



CompuGroup™
Medical

Multi-Factor Authentication Instructions

March 05, 2024

CGM CONNECTION™
Patient Relationship Management



Table of Contents

- About this Document 3
- MFA Requirements 3
- MFA Setup Instructions 3
 - Authenticator Application Setup Instructions 4
 - Hardware Token Setup Instructions 9
 - Invalid MFA Security Code 11
- Logging in After Initial MFA Setup Completed 12
- Reset MFA for a User 13
 - Overwrite an Existing MFA Account 13
 - Removing an Existing MFA Account 14

ABOUT THIS DOCUMENT

This document includes detailed information for using Multi-Factor Authentication (MFA) with CGM CONNECTION. MFA is a multi-step account login process that requires users to authenticate their account with more than just a password to add an additional layer of security to help protect your data. If you are unable to deploy a mobile device application and require an alternative solution, please contact your sales team to discuss using a hardware token provided by CGM instead.

You must set up MFA with your first login to CGM CONNECTION after the release of version 2024.1.0

Note: Please verify that all pop-up blockers are turned off or you allow pop-ups from <https://cnx.cgmus.com/Account/Login>. If pop-up blockers are in place, a warning message displays indicating pop-ups are blocked and the login/MFA cannot proceed until corrected.

MFA REQUIREMENTS

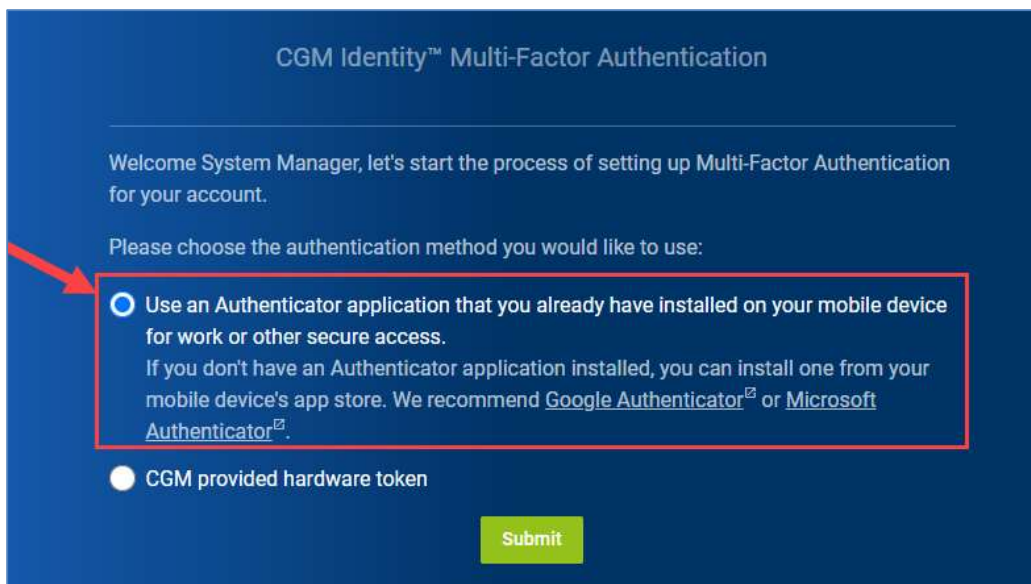
CGM CONNECTION requires a mobile device for each individual user that will log on to CGM CONNECTION with one of the following MFA apps installed:

- Microsoft Authenticator
- Google Authenticator

Alternate option is to use a hardware token provided by CGM.

MFA SETUP INSTRUCTIONS

Go to the CONNECTION login screen <https://cnx.cgmus.com/Account/Login> login and type your Username and Password and click **Login**. The log in process triggers MFA. Select the **Use an Authenticator application...** option unless you have contacted your Sales representative to make alternate arrangements for using a hardware token for MFA. Click **Submit**.



CGM Identity™ Multi-Factor Authentication

Welcome System Manager, let's start the process of setting up Multi-Factor Authentication for your account.


