Immigration Case Management (ICM)
Required MFA for Immigration Practitioners & HR Users

Multifactor Authentication (MFA) is an additional layer of access security that requires a secondary factor of authentication in order to login to a site.

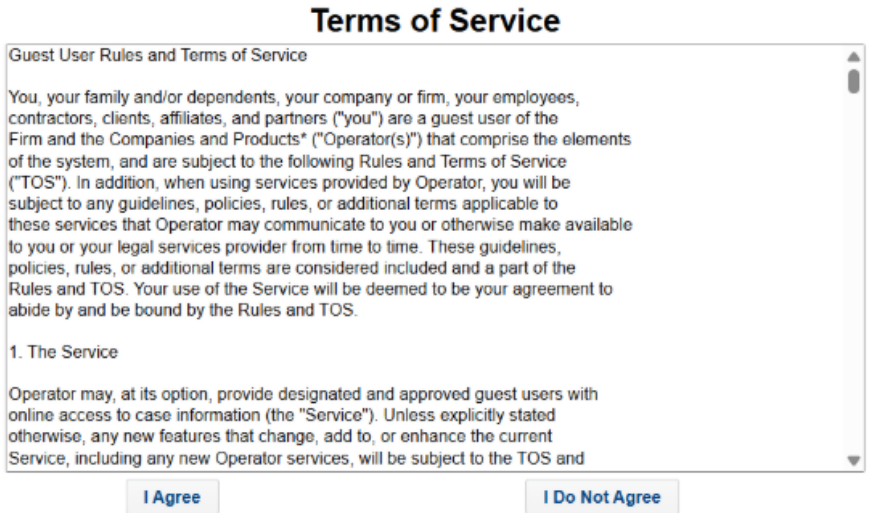
Immigration Practitioners (i.e., firm users) and HR Users will be required to download a trusted authenticator app on their mobile device (examples include: Google Authenticator, Microsoft Authenticator, LastPass Authenticator, and many more) to authenticate their identity before access is granted to ICM.

NOTE: Single Sign On (SSO) Users are not affected by this authentication change.

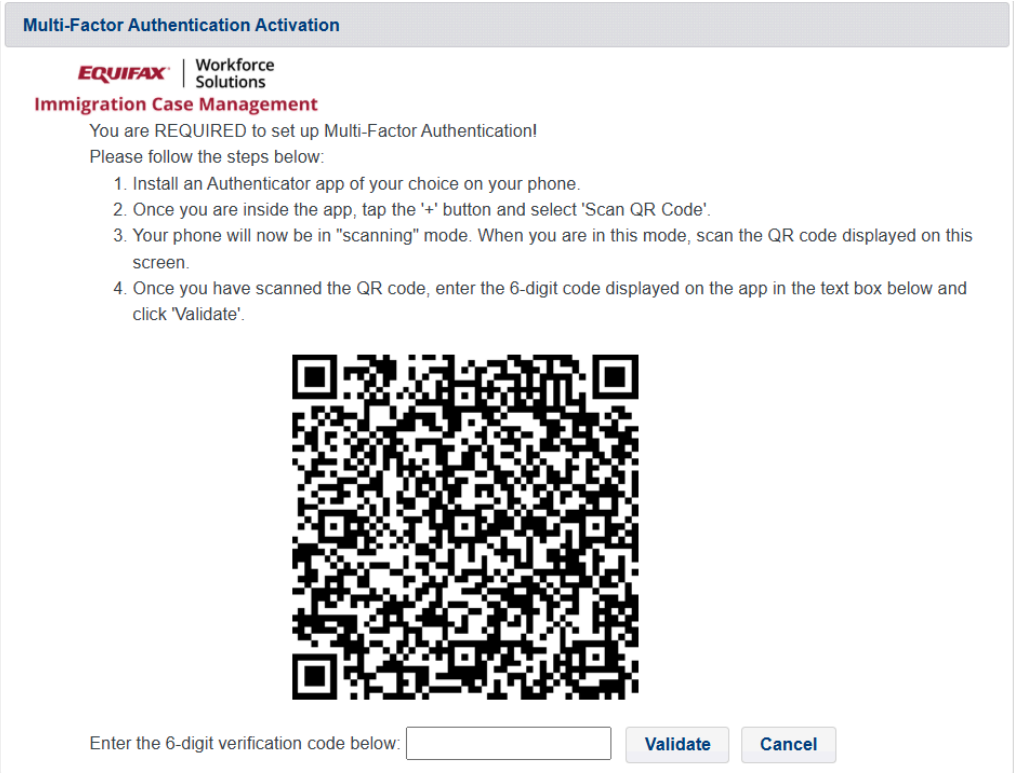
Authenticator apps create a secure second layer of protection for your online accounts by generating time-based one-time passwords (TOTPs) directly on your device. These codes are more resistant to interception, because they're not transmitted over a network, and their brief lifespan makes them difficult for attackers to steal and use.

