NITA UGANDA
- Driving the IT Revolution -

national cert.ug

MINISTRY OF ICT & NATIONAL GUIDANCE
A Knowledge and Productive Society driven by ICT & National Ideology

How to use Zoom securely

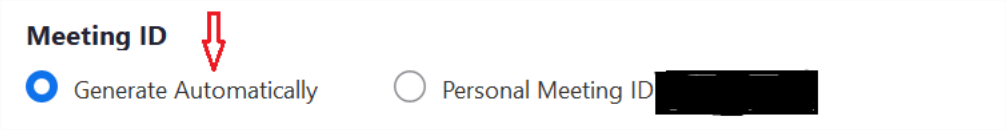
1. Always keep your software up to date

Vulnerabilities in applications are fixed through releasing newer versions of the applications. Therefore always make sure you keep your version of the Zoom application up to date to lower your risk of compromise.

Open zoom desktop App. ***Click*** on the ***down arrow*** to the right of your username. From the ***drop down*** menu click on ***Check for updates***. Download the latest version and then re-open zoom.

2. Never share your personal meeting ID

Do not use a Personal Meeting ID but rather allow Zoom to generate a random ID for each meeting. When scheduling a meeting, chose the ‘Generate Automatically’ option under the ***Meeting ID*** feature.



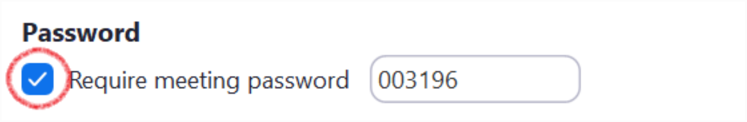
Meeting ID

● Generate Automatically ○ Personal Meeting ID [redacted]

A personal Meeting ID is unique to each user account and as such can be used by adversaries during targeted attacks.

3. Always use passwords to protect your meeting

Always set a password for each new meeting, never embed the password in the meeting link and always require password for participants joining by phone. Activate use of this by ticking the ‘Require meeting password’ option under the ***Password feature*** when scheduling your next meeting.



Password

☑ Require meeting password 003196

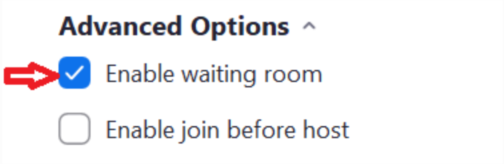
Kindly note the generated password as this will have to be securely shared with all meeting participants. If a meeting is not being password protected, then uninvited guests can intrude such meeting or chat.

4. Always share the meeting details securely

Never share meeting details like meeting links, or meeting ID, or meeting password, or pictures of your zoom meeting on public platforms like websites or on social media such as twitter or Facebook. Once the meeting link has been generated, share the link by **email** only with the people you are inviting. In addition, avoid taking pictures of active zoom meetings and posting them online since this will reveal information about the meeting.

5. Always use a meeting waiting room

The waiting room allows the host to screen everyone entering the meeting to ensure no one uninvited can get in. Find this feature under the advanced options when scheduling your next meeting. To make use of this feature, tick the ‘enable waiting room’ option.



Advanced Options ^

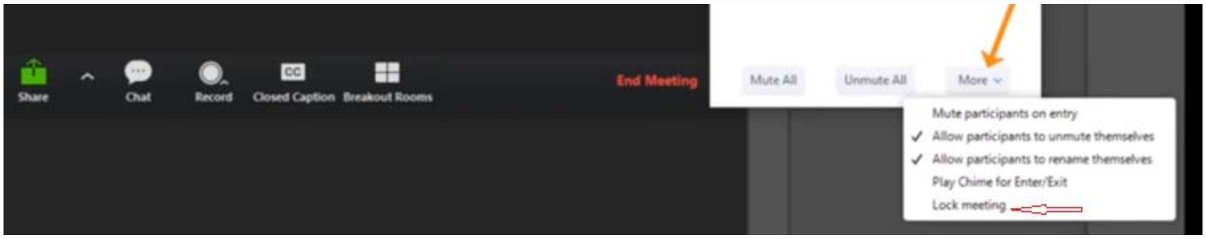
☑ Enable waiting room

□ Enable join before host

6. Always lock the meeting to restrict joining

The meeting host should always lock the meeting once all participants have joined so no new participants can join the meeting even if they have the meeting ID and password.

While in the meeting, click ***Participants*** at the bottom of your Zoom window. In the Participants ***pop-up box***, click more from where you will see the ***Lock Meeting*** option.



