

eMOMED – MFA Setup and Troubleshooting Guide

This guide is for all eMOMED users and provides information for MFA setup and troubleshooting during login.

What is Multi-Factor Authentication (MFA)?

MFA adds an extra layer of security during login by requiring a one-time password (OTP) sent through email, SMS, or an Authenticator app.

Why does eMOMED use MFA?

To protect sensitive Medicaid information and meet state and federal security requirements, eMOMED requires MFA for all users.

What MFA methods does eMOMED support?

eMOMED supports multiple MFA options:

- Email verification OTP
- SMS text message verification OTP
- Authenticator apps (Time-Based One-Time Passwords):
 - IBM Verify app (Recommended)
 - Optionally, can use Google Authenticator or Microsoft Authenticator apps

How do I set up Email or SMS MFA?

- Email and SMS MFA use the contact information already on file in your eMOMED user profile.
- During login, select Email or SMS as your verification method.
- A one-time password will be sent to your registered email address or mobile phone number.
- Enter the OTP on the login screen to complete authentication.
- If your email address or phone number is incorrect or outdated, update it before proceeding or use the Reset Password link to reverify your information. This can be updated using Maintain User Profile (Home / ePassport / Maintain User Profile) page.

Can I use other authenticator apps instead of IBM Verify?

Yes. Google Authenticator or Microsoft Authenticator apps using Time-Based One-Time Passwords (TOTP) work with eMOMED.

How do I use IBM Verify?

1. Install IBM Verify on a device.

Download and setup IBM Verify:

- Google Play Store: [IBM Verify - Apps on Google Play](#)
- Apple App Store: [IBM Verify App - App Store](#)
- IBM Verify Setup Guide: <https://www.ibm.com/docs/en/security-verify?topic=launchpad-managing-your-verify-authenticators>

2. Log in to eMOMED and select 'Set up Authenticator App'.

3. Scan the QR code displayed on the screen.

4. Enter the 6-digit OTP generated by IBM Verify.

What if my IBM Verify app setup was not completed?

If the IBM Verify authenticator app setup/verification was not saved or completed for any reason, you will need to restart the setup process.

This can happen for several reasons, for example:

- Your session timed out
- You closed the browser
- You opened a new browser or window
- You cancelled the enrollment process and attempted to complete it later

What to do:

1. Log back in to eMOMED.
2. Select Authenticator App checkbox in popup window or under User Profile.
3. Click on the Generate QR button
4. Scan the new QR code shown on the screen using the IBM Verify app.

5. Enter the new 6-digit OTP from the app to complete setup.

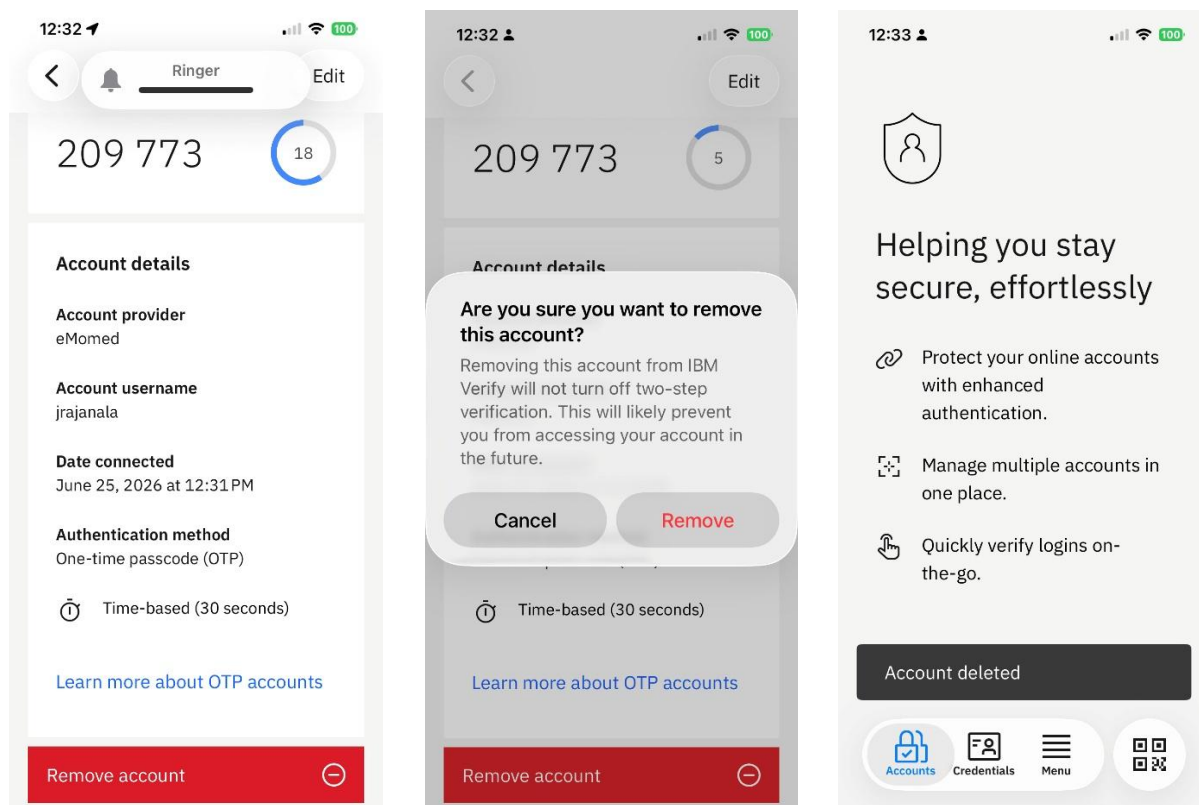
Note: Each QR code is one-time use only. If the setup is interrupted, the previous QR code will no longer work and must be generated again.

