Web Meeting Security Overview

This document describes the different encryption mechanisms of Web Meeting sessions.

From legal standpoint, please refer to our Privacy Policy, our GDPR policy and our data retention here: http://www.allocloud.com/gdpr.

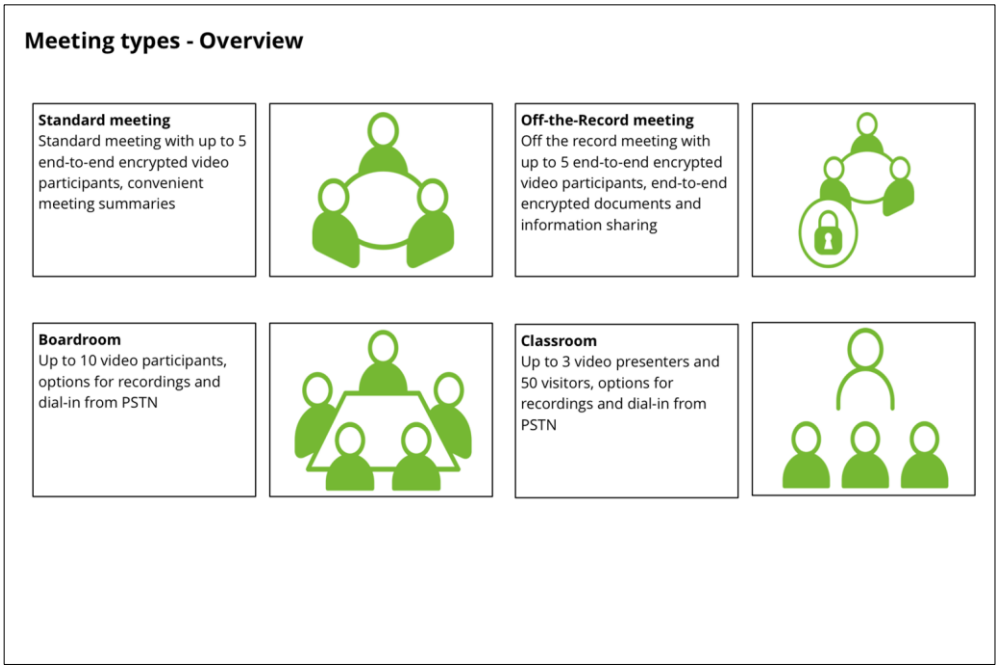
Additionally, all our services are hosted in Europe and do not fall under any circumstance under US or Chinese regulations.

Data flow and encryption

Meeting types and data flow

Web Meeting supports various meeting types. Each meeting type comes with special features, network requirements and security considerations.

Overview

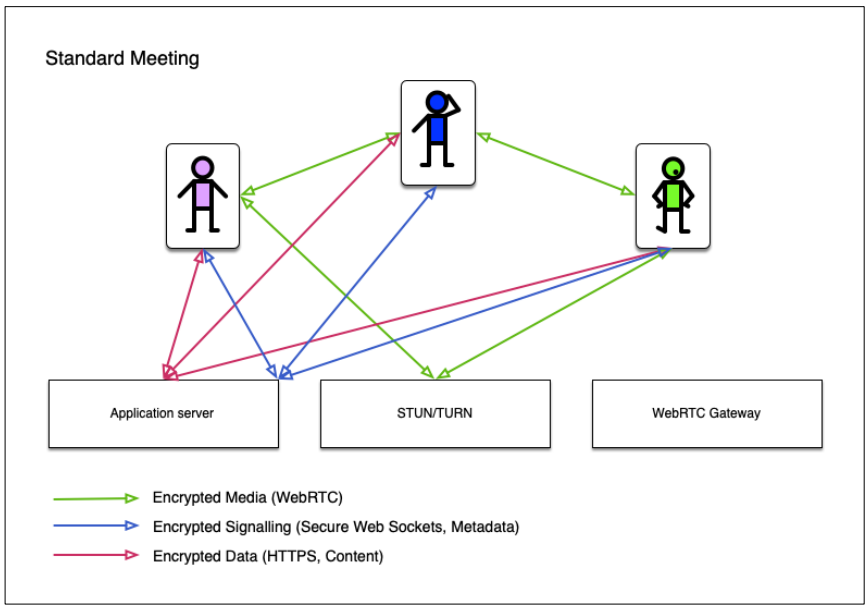


Standard meeting

Participants in a standard meeting room communicate with end-to-end encrypted audio and video. In certain circumstances a direct peer-to-peer connection cannot be established. In these cases, a TURN server relies data between the participants. Documents and other information that are shared during

