

Securing Zoom Meetings

Tactics for handling uninvited automated meeting tools, dial-in, and third-party room system participants



zoom

Last Updated December 4, 2023

Table of Contents

Securing Zoom Meetings Overview

Zoom empowers users and admins to use automated meeting tools in a secure and effective manner

Automated meeting tools can enhance your experience during a Zoom session

Zoom provides security and approval measures for automated meeting tools

Automated meeting tool installation and in-meeting functionality

Zoom provides administrative settings for the management of automated meeting tools used on your account

Zoom App Marketplace for application analytics and management

Automated meeting tools can be pre-approved by administrators

Using the Active Apps Notifier Report

Administrators can configure their Zoom account according to their organization's policy on automated meeting tools

Manage the automated meeting tools, dial-in users, and third-party room devices in your Zoom Meetings with these features

Enabling Waiting Room

Enable the "Identifying guests in the meeting/webinar" setting to view external users who have joined your meeting

Use the in-meeting Active Apps Notifier

Prevent uninvited automated meeting tools, dial-in users, and third-party room devices with these account settings

Enabling Waiting Room when scheduling meetings

Meeting passcodes

Automatically generated meeting IDs

Requiring authentication

Image watermarks

Only allow local recording requests to come from meeting participants who are on your Zoom account

Audio watermarks

Select Computer Audio as the meeting Audio Type to stop dial-in participants

Block dial-in users when Waiting Room is disabled

Use end-to-end encryption (E2EE) to require that participants join your meeting from the Zoom desktop client or mobile app, or a Zoom Room

Enable CAPTCHA on your Zoom account

Use Zoom Events or Zoom Webinars for public virtual events

Meeting hosts can invoke additional security measures during a meeting

Locking your meeting

Suspending participant activities

Remove uninvited or disruptive participants

[Report a meeting participant for inappropriate behavior](#)

[Use Zoom's in-meeting features to manage automated meeting tools](#)

Securing Zoom Meetings Overview

Zoom Meetings are best experienced through the native Zoom desktop client, mobile app, or a Zoom Room, but you can also join from the web, as a dial-in user (by calling into the meeting by

phone), or via third-party room devices (Zoom's Conference Room Connector allows SIP/H.323-based video conferencing devices) to attend a Zoom meeting.

Additionally, the Zoom App Marketplace is your resource to access and download applications and integrations that can enhance your meeting or event experience. Among those applications are bots, which, along with certain integrations and third-party services, constitute automated meeting tools. Some automated meeting tools utilize Zoom's Meeting software developer kit (SDK) to attend meetings and access meeting audio and video content on behalf of the meeting participants that manage them.

While automated meeting tools are intended to extend and enhance the Zoom Meetings experience, their presence may lead to unwanted data access through the recording of in-meeting real-time video, audio, screen or whiteboard sharing, chat, or files shared in the meeting. This document provides an overview of the available settings and in-meeting features you can use to secure Zoom Meetings against such uninvited participants. Many of the following security features have individual user-level controls that empower Zoom users to manage the security of their own meetings, but you will also find several administrator-level configurations that owners and admins can use to make meetings more secure for your entire account.

Zoom empowers users and admins to use automated meeting tools in a secure and effective manner

Automated meeting tools can enhance your experience during a Zoom session and improve workflows

Automated meeting tools (applications—including bots, integrations, and third-party services) are helpful tools that can enhance the Zoom session experience and assist users with several tasks, such as meeting notation, summarization, transcription, and recording. Enterprise professionals may use automated meeting tools to record their collaboration sessions for coaching purposes, and educators and students may use them to summarize lectures to be revisited during study sessions. Automated meeting tools can be downloaded at marketplace.zoom.us or from the Apps icon found in the Zoom client. Your developers can also create unpublished or internal automated meeting tools to serve specific functions within your organization.

Zoom provides security and approval measures for automated meeting tools that are published in the Zoom App Marketplace

All automated meeting tools that utilize the Zoom Meeting SDK must comply with the [Zoom SDK App Requirements](#) so they trigger the appropriate notifications when meeting content is being accessed.

All automated meeting tools that are intended to be published to the Zoom App Marketplace undergo a dedicated [review process](#) that evaluates whether they are safe and effective tools suitable for public use. Once an automated meeting tool is submitted, the App Marketplace team reviews and either approves it or provides feedback to the developer on any remediation work required for it to be approved.

The review process' primary goals are to:

- Confirm that the automated meeting tool is ready for use by end users.
- Confirm that the automated meeting tool follows best practices for privacy and security to reduce risks to users.

Note

[Private-use and beta automated meeting tools](#) that are not published to the Zoom App Marketplace do not require review.

Warning

As of July 16, 2023, all newly submitted automated meeting tools must be approved by the App Marketplace team to join meetings that are hosted by other Zoom accounts. Automated meeting tools that are not approved by the App Marketplace team will only be able to join meetings that are hosted by the account in which they were developed after this date.

Zoom publishes best practices for developers to use when building automated meeting tools

Zoom's [developer website](#) is your guide to building, designing, and testing new automated meeting tools. The site contains best practice information, including how to use Zoom's [Meeting software developer kit \(SDK\)](#) to build [meeting bots](#). There are also reference implementations available for [Meeting SDK for Windows](#) or the [Meeting SDK for Web](#).

Privacy policies and support resources for automated meeting tools are published on the Zoom App Marketplace

Navigate to the **Developer resources** section for each application, integration, or service available in [App Marketplace](#) to view its privacy policy and other support resources.

Automated meeting tools join and record meetings when initiated by the user who manages them

Automated meeting tools are managed by the user who downloads them, and it is at that user's direction that the automated meeting tool joins a meeting and records content on their behalf.

Automated meeting tools can be manually initiated after a meeting has started

You can manually initiate an automated meeting tool and have it join an active meeting by clicking the Apps menu found in the Zoom client or through the automated meeting tool's respective web interface. The automated meeting tool will join the meeting, start recording the specific content for which it was designed, and be listed in the Active Apps Notifier. The automated meeting tool will also trigger a recording notification, informing all attendees of its presence and function in the meeting.

