OneView®

Tip Guide - Okta

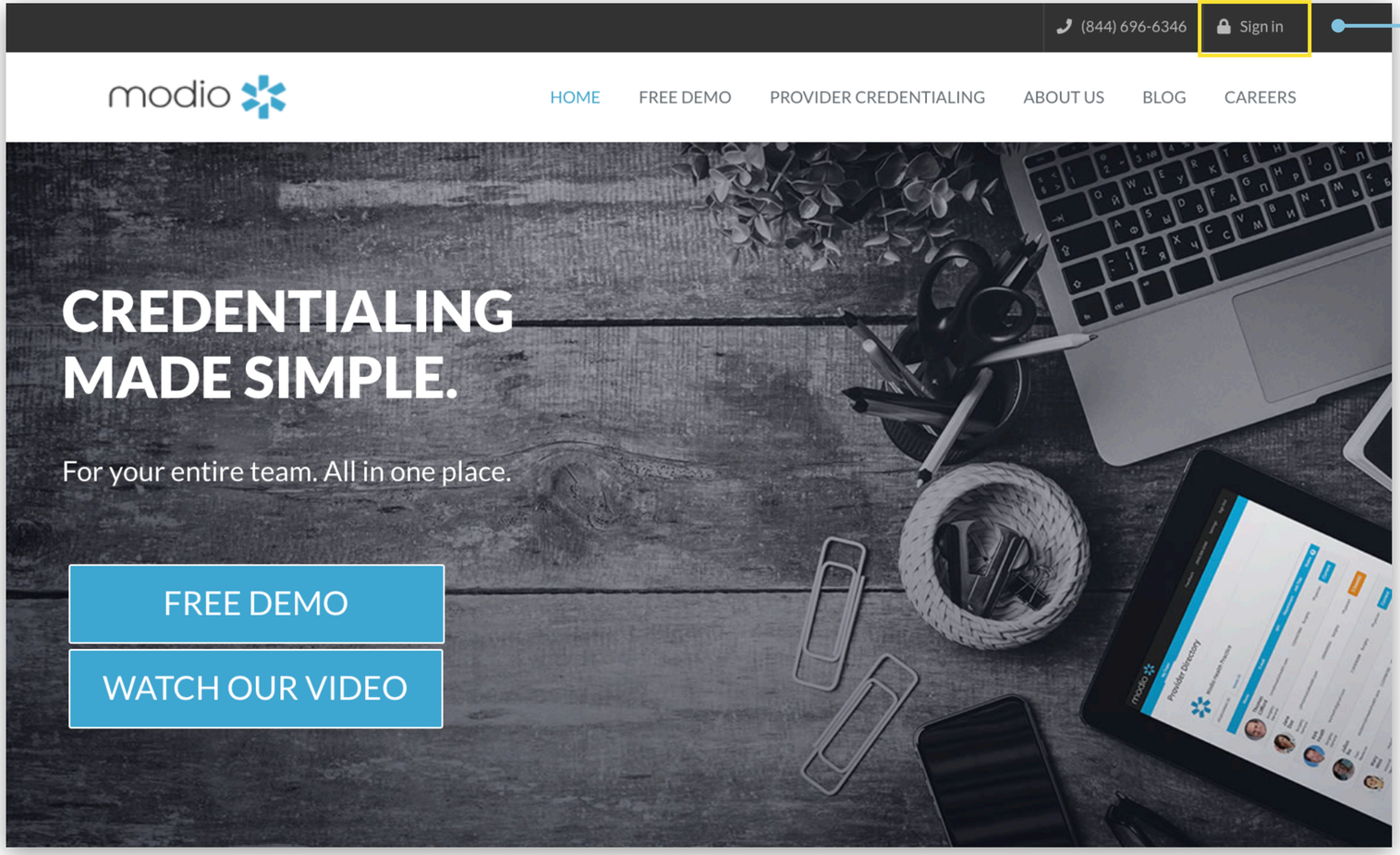
modio

Overview

Effective Oct 11th, 2022, Sign in for the OneView platform will be done via Okta.

What is Okta?

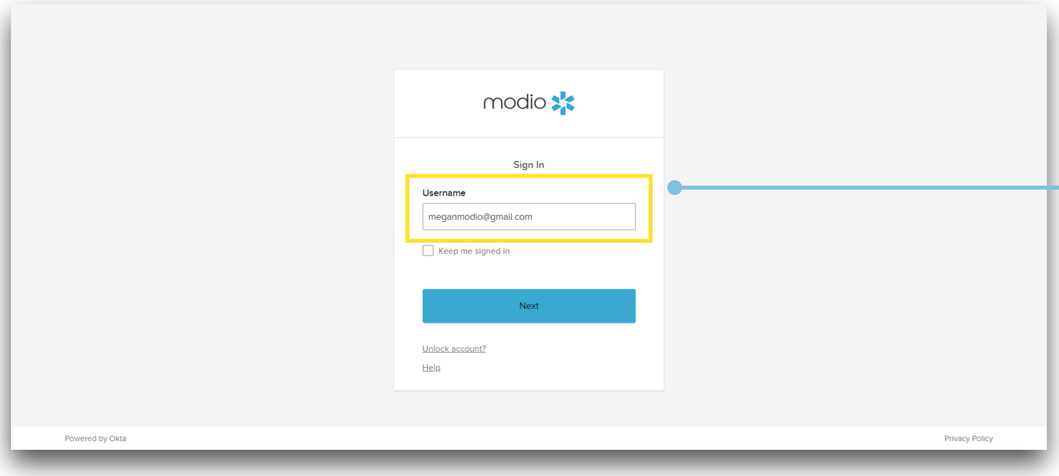
Okta provides secure sign-in from anywhere using virtually any device. It provides an extra layer of protection to your data by granting access to only those with verified credentials. To learn more about Okta; visit this link.



