Understanding encryption in the Zoom Workplace platform

WHITEPAPER

September 2024 | VERSION 01

Table of Contents

Introduction

NOTE

This document provides a compilation of information for common questions regarding encryption related to Zoom's core communications products, including meetings, chat, and phone offerings. This document also does not specifically address other Zoom products or services, including, for example, Zoom Developer Platform, Zoom Apps, Zoom for Government, or other non-referenced product offerings.

All statements are relevant as of the date listed. In our continuing commitment to empowering productivity — while keeping security at the core of our products — the features described in this paper may evolve.

At Zoom, we're committed to protecting the security and privacy of our customers' data throughout Zoom Workplace — Zoom's open collaboration platform with AI Companion that empowers teams to work happy. Our robust solutions can help you enable meaningful collaboration, effective communication, and engaging experiences across your preferred channels. With security threaded throughout each solution, Zoom Workplace consolidates the key aspects of modern communication into one application. It offers an aggregate of robust features and controls — configured by either default or the customer — which are designed to protect your information.

Most prominent are our industry-standard methods of encryption, which underpin our solutions at Zoom. The goal of our encryption design is to provide powerful security features that support the diverse needs of our user base. This paper discusses encryption protocols for the data in transit between the Zoom Workplace app and the Zoom Cloud Platform and the server-side encryption methods the Zoom Cloud Platform employs to secure customer content at rest. Lastly, this paper provides an overview of advanced encryption options, such as additional client-side encryption options, that are available to customers.

Encryption by design

Encryption in transit

The Zoom Workplace app is your home base for accessing Zoom Workplace and is available for multiple operating systems (macOS, Windows, Linux, Android, iOS) and a range of devices (desktop, mobile, web, Zoom Rooms). Whether you use the Zoom Workplace app, join meetings, or access the Zoom web portal via your browser, Zoom Workplace is designed to encrypt customer data **in transit** using trusted methods when communicating with the Zoom web portal or services in the Zoom Cloud Platform.

By default for connections other than real-time media, the Zoom Workplace app uses HTTPS over, at a minimum, Transport Layer Security (TLS) 1.2 encryption with Public Key Infrastructure (PKI) certificates issued by a trusted commercial certificate authority. This is an industry-standard encryption method widely used across the internet. For real-time media (video, audio, and in-meeting shared content such as desktop sharing and in-meeting chat and file sharing) for Zoom Meetings, we use 256-bit Advanced Encryption Standard-Galois/Counter Mode (AES-GCM) encryption over User Datagram Protocol (UDP). For Zoom Phone, we use Session Initiation Protocol (SIP) over TLS 1.2 with 256-bit AES-GCM encryption for calls and phone provisioning. In addition, call media is transported and protected by Secure Real-Time Transport Protocol (SRTP) with 256-bit AES-GCM encryption for Zoom Workplace desktop and mobile apps and with 128-bit AES encryption for devices at a minimum. Supported device models can upgrade to AES-256 bit encryption. Both Zoom Meetings and Zoom Phone media remain encrypted as they pass through the Zoom Cloud Platform until they reach another Zoom Workplace app or a specific Zoom service such as our cloud recorder, transcription service, AI Companion, or gateways to other meeting or traditional phone services.

As an open platform, Zoom offers methods for a range of devices and services to connect with the Workplace platform. This includes support for use cases such as using a SIP/H.323 device (e.g., video conferencing equipment or phone devices) when connecting to a Zoom Meeting or on a Zoom Phone call, broadcasting meetings or webinars over popular streaming services, and calling into a meeting with a standard phone line (i.e., over the public switched telephone network (PSTN) and not via the Zoom Workplace app). As these integrations must leverage communication protocols native to the specific third-party device or service, encryption methods will be limited to what is possible on that device or service. Where possible, Zoom recommends that customers use encryption with third-party devices and services; however, customer data transmitted using these devices and services may not be encrypted in transit between users and the Zoom Cloud Platform. Learn more about encryption for SIP devices for Zoom Phone here and for third-party endpoints here.

Encryption at rest

Zoom services in the Zoom Cloud Platform may store customer content such as meeting recordings, transcripts, voicemails, or chat messages. Our system is designed to use a minimum 256-bit AES encryption when storing such data **at rest**. The encryption keys are either generated and managed by Zoom's Key Management System (KMS) or, if Zoom Customer Managed Key has been licensed and enabled, by the customer's KMS.

