Multi-factor Authentication (MFA)

Implementation Plan

This document provides an overview of Multi-factor Authentication (MFA) and the steps needed to successfully launch the use of MFA for eVero clients.

Latest Revision | June 2022

Table of Contents

MFA Implementation Timeline 2

Step 1: Introducing MFA and Educating All Users 2

- What is MFA? 2
- What are the Benefits of MFA? 2
- What Does this Change? 3
- How to Update MFA Methods 4
  - From the Web 4
  - From the Mobile App 5
- How to Log in with an MFA Enabled Account 7
- What Device Types (or Methods) are Supported for eVero MFA? 8
  - Email 8
  - Phone 8
  - Authenticator 9
  - FOB 9
- How Often is MFA Needed to Log In to the eVero System? 10

Step 2: Exploring Enrollment Options 11

- Auto Option: Enabling MFA for All 11
- Staggered Option: Enabling MFA for Selected Users 11

Step 3: Implementing MFA & Enrolling Accounts 12

- Establishing Permissions for Agency-Designated MFA Managers 12
- Accessing the MFA Manager Screen in Admin Tasks 13
- Enrolling User Accounts in MFA 13
  - Auto Enrollment: MFA for All 13
  - Staggered Enrollment: MFA for Selected Users 13

Troubleshooting and Support 14

MFA Implementation Timeline

6/29/2022	eVero MFA Initiative Launch. "Implementing MFA for Your Agency" webinar to be offered LIVE at 12pm via Zoom.
6/29/2022-7/15/2022	Implementation Plan Step 1 Complete Leveraging resources found on eVero Ed, Agencies are expected to have completed Step 1 of this Implementation Plan by 7/15/2022. This includes ensuring that current contact information for all is stored within the system.
7/15/2022-9/1/2022	Implementation Plan Steps 2 & 3 Complete Agencies are expected to choose the roll out approach that best fits their agency needs and to have completed the roll out of MFA during this time-period.

Step 1: Introducing MFA and Educating All Users

The first and most important step of implementing anything new or different is to ensure that those affected are appropriately trained and educated regarding what is happening and how these changes will affect them.

What is MFA?

Multi-factor Authentication is an electronic verification system in which the user provides two or more verification factors to gain admittance into the software. Verifying methods may include, but are not limited to, an additional password, PIN number, fingerprint, facial recognition, among others. Regardless of the methods used, once the criteria are met, the user will then gain access.

What are the Benefits of MFA?

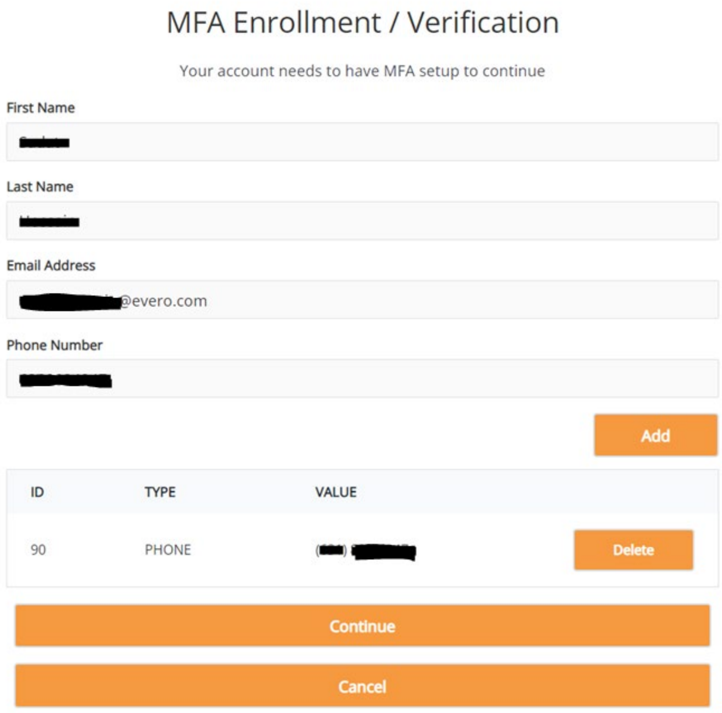
Multi-factor Authentication is beneficial to users for many reasons:

1) MFA provides a more secure login for all users which ultimately protects the personal and confidential information belonging to agencies and the people supported.
2) MFA reduces typical password risks and fatigue
3) The MFA process also helps meet various compliance requirements and protects users against hackers and malicious attacks
4) MFA reduces fraud and identity theft
5) MFA increases trust! The people we support, their family members, and advocates can rest assured knowing that the sensitive information entered into the eVero system is much less likely to be maliciously accessed or shared.

What Does this Change?

Not much, really. It is just one extra step to ensure security of the account. Once the username and password are entered, a new MFA validation screen will be displayed asking that the user select a method from the list to validate, just once more, that they are who they say they are.

Additionally, beginning on July 10th, 2022, all users will be prompted to verify their contact information when logging in.



