

OKTA Enrollment Guides

Русский

Français

Deutsch

Dutch

Português

Arabic

Español

Polska

中文

Japanese

Korean

Thai

Which verification method do I setup?

Register as many verification methods as possible. Every time Okta prompts you to verify your system log in you will be able to choose any registered verification method.

You can register for a method even if you are not able to use it every time you log in.

 *Security protection level

If you have a smart phone begin the enrollment process here:

 **Okta Verify App. Recommended for smartphone users**



Qualifications:

- Associate has access to a smart phone or mobile device

*This mobile app can be installed from your device's app store ("App store" on iPhone and iPad and "Google Play Store" on Android). It allows you to approve a request to log in via device notification from Okta or by typing a numeric code when prompted.

If you have a phone begin the enrollment process here:

 **Okta SMS Authentication. For any type of mobile**



Qualifications:

- Associate is able to receive an SMS message

*This option allows Associates to receive an SMS message containing a numeric code to verify a log in.

 **Voice Call Authentication. For any type of phone**



Qualifications:

- Associate has access to a telephone

*This option initiates a phone call to the Associate-given phone number providing the Associate with a numeric PIN code to verify.

If you do not have access to a phone, begin the enrollment process here:

 **Security Question. For non-smartphone users only**



Qualifications:

- Associate lacks a smartphone or other mobile device while at place of work

*Please note that this is the weakest security verification and should only be used if no other method is available to you.

 **Security Key or built-in biometric authenticator**



Qualifications:

- Associate has a biometric device such as TouchID on Mac books, or a USB token such as a Yubikey

*This option offers highest security and allows biometrics and USB tokens to prove identity during login. **Windows Hello and USB Security Keys are NOT currently available.** This feature will launch globally at a later date.

Authenticating To Okta Using Okta Verify

Log into Okta

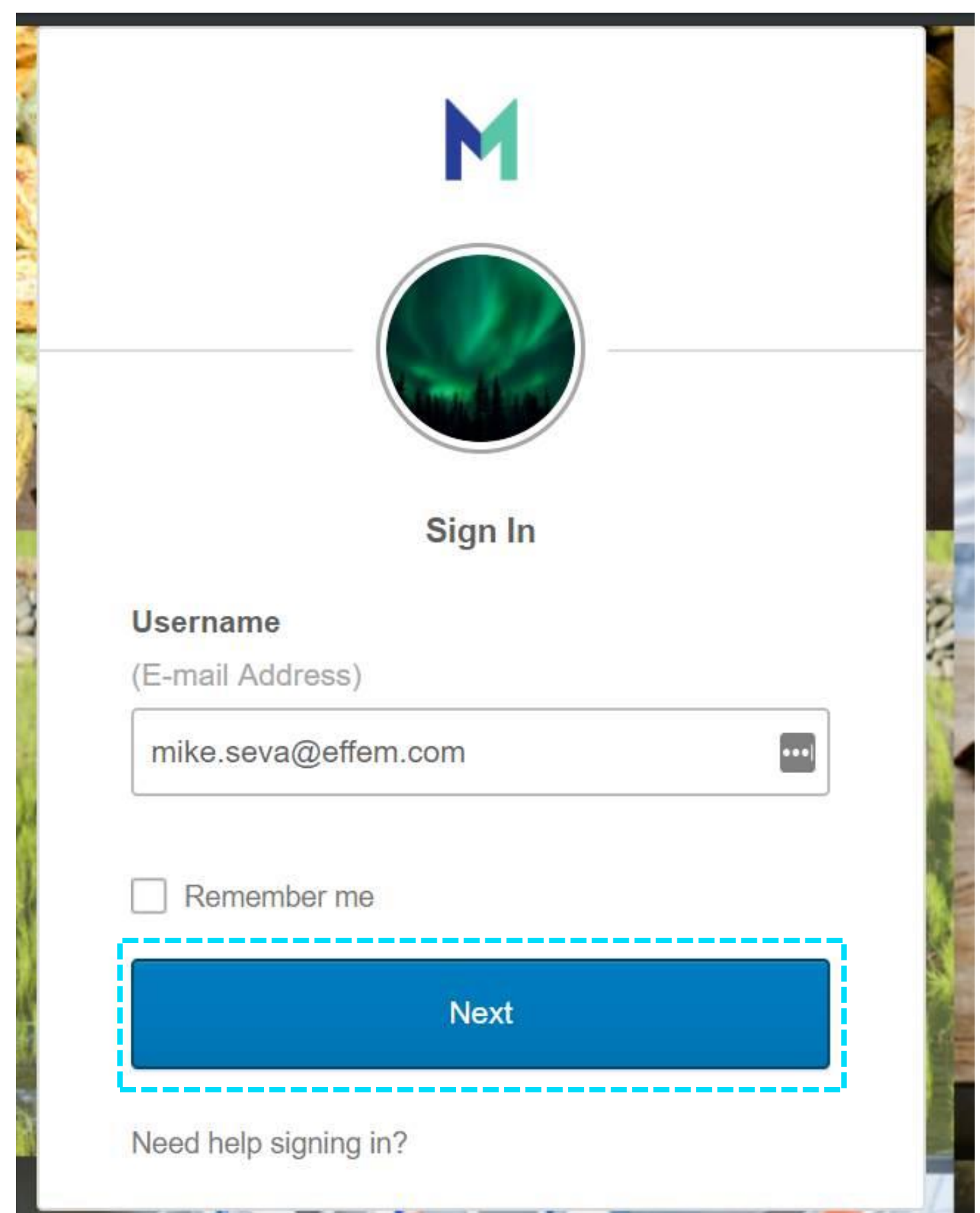
1 Open a web browser on your **PC/laptop** and make sure you have your mobile device (Personal or Corporate) ready to use.

If you do not have a mobile device available, please [setup Security questions by clicking here](#)

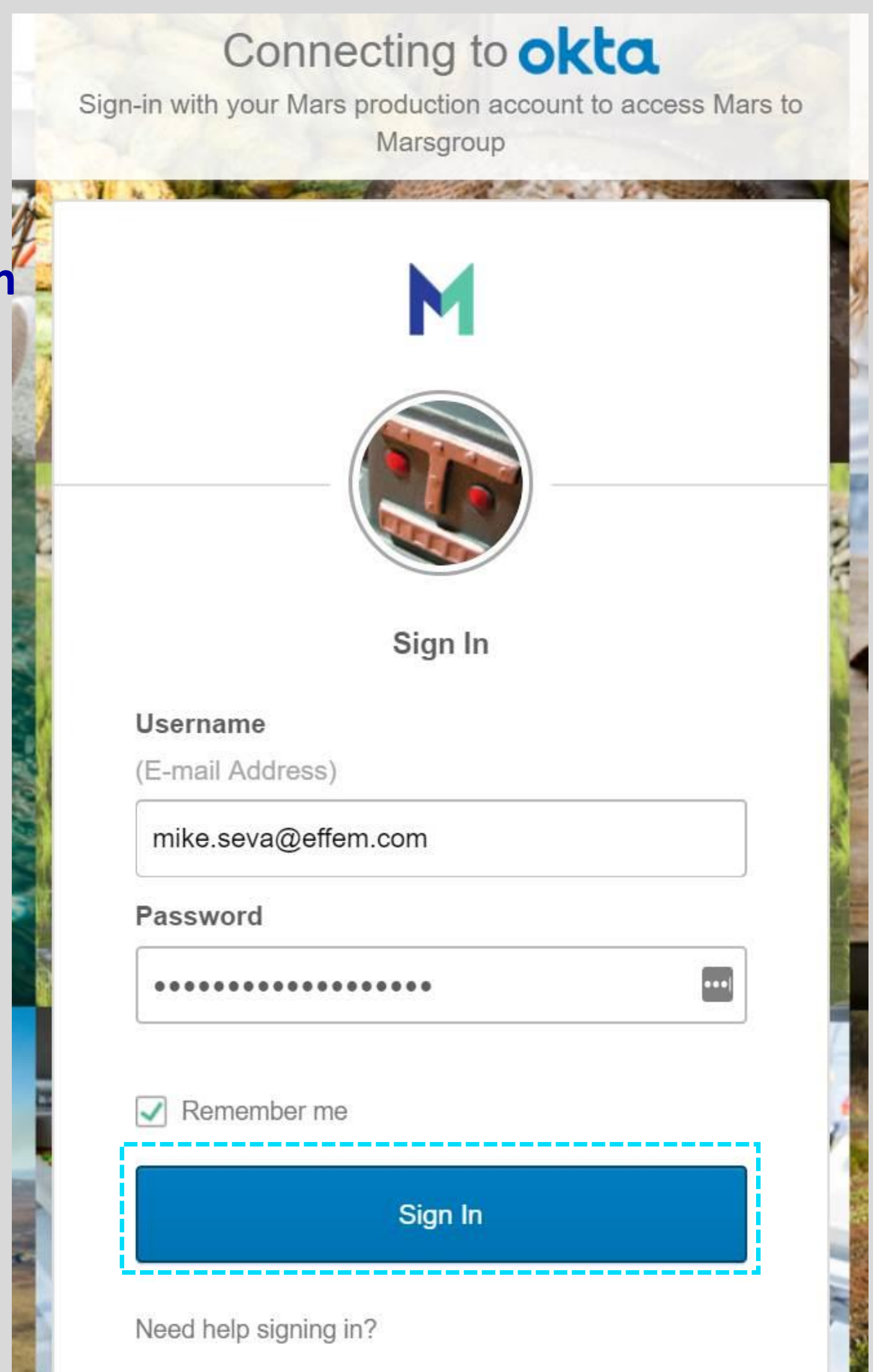
2 In your PC/laptop browser, type **Mars-Group.Okta.com** in the address bar.

**If you access a Mars application that requires you to authenticate with OKTA, you will be prompted to log-in (see image) and follow the steps below.*

3 On your PC/laptop, type your corporate **email address** and click **Next**.



4 **If working remotely** you will be prompted to type your corporate email and password and click **Sign In**.





Set up multifactor authentication

Your company requires multifactor authentication to add an additional layer of security when signing in to your Okta account



Okta Verify

Use a push notification sent to the mobile app.

Setup

5

Choose the **Setup** option next to the Okta Verify icon.

6

On your PC/laptop, choose the mobile device type you will install Okta Verify on

On the **Setup Okta Verify** screen on your PC/Laptop, click the icon associated with your mobile device (iPhone, Android, Windows phone)



Setup Okta Verify

Select your device type



Install Okta Verify



Download Okta Verify from the App Store onto your mobile device.

Next

Back to factor list

7

Click **Next**.

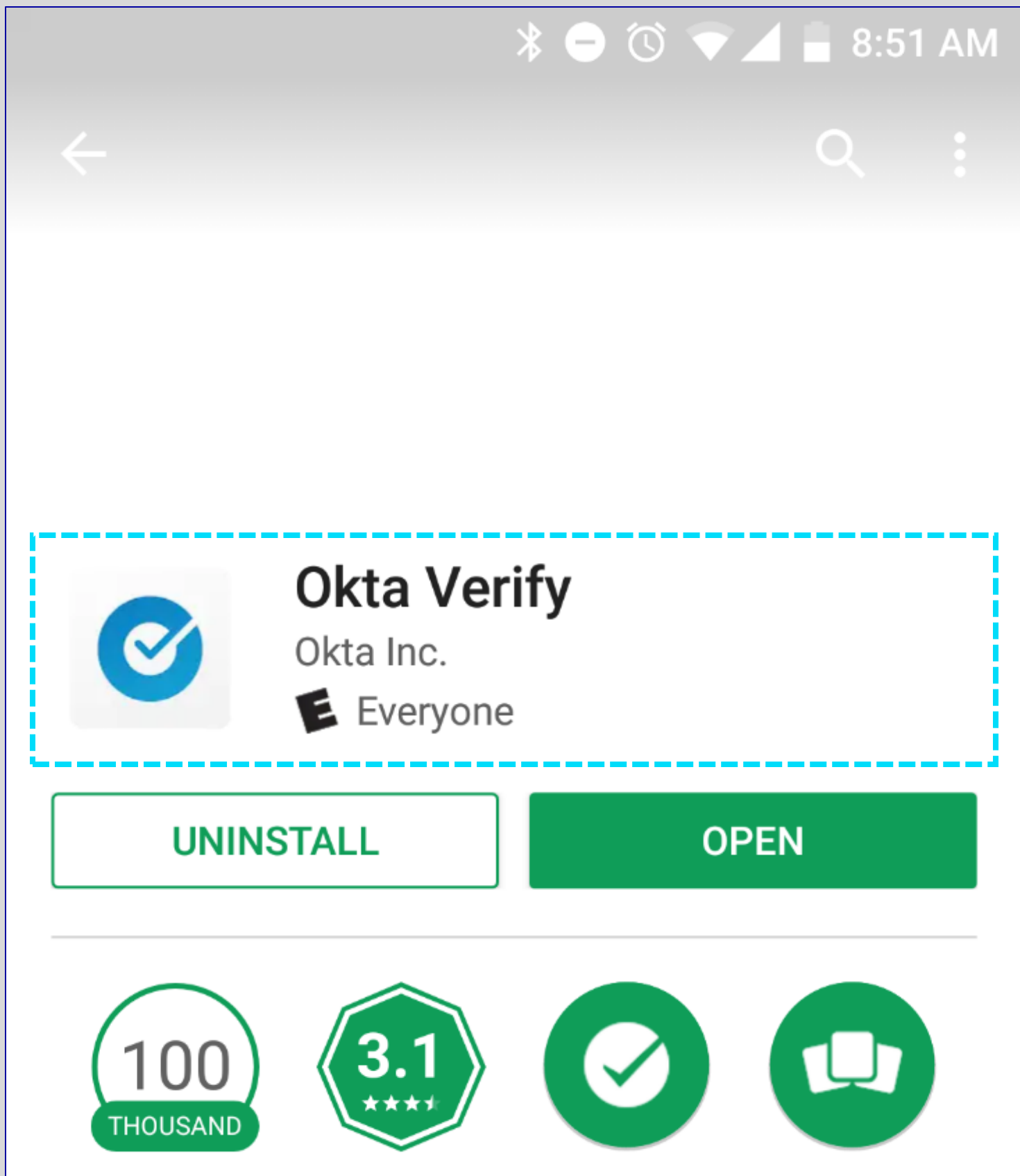
8

On your mobile device, open the App store.

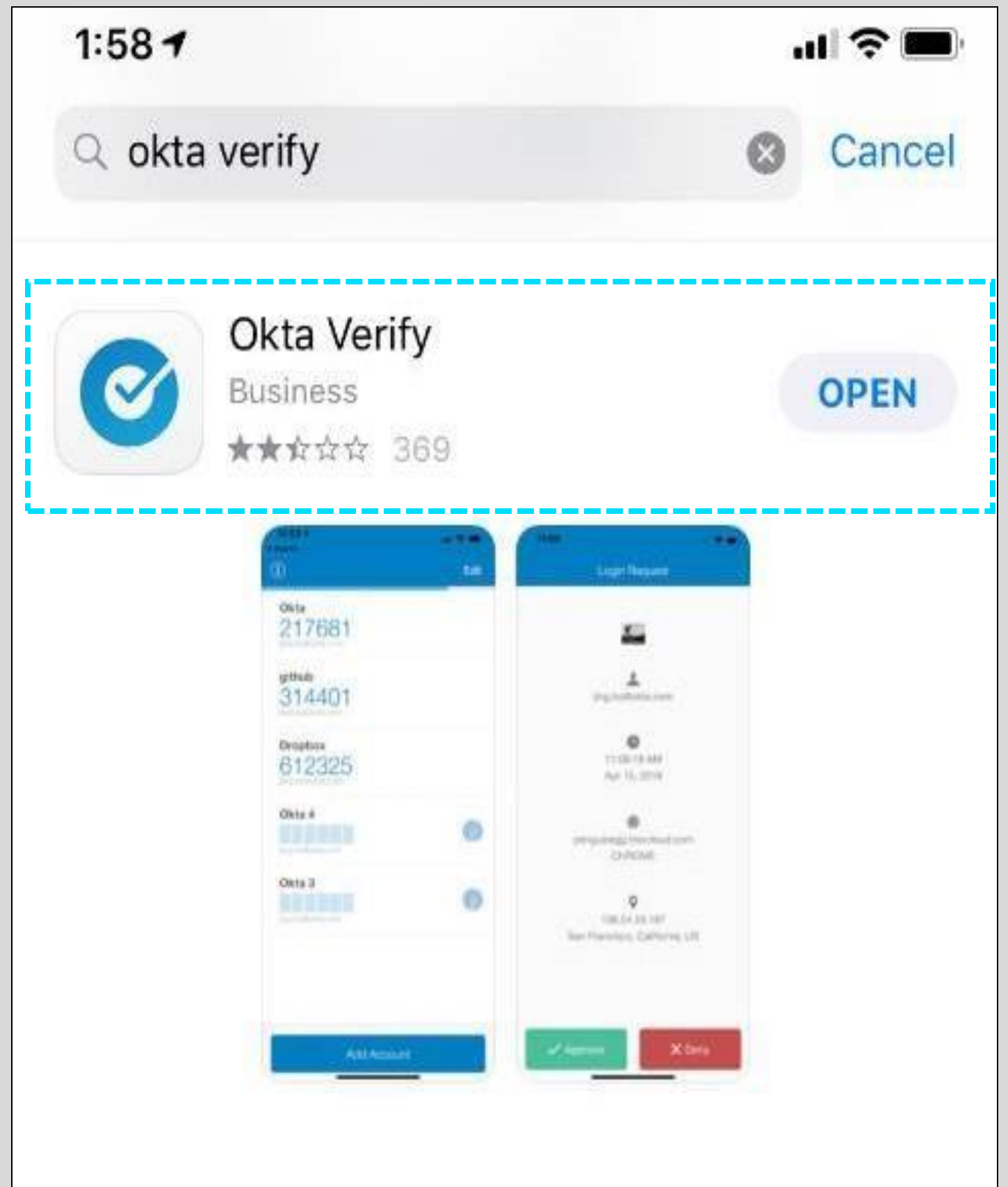
Mars Corporate devices will have the app pushed down automatically, or use the Intune Company Portal

- On an iPhone open the App Store.
- On an Android device open the Google Play Store

