NCSAEL

National Cyber Security Auditing and Evaluation Lab

Security Guidelines for Online Classes, using Tele-Conferencing Software

2020

National Cyber Security Auditing and Evaluation Lab (NCSAEL)
National University of Sciences & Technology (NUST)
Military College of Signals (MCS)

Since countries have begun enforcing shelter-in-place and stay-at-home orders due to virus pandemic, the video conferencing software have become a popular way to keep in touch with friends and family; holding business meetings, working from home, and so on. The education sector is a good case in point: universities have been delivering distance learning as a feature by conducting online lectures for the students. However, with the increasing popularity of tele-conferencing software, the attack and security breaches are also increasing. Video conferences are high profile targets, targets, and the combination of unsecured networks and subpar video conferencing security practices impose serious threats and vulnerabilities to the data residing in your device (computers, mobiles). Therefore, it is necessary to follow some best practices regarding video conference calls. Outlined below are some key considerations to be taken care of when initiating a video conference call.

Work Environment

Please ensure that all the sensitive and confidential material is removed from the camera scrutiny. Thoroughly examine your environment, make sure that video streaming doesn't contain some sensitive material. Video conferences conducted at a user's desk should train the camera to focus on the user's face, and any visible confidential data should be removed from camera view.

Consider the effects of any kind of interruption for instance, toddler entering the video. Ensure necessary mitigations are in place before the meeting starts. Moreover, never leave your device unattended.

1. Control Access- Domain Based Security

Video conferencing providers that take a domain-based approach to security are ideal in a way that they allow people to collaborate in a secure and well-controlled environment. Domain-based security enables the system administrator to control access to video conferences by assigning various levels of permission to users. For example, if your video system uses domain-based security, an outsider who attempts to start a video call with someone in your company must wait until a user with the required permissions performs a sign-in and grants that person access.

Moreover, most video conferencing platforms allow for the creation of groups of users or the ability to restrict access by internet domain so only users with an email address from your institution would be able to join the call. Alternatively, only allow attendees that are invited by adding their email addresses to the invite when scheduling the call.

2. Set a Meeting Password

Make sure to set a meeting password in order to mitigate any kind of exploitation. When scheduling an online meeting, creating a password option exists which adds a randomly generated password. This password will be required to join the meeting. Also, make sure to not embed the password in the meeting link. Set strong passwords on boots and set inactivity timeouts.

3. Multi Factor Authentication (MFA)

We suggest that you can also beef up your logins with MFA also called as Two Factor Authentication. In this way, you don't have to entrust your passwords only.

4. Use of Waiting Rooms

Holding participants in a "Waiting Room" and approving the connection of each one gives the meeting holder ultimate control over who is in the meeting. To handle this for larger meetings you may be able to promote other trusted attendees to an organizer or a moderator role.

5. Secure Data Transmission

Data transmission is the most vulnerable area of video-conferencing security since the data must travel over so many public and private networks to reach its destination. Encryption and network security are the keys to protect data transmission during a video conference. Our recommendation is to prioritize your active in-flight video calls and at-rest recordings with utmost level of data security.

- Enforce encrypted traffic. Do not take it for granted that systems have this option enabled by default for video communications. Some services encrypt chat by default but not video unless specifically requested
- If third-party endpoint client software is permitted, then ensure it complies with the requirements for end-to-end encryption
- If file transfers are required, then consider limiting the types of files that can be sent; for example, don't allow executable files

6. Use VPN to Access Organization Internal Network

Always use a VPN to connect remote workers to the organization's internal network. This prevents man-in-the-middle attacks from remote locations. Since you're now working from home, the traffic is now flowing over public networks.

7. Screen Sharing

Screen sharing should be made limited to the person with administrative access. When sharing the screen, only share the needed application not the whole desktop. Any side information that might contain an icon or folder name, can give away your sensitive information.

8. Privacy Policy

We insist to check the privacy policy of the service you are using. If it's a freeware, make sure to check whether the company is collecting, selling or sharing your data to fund the provision of its 'free' service.

9. Logout When Not in Use

Make sure to logout when you are finished with all the mandatory tasks.

