OneView®

Okta Tip Guide

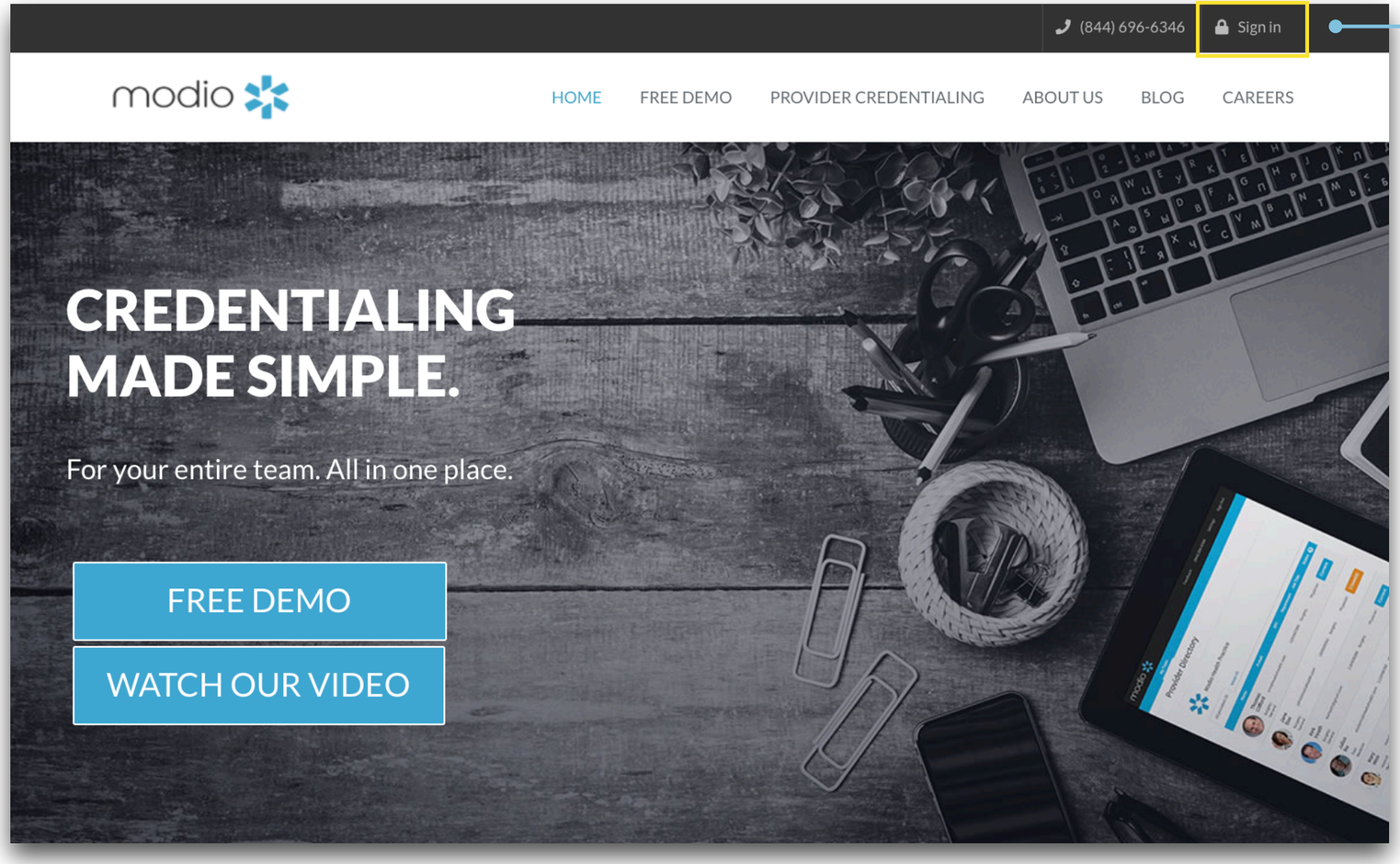
Overview

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.

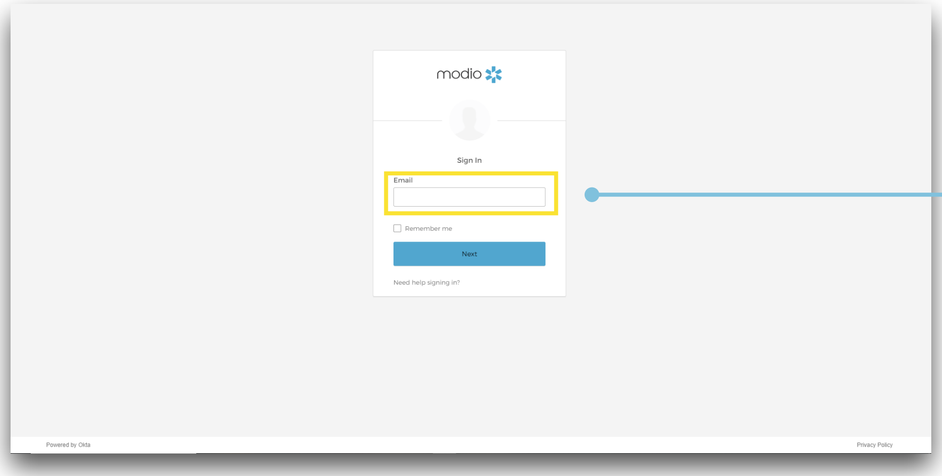
1



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

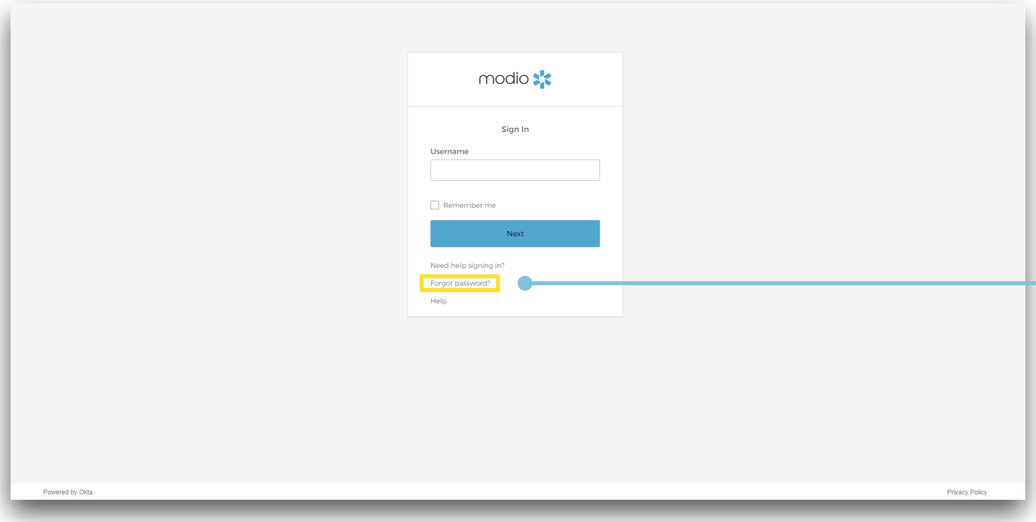
Enter your password:
Use your current OneView password. If that password does not meet the complexity requirements, you will be prompted to update it.