How do I remove the existing IBM Verify account before rescanning the QR code?

If you need to rescan a new QR code in the IBM Verify authenticator app, first remove the existing account from the app. This eliminates errors and ensures that the new account setup is completed correctly.

1. Open the IBM Verify authenticator app on your device and select the existing eMOMED account.
2. On the account screen, scroll down.
3. Select **Remove account**.
4. When the warning message appears, confirm that you want to remove the account.
5. Return to eMOMED, restart the setup if needed, and scan the new QR code shown on the screen.

IBM Verify app screenshots:



Note: After removing the old account, scan the latest QR code displayed in eMOMED and enter the new 6-digit OTP from IBM Verify to finish setup.

I did not receive my email/SMS OTP. What should I do?

- Check your email spam/junk folder.
- Ensure your mobile phone number is valid and able to receive SMS Text messages.
- If you use a work phone, ensure SMS is not blocked by your employer.
- Ensure mobile network coverage.
- Verify that your contact information (email and mobile phone number) is up to date.
- User cannot reverify again using the resend button for three (3) minutes.
- If the user makes more than five (5) invalid OPT attempts in three (3) minutes, the user will have to wait for three (3) minutes before attempting to verify again.

What is the new login flow after username and password?

After entering a valid username and password, eMOMED will direct the user to the MFA selection page. The user must choose an available verification method, complete OTP verification, and then continue to the eMOMED home page after successful validation.

Login steps:

1. Enter the eMOMED username and password on the login page.

MoHealthNet eMOMED

External Links

- State of Missouri Web site
- Department of Social Services
- MO Medicaid Audit & Compliance
- Provider Enrollment Information
- MO HealthNet Division
- Provider Information
- Provider Education & Training
- Participant Information
- Claims Processing Schedule
- Electronic Billing Documents
- Download IBM Verify App Guide

Public News

Resources

Welcome

Alerts (1) - Click to hide

As part of our commitment to enhance security, we are implementing Multi-Factor Authentication (MFA) for eMOMED. Starting 5/20/2026, all users will be prompted to select and register an MFA method. Options will include SMS, Email and Authenticator App. Although MFA verification will not be required or enforced until August, and access to eMOMED will continue as usual until then, we encourage all users to complete the selection process early to ensure a smooth transition. Thank you for your cooperation as we enhance the security of our systems.

Welcome to the MO HealthNet Web Portal

The complete source for all MO HealthNet Participant and Provider related services.

Find everything you need from one convenient portal

Provider Enrollment Application

To begin enrollment as a MO HealthNet (Missouri Medicaid) provider, or to access your pending application, [click here](#).

ERA Enrollment

Provider Sign up for Electronic Remittance Advice (ERA) [Click Here!](#)

Login

ATTENTION: Each individual eMOMED user should have their own account identified by their SSN.

User ID: Password:

Login

To reset your password/MFA methods, [Click Here!](#)

Not registered? [Register Now!](#)

WARNING! THIS SYSTEM CONTAINS GOVERNMENT INFORMATION. BY ACCESSING AND USING THIS COMPUTER SYSTEM, YOU ARE CONSENTING TO SYSTEM MONITORING FOR LAW ENFORCEMENT AND OTHER PURPOSES. UNAUTHORIZED USE OF, OR ACCESS TO, THIS COMPUTER SYSTEM MAY SUBJECT YOU TO STATE AND FEDERAL CRIMINAL PROSECUTION AND PENALTIES AS WELL AS CIVIL PENALTIES.

