# Multi factor authentication (MFA) frequently asked questions

**Why is MFA being implemented for ProCare platforms?**

Keeping patient and practice data safe is important to ProCare. The recent data breach incidents with other health organisations have highlighted the very real threat that our systems are under.

We have already implemented a limit on login attempts before accounts are locked for 30 minutes to protect against brute force attacks and geo-restricted access has also been implemented. To better protect our data from cyber-attacks, ProCare will be adding multi factor authentication (MFA) to the login process for ProCare platforms (Provider Portal, web-based ProFusion, Tableau). This is an important security measure which will significantly reduce the chances of an attack using your stolen credentials. MFA requires users to enter a code which they can generate from an authenticator app from their mobile phone. This means even if cybercriminals steal your login details they won't have the code from your authenticator app so won't be able to gain access.

**What does MFA involve?**

When logging into one of ProCare's platforms the user will be required to download an authenticator app on their mobile phone and set up a 'ProCare IDAM' account in the app. Once this one off set up has been completed, users will be required to generate a password code in their authenticator app and enter it into the login screen when prompted.

**Were users involved in determining the approach to rolling out MFA and testing MFA set up?**

The approach to rolling out MFA was co-designed with different user groups (including practice staff) and the implementation plan has been approved by ProCare's Clinical Quality Committee (made up of GPs and nurses from the ProCare network). The goal was to identify a method of roll out that balances ease of use for users, with providing an adequate level of protection from security breaches. Users from the different user groups also tested and provided feedback to ensure the MFA set up process was intuitive and the right support measures would be available to guide users through the MFA set up process.

**Which platforms are affected?**

You will be required to set up MFA to access ProCare platforms including web-based ProFusion, Tableau and the MRI Provider Portal.

**What is a 'trusted location'?**

ProCare can set up organisations that have a static/fixed IP address (see 'what is an IP address?' below) as a 'trusted location'. This means that when users log into a ProCare platform from a 'trusted location' they will only be required to set up and complete MFA once and won't be asked again when logging in from that location.

**How do I set up my organisation as a 'trusted location'?**

Your organisation can only be set up as 'trusted location' if it has a fixed IP address. If your organisation has a fixed IP address you can determine what it is by referring to the question 'If my organisation has a

fixed IP address, how do I find our IP address?' below. You will need to provide consent for ProCare to set your location up as a 'trusted location' by completing this form. You will need to set up MFA from your organisation's physical location first before we can set it up as a trusted location.

**What is an IP address?**

It is a unique address that identifies a device on the internet or a local network. It allows information to be sent between devices on a network and contains location information. Most devices use dynamic IP addresses, which are assigned by the network when they connect and change over time. Dynamic IP addresses change if you reset your router, change internet providers, have unstable network connections (e.g. rural). Some organisations will have a fixed IP address already set up.

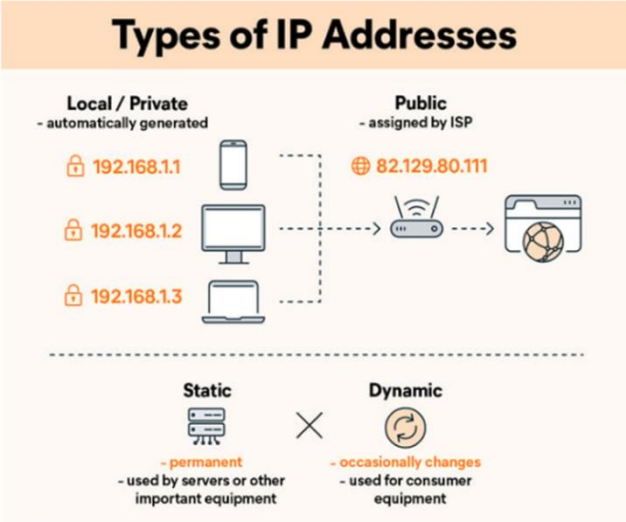
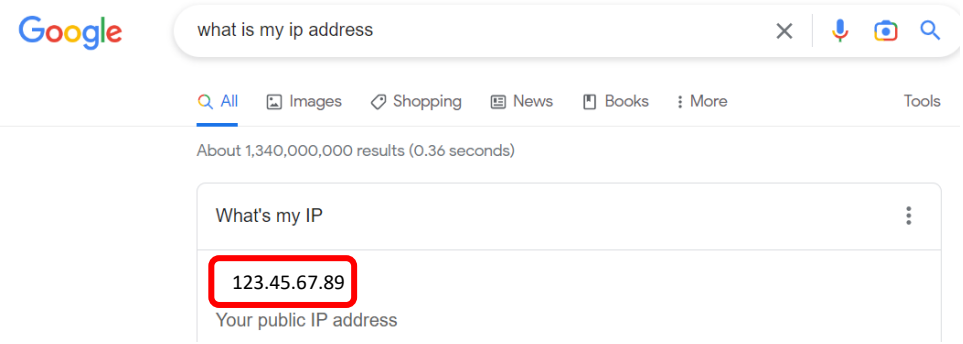



*Diagram courtesy of What is an IP Address? | IP Address Definition | Avast*

**If my organisation has a fixed IP address, how do I find our IP address?**

When at your organisation's physical location go to www.google.co.nz and type 'what is my ip address' and click enter. Your IP address will be displayed at the top of the search results.




**If my fixed IP address is set up as a 'trusted location' why do I still need to set up and complete MFA once?**

If MFA is not set up then it does not exist and so it will not stop a cyber attacker. We need it to be set up so if a cyber attacker tries to use your login credentials, they won't be able to access the password code from your authenticator app so they won't be able to successfully login.

**If my IP address hasn't been set up as a 'trusted location' how often will I need to complete MFA?**

If you login from a fixed/static IP address, you will be prompted to complete MFA every 30 days. If you login from a dynamic IP address, you will be required to complete MFA at least every 30 days or sooner if your IP address changes.

**Why was 30 days chosen as the MFA frequency for users logging in from an IP address that isn't set up as a 'trusted location'?**

30 days was chosen as it balances security risk with convenience for users. It is also often enough that users don't forget how to complete MFA. If we make the time period between MFA prompts too long, we increase the chance of a security breach and users forgetting how to complete MFA. If we make the time period too short, it will be a higher burden on users.

**What support is available to help me with setting up MFA?**

User guides

- User guides are available for how to set up MFA using the Microsoft and Google authenticator apps.

'Trusted locations'

See previous questions relating to 'trusted locations'.

Other support

- ProCare IT HelpDesk 0800 735 900

**What happens if I don't agree to set up MFA?**

From July MFA will be mandatory for users from your practice/organisation. Users who have not set up MFA by July will not be able to access ProCare platforms (Provider Portal, web-based ProFusion, Tableau). MFA significantly reduces the chance of a cyber attacker from being able to access your practice's/organisation's data and it needs to be mandatory for all users otherwise we are vulnerable to potential cyber-attacks.