UC MAX MEETINGS

A guide outlining some of the security benefits of UC MaX Meetings

UC MaX Meetings uses some components from Zoom (In Meeting video technology) and this quide explains how, and if, these vulnerabilities affect UC MaX Meetings.

ZOOMBOMBING

ZoomBombing is where when uninvited attendees break into and disrupt a meeting. This can happen when a Meeting URL is posted on a public forum, or the Meeting ID is guessed by a 3rd party.

FACT: Ways to prevent Zoombombing by enabling below features:

- Meetings can have password protection.
- Waiting rooms require the host to actively admit new participants.
- Chime upon entry notifies the participants when someone new joins

END-TO-END ENCRYPTION

End to End Encryption is supported and can be enabled in UC MaX Meetings advanced settings:

FACT: If all users of the meeting are using UC MaX Meeting clients, then the traffic is encrypted at all times, only being decrypted on the endpoints themselves.

CALLS ROUTED THROUGH CHINA

FACT: UC Max Meetings is hosted on a completely separate instace to Zoom. Servers for these instances are exclusively hosted in the United States, so **NO** Calls are routed through China.

SHARING OR SELLING USER DATA

FACT: UC MaX Meetings has dedicated separate instances of Zoom's software with separate user database. This software does not include email, address, job titles etc.. So **NO** this does not apply to UC MaX Meetings.

CLIENT SHARING DATA WITH FACEBOOK

FACT: As mentioned UC MaX Meetings software is seperate from Zoom's software and database. So **NO** this does not apply to UC MaX Meetings.