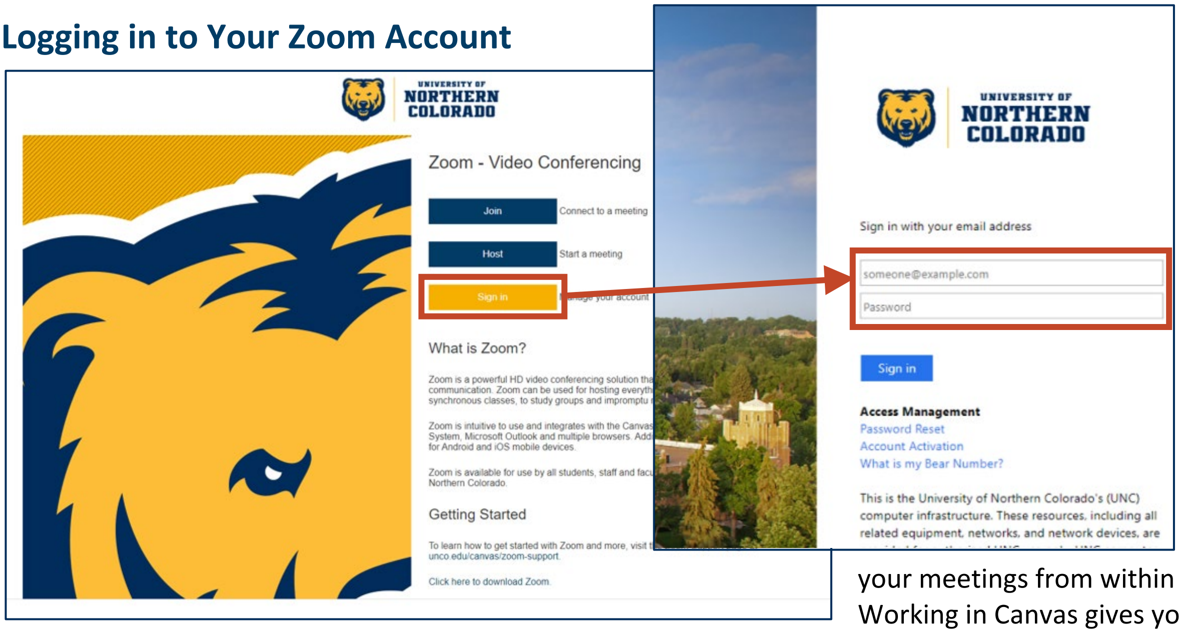
ZOOM SECURITY - BEST PRACTICES

UNC
Instructional Design & Development

Zoom is a great teaching and learning tool because it is easy to use and nicely integrated into Canvas. The ease and openness of Zoom also makes it vulnerable to attack. Use this guide to review your Zoom settings, and make changes as appropriate to make your meetings as secure as possible.

Logging in to Your Zoom Account

If you have not done so, open UNC's Zoom Portal, and then Sign in with your credentials. Logging in through the Zoom portal gives you access to all of your settings and to your recordings. After setting up your Zoom room, then the best practice for teaching is to run your meetings from within your Canvas course. Working in Canvas gives you more security.



Zoom is a powerful HD video conferencing solution tha communication. Zoom can be used for hosting everyth synchronous classes, to study groups and impromptu

Zoom is intuitive to use and integrates with the Canvas System, Microsoft Outlook and multiple browsers. Add for Android and iOS mobile devices.

Zoom is available for use by all students, staff and facu Northern Colorado.

To learn how to get started with Zoom and more, visit t unco.edu/canvas/zoom-support.

This is the University of Northern Colorado's (UNC) computer infrastructure. These resources, including all related equipment, networks, and network devices, are

Student Access

Students do not need to have a Zoom account to access and attend your class meetings in Zoom. If they have the link to the meeting, they can join by clicking on the link. The most secure way to have students join your meetings is to join from within their Canvas courses. Meetings that are set up within a Canvas course can be accessed from students' To Do Lists, Calendars, and from the Zoom page within that course.

Using Zoom to Produce Course Video

Delivering recorded content online is a very secure option. Panopto is the best tool that we have for doing this inside of Canvas. If you are giving lectures inside of Zoom, it is a good idea to record those lectures. You can then download them to your desktop, and upload them into Panopto so your students can review those lectures. This redundancy can enhance student learning.