Some automated meeting tools can join meetings automatically when synced with a user's calendar

Many automated meeting tools can be synchronized with a user's calendar and their Zoom account. This allows the tool to access calendar invites that may include a Zoom Meeting invitation and automatically join those meetings if instructed by its user. You can enable or disable an automated meeting tool's ability to automatically join meetings on your calendar.

Note

Automated meeting tools that have access to your calendar events will automatically reference the unique or personal meeting ID and passcode for each calendar event containing a Zoom Meeting invitation and use that information to automatically join the meeting.

Zoom Recommendation

Review your upcoming meetings to confirm whether it is appropriate for your automated meeting tool to join any meeting automatically. Disable the tool from auto-joining a scheduled meeting if the meeting content should not be recorded.

Automated meeting tools appear as participants once they join a meeting

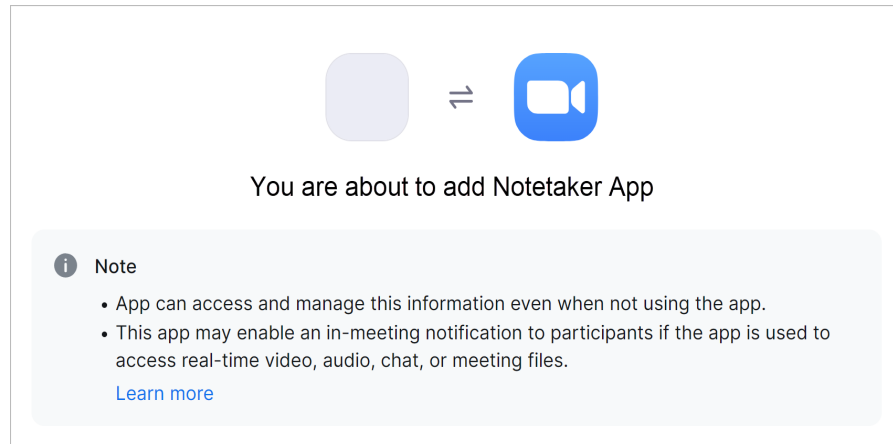
Automated meeting tools commonly join meetings as participants and appear in a manner similar to the people attending the meeting. This means they have their own video thumbnail that appears next to the other meeting participants and is clearly labeled with the name of the user who initiated it and its function (e.g., "Steve Miller's notetaking app"). While in a meeting, the Participants list and the Waiting Room feature (when enabled) will list any automated meeting tools along with all other users, allowing hosts and participants to identify and manage automated meeting tools within their meetings.

Automated meeting tools can access certain in-meeting content

Automated meeting tools are developed to access certain in-meeting content such as real-time video, audio, screen or whiteboard sharing, chat, or files shared in the meeting, which are then used to improve workflows like meeting summarization, transcription, or other functions.

During installation, an authorization prompt will inform users of the specific meeting data the automated meeting tool will access

The authorization prompt explains what types of media and data the automated meeting tool will access during a meeting. This prompt will also describe the types of user data the tool will access, which may include profile information, calendar synchronization, or account settings.



Some automated meeting tools have a local recording function that will access camera video and microphone audio outside of meetings when initiated by the user who manages the tool

A user may initiate an automated meeting tool with a local recording function which accesses camera video and microphone audio *outside of meetings*. This function can be invoked from the tool's web interface. When using the local recording function, these tools will use a local recording of the user's audio and video but do not join meetings. This local recording function can only be initiated by the user who manages the tool, and it will not access microphone audio, camera video, screen sharing, or other content without the user's initiation.

Zoom provides administrative settings for the management of automated meeting tools used on your account

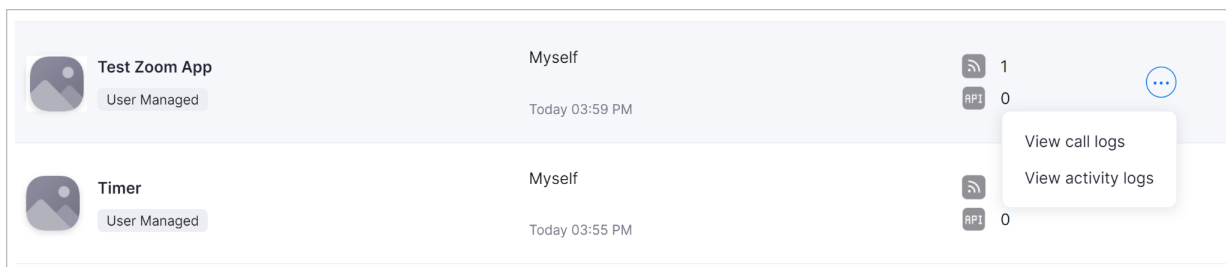
Administrators can access the Zoom App Marketplace for application analytics and management

Account administrators have visibility into what automated meeting tools are installed and how they're utilized by their account users through the analytics provided in the App Marketplace. Admins can see an activity log for each automated meeting tool, including:*

- which users are pre-approved to use the tool
- when a tool was pre-approved
- which users installed the tool and when
- which users have uninstalled the tool and when
- API calls made by users on the account

*This is a non-exhaustive list

Log in to marketplace.zoom.us as an administrator. Click **Manage** in the upper right corner of the screen and then click **Apps on Account** within the Admin App Management menu to see the list of automated meeting tools added to your organization's account. Logs and management options for each tool can be accessed here:



Automated meeting tools can be pre-approved by administrators of multi-user Zoom accounts

Administrators of multi-user managed accounts have the ability to [pre-approve](#) or restrict certain automated meeting tools. Your account type may impact whether or not admin pre-approval is required. The ability to use certain tools may or may not be automatically enabled and visible in the meeting client depending on your account type, as well.

Log in to marketplace.zoom.us as an administrator and click **Manage** in the upper right corner of the screen, then go to the **Admin App Management** section of the menu. Click **Permissions** to manage the approval of automated meeting tools. Click **Notifications** to manage how your admins are notified of requests, and also manage how users are notified of approvals.

