

CGM ANALYTICS™ Multi-Factor Authentication

Published: 02.02.2024



Business Intelligence Solution

Contents

ce	3
i-factor authentication	4
t up multi-factor authentication for your ANALYTICS user account.	5
Use an authenticator application on a mobile device	6
Use a hardware token	9
g in using multi-factor authentication	10
valid MFA code entered	11
set MFA for an ANALYTICS user account	11
move the MFA account from the authenticator app	12
verwrite an existing MFA account on the authenticator app	13

Notice

This document contains valuable, confidential, and proprietary information belonging to CompuGroup Medical (CGM). No part of this documentation may be transmitted, distributed, copied, reproduced, translated, or otherwise duplicated without written consent of CGM. If written consent is given, the same confidential, proprietary, and copyright notices must be affixed to any permitted copies as were affixed to the original.

Use of the software programs described herein, and this documentation, is subject to applicable license agreements and nondisclosure agreements. Unless specifically otherwise agreed in writing, all rights, title, and interest to this software and documentation remain with CGM.

Information in this documentation has been carefully reviewed and is believed to be accurate. However, this information is subject to change without notice, and CGM assumes no responsibility for any inaccuracies that may be contained in this documentation. In no event will CGM be liable for direct, indirect, special, incidental, or consequential damages resulting from any defect or omission in this technical note, even if advised of the possibility of such damages.

In the interest of continued product development, CGM reserves the right to make improvements to this documentation and the products it describes at any time, without notice or obligation.

The trademarks, logos, and service marks ("Marks") displayed in this document are the property of CGM or other third parties. You are not permitted to use the Marks without the prior written consent of CGM or such third party, which may own the Marks.

Multi-factor authentication

CGM ANALYTICS

CGM ANALYTICS has implemented multi-factor authentication (MFA) to help protect user accounts from unauthorized access. Before you can log in to your account, you are required to setup up MFA for your account using an external authenticator application (app) on your mobile device. Installing the Microsoft Authenticator or Google Authenticator app (shown below) on your mobile device is recommended, although other commercially available authenticator apps should be compatible. Once MFA is set up for your ANALYTICS account, you will use the six-digit code provided in the authenticator app to log in to ANALYTICS. The six-digit code needs to be entered only once per 12-hour period if you are not logged off by ANALYTICS.





Note

Consult the help for your mobile device or contact your IT department if you need assistance installing and configuring an authenticator app on your device.

Business Intelligence Solution

CGM ANALYTICS

Set up multi-factor authentication for your ANALYTICS user account.

Review and use the following steps to set up multi-factor authentication (MFA) for your ANALYTICS account. You can have multiple MFA accounts on the authenticator app, but only one MFA account per ANALYTICS user account. An MFA account is needed for every ANALYTICS user account.



Note

The examples included in this document use Microsoft Authenticator version 6.8.2 on an iPhone running iOS 7.2.1.

1. Start the ANALYTICS application, then enter your username and password, and then click Login.



2. On the **CGM Identity Multi-Factor Authentication** window, select if you will be using an authenticator application on your mobile device or a CGM provided hardware token to access the six-digit code that must be entered to access ANALYTICS.



Use the links below and follow the instructions for the authentication method you selected.

- Use an authenticator application on a mobile device
- Use a hardware token

Use an authenticator application on a mobile device

The following steps assume the use of an authenticator application on a mobile device to setup up your MFA account.

1. On the CGM Identity Multi-Factor Authentication window, click Use an Authenticator application ... and then click Submit.

0	Use an Authenticator application that you already have installed on your mobile device
	for work or other secure access.

2. In the text box, edit the name if needed, and then click **Submit**.

The text box displays "CGM ANALYTICS." You can leave the name unchanged or modify it as needed. Once the MFA setup is complete, the name in the authenticator app displays as follows:

<Name in text box> <Username>

	Authenticator Application Setup
How would	you like to identify this application in your Authenticator application?
CGM ANA	ALYTICS - Testing MFA

3. Open the authenticator app (Microsoft Authenticator) on your mobile device and then unlock it with your alphanumeric or biometric passcode.





Note

You can disable the need to unlock the Microsoft Authenticator app each time you use it to access the MFA code. Within the Microsoft Authenticator app, tap the **More** icon **E**, then tap **Settings**, and then tap **App Lock**.

