

interChange Provider Important Message

Attention: All Providers, Trading Partners and Drug Labelers

Multi-Factor Authentication (MFA) Security Updates Effective July 14, 2026

The Connecticut Medical Assistance Program (CMAP) Secure Web Portal is implementing additional Multi-Factor Authentication (MFA) security enhancements effective **July 14, 2026**.

1. Authenticator App Enrollment Limited to One Device Per Account

To further strengthen account security, users enrolled in MFA using an Authenticator App will be limited to **one enrolled device per user account**.

Beginning July 14, 2026:

- Only one Authenticator App device may be enrolled per account.
- Users currently enrolled on multiple devices will be required to remove additional devices and retain only one enrolled device.
- If multiple devices are currently enrolled, the Secure Web Portal will require users to remove excess devices before continuing.

Users can review and manage their enrolled Authenticator App devices by:

1. Logging into the Secure Web Portal.
2. Selecting the **Account** tab.
3. Selecting **MFA Enrollment**.
4. Removing the device they no longer wish to use and retaining their preferred device.

Important: Before removing a device, ensure you have access to the device you intend to keep for future authentication.



interChange Provider Important Message

After logging in securely and going through the Security Verification, you will be directed to the Multi Factor Authentication Enrollment page and will be required to remove the extra device(s).



Connecticut Department of Social Services
Making a Difference

Help Site: PreMO
Current User: [redacted] Logout
Tuesday, June 30, 2026 at 10:58:03 AM

Multi-Factor Authentication Enrollment

Please enroll only one authenticator device and remove any extras by 7/14/2026 from the MFA Enrollment page to help ensure uninterrupted access.

You have 2 authenticator device(s) registered, but only 1 is allowed. Please remove extra devices from the list below to continue to Account Home.

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. One device supported.	✓ Enrolled	Remove All Maximum of 1 device allowed. Remove a device to add a new one.
Email Verification (OTP) One-time code sent to your registered email. One registration per account.	✓ Enrolled Email: ctix-sysba@gainwelltechnologies.com	De-register

Enrolled Devices

Device Name	App	Enrolled Date	Status	Action
ADDTEST1MK	Microsoft Authenticator	06/30/2026	Active	Remove
MKTEST	Microsoft Authenticator	06/30/2026	Active	Remove

Last 10 Activities

Remove device(s).

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. One device supported.	✓ Enrolled	Remove All Maximum of 1 device allowed. Remove a device to add a new one.
Email Verification (OTP) One-time code sent to your registered email. One registration per account.	✓ Enrolled Email: ctix-sysba@gainwelltechnologies.com	De-register

Enrolled Devices

Device Name	App	Enrolled Date	Status	Action
ADDTEST1MK	Microsoft Authenticator	06/30/2026	Active	Remove
MKTEST	Microsoft Authenticator	06/30/2026	Active	Remove

Last 10 Activities

Remove Device

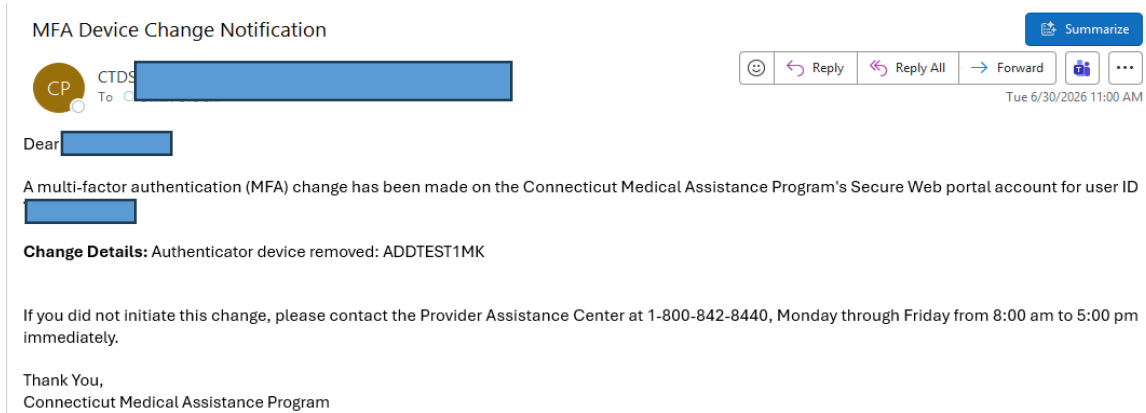
Remove this device from your account?

Cancel

Remove

After the device is removed, a notification email will be received.

interChange Provider Important Message



2. Choosing Your Preferred Authentication Method

Users who are enrolled in both Authenticator App and Email Verification may choose which verification method they would like to use when completing Multi-Factor Authentication (MFA).

On the **Security Verification** page, users may select Use Email Verification Instead if they prefer to receive a one-time verification code by email rather than using the code generated by their Authenticator App.

When selecting the email verification option:

- A one-time verification code will be sent to the user's registered email address.
- The user must enter the 6-digit code received by email to complete verification.
- If the email is not received, users should check their spam or junk folder.
- Users may return to using the Authenticator App option when available.

This option is only available for users who have enrolled in both MFA methods. Users may enroll with an Authenticator App, Email Verification, or both methods, and may choose their preferred option during login.

interChange Provider Important Message



Help Site: PreMO
Current User Logout
Tuesday, June 30, 2026 at 11:09:50 AM

Security Verification

How to get your verification code

1. Open your authenticator app (Google Authenticator, Microsoft Authenticator, Authy, etc.) on your mobile device.
2. Find the entry labeled **CT Medicaid Portal**.
3. Enter the 6-digit code shown below — It refreshes every 30 seconds.

This is not a push notification. No alert will appear on your phone — you must open the app yourself to view the code.

Verification Code

Verify Cancel

⚠ You have 2 authenticator device(s) registered, but only 1 is allowed. After verification, you will be redirected to **MFA Enrollment** and must remove extra devices before continuing.

⊞ Use email verification instead

📞 **Having trouble?** If you are unable to complete verification, ask your **Master User** to remove your MFA enrollment so you can re-enroll. If you are the Master User, call the **Provider Assistance Center at 1-800-842-8440** (Mon–Fri, 8:00 am–5:00 pm) to have your MFA reset.

Reminder: Users may enroll in one or both available MFA methods. If both methods are enrolled, either option may be used to complete authentication.

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.