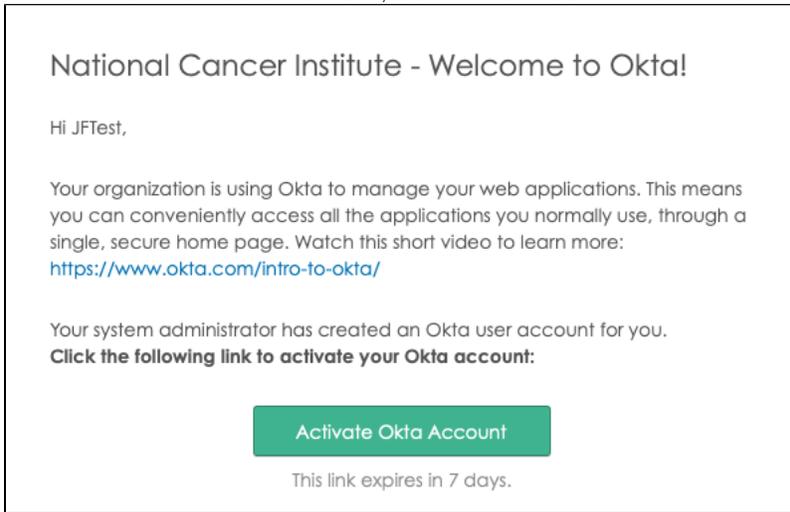


Okta account Creation - Include 20210107

Creating your Okta account:

1. In the email notification received from Okta, select the "Activate Okta Account" button. This will launch the Okta account creation page.



2. On the Create your National Cancer Institute - Prod account page, follow the steps to create a password and choose a security image. Select the "Create My Account" button.

Welcome to National Cancer Institute - Prod, JFTest!
Create your National Cancer Institute - Prod account



Enter new password

Password requirements:

- At least 8 characters
- A lowercase letter
- An uppercase letter
- A number
- A symbol
- No parts of your username
- Does not include your first name
- Does not include your last name
- Your password cannot be any of your last 6 passwords
- At least 1 day(s) must have elapsed since you last changed your password

Repeat new password



Click a picture to choose a security image

Your security image gives you additional assurance that you are logging into Okta, and not a fraudulent website.



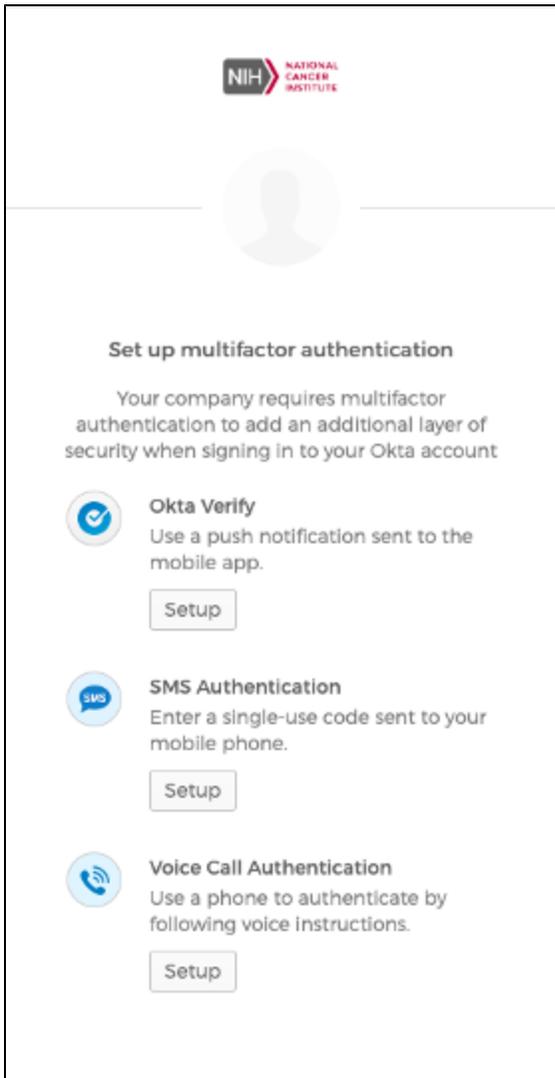
Create My Account

3. The Okta "Set up multifactor authentication" window launches next displaying the three multifactor authentication methods available:

Okta Verify - "Use a push notification sent to the mobile app."