1

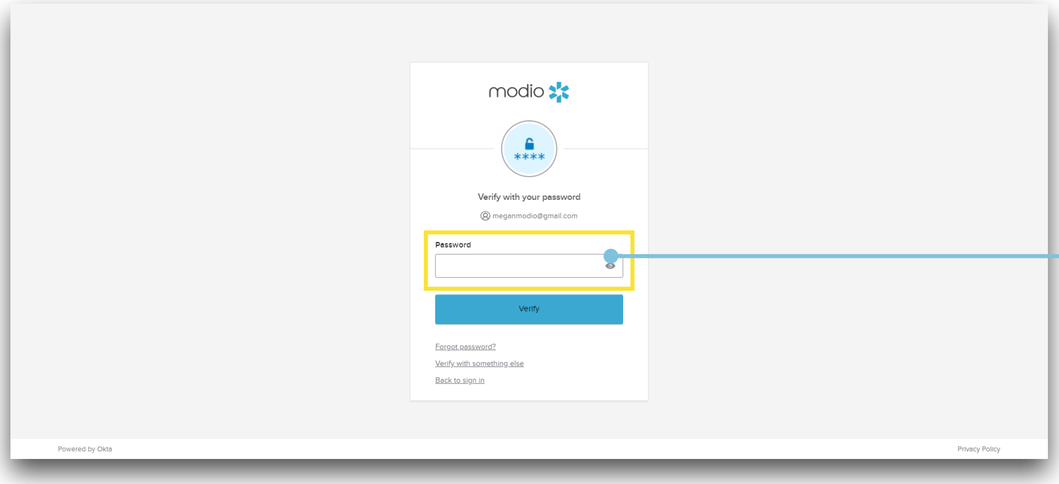
Navigate to Modio:

Visit our website at: www.modiohealth.com and click **"Sign in,"** which is located on the top right hand corner. If you have previously bookmarked the login page you will be automatically redirected to the new login page, which you can also bookmark for quick access.



2

Logging into OneView:
Use the email address you use to sign into OneView currently in the Username field. *Contact the Modio Support team if you have not received your login information yet by emailing support@modiohealth.com.



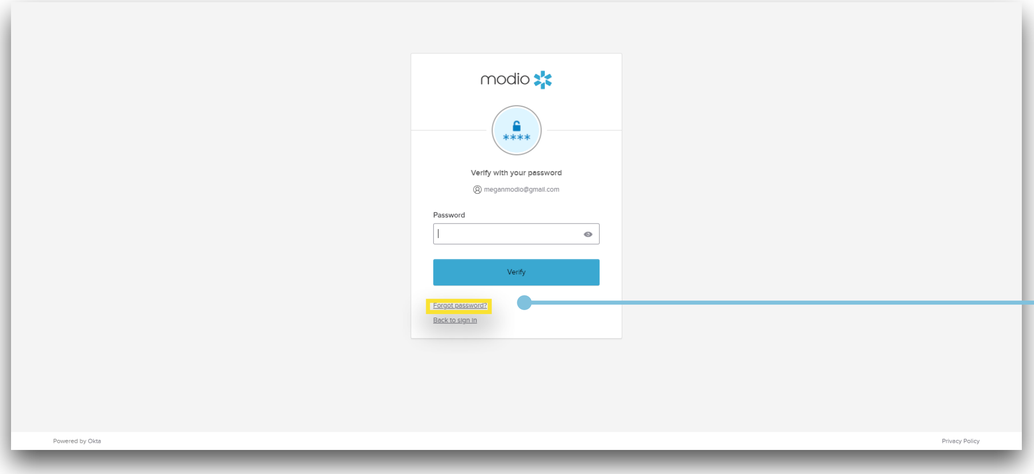
3

Enter your password:
Use your current OneView password. If that password does not meet the complexity requirements, you will be prompted to update it.

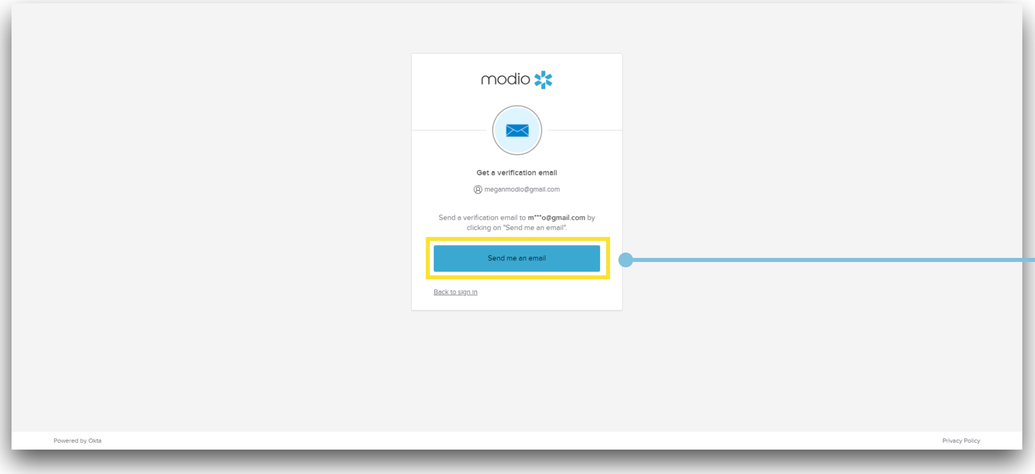
Using a complex password: Your password must include at least 3 out of 4 of the following requirements:

1. Upper case letter
2. Lower case letter
3. Number
4. Special character

Save your password:
Select “Keep me signed in” to save your credentials for next time.



1 **Having trouble accessing your account?**
Select “Forgot password?”.



2

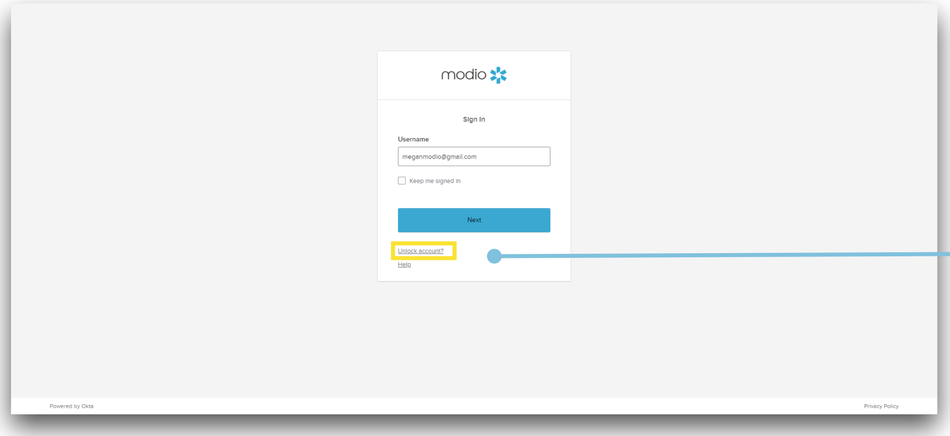
Reset your password: Send a verification email to the email associated with your account by clicking on “Send me an email”.

Access your email: Open the email from noreply@modiohealth.com and click the Reset Password link. This link expires within an hour.

