

Multi-factor Authentication for Foreign National (FN) 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.

Immigration Case Management (ICM) offers two approaches for managing MFA for Foreign National (FN) users. Firms can: (1) Allow FN users to voluntarily enable MFA, or (2) Selectively require MFA for all FN users of a specific Company.

Voluntarily Enabling MFA

To opt-in to optional MFA, FNs will:

1. Sign into the FN portal.
2. Click their name at the top of the page to navigate to **User Settings**.
3. Under User MFA, select **Yes**.
4. Click **Update Settings**.

Requiring MFA for all FNs from a Specific Company

When organizations have multiple companies set up in the system, MFA can be disabled or enabled at the Company level as needed.

To modify MFA settings at the Company level:

1. Sign into ICM.
2. Select **Companies** from the left navigation menu.
3. Click the appropriate Company name.
4. Click the **General** tab.
5. Locate the **Require MFA for All FNs** option, and select **Yes**.
6. Click **Update Info**.

MFA Experience in the FN Portal

After Multi-factor Authentication is enabled by the FN or by an Administrative Firm user, FN users will see a pop-up message the next time they attempt to log in. Please note, this pop-up message will appear only after the FN user has agreed to Terms of Service and General Data Protection Regulations (GDPR) consent, if applicable.

The pop-up message features a QR code and instructions for the FN.

Notes:

- The QR code is for setup/initial use only. During subsequent logins, only the numeric code from the authenticator app is required to log in.
- In addition to these instructions, the FN user may click the “Need Help? E-Mail Your Case Manager” link in the upper right. This will open a new overlay where a FN user may send a SureMessage to their assigned case manager for assistance.
- The pop-up message will not appear if a Firm user is utilizing the Login as FN function within ICM.

Device Pairing and Account Reset

An FN user may only be paired to one device and one authenticator app at a time. If users get a new mobile device or 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.

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 the ICM application.
2. From the **Dashboard** screen, 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, users will need to remove the related account from their existing authenticator app. Users 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.