Multi-Factor Authentication for the Integrated Justice Portal

New York State has implemented Multi-Factor Authentication (MFA) on most of its browser/web-based applications. MFA will be implemented for the Integrated Justice (IJ) Portal on October 16, 2023.

Contents

What is MFA and why is it important?

- MFA helps ensure the safety and security of your account, by requiring 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 possess (a device to which a one-time code will be sent).

How will MFA work on the IJ Portal?

Internet Access

For users that access the IJ Portal from the internet (coming from outside the state network), most will have a smartphone, which supports choosing from the following four factors:

- Okta Verify app (IOS/Android/Windows) – provides push notifications and single-use codes
- Google Authenticator app (IOS/Android) – provides single-use codes
- SMS Authentication – provides text messages with single-use codes
- Voice Call Authentication – provides telephone calls with audio single-use codes

We recommend that you set up multiple second factors in case you lose or replace your smartphone.

State Network Access

For users that access the IJ Portal from the state network (NYeNet), including those that use a virtual desktop interface (VDI) and/or virtual private network (VPN), you will be **automatically enrolled in the Email MFA factor**. Email verification can easily be used with or without a smartphone, as all state Portal users have email access.

Once logged into the Portal, if you do not have a mobile device, then you are all set!

If you do have a mobile device, we recommend that you set up multiple second factors; the following two additional factors will be available to those on the state network:

- Okta Verify app (IOS/Android/Windows) – provides push notifications and single-use codes
- Google Authenticator app (IOS/Android) – provides single-use codes

Please note that state users may also have occasion to access the portal via the internet (i.e., if they need to access the Portal from home), and in those cases will be presented with the Internet Access protocol above.

How do I set up MFA?

- You will receive a prompt to enroll in MFA the first time you attempt to use the IJ Portal from the internet. When accessing the IJ Portal from the state network, you are automatically enrolled to use email as your second factor.
- After logging in, you will see a screen prompting you to set up MFA.
    - From the internet: it will give you a choice of factors to set up. You can set up as many of these as you like, but you will need to set up at least one. Instructions on setting up each enrollment factor is included below. After you have set up as many as you wish, you will close the enrollment page and go to your application.
    - From the state network: you will be prompted to go to your email to verify yourself. You can then click the link in your email to access the Portal or copy the code and go back to the webpage to enter it, then proceed to the application.

After I set up MFA, how do I use it?

- The next time you log into the IJ Portal, you will be prompted to complete your MFA login.
    - From the internet: you will see a list of all factors that you have set up, and you can choose which one you want to use. (Note that if you've replaced your smartphone but still have the same phone number, this will allow you to use SMS (if you've set it up) even if you usually use Okta Verify or Google Authenticator.) Once verified, go to the original Portal tab.
    - From the state network: you will be prompted to go to your email to verify yourself. Once verified, go to the original Portal tab.
- See below for Step-by-Step Instructions

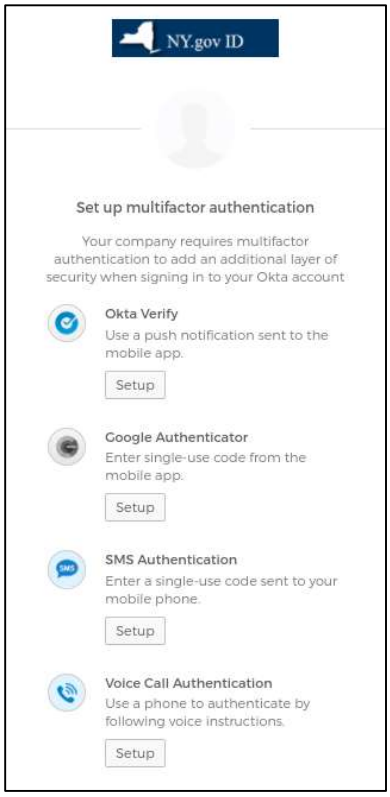
Step-by-Step Instructions for Users accessing the IJ Portal from the Internet

1. Access the IJ Portal using the URL:

   To pre-enroll prior to 10/16/2023: https://new.ejustice.ny.gov
   To enroll on or after 10/16/2023: https://www.ejustice.ny.gov

