Multi-Factor Authentication Instructions

August 06, 2024

CGM webPRACTICE™

Fully Web-Based Practice Management Suite

Table of Contents

ABOUT THIS DOCUMENT

This document includes detailed information for using Multi-Factor Authentication (MFA) with CGM webPRACTICE. 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.

MFA is required for all Hosted clients and Self-Hosted clients have the option to enable the functionality using the *Mult-Factor Authentication Integration* function.

If you are unable to deploy a mobile device application and require an alternative solution, please contact your sales team to discuss this further.

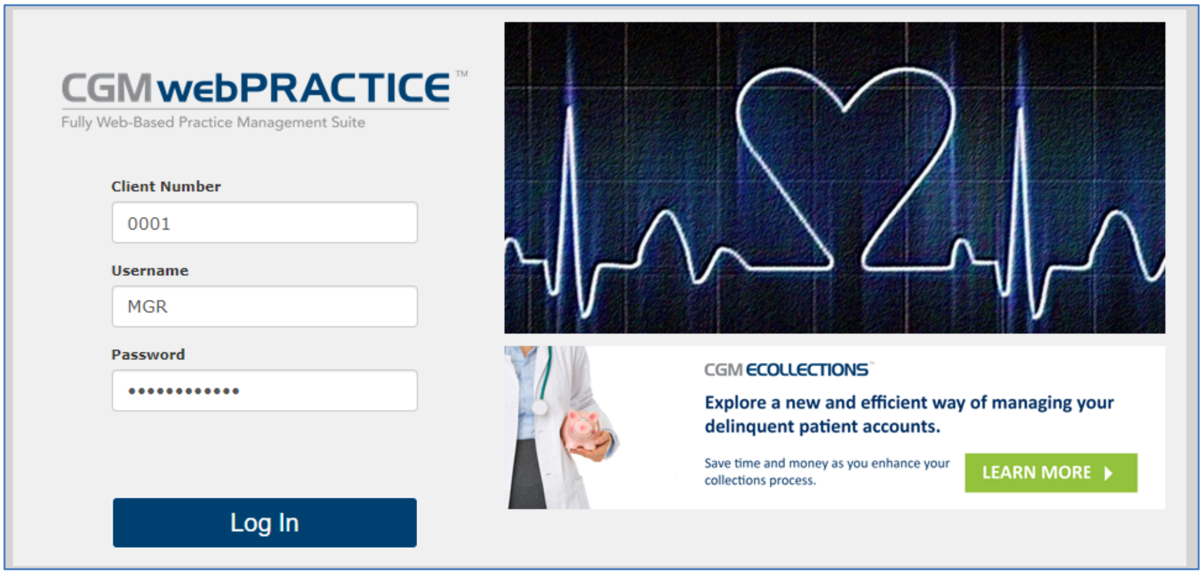
MFA REQUIREMENTS

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

- Microsoft Authenticator
- Google Authenticator

MFA SETUP INSTRUCTIONS

Access the Login page for CGM webPRACTICE. Enter your Client Number, Username and Password and click **Log In**.



CGM webPRACTICE™
Fully Web-Based Practice Management Suite

Client Number: 0001

Username: MGR

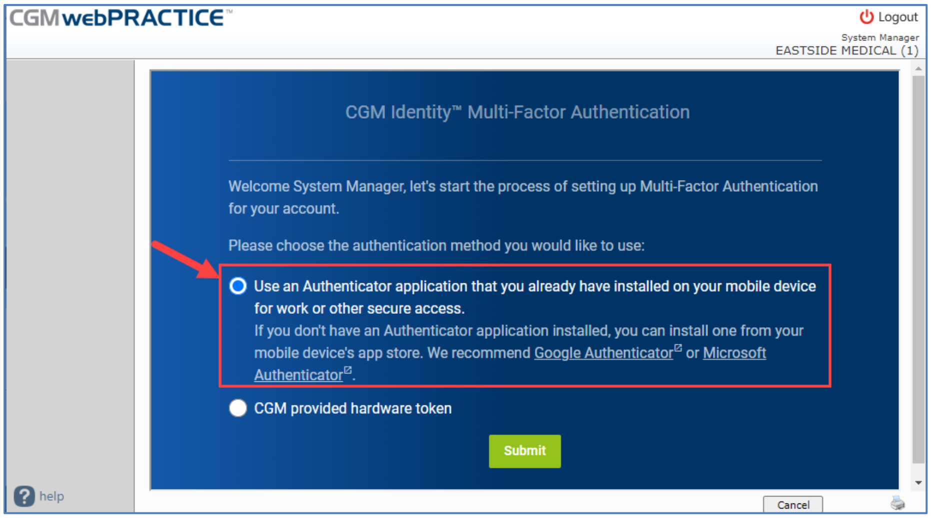
Password: ••••••••••••

Log In
CGM ECOLLECTIONS
Explore a new and efficient way of managing your delinquent patient accounts.
Save time and money as you enhance your collections process.
LEARN MORE

The log in process triggers MFA.

For detailed instructions, click **Help** in the lower-left corner.

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.

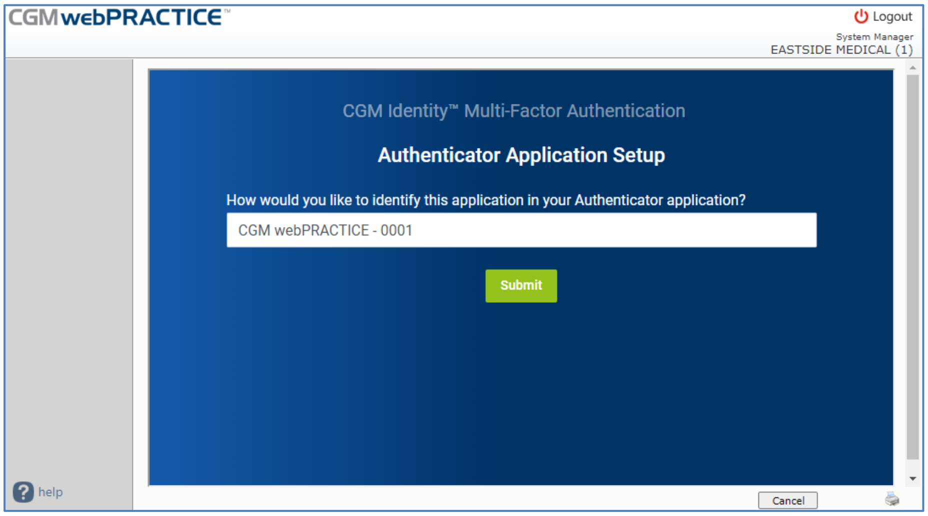
Please choose the authentication method you would like to use:

○ 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 or Microsoft Authenticator.