Enter a strong password: You’ll be required to create a complex password that meets the following requirements:

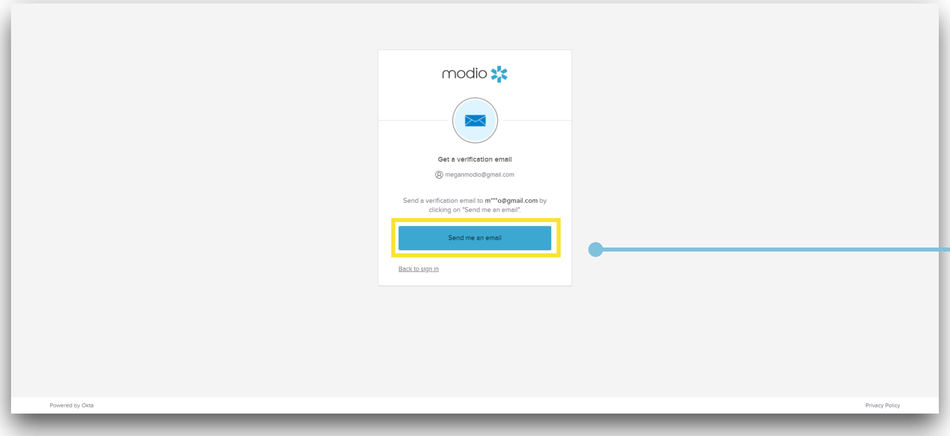
1. Use of upper case letters, lower case letters, numbers, and special characters
2. At least 8 characters long
3. Includes no part of your username
4. Does not match any of your last 5 passwords

Note: Previously password resets were conducted in the "settings" section of OneView. New password changes will only be accessible by clicking the “Forgot password?” link on the sign-in page.



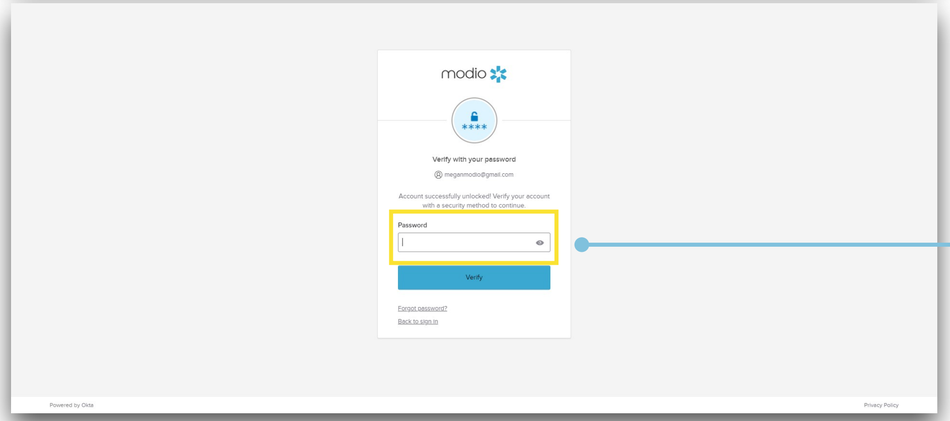
1 **Were you notified that your account is locked?**

If we see suspicious activity on your account, like repeated failed attempts to sign-in, then your account may be locked. On the sign-in page, you should see the link "Unlock account?". Enter your username on the next page.



2 **Initiate an unlock:** Send a verification email to the email associated with your account by clicking on “Send me an email”.

Access your email: Open the email from noreply@modiohealth.com and click the Unlock Account link or enter the code instead. This link expires within 5 minutes.

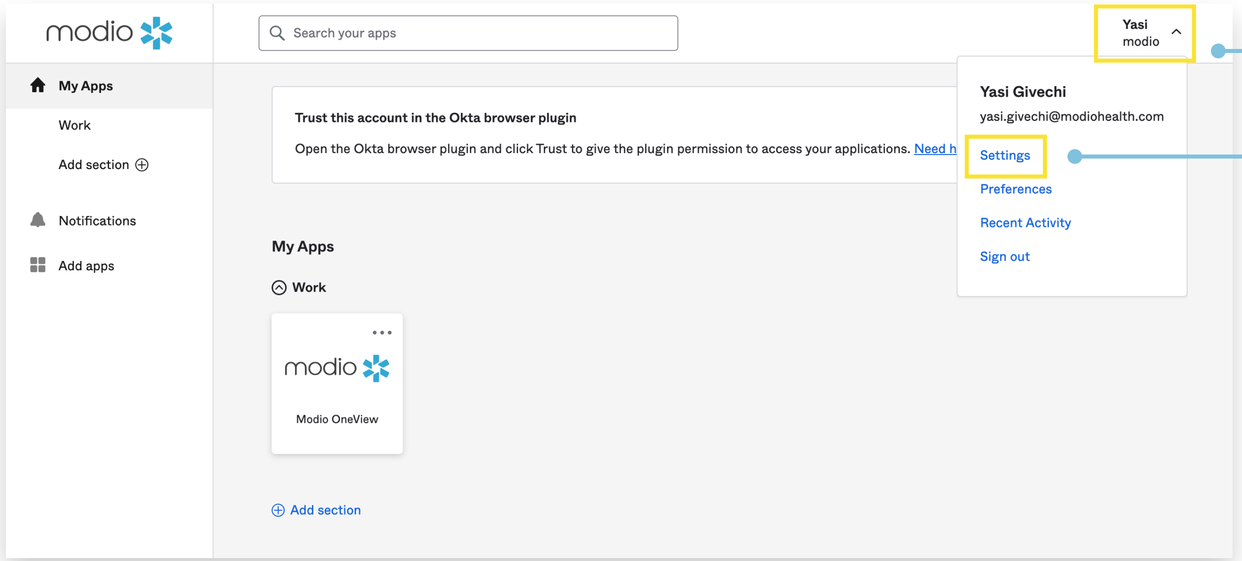


3 **Complete sign-in:** You’ll be required to enter your password to finish signing in. If necessary, you can select "Forgot Password" to create a new password.

