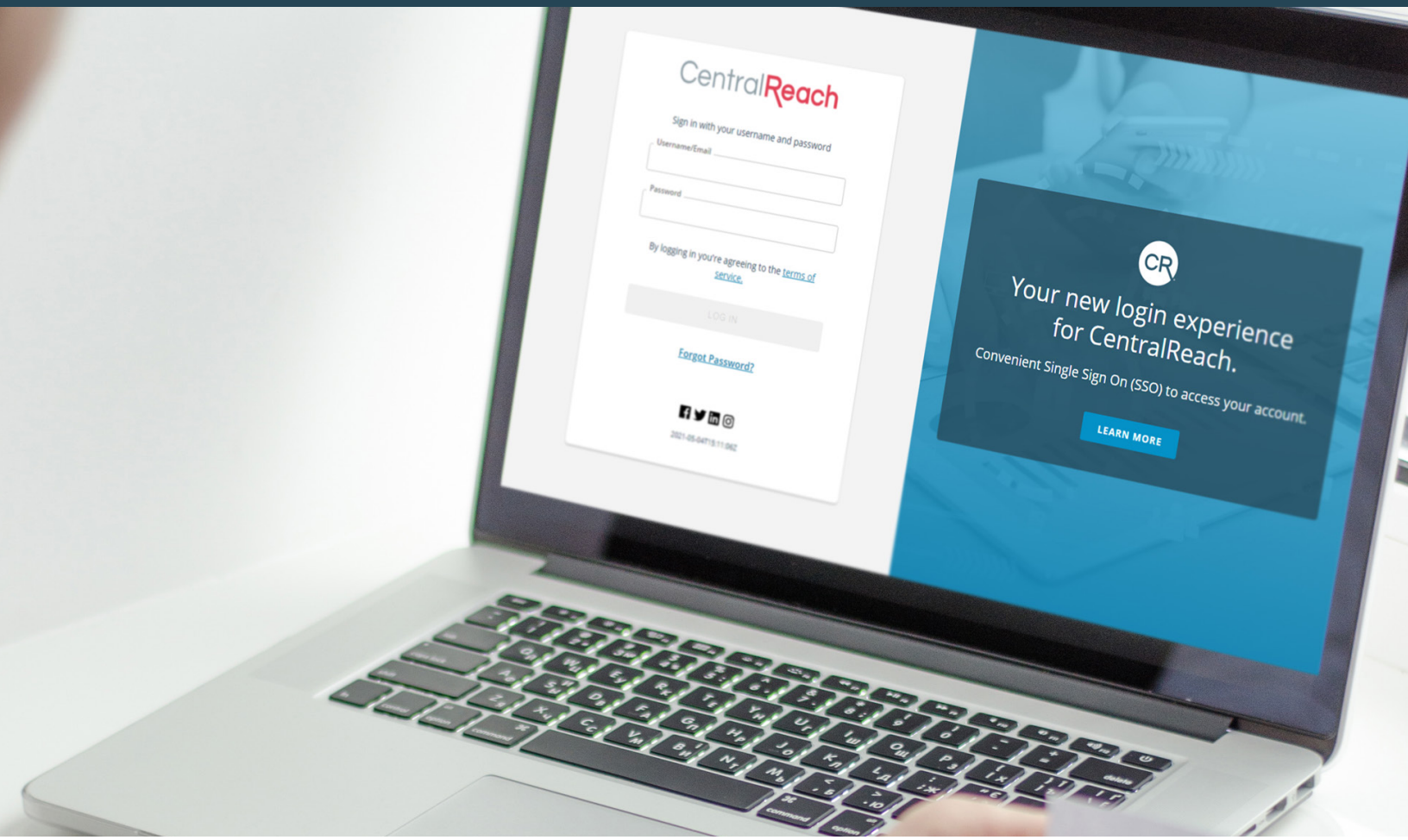

CentralReach®

Got questions about the new CentralReach 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, organizations may choose to enable MFA security for their users.
- **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?

When each user has a unique email address, organizations gain two clear benefits. First, HIPAA compliance and audit trails are much more clear, providing confidence that only authorized users are making changes with the sensitive Personal Health Information (PHI) in your CentralReach account. Second, the unique email address provides a way to link all your CentralReach accounts and products, which will save you time as **we roll out SSO to additional products.**

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 and then gain access to all of their connected platforms. It saves time by not requiring the user to log into many applications. As part of our commitment to your security, CentralReach is launching SSO along with **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. Each organization may choose whether or not to enable MFA for all users (and, if needed, individually opt-out individual users). However, the small, recommended step of 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. **CentralReach offers 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. If your organization enables MFA, users will be required to select an MFA verification method. Then at login, 6-digit code will be sent to that method, which users enter on-screen to confirm their identity.

Can a user still opt-in to MFA if my organization does not automatically opt them in?

Yes, users (including clients who access the Client Portal) will have the ability to manage their own login credentials, including the ability to opt-in to MFA.

Can I opt-in some users in bulk but not others?

No, you can either opt-in all of your users (this would include clients who access the Client Portal) or none of your users. You can, however, opt-in all users and then individually opt them out.

What is the SSO roadmap? Will you add additional products?

Yes! Soon, additional CentralReach products will be accessible through the new SSO login experience. Stay tuned to learn more about which products will be added to the SSO Roadmap.

Is anything changing with how my organization creates, deletes, or manages users?

Your organization will continue to create contacts (employee, client, and generic) the same way that you do today.

Deactivation of users will work the same way it does today: deactivated users will not be able to access CentralReach, though they will be able to see the new Single Sign On page.

However, there are two small changes to managing existing users:

- **Before,** user login credentials were managed on the Profile > Login & Access page
  Now, (1) Already-created users can update their email address and password on the new Single Sign On Settings page. This will trickle down to CentralReach and, in the future, additional products. (2) Organization Administrators (with Org login access) can enable recommended MFA for their users as a whole, but opt-out individual users as desired from the new Single Sign On Settings > Users Management page.

What can I do if I have additional questions?

We recognize this FAQ may not cover your specific questions and existing login workflows. To start, please view the webinar and videos for visual walkthroughs. Then, reach out to your CentralReach Customer Success Lead (CSL) for any specific questions you may have.

Deactivation of users will work the same way it does today: deactivated users will not be able to access CentralReach, though they will be able to see the new Single Sign On page.