

Multifactor Authentication Set-up Instructions

New York State has started using Multi-Factor Authentication (MFA) on some of its public-facing applications.

MFA is a way to help ensure the safety and security of your account. It requires a second factor of proving that you are who you say you are, beyond just a password. If you are using an MFA-protected application, even if someone were to guess or steal your password, they still would not be able to log in without your second factor. While a password is something that you know, the second factor is something that you are (usually read by a biometric device) or something that you have.

This document is intended to assist with helping assist customers with setting up their Multifactor Authentication on their NY.gov account.

INDEX

[Google Authenticator](#)

[Okta Verify](#)

[SMS Verify](#)

[Voice Call Authentication](#)

Setting up Google Authenticator Multifactor Authentication

If you are not yet enrolled in MFA, you will be prompted to enroll after logging into Labor Online Services and clicking on the “Unemployment Services” application button.

On your computer screen, you will see a screen that asks you to set up your Multifactor Authentication.

- On your smartphone, download the Google Authenticator app. See below for instructions for downloading the app.
- On your computer screen, click **Setup** under Google Authenticator to begin the setup process.
- Choose either iPhone or Android depending on your device.
 - You will be instructed to download the Google Authenticator app from the Google Play Store (Android) or the App Store (iPhone). If you have not already, you should download this app now. See below for instructions on downloading the app.

TIP: If you have an Apple tablet, choose iPhone.

- Click the **Next** button.
- **Use the following directions for downloading the Google Authenticator app onto an Android Device (Google Play) or an Apple Device (App Store).**
- On your smartphone or tablet, navigate to Google Play (Android) or the App Store (Apple Device). Make sure your smartphone or tablet is running the latest version of the operating system (OS).
- In Google Play (Android) or the App Store (Apple Device), search for the Google Authenticator app.
- Select the Google Authenticator app.
- Download and install the app.
- Once you have installed the Google Authenticator app on your smartphone or tablet, navigate to the app on your device and open it. (*NOTE: App may appear slightly different depending on version of phone*)
- **Use the following directions to use the Google Authenticator App on your smartphone or tablet.**
- After choosing Apple Device or Android on your computer screen, your computer screen will show a dialog box with a Quick Response (QR) code in it. The QR code will appear as a square filled with black dots.

- If you are unable to scan the QR code into your smartphone or tablet, click the **Can't Scan?** option under the QR code on your computer screen.
- If you are able to scan the QR code on your smartphone or tablet, navigate to your Google Authenticator App and open it, if it is not open already.
- Click **Get Started**.
- You will be given the option to either **Scan a QR** code or **Enter a setup key**. Choose one.
 - TIP: If you cannot scan the code, select **Enter a setup key**. See below for the Enter a Setup Key directions.
- If you have an Android phone, the app will ask for permission to use your camera. Click "While Using the App".
- If you have an Apple Device, you will see a message that *"Authenticator" Would Like to Access the Camera*. Click OK.
- After giving your phone permission to use the camera, your smartphone's screen will show a blank screen with a square in the center.
- Point your smartphone or tablet's camera at the QR code that's on your computer screen, so that the QR code on the computer screen appears in the green box on your smartphone's screen. The app will automatically scan the code into your phone or tablet.
- **Use the following directions if you selected Enter a Setup Key in the app instead of Scan a QR code.**
- On your computer screen, you will be shown a Secret Key. This is the code you will enter in the Google Authenticator app. You will be shown a screen that contains Instructions for Enter a Setup Key.
- On your Google Authenticator app, you will see a screen to Enter Account Details. On this screen, enter the following information:
 - Your NY.gov account name in the 'Account name' field.
 - Your Secret Key in the 'Your Key' field.
 - Select 'Time-Based' from the Type of Key dropdown.
- Click the **Add** button.
- **Use the following directions to enter the code from your Google Authenticator app into your computer.**
- Once the app has either successfully scanned the QR code or you have successfully entered the Secret Key into the app, the app will show you a screen with your username and a six-digit code. This is the code you will enter in the computer in the next steps. This code will change every 30 seconds.