Note

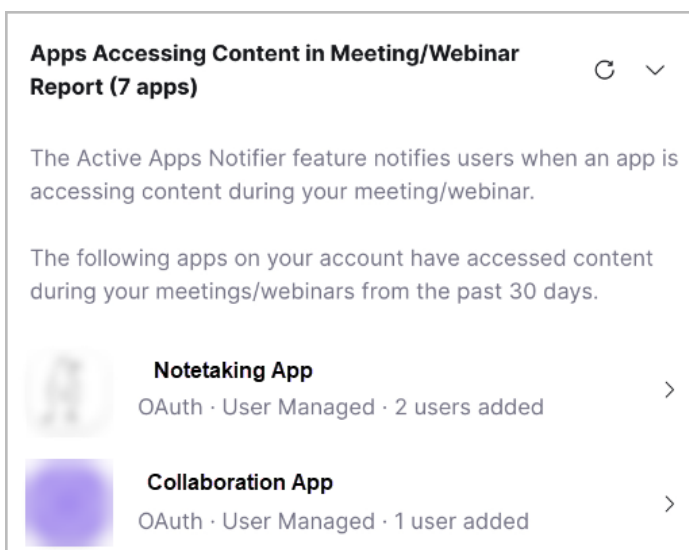
Prohibiting the use of an automated meeting tool will stop it from being used on your account but will not stop external users' uninvited automated meetings tool from potentially joining meetings hosted by users on your account. Enabling the Waiting Room, implementing CAPTCHA, and other features can help prevent uninvited tools from joining meetings, as discussed further below.

Administrators can use the Active Apps Notifier Report to view analytics regarding automated meeting tool usage on an account

The [Active App Notifier Report](#) allows admins to see and manage the automated meeting tools that have accessed all account users' meeting content during the past 30 days. This gives admins the opportunity to make informed decisions about whether they want to approve the use of these tools in their meetings and webinars. Admins can also use the report to easily view the [App Marketplace](#) page for each active tool to learn more about it and disable it if needed.

To view the Active App Notifier Report, log in to marketplace.zoom.us as an administrator. Click **Manage** in the upper right corner of the screen and then click **Apps on Account** within the Admin App Management menu to see a list of automated meeting tools added to your organization's account.

The Active Apps Notifier Report will appear in the lower-right corner of the screen and will list the tools that have accessed meeting or webinar content on your account in the past 30 days.



Apps Accessing Content in Meeting/Webinar Report (7 apps)

The Active Apps Notifier feature notifies users when an app is accessing content during your meeting/webinar.

The following apps on your account have accessed content during your meetings/webinars from the past 30 days.

- Notetaking App**
OAuth · User Managed · 2 users added
- Collaboration App**
OAuth · User Managed · 1 user added

Administrators can configure their Zoom account according to their organization's policy on automated meeting tools

There are several [administrative settings](#) shared later in this document that can be enabled on your account to manage automated meeting tools, along with dial-in users or third-party room devices. These account-level settings help to ensure that the automated meeting tools joining your meetings are authorized according to your organization's meeting security policy.

Zoom Recommendation

Establish an automated meeting tools policy within your organization that outlines how they may or may not be utilized on your account. Specify which tools are approved for use and configure your account settings according to your organization's best practices.

Manage the automated meeting tools, dial-in users, and third-party room devices in your Zoom Meetings with these features

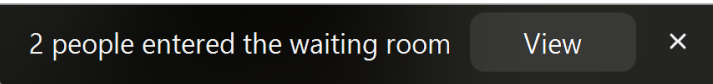
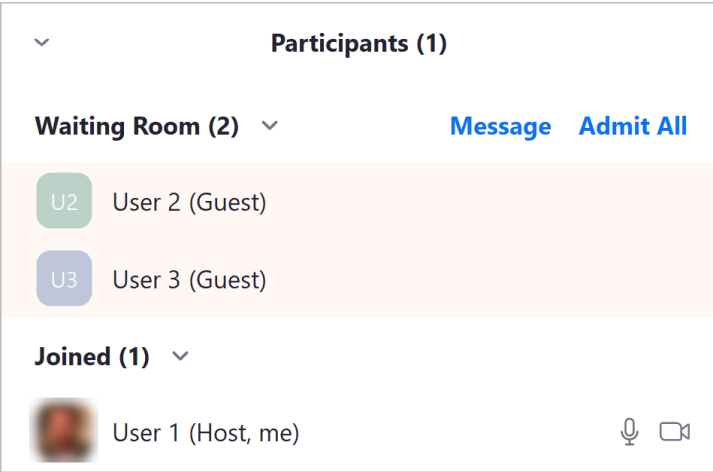
The following security features allow meeting hosts to view and manage the participants who have joined or are attempting to join a meeting. These participants may be joining as automated meeting tools or dial-in users, or via third-party room devices, Zoom Rooms, or the Zoom client. Automated meeting tools join as participants and will also be visible in the following security features.

Enable Waiting Room to view and manage all participants that attempt to join your meeting

[Waiting Room](#) is a virtual staging area that stops participants from joining a meeting until you, the meeting host, are ready to start the meeting. Waiting Room is an effective way to screen who is trying to enter your meeting and keep uninvited automated meeting tools, dial-in users, or third-party room systems out. Uninvited participants can be identified in the Waiting Room and removed before they join the meeting.

The Waiting Room can be viewed by clicking the **Participants** icon while in a Zoom Meeting. This list will show which participants are in the Waiting Room and which participants have been admitted to the meeting. The host or co-host(s) can admit users one by one or click **Admit All** to allow all users in the Waiting Room into the meeting. If the host identifies an uninvited participant in the Waiting Room, they can remove and block them from trying to re-enter the Waiting Room.

While in a meeting with Waiting Room enabled, hosts will receive an on-screen notification banner when new participants have entered the Waiting Room.



Note

If Waiting Room is enabled in your meeting settings, the **Join before host** setting will only work for participants that you have configured to bypass the Waiting Room.

Allow users on your Zoom account or with specified domains to bypass the Waiting Room

You can configure your [Waiting Room Options](#) in the Zoom web portal to allow users from your account to bypass the Waiting Room. Entire domains can also be specified, which allows participants from these specified domains to bypass the Waiting Room, as well. By allowing users from trusted accounts and domains directly into the meeting, the host will have a smaller number of participants in the Waiting Room to review and admit.