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

Voice Call Authentication - "Use a phone to authenticate by following voice instructions."



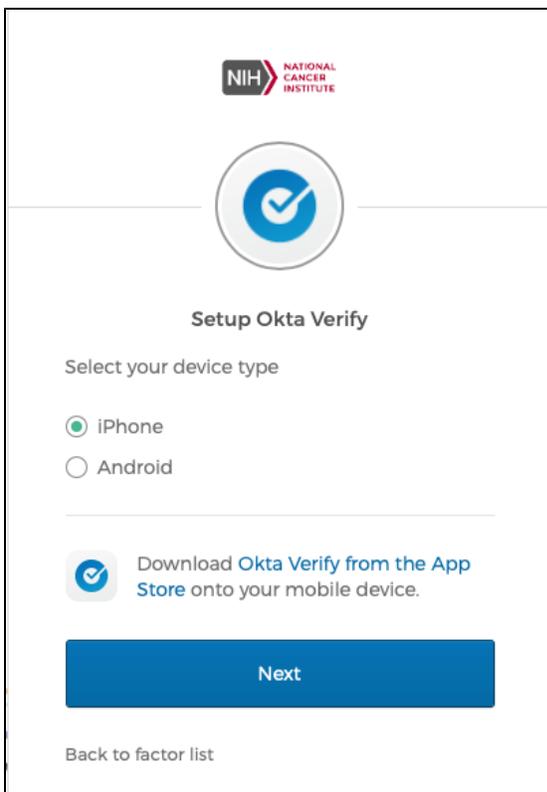
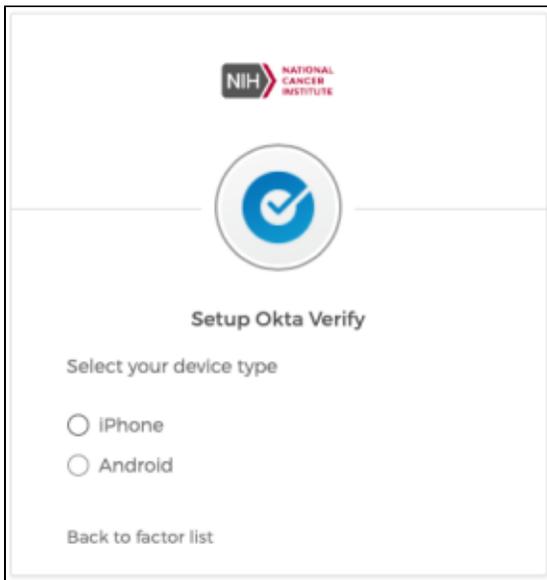
4. Choose "Setup" on the desired authentication method.

Setting up Okta multifactor authentication:

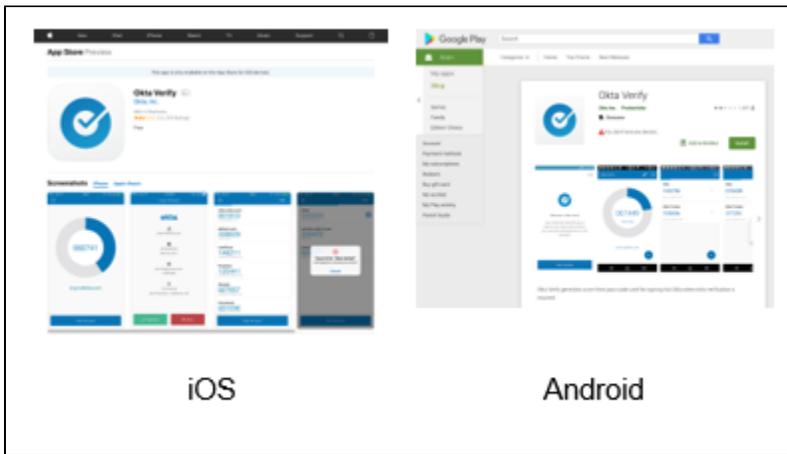
The following sections define the different Okta multifactor authentication methods available. A user account can use any/all of these methods. Please see the section titled "Two Factor Option: Multiple Methods" for additional information on using multiple multifactor authentication methods.

