Enable Support for TLS 1.2 or 1.3 on Web Browsers

Older web browsers use out-of-date protocols that do not support modern encryption and contain security vulnerabilities that can be exploited by attackers. **Effective July 1, 2021**, only web browsers that support versions 1.2 or 1.3 of the Transport Layer Security (TLS) protocol will be permitted to access University web services. Browsers that use TLS version 1.0 or 1.1 will not be supported.

To ensure your web browser supports TLS 1.2 or 1.3, complete the steps below.

**Microsoft Edge**
TLS 1.2 is automatically enabled in all versions of Microsoft Edge.

**Google Chrome**
TLS 1.2 is automatically enabled in Google Chrome version 29 or greater.

- [Ensure you are using the most recent version of Chrome ...](#)

**Apple Safari**
TLS 1.2 is automatically enabled in Safari version 7 or greater.

- [Ensure you are using the most recent version of Safari ...](#)
Mozila Firefox

TLS 1.2 is automatically enabled in Firefox version 27 or greater.

- Ensure you are using the most recent version of Firefox ...

To enforce TLS version 1.3 in Firefox, complete the steps below.

1. Open Firefox.
2. In the address bar, type `about:config` and press Enter.
3. In the Search field, enter `tls`. Find and double click the entry for `security.tls.version.max`.
4. Set the integer value to 4 to force a maximum protocol of TLS 1.3.
5. Click OK.
6. Close your browser and restart Mozilla Firefox.
Microsoft Internet Explorer

1. Open Internet Explorer.

2. From the menu bar, click Tools, then Internet Options, then click the Advanced tab.

3. Scroll down to the Security category and manually check the box next to Use TLS 1.2.

4. Click OK.

5. Close your browser and restart Internet Explorer.