Allow approved third-party room devices to bypass the Waiting Room

Approved third-party room devices (SIP/H.323-based video conferencing systems) can also be pre-approved to bypass the Waiting Room. This setting is found in the **Waiting Room Options** section of the web portal. The list of [approved third-party room devices](#) within your account will bypass the Waiting Room when the **Approved SIP/H.323 Devices** checkbox is selected in the Waiting Room Options section.

The following pre-approval options allow third-party room devices to bypass the Waiting Room:

- **SIP/H.323 Rooms managed by Zoom Connector**
Managed devices will be pre-approved to bypass the Waiting Room.
- **SIP/H.323 devices by IP address**
Devices using the specified IP addresses, or addresses within the specified range, will be pre-approved when joining the Waiting Room.
- **SIP/H.323 devices with specific public certificates**
This allows the uploading of a certificate that will be used to verify if a device has been pre-approved.

Customize the look and message of the Waiting Room on your paid Zoom plan

Users on paid Zoom plans can log in to the Zoom web portal and [customize](#) the message and title of their Waiting Room. This area is a great spot to post rules, guidelines, or an agenda for your meeting. You can also add a logo, image, or video (within size limitations). These customizations

help participants know that they are in the right meeting and what to expect for the session once they are admitted.

Enable Waiting Room at any time

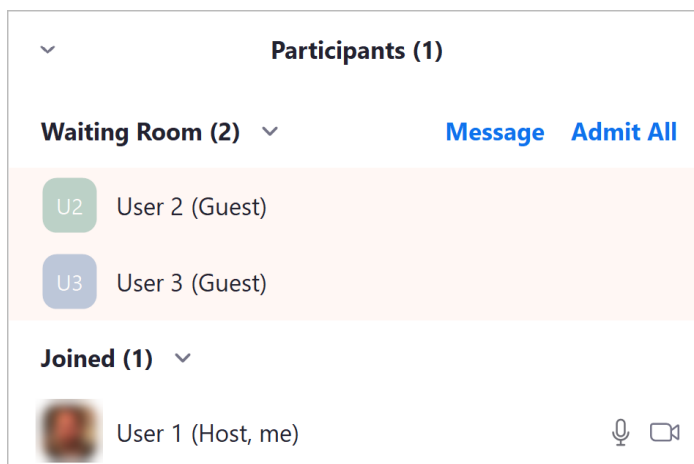
Waiting Room can be [enabled proactively](#) for an entire account or group by an administrator or account owner. Meeting hosts can choose to enable Waiting Room while scheduling individual meetings or enable it proactively within their personal settings in the Zoom web portal. Waiting Room can also be enabled during a live meeting to allow hosts to remove disruptive participants, which could include uninvited automated meeting tools, from the meeting.

Enable the “Identifying guests in the meeting/webinar” setting to view external users that have joined your meeting

The [Identifying guests in the meeting/webinar](#) setting allows you and participants who are users on your account to see that a guest is participating in a meeting or webinar. A guest is identified as someone who either is not signed in to a Zoom account or is signed in with an email address that is not on the same account as the host. Uninvited automated meeting tools, dial-in users, or third-party room devices will be listed as guests with this setting enabled.

Meeting guests will be identified with descriptive text in both the Waiting Room (if enabled) and the Participants list for the active meeting.

The **Identifying guests in the meeting/webinar** setting can be enabled by administrators at an account and group level, and also in individual user settings.




Use the in-meeting Active Apps Notifier to see when an automated meeting tool is active and accessing content during a meeting

[Active Apps Notifier](#) is an in-meeting notification that informs users when a host or other participant is using an automated meeting tool that is accessing meeting or webinar content, such as real-time video, audio, screen or whiteboard sharing, chat, or files shared in the meeting. These

notifications are designed to empower users to know that participants are sharing content with third-party apps and make informed decisions about if and how they participate in a Zoom session.

Use the Active Apps Notifier to view any automated meeting tools participating in your meeting

The Active Apps Notifier icon  will appear in the top-left corner of the meeting window when an automated meeting tool begins accessing meeting or webinar content.

A user can click the icon to show a list of automated meeting tools that are accessing content during that session, along with what type of content they have access to and which users are using them.

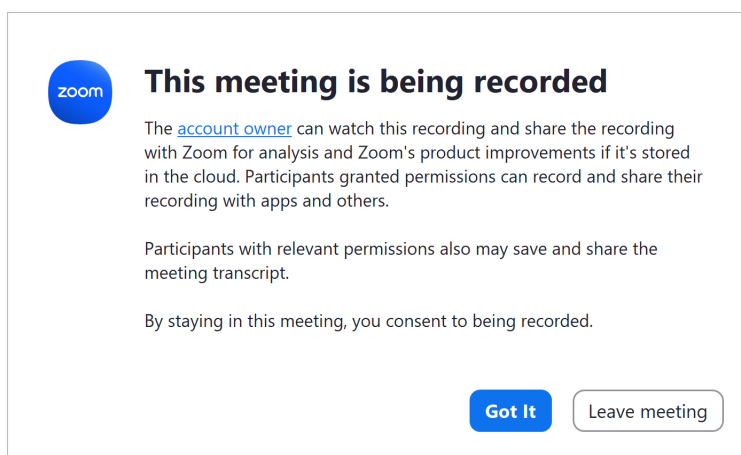
The meeting host may allow the automated meeting tool to stay in the meeting, or the host may remove and/or report it if the automated meeting tool is uninvited.



Review recording notifications to decide if you wish to participate in content sharing

In addition to the Active Apps Notifier, automated meeting tools will trigger a recording notification when they join a meeting and initiate content recording.

This is a prompt for meeting participants to consent to the use of the app or leave the meeting if they decline to consent.




Prevent uninvited automated meeting tools, dial-in users, and third-party room devices with these account settings

Users and admins can use the following settings to prevent uninvited automated meeting tools, dial-in users, and third-party room systems from joining Zoom Meetings.

