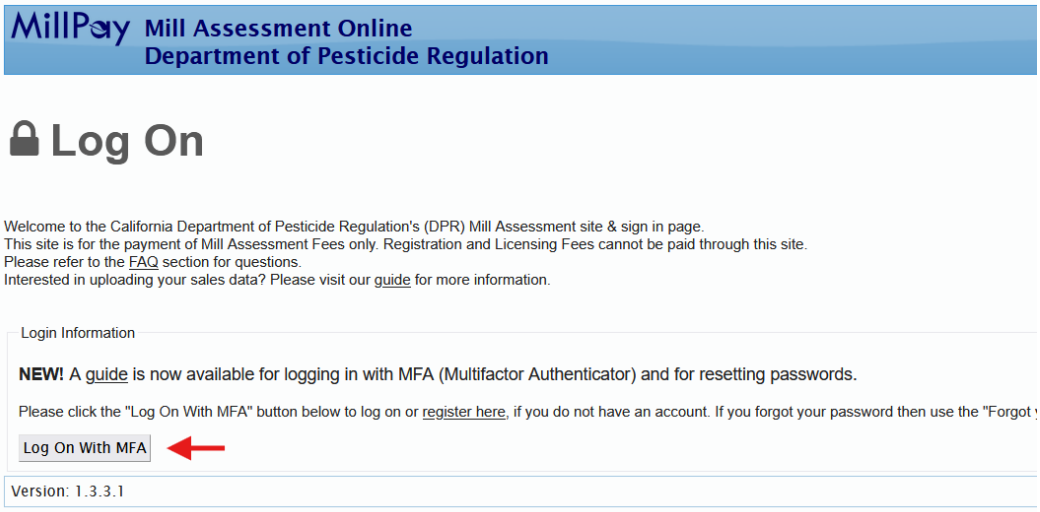
EXTERNAL USER LOGIN GUIDE

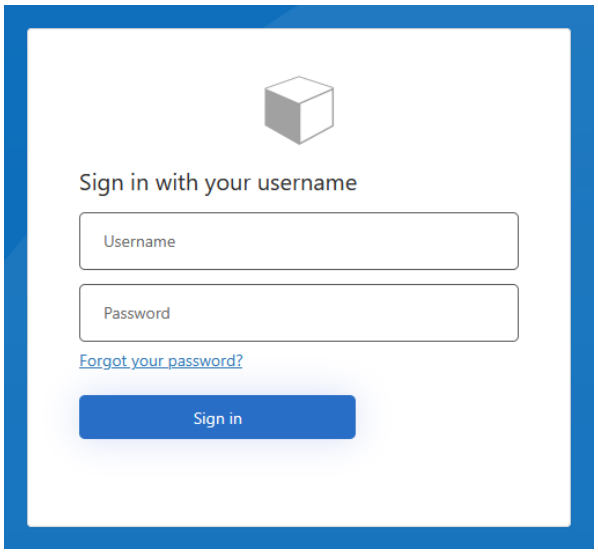
To ensure compliance with State Information Management Manual (SIMM) 5305- A, DPR has implemented Multi-Factor Authentication (MFA). Any publicly accessible information asset that stores, processes, transmits or visually presents confidential, sensitive, or personal information (as defined in Civil Code sections 1798-1798.140) is subjected to this standard. This standard is designed to align with and support the California Information Practices Act of 1977 and Cal-Secure.

Instructions

On the MillPay landing page, users will now be presented with a “Log On With MFA” button.



After clicking the “Log On With MFA” button, users will be redirected to the Azure B2C login portal.



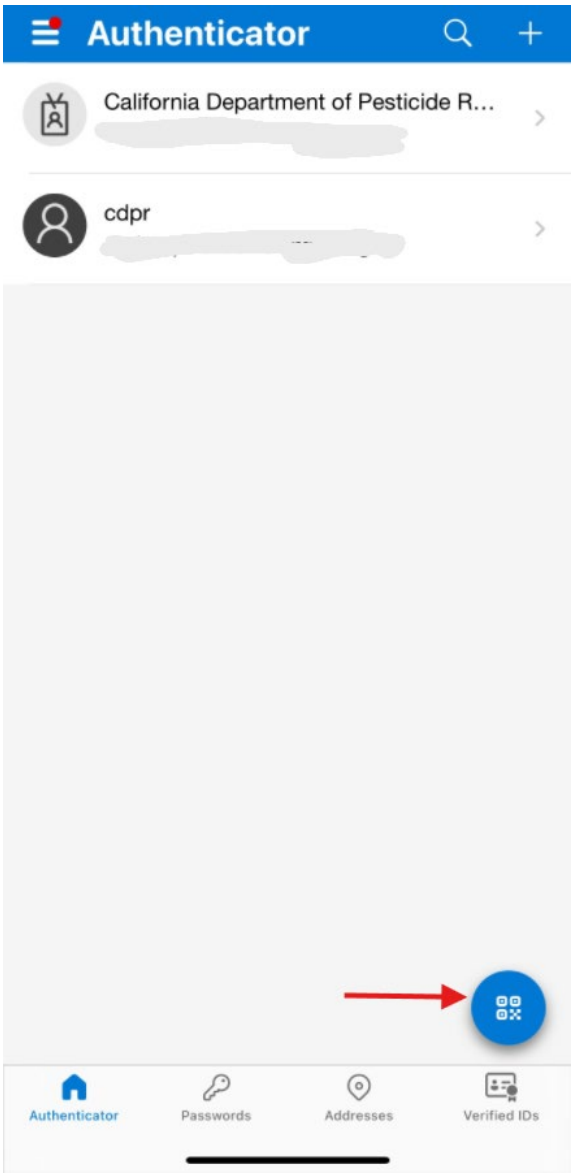
Users will be able to use their existing MillPay username and password to sign in. A “Forgot your password?” link is also available so that the users can reset their own password if they forget it (instructions at the end of this document). After entering their MillPay credentials, if the user has not set-up MFA, they will be prompted to do so. If they have already set-up MFA, they will be prompted to enter their one-time password code.