MFA Enrollment / Verification

Your account needs to have MFA setup to continue

First Name

[redacted]

Last Name

[redacted]

Email Address

[redacted]@evero.com

Phone Number

[redacted]

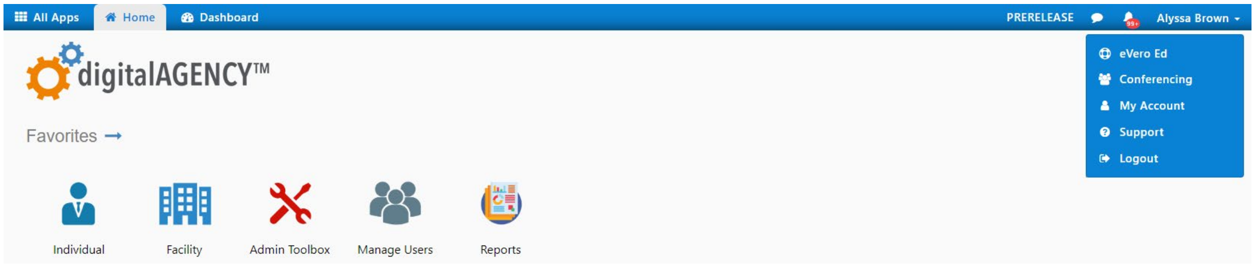
ID	TYPE	VALUE	
90	PHONE	[redacted]	Delete

How to Update MFA Methods

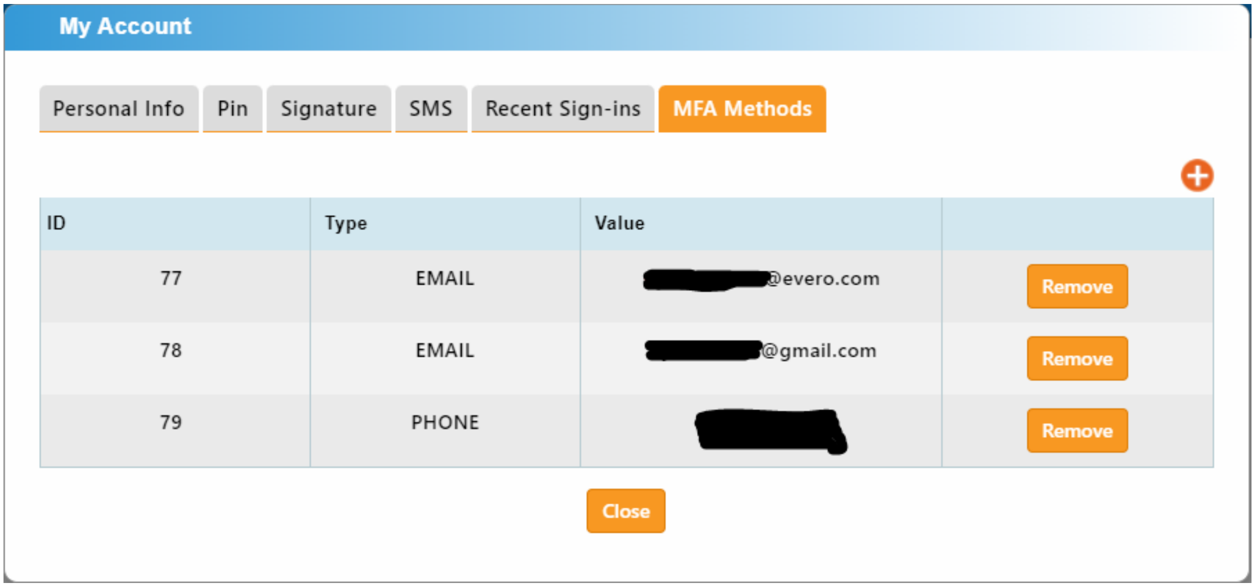
From the Web

Stored contact information for a user can be updated from the web by each user following these steps…

1. Login to the eVero system via the web
2. From the user's home screen, the user will select their name from the upper right-hand corner of the screen and select My Account from the dropdown.

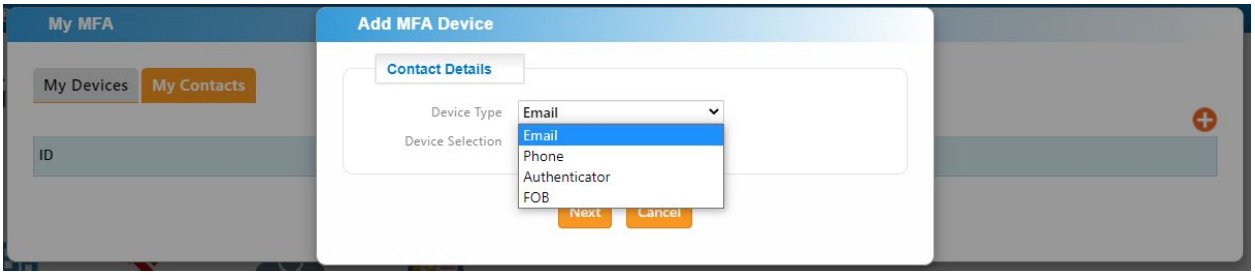


3. Once the My Account Popup is open, the user will click the MFA Methods tab at the top.



ID	Type	Value	
77	EMAIL	[redacted]@evero.com	Remove
78	EMAIL	[redacted]@gmail.com	Remove
79	PHONE	[redacted]	Remove

4. In the MFA Methods tab, the user has the ability to add or remove various MFA Methods including email, phone, Authenticator, FOB. Click the plus sign to add a new method.
5. In the Add MFA Device pop up, the user will select the device type from the list and enter the information required to proceed. A code will be provided when adding a new MFA method as it is when using MFA to login to the system.