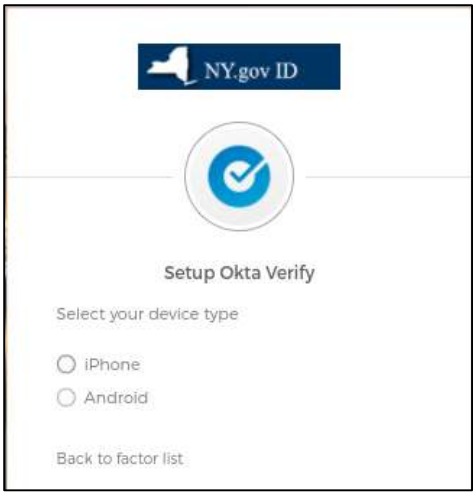
   NOTE that you do not need to change your "Favorites" as the Portal URL is not changing.

2. Enter your password as usual
3. You will be presented with four MFA factors/options:

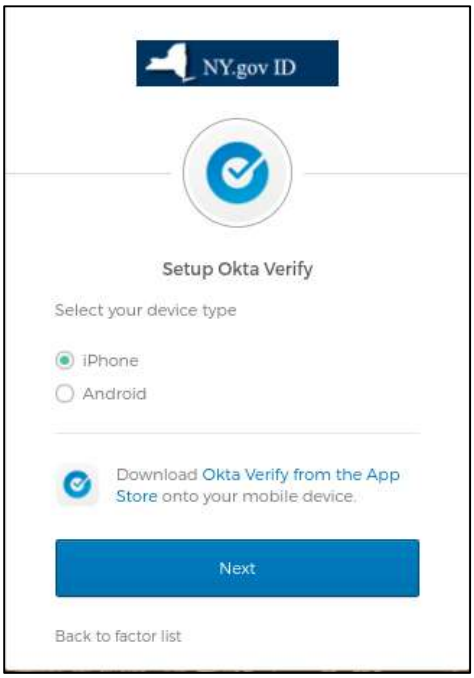


Setting up your second factors

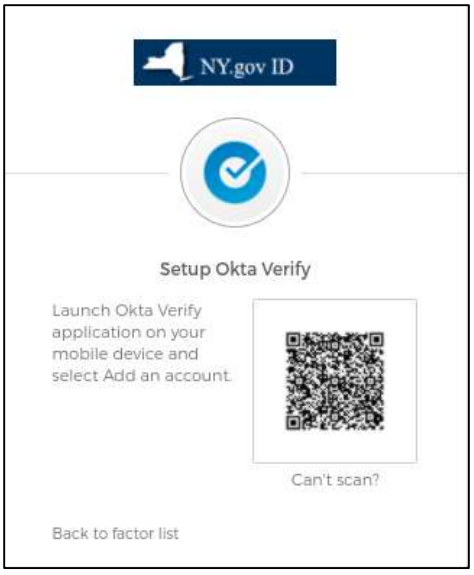
- Okta Verify – the following steps and images will guide you through this option
  - Select device type (iPhone, Android)



- You will be prompted to download app from App Store/Google Play/Windows Store
- Make sure device is running latest version of OS
- Follow the installation prompts
- Open app
- Click “Next” on enroll screen – will pop up a QR code

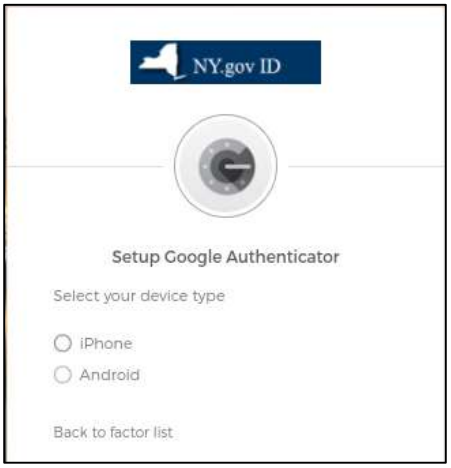


- Tap “Add Account” in app
- Scan QR code from app (or follow “no barcode” prompt)

