



## HOW TO SECURE MICROSOFT TEAMS

Teams is a complicated application, and complexity lies underneath its apparent simplicity.

### Secure Microsoft Teams Users

All apps run the danger of being vulnerable if user accounts are. Forcing the use of MFA is the single most crucial action you can do to ensure safe users (MFA). To make sure that everyone follows the rules, you may use conditional access policies in conjunction with MFA if you have Azure AD Premium licenses.

### Secure Microsoft Teams External Access

The attention shifts to persons whose identities reside outside of your business in other Microsoft 365 tenants or other directories like Google after ensuring that tenant users are protected. These users have access to Teams by using:

- **Azure AD B2B Collaboration:** Used to give outsiders access to teams as guest members with access to public and private channels as well as the team and private sites on SharePoint Online.
- **Azure AD B2B Direct Connect:** Used to give outsiders access to the SharePoint Online sites for shared channels by allowing them to join as members.

The first choice to make is whether to let access from the outside. Because it's challenging to cooperate just internally, most firms do. External access is the process of allowing individuals inside your firm who have valuable, unique experience, information, and skills in.

The emphasis switches to Azure AD because it controls inbound connections, assuming that external users are welcome. Every organization is advised to concentrate their attention to two groups of settings in the External Identities part of the Azure AD admin centre after choosing who is allowed to add guest members.

- **Collaboration restrictions under External collaboration settings.** These regulate the external domains that guests' accounts may originate from. You can have a single accept list that only allows visitors from certain domains or a deny list that only allows visitors from these domains. One alternative is to use a brief deny list (Figure 1). Most businesses restrict rival names, and many of them don't let visitors from customer domains like Outlook.com in. Smaller

companies frequently utilize these email services, therefore barring visitors from consumer domains has its drawbacks.