○ CGM provided hardware token

Authenticator Application Setup Instructions

The account name to be used in the Authenticator app automatically defaults with CGM webPRACTICE – (*Client #*) but you can change it if you want. Click **Submit**. The authenticator app login is valid for a 30-minute duration. After you have logged in, MFA will not prompt again for 30 minutes.



CGM Identity™ Multi-Factor Authentication

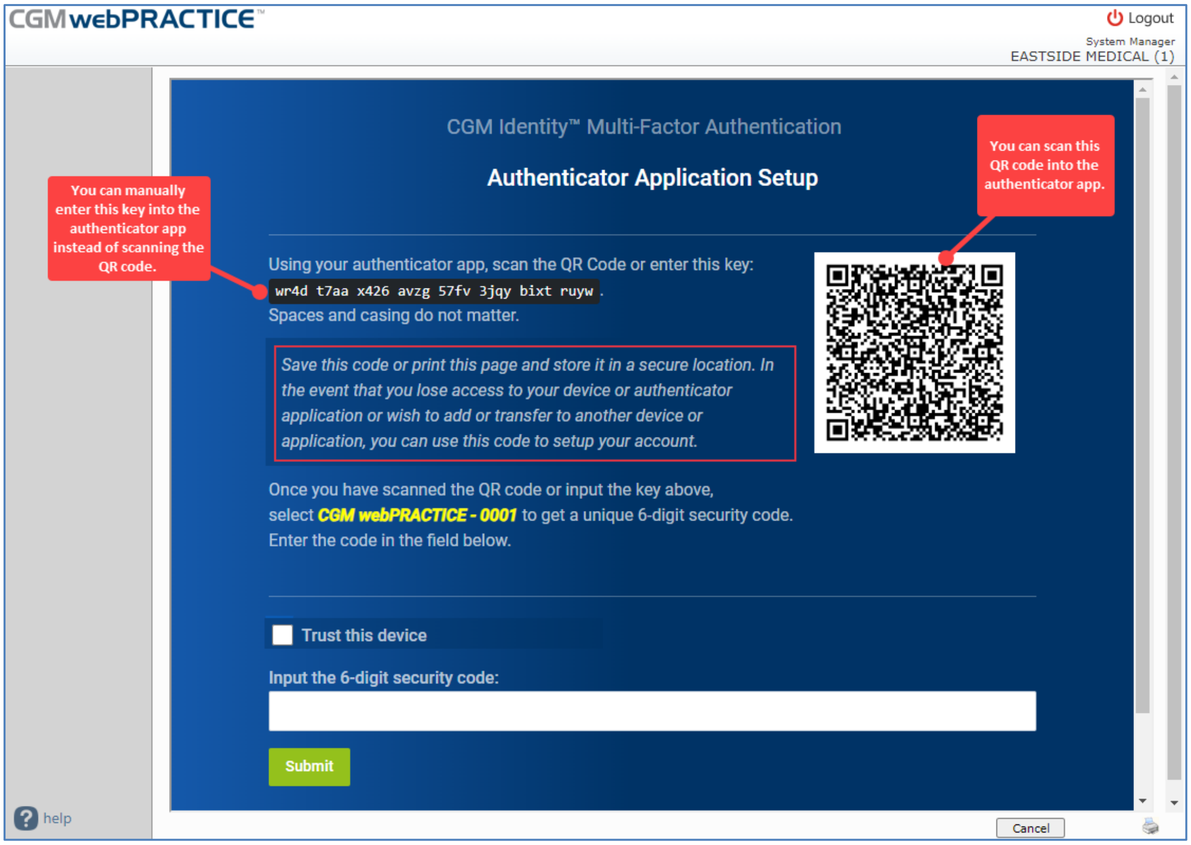
Authenticator Application Setup

How would you like to identify this application in your Authenticator application?

CGM webPRACTICE - 0001

Note: You will not be permitted to log in to CGM webPRACTICE without using an authentication method. If you need to exit the MFA process, click **Logout** in the upper-right corner.

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



You can manually enter this key into the authenticator app instead of scanning the QR code.

You can scan this QR code into the authenticator app.

CGM Identity™ Multi-Factor Authentication

Authenticator Application Setup

Using your authenticator app, scan the QR Code or enter this key:
`wr4d t7aa x426 avzg 57fv 3jqy bixt ruyw`.
Spaces and casing do not matter.

Save this code or print this page and store it in a secure location. In the event that you lose access to your device or authenticator application or wish to add or transfer to another device or application, you can use this code to setup your account.

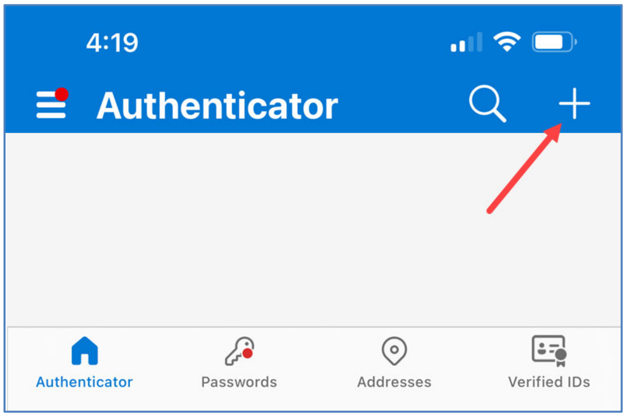
Once you have scanned the QR code or input the key above, select ***CGM webPRACTICE - 0001*** to get a unique 6-digit security code. Enter the code in the field below.