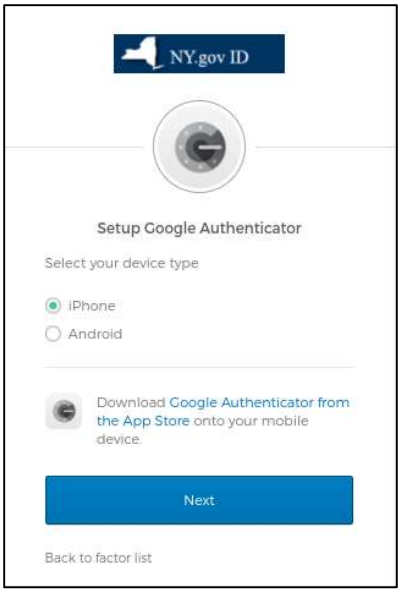


- Will see 6-digit code (changes every 30 seconds)
- Type into setup field and click Verify
- Redirected back to enroll screen where you can set up another factor, if desired.

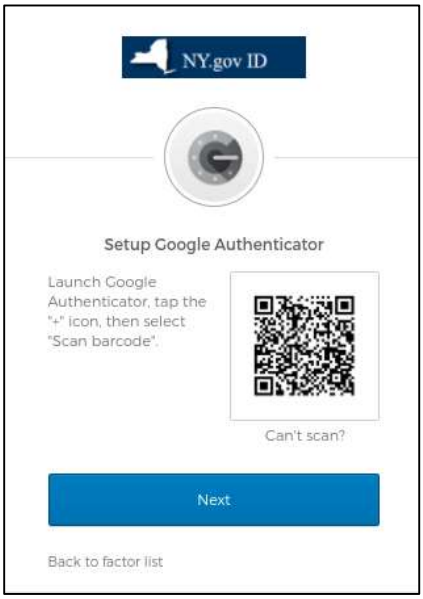
- Google Authenticator – the following steps and images will guide you through this option
  - Select device type (iPhone, Android)



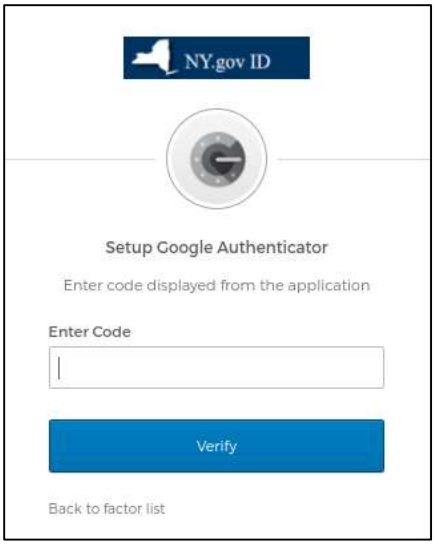
  - You will be prompted to download app from App Store/Google Play/Windows Store
  - Make sure device is running latest version of OS
  - Follow the installation prompts
  - Open app
  - Click “Next” on enroll screen – will pop up a QR code



- Tap “Add Account” in app
- Scan QR code from app (or follow “no barcode” prompt)

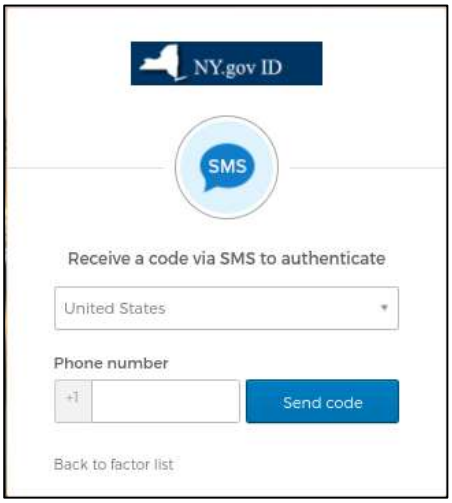


- Will see 6-digit code (changes every 30 seconds)
- Type into setup field and click Verify



- Redirected back to enroll screen where you can set up another factor, if desired.

