ONSIGHT CONNECT

ONSIGHT FIREWALL AND PROXY CONFIGURATION GUIDE

ON SIGHT CONNECT

Librestream
Onsight Firewall and Proxy Configuration Guide
Doc #: 400295-06, rev A

December 2019

Information in this document is subject to change without notice.

Name of Librestream Software: Onsight Connect

Patents Notice: United States Patent # 7,221,386, together with additional patents pending in Canada, the United States and other countries, all of which are in the name of Librestream Technologies Inc.

TABLE OF CONTENTS

ONSIGHT FIREWALL AND PROXY CONFIGURATION GUIDE

INTRODUCTION

This guide specifies the ports and white listing which need to be configured on a firewall and proxy for Onsight Connect services. These settings are required for Onsight clients to use SIP, Media and TeamLink services.

Most Customers will follow the Onsight Default Configuration specified in this document. This configuration means you are using Onsight Hosted SIP Services with the option of using TeamLink. This configuration allows direct access to Onsight Hosted SIP and Media Services through your Firewall with the option of using TeamLink when clients are at a location that do not allow these ports.

NEW: Commencing Feb 1 , 2020 additional Onsight servers will be brought online. The ports and white listing which need to be configured on your firewall and proxy for Onsight Connect services by that date are provided in section 2.0.

Note: Customers who use have their own SIP Infrastructure can use an Onsight Private SIP Server Configuration. The Private configuration also includes the option of using TeamLink services to pass through firewalls. Onsight Connect will utilize your Private SIP server settings as configured in your Onsight Platform Manager domain. Please contact Librestream Ssupport for details.

1.0 DEFAULT CONFIGURATION

NOTE: 1.0 Default Configuration will be deprecated later in 2020; It is important that you also configure for the 2.0 Configuration, see below.

The following is required when using Onsight Connect including Onsight SIP Services. Tables 1.1.1 and 1.1.2 are mandatory for Onsight Services. Note that Onsight Connect and TeamLink HTTP/HTTPS connectivity is 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 servers then you must do both tables below. If you are only allowing network access via Teamlink then you do not need to do Table 1.1.2.

1.1.1 Table: Web Proxy and SSL Inspection White Listing

Web Proxy and SSL Inspection		
White list *.librestream.com, disable SSL inspection.		
Server	IP addresses	Transport, Port, Protocol
onsight.librestream.com teamlink*.*.librestream.com tcm.*.librestream.com	Proxy configuration should be URL based.	TCP, 443, HTTPS
workspace.librestream.com (required if Workspace is enabled.)	Proxy configuration should be URL based.	TCP, 443, HTTPS

1.1.2 Table: Onsight SIP and Media Services

[1]Reserved

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.

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, RTP, RTCP

Note: above IP addresses are being retired in 2020.

2.0 Additional Rules for 2020

The following additional rules are introduced beginning Feb 1 , 2020.

If you have chosen to permit direct network access to Onsight servers then you must configure for both tables below. If you are only allowing network access via Teamlink then you do not need Table 2.1.2.

2.1.1 Table: Web Proxy and SSL Inspection White Listing

Web Proxy	Note	Transport, Ports, Protocol
*.librestream.com	White list *.librestream.com and disable SSL Inspection.	TCP, 80, HTTP[1] TCP, 443, HTTPS

2.1.2 Table: Onsight SIP and Media Services

Service/Product	IP Addresses[2]	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[1]; TCP, 443, HTTPS;

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 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.

Note: Use networktest.librestream.com to run a live check of your firewall/proxy compatibility and confirm successful configuration.

3.0 Push Notifications

Push notifications are used to deliver call invites when Onsight Connect is running in the background.

Apple push notifications require that your Firewall allow TCP ports 5223, 2195, 2196, and 443 on the entire 17.0.0.0/8 address block. If this is not allowed 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) use TCP ports 5228, 5229 and 5230 for incoming messages. For details refer to https://firebase.google.com/docs/cloud-messaging/concept-options

If your configuration does not fit within these guidelines, please contact Librestream Support for assistance.

4.0 FOR MORE INFORMATION

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