
Multifactor Authentication

This article describes how to set up and use Multifactor Authentication (MFA) for users to access their Nelnet account.

What is Multifactor Authentication?

Multifactor authentication (MFA) adds a layer of protection to the sign-in process. When accessing their account for the first time, users are presented with a prompt to add another layer of identity verification. Once that has been setup, then each time a user logs in, they will be required to submit that added step during the login process. Nelnet Campus Commerce currently requires use of an email address or an authenticator app as a method for multi-factor authentication.

Who Must Use MFA?

MFA is only required for users who are directly authenticating into a Nelnet Campus Commerce system with a username and password or who may be accessing via SSO from an external system that does not require MFA.

Authenticator Apps

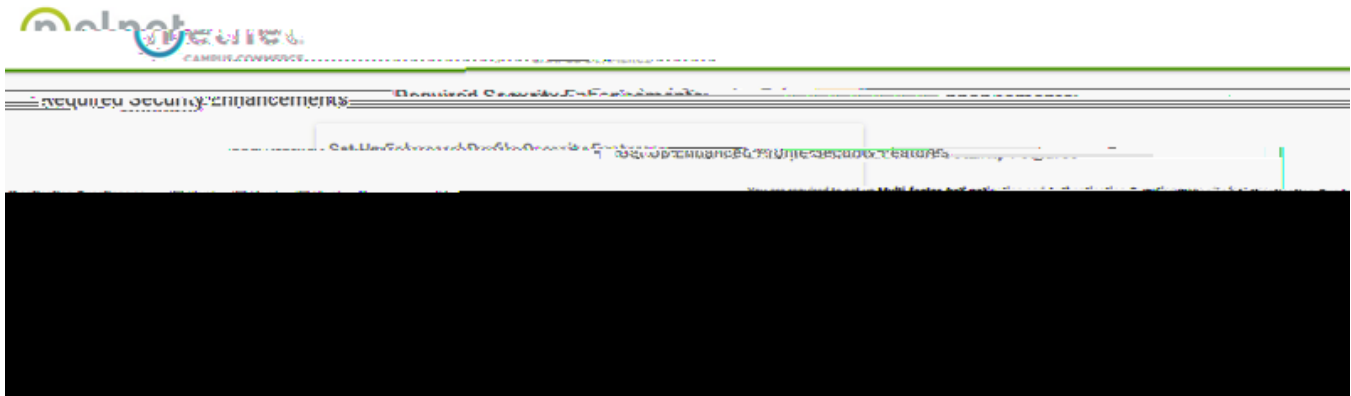
Authenticator apps can be downloaded on your smart phone and/or your desktop computer. Apps such as Authy have both a phone and desktop version. If you have an existing authenticator app, it should be relatively simple to add your Nelnet Campus Commerce account. If you do not already have an authenticator app, some of the most common ones are:

- Google Authenticator
- Microsoft Authenticator
- Authy by Twilio (includes desktop version)
- Lastpass
- 2FA Authenticator
- Duo Mobile
- Aegis authenticator

