

CLX Multi-Factor Authentication (MFA) FAQs



Answers to the most common questions about setting up and using MFA for CLX.



Best Practice

Which authenticator apps should I use?

For the best experience, we recommend using one of the following trusted authenticators:

Recommended:

- ★ Ente Auth (Desktop)
Best option for offices using shared CLX accounts
- ✓ Google Authenticator (Mobile)
- ✓ Microsoft Authenticator (Mobile)
- ✓ FreeOTP (Mobile)

Important:

- ❗ We do not recommend using Google Authenticator for desktop.

We've received reports of compatibility issues that may prevent successful authentication with CLX. Instead, use Ente Auth if you need an authenticator on your desktop or shared office computer.

We use a shared login. What's the best way to set up MFA?

If your office uses a shared CLX login, install Ente Auth on the office computer rather than setting up MFA on one employee's personal phone. This allows authorized staff to access authentication codes even when the doctor or another employee is out of the office and helps avoid login interruptions.

<https://ente.com/auth/>

Can multiple users use the same recovery email address?

No. Each CLX user must have a unique recovery email address. If two users attempt to use the same email address as their recovery email, the second user will not be able to complete the setup because that email address is already associated with another CLX account.

For example, if two staff members share a CLX login but each have their own user account, they should not use the same recovery email address. Each user should enter a unique email address that they can access.

Can I use any app named "Authenticator"?

No. Many third-party applications include the word "Authenticator" in their name, but not all are compatible with CLX MFA. Always download authenticator software from a trusted publisher.

Recommended: Google Authenticator (mobile). Microsoft Authenticator (mobile), FreeOTP (mobile), Ente Auth (desktop).

I don't want to use a mobile phone. What are my options?

You have several alternatives.

Recommended: Ente Auth (Desktop)

Others: Browser-based authenticator extensions for Chrome or MS Edge

Can I use more than one device?

Yes. If your practice uses a shared CLX account, the same MFA setup can be configured on multiple authorized devices during the initial enrollment process. This allows multiple staff members to generate the same verification codes. See the other FAQ regarding shared logins.

My authenticator app isn't working.

Before contacting support, verify the following:

- ✓ You are using an authenticator app from a trusted publisher.
 - ✓ The app is using its default (standard) settings. Custom or modified settings may prevent MFA from functioning properly.
 - ✓ Your computer or mobile device has the correct date and time. Incorrect system time can cause verification codes to fail.
 - ✓ You are entering the current six-digit code before it expires.
-

Does MFA have to be on the same device I'm logging in from?

The authenticator code is not tied to the computer you're using. The authenticator app simply generates the verification code. It does not have to be installed on the computer you're using to log in. Whatever device you are logging into, you'll always enter the current code displayed in your authenticator app.

Can I use the same authenticator on multiple office computers?

Yes. If you use a shared CLX account, you can configure the same MFA setup on multiple authorized office computers during the initial enrollment process. This allows each computer to generate the same verification code, so staff can continue accessing CLX without relying on one person's mobile device.

Note: If MFA has already been configured on only one device, contact CLX Support before attempting to set it up on additional devices. Support can help you reset and reconfigure MFA correctly.

Why is CLX requiring Multi-Factor Authentication (MFA)?

MFA provides an additional layer of security by requiring a verification code in addition to your password. This helps protect your CLX account and your practice's data from unauthorized access.

The doctor set up MFA on their phone, but they're out of the office. Now no one can log in.

This is the most common issue we see. Because the authentication code is only available on the device that completed the original setup, other staff members will not be able to log in unless they have access to that device.

Recommended: Reset MFA through CLX Support.

Otherwise, reconfigure MFA using a shared desktop authenticator (such as Ente Auth) or another authentication method appropriate for your office.



I need additional help.

Contact CLX Customer Support:
Email: customerservice@CLXsystem.com
Phone: (800) 874-6601

