U.S. Coast Guard Auxiliary

Computer Software & Systems Directorate
Cybersecurity Division

CYBERSECURITY AWARENESS BULLETIN

RECOMMENDED PRACTICES FOR CONDUCTING SECURE VIDEO CONFERENCES

Serial:	CI-AWA-2021-110-01
Date:	20 APRIL 2021

Overview

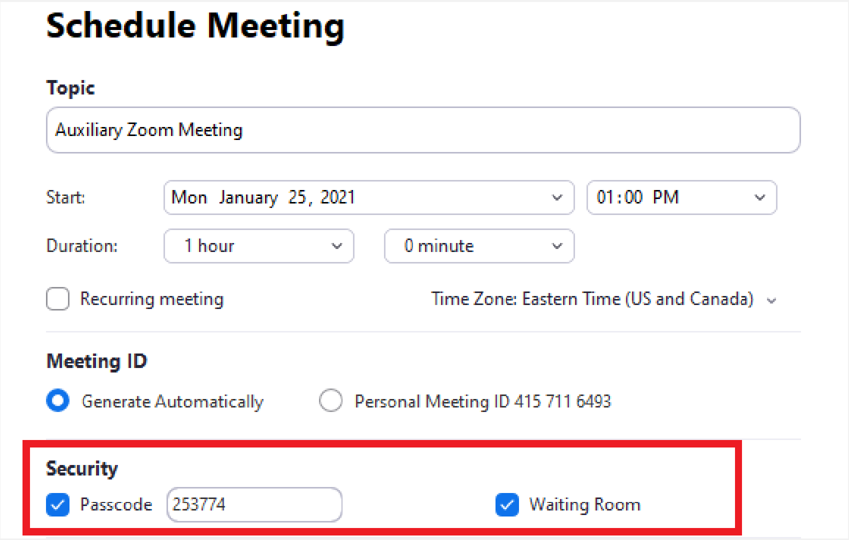
The COVID-19 pandemic has forced Auxiliary units to move nearly all their meetings and training sessions to online video conferencing platforms. If these meetings and training sessions are left unprotected, malicious actors can gain unauthorized access to these meetings, known as "Zoom bombing," which is intrusive and disruptive to Auxiliary business. Zoom bombing can lead to unauthorized disclosures of Auxiliarists' personally identifiable information (PII). It can also compromise sensitive data about Auxiliary strategies, plans, and operations that are discussed during online meetings. To prevent this, we recommend that Auxiliarists enable certain security features in their online video conference platforms.

Below, we describe the steps Auxiliarists will need to take to enable these security features on several of the most popular online video conferencing platforms: Zoom, GoToMeeting, Microsoft Teams, WebEx, and Google Meet.

Enabling password, waiting room features on Zoom

We recommend setting a meeting password for attendees and enabling the "waiting room" feature on Zoom. This creates at least two layers of security protection for Zoom meetings.

To enable the meeting password and "waiting room" features, the meeting organizer should select the "enable password" and "waiting room" check boxes when scheduling the Zoom meeting. These options are highlighted in red in Figure 1, below.



