OneView®

Tip Guide: (MFA) Multi-Factor Authentication

modio

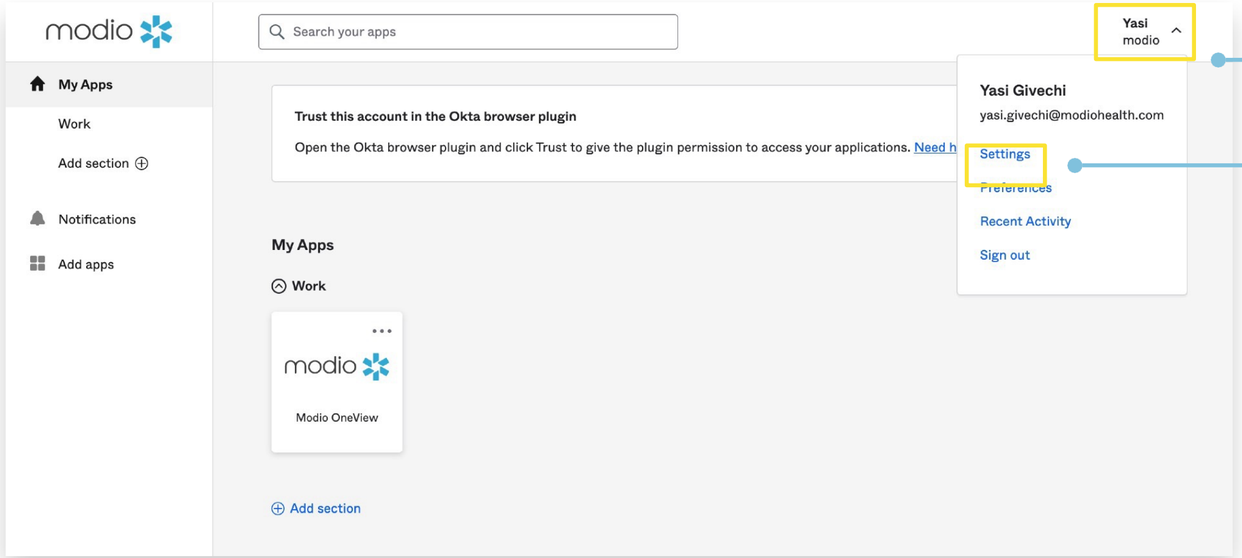
Overview

Multi-Factor Authentication is an effective way to provide enhanced security. MFA creates multiple layers of security to help increase the confidence that the user requesting access is who they claim to be.

What is Multi-Factor Authentication?

Multi-Factor Authentication (MFA) is a security practice that requires more than one method of authentication, using independent categories of credentials to verify a user's identity. MFA is widely used by financial institutions, healthcare providers, government agencies, educational institutions, and technology companies to protect sensitive data and ensure secure access to their systems.

Turning On multi-factor Authentication (MFA)

