



Advanced Security
Configurations & Tips

The ultimate guide to secure MS Teams



hello@cytex.io

cytex.io



Microsoft Teams security best practices

The MS Teams platform has many settings that can easily be overlooked. This cheat sheet serves as a vital resource for both new and experienced users, aiming to prevent data breaches and unauthorized access while providing a strategic plan to bolster organizational security. It begins with an overview of the Microsoft Teams ecosystem, focusing on proper configuration and identifying potential security vulnerabilities.



1 Recommendations for three tiers of protection for data, identities, and devices:

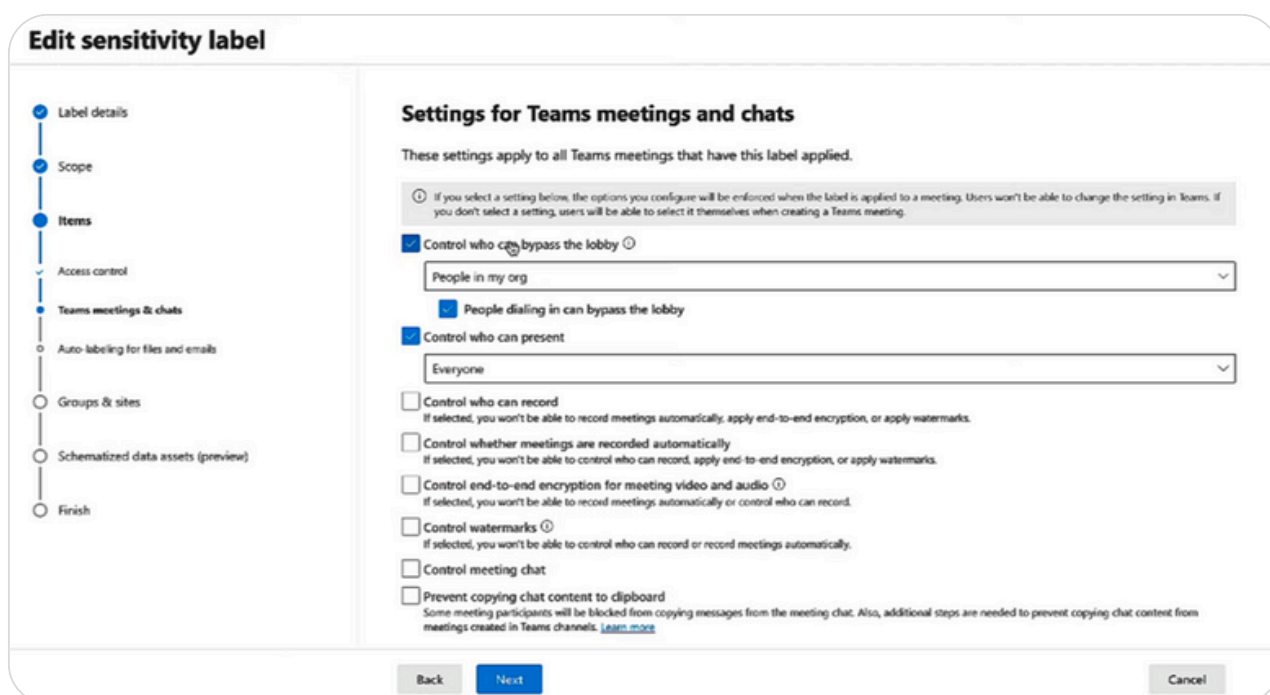
1. Baseline protection
2. Sensitive protection
3. Highly sensitive protection

Baseline protection features public and private teams. Public teams are accessible to anyone in the organization, while private teams are restricted to members only. Both configurations limit sharing of the associated SharePoint site to team owners for better permissions management.

Sensitive protection teams are private groups with restricted sharing and access for associated sites. Sensitivity labels define policies for guest sharing, device access, and content encryption.

2 Sensitivity labels

The sensitive and highly sensitive tiers use sensitivity labels to help secure the team and its files. To implement these tiers, you must enable sensitivity labels to protect content in Microsoft Teams, Microsoft 365 Groups, and SharePoint sites.



Edit sensitivity label

Label details
Scope
Items
Access control
Teams meetings & chats
Auto-labeling for files and emails
Groups & sites
Schematized data assets (preview)
Finish

Settings for Teams meetings and chats

These settings apply to all Teams meetings that have this label applied.

