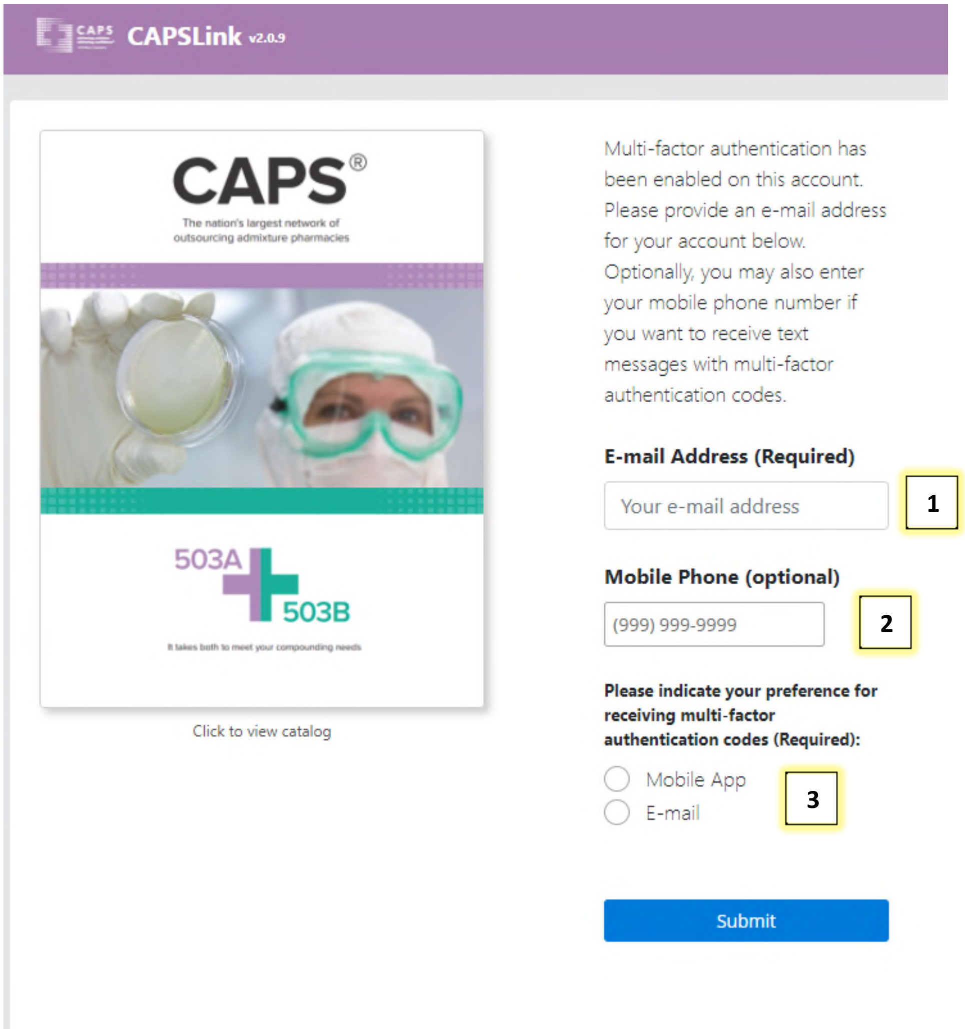
CAPSLink Multifactor Authentication

If CAPS has enabled MFA for your site a Multifactor Authentication (MFA) sequence will follow the normal login process. Users will have the option to receive login codes via email, SMS text, or through the Microsoft Authenticator application. This provides an extra level of security to protect sensitive patient health information.

1.1. *Multifactor Authentication Setup*

After logging in, the user will be presented with options for how they would like to receive their Multifactor Authentication login code.



CAPSLink v2.0.9
CAPS®
The nation's largest network of outsourcing admixture pharmacies
503A
503B
It takes both to meet your compounding needs
Click to view catalog
1
2
3
Submit

Multi-factor authentication has been enabled on this account. Please provide an e-mail address for your account below. Optionally, you may also enter your mobile phone number if you want to receive text messages with multi-factor authentication codes.

E-mail Address (Required)

Your e-mail address

Mobile Phone (optional)

(999) 999-9999

Please indicate your preference for receiving multi-factor authentication codes (Required):

○ Mobile App
○ E-mail

Figure 1 - Multifactor Authentication initial setup

Figure 1, item 1 – Email address field for entering the user's email. This field is required.

Figure 1, item 2 – Mobile Phone field for entering the user's mobile phone number. This field is optional and is intended for the user who wishes to receive authentication codes via SMS text.

Figure 1, item 3 – Preferences for receiving your authentication login code. If the user would like to receive their code through SMS text, the SMS option will display only if a phone number was entered in the Mobile Phone field (see ***Figure 1, item 2*** for location)

1.2. *Accessing your first login code*

After setting up the user for Multifactor Authentication, the first login code will be sent to the email provided. After username/password entry, a field for login code entry will display (Figure 2).