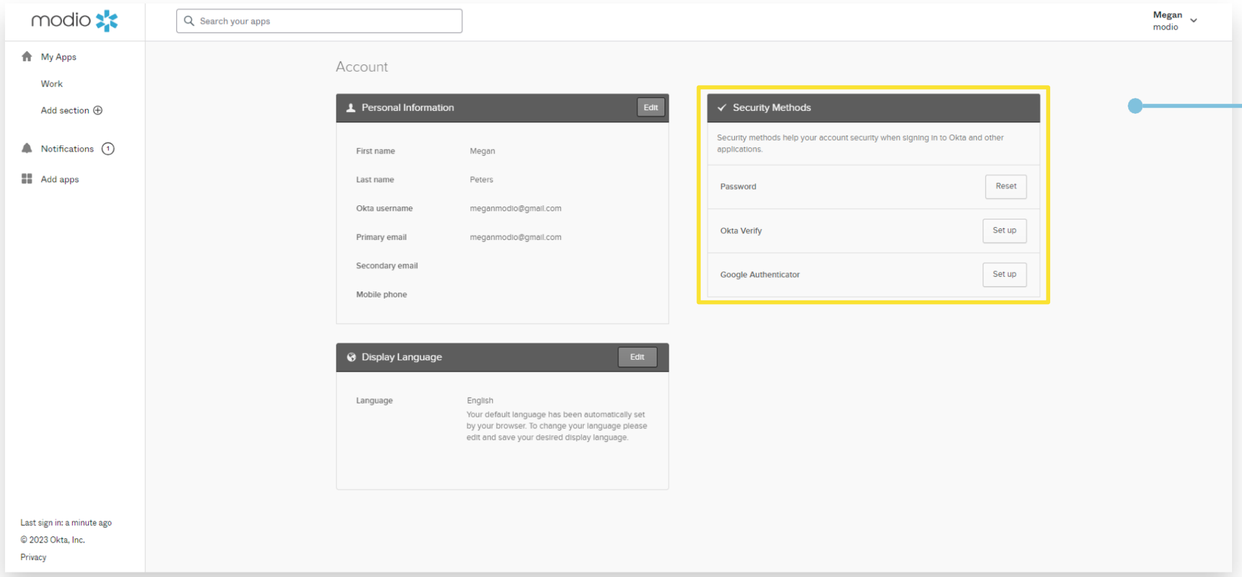


1 Starting Steps:

1. Visit https://auth.modiohealth.com/ and sign in.

2

2. Access your personal settings. On your Okta dashboard, select your **name** in the upper righthand corner and then click **Settings**.



Access the Security Methods section:

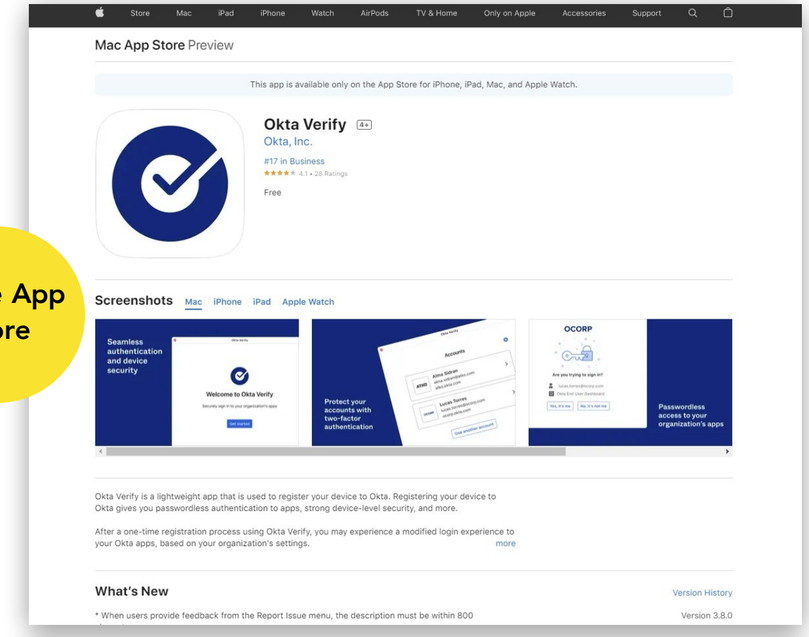
3

3. You have two options for MFA. We recommend setting up both methods for an extra layer of security.

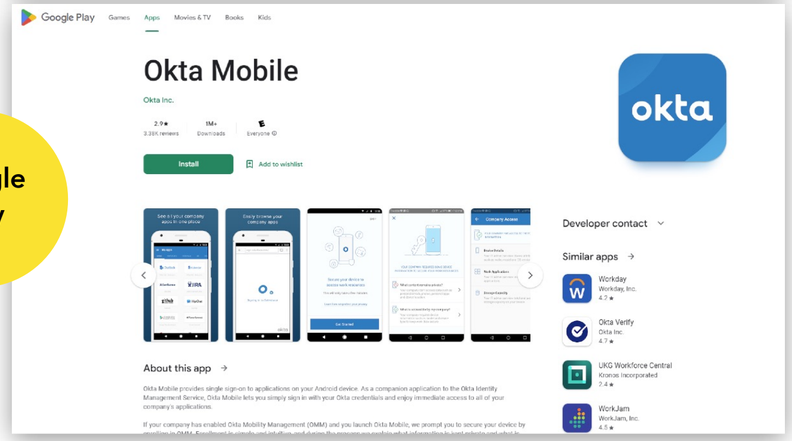
- To set up Okta Verify, go to step 4 (page 9)
- For Google Authentication, go to step 5 (page 12)

4b. Download Okta Verify from the app store.

