

Securing Your Zoom Meetings

This guide will walk you through securing your Zoom meetings so that virtual get-togethers, meetings and exercise classes are not Zoom-bombed by unauthorized users.

Keep Zoom client updated

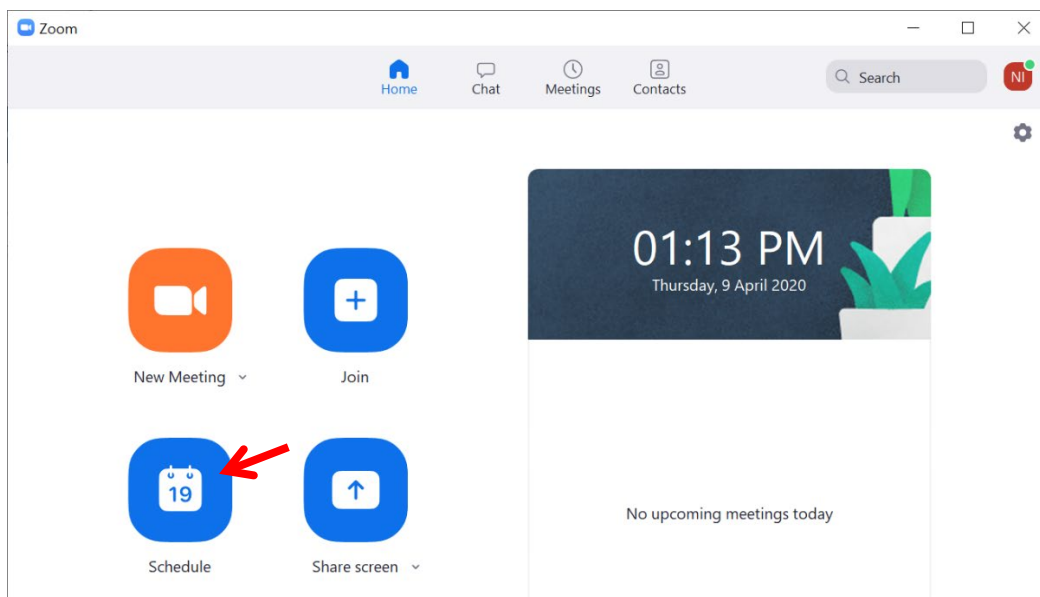
If you are prompted to update your Zoom client, please install the update.

The latest Zoom updates enable Meeting passwords by default and add protection from people scanning for meeting IDs.

By installing the latest updates as they are released, you will be protected from any discovered vulnerabilities.

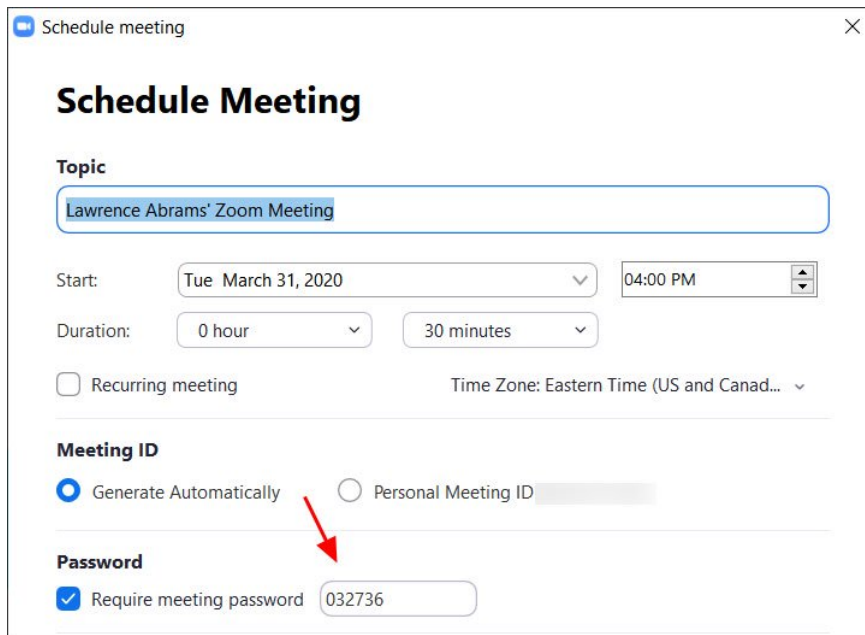
Things to note before scheduling a meeting

Before scheduling a meeting with coworkers, you can familiarize yourself with the various ways you can secure Zoom meetings using the steps below.