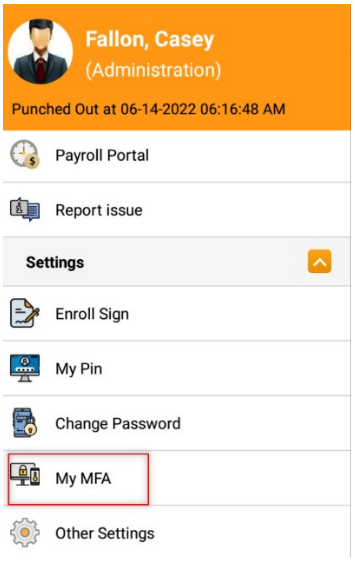


Please note, these additional email addresses and phone numbers will not change or override the data currently on file under Manage Users. These new contact methods will be saved in addition to the current information stored.

From the Mobile App

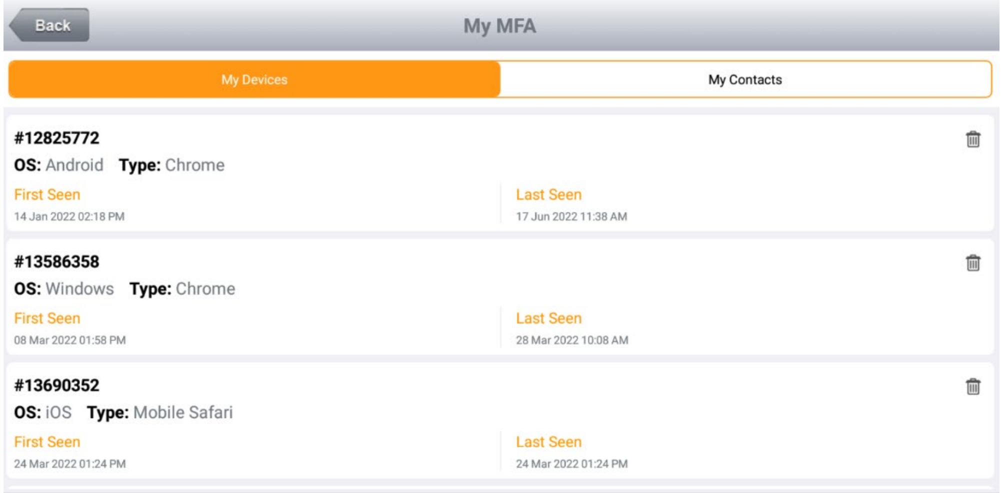
Stored contact information for a user can be updated from the mobile app by each user following these steps...

1. Login to digitalAGENCY™ Mobile.
2. From the menu, select My MFA.



3. The My MFA screen will provide the user with the ability to toggle between My Devices and My Contacts.

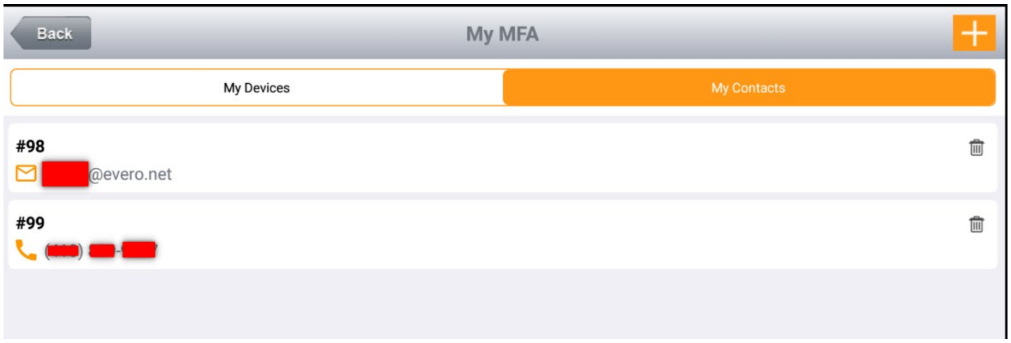
a. My Devices allows the user to manage their MFA approved devices and sessions.
b. My Contacts allows the user to manage their methods of contact.



#12825772
OS: Android **Type:** Chrome
First Seen 14 Jan 2022 02:18 PM
Last Seen 17 Jun 2022 11:38 AM

#13586358
OS: Windows **Type:** Chrome
First Seen 08 Mar 2022 01:58 PM
Last Seen 28 Mar 2022 10:08 AM

#13690352
OS: iOS **Type:** Mobile Safari
First Seen 24 Mar 2022 01:24 PM
Last Seen 24 Mar 2022 01:24 PM



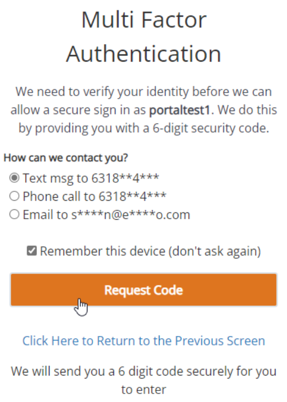
#98
✉ [redacted]@evero.net

#99
☎ ([redacted]) [redacted]-[redacted]

How to Log in with an MFA Enabled Account

The login process for an MFA Enabled Account will look like this…

1. The user will enter the login name and password and click Sign In when ready
2. Next, the Multi-factor Authentication screen will be displayed, and the user will be prompted to verify their identity by selecting a method of contact from the list provided. *Note: this list is generated from the information stored within the system.