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

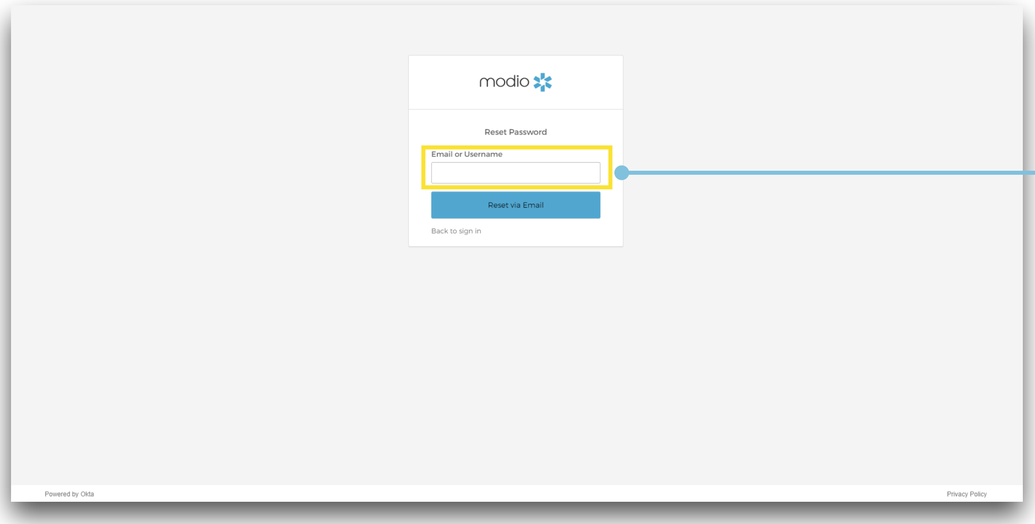
Save your password:
Select “Remember me” to save your credentials for next time.

1



Having trouble accessing your account?
Select “Need help signing in?” and click “Forgot password?”.

2



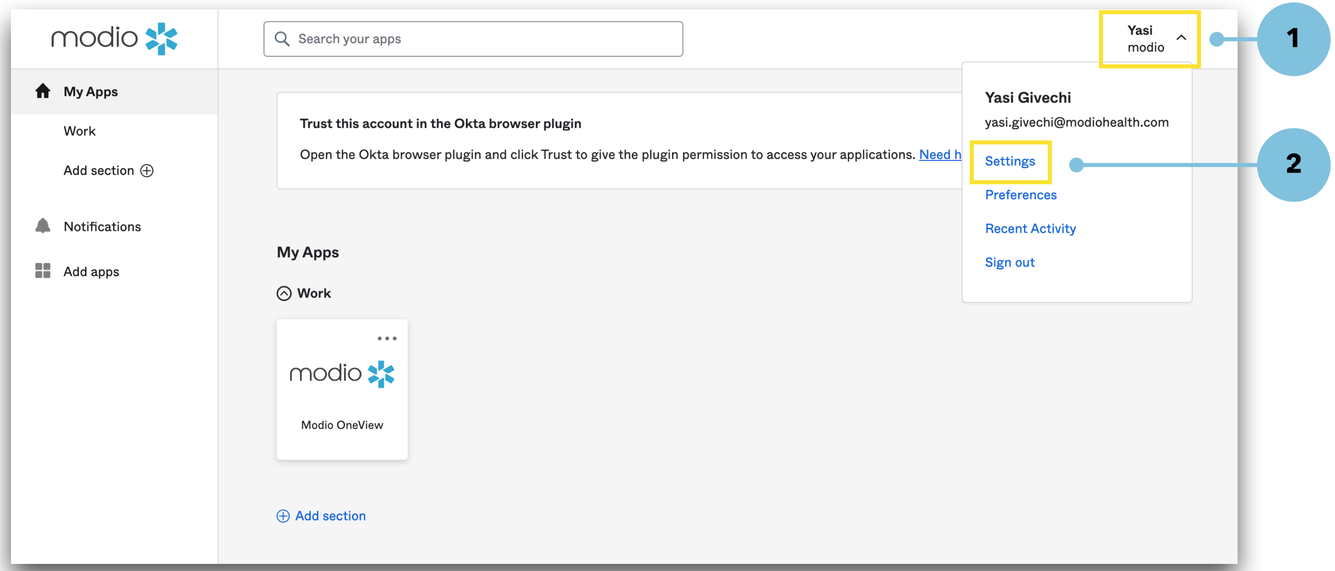
Reset your password: Enter your email address that you use to access OneView and choose to “Reset Via Email”.

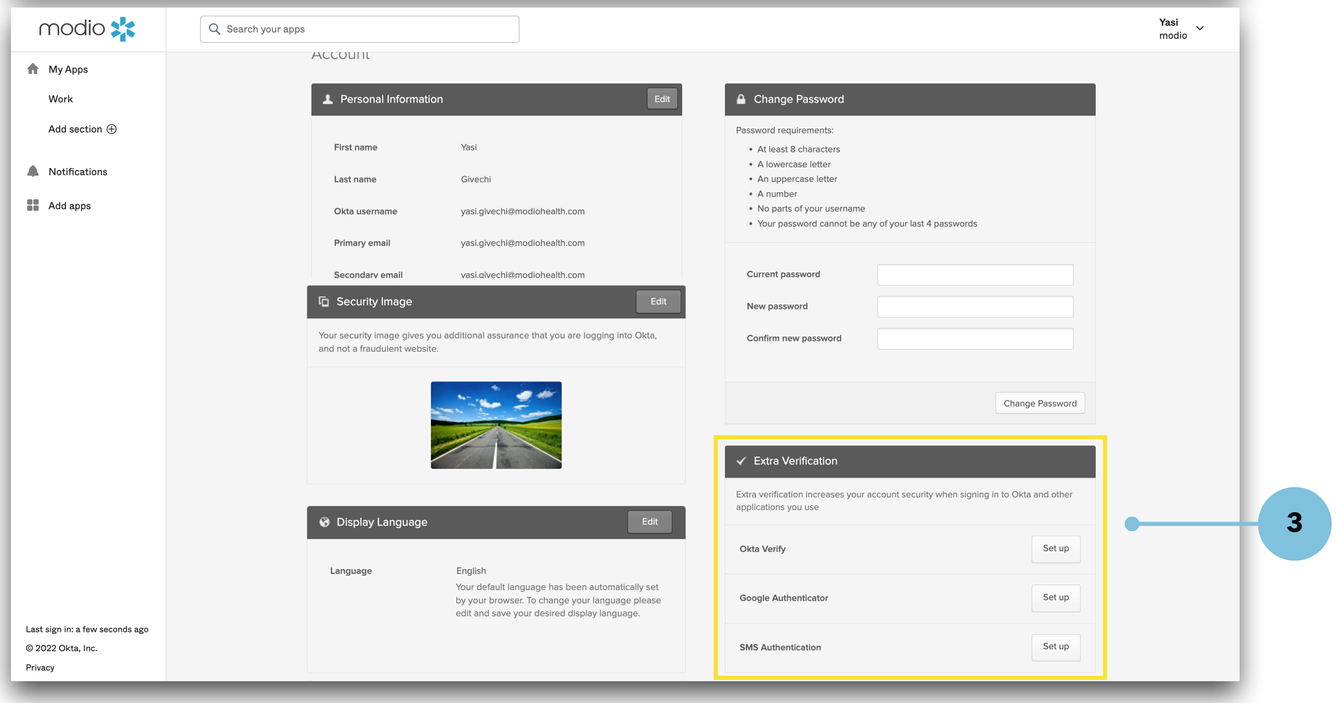
Access your email: Open the email from noreply@modiohealth.com and click the Reset Password link. This link expires within an hour.

