

CERT-In advisory to host secure Zoom meetings while working from home

Many organizations have allowed its staff to work from home to stop the spread of coronavirus. These people are using online communication platforms such as Zoom, Microsoft's Teams, and Teams for Education, Slack, Cisco's WebEx for remote meetings and webinars. With a majority of employees using these platforms, it has become paramount to use these apps securely.

ZOOM is one among widely used go-to video conferencing platform. Cyber criminals are trying to exploit this platform to harvest sensitive information such as meeting details and conversations. The following measures will increase the security of your Zoom sessions and reduce security risks-

1. Keep your Zoom software patched and up-to-date.
2. Always set strong and unique passwords (make your password at least eight characters long and use at least three of the following types of characters: lowercase letters, uppercase letters, numbers, symbols) for all meetings and webinars. This is especially recommended for any meetings where sensitive information may be discussed.

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.

☐ Require a password for meetings which have already been scheduled ⓘ



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



Require password for participants joining by phone

A numeric password will be required for participants joining by phone if your meeting has a password. For meeting with an alphanumeric password, a numeric version will be generated.



Password Default for Meeting and Webinar

3. Enable "Waiting Room" Feature so that call manager will have a better control over participants. All participants can join a virtual "Waiting Room" but they will be approved by call manager to be part of the actual meeting.

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. ⓘ

Choose which participants to place in the waiting room:

- ☐ All participants
- ☒ Guest participants only ⓘ
- ☐ Allow internal participants to admit guests from the waiting room if the host is not present

Save

Cancel

Customize the title, logo, and description ✎

4. Disable Join Before Host Feature: The "Join Before Host" option let others to continue with a meeting in the absence of actual host, but with this option enabled, the first person who joins the meeting will automatically be made the host and will have full control over the meeting. Alternatively, "Scheduling Privilege" may be given to a trusted participant to host the meeting in the absence of an actual host.

Join before host



Allow participants to join the meeting before the host arrives

Schedule Privilege

You can assign users in your account to schedule meetings on your behalf. You can also schedule meetings on behalf of someone that has assigned you scheduling privilege. You and the assigned scheduler must be on a Paid plan within the same account.

Assign scheduling privilege to
No one



I can schedule for

 X

Assign scheduling privilege

example: sales.ea@company.com,marketing.ea@company.com

Enter the email addresses of those who can schedule meetings on your behalf.
Use a comma to separate multiple email addresses.

Assign

Cancel

5. If not required restrict/disable file transfers.
6. From settings and controls, ensure removed participants are unable to rejoin meetings.
7. If not required one can limit Screen Sharing to the Host only.
8. Lock the meeting session once all your attendees have joined.

9. Restrict the call record feature "Allow Record" to trusted participants only.


[Groups](#) > [Admin Group 1](#) > [Settings](#)

Meeting

Recording

Telephone

Groups members will use the following settings by default. If you don't want the settings below to be default, you can lock the settings here. [Learn More](#).

Features	Status
Local recording Allow hosts and participants to record the meeting to a local file	<input checked="" type="checkbox"/> 

References:

1. <https://blog.checkpoint.com/2020/03/26/whos-zooming-who-guidelines-on-how-to-use-zoom-safely/>
2. <https://it.cornell.edu/zoom/keep-zoom-meetings-private>
3. <https://www.inc.com/jason-aten/zoom-has-a-major-security-flaw-that-could-let-malicious-websites-literally-spy-on-you.html>
4. <https://www.foxbusiness.com/technology/securely-host-zoom-meeting>
5. <https://www.forbes.com/sites/zakdoffman/2020/01/28/new-zoom-roulette-security-warning-your-video-calls-at-risk-from-hackers-heres-what-you-do/#591e905d7343>