Multi Factor Authentication

We need to verify your identity before we can allow a secure sign in as **portaltest1**. We do this by providing you with a 6-digit security code.

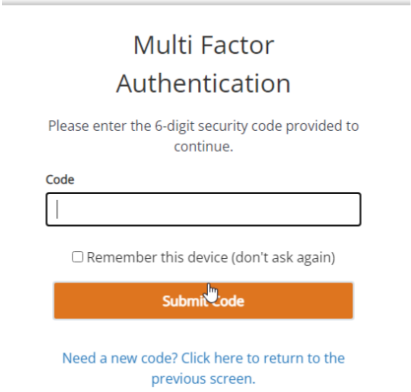
How can we contact you?

● Text msg to 6318**4***
○ Phone call to 6318**4***
○ Email to s****n@e****o.com

☑ Remember this device (don't ask again)

We will send you a 6 digit code securely for you to enter

3. Once the method of contact is selected, click Request Code. *Note: If you do not receive the code within a few minutes, please click the "Need a new code?" link provided.
4. Once received, enter the code into the field and click Submit Code to proceed.



Multi Factor Authentication

Please enter the 6-digit security code provided to continue.

Code

□ Remember this device (don't ask again)

Need a new code? Click here to return to the previous screen.

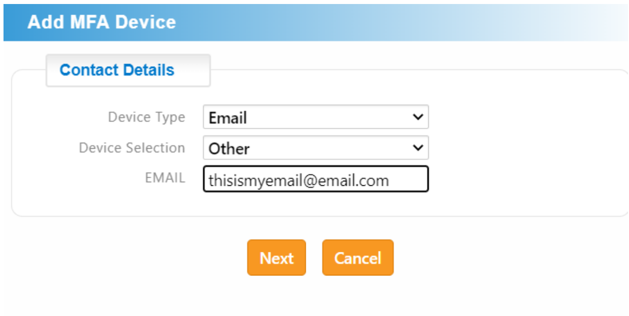
5. Once the code is confirmed, the user has been verified and access will be granted.

What Device Types (or Methods) are Supported for eVero MFA?

The following device types are eVero approved for MFA.

Email

Simply add your email address and retrieve the code sent to that address to confirm this method for MFA. Follow the on-screen instructions.



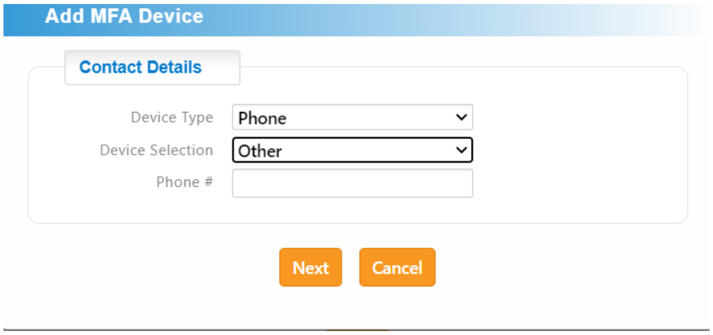
Device Type: Email

Device Selection: Other

EMAIL: thisismyemail@email.com

Phone

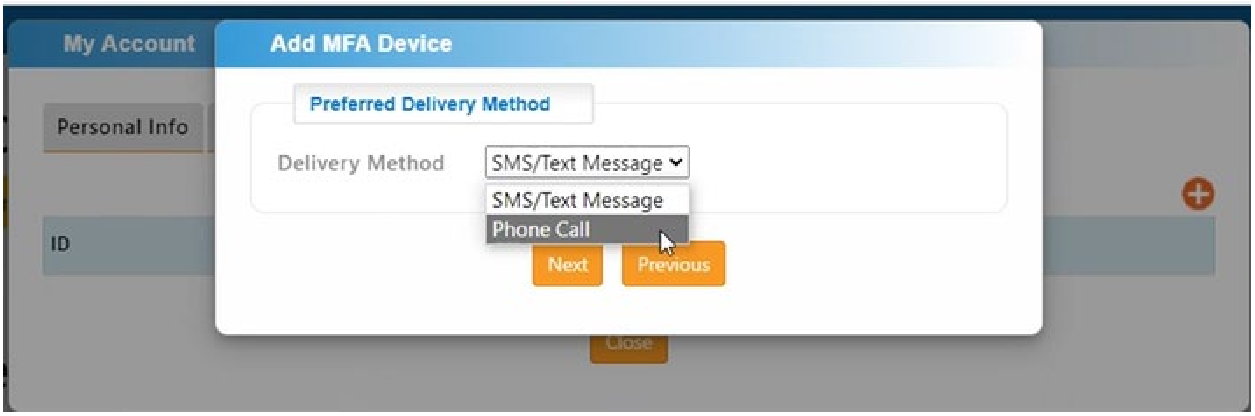
Users can add a phone number and then select whether this number will be used for SMS or voice call. Follow the on-screen instructions.



