Onsight Firewall & Proxy
Configuration Guide

LIBRESTREAM.COM

LIBRESTREAM

Copyright

Onsight Firewall & Proxy Configuration Guide

Doc #: 400295-08 Rev: D

December 2022 (v11.4.11)

Contents

1. INTRODUCTION

This guide specifies the ports and white listing that need to be configured on a firewall and proxy to permit Onsight Client devices to access Onsight Connect services. These settings are required for Onsight clients to use *Session Initiation Protocol (SIP)*, *Media* and Onsight *TeamLink* services.

Most Customers will follow the Default Configuration specified in this document. This configuration means your Onsight Connect endpoints are using Onsight Hosted *SIP* Services with the option of using *TeamLink*. This configuration allows direct access to Onsight Hosted SIP and Media Services where permitted by your local firewall rules, with the option of automatically switching to *TeamLink*/*Hypertext Transfer Protocol Secure (HTTPS)* when clients are at a location that does not allow these ports.

Tip: Onsight Connect and TeamLink traffic are based on Hypertext Transfer Protocol (*Hypertext Transfer Protocol (HTTP)*)/*HTTPS* and they are managed by your proxy. *SIP* and *Media* connectivity is managed by your Firewall.

Note: Customers may choose to not use Librestream's Hosted *SIP* service, and instead provide their own *SIP* server infrastructure. Please contact Librestream Support to discuss this option.

2. DEFAULT CONFIGURATION

The following settings are required when your Onsight Connect endpoints are using Onsight Hosted Services. Table 1 and table 2 are mandatory for Onsight Services.

Note: Onsight Connect and TeamLink traffic are based on Hypertext Transfer Protocol (HTTP)/HTTPS and they are managed by your proxy. SIP and Media connectivity is managed by your Firewall.

The OPM Client Policy **SIP Detection Method** must be set to **SIP Server Full** for all clients.

If you have chosen to permit direct network access to Onsight SIP servers then you must implement Table 2-1 *(on page 7)* and Table 2-2 *(on page 8)* for new customers. If you are only allowing network access via Teamlink then you only need to implement Table 2-1 *(on page 7)*.

Table 2-1 Web/HTTPS Proxy and SSL Inspection White Listing

Web/HTTPS Proxy and SSL Inspection	**TCP, 443, HTTPS**
1. Allow HTTPS traffic to *.librestream.com 2. Disable SSL inspection on the above traffic. **Note:** 1. If you have requested to allow Onsight Connect endpoints to use Teamlink in China, add this third rule to all proxies: ◦ Allow HTTPS traffic to *.librestreamtech.cn 2. Please ensure you include any custom domains that you have pointed at Librestream resources (eg: Onsight Connect for Web) within your proxy white list.	TCP, 443, HTTPS

Table 2-2 Onsight SIP and Media Services (For New Customers)

Service/Product	IP Addresses	Transport, Ports, Protocol
Call Services	52.142.34.48/28; 51.105.215.0/28; 52.253.84.80/28;	UDP, 3478, STUN; * TCP, 5060, SIP; TCP, 5061, SIP-TLSv1.2; UDP, 15000-65000, (S)RTP, (S)RTCP, STUN;* TCP, 80, HTTP Refer to Note 1 *(on page 8)*; TCP, 443, HTTPS; *Required if TeamLink is enabled.
Redundancy and backup	52.146.156.64/28 13.70.46.96/28 13.64.48.96/28	

Table 2-3 Onsight SIP Services (For Legacy Customer Domains)

Onsight SIP Servers **(sip.librestream.com)**	**IP addresses**	**Transport, Port, Protocol**
US West	54.213.166.17	UDP, 3478, STUN* UDP, 58024, STUN* UDP, 58523, STUN* TCP, 5060, SIP TCP, 5061, SIP-TLSv1.2 *Required if TeamLink is enabled.

Table 2-4 Onsight SIP Media Services (For Legacy Customer Domains)

Media Servers RTP	IP addresses	Transport, Port, Protocol
US West	54.200.152.202, 54.201.34.23, 54.213.38.103, 54.218.75.97, 54.213.75.101, 54.200.248.252	UDP, 15000 - 65000, Secure (S)RTP, (S)RTCP

Note:

1. Port 80 is only required for *HTTPS* redirects from a browser. If you allow Port 80, requests will automatically redirect traffic to 443 after first request.

2. If using Internet Protocol (IP) addresses in firewalls/routing/other services, please register with support@librestream.com or call **1.800.849.5507** or **+1.204.487.0612**; In the event that we add additional IP Ranges in the future, registration will ensure you receive updates and help coordinate uninterrupted service.

3. The OPM Client Policy **SIP Detection Method** must be set to **SIP Server Full** for all clients.

3. ENDPOINT

The Onsight Connect app is available for Windows, *iPhone Operating System (iOS)* and Android endpoints. The outbound port usage is as follows:

Table 3-1 EndPoints

Protocol	Ports
SIP	Random
RTP	6000 – 6200 (if these ports are in use by other applications then higher ports will be used)
HTTPS	Random

Note: In the case where direct Onsight Connect client to Onsight Connect client media communications are allowed by your SIP server, client devices use UDP destination ports 6000-6199 for SRTP (media/data streams).