□ Trust this device

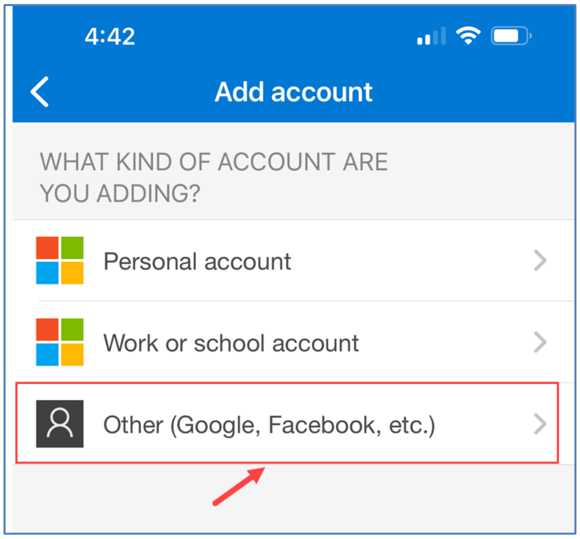
Input the 6-digit security code:

Submit

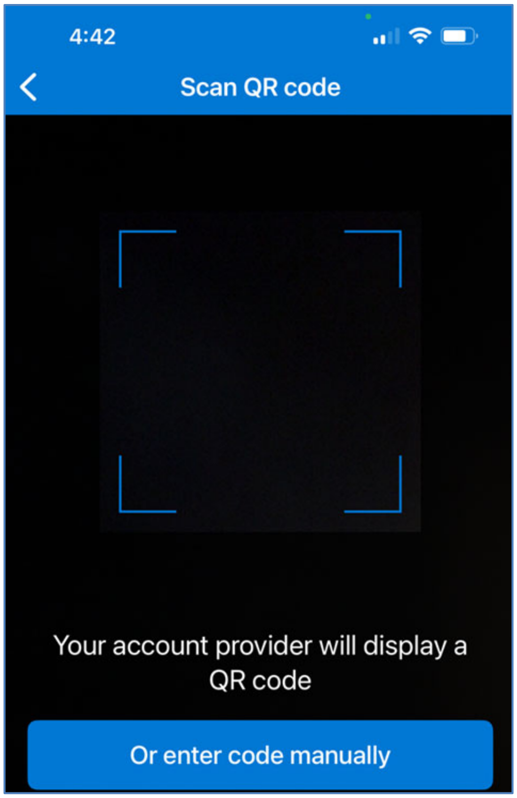
Open the Authenticator app on your phone. The following example is from Microsoft Authenticator. On the Authenticator screen, tap the **Add** icon (**+** sign) to add an account in the Authenticator.



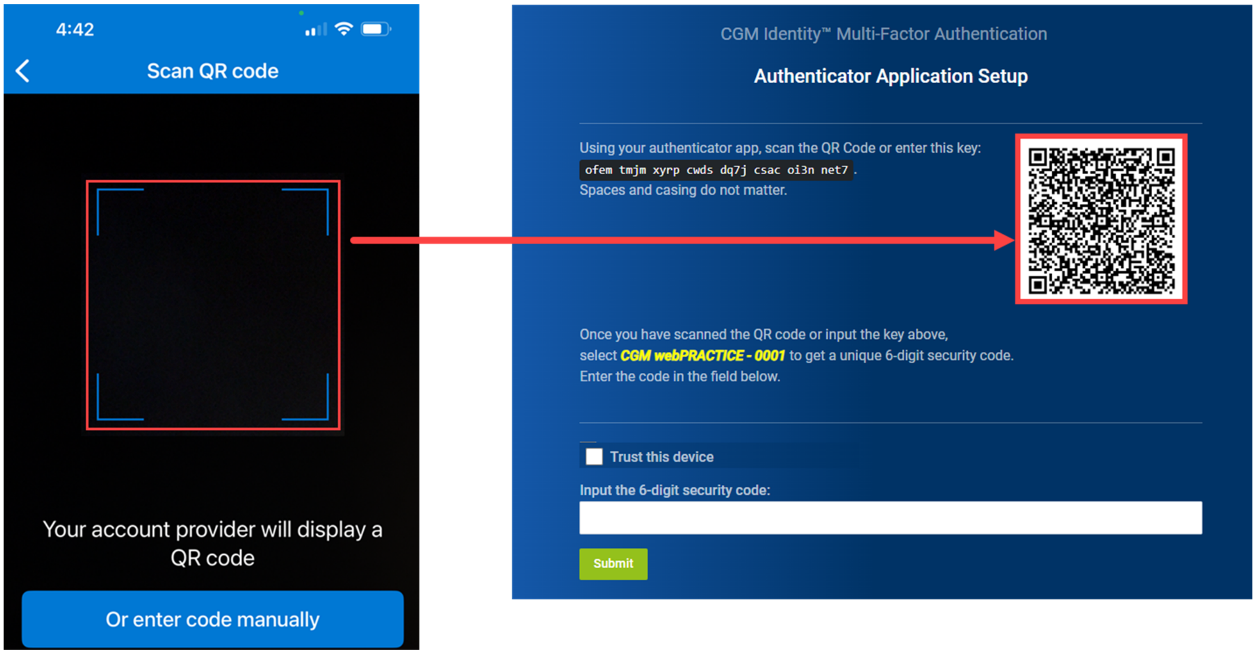
On the Add Account screen, tap **Other (Google, Facebook, etc.)**.


4:42
Add account
WHAT KIND OF ACCOUNT ARE YOU ADDING?
Personal account
Work or school account
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 Identidy 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.



