OnceHub Support

Zoom security best practices

Last Modified on Dec 9, 2024

At OnceHub, we designed our native Zoom integration with security at the forefront of our minds. Many of our integration features help you secure your meetings from uninvited guests.

Unique meeting IDs and links for every session

If you're used to offering a static link, break that habit fast and connect our native Zoom integration instead. It may be simpler to use the same customized meeting link to everyone meeting with you, but that opens a huge vulnerability for uninvited guests. Each session needs its own meeting created, with its own meeting ID.

There's no need to waste time signing into Zoom, creating the meeting, and sending a separate email with the conferencing information. When a customer books with you, OnceHub automatically creates a meeting in Zoom and includes all conferencing information in the booking confirmation notification and on the calendar event.

Note: Once you have a unique meeting ID, be sure only to share the conferencing information with those you want to join. Many make the mistake of including a joining link on publicly available posters or websites. This increases the risk of an insecure meeting.

Dynamic passcodes for every session

Some hackers can use technology to guess unique meeting IDs or may take advantage of publicly-posted information. Make sure anyone joining your session also receives a meeting passcode and don't advertise it anywhere except among authorized attendees. This gives an additional measure of security, creating another barrier for uninvited guests.

With OnceHub's native integration, you can ensure each Zoom session requires a dynamic passcode, different for each booking. Our Zoom integration creates the dynamic passcode automatically and adds it to your meetings and all conferencing information provided in notifications.

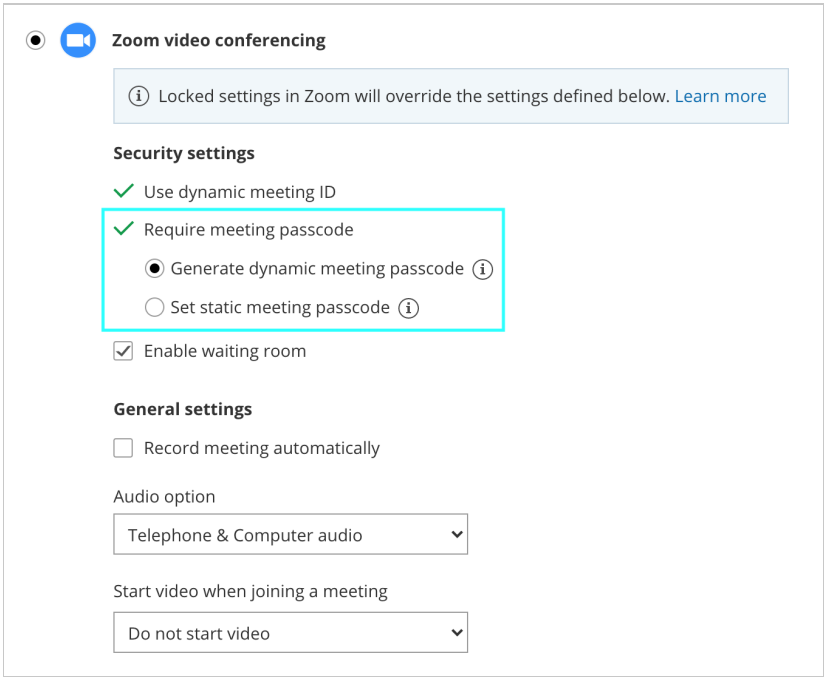

Figure 1: Generate dynamic meeting passcode

Using the waiting room

If you're concerned for uninvited guests, be sure to select the waiting room feature. This allows you to authorize individuals before they're able to access your meeting. Uninvited guests may have guessed your link or passcode, but they still won't be able to join your session without your express permission.

If you have many people joining, we recommend defining an additional co-host to watch the waiting room notifications and grant people access.