Schedule Meeting

Topic

Auxiliary Zoom Meeting

Start: Mon January 25, 2021 — 01:00 PM

Duration: 1 hour — 0 minute

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

Meeting ID

● Generate Automatically ○ Personal Meeting ID 415 711 6493

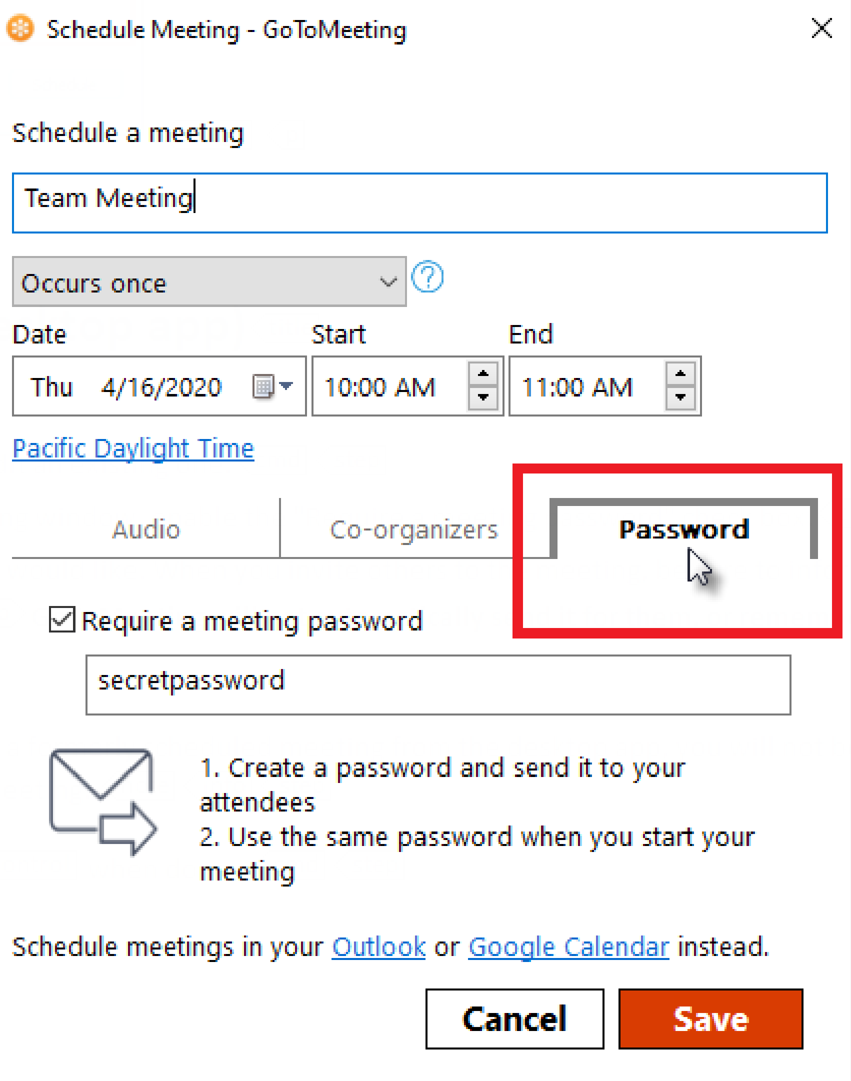
Security

☑ Passcode 253774 ☑ Waiting Room

Figure 1: The passcode and waiting room security features for Zoom meetings are highlighted inside the red rectangle.

Enabling password, waiting room features on GoToMeeting

To enable passwords on GoToMeeting, click the “password” tab when scheduling a meeting, then enter a password for your meeting attendees to use. Be sure to send this password to your attendees prior to the start of the meeting. This option is highlighted inside a red rectangle in Figure 2, below.



Schedule Meeting - GoToMeeting

Schedule a meeting

Team Meeting

Occurs once

Date: Thu 4/16/2020

Start: 10:00 AM

End: 11:00 AM

Pacific Daylight Time

☑ Require a meeting password

secretpassword

1. Create a password and send it to your attendees
2. Use the same password when you start your meeting

Schedule meetings in your Outlook or Google Calendar instead.

Figure 2: In this screenshot from goto.com, the password setting for meetings appears inside a red rectangle.

We also suggest that you lock your meeting once attendees have arrived. This will not prevent latecomers from attending your meeting. Instead, those who attempt to join your meeting after you've locked it will be placed into a waiting room. They can then be admitted to your meeting manually. To enable this security feature, click the lock icon at the top of the GoToMeeting app, shown in Figure 3.