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.





Starting Steps:

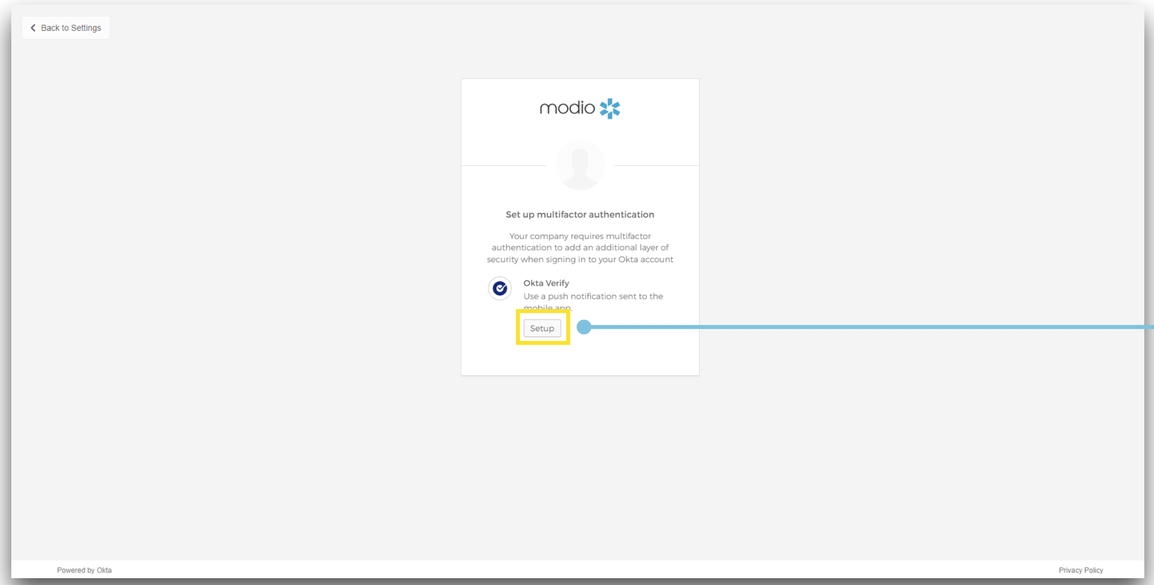
1. Visiting: **auth.modiohealth.com** and sign in.
2. Visit your personal settings. On your Okta dashboard, select your **name** in the upper righthand corner and then click **Settings**.

Access the Extra Verification section:

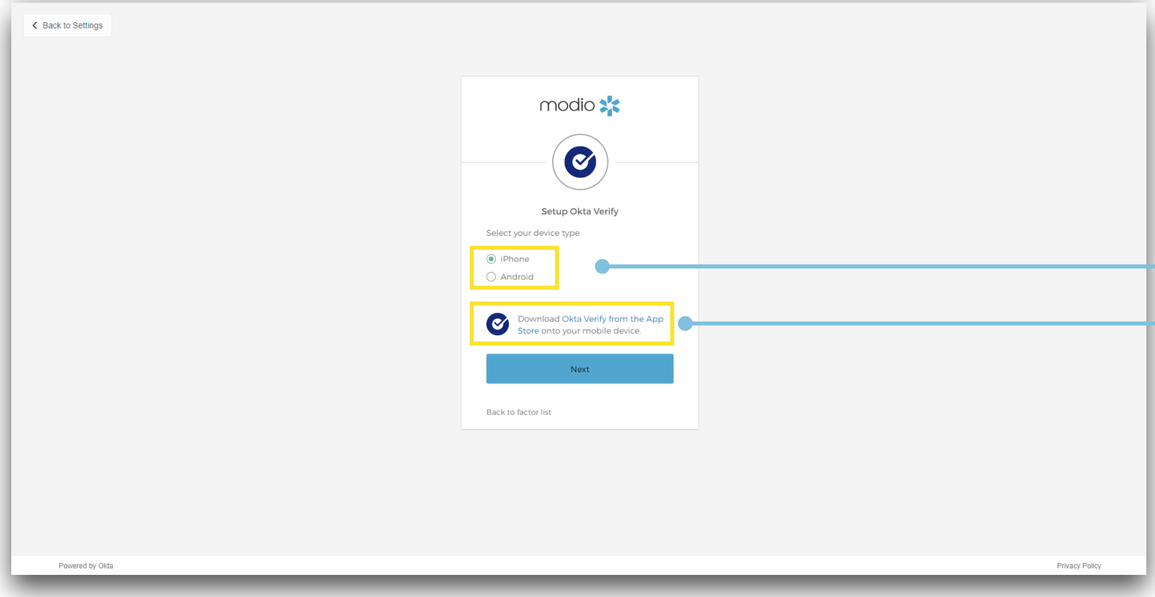
3. You have three options for MFA. We recommend setting up two methods for an extra layer of security.

- To set up Okta Verify, go to step 4 (page 7)
- For Google Authentication, go to step 5 (page 11)
- For SMS authentication, go to step 6 (page 15)

Okta Verify Setup



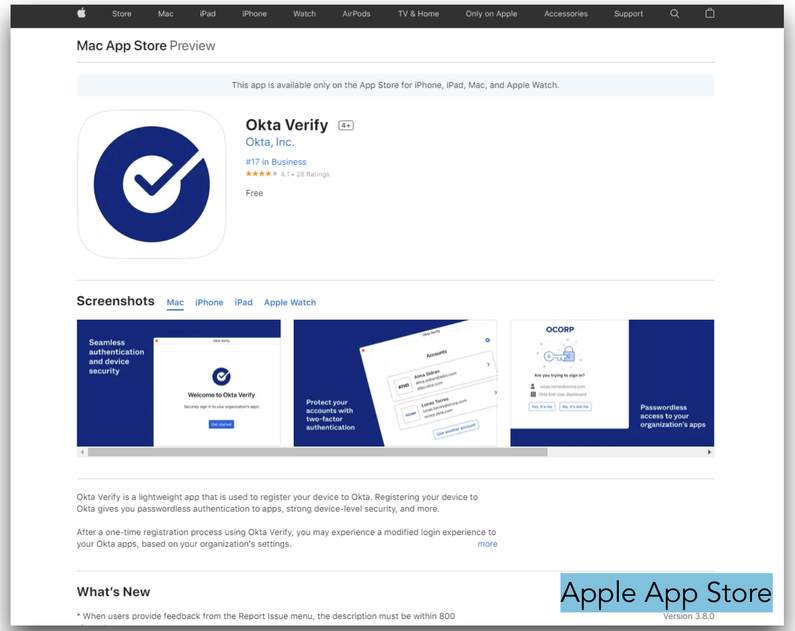
4. Set up Okta Verify: To use this, you will need access to a mobile device.

