Account Holder MFA User Guide

Verra offers a Multi-Factor Authentication (MFA) option for Verra Registry users providing them with a more secure method to access their Verra Registry accounts. By default, all **new** Verra Registry users registering an account in the Verra Registry on or after 21 September 2022 will be opted into the MFA requirement. All **existing** Verra Registry users who registered an account in the Verra Registry before 21 September 2022 will be opted out of the MFA requirement. Both new and existing Verra Registry users may change their MFA settings at any time.

By default, all new Verra Registry users registering an account in the Verra Registry on or after 21 September 2022 will be opted into the MFA requirement. All existing Verra Registry users who registered an account in the Verra Registry before 21 September 2022 will be opted out of the MFA requirement. Both new and existing Verra Registry users may change their MFA settings at any time.

Note, the MFA requirement preference is applicable to all login IDs within a given account, i.e., if the MFA requirement is activated at the account level, all login IDs within that account must authenticate via the MFA process. If the MFA requirement is deactivated at the account level, then no login IDs within that account will be authenticated via the MFA process.

1. For Verra accounts opted n to the MFA requirement, every user within that account will be prompted to authenticate via one of the authentication channels below:
   a. **Email**: a one-time passcode is delivered to the contact email address registered to the user's login ID. (Tip: If the email is not received, be sure to check your spam or junk folder).
   b. **SMS Text**: a one-time passcode is delivered to the mobile number registered to the user's login ID via text message.
      i. When selecting this authentication channel, the user's mobile number will need to be verified before it can be registered to the login ID and used for authentication.

ii. Only the person using the login ID can register a mobile number to that login ID. Neither the Verra Registry administrator nor the account manager can register a mobile number on behalf of another login ID.

c. **Voice**: a one-time passcode is delivered to the mobile number registered to the user's login ID via an automated phone call.

i. When selecting this authentication channel, the user's mobile number will need to be verified before it can be registered to the login ID and used for authentication.

ii. Only the person using the login ID can register a mobile number to that login ID. Neither a Verra Registry administrator nor the account manager can register a mobile number on behalf of another login ID.

d. **Authentication App**: the user registers their Verra login ID to their preferred authentication app, then authenticates via the time-limited passcode generated by the authentication app.

i. [Review information on the authentication app channel option](#)

LOG IN - MULTI FACTOR AUTHENTICATION

Multi Factor Authentication

Please select your preferred two-factor authentication channel below. Upon making the selection, only your preferred authentication channel will be presented to you for future login instances.

✉ ● Receive authentication code email to jwe****@apx***

💬 ○ Receive authentication code text to *******701

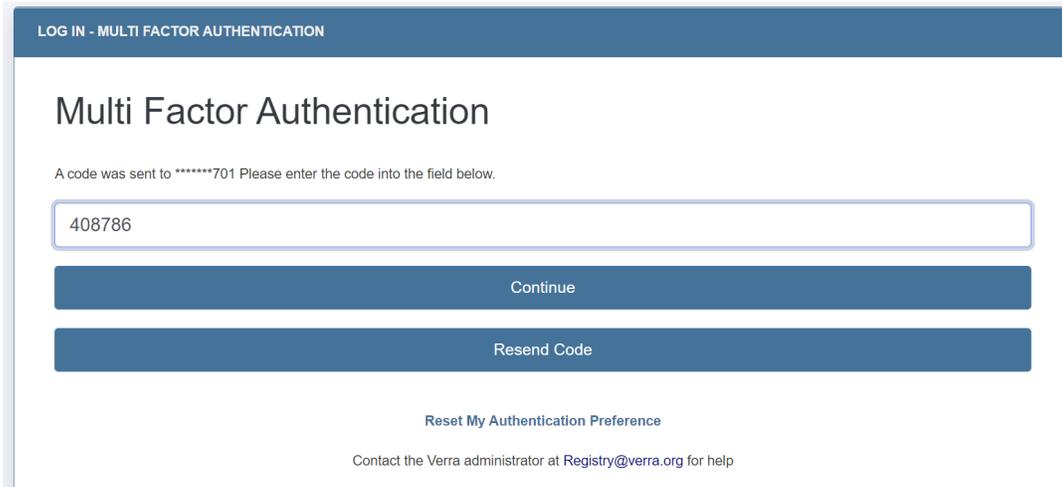📞 ○ Receive authentication code call to *******701

📱 ○ Authentication with an Authentication App
Learn more and download

[Cancel] [Proceed with Authentication]

Contact the Verra administrator at Registry@verra.org for help

---

2. A Verra Registry administrator can deactivate any of the 4 authentication channels at any time, which would require Verra users to utilize one of the remaining authentication channels at that time.