Two Factor Method: Okta Verify

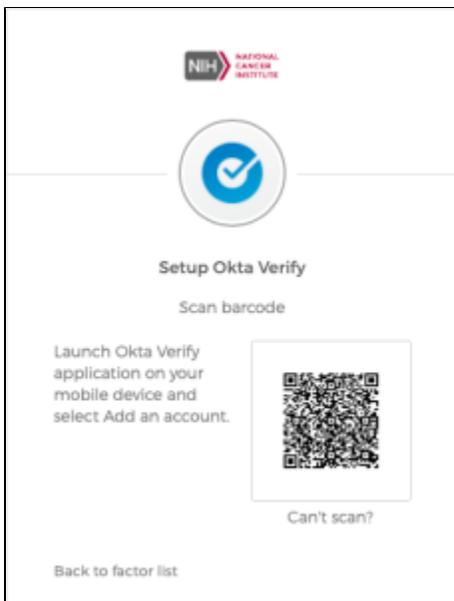
1. On the "Setup Okta Verify" window, select the brand of mobile phone being used and select "Next". You will then be prompted by Okta to download the Okta Verify app. (Select "Back to factor list" to choose a different authentication method).



2. Okta will display a notification to download the Okta Verify app from the manufacturers App Store. Download the app on the mobile phone to continue configuring Okta Verify.



3. Once the Okta Verify app is downloaded on the mobile device, select "Next" in Okta, and tap on the "Add Account" button in the Okta Verify mobile app. (If asked, allow the app to access your mobile phone camera and allow it to send push notifications).
4. The Okta Verify app will open a camera screen, and your computer screen will display a QR code (square-shaped barcode).



5. Capture the QR code with your mobile phone.
6. The Okta Verify app will scan the QR code and connect the mobile phone to your Okta account. An "Account Added" confirmation will display in Okta, and a new entry in the "Connections" tab will be added in the Okta Verify app.
7. Okta will return to the "Set up multifactor authentication" page.
8. Select "Finish", or continue to setup additional multifactor authentication methods if desired.

NIH NATIONAL CANCER INSTITUTE

Set up multifactor authentication

You can configure any additional optional factor or click finish

Enrolled factors

Okta Verify

Additional optional factors

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

Voice Call Authentication
Use a phone to authenticate by following voice instructions.

Any subsequent logins to Okta will use a "push" to authenticate. Please take note of the following steps:

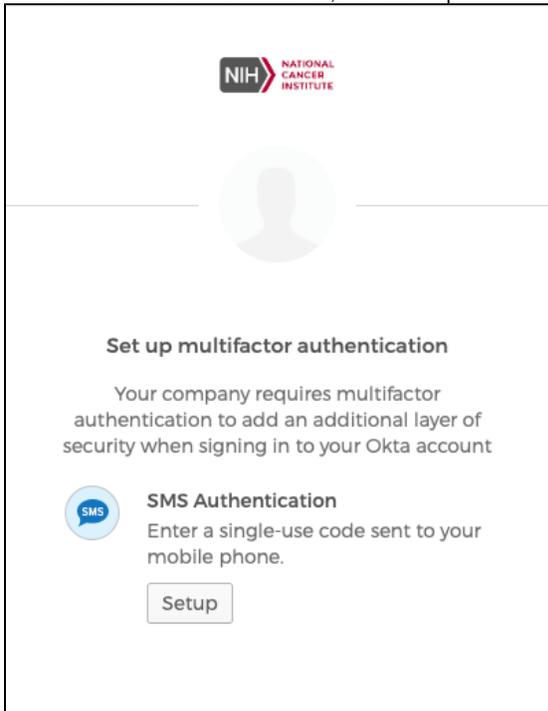
Upon entering a username and password, a window for Okta Verify with a button to "Send Push" will be displayed. Selecting "Send Push" will send an alert to the Okta Verify app on the mobile device configured with the Okta account to approve the login request.