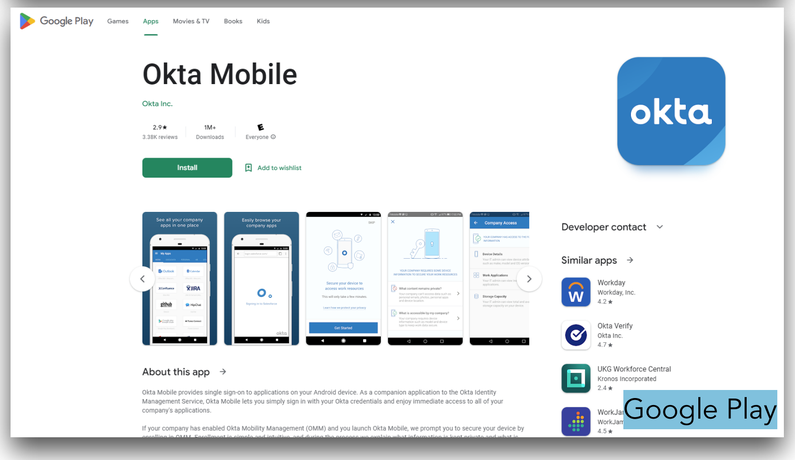


4a. Select device type. Indicate whether you will be using an iPhone or Android to access the Okta Verify app. Next, download **Okta Verify** from the app store.

(View on your computer browser)

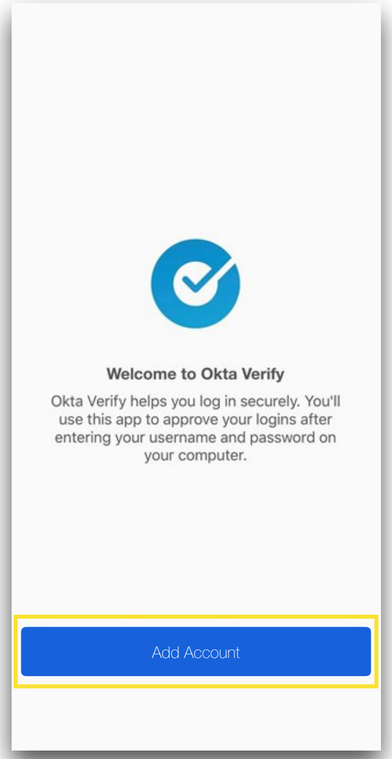
4b. Download **Okta Verify** from the app store.





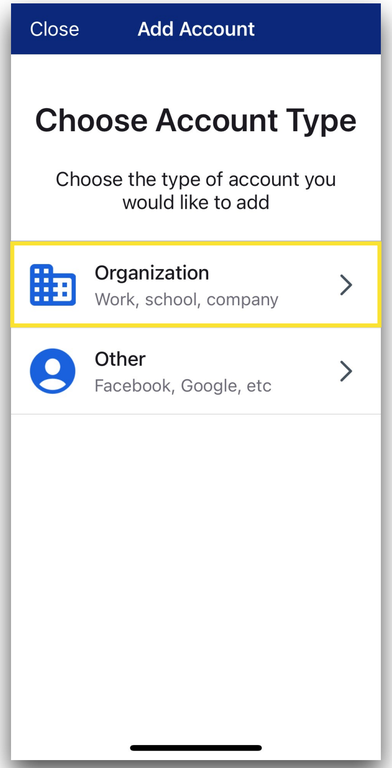
(View on your computer browser)

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



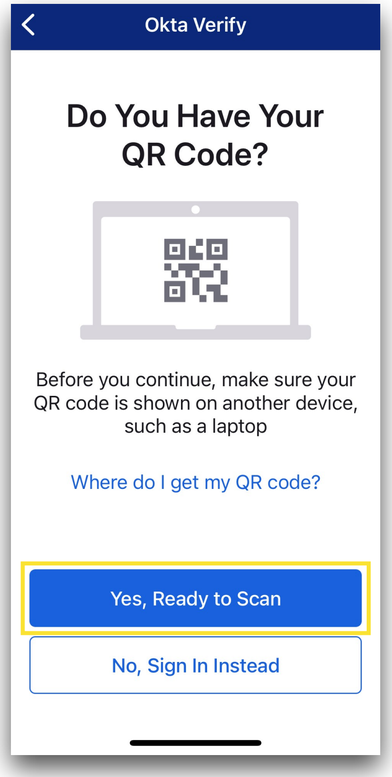
(View on your mobile device)

4d. Choose the **Organization** account type



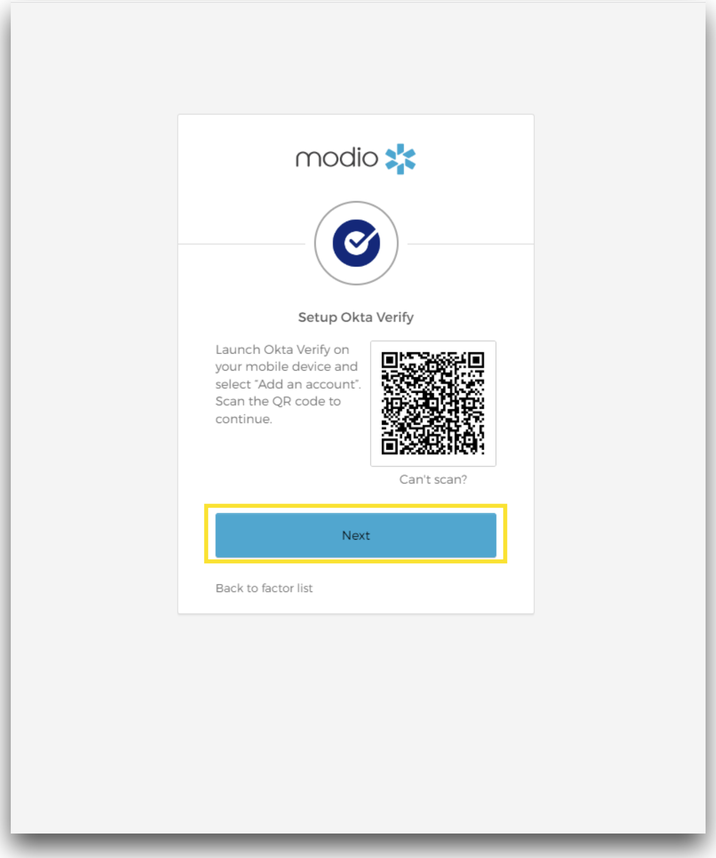
(View on your mobile device)