3. Upon logging in for the first time after activation of the MFA requirement, the user will be presented with all available authentication channels. Once the user selects their desired authentication channel, the user will be prompted to use the same preferred authentication channel for every subsequent login attempt.

a. The authentication channel can be reset at any time by the user. See step 8 below.

4. A one-time passcode will be sent to the user via their preferred authentication channel.

a. If needed, the user can click the Resend Code button in the authentication window to resend the passcode to their selected authentication channel when using email, SMS text, or voice.

5. Once the user provides the correct passcode into the authentication screen, they will be granted access to their account.
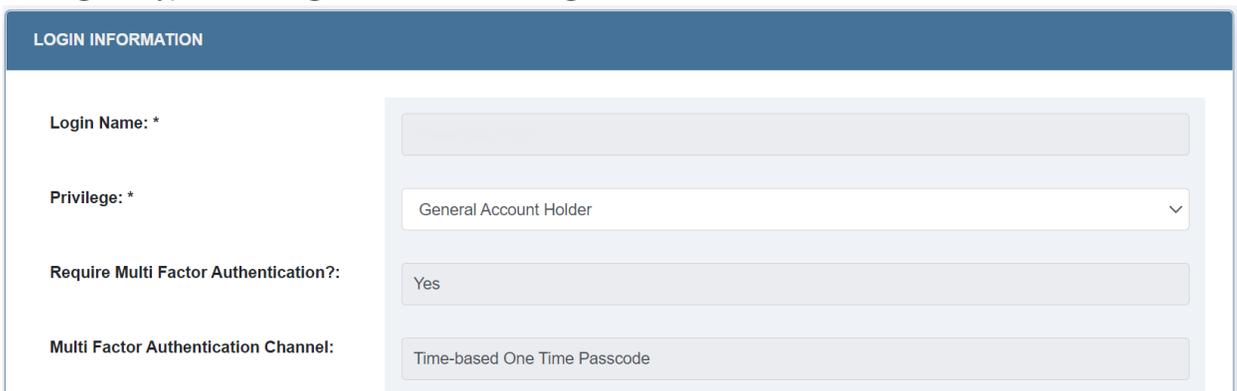
LOG IN - MULTI FACTOR AUTHENTICATION

Multi Factor Authentication

A code was sent to *******701 Please enter the code into the field below.

> 408786

> Continue

> Resend Code

Reset My Authentication Preference

Contact the Verra administrator at Registry@verra.org for help

6. The account holder can update their MFA requirement preference at any time by clicking the Change Profile link in their "My Account Setup" module, scrolling down to the "Account Manager Information" section, then updating the "Require Multi Factor Authentication?" designation as desired. Remember to click the "Save" button at the bottom of the screen.

Require Multi Factor Authentication?: *

| No ▾ |
| Yes |
| No |

7. The account holder can view the preferred authentication channels for all users within the account by clicking the Review/Edit/Add Logins link in their "Account Management" module, then clicking the hyperlinked login name, then viewing the "Multi-Factor Authentication Channel" field.

LOGIN INFORMATION

Login Name: *

Privilege: *
> General Account Holder ▾

Require Multi Factor Authentication?:
> Yes

Multi Factor Authentication Channel:
> Time-based One Time Passcode

8. The user can reset their preferred MFA channel preference during the login and authentication process by clicking the "Reset My Authentication Preference" link. This will trigger an email notification to the user's registered email address with guidance on next steps.

Multi Factor Authentication

A code was sent to *******701 Please enter the code into the field below.

408786

Continue

Resend Code

Reset My Authentication Preference

Contact the Verra administrator at Registry@verra.org for help