IPVideoTalk

Any internet technology involves security concerns, but we take your security seriously. Grandstream has various measures in place to keep your information safe when using IPVideoTalk.

How are my IPVideoTalk Meetings being Secured?

WebRTC and Security

WebRTC as a technology has multiple safeguards in place that keep your communications secure. Here are the four main characteristics of WebRTC that make it a secure option:

Browser Trust Model: Most internet browsers are built to allow the safe use of the internet by verifying traffic and securing communications. When using WebRTC-capable browsers like Google Chrome and Firefox you can count on the fact that security issues are patched as they arise in a promt fashion.

Same Origin Policy (SOP): The Same Origin Policy, also known as SOP means that scripts run in isolated sandboxes. This prevents pages other than those intended, from running maliciously or accidently. In other words, any server or web page or advertisement cannot just interrupt and steal your log in credentials.

Encryption: All WebRTC communications, including signaling are encrypted using DLTS and SRTP. In the specific case of IPVideoTalk, AES Encryption is used. AES is used by international governments and financial institutions to protect their communication data.

Requiring Explicit Permission for Use of Camera, Mic, and for screensharing: IPVideoTalk, like most WebRTC applications requires explicit permission each time the camera and microphone are accessed before sharing within a meeting, this prevents unauthorized use or access. Additionally, you must click to share your screen and confirm before the content is shared.

Other Security Measures of IPVideoTalk

Password Protection

Any meeting can be password protected from the IPVideoTalk Portal.

Hidden Internal System Structure

IPVideoTalk's internal structure is hidden and firewall protected. The hidden structure makes it difficult for hackers to gain the knowledge necessary for attacking servers directly. Additionally, there is a firewall in place to block unauthorized traffic.

In addition to the above measures, Grandstream and AWS are continuously monitoring for suspicious activity and malicious traffic.