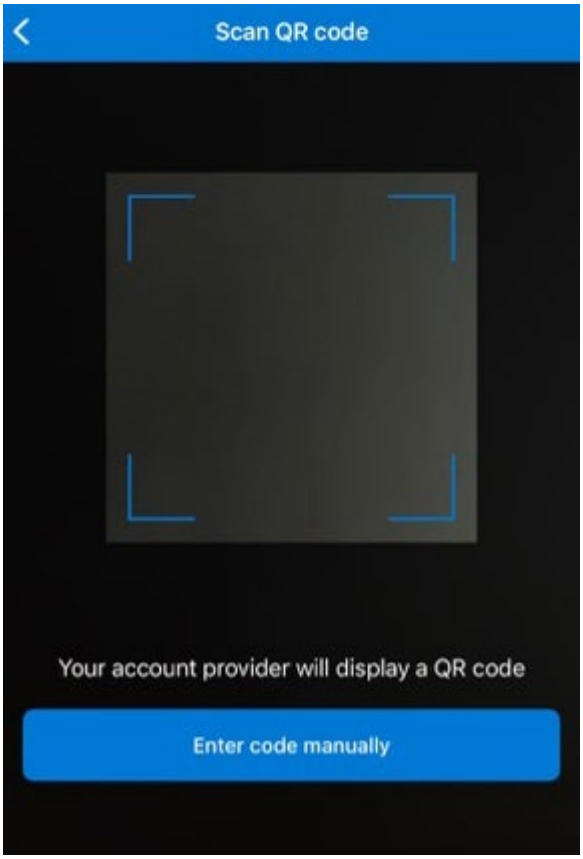
If the user is prompted with instructions to set-up MFA, they may use any authenticator app such as Microsoft Authenticator to set-up their account. If the user does not have an authenticator app, they may download one by using either the Google Play store for Android devices or the App Store for Apple devices.

IMPORTANT NOTE: The user will scan the QR code **using their authenticator application such as Microsoft Authenticator.** *This **will not work** if you scan the QR code with your phone camera*. Once scanned, the authenticator application will create a profile containing a time-based one-time password which will be used each time the user logs in.

Screenshots that are provided below demonstrate the process of setting up MFA within Microsoft Authenticator.

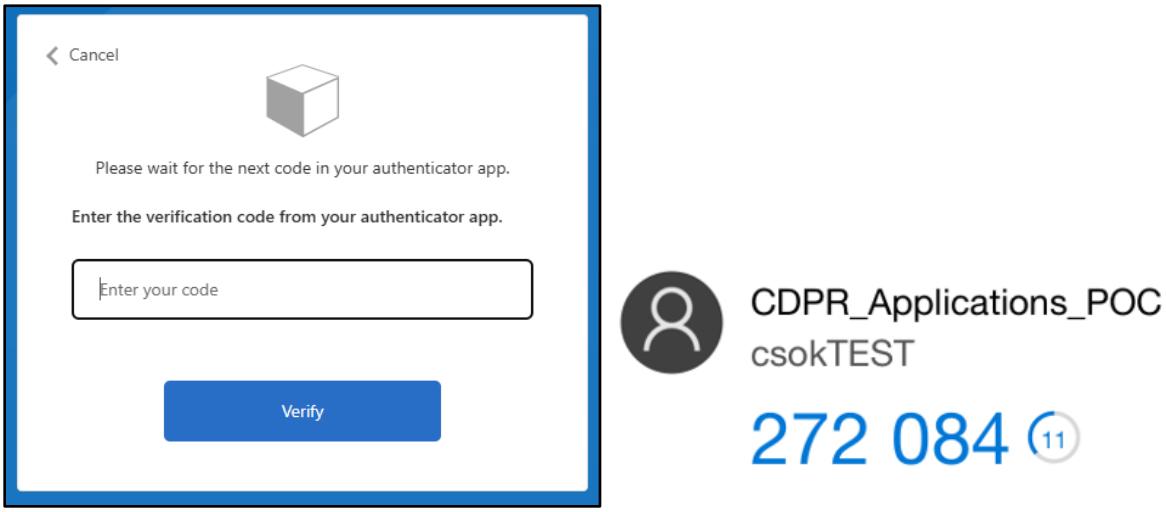
NOTE: Steps may defer dependent on the authenticator app being used.