In the Okta Verify app, tap on the "Approve" button to authenticate.

Following the authentication, the application will load.

Two-Factor Method: SMS Authentication

1. On the "SMS Authentication" window, select "Setup".



NIH NATIONAL
CANCER
INSTITUTE

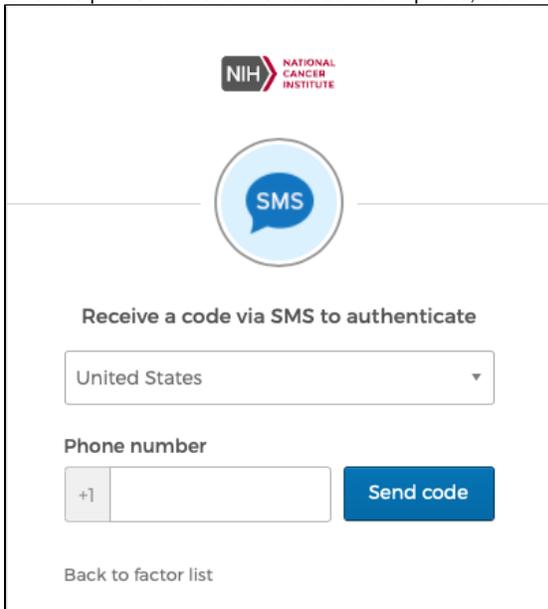
Set up multifactor authentication

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

2. Use the dropdown picklist to choose the country of your location (United States is selected by default). The choice of country automatically populates the appropriate country code prefix for the Phone number text box. (Select "Back to factor list" to choose a different authentication method).
3. Enter the phone number of the desired mobile phone, select "Send code".



NIH NATIONAL
CANCER
INSTITUTE

SMS

Receive a code via SMS to authenticate

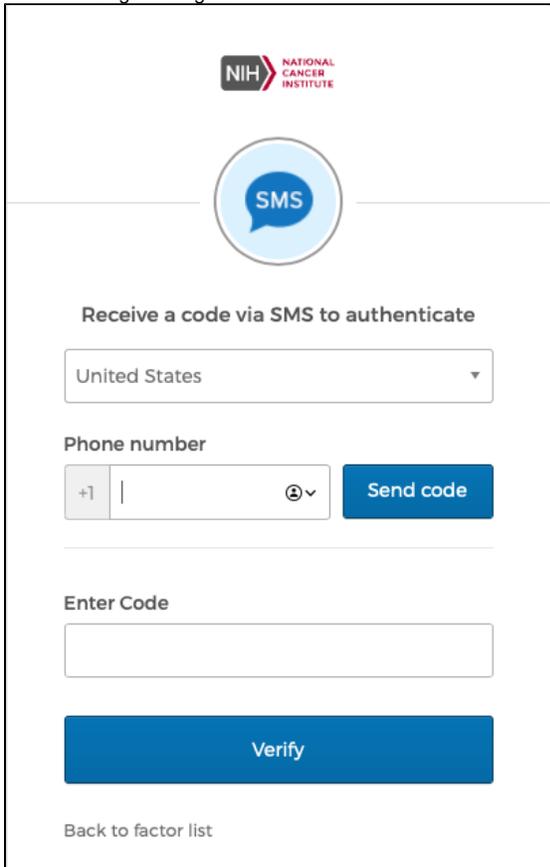
United States

Phone number

+1 Send code

[Back to factor list](#)

