Multi-Factor Authentication (MFA)

For Sandata EVV and the Sandata Aggregator with MFA Reset Functionality

Sandata

Rev. February 2025
Sandata Technologies, LLC
sandata.com

`

Table of Contents

`

What is Multi-Factor Authentication

Sandata has launched Multi-Factor Authentication (MFA) for Sandata EVV and the Sandata EVV Aggregator. MFA ensures that users, when logging into either product, are challenged to enter a code provided to their individual device to validate their identity. This helps to ensure that the data we maintain on behalf of our customers is secured from unauthorized access.

MFA is enabled at the full program level including all accounts associated with the program and the program's Aggregator at the same time. Once enabled, as users log in, they will be required to enroll in MFA on their first or next login. The user will no longer be able to login without utilizing MFA. This process does not impact password management or application access which will still utilize the same process as it does today.

The Process

When MFA is enabled for a program, all users and accounts will be impacted. For first time users, they will go through the authentication process on their first login. For existing users, the next time they login to the application, they will be asked to go through the MFA enrollment process to convert their application user to MFA.

Prerequisites:

- You must have access to an available email address or a smart phone / device that can download and run an application.
- Your smart phone / device must have a camera able to take a picture of a QR code.
- If your device is an Apple iPhone, go to the **App Store**, search for **Google Authenticator**, and download. This is a free utility.
- If your device is using an Android operating system, go to the **Google Play Store**, search for **Google Authenticator**, and download. This is a free utility.

If you prefer, you can also use the **Microsoft Authenticator** applications.

First Time User / First Login

1. A user with access to Sandata EVV or Sandata Aggregator with permissions to create a user will create a new user using the standard processes. The screens shown below are for Sandata EVV but the process for Sandata Aggregator is similar.

   NOTE: When a user is first created, the MFA reset button will not be present. The MFA reset button will only appear after the user has initiated the MFA process.

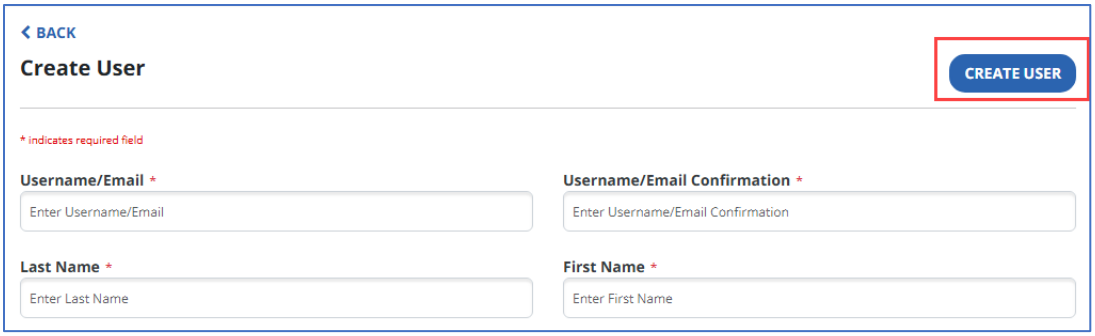


Figure 1: Creating a New User in Sandata EVV

2. When the user is created, an email will be sent to the email address of the user. The user will receive an email from 'no-reply@sandata.com' with a temporary password.

Figure 2: Temporary Password Email

3. At this point, the user can either use the login button presented or go to the Sandata Login Page. https://evv.sandata.com/VM/Login

The user will enter:

a. AGENCY - the Agency account for Sandata EVV (or leave blank for Sandata Aggregator)
b. USERNAME – user's email address
c. PASSWORD – the temporary password received in email

Figure 3: Login with Your Temporary Password

4. The screen will prompt the user to select to authenticate via Authenticator App or Email.

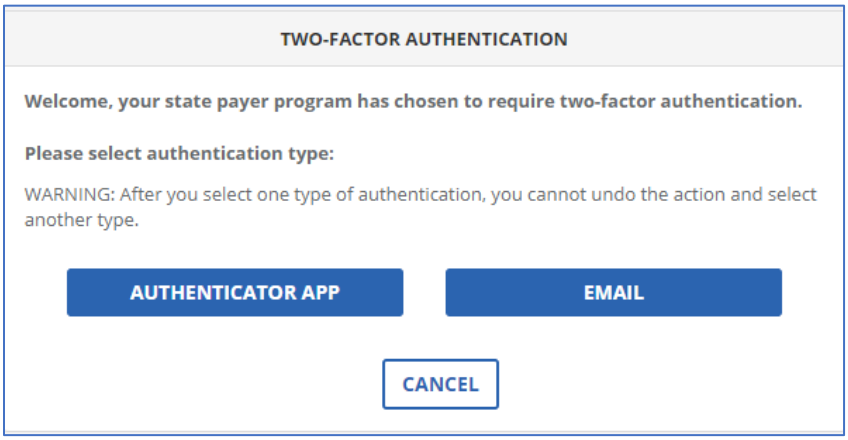


Figure 4: Two-Factor Authentication Welcome Screen

5. If **Authenticator App** is selected, the user will be presented with the following screen.

NOTE: This screenshot references Google Authenticator but MFA also works with Microsoft Authenticator. Instructions that follow are for Google Authenticator.