Security Guidelines for Zoom Software

The video conferencing app Zoom has seen an explicit rise in the number of users since the amid lockdown. However, there have been various concerns about the security and privacy of end users while using this application. The company has also faced criticism over privacy invasions and alleged phishing attacks. Zoom has had security flaws in the past. Last year, researchers revealed hackers were able to spy via webcams of users because of a bug in its code. Since many educational institutions are conducting online classes, instructors and students are using video conferencing applications. Specifically, "Zoom" video chat is used by many people for video conferencing, studying, working, or socializing from home. However, there are certain attacks and threats while using this facility such as the "Zoom bombing" attack in which an attacker gains unauthorized access to a Zoom meeting. Uninvited guests who "zoom-bomb" online gatherings on Zoom have become a big enough problem. Now that you know the potential hazards, listed below are the necessary measures to reduce the risks for Zoom meetings.

1. **Use Updated Zoom Software:** Before initiating the meeting, make sure that all the participants have latest Zoom software. Please install the Zoom client update. The latest Zoom updates enable meeting passwords by default and add protection from people scanning for meeting IDs.

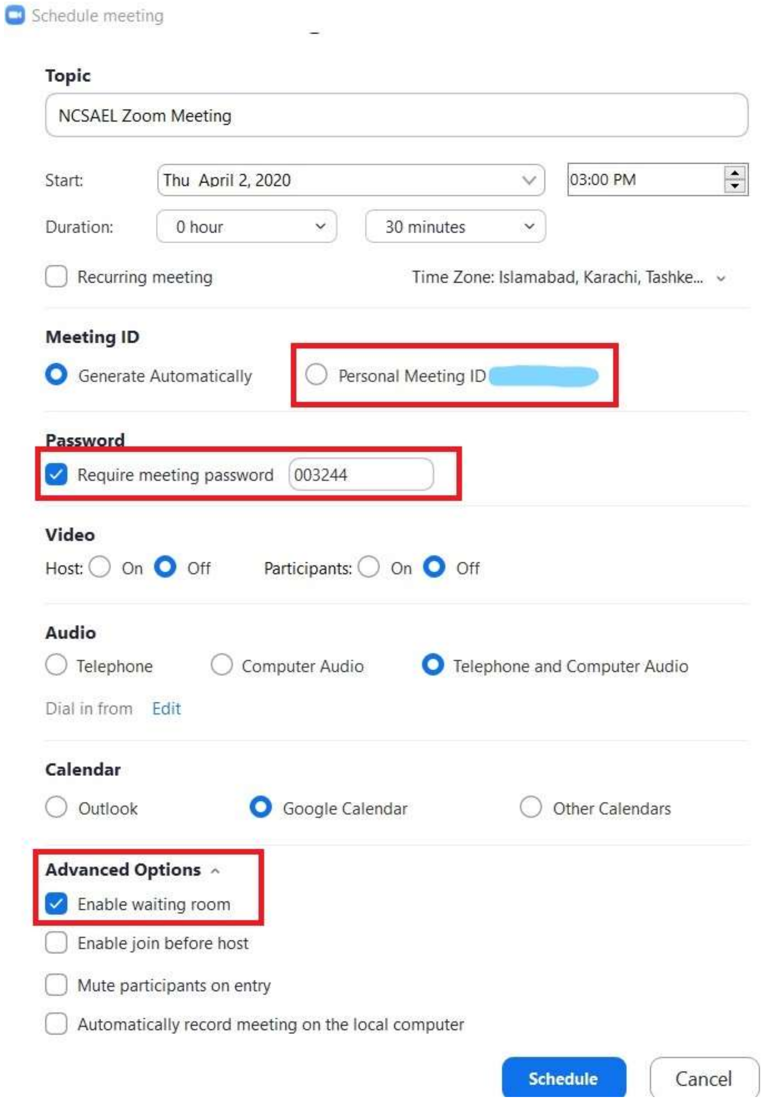
2. **Personal Meeting ID (PMI) Concealment:** Remember not to share your PMI with anyone. Each Zoom user is allotted PMI for the account, if it gets leaked somehow then status of the ongoing meetings can be checked and anyone who has access to your PMI can join the meetings if the password is not configured.

