Security Guide

White Paper - August 2021

zoom

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 Phone, 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 and commercial cloud data centers with SSAE 16 SOC 2 Type 2 certifications.

Real-time media processing

A distributed network of low-latency multimedia software routers connects Zoom's communications infrastructure. With these Multimedia Routers (MMR), all session data originating from the host's device and arriving at the participants' devices is dynamically routed between endpoints.

Firewall compatibility

During session setup, the Zoom client connects via HTTPS 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. For increased compatibility and support of enterprise SSL proxies, connection can also be made via HTTPS. 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 passcode
- Schedule a secured meeting with passcode

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 email domain 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 real-time media content at the application layer using Advanced Encryption Standard (AES).

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.

Advanced encryption: Advanced chat encryption allows for a secured communication where only the intended recipient can read the secured message.

End-to-end encryption: End-to-end encryption, when enabled, ensures that communication between all meeting participants in a given meeting is encrypted using cryptographic keys known only to the devices of those participants. This ensures that no third party — including Zoom — has access to the meeting's private keys. End-to-end encryption is available as a technical preview to all customers.

Meeting security

Role-based user security

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

- 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 passcode protected meeting: The host can require the participants to enter a passcode 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 meetings, 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.

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
- Encrypts all real-time media (audio, video, screen sharing) using the AES encryption standard
- Encrypts other data using TLS encryption standard
- Provides a visual identification of every participant in the meeting

Authentication

Authentication methods include password, or single sign-on (SSO) with SAML or OAuth. Users authenticating with username and password can also enable two-factor authentication (2FA) as an additional layer of security to sign in.

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 several third-party enterprise identity management solutions. 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 associate users to your account with domains. Once your associated domain application is approved, all existing and new users with your email address domain will be given the choice to 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 (with the option to enable two-factor authentication (2FA) as an added layer of security), or SAML SSO
- Add user and admin to account
- Upgrade or downgrade account 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.

Zoom 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 the customer's internal network. All real-time media 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.

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 TLS encryption and meeting, webinar and messaging content is encrypted using AES encryption. The Zoom Rooms app is

secured with App Lock Code. The App Lock Code for Zoom Rooms is a required 1-16 digit number or characters lock code that is used 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 one-one or in groups. Users can click “Meet” from any chat to start an instant Zoom video meeting with the group participants.

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).

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).

Authentication

- Zoom Phone SIP registration leverages TLS encryption

Real-time media encryption

- VoIP media is transported and protected by Secure Real-Time Transport Protocol (SRTP) with AES 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 utilizes access control and automated detection capabilities to detect irregular calling patterns to help prevent toll fraud. Our security department can then notify customers of potential fraudulent activities.

Calling block lists

- Customizable global and personal block lists enables 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 50,000 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, Facebook and other services 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 within Zoom clients and using RTMPS (TLS) encryption standard when supported by the third-party services.

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 passcode-protected or available only to viewers logged in to the account. The recordings can be 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

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 reports 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 are 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.

Zoom Rooms Voice Commands

You can start a scheduled meeting in a Zoom Room by saying, "Hey Zoom, start meeting." We do not upload or store your voice; it is processed on your local device only. The Zoom Room will listen for commands starting 10 minutes before each scheduled meeting. It ignores your voice beginning when the meeting is started or after 20 minutes.

Privacy

Privacy is an extremely important topic, and we want you to know that at Zoom, we take it very seriously. Here are the facts about user privacy as it relates to Zoom and your use of our services:

- We do not sell your personal data. Whether you are a business or a school or an individual user, we do not sell your data.
- We do not use data we obtain from your use of our services, including your meetings, for any advertising. We do use data we obtain from you when you visit our marketing websites, such as zoom.us. You have control over your own cookie settings when visiting our marketing websites.

For more information about our privacy policy, please see our Privacy Statement, K-12/Primary and Secondary Schools Privacy Statement and California Privacy Rights Statement at https://zoom.us/privacy.

Security & 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.

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.

Zoom Video Communications, Inc. (NASDAQ: ZM) brings teams together to get more done in a frictionless video environment. Our easy, reliable, and innovative video-first unified communications platform provides video meetings, voice, webinars, and chat across desktops, phones, mobile devices, and conference room systems. Zoom helps enterprises create elevated experiences with leading business app integrations and developer tools to create customized workflows. Founded in 2011, Zoom is headquartered in San Jose, California, with offices around the world. Visit zoom.com and follow @zoom.