Creating Secure Meetings

The best way to secure your online classroom is to work as much as possible inside Canvas, avoid having Zoom send your invitations by email, and limit attendee ability to take control of the tools in your Zoom classroom. For an additional level of security, **add a Co-Host** (a colleague or a GTA) to monitor your meeting. Also, your meetings will be more secure if you create a new meeting room for every class or individual meeting. If you can't do that, at least be sure to protect your personal meeting room from trolls and hackers by limiting who gets the consistent link to your personal room.

Send class invitations from the course, and if using a password, share it as an announcement just prior to your meeting.

Recommended Settings

Find **Settings** in your Zoom admin portal, and then check them against this list of secure settings. We are highlighting only those settings that are most closely related to security. Begin with the most secure settings so you know how they work, and then change them if they are too restrictive.

ZOOM SECURITY - BEST PRACTICES

Security

Waiting Room ●
(We recommend that you customize your waiting room)

Embed password in meeting link ○

Require a passcode ●
(This is a good security approach for all three types of meetings)

Only authenticated users can join meetings ○
(The best practice is to use at least one of these top three security measures)

Schedule Meeting

Host Video ●

Participants Video (Off) ○

Mute participants upon entry ●

Join before host ●
(If you have a waiting room, otherwise, don't allow)

Use personal meeting ID ●
(To be safe, always create a new meeting room for every meeting

In Meeting (Basic)

Chat ●
(Chat is important for monitoring your meeting)

Private Chat ○
(Keeps students from attacking other students)

File transfer ○

Co-host ●
(Have a co-host to monitor your meeting throughout)

Screen sharing ●
(Must be enabled for presenters)

Who can share? **HOST ONLY**
(Do not give up control of your screen unless you know who is taking control. To secure large meetings, turn off sharing tools)

Disable desktop/screen share for users ○

Annotation ○

Whiteboard ○

Remote control ○

Non-verbal feedback ○

Meeting reactions ○

Join different meetings simultaneously ○

Allow participants to rename themselves ○

Allow removed participants ● to rejoin ***(for anyone removed unintentionally)***

In Meeting (Advanced)

Report to Zoom ●

Remote support ○

Far end camera control ○

Virtual background ○

Video filters ○

Identify guest participants ○

Auto-answer group in chat ○

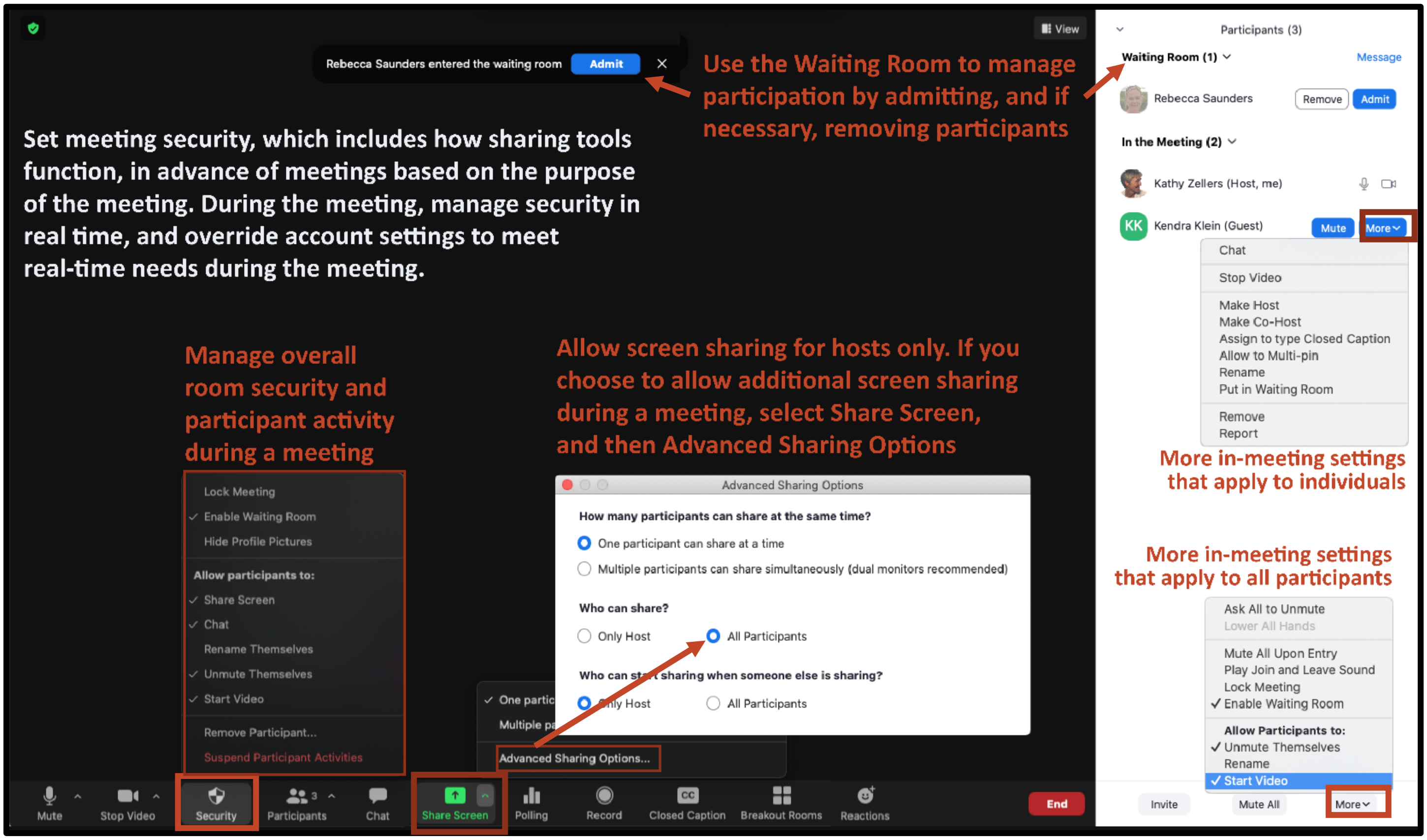
Only show default email when sending email invites ○