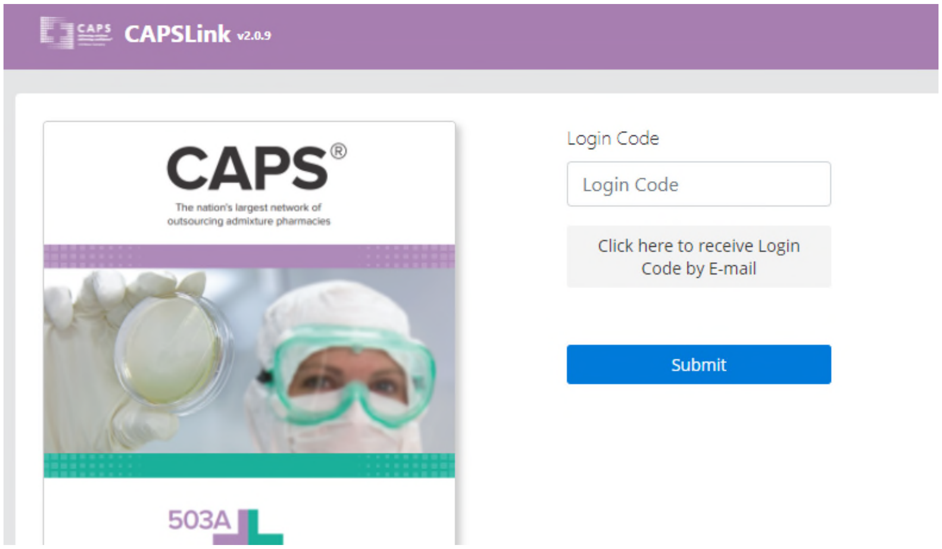
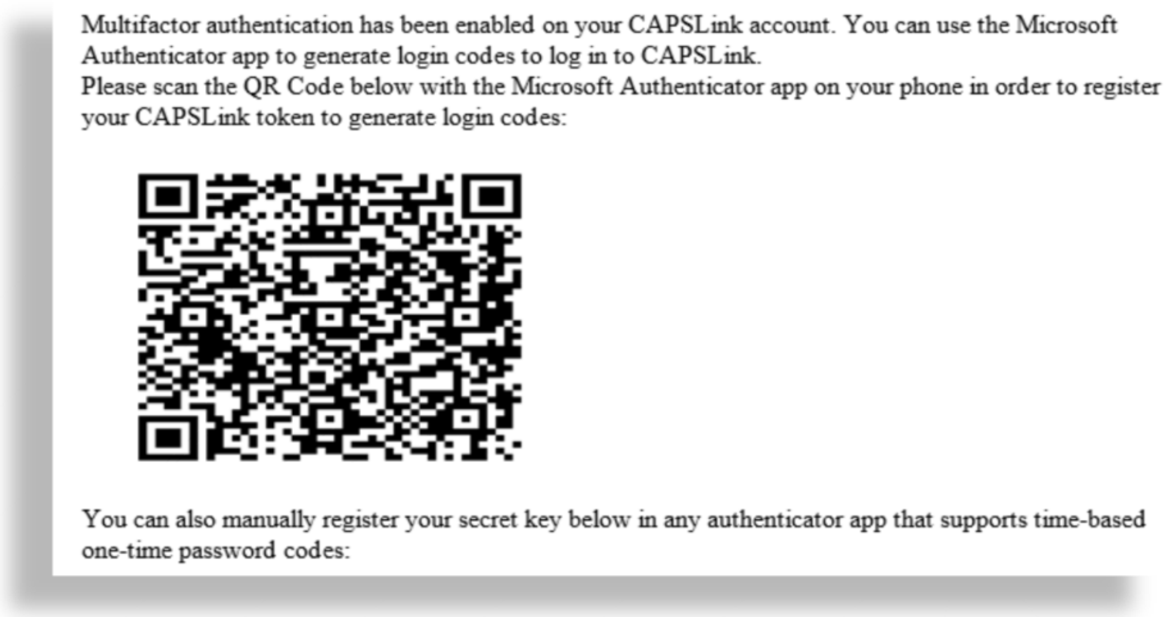

CAPSLink v2.0.9
CAPS®
The nation's largest network of outsourcing admixture pharmacies
503A
Login Code
Login Code
Click here to receive Login Code by E-mail
Submit

Figure 2 - Login Code Entry

Entering the login code sent to the email provided and clicking the Submit button will result in access to the CAPSLink application. If the user cannot locate the login code sent, another code can be resent by clicking on the grey button "Click here to receive Login Code by E-mail. Once initial login is complete, future codes will arrive by the user selected option (see ***Figure 1, item 3***).

1.3. *Microsoft Authenticator Application*

If the user selected to receive their login code through the Mobile App (see ***Figure 1, item 3)***, a QR code will need to be scanned into the Microsoft Authenticator application to complete setup. A QR setup is provided through the email entered during setup and will be sent following the initial login with the email generated code. Figure 3 below is an example of the email which is sent to the user.