ABOUT SSL CERTIFICATES

Current Environment = NEWTEST Webservices Environment = CICMMITJ (30120) RTA Environment = MISOTJ (30132) Current Schema = MMITCGTJ

- After the username and password are accepted, the MFA selection page will be displayed.

One-Time Password Delivery Selection

Please select the one-time password delivery mode and destination:
The one-time password value can be delivered using the email address or mobile numbers registered on the user account.

The one-time password delivery methods:

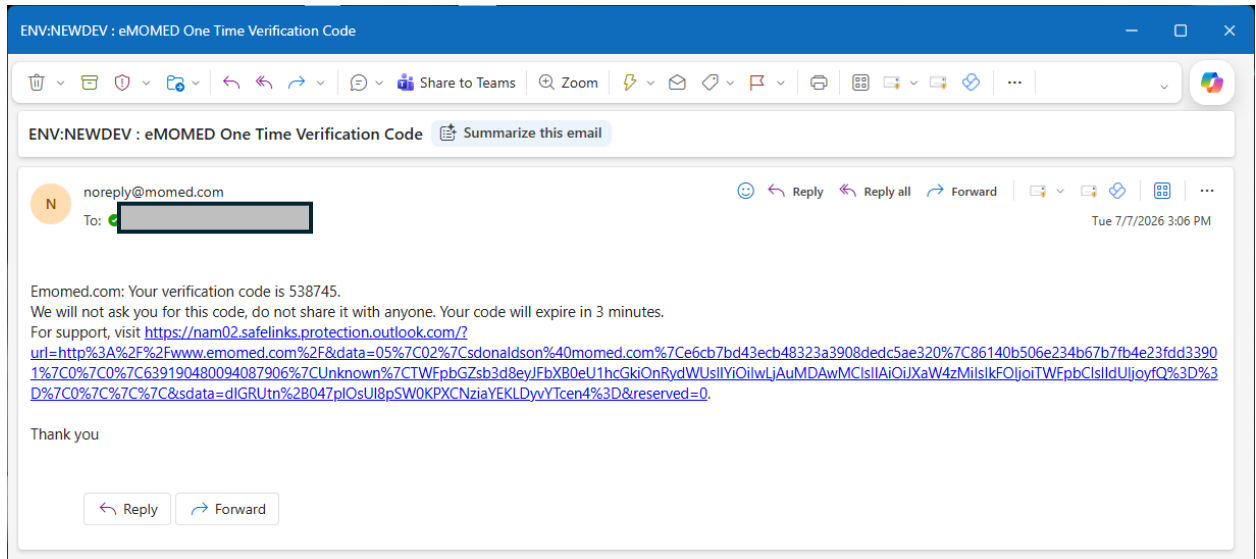
☒ SMS Text

☐ Email

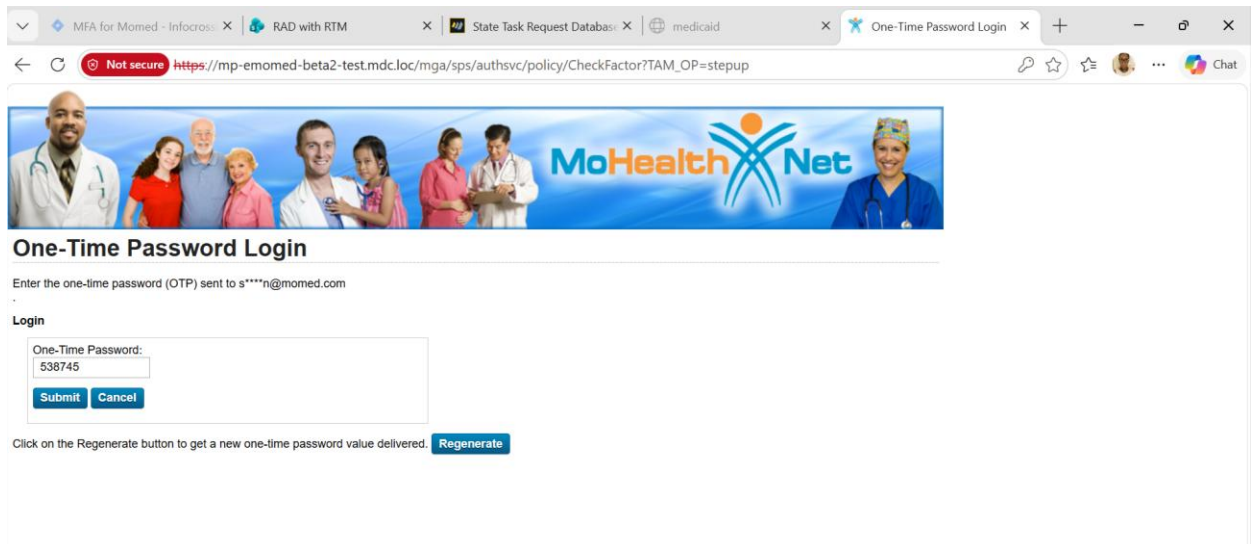
☐ Authenticator App

Submit Cancel

- Select one available MFA method, such as Email, SMS, or Authenticator App.
- A one-time password will be sent or generated based on the selected MFA method.



5. Enter the OTP on the OTP input page and submit it for validation.



6. If the OTP is valid, eMOMED will complete authentication and display the home page.

Note: If OTP validation fails, confirm that the latest OTP was entered correctly. If needed, request a new OTP after the resend waiting period or select another available MFA method.

Troubleshooting MFA during login

If MFA verification cannot be completed during login, review the following guidance before contacting the Help Desk:

- Use the latest OTP, as previously generated codes may no longer be valid.
- If an email or SMS code is not received, allow at least three minutes before requesting another.

- When using SMS, ensure the mobile device can receive text messages and has adequate network signal.
- When using email, review spam or junk folders and confirm the email address on file is accurate.
- For IBM Verify authenticator apps, ensure the device date and time settings are automatic, as incorrect settings may prevent successful validation.
- If the IBM Verify authenticator setup was not completed earlier, generate a new QR code in eMOMED and complete the setup again.
- If multiple verification methods are available, select an alternate method to proceed.
- If the login session expires, restart the process by closing the window and signing in again.
- After repeated invalid OTP entries (more than five attempts within three minutes), pause for three minutes before trying again.

Contact the Help Desk at (573) 635-3559 if:

- Access to registered MFA methods (email, phone, or authenticator app) is no longer available
- The registered device has been replaced or is no longer accessible