Add a password to all meetings!

When creating a new Zoom meeting, Zoom will automatically enable the "Require meeting password" setting and assign a random 6 digit password.



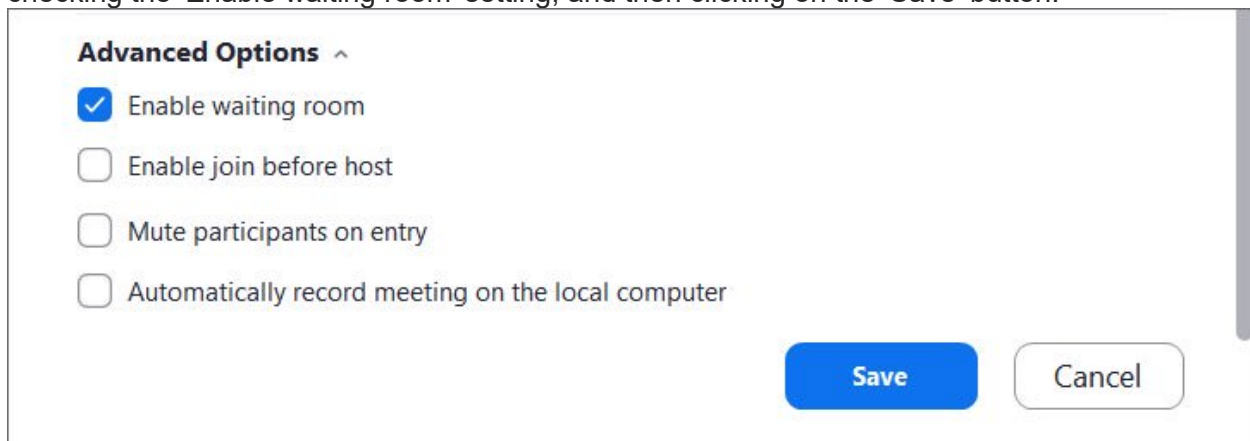
The screenshot shows the 'Schedule Meeting' dialog box in Zoom. The 'Topic' field contains 'Lawrence Abrams' Zoom Meeting'. The 'Start' date is 'Tue March 31, 2020' and the time is '04:00 PM'. The 'Duration' is set to '0 hour' and '30 minutes'. The 'Recurring meeting' checkbox is unchecked. The 'Time Zone' is 'Eastern Time (US and Canad...'. Under 'Meeting ID', 'Generate Automatically' is selected. Under 'Password', 'Require meeting password' is checked, and the password '032736' is entered. A red arrow points to the 'Require meeting password' checkbox.

You **should not uncheck** this option as doing so will allow anyone to gain access to your meeting without your permission.

Use waiting rooms

Zoom allows the host (the one who created the meeting) to enable a waiting room feature that prevents users from entering the meeting without first being admitted by the host.

This feature can be enabled during the meeting creation by opening the advanced settings, checking the 'Enable waiting room' setting, and then clicking on the 'Save' button.

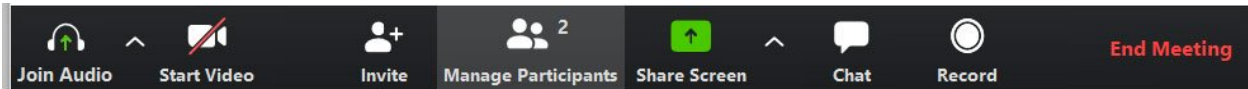


The screenshot shows the 'Advanced Options' section in the Zoom meeting creation interface. The 'Enable waiting room' checkbox is checked. Other options include 'Enable join before host', 'Mute participants on entry', and 'Automatically record meeting on the local computer'. The 'Save' and 'Cancel' buttons are visible at the bottom right.