- Type the six-digit code from your app into the Enter Code field on your computer screen and click **Verify**.
- You will be redirected back to the enroll screen where you can set up another Multifactor Authentication method. Notice that Google Authenticator is now under the Enrolled factors heading.
 - TIP: It is recommended that you set up more than one multifactor authentication method.
- When you have set up all the Multifactor Authentication methods that you want, click the **Finish** button.
 - TIP: If you will be setting up a multifactor authentication method that uses a phone app, download the apps before you click the **Setup** button on the “Set up multifactor authentication” browser page. The two multifactor authentication methods that use apps are Okta Verify and Google Authenticator.

Potential Error Messages and How to Resolve Them.

- Error Message: Session has expired.
- Remedy: Customer must sign in again.

- Error Message: Token Doesn't Match.
- Remedy:
 - Customer should check accuracy.
 - Customer should “Send” code again.

- Error Message: Found Error.
- Remedy: Customer must input code.

- Error Message: Barcode doesn't scan.
- Remedy:
 - Try Alternative methods given.
 - “Send Activation by SMS” – Customer can input a phone number.
 - “Setup manually without push” – Customer will see a temporary code.

- “Send activation email” – Customer will be sent an email to the email account used in creation of their account.
- Ensure customer’s device “allowed” access to camera

[Return to Main Page](#)

Setting up Okta Verify Multifactor Authentication

On your computer screen, you will see a screen that asks you to set up your Multifactor Authentication.

- On your smartphone, download the Okta Verify app. See below for instructions for downloading the app.
- On your computer screen, click **Setup** under Okta Verify to begin the setup process.
- Choose either iPhone or Android depending on your device.
 - You will be instructed to download the Okta Verify app from the Google Play Store (Android) or the App Store (iPhone). If you have not already, you should download this app now. See below for instructions on downloading the app.

TIP: If you have an Apple tablet, choose iPhone.

- Click the **Next** button.
- **Use the following directions for downloading the Okta Verify app onto an Android Device (Google Play) or Apple Device (the App Store)**
- On your smartphone or tablet, navigate to Google Play (Android) or the App Store (Apple Device). Make sure your smartphone or tablet is running latest version of the Operating System (OS).
- In Google Play or the App Store, search for the Okta Verify app.
- Select the Okta Verify mobile app.
- Download and install the app.
- Once you have installed the Okta Verify app on your smartphone or tablet, navigate to the app on your device and open it.
- **Use the following directions to set up the Okta Verify App on your smartphone or tablet.**
- Your computer screen will now show a dialog box with a Quick Response (QR) code in it. The QR code will appear as a square filled with black dots.
 - If you are unable to scan the QR code, click the **Can’t Scan?** option under the QR code on your computer screen. See below for directions for setting up Okta Verify after clicking on Can’t Scan.

- If you are able to scan the QR code, navigate to the Okta Verify app on your device and open the app.
- Click **Get Started**.
- Click **Next**.
- Click **Add Account**.
- Click **Other**.
- You will be given the option to either **Scan a QR** code or **Enter Key Manually**. Choose one.
 - If you choose **Enter Key Manually**, you will need to follow the steps below for Verify Manually Without Push Notification from the Can't Scan dropdown list below.
- **Use the following directions for using the Okta Verify app to scan a QR code.**
- If you have an Android device, the app will ask for permission to use your camera. Click OK.
- If you have an Apple Device, you will see a message that *“Okta Verify” Would Like to Access the Camera*. Click OK.
- Point your smartphone or tablet’s camera at the QR code that’s on your computer screen. The app will automatically scan the code into your phone or tablet.
- On your computer monitor, you will see the enroll screen with a pop up with a QR code.
- In the Okta Verify app, tap **Add Account**.
- Point your smartphone or tablet’s camera at the QR code on your computer monitor.
- After you scan the QR code, a new screen will appear on your app asking you Allow Push Notifications? Choose either **Allow** or **Skip**.
- After successfully scanning the QR code into your smartphone, your computer screen will indicate you have successfully scanned the code.
- **Use the following directions to set up Okta Verify via email or SMS after clicking on Can’t Scan.**
- After clicking on **Can’t Scan** on your computer screen, you will see a screen that says Setup Okta Verify. On this screen, there is a dropdown list that offers the following options: Send activation link via email, Send activation link via SMS, and Setup Manually Without Push Notification.
 - TIP: The Setup Manually Without Push Notification directions follow below.
- Click on **Send activation link via email** or **Send activation link via SMS**. You will be sent a link.