Please choose the authentication method you would like to use:

- Use an Authenticator application that you already have installed on your mobile device for work or other secure access.
If you don't have an Authenticator application installed, you can install one from your mobile device's app store. We recommend [Google Authenticator](#)² or [Microsoft Authenticator](#)².
- CGM provided hardware token

Submit

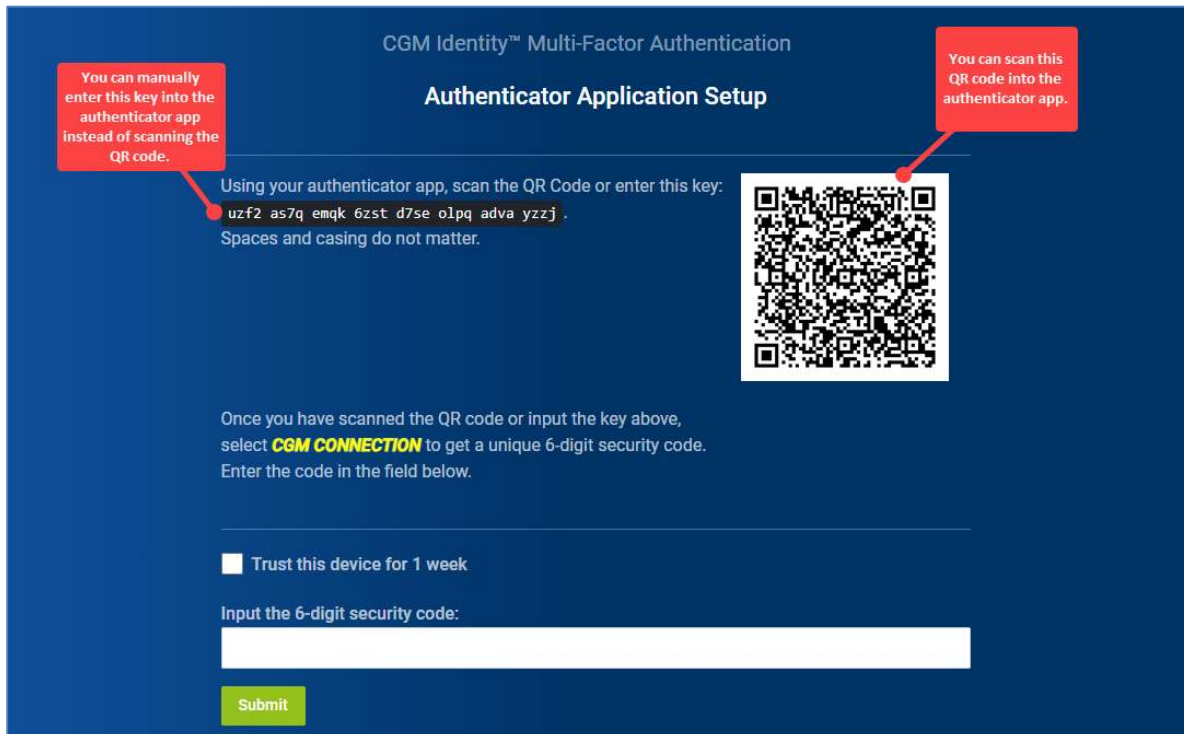
Authenticator Application Setup Instructions

The account name to be used in the Authenticator app automatically defaults with CGM CONNECTION but you can change it if you want. Click **Submit**.