9 Search for **Okta Verify** in AppStore or Play Market and install it



i Okta Verify on Android



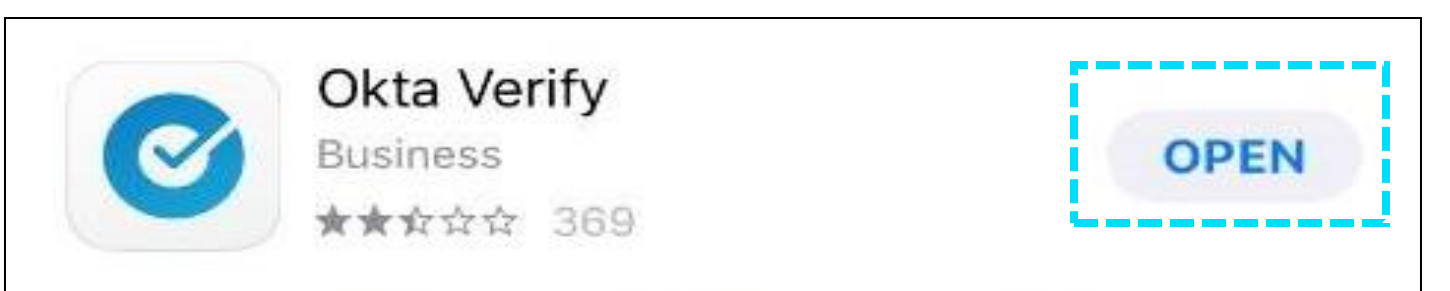
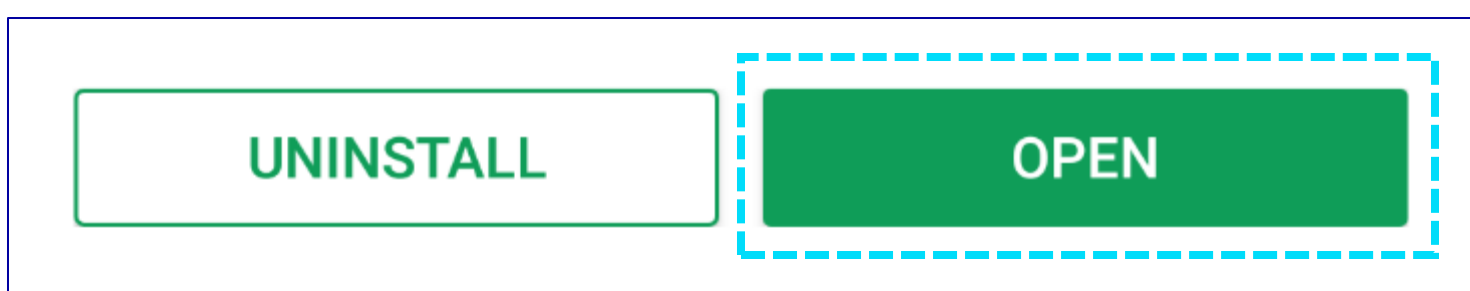
i Okta Verify on iOS

10 Open the **Okta Verify** on your mobile device

When you launch Okta Verify, make sure that “Notifications” are authorized for this app.

On an iPhone, you will be prompted to allow Notifications

On Android devices: Notifications-> Okta Verify-> enable notifications

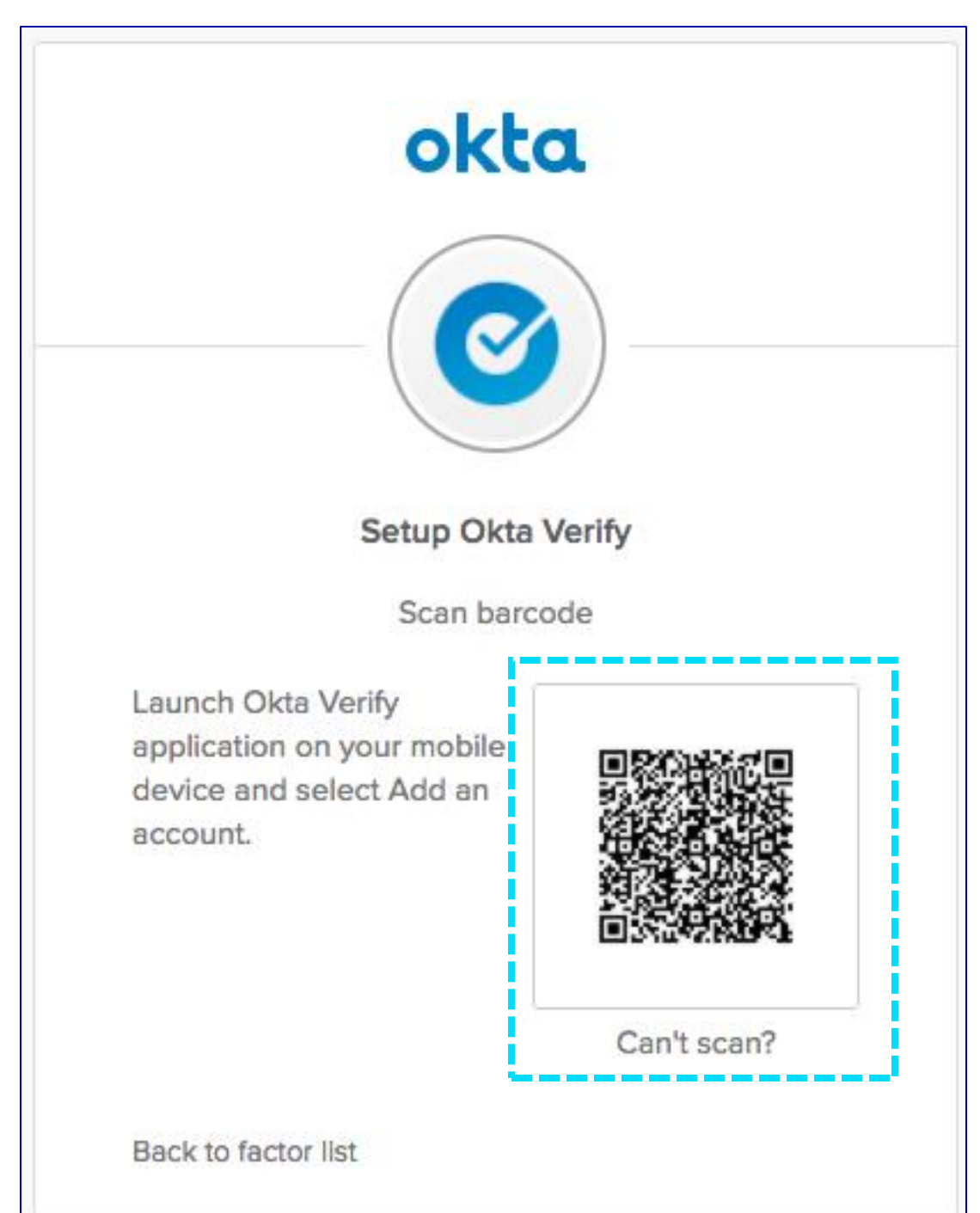
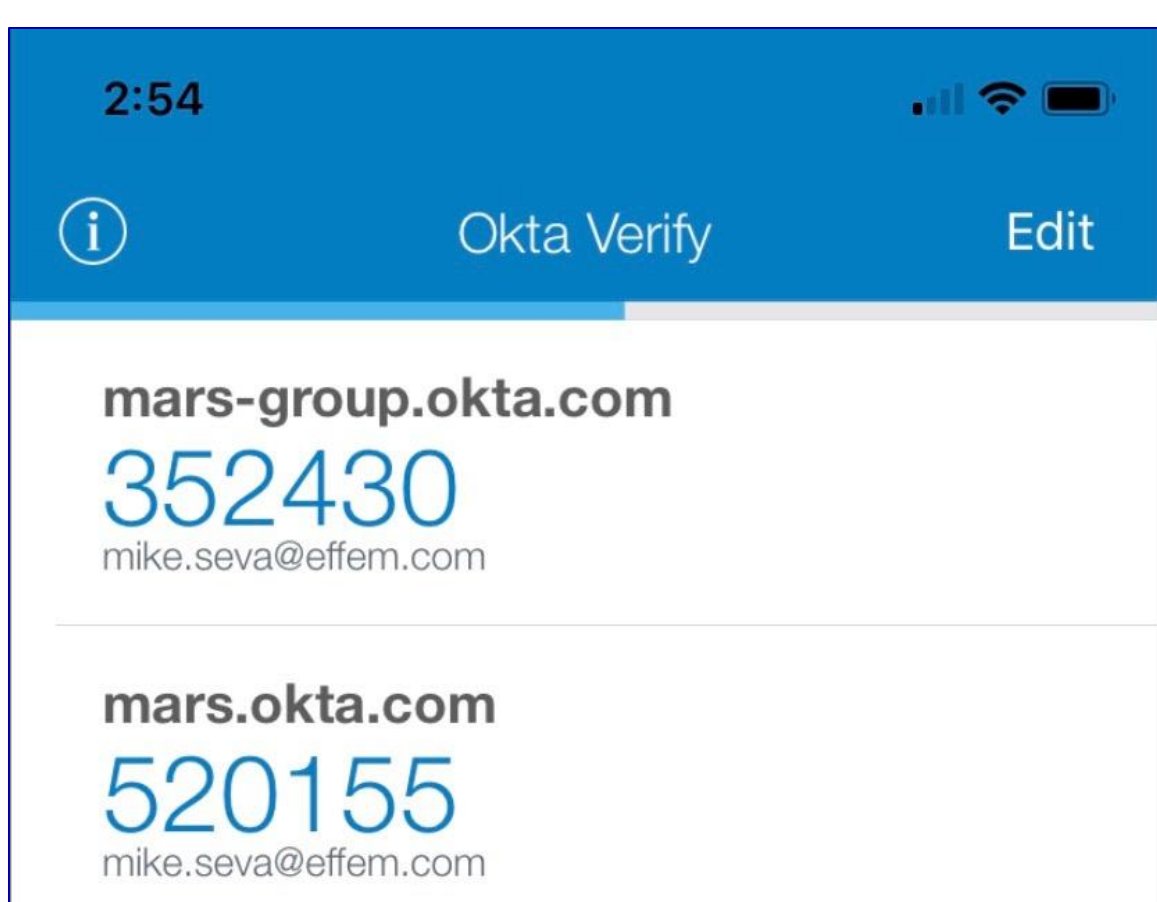


11 On the **Welcome to Okta Verify** screen, tap **Add Account**.

12 Your PC/Laptop screen will **display a QR code** from Step 7.

Scan the QR code on the screen using your mobile device.

*Associates must scan the QR code in Okta Verify. Once completed, they will see the below image of their account and OTP.



13 Click **Finish**.

Complete the Okta Log In

14 On your PC/laptop, you will be prompted to update your profile. Please select **two options** to complete your enrollment. After you have updated your profile, you will receive a call or text confirming **you have successfully enrolled in Okta**.

If you have pre-enrolled you will not see any applications in Okta until after the go-live date.

Please update your profile

+ Add Phone Number

+ Add Phone Number

Remind me later

15

After first log-in following successful enrollment, the tool will prompt you to push a log-in confirmation to your mobile device.

MARS

Okta Verify (Michael's iPhone)

Send Push

Or enter code

Send push automatically

16

Check **Send Push Automatically** and **Do Not Challenge Me On This Device**.

MARS

Okta Verify (Michael's iPhone)

Send Push

Or enter code

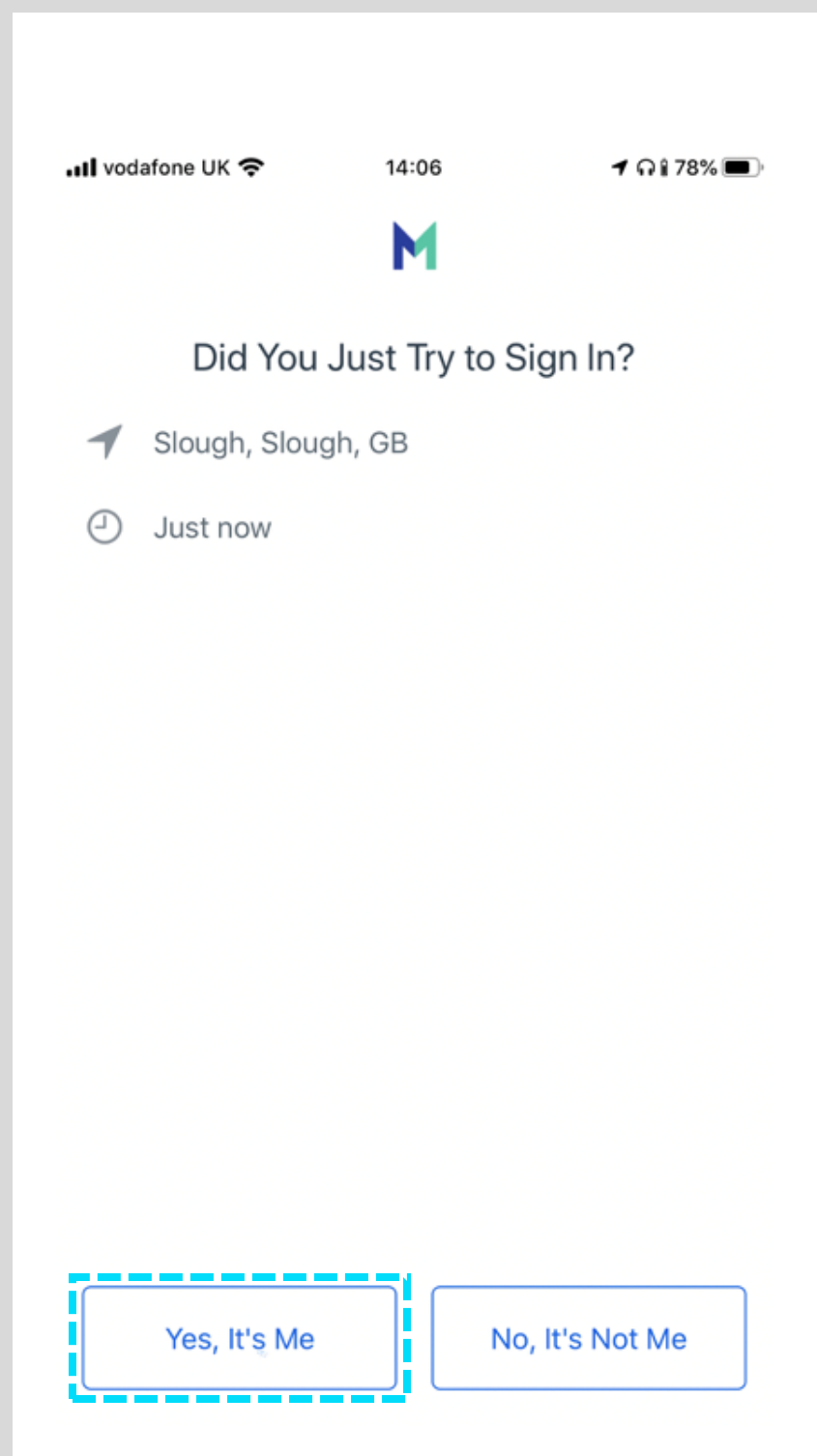
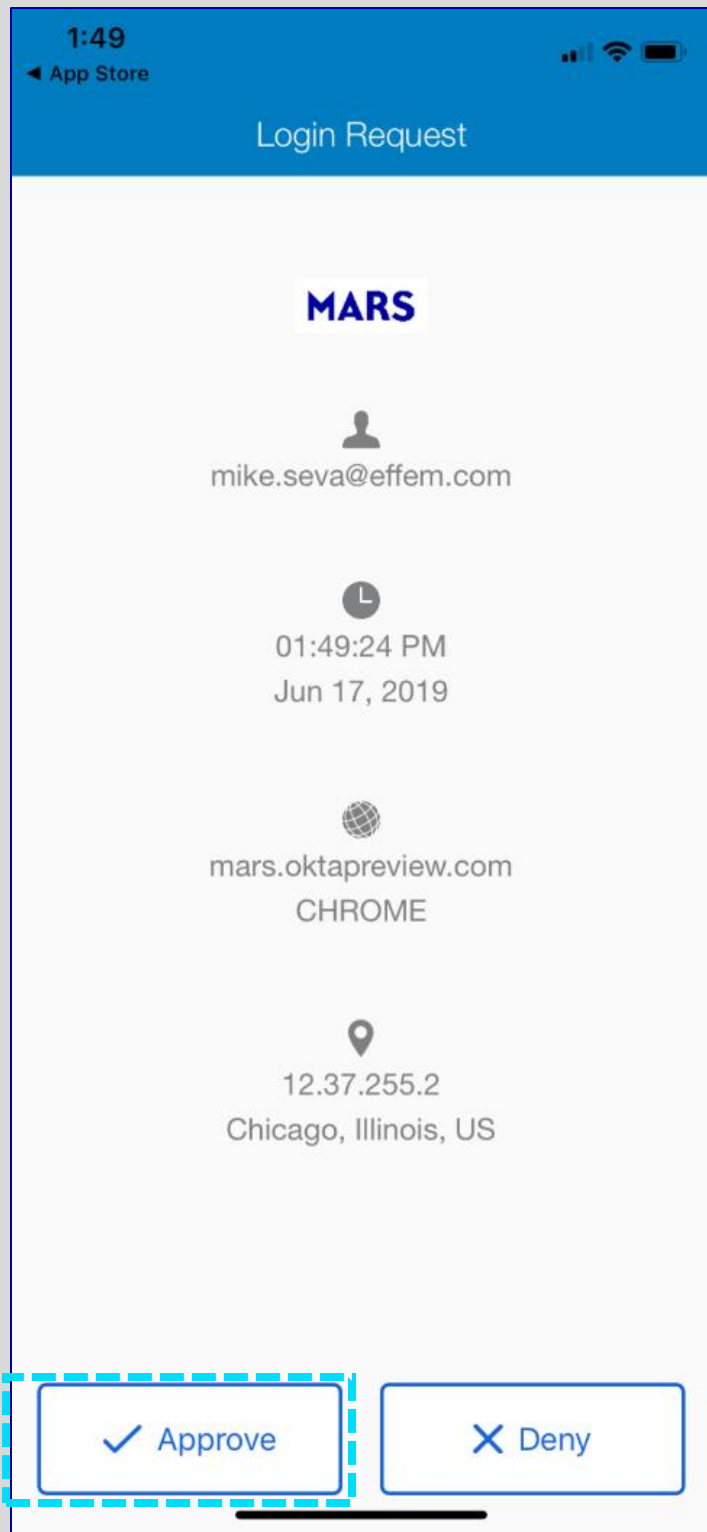
Send push automatically

Do not challenge me on this device for the next 15 minutes

Sign Out

17

Click **Send Push**.