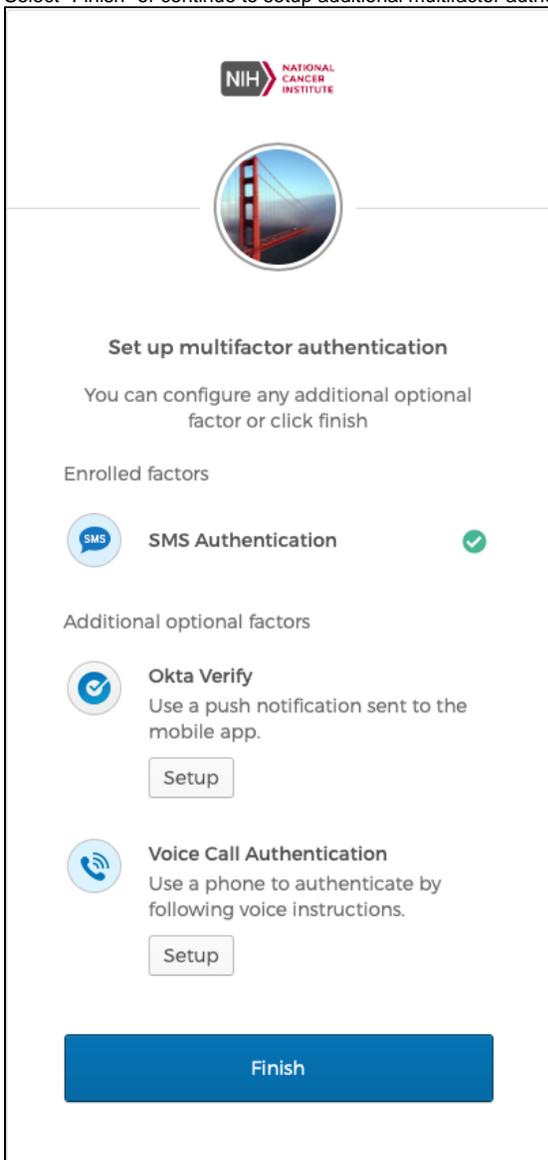
4. A text message stating "Your verification code is xxxxxx." will be sent to the phone number provided.



The screenshot shows the NIH National Cancer Institute SMS authentication interface. At the top is the NIH logo. Below it is a blue circular icon with a white speech bubble containing the text "SMS". 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 the "Phone number" section, which includes a field for the country code (pre-filled with "+1"), a field for the phone number, a dropdown for the area code (pre-filled with a circled plus sign), and a blue "Send code" button. Below the phone number section is the "Enter Code" section, which has a large empty text input field. At the bottom of the form is a large blue "Verify" button. A link labeled "Back to factor list" is located at the very bottom of the page.

5. Enter the code in the "Enter Code" textbox and select "Verify".

6. Select "Finish" or continue to setup additional multifactor authentication methods if desired.



Any subsequent logins to Okta will use SMS Authentication to authenticate. An SMS Authentication window will appear asking to approve the sending of a text message to the number provided (With the exception of the last 4 digits, the number will be masked).

Two Factor Method: Voice Call Authentication

1. On the "Follow phone call instructions to authenticate" window, choose the country of your location (United States is selected by default). The choice of country automatically populates the appropriate country code prefix for the "Phone number" text box. (Select "Back to factor list" to choose a different authentication method).



