Set up and use Zoom in a more secure way

Minimum settings for administrators configuring Zoom for COVID-19 response teams

From: **Cabinet Office** and **Government Digital Service**
Date: **2 April 2020**

GDS guidance, based on consultations with GSG and the NCSC, is that Zoom may be used at OFFICIAL for cross-government COVID-19 meetings. Administrators should use this guidance to set up Zoom in a more secure way for that purpose and to provide end users (including meeting hosts and participants) with information on how to use it.

Zoom should not be used where existing videoconferencing services (e.g. Hangouts or Teams) would work instead. Further guidance on which tools to use, and how to use them, is currently being worked on by GDS, GSG and the NCSC.

This is a recommended baseline configuration to set up the Zoom video conference tool, aimed at keeping information as secure as possible and providing users with flexibility. Your organisation's configuration may vary depending on user needs and your current technology estate.

Make sure you share important security messages and information about how to use Zoom with your end users.

End users must only use Zoom to share OFFICIAL information which is not of a particularly sensitive nature and which could not be of use to UK adversaries or cause significant harm. Zoom is not suitable for information at SECRET or above.

Use a paid-for account

You should tell your users to only host a Zoom meeting with a paid-for Pro or Business account. Never host a Zoom meeting from a free account.

Participants in meetings do not have to use a paid account to dial into a Zoom meeting, but if they want to host a meeting then they must use a Pro or Business account.

Sign-in settings

We recommend turning on Single Sign On (SSO) if your organisation has a single identity provider and only users within your organisation will be hosting Zoom meetings. To use SSO you'll need to sign up to a paid plan with more than 10 hosts such as Business or Education.

If you need to use Zoom across several identity providers, or it's too hard to get SSO working, we recommend you disable this setting and follow NCSC guidance for good authentication.

Sign-in setup options	Admin settings to use
Allow users to sign in with Google	On (only allow if you use G Suite within your organisation and only allow users to sign in with their work Google account)

Allow users to sign in with Facebook	Off

Security settings

Security setup options	Admin settings to use
Only account admins can change users' name, profile picture, sign-in email, and host key	On
Name (first name and last name)	On
Profile picture	On
Sign-in email	On
Host key	On
Only account admins can change pro users' Personal Meeting ID and Personal Link Name	On
Personal Meeting ID	On
Personal Link Name	On
Allow importing of photos from the photo library on the user's device	Off
Hide billing information from administrators	On
Users need to sign in again after a period of inactivity	Off
User need to input Host Key to claim host role with the length of X digital number	6
Sign in with Two-Factor Authentication (2FA)	On (If using SSO set it to Off)

Authentication settings

Authentication setup options	Admin settings to use
Minimum of 8 characters	On
Cannot contain only one character (e.g. "111111" or "aaaaaa")	On

Cannot contain only consecutive characters (e.g. "123456" or "abcdef")	On
Have at least 1 letter (a, b, c...)	On
Have at least 1 number (1, 2, 3...)	On
Include both Upper case and Lower case characters	On
Have a minimum password length	12
Have at least 1 special character (!, @, #...)	Off
New users need to change their passwords upon first sign-in	Off
Password expires automatically and needs to be changed after the specified number of days	Off
Users cannot reuse any password used in the previous X number of times	On, default is 3
Users can change their password a maximum number of times every 24 hours	Off

Integration settings

You should disable integration with marketplace apps and tools including Google (Calendar, Drive, Gmail), Dropbox, Microsoft Office 365 and OneDrive.

If you are using multiple tools and want to create integrations between them, you need to understand the security of your ecosystem, manage privacy considerations and monitor cookie behaviour of 3rd-party tools.

Meeting settings

Administrators can configure settings and then choose to ‘Lock’ or ‘Unlock’ settings depending on end user needs.

Meeting setup options	Admin settings to use
Host Video	Off (leave setting unlocked for meeting host)
Participants video	Off (leave setting unlocked for meeting host)
Audio Type	Telephone and Computer Audio (leave setting

