# Security Guide

Zoom Video Communications, Inc.

Zoom helps businesses and organizations bring their teams together in a frictionless environment to get more done. Our easy, reliable cloud platform for video, voice, content sharing, and chat runs across mobile devices, desktops, telephones, and room systems.

Zoom places security as the highest priority in the operations of its suite of products and services. Zoom strives to continually provide a robust set of security features and practices to meet the requirements of businesses for safe and secure collaboration.

The purpose of this document is to provide information on the security features and functions that are available with Zoom. The reader of this document is assumed to be familiar with Zoom functionalities related to meetings, webinars, chat, file sharing, and voice calling.

Unless otherwise noted, the security features in this document apply across the product suite of Zoom Meetings, Zoom Video Webinars, Zoom Rooms, and Zoom Voice, across supported mobile, tablet, desktop, laptop, and SIP/H.323 room system endpoints.

## Infrastructure

The Zoom cloud is a proprietary global network that has been built from the ground up to provide quality communication experiences. Zoom operates in a scalable hybrid mode; web services providing such functions as meeting setup, user management, conference recordings, chat transcripts, and voice mail recordings are hosted in the cloud, while real time conference media is processed in globally distributed tier-1 colocation data centers with SSAE 16 SOC 2 Type 2 certifications.

### Realtime Media Processing

A distributed network of low-latency multimedia software routers connects Zoom's communications infrastructure. With these multimedia routers, all session data originating from the host's device and arriving at the participants' devices is dynamically routed between endpoints. Zoom real-time sessions operate analogously to the popular mobile conversation over the public mobile network.

April 2020

### Firewall Compatibility

During session setup, the Zoom client connects via HTTPS (port 443/TLS) to Zoom servers to obtain information required for connecting to the applicable meeting or webinar, and to assess the current network environment such as the appropriate multimedia router to use, which ports are open and whether an SSL proxy is used. With this metadata, the Zoom client will determine the best method for real time communication, attempting to connect automatically using preferred udp and tcp ports 8801, 8802, and 8804. For increased compatibility and support of enterprise SSL proxies, connection can also be made via HTTPS (port 443/TLS). An HTTPS connection is also established for users connecting to a meeting via the Zoom web browser client.

## Client Application

### Role-based user security

The following pre-meeting security capabilities are available to the meeting host:

- Secure log-in using standard username and password or SAML single sign-on
- Start a secured meeting with password
- Schedule a secured meeting with password

**Selective meeting invitation:** The host can selectively invite participants via email, IM, or SMS. This provides greater control over the distribution of the meeting access information. The host can also create the meeting to only allow members from a certain domain email to join.

**Meeting Details Security:** Zoom retains event details pertaining to a session for billing and reporting purposes. The event details are stored at the Zoom secured database and are available to the customer account administrator for review on the customer portal page once they have securely logged-on.

**Application security:** Zoom can encrypt all presentation content at the application layer using the Advanced Encryption Standard (AES) 256-bit algorithm.

**Zoom client group policy controls:** Specifically applicable to the Zoom Meetings client for Windows and Zoom Rooms for Windows, administrators can define a broad set of client configuration settings that are enforced through Active Directory group policy controls.

**E2E Chat Encryption:** Zoom E2E chat encryption allows for a secured communication where only the intended recipient can read the secured message. Zoom uses public and private key to encrypt the chat session with Advanced Encryption Standard (AES-256). Session keys are generated with a device-unique hardware ID to avoid data being read from other devices. This ensures that the session can not be eavesdropped on or tampered with.

