

Setting Up Time-based One Time Passcode (TOTP) in AHCUDigital

The use of this feature is not mandatory. It can be used to enhance existing login authentication as a secondary authentication mechanism when using an unrecognized device.

1. Login AHCUDigital. If prompted, select *Enroll Now* from the TOTP Prompt.
 - a. If prompt is declined or not automatically prompted, enrollment can be completed via My Settings > Security Options > Security Options > Select Edit.

2. Within Confirming your identity, flip the *By authenticator* switch from OFF to ON.
3. Enter AHCUDigital password in *Current password* field.
4. Press *Save*.

Confirming your identity

If we do not recognize your computer or device, we confirm your identity by one of the methods below.

By phone Confirm your identity by responding to a text or call to a phone you have handy.

+1 [Country Code] [Phone Number] [X]

+1 [Country Code] [Phone Number] [X]

By authenticator Confirm your identity with an authenticator.

Save this setting to generate a code for your authenticator app. You will need to provide the code to your app to finish setup.

▶ [What is an authenticator?](#)

▶ [How do I get an authenticator?](#)

By email Receive one-time security codes by your primary email address, diuniversity.di@ncr.com. [Update primary email](#)

Current password Password [SHOW](#)

[Save](#) [Cancel](#)


5. Once the security options have been saved, an activation box will appear page, with one of two available options:
 - a. Scan the QR code
 - b. Copy the authentication code

Security options | [Edit](#) (404) [Enable for text](#) v

(615) Text enabled

Authenticator Code Activated | [Display Code](#) ^

Scan this QR code with your authenticator app



-OR-

Enter this code into your authenticator app

L2UYBUA5NDBXEG5CR4UFQ4W [Copy](#)

Note: Before moving to the following steps the authenticator app of choice (Microsoft Authenticator or Google Authenticator) needs to be downloaded onto device from respective app store.

6. Open authenticator app of choice on device. App prompt should be displayed to accept either QR code scan or input of code from AHCUDigital to activate.

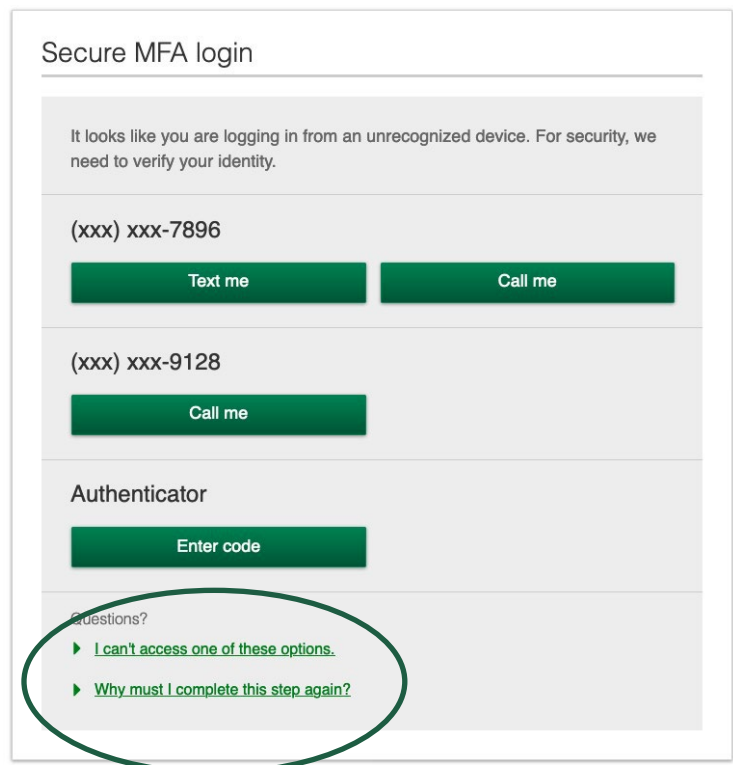
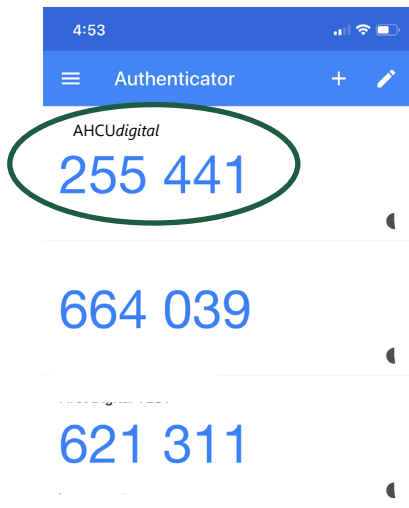
Note: You may need to select the "Add" option in the authenticator app in order to add AHCUDigital into the app.

7. If this setup is being completed on a single device (mobile phone), copy the code using the Copy button. If using multiple devices for setup (i.e. laptop and mobile device), the QR code displayed can be scanned from separate device screen by mobile device to continue. (i.e. displayed on laptop screen and scanned with mobile device).
8. Once the code has either been copied or QR code scanned within the authenticator app on device, the setup is complete.

Using Time-based One Time Passcode (TOTP) in AHCUDigital

Once authenticator setup is completed, the option to use will use within the Secure MFA login screen.

1. Open the authenticator app on device, retrieve the code associated with your AHCUDigital login.



2. Once retrieved, go back to AHCUDigital and enter code to proceed.

Secure MFA login

It looks like you are logging in from an unrecognized device. For security, we need to verify your identity.

Get a verification code from your authenticator app

Enter code

[▶ Didn't get the code?](#)

i Save time by registering this device.

If this is your personal device, register it now. We won't need to contact you the next time you log in.

[Yes, register my private device](#) [No, this is a public device](#)

Questions?

- [▶ I can't access one of these options.](#)
- [▶ Why must I complete this step again?](#)

For questions or concerns, please contact us at 763.422.0290 or through secure messaging within AHCUDigital.