ON SIGHT CONNECT

TECHNICAL SETUP, CONFIGURATION, AND INSTALLATION GUIDE

Librestream
Technical Setup, Configuration, & Installation Guide
Doc #: 400278-02, rev A

May 2017

Information in this document is subject to change without notice.

Name of Librestream Software: Onsight Connect

TABLE OF CONTENTS

OVERVIEW

The purpose of this document is to provide an overview of the stages involved in a mid-to-large scale deployment of Onsight Connect.

The following Deployment stages will be discussed:

- Network Infrastructure
  - o Required infrastructure such as a Wireless Access Points, SIP server, and firewall considerations.
- Onsight Platform Manager
  - o Configuration
  - o Software Installation

Infrastructure Readiness

Confirm the exiting network infrastructure can support the Onsight Connect deployment:

- Onsight Connect for Windows requires Ethernet or Wireless connections. Ethernet is recommended.
- Onsight Devices require Wireless network connections for mobility.
- Wireless network coverage must provide reliable signal quality and bandwidth to support streaming Audio/Video. Adding extra Wireless Access Points in areas of little or no coverage may be required.
- A Wireless Site Survey will identify areas that require upgrades or additional Wireless network infrastructure.

STAGE 1: NETWORK INFRASTRUCTURE

Both the Wireless and Wired network infrastructure need to be configured to allow for and optimize continuously streaming video.

Network Infrastructure Checklist

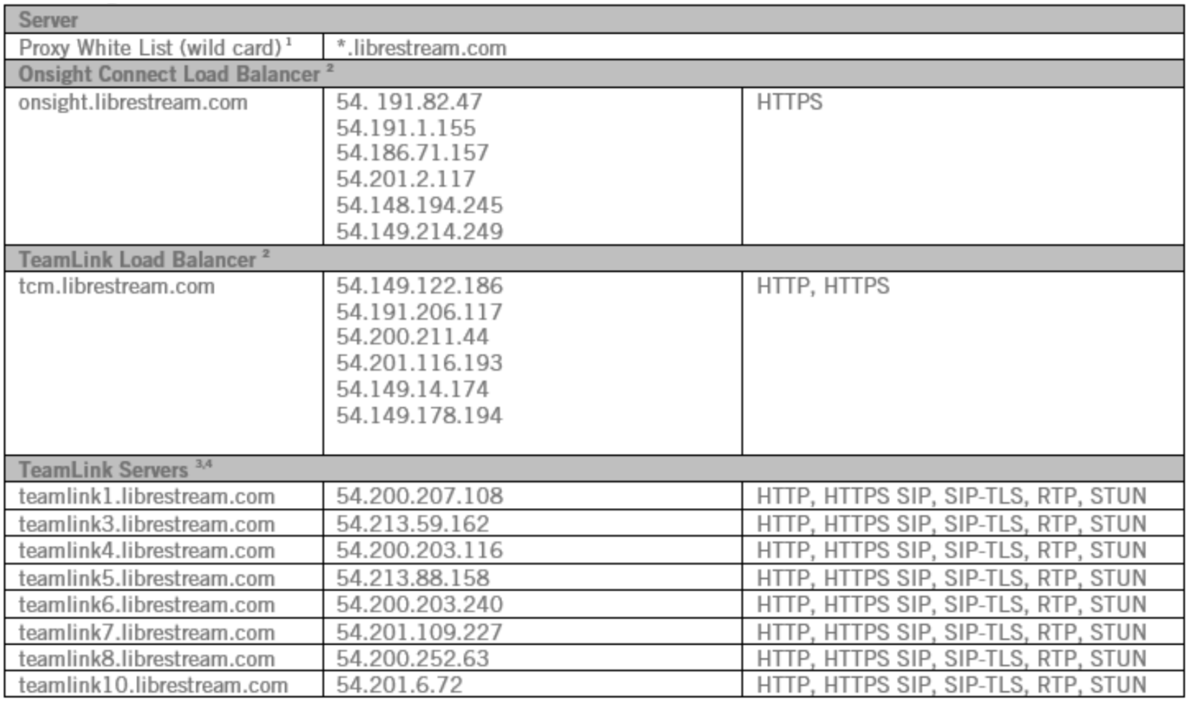
- Wireless Infrastructure supports video streaming
- Network policy allows and is configured for the required network protocols
- Security policy is defined
- SIP Server is installed/configured
  - o Most Onsight Connect Customers will use Onsight SIP but the option exists to use existing SIP infrastructure.
- Proxy configuration
- Firewall ports have been configured to allow SIP and Media traffic
- Decisions made on Onsight security methods
- Install Firewall/Router Port forwarding established for the OMS Web Service

Firewall Traversal

The Firewall must be configured to allow Onsight Services including SIP and media traffic.

