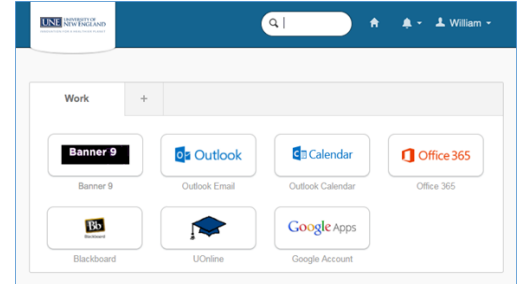


USING OKTA MULTIFACTOR AUTHENTICATION

[Version 2.0 - Updated 07.09.2021]

UNE will begin using Multifactor Authentication (MFA) which requires a secondary verification after your password, either through the OKTA Verify app or SMS/Text messages. This increased security helps to protect your account and UNE.

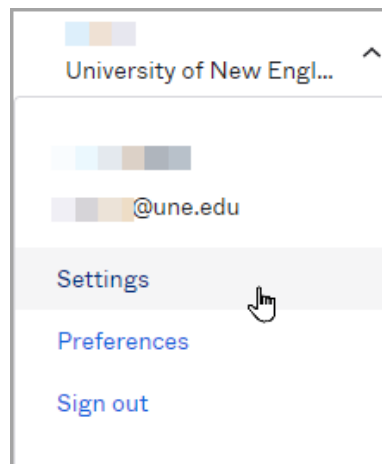


SETTING UP MULTIFACTOR AUTHENTICATION

Starting on your desktop, go to <https://okta.une.edu>

NOTE: The "https://" is required. If you do not include it, you will be redirected to <https://une.okta.com>. This is by design.

After entering your password, go to your settings in the top right corner of the screen.



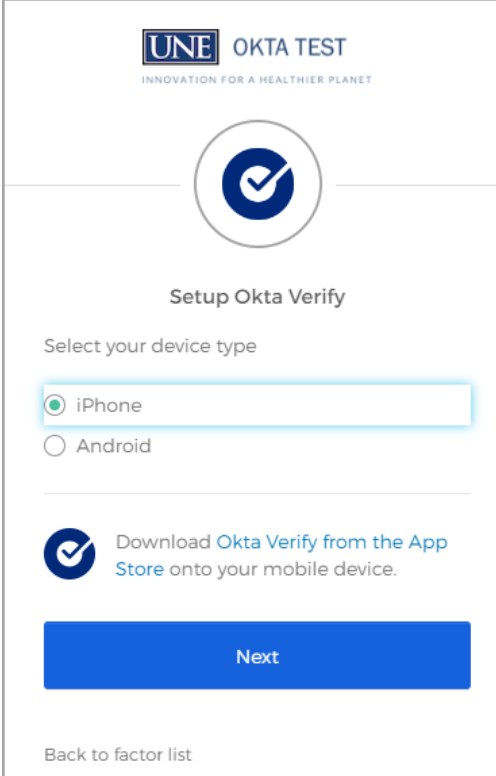
At the bottom right of the settings pages, you will find your Extra Verification options.

- Depending on how recently you logged in and your IP address, you may see Edit Profile button that you must click before editing your Extra Verification. This is normal.

Follow the steps below for either OKTA Verify (recommended) or SMS/Text messaging.

OKTA VERIFY

If you click Setup under OKTA Verify, you will be asked to specify your phone's operating platform & then prompted to download the app from the platform's app store.



- Download the OKTA Verify app from your app store
- Click through the app's initial set up screens
- Choose Organization as Account Type
- After you've reach the QR code screen on the app
 - click **Next** on your desktop to display the QR code
 - click **Yes, Ready to Scan** on the app on your phone
 - Scan the QR code on your screen with your phone
- When asked if you will allow the app to send notifications, we recommend you select **Allow** – these notifications are time sensitive for your login, so it is fastest and simplest to receive a notification.

Do You Have Your QR Code?



Before you continue, make sure your QR code is shown on another device, such as a laptop

Where do I get my QR code?

Yes, Ready to Scan

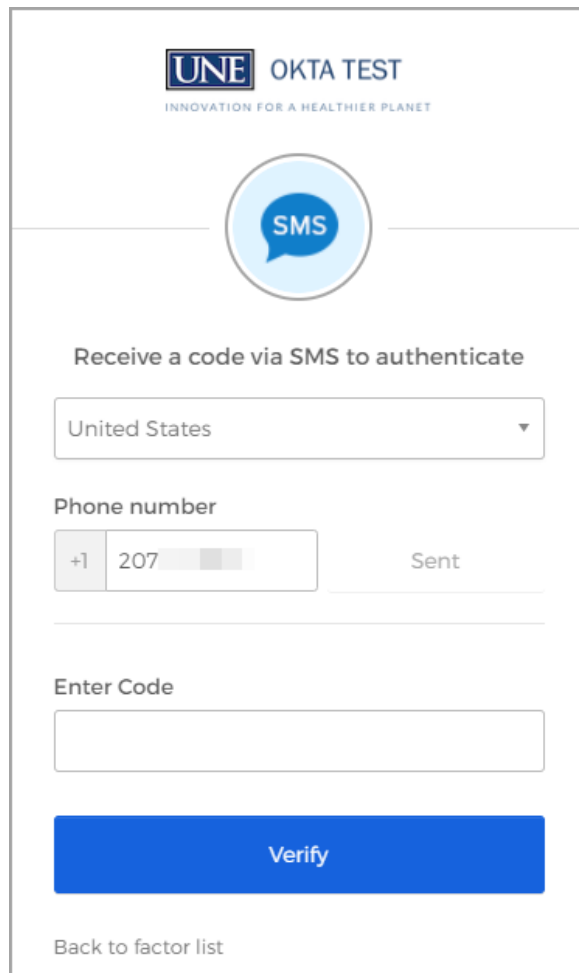
No, Sign In Instead

SMS/TEXT AUTHENTICATION

If you choose to authenticate through SMS/Text, you will need to be sent a code every time you need to log in. Please note, if you set up SMS first, you may opt to set up OKTA Verify as an additional option. The reverse is not true.

