Two-Factor Authentication

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 only open to 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).

General Info is on the Two-Factor Authentication Overview Page.

If your password is compromised through a phishing attack or other malicious means, a cybercriminal 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.

<table>
<thead>
<tr>
<th>Get Started</th>
<th>How-to Articles and FAQ</th>
</tr>
</thead>
<tbody>
<tr>
<td>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 - its good to have . For more information, refer to Two-Factor Authentication with Duo Enrollment Process.</td>
<td>Two-Factor Authentication with Duo Prompt (SSO): How to provide your second factor when using Lehigh SSO.</td>
</tr>
<tr>
<td>Duo’s instructions for using your devices:</td>
<td>Adding and removing New Devices: How to add and remove devices, sometimes referred to as authentication methods.</td>
</tr>
<tr>
<td>Duo Mobile (Push Notifications or Passcodes): Apple iPhone, Apple Watch, Android Phone, and Windows Phone</td>
<td>If you are running privacy browser extensions, you might need to whitelist sso.lehigh.edu.</td>
</tr>
<tr>
<td>Other Devices: Cell Phones and Landlines for SMS/Text or Voice Callback, Hardware Tokens and U2F Authenticators.</td>
<td>Generate Duo Backup Codes: How to print backup codes in an event your primary factor, such as cell phone, is unavailable.</td>
</tr>
<tr>
<td></td>
<td>For answers to common questions, visit the Two-factor Authentication with Duo FAQ.</td>
</tr>
</tbody>
</table>

Lehigh Videos

Enrollment examples

Sign In Video examples

The initial Duo setup screen
Two-Factor Authentication with Duo Prompt

- **If you have multiple devices, select which device to use**

- **Device:** iPhone [device ID]

- **Choose an authentication method**
  - Duo Push
  - Call Me
  - Pascode

- **Send Me a Push**
- **Call Me**
- **Enter a Pascode**

- **Select to remember device**
  - not recommended for public systems

Two-Factor Authentication with Duo Getting Started Videos