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

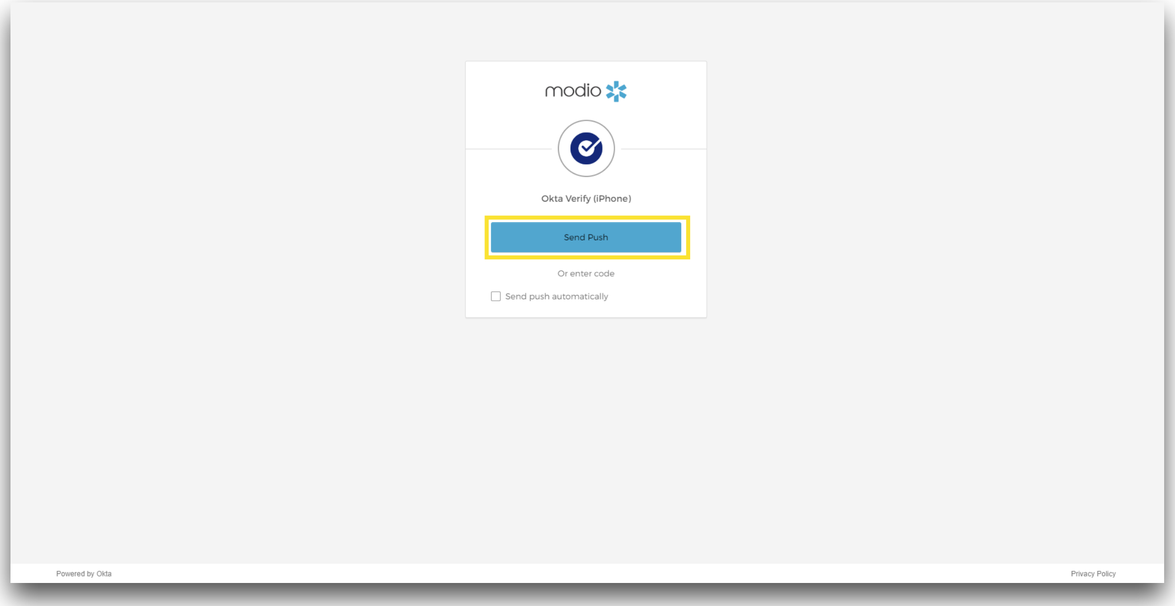


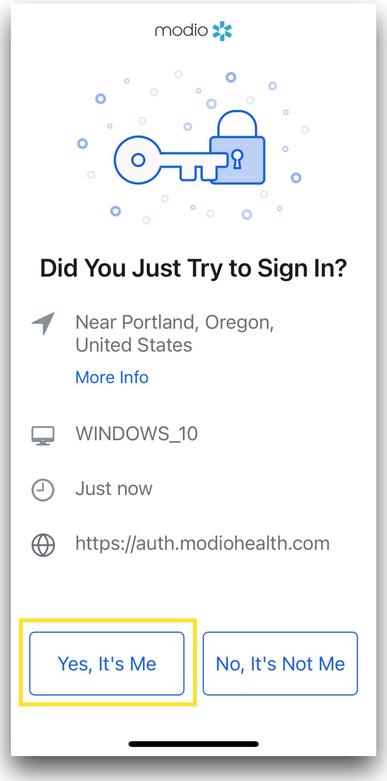
(View on your mobile device)

4f. You are now enrolled and can go back to your computer browser.

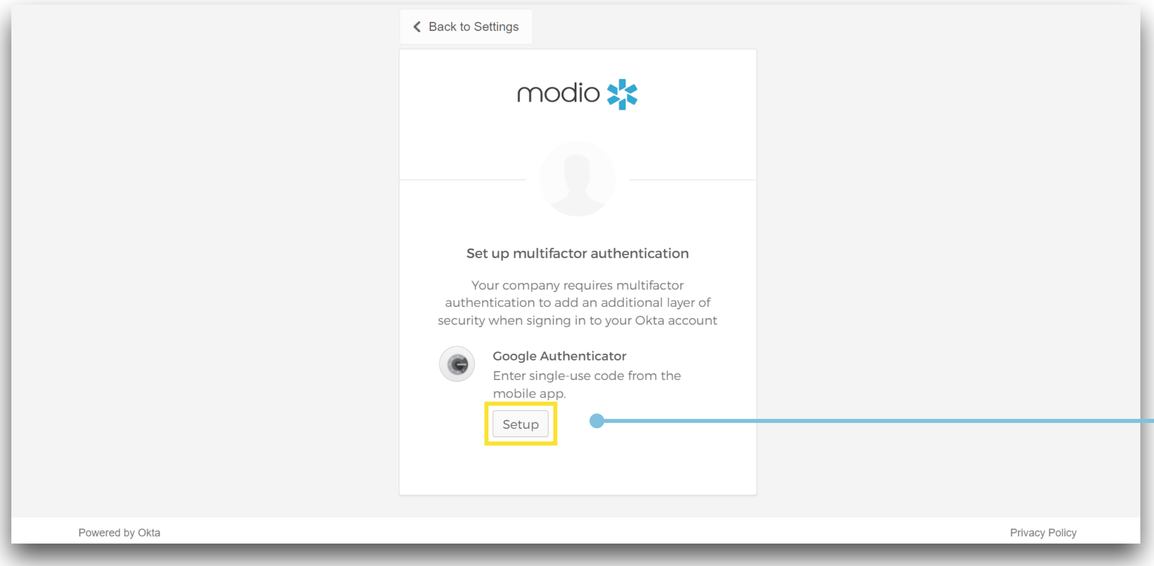


4e. If you are prompted for MFA, select **Send Push**.
Next, in your Okta Verify app, you can confirm that it is you trying to sign in by click **"Yes, its Me"**