Note: If you need additional help, reach out to our support team at support@modiohealth.com to help unlock your account.

modio

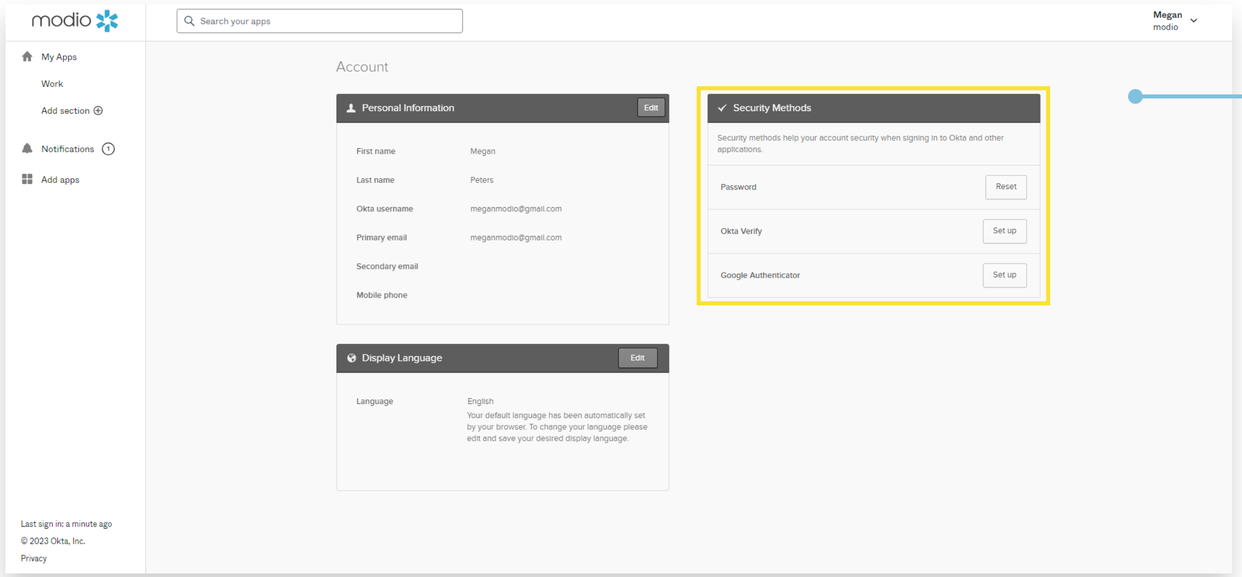
Turning On multi-factor Authentication (MFA)



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**.

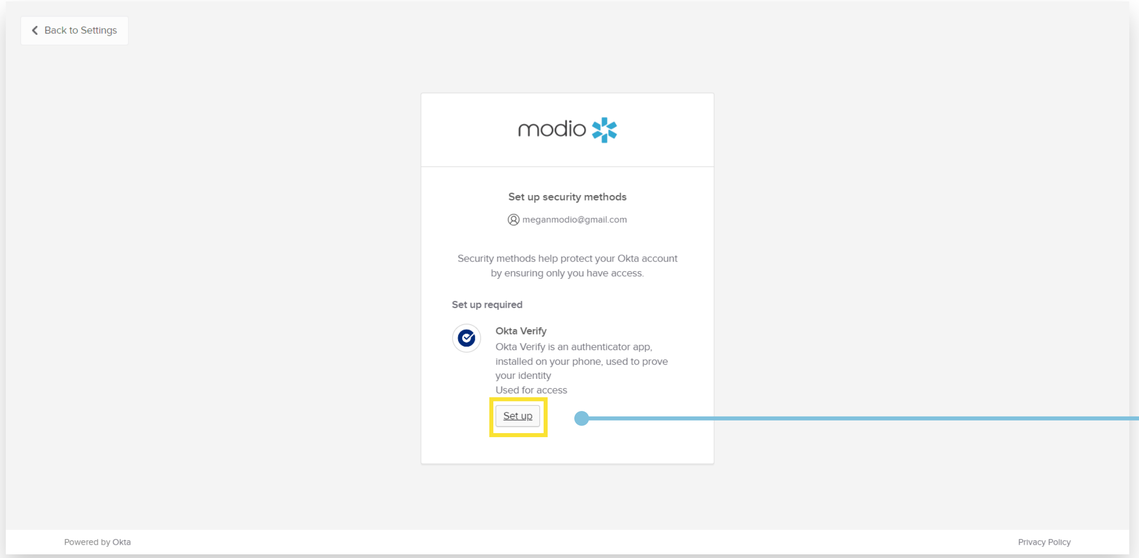


3 **Access the Security Methods section:**

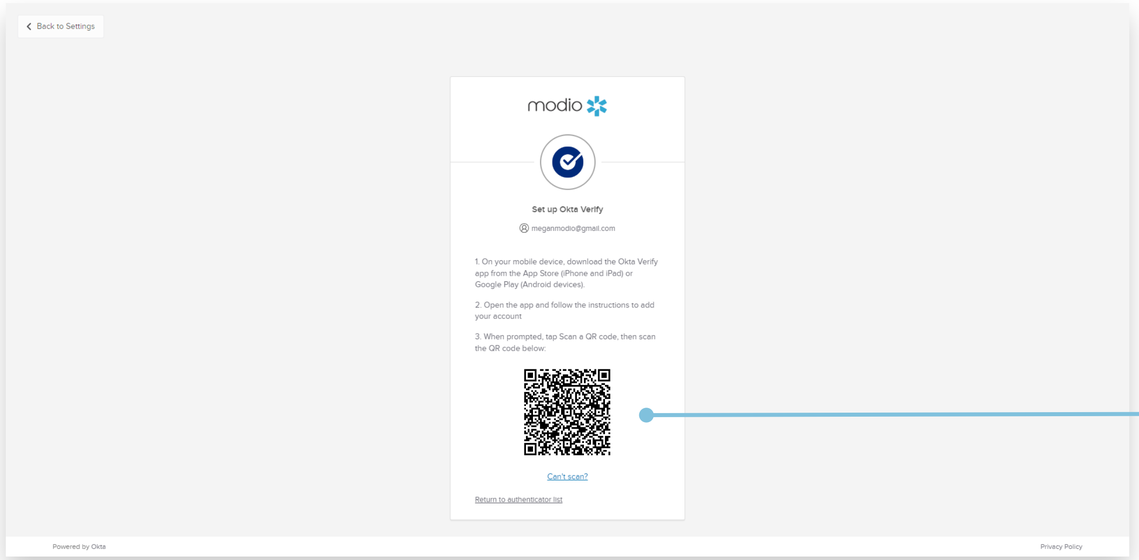
3. You have two options for MFA. We recommend setting up both methods for an extra layer of security.