18

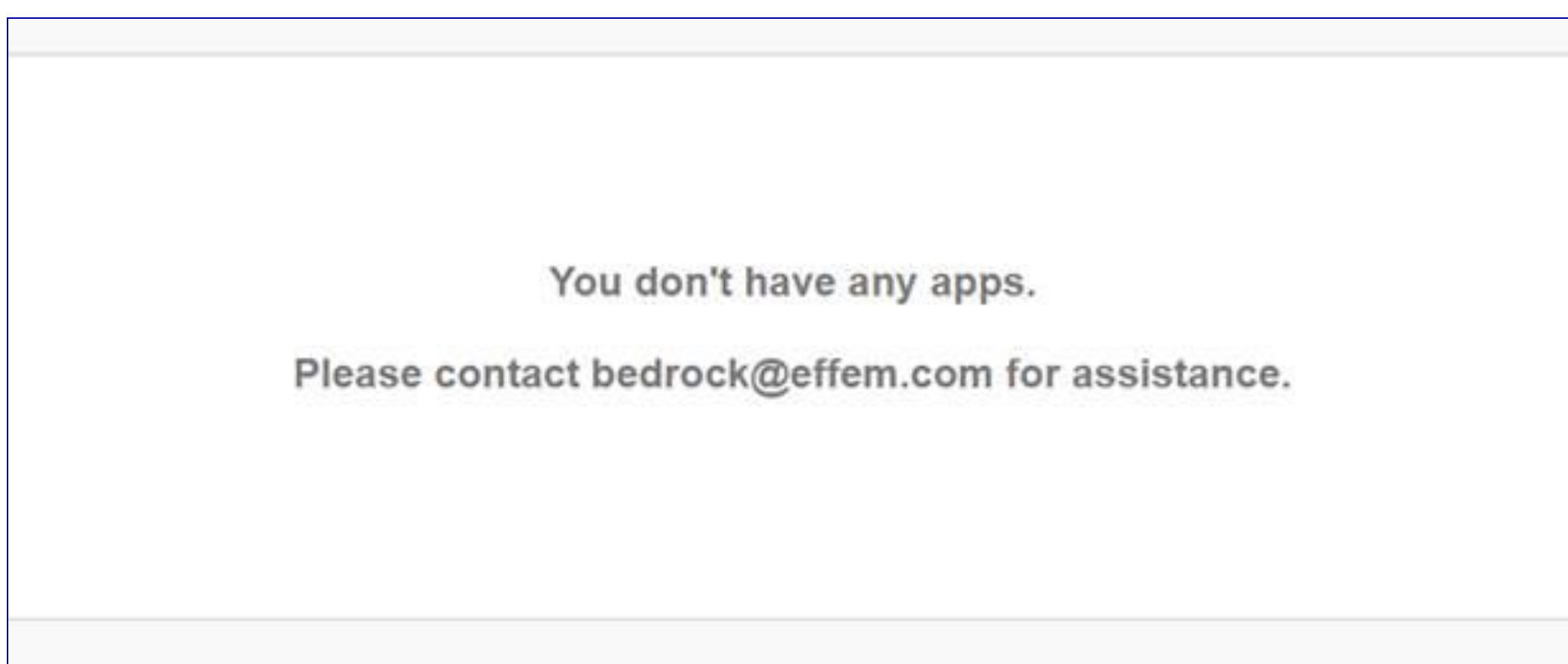
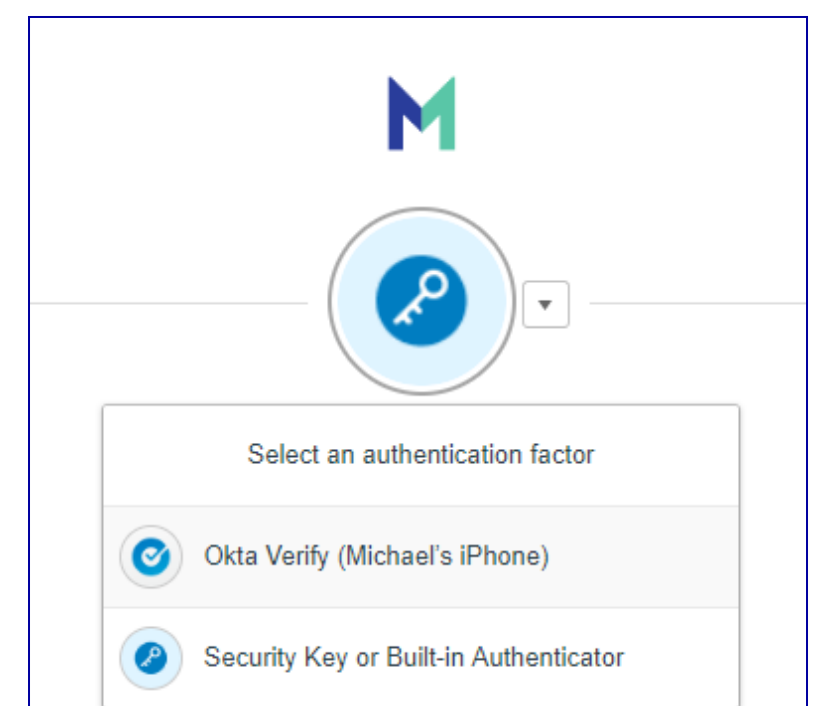
On your mobile device, click **Approve** when you receive a push notification.

If you don't receive any notification on your mobile phone, **open the Okta Verify App and approve.**

Thank you for helping us keeping Mars **#SecureTogether**

PLEASE NOTE:

- After configuring multiple authentication factors, you can click the **drop down** (see image on the right) **to change authentication factor.**
- If you are pre-enrolling in Okta, the message below is expected. You will not see applications in the Okta Dashboard until after go-live.



Authentication To Okta Using Okta SMS Authentication

Multifactor authentication (MFA) provides an additional layer of security for your applications by adding another factor to the sign on process.

This describes how to sign on to Okta using **SMS** as the second factor.


Log into Okta

1

Open a web browser and make sure you have your mobile device (Personal or Corporate) ready to use as part of this process . If you do not have a mobile device please proceed with verification questions.

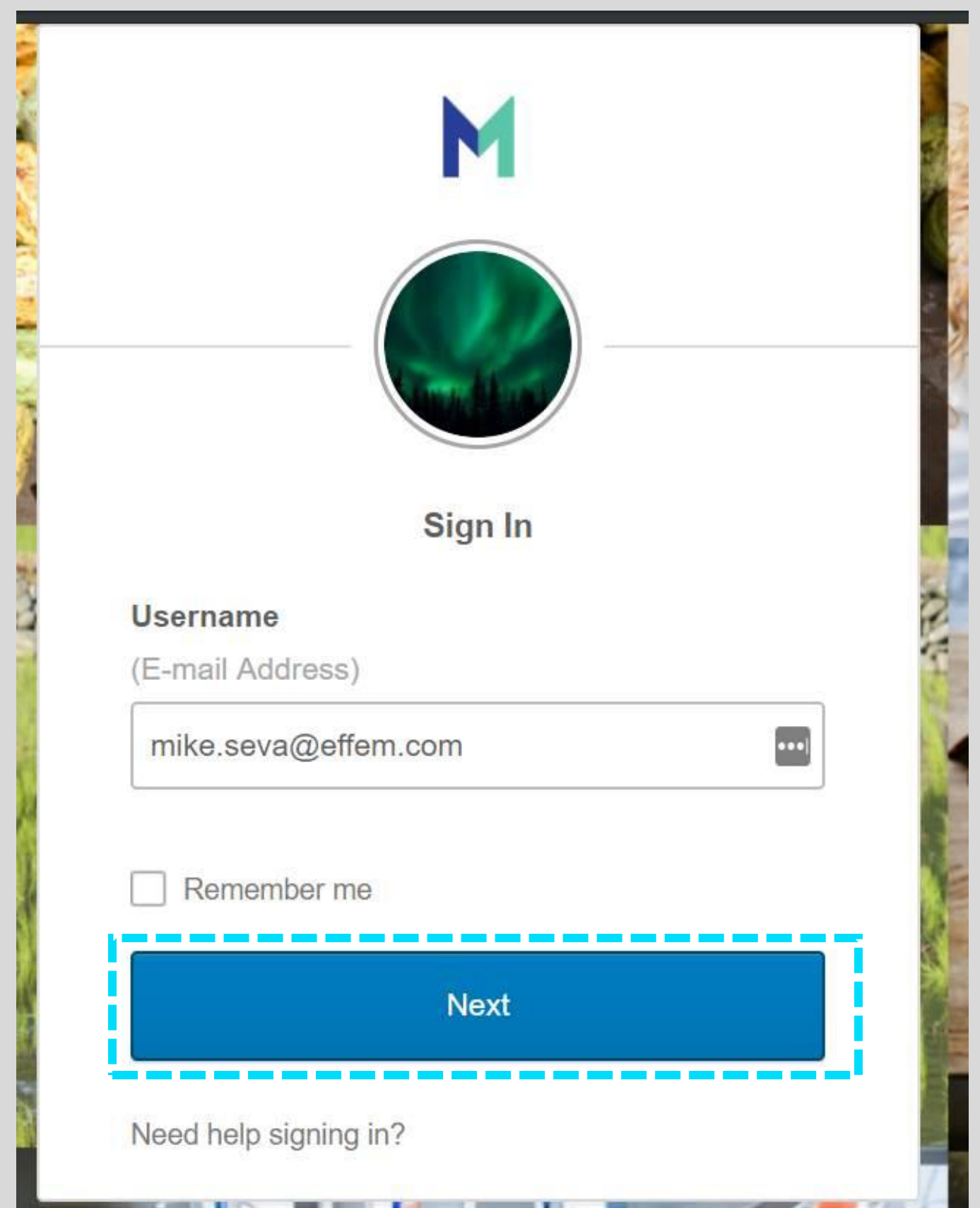
2

In the Address bar, type Mars-Group.Okta.com.

 **If you access a Mars application that requires you to authenticate with OKTA, you will be prompted to log-in (see image) and follow the steps below.*

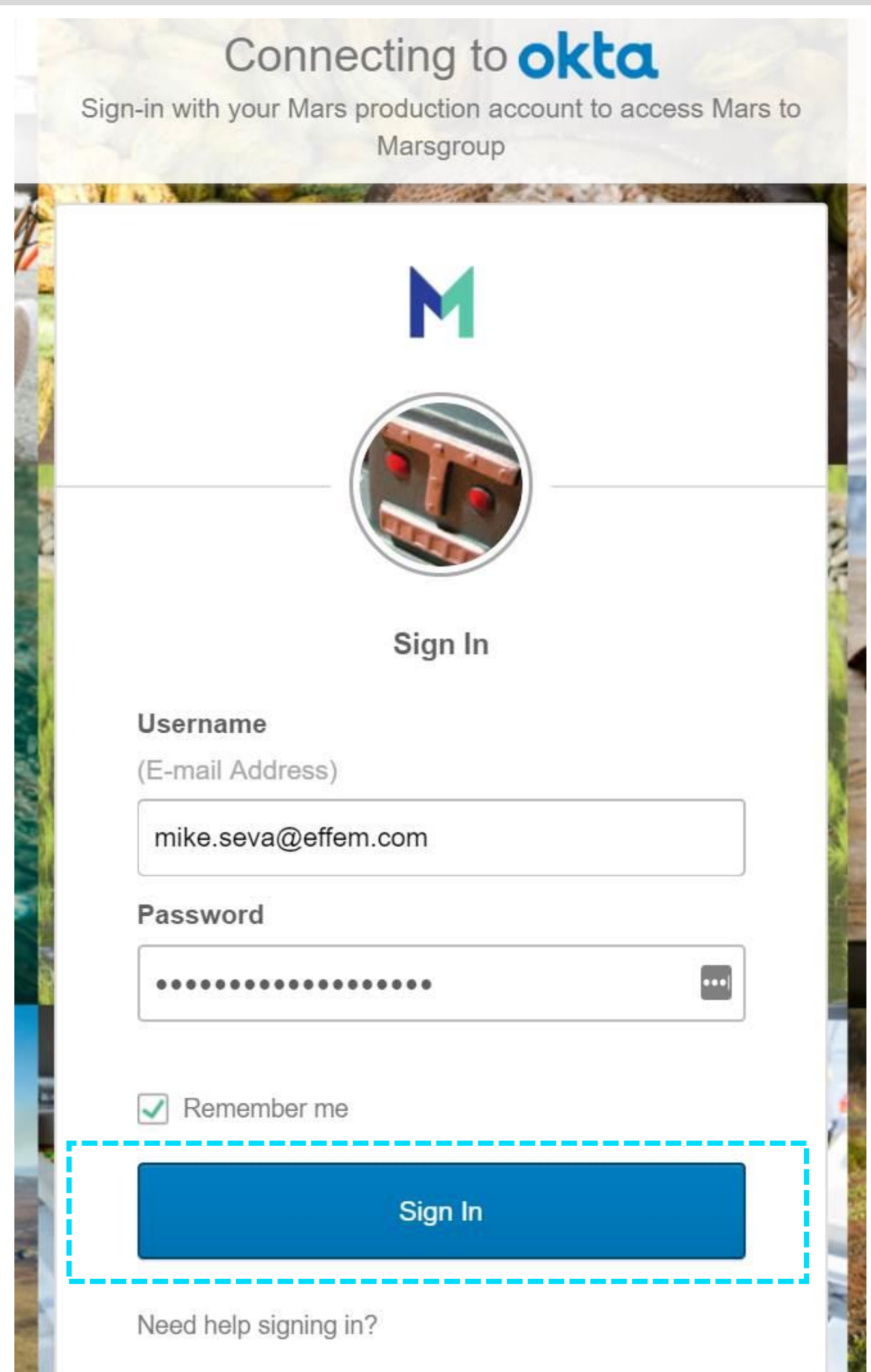
3

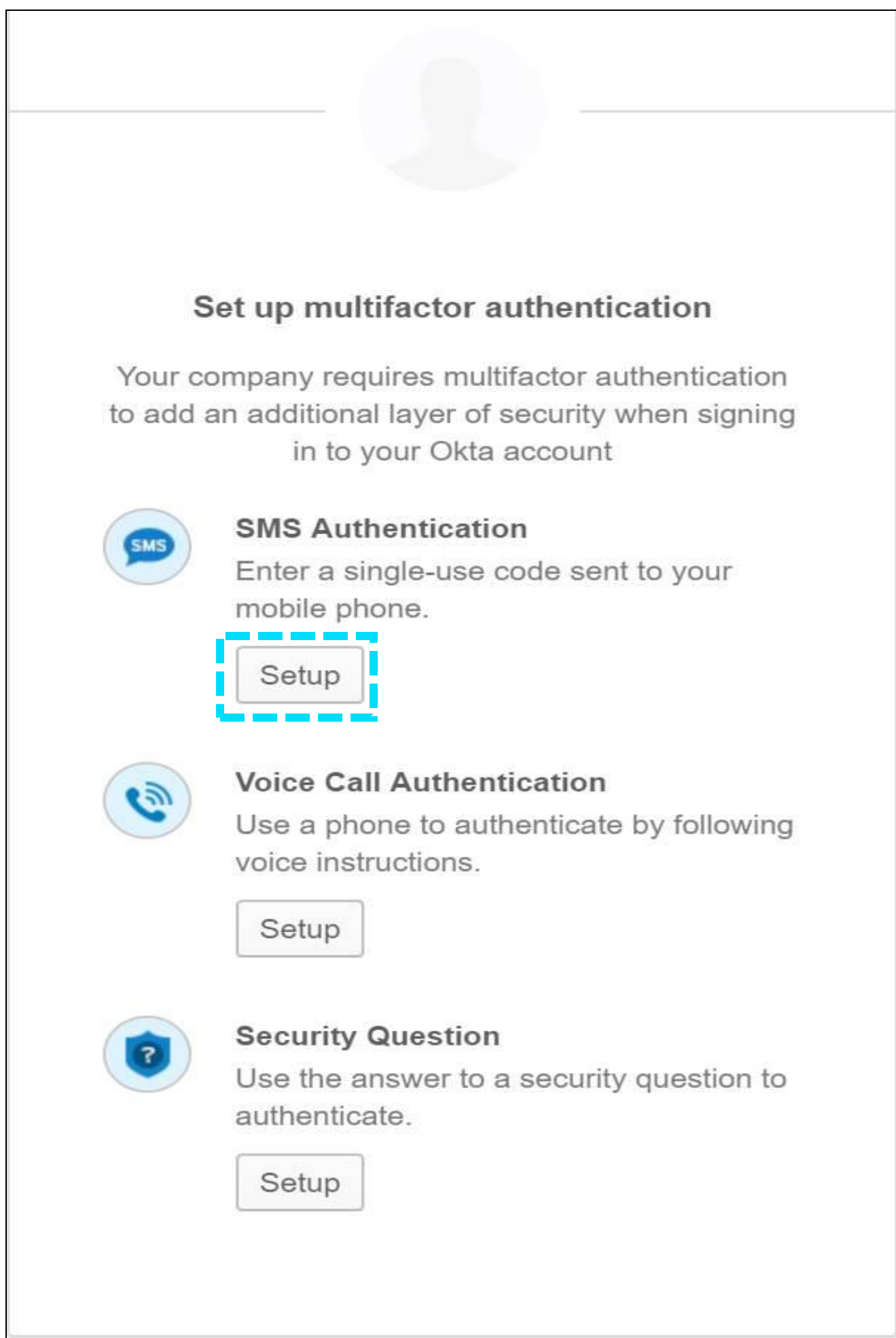
Type your corporate email and click **Next**.



4

If working remotely you will be prompted to type your corporate email and password and click **Sign In**.





5

On the **Set up multifactor authentication** screen, click **Setup for SMS Authentication**.

