Frequently asked questions

Protect your practice data with multi-factor authentication

What's multi-factor authentication?

Delta Dental is adding extra sign-in security that provides an additional layer of protection to external users every time they sign in from a browser. This feature is referred to as **multi-factor authentication (MFA)** or two-factor authentication. When you attempt to log in to your provider account with your username and password, Delta Dental will send a one-time code by voice call, email, or text message.

You must also enter that code on the sign-in screen to verify your identity and complete authentication.

Why is this important?

MFA is crucial because it significantly enhances security by requiring you to verify your identity with more than just a password. This makes it much harder for cybercriminals to access your account and steal your information.

This added layer of security helps protect against various threats, including phishing attacks and credential theft, which are increasingly common methods used by cybercriminals to gain access to your account.

When is it happening?

MFA will be optional on Delta Dental provider accounts starting September 18, 2025. On October 20, 2025, MFA will be required.

How will it impact you?

You must enroll in MFA to maintain access to Delta Dental provider accounts. Once enrollment begins, an option to enroll with MFA will be provided automatically after you sign in. Once enrolled, you must use MFA each time you sign in. If you do not enroll, you will not be able to access Delta Dental provider accounts.

How do I access a Delta Dental provider account?

After enrollment, you must use MFA to sign in. Signing in with MFA will include both your usual password and a code sent to either your email address or phone.

What MFA verification methods are supported?

We support email or phone. With these options, you will receive a temporary code which you must enter during the sign-in process.

We currently do not support authenticator apps or biometrics to access Delta Dental provider accounts.

What will happen if I don't have access to any of my MFA verification methods?

Our teams can help you with changing your email address. Once that's done, you will be able to sign in using your new email and password, allowing you to update your phone number on your own.

Can you disable MFA for my account?

While we cannot disable MFA, Delta Dental of Colorado's customer experience can help you recover access or update your authentication methods if needed. You can reach them at 1-800-610-0201 or **customer_experience@ddpco.com**.

Can I use a password manager?

Yes, you can use a password manager to autofill your username and password when you attempt to sign into Delta Dental provider accounts. You will, however, still be prompted to complete your MFA verification using a one- time code.

How often will I be required to use MFA verification?

Once enabled, you will receive a one-time code to verify your identity each time you sign in on a browser with your username and password.

I already logged in with MFA, why can't I use "remember me"?

To ensure our MFA solution and portal security is compliant with industry expectations and best practices, this feature is not currently being made available. You must use MFA each time you sign in.

What happens if I do not enroll?

MFA is the new sign-in standard. It will be required going forward to access all Delta Dental provider accounts.