Follow phone call instructions to
authenticate

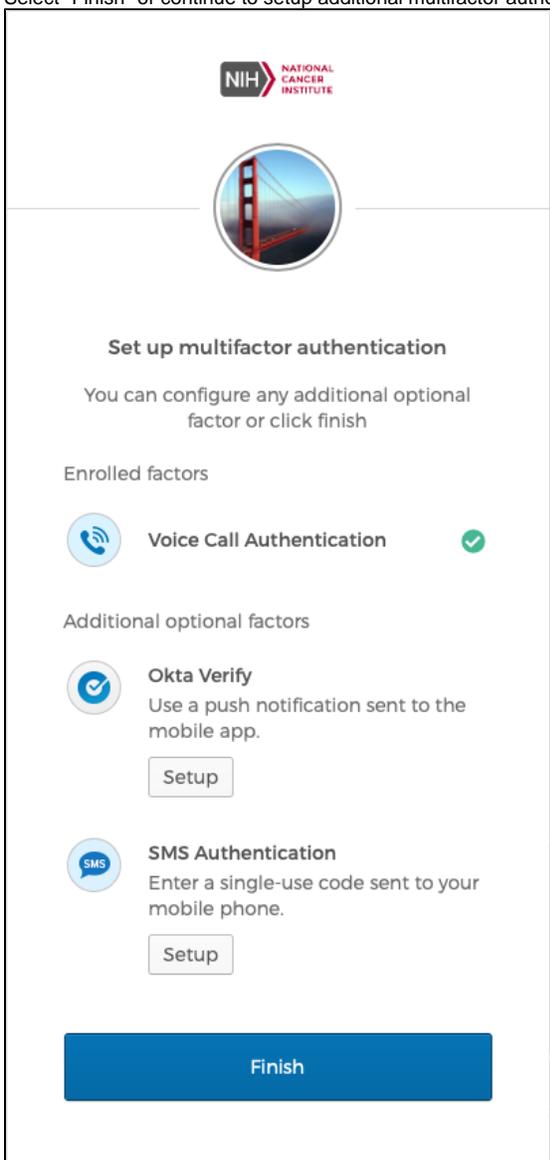
Phone number

Extension

[Back to factor list](#)

2. Enter the phone number and extension (if applicable), select "Call".
3. A phone call will be initiated to the phone number provided with a recorded message.
4. Enter the code given and click the "Verify" button.

5. Select "Finish" or continue to setup additional multifactor authentication methods if desired.



Any subsequent logins to Okta will use Voice Call Authentication to authenticate. A Voice Call window will appear asking to approve a phone call to the number provided (With the exception of the last 4 digits, the number will be masked).

Two-Factor : Multiple Methods

It is possible to set up more than one of the authentication methods. While only one method is needed for each login, and each type of authentication may only be associated with one phone number, this configuration allows some flexibility for users who want the option of using two different phone numbers.

Here are some examples of how this might be used:

- Okta Verify Authentication (mobile phone), Voice Call Authentication (office phone).

User sets up Okta Verify authentication to send push notifications to their mobile phone, and sets up Voice Call Authentication to their office phone number. If the user does not have mobile service in their office, they can use their office phone to authenticate, and they can authenticate via Okta Verify push on their mobile phone if they are away from their office.

- SMS Authentication (personal mobile phone), Okta Verify Authentication (work mobile phone).

User sets up Okta Verify Authentication to send push notifications to their company-issued mobile phone, and sets up SMS Authentication to their personal mobile phone. The user does not wish to install an app on their personal mobile phone, but would like to have a backup method of authentication in case of any changes to their work mobile phone number.

- Okta Verify Authentication (mobile phone), SMS Authentication (mobile phone), Voice Call Authentication (office phone).

User wishes to have several methods for authentication, especially since their day-to-day schedule is extremely varied. This allows the user to choose the method that best suits their situation at login time.

1. Determine the configuration that best fits your situation and decide which of the authentication method(s) that you want to use, and which phone number you want to use with each.
2. When the Okta "Set up multifactor authentication" window launches, configure the desired multifactor authentication per the instructions above.
3. The next time you log into the application, one of the authentication methods will be selected by default, but you may choose another method you have set up. Click on the down-arrow icon next to the Okta symbol in the window and choose a different authentication method from the picklist.