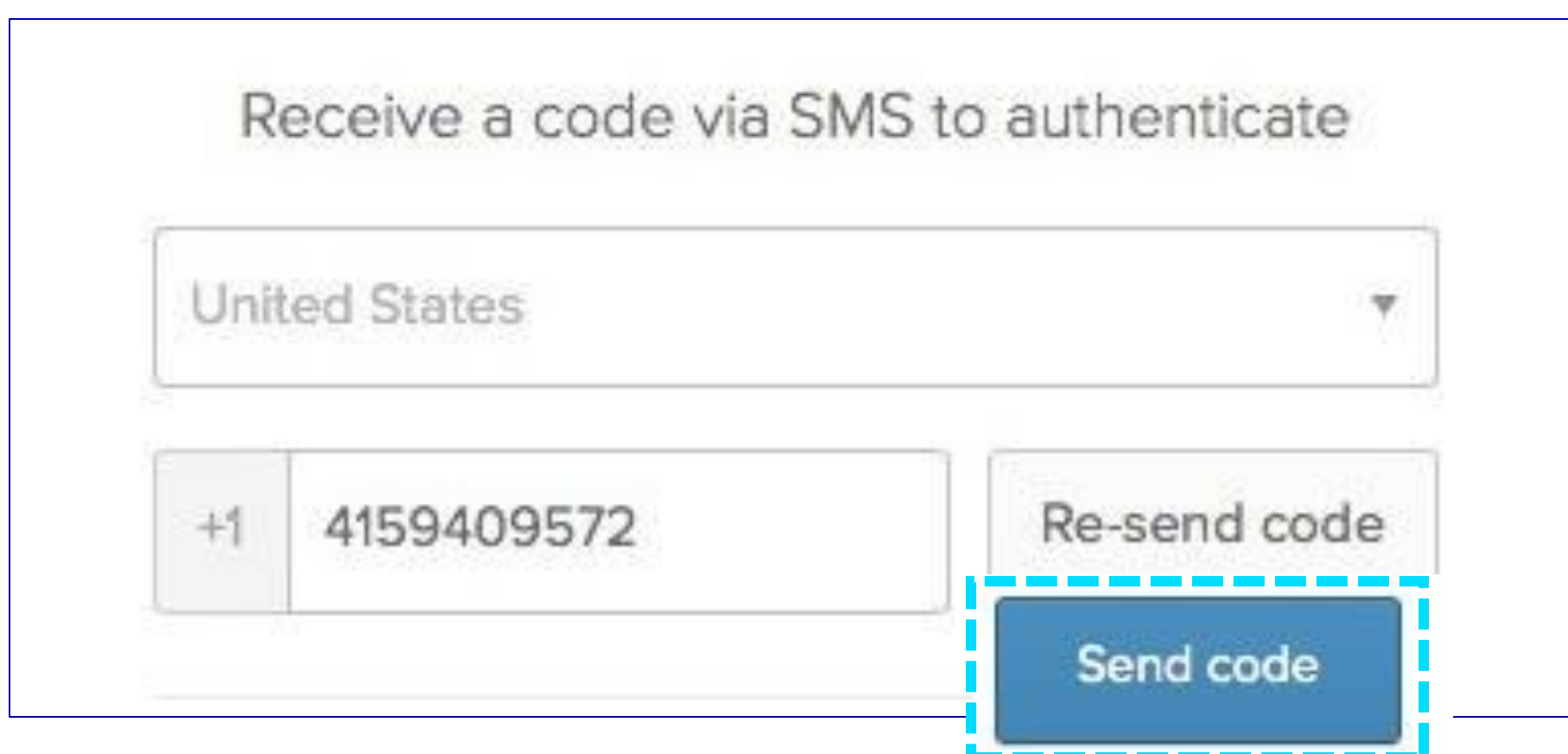
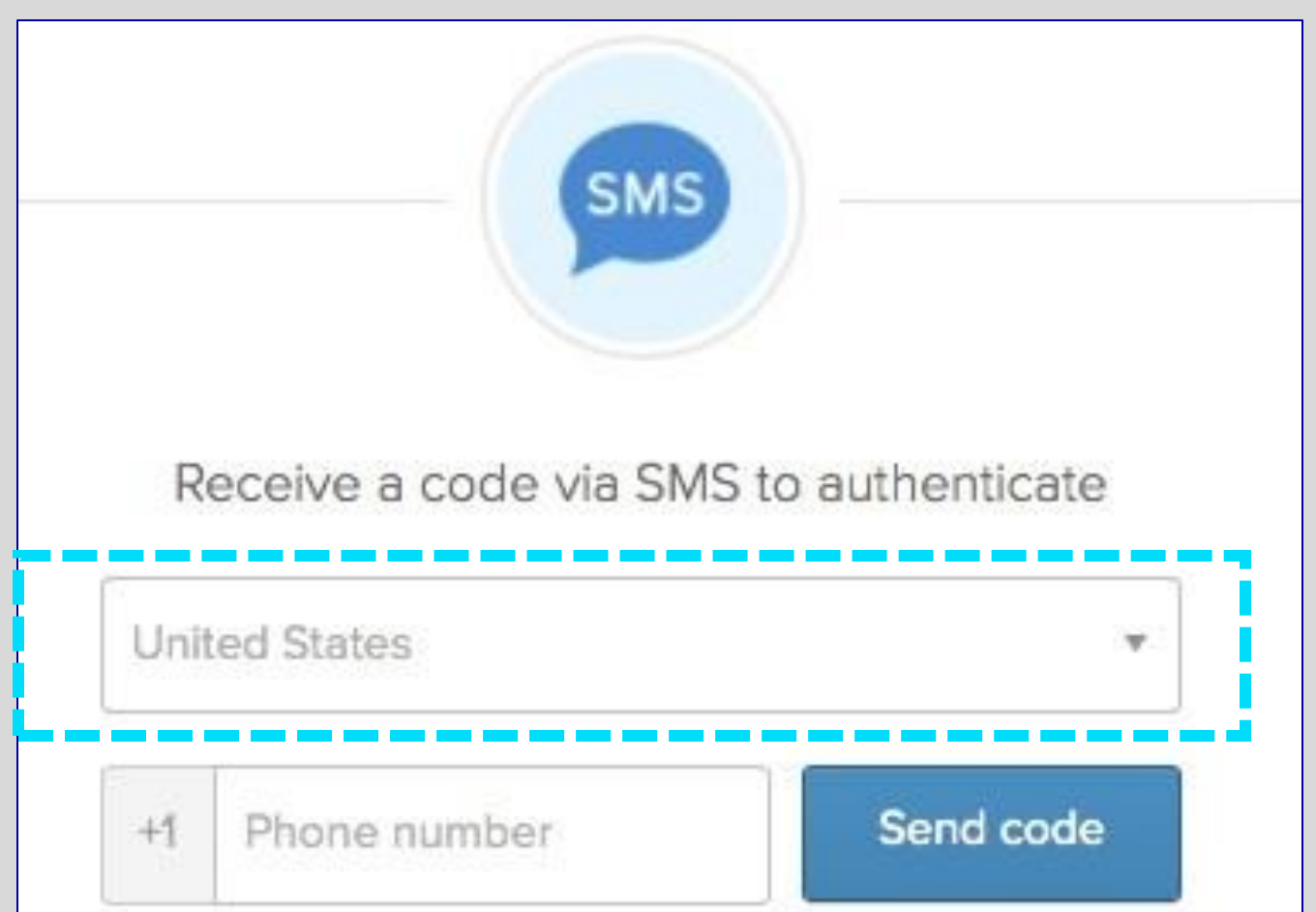
Also perform the set up steps for [Voice Call Authentication](#) and [Security Question](#).



6

Provide Your Phone Number

On the **SMS** screen, select your country code from the drop-down and type your phone number.

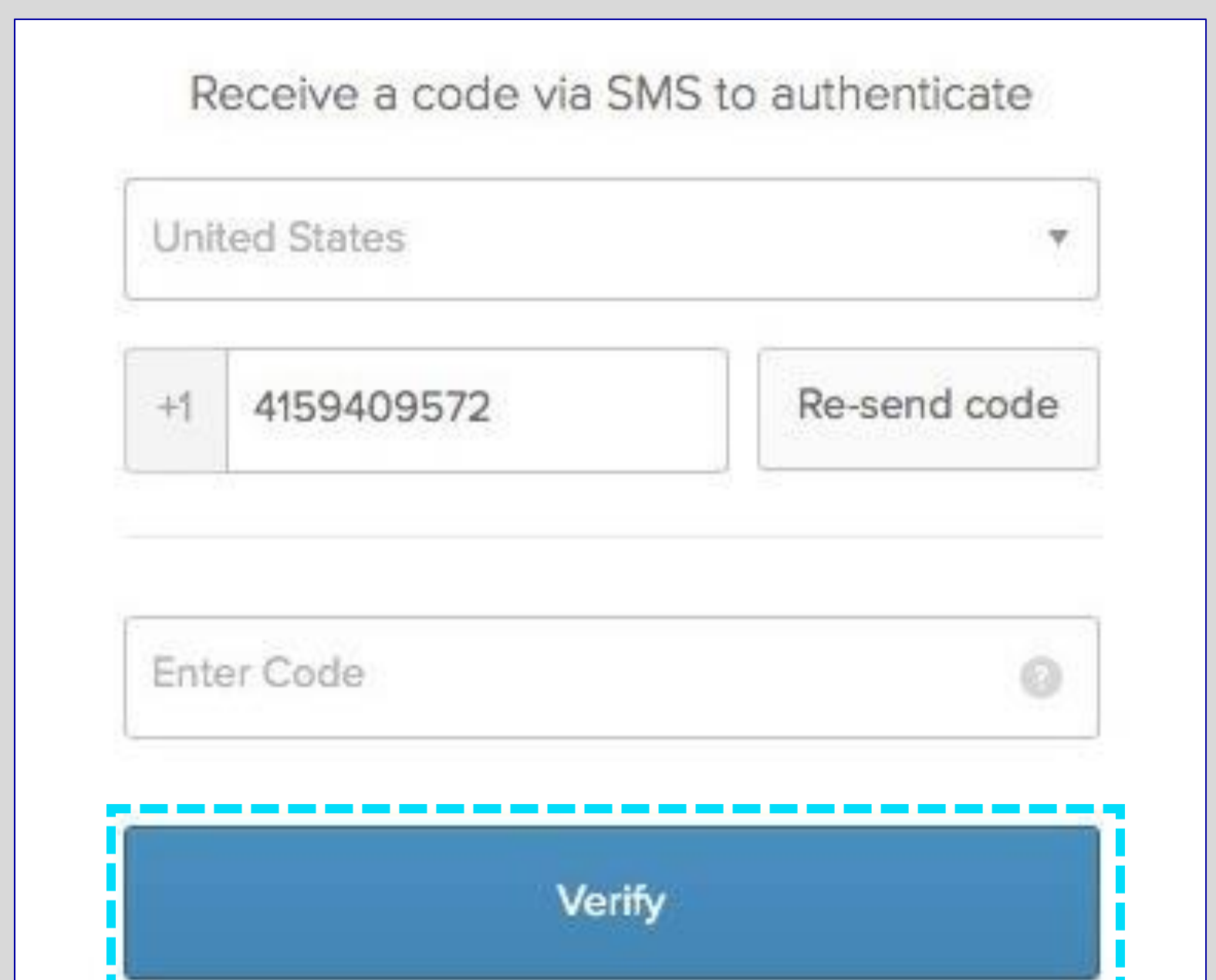


7



Code Verification
Click **Send code**.

8

Type the SMS code received on your mobile device, into the **Receive a code via SMS to authenticate** screen on your computer and click **Verify**.





Click **Finish**.



Set up multifactor authentication

You can configure any additional optional factor or click finish

Enrolled factors

-  **SMS Authentication** 

Additional optional factors

-  **Voice Call Authentication**
Use a phone to authenticate by following voice instructions.
-  **Security Question**
Use the answer to a security question to authenticate.

10

You will be prompted to update your profile.

Please select **two options** to complete your enrollment. After you have updated your profile you have successfully enrolled in Okta.

If you have pre-enrolled (before the go-live date) you will not see any applications in Okta until after the go-live date.

Please update your profile



Add a phone number for resetting your password or unlocking your account using SMS (optional)

Okta can send you a text message with a recovery code. This feature is useful when you don't have access to your email.

+ Add Phone Number



Add a phone number for resetting your password or unlocking your account using Voice Call (optional)

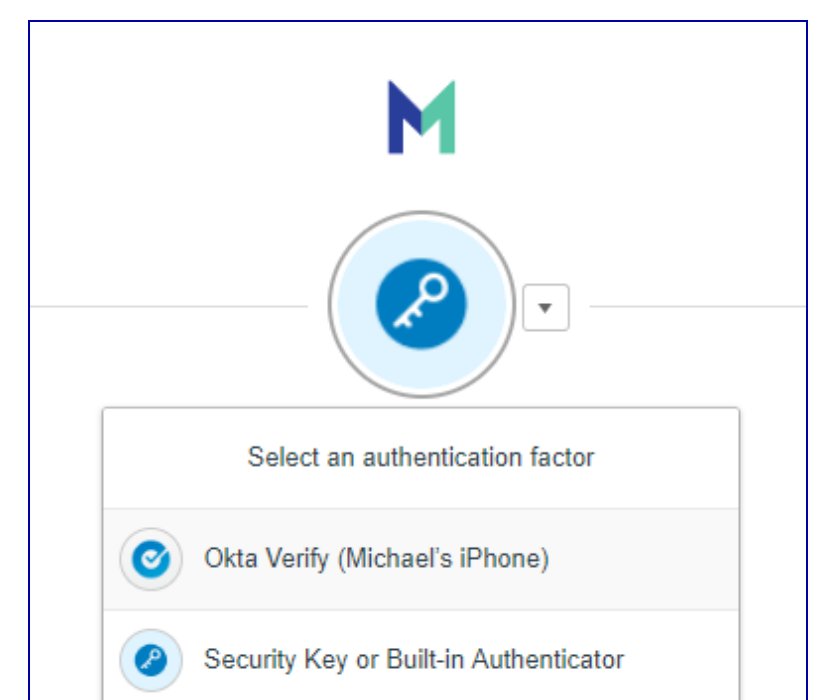
Okta can call you and provide a recovery code. This feature is useful when you don't have access to your email.

+ Add Phone Number

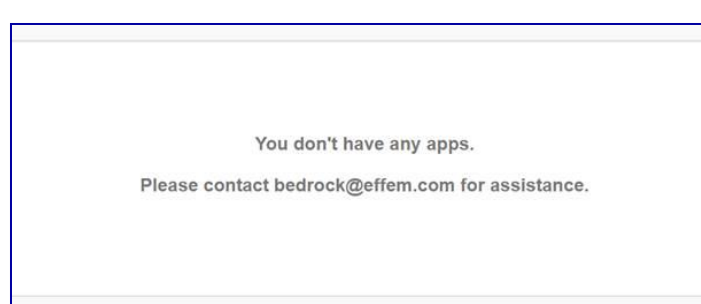
Remind me later

PLEASE NOTE:

- After configuring multiple authentication factors, you can click the drop down (see image on the right) **to change authentication factor**.



- If you are pre-enrolling in Okta, the message below is expected. You will not see applications in the Okta Dashboard until after go-live.




Thank you for helping us keeping Mars
SecureTogether

For more information contact bedrock@effem.com

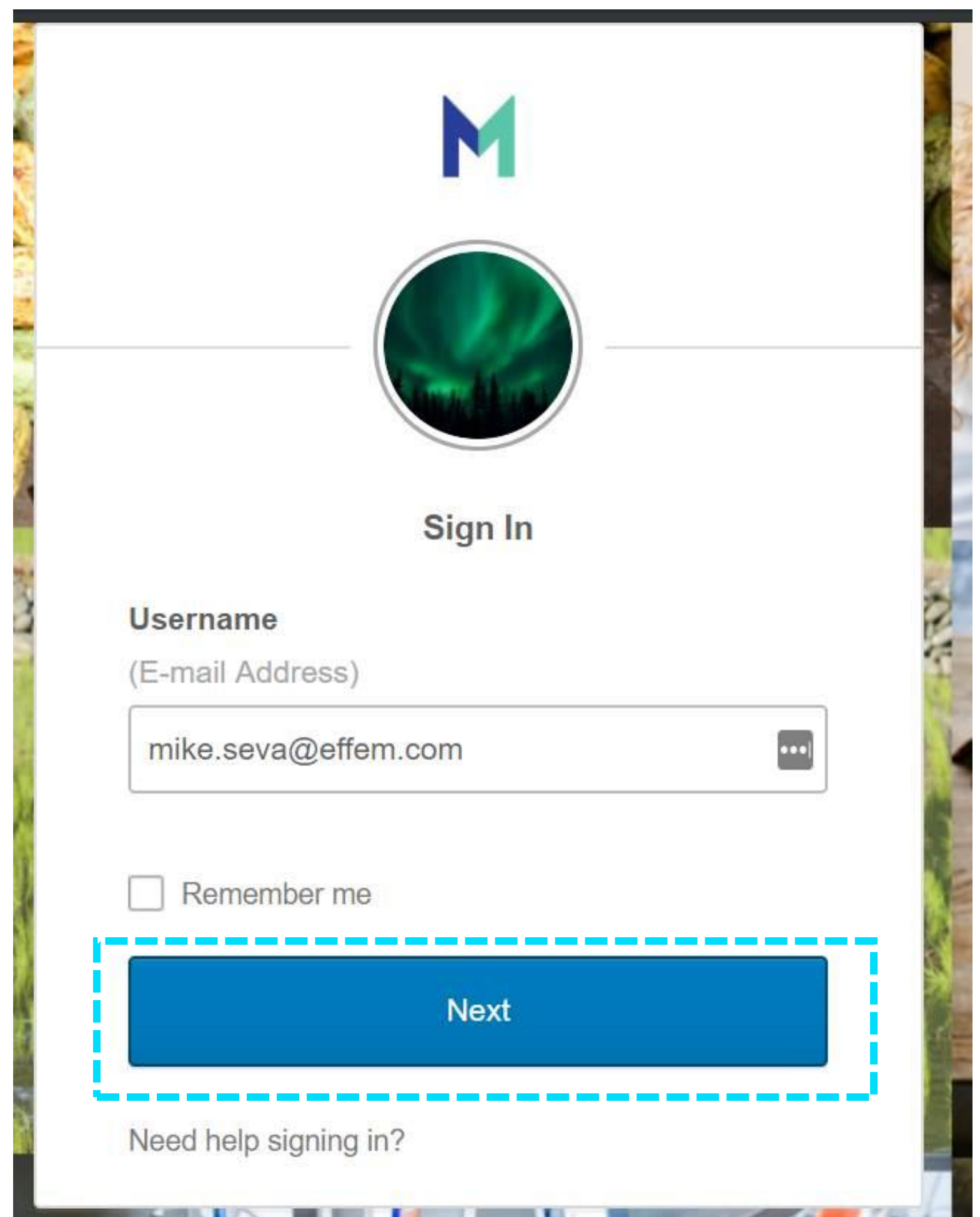
Authenticating To Call Authentication As A Factor