the meeting are sent to the application server over HTTPS. The application server will create a meeting summary at the end of the meeting. Recording and dial-in is not possible.

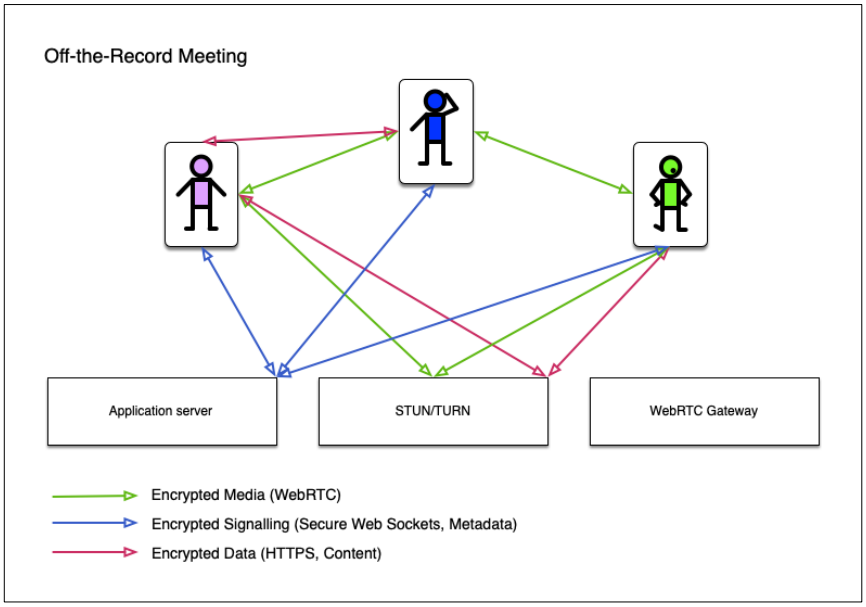
All signaling and content data sent between the web browsers and the servers is always 256-bit TLS 1.2 encrypted. All media (audio and video) is end-to-end encrypted with DTLS 1.2/SRTP encryption standards. The media remains end-to-end encrypted, even if the traffic is routed through a TURN server.



Off-the-record meeting

The Off-the-record (OTR) meeting is a variation of the standard meeting room. Audio and video are share in the same way. Documents and any other information shared during a OTR meeting are distributed among the participants through end-to-end encrypted data channels. Therefore, the Web Meeting system has no knowledge of the content of the meeting and does not produce a meeting summary. Recording and dial-in is not possible.

All signaling sent between the web browsers and the servers is always 256-bit TLS 1.2 encrypted. All media (audio and video) and data is end-to-end encrypted with DTLS 1.2/SRTP encryption standards. The media and data remain end-to-end encrypted, even if the traffic is routed through a TURN server.



Boardroom / Classroom (Webinar)

Boardroom and Classroom (Webinar) meetings are not end-to-end encrypted. Audio and video are always sent the SFU and distributed from there to the other participants of the meeting. The browser and the SFU communicate encrypted with each other, the SFU decrypts each video stream and encrypt it again for distribution. This allows for optional recording. All other data and information shared in a Boardroom or Classroom are stored on the application server for further use in meeting summaries. Recording and dial-in can be configured for these types of meetings.

All signaling and content data sent between the web browsers and the servers is always 256-bit TLS 1.2 encrypted. All media (audio and video) sent between the web browsers and the servers is always point-to-point encrypted with DTLS 1.2/SRTP encryption standards.