentication methods".

If you are running privacy browser extensions, you might need to whitelist sso.cc.lehigh.edu.

Generate Duo Backup Codes: How to print backup codes in an event your primary factor, such as cell phone, is unavailable.

For answers to common questions, visit the Two-factor Authentication with Duo FAQ.

"Traditional" Prompt

New "Universal" Prompt
Universal Prompt: Other Options, Help Screen, Trust Browser Screen
Lehigh Videos

Enrollment examples

Sign In Video examples

Duo Videos