Device Type: Phone

Device Selection: Other

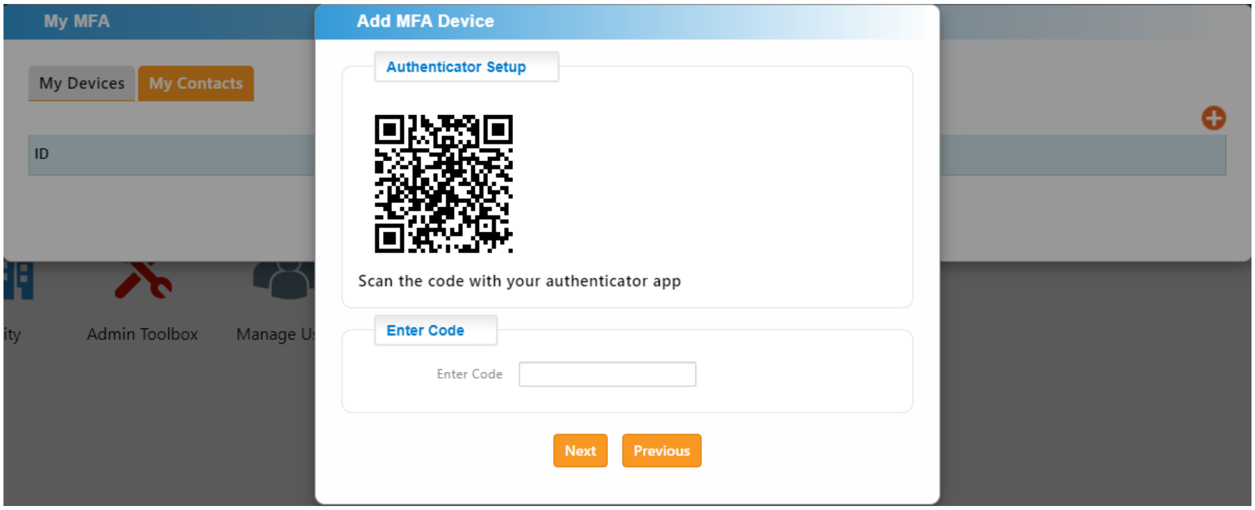
Phone #:



Delivery Method: SMS/Text Message

Authenticator

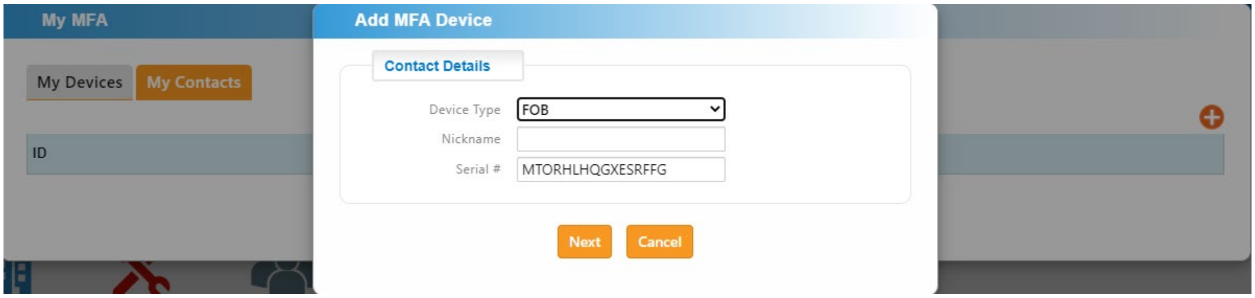
The use of a reputable Authenticator to support the MFA login is also an eVero approved method for verification. During setup, a QR code will be displayed and when scanned, a code will be generated. Enter that code in the field provided and follow the on-screen instructions. Examples of reputable Authenticators may include Google, Microsoft, and Authy.



Scan the code with your authenticator app

FOB

Adding an eVero FOB device is another approved method for MFA. When adding a FOB as an MFA Method to a user account, the user will be prompted to provide a nickname and to enter the FOB serial number. Interested in this method? Contact eVero for more details.



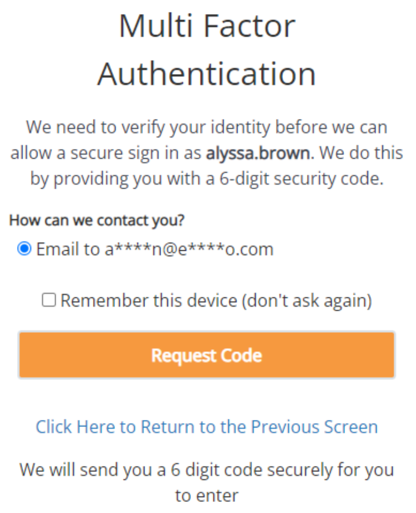
Device Type: FOB

Nickname:

Serial #: MTORHLHQGXESRFFG

How Often is MFA Needed to Log In to the eVero System?

