



APP NOTES

Onsight Connect Network Requirements

January 2018

Table of Contents

1. Overview.....	4
1.1 Onsite Connect Solution Architecture.....	4
1.2 Three Stages of Onsite Connectivity.....	5
2. Web (HTTP/S) Proxy Configuration	6
3. Firewall Requirements – Allowing SIP Traffic	6
4. Onsite Endpoint SIP Server Registration	10
5. Onsite TeamLink HTTP/S Tunneling Service.....	10
5.3 TeamLink - Firewall Detect.....	10
6. Connectivity Summary	14
6.4 Default Configuration.....	14
6.5 Private SIP Server Configuration.....	15
7. For More Information.....	16

Document Revision

Librestream

Onsite Connect Network Requirements

Doc #: 400210-10

January 2018

Information in this document is subject to change without notice.

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

Copyright © 2006–2018 Librestream Technologies, Incorporated.

All rights reserved.

Name of Librestream Software Onsite Connect

Copyright Notice: Copyright 2004–2017 Librestream Technologies Incorporated. All Rights Reserved.

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.

Trademark Notice: Librestream, the Librestream logo, Onsite, Onsite Connect, Onsite Mobile, Onsite Enterprise, Onsite License Manager, Onsite TeamLink, Onsite Platform Manager and Onsite Management Suite are either registered trademarks or trademarks of Librestream Technologies Incorporated in Canada, the United States and/or other countries. All other trademarks are the property of their respective owners.

1. Overview

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