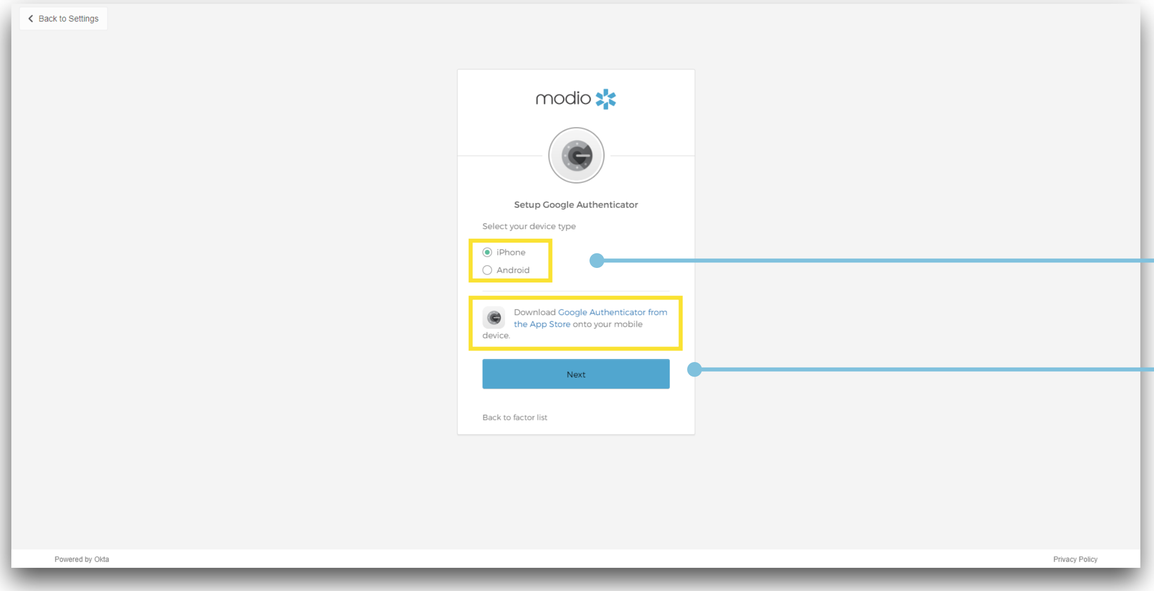




Google Authentication Setup



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

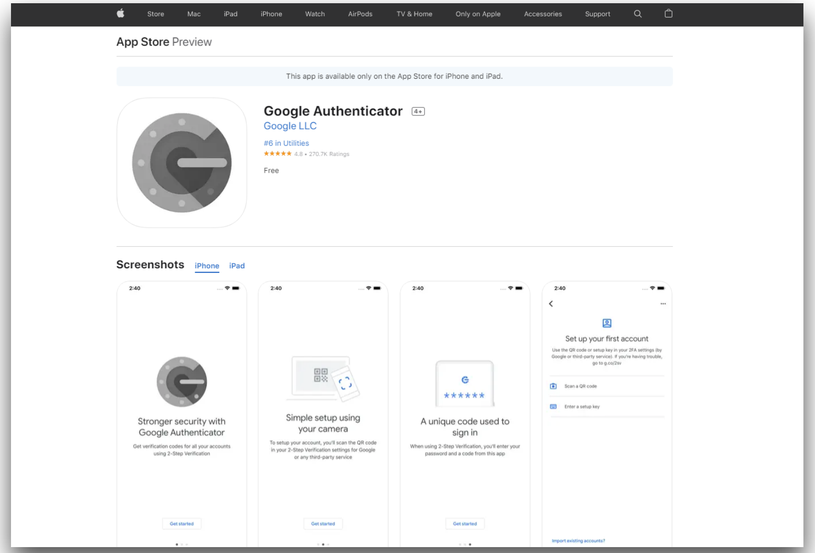


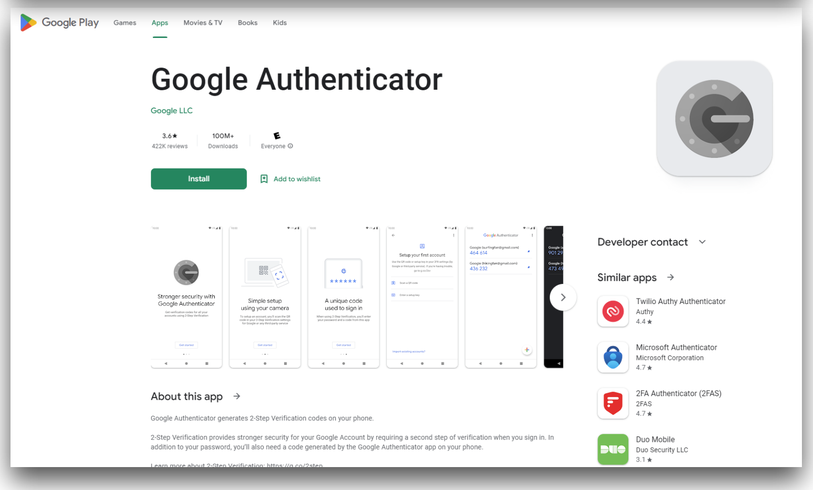
5a. Select device type. Indicate whether you will be using an iPhone or Android to access the Google Authentication app.

5b. Download **Google Authentication** from the app store on your **mobile device**.

(View on your computer browser)

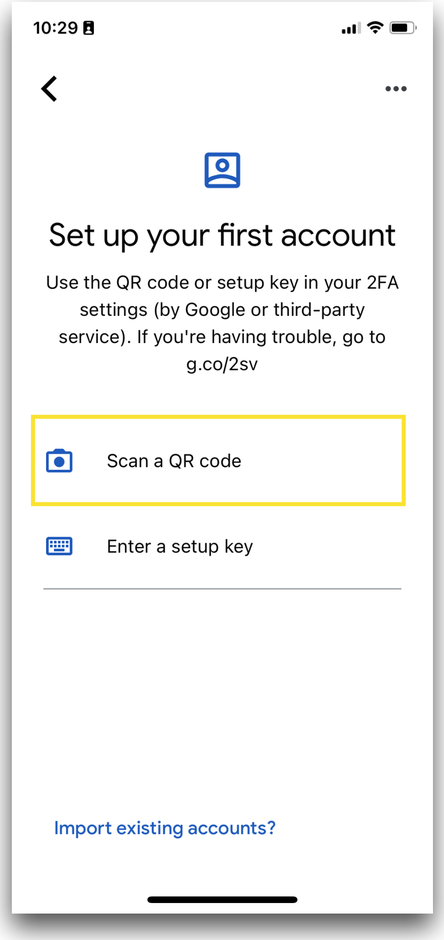
5c. Launch **Google Authenticator**.
Set up your first account or tap the + sign.