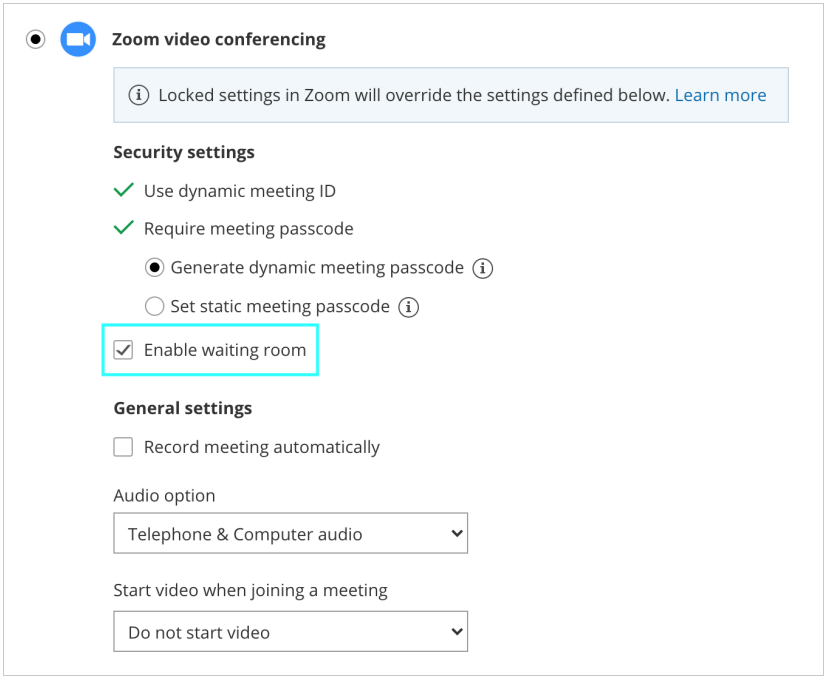

Figure 2: Enable waiting room

Learn more about Zoom's waiting room feature

Starting video for host and/or participants when they join

Depending on your organization, you may prefer everyone use video upon joining, so you can understand who is in your meeting and confirm no one is providing a name that isn't theirs to use.

In this case, you can opt to start video for all participants, or all participants and the host, upon joining the Zoom session.

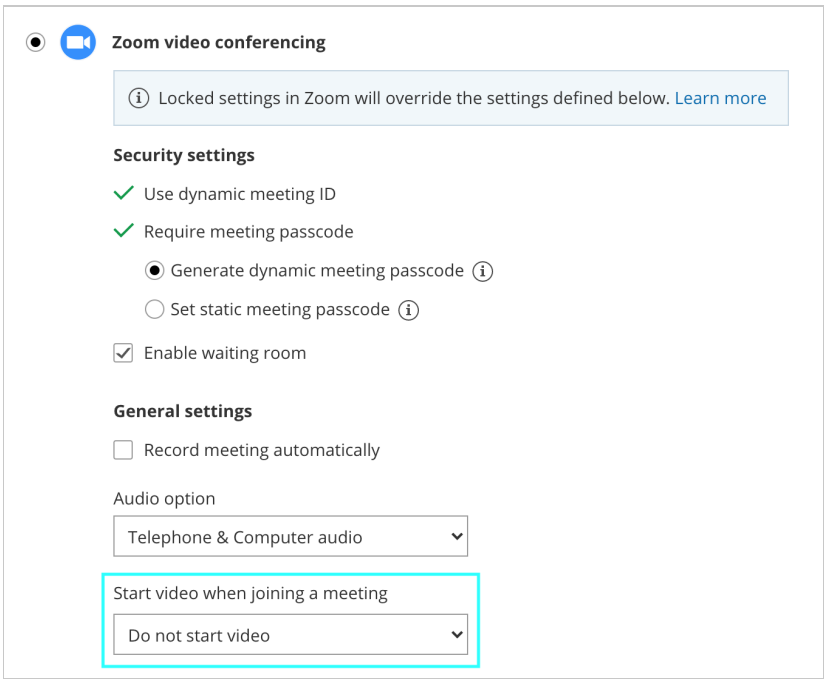

Figure 3: Start video when joining a meeting

Educate your team members before they go live

Be sure not to skip a dry run for each team member giving meetings. That dry run is one of the most important steps helping them maintain professionalism in their video meetings. Especially if they've not used the video conferencing app much, there's a learning curve they'll need to adjust to in order to feel comfortable leading their session.

They should have a high awareness of all their available features. Notable settings that help them control the experience include:

- Waiting room features
- Chat features, including disabling private chat
- Muting participants
- Disabling video
- Turning off annotation
- Managing screen sharing of fellow attendees
- Removing participants

If they'll be occupied with meeting content and a number of people will be present, it may be worth having another person from your organization join. The team member leading the meeting can designate this additional team member as a co-host. The co-host can control the above listed features while the original host leads the meeting.

Team members should also ensure they've downloaded the correct software version before their session and join a few minutes early, just in case they encounter technical difficulties. These can be challenging to predict, so their best bet is always to join four or five minutes early, so they can address any unexpected issues.

With a strong handle on the features available to them, they'll be able to lead the session with authority and be prepared to shut down any unanticipated security issues that come their way. For most sessions, they won't need to use this knowledge, but everyone (except the uninvited guests) will be grateful they're ready if a security breach occurs.