	unlocked for meeting host)
Join before host	Off (Lock setting for meeting host)
Use Personal Meeting ID (PMI) when scheduling a meeting	Off
Only authenticated users can join meetings	Off (Lock setting for meeting host)
Add watermark	Off (Lock setting for meeting host)
Add audio watermark	Off (leave setting unlocked for meeting host)
Always display "Zoom Meeting" as the meeting topic	Off (leave setting unlocked for meeting host)
Require a password when scheduling new meetings	On (Lock setting for meeting host)
Require a password for meetings which have already been scheduled	Unticked
Require a password for instant meetings	On (Lock setting for meeting host)
Require a password for Personal Meeting ID (PMI)	Off (Leave unlocked for meeting host)
Require a password for Room Meeting ID (applicable for Zoom Rooms only)	Off (Leave unlocked for meeting host)
Embed password in meeting link for one-click join	Off (Leave unlocked for meeting host)
Require password for participants joining by phone	On (Lock setting for meeting host)
Bypass the password when joining meetings from meeting list	Off (Lock setting for meeting host)
Mute participants upon entry	Off (Leave setting unlocked for meeting host)
Calendar and Contact Integration	Off (Lock setting for meeting host) unless you have a use case for it. This could allow Zoom to access your users calendars and contacts which may require further security consideration
Office 365 users can consent to enterprise applications accessing company data on their behalf	Off
Upcoming meeting reminder	On (Leave setting unlocked for meeting host)
Enforce to use OAuth 2.0 only for authenticate Office365 calendar integration	Off
Require Encryption for 3rd Party Endpoints (H.323/SIP)	On (Leave setting unlocked for meeting host). Zoom supports Cisco, Polycom, Lifesize and other H.323/SIP endpoints.
Chat	On (Leave setting unlocked for meeting host)
Prevent Participants from Saving Chat	On (Lock setting for meeting host)

Private chat	Off (Leave setting unlocked for meeting host)
Auto saving chats	Off (Lock setting for meeting host)
Play sound when participants join or leave	On (Lock setting for meeting host and select “Heard by host and all attendees”)
When each participant joins by telephone, record and play their own voice	Ticked
File transfer	Off unless you have use cases for it. This could allow your users to share and store documents on Zoom which may require further security, data protection and information governance considerations. (Lock setting for meeting host)
Feedback to Zoom	Off (Lock setting for meeting host)
Display end-of-meeting experience feedback survey	Off (Lock setting for meeting host)
Co-host	Off (Leave unlocked for meeting host)
Polling	Off (Leave unlocked for meeting host)
Allow host to put attendee on hold	Off (Leave setting unlocked for meeting host)
Always show meeting control toolbar	On (Leave unlocked for meeting host)
Show Zoom windows during screen share	Off (Leave unlocked for meeting host)
Screen sharing	On (Leave unlocked for meeting host)
Who can share?	Select “All participants”
Who can start sharing when someone else is sharing?	Select “Host only”
Disable desktop/screen share for users	Off (Leave setting unlocked for meeting host)
Annotation	On (Leave setting unlocked for meeting host)
Whiteboard	On (Leave setting unlocked for meeting host)
Auto save whiteboard content when sharing is stopped	Unticked
Remote control	Off (Lock setting for meeting host)
Nonverbal feedback	On (Lock setting for meeting host)
Allow removed participants to rejoin	Off (Lock setting for meeting host)
Breakout room	Off (Leave setting unlocked for meeting host)
Remote support	Off unless you have a strong use case why remote control of other devices through Zoom is required (Lock setting for meeting host)

Closed captioning	Off (Lock setting for meeting host)
Save Captions	Off (Lock setting for meeting host)
Far end camera control	Off (Lock setting for meeting host)
Group HD video	On (Leave setting unlocked for meeting host)
Virtual background	On (Leave setting unlocked for meeting host)
Identify guest participants in the meeting/webinar	On (Lock setting for meeting host)
Auto-answer group in chat	Off (Lock setting for meeting host)
Peer to Peer connection while only 2 people in a meeting	On
Listening ports range	Unticked
Only show default email when sending email invites	Off (Lock setting for meeting host)
Use HTML format email for Outlook plugin	Off (Lock setting for meeting host)
DSCP marking	Off (Lock setting for meeting host)
Allow users to select stereo audio in their client settings	Off (Leave setting unlocked for meeting host)
Allow users to select original sound in their client settings	Off (Leave setting unlocked for meeting host)
Attention tracking	Off (Lock setting for meeting host)
Waiting room	On for All Participants (Leave setting unlocked for meeting host)
Show a "Join from your browser" link	On (Lock setting for meeting host)
Allow live streaming meetings	On (Leave setting unlocked for meeting host)
Allow Skype for Business (Lync) client to join a Zoom meeting	On
When a cloud recording is available	Off (Lock setting for meeting host)
When attendees join meeting before host	On (Leave setting unlocked for meeting host)
When a meeting is cancelled	On (Leave setting unlocked for meeting host)
When host licenses are running low	On - notify at 80% licenses
When an alternative host is set or removed from a meeting	On (Leave setting unlocked for meeting host)
When someone scheduled a meeting for a host	On (Leave setting unlocked for meeting host)
When the cloud recording is going to be permanently deleted from trash	Off (Lock setting for meeting host)

When the meeting duration exceeds the limit	Off
Blur snapshot on iOS task switcher	Off (Leave setting unlocked for meeting host)
Display meetings scheduled for others	Off
Use content delivery network (CDN)	On (select Default option)
Allow users to contact Zoom's Support via Chat	On
Show one person meetings on Dashboard and Reports	Off

Recording settings

Session video recording offers the ability to replay what was said for sharing or audit purposes. You must consider privacy and information management implications, and speak to your privacy/data protection teams before enabling video recording. In some cases consent forms and an update to your privacy notices could be necessary.