To set it up:

- Click **Setup** under the SMS option
- Enter your phone number (and adjust country, if needed)
- Click **Send Code** (the button will change to say Sent and gray out)
- Enter the 6-digit code texted to your phone
- Click **Verify**



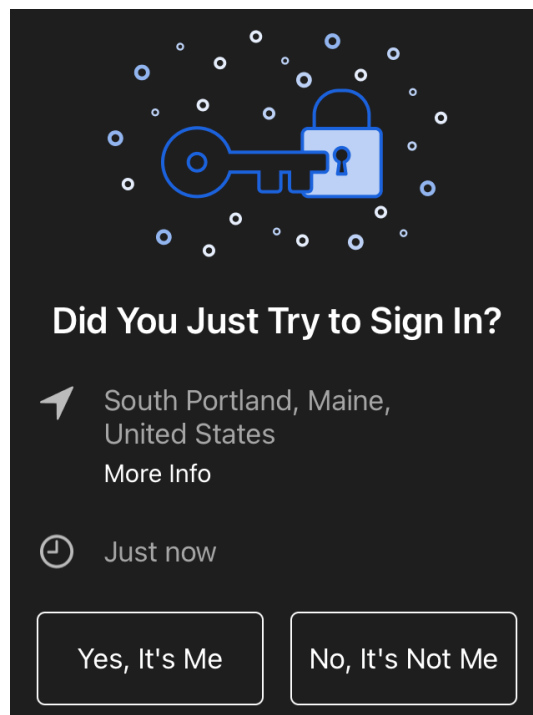
The screenshot shows the OKTA TEST interface for SMS authentication. At the top, it displays the UNE logo and the text "OKTA TEST" and "INNOVATION FOR A HEALTHIER PLANET". Below this is a circular icon with "SMS" inside. The main heading is "Receive a code via SMS to authenticate". There is a dropdown menu for the country, currently set to "United States". Below that is a "Phone number" field with a country code dropdown set to "+1" and a text input field containing "207" followed by three grayed-out boxes. To the right of the phone number field is a "Sent" button. Below the phone number field is an "Enter Code" label and a large empty text input field. At the bottom is a large blue "Verify" button and a link that says "Back to factor list".

LOGGING IN WITH MFA

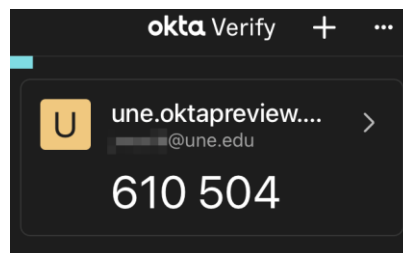
Once you've set up your Multifactor Authentication, you will go through the process you've chosen each time you login. After entering your password, you'll see the steps below (according to the verification used).

OKTA VERIFY

When logging in using OKTA Verify, you will receive a notification from the app when you sign in.

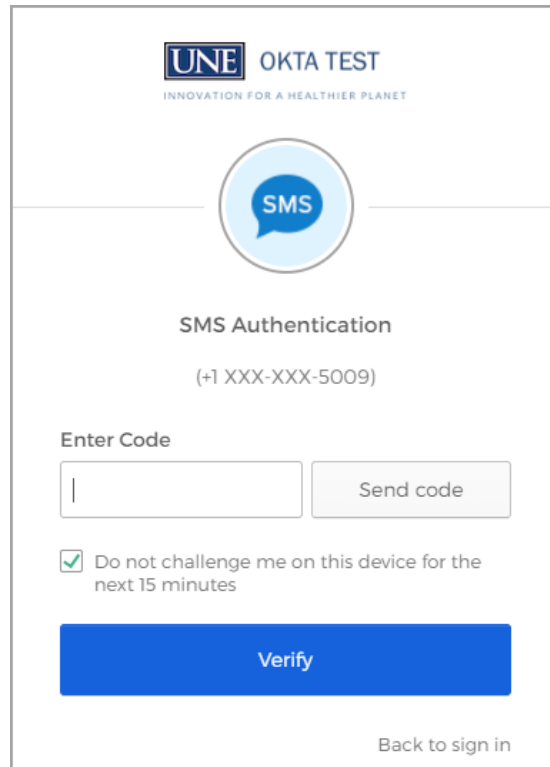


If OKTA Verify is already open and past the **Yes, It's Me** screen, you may also use a code shown within the app that changes every 30 seconds. The amount of time lapsed is shown in a blue bar across the top of the screen.



SMS/TEXT AUTHENTICATION

After you have set up your SMS/Text authentication, you will need to click Send Code and enter the code from the verification text each time you sign in.



The screenshot shows the OKTA TEST SMS Authentication interface. At the top, it features the UNE logo and the text "OKTA TEST" and "INNOVATION FOR A HEALTHIER PLANET". Below this is a circular icon with a speech bubble containing the letters "SMS". The main heading is "SMS Authentication" followed by the phone number "(+1 XXX-XXX-5009)". There is a section labeled "Enter Code" with a text input field containing a vertical bar and a "Send code" button. Below the input field is a checked checkbox with the text "Do not challenge me on this device for the next 15 minutes". At the bottom of the form is a large blue "Verify" button and a link that says "Back to sign in".