3. **Recording Zoom Meetings:** One of the most important things to remember is that a Host (the one who created the meeting) can record a Zoom session, including the video and audio, to their computer. Therefore, be careful saying or physically 'revealing' anything that you would not want someone else to potentially see or know about.

4. **Password Protected Zoom Sessions:** When creating a new Zoom meeting, Zoom will automatically enable the "Require meeting password" setting and assign a random 6-digit password.

5. **Disable "Join before Host" Option:** This way, organizers will have full control over the meeting that too from the very start.

6. **Use Waiting Room:** Zoom allows the host to enable a waiting room feature that prevents users from entering the meeting without first being admitted by the host.



Schedule meeting

Topic

NCSAEL Zoom Meeting

Start: Thu April 2, 2020 03:00 PM

Duration: 0 hour 30 minutes

□ Recurring meeting Time Zone: Islamabad, Karachi, Tashke...

Meeting ID

● Generate Automatically ○ Personal Meeting ID [redacted]

Password

☑ Require meeting password 003244

Video

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

Audio

○ Telephone ○ Computer Audio ● Telephone and Computer Audio

Dial in from Edit

Calendar

○ Outlook ● Google Calendar ○ Other Calendars

Advanced Options

☑ Enable waiting room

□ Enable join before host

□ Mute participants on entry

□ Automatically record meeting on the local computer

7. **Screen Sharing Control:** If the meeting participants don't want to share their screen, they should simply turn the option off, by sliding the button to the right. For the cases where screen sharing with the participants is necessary, screen sharing slider should be turned on with Only Host option.

8. **Enable "Only Host" Option for Screen Sharing:** If you want your video session to not get hijacked then necessarily limit the screen sharing option to one participant the Host only. By clicking on the advanced setting, go to
Advanced Sharing Options -> One participant can share at a time -> Only Host
This way, hosts can prevent others from posting the videos or screen sharing.

9. **Avail Lock Meeting:** Better enable the Lock meeting option after everyone has joined the meeting. This way, no one can join the meeting afterwards. Go to
Manage Participants -> More -> Lock Meetings

10. **Use Silencer Option:** If someone is making unnecessary interruptions, video for participants can be disabled and any individual can be muted.

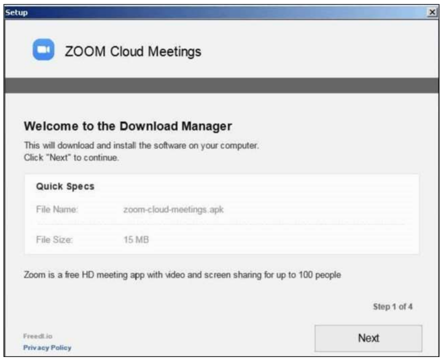
11. **Cut the Chatter Box:** Text chat option can be made disabled to limit the unwanted messages.

12. **Boot the Uninvited:** Using Remove Option, host can remove any of the attendee he wants or can permanently block people from rejoining the meetings.

13. **Never Post Pictures of Zoom Meeting:** Posting pictures of your zoom meeting might contain the associated zoom ID of your account. This can then be used by uninvited people to try and access the meeting, if it is not password-protected.

14. **Never Post the Zoom Meeting Link:** When creating Zoom meetings, you should never publicly post a link to your meeting. Doing so will cause search engines such as Google to index the links and make them accessible to anyone who searches for them. Email or text the link directly to the attendees.

15. **Beware of Zoom Malware:** Stay cautious of the adware or malware that pretend to be Zoom client installers.



Welcome to the Download Manager

This will download and install the software on your computer.
Click "Next" to continue.