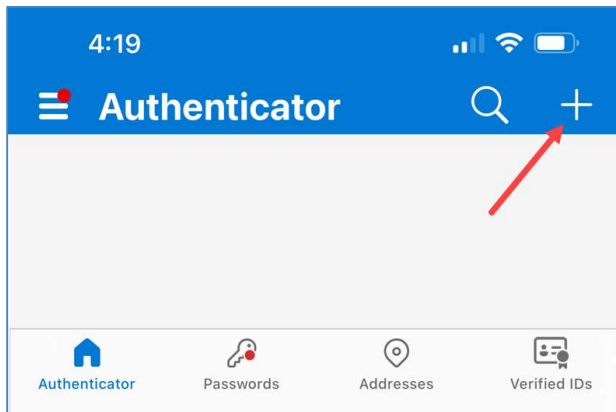


Note: You will not be permitted to log in to CGM CONNECTION without using an authentication method. If you need to exit the MFA process, exit completely out of the browser.

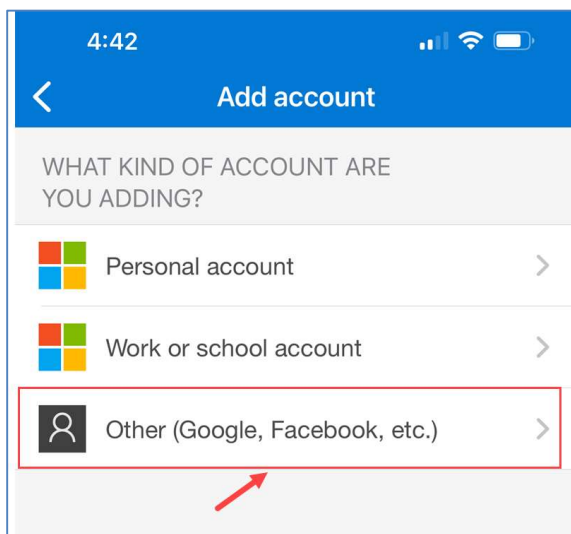
Next, you can either scan the QR code or manually enter the key in the Authenticator app.



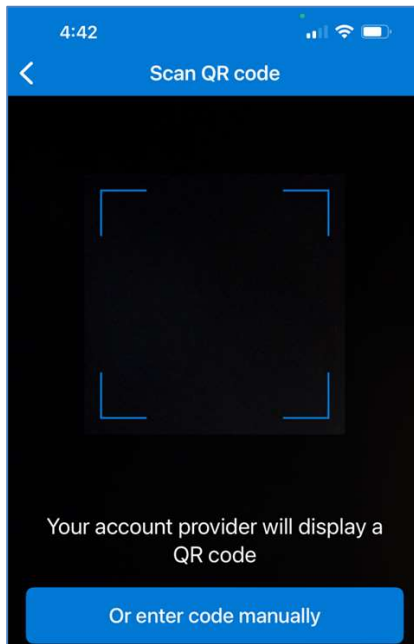
Open the Authenticator app on your mobile device. The following example is from Microsoft Authenticator. On the Authenticator screen, tap the **Add** icon (+ sign) to add an account in the Authenticator.



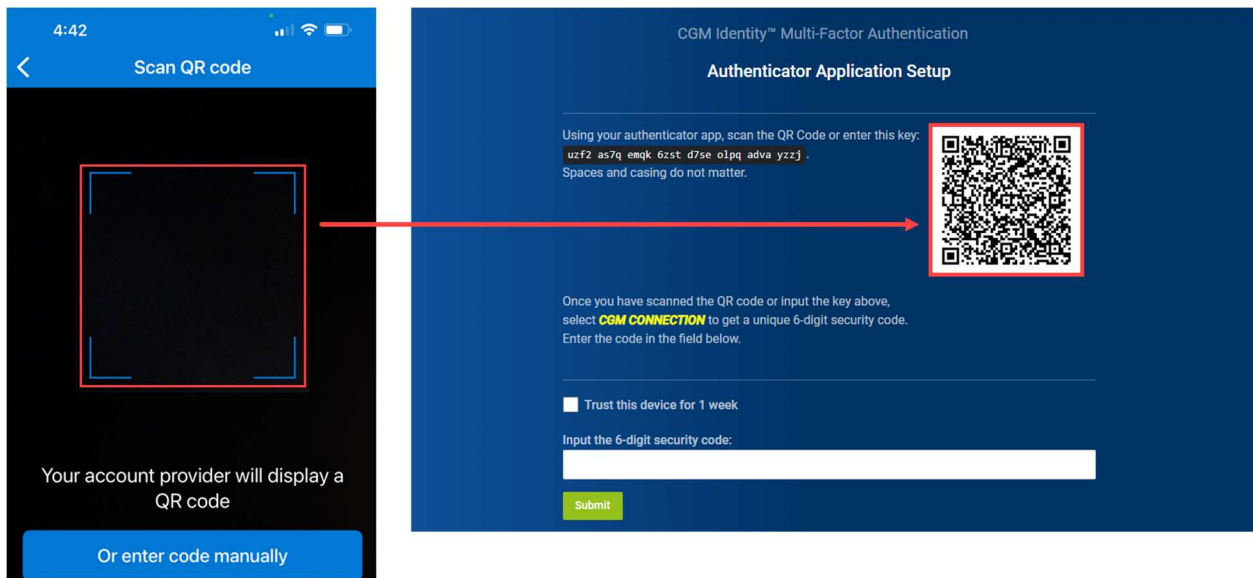
On the Add Account screen, tap **Other (Google, Facebook, etc.)**.



