Getting Started with Two-Factor Authentication with Duo Security

As a response to the increasing number of phishing scams that impact Fredonia employees and the University's overall risk for a data breach, the Information Technology Services department has implemented a high-security login process for Fredonia eServices and other critical electronic resources that requires a second method to confirm the identity of the person logging in.

Referred to as two-step or two-factor authentication, this process, which uses Duo Security, asks individuals logging in to confirm their identity using a smartphone, via automated voice calls, or a hardware token.

Duo Security accounts will be provisioned out to users based on the risk associated with the data and systems they have access to.

Currently Duo Security is protecting the following Fredonia electronic services:

- Drupal Web Publishing
- FredApps (GSuite)
- OnCourse
- Starfish
- SUNY Employee Portal
- 1Password Teams
- University owned computers

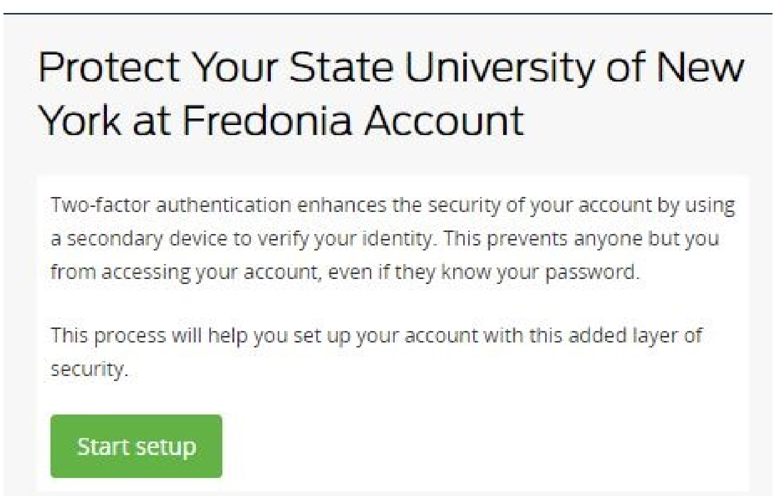
NOTE: other Fredonia electronic services will be protected as technical and funding limitations are addressed.

Getting Started

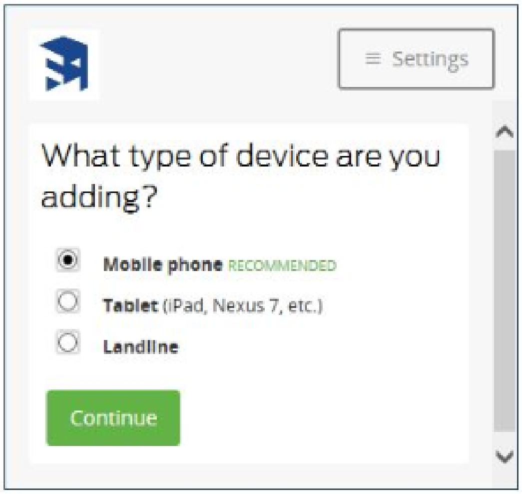
1. ITS will add your eServices account to the Duo Security system based on the risk associated with the services and sensitive data you have access to.
2. Fredonia permits you to register a smartphone (Android, iPhone, or Windows), a landline, or a tablet as your second factor. You may have as many second factors as you wish (e.g. smart phone, landline, tablet, hardware token), but we highly recommend that you have at least one backup second factor device.

   NOTE: Please make sure that you have your second factor device with you when you start the enrollment process. If you are starting your enrollment process from the device that you will be using as a second factor, please follow this instructions.

3. The first time you attempt to log in to any Fredonia service that requires two-factor authentication, you will be redirected to a set-up page. Click on Start setup.



NOTE: It is strongly recommended that all mobile devices used as a second factor be encrypted and have a screen lock enabled. We also recommend that you register a second device as an alternative method of authenticating.



See Related articles below for specific device instructions.

NOTE: All faculty can be issued an optional hardware token to use as a secondary 2nd factor device for Duo Security. These hardware tokens are provided to the employee at no charge for the first token. The token is NYS property and needs to be returned to the ITS Service Center upon employee separation from service. If the employee loses the hardware token, the employee or department will need to replace it at their expense. Please visit the ITS Service Center located in Thompson Hall to be issued a hardware token.

Short URL to this page: https://answers.fredonia.edu/x/$action.getTinyUrl()

Related articles

- Authentication via Duo Mobile Passcode
- Authentication via Duo Push
- Duo Security Frequently Asked Questions
- Enroll a Device with Duo
- Enroll a Landline or Cell Phone with Duo
- Enroll a Mobile Phone with Duo
- Enroll a Tablet with Duo
- eServices Login with Duo
- Guide to Security Checkup feature in Duo Mobile
- Guide to the Duo Restore feature for Duo Mobile account recovery
- How do I activate Duo Mobile directly from my smartphone or tablet?
- Managing my devices and settings in Duo
- Using Hardware Tokens with Duo