Quick Specs

File Name:	zoom-cloud-meetings.apk
File Size:	15 MB

Zoom is a free HD meeting app with video and screen sharing for up to 100 people

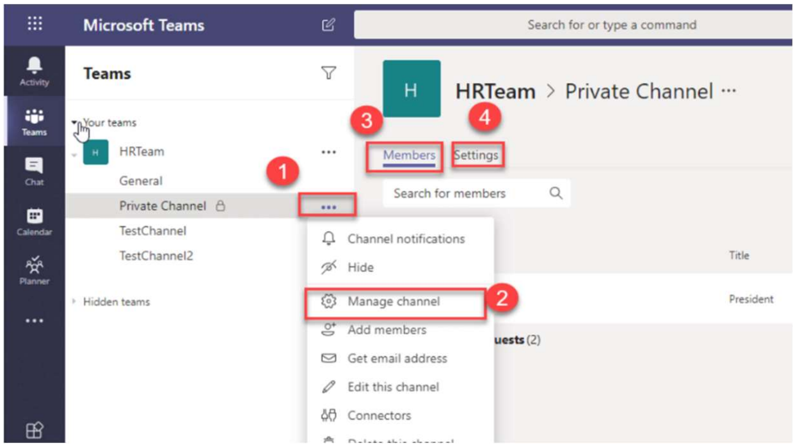
16. If you are using a desktop with plugin webcam, when webcam is not in use make sure to unplug it. Secondly, if you are using laptop with webcam, coverup the webcam with the piece of tape, also disable the built-in microphone when not in use. So that hackers cannot listen and record whatever the conversation is taking place on the video.

17. Prefer using Browsers to connect to zoom meeting rather than Zoom app. Because, unlike the applications many browsers are recently hardened against attacks.

Security Guidelines for Microsoft Teams Software

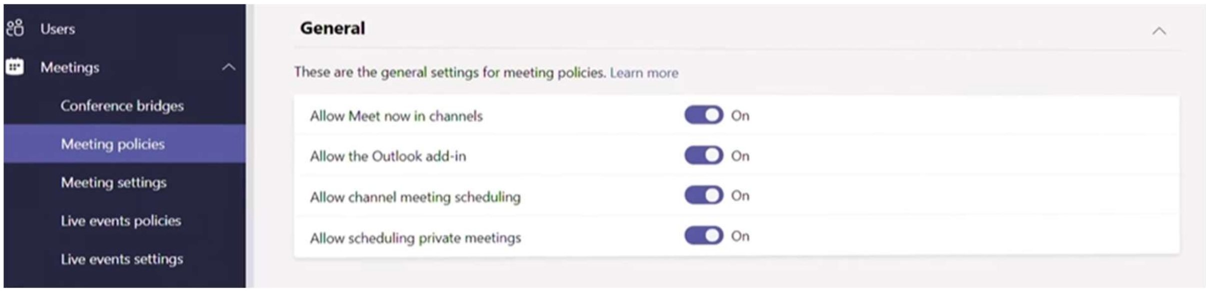
Similarly, an increased user base for Microsoft Teams has also been observed. Microsoft Teams is a fully integrated communications platform for Office 365. Microsoft includes Teams in most Office 365 plans, and now allows guest access to Teams channels for cross organizational collaboration. Teams is available for most licenses of Office 365, so you will find it in corporate or business settings, the federal government, and educational institutions. Microsoft Teams, as part of the Microsoft 365 (M365) service, follows all the security best practices and procedures such as service-level security through defense-in-depth, customer controls within the service, security hardening and operational best practices. However, following are the few guidelines that should be observed while using Microsoft teams for online classes, meetings, content sharing, and so on.

1. **Private Channels in Microsoft Teams:** Private channels in Microsoft Teams create focused spaces for collaboration within your teams. Only the users on the team who are owners or members of the private channel can access the channel. Anyone, including guests, can be added as a member of a private channel as long as they are already members of the team. A lock icon indicates a private channel. Only members of private channels can see and participate in private channels that they are added to.



2. **Add Teams Gradually:** When you first roll out Teams, we recommend starting with a small number of teams and team members. Add new people or groups as you go.

