ON SIGHT

APP NOTES

Onsight Connect Network Requirements

July 2016

LIBRESTREAM

Table of Contents

1. Overview 4

1.1 Onsight Connect Solution Architecture 4

1.2 Three Stages of Onsight Connectivity 5

2. Web (HTTP/S) Proxy Configuration 5

3. Firewall Requirements – Allowing SIP Traffic 6

4. Onsight Endpoint SIP Server Registration 9

5. Onsight TeamLink HTTPS Tunneling Server 9

5.3 TeamLink - Firewall Detect 9

6. For More Information 10

Document Revision

Librestream

Onsight Connect Network Requirements

Doc #: 400210-06

July 2016

Information in this document is subject to change without notice.

Reproduction in any manner whatsoever without the written permission of Librestream is strictly forbidden.

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.

1. Overview

This document provides a description of the network requirements for Onsight Connect on a Local Area Network and on the Internet.

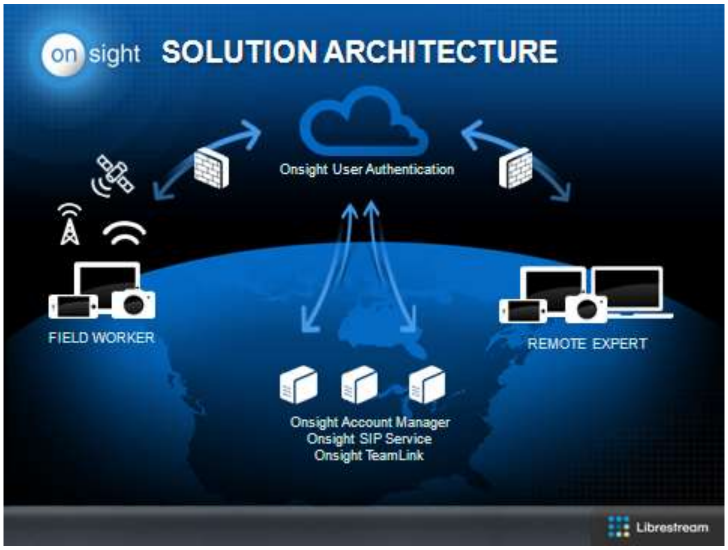
Onsight Connect Services consists of 3 distinct functions; Onsight Account Manager (OAM); Onsight SIP Service and Onsight TeamLink.

OAM is a cloud based service that provides Onsight user authentication and endpoint configuration. It relies on the HTTPS protocol. All communications between the user and OAM are encrypted using SSL. When a user attempts to log in to their Onsight endpoint they are authenticated by OAM based on their user credentials. Once authenticated by OAM the user's Onsight endpoint automatically receives configuration settings from OAM allowing them to begin using Onsight Connect. Onsight Account Manager only handles user authentication and configuration of the Onsight endpoint all other aspects of Media collaboration is handled by the Onsight SIP Service and Media Relays (Customers can choose to use their own SIP Infrastructure).

The Onsight SIP Service provides the "connection" functionality associated with establishing a call between Onsight endpoints. The protocol used by this service is Session Initiation Protocol (SIP). SIP is a signaling protocol that uses TCP relies on certain firewall ports to be open (to outbound traffic). Refer to section 2 for details. Onsight Services are interoperable with 3rd party SIP servers.

Onsight TeamLink is an optional service that provides an alternative method of firewall traversal for SIP messaging and Media streams. If a Firewall does not allow outbound SIP and Media traffic the TeamLink option can be used to proxy all SIP and Media traffic through an HTTPS tunnel to a TeamLink server. TeamLink will forward all SIP and Media traffic to the appropriate SIP Server and all return traffic back to the Onsight endpoint. This method is only recommended when it is not possible to traverse the Firewall using the standard SIP ports.

1.1 Onsight Connect Solution Architecture



*Your Enterprise Firewall and/or Web Proxy must allow traffic to onsight.librestream.com, Onsight SIP and Media Servers, and TeamLink Servers. You must add *.librestream.com as an allowed domain to the Web Proxy White List at your location.*

SSL requires that all Onsight Endpoints have accurate date and time set to allow authentication.

1.2 Three Stages of Onsight Connectivity

1.2.1 Onsight Endpoint Authentication

The User logs in to the Onsight Endpoint which connects to the Onsight Connect Server to Authenticate the User. The Onsight endpoint receives it configuration from the Onsight Connect Server once User authentication is complete.