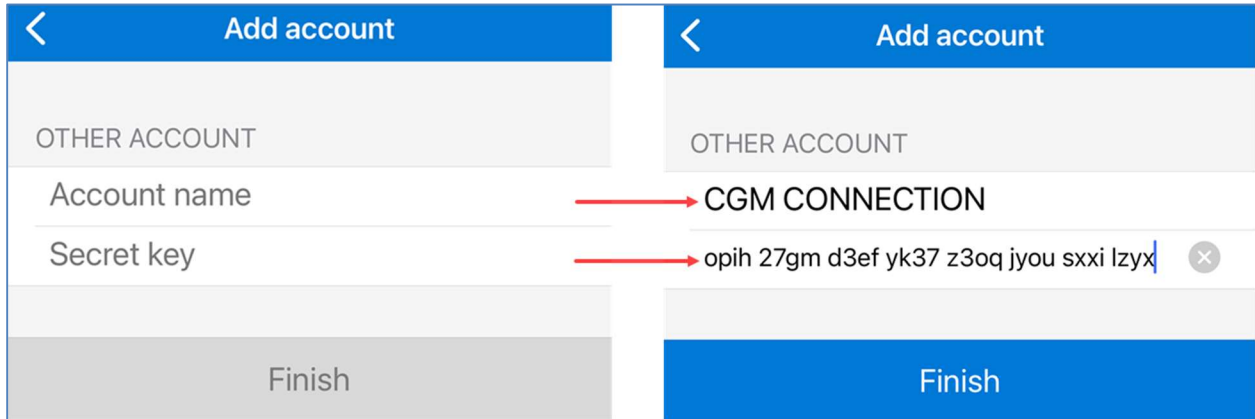
Either scan the QR code or tap the **Or enter code manually** button.



Example of scanning the QR code using the camera on your mobile device. Hold your mobile device close to the QR code on the **CGM Identity Multi-Factor Authentication** window and center it within the box on the **Scan QR code** screen to automatically add the MFA account to the authenticator app.



Example of manually entering the account name and key on your mobile device. Tap the **Or enter code manually** button on the **Scan QR code** screen. In the **Account name** field enter the account name to be used in the Authenticator app CGM CONNECTION and in the **Secret key** field enter the 32-character key shown on the **CGM Identity Multi-Factor Authentication** window.

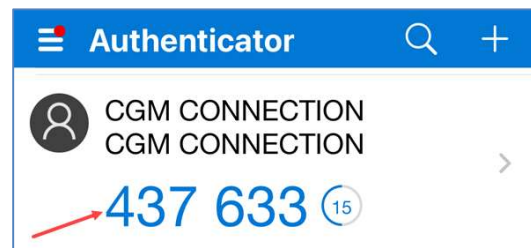


After the QR Code is scanned or you manually typed the key in, the authenticator app provides a 6-digit verification code that you will enter in the authentication screen. You will have 30 seconds to use the code before it is reset to a new code.

