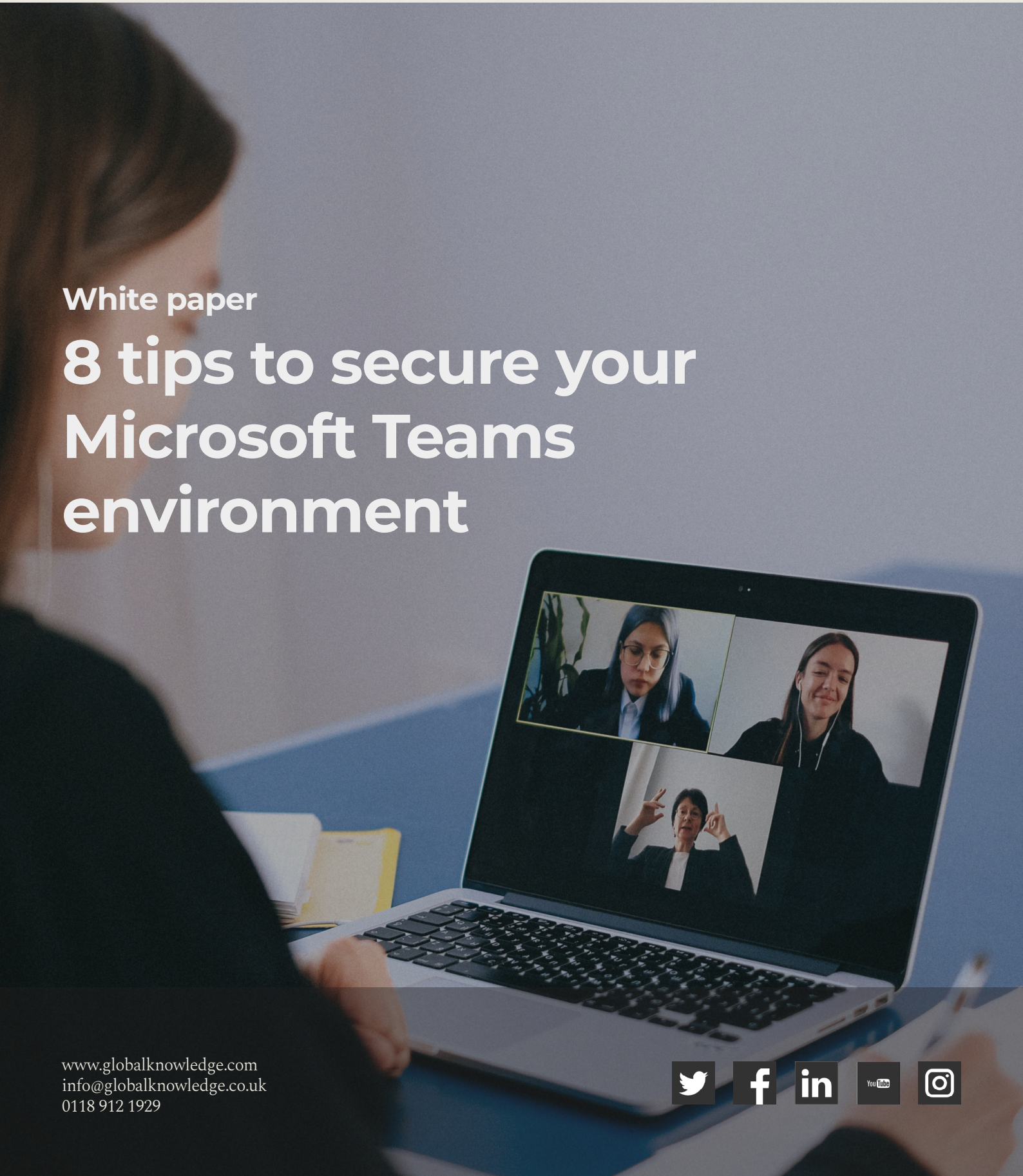
skillsoft global knowledge™

White paper

8 tips to secure your Microsoft Teams environment



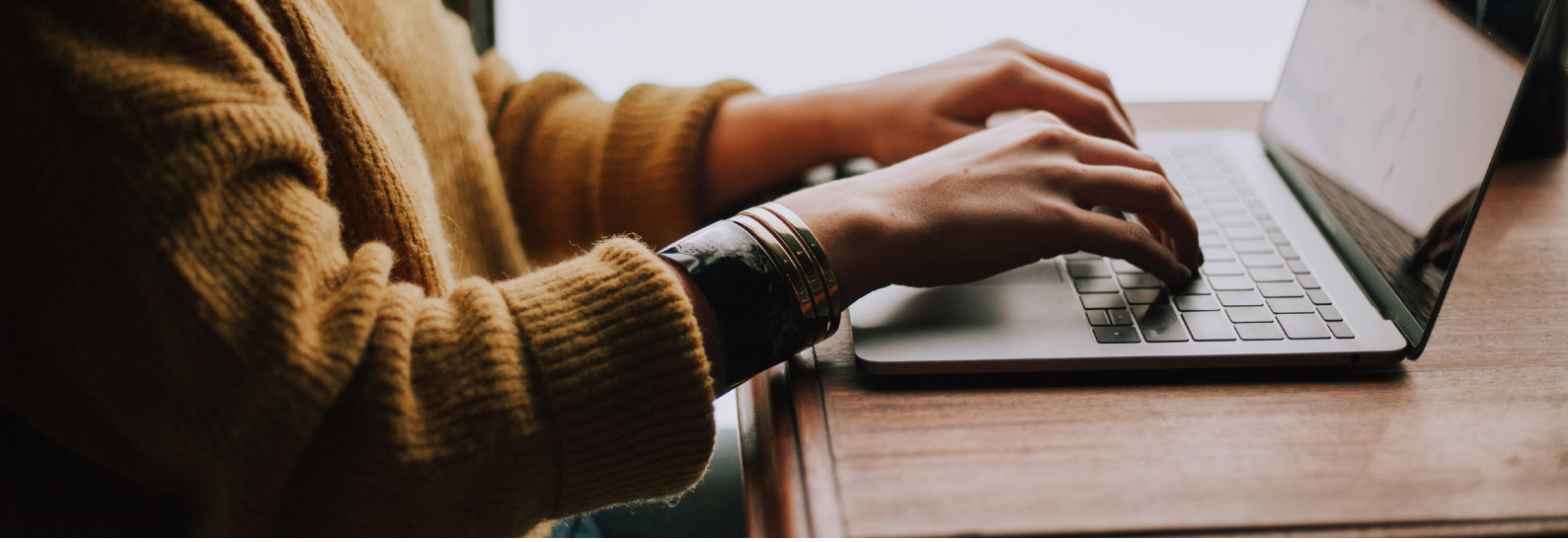
www.globalknowledge.com
info@globalknowledge.co.uk
0118 912 1929

Introduction

Microsoft Teams is a versatile messaging app and workspace for real-time communication and collaboration. Video meetings, file and app sharing, and messaging: Microsoft Teams brings all of these functionalities together in one open place that is accessible to everyone within (and even to people of your choosing outside) your organisation. 90% of users state that Teams simplifies group work and facilitates shorter and more focused meetings.

The shift to remote working, partially fueled and definitely accelerated by the COVID-19 pandemic, has created an explosion of demand for Teams and other remote communication and collaboration tools. Many organisations were forced to adopt and roll out Teams very rapidly to adapt to the new workspace reality and keep operations and communications flowing smoothly. However, due to the often high adoption speed, many organisations deployed Teams without proper governance or security in place, leaving them vulnerable to a growing number of internal and external threats.

Security should be a top priority if Microsoft Teams plays an important role within your organisation. In this white paper, we will provide you with eight useful tips to adequately secure your Teams environment. Use them to your advantage to reap the benefits of Teams in a safe manner!