## Meeting Security

**Role-based user security**

The following in-meeting security capabilities are available to the meeting host:

- Meetings are encrypted by default
- Waiting Room
- Enable wait for host to join
- Expel a participant or all participants
- End a meeting
- Lock a meeting
- Chat with a participant or all participants
- Mute/unmute a participant or all participants
- Screen share watermarks
- Audio signatures
- Enable/disable a participant or all participants to record
- Temporary pause screen-sharing when a new window is opened

The following in-meeting security capabilities are available to the meeting participants:

- Mute/unmute audio
- Turn on/off video
- Blur snapshot on iOS task switcher

**Host and Client authenticated meeting:** A host is required to authenticate (via https) to the Zoom site with their user credentials (ID and password) to start a meeting. The client authentication process uses a unique per-client, per-session token to confirm the identity of each participant attempting to join a meeting. Each session has a unique set of session parameters that are generated by Zoom. Each authenticated participant must have access to these session parameters in conjunction with the unique session token in order to successfully join the meeting.

**Open or password protected meeting:** The host can require the participants to enter a password before joining the meeting. This provides greater access control and prevents uninvited guests from joining a meeting.

**Edit or delete meeting:** The host can edit or delete an upcoming or previous meeting. This provides greater control over the availability of meetings.

**Host controlled joining meeting:** For greater control of meeting, the host can require participants to only join the meeting after the host has started it. For greater flexibility, the host can allow participants to join before the host. When joining before the host, participants are restricted to a 30-minute meeting.

**In-meeting security:** During the meeting, Zoom delivers real-time, rich-media content securely to each participant within a Zoom meeting. All content shared with the participants in a meeting is only a representation of the original data. This content is encoded and optimized for sharing using a secured implementation as follows:

- Is the only means possible to join a Zoom meeting
- Is entirely dependent upon connections established on a session-by-session basis
- Performs a proprietary process that encodes all shared data
- Can encrypt all screen sharing content using the AES 256 encryption standard
- Can encrypt the network connection to Zoom using 256-bit TLS encryption standard
- Provides a visual identification of every participant in the meeting

**Host controlled joining meeting**

Authentication methods include single sign-on (SSO) with SAML or OAuth.

With SSO, a user logs-in once and gains access to multiple applications without being prompted to log-in again at each of them. Zoom supports SAML 2.0 which enables web-based authentication and authorization including SSO. SAML 2.0 is an XML-based protocol that uses security tokens containing assertions to pass information about a user between a SAML authority (an identity provider) and a web service (such as Zoom). Zoom works with Exchange ADFS 2.0 as well as enterprise identity management such as Centrify, Fugen, Gluu, Okta, OneLogin, PingOne, Shibboleth, Symplified, and many others. Zoom can map attributes to provision a user to different group with feature controls.

OAuth-based provisioning works with Google or Facebook OAuth for instant provisioning. Zoom also offers an API call to pre-provision users from any database backend.

Additionally, your organization or university can add users to your account automatically with managed domains. Once your managed domain application is approved, all existing and new users with your email address domain will be added to your account.

## Administrative Controls

The following security capabilities are available to the account administrator:

- Secure login options using standard username and password or SAML SSO
- Add user and admin to account
- Upgrade or downgrade user subscription level
- Delete user from account

- Review billing and reports
- Manage account dashboard and cloud recordings

## Special Security Features/Options API

APIs are available for integrating Zoom with custom customer applications and third party applications. Each customer account may include API integration key credentials managed by the customer account admin. API calls are transmitted securely over secure web services and API authentication is required.

### Meeting Connector

Zoom Meeting Connector is a hybrid cloud deployment method, which allows a customer to deploy a Zoom multimedia router (software) within the customer's internal network.

User and meeting metadata are managed in Zoom communications infrastructure, but the meeting itself is hosted in customer's internal network. All real-time meeting traffic including audio, video, and data sharing go through the company's internal network. This leverages your existing network security setup to protect your meeting traffic.

When customers choose a hybrid deployment, they have the option to segment by type of user where Pro and Free (Basic) user types will use the cloud, and Business and Enterprise user types will use the on-premise.

If on-premise is offline, the meeting will automatically revert to the cloud. Both our cloud and on-premise solutions are designed with failover and load balancing mechanisms when deployed.