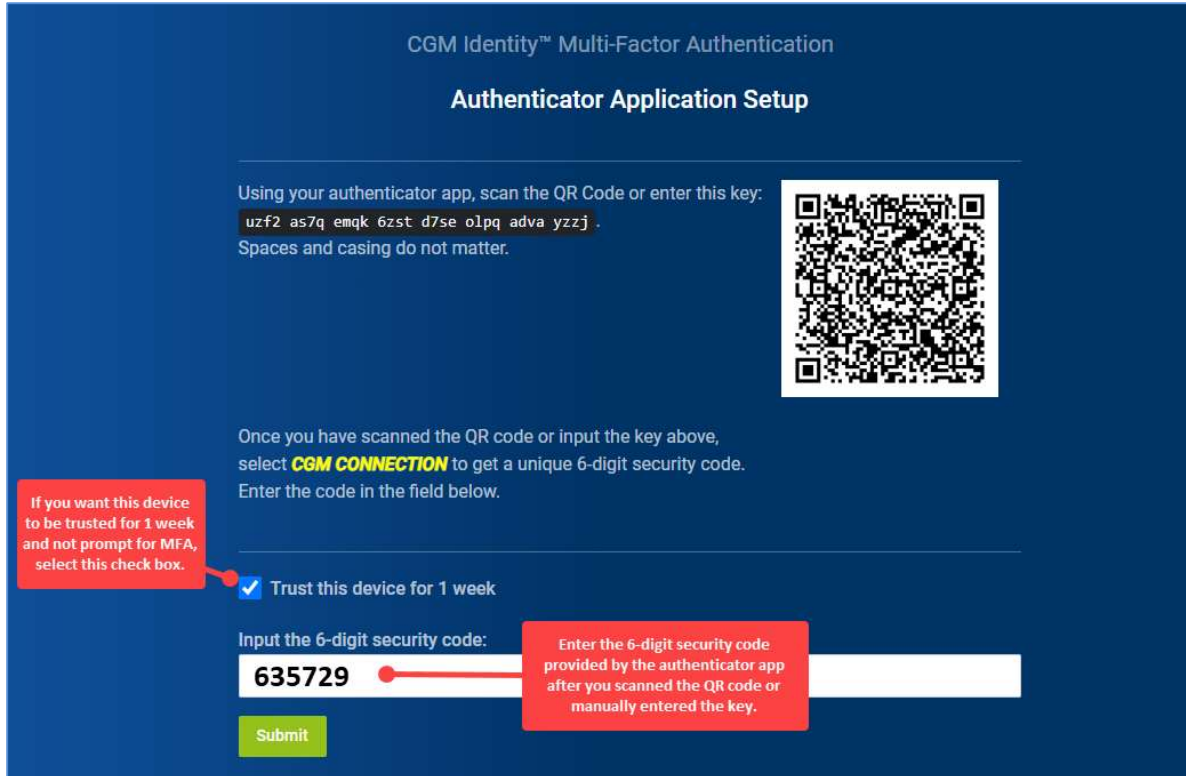
Example after scanning QR code:



Example after manually entering key:




If you want this device to be trusted for 1 week and not be prompted for MFA, select the **Trust this device for 1 week** check box (*otherwise the default setting is 12 hours*) and then enter the 6-digit security code (without any spaces-as shown below). As soon as you finish entering the code - without any errors, the screen automatically completes the MFA process. It is not necessary to click **Submit**.



CGM Identity™ Multi-Factor Authentication

Authenticator Application Setup

Using your authenticator app, scan the QR Code or enter this key:
`uzf2 as7q emqk 6zst d7se o1pq adva yzzj .`
Spaces and casing do not matter.