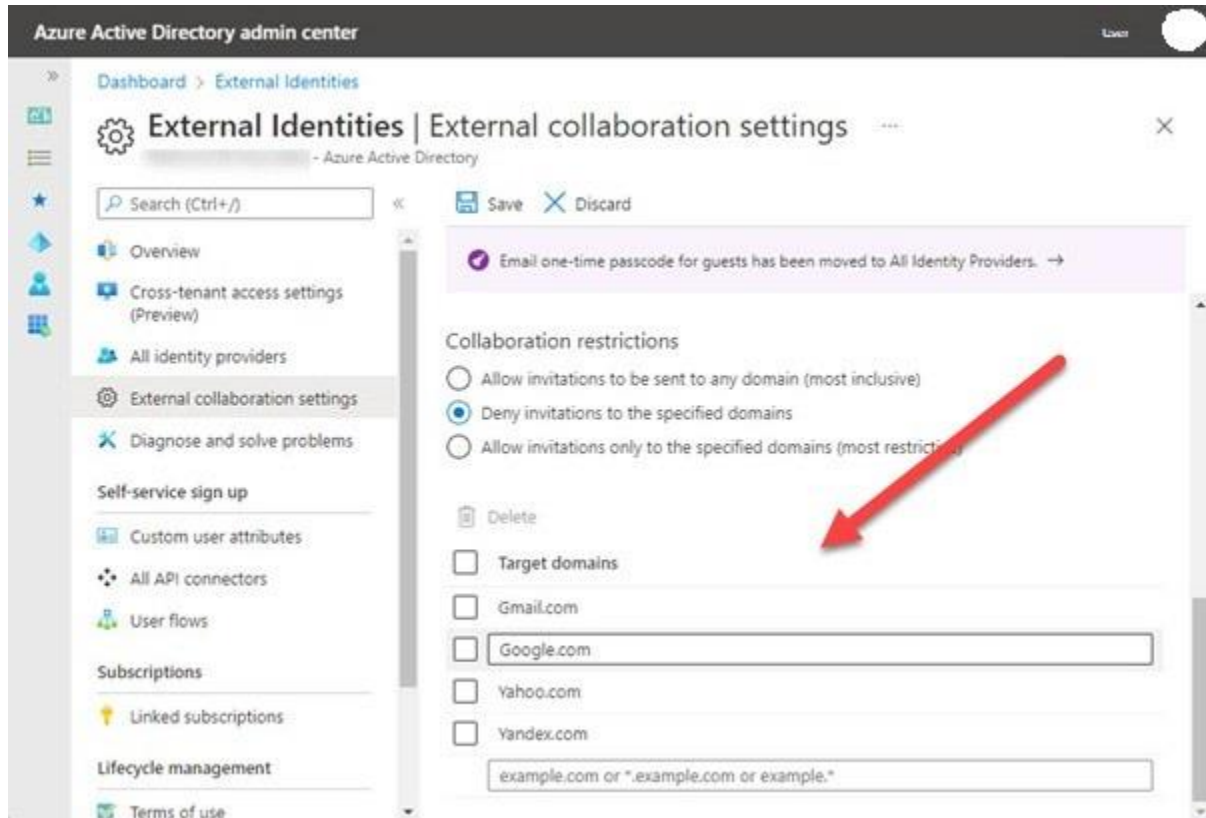


Figure 1: Blocking domains for external collaboration

- **Settings for cross-tenant access.** Teams shared channels is the first application to use this technique of restricting outsider access. Because Azure AD accepts the credentials provided by their home tenant, external participants of shared channels don't need guest accounts. With these parameters, you may be specific. It is advised to select default settings that are effective for all tenants and to only establish tenant-specific settings when necessary, such as when you need to impose access restrictions on a particular user group from another tenant. Settings for cross-tenant access may also be set up in Azure B2B Collaboration's control panel. Simply build a cross-tenant policy that disables outbound access to another Microsoft 365 tenancy if you don't want your users to become guests there (Figure 2).