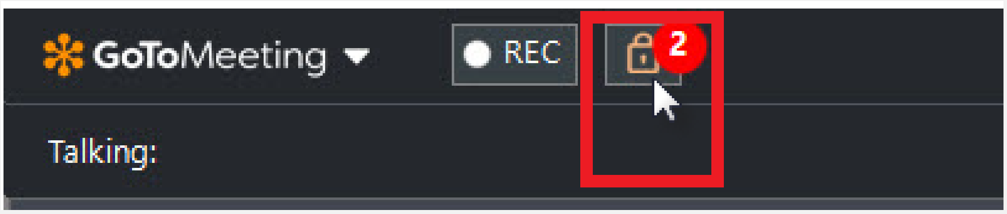
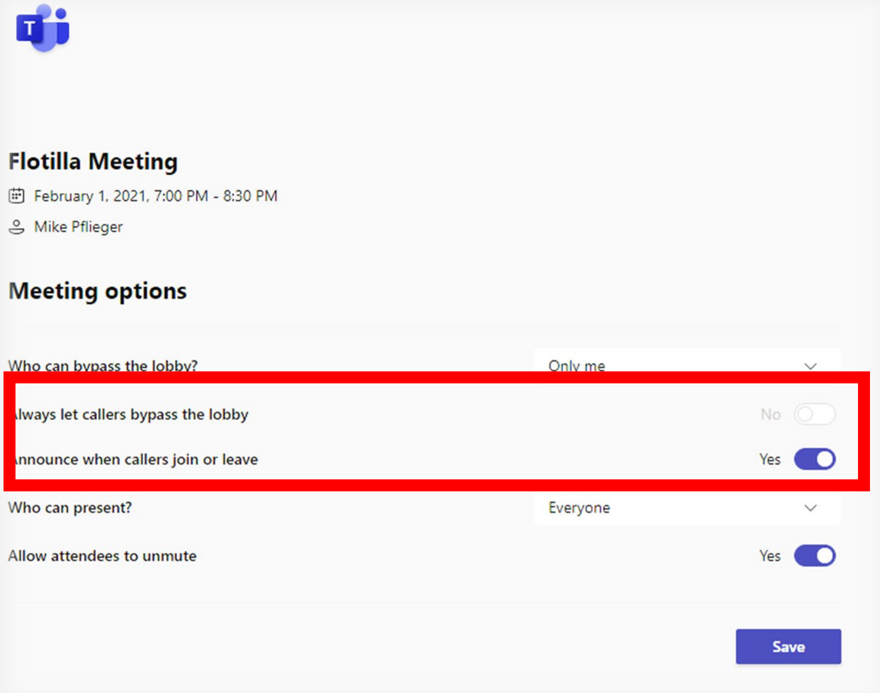


Figure 3: In this screenshot from goto.com, the lock icon--which places late arrivals to your meeting in a waiting room--appears inside a red rectangle.

Enabling waiting room features on Microsoft Teams

Currently Microsoft Teams doesn't have a password feature, but we recommend enabling the "waiting room" feature on Teams meetings. This creates basic security protection for Teams meetings. These are found in Meeting Options.

To enable the "waiting room" features, the meeting organizer should set the "Who Can Bypass the lobby" to "Only Me" and set "Always let callers bypass the lobby" to "No". These options are highlighted in red in Figure 4, below.