If a user has signed into their account successfully using MFA and checked Remember this Device when doing so, they will not be prompted to login with the additional layer of security on that specific device for 90 days. If Remember this Device is not checked, then MFA will need to be used every time the account is accessed, regardless of the device used.



Multi Factor Authentication

We need to verify your identity before we can allow a secure sign in as **alyssa.brown**. We do this by providing you with a 6-digit security code.

How can we contact you?

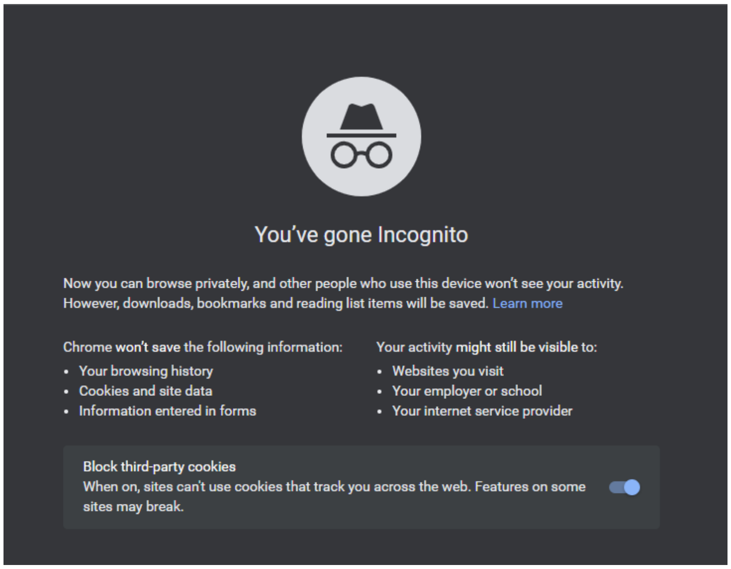
● Email to a****n@e****o.com

☐ Remember this device (don't ask again)

Click Here to Return to the Previous Screen

We will send you a 6 digit code securely for you to enter

Note: If a user were to log in to the system with their device in "Incognito" Mode, or private browsing mode, the system will not recognize this device and will be unable to bypass MFA if previously marked as Remember this Device. If a user were to clear their cookies/browser this would also cause MFA to be reauthenticated.



You've gone Incognito

Now you can browse privately, and other people who use this device won't see your activity. However, downloads, bookmarks and reading list items will be saved. Learn more

Chrome won't save the following information:

- Your browsing history
- Cookies and site data
- Information entered in forms

Your activity might still be visible to:

- Websites you visit
- Your employer or school
- Your internet service provider

Block third-party cookies

When on, sites can't use cookies that track you across the web. Features on some sites may break.

Step 2: Exploring Enrollment Options

Agencies have the option to decide how to roll out MFA for their users. There are two suggested routes, 1) Enable MFA for all users, all at once; or 2) Enable MFA for selected users by filtering through program and facility or sorting by username, name, or job title. In addition to educating and informing all users about MFA and ensuring up to date contact information is stored within the system prior to enabling MFA, Agencies must also decide what sort of roll out has the most potential for success.

Auto Option: Enabling MFA for All

This option allows the designated Agency MFA Manager(s) to turn MFA on for all affected users with just a few easy clicks!

Staggered Option: Enabling MFA for Selected Users

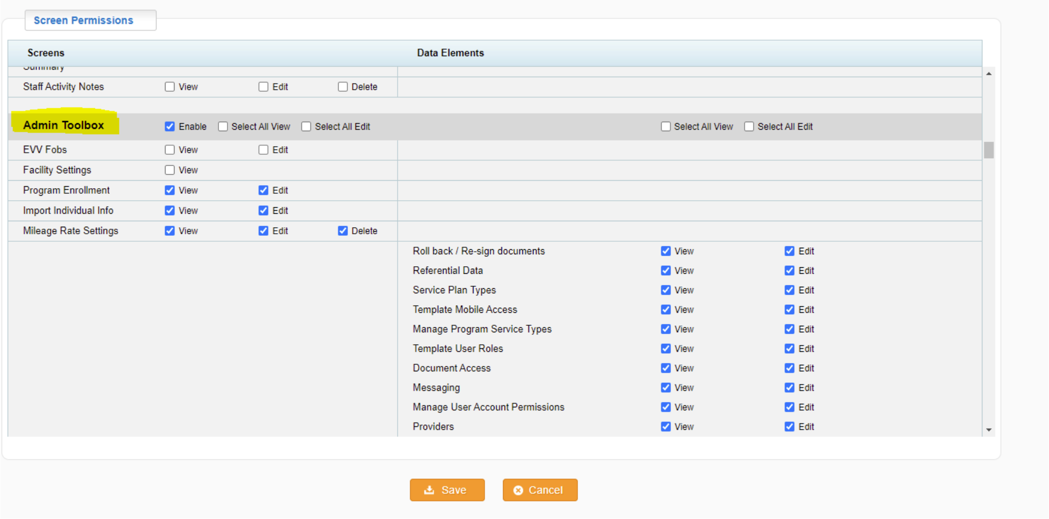
This option allows the designated Agency MFA Manager(s) to customize and stagger or phase in the addition of MFA to the login process by enabling MFA for certain groupings of users vs all at once. Example, Agencies opting to pursue the staggered approach will have the opportunity to enable MFA for a certain department first or a certain percentage of the alphabet if sorted by name.