ⓘ If you select a setting below, the options you configure will be enforced when the label is applied to a meeting. Users won't be able to change the setting in Teams. If you don't select a setting, users will be able to select it themselves when creating a Teams meeting.

☒ Control who can bypass the lobby ⓘ
People in my org

☒ People dialing in can bypass the lobby

☒ Control who can present
Everyone

☐ Control who can record
If selected, you won't be able to record meetings automatically, apply end-to-end encryption, or apply watermarks.

☐ Control whether meetings are recorded automatically
If selected, you won't be able to control who can record, apply end-to-end encryption, or apply watermarks.

☐ Control end-to-end encryption for meeting video and audio ⓘ
If selected, you won't be able to record meetings automatically or control who can record.

☐ Control watermarks ⓘ
If selected, you won't be able to control who can record or record meetings automatically.

☐ Control meeting chat

☐ Prevent copying chat content to clipboard
Some meeting participants will be blocked from copying messages from the meeting chat. Also, additional steps are needed to prevent copying chat content from meetings created in Teams channels. [Learn more](#)

Back Next Cancel

MS Teams Sensitivity labels

3 MS Teams documents permission management and SharePoint site

Each team is assigned a dedicated SharePoint site for document storage, linked to team permissions. This is the the Files tab in a teams' channel.

Team owners hold the role of site owners, while team members are designated as site members. Team owners possess the authority to manage the site and have complete control over its contents, while team members are allowed to create and modify files within the site.

4 Identity and access management

All admins must enable MFA. For MS Teams subscriptions or trials purchased after October 21, 2019, security defaults are automatically enabled if prompted for MFA upon signing in.

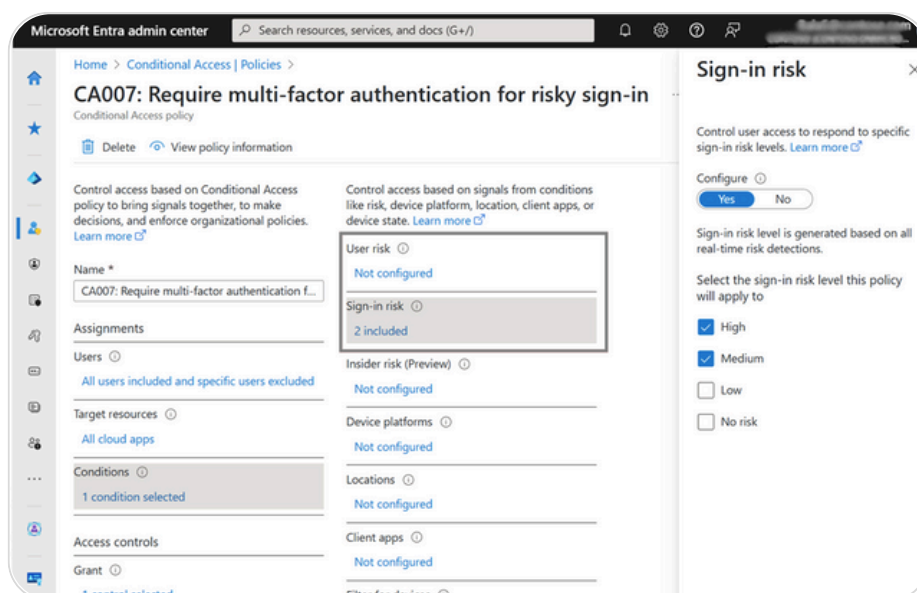
Enforce an admin least privilege policy (Least Privilege Access), assign roles and permissions based on a "need-to-know" principle. Avoid giving broad access to all users. Assign users roles such as Password Administrator or Exchange Online Administrator, rather than Global Administrator, to reduce the risk of breaches in global administrative accounts.

Configure guest access settings to limit what guests can do and see within Teams channels and chats.

Implement Conditional Access policies based on identity, device, and location to restrict access to Teams and dependent services.

5 Configure and enable user risk policies

There are two types of risk policies in Microsoft Entra Conditional Access, user risk policy and sign-in risk policy. These policies automate responses to detected risks, enabling users to self-remediate.



