induction healthcare

Attend Anywhere: Security & Whitelisting FAQs

Some answers to common questions relating to the security and whitelisting requirements for our latest product version due for release in May 2024.

What network addresses are used?

The following network destinations are required when running Attend Anywhere in your environment.

Function	Domain	Subnet
Video	*.chime.aws	99.77.128.0/18
Video	*.sdkassets.chime.aws	99.77.128.0/18
Call screen	nhs.attendanywhere.com	
Call screen	england.nhs.attendanywhere.com	
Call screen	wales.nhs.attendanywhere.com	
Call screen	consult.attendanywhere.co.uk	
Call screen	dwp.attendanywhere.co.uk	

Table 1 - Addresses

What ports do I need to whitelist?

Video calls default to UDP as recommended by Attend Anywhere and our partner AWS. **Note:** If the UDP port is unavailable then calls will automatically be made over TCP, but this could impact performance. Ports should be whitelisted as per the below table:

Function	Ports
Video	TCP:443 UDP:3478
Call screen	TCP:443

Table 2 – Ports

How many addresses might I have to whitelist?

We use a large range of network IP addresses to support the video calls. If your network security devices and/or solutions cannot support whitelisting by domain name (*.chime.aws)then you will need to whitelist all the addresses in the following range: **99.77.128.1 - 99.77.191.254**

How are the video calls secured?

When connected to a meeting, your audio, messages, video, and content shared through screen sharing is encrypted while in transit using the following industry standard cryptographic protocols:

Transport Layer Security (TLS), Datagram Transport Layer Security (DTLS), and Datagram Transport Layer Security-Secure Real-Time Transport Protocol (DTLS-SRTP).

We use the following security protocols for our video consultation platform:

Protocol/Details	Description
TLS	Transport Layer Security
Version	1.2 and above
Ciphers	ECDHE-RSA-AES256-GCM-SHA384
Key Exchange	ECDHE
TLS key size	AES 256 bit
Hash Algorithm size	SHA 384 bit

Table 3 – Web Security Ciphers

We use the following security protocols for the video calls:

Protocol/Details	Description
DTLS-SRTP	Secure real-time protocols
TLS key size	AES 128 bit

Table 4 – Video Security Ciphers

Are video calls via UDP secure?

Yes, the communications are secured using Datagram Transport Layer Security (DTLS), and Datagram Transport Layer Security-Secure Real-Time Transport Protocol (DTLS-SRTP) as detailed in Table 4 above.

References:

Understanding Security in the Amazon Chime Application and SDK

FAQs | amazon-chime-sdk-js (aws.github.io)

Network configuration and bandwidth requirements - Amazon Chime SDK