The following servers are required for Onsight Cloud Service. They must be accessible from the network via the Firewall or Proxy.

Table: Onsight Cloud Servers



Server		
Proxy White List (wild card) [1]	*.librestream.com	
Onsight Connect Load Balancer [2]		

onsight.librestream.com	54. 191.82.47
	54.191.1.155
	54.186.71.157
	54.201.2.117
	54.148.194.245
	54.149.214.249
		HTTPS

TeamLink Load Balancer [2]		
tcm.librestream.com	54.149.122.186 54.191.206.117 54.200.211.44 54.201.116.193 54.149.14.174 54.149.178.194	HTTP, HTTPS
TeamLink Servers [3,4]		
teamlink1.librestream.com	54.200.207.108	HTTP, HTTPS SIP, SIP-TLS, RTP, STUN
teamlink3.librestream.com	54.213.59.162	HTTP, HTTPS SIP, SIP-TLS, RTP, STUN
teamlink4.librestream.com	54.200.203.116	HTTP, HTTPS SIP, SIP-TLS, RTP, STUN
teamlink5.librestream.com	54.213.88.158	HTTP, HTTPS SIP, SIP-TLS, RTP, STUN
teamlink6.librestream.com	54.200.203.240	HTTP, HTTPS SIP, SIP-TLS, RTP, STUN
teamlink7.librestream.com	54.201.109.227	HTTP, HTTPS SIP, SIP-TLS, RTP, STUN
teamlink8.librestream.com	54.200.252.63	HTTP, HTTPS SIP, SIP-TLS, RTP, STUN
teamlink10.librestream.com	54.201.6.72	HTTP, HTTPS SIP, SIP-TLS, RTP, STUN

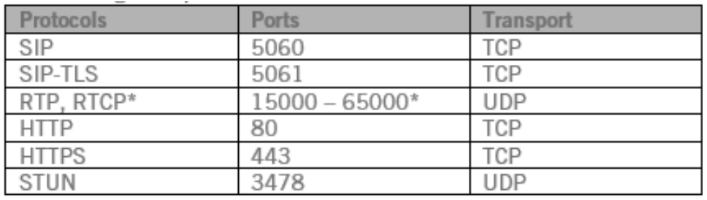
Notes on the following page

Notes

1. The wild card character may be different depending on the Web Proxy in use.
2. Active Load Balancers can change IP addresses without advance notification.
3. TeamLink servers are assigned to Onsight Endpoints by the TeamLink Cluster Manager via the TeamLink Load Balancer.
4. SIP, SIP-TLS, RTP and STUN are only required if SIP Detection Method is set to TeamLink for the Firewall Detect Test.

The following servers are required for Onsight Cloud Service. They must be accessible from the network via the Firewall or Proxy.

Table: Onsight Required Port and Protocols



Protocols	Ports	Transport
SIP	5060	TCP
SIP-TLS	5061	TCP
RTP, RTCP*	15000 – 65000*	UDP
HTTP	80	TCP
HTTPS	443	TCP
STUN	3478	UDP

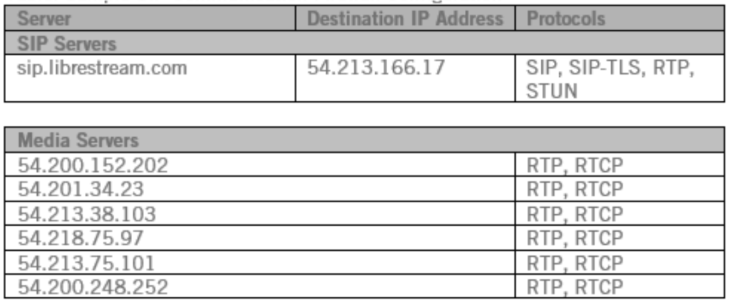
Firewall - SIP Server

When the Onsight Endpoints are located on different networks, SIP traffic must cross Firewall/NAT borders. A SIP Server is required to manage the traffic between the endpoints. The SIP Server also allows URI addressing (format: user@sipdomain.com) to simplify contact lists.

Each Onsight Connect User requires a unique SIP account on the SIP Server.

SIP Server Address, SIP URI, Authentication Transport, Authentication name and password are required when setting up users in Onsight Platform Manager.