`

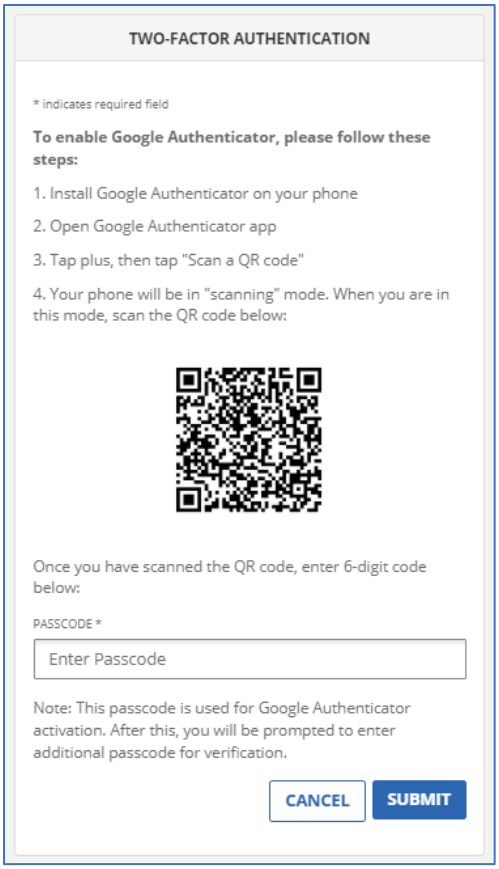


Figure 5: TFA Scan Code Screen

6. The user opens Google Authenticator on their phone/device.
7. On the bottom right of the phone application, there is a **+** sign which allows the user to add a new application for authentication.
8. Tap **+**, then select "Scan a QR Code."
9. The device camera will be presented. Make sure the full QR Code shown is in the square frame.
10. Once the code has been scanned, a code appears. The code shown will start with Sandata which, if you are using the authenticator for other applications, will help you distinguish which is the Sandata code.
11. Enter the passcode on screen in the box labeled 'Passcode' and tap "Submit".
12. If **Email** was selected, the user will need to find the email with the verification code.

`

Figure 6: Email with Verification Code

Note: The user will have 5 minutes after email is sent to enter the authentication code.

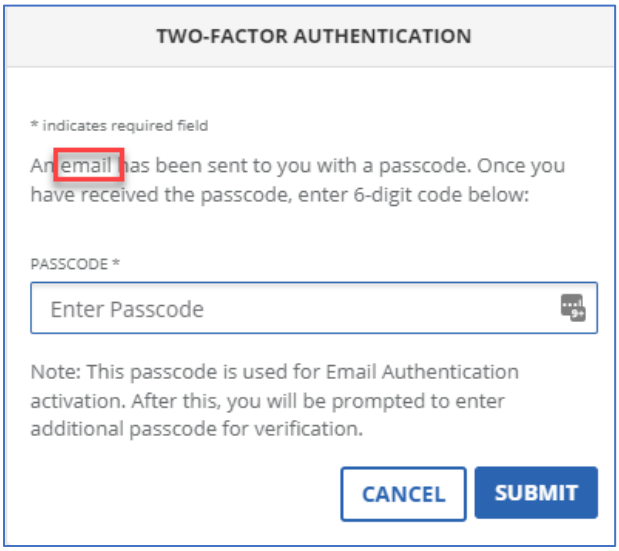


Figure 7: Window Prompt for Email Passcode

13. If this is the first time using MFA for Sandata EVV, the user will be sent a **second** email and then will be asked to enter a second passcode, which will be different than the one entered in the previous step.

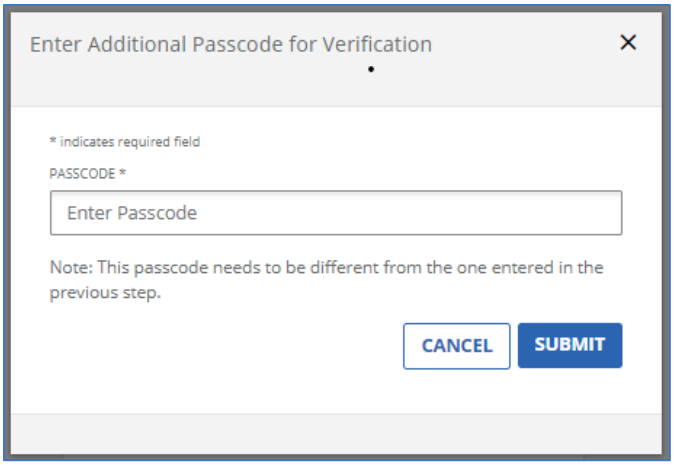


Figure 8: Additional Passcode Prompt

A new user will be taken to the standard change password screen to enable the user to change the temporary password.