Once you have scanned the QR code or input the key above, select **CGM CONNECTION** to get a unique 6-digit security code. Enter the code in the field below.

Trust this device for 1 week

Input the 6-digit security code:

Submit

If you want this device to be trusted for 1 week and not prompt for MFA, select this check box.

Enter the 6-digit security code provided by the authenticator app after you scanned the QR code or manually entered the key.

When the authentication process is completed, you will be logged into CGM CONNECTION as normal.

Hardware Token Setup Instructions

If you made alternate arrangements to use a hardware token for MFA, select the CGM provided hardware token option. Click **Submit**.



CGM Identity™ Multi-Factor Authentication

Welcome System Manager, let's start the process of setting up Multi-Factor Authentication for your account.

Please choose the authentication method you would like to use:

- Use an Authenticator application that you already have installed on your mobile device for work or other secure access.
If you don't have an Authenticator application installed, you can install one from your mobile device's app store. We recommend [Google Authenticator](#) or [Microsoft Authenticator](#).
- CGM provided hardware token**

Submit

The account name to be used for your hardware token automatically defaults with CGM CONNECTION but you can change it if you want. Enter the 32-character code provided by CGM for your hardware token. Click **Submit**.



CGM Identity™ Multi-Factor Authentication

Hardware Token Setup

How would you like to refer to your Hardware Token for this MFA setup?

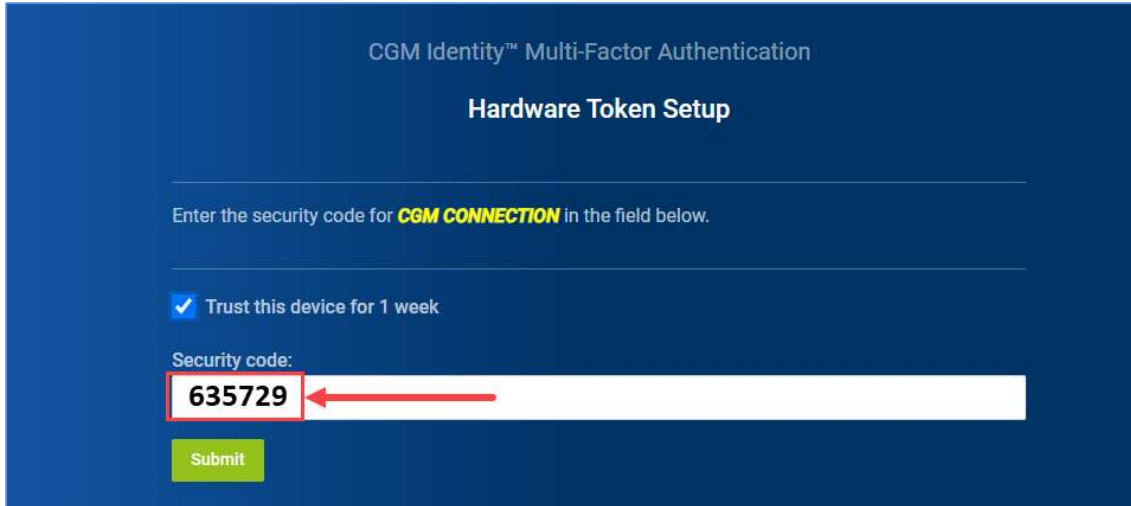
CGM CONNECTION

Enter the 32 character code that was provided with the Hardware Token:

JBSWY3DPEHPK3PXPJBSWY3DPEHPK3PXP

Submit

If you want this device to be trusted for 1 week and not be prompted for MFA, select the **Trust this device for 1 week** check box (*otherwise the default setting is 12 hours*) and then enter the 6-digit security code (without any spaces-as shown below). As soon as you finish entering the code - without any errors, the screen automatically completes the MFA process. It is not necessary to click **Submit**.



CGM Identity™ Multi-Factor Authentication

Hardware Token Setup

Enter the security code for **CGM CONNECTION** in the field below.