You must not record conferences by default. Where session video recording is required to be enabled, this must be authorised by the Data Protection/Privacy Officer and only ‘cloud recording’ is recommended.

Recording setup options	Admin settings to use
Local recording	Off (Lock setting for meeting host)
Cloud recording	On (Leave unlocked for meeting host)
Automatic recording	Off (Lock setting for meeting host)
Prevent hosts from accessing their cloud recordings	On (Lock setting for meeting host)
Cloud recording downloads	Off (Lock setting for meeting host)
IP Address Access Control	Off (Lock setting for meeting host)
Only authenticated users can view cloud recordings	On (Lock setting for meeting host)
Authentication Options	Refer to guidance above for when to enable SSO authentication.
Require password to access shared cloud recordings	On (Lock setting for meeting host)
Require a password to access the existing cloud recordings	Unticked (as recordings disallowed)

The host can delete cloud recordings	On (Lock setting for meeting host)
Auto delete cloud recordings after days	Off (Lock setting for meeting host)
Allow recovery of deleted cloud recordings from Trash	On
Recording disclaimer	On (Lock setting for meeting host)
Ask participants for consent when a recording starts	Ticked
Ask host to confirm before starting a recording	Ticked
Multiple audio notifications of recorded meeting	Off (Lock setting for meeting host)

Telephone settings

Telephone setup options	Admin settings to use
Toll Call	On (Lock for meeting host)
3rd Party Audio	Off (Leave unlocked for meeting host)
Mask phone number in the participant list	On (Lock for meeting host)
Global Dial-in Countries/Regions	No Option

Using the Zoom client applications

Zoom conferences can be joined through a modern web browser, a SIP/H.323 client (if enabled) or Zoom client applications. You should encourage users to join a Zoom conference without signing in on their device. This can reduce the number of Zoom licenses your organisation needs.

Users should only use the free version to join meetings. If a user needs to host a meeting then they should use an existing solution or, if this is not fit for purpose, then a license would need to be purchased for the user.

Use of the browser version of Zoom, not the mobile application, should be encouraged as far as possible.

When deploying Zoom via client applications, make sure you configure devices to either block or allow content from Zoom (such as contacts, calendars or file sharing) in line with your organisational policy. Tools/methods that help you do this include:

- Unified Endpoint Management (UEM)

- Mobile Device Management (MDM)
- Mobile Application Management (MAM)
- Microsoft Group Policy Objects (GPO)

Do not deploy Zoom client applications without enterprise management.

Zoom client applications do not currently support 2FA and will allow the user to authenticate with only a username and password even if 2FA is enabled. Using SSO is strongly recommended.

Security messages for end-users

To make sure that Zoom is used properly by end users you must share important security messages within your organisation. You must tell users to:

- use a strong and separate password for Zoom accounts (this may not apply where your organisation is using single sign-on)
- only use Zoom for OFFICIAL information, it is not suitable for SECRET or above
- use your name or role, not your e-mail address or other identifying info, when you log into Zoom (your name can be changed by right-clicking on your ID in the Participants panel and clicking “Rename”)
- not join sensitive video and audio conferences in public
- check you’ve sent meeting invitations to the right participants
- check that only verified people ask to join or have join a meeting
- monitor attendance throughout the meeting
- make sure all participants use their real names or applicable role title
- use the waiting room features to control access to meetings wherever possible
- be careful if when sharing screens (making sure your email, open documents are not shared)
- stop any meetings to check who is present if unknown participants have joined
- send participants back to a waiting room during the meeting until any identity concerns are resolved
- tailor content to your audience, especially when attendees include external parties who may not have non-disclosure agreements and could make information public

Helping users get started with Zoom

These guides from Zoom may help your users use the tool effectively and safely. The guides required may vary based on the Zoom features you have enabled or disabled. You should provide end users with links to help them:

- access Zoom from a desktop
- access Zoom from a mobile device
- join a meeting by phone
- create an instant meeting
- create a waiting room
- schedule a meeting
- test audio

- test video
- share screens