

FAQs: Multi-Factor Authentication (MFA) for Event Manager

What is changing with Event Manager access?

From 11 August, all users will need to use Multi-Factor Authentication (MFA) to log in to Event Manager.

Why is MFA being introduced?

MFA adds an extra layer of security to protect accounts and the information held in Event Manager, helping prevent unauthorised access and reducing the risk of security incidents.

Who does this apply to?

This change applies to all Event Manager users (including Citycare Property customers and subcontractors) who do not already use Single Sign-On (SSO).

What do I need to do?

- Before 11 August, ensure you have your own individual Event Manager login by emailing the following details to subcontractors@citycareproperty.co.nz
 - Name of organisation
 - Name of main organisation contact
 - Names and email addresses of all staff who need a login
 - Customers or contracts you have with Citycare Property
- Download an authenticator app (e.g. Microsoft Authenticator or Google Authenticator) in preparation.
- Follow the instructions to complete the MFA setup to access Event Manager from Tuesday, 11th of August. You will be prompted when this is live.

What are the benefits of using MFA?

- Stronger protection of customer and operational data
- Reduced risk of unauthorised access
- Alignment with modern security best practices

What happens if I don't set up MFA?

If MFA isn't set up, you will not be able to access Event Manager from 11 August and would not be able to see the jobs assigned to you.

How long does it take to set up MFA?

Setup only takes a few minutes and will be guided step-by-step within Event Manager when you log in on 11 August or when you next log in after that date.

What is MFA and how does it work?

MFA requires you to log in with your password plus a one-time code generated by an app on your mobile phone.

FAQs: Multi-Factor Authentication (MFA) for Event Manager



Can we use SMS or email instead of an authenticator app?

No. SMS and email are not currently available as authentication options because they provide weaker protection and can be intercepted by attackers. An authenticator app provides stronger protection for your account, our systems, and the information held in Event Manager.

Do I need a mobile phone?

Yes, you'll need access to a mobile device to use an authenticator app for MFA setup and login.

How often will I need to authenticate?

After setup, you'll typically only need to confirm your identity roughly every 30 days on the same device, or when using a new device or browser.

What will be different when I log in?

After entering your password, you'll need to enter a code from your authenticator app to complete login.

Will this slow me down?

The additional step is quick (entering a short code) and is only required periodically when using the same device.

What if I lose my phone or can't access my authenticator app?

Contact the Event Manager support team and they can reset your MFA so you can set it up again.

Will I get help setting this up?

Yes, a step-by-step setup guide (with screenshots) is available.

Will this affect my day-to-day work?

There will be a small change to the log in process, but no change to how you use Event Manager once logged in.

Can I set up MFA on more than one device?

MFA is typically set up on one primary device (your mobile phone). If you need to change devices later, you can set up MFA again during login or contact our support team if you need to reset your access.

What if multiple people in our business currently share one device?

Each user must have their own account and their own MFA setup. Sharing a device for authentication is not recommended, as MFA is designed to verify an individual user's identity. To meet the new requirements, each person should use their own device and login.

FAQs: Multi-Factor Authentication (MFA) for Event Manager



Can I use MFA across multiple computers or browsers?

Yes, you can log in from multiple devices, but you may be asked to authenticate again when using a new device or browser. On trusted devices, you can choose to “remember” your login for up to 30 days to reduce how often MFA is required.

What happens if I get a new phone?

If you change or upgrade your phone, you’ll need to set up MFA again on your new device.

What if I accidentally delete my authenticator app?

If the app is removed or reset, simply reinstall it. If you’re unable to log in because your MFA connection has been lost, contact our support team to reset your access and complete setup again.

Accounts and Access (For Subcontractors)

Can we continue using shared logins?

No, shared logins will be phased out. Each user must have their own individual Event Manager account.

Why are shared accounts being removed?

Shared accounts create security risks and make it difficult to track activity. Individual logins improve accountability and security.

Our business has multiple staff that access Event Manager. What do we need to do?

Each staff member who uses Event Manager will need their own login. You need to request new accounts before 11 August. Email subcontractors@citycareproperty.co.nz before 11 August to avoid disruption in receiving and accessing jobs.

How will this affect how we manage work across our team?

While each individual will have their own login, your organisation will still be able to view and manage work across your jobs. This change improves visibility of who is doing what, without changing your ability to operate as a team.