zoom

February 2022

Security Onboarding Guide

Today’s cybersecurity landscape is more complex than ever before. Businesses are hoping to implement and scale new ways of working while building a flexible yet effective security strategy. That’s why we’ve created the entire Zoom platform with security, privacy, and compliance in mind.

From Zoom Meetings to Zoom Rooms to Zoom Events, we continuously update and improve our products to help protect and support our customers.

In this guide, you’ll find a list of handy features, tips and tricks, and do’s and don’ts to help you secure your meeting, phone call, event, and more.

Zoom Meetings

We're honored that millions of people around the world use Zoom Meetings to collaborate and stay connected. However, without precautions, meetings that are designed to bring people together could be attended by a person who is not invited.

Disruptions typically occur when meeting information is made open to the public. A user could post a private meeting link on social media, share their virtual classroom information, and more. But when these links are out on social media or other public forums, that makes your meeting completely public and anyone with the link can join it.

Here are a few easy ways you can help prevent meeting disruptions:

Use the right Zoom solution for your need: If you're specifically hoping to use Zoom to host a virtual event with people you may not know, make sure to steer your attention from Zoom Meetings to Zoom Webinar or Zoom Events — products designed specifically for digital events.

Avoid using your Personal Meeting ID (PMI): Your PMI is basically one continuous meeting and you don't want outsiders crashing your personal virtual space after your designated meeting is over.

Manage screen sharing: Don't let attendees in your public session take control of the screen and share unwanted content with the group. You can restrict this — before the meeting and during the meeting in the host control bar — so that you're the only one who can screen share. If you disable screen sharing, the Whiteboard setting will be automatically disabled as well.

Manage your participants

Allow only signed-in users to join: If someone tries to join your meeting and isn't logged into Zoom with the email they were invited through, they will receive a message that says, "This meeting is for authorized attendees only." This is useful if you want to control your guest list and invite only those you want at your meeting — other students at your school or colleagues, for example.

Lock the meeting: It's always smart to lock your front door, even when you're inside the house. When you lock a Zoom Meeting that's already started, no new participants can join, even if they have the meeting ID and passcode. Just click the Security icon at the bottom of your Zoom window. In the pop-up, click the button that says Lock Meeting.

Remove unwanted or disruptive participants: You can remove someone from your meeting by using the Security icon or Participants menu. On the Participants menu, you can mouse over a participant's name and several options will appear, including Remove. Click that to kick someone out of the meeting. When you do remove someone, they can't rejoin the meeting. But you can toggle your settings to allow removed participants to rejoin in case you boot the wrong person.

Disable video: Hosts can turn off a participant's video. This will allow hosts to block unwanted, distracting, or inappropriate gestures on video.

Mute participants: Hosts can mute/unmute individual participants or all of them at once. Hosts can block unwanted or distracting noise from other participants. You can also enable "Mute Upon Entry" in your settings to keep the clamor at bay in large meetings.

Suspend participant activities: Hosts and co-hosts can pause the meeting to remove and report an offending party and prevent further disruption. Click the Security icon and select "Suspend Participant Activities" to temporarily halt all video, audio, in-meeting chat, annotation, screen sharing, and recording, and end Breakout Rooms. You can resume the meeting by re-enabling the individual features.

Turn off file transfer: In-meeting file transfer allows people to share files through the in-meeting chat. Toggle this off to keep the chat from getting bombarded with unsolicited pics, GIFs, memes, and other content.

Turn off annotation: You and your attendees can doodle and mark up content together using annotations during a screen share. You can disable the annotation feature in your Zoom settings to prevent people from writing all over the screens.

Disable private chat: Zoom has in-meeting chat, which participants can use to message the entire group or each other privately. You can restrict participants' ability to chat amongst one another while your meeting is going on and cut back on distractions. Click "Chat" in the meeting controls, then at the bottom of the in-meeting Zoom Group Chat window click the three dots. From there you can toggle on options for who can chat with who in your meeting.

Report a user: Hosts can report users to Zoom's Trust & Safety team, who will review any potential misuse of the platform and take appropriate action. Find this option within our Security icon or under the green shield icon in the top left corner of your meeting, where you can attach screenshots and other documentation as needed.

Enable the Waiting Room

The Waiting Room is an important feature for securing a Zoom Meeting. Just like it sounds, the Waiting Room is a virtual staging area that stops your guests from joining until you're ready for them. It's almost like the velvet rope outside a nightclub, with you as the bouncer carefully monitoring who gets let in.

Meeting hosts can customize Waiting Room settings for additional control, and you can even personalize the message people see when they hit the Waiting Room so they know they're in the right spot. This message is really a great spot to post any rules/guidelines for your event, like who it's intended for.