Log into Okta

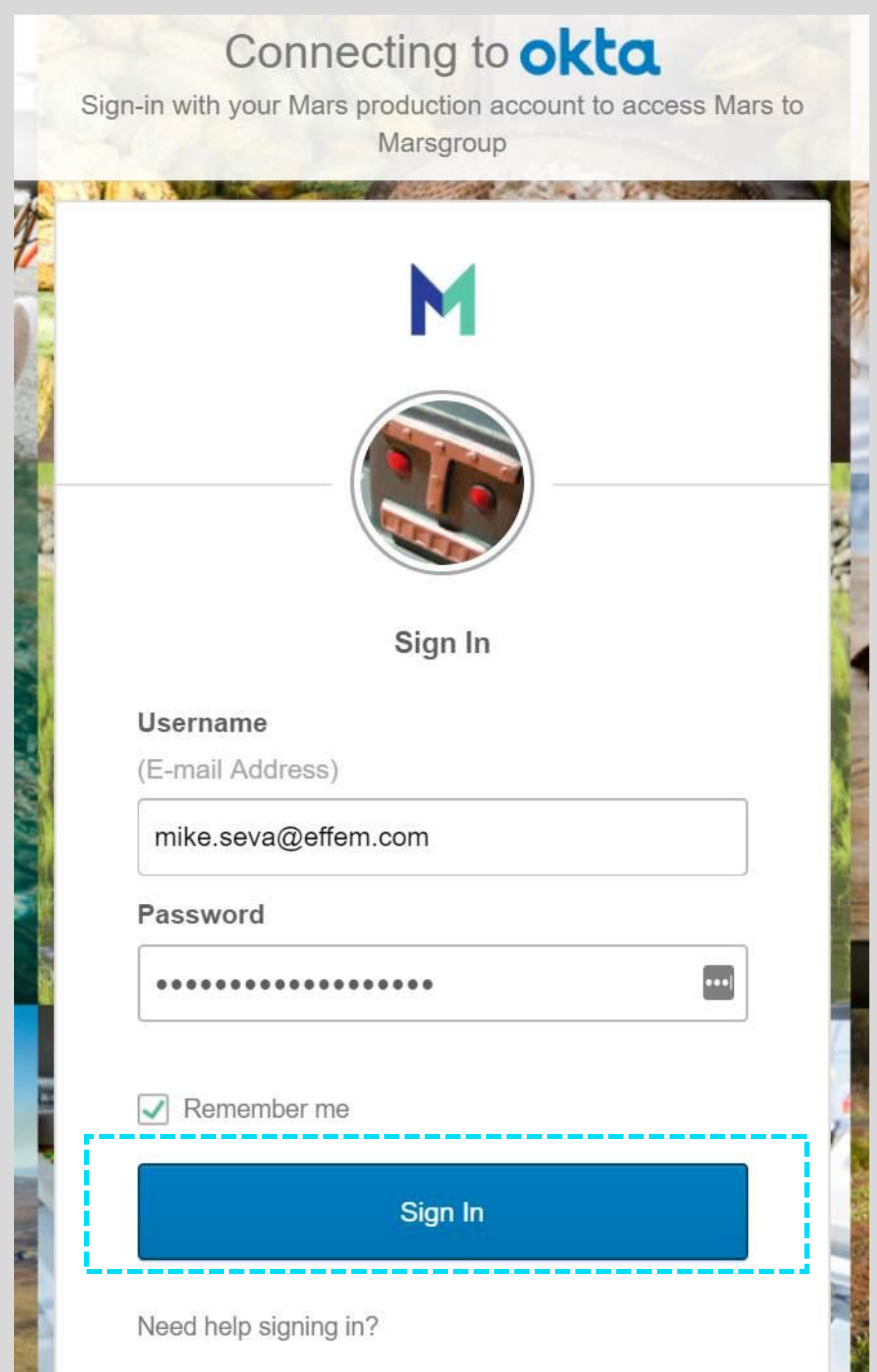
1 Open a web browser and make sure you have your mobile device (Personal or Corporate) ready to use. If you do not have a mobile device please proceed with verification questions.

2 In the Address bar, type Mars-Group.Okta.com.
 **If you access a Mars application that requires you to authenticate with OKTA, you will be prompted to log-in (see image) and follow the steps below.*

3
Type your corporate email and click **Next**.



4
If working remotely you will be prompted to type your corporate email and password and click **Sign In**.





Set up multifactor authentication

Your company requires multifactor authentication to add an additional layer of security when signing in to your Okta account



SMS Authentication

Enter a single-use code sent to your mobile phone.

Setup



Voice Call Authentication

Use a phone to authenticate by following voice instructions.

Setup



Security Question

Use the answer to a security question to authenticate.

Setup

5

On the **Set up multifactor authentication** screen, click **Setup** under **Voice Call Authentication**.

6

On the **Setup Voice Call Authentication** screen, select your country code from the drop-down and type your phone number.

okta



Follow phone call instructions to authenticate

United States

+1 Phone number

Extension

Call

Back to factor list

okta



Follow phone call instructions to authenticate

United States

+1 Phone number

Extension

Call

Back to factor list

7

Click **Call**.

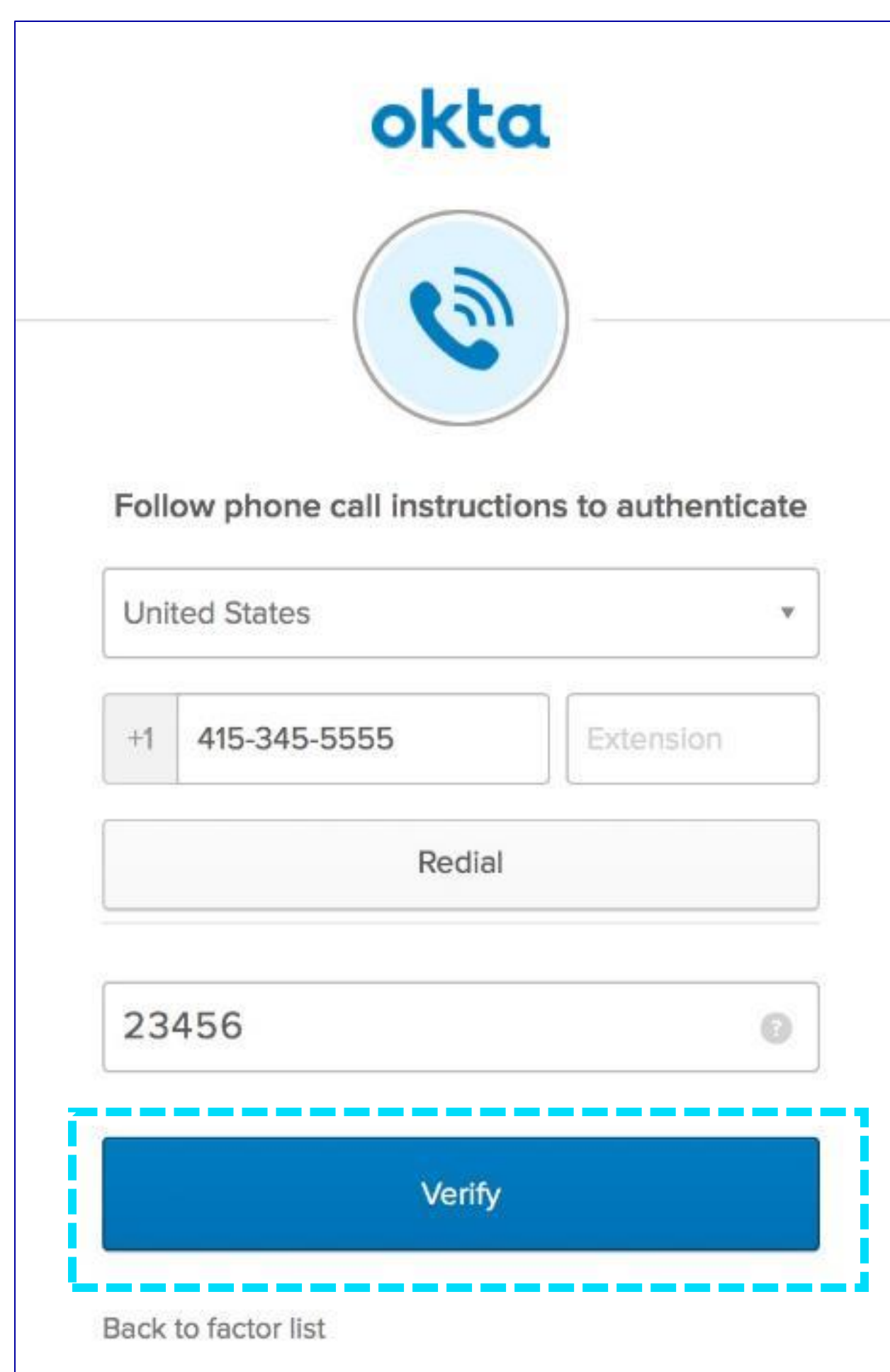
VERIFICATION OF THE PHONE NUMBER

8 Answer the call for the number that you provided above.

9 Enter the code provided.

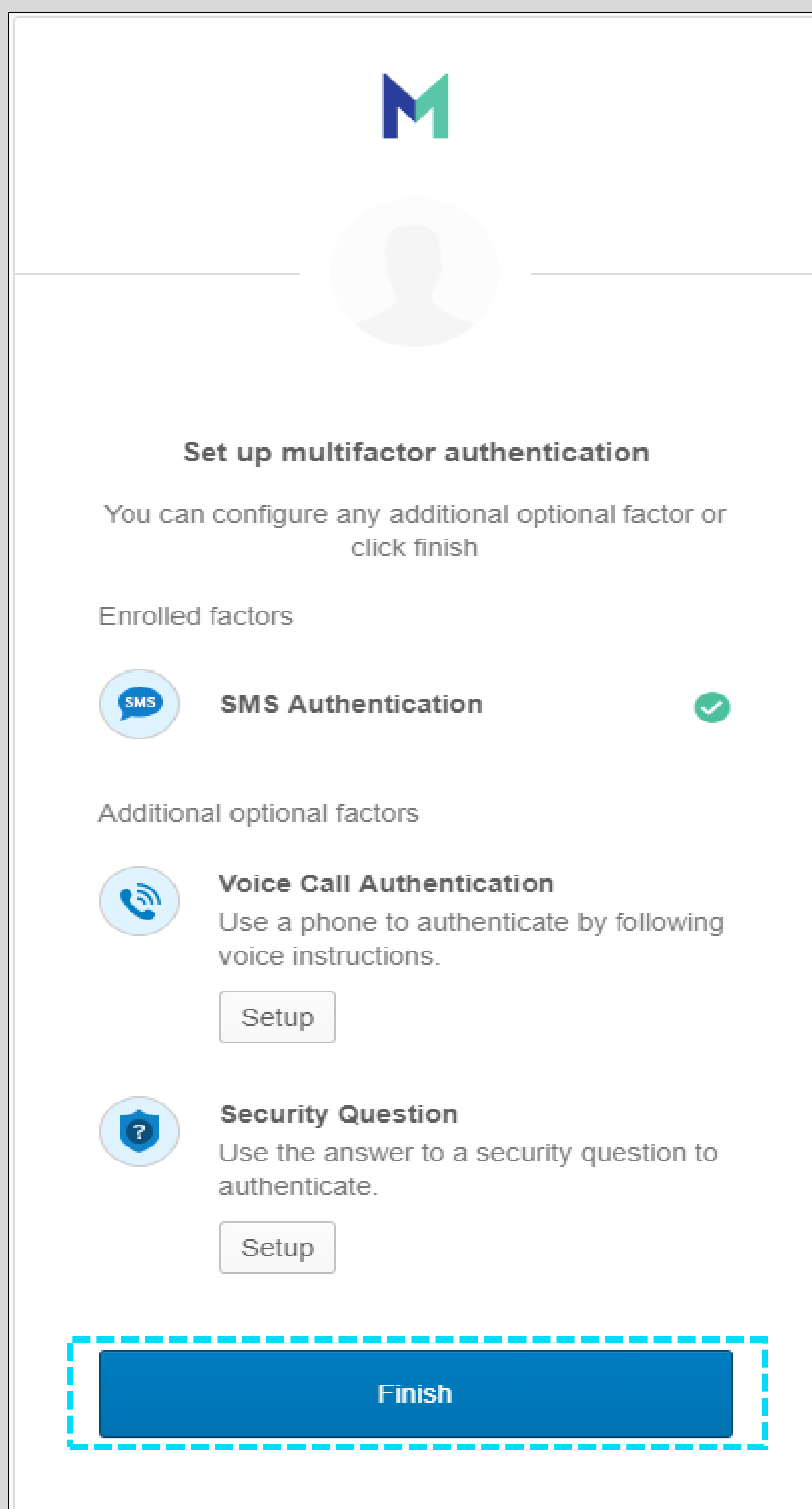
10

Click **Verify**.



The image shows a mobile application interface for Okta. At the top is the Okta logo and a phone icon. Below that, the text reads "Follow phone call instructions to authenticate". There is a dropdown menu for "United States", a text input field for the phone number "+1 415-345-5555" with an "Extension" field to its right, and a "Redial" button. Below these is a text input field containing the code "23456". A blue "Verify" button is highlighted with a dashed red border. At the bottom, there is a link for "Back to factor list".

11 Click **Finish**.



The image shows a mobile application interface for setting up multifactor authentication. At the top is a logo with the letter "M" and a user profile icon. The main heading is "Set up multifactor authentication". Below this, it says "You can configure any additional optional factor or click finish". There are two sections: "Enrolled factors" and "Additional optional factors". Under "Enrolled factors", there is a "SMS Authentication" option with a green checkmark. Under "Additional optional factors", there are two options: "Voice Call Authentication" with a "Setup" button and "Security Question" with a "Setup" button. A blue "Finish" button is highlighted with a dashed red border at the bottom of the screen.

12

You will be prompted to update your profile. Please select **two options** to complete your enrollment. After you have updated your profile you have successfully enrolled in Okta. If you have pre-enrolled you will not see any applications in Okta until after the go-live date.

Please update your profile

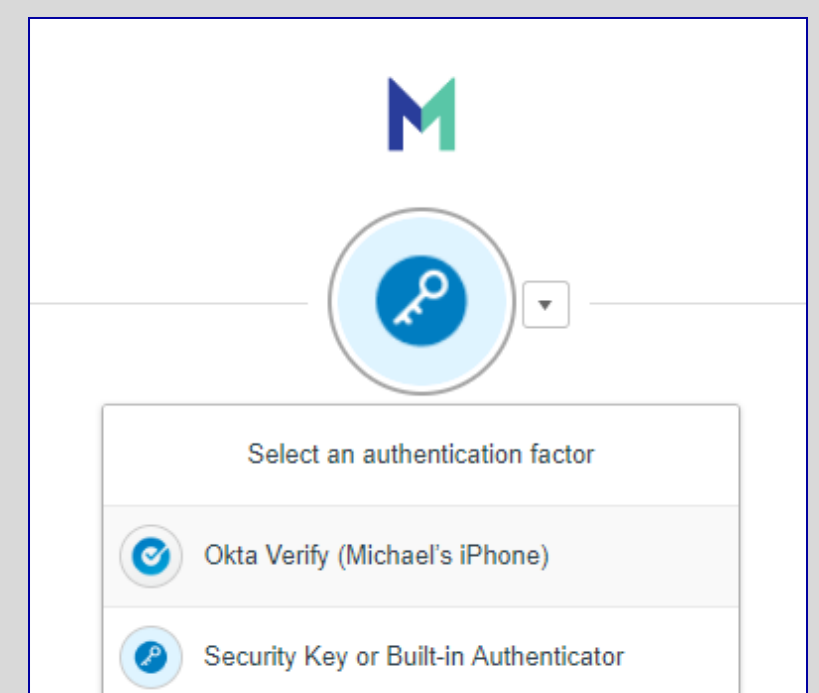
+ Add Phone Number

+ Add Phone Number

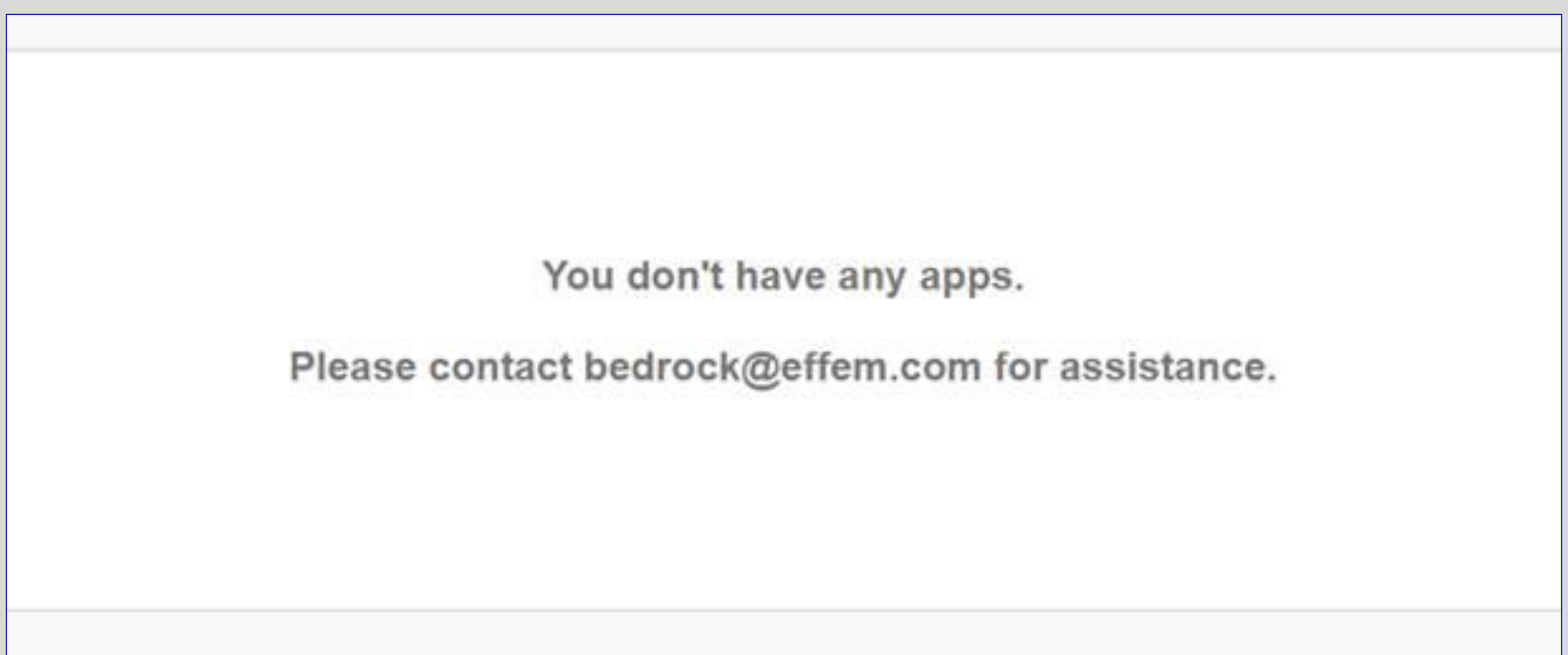
Remind me later

PLEASE NOTE:

- After configuring multiple authentication factors, you can click the drop down (see image on the right) **to change authentication factor**.