Trust this device for 1 week

Security code:

Submit

When the authentication process is completed, you will be logged into CGM CONNECTION as normal.

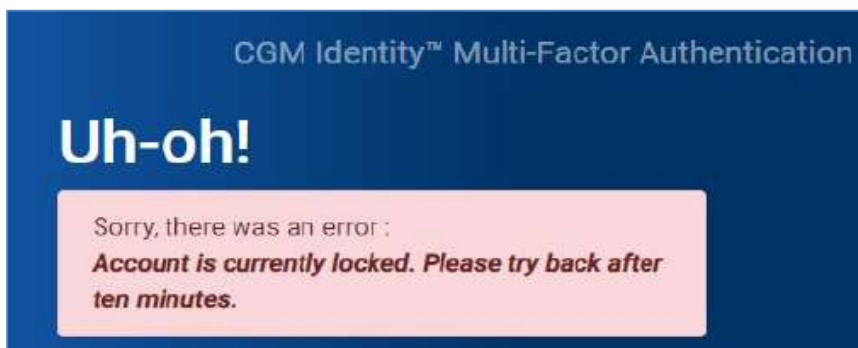
Invalid MFA Security Code

If you enter the security code incorrectly an **Invalid Code** message will display and you will need to re-enter the correct code. You may have entered the code incorrectly or the code updated in the authenticator app on your mobile device or on the hardware token before you completed the entry. Verify that you have entered the code correctly or wait for the code to update on the authenticator app or hardware token and enter the new code.



If you enter an incorrect code three consecutive times during the same log in attempt, you will be locked out of CGM CONNECTION for 10 minutes. After the lockout period is over, log back in to CGM CONNECTION and enter the correct six-digit code displayed on the authenticator app.

If the issue persists or if you have any questions, please contact Customer Support.

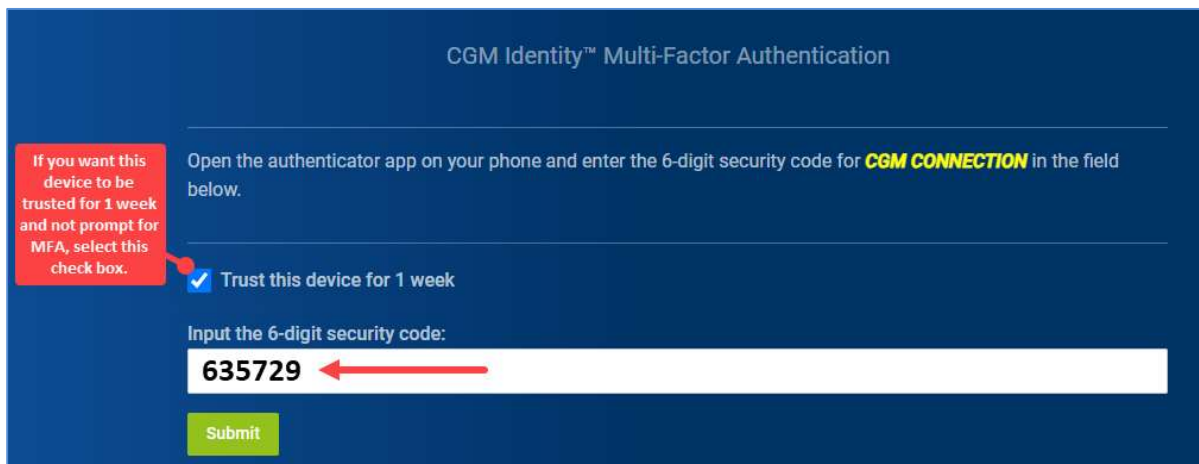


LOGGING IN AFTER INITIAL MFA SETUP COMPLETED

After you have completed the *MFA Setup Instructions*, when you log in in the future the login process will only require you to enter the 6-digit security code from the authenticator app or hardware token on an ongoing basis (*every 12 hours or after 1 week if you selected to trust your device for 1 week during setup*).