Use HTML format email for Outlook plugin ○

REMEMBER: These settings are the most secure settings, and they are ideal for large meetings. Try them and adjust to your situation, particularly for smaller classes where sharing is an important part of student engagement.

ZOOM SECURITY - BEST PRACTICES

Manage a Secure Meeting - Host Controls



Set meeting security, which includes how sharing tools function, in advance of meetings based on the purpose of the meeting. During the meeting, manage security in real time, and override account settings to meet real-time needs during the meeting.

Use the Waiting Room to manage participation by admitting, and if necessary, removing participants

Manage overall room security and participant activity during a meeting

Allow screen sharing for hosts only. If you choose to allow additional screen sharing during a meeting, select Share Screen, and then Advanced Sharing Options

More in-meeting settings that apply to individuals

More in-meeting settings that apply to all participants

Rebecca Saunders entered the waiting room

Advanced Sharing Options

How many participants can share at the same time?

● One participant can share at a time

○ Multiple participants can share simultaneously (dual monitors recommended)

Who can share?

○ Only Host ● All Participants

Who can start sharing when someone else is sharing?

● Only Host ○ All Participants

Waiting Room (1): Rebecca Saunders

In the Meeting (2): Kathy Zellers (Host, me); Kendra Klein (Guest)

Manage Participants – *During your meeting,* you have several settings to manage. Your meeting functions according to the settings you initially established in your account, but most of these settings can be adjusted, as needed, during your meeting. Select Participants in your meeting menu across the bottom of your room to see all of the meeting participants. In this area, you can manage all participant settings, and individual settings, in real time.

The Waiting Room secures your meeting so that you control who enters. You can also remove participants from your meeting at any time. If necessary, you can put someone in the waiting room during your meeting.

Add a Co-Host – Managing the waiting room takes time and attention, and so having a co-host monitor your waiting room is advised. A co-host can monitor participant activity, monitor and answer chat, and both watch for and resolve technical and/or security issues. A co-host greatly enhances meeting security.

Secure Sharing – If you have your meeting locked down in advance, then participants will not be able to share without your knowledge or permission. If during the meeting you find the need to allow someone to share, then you can make adjustments in the meeting through the Security and Share Screen controls and menus shown above. If you know all of the participants in your meeting, as well as all of the functions you need, then you can adjust your settings before the meeting so that you will not have enable them during the meeting.

REMEMBER: After you set up your Zoom account with all your default security settings, your class meetings and lectures will be most secure when you create and launch them from your course within Canvas.