Additional client-side encryption options across the Zoom Workplace platform

Safeguarding data and private information looks different from one business to the next. With this in mind, we have developed optional encryption offerings that can be tailored to fit individual customer preferences. Some features are only available for certain paid subscriptions and may need Zoom or an account admin to enable them.

As described above, the default in-transit and at-rest encryption protocols are designed to permit the availability of the decryption keys to the Zoom Cloud Platform in order to provide features that require access to the encrypted content, such as search, cloud recording and transcription, and AI Companion. To maximize flexibility for customer needs, some services can be configured to use certain client-side encryption options. These options allow devices leveraging the Zoom Workplace app to generate, store, and exchange the encryption keys between other participating devices while limiting Zoom Cloud Platform access to those keys.

For example, Zoom Phone and Zoom Meetings offer **end-to-end encryption (E2EE)**, where the cryptographic keys are known only to the participants' devices. Advanced chat encryption for Zoom Team Chat also allows for keys to be generated and stored by the chat participants' devices, but Zoom's servers aid in the management of these keys for ease of use.

Additionally, we offer device-managed encryption for Zoom Mail Service and restricted voicemails for Zoom Phone, for customers who would like to manage which of their devices can access encrypted emails and restricted voicemails. With Zoom's device-managed encryption, certain data is encrypted such that the decryption keys are known only to authorized users' devices, and users are required to manage authorization for their own devices and cryptographic keys. In some cases with device-managed encryption, Zoom servers have access to keys to encrypt data for the user's devices, but not to decrypt it. This allows the server to encrypt data received from external users (such as voicemails over PSTN) on services that do not support device-managed encryption and minimizes the time during which the server has access to this data. On the other hand, if data is device-managed encrypted by a user themselves using their Zoom Workplace app, as in certain Zoom Mail Service emails, those messages are considered end-to-end encrypted. We also offer escrow as a way for account administrators to back up and access their users' content encrypted with device-managed encryption.

Below is additional information on Zoom's advanced or customizable encryption offerings.

End-to-end encryption for Zoom Meetings

For Zoom Meetings where additional communication privacy and data protection is desired, the end-to-end encryption **(E2EE)** feature can be enabled.

Zoom's E2EE feature uses the same 256-bit AES-GCM encryption method that supports standard enhanced encryption to encrypt real-time media in meetings during transit between meeting participants using the Zoom Workplace app. The difference here is that the feature is designed so that the cryptographic keys are known only to the devices of the meeting participants. This makes it so that third parties — including Zoom — do not have access to the meeting's private keys. E2EE is also available for breakout rooms with each room having a unique meeting encryption key. Using E2EE disables certain features, such as cloud recording, and requires all meeting participants to join from the Zoom Workplace desktop or mobile app or Zoom Rooms.

As users update their Zoom Workplace app to version 6.0.10 or higher, end-to-end encrypted meetings will start leveraging our latest post-quantum end-to-end encryption (PQ E2EE) protocol. If PQ E2EE is unsupported by any participant's device, the meeting will default to standard end-to-end encryption (E2EE) when enabled. PQ E2EE in Zoom Meetings is designed to withstand the threat of an adversary who can capture encrypted network traffic now, hoping to acquire a quantum computer in the future and use it to decrypt the captured data later. PQ E2EE offers the same security property as standard E2EE, namely that the cryptographic keys are known only to the meeting participants' devices. Meeting participants can confirm whether a meeting is using standard or post-quantum end-to-end encryption by tapping the shield icon to display the meeting information, including the type of encryption enabled for the meeting.

Learn more about using end-to-end encryption in meetings, including the minimum version requirements and supported app types for standard and post-quantum end-to-end encryption.

NOTE

Zoom's PQ E2EE is not designed to defend against potential attacks that would require the current existence of a quantum computer capable of breaking classical cryptography at the time a meeting takes place. Zoom is closely monitoring advancements in this space, and preparing for further protocol updates once this becomes a more concrete threat. See our cryptography whitepaper for more details.

