Zoom Security Guidance 11/02/2020

Timothy M. Chester, Vice President for Information Technology

Going forward, units using Zoom to host high-profile special events beyond ordinary instruction and administrative meetings (particularly those that include individuals outside the University) are expected to ensure that the following list of best practices is followed:

1. Ensure the Meeting ID section is marked "Generate Automatically" for each session being hosted in order to avoid reusing the same number. Do not use a Personal Meeting ID (PMI) for special events.

2. Set a password for your meeting to prevent unanticipated guests from joining.
   When scheduling a meeting, under **Meeting Options**, select **Require meeting password**, then specify a six-digit code. Participants will be asked to enter this code in order to join your meeting. Never post both the meeting ID and password together (or a URL combining both) on a public-facing Web site. Require your guests to register for the meeting, and only share the password with those identifiable individuals who have registered to attend.

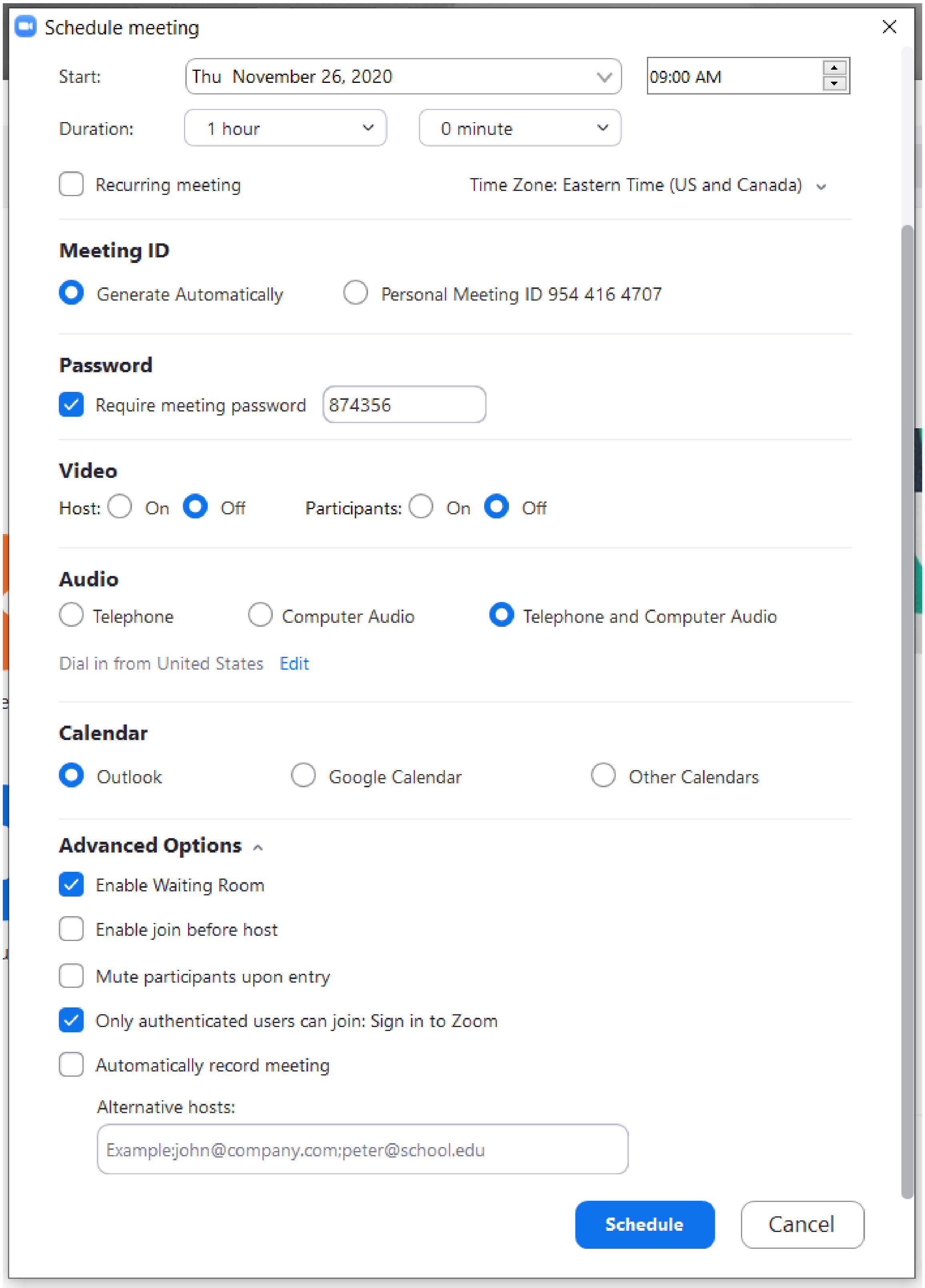
3. Use the Waiting Room to control when participants join your meeting.
   As the meeting host, you can admit attendees individually or hold all attendees in the virtual waiting room and admit all when you are ready to begin. Admitting participants from the Waiting Room requires an additional step, but it provides increased control to allow participants to join the meeting when you accept them. **Special events should also have multiple hosts, including one whose sole role is to manage the waiting room and be prepared to quickly eject participants who disrupt the meeting.** In cases where breakout rooms are used, each breakout room should have one host minding the breakout room.

4. Disable the "join before host" functionality.
   When this is disabled, participants will see a pop-up dialog that says, "Please wait for the host to start this meeting." If you are the host, there is a login button to log in and start the host meeting.

5. Limit screen sharing to the host. This restriction can help prevent intrusive sharing and potential meeting disruptions.

6. Consider requiring MyID authentication for your meeting.
   By default, anyone with the join link or meeting ID (and password) can join a meeting hosted by users on your account, even if they are not signed in to Zoom. To prevent unknown participants from entering the session, you have the option to restrict meeting participants to users who are signed in to Zoom. We are exploring enabling a new Zoom feature, by default, that would automatically assign non-MyID users to the waiting room. This setting will allow meeting hosts to be a gatekeeper and potentially prevent unknown users from entering the meeting.

If you ever have any questions about how to ensure that your event or meeting occurs without disruption, please reach out for support by emailing helpdesk@uga.edu.



Schedule meeting

Start: Thu November 26, 2020 | 09:00 AM

Duration: 1 hour | 0 minute

□ Recurring meeting Time Zone: Eastern Time (US and Canada)

Meeting ID

● Generate Automatically ○ Personal Meeting ID 954 416 4707

Password

☑ Require meeting password 874356

Video

Host: ○ On ● Off Participants: ○ On ● Off

Audio

○ Telephone ○ Computer Audio ● Telephone and Computer Audio

Dial in from United States Edit

Calendar

● Outlook ○ Google Calendar ○ Other Calendars

Advanced Options

☑ Enable Waiting Room

□ Enable join before host

□ Mute participants upon entry

☑ Only authenticated users can join: Sign in to Zoom

□ Automatically record meeting

Alternative hosts: Example:john@company.com;peter@school.edu

If you ever have any questions about how to ensure that your event or meeting occurs without disruption, please reach out for support by emailing helpdesk@uga.edu.