Steps to Set Up Multifactor Authentication (MFA)

Immigration practitioners and HR users will automatically be presented an MFA pop-up message the next time they attempt to login. Please note, this pop-up will appear after the user has agreed to terms of service (if they have not accepted this previously).

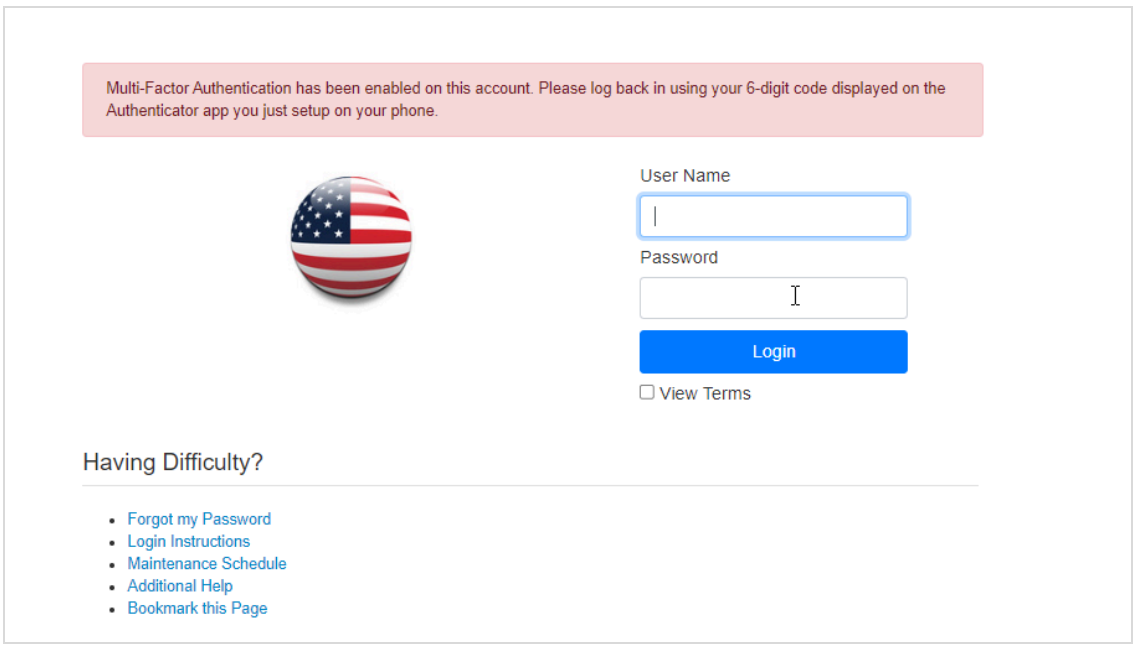


The pop-up will feature a QR code and the following instructions:

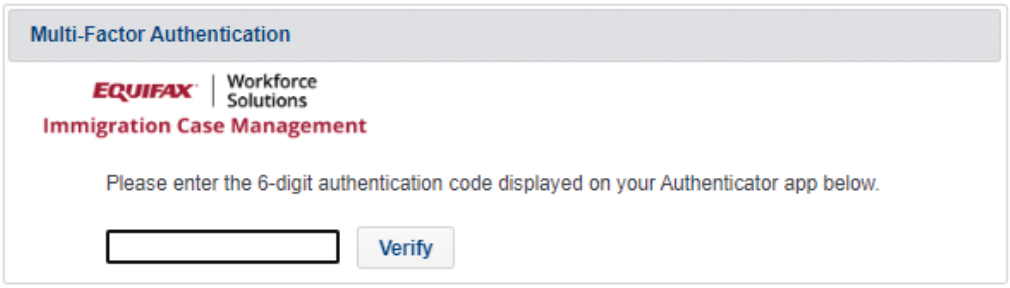


NOTE: The QR code is for set up / initial use only, and is not applicable during subsequent logins.

Once the user completes the setup process by entering the 6 digit code from their authenticator app, they will be logged out of the system and asked to log in again:



After completing the login and password step after logout, the User will be presented with the MFA code entry screen. This step will be required after every subsequent login attempt going forward.