### Zoom Rooms

Zoom Rooms is Zoom's software-based conference room system. It features video and audio conferencing, wireless content sharing, and integrated calendaring running on off-the-shelf hardware. Communications are established using 256-bit TLS encryption and all shared content is encrypted using AES-256 encryption. The Zoom Rooms app is secured with App Lock Code. The App Lock Code for Zoom Rooms is a required 1-16 digit numeric lock code that is use to secure your Zoom Rooms application. This prevents unauthorized changes to your Zoom Rooms application and settings on your accompanying hardware.

### Zoom Chat

Persistent, cross-platform chat is a feature of Zoom Meetings that enables users to chat and share files 1-1 or in groups. Users can click "Meet" from any chat to start an instant Zoom video meeting with the group participants. Chat can be encrypted for HIPAA-compliant settings.

### Zoom Phone

Zoom Phone is a cloud phone system available as an add-on to Zoom's platform. Support for inbound and outbound calling through the public switched telephone network (PSTN) and seamlessly integrated telephony features enable customers to replace their existing PBX solution and consolidate all of their business communication and collaboration requirements into their favorite video platform.

Utilizing standards-based Voice-over-Internet-Protocol (VoIP) to deliver best in class voice services, Zoom Phone delivers a secure and reliable alternative to traditional on-premise PBX solutions. Call setup and in-call features are delivered via Session Initiation Protocol (SIP). While leveraging OPUS as the preferred codec to ensure the highest quality possible, Zoom Phone also supports additional industry standard codecs G.722, G.711, and G.729 for media transcoding.

*Authentication*

- Zoom Phone SIP registration authenticates using AES-128 bit TLS 1.2 encryption

*Media Encryption*

- VoIP media is transported and protected by Secure Real-time Transport Protocol (SRTP) with AES-128 encryption

*Private Network Peering*

- Zoom has established direct private network peering links between Zoom Phone data centers and Zoom Phone PSTN service provider networks to ensure maximum protection.

*Emergency Calling*

- Zoom Phone supports E911 (USA/CAN) enhanced emergency services to provide caller location to the local Public Safety Answering Point (PSAP) as required by law. Originating call location addresses can be defined and assigned at the account and individual user level.
- Emergency calls made from the Zoom mobile app on iOS and Android smartphones will automatically default to the mobile device's native outbound cellular calling feature and bypass the Zoom Phone service to directly route the emergency call to the mobile network operator's PSAP.
- Zoom Phone administrators may optionally choose to automatically intercept and reroute emergency calls to internal response teams.

*Toll Fraud*

- Zoom Phone prevents toll fraud through access control and automated detection capabilities. Our security department actively monitors customers' accounts to detect irregular calling patterns and will notify customers of potential fraudulent activities.

*Calling Black Lists*

- Customizable global and personal black lists allow users and administrators to easily add and manage blocked phone numbers

*Invoking Elevate-to-Meeting feature*

- When elevating a Zoom Phone call to a Zoom Meeting, all available Zoom Meeting security features will then apply to the interaction.

### Zoom Video Webinars

In Zoom Video Webinars, up to 100 video panelists can present with video, audio, and screen sharing with up to 10,000 view-only attendees. These webinars feature registration options, reporting, Q/A, polling, raise hand, attention indicators, and MP4/M4A recording). Zoom Video Webinars can stream to YouTube and Facebook Live to reach an unlimited live audience. Panelists are full participants in the meeting. They can view and send video, screen share, annotate, and so forth. Panelist invitations are sent separately from the Webinar attendees. Webinar contents and screen sharing are secured using AES 256 and communicate over secured network using 256-bit encryption standard.

*Registration Webinar*

- Manually Approve Registration - The host of the Webinar will manually approve or decline whether a registrant receives the information to join the webinar.
- Automatically Approve Registrants - All registrants to the webinar will automatically receive information on how to join the webinar.

*Registration-less Webinar*

- One-Time - Attendees will join the webinar only once. After the webinar ends, attendees will not be able to use the same information to join the Webinar.
- Recurring - Attendees will be able to repeatedly join the same Webinar with the information provided.