Table: Sample SIP Communication Firewall Configuration



Server	Destination IP Address	Protocols
SIP Servers		
sip.librestream.com	54.213.166.17	SIP, SIP-TLS, RTP, STUN

Media Servers	
54.200.152.202	RTP, RTCP
54.201.34.23	RTP, RTCP
54.213.38.103	RTP, RTCP
54.218.75.97	RTP, RTCP
54.213.75.101	RTP, RTCP
54.200.248.252	RTP, RTCP

TeamLink can tunnel SIP and Media traffic through the Firewall using HTTPS port 443.

Security

Onsight Connect provides enterprise security options to safeguard the media and communication. These options include:

- Onsight Connect Service User Authentication (HTTPS TCP:443)
- Wireless Security (802.11 a/b/g/n)
- Media Encryption (AES-128)
- SIP-TLS Encryption (AES-128)
- Proxy Authentication support
- Privacy (disables video and image saving)
- FIPS 140-2 Encryption

These options should be reviewed by the stakeholders to confirm the features and options your Enterprise would utilize.

For more information see: **http://librestream.com/media/LIB-ONSIGHT-APP-NOTES-SECURITY_OVERVIEW.pdf.**

Librestream has tested Onsight Connect with the following SIP servers:

- Onsight SIP Service
- Cisco Video Communication Server (VCS)

The following servers are required for Onsight SIP Service. Firewall rules must allow traffic to all servers listed to guarantee SIP service. SIP traffic cannot be routed through a Web proxy it must be direct to the SIP and Media Servers. (TeamLink can be used to tunnel all SIP and Media traffic through a Web Proxy.)

STAGE 2: ONSIGHT PLATFORM MANAGER

Onsight Platform Manager (OPM) is the central management system for configuring the Onsight Connect endpoints.
The Onsight Account Administrator is assigned by your organization and configures the settings using the Onsight Platform Manager Web interface located at **https://www.onsight.librestream.com**.

Group Client Policy, Security, and Endpoint Settings should be configured before adding users to the system.

For complete details on using Onsight Platform Manager, refer to the OPM User Manual at **http://librestream.com/onsight-support/**.

Configuring Onsight Connect for Windows

Onsight Connect for Windows Installation

When a user is added to the Onsight system, they receive a Welcome email from Onsight Platform Manager. Download, install and login information is included in the email.

The Onsight Connect for Windows software is also available for download from Librestream's Software download page. Enterprises typically store the Installation package on a network drive and distribute it to the appropriate staff via a link to this central storage location. The recipient would typically run the software install from the network folder in order to install it on their computer. Once installed, they login to Onsight Connect using the credentials received in the Welcome Email.

Configuring Onsight Connect for iOS and Android

Onsight Connect for Smartphones (iOS and Android) is controlled by configuring Group Client Policy using OPM. Users are free to download the app from the Apple App Store or Google Play Store; however, they must have a valid user account in order to login. Smartphone users can be configured to use the application in either Expert or Field mode. See the OPM User Manual for details.

Configuring Onsight Devices

All Onsight Devices must have a network connection in order to contact the Onsight Connect Service and place calls:

- Onsight Connect for Windows will use the PC's existing network connection.
- Onsight for iOS will use the existing iPhone or iPad's network connection. This will include Wi-Fi or 3G/4G.
- Onsight Devices, e.g. 5000HD, must be configured to connect to the network using either wireless or Ethernet connections. Wireless is the preferred method for mobility.

The Onsight Devices must be manually configured to connect to the Wireless Network before being able to contact the Onsight Connect Service.

For Ethernet connectivity attach an I/O sled to the Onsight Rugged Smart Phone.

For complete details on using configuring Onsight Devices refer to the Onsight Account Service Setup Guide at **http://librestream.com/onsight-support/**.

Additional Resources

Refer to the Onsight Device User Manual for more details.

Refer to the OMS User Manual for more details on Onsight endpoint configuration, package creation and deployment.

Onsight Platform Manager Checklist

- Your Onsight Administrator has been assigned and has received their Welcome email from Onsight Manager.
- You have obtained the required number of license subscriptions to support your deployment of Onsight Connect users.
- SIP Service arrangements have been made to provide SIP accounts to your Onsight Connect users.
- If downloading Onsight Connect for Windows directly from the Onsight Connect Server is not preferred, Set-up a central location for users to access the Onsight Connect for Windows installation.
- Perform test calls with a sample of the Onsight Connect for Windows users, a subset of users can be added initially to facilitate initial testing.
- Add all users to Onsight Platform Manager.
- Create Groups and Configure Client Policy for all Users based on Group membership.

Additional Resources

Refer to **http://librestream.com/onsight-support/** for more details.

CONTACT SUPPORT

If you need assistance, please contact **support@librestream.com** or call **1.800.849.5507** or **+1.204.487.0612.**