Press the QR button to enable your phone camera to scan the QR code that was prompted when setting up MFA.

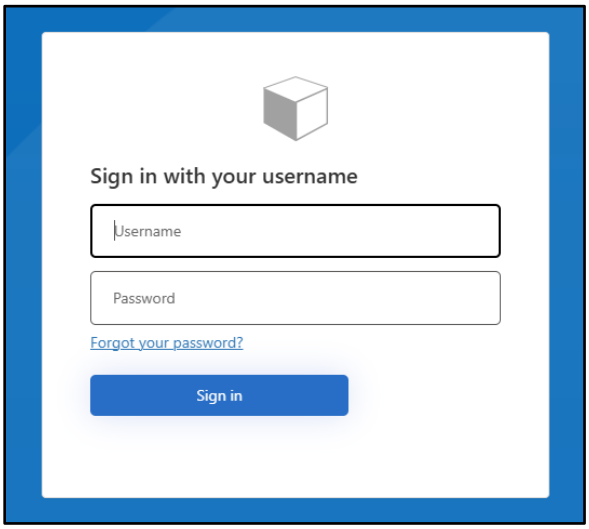
If the user is prompted to enter their one-time password, they will need to open the authenticator application on their phone, and enter the displayed one-time password registered to their MillPay login.



After entering the code from the authenticator application, the user will be logged in and redirected to MillPay.

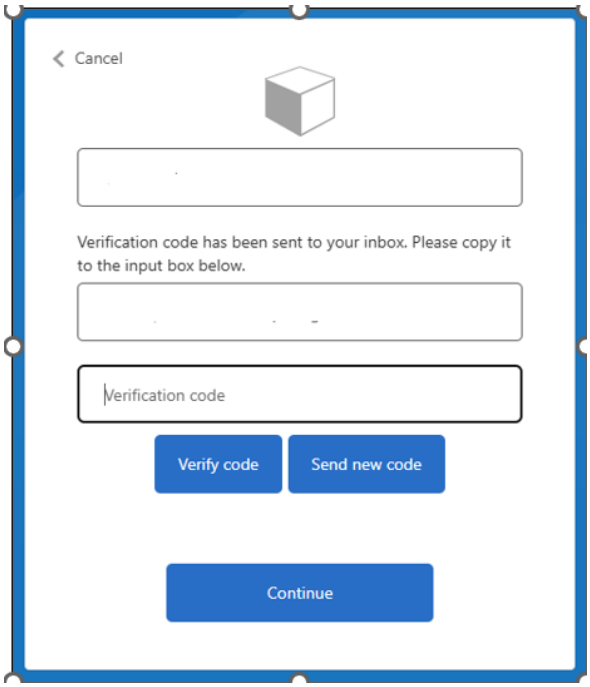
SELF SERVICE PASSWORD RESET

On the Azure B2C login screen, the user has the option of clicking a “Forgot your password?” link to begin the self-service password reset process.

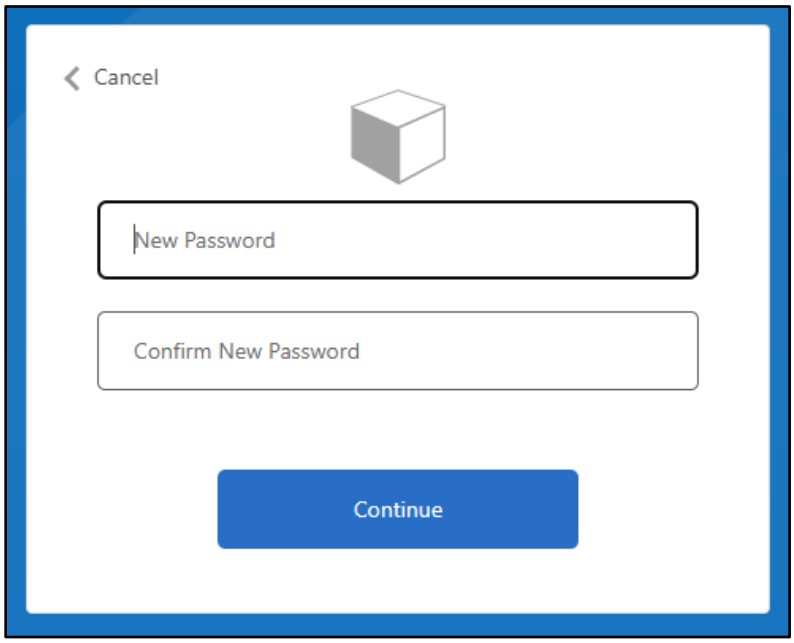


The user must enter their MillPay username, and the email address associated with their MillPay username. After clicking “Send Verification Code”, the user will receive an email with a one-time password.

The user then enters the code into the verification code field.



After clicking “Verify code” and “Continue”, the user will be prompted to enter a new password.



After entering a new password and clicking “Continue”, the user will be prompted for their one-time password from their authentication device and will be logged into MillPay.