CentralReach®

Got questions about the new Client Portal login?

Find answers to your frequently asked questions about the new login experience, convenient Single Sign On (SSO) and recommended Multi-Factor Authentication (MFA) for CentralReach.

What is changing?

- **Before,** users logged into members.centralreach.com
  Now, users will be automatically redirected to login.centralreach.com
- **Before,** users logged into CentralReach with a username and password.
  Now, users will log into CentralReach with a unique email address and password.
- **Before,** users sometimes had invalid email addresses in their profiles.
  Now, users will be required to have valid email addresses that they can access.
- **Before,** Multi-Factor Authentication (MFA) security was unavailable.
  Now, you may choose to enable MFA security.
- **Before,** already-created user login credentials were managed on the Profile > Login & Access page.
  Now, already-created user login credentials are managed on a new Single Sign On Settings page.

  Moving forward, users can update their email address and password on this new SSO page.

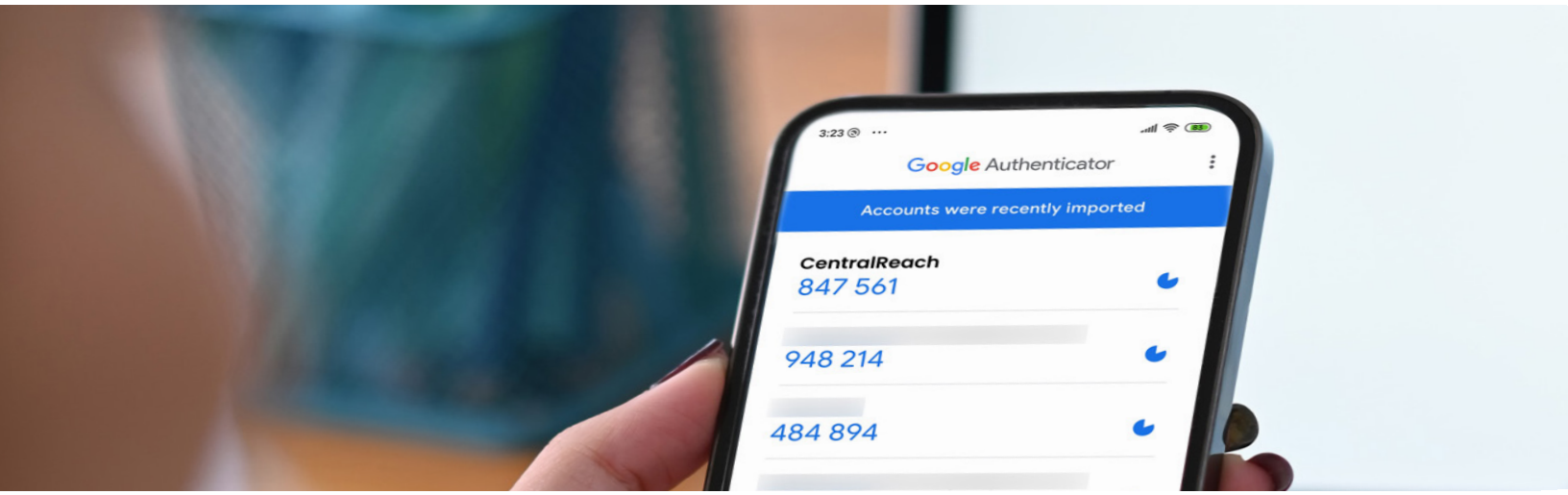
Why is a unique email address for the new login experience?

HIPAA compliance and audit trails are much more clear, providing confidence that only authorized users are making changes with the sensitive information in your Client Portal account.

What is Single Sign On (SSO)?

Single Sign On (SSO) streamlines the login experience across multiple platforms and websites. With just one set of credentials, a user can authenticate themselves to protect against hackers and cyber criminals from access your information.

The Client Portal will also provide the option to enable Multi-Factor Authentication (MFA). We recommend enabling MFA to guard organizations and individuals against hackers, who might otherwise have all-in-one access if login credentials are stolen.



What is Multi-Factor Authentication (MFA)?

Multi-Factor Authentication (MFA) is a powerful, familiar way to confirm your identity when accessing sensitive information like online banking details or electronic health information. MFA is simply the best way to protect your account from common threats like phishing and account takeovers.

MFA utilizes both a factor you know (your email/password) and a factor you have (like a code sent to an app, email, or phone) to verify your identity and prevent bad actors from accessing your account. **There are 3 options for MFA verification:**

1. An authenticator app (Microsoft Authenticator, Twilio Authy, or Google Authenticator. These are freely downloadable from the iTunes and Googleplay stores.)
2. A validated email address
3. A SMS text message to your phone

While authenticator apps are recommended as the most secure method, any of these 3 methods will enhance security.