`

Subsequent Logins (after MFA has been Configured)

1. Go to the EVV login page and log in with your credentials. Assuming the credentials are correct, you will be presented with the following screen.

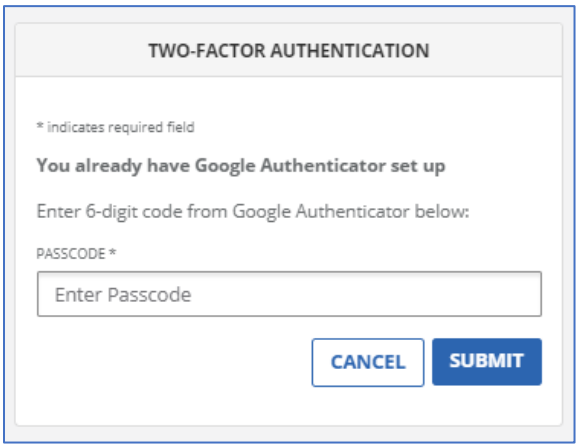


Figure 9: Returning User MFA

2. Go to your Google Authenticator app on your smart device, or to your email inbox, and enter the code shown in the Passcode field above. Make sure to use SUBMIT.
3. Once the code has been entered and verified, you will be logged into the system and go to your normal landing page.

Note: For any user that has shared User IDs in multiple programs (i.e., a user working for a parent entity for a multi-state provider agency), once the user ID is converted to MFA in one account, MFA will be required in all accounts.

`

Multi-Factor (MFA) Reset in Sandata

Authorized users may reset the MFA authentication for a user who has locked themselves out of MFA. This could happen for a multitude of reasons, but the main reasons are:

- They select Authenticator App as their authentication method and have had their smart phone replaced or have deleted their authentication.
- They select either Authenticator App or Email as their authentication method, but the user doesn't have access to that method when trying to access the EVV Portal.

1. To reset the MFA, an authorized user will access the Security > Manage Users area in the EVV portal or aggregator.
2. After finding the user, the Reset MFA button will be available.

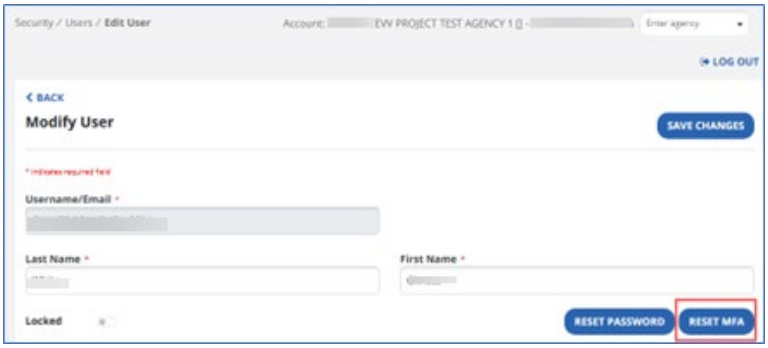


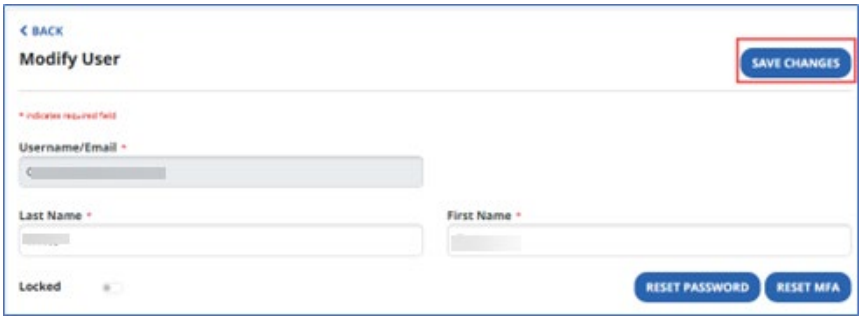
Figure 10: Creating a New User in Sandata EVV

3. The authorized user clicks the Reset MFA button. They will receive the following message then click the OK button.

Figure 11: Reset MFA Prompt

4. After a confirmation message appears that the MFA has been reset, the Reset MFA button will disappear.

`



5. Click Save Changes.
6. Once the MFA is reset, the user will log in with their credentials, which will include the password change they made, and they will be taken through the MFA process with the option of either the Authenticator App or Email.