Zoom Chat

Zoom Chat comes included with your Zoom license and is an efficient way to quickly communicate with people in or out of your organization.

Here are a few key pointers for additional security when using Zoom Chat:

Advanced chat encryption: This feature allows for a secured communication where only the intended recipient can read the secured message. When advanced chat encryption is enabled, data at rest is encrypted by keys generated and operated on chat participants' devices. Chat data in transit, however, is encrypted in transit using Transport Layer Security (TLS) encryption.

External contact management: Account owners and admins can enable or disable the ability for users to chat with or add external contacts. When the feature is enabled, users can add external Zoom users as a contact by specifying their email address. After the external user approves the contact request, internal users will be able to chat, share images and files, and meet instantly. Admins can view and remove all external contacts.

Zoom Webinar

Our Zoom Webinar solution comes with security controls that are designed to help hosts and co-hosts manage and safeguard the experience while maximizing the potential of their session.

Here are few key ways you can help secure your webinars:

Turn off chat for attendees: To prevent side chatter or unwarranted commentary during your webinar, you can disable the chat feature for all participants. If the host has disabled attendee chat, the host and other panelists can still chat among themselves. You can disable chat in your account settings or during the webinar.

Control the Q&A: The Q&A feature allows attendees to ask questions during the webinar, and for the panelists, co-hosts, and host to answer them. To help manage the Q&A function from potentially being abused by an attendee, disable "Allow attendees to view" in the Q&A section of your "Webinars" panel in the Zoom web portal. That way, attendees will only be able to view the questions that hosts and panelists have chosen to answer.

Remove the anonymous feature: In the Q&A tab in your settings, turn off "Allow anonymous questions" to disable anonymous submissions. By removing this option, participants won't be able to send questions without providing their name to the host, co-host, and panelists.

Require a passcode: Webinar hosts can require passcodes for an added layer of security. Passcodes can be enabled in account settings, and attendees will need the passcode to access the webinar.

Manage your panelists and participants: You can manage both panelists and attendees in your webinar via the host controls:

- **Panelists:** Hosts can mute/ask to unmute, put on hold, or remove panelists. You can also promote a panelist to co-host or change their role to attendee.
- **Attendees:** Hosts can lower attendees' raised hands, as well as rename or remove the attendee. They can also promote an attendee to be a panelist, which means they'll be able to appear on video and audio so other audience members can see and hear them.

Lock the webinar: Once the intended audience has joined your webinar, you can prevent any new panelists or attendees from joining the session by locking it via the host controls. Once a webinar is locked, no new attendees or panelists will be able to join unless you unlock it.

Set up authentication for your webinar: Admins can enable authentication profiles to require webinar attendees to be logged into their Zoom account to join a session. You can further limit access to Zoom users whose email address matches a certain domain or prevent users in specific domains from joining meetings or webinars. This feature, which is implemented at the account level, can be useful if you want to restrict your participant list to verified users or users from a certain organization, such as for an internal all-hands.

Zoom Rooms

Zoom Rooms are reinforced through a hardware partner security evaluation process, our 256-bit AES-GCM encryption, and a robust set of security features. Similar to Zoom Meetings, these Zoom Rooms features are designed to protect user and meeting privacy, as well as promote the seamless Zoom experience.

To tailor Zoom Rooms' security features to your needs and lock down your conference room meeting, here are a few do's and don'ts you should follow:

Do

Leverage the Security icon: Whenever you start a meeting in your Zoom Room, a Security icon will be available at the bottom of your screen or on your Zoom Rooms Controller. Use this icon to take safety measures, with options such as "Lock Meeting," "Suspend Participant Activities," and more.

Hide host and ID from private meetings: This is a setting admins can enable in the Zoom Rooms account settings when they want to keep the meeting host and meeting ID, in addition to the meeting topic, hidden from the Zoom Rooms display for private meetings.

Send whiteboard to internal contacts only: Zoom Rooms for Touch whiteboards can be restricted to only allow sharing with internal users. This option can be enabled account-wide or at the device level by account administrators.

Require encryption for third-party endpoints: Zoom offers a setting to require encryption for H323/SIP third-party endpoints, a setting that can be enabled by the host of a meeting or by an admin for all users and accounts. If this setting is selected, those dialing in via SIP/H.323 will be required to use encryption when dialing into the Zoom meeting.

Enable a passcode to exit the Zoom Rooms application and alter settings: Admins can enable a Room Passcode for Zoom Rooms, which requires a 1-16 digit numeric lock code. This helps prevent users from making setting changes on the Zoom Room controller or closing the Zoom Room application on the computer. Be sure to change the passcode from the default one.