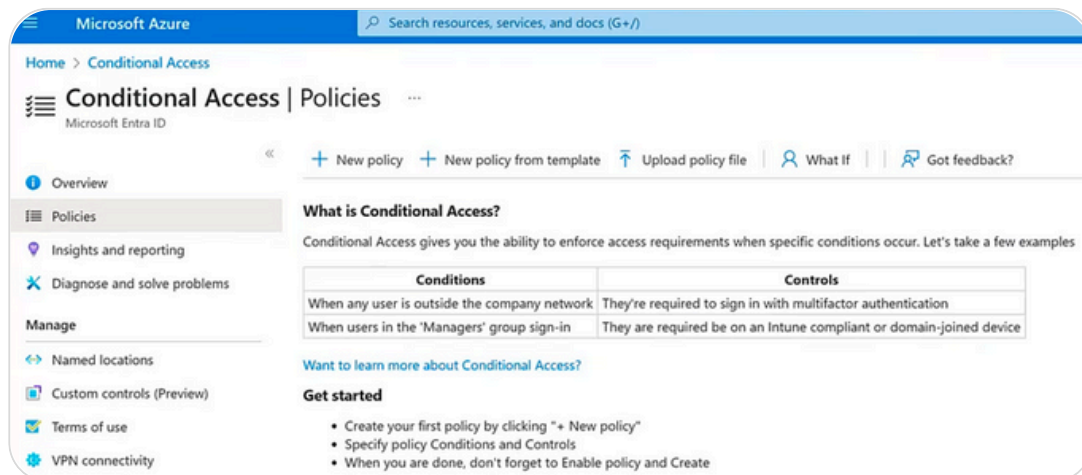
MS Teams user risk policies

6

Setup conditional access policy

Conditional access enables admins to manage resource access based on specific conditions, enhancing security by preventing unauthorized access and minimizing data breach risks. An Azure AD Premium P1 license is required to use Microsoft Office 365's conditional access policy feature. Here's how to activate it for MS Teams:

- Navigate to Azure Active Directory > Security > Conditional Access.
- Click + New Policy, naming it (e.g., "Teams Conditional Access Policy").
- Assign the policy to specific users or groups.
- Select "Microsoft Teams" under Cloud apps or actions.
- Set conditions for policy enforcement, like restricting access by location or device type.
- Choose access controls, such as requiring multi-factor authentication or blocking access.
 - Save the policy to apply it to the designated users or groups accessing Microsoft Teams.



Access policies

7

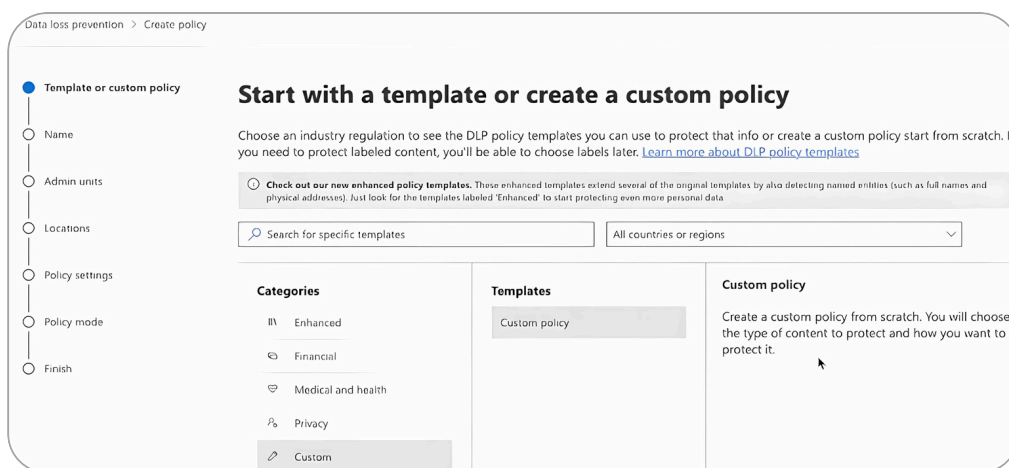
Prevent data leakage in MS Teams

Microsoft Purview Data Loss Prevention (DLP) helps prevent the sharing of sensitive information in Microsoft Teams. It requires an E5 license for DLP licensing. Here's how to apply DLP policies in MS Teams:

- In Microsoft Purview Compliance Center navigate to Data Loss Prevention > Policy.
- Choose to create a DLP policy from templates or customize one.
- For a custom policy, select "custom" from the Categories tab and name it.
- Assign admin units from Azure Active Directory to restrict the policy to specific users/groups.
- Ensure the toggle for 'Teams chat and channel messages' is on when choosing locations.
- Define policy settings for advanced DLP rules.
- Create the DLP policy with conditions, exceptions, and actions as needed.
- Test and review the policy before saving.