### Recording Storage

Zoom offers customers the ability to record and share their meetings, webinars, and Zoom Phone calls. Meetings and Webinar recordings can be stored on the host's local device with the local recording option or Meetings, Webinars, and Zoom Phone calls can be stored in Zoom's cloud with the Cloud Recording option (available to paying customers). Recordings stored locally on the host's device can be encrypted if desired using various free or commercially available tools.

Cloud Recordings are processed and stored in Zoom's cloud after the meeting has ended; these recordings can be password protected or available only to viewers logged in under a certain domain email. The recordings are stored in both video/audio format and audio only format. In-meeting chat messages, shared files and meeting transcripts can be optionally saved to Zoom's cloud, where they are stored encrypted as well. The meeting host can manage their recordings through the secured web interface. Recordings can be downloaded, shared, or deleted. Zoom Phone voicemail recordings are processed and stored in Zoom's cloud and can be managed through the secured Zoom client.

### Zoom Rooms People Counting

Zoom Rooms people counting is a feature that is off by default, but can be turned on by room administrators. This feature allows administrators to view data around number of in-room meeting participants joined from Zoom Rooms.

This feature works by capturing images throughout the duration of the meeting. Images are temporarily stored on the Zoom Rooms local hard-drive and never sent to the cloud. Once the meeting ends, the locally-stored images are used to count the max number of visible in-room meeting participants. Throughout this process, face detection (without ties to personal information) is used to count individuals based on the images captured. Once the images are done being processed to capture the number of people, the images are permanently deleted.

By enabling the participant count feature for Zoom Rooms, you acknowledge your obligation to comply with all laws and that it is your responsibility to ensure that you provide adequate notice to users that this feature is enabled and have gathered appropriate consent from data subjects in compliance with applicable recording and/or privacy regulations for both the collection and storage of this data.

**Privacy**

Zoom only stores basic information under user account profile information:

- Email address
- User password - salted, hashed
- First name
- Last name
- Company name (optional to provide)
- Company phone number (optional to provide)
- Profile picture (optional to provide)

For more information about our privacy policy, visit https://zoom.us/privacy.

**Billing Details**

Zoom leverage a third-party, PCI-compliant partner to process payment and handle all aspects of billing. We do not store any user credit card information or billing information in our database.

## Security and Privacy Certifications

### SOC2:

The SOC 2 report provides third-party assurance that the design of Zoom, and our internal processes and controls, meet the strict audit requirements set forth by the American Institute of Certified Public Accountants (AICPA) standards for security, availability, confidentiality, and privacy. The SOC 2 report is the de facto assurance standard for cloud service providers.

### TRUSTe:

TRUSTe has certified the privacy practices and statement for Zoom and also will act as dispute resolution provider for privacy complaints. Zoom is committed to respecting your privacy. If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third-party dispute resolution provider (free of charge) at https://feedback-form.truste.com/watchdog/request.

### EU-US Privacy Shield:

Zoom participates in and has certified its compliance with the EU-U.S. Privacy Shield Framework. Zoom has committed to subjecting all personal data received from European Union (EU) member countries, in reliance on the Privacy Shield Framework, to the Framework's applicable principles. To learn more about the Privacy Shield Framework, visit the U.S. Department of Commerce's Privacy Shield List https://www.privacyshield.gov/list.

### FedRAMP:

Zoom is authorized to operate under The Federal Risk and Authorization Management Program (FedRAMP), a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services used by federal agencies.

---

*Enterprise businesses, healthcare organizations, and educational institutions around the world use the Zoom platform everyday to connect their teams, grow their organizations, and change the world. Zoom places privacy and security as the highest priority in the lifecycle operations of our communications infrastructure and meeting connector networks. In addition, we strive to continually provide a robust set of security features to achieve our goal of providing the most efficient and secure video-first unified communications.*