Flotilla Meeting

February 1, 2021, 7:00 PM - 8:30 PM

Mike Pflieger

Meeting options

Who can bypass the lobby? Only me

lways let callers bypass the lobby No

nnounce when callers join or leave Yes

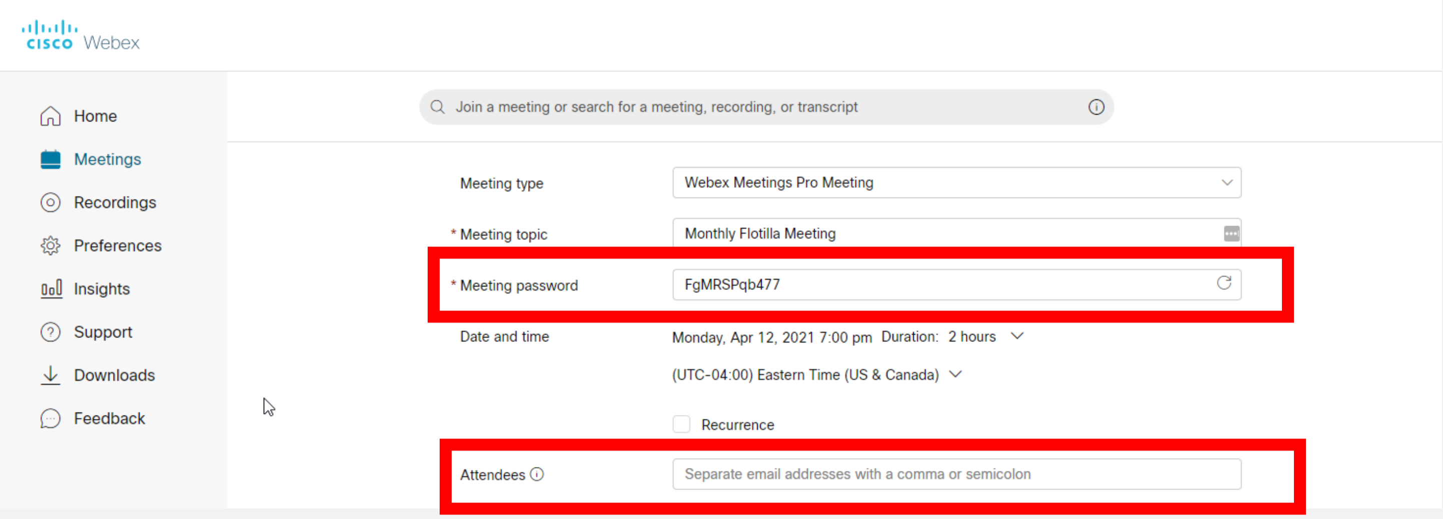
Who can present? Everyone

Allow attendees to unmute Yes

Figure 4: The waiting room security feature for Teams meetings are highlighted inside the red rectangle.

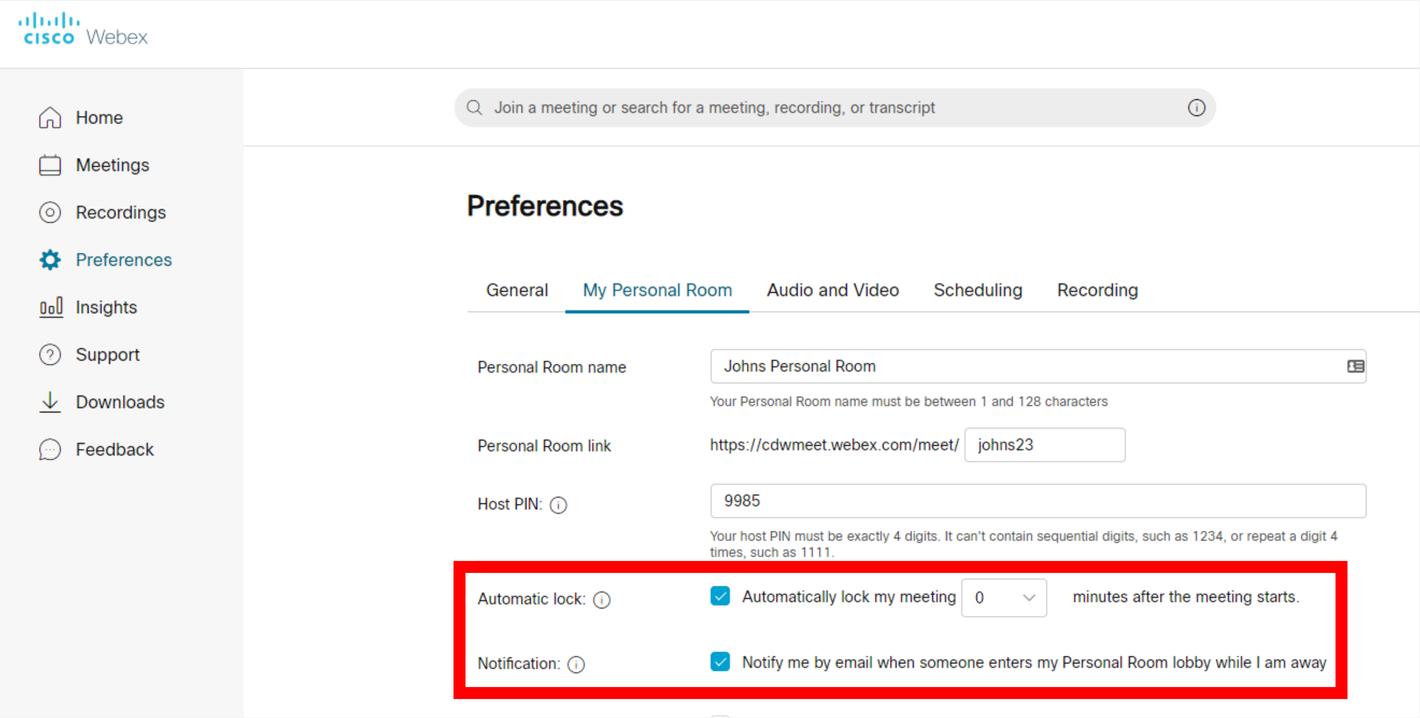
Enabling password and waiting room features on Cisco WebEx

You should schedule individual meetings versus using a personal room. This means the meeting invitation is only good for the scheduled meeting, versus using your personal meeting room. A meeting password is therefore required. Do no post this password, rather send it in the invitation to guests via email or by adding them as attendees.