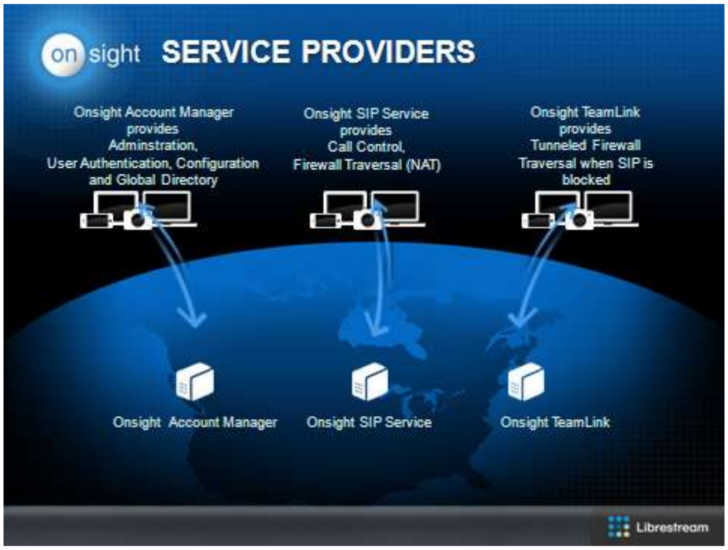
1.2.2 Onsight Connect SIP Registration

The Onsight Endpoint Registers to a SIP Server to gain SIP connectivity. The SIP Server can be either an Onsight SIP Server or the Customer's private SIP Server Infrastructure.

1.2.3 Onsight TeamLink Registration (Optional)

The Onsight Endpoint has the option of using Onsight TeamLink as a proxy method of registering to the SIP Server. This method is only recommended when it is not possible to traverse the Firewall using the standard SIP ports. This is typically used when an Onsight endpoint is connected to a Network that is not configured to allow SIP traffic but does allow HTTP or HTTPS. If TeamLink is enabled the Firewall Detect test determines when it's necessary to register to the TeamLink server.

Onsight Connect Service Providers



on sight SERVICE PROVIDERS

Onsight Account Manager provides Adminstration, User Authentication, Configuration and Global Directory

Onsight SIP Service provides Call Control, Firewall Traversal (NAT)

Onsight TeamLink provides Tunneled Firewall Traversal when SIP is blocked

2. Web (HTTP/S) Proxy Configuration

Onsight Connect and TeamLink use HTTPS (HTTP is optional) to communicate with the Onsight Connect service and tunnel SIP traffic; it required that it be routed through an internal Web (HTTPS) Proxy or be unblocked by the Firewall at your location. It may be necessary to add the Onsight URIs to the Proxy white list at your location.

Your Enterprise's Web Proxy White List must include the wildcard URL pattern '.librestream.com'. Note the wildcard character may be different for your Web Proxy.*

Direct SIP Traffic is not sent through a Web Proxy, it is only routed through a Web Proxy when TeamLink is enabled and the connection method is HTTPS or HTTP. The Firewall Detect test determines the suitable connection method: SIP, HTTPS or HTTP, depending on the results of the Firewall test.

3. Firewall Requirements – Allowing SIP Traffic

Firewall rules need to be set up based on how an endpoint will connect to the Onsight Server (onsight.librestream.com) and the SIP Server it will use. TeamLink is not required, it's provided as an alternative to registering directly to a SIP Server. Direct SIP Registration is always preferred.

There are 4 basic Firewall scenarios:

Definitions:
Onsight SIP Service = Librestream's Cloud SIP Service
Enterprise SIP Service = Customer's private SIP Infrastructure (Cisco VCS or alternative)
Migrate across Firewall = Onsight endpoints connect both inside and outside the Enterprise network.

1. Onsight Connect including Onsight SIP Service (TeamLink - not required) - The Customer requires onsight.librestream.com with sip.librestream.com connectivity. The Customer always connects directly to the SIP Server. There is no need to use TeamLink since endpoints don't migrate across the Firewall or will operate in an unrestricted Cloud environment.

2. Onsight Connect including Onsight SIP Service (TeamLink - enabled) - The Customer requires onsight.librestream.com with sip.librestream.com and TeamLink Connectivity. In this scenario the Onsight Endpoint is migrating inside and outside the Customers network and must determine when to use TeamLink. Their Corporate network must be configured to allow all traffic to all of our Servers so that the Firewall Detect test can determine when to use TeamLink.

3. Onsight Connect with Enterprise SIP Service (TeamLink - not required) - The Customer requires onsight.libresteam.com but uses their own SIP infrastructure. This will require onsight.librestream.com being added to either the Firewall Rules or the Proxy White List. There is no need to use TeamLink since endpoints don't migrate across the Firewall or will operate in an unrestricted Cloud environment.

4. Onsight Connect with Enterprise SIP Service (TeamLink - enabled) - The Customer uses onsight.librestream.com and their private SIP Infrastructure but also uses TeamLink. This requires onsight.librestream.com and all the TeamLink Servers to be added to the Firewall rules or Proxy White List. In this scenario the Customer's SIP Server must have a Public interface for TeamLink connectivity.

