

interChange Provider Important Message

Attention: All Providers, Trading Partners and Drug Labelers Recent Security Update Reminder – Security Question Updates, Notifications and Multi-Factor Authentication Enrollment for Master Users and Clerks

1. Web Portal Security Question and Notification Changes effective May 13, 2026

The Connecticut Medical Assistance Program (CMAP) secure Web Portal will undergo a change in security question structure and change notification. When a user needs to reset a password, Master users/local administrators and clerks will be required to select two (2) security questions from a structured list of questions utilizing a drop-down menu and entering corresponding answers to these questions, this replaces free form questions effective May 13, 2026.

Master Users/local administrators and clerks also have the ability after May 13, 2026 to reset their own security questions and answers using the new structure by accessing Account Maintenance within their secure Web Portal. Go to Account and select Account Maintenance. Questions and answers may be modified using the drop-down structured questions.

The screenshot shows the 'Account Maintenance' page in a web portal. At the top, there is a navigation bar with links: Home, Information, Provider, Trading Partner, Pharmacy Information, Hospital Modernization, Telehealth Information, Electronic Visit Verification, Claims, Eligibility, Prior Authorization, Trade Files, Messages, Behavioral Health Attestation, and Account. Below this is a secondary navigation bar with links: home, account home, account maintenance (highlighted), account setup, change password, document upload, reset password, and switch provider. A 'log out' link is also present. The main content area is titled 'Account Maintenance' and contains a 'User Profile' section with the following fields: User ID (CLERKTEST30), Contact First Name* (Joe), Contact Last Name* (Test), Phone Number* (two input boxes), EMail* (input box), Confirm EMail* (input box), and AVR ID (input box). Below the user profile is a 'Security Questions' section with two rows: '1st Secret Question*' (dropdown menu showing '-- Select a Question --'), '1st Answer*' (input box), '2nd Secret Question*' (dropdown menu showing '-- Select a Question --'), and '2nd Answer*' (input box). At the bottom of the form are four buttons: 'save', 'cancel', 'change password', and 'reset AVR Pin'.

Once a password, contact information or security questions are updated a user and/or their Master User will receive the following message:

Dear [USER ID NAME]

The security information associated with the Connecticut Medical Assistance Program's Secure Web portal account for user ID [USER ID NAME] has changed.

interChange Provider Important Message

If you did not initiate this change and you are a master user, please contact the Provider Assistance Center at 1-800-842-8440, Monday through Friday from 8:00 am to 5:00 pm. If you are a Drug Manufacturer, please email ctdrugrebate@gainwelltechnologies.com. If you are a clerk, please contact the Master User for your organization.

Thank you,

Connecticut Medical Assistance Program

Security Reminders:

Every 60 days, master users/local administrators and clerks are prompted to change their password. Users enter their existing password, their new password, and then are asked to confirm this new password. If the new passwords do not match, the user is given a “New Password must be same as Confirm New Password” error message. Once confirmed, a new password is saved in the database table. Users may not re-use any of their last 6 passwords.

Password Requirements:

- The Password you enter must be **15 - 30 characters** in length. The Password and Confirm Password fields must match exactly. The password must have **at least 3 of the 4 character types** - upper case, lower case, number, special character. Special characters include such characters as the following: # \$ % ^ @ *
- Both Secret Question and Answer fields are required. Questions are selected from the drop-down menu. Answers should not contain any special characters, only upper- and lower-case alpha, 0-9 numeric characters, and blank spaces are permitted.

Users have the ability to make **4** attempts to enter the correct ID / password or two security question / answer combinations before the account is locked.

Please correct the following errors:

We are sorry but the user name or password is incorrect. Your account will be locked after 4 invalid attempts. Please try again.

After 4 attempts you will receive the following message:

Your account has been locked due to too many invalid password attempts. Please select the reset password button to answer security questions and unlock your account. If you are a Master User that is unable to use the reset password service, please contact the Provider Assistance Center at 1-800-842-8440. If you are a Drug Manufacturer, please email CTDrugRebate@gainwelltechnologies.com. If you are a Clerk, please contact the Master User for your organization.

Master Users are able to UNLOCK clerk IDs through the portal.

If the master user/local administrator or clerk does not use their ID and password for 90 days, their user account is disabled. The local administrator and/or clerk should follow the self-service instructions on the Secure Web site log in page to



interChange Provider Important Message

reactivate their account. The provider or trading partner's master user/local administrator should only contact the Provider Assistance Center for help at 1-800-842-8440 if panel messages indicate that an account is in a locked/disabled where there is no longer any self-service functionality available. If the local administrator is a labeler/drug manufacturer, an email should be sent to ctdrugrebate@gainwelltechnologies.com.