Apple App Store

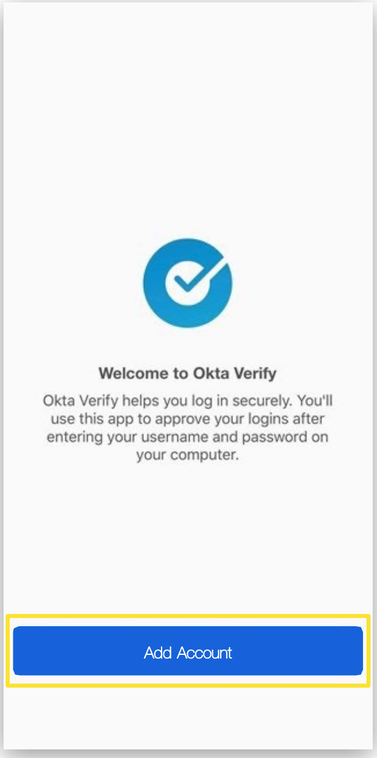


Google Play



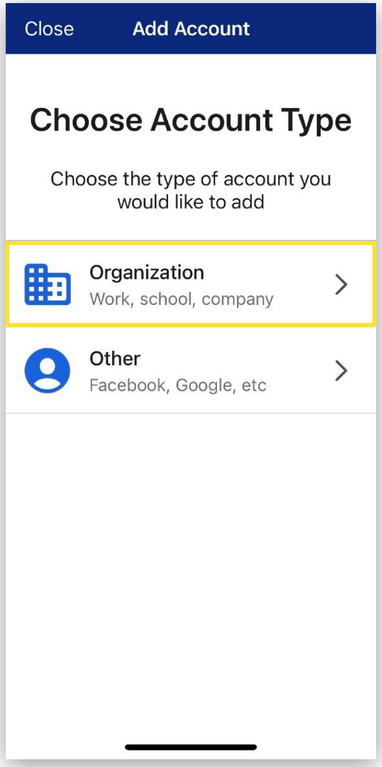
(View on your computer browser)

4c. Once downloaded, Open the Okta Verify app. Select Add Account or tap the + button.



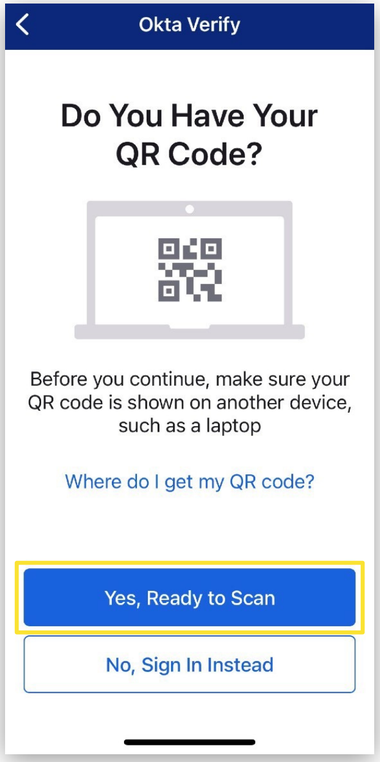
(View on your mobile device)

4d. Choose the Organization account type



(View on your mobile device)

4e. Select "**Yes, Ready to Scan".** Use the device's camera to scan the QR code on your computer. This will complete the enrollment.