Meeting type: Webex Meetings Pro Meeting
* Meeting topic: Monthly Flotilla Meeting
* Meeting password: FgMRSPqb477
Date and time: Monday, Apr 12, 2021 7:00 pm Duration: 2 hours
(UTC-04:00) Eastern Time (US & Canada)
□ Recurrence
Attendees: Separate email addresses with a comma or semicolon

If you must use your personal room, set it to automatically lock when your meeting starts. We recommend locking your room at 0 minutes. You can set auto lock settings by selecting Preferences > My Personal Room

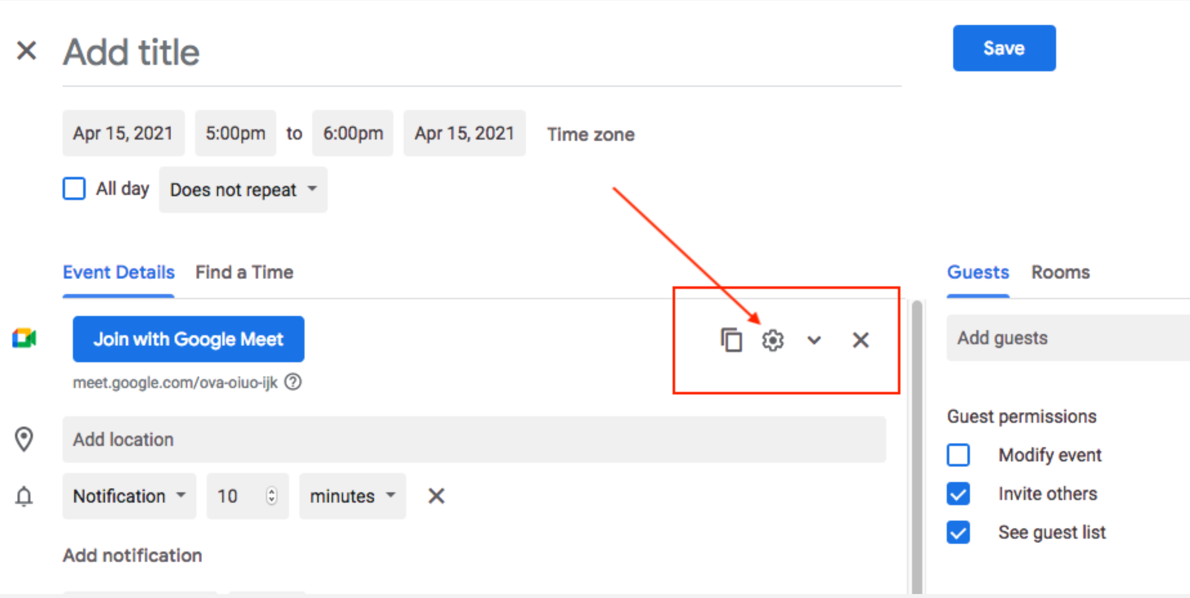


Personal Room name: Johns Personal Room
Your Personal Room name must be between 1 and 128 characters
Personal Room link: https://cdwmeet.webex.com/meet/ johns23
Host PIN: 9985
Your host PIN must be exactly 4 digits. It can't contain sequential digits, such as 1234, or repeat a digit 4 times, such as 1111.
Automatic lock: ☑ Automatically lock my meeting 0 minutes after the meeting starts.
Notification: ☑ Notify me by email when someone enters my Personal Room lobby while I am away

You should choose to be notified when someone enters your Personal Room lobby.