Go to the CONNECTION login screen <https://cnx.cgmus.com/Account/Login> and type your Username and Password and click **Login**.

Open the Authenticator app on your mobile device or access your hardware token. The following example is from Microsoft Authenticator. If you want this device to be trusted for 1 week and not be prompted for MFA, select the **Trust this device for 1 week** check box (*otherwise the default setting is 12 hours*) and then enter the 6-digit security code from the authenticator app (without any spaces-as shown below). As soon as you finish entering the code - without any errors, the screen automatically completes the MFA process. It is not necessary to click **Submit**.



You will be logged into CGM CONNECTION as normal.

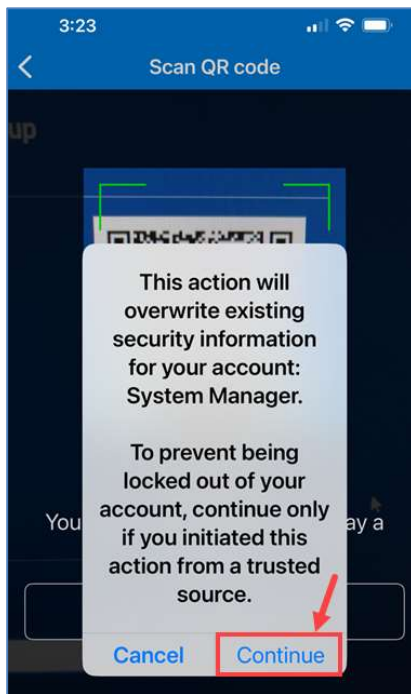
RESET MFA FOR A USER

If a User's MFA needs to be reset, please contact Customer Support.

When the reset is complete you can instruct the User to perform the Multi-Factor Authentication setup steps again.

Overwrite an Existing MFA Account

If MFA was reset for your User code in CGM CONNECTION and you are performing the Multi-Factor Authentication setup steps again, after you scan the QR code or manually type the key you will be informed the existing security information for your account will be overwritten in the Authenticator app. Click **Continue** and proceed with the remaining setup steps.



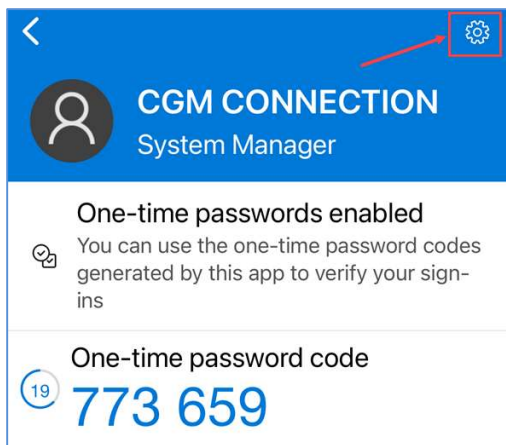
Note: When repeating the setup steps, if you happened to change the **Account Name** on the **CGM Identity Multi-Factor Authentication** window, the original MFA account that was created will not be overwritten and a new MFA account will be created in the authenticator app. The original MFA account will no longer be valid to log in to CGM CONNECTION though and should be removed.

Removing an Existing MFA Account

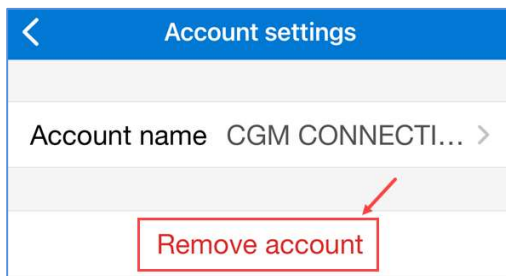
To remove an account from the Authenticator app on your mobile device, open the Authenticator app on your phone. On the Authenticator screen, tap on the name of the account to be removed or the right-arrow.



Tap the **Settings** icon.



Tap **Remove account**.



Tap **Continue**.