4. On the Authenticator screen, tap the Add icon.



CGM ANALYTICS Multi-Factor Authentication | Revised 2.2.2024

Business Intelligence Solution

CGM ANALYTICS

5. On the Add account screen, tap the account type you are adding.



- 6. Do one of the following:
 - For Other (Google, Facebook, etc.), which is recommended, the Scan QR code screen shows automatically.
 - For Personal account or Work or school account, tap Scan QR code.



- 7. Do one of the following:
 - 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.



CGM ANALYTICS

137 192

• For Other (Google, Facebook, etc.) account types only, tap the Or enter code manually button, then on the Add account screen, in the Account Name box, enter the account name (yellow text) from the CGM I Multi-Factor Authentication window, and then in the Secret Key box, enter the 32-character key (black box).

• III AT&T WI-FI	.il AT&T WI-FI 6:54 PM ◙ 100% ✓ Add account
OTHER ACCOUNT	OTHER ACCOUNT
Account name	CGM ANALYTICS - Testing MFA 🛛 😒
Secret key	→ os5ym64cbe7sxatsos55lvczvbdcswxg 🗵
Finish	Finish

The MFA account is added to the authenticator app displaying a six-digit code and timer indicating the number of seconds until the code changes. Click the name or right arrow to display the full name MFA account name.

	ııl AT&T Wi-Fi 중 6:27PM 1 @ 76% ■) 〈
■ILATET WI-FI G:26 PM	CGM ANALYTICS - Testing MFA
CGM ANALYTICS - T Developer Clinical	Developer Clinical
137 192 @	One-time passwords enabled You can use the one-time password codes generated by this app to verify your sign-ins
Authenticator Passwords Addresses Verified IDs	One-time password code

8. On the **CGM Identity Multi-Factor Authentication** window, in the **Input the 6-digit security code** box, enter the six-digit code shown on the authenticator app for the MFA account, and then click **Submit**.

The CGM Identity Multi-Factor Authentication window closes, and the ANALYTICS application opens.

137192

Submit

	notes
Do not include the space shown betw	veen the two sets of three digits.
Leave the Trust this device for 1 we	ek check box cleared.
	Leave the Trust this device for 1 wee



Use a hardware token

Notes
 If you are interested in purchasing a CGM hardware token, contact your sales team member.
 Contact Support if you need assistance with hardware tokens.

1. On the CGM Identity Multi-Factor Authentication window, select CGM provided hardware token, and then click Submit.

Welcome c	kstewart, let's start the process of setting up Multi-Factor Authentication for ht.
Please cho	pse the authentication method you would like to use:
Use an device f If you d	Authenticator application that you already have installed on your mobile or work or other secure access. on't have an Authenticator application installed, you can install one from you device's app store. We recommend <u>Google Authenticator¹² or Microsoft</u>
Authen	<u>icator</u> ² .

The following steps assume the use of a hardware token to setup up your MFA account.

2. In the top text box, enter a name to identify the hardware token for this MFA setup, and then in the bottom text box, enter the 32-character code for the hardware token, and then click **Submit**.

	Hardware Token Setup
How would	you like to refer to your Hardware Token for this MFA setup?
CGM AN/	ALYTICS MFA
Enter the 3 JBSWY3D	2 character code that was provided with the Hardware Token: PEHPK3PXPJBSWY3DPEHPK3PXP

Log in using multi-factor authentication.

Once your ANALYTICS account is set up with multi-factor authentication, the log in process requires entering only the six-digit code from the authenticator app.

1. Start the ANALYTICS application, then enter your username and password, and then click Login.

CGM ANALYTICS	
SIMPLE	POWERFUL W DATA ANALYSIS
Focused Analytics	Login
As a Global Leader in health information technology, CompuGroup Medical is focused on providing the best solutions for the industry. CGM Analytics was built from the ground up to provide you, as a single physician practice to a large FQHC or ACO the intelligent analytics for all of your data, all in one place.	Email Address clinical@cgm.com
CGM Analytics presents the data you care about in an easy to use platform; all of your labs, vitals, medications, appointments, financials and more all at your finger tips. CGM Analytics lets you slice and join the data any way presents it without because on the data and way and the performance of the data and way and the data and way and the data and the data and way and the data and way and the data a	Password *

- 2. Open the authenticator app on your mobile device or access your hardware token.
- 3. Select the **Trust this device for 1 week** check box if for the next seven days you do not want to enter the six-digit code each time you log in.

	de la
Ť	 -
	_

Note

ANALYTICS does not require you to enter the six-digit code within 12 hours after logging out when the **Trust this device for 1 week** check box is not selected.