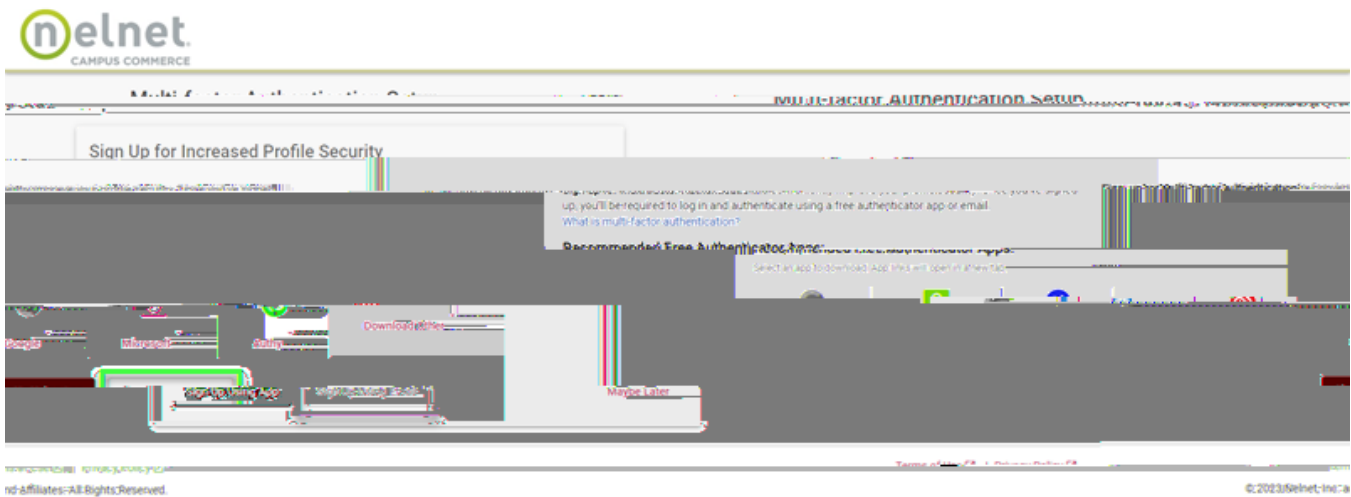
What Does The Login Process Look Like?

Initial Set Up - Email

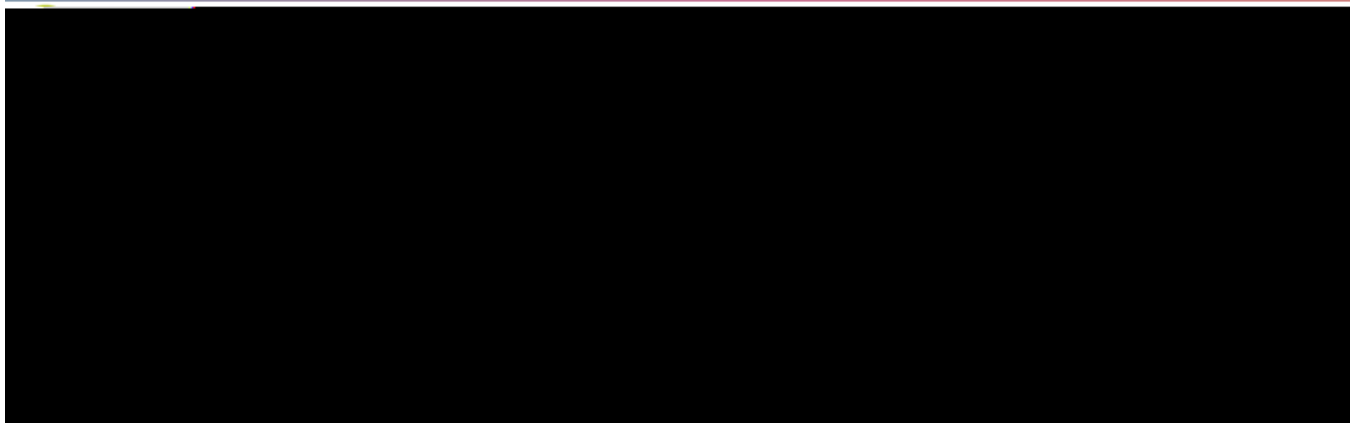
1. With their initial login a user will be prompted to sign up for multi-factor authentication. Click the **Begin** button to proceed.



2. Click the **Sign-Up Using Email** button to proceed.



3. If you have multiple email addresses saved in your profile you will be asked to select the one to which you'd like the authentication code to be sent. Make your selection and click the **Send Code to Email Button**. If you have only one email stored with your profile the authentication code will automatically be sent to that email address.