TIP: You **must** click the link from your smartphone or tablet.

- On your smartphone or tablet, navigate to your email or text message app to access the link. Open the email or text message you have been sent. Click on the link contained in the message.
- You will be taken to the Okta Verify website.
- Click on **Get Started**.
- Your smartphone will connect to the Okta Verify website and verify the link. Your computer screen will indicate you have successfully scanned the code.
- **Use the following directions to set up Okta Verify via Manually Without Push Notification from the Can't Scan dropdown list.**
- After clicking on **Can't Scan** on your computer screen, you will see a screen that says Setup Okta Verify. On this screen, there is a dropdown list that offers the following options: Send activation link via email, Send activation link via SMS, and Setup Manually Without Push Notification.
- Choose the option: Verify manually without push notification.
- You will be taken to a screen that contains a Secret Key.
- Open your Okta Verify app.
- Click **Get Started**.
- Click **Next**.
- Click **Add Account**.
- Click **Other**.
- Choose Enter Key Manually.
- Enter the code on your computer screen into your smartphone screen. On your smartphone, you will enter an Account Name (created by you) and the Secret Key that is showing on your computer screen.
- Click **Add Account**.
 - After the code has been verified, your computer screen will indicate you have successfully scanned the code.
- Click **Done**.
- **Use the following directions after you have successfully scanned a QR code or manually verified the code with your app.**
- Once the QR code has been scanned, the app will change to a screen with a six-digit code. This code will change every 30 seconds.

- After successfully setting up your Okta Verify app, your computer screen will show the Enroll screen where you can set up another Multifactor Authentication method. The screen will now show that Okta Verify is under the Enrolled factors heading.
- When you have set up all the Multifactor Authentication methods that you want, click the Finish button.

TIP: If you will be setting up a multifactor authentication method that uses a phone app, download the apps before you click the **Setup** button on the “Set up multifactor authentication” browser page. The two multifactor authentication methods that use apps are Okta Verify and Google Authenticator.

Potential Error Messages and How to Resolve Them.

- Error Message: Session has expired.
- Remedy: Customer must sign in again.

- Error Message: Token Doesn't Match.
- Remedy:
 - Customer should check accuracy.
 - Customer should “Send” code again.

- Error Message: Found Error
- Remedy: Customer must input code.

- Error Message: Barcode doesn't scan.
- Remedy
 - Try Alternative methods given.
 - “Send Activation by SMS” – Customer can input a phone number.
 - “Setup manually without push” – Customer will see a temporary code.
 - “Send activation email” – Customer will be sent an email to the email account used in creation of their account.
 - Ensure customer's device “allowed” access to camera.

[Return to Main Page](#)

SMS Verify

On your computer screen, you should see a screen that asks you to set up your Multifactor Authentication.

- Click Setup under SMS Authentication.
- You will be asked to enter a phone number.
TIP: This phone number must be capable of receiving text messages.
- After you enter your phone number, click **Send code**.
- You will receive a text message with a code in it. Enter this code into the Enter Code box.
- Press **Verify**.
- You will be redirected back to the Multifactor Authentication enrollment screen. Notice that SMS Authentication is now under the Enrolled factors heading.
- It is recommended that you set up more than one multifactor authentication method.
- When you have set up all the Multifactor Authentication methods that you want, click the **Finish** button.

[Return to Main Page](#)

Voice Call Authentication

On your computer screen, you should see a screen that asks you to set up your Multifactor Authentication.

- Click Setup under Voice Call Authentication.
- You will be asked to enter a phone number.
- After you enter your phone number, click **Call**.
- You will receive a phone call. When you answer the call, a recorded voice will read a five-digit number to you.
TIP: The number will only be repeated once. Be sure to have a pen and paper ready to record the number.
- Enter this code into the Enter Code box.
- Press **Verify**.
- You will be redirected back to the Multifactor Authentication enrollment screen. Notice that Voice Call Authentication is now under the Enrolled factors heading.
- It is recommended that you set up more than one multifactor authentication method.

WE ARE YOUR DOL



- When you have set up all the Multifactor Authentication methods that you want, click the Finish button.

[Return to Main Page](#)