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

Okta Verify Setup



4. Set up Okta Verify:
To use this, you will need access to a mobile device.

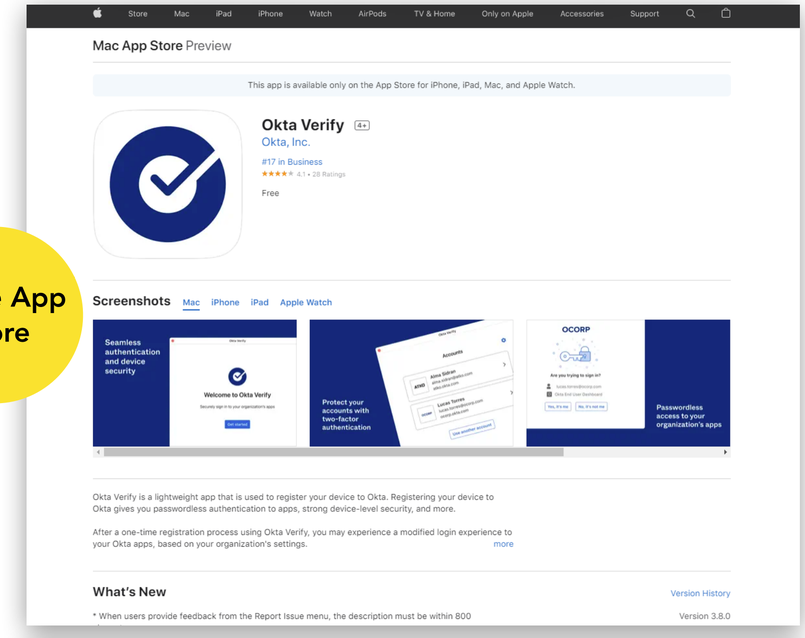


4a. On your mobile device, download Okta Verify from the app store. Follow the steps on the next page to open the camera in app to scan the QR code on your computer browser.

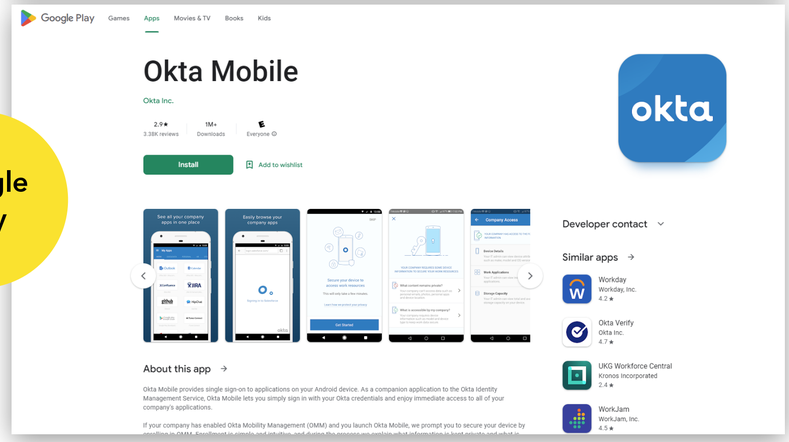
(View on your computer browser)

4b. Download Okta Verify from the app store.

Apple App Store

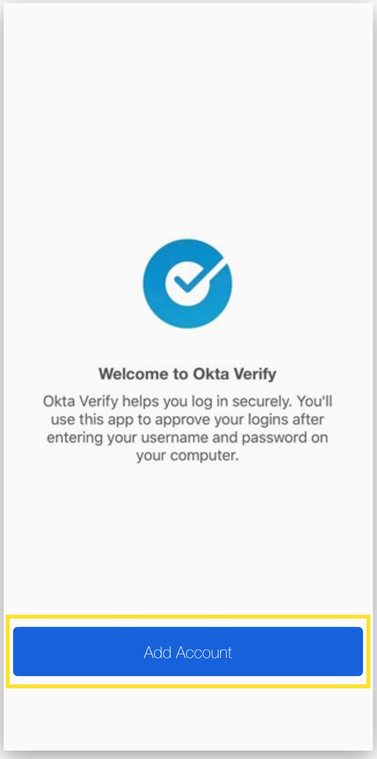


Google Play



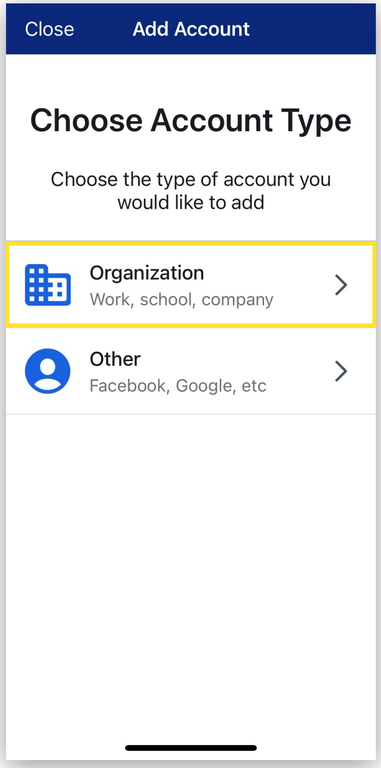
(View on your computer browser)

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



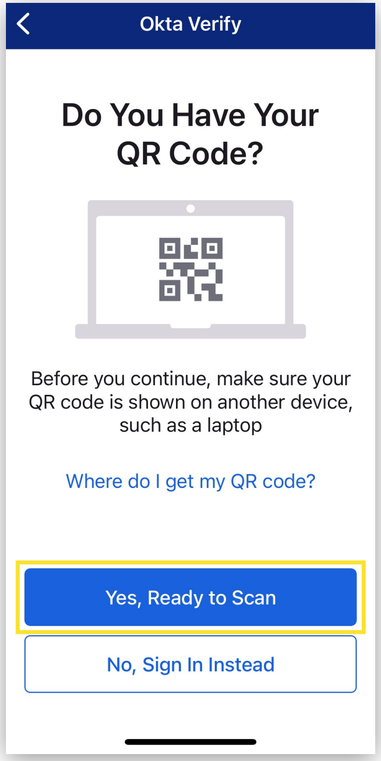
(View on your mobile device)

4d. Choose the Organization account type



(View on your mobile device)