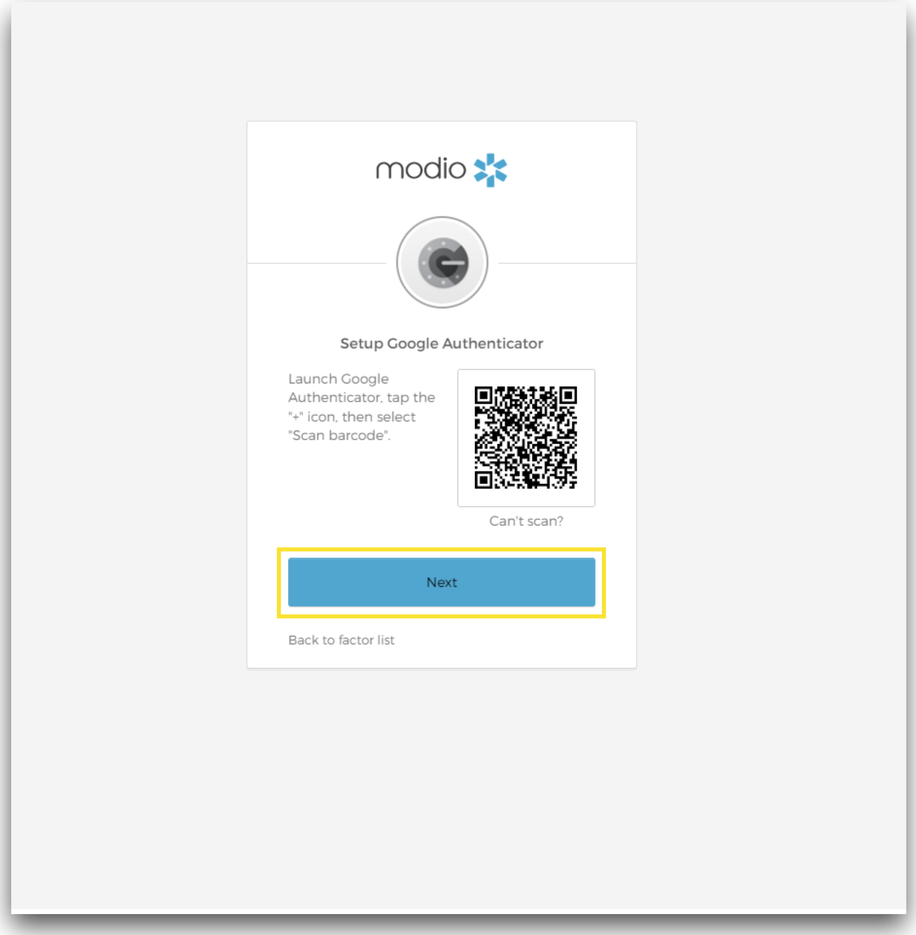


(View on your computer browser)

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)

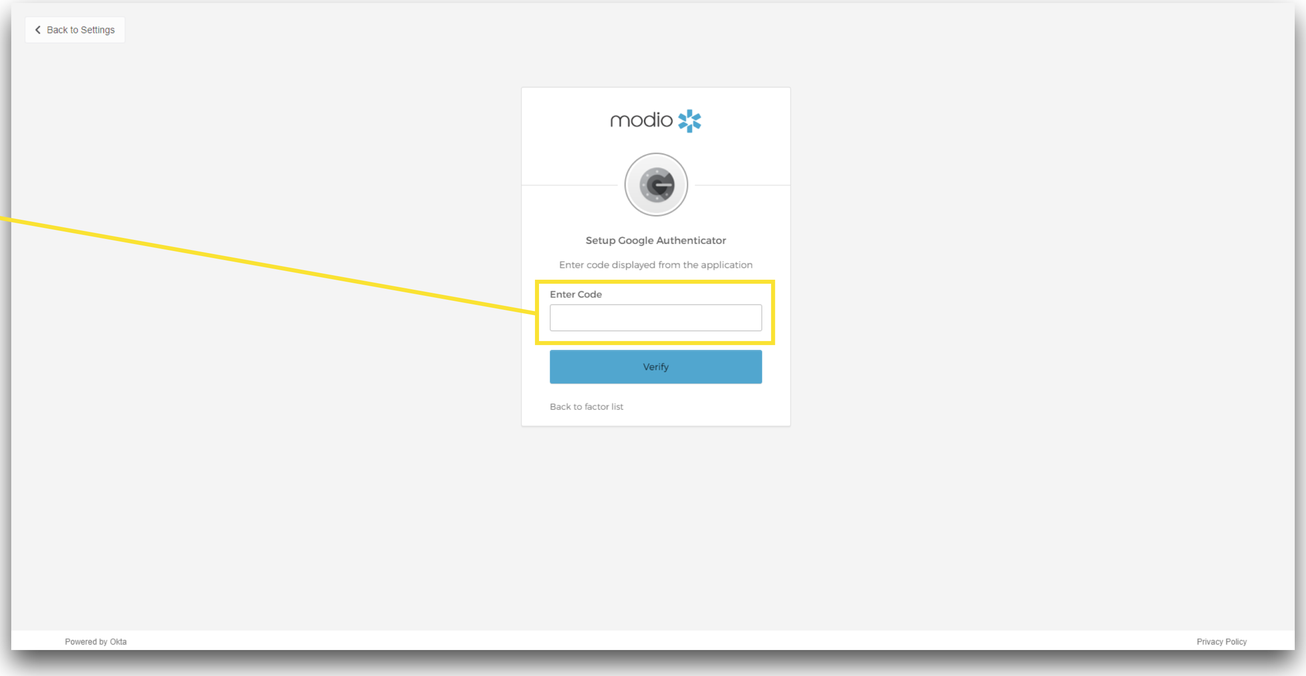


(View on your computer browser)

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.

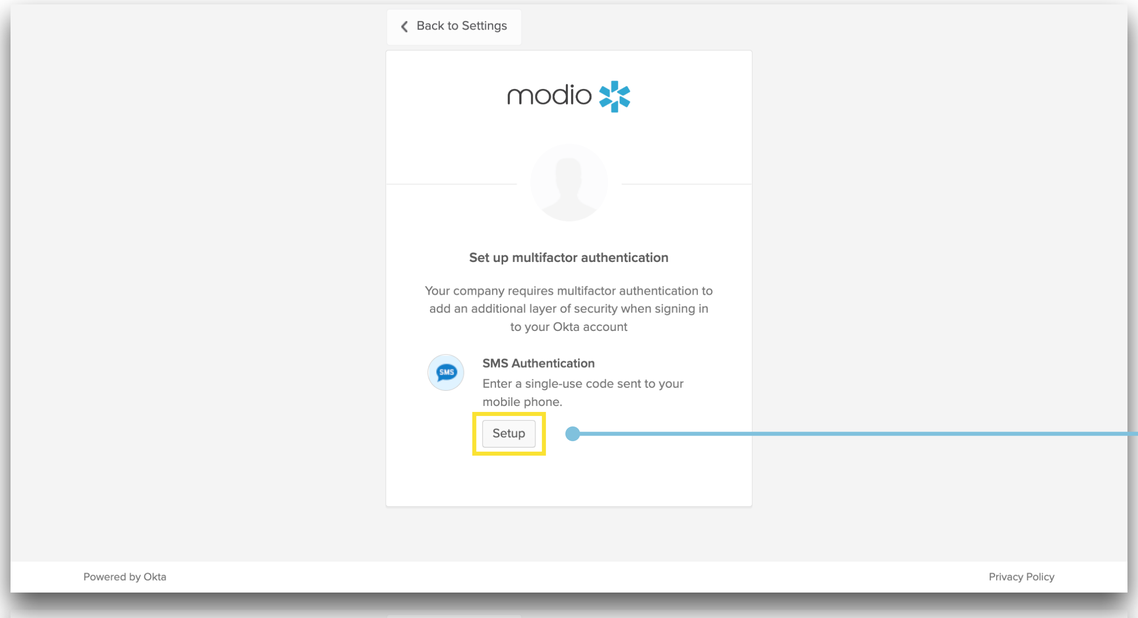


(View on your computer browser)