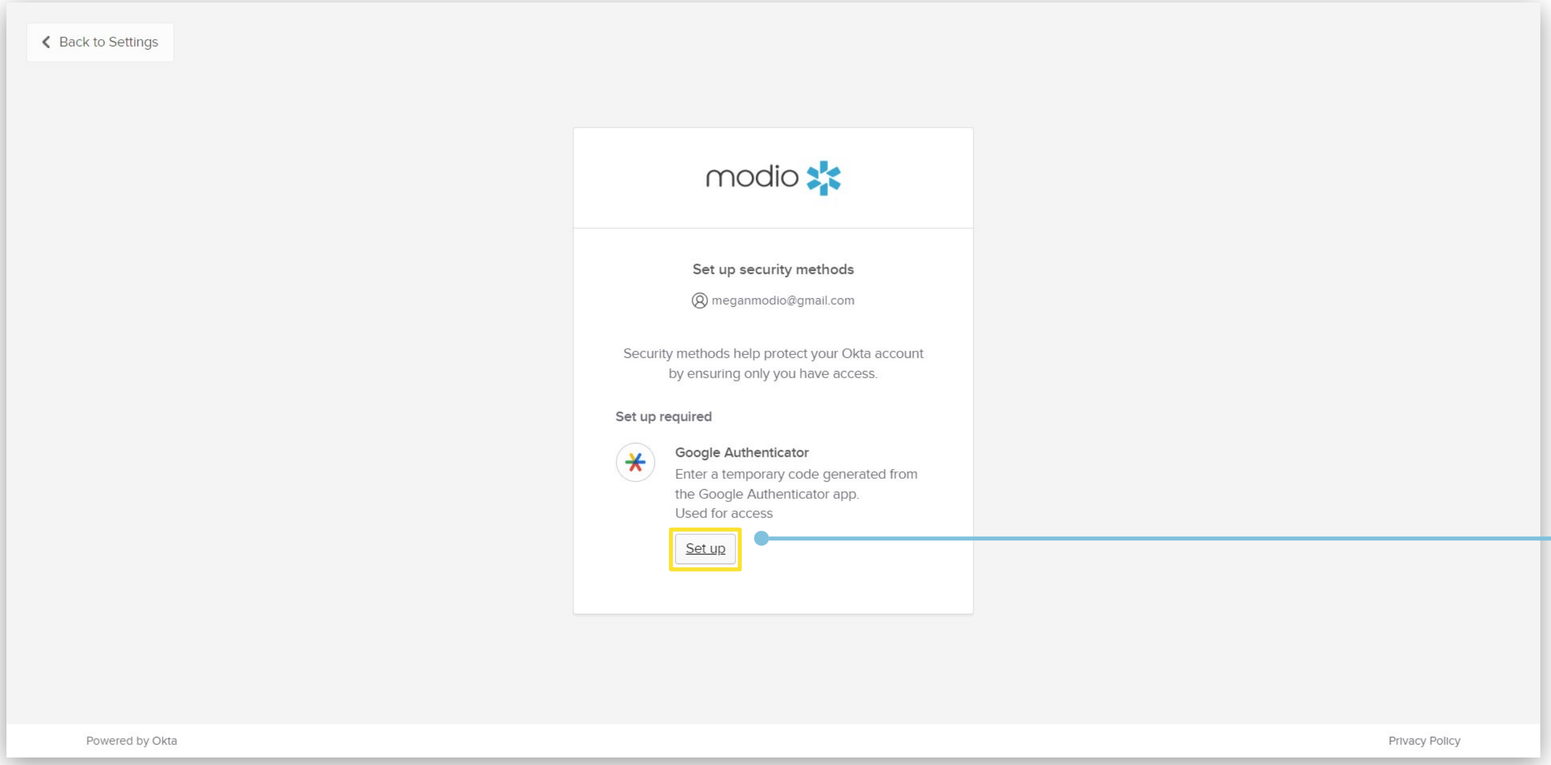


(View on your mobile device)

Note: Okta Verify recommends using Face ID on iPhones to ensure security and may prompt you to enroll.