4. Check your email. You'll find an email such as this one containing your one-time use code.

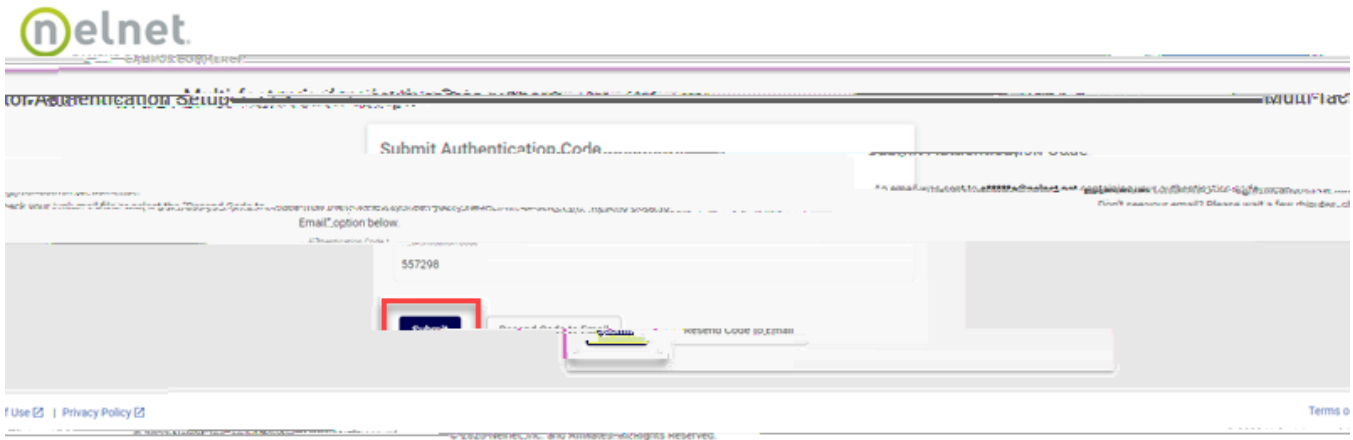


5. Enter the provided code and click the **Submit** button.

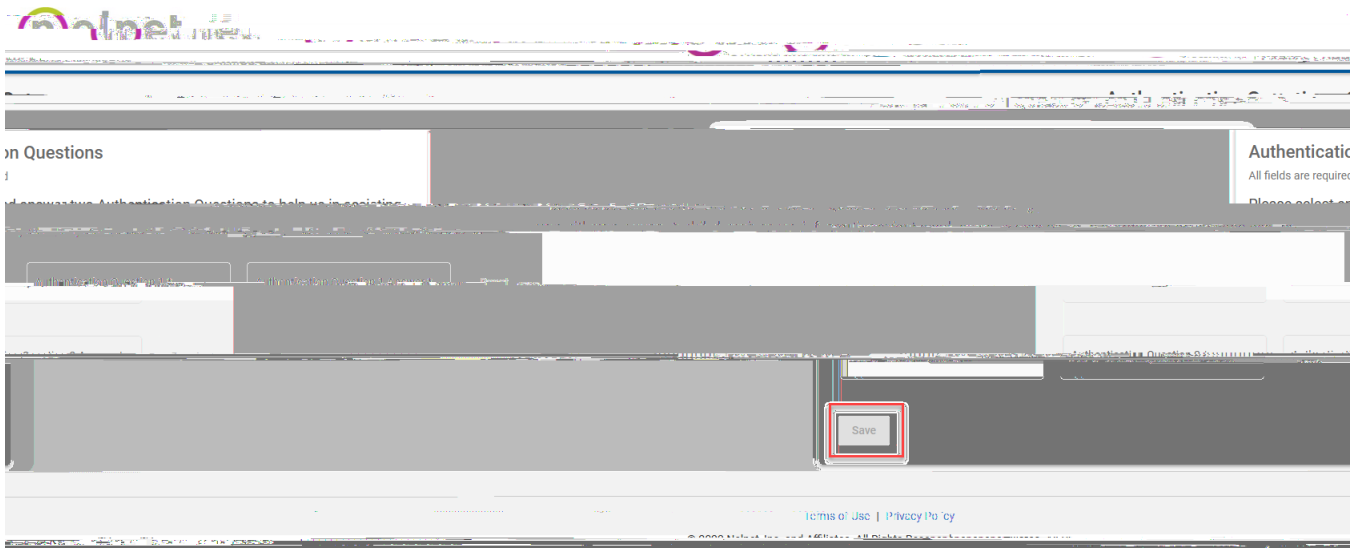


Tip

If you cannot find your emailed authentication code check your junkmail folder or use the **Resend Code to Email** button to generate a new email.