3. For meetings, Teams provide the General settings option.

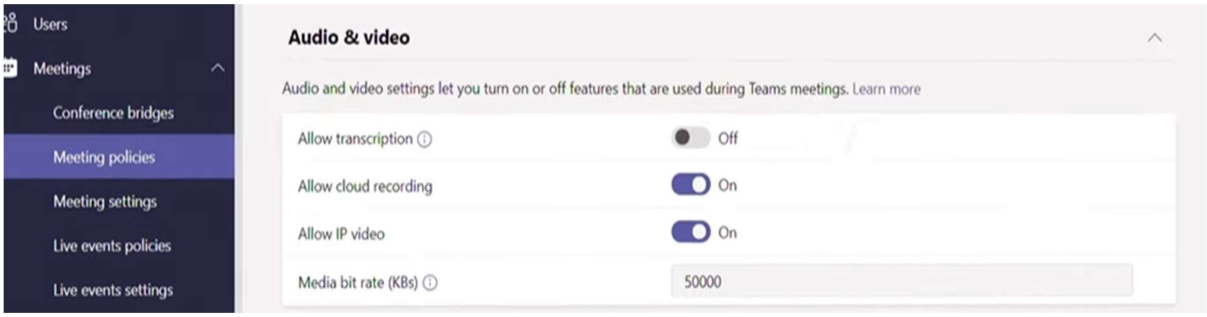


General

These are the general settings for meeting policies. Learn more

Allow Meet now in channels	On
Allow the Outlook add-in	On
Allow channel meeting scheduling	On
Allow scheduling private meetings	On

4. Avail the audio and video setting options for secure communication during Team Meetings

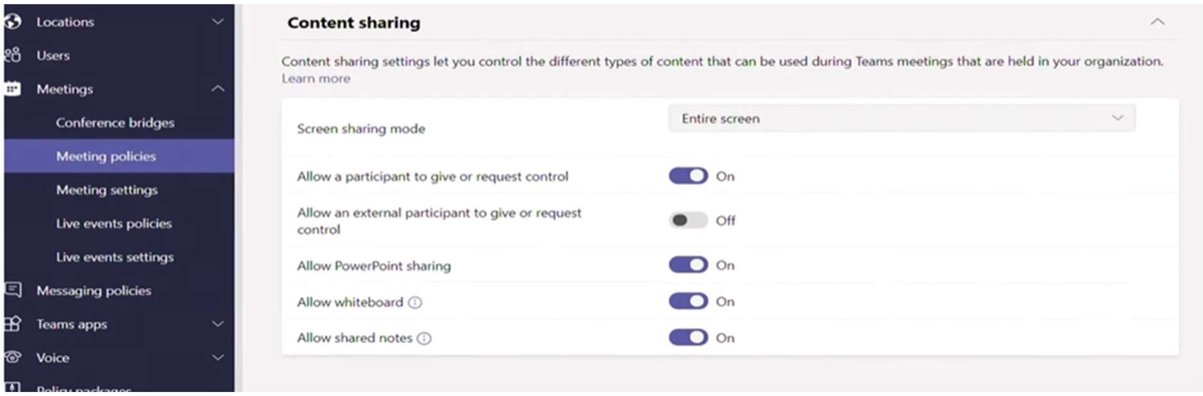


Audio & video

Audio and video settings let you turn on or off features that are used during Teams meetings. Learn more

Allow transcription ⓘ	Off
Allow cloud recording	On
Allow IP video	On
Media bit rate (KBs) ⓘ	50000

5. Make sure to add checks for content sharing.



Content sharing

Content sharing settings let you control the different types of content that can be used during Teams meetings that are held in your organization. Learn more

Screen sharing mode	Entire screen
Allow a participant to give or request control	On
Allow an external participant to give or request control	Off
Allow PowerPoint sharing	On
Allow whiteboard ⓘ	On
Allow shared notes ⓘ	On

Some of the best practices for managing Teams include:

- Create different channels in Teams to direct conversation
- Allow users to create new Teams, but maintain oversight and clean up after them
- Take advantage of integrations with other software in your technology stack
- Leverage chatbots to promote daily activity and tasks
- Use PowerShell to manage Teams

And for File Sharing, consider the recommendations below:

- Require multi-factor authentication
- Enforce least privileged access across Teams and Office 365
- Classify sensitive data and use Varonis and Microsoft AIP for additional protection

- Prevent file download to unmanaged devices
- Audit external sharing

So, in the end take your time to step through all the options in the settings of the tele-conferencing system you may already have or are thinking of using. Make sure that you are using software that provides encryption by default. For video conferencing encryption is done by your video conferencing software provider. Use secure and encrypted video, audio, presentation (media) and call setup (signaling) in every call end to end.

Home is not the office or your institution and it needs significant assistance to adapt. Setting up right security configurations for your environment is an important task to undertake in order to ensure secure communication for Teleworking.

Make Your Choice…

Stay Safe- and Secure!