The following table lists Protocols, Ports and Transport for the Onsight Services.

Table: Onsight Required Ports 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

*Subject to change if the Customer is using their own SIP Server.

The following table lists the IP addresses for Onsight Account Manager, Onsight SIP Server, sip.librestream.com and Media Servers. If the Customer is using their own SIP Server the Ports must match that configuration.

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) [3]	*.librestream.com
Onsight Connect Load Balancer	
onsight.librestream.com	HTTP, HTTPS
TeamLink Load Balancer	
tcm.librestream.com	HTTP, HTTPS
TeamLink Cluster Manager	
tcm1.librestream.com	HTTP, HTTPS SIP, RTP, STUN
tcm2.librestream.com	HTTP, HTTPS SIP, RTP, STUN
tcm3.librestream.com	HTTP, HTTPS SIP, RTP, STUN
TeamLink Servers	
teamlink1.librestream.com	HTTP, HTTPS SIP, RTP, STUN
teamlink2.librestream.com	HTTP, HTTPS SIP, RTP, STUN
teamlink3.librestream.com	HTTP, HTTPS SIP, RTP, STUN
teamlink4.librestream.com [2]	HTTP, HTTPS SIP, RTP, STUN
teamlink5.librestream.com	HTTP, HTTPS SIP, RTP, STUN
teamlink6.librestream.com	HTTP, HTTPS SIP, RTP, STUN
teamlink7.librestream.com	HTTP, HTTPS SIP, RTP, STUN
teamlink10.librestream.com [1,2]	HTTP, HTTPS SIP, RTP, STUN

Notes:

1) These are required for backwards compatibility for existing customers
2) These are required where customers may have a single TeamLink server configuration instead of clustered.
3) The wild card character may be different depending on the Web Proxy in use.

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.)

Table: Sample SIP Communication Firewall Configuration

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

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

4. Onsight Endpoint SIP Server Registration

Onsight Endpoints support the ability to configure both a Public and Private SIP Server. The Public server is used when the Onsight endpoint is located outside the Firewall and must connect to a SIP Server that has a Public interface e.g. Cisco VCS Expressway. The Private Server is used when the Onsight endpoint is located inside the Firewall on an internal network and registers to an internal SIP Server with a private interface, e.g. Cisco VCS Control.

When both the Public and Private Server settings are configured the Onsight endpoint will determine which one to register to by first sending a SIP OPTIONS message to the Private server. If the Private server responds, the Onsight endpoint registers to it. If the Private server does not respond the Onsight endpoint will attempt to register to the Public server.

If only one of the Public or Private Server settings is configured, the Onsight endpoint will attempt to register to it.

5. Onsight TeamLink HTTPS Tunneling Server

In situations where it is not possible or practical to open the required SIP and UDP ports on the Firewall, TeamLink can be used to tunnel all SIP and Media traffic encapsulated in HTTPS packets to a TeamLink Server. The TeamLink Server will proxy all traffic to the SIP Server on behalf of the Onsight Endpoint behind the Firewall. The advantage of this method is that TeamLink can use existing open ports on the Firewall, TCP 443 for HTTPS (or TCP 80 for HTTP if preferred).

For details on TeamLink please refer to the TeamLink application note.

5.3 TeamLink - Firewall Detect

Firewall Detect is an Onsight System feature that tests the ports on the local Firewall to determine the best method for SIP Registration or rather when to use TeamLink versus direct registration to the SIP server. *Firewall Detect is only active if TeamLink is enabled.* The test is conducted by sending test traffic to a Test Server, one of either: the TeamLink Cluster Manager, the TeamLink server or the Onsight SIP Server. The destination is dependent on configuration of the Onsight endpoint's SIP Detection Method. In most cases the Test Server will be sip.librestream.com.
If Firewall Detect determines that the local firewall ports are open to the Test server, then the Onsight Endpoint assumes the ports are also open to the SIP Server. That is, if SIP ports are open to the Test Server the Onsight Endpoint attempts to SIP register directly to the SIP Server; if SIP ports are closed the Onsight Endpoint will use TeamLink to register to the SIP Server indirectly. In some cases the Test Server is the SIP Server.

For details on Firewall Detect please refer to the TeamLink application note.

The Firewall Detect test needs to have the ports open to the TCM Servers or TeamLink Serves to properly determine when using TeamLink is required. TeamLink configuration on the Onsight endpoint determines whether TCM or TeamLink Servers are the target for the Firewall Detect test.

6. For More Information

If you need assistance please contact Librestream at support@librestream.com.