

Okta FAQ's

1) Do I need a new RN login account for my current RN to remain valid?

No. Unless you have previously cancelled your RN, your RN will still remain valid even without a login account. However, you will need to create a login account if you need to update any information or cancel the RN.

2) If I already have an RN login account, what do I need to do to access the new system?

If you had an account in the old system, you need to register in the new system using the exact same email account you used in the old RN system. Please follow the registration instructions to securely access the system. (Refer to section 3.1.1 Registration in the [RN System User Registration Guide](#))

3) I received a Welcome email. What do I do with it?

After registering on the RN site, you will receive a Welcome to the RN System email. This email will help you complete the final steps in your registration process by setting up Okta Verify, Google Authenticator or FIDO2 (WebAuthn). Click here for detailed instructions. (Refer to section 3.1.2 Account Activation and section 3.1.3 Setup Multi-Factor Authentication in the [RN System User Registration Guide](#))

4) I forgot my login password. How can I reset it?

Go to the login screen via rn.ftc.gov and click "Forgot password?" Follow the prompts to receive a password reset link via your registered email.

5) How can I install and use the Google Authenticator app?

Download Google Authenticator from the Apple App Store or Google Play on your mobile phone, if you don't have it already installed. Then log in to Okta on your computer, go to Settings > Extra Verification, and select Set up next to Google Authenticator. Open the app on your phone, tap the + icon to scan the QR code shown on screen, and enter the 6-digit code in Okta to complete setup. For more detailed information click here. (Refer to section 3.1.3 Setup Multi-Factor Authentication (A) in the [RN System User Registration Guide](#))

6) How can I install and use the Okta Verify app?

Download Okta Verify from the Apple App Store or Google Play on your mobile phone, if you don't have it already installed. Then log in to Okta on your computer, go to Settings > Extra Verification, and select Set up next to Okta Verify. Scan the QR code shown on screen with your mobile app to link your account. For more detailed

information click [here](#). (Refer to section 3.1.3 Setup Multi-Factor Authentication (B) in the [RN System User Registration Guide](#))

7) How can I enroll a YubiKey using FIDO2 (WebAuthn)?

Insert your YubiKey into a USB port on your computer. Log in to Okta and follow the on-screen prompts to set up FIDO2 security key authentication during account creation. To add or update this later, go to Settings > Extra Verification and select Set up next to Security Key or Biometric Authenticator. When prompted, tap your YubiKey to register it. Follow all on-screen instructions to complete enrollment. A confirmation message will appear once your YubiKey has been successfully registered. If using a different FIDO2-compatible device (such as a built-in biometric sensor), follow the prompts specific to that method. For more detailed information click [here](#). (Refer to section 3.1.3 Setup Multi-Factor Authentication (C) in the [RN System User Registration Guide](#))

8) I'm having trouble setting up Multi-Factor Authentication, who can I contact?

For assistance with setting up Multi-Factor Authentication, please contact support.rnsystem@ftc.gov.

For more detailed information, you can refer to Okta's, Google's or YubiKey official documentation:

- [Reset a user password | Okta](#)
- [Manage self-service password reset | Okta](#)
- [User settings | Okta](#)
- [Manage account settings | Okta](#)
- [Google Authenticator](#)
- [FIDO2 \(WebAuthn\) YubiKey](#)