End-to-end encryption for Zoom Phone

Zoom Phone users making one-on-one calls between users on the same Zoom account via the Zoom Workplace app have the option to elevate the session to an end-to-end encrypted phone call. E2EE is designed to encrypt the call media using cryptographic keys known only to the devices of the caller and receiver. Using E2EE disables certain features, such as automatic call recordings, ad hoc recording, call monitoring, switch to carrier, or AI Companion, and requires call participants to join from the Zoom Workplace desktop or mobile app or Zoom Phone appliances. Learn more about using end-to-end encryption in Zoom Phone calls.

As users update their Zoom desktop and mobile apps to version 6.1.0 or higher, E2EE calls will start leveraging our PQ E2EE protocol. If PQ E2EE is unsupported by any participant's device, the call will default to standard end-to-end encryption (E2EE) when enabled.

Restricted voicemails for Zoom Phone

Account admins can enable the **restricted voicemails** feature for Zoom Phone. The feature is designed so that voicemails are encrypted by Zoom so that only the intended recipient's devices can listen to them. When enabled, cloud services, such as AI Companion and search, or traditional telephone access, are not available. For enterprise users with the escrow feature enabled, these keys might be also shared with the user's account admins. Learn more about using restricted voicemails for Zoom Phone.

Advanced chat encryption for Zoom Team Chat

By default, Zoom Team Chat is designed to use TLS 1.2 or higher to encrypt in-transit Team Chat messages between users and the Zoom Cloud Platform and also encrypt at-rest messages stored in the Zoom Cloud Platform. For additional communication privacy, an account admin can enable the **advanced chat encryption** feature on paid accounts. Once enabled, chat messages are encrypted on the app using 256-bit AES using keys exchanged between the participating devices. Advanced chat encryption is designed to use a device-generated and stored key to encrypt messages between users in a chat, and then additionally encrypt these messages in transit between users and the Zoom Cloud Platform using TLS. Using advanced chat encryption disables certain features, such as AI Companion, message previews, message translation, setting message reminders, and scheduling a meeting from a group chat.

When used, an account admin can still see chat metadata, reactions to messages, and also external messages received if advanced chat encryption is not enabled in the external account. Advanced chat encryption cannot be combined with continuous meeting chat or Zoom Customer Managed Key. Learn more about using advanced chat encryption.

End-to-end encryption for Zoom Mail Service

Zoom Mail Service is a Zoom-hosted email provider with optional end-to-end encryption for emails sent directly between active users on the Zoom Mail Service system. Account owners and admins can select whether a specific domain will be configured to use device-managed encryption, encryption at rest with server-managed keys, or a combination of the two. End-to-end encryption for those emails depends on factors such as user or account level settings, whether the sender and receiver have already generated encryption keys, and whether the sender and receiver are running the latest app version.

The user interface is designed to indicate when the drafted email will be end-to-end encrypted. Customers who choose a custom domain have the option to set up escrow on their account, which allows a designated escrow admin to receive backup copies of keys from all users in that account. Holding copies of these keys will let the escrow admin access all emails in the account. Learn more about end-to-end encryption for Zoom Mail Service.

Enterprise encryption products

Enterprise customers may have specialized needs for administrative access and control to meet their compliance, security, and communication privacy requirements. Zoom provides additional products and services to meet those needs.

Customer managed encryption

Zoom Customer Managed Key (CMK) is designed to allow customers to bring their own key (BYOK), or, more specifically, to hold their own key (HYOK) for encryption of selected customer data stored at rest within the Zoom Cloud Platform such as recordings, chat messages, whiteboards, and summaries generated by AI Companion.

Customer hosted servers

Zoom Node is a hybrid cloud solution that integrates your data center servers with Zoom's Cloud Platform to help deliver Zoom services to your offices. Zoom Node modules allow private meetings to be hosted and recorded on customers' servers, where the meeting encryption keys are generated. Services in the Zoom Cloud Platform, such as AI Companion or Whiteboard are not available for meetings in private-only mode unless the account admin has specifically granted access.

Bringing it all together

These encryption technologies are key aspects of Zoom's larger security strategy, helping to stitch together a unified communications experience built with security in mind. That experience is contained in Zoom Workplace — our open collaboration platform with AI Companion — which packages our chat, phone, whiteboard, meetings, and other solutions to provide your teams with multiple ways to connect and collaborate. These products are purpose-built to work together to enable meaningful connections with less friction. Learn more about this framework by visiting our Zoom Workplace webpage.