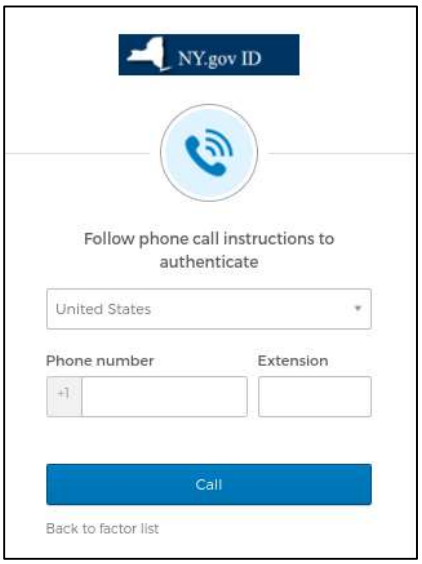
- SMS Authentication – the following steps and images will guide you through this option
  - Enter phone number and click "Send Code"



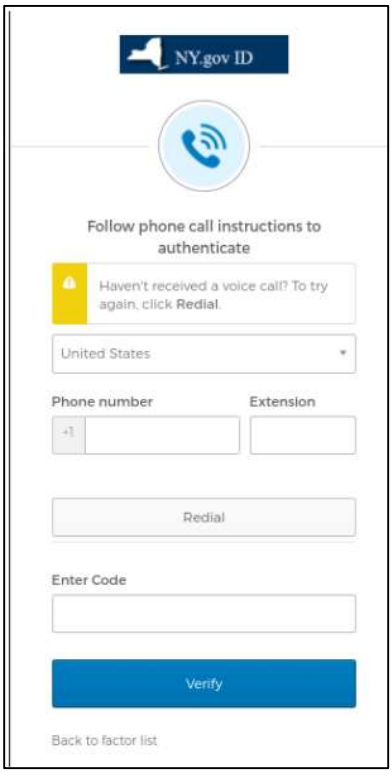
  - Receive text with 6-digit code
  - Type code into "enter code" field and click Verify

- Redirected back to enroll screen where you can set up another factor, if desired.

- Voice call – the following steps and images will guide you through this option
  - Enter phone number and click “Call”

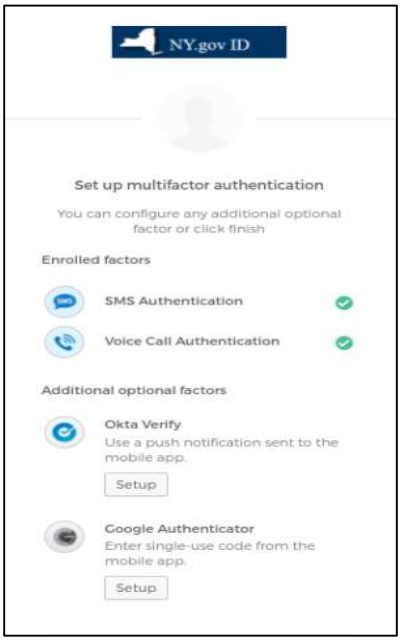


  - Receive call with 6-digit code
  - Type code into “enter code” field and click Verify



- Redirected back to enroll screen where you can set up another factor, if desired.

On completion of each option, a green check mark will show the factors you're enrolled in.



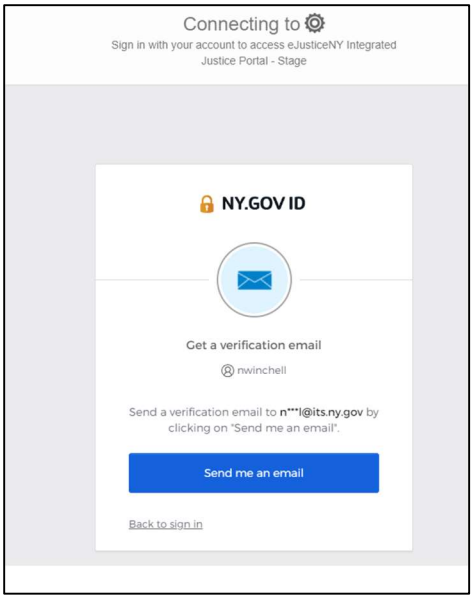
Step-by-Step Instructions for Users accessing the IJ Portal from the State Network