4. Without including the space between the two set of three digits, enter the six-digit code for your account in the **Input the** 6-digit security code box on the CGM Identity Multi-Factor Authentication window.

The CGM Identity Multi-Factor Authentication window closes, and you will be logged in to ANALYTICS.

제 시지하다 Wi-Fi 중 7:42 PM 4 월 83% 📼)	CGM Identity [™] Multi-Factor Authentication
Authenticator Q + CGM ANALYTICS - T Developer Clinical	Open the authenticator app on your phone and enter the 6-digit security code for CGM ANALYTICS - Testing MFA in the field below.
Authenticator Passeords Addresses Vertice IDs	Trust this device for 1 week
	128256 Submit

Invalid MFA code entered

If an invalid six-digit code is entered in the **Input the 6-digit security code** box, you will see the **Invalid Code** message below the box. 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.

604750		
091700		

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

CGM I	dentity™ Mul	ti-Factor Au	Ithenticatio
Jh-oh!			
Sorry, there was an Account is currently ten minutes.	error : Iocked. Please	try back after	

Reset MFA for an ANALYTICS user account

A user account can have the MFA reset if necessary. An **Administrator** user can reset MFA for a user account by following steps listed below.

- 1. Log in to ANALYTICS.
- 2. Click the Admin button.
- 3. On the Administration page, click the user to get to open User Detail page.
- 4. Click the Reset MFA button.

The following dialog box displays.

Administration

Users
MFA successfully reset for user

5. After the prescribed time, the user can log in to ANALYTICS and set up MFA again for their account.

<u></u>	Note	
	The user who had MFA reset for their ANALYTICS account must set up their MFA account again using the steps in the "Set up multi-factor authentication for your ANALYTICS user account" section.	



CGM ANALYTICS

Remove the MFA account from the authenticator app

An MFA account on the authenticator app on your mobile device can be removed. Once removed, you cannot log in to your account on ANALYTICS without completing the MFA setup process again.

Use the steps below to delete an account on the Microsoft Authenticator app.

			1	
4	•	•	0	
Ŧ			-	
Ŧ				
+				

Note

Best practice for a user having the MFA reset for their ANALYTICS account is to remove the MFA account from the authenticator app on their mobile device before resetting the MFA for their ANALYTICS account. See the "Overwrite an existing MFA account on the authenticator app" section of this document if the MFA account was not removed first.

- 1. Open the Microsoft Authenticator app on your mobile device and unlock it with your alphanumeric or biometric password if necessary.
- 2. On the account to be deleted, tap the name or right arrow.



3. On the Account Details screen, at the top right corner, tap the Account Settings icon.



4. On the Account Settings screen, tap Remove account.



Business Intelligence Solution

CGM ANALYTICS

5. On the dialog box, tap **Continue**.



The account is removed from the authenticator app. You cannot log in to ANALYTICS with the ANALYTICS user account associated with the removed MFA account without completing the MFA setup process again.

Overwrite an existing MFA account on the authenticator app

An MFA account on the authenticator app can be overwritten instead of being removed. This action is useful if MFA was reset for your user account within ANALYTICS prior to removing your MFA account on the authenticator app.

Because MFA for your ANALYTICS user account was reset, you cannot log in to ANALYTICS without completing the steps in the "Set up multi-factor authentication for your account" section of the document. When you reach "Step 7," the authenticator app displays the dialog box shown below. Click **Continue** to replace the existing MFA account, and then complete "Step 8" to finish the MFA setup.





Note

If you change the name in the text box on the **CGM Identity Multi-Factor Authentication** window during the MFA setup process, the original MFA account is not overwritten and a new MFA account is created in the authenticator app for your ANALYTICS user account. The original MFA account is no longer valid to successfully log in and should be removed.