Enable Waiting Room when scheduling meetings or for your entire account to proactively secure your meetings

[Waiting Room](#) is a virtual staging area that stops participants from joining a meeting until the meeting host admits them. Waiting Room has several [configurations described earlier](#) in this document that can be enabled on multiple levels within your Zoom account, ensuring that Waiting Room is active for all meetings or for specific users.

The following Waiting Room settings can be enabled by individual users in their personal settings, as well as at the group and account levels by administrators and owners:

Waiting Room 

When participants join a meeting, place them in a waiting room and require the host to admit them individually. Enabling the waiting room automatically disables the setting for allowing participants to join before host.

Waiting Room Options

The options you select here apply to meetings hosted by users who turned 'Waiting Room' on

- ✓ Everyone will go in the waiting room
- ✓ People in the waiting room are sorted by join order

[Edit Options](#) [Customize Waiting Room](#)

Users can also choose to enable Waiting Room while scheduling individual meetings:

Security

Passcode
Only users who have the invite link or passcode can join the meeting


Waiting Room
Only users admitted by the host can join the meeting

Require authentication to join


Use a meeting passcode to require all participants to enter a numeric code to gain access to a meeting


Requiring a [meeting passcode](#) is an integral security measure to help prevent uninvited participants from attempting to join meetings.

These settings can be enabled by individual users, or at the group and account levels by admins and owners:

Require a passcode when scheduling new meetings 

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

Require a passcode for meetings which have already been scheduled 

Passcode for already scheduled meetings 


Account owners and admins can lock settings to require passcodes for all meetings on their account and configure minimum passcode requirements.

Use automatically generated meeting IDs to create unique, single-use meeting IDs

Automatically generated meeting IDs are unique, randomly generated meeting ID numbers that temporarily expire after a meeting ends. This will prevent users from returning to existing meeting IDs and potentially misusing them. An automatically generated meeting ID number will not be reused for thirty days after a meeting has ended. If a meeting with an automatically generated ID number is restarted by the host, the thirty-day blackout period for that ID number will restart.

Select the **Generate Automatically** option under the Meeting ID section while scheduling a meeting from the Zoom desktop client, mobile app, or web portal.

Meeting ID

Generate Automatically 

Generate Automatically

Personal Meeting ID

Note

Automated meeting tools that have access to your calendar or Zoom account will automatically reference the unique or personal meeting ID and passcode for each calendar event containing a Zoom Meeting invitation and use that information to automatically join the meeting.

Limit the use of your Personal Meeting ID to meetings with known, trusted, and internal users

Your Personal Meeting Room is a virtual meeting room permanently reserved for you that you can access with your Personal Meeting ID (PMI) or personal link, if applicable. You can start instant meetings with your PMI, or you can schedule a meeting that uses your PMI.

Warning

Your Personal Meeting ID (PMI) is ideal for use with people you know and meet with regularly. Because it is always accessible with the same Meeting ID and personal link, your PMI should not be used for back-to-back meetings or with unknown people outside of your organization. Limiting the use of your PMI to interactions with trusted users will help keep it from being distributed for potential misuse.

The following PMI settings can be enabled by individual users in their personal settings, as well as at the group and account levels by administrators and owners:

Enable Personal Meeting ID

A Personal Meeting ID (PMI) is a 9 to 11 digit number that is assigned to your account. You can visit [Personal Meeting Room](#) to change your personal meeting settings. [Learn more](#)

Require authentication to allow only users logged in to Zoom or from your domain to join meetings

The [Only authenticated meeting participants and webinar attendees can join meetings and webinars](#) option requires participants to sign in to Zoom before they can join a Zoom Meeting or Webinar once enabled. Hosts can further restrict meeting participants and webinar attendees to Zoom users whose email addresses match a certain domain. This can be useful if you want to restrict your participant list to verified users or users from a specific organization. These settings can be enabled by individual users, or at the group and account levels by admins and owners:

Only authenticated meeting participants and webinar attendees can join meetings and webinars

Meeting participants and webinar attendees will need to authenticate prior to joining a session. Hosts can choose one of the options below when scheduling meetings or webinars. [Learn more](#)

Meetings & Webinar Authentication Options:

Sign in to Zoom (Default)

[Edit](#) [Hide in the Selection](#)

Sign in to Zoom with specified domain

[Edit](#) [Hide in the Selection](#)

Allow authentication exception [?](#)

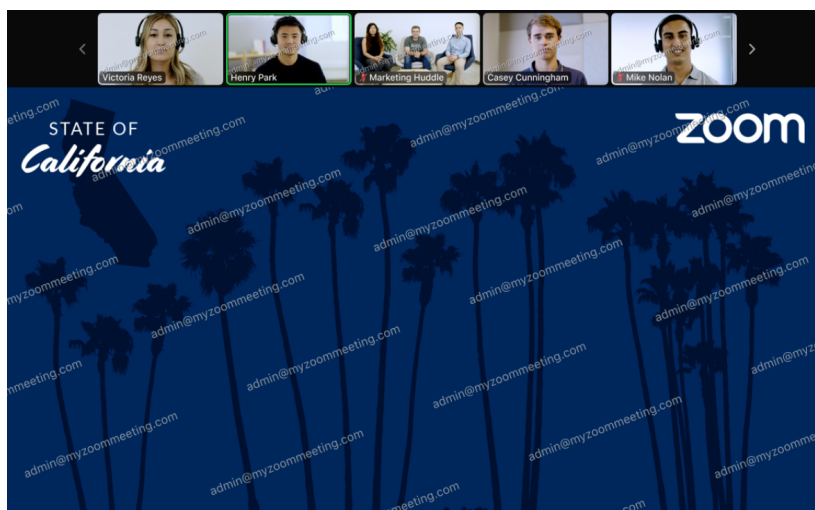
Note

If authentication is required, participants without a Zoom account will not be able to join the meeting or webinar.

Use image watermarks to help identify the source of any video content captured during a meeting

The [image watermark](#) feature superimposes an image consisting of the viewing participant's email address onto the shared content and over their video in most video layouts (Speaker, Gallery, Side-by-side). You can also display several instances of the watermark so that it's more visibly apparent across the video or shared screen. This feature can help deter the unintended capture of content shared during meetings.

