Multi-factor Authentication FAQ's

What is MFA and how does it work?

MFA is an effective way to increase protection for user accounts against common threats like phishing attacks, credential stuffing, and account takeovers. It adds another layer of security to your login process by requiring users to enter two or more pieces of evidence — or factors — to prove they're who they say they are. One factor is something the user knows, such as their username and password combination. Other factors are verification methods that the user has in their possession, such as an authenticator app or security key. A familiar example of MFA at work is the two factors needed to withdraw money from an ATM. Your ATM card is something that you have, and your PIN is something you know.

By tying user access to multiple, different types of authentication factors, it's much harder for a bad actor to access your Salesforce environment. For example, even if a user's password is stolen, the odds are very low that an attacker will also be able to guess or hack a code from the user's authentication app.

Is medEbridge® requiring customers to enable MFA?

Yes, from the 5th of December, medEbridge will require all customer to use MFA to access the platform.

Why is medEbridge® requiring MFA?

There's nothing more important than the trust, security, and success of our customers. We understand that the confidentiality, integrity, and availability of each customer's data is vital to their business, and we take the protection of that data very seriously. As the global threat landscape evolves, it's important for our customers to understand that the types of attacks that can cripple their business and exploit consumers are on the rise. As businesses transition to remote work environments, it's more important than ever to implement stronger security measures.

A key part of your security strategy is safeguarding access to your medEbridge user accounts. On their own, usernames and passwords no longer provide sufficient protection against cyberattacks. That's where MFA comes in. It's one of the simplest, most effective ways to prevent unauthorized account access and safeguard your data and your customers' data. We're requiring customers to implement MFA to help mitigate the risks stemming from threats like phishing attacks, credential stuffing, and compromised devices.

Multi-factor Authentication FAQ's

What are the options to enable MFA on the medEbridge® Platform?

medEbridge will be offering 2 solutions:

1. A corporate approach leveraging **Microsoft Azure AD Authentication or OKTA.** This allows AD domain users to login to medEbridge using their domain credentials.

2. When Azure AD or OKTA is not a suitable solution for a medEbridge user then a **native multi-factor authentication solution** will be used. This is by using **either the Microsoft or Google Authenticator app** on the user's mobile device and registering their medEbridge account on the app.

If I have any questions, who do I contact?

For Multi-factor Authentication enquiries, you can reach our team at MFA@medEbridge.com.au