Mute participants on entry

✓ Allow participants to unmute themselves

✓ Allow participants to rename themselves

Play Chime for Enter/Exit

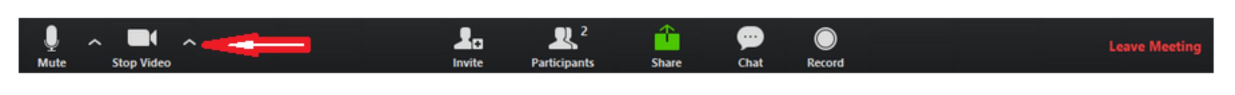
Lock meeting

7. Beware of phishing

Always be careful when clicking on any meeting invite links to avoid being led to a malicious site to download malware or enter details. Always copy the meeting ID from the link provided and enter it in the official application to join. You can as well hover your mouse over the meeting to make sure the link includes the zoom.us domain within it.

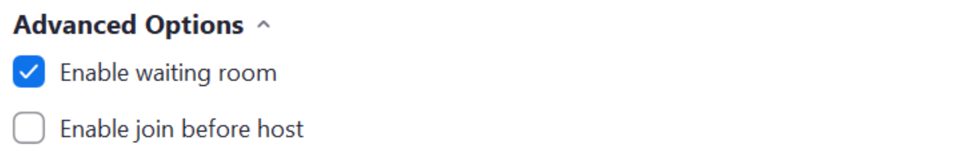
8. Quality of service

If you experience poor quality of service during a meeting, like glitches or breakage in service, then most likely your internet connection is not good. Kindly turn off video and proceed with a voice only meeting. Voice only meeting is better when the number of users are many and when the quality of internet connection isn't good. To turn off your video during a meeting, make use of your controls that appear at the bottom left of your screen.



9. Disable join before host

Participants cannot join the meeting before the meeting host joins and they will see a pop up that says, "The meeting is waiting for the host to join". To use this option, make sure the 'enable join before host' is un-checked under the Advanced options when scheduling the meeting.



Advanced Options ^

☑ Enable waiting room

□ Enable join before host

10. Limit Screen Sharing to the Host

Allow only the host to share content during meetings. This is preventing any unwanted content to be shown during a meeting. You can change this if you need to allow other attendees to share their screens.

- Click the up-arrow next to Share Screen.
- Select Advanced Sharing Options.
- Under Who can share, click Only Host.

10. Enable only authenticated users to join

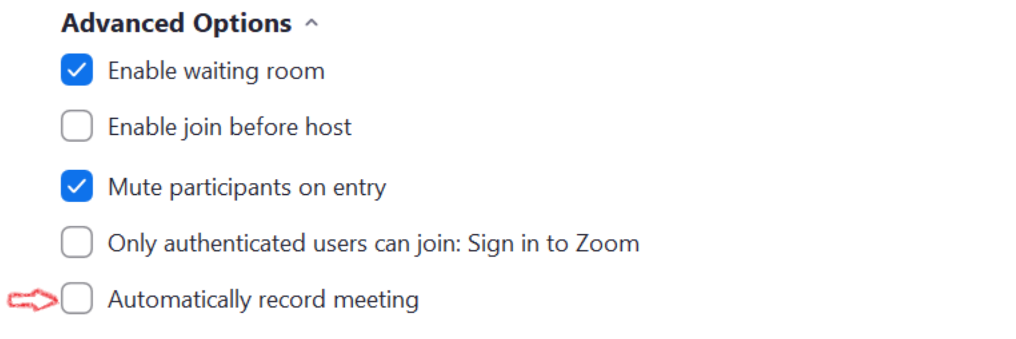
Only participants who have signed into their Zoom account can access this particular meeting. Only authenticated users can join meetings. Controls what type of users can join Zoom meetings. **Note:** Do not use this feature if you intend to host participants who don't have Zoom accounts.

11. Require registration

Allows you to have your participants register with their e-mail, name, other questions, and custom questions. This will help you evaluate who's attending. **Note:** The participants should have Zoom accounts

12. Disable Automatic Recording of Meetings

We recommend all meeting host not to record zoom meetings. Minutes should be taken by the meeting secretary as is the normal practice. When scheduling a meeting, make sure the 'Automatically record meeting' option is unchecked under the Advanced Options.



Advanced Options ^

☑ Enable waiting room

□ Enable join before host

☑ Mute participants on entry

□ Only authenticated users can join: Sign in to Zoom

□ Automatically record meeting

For more information including any suspicious activities, please contact us via security@nita.go.ug