Enabling security features on Google Meet

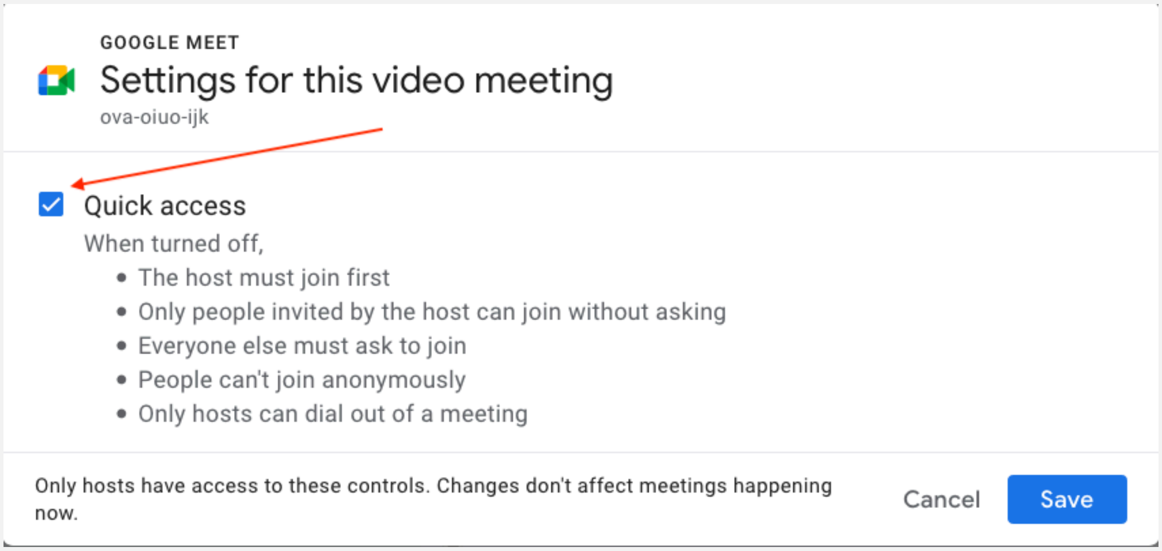
When scheduling a conference on Google Meet, we recommend that you disable the “quick access” feature. Doing this will activate many security functions. To get started, look for the gear icon, which is indicated with a red arrow in the figure below.



☐ Modify event
☑ Invite others
☑ See guest list

Figure 5: Click the gear icon, shown here inside the red rectangle, when schedulng a conference on Google Meet. Doing this will show you an option to enable important security features.

Next, you should uncheck the “Quick Access” box, highlighted in Figure 6 with a red arrow. Doing this will enable several security features at once. These measures include blocking individuals who attempt to join the conference anonymously and requiring the host to admit attendees manually who have not previously been invited to the meeting.


GOOGLE MEET

Settings for this video meeting

ova-oiuo-ijk

☑ Quick access

When turned off,

- The host must join first
- Only people invited by the host can join without asking
- Everyone else must ask to join
- People can't join anonymously
- Only hosts can dial out of a meeting

Only hosts have access to these controls. Changes don't affect meetings happening now.

Figure 6: The Quick Access setting should be disabled when scheduling a conference on Google Meet. You can disable quick access by unchecking the blue box shown above.

Additional General Web Conferencing Tips

Here are some tips regardless of what platform you are using:

1) Connect securely. Make sure your home network is secure.
2) Keep your PC or device updated with patches. Running Windows Update for example or using a free tool like PatchMyPC can help unsure you keep your device updated.
3) Keep your application up to date. If your application uses a downloaded client make sure to keep it updated.
4) Control access. Know who you invited and who is entering the meeting.

Conclusion

Using the basic security features that are built into video conferencing software applications like Zoom, GoToMeeting, and Microsoft Teams is a simple and effective way to secure Auxiliary communications.

In addition to implementing the video conference security measures described in this bulletin, we encourage Auxiliarists to stay up to date with the latest cybersecurity division guidance on our website.

Sources

https://support.zoom.us/hc/en-us/articles/360033559832-Meeting-and-Webinar-Passwords-

https://support.zoom.us/hc/en-us/articles/115000332726-Waiting-Room

https://support.goto.com/meeting/help/password-protect-a-meeting-g2m090084

https://support.goto.com/meeting/help/lock-your-meeting-g2m040025

https://docs.microsoft.com/en-us/microsoftteams/meeting-settings-in-teams

https://www.cisa.gov/sites/default/files/publications/CISA_Guidance_for_Securing_Video_Conferencing_S508C.pdf

https://support.google.com/meet/answer/9852160?hl=en#zippy=%2Csafety-best-practices