Your account provider will display a QR code

CGM Identity™ Multi-Factor Authentication

Authenticator Application Setup

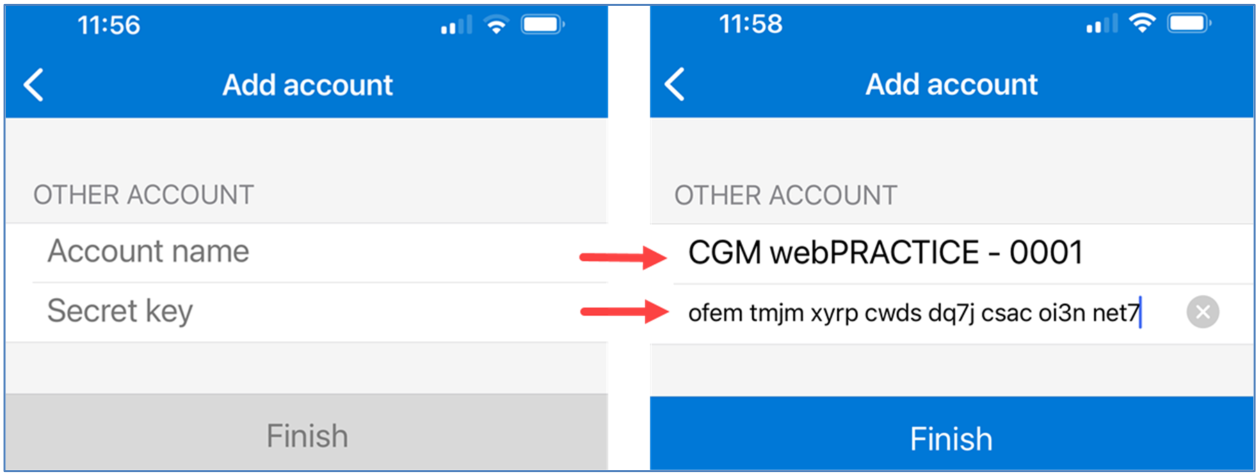
Using your authenticator app, scan the QR Code or enter this key: `ofem tmjm xyrp cwds dq7j csac oi3n net7` . Spaces and casing do not matter.

Once you have scanned the QR code or input the key above, select ***CGM webPRACTICE - 0001*** to get a unique 6-digit security code. Enter the code in the field below.

□ Trust this device

Input the 6-digit security code:

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 webPRACTICE – (*your Client #*) and in the **Secret key** field enter the 32-character key shown on the **CGM Identidy Multi-Factor Authentication** window.

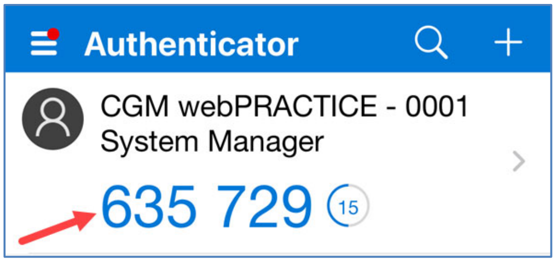


CGM webPRACTICE - 0001

ofem tmjm xyrp cwds dq7j csac oi3n net7

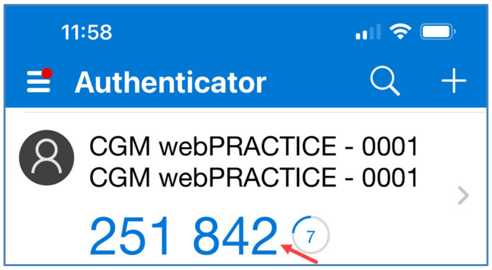
After the QR Code is scanned or you manually typed the key in, the authenticator app provides a 6-digit verification code that you will enter in the authentication screen. You will have 30 seconds to use the code before it is reset to a new code.

Example after scanning QR code:



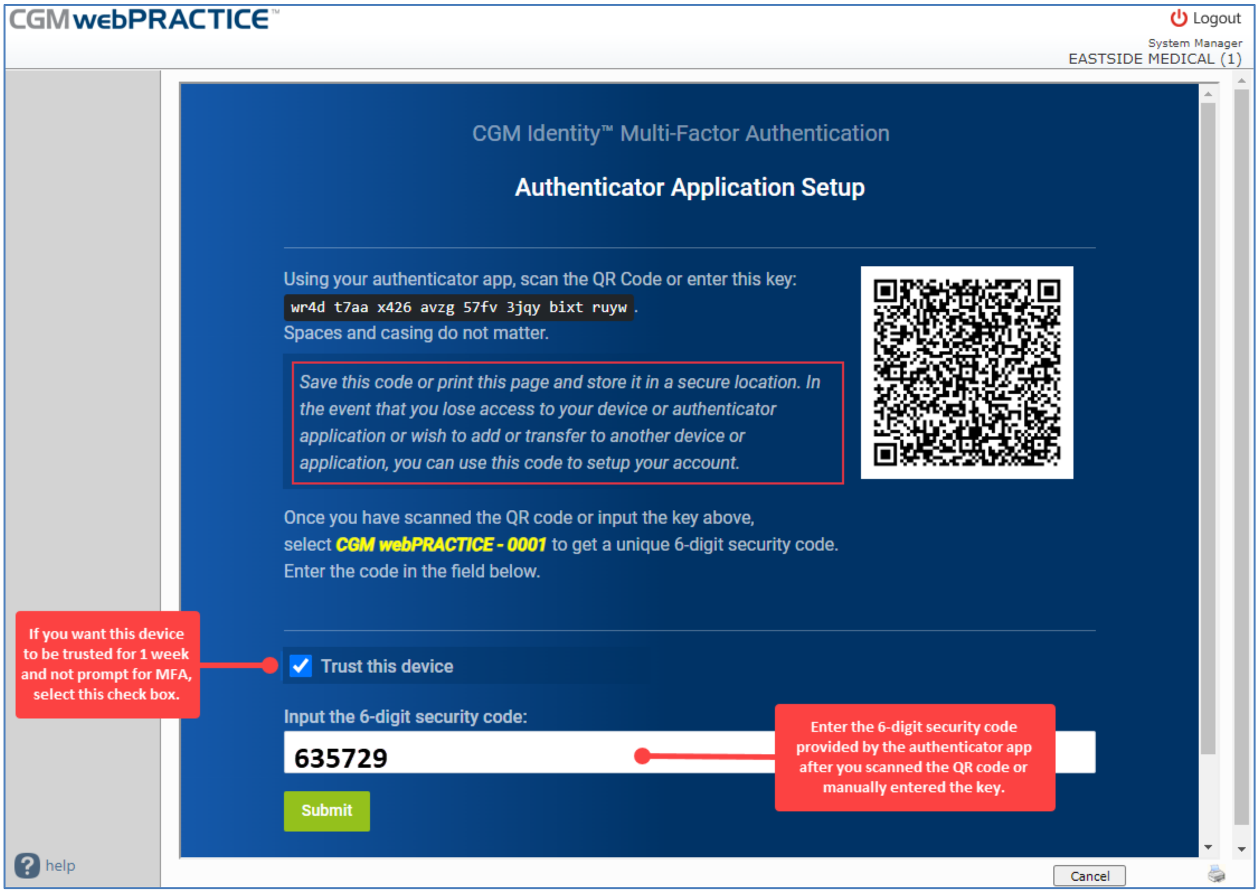
CGM webPRACTICE - 0001
System Manager
635 729 15

