FinGarde
YOUR RIA TECHNOLOGY PARTNER

Zoom Security Measures

LEVELS OF PROTECTION

Basic

SOUND NOTIFICATION

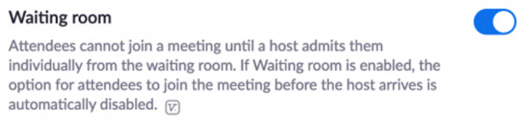
Enable notifications for visibility of new attendees throughout the conference.

Proactive

(In addition to Basic Level of Protection)

WAITING ROOM

Enable approval for all attendees that join. Ensure you are expecting and approving your attendees.



Waiting room

Attendees cannot join a meeting until a host admits them individually from the waiting room. If Waiting room is enabled, the option for attendees to join the meeting before the host arrives is automatically disabled.

BYPASS WAITING ROOM

Configure whitelisted domains for bypassing the Waiting Room, such as your own internal corporate domain: Account owners and admins can now add domains which can bypass the Waiting Room. If a user is logged in to their Zoom account with an email address at this domain, they will bypass the Waiting Room and join directly into the meeting.

LIMIT SCREEN SHARING

If you want other participants in the meeting to be able to share their screens, or if you want to be the only one with that ability, you can easily toggle this feature on and off from the screen sharing menu, as well as the security menu.

Note: Limit sharing to a required application vs entire desktop. This will avoid disclosure of other data that may be available on your screens during the session. Admins can enable the available option to enforce with "Disable desktop or screen share in a meeting and only allow sharing of selected applications."

Enhanced

(In addition to Basic and Proactive Level of Protection)

JOIN BEFORE HOST

Do not allow others to join a meeting before you, as the host, have arrived. The first person who joins the meeting may automatically be made the host and will have full control over the meeting.

FILE TRANSFERS

Disable File Transfers to avoid the transfer of malicious files exchanged within attendees. Utilize more secure methods of file transfer.

REQUIRING A PASSWORD

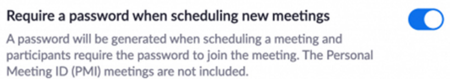
Require a Password to Join. This feature can be applied to both your Personal Meeting ID, so only those with the password will be able to reach you, and to newly scheduled meetings.

If you use the "Copy Invitation" functionality to copy the meeting link and send it to your participants, that link might include your meeting password. Look out for an unusually long URL with a question mark in it, which indicates it includes your meeting password.

If you plan to send the meeting link directly to trusted participants, having the password included in the link will be no problem. **But if you want to post the meeting link in a Facebook group, on Twitter, or in another public space, then it means the password itself will also be public.** If you need to publicize your event online, consider posting only the meeting ID, and then separately sending the password to vetted participants shortly before the meeting begins.

REGISTERED USERS ONLY

Only allowing Registered or Domain Verified Users onto a Zoom call can also give you peace of mind by letting you know exactly who will be attending your meeting. When scheduling a meeting, you can require attendees to register with their e-mail, name, and custom questions. You can even customize your registration page with a banner and logo. By default, Zoom also restricts participants to those who are logged into Zoom, and you can even restrict it to Zoom users whose email address uses a certain domain.



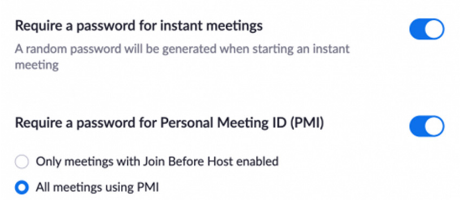
Require a password when scheduling new meetings

A password will be generated when scheduling a meeting and participants require the password to join the meeting. The Personal Meeting ID (PMI) meetings are not included.

CHAT

Disable Private Chat

In-meeting chat adds another dimension of collaboration to your meetings, creating a place for questions to be asked and fielded later, or for supplemental resources to be posted. But sometimes chat can become distracting or unproductive. Zoom allows you to disable and enable chat throughout your meeting.



Require a password for instant meetings

A random password will be generated when starting an instant meeting

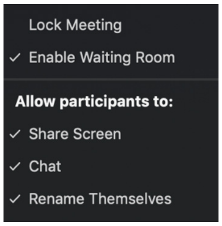
Require a password for Personal Meeting ID (PMI)

○ Only meetings with Join Before Host enabled

● All meetings using PMI

Saving Chat

Prevent participants from saving chat for potential privacy or legal concerns.



Lock Meeting

✓ Enable Waiting Room

Allow participants to:

✓ Share Screen

✓ Chat

✓ Rename Themselves

CHANGE PERSONAL MEETING ID

Don't Use Personal Meeting ID for Public Meetings. Your Personal Meeting ID (PMI) is the default meeting that launches when you start an ad hoc meeting. Your PMI doesn't change unless you change it yourself, which makes it very useful if people need a way to reach you. But for public meetings, you should always schedule new meetings with randomly generated meeting IDs. That way, only invited attendees will know how to join your meeting. You can also turn off your PMI when starting an instant meeting in your profile settings.

TURN OFF ANNOTATION

Like screen sharing and in-meeting chat, annotation can be a great tool when you need it, but it can also be an opportunity for mischief when you don't. To avoid unwanted annotation, Zoom allows you as the meeting host to remove all participants ability to annotate during a screen share. You can disable this for the entire meeting, or just temporarily.

MUTING PARTICIPANTS

We've all been in meetings where somebody forgets to mute, or their microphone picks up some background noise that interrupts the meeting. Zoom allows you to solve this problem with a simple button to mute all participants. For an added layer of security, you can also disable participant's ability to unmute themselves. When you're ready to make the meeting interactive again, you can simply hit the "Unmute All" button or allow participants to unmute themselves.

Recommendations for Registered Zoom Hosts

UTILIZE A STRONG PASSWORD

- Have a minimum password length: 10-12 characters (16 is a great goal!)
- Have at least 1 special character (!, @, #...)
- Cannot contain consecutive characters (e.g. "11111", "12345", "abcde", or "qwert")
- Use enhanced weak password detection
- New users need to change their passwords upon first sign-in
- Password expires automatically and needs to be changed after the specified # of days
- Users cannot reuse any password used in the previous number of times

ENCRYPTION

Zoom provides end-to-end encryption for in-meeting and in-webinar presentation content. Dial-in participants joining by phone are limited by the participant's phone network. Encryption can be enabled for corporations with H.323 and SIP devices by the administrator. This setting is configured at the account level, group, or user level. To ensure encryption, utilize the updated Zoom client of web meeting.

VIRTUAL BACKGROUNDS

Account owners and admins can add virtual backgrounds to the Zoom web portal for all users on their account. If the virtual background setting is locked, users will only have access to the admin uploaded virtual backgrounds and will not be able to add their own from the Zoom client. This setting is available at the account and group level and requires Zoom client version 5.1.0 and above.

ZOOM DESKTOP UPDATES

Ensure Zoom Desktop client is updated at all times. If you are not sure its on the latest version or require immediate access to a zoom conference, use the web client.