8 tips to secure your Microsoft Teams environment

1. Use end-to-end encryption

Using end-to-end encryption is an important part of the Teams security equation. It means that content is encrypted before it's sent and decrypted only by the intended recipient. With end-to-end encryption, only the two endpoint systems are involved in encrypting and decrypting the call data. No other party, including Microsoft, has access to the decrypted conversation.

During an end-to-end encrypted call, the application secures the audio, video and screen sharing features of the participants. Certain advanced Teams features, such as live captions and transcription, call transfer, call merge, call park, recording, and adding a participant, are not available during an end-to-end encrypted call.

You can enable end-to-end encryption for your organisation by creating one or more policies that define who can use end-to-end encryption. You can activate end-to-end encrypted calls in the Teams settings on your device. Each user needs to complete this task, but they only need to do it on one device. Subsequently, Teams synchronises this setting across supported endpoints for each user.

2. Azure Sentinel and Microsoft Teams

Using Azure Sentinel in combination with Microsoft Teams allows you to harness the power of advanced automated threat analysis in your central collaboration and communication hub. Hunting in logs and the real-time monitoring of meetings are two important Azure Sentinel security features. Sentinel also allows administrators to carry out security management tasks (monitoring third-party devices, managing Microsoft Threat Protection and 365 workloads) in and from one location.

But the most important takeaway is that Sentinel workbooks and runbooks make security monitoring in Teams a systematic affair. This makes it easier to prioritise specific threats and provide the proper security contexts. Because Teams logs activity through Microsoft 365, audit logs aren't collected by default. This means you first need to turn on this feature with **these steps.** Teams data is collected in the Microsoft 365 audit under Audit.General. If you enable the Office 365 data connector, Azure Sentinel also allows you to ingest Teams data into Sentinel together with other Office 365 data.

3. Apply identity models and authentication for Microsoft Teams

Microsoft Teams supports all the identity models that are available with Microsoft 365 and Office 365. These include:

- Cloud-only. User accounts are created and managed in Microsoft 365 or Office 365 and stored in Azure Active Directory (Azure AD). User sign-in credentials (account name and password) are validated by Azure AD.
- Hybrid. User accounts are typically managed in an on-premises Active Directory Domain Services (AD DS) forest. Depending on the configuration, credential validation can be done by Azure AD or AD DS, but also by a federated identity provider.

Check this **table** for the configurations that fit your identity and organisation model. To provide an additional level of security, Microsoft Teams also gives you the option to use multi-factor authentication. This means that the combination of a username and password doesn't suffice: you need an additional verification method to get access to the app, calls and meetings.