Example after manually entering key:



CGM webPRACTICE - 0001
CGM webPRACTICE - 0001
251 842 7

If you want this device to be trusted (default is set to 7 days) and not be prompted for MFA, select the **Trust this device** check box 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: `wr4d t7aa x426 avzg 57fv 3jqy bixt ruyw` .
Spaces and casing do not matter.

Save this code or print this page and store it in a secure location. In the event that you lose access to your device or authenticator application or wish to add or transfer to another device or application, you can use this code to setup your account.

Once you have scanned the QR code or input the key above, select ***CGM webPRACTICE - 0001*** to get a unique 6-digit security code. Enter the code in the field below.

☑ Trust this device

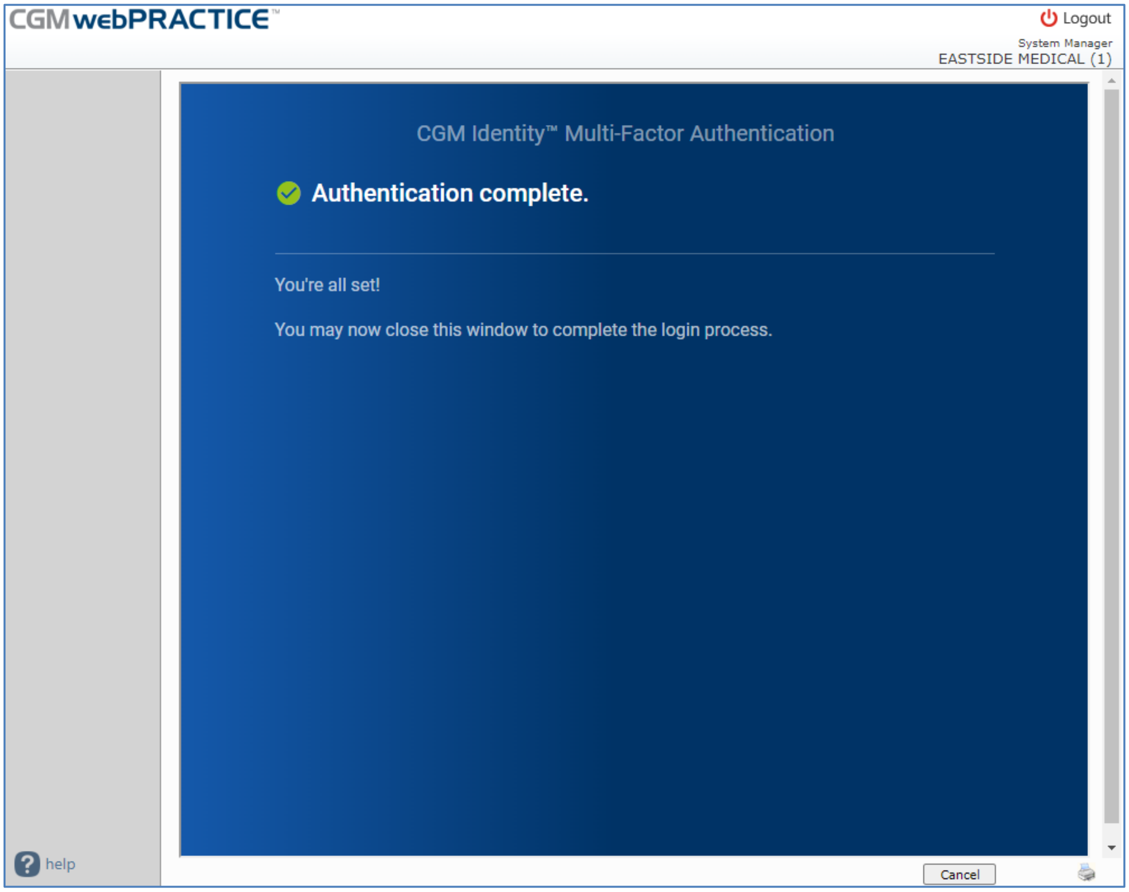
Input the 6-digit security code:
635729

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, the following screen will display for a couple of seconds and then you will be logged into CGM webPRACTICE as normal.



CGM Identity™ Multi-Factor Authentication

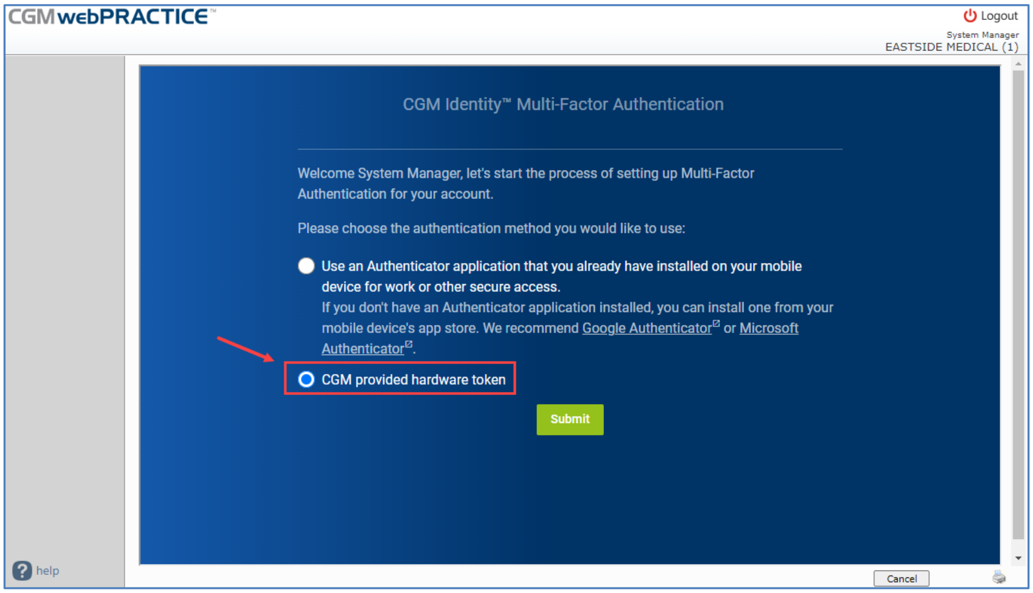
✓ Authentication complete.