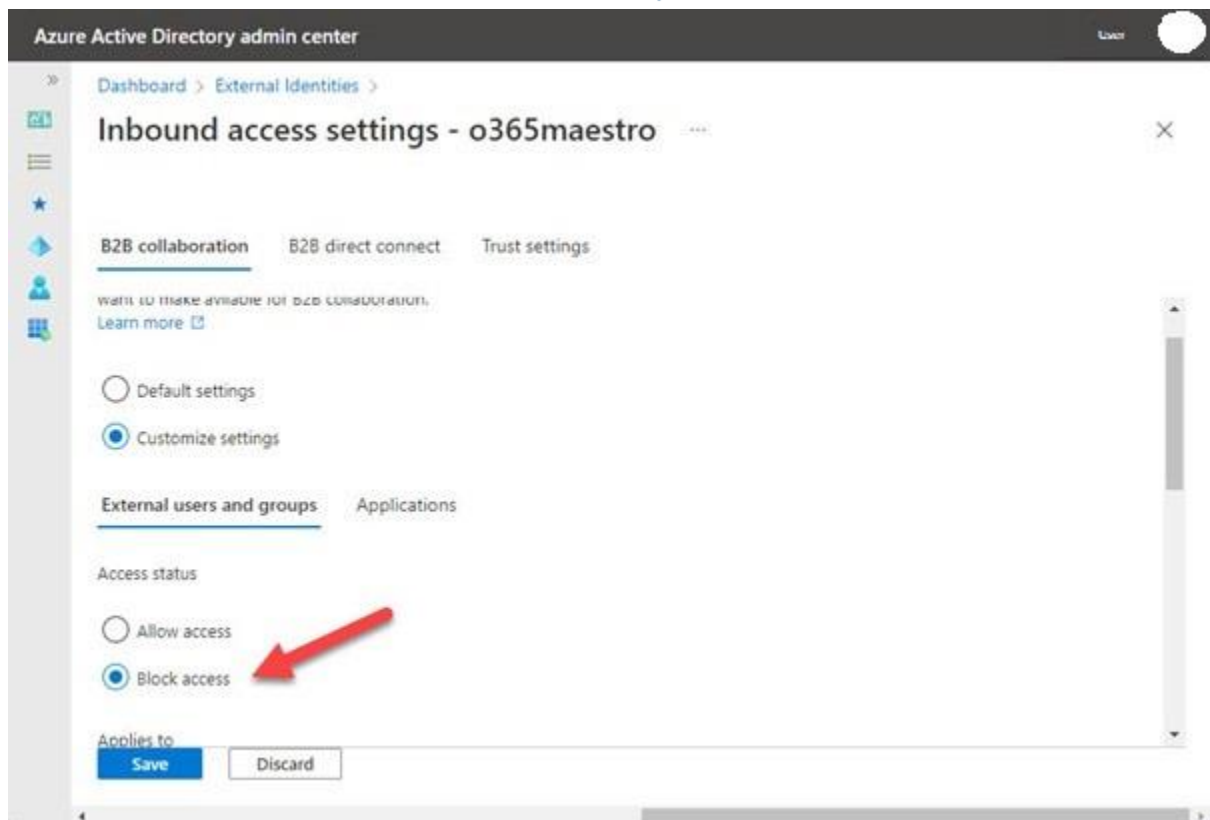


Figure 2: Blocking guest access to another Microsoft 365 tenant

## Securing Microsoft Teams

We go on to secure teams (the collaboration spaces managed by the Teams service) after tenant users are secured by MFA and external access is under control.

If you have an Office 365 E5 license or a Microsoft 365 Compliance license, Microsoft 365 Data Loss Prevention policies can monitor chat and channel communications. It's a good approach to employ if you need to prevent various user groups (organization segments) from interacting with one another in chat, channels, and meetings.

## Labels for sensitivity and container management

Container management refers to using sensitivity labels to manage team settings (available in Office 365 E3 and above). For instance, all teams that are permitted to have guest members have the Guest Access sensitivity label attached to them. Several settings for the team's SharePoint Online site, including privacy and visitor access settings, are inherited by the team when it obtains the label (Figure 3).