4. The way you sign in to Microsoft Teams

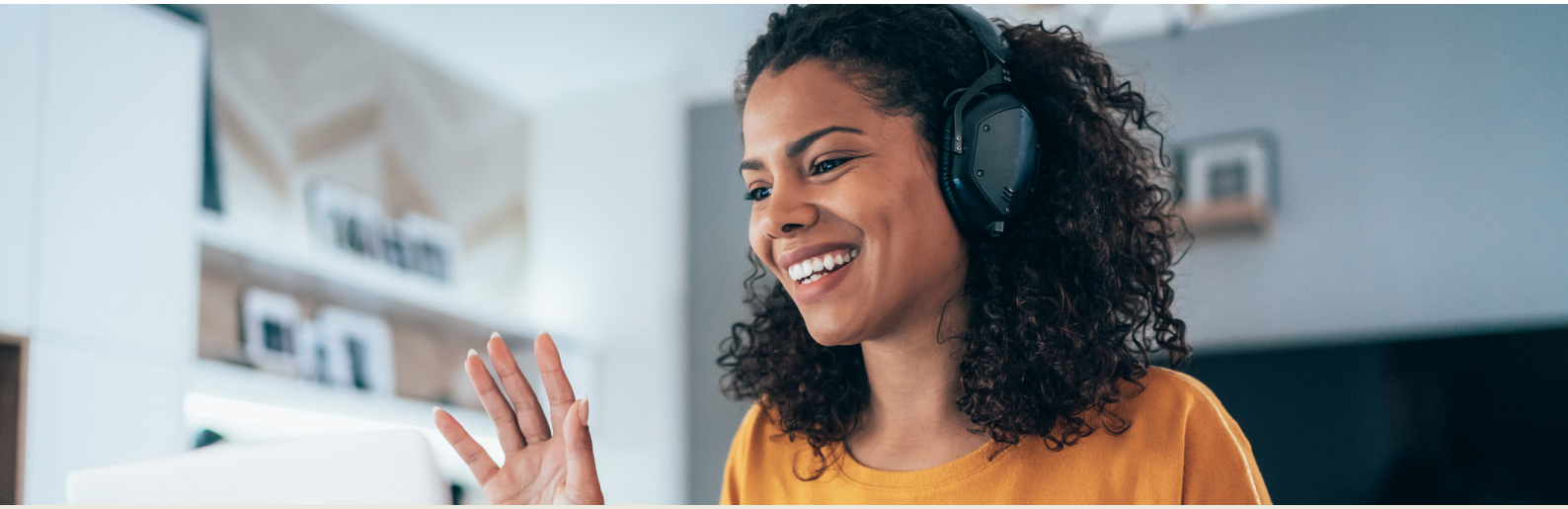
The way you sign in also affects the security level of Teams. Modern authentication is a process available to every organisation that uses Teams. It lets Teams know that users have already entered their credentials, such as their work email and password, elsewhere and that they shouldn't be required to enter them again to start the app. Using this functionality in combination with multi-factor authentication allows your employees to sign in in a user-friendly and safe manner. In addition, Microsoft Teams gives you the opportunity to **restrict** abilities to sign in on mobile and desktop devices.

5. The way you sign out of Microsoft Teams

Teams allows users to sign out of the app and end their session in a safe and easy manner. The application's single sign-on design allows users to use multiple apps on their device without requiring them to sign in to every single app. When people sign out of Teams, the app removes the data associated with their accounts. However, other apps on the device can continue to have access to the account.

Teams Android also supports global sign-in and sign-out for frontline workers. Employees can pick a device from the shared device pool and do a single sign-in to "make it theirs" for the duration of their shift. At the end of the shift, users are able to globally sign out on the device. This will remove all of their personal and company information from the device so they can return it to the device pool.

"Course M-MS700, Managing Microsoft Teams (MS-700) helps you to become a Teams Administrator and Microsoft Access and Identity Administrator helps you to become an administrator with security in mind."



6. Apply Safe Links settings

The Safe Links feature, which is a part of **Defender for Office 365**, is a great way to improve the security level of your Teams environment. It provides URL scanning and rewriting of inbound email messages in mail flow, but also time-of-click verification of URLs and links in email messages and other locations.

How does it work? When a user starts the Teams app, Microsoft 365 verifies that the user's organisation includes Microsoft Defender for Office 365. Safe Links also checks if the user is included in an active Safe Links policy where protection for Microsoft Teams is enabled. Subsequently, URLs are validated at the time of click for the user in chats, group chats, channels and tabs. You enable or disable Safe Links protection for Microsoft Teams in Safe Links policies. Read **this article** for extra and more detailed information about Safe Link settings.

