MFA TRUSTED NETWORK

FREQUENTLY ASKED QUESTIONS

Why do I need Multi-Factor Authentication (MFA) when using my Endeavour Foundation device?

We recently rolled out MFA across all users who access the Endeavour Foundation network, to enhance our data security. MFA is one of the best ways we can protect ourselves against cybersecurity threats. The good news is the roll out was successful, which means we can now move on to the next phase, Trusted Network.

What is a Trusted Network?

A Trusted Network allows only trusted and secure data to be transmitted, making your connection safe. The Endeavour Foundation network is authorised and can be trusted to have a safe connection. When you log-in off-site using the Sophos VPN you are connecting through a Trusted Network. Trusted Network is designed to make it quicker and easier for you to log into our programs and systems. As an employee, you will no longer be prompted for MFA when you log in at any Trusted Network site, however, MFA will continue working in the background to protect you.

What does this mean for you?

When you log in from the office or your home you should no longer receive MFA prompts. This includes when you log in to Microsoft 365 applications (e.g. SharePoint, MS Teams, etc.).

What and who will Trusted Network cover?

Trusted Network will cover all Endeavour Foundation sites, including VPN users connected via Sophos.

What and who are not covered by Trusted Network?

The Connect2Work platform, tablets and mobile phones are not part of the Trusted Network. However, if a device is connected to an Endeavour Foundation site wi-fi, it will recognise a trusted network connection.

What if I am working from outside an Endeavour Foundation site's wi-fi or somewhere that is not a Trusted Network?

If the device is being used from somewhere that is not a Trusted Network site, i.e. a coffee shop wi-fi, you will receive MFA prompts.

What if I continue to receive MFA prompts when working from home or at the office?

To avoid receiving MFA prompts when working remotely (from home), connect to the Sophos VPN on your laptop immediately. When you do this first, you will not receive MFA prompts. If you do receive a prompt for MFA, please proceed with log-in and authentication and contact the #TeamPossible Support Hub or call 1300 742 212.

What to do if you use Microsoft Authenticator and are prompted for MFA?

Microsoft have introduced a new two-digit number matching feature when logging into MS365 apps outside a Trusted Network. You will receive this two-digit number verification if you have logged in to an MS365 app

(Teams, Sharepoint, Outlook etc.) outside the Trusted Network without having first connected through the Sophos VPN. If this is the case, follow the prompts for verification using the two-digit code shown on the MS365 app to which you are trying to log-in.

Alternatively, if you receive this two-digit number verification when you have connected firstly through the Sophos VPN or at a Trusted Network site, it may mean that your account has been hacked. You will be able to view the geolocation for the attempted log-in in Microsoft Authenticator to check if it is you. If the log-in attempt is not at your location, Click ‘No, it’s not me’ to verify it is not you attempting to log-in and report this to the #TeamPossible Support Hub or call 1300 742 212. You will need to re-set your password to a stronger password.