modio

GOOGLE AUTHENTICATION SETUP

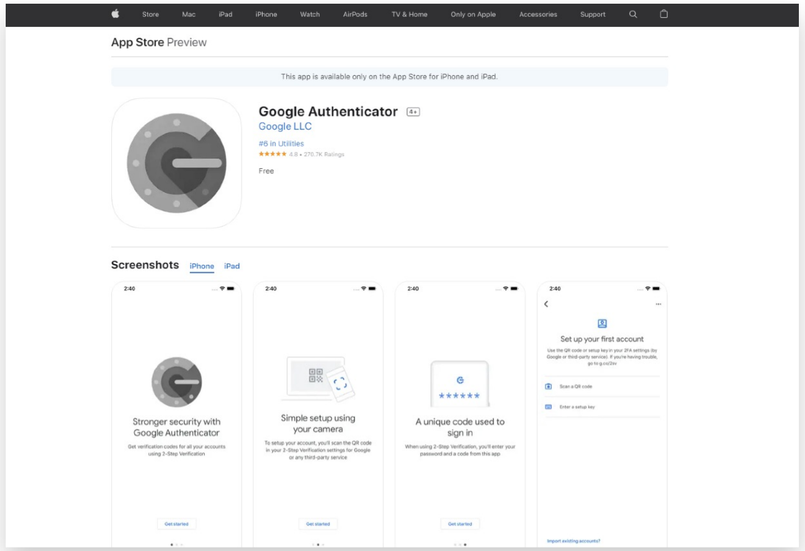


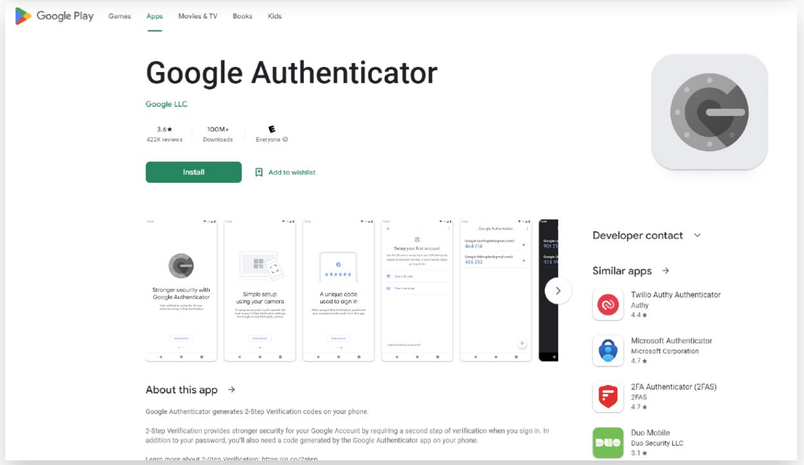
5

5. Set up Google Authentication:
To use this, you will need access to a mobile device.

(View on your computer browser)

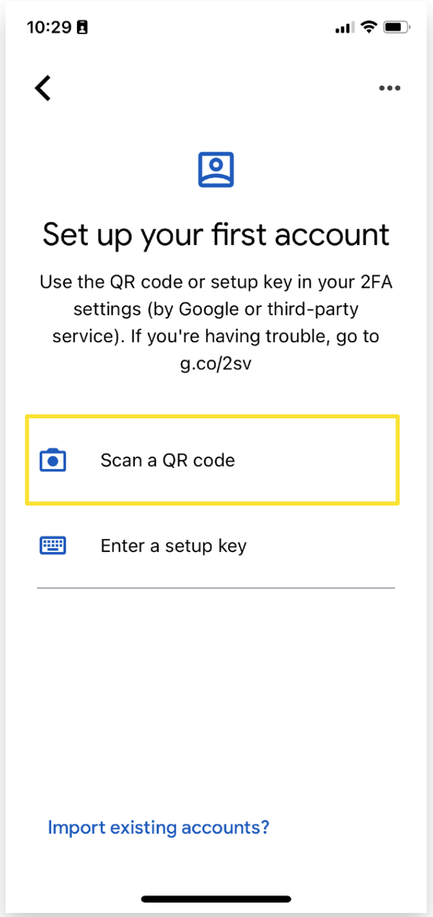
5c. Launch Google Authenticator.
Set up your first account or tap the + sign.