You're all set!

You may now close this window to complete the login process.

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

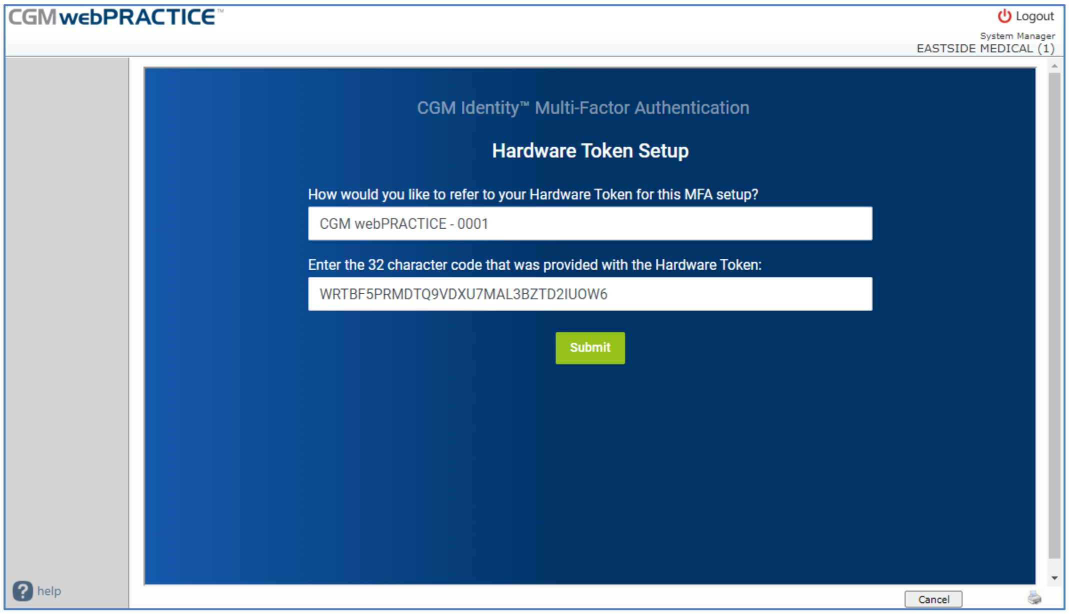
Welcome System Manager, let's start the process of setting up Multi-Factor Authentication for your account.

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

The account name to be used for your hardware token automatically defaults with CGM webPRACTICE – (*Client #*) but you can change it if you want. Enter the 32-character code provided by CGM for your hardware token. Click **Submit**. The authenticator app login is valid for a 30-minute duration. After you have logged in, MFA will not prompt again for 30 minutes.



CGM Identity™ Multi-Factor Authentication

Hardware Token Setup

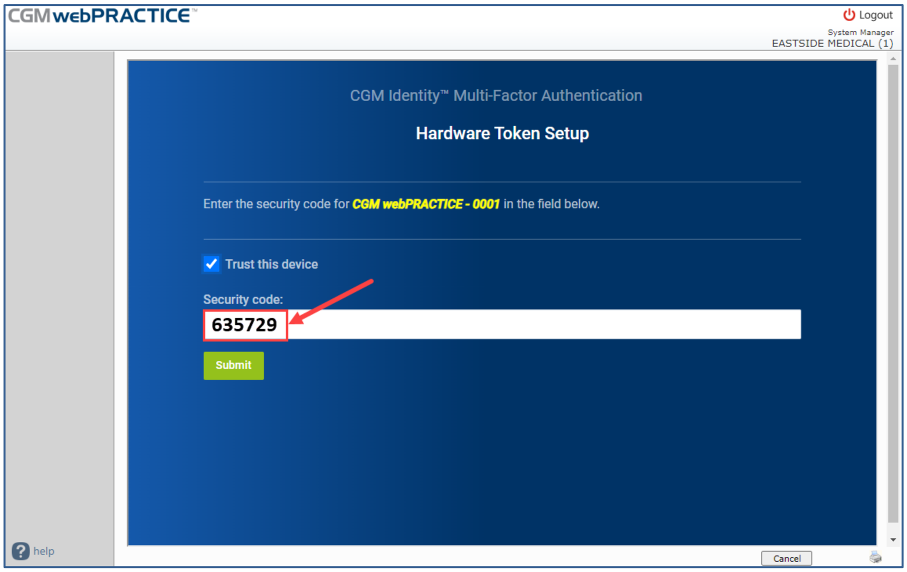
How would you like to refer to your Hardware Token for this MFA setup?