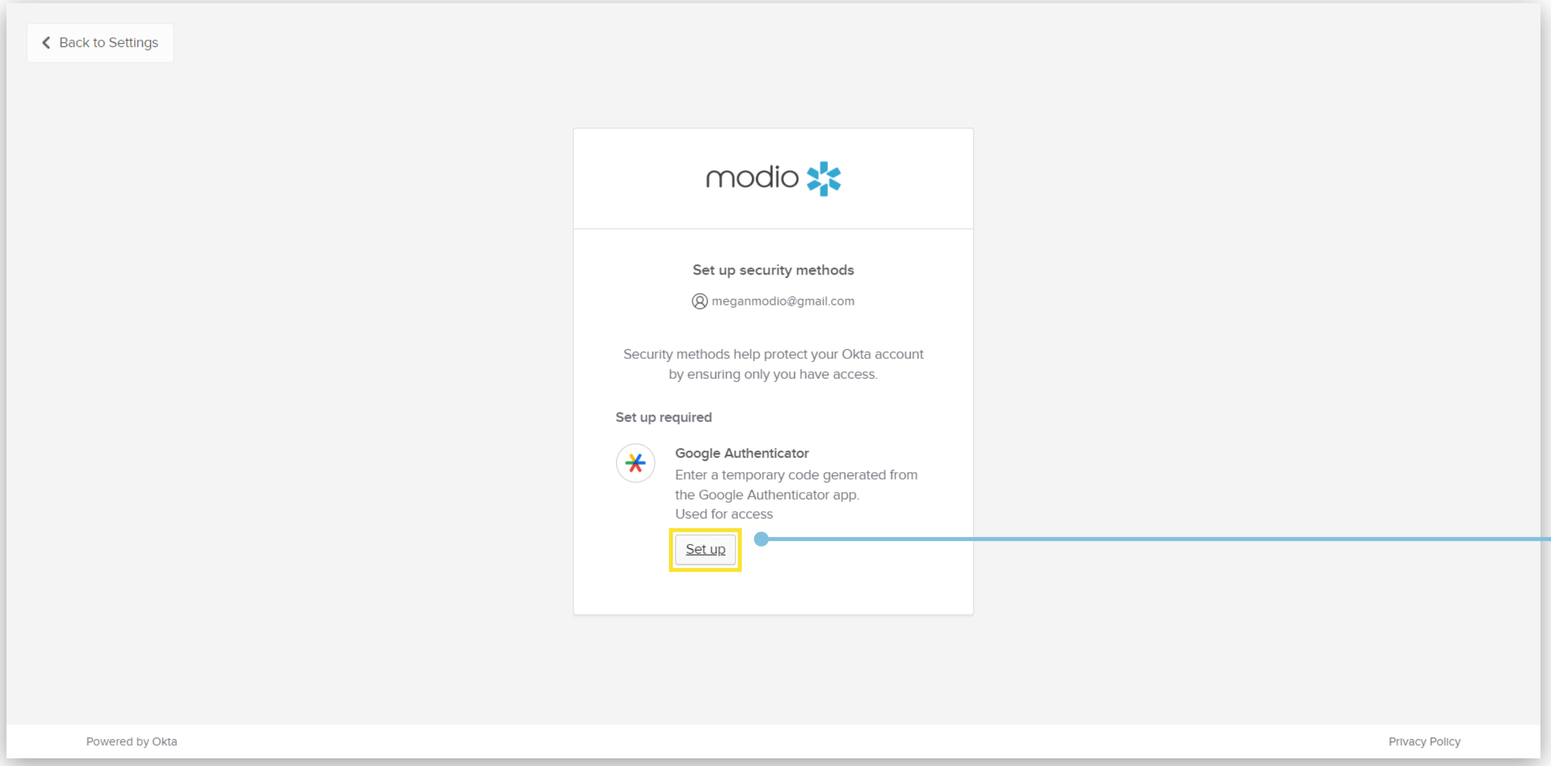
4e. Select "**Yes, Ready to Scan".** Use the device's camera to scan the QR code on your computer. This will complete the enrollment.



(View on your mobile device)

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

Google Authentication Setup



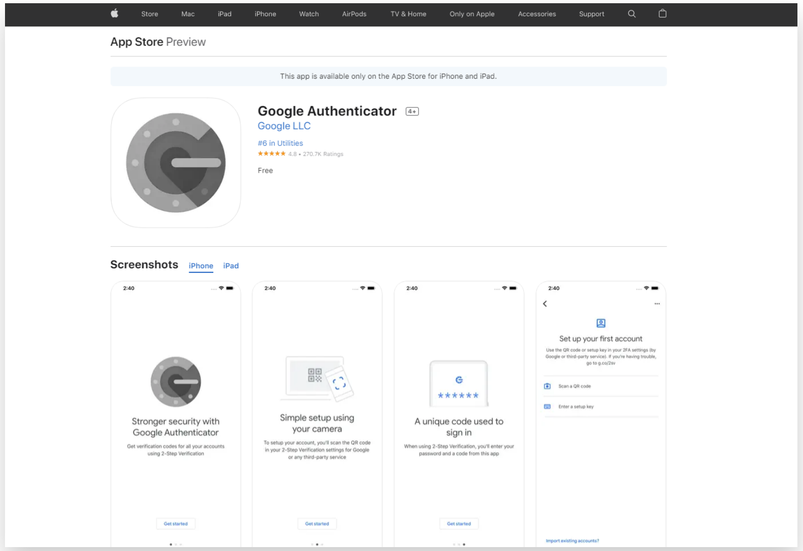
5

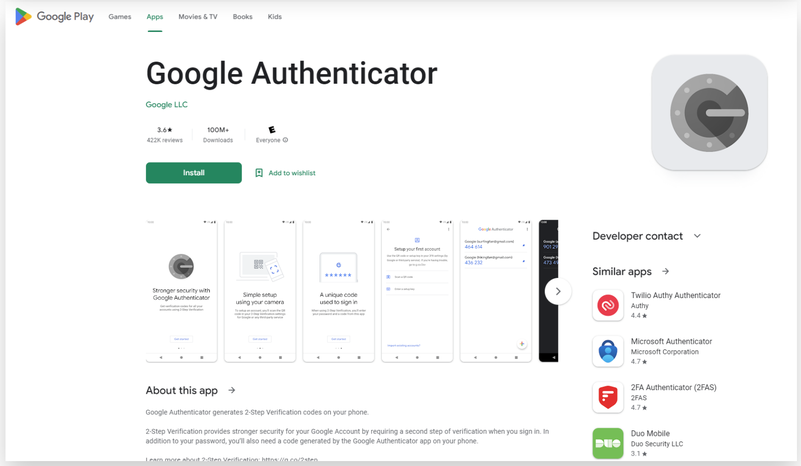
5. Set up Google Authentication: To use this, you will need access to a mobile device.

(View on your computer browser)

5c. Launch Google Authenticator.

Set up your first account or tap the + sign.