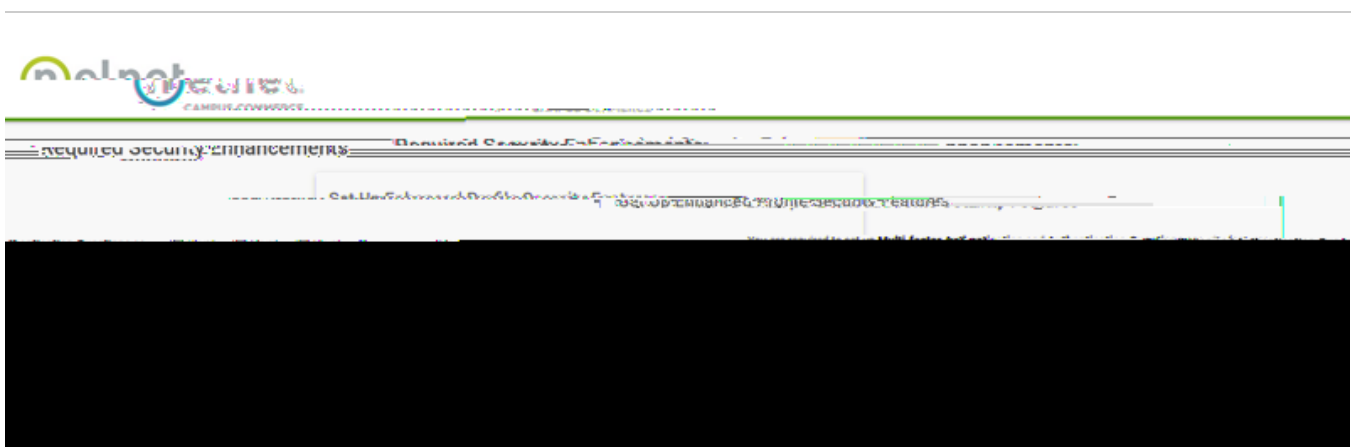


6. Authentication questions will be used to verify your identity should you need assistance with resetting your MFA in the future. Choose two questions and provide an answer. When finished click **Save** to be logged into your account.



Initial Set Up - Authenticator App

1. With their initial login a user will be prompted to sign up for multi-factor authentication. Click the **Begin** button to proceed.