- If you are pre-enrolling in Okta, the message below is expected. You will not see applications in the Okta Dashboard until after go-live.



Thank you for helping us keeping Mars
#SecureTogether

For more information contact bedrock@effem.com


Authenticating to Okta Using A Security Question

Multifactor authentication (MFA) provides an additional layer of security for your applications by adding another factor to the sign on process.

This describes how to sign on to Okta using a **Security Question**.

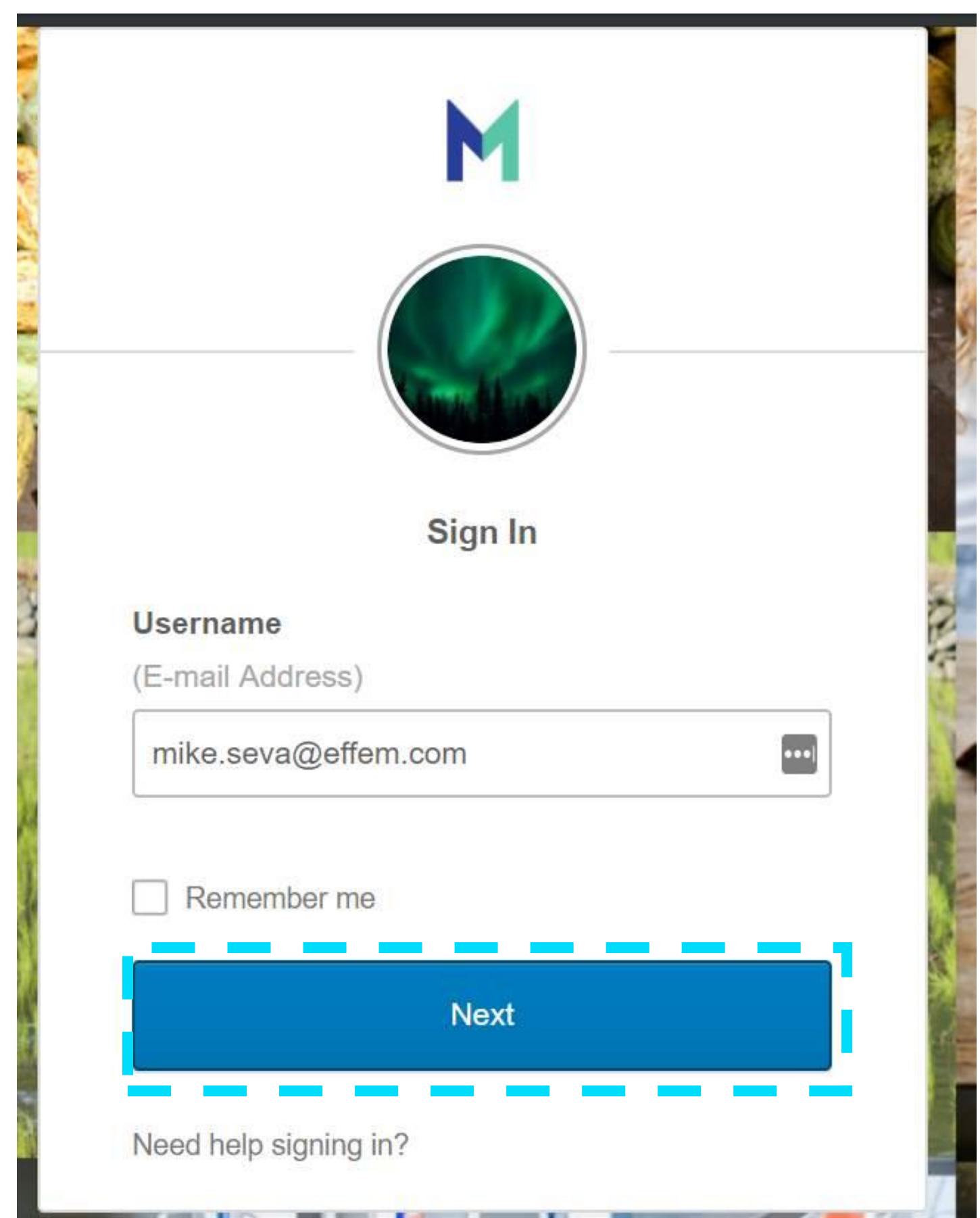
1 Open a web browser

In the Address bar, type Mars-Group.Okta.com.

 **If you access a Mars application that requires you to authenticate with OKTA, you will be prompted to log-in (see image) and follow the steps below.*

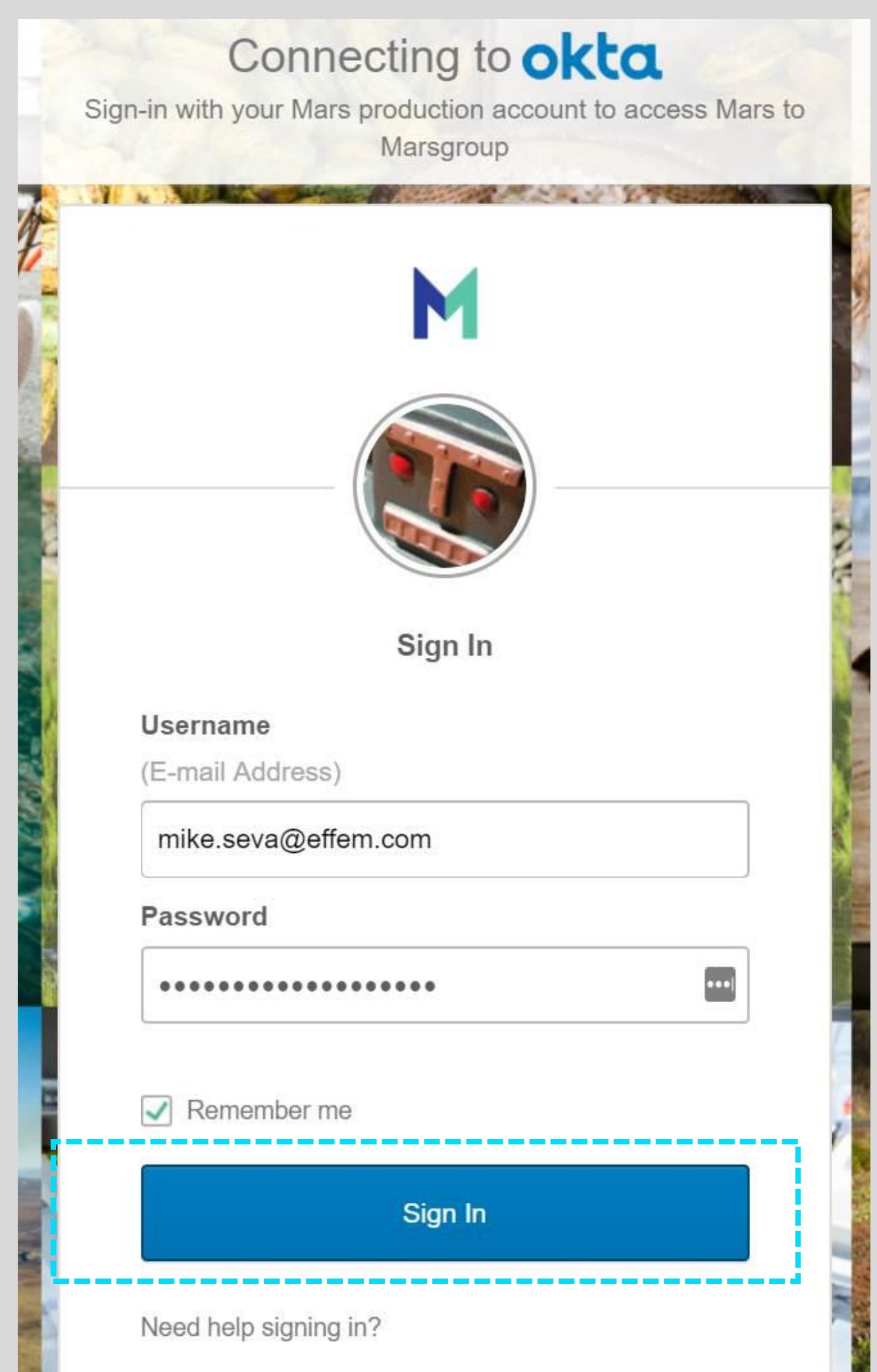
2

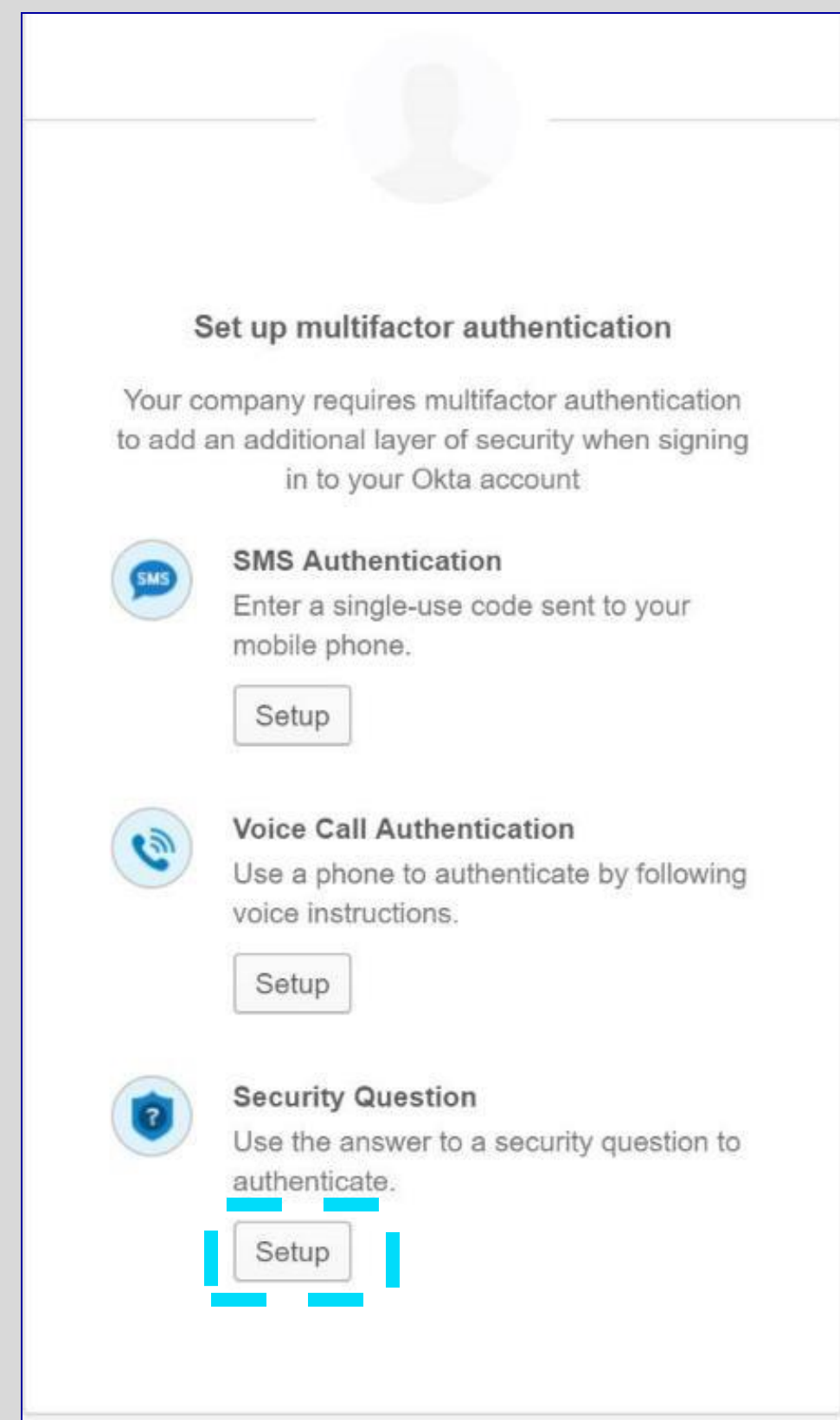
Type your **company email address** and click **Next**.



3

If working remotely you will be prompted to type your corporate email and password and click **Sign In**.



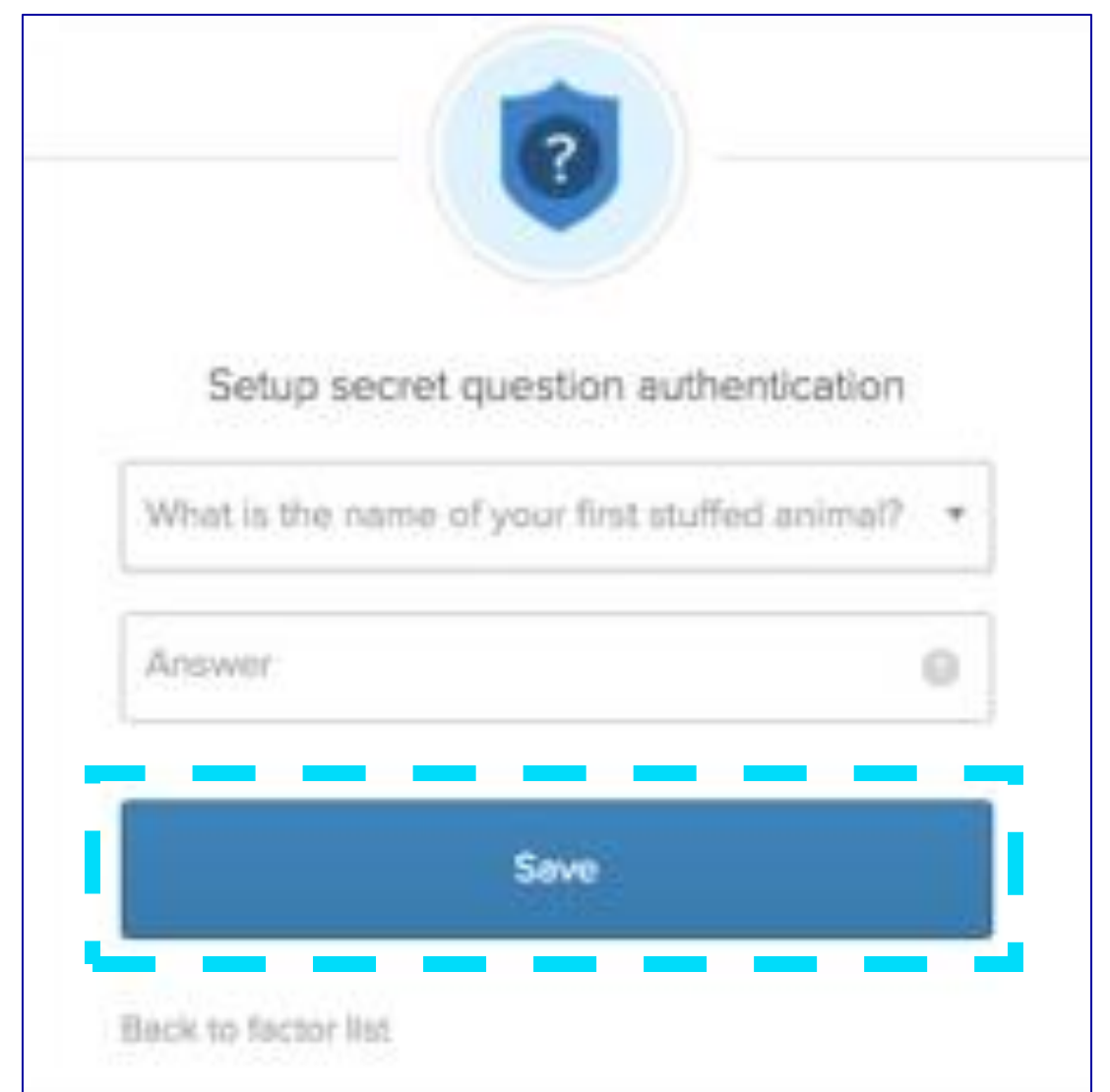


4

On the **Set up multifactor authentication** screen, click **set up**.