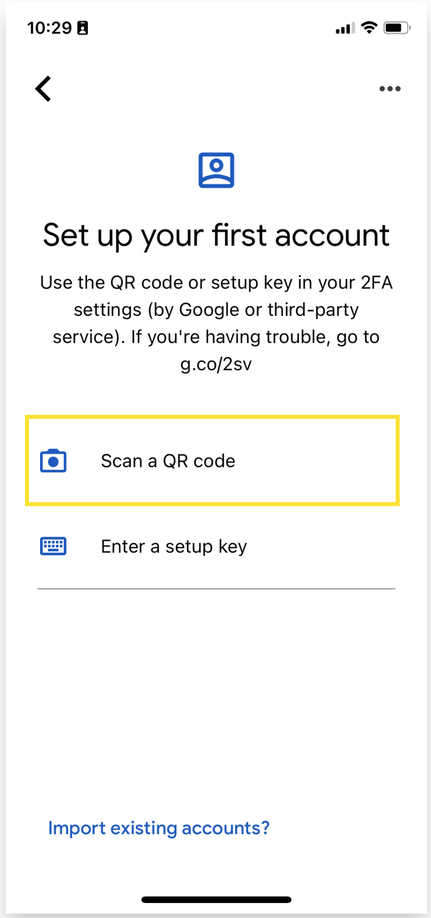




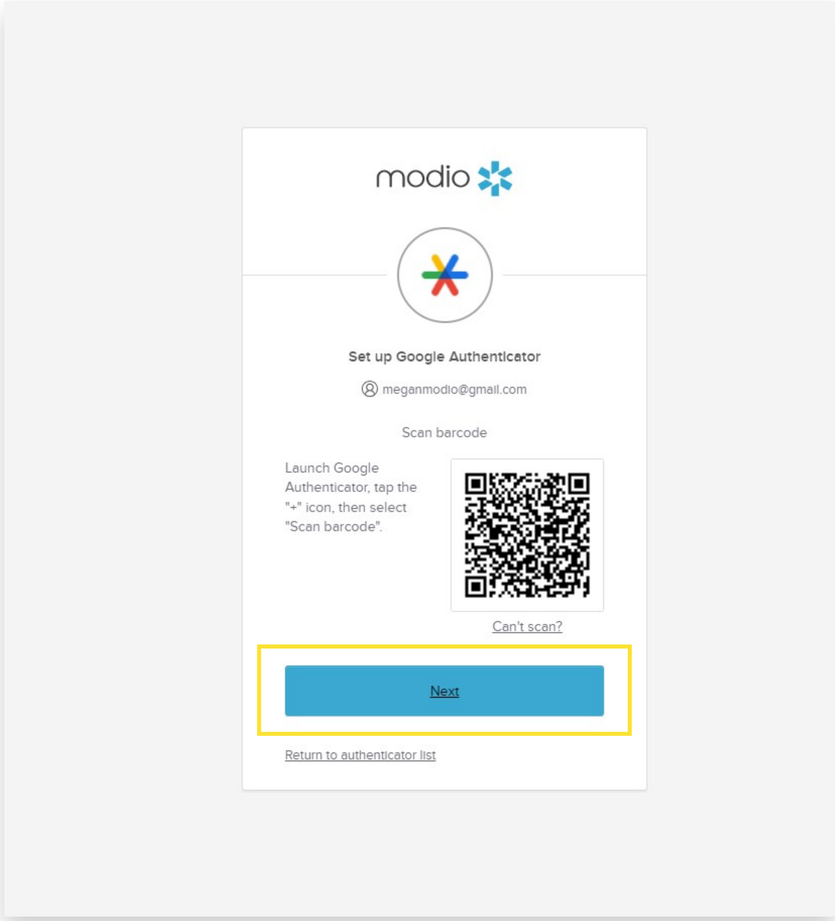
(View on your computer browser)

5d. Tap Scan a QR code.

Use the device's camera to scan the QR code on your computer. Click Next.

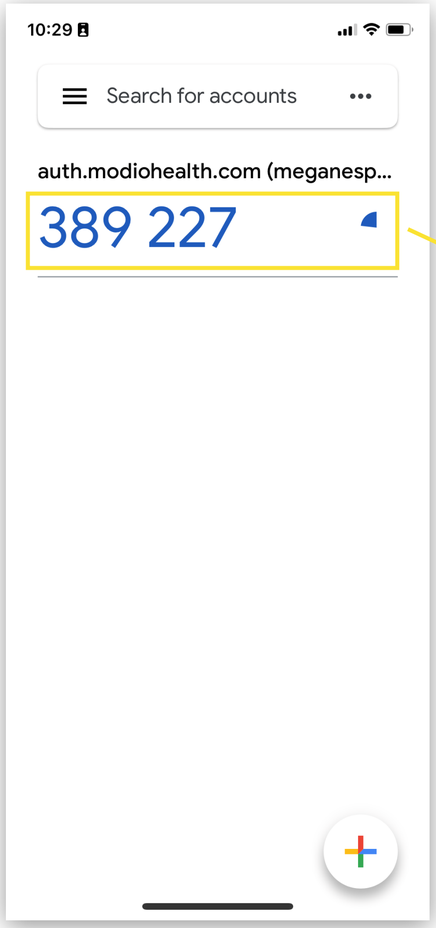


(View on your mobile device)



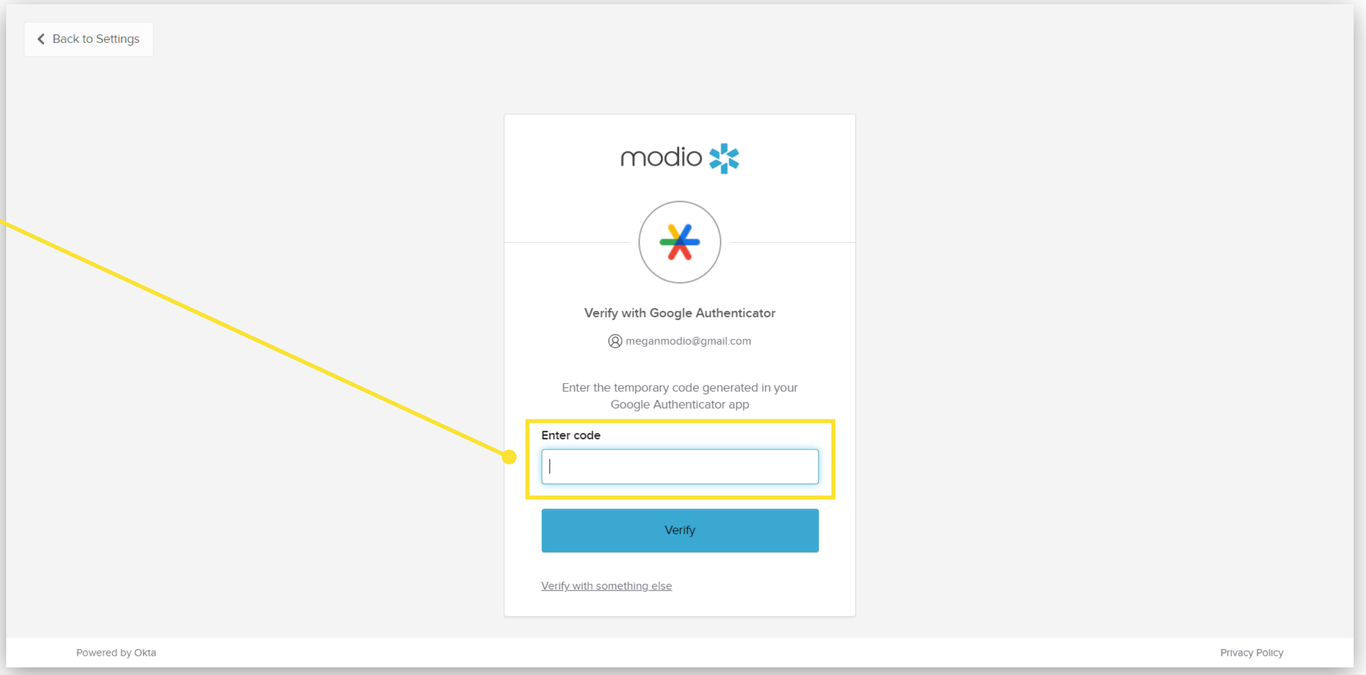
(View on your computer browser)