When a participant shares their screen during a meeting or webinar, the email of the user who is viewing the content will be patterned across the shared content, as well as on the video of the other visible participants. For example, if `admin@myzoommeeting.com` is viewing shared content, the watermark of `admin@myzoommeeting.com` will be patterned across the shared content and the videos of the participants as shown in this image.



Note

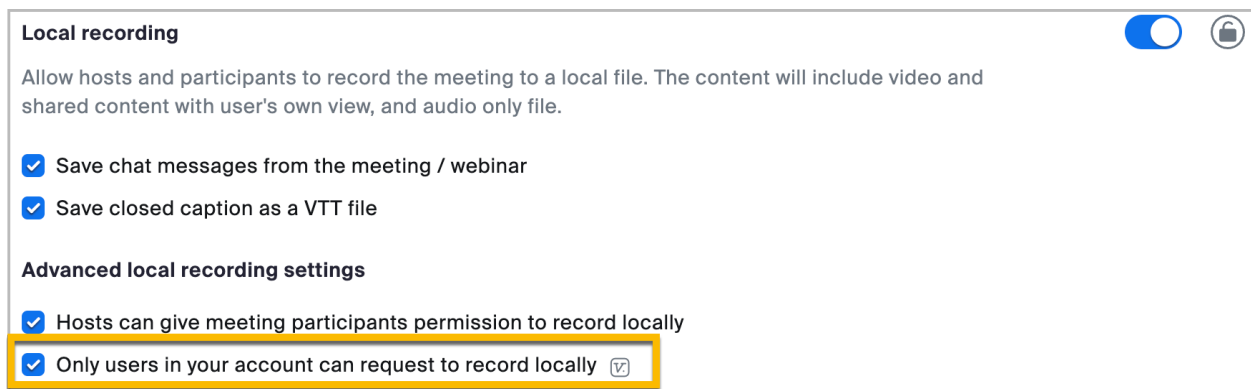
The [Only authenticated meeting participants and webinar attendees can join meetings and webinars](#) setting must be enabled to use video watermarks.

The image watermark setting is only available when scheduling meetings through the Zoom web portal. Other scheduling methods, such as the Zoom desktop client or the Microsoft Outlook plugin or add-in, do not support the availability of the image watermark settings.

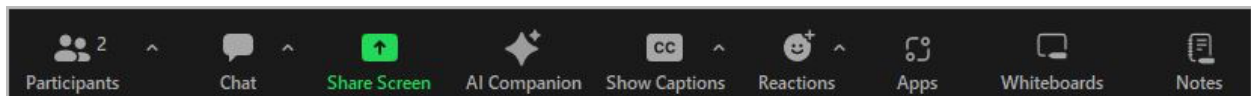
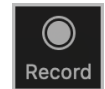
Only allow local recording requests to come from meeting participants who are on your Zoom account

During Zoom Meetings, participants and automated meeting tools may request the ability to start a local recording that will be stored on the computer of the participant making the request. The meeting host can grant or deny any local recording requests sent to them.

The **Only users in your account can request to record locally** setting helps to ensure that any requests to start a local recording during an active Zoom Meeting are being made by participants or automated meeting tools from within the same Zoom account as the meeting host. This setting can be enabled at the account level and group level by the account owner or administrators.



When this setting is enabled, the record button will be removed from the participant control menu for external participants who have joined the Zoom Meeting.



Enable audio watermark to help identify the source of any audio content captured during a meeting

[Audio watermark](#), or audio signature, embeds a user's personal information in the received audio as an inaudible watermark. This means that if someone records the meeting with either a separate microphone or a third-party tool and shares the audio file without permission, Zoom can assist with determining which participant was responsible. The audio watermark feature can only be enabled by account owners and administrators through the Account Management settings.

Note

The [Only authenticated meeting participants and webinar attendees can join meetings and webinars](#) setting must be enabled to use audio watermark.

Select Computer Audio as the meeting Audio Type within account settings or while scheduling meetings to disable all telephone dial-in options

By selecting Computer Audio as your desired audio type for Zoom Meetings, you can disable all meeting participants' ability to dial in by telephone/PSTN. This may be an effective option if your organization does not use telephone or third-party audio to join meetings and would like to block any uninvited participants from trying to dial in.

Audio Type can be selected by individual users, or at the group and account levels by admins and owners:

Audio Type

Determine how participants can join the audio portion of the meeting. When joining audio, you can let them choose to use their computer microphone/speaker or use a telephone. You can also limit them to just one of those audio types. If you have 3rd party audio enabled, you can require that all participants follow the instructions you provide for using non-Zoom audio.

- Telephone and Computer Audio
- Telephone
- Computer Audio
- 3rd Party Audio

Zoom Recommendation

Confirm that your organization or external meeting participants are relying on something other than telephone/PSTN dial-in options to join your meetings before selecting **Computer Audio** as your preferred audio type.

Block dial-in users when Waiting Room is disabled

Meeting hosts who are not using Waiting Room can block dial-in users who intend to call in to a meeting by selecting the following setting within the Zoom web portal. This setting is in the meeting security section and can be enabled by individual users, or at the group and account levels by admins and owners:

If Waiting Room is enabled, phone-only users will be placed in the Waiting Room.

If Waiting Room is not enabled, phone dial-in only users will:

- Be allowed to join the meeting
- Be blocked from joining the meeting

Note

This setting will only block dial-in users when Waiting Room is *not* enabled.

Use end-to-end encryption (E2EE) to require that participants join your meeting from the Zoom desktop client or mobile app, or a Zoom Room

[End-to-end encryption](#) (E2EE) for meetings provides additional protection when needed and requires all meeting participants to join from the Zoom desktop client or mobile app, or a Zoom Room.