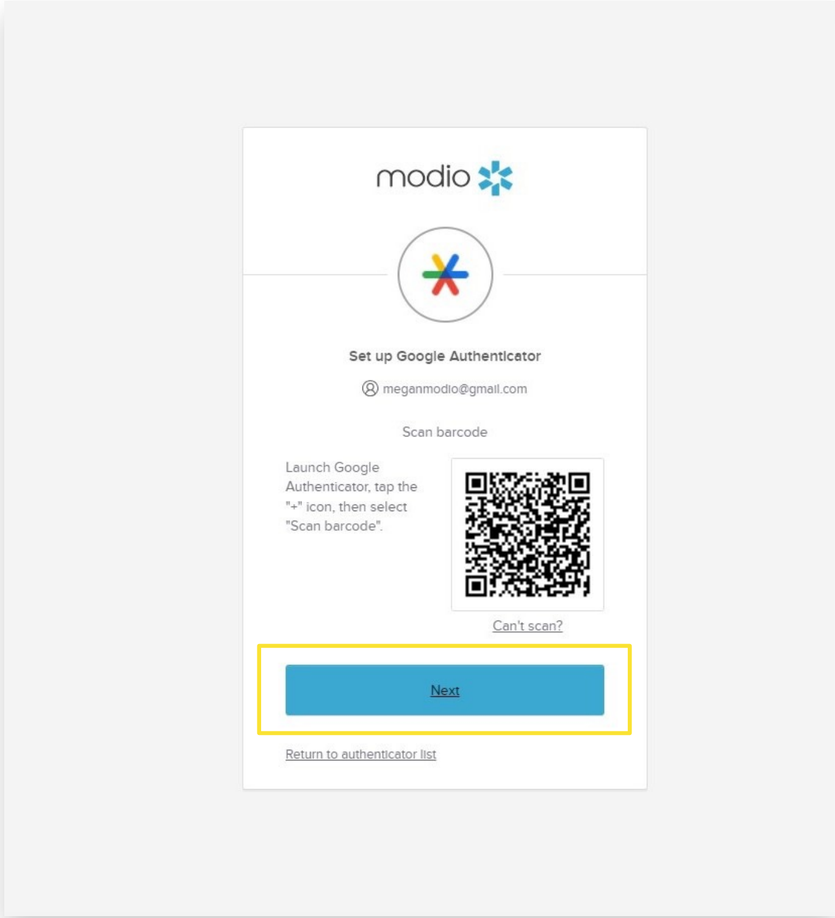


(View on your computer browser)

5d. Tap Scan a QR code. Use the device's camera to scan the QR code on your computer. Click Next.

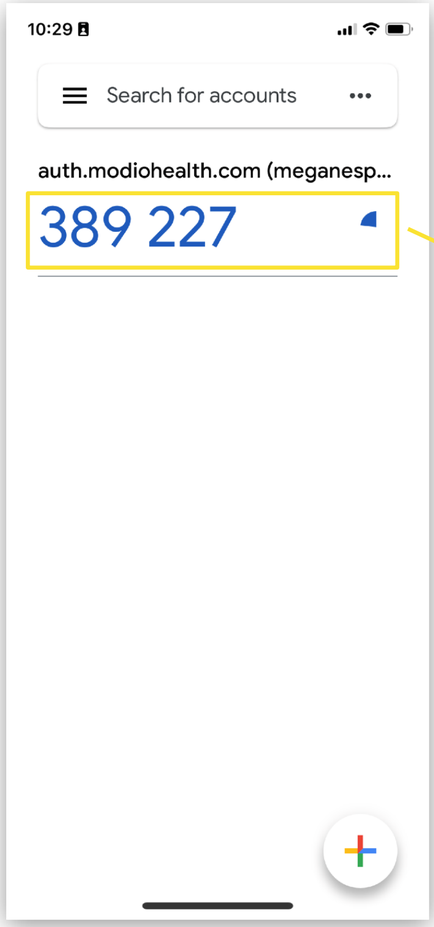


(View on your mobile device)