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



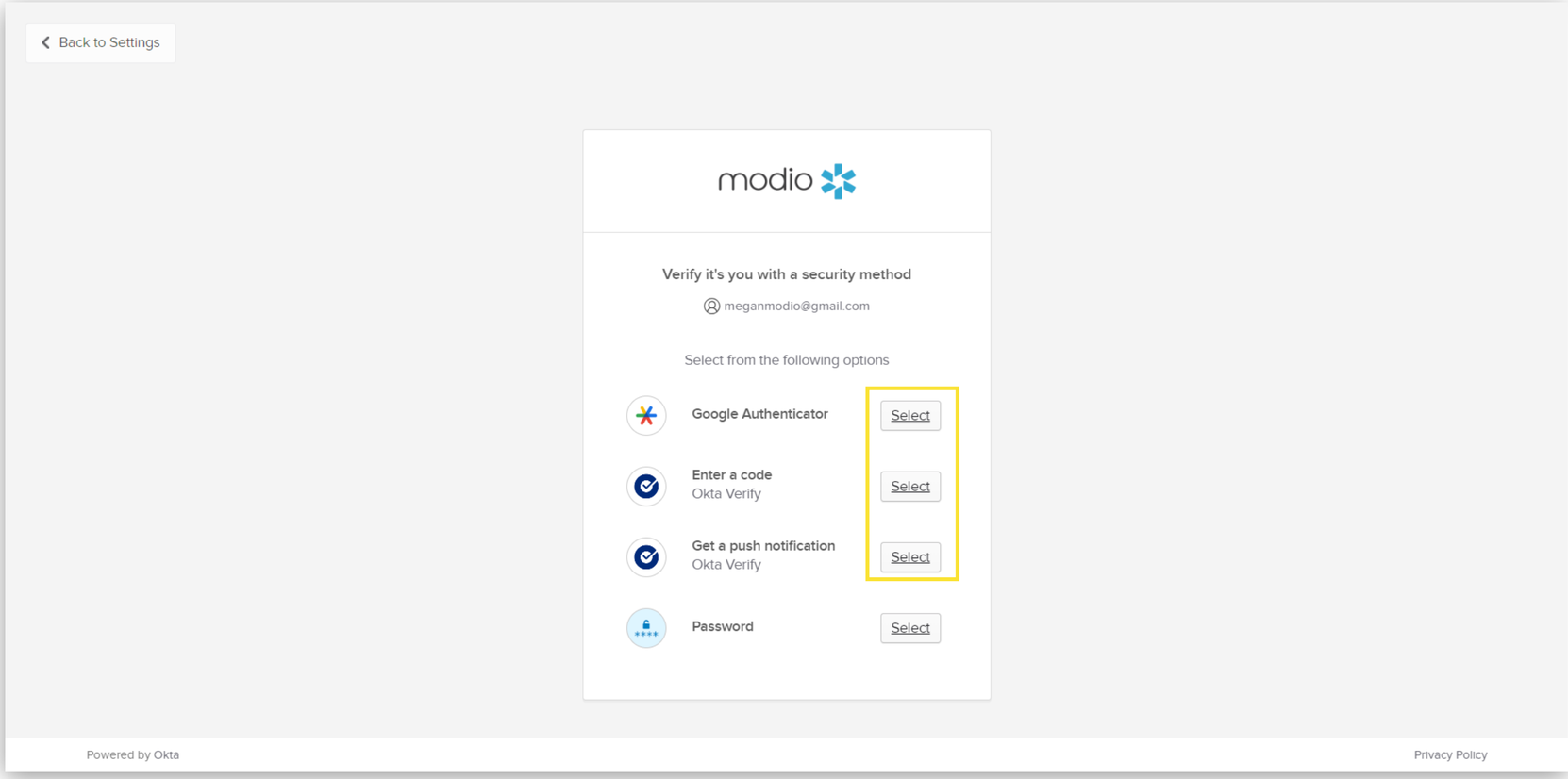
(View on your mobile device)

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.



FAQ

Q: What do I need for a complex password?
A: On a basic level, "strong passwords" are about password length and complexity, making it difficult for unauthorized users to gain access to your account. After this release, your password must include at least 3 out of 4 of the following requirements:

i. Upper case letter
ii. Lower case letter
iii. Number
iv. Special character

If your current password does not meet these requirements, you will be prompted to create a new password upon your first sign-in.

Q: How often will I need to reset my password?
A: You will be prompted to update your password every 180 days. Expect an email from us a few days before your password expires so that you can change it in advance.

Q: What does it mean if my account is locked?
A: If we see suspicious activity on your account, like repeated failed attempts to sign-in, then we will lock your account. Follow the steps on page 6 or reach out to our support team at support@modiohealth.com to help unlock your account.

Q: What if I don't have access to the email for my account? How can I update my email?
A: If you need to update the email address on your account, reach out to our support team at support@modiohealth.com.

Q: How do I remove a user?
A: If you need to remove a coordinator from your account, reach out to our support team at support@modiohealth.com.

Q: Can my coordinators share an account login?
A: We do not support allowing shared logins to ensure all activity in the platform is captured accurately in the audit trail. Resetting your password also requires that you have access to the email address on your account.

Q: Which NCQA requirements does this meet?
A: In 2022, NCQA released new guidelines around protecting credentialing information with system controls for organizations seeking certification. These requirements include identity and authentication policy for the system used to store credentialing information, i.e., OneView.

We have configured our Okta settings to meet the following requirements:
1. Passwords change immediately after first use
2. Limit repeated access attempts by locking out the user ID after not more than 8 attempts
3. All user passwords change every 180 days and must be different than the previous 5 attempts
4. Set the lockout duration to a minimum of 5 minutes

FAQ - Continued

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.

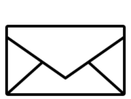
Q: How can I start using MFA for my employees?
A: Employees can individually turn on MFA through their Okta dashboard. Use the steps described on pages 4-10 to enable authentication through Okta Verify or Google Authentication. We recommend enrolling two methods, in case you lose access to either app.

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