Don't

Show the sharing key on-screen in public spaces: A sharing key is just one of the ways participants can connect to a Zoom Room to share content. If an outsider gets ahold of a key, they could potentially share unwanted content in the meeting — so remain vigilant about displaying sharing keys in public spaces.

Automatically accept incoming camera control: Be sure to carefully analyze any incoming requests for camera control, as allowing an outside party to control your camera could lead to potential meeting disruptions.

Automatically start scheduled meetings: Admins can configure all the Zoom Rooms in an account to automatically start or stop based on calendars. If you share a conference space with others or another party has access to your conference room, you want to disable this feature to prevent any unwarranted access to your calls.

Use Room Meeting ID when starting an instant meeting: All Zoom Rooms are automatically assigned a Room Meeting ID. If you share the Room Meeting ID for an instant meeting, anyone with the number could potentially join any meeting that's using that ID in the future.

Zoom Events

Zoom Events provides everything you need to confidently build, host, and manage a virtual or hybrid event, whether it's a large sales meeting, unique customer experience, internal event, trade show, or corporate summit.

For users hoping to create a safe and engaging event experience using Zoom, our Zoom Events solution has a few key security features you should know about.

Here are a few ways Zoom Events works to help protect your online event experience:

Unique ticket creation: Zoom Events generates a unique ticket to speakers and each person who registers for an event to help maintain accurate attendance. In order to join an event, the attendee has to be logged in to Zoom with the same account they used to register.

No unregistered users: Every attendee has to sign up for Zoom to join a Zoom Event, which helps reduce the potential for uninvited guests. Users do not need a paid account to attend.

User authentication: Attendees have to be authenticated by the Zoom website and the Zoom client to be able to join an event.

Be consistent with updates: To use Zoom Events, users mus t be on the latest version of the Zoom client to help reinforce events with any recent fixes and feature updates.

Event visibility: Events can be configured as 'viewable' to anyone with the session URL, or internal to users within your Zoom account.

Restricted guest list: Hosts can set up private events for a limited guest list or restrict users from specific domains.

Optional event lobby: Hosts can create an optional "lobby" where attendees can interact and network. While a great way to foster connection, the event lobby feature can be turned off if desired.

Registration summary: Within the Zoom Events interface, you can easily track the tickets sold to see who has registered for your event.

Individual sessions on Zoom Events can be held with Zoom Meetings or Zoom Webinar. For security tips and recommendations on both of these solutions, check out the corresponding sections within this guide.

Zoom Phone

Zoom Phone is a modern cloud phone solution natively built for the Zoom platform. Seamless and secure, Zoom Phone streamlines the telecommunications experience with enterprise-class features, many of which are designed to help users manage and safeguard their cloud calling experience.

Here are a few key features that help weave security into the Zoom Phone experience:

Encryption:

- **256-bit AES-GCM encryption:** We use 256-bit AES-GCM encryption as our standard for real-time content and media, which applies to data in transit across Zoom Meetings and Chat, Zoom Webinar, meetings occurring via Zoom Rooms, and Zoom Phone data transmitted over the public internet.
- **End-to-end encryption (E2EE) for Zoom Phone (coming soon):** Previously only available in Zoom Meetings, our E2EE offering will be extended to Zoom Phone this year. Zoom Phone users making on-net calls on the Zoom Phone network will have a new option to upgrade to E2EE during one-on-one, intra-account phone calls that occur via the Zoom client.
- **TLS encryption:** During SIP registration, Zoom Phone leverages TLS encryption.

Caller ID masking: Depending on the purpose of the call, users can choose to display their direct number, a main office number, a call queue number, or no number as the outbound caller ID. This feature helps support the privacy and security of employees' personal contact information.

Private network peering: Zoom Phone is optimized for secure internet traversal. For additional traversal considerations, Zoom has established direct private network peering links between Zoom Phone data centers and Zoom Phone PSTN service provider networks to prioritize data protection.

Toll fraud: Zoom Phone utilizes access control and automated detection capabilities in order to detect irregular calling patterns to help prevent toll fraud. If irregularities are detected, our security department will notify users of potential fraudulent activities.

Calling block lists: Customizable global and personal block lists enable Zoom Phone users and administrators to easily add and manage blocked phone numbers.

Security at Zoom

We're dedicated to providing a seamless and secure experience for our users, empowering them to safely exchange and store valuable information via our platform.

As we continue to evolve our solutions, security and privacy will guide any new updates we make. We're committed to being a platform users can trust — with their online interactions, information, and business.

To learn more about Zoom's approach to security, explore our Trust Center, a one-stop shop containing our privacy, safety, and security resources.