Step 3: Implementing MFA & Enrolling Accounts

Establishing Permissions for Agency-Designated MFA Managers

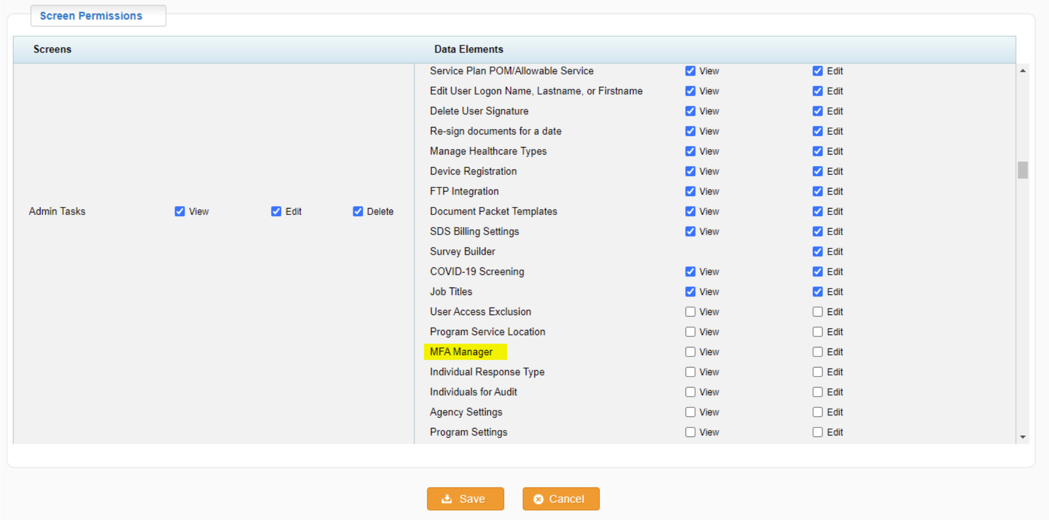
For an eVero system user to be able to enable MFA for others, they must first be provided with appropriate permissions that will allow access to MFA Management.

Open Manage Users from the All Apps Menu and select the user that will be responsible for enabling user accounts for MFA. Click on the desired username to open the User Security screen. Click Edit to enable editing of this users profile and scroll down to the Screen Permissions section. Under Admin Toolbox, locate MFA Manager and ensure that view/edit are checked. Click Save to confirm your changes.



Screen Permissions

Screens				Data Elements		
Staff Activity Notes	□ View	□ Edit	□ Delete			
Admin Toolbox	☑ Enable	□ Select All View	□ Select All Edit		□ Select All View	□ Select All Edit
EVV Fobs	□ View	□ Edit				
Facility Settings	□ View					
Program Enrollment	☑ View	☑ Edit				
Import Individual Info	☑ View	☑ Edit				
Mileage Rate Settings	☑ View	☑ Edit	☑ Delete			
				Roll back / Re-sign documents	☑ View	☑ Edit
				Referential Data	☑ View	☑ Edit
				Service Plan Types	☑ View	☑ Edit
				Template Mobile Access	☑ View	☑ Edit
				Manage Program Service Types	☑ View	☑ Edit
				Template User Roles	☑ View	☑ Edit
				Document Access	☑ View	☑ Edit
				Messaging	☑ View	☑ Edit
				Manage User Account Permissions	☑ View	☑ Edit
				Providers	☑ View	☑ Edit