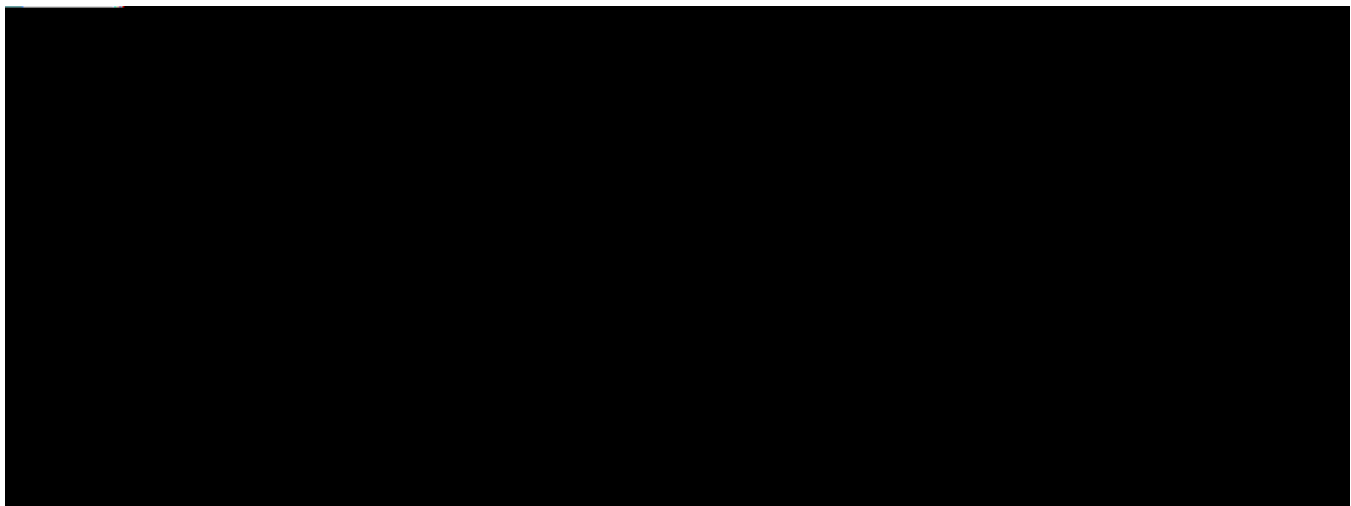


2. Click the **Sign-Up Using App** button to proceed.



Tip

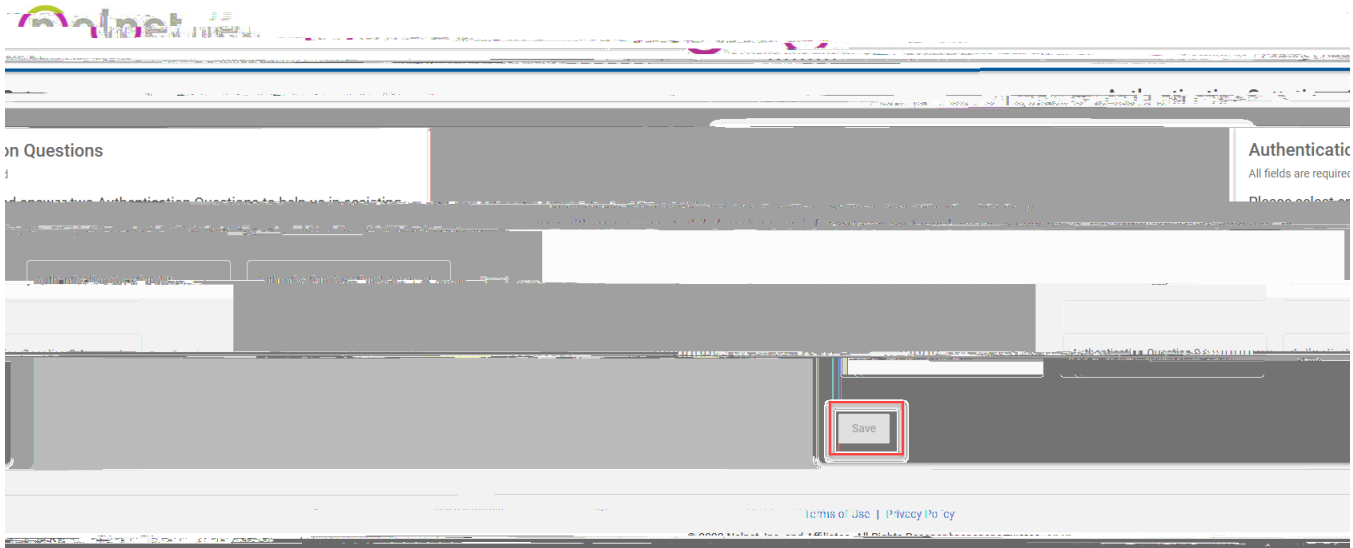
If you choose to enroll using an authenticator app don't yet have an established app, you should download one before proceeding.



3. To register your app, scan the QR code and follow any prompts that you may receive in your app. Once completed, click **Next**.