7

Prevent data leakage in MS Teams



DLP Policies

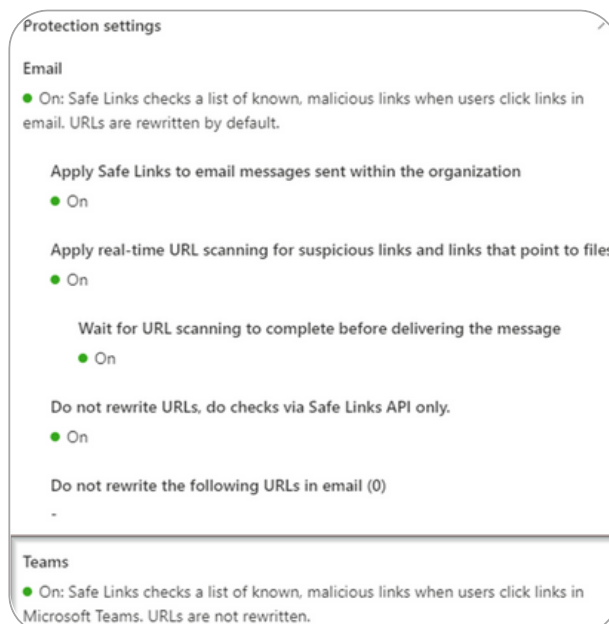
After creating the policy, it will be enforced in Microsoft Teams to block or flag sensitive information for review based on your chosen actions.

8

Secure MS Teams against phishing attacks

Microsoft Teams, combined with Defender for Office 365, offers enhanced protection against malicious phishing attacks using weaponized URLs. This feature provides time-of-click protection for links in chats and channels, safeguarding teams from threats. Accessing the Microsoft Defender portal requires an E5 license. Here's how to enable Microsoft Defender for Office 365 in Teams:

- Sign into the Microsoft 365 Defender Portal: <https://security.microsoft.com/>
- Go to Policies & rules → Threat Policies → Safe Attachments.
- Click on 'Global Settings' and ensure 'Turn on Defender for Office 365 for SharePoint, OneDrive, and Microsoft Teams' is enabled.
- Navigate to Policies & rules → Threat Policies → Safe Links.
- Select each policy (if multiple) and under Protection settings → Teams, ensure 'Safe Links checks a list of known, malicious links when users click links in Microsoft Teams' is checked. Turn it on and save if necessary.