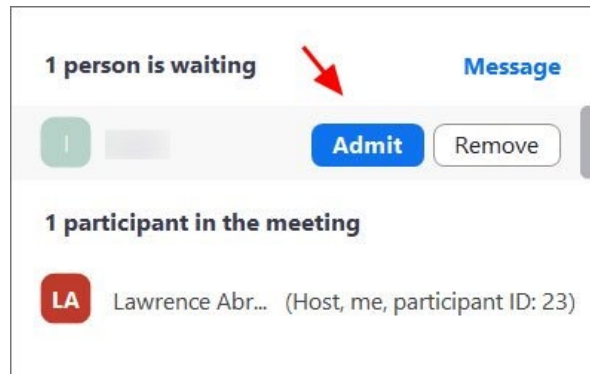
Enable waiting room setting

When enabled, anyone who joins the meeting will be placed into a waiting room where they will be shown a message stating "Please wait, the meeting host will let you in soon."

The meeting host will then be alerted when anyone joins the meeting and can see those waiting by clicking on the 'Manage Participants' button on the meeting toolbar.



You can then hover your mouse over each waiting user and 'Admit' them if they belong in the meeting.



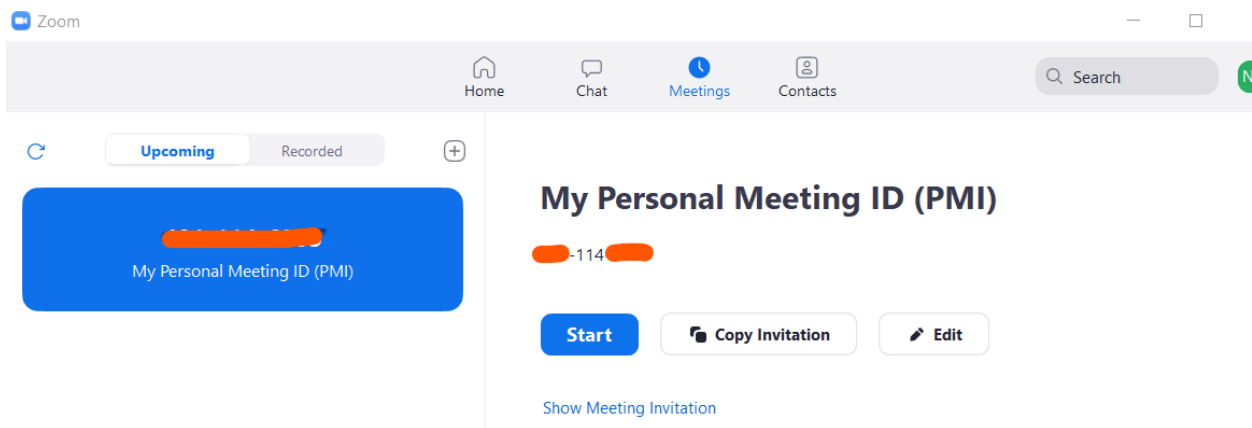
Admit a person into the meeting

Do not share your meeting ID

Each Zoom user is given a permanent 'Personal Meeting ID' (PMI) that is associated with their account.

If you give your PMI to someone else, they will always be able to check if there is a meeting in progress and potentially join it if a password is not configured.

Instead of sharing your PMI, create new meetings each time that you will share with participants as necessary.