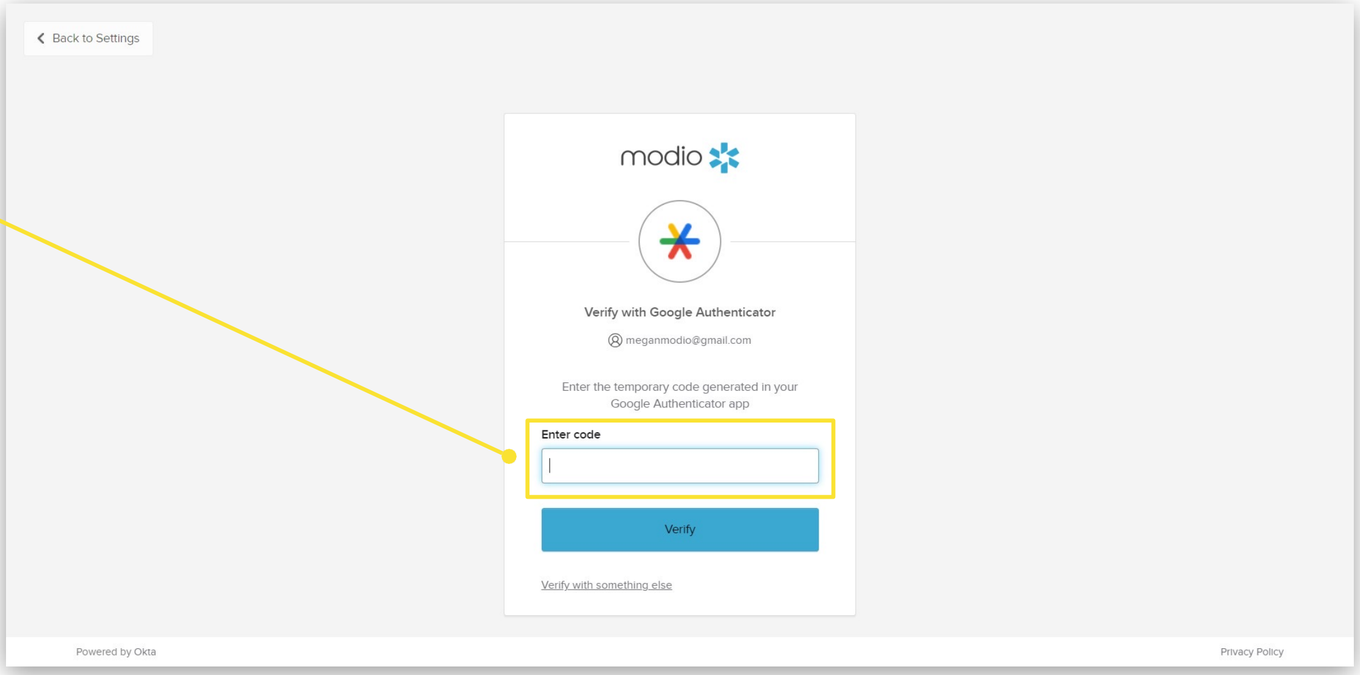
(View on your computer browser)

5e. Enter the code shown on your mobile device in the Enter Code field.