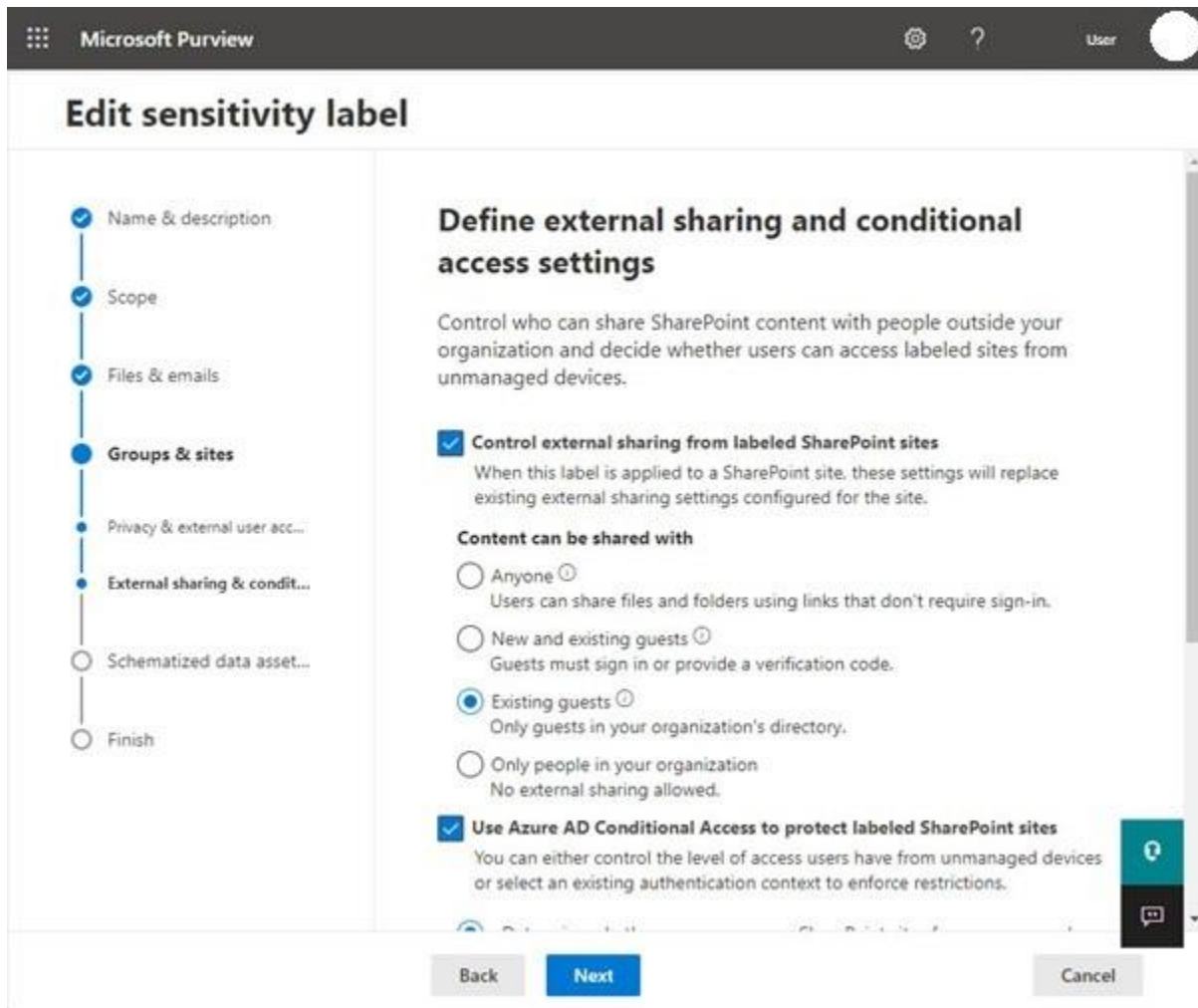


Figure 3: Configuring a sensitivity label for container management

The most significant benefit of adopting sensitivity labels for container management is that the company applies identical settings across all labelled teams. Microsoft is expanding the collection of container controls in sensitivity labels (the newest addition is site sharing permissions). Because the team will inherit the essential settings from the label, businesses might, for instance, shut down crucial and confidential teams by applying the appropriate sensitivity label to them.

Teams with visitors and shared channels frequently contain private information that should not be accessible to outsiders. Private channels are one method to do this, but sensitivity labelling and encryption can also be used to safeguard private documents. This kind of sensitivity label includes permissions given to various individuals and groups. Visitors can see that there is private information on the team's SharePoint Online site if the label restricts access to tenant accounts, but they are unable to read protected documents.



## **Applications**

You may use setup rules to install applications for users and you can prohibit apps on an individual or organizational level. Check the state of the app's MS365 app certification before making any decisions regarding its deployment to learn what user data access the app requires.

## **Limit sprawl**

Sprawl refers to the creation and potential usage of an excessive number of groupings. Group sprawl is important because when a company has hundreds of teams, managing each team requires more effort. This time may be better spent by administrators examining Azure AD sign-in logs or learning how to utilize tools like MS Sentinel to find issues. Teams that are no longer needed or requested can be removed using tools like the group expiration policy, but management is also required. Controlling the formation of new teams and preventing sprawl is the best strategy.

## **Auditing**

Over 1,500 distinct events for workload activities may be recorded by Microsoft 365 tenants with Office 365 E3 and higher licenses in a unified audit log that can be searched using PowerShell or the Microsoft Purview Compliance interface. Tenant administrators must be aware of what is happening to be secure. If they do, they'll see indications of unusual behaviour that might be first signals of an assault or compromise. It is worthwhile to take the time to become familiar with the Search-UnifiedAuditLog cmdlet's operation and the outcomes it produces. It's worthwhile to browse the audit log to discover what events are associated with activities in Teams, Exchange Online, Azure AD, and other workloads as Microsoft continually adds new events to the audit log.

## **Source**