This setting is in the meeting security section of the Zoom web portal and can be enabled by individual users, or at the group and account levels by admins and owners:

Allow use of end-to-end encryption



Choose between enhanced encryption (encryption keys stored in the cloud) and end-to-end encryption (encryption keys stored on your local device) when scheduling or starting a meeting. When using end-to-end encryption, several features (e.g. cloud recording, phone/SIP/H.323 dial-in) will be automatically disabled. [Learn more](#)

Note

Users will not be able to use any of the following technologies to join meetings when end-to-end encryption is enabled:

- Telephone/PSTN
- Third-party SIP/H.323 devices
- On-premise configurations (Zoom Meeting Connector and Virtual Connector)
- Zoom web client
- Third-party clients leveraging the Zoom Web SDK
- Microsoft Lync/Skype clients

Enable CAPTCHA on your Zoom account to help prevent uninvited automated meeting tools from joining meetings from the Zoom website

Users can join a Zoom Meeting without [a Zoom account](#) or from the web if they are unable to download the Zoom desktop client or mobile app. These participants can join as a guest by navigating to [zoom.us](#) and clicking **Join** and then **Join by Meeting ID**. The meeting guest can then enter the meeting ID and passcode (if applicable) to join the meeting.

Some users may also join or start meetings via their web browser by entering these URLs:

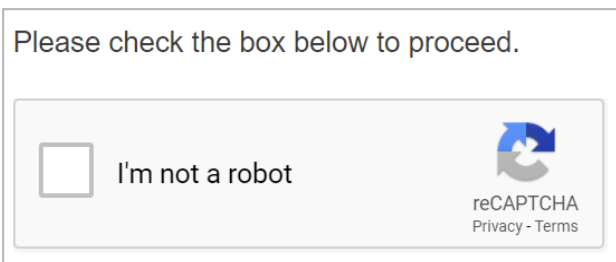
- <https://zoom.us/jc/join/meetingID>
- <https://zoom.us/jc/meetingID/start>

CAPTCHA helps prevent uninvited automated meeting tools from joining meetings from the web by challenging unauthenticated users before they can enter

Account admins can require CAPTCHA security checks to suppress uninvited automated meeting tools from joining meetings and webinars through the web client. The CAPTCHA security check will only be displayed to users who join and are not signed in to Zoom. Users who are signed in will not see the CAPTCHA screen during the join process.

When CAPTCHA is active on a Zoom account, unauthenticated or guest users joining from the web must solve the CAPTCHA before they can join a meeting.

Human users will be able to follow and execute the CAPTCHA prompt, while unauthenticated automated meeting tools typically will not be able to execute the prompt and thus will not be able to join the meeting.



Note


The CAPTCHA prompt only applies to individuals who are not signed in to Zoom when joining a meeting or webinar. Authenticated clients and automated meeting tools will not see the CAPTCHA.

Warning

Enabling CAPTCHA on your Zoom account may block some authorized automated meeting tools that attempt to join as unauthenticated guests through the web.

CAPTCHA must be enabled on your Zoom account


The CAPTCHA setting checkbox is in the **In Meeting (Advanced)** section of the web portal and can be enabled by individual users, or at the group and account levels by admins and owners.

Show a "Join from your browser" link 

Allow participants to bypass the Zoom application download process, and join a meeting directly from their browser. This is a workaround for participants who are unable to download, install, or run applications. Note that the meeting experience from the browser is limited

- On desktop browser
- On mobile browser

Note that the meeting experience from the mobile browser is more limited than the desktop browser

- Require solving a CAPTCHA for guest users (users who are not signed in) 

Use Zoom Events or Zoom Webinars for public virtual events for more secure sessions when inviting unknown participants

Zoom Meetings is a powerful tool for collaboration among your peers and Zoom users that you know and trust. However, if you intend to hold a public event with unknown participants, please consider using [Zoom Webinars](#) or [Zoom Events](#).

Zoom has a robust set of security features designed to help hosts manage and safeguard their event experience. A Zoom Webinar or Event host may choose to manually approve or decline anyone who registers. Hosts can also remove an attendee or lock a webinar or event to prevent additional attendees from joining once the webinar or event has started. In addition, webinar and event hosts can choose to require passcodes or authentication for an added layer of security.

Meeting hosts can invoke additional security measures during a meeting

There are multiple [in-meeting security features](#) that can be used if an uninvited automated meeting tool, dial-in user, or third-party room device joins your meeting. See the following options for managing, removing, and reporting uninvited meeting participants.

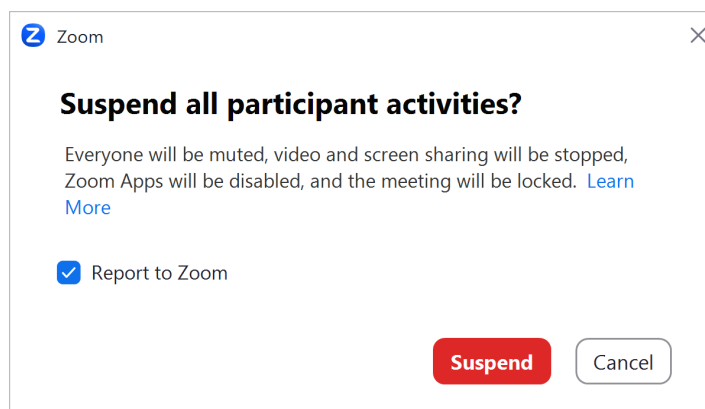
Lock your meeting to prevent uninvited automated meeting tools, dial-in users, or third-party room devices from joining after all invited participants are present

When a Zoom meeting is locked, no new participants can join, even if they have the meeting ID and passcode. To lock a meeting, click the **Security** icon at the bottom of your Zoom window and click the **Lock Meeting** option. The meeting can also be unlocked if new participants need to be added.

Suspend participant activities if your meeting is being disrupted or an uninvited participant or automated meeting tool joins

By suspending participant activities in a meeting, hosts can stop meeting activity and take action regarding any uninvited or disruptive participants that have joined. This may include managing or removing uninvited automated meeting tools, dial-in users, or third-party room devices.

During your meeting, click the **Security** icon and select **Suspend Participant Activities** to temporarily halt all in-meeting video, audio, screen or whiteboard sharing, chat, access to files shared in the meeting, and recording, and close any active Breakout Rooms. This prompt gives you the option to report the issue to Zoom's Trust & Safety team and confirm your choice to suspend activity.

