MFA cAdmin Documentation

Version 1.5

June 2023

FOR PROFESSIONAL USE ONLY

Notice of non-liability:

Coe-Truman Technologies is providing the information in this document to you AS-IS with all faults. Coe-Truman Technologies makes no warranties of any kind (whether express, implied or statutory) with respect to the information contained herein. Coe-Truman Technologies assumes no liability for damages (whether direct or indirect), caused by errors or omissions, or resulting from the use of this document or the information contained in this document or resulting from the application or use of the product or service described herein. Coe-Truman Technologies reserves the right to make changes to any information herein without further notice.

Coe-Truman Technologies does not guarantee that the features described in this document will be announced or made available to anyone in the future.

Table of Contents

Summary of Document Changes

Date	Modifications	Document Version
01/11/2023	Baseline document for CTI Staff ONLY	1
01/12/2023	Removed the “My Work Computer Authenticator Option”	1.1
01/24/2023	Updated FAQs	1.2
03/09/2023	Document issued to Distributor Administrators and Association Administrators	1.3
5/10/2023	Updated terminology for clients	1.4
6/28/2023	Alternative Email MFA added	1.5

Function Summary

Multi-factor authentication (MFA) is a widely used security system that requires users to provide more than one form of authentication to access a system or service. For CTI and cOASIS, this will include something that the user knows (their username and password), and something that the user has (a security token from an app on a computer/phone/tablet). MFA ensures the security of CTI’s sensitive client information is being protected, making it more difficult for unauthorized users to gain access.

Choosing an MFA

A user has many options but can only choose one authenticator app for CTI/cOASIS login, which will provide different login steps. The recommended choices are:

- Google Authenticator – You can download the Google Authenticator app from the Play Store or App Store on your phone or tablet, which allows you to set up the MFA authentication used in this process.
- Microsoft Authenticator – You can download the Microsoft Authenticator app from the Play Store or App Store on your phone or tablet, which allows you to set up the MFA authentication used in this process.

Login Failing Reasons

Regardless of the MFA chosen, login will fail if the user’s password OR the 6-digit code is incorrect. Following best security practices, the CTI application will not notify the user which authentication component (user login, password, or MFA token) is wrong. CTI assigns usernames (emails) that “must enroll” to MFA, prompting you to enroll. If you do not see a prompt to enroll in MFA, please contact CTI.

MFA cOASIS Setup

Google Authenticator (Phone or Tablet)

Use the Google Authenticator app to get a verification code to enter every time you log in to CTI/cOASIS.

1. Install the latest version of the Google Authenticator app based on your operating system:
    a. Google Android. On your Android device, go to Google Play to download and install the Google Authenticator app.

    b. Apple iOS. On your Apple iOS device, go to the App Store to download and install the Google Authenticator app.
2. Use your computer to sign in with your username and password for CTI/cOASIS
3. Open the Google Authenticator app on your phone/tablet and accept any permissions.
4. On the Google Authenticator, select (+) in the bottom right-hand corner and either:
    a. Select “Scan a QR code” and point your camera at the QR code or
    b. Select “Enter a setup key” and input the Manual token
5. After your account appears in your Authenticator app, click Continue to input the CTI/cOASIS one-time code to sign in.
    a. The code resets every 30 seconds, so if you do not have enough time, retry with the reset code.
6. Click Continue once the authenticator app has added the new code.

Microsoft Authenticator (Phone or Tablet)

Use the Microsoft Authenticator app to get a verification code to enter every time you log in to CTI/cOASIS.

1. Install the latest version of the Microsoft Authenticator app based on your operating system:
    a. Google Android. On your Android device, go to Google Play to download and install the Microsoft Authenticator app.
    b. Apple iOS. On your Apple iOS device, go to the App Store to download and install the Microsoft Authenticator app.
2. Use your computer to sign in with your username and password for CTI/cOASIS
3. Open the Authenticator app on your phone/tablet and choose “Add Account” or select (+) in the upper right corner.
4. Select the “Work or school account” and choose either:
    a. Scan the QR code and point your camera at the QR code from step 2 or
    b. Scan the QR code and tap “Or enter code manually” to enter the Manual token code from step 2
5. After your account appears in your Authenticator app, click Continue to input the CTI/cOASIS one-time code to sign in.
    a. The code resets every 30 seconds, so if you do not have enough time, retry with the reset code.
6. Click Continue once the authenticator app has added the new code.

Returning MFA Login

1. Use your username and password to log in to CTI/cOASIS
2. Open either your Google or Microsoft Authenticator
3. Enter the 6-digit verification code labeled CTI/cOASIS and click Continue
    a. The code resets every 30 seconds, so if you do not have enough time, retry with the reset code.