4. PUSH NOTIFICATIONS

Push notifications are used to deliver notification of an Incoming call when Onsight Connect is running in the background on an Android and *iOS* devices.

Apple push notifications require that your Firewall allow outbound connections to *Transmission Control Protocol - Internet Protocol (TCP-IP)* ports 5223, 2197, and 443 on the entire 17.0.0.0/8 address block. If this is not enabled, Onsight Connect will not receive push notifications and will not receive calls when the app is in the background, or not running. For more information, please visit https://support.apple.com/en-ca/HT203609 .

Google's Firebase Cloud Messaging (push notifications) uses *TCP* ports 443, 5228, 5229 and 5230 for incoming messages. For details refer to https://firebase.google.com/docs/cloud-messaging/concept-options.

5. FOR MORE INFORMATION

Please contact support@librestream.com or call **1.800.849.5507** or **+1.204.487.0612**.

Appendices

Glossary

Domain Name Server

A Domain Name Server (DNS) translates a computer's host name into a unique Internet Protocol (IP) address.

Combined

(DNS)

Hypertext Transfer Protocol

Hypertext Transfer Protocol (HTTP) is the protocol used for transferring information from a user's web browser to the website they are visiting.

Hypertext Transfer Protocol (HTTP)

HTTP

Hypertext Transfer Protocol Secure

Hypertext Transfer Protocol Secure (HTTPS) is similar to Hyper Transfer Protocol (HTTP) except it uses separate protocols called Secure Sockets Layer (SSL) and Transport Layer Security (TLS) to ensure that the information travels through a safe tunnel to its destination.

Hypertext Transfer Protocol Secure (HTTPS)

HTTPS

Internet Protocol

Internet Protocol (IP) represents a unique string of characters that identifies each device on a network using an Internet Protocol address.

Internet Protocol (IP)

IP

iPhone Operating System

The operating system for Apple mobile devices such as an iPhone and iPad.

iPhone Operating System (iOS)

iOS

Media

Video, audio, and data content which is delivered via streaming in an Onsight session.

Network Address Translation

Network Address Translation (NAT) is a method for mapping multiple local private addresses to a public address before transferring information.

Network Address Translation (NAT)

NAT

Real-time Protocol

Real-time Protocol (RTP) is a network standard that can transmit audio and video content that is optimized for consistent delivery of live data using the internet.

Real-time Protocol (RTP)

RTP

Secure Real-time Transport Protocol

Secure Real-time Transport Protocol (SRTP) is a profile for *Real-time Protocol (RTP)* intended to provide encryption, message authentication and integrity, and replay attack protection to the *RTP* data in both unicast and multicast applications.

Secure Real-time Transport Protocol (SRTP)

SRTP

Real-time Transport Control Protocol

Real-time Transport Control Protocol (RTCP) is a network standard for delivering audio and video content over *Internet Protocol (IP)* networks.

Real-time Transport Control Protocol (RTCP)

RTCP

Secure Real-time Transport Control Protocol

Secure Real-time Transport Control Protocol (SRTCP) provides the same security services to Real-time Transport Protocol (RTCP) as Secure Real-time Protocol (SRTP) does to Real-time Protocol (RTP).

Secure Real-time Protocol (SRTCP)

SRTCP

Secure Sockets Layer

Secure Sockets Layer (SSL) enables internet connections to be secure and safeguards sensitive information that is transmitted between two systems. SSL provides encryption and server authentication over the internet.

Secure Sockets Layer (SSL)

SSL

Session Initiation Protocol

Session Initiation Protocol (SIP) is the underlying call control protocol that connects all Onsight Connect sessions. Each Onsight Connect user will have a SIP account automatically assigned to them.

Session Initiation Protocol (SIP)

SIP

Session Traversal Utilities for Network Address Translator

The Session Traversal Utilities for Network Address Translator (STUN) protocol is a client-server protocol that was designed to resolve issues with traversing *Network Address Translation (NAT)* for *Voice over Internet Protocol (VoIP)* implementations.

Session Traversal Utilities for Network Address Translator (STUN)

STUN

TeamLink

TeamLink enables HTTPS tunneling (firewall traversal) of data through a firewall that does not allow SIP or Media traffic

Transmission Control Protocol

Transmission Control Protocol (TCP) - Internet Protocol (IP) is a communications standard that enables computers to communicate by sending and receive messages over a network such as the internet.

Transmission Control Protocol - Internet Protocol (TCP-IP)

TCP

Transport Layer Security

Transport Layer Security (TLS) is the successor to *Secure Sockets Layer (SSL)* that enables communications to be secure over a computer network and internet.

Transport Layer Security (TLS)

TLS

User Datagram Protocol

User Datagram Protocol (UDP) is a light-weight protocol that runs on top of the Internet Protocol (IP) and transmits datagrams (Independent, self-contained messages) over a network.

User Datagram Protocol (UDP)

UDP

Voice over Internet Protocol

Voice over Internet Protocol (VoIP) enables you to make voice calls using an internet connection in place of a regular analog phone line.

Voice over Internet Protocol (VoIP)

VoIP