1. Access the IJ Portal using the URL:

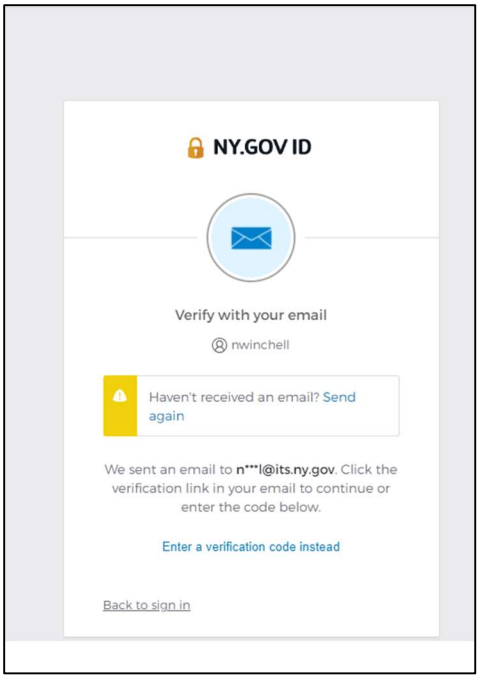
   To pre-enroll prior to 10/16/2023: https://new.ejustice.ny.gov
   To enroll on or after 10/16/2023: https://www.ejustice.ny.gov

   NOTE that you do not need to change your "Favorites" as the Portal URL is not changing.

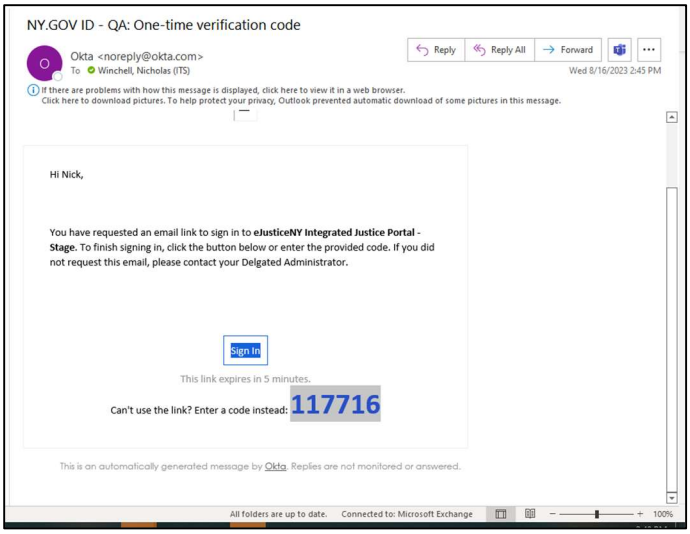
2. Enter your password as usual
3. You will be auto enrolled in email MFA and will see the following message:



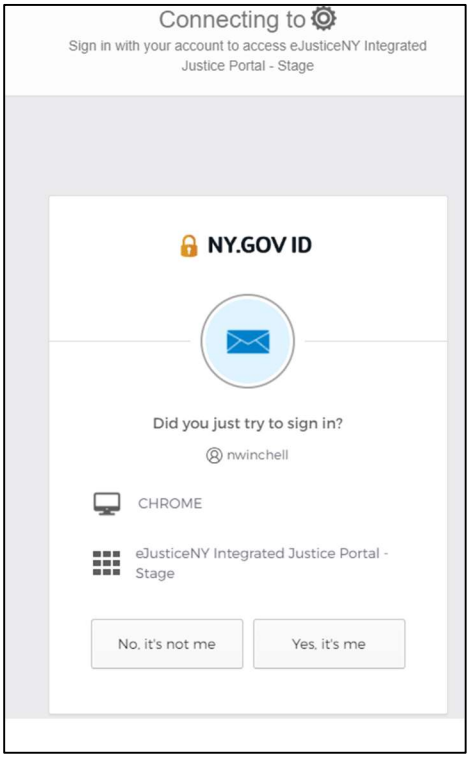
4. Click “Send me an email” button



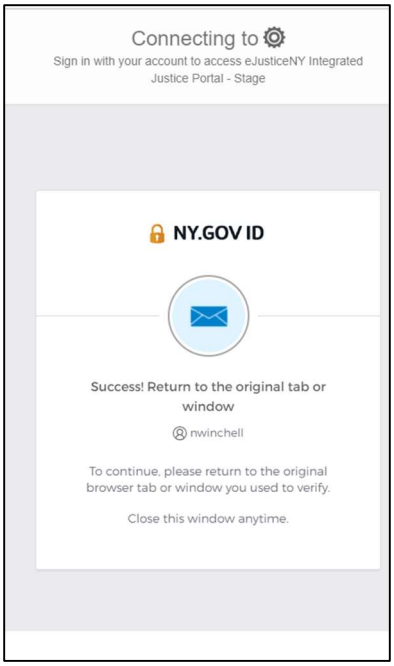
5. Open your email and look for the message from Okta <noreply@okta.com>. Click on the Sign In button or copy the 6-digit pin at the bottom of the e-mail. *If copying pin, jump to step 9.*



6. Clicking the Sign In button will open a new browser tab ask you to confirm your browser type and the app you are logging into. Click the "Yes, It's me" button.

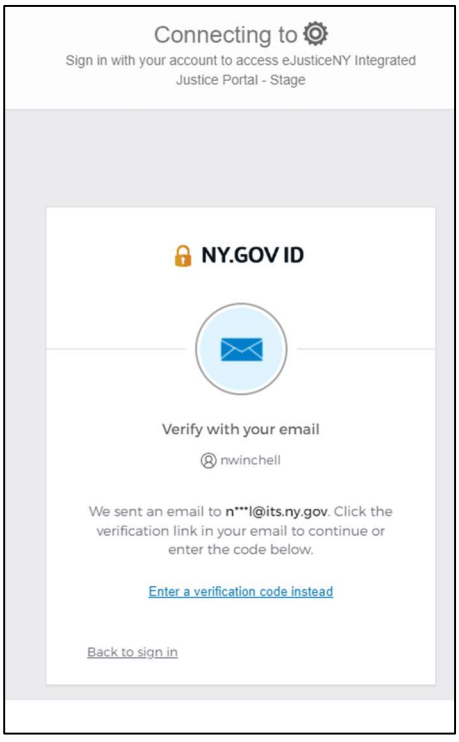


7. Upon Clicking "Yes, it's me" you will be notified you can close that tab and return to the original IJ Portal login tab.

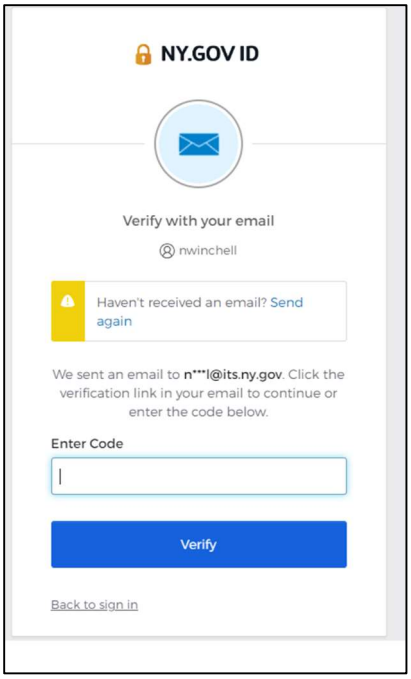


8. Return to original tab where IJ Portal will be available. <<*End of instructions if you clicked on the Sign In button in Step 5 above.*>>

9. *<u>If you copied the 6-digit code in Step 5 above</u>* - click link to "Enter Verification code instead."



10. Copy 6-digit pin from the email and paste into the code box and click the Verify Button.



11. Login will proceed upon pin verification.

FAQs and Tips

Q1 – Why can't we use "secret questions" for MFA as we do on other sites?

A1 - The latest industry security standards have determined that "secret questions" factors are not sufficiently secure and should no longer be used. New York State is working to move away from them.

Q2 – Can I use a landline phone instead of a smartphone for voice call authentication?

A2 – Yes

Tip: If you lose or replace your smartphone and your new phone keeps the same number, you could use SMS authentication on your new phone while you re-enroll your smartphone apps on the new phone.

Tip: Google allows you to generate a list of backup codes from your Google account to use with Google Authenticator if your smartphone is not available. This way, you can use a code from your list if you do not have your smartphone handy, or if you do not have a smartphone.