Setting up MFA on Multiple Devices

Setting up multiple devices will enable users to see their 6-digit code simultaneously across two or more computers, phones, or tablets. This may be helpful for users who want multiple access points for backup options. Be sure only to use devices you regularly use, as anyone else with the device may be able to use your MFA and log in.

Please use the following support documentation from Google and Microsoft on setting up MFA on multiple devices:

Google MFA on Multiple Devices Documentation

Microsoft MFA on Multiple Devices Documentation

Resetting MFA

Resetting multi-factor authentication (MFA) is a necessary process that requires careful consideration and authorization due to the sensitive security implications involved. Only specific roles have the authority to reset an individual's MFA. These roles include:

- Association Administrator
- Distributor Administrator
- CTI Client Services Administrators

If an individual's MFA device has broken or been lost, they must contact one of the authorized roles above to reset their MFA.

Process for Resetting MFA

The authorized administrator role can follow these steps:

1. By default, each role required for MFA must use an authenticator app. If an administrator needs to reset a user's MFA, cAdmin will reset all their MFAs (both MFAs if set and alternate email).
2. If a Program Team Member or Team Leader is on-site and needs to reset their MFA, they should contact (call or email) the association helpdesk (or client queue). If it's a call, the person calling should verify their email address without being told what it is.
3. The administrator with the necessary resetting capabilities will be notified and confirm that an email will be sent to the user without disclosing their email address. To proceed, the Help Desk person, Distributor Administrator, Association Administrator, or CTI Client Services Administrator must know the person requesting the MFA reset.
4. The administrator will go to the user's Staff Account page (Settings -> Association info & administration -> Staff accounts) and select the "Reset MFA" action button.
5. This action will trigger an automated email to the user containing the standard cAdmin login link to reset their MFA. The email will notify the user that their MFAs have been reset and prompt them to create another MFA according to the same "new user initial setup MFA" process we already have. If the user doesn't create a new MFA in time, they will need to contact their association to reset their MFA again.
6. Upon the user's next login, they will be forced to create another Authentication App MFA. A notification email will be sent to the user confirming that their MFA has been reset.

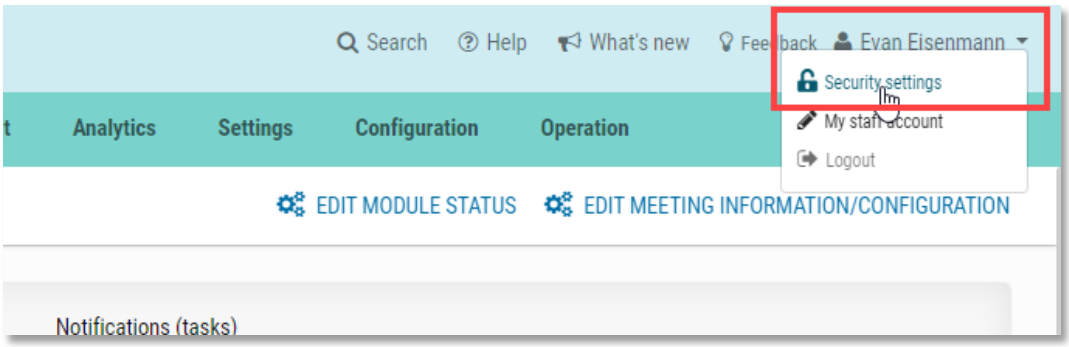
It is important to note that resetting an individual's MFA should only be done in the case of a broken or lost device. Resetting MFA for any other reason is not recommended, as this could compromise the security of the individual's account.

Alternative Email MFA

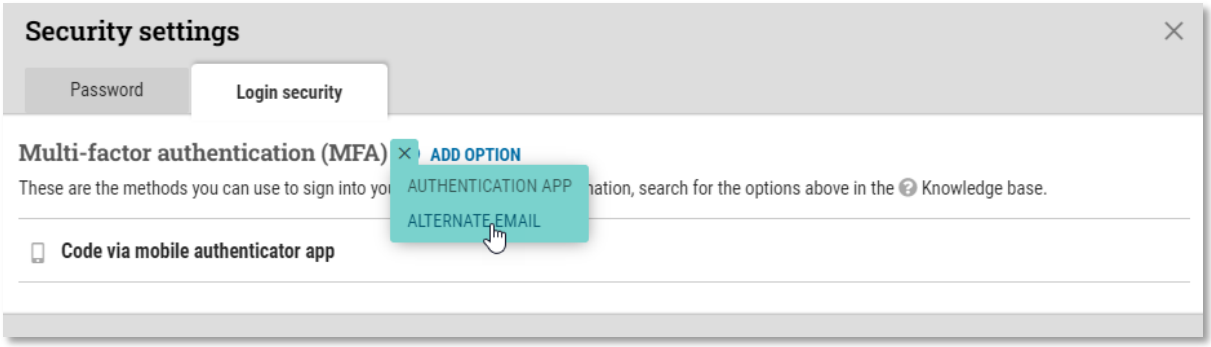
Once you have enabled your MFA authenticator, you may decide to exclusively utilize an Alternative Email MFA method going forward for cAdmin login. This method allows you to use a second email address to receive the 6-digit code.