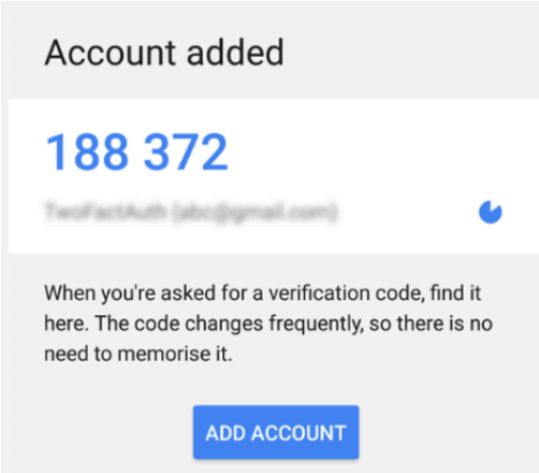


The user may not close out or otherwise circumnavigate the MFA pop-up until the validation steps are completed.

They must enter the numeric code displayed on their mobile device in the **Verify** field within the MFA pop-up and click **Validate** to proceed.

- Code for validation will appear as 'WelcomeClient' depending on the authenticator app used.

Example image:



NOTE: The screenshot above is from Google Authenticator. This screen will look slightly different based on the authenticator app used.

Please note, the validation code will be refreshed after a certain amount of time within the authenticator app. This is expected behavior. If a user sees a 'validation failed' message, they may simply enter in the latest numeric code the authenticator app has provided.

Once successfully validated, users will be able to access ICM. After signing out, users will be prompted to enter the validation code from their Authenticator App, in addition to their sign in credentials moving forward.

Device Pairing and Account Reset

A user may only be paired to **one** device and **one** authenticator app at a time. If a user gets a new mobile device or wishes to change authenticator apps, they will be required to *reset MFA* using the instructions below. This process effectively unpairs the old device and allows pairing with a new one.

Firm Users

Firm users must contact an administrative user to Reset MFA.

To Reset MFA, the admin must:

1. Sign into ICM.
2. Click their name displayed in the upper right of the Dashboard screen.
3. Click Administrative Settings from the dropdown menu that appears.
4. Go to the Users tab
5. Click on the applicable firm user
6. On the Firm user's General tab, scroll down to the section labeled Login Information
7. Click Reset MFA

HR Users

HR users must contact their law firm representative (i.e., firm user) to Reset MFA.

Any firm user can reset MFA for an HR user. To do so, the firm user must:

1. Sign into ICM.
2. Click on Company under the Menu on the Dashboard Screen
3. Find and click into the applicable company the HR user is associated with
4. Go to the Contacts tab
5. Click on the applicable HR contact
6. On the HR contact's General tab, scroll down to the section labeled Login Information
7. Click Reset MFA.

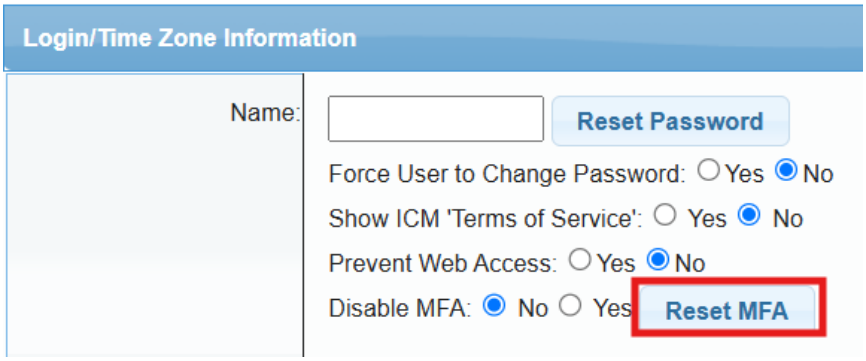
Foreign National (FN) Users

FN users must contact their law firm representative (i.e., firm user) to Reset MFA.

Any firm user can reset MFA for a FN user. To do so, the firm user must:

1. Sign into ICM.
2. Click on FN/Individual under the Menu on the Dashboard Screen
3. Find and click into the applicable FN

4. Scroll down the FN's Personal Tab to the section labeled Login/Time Zone Information
5. Click Reset MFA



After the Reset MFA step is complete, users will need to remove the related account from their existing authenticator app. From here, the user can proceed with desired next steps, whether they choose to set up MFA on a new device or download and use a different authenticator app moving forward.