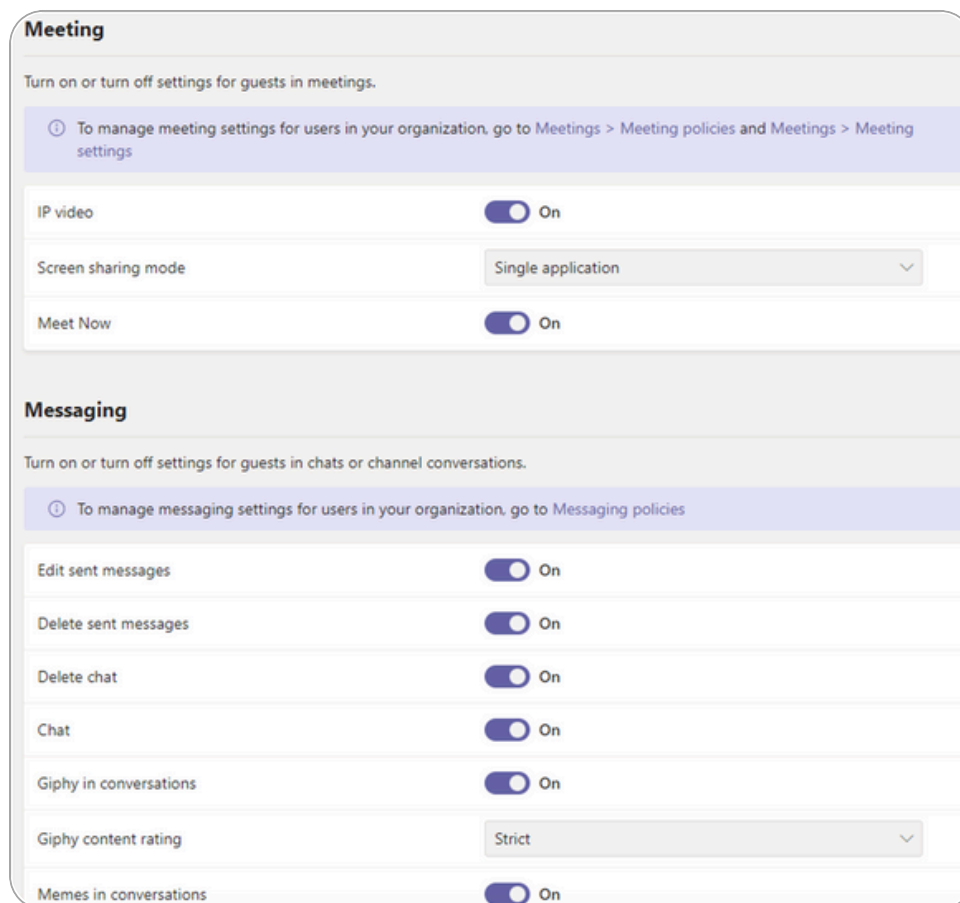
Safe Links Protection for MS Teams

9 Configure Teams Guest access settings

You can improve collaboration and communication in Microsoft Teams by inviting guests. To protect the security and privacy of your data, it's crucial to set the appropriate guest access settings. The Teams admin center allows you to customize these guest access rules to meet your specific requirements.

Setting appropriate guest access rules allows secure collaboration with clients and partners. Additionally, with the ability to disable screen sharing during video meetings ensures confidential information remains secure.

- Go to Microsoft Teams admin center → Users → Guest Access.



The screenshot displays the 'Meeting' and 'Messaging' sections of the Microsoft Teams admin center. The 'Meeting' section includes settings for IP video (On), Screen sharing mode (Single application), and Meet Now (On). The 'Messaging' section includes settings for Edit sent messages (On), Delete sent messages (On), Delete chat (On), Chat (On), Giphy in conversations (On), Giphy content rating (Strict), and Memes in conversations (On). Each setting is accompanied by a toggle switch or a dropdown menu.

Guest user access permissions in MS Teams admin center

10 Control who can send email to Team's channel

To enhance the security of Microsoft Teams communication, restrict channel email messages to approved domains. This prevents unauthorized access and potential security breaches. Follow these steps:

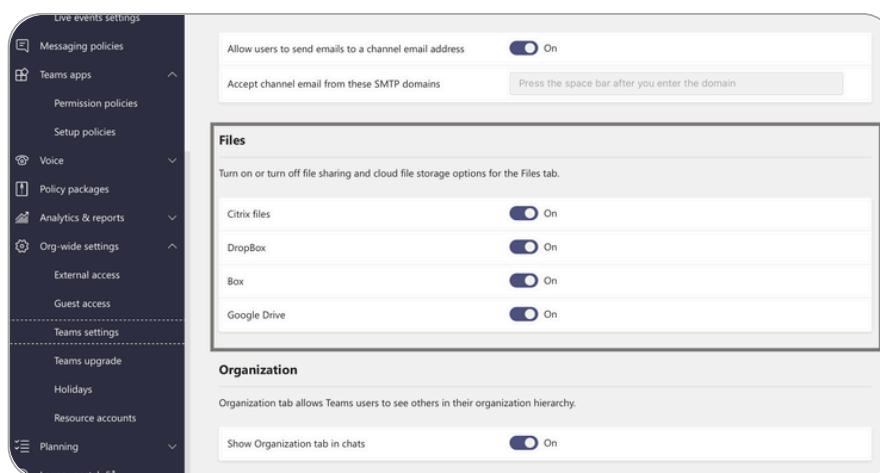
- Access the Microsoft Teams admin center.
- Go to Teams → Teams settings.
- Use the 'Email integration' toggle to control email permissions.
- If allowed, enter accepted domains in the 'Accept channel email' field and click Save.

11

Securing third-party storage

With Teams, you can store files on third-party services like Citrix, Dropbox, Google Drive, and more. However, some may risk data leakage, so you can disable unsupported providers to keep your data secure. Here's how to control third-party cloud storage access in MS Teams:

- Access the Microsoft Teams admin center.
- Go to Teams → Teams Settings.
- Under 'Files', select desired storage providers for the files tab and click Save.