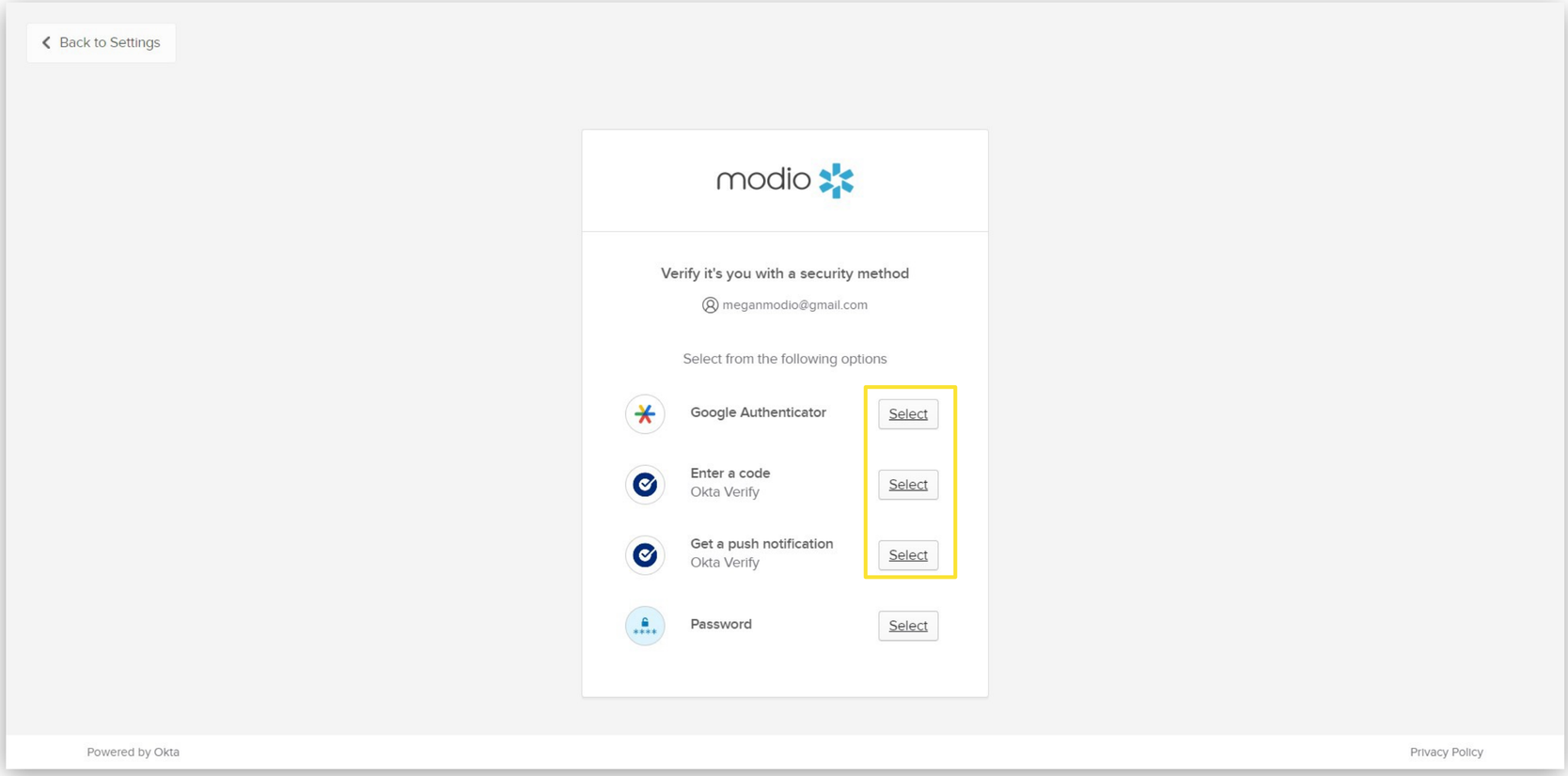
(View on your mobile device)

5f. Once you've entered the code in the Setup Google Authenticator field, Click Verify. You are now enrolled.



(View on your computer browser)

4g. When updating security methods, you will be prompted to use MFA. Choose between Google Authenticator or Okta Verify (Enter a code or Get a push notification). You can also choose to enter your password.



FAQs

Q: What is Multi-Factor Authentication (MFA)?
A: Multi-Factor Authentication is a security practice that requires more than one method of authentication, using independent categories of credentials to verify a user's identity. For example, you may log in to a system using your password ("what you know") and then verifying a separate six-digit number that is sent to your phone ("what you have"). By combining "what you know" and "what you have" verification, it becomes much more challenging for unauthorized users to access OneView as they would need both to gain access.

Q: What is the benefit of using MFA?
A: MFA is an effective way to provide enhanced security. Traditional usernames and passwords can be stolen, and they've become increasingly more vulnerable to malicious activity, and cyber-attacks like phishing or brute force attacks. MFA creates multiple layers of security to help increase the confidence that the user requesting access is who they claim to be.

Q: If I opt-in to use MFA will I have to sign in to OneView using MFA every time?
A: No! The OneView® MFA parameters require you to authorize via MFA once every seven days, if you are logging in from the same computer. If Okta identifies that you are logging in from a different computer, it will automatically require a new MFA authorization, even if you are within the seven days.

Q: How can I start using MFA for my employees?
A: Employees can individually turn on MFA through their Okta dashboard. Use the steps described on pages 4-10 to enable authentication through Okta Verify or Google Authentication. We recommend enrolling two methods, in case you lose access to either app.

Q: Why can't we use SMS as a verification method?
A: Okta and the rest of the identity verification industry are moving away from SMS as a secure method of authentication, due to mobile security threats and data breaches. SMS is not designed to securely transport data whereas mobile apps can use additional layers of security like biometrics. Learn more in this article.

Q: Can we turn on MFA for our organization all at once?
A: Yes! If you would like to turn on MFA for your organization, please reach out to our support team (support@modiohealth.com) and we can enable that for all users.

For additional questions or further training, contact the Modio Team:

Online:
Live Chat Support

Email:
support@modiohealth.com

Phone:
844.696.6346