Cited

Multi-factor Authentication FAQs

At Cited, our core company values include a statement that “The privacy of data is our highest priority.”

Our focus on privacy and security is one of the reasons Cited is trusted by organisations that operate in highly regulated environments around the world.

In accordance with that mindset, we are introducing increased security for access to your Cited account.

What is multi-factor authentication (MFA)?

Multi-factor authentication (MFA) is a security process that uses at least two different factors, something you know (your password) and something you have (email or mobile device), before you can enter your account.

This second layer of security is designed to prevent anyone but you from accessing your account even if they know your password. MFA is also referred to as 2FA, which stands for two-factor authentication. MFA helps protect your invaluable data by adding a second layer of security.

Why is MFA being mandated?

With the increase in security breaches and account compromises, it's important to step up security. As custodians of sensitive client data, keeping everyone's data secure is a top priority.

Users may be at greater risk of compromised passwords than they realise, particularly if they use the same password on more than one website. Downloading software and clicking on links in emails can also expose an individual to password theft.

MFA provides an extra level of security giving you comfort that should your password ever be compromised; your data is still secure.

Who is it mandatory for?

All Cited users in all regions will be required to enable MFA as of October 3, 2022.

What is the value for Cited customers?

In addition to aligning with their business security policies, organisations can feel more secure in the knowledge that their data is protected as is the data they have requested from their people.

Individuals can feel more secure in the knowledge that their data is protected and not being used for fraudulent purposes - even if their password is compromised.

Do I have to authenticate each time I log in to Cited?

Following a successful login, Cited will remember the device you've logged in with for 30 days, but you'll need to authenticate again at the end of the 30 days, or if you log in with a new device or browser.

I've lost my phone or I don't have access to my phone right now. How can I use multi-factor authentication?

MFA verification codes are sent via email to your user account email address. Where there is a mobile phone number associated with the user account, the verification code will also be sent via SMS to that number.

Does the time setting on my mobile device matter?

No. MFA verification codes are sent via email and SMS immediately.

Can we use a password manager as an alternative to MFA?

A password manager plays an important role in your defense-in-depth strategy, but it's not a substitute for MFA.

Password managers help drive sound and secure password practices. You can use this type of tool to ensure that users create strong and hard-to-predict passwords, don't reuse passwords, and change passwords on a recommended schedule. But passwords — even strong ones — aren't sufficient protection against unauthorized account access because they can be compromised by common threats like phishing attacks, credential stuffing, and malware.

Password managers don't provide the enhanced login security that you get by requiring two or more authentication factors via MFA.