- Verification issues continue after completing the steps above

How do I set up or update my MFA?

To set up or update your MFA, use the **To reset your password/MFA methods** link on the login page. You do not need to contact the Help Desk unless you are unable to complete the process using the link.



eMOMED

Contact

Troubleshooting



eMOMED / Login

External Links

- State of Missouri Web site
- Department of Social Services
- MO Medicaid Audit & Compliance
 - Provider Enrollment Information
- MO HealthNet Division
 - Provider Information
 - Provider Education & Training
 - Participant Information
 - Claims Processing Schedule
 - Electronic Billing Documents
 - Download IBM Verify App Guide

Public News



Resources

Welcome

Alerts (1) - Click to hide

As part of our commitment to enhance security, we are implementing Multi-Factor Authentication (MFA) for eMOMED. Starting 5/20/2026, all users will be prompted to select and register an MFA method. Options will include SMS, Email and Authenticator App. Although MFA verification will not be required or enforced until August, and access to eMOMED will continue as usual until then, we encourage all users to complete the selection process early to ensure a smooth transition. Thank you for your cooperation as we enhance the security of our systems.

Welcome to the MO HealthNet Web Portal



The complete source for all MO HealthNet Participant and Provider related services.

Find everything you need from one convenient portal!

Provider Enrollment Application

To begin enrollment as a MO HealthNet (Missouri Medicaid) provider, or to access your pending application, [click here](#).

ERA Enrollment

Provider Sign up for Electronic Remittance Advice (ERA) [Click Here!](#)

Login

ATTENTION: Each individual eMOMED user should have their own account identified by their SSN.

User ID *

Password *

Login

To reset your password/MFA methods, [Click Here!](#)

Not registered? [Register Now!](#)

WARNING! THIS SYSTEM CONTAINS GOVERNMENT INFORMATION. BY ACCESSING AND USING THIS COMPUTER SYSTEM, YOU ARE CONSENTING TO SYSTEM MONITORING FOR LAW ENFORCEMENT AND OTHER PURPOSES. UNAUTHORIZED USE OF OR ACCESS TO THIS COMPUTER SYSTEM MAY SUBJECT YOU TO STATE AND FEDERAL CRIMINAL PROSECUTION AND PENALTIES AS WELL AS CIVIL PENALTIES.

eMOMED | Contact | Troubleshooting



Current Environment = NEWTEST Webservices Environment = CICMMITJ (30120) RTA Environment = MISOTJ (30132) Current Schema = MMITCGTJ