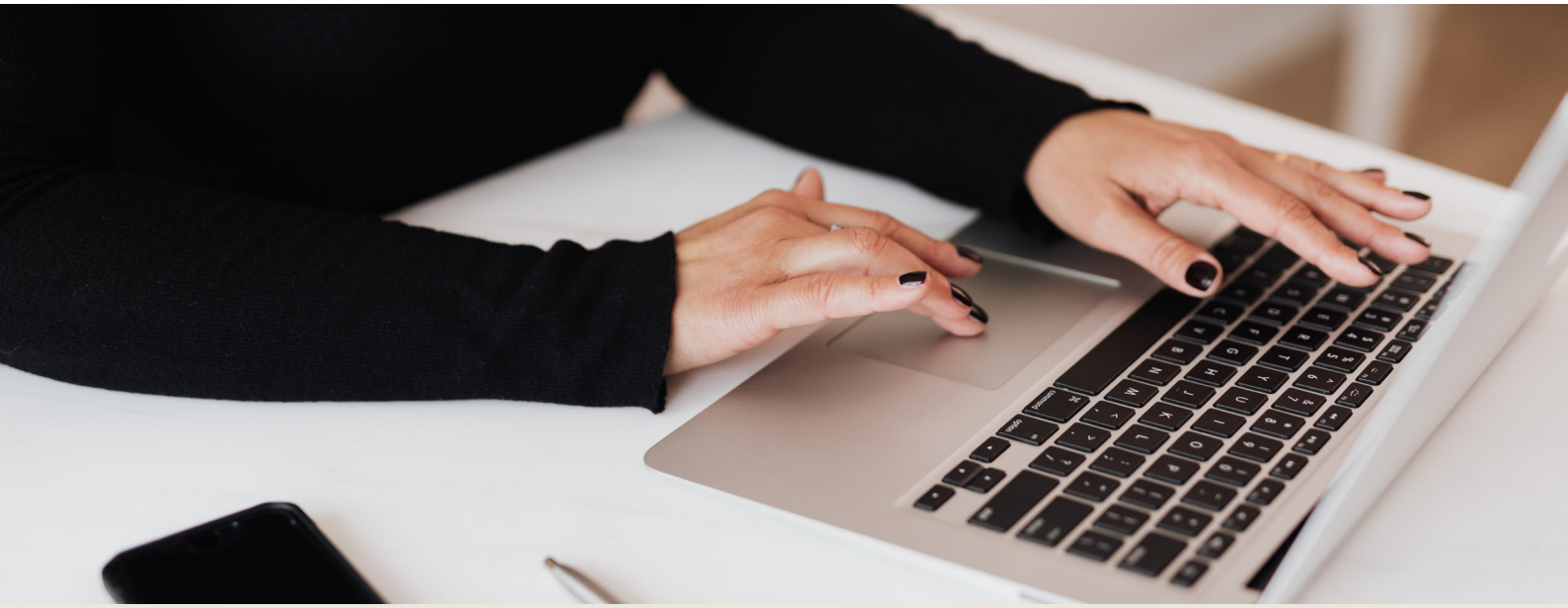
7. AppLocker control policies

AppLocker is specially designed to restrict script and program execution by non-admins. Using the tool requires the creation
of AppLocker-based allow listing policies.
AppLocker rules are organised into specified collections of rules. They apply to the targeted app and form the components that make up the AppLocker policy.
The **publisher condition rules** are generally the best option for Microsoft Teams. The digital signature of a Teams file contains information about the company that created the app file (the publisher). AppLocker policies check this information and provide you with valuable information about the safety status of a specific Teams file.

8. Block access to SharePoint

It is also possible to block access to SharePoint files (upload, download, view, create, edit), but at the same time allow your employees to use the Teams desktop, mobile, and web clients on unmanaged devices.
You can block or limit access to SharePoint files for users in the organisation, for some users or specific security groups, all sites in the organisation, or only a limited number of sites.

"The more knowledge you have of the Teams solution the better you will be able to secure your environment."



How Global Knowledge helps

Do you want to use Microsoft Teams in a safe and user-friendly way? Then understanding the application and the aforementioned security checks is of the utmost importance. Our **Microsoft and Azure training courses** will help you get the hang of security, identity and access management in Teams. The course "**Microsoft Access and Identity Administrator**" teaches you everything you need to know about implementing and managing the right security policies for your Teams environment.

More information

Would you like to know more about the best security practices for your Microsoft Teams environment? Then don't hesitate to **contact** us and explore our rich plethora of intensive, interesting and high-quality training courses.

CONTACT US