IMPORTANT: If a clerk is not able to use the self-service functionality, they should contact the master user/local administrator of their organization to reset their password.

REMEMBER: User IDs and passwords must always be safeguarded and should never be shared.

Additional instructions on Web Portal set up as well as ongoing account maintenance can be found on the www.ctdssmap.com Web site, under **Information > Publications > Chapter 10 Web Portal/AVRS > Web Security Administration**.

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. If you are a Drug Manufacturer, please email ctdrugrebate@gainwelltechnologies.com.

2. 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 in the next few weeks.

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.



interChange Provider Important Message

Screen Example:

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

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**



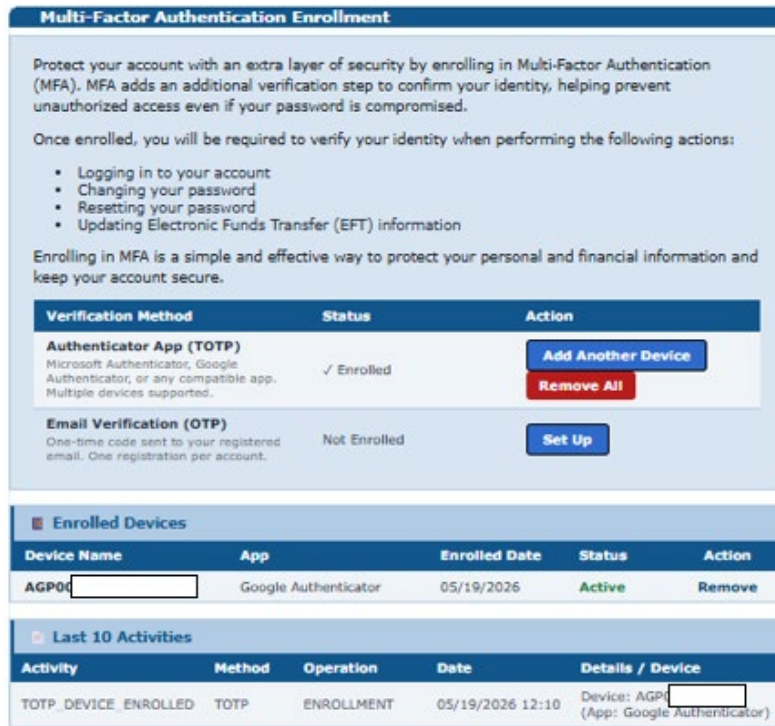
The screenshot shows a web-based interface for setting up an authenticator app. The title is "Multi-Factor Authentication Enrollment" and the sub-header is "Set Up Authenticator App". The process is divided into four numbered steps:

- 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 displayed with a diagonal white line through it. Below it is a "Manual entry key:" field containing the text "JKLVLP".
- 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

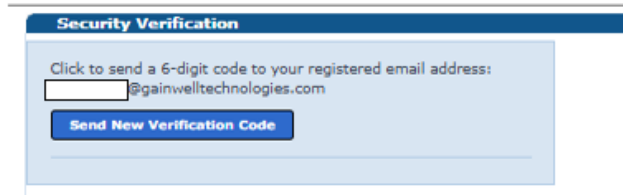
Last 10 Activities

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

2. E-mail Verification

During Setup - after clicking Set Up button:

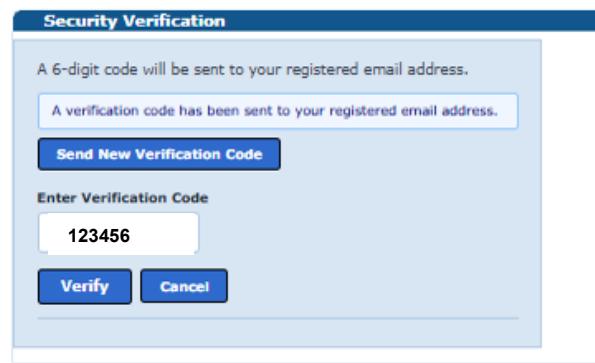
- A verification code will be sent to your registered e-mail address
- Enter the **6-digit code** received via e-mail
- Select **Verify & Enroll** to complete the process



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"/> @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.