CGM webPRACTICE - 0001

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

WRTBF5PRMDTQ9VDXU7MAL3BZTD2IUOW6

If you want this device to be trusted (default is set to 7 days) and not be prompted for MFA, select the **Trust this device** check box 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

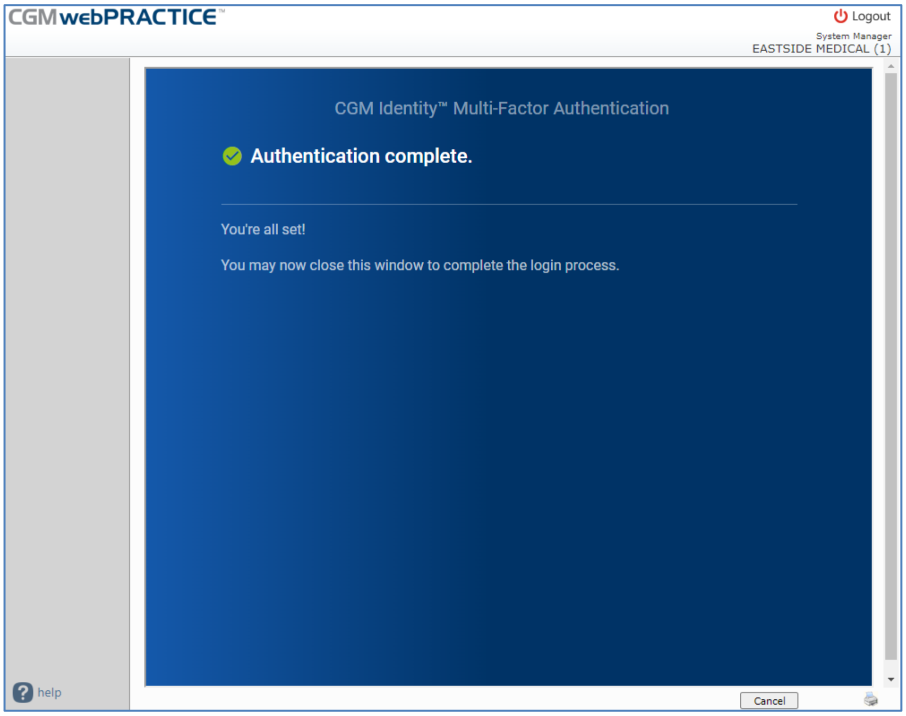
Enter the security code for CGM webPRACTICE - 0001 in the field below.

☑ Trust this device

Security code: 635729

Submit

When the authentication process is completed, the following screen will display for a couple of seconds and then you will be logged into CGM webPRACTICE as normal.



CGM Identity™ Multi-Factor Authentication

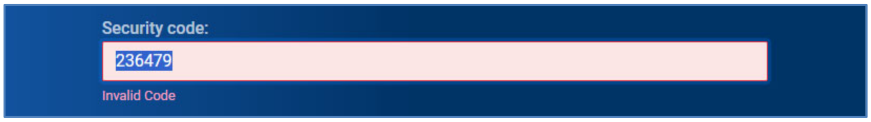
✓ Authentication complete.

You're all set!

You may now close this window to complete the login process.

Invalid MFA Security Code

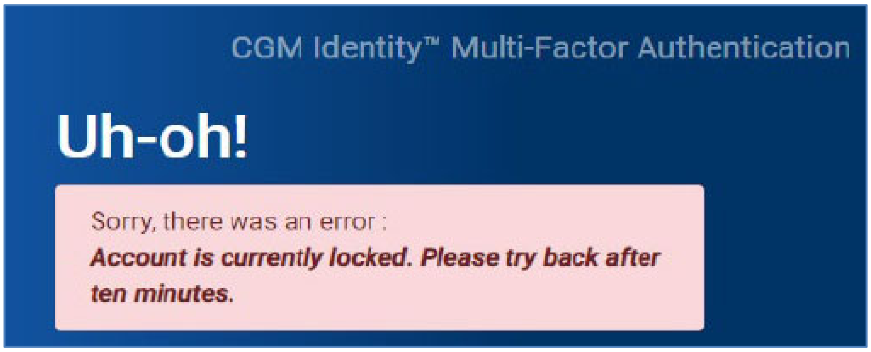
If you enter the security code incorrectly an **Invalid Code** message will display and you will need to re-enter the correct code. You may have entered the code incorrectly or the code updated in the authenticator app on your mobile device or on the hardware token before you completed the entry. Verify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



Security code: 236479

Invalid Code

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



CGM Identity™ Multi-Factor Authentication

Uh-oh!

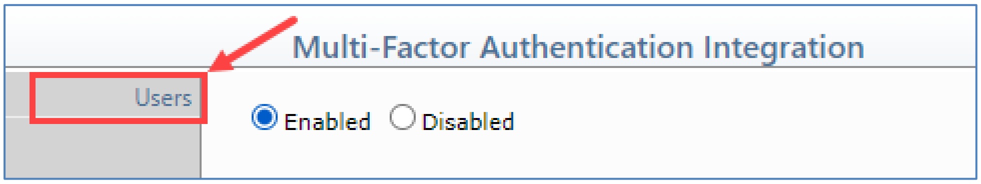
Sorry, there was an error :

Account is currently locked. Please try back after ten minutes.

RESET MFA FOR A USER

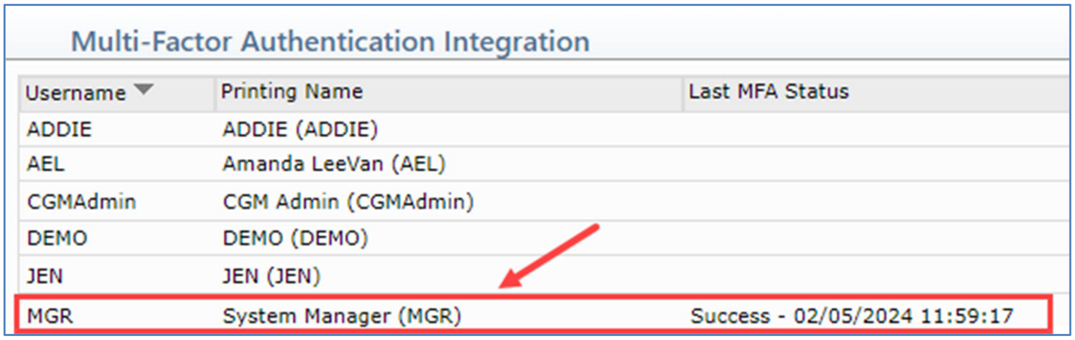
Access the *Multi-Factor Authentication Integration* function in CGM webPRACTICE (*System, Database Maintenance Menu > Integrations > Multi-Factor Authentication Integration*).

Click the **Users** Action Column button.