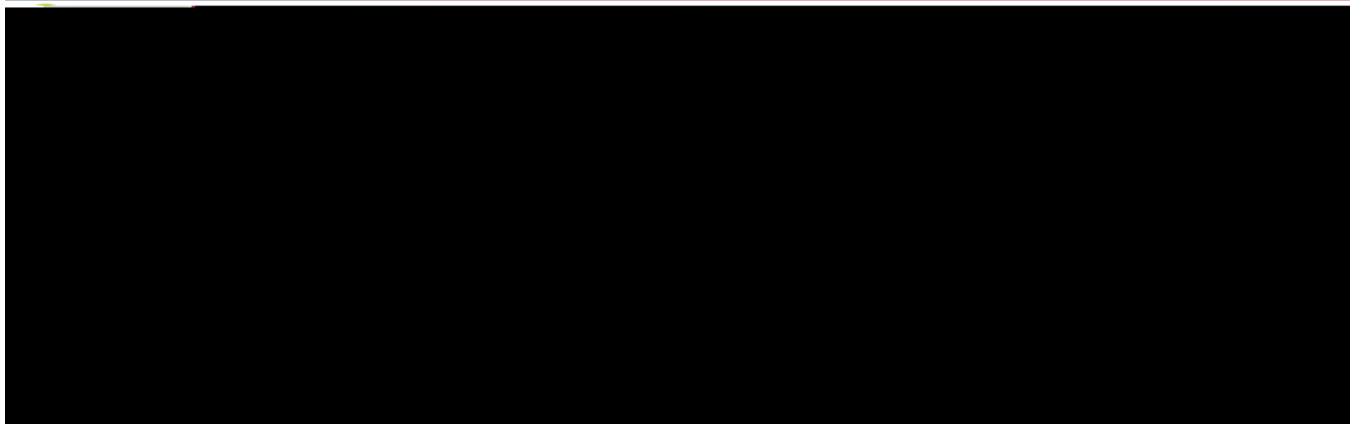


6.

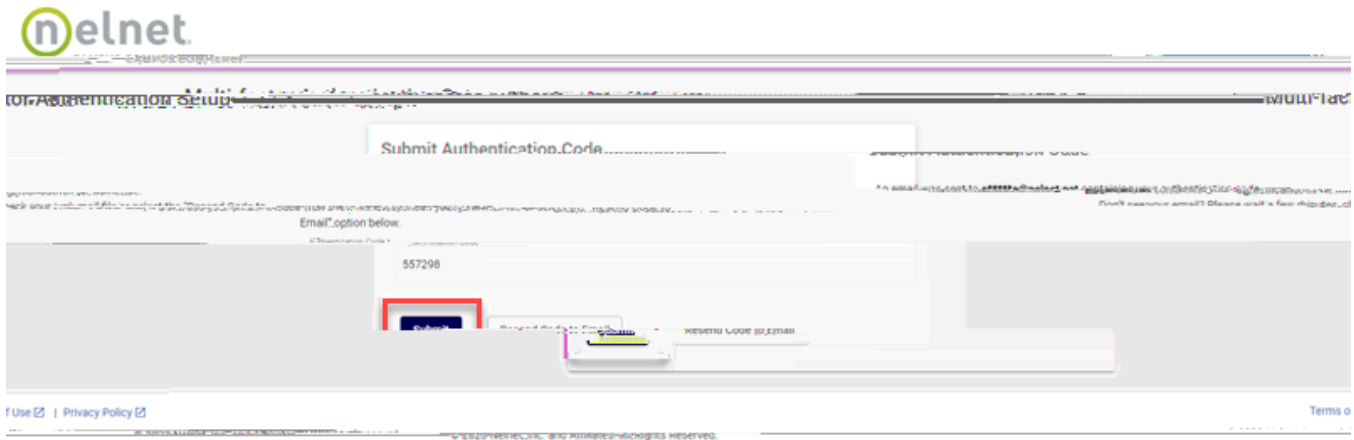


Logging in with MFA - Email

After entering your username and password you will be asked to select the email to which you'd like the authentication code to be sent (if you have multiple email address saved in your profile). Make your selection and click the **Send Code to Email Button**. If you have only one email stored with your profile the authentication code will automatically be sent to that email address.



Check your email to find your one-time use code. Enter the provided code and click the **Submit** button.



Logging in with MFA - Authenticator App

After entering your username and password you will be asked to enter a **Verification Code** from your authenticator app. Enter the code and then click **Verify**