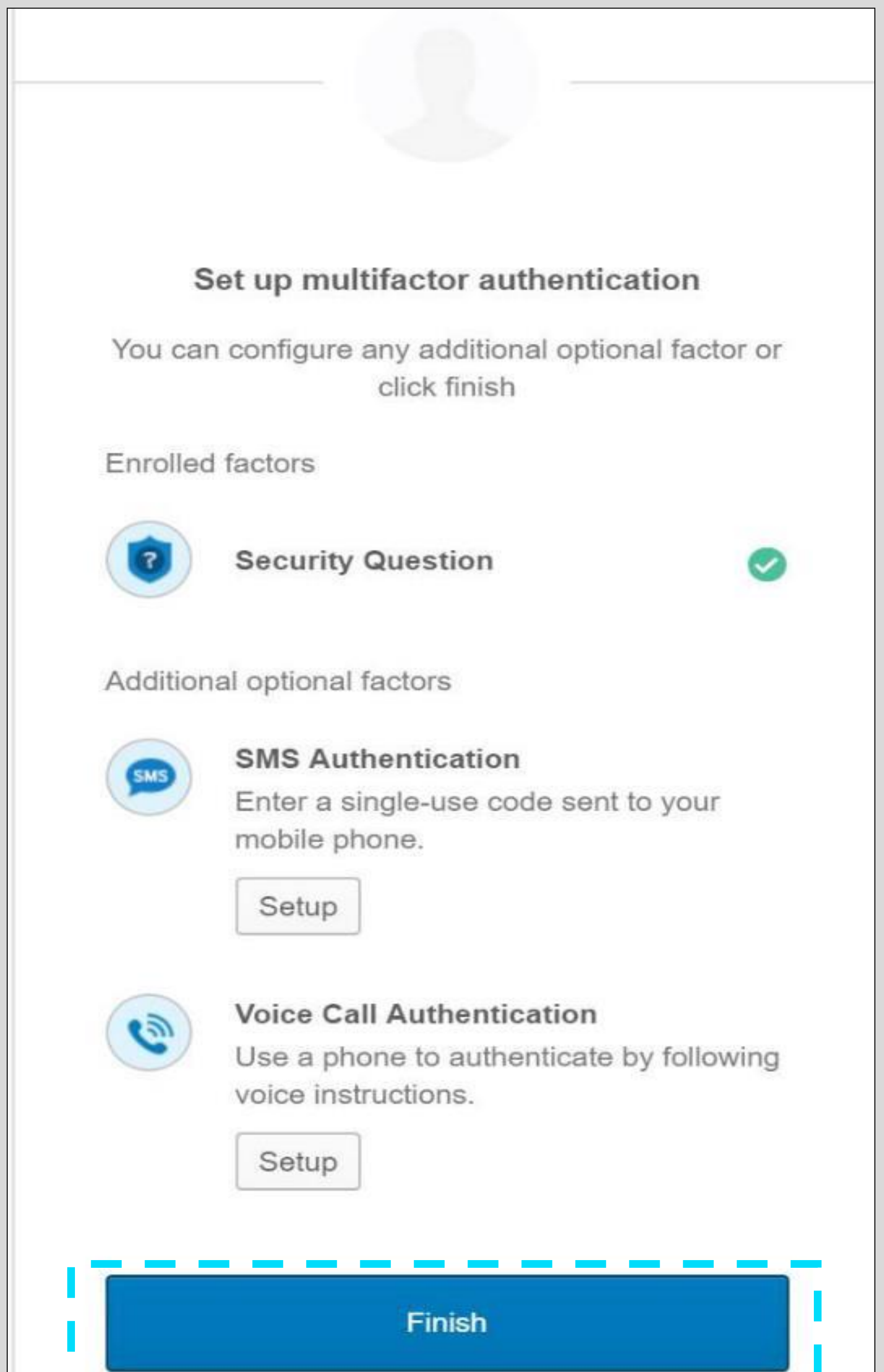
5 On the **Setup secret question authentication** screen, complete the following steps:

- Select a question.
- Type an answer.
- Click **Save**.



6

Click **Finish**.



7

You will be prompted to update your profile. Please select **two options** to complete your enrollment. After you have updated your profile you have successfully enrolled in Okta.

If you have pre-enrolled you will not see any applications in Okta until the go-live date.

Please update your profile

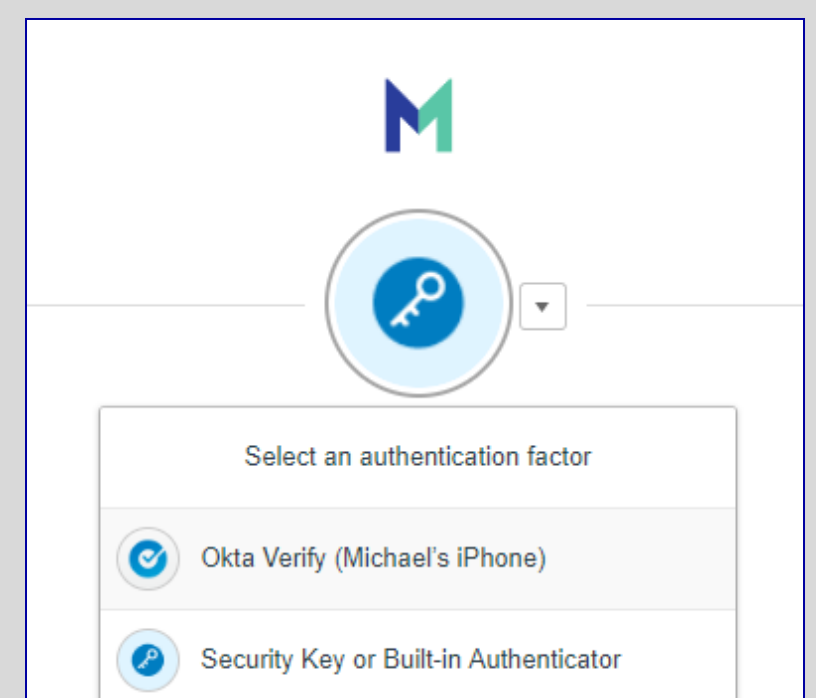
+ Add Phone Number

+ Add Phone Number

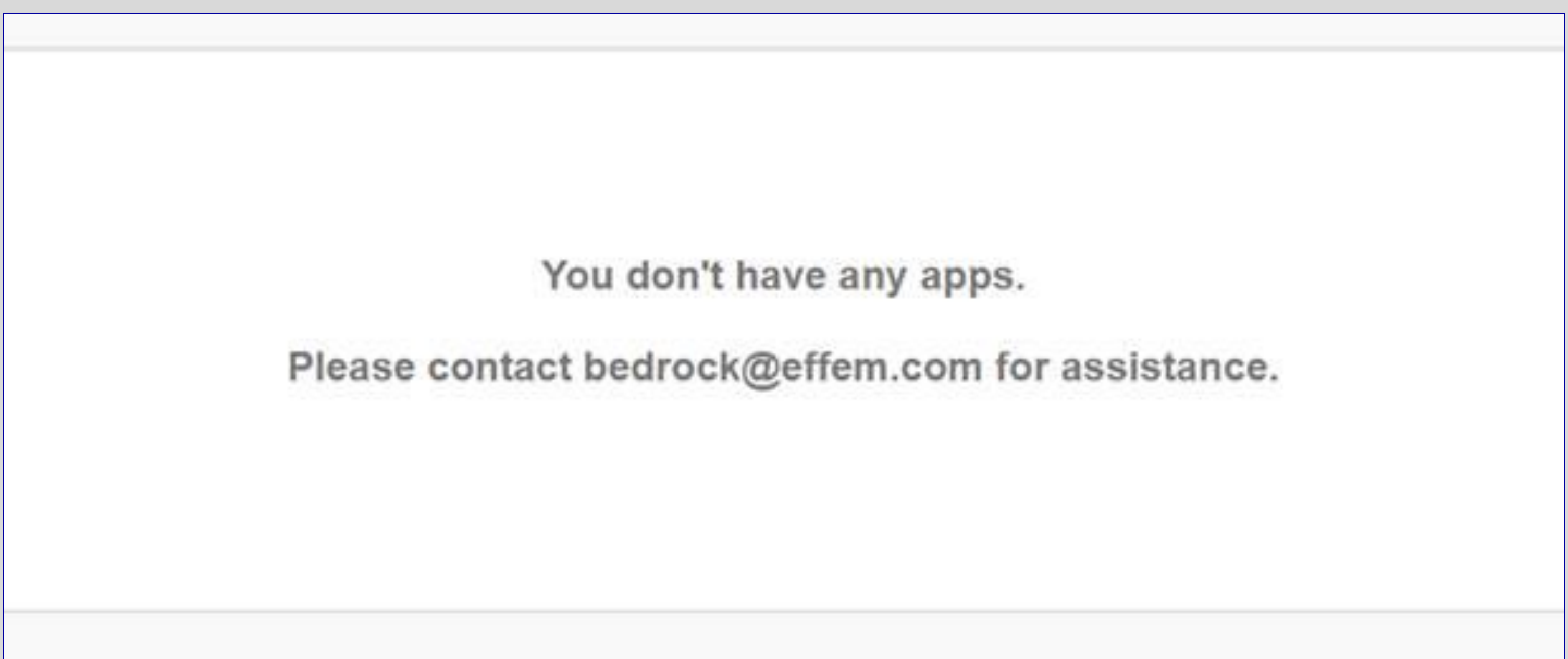
Remind me later

PLEASE NOTE:

- After configuring multiple authentication factors, you can click the drop down (see image on the right) **to change authentication factor**.



- If you are pre-enrolling in Okta, the message below is expected. You will not see applications in the Okta Dashboard until after go-live.



Thank you for helping us keeping Mars
#SecureTogether


For more information contact bedrock@effem.com

Configuring Yubikey As An Mfa Factor

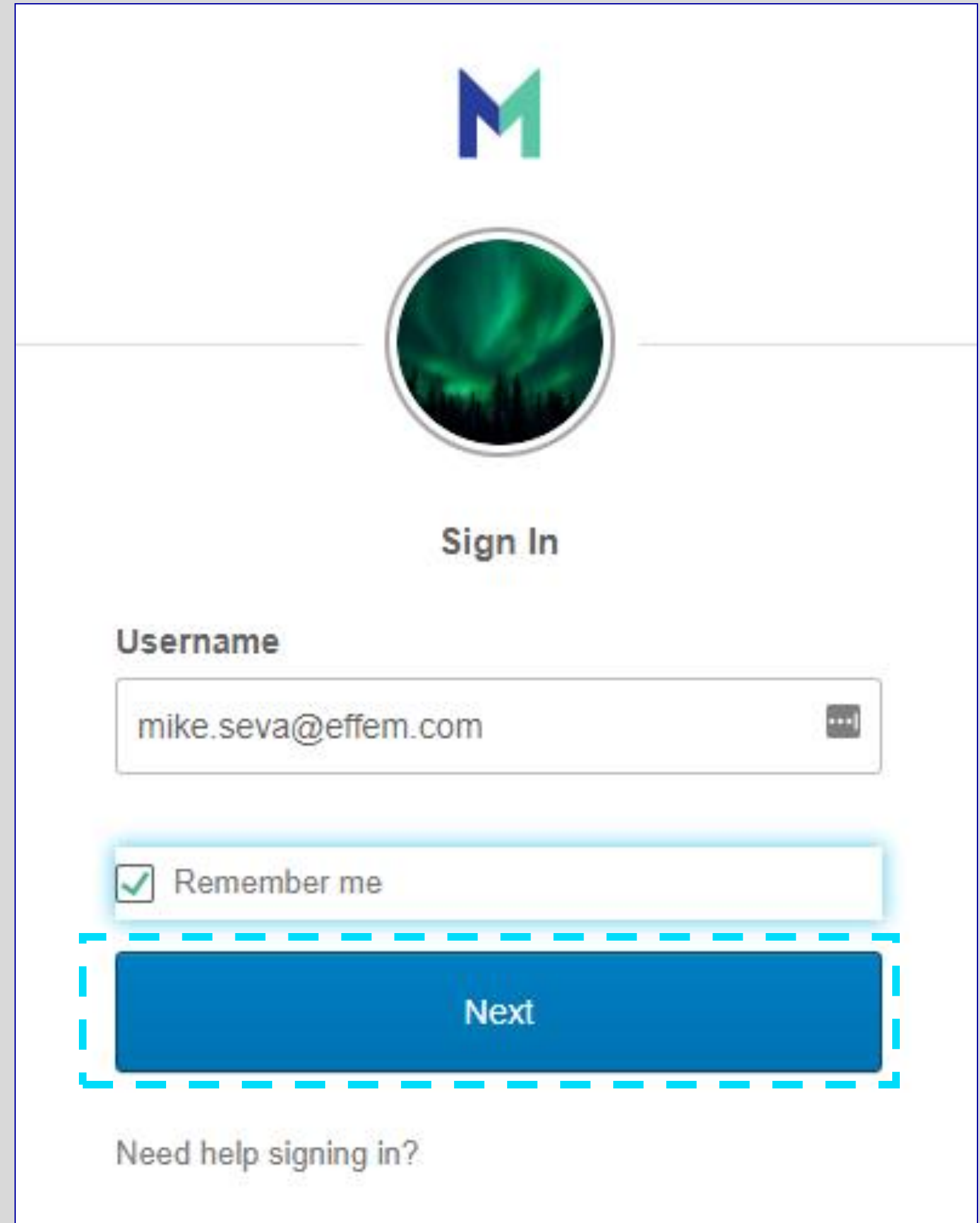
Log into Okta

1

Navigate to [Mars-group.okta.com](https://mars-group.okta.com) and enter your corporate e-mail address
Click **Next**

 You will automatically be redirected to setup MFA when accessing.

If you are accessing from **outside a Mars site** you will have to enter your **email and password**



Mars logo

Sign In

Username

mike.seva@effem.com

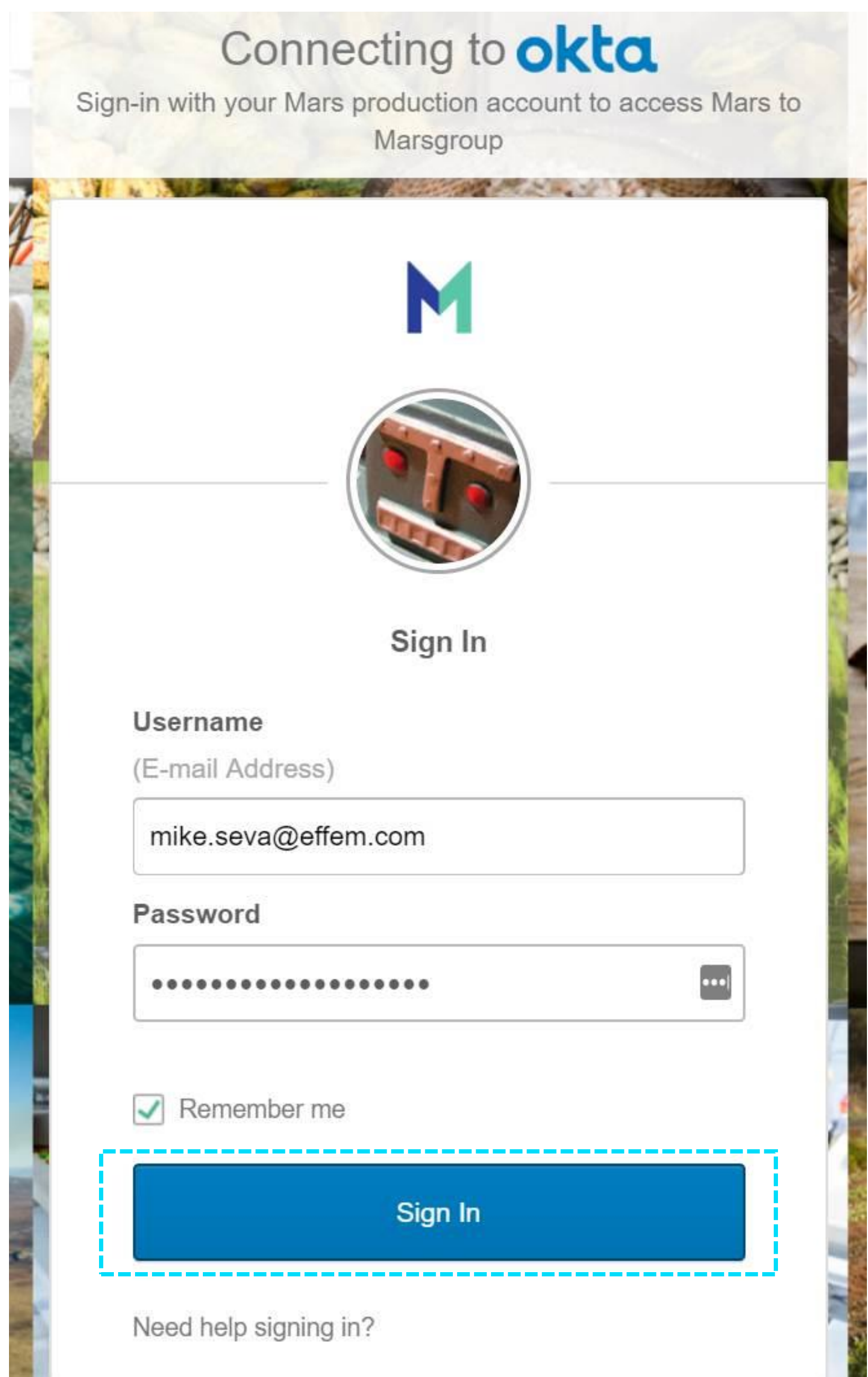
Remember me

Next

Need help signing in?

2

If working remotely you will be prompted to type your corporate email and password and click **Sign In**.



Connecting to **okta**

Sign-in with your Mars production account to access Mars to Marsgroup

Mars logo

Sign In

Username
(E-mail Address)

mike.seva@effem.com

Password

.....