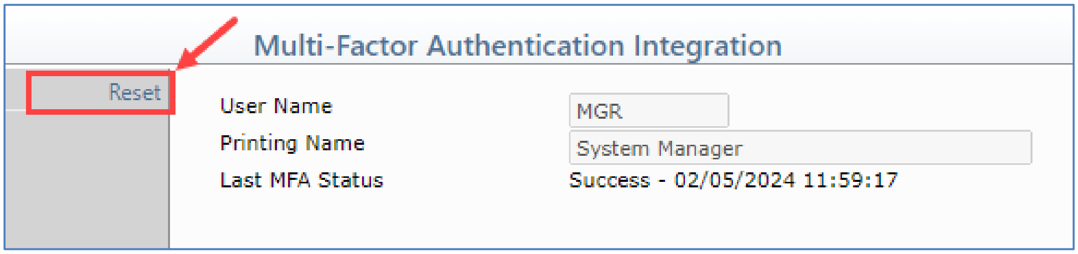
● Enabled ○ Disabled

Select the User you want to reset by clicking anywhere in the row.



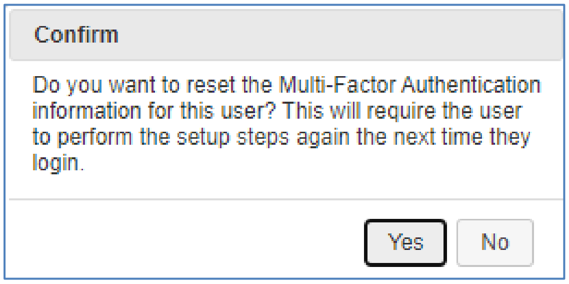
Username	Printing Name	Last MFA Status
ADDIE	ADDIE (ADDIE)	
AEL	Amanda LeeVan (AEL)	
CGMAdmin	CGM Admin (CGMAdmin)	
DEMO	DEMO (DEMO)	
JEN	JEN (JEN)	
MGR	System Manager (MGR)	Success - 02/05/2024 11:59:17

Confirm you have selected the correct User then click the **Reset** Action Column button.



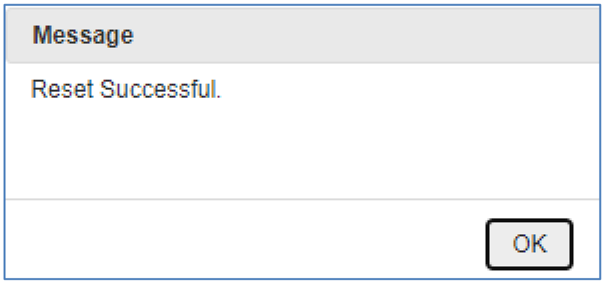
User Name: MGR
Printing Name: System Manager
Last MFA Status: Success - 02/05/2024 11:59:17

Click **Yes** to confirm you want to reset MFA for the user.



Do you want to reset the Multi-Factor Authentication information for this user? This will require the user to perform the setup steps again the next time they login.

When the reset is complete you will receive the following message. Click **OK** to proceed.



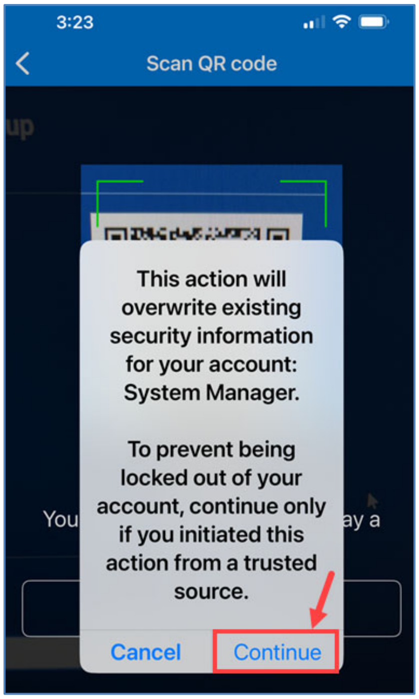
Message

Reset Successful.

At this point, 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 webPRACTICE 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.



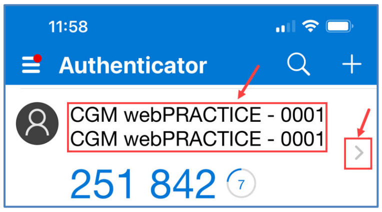
This action will overwrite existing security information for your account: System Manager.

To prevent being locked out of your account, continue only if you initiated this action from a trusted source.

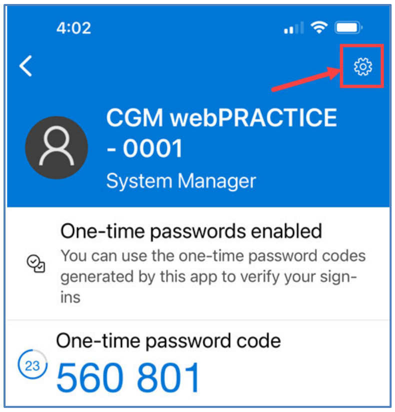
Note: When repeating the setup steps, if you happened to change the **Account Name** on the **CGM Identity Multi-Factor Authentication** window, the original MFA account that was created will not be overwritten and a new MFA account will be created in the authenticator app. The original MFA account will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

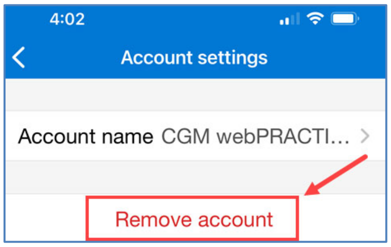


Tap the **Settings** icon.

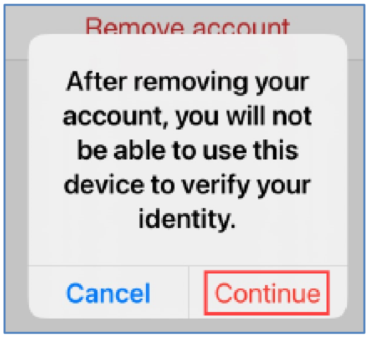


You can use the one-time password codes generated by this app to verify your sign-ins

Tap **Remove account**.



Tap **Continue**.



After removing your account, you will not be able to use this device to verify your identity.