100 XP

Address threats to Teams meetings

3 minutes

Microsoft Teams provides the capability for your organization's users to create and join meetings in real time. Participants in a Teams meeting can invite external users to join, who aren't authenticated to your tenant. Users who are employed by external partners with a secure and authenticated identity can join meetings and, if promoted to do so, can act as presenters. Extending participation to external users can introduce security risks.

Suppose you have a requirement to grant access for guests to join meetings. To meet the organizations regulatory compliance, you want to explore how you can enable external users to access the meetings, while controlling how much a guest can see and interact with in your meetings.

Here, you'll learn how to control who arrives in Teams meetings and who will have access to any information presented.

Security considerations

An anonymous user is one that isn't authenticated in your organization's tenant. This means that by definition all external users are considered anonymous. Enabling an external user to participate in a meeting can introduce security risks. Teams addresses these risks with these safeguards:

- Participant roles determine meeting control privileges.
- Participant types allow you to limit access to specific meetings.
- Scheduling meetings is restricted to users who have an Azure Active Directory account and a Teams license.
- Anonymous, that is, unauthenticated, users who want to join a dial-in conference must dial one of the conference access numbers. If the **Always allow callers to bypass the lobby** setting is turned **On**, then they also need to wait until a presenter or authenticated user joins the meeting.

Use lobby settings to control anonymous access to Teams meetings

In Teams, anonymous users are transferred to a waiting area called the lobby. Presenters can then either **admit** these users into the meeting or **reject** them. When these users are

transferred to the lobby, the presenter and attendees are notified, and the anonymous users must then wait until they're either accepted or rejected, or their connection times out. Meeting organizers control whether participants join a meeting without waiting in the lobby.

Anonymous users can't create or join a meeting as a presenter, but they can be promoted to presenter after they join.

Each meeting can be set up to enable access using any one of the following methods:

The defaults are:

- **People in my Organization** - Everyone external to the organization will wait in the lobby until admitted.
- **People from my organization and trusted organizations** - Authenticated users and external users from Teams and Skype for Business domains that are in the external access allow list can bypass the lobby. All other users will wait in the lobby until admitted.
- **Everyone** - All meeting participants bypass the lobby once an authenticated user has joined the meeting.

Use structured meetings to control guest participation in a Teams Meeting

The other approach to mitigating the risk of allowing external users to join Teams meetings is to use **structured meetings**. The approach grants the Presenter of the meeting with enough control to manage what the attendees do.

Actions	Presenters	Attendees
Speak and share their video	Y	Y
Participate in meeting chat	Y	Y
Change settings in meeting options	Y	N
Mute other participants	Y	N
Remove other participants	Y	N
Share content	Y	N
Admit other participants from the lobby	Y	N
Make other participants presenters or attendees	Y	N

Actions	Presenters	Attendees
Start or stop recording	Y	N
Take control when another participant shares a PowerPoint	Y	N

Next unit: Configure Teams meeting settings

Continue >