

interChange Provider Important Message

Attention: All Providers, Trading Partners and Drug Labelers

Secure Web Portal Multi-Factor Authentication (MFA) Enrollment for Master Users and Clerks available June 2, 2026

The Connecticut Medical Assistance Program's (CMAP) secure Web Portal will introduce **Multi-Factor Authentication (MFA)** to enhance security for Master Users and Clerks. MFA setup begins June 2, 2026, and is currently optional; a future compliance date requirement will be announced.

On Tuesday, June 2, users will see an enrollment screen upon login. Users will have two options, using an Authenticator App (downloaded to a device of your choice) or Email Verification. Users may opt to enroll with one or both methods, and choose their preferred option each time they log in. Enrollment can be bypassed until a compliance date is announced by clicking on the Skip for Now button.

Multi-Factor Authentication Enrollment

Protect your account with an extra layer of security by enrolling in Multi-Factor Authentication (MFA). MFA adds an additional verification step to confirm your identity, helping prevent unauthorized access even if your password is compromised.

Once enrolled, you will be required to verify your identity when performing the following actions:

- Logging in to your account
- Changing your password
- Resetting your password
- Updating Electronic Funds Transfer (EFT) information

Enrolling in MFA is a simple and effective way to protect your personal and financial information and keep your account secure.

Verification Method	Status	Action
Authenticator App (TOTP) Microsoft Authenticator, Google Authenticator, or any compatible app. Multiple devices supported.	Not Enrolled	Set Up
Email Verification (OTP) One-time code sent to your registered email. One registration per account.	Not Enrolled	Set Up

[Skip for Now](#) You can enroll at any time from your account settings. You will be reminded at each login.

interChange Provider Important Message

1. Authenticator App

Users may set up MFA using an authenticator application downloaded to their mobile device for free from the Google Play store (Android) or the Apple App Store (iPhone/iPad).

Recommended applications include (this is the user's choice):

- Microsoft Authenticator
- Google Authenticator
- Authy Authenticator
- RFC 6238 compatible application

During Setup - after clicking Set Up button:

- A screen will display a **QR code** and a **manual entry key**
- Scan the QR code with your authenticator app
- Enter the generated **6-digit code**
- Select **Verify & Enroll Device**



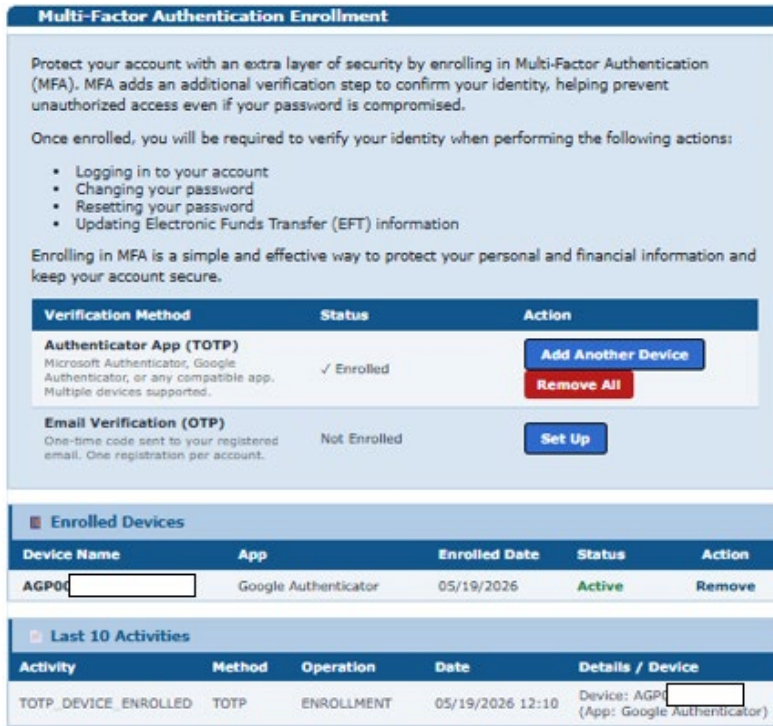
The screenshot displays the 'Multi-Factor Authentication Enrollment' interface. The main heading is 'Set Up Authenticator App'. It contains four numbered steps:

- 1 Install an authenticator app on your mobile device**
Recommended: Microsoft Authenticator, Google Authenticator, Authy, or any RFC 6238 compatible app.
- 2 Scan the QR code or enter the key manually**
A QR code is shown with a diagonal slash through it. Below it is a 'Manual entry key:' field containing the text 'JKLVLPB'.
- 3 Name this device and select your app**
The 'Device Name' field contains 'CLERK'. Below it is a note: 'Required — helps identify this device later.' The 'Authenticator App' dropdown menu is set to 'Microsoft Authenticator'.
- 4 Enter the 6-digit code shown in your app to confirm**
The 'Verification Code' field contains '123456'.

At the bottom, there are two buttons: 'Verify & Enroll Device' and 'Cancel'.

interChange Provider Important Message

- Once Enrolled you will be able to **add** another device by clicking on the Add Another Device button or **remove** a device by clicking on the Remove All button.



