EQUIFAX®

Client Training HQ

Multi-factor Authentication for Firm and HR Users

Multi-factor Authentication (MFA) is an additional layer of access security that requires multiple identity verification methods, such as a password combined with a code sent via SMS, email, or an authenticator app, in order to log into a site.

If you are a Firm user or HR user who does not utilize Single Sign-on, you are required to download a trusted authenticator app on your mobile device (e.g., Google Authenticator, Microsoft Authenticator, LastPass Authenticator, etc.) to authenticate your identity before access is granted to Immigration Case Management (ICM).

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 more difficult for attackers to steal and use.

***Note*:** Single Sign-on (SSO) users are not affected by this additional authentication requirement.

Setting Up Multi-factor Authentication (MFA)

If you are a Firm user or HR user who does not utilize Single Sign-on, you will automatically be presented with an MFA pop-up message the first time you attempt to log in.

> ***Note:*** The MFA pop-up message will appear only after you click **I Agree** to the Terms of Service.

The MFA pop-up message features a QR code to scan and instructions.

> ***Note*:** The QR code is for setup/initial use only and is not applicable during subsequent logins.

Once you complete the setup by entering the 6-digit code from your authenticator app, you will be logged out of the system and prompted to log in again.

You will be presented with the MFA code entry screen. This step is required after every subsequent login attempt.

Copyright © 2026, Equifax Inc., Atlanta, Georgia. All rights reserved. Equifax and the Equifax marks used herein are trademarks of Equifax Inc. Other product and company names mentioned herein are the property of their respective owners.

Do not close out or otherwise circumnavigate the MFA pop-up message until you have completed the validation steps. Enter the numeric code displayed on your mobile device in the Verify field in the MFA pop-up message and click **Validate**.

The validation code will be refreshed on a regular basis. This is expected behavior. If you see a "validation failed" message, verify you have entered the latest numeric code your authenticator app has provided.

Once successfully validated, you will be able to access ICM. After signing out, you will be prompted to enter the validation code from your authenticator app, in addition to your sign-in credentials moving forward.

Device Pairing and Account Reset

You may only be paired to one device and one authenticator app at a time. If you get a new mobile device or change authenticator apps, you 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 will:

1. Sign into ICM.
2. Click their name displayed in the upper right corner of the **Dashboard** screen.
3. Click **Administrative Settings** from the drop-down 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 will:

1. Sign into ICM.
2. From the **Dashboard** screen menu, click **Company**.
3. Go to the **Contacts** tab.
4. Click on the applicable HR contact.
5. On the HR contact's **General** tab, scroll down to the section labeled **Login Information.**
6. 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 an FN user. To do so, the Firm user will:

1. Sign into ICM.
2. From the **Dashboard** screen menu, click on FN/Individual name.
3. Scroll down to the section labeled **Login/Time Zone Information**.
4. Click **Reset MFA**.

After the Reset MFA step is complete, you will need to remove the related account from your existing authenticator app. You may then choose to set up the same authenticator app on the new device or download a different authenticator app to the new device.

More Training Available!

Check out additional training resources available on our site, Connections.

The information provided is intended as general guidance and is not intended to convey any tax, benefits, or legal advice. For information pertaining to your company and its specific facts and needs, please consult your own tax advisor or legal counsel.