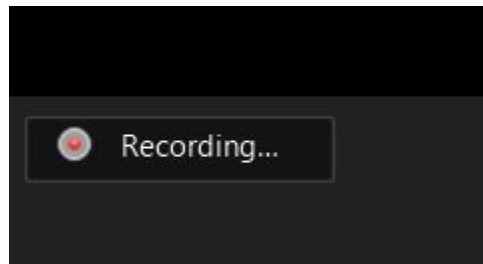


Things to note in a Zoom meeting

Privacy considerations when using Zoom

One of the most important things to remember is that a Host can record a Zoom session, including the video and audio, to their computer. Therefore, be careful saying or physically 'revealing' anything that you would not want someone else to potentially see or know about.

Meeting participants will know when a meeting is being recorded as there will be a 'Recording...' indicator displayed in the top left of the meeting as shown below.

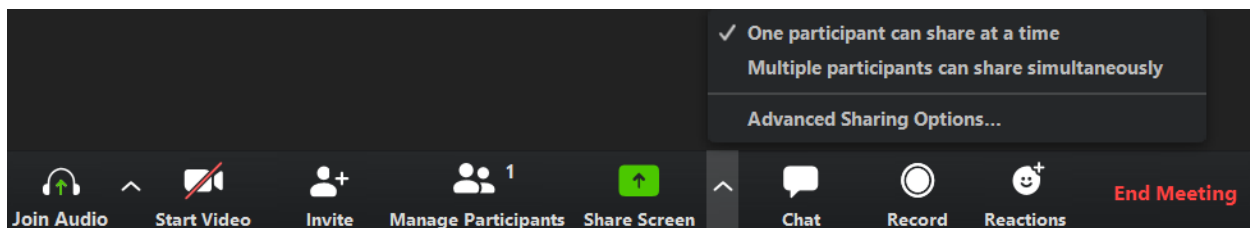


It is also important to remember that a user can download their chat logs before leaving a meeting. These logs will only contain messages that you could see, but not the private chat messages of other users.

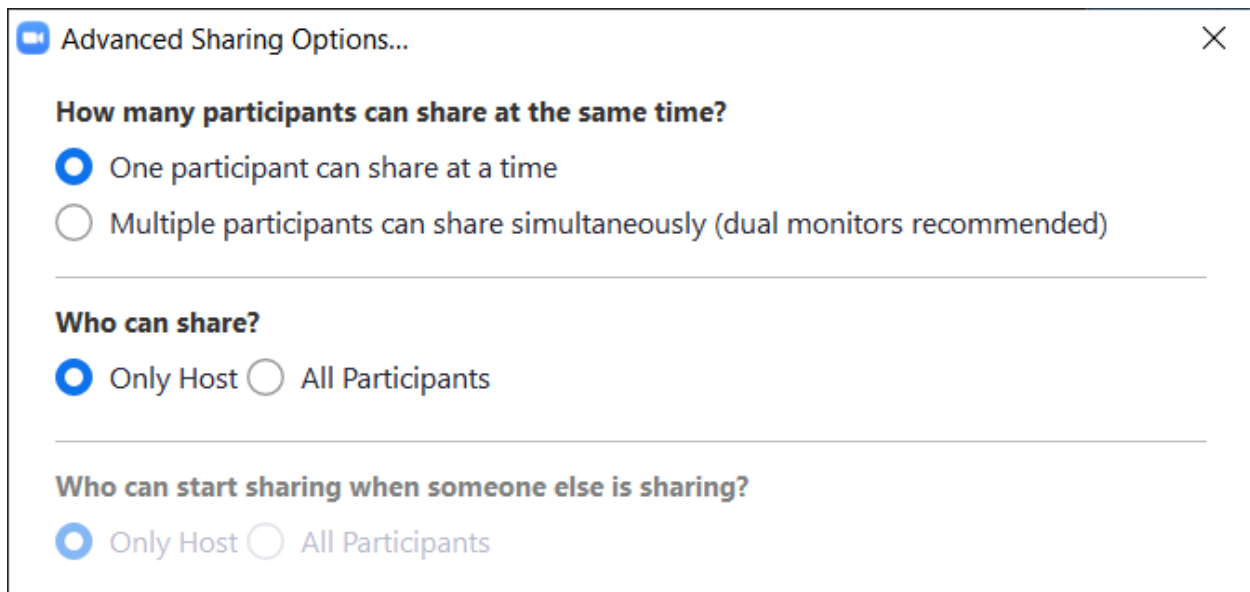
Disable participant screen sharing

To prevent your meeting from being hijacked by others, you should prevent participants other than the Host from sharing their screen.

As a host, this can be done in a meeting by clicking on the up arrow next to 'Share Screen' in the Zoom toolbar and then clicking on 'Advanced Sharing Options' as shown below.



When the Advanced Sharing Options screen opens, change the 'Who Can Share?' setting to 'Only Host'.

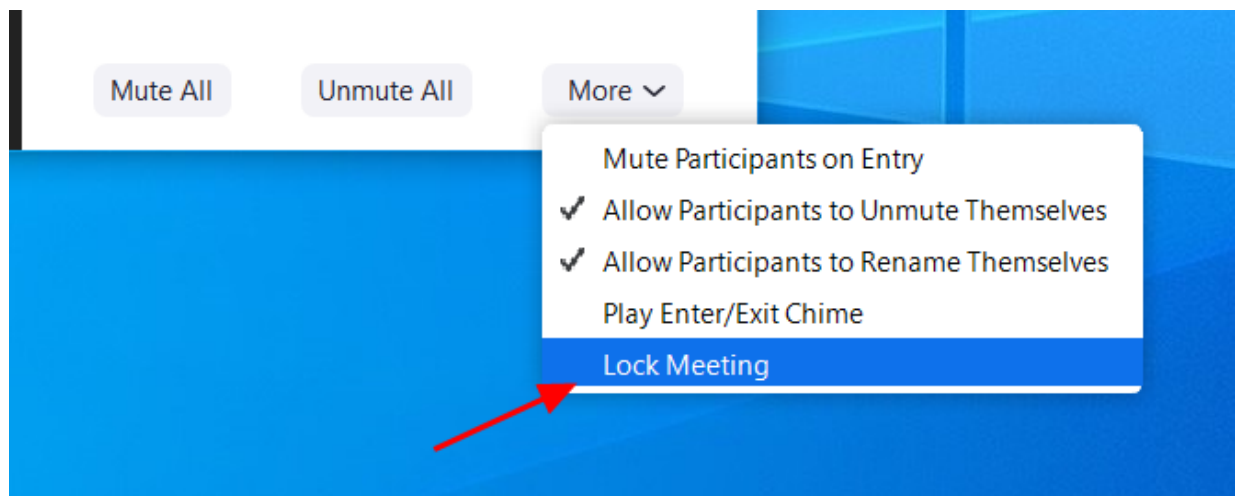


You can then close the settings screen by clicking on the X.

Lock meetings when everyone has joined

If everyone has joined your meeting and you are not inviting anyone else, you should Lock the meeting so that nobody else can join.

To do this, click on the 'Manage Participants' button on the Zoom toolbar and select 'More' at the bottom of the Participants pane. Then select the 'Lock Meeting' option as shown below.



Do not post pictures of your Zoom meetings

If you take a picture of your Zoom meeting than anyone who sees this picture will be able to see its associated meeting ID. This can then be used uninvited people to try and access the meeting.

This could have been used by attackers to try and gain unauthorized access to the meeting by manually joining via the displayed ID.

Useful Online Resources:

How to Keep Uninvited Guests Out of Your Zoom Event

https://blog.zoom.us/wordpress/2020/03/20/keep-uninvited-guests-out-of-your-zoom-event/?_ga=2.183747748.30273182.1586402351-900247869.1581261335

Best Practices for Securing Your Virtual Classroom

https://blog.zoom.us/wordpress/2020/03/27/best-practices-for-securing-your-virtual-classroom/?_ga=2.183747748.30273182.1586402351-900247869.1581261335

Privacy & Security for Zoom Video Communications

<https://zoom.us/docs/en-us/privacy-and-security.html>