Multi-Factor Authentication Enrollment

Protect your account with an extra layer of security by enrolling in Multi-Factor Authentication (MFA). MFA adds an additional verification step to confirm your identity, helping prevent unauthorized access even if your password is compromised.

Once enrolled, you will be required to verify your identity when performing the following actions:

- Logging in to your account
- Changing your password
- Resetting your password
- Updating Electronic Funds Transfer (EFT) information

Enrolling in MFA is a simple and effective way to protect your personal and financial information and keep your account secure.

Verification Method	Status	Action
Authenticator App (TOTP) Microsoft Authenticator, Google Authenticator, or any compatible app. Multiple devices supported.	✓ Enrolled	Add Another Device Remove All
Email Verification (OTP) One-time code sent to your registered email. One registration per account.	Not Enrolled	Set Up

Enrolled Devices

Device Name	App	Enrolled Date	Status	Action
AGP0[redacted]	Google Authenticator	05/19/2026	Active	Remove

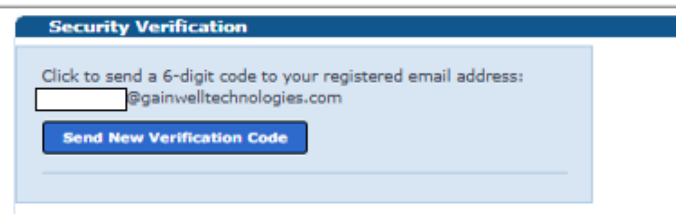
Last 10 Activities

Activity	Method	Operation	Date	Details / Device
TOTP_DEVICE_ENROLLED	TOTP	ENROLLMENT	05/19/2026 12:10	Device: AGP0[redacted] (App: Google Authenticator)

2. E-mail Verification

During Setup - after clicking Set Up button:

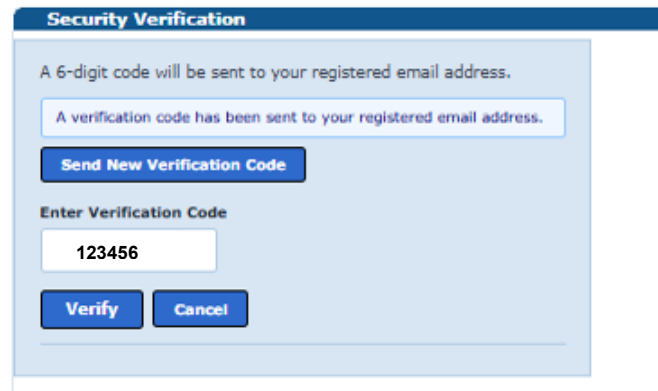
- A verification code will be sent to your registered e-mail address
- Enter the **6-digit code** received via e-mail
- Select **Verify & Enroll** to complete the process



Security Verification

Click to send a 6-digit code to your registered email address:
[redacted]@gainwelltechnologies.com

[Send New Verification Code](#)



Security Verification

A 6-digit code will be sent to your registered email address.

A verification code has been sent to your registered email address.

[Send New Verification Code](#)

Enter Verification Code

123456

[Verify](#) [Cancel](#)

interChange Provider Important Message

Example of email sent:

CT Medicaid Portal - Your Security Verification Code



ctportal@gainwelltechnologies.com

To

☺ Reply Reply All

Hello POC

Your one-time security verification code for **Sign In** on the CT Medicaid Portal is:

123456

This code is valid for **10 minutes**.

Do not share this code with anyone. If you did not request this code, please contact the Provider Assistance Center at 1-800-842-8440, Monday through Friday from 8:00 am to 5:00 pm immediately.

Note: The Email verification code is only valid for **10 minutes**, after that you will need to select **Send New Verification Code** again.

Multi-Factor Authentication Enrollment

Protect your account with an extra layer of security by enrolling in Multi-Factor Authentication (MFA). MFA adds an additional verification step to confirm your identity, helping prevent unauthorized access even if your password is compromised.

Once enrolled, you will be required to verify your identity when performing the following actions:

- Logging in to your account
- Changing your password
- Resetting your password
- Updating Electronic Funds Transfer (EFT) information

Enrolling in MFA is a simple and effective way to protect your personal and financial information and keep your account secure.

Verification Method	Status	Action
Authenticator App (TOTP) Microsoft Authenticator, Google Authenticator, or any compatible app. Multiple devices supported.	Not Enrolled	Set Up
Email Verification (OTP) One-time code sent to your registered email. One registration per account.	✓ Enrolled Email: <input type="text" value="ctportal@gainwelltechnologies.com"/>	De-register

Once enrolled with MFA you will be required to use this authentication for the following actions:

- **Logging into the portal**
- **Changing/resetting passwords**
- **Updating electronic fund transfer (EFT) information**

For questions, please contact the Provider Assistance Center, Monday through Friday from 8:00 a.m. to 5:00 p.m. at 1-800-842-8440.