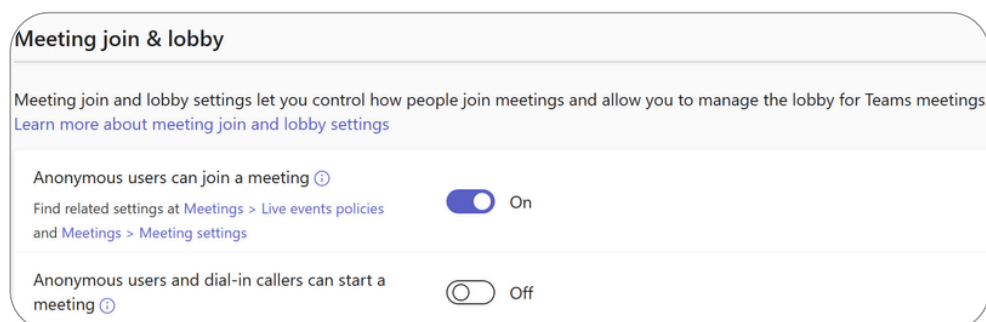
MS Teams third-party file integrations

12

Manage meeting policies to minimize the attack surface

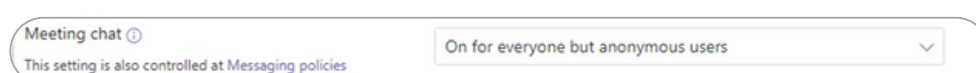
Managing Microsoft Teams meeting settings is crucial for customizing the meeting experience and enhancing security. To minimize risks and restrict content sharing, follow these steps:

- Microsoft Teams admin center → Meetings → Meeting Policies → Global Policy.
- In the Meeting join & lobby tab, turn off 'Anonymous users can join a meeting' and 'People dialing in can bypass the lobby.'



MS Teams meeting lobby settings

- Microsoft Teams admin center → Meetings → Meeting Policies → Global Policy.
- Under Meeting engagement, allow Meeting chat option for Everyone but anonymous users.

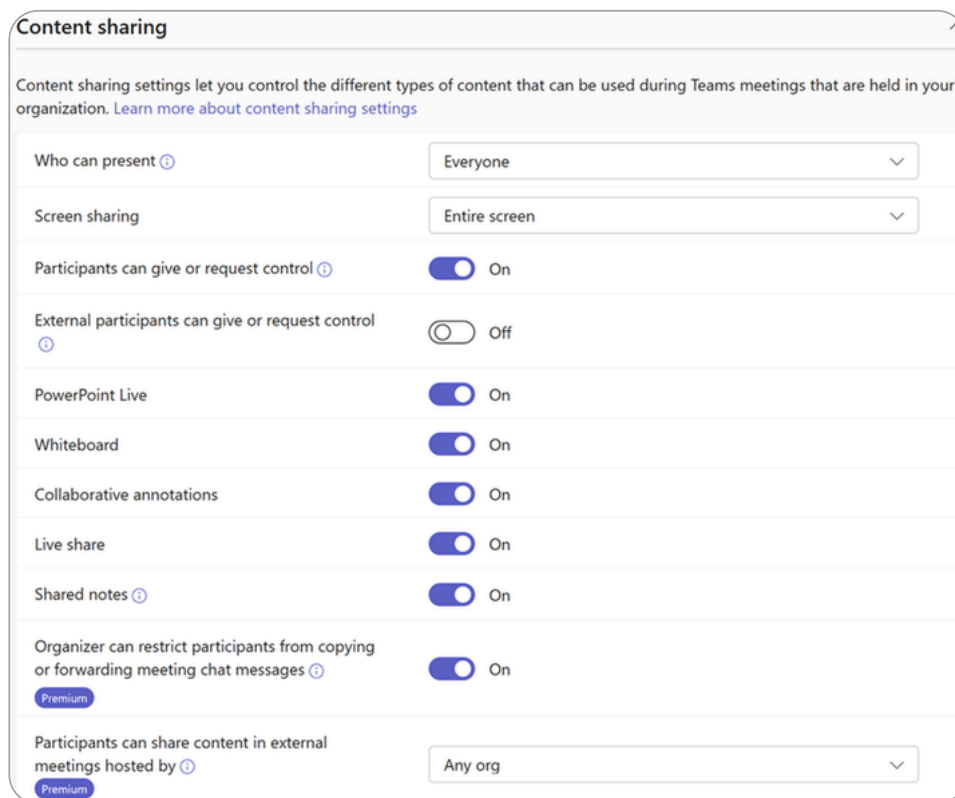


MS Teams meetings engagement settings

13

Content sharing settings

To prevent sharing inappropriate content, turn off the setting for 'External participants can give or request control' in Content Sharing. Additionally, limit the 'who can present' option to "People in my organization and guests."