Multifactor authentication has been enabled on your CAPSLink account. You can use the Microsoft Authenticator app to generate login codes to log in to CAPSLink.
Please scan the QR Code below with the Microsoft Authenticator app on your phone in order to register your CAPSLink token to generate login codes:

You can also manually register your secret key below in any authenticator app that supports time-based one-time password codes:

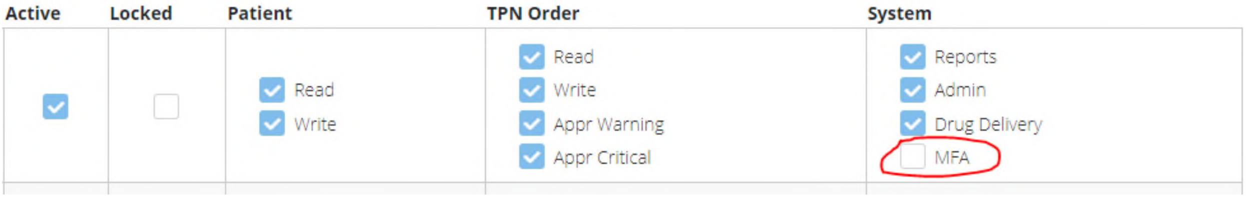
Figure 3 - QR Code Email Example

1.4. *Admin Functions for Individual/Global Settings*

As an Admin, you will have the ability to enable or disable MFA for individual users, as well as set the MFA Token Persistence time.

1.4.1. Individual Settings

The option for enabling or disabling MFA for an individual user exists in their User Maintenance profile under the System heading (see ***Figure 4***).

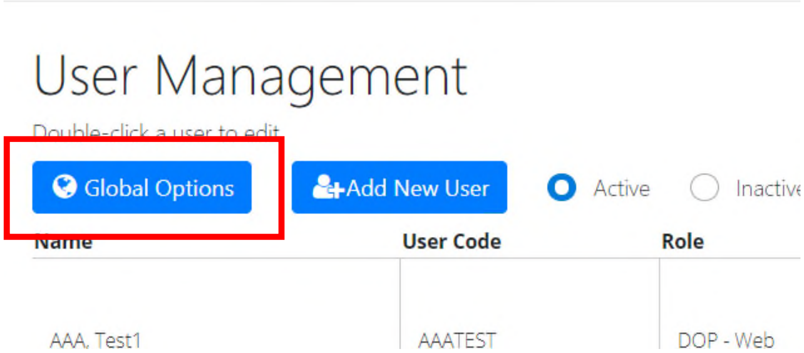


Active	Locked	Patient	TPN Order	System
☑	☐	☑ Read ☑ Write	☑ Read ☑ Write ☑ Appr Warning ☑ Appr Critical	☑ Reports ☑ Admin ☑ Drug Delivery ☐ MFA

Figure 4 – MFA setting in User Maintenance

1.4.2. *Global Settings*

An admin user can access Global Options from the User Management screen by clicking the applicable button (see ***Figure 5***).

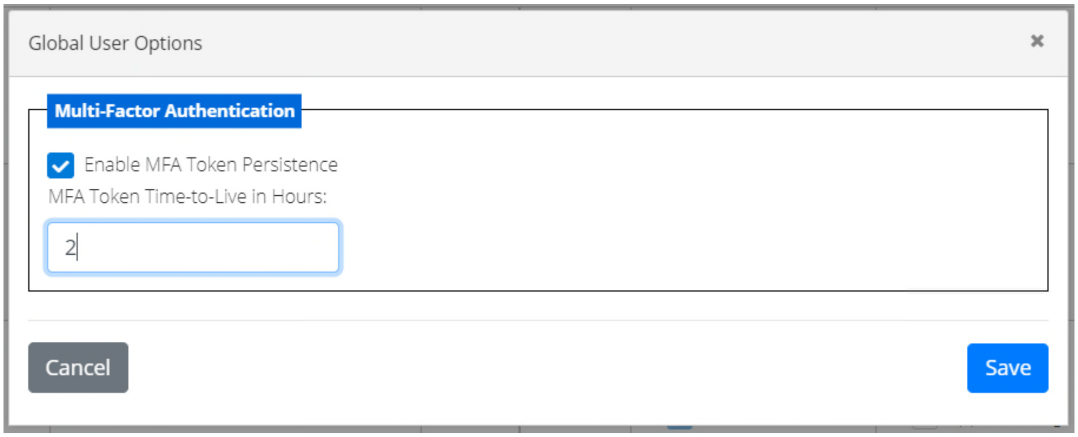

User Management

Double-click a user to edit

Name	User Code	Role
AAA, Test1	AAATEST	DOP - Web

Figure 5 Global Options Location

By clicking the checkbox for Enable MFA Token Persistence and entering a time in hours in the available field (see ***Figure 6***), a user will be able to log back into the system without being prompted for MFA until the configured time elapses. Once the persistence time elapses, the user will once again be required to use MFA to login.


Global User Options

Multi-Factor Authentication

☑ Enable MFA Token Persistence

MFA Token Time-to-Live in Hours: 2

Figure 6 – MFA Token Persistence setting