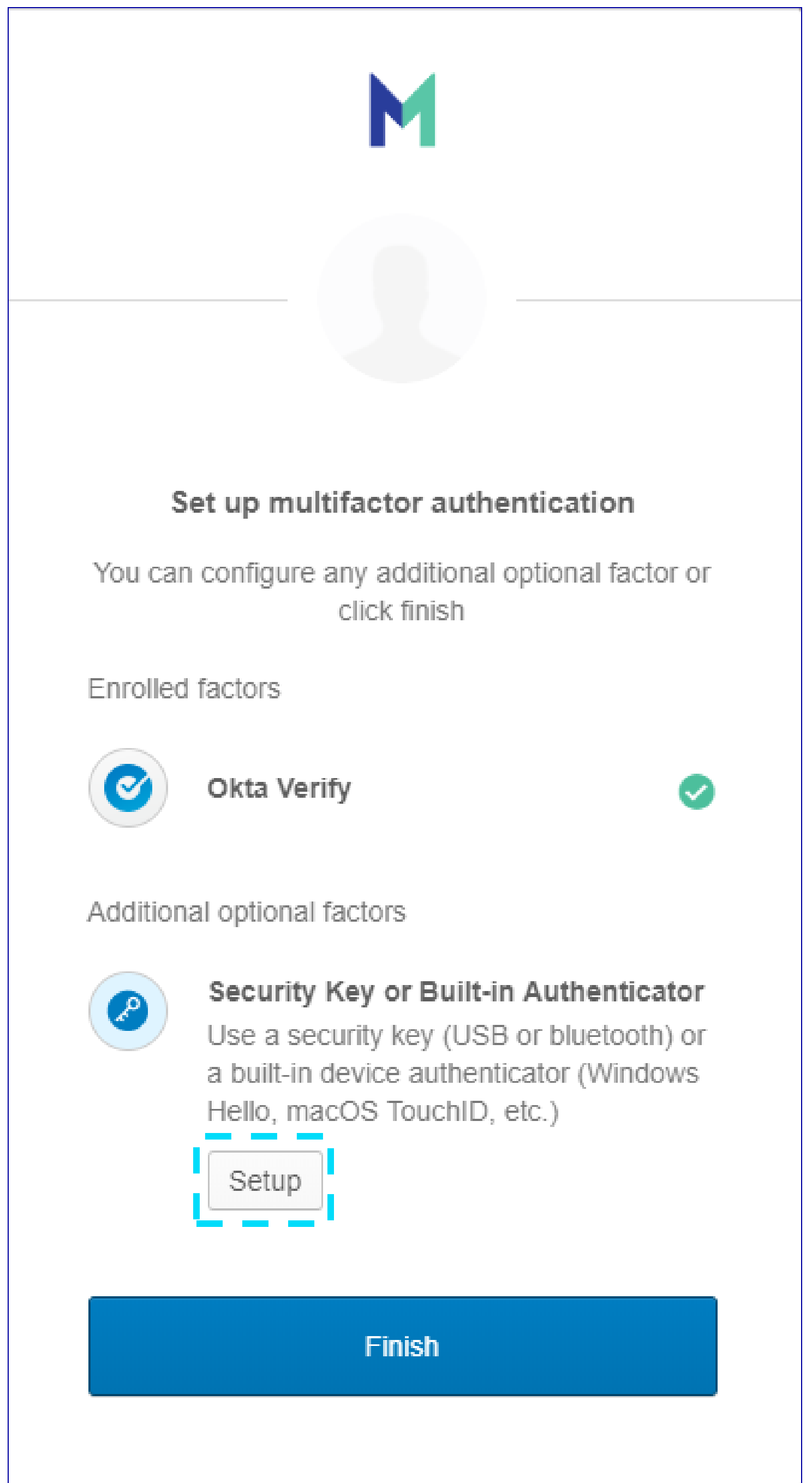
Remember me

Sign In

Need help signing in?

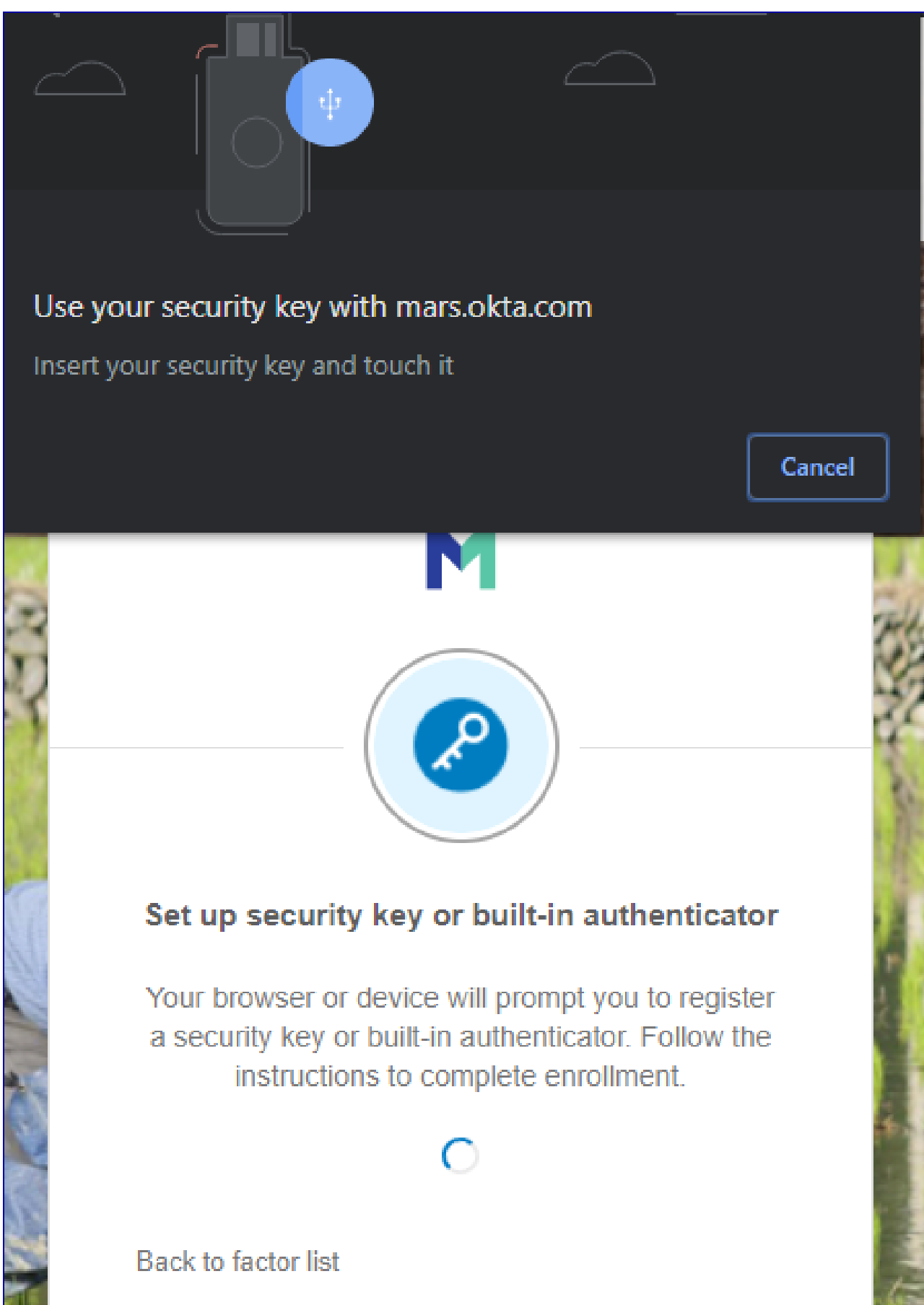
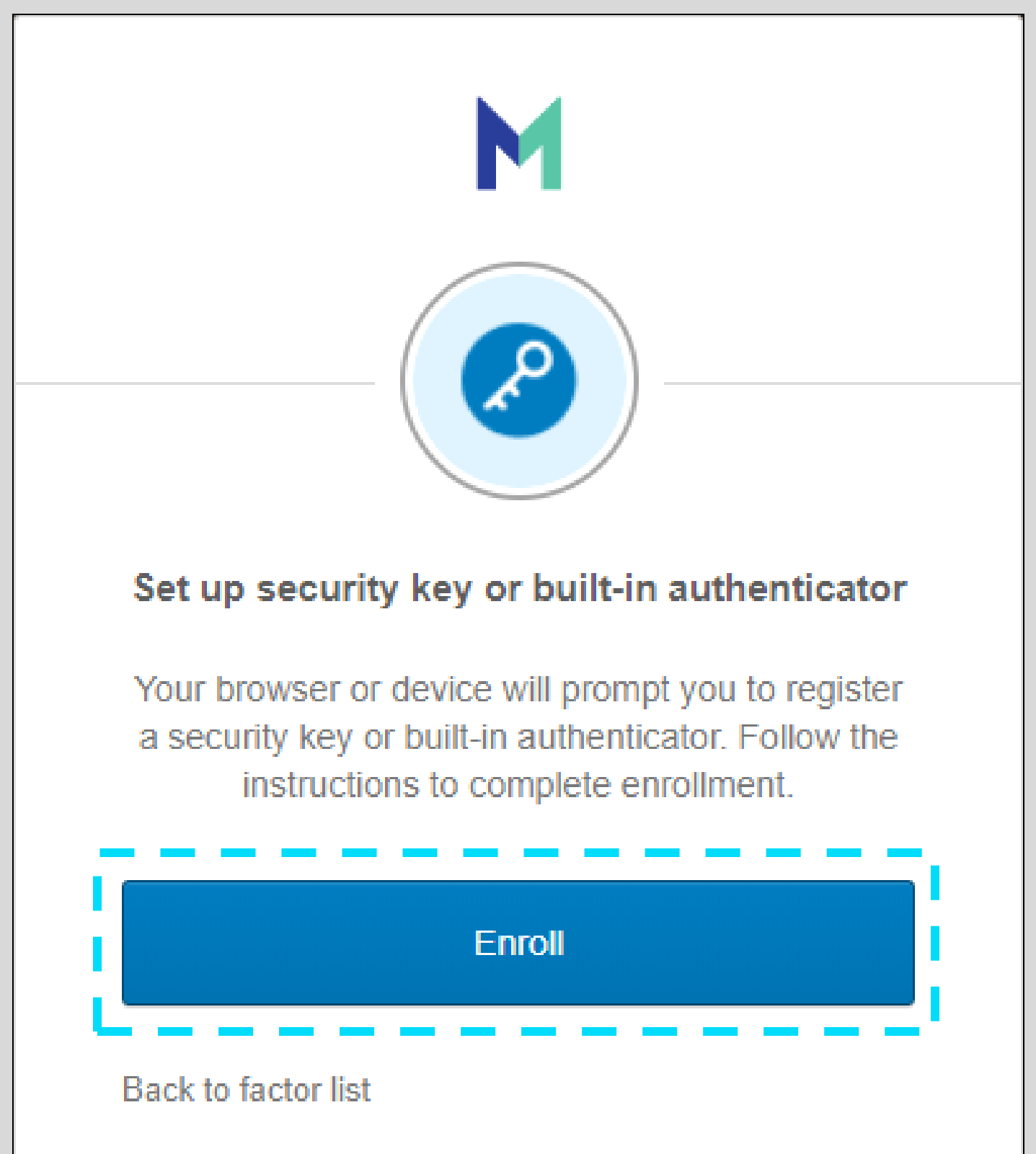
3

Click **Setup** under Security Key or built-in biometric authenticator (Touch ID/Face ID etc)



4

After clicking **setup**, click **enroll** on the next screen.

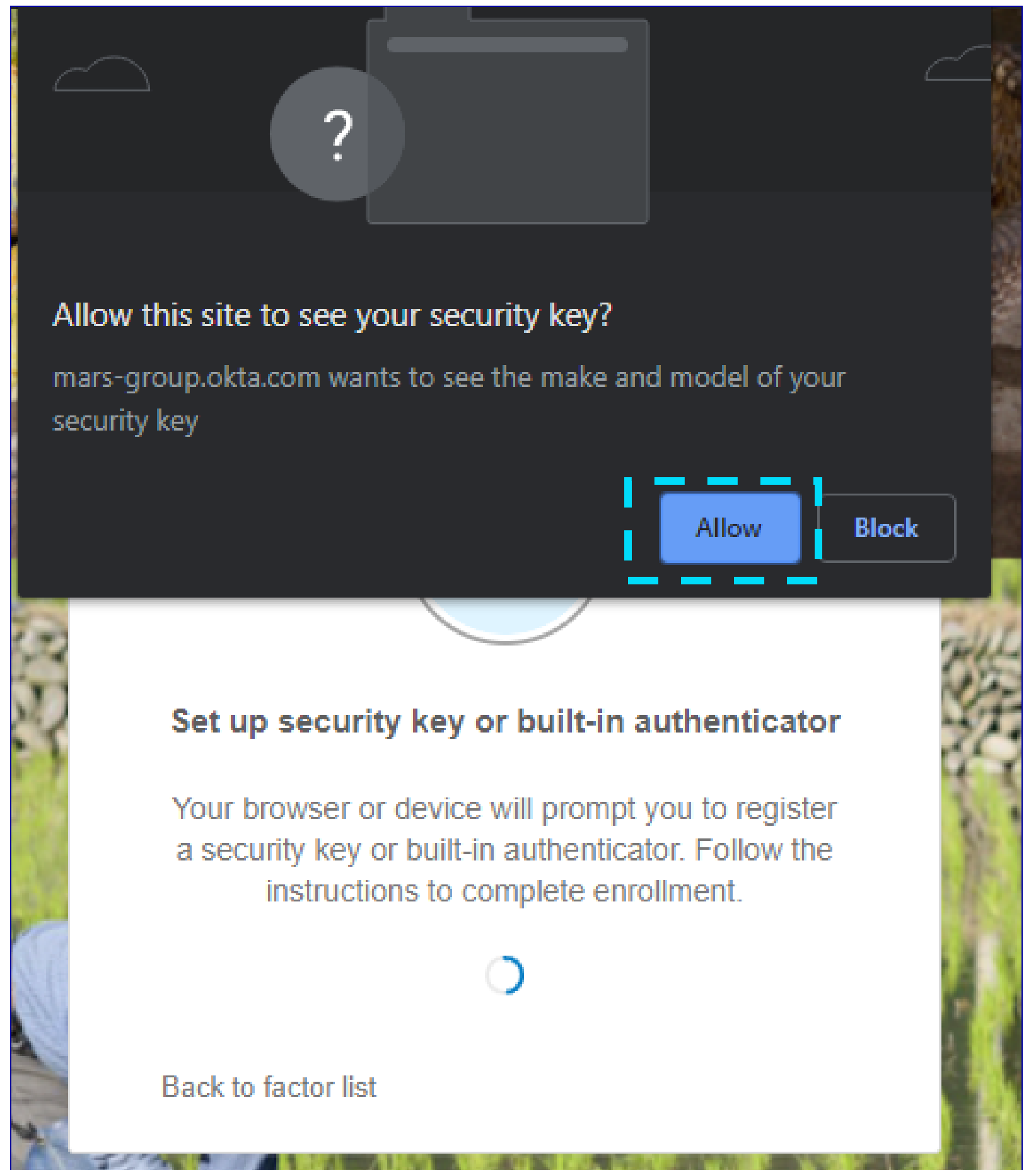


5

You will receive this prompt (see image). Please **insert your Yubikey and touch the metal part** while receiving this prompt.

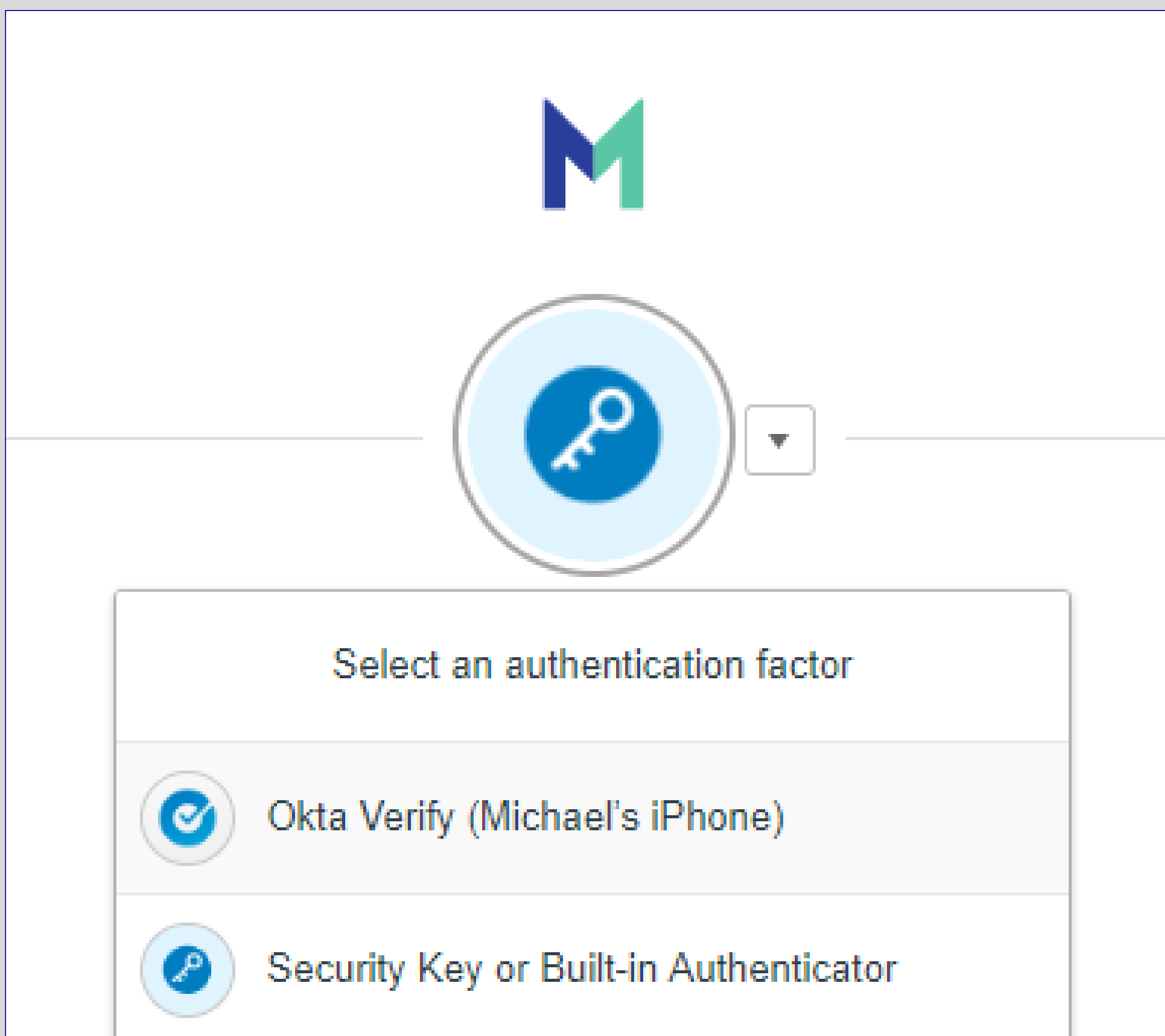
6

If done correctly you receive this message (see image),
Click **allow** to finish your set-up.



7

After configuring multiple authentication factors, click the **drop down** (see image) **to change authentication factor**.



PLEASE NOTE:

- If you are pre-enrolling in Okta, the message below is expected. You will not see applications in the Okta Dashboard until after go-live.

Thank you for helping us keeping Mars
#SecureTogether

For more information contact bedrock@effem.com