The screenshot shows the 'Content sharing' settings window in MS Teams. It includes a title bar, a description, and several settings with dropdown menus and toggle switches. The settings are as follows:

Setting	Value
Who can present	Everyone
Screen sharing	Entire screen
Participants can give or request control	On
External participants can give or request control	Off
PowerPoint Live	On
Whiteboard	On
Collaborative annotations	On
Live share	On
Shared notes	On
Organizer can restrict participants from copying or forwarding meeting chat messages	On
Participants can share content in external meetings hosted by	Any org

MS Teams content sharing settings

14

MS Teams updates

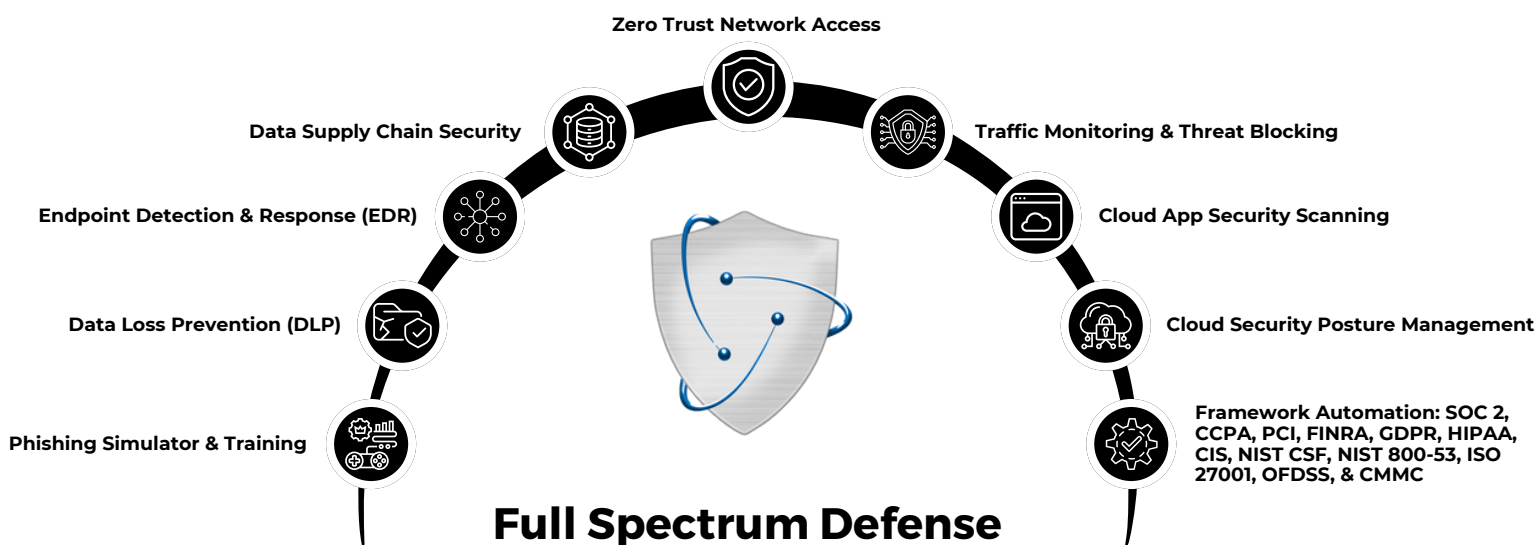
Make sure to enable updates for the following software components in the Teams admin center. Additionally, remember to update any components that need manual updates.

- Teams app: Manual and Automatic updates available.
- Device firmware: Manual and Automatic updates available.
- Company Portal app: Manual updates only.



Explore **Cytex Unified Resilience Platform** today

[Schedule demo](#)



<https://cytex.io>



hello@cytex.io



[@cytexsmb](#)



[@cytexsecure](#)