To utilize the Alternative Email MFA method, follow these steps:

1. After logging in with an authenticator MFA used above, locate your name in the upper right-hand corner of the page and click on it.

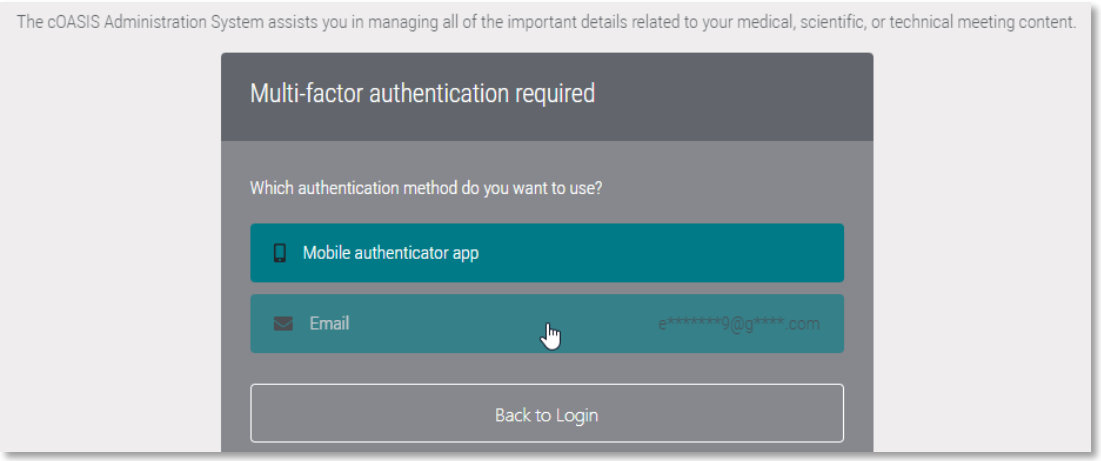


2. From the drop-down menu, select "Security settings."
3. Click on the "Login security" tab in the Security settings section.
4. Click on the "+ Add Option" button to add the "Alternate Email" option.



5. Enter an alternative email address. Please be aware that you cannot use the same email address that you use for signing into cAdmin.
6. To proceed, the system will ask you to provide the 6-digit code from your MFA authenticator app (e.g., Microsoft or Google) to verify that you are the person updating your MFA. Click "Continue."
7. Enter the verification code sent to your alternative email address. Click "Continue."
8. Close the dialog box and log out of cAdmin to test the new alternative email MFA.

9. You will see both the “Mobile authenticator app” and “Email” options available during login after entering your Username and Password.
10. Choose the "Email" option to have a verification code sent to your alternative email address.



11. Ensure that you use the verification code within 5 minutes of requesting it; otherwise, it will expire, and you will need to retry. Regardless of the MFA chosen, login will fail if the user’s password OR the 6-digit code is incorrect.

FAQs

Question: Do you have to use a phone or tablet as the second access point?
Answer: Using a phone or tablet is highly recommended.

Question: Can you have multiple MFA accounts?
Answer: Yes, but you only need one. The user should use an alternative device to set up another MFA account. You can set up an alternative MFA account for another device and an alternative email address under your username’s “Security settings” in the upper right-hand corner of cAdmin.

Question: I lost or broke my phone. How do I sign in?
Answer: Contact CTI, a Distributor Administrator, or your Association Administrator to walk you through the MFA re-enrollment process.

Question: Can I have MFA on multiple devices?
Answer: Yes, please see the above section, “Setting up MFA on Multiple Devices.” Google and Microsoft have their own documentation on how MFA can be set up on multiple devices (e.g., a phone and a tablet).

Question: Does MFA work on an airplane or when my phone’s on Airplane mode?
Answer: Yes, both Google and Microsoft Authenticator work on Airplane mode as long as the app is already downloaded and set up on your device.

Question: Does MFA work when Wi-Fi or cellular data is limited?
Answer: Yes, both Google and Microsoft Authenticator work when Wi-Fi or data is limited as long as the app is already downloaded and set up on your phone.

Question: What other app authenticators can I use?
Answer: Technically, any app authenticator that gives a code every 30 seconds should work, but we thoroughly tested Microsoft and Google. Apple authenticators are not recommended, but will work as well.