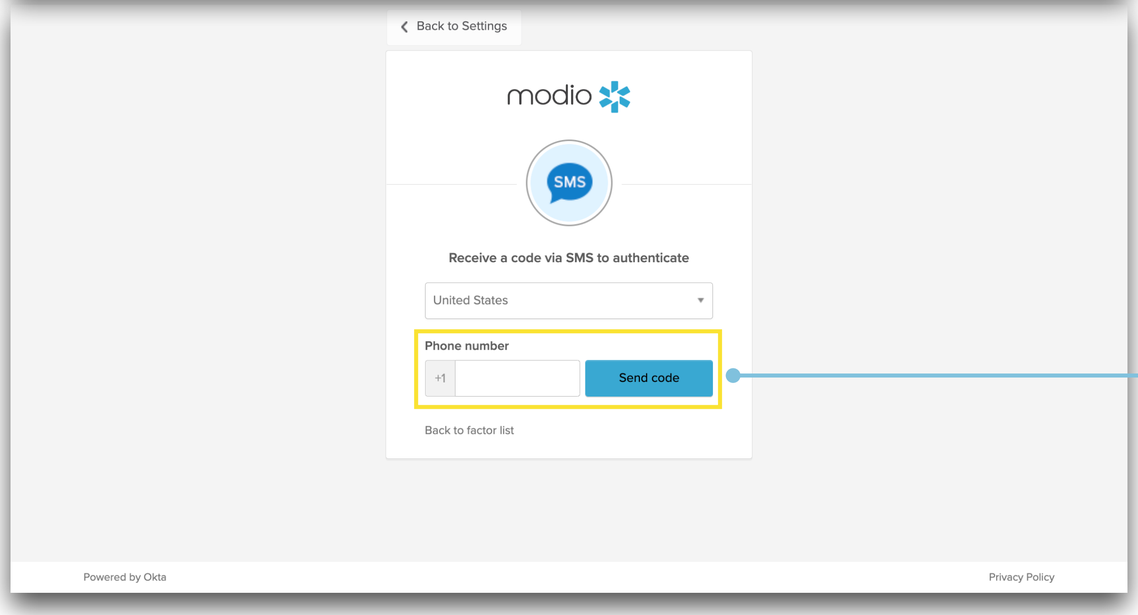
Tip Guide: Okta

modio

SMS Authentication Setup

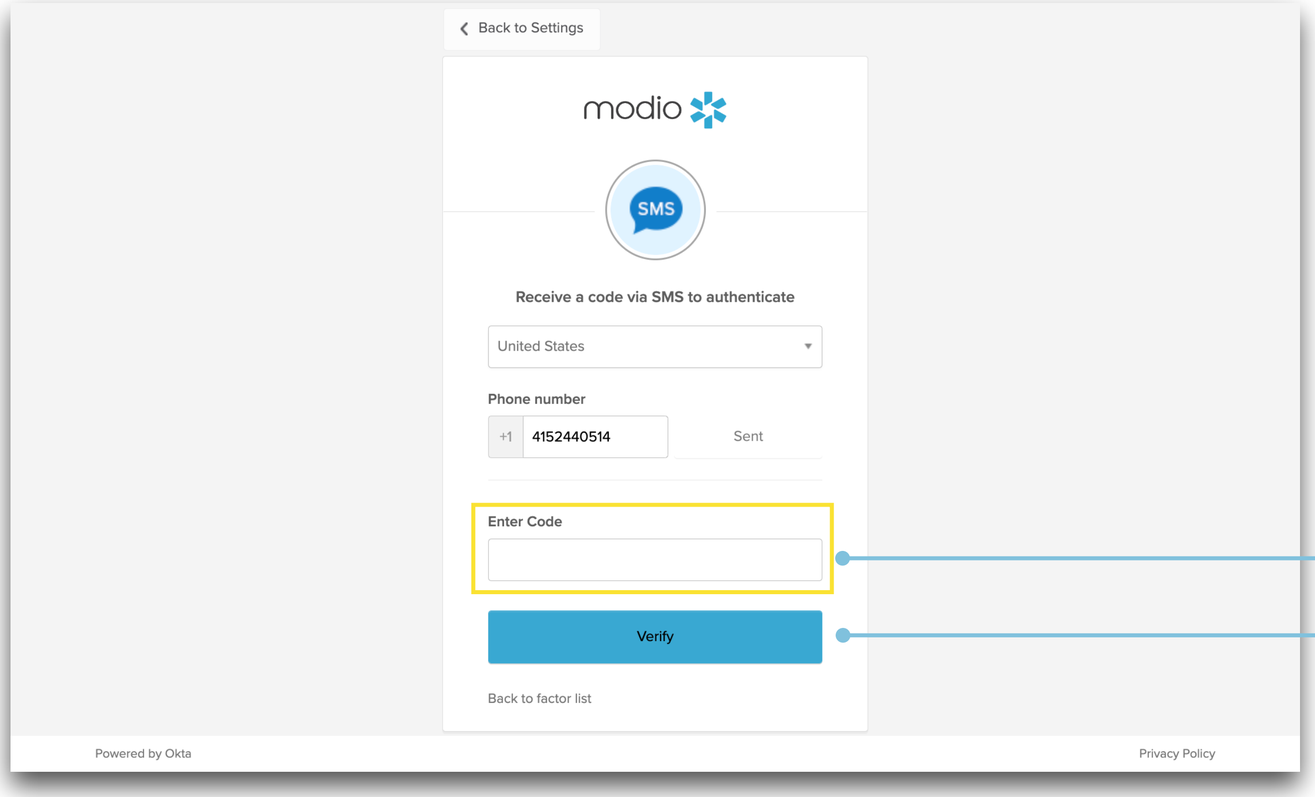


6. **Set up SMS Authentication**. You will need to enter a single-use code sent to your mobile phone. Start by clicking **Setup**.



6a. Enter your mobile phone number. Once you send the code, you will receive a text message in your mobile device with a code that you will use to verify and enroll.

(View on your computer browser)



(View on your computer browser)

6b. Once you receive the code, enter the code and complete this step by clicking **Verify**.

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. 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, the hackers will have a harder time breaking into our systems as they may not have both your password and your phone.

When you log in to an account or application, you're asked for a password so you can prove you are who you say you are. You may then be asked for a second factor.

Q: What is the benefit of using MFA?

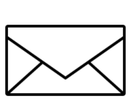
A: MFA is an effective way to provide enhanced security. Traditional usernames and passwords can be stolen, and they've become increasingly more vulnerable to malicious activity, and cyber-attacks like phishing or brute force attacks. MFA creates multiple layers of security to help increase the confidence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

Q:How can I start using Multi-Factor Authentication (MFA) for my employees?

A: Employees will need to individually turn on MFA through their Okta dashboard. Use the steps described on pages 7-17 to enable authentication through Okta Verify, Google Authentication, or SMS. This will trigger MFA as an additional step in the sign-in process if suspicious behavior occurs, like signing in from a new device or location. We recommend enrolling two methods, in case you lose access to the app and/or SMS ability.

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

Online:
Live Chat Support



Email:
support@modiohealth.com

Phone:
844.696.6346