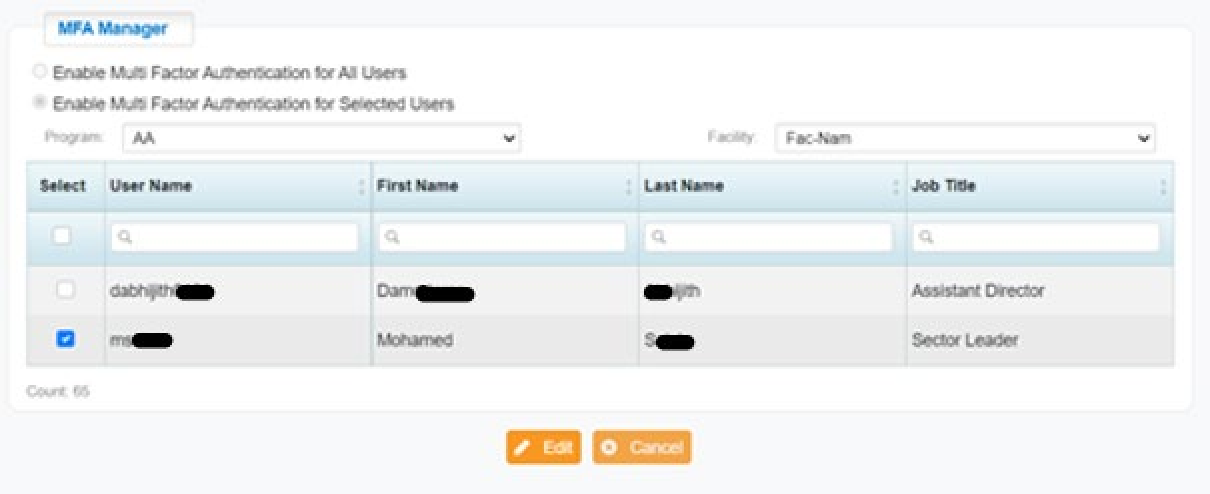
Screen Permissions

Screens				Data Elements		
Admin Tasks	☑ View	☑ Edit	☑ Delete	Service Plan POM/Allowable Service	☑ View	☑ Edit
				Edit User Logon Name, Lastname, or Firstname	☑ View	☑ Edit
				Delete User Signature	☑ View	☑ Edit
				Re-sign documents for a date	☑ View	☑ Edit
				Manage Healthcare Types	☑ View	☑ Edit
				Device Registration	☑ View	☑ Edit
				FTP Integration	☑ View	☑ Edit
				Document Packet Templates	☑ View	☑ Edit
				SDS Billing Settings	☑ View	☑ Edit
				Survey Builder		☑ Edit
				COVID-19 Screening	☑ View	☑ Edit
				Job Titles	☑ View	☑ Edit
				User Access Exclusion	□ View	□ Edit
				Program Service Location	□ View	□ Edit
				MFA Manager	□ View	□ Edit
				Individual Response Type	□ View	□ Edit
				Individuals for Audit	□ View	□ Edit
				Agency Settings	□ View	□ Edit
				Program Settings	□ View	□ Edit

Click Save to proceed. Repeat for other users, if needed.

Accessing the MFA Manager Screen in Admin Tasks

Once a user has been provided with access to the MFA Manager screen, that user will select Admin Toolbox from the All Apps menu and select MFA Manager from the Admin Tasks list that defaults once opened. The ability to manage enrollments for MFA will be conducted within this screen.



MFA Manager

○ Enable Multi Factor Authentication for All Users
● Enable Multi Factor Authentication for Selected Users

Program: AA
Facility: Fac-Nam

Select	User Name	First Name	Last Name	Job Title
☐				
☐	dabhijith[redacted]	Dam[redacted]	[redacted]ijith	Assistant Director
☑	ms[redacted]	Mohamed	S[redacted]	Sector Leader

Count: 65

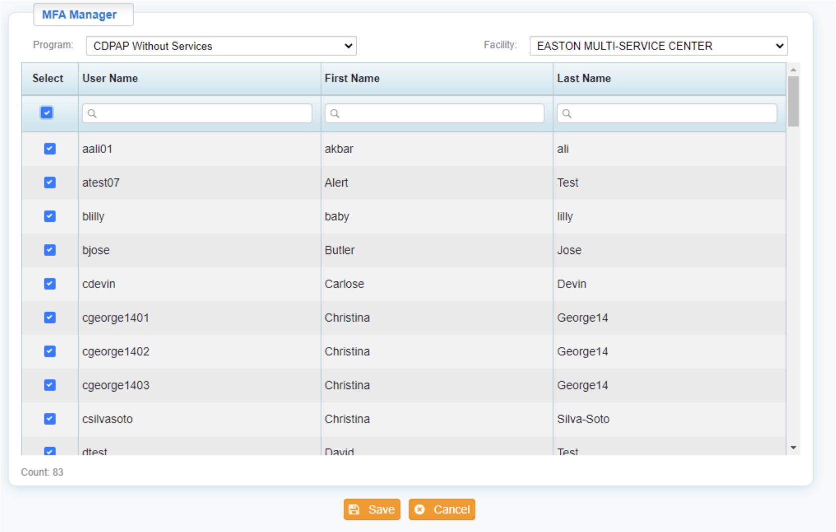
Enrolling User Accounts in MFA

Auto Enrollment: MFA for All

Agencies that wish to enable MFA for all, all at once, will open the MFA Manager and click Edit. Once in edit mode, the user will select the first radio button at the top of this screen to “Enable Multi-factor Authentication for All Users”. Click save to enroll all users in MFA.

Staggered Enrollment: MFA for Selected Users

Agencies that wish to enable MFA in a more staggered approach, (i.e. by department or a certain percentage of the alphabet for example), will open the MFA Manager and click Edit. Once in edit mode, the user will select the second radio button at the top of this screen to “Enable Multi-factor Authentication for Selected Users”. The MFA Manager now has the ability to decide which users will be enabled by utilizing the filtering and sorting options provided and by checking the box(es) to the left of the username for each desired account. Click save to enroll the selected users in MFA.



Program: CDPAP Without Services

Facility: EASTON MULTI-SERVICE CENTER

Select	User Name	First Name	Last Name
☑			
☑	aali01	akbar	ali
☑	atest07	Alert	Test
☑	blilly	baby	lilly
☑	bjose	Butler	Jose
☑	cdevin	Carlose	Devin
☑	cgeorge1401	Christina	George14
☑	cgeorge1402	Christina	George14
☑	cgeorge1403	Christina	George14
☑	csilvasoto	Christina	Silva-Soto
☑	dtest	David	Test

Count: 83

Troubleshooting and Support

Visit our website for further info on MFA. Stay diligent! Follow up with affected users in the first several days or even weeks when MFA is implemented to ensure all are finding success with accessing the system, as needed. Struggling? Reach out to support@evero.com.