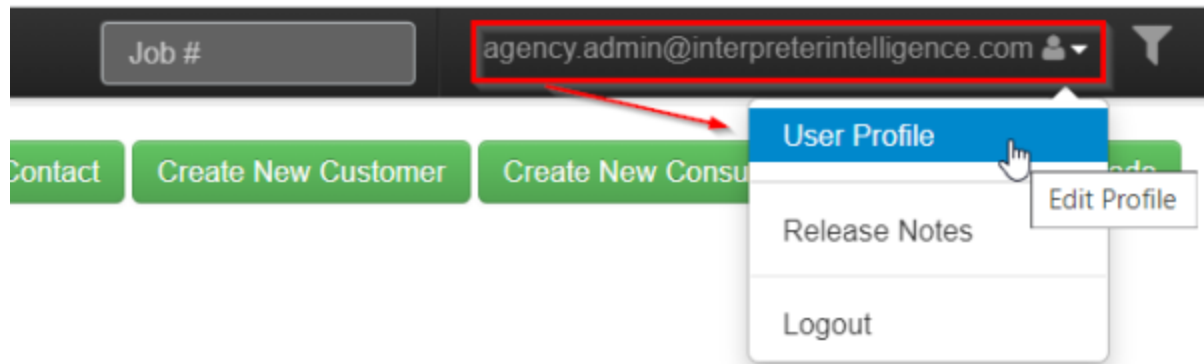


User Management - MFA

A user can enable **Multi Factor Authentication (MFA)** from their own profile. This will mean that when the user logs in as normal with their II username and password, they will also be asked for a Security code which will be generated by an authenticator app.

Click on your username on the top right of II and select **User Profile**



Click on the **Configuration** tab and select **Enable** on **MFA** at the bottom of the page

A screenshot of the user configuration page. The 'Configuration' tab is selected and highlighted with a red box. Below the tab, there are several sections: 'Change Password' with fields for 'Current Password', 'Password', and 'Password Confirm'; 'Time Zone Preference' with a 'Time Zone' dropdown; 'Locale Preference' with a 'Locale' dropdown; and 'Multi Factor Authentication (MFA)' with an 'Enable' checkbox and an 'MFA Method' dropdown. A red arrow points from the 'Enable' checkbox to the 'MFA Method' dropdown.

The user will need to install an authenticator app such as Google Authenticator or Twilio Authy. When they Enable MFA per above they will be presented with a QR code that they can scan in the authenticator app.

Then click on **Apply** in the QR code box and click on the blue **Save** button on the user profile.

1. Download an authenticator app like Google Authenticator or Authy to your mobile device
2. Scan the following QR code from the authenticator app to start getting the Interpreter Intelligence security code
3. Click on the apply button
4. Save user preferences



Cancel

Apply

At next login, the II user will enter their II **username** and **password** as normal and they will also be asked for a **Security code** which will be generated by an authenticator app. Various authenticator apps will have slightly different functionality but usually you click on your account in the app and this generates a code which will be active for a short period of time. Once the user enters a valid security code they can access II as normal.

If a user can no longer login using MFA, for e.g. they removed the authenticator app or lost access to it, an Internal agency user can switch off MFA by going to **Admin -> User Management** and unchecking the **MFA Enabled** box and saving the user profile. The user can then login without MFA. Note that Internal agency users cannot enable MFA for other users; only individual users can enable this on their own account.

Admin - Job # agency.admin@interpreterintelligence.com

User: agency.admin@interpreterintelligence.com (Agency Admin)

Details

Username agency.admin@interpreterintelligence.com

Email agency.admin@interpreterintelligence.com

Password Password

Confirm Password Password

First Name Agency

Last Name Admin

Business Units

Eastern Region

North Region

Southern Region

Western Region

User Type

☐ Customer

☒ Internal

☐ Interpreter

Configuration

☒ Admin

☒ Financial

☐ Interpreter Manager

☒ Can Read Reports

☒ Can Close Jobs

Settings

☒ Account Enabled

☐ Account Expired

☐ Account Locked

☐ Password Expired

☒ MFA Enabled (authenticator)

Save New User

If a user has multiple accounts on II (e.g. **Internal & Interpreter**) they can have MFA enabled for each account but they should rename their accounts in the authenticator app to avoid any confusion when logging in.