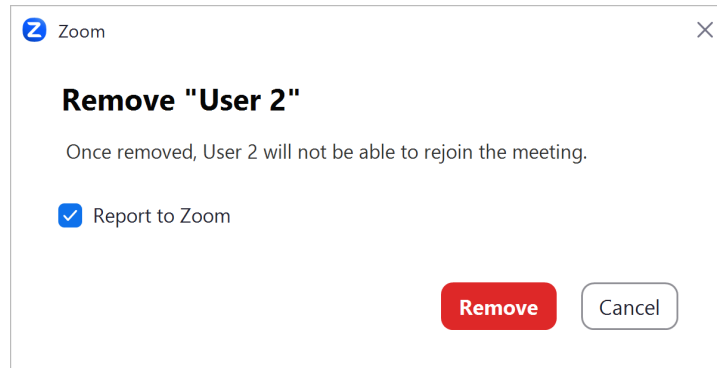


You can resume the meeting by re-enabling the suspended features individually from the Security menu.

Remove uninvited or disruptive participants from your meeting

A host can remove disruptive or uninvited participants or automated meeting tools from their meeting.


This can be done by clicking the **Security** icon in the Zoom Meeting window and then clicking **Remove Participant**. You can then select the participant to be removed from the meeting. You can also report the user to Zoom's Trust & Safety team. The removed participant cannot rejoin the meeting.



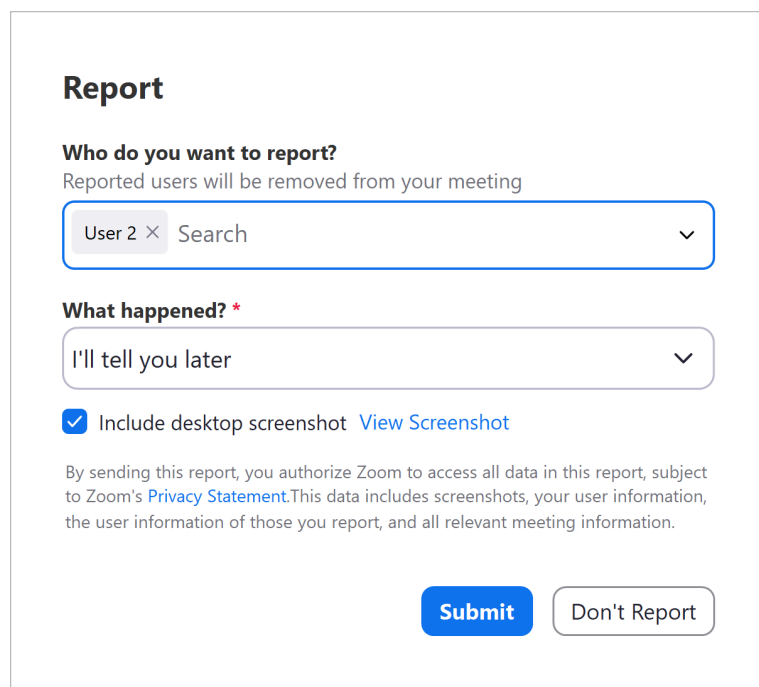
The screenshot shows a Zoom dialog box titled "Remove 'User 2'". It contains the text "Once removed, User 2 will not be able to rejoin the meeting." and a checked checkbox labeled "Report to Zoom". At the bottom right, there are two buttons: a red "Remove" button and a white "Cancel" button.

Report a meeting participant for inappropriate behavior

You can also [report participants for inappropriate behavior](#) during meetings. This may include uninvited automated meeting tools, dial-in users, third-party room devices, or users joining from the Zoom meeting client or mobile app, or a Zoom Room.

Report a meeting participant engaging in inappropriate behavior by clicking the blue menu button  in the upper right corner of the participant's video thumbnail and then clicking **Report...** in the menu.

You can include a screenshot if necessary and use the dropdown menu to provide a reason why you are reporting the participant. This report is automatically sent to the Zoom Trust & Safety team, which will determine whether any misuse of the platform occurred and block the user if necessary. The user(s) will be removed from your meeting once the report is submitted.



The screenshot shows a "Report" form. It has a title "Report" and a section "Who do you want to report?" with the text "Reported users will be removed from your meeting". Below this is a dropdown menu showing "User 2" with a search icon and a dropdown arrow. The next section is "What happened?*" with a dropdown menu showing "I'll tell you later" and a dropdown arrow. There is a checked checkbox labeled "Include desktop screenshot" with a link "View Screenshot". At the bottom, there is a paragraph of text: "By sending this report, you authorize Zoom to access all data in this report, subject to Zoom's [Privacy Statement](#). This data includes screenshots, your user information, the user information of those you report, and all relevant meeting information." At the bottom right, there are two buttons: a blue "Submit" button and a white "Don't Report" button.

Use Zoom's in-meeting features to manage automated meeting tools if they join your meeting

Hosts and participants can use the following in-meeting tools to see when an automated meeting tool has joined a meeting. This gives users the ability to confirm that the tool has been initiated by one of the meeting attendees. Hosts can also remove and report an automated meeting tool if they are unable to positively identify the participant who manages it or feel that the tool should not be in the meeting or webinar.

Identify automated meeting tools that have joined your meeting

The [Active Apps Notifier](#) is an in-meeting tool that notifies the host and participants that an automated meeting tool has joined a meeting and also indicates what kind of data the tool is accessing. An automated meeting tool can also be identified in the [Participants list](#) and the [Waiting Room](#) (if enabled for the meeting).

Look at the name of the automated meeting tool attending the meeting to confirm that it is owned by one of the meeting participants. Evaluate whether it is appropriate for the tool to record meeting content in that meeting. You can [suspend all participant activity](#) if you are unsure if the automated meeting tool should be in your meeting to help keep your meeting content secure.

Remove automated meeting tools from your meeting

You may wish to [remove](#) an automated meeting tool from a meeting if it is not claimed by a participant or if you do not want the content of that meeting to be recorded. You can also [report](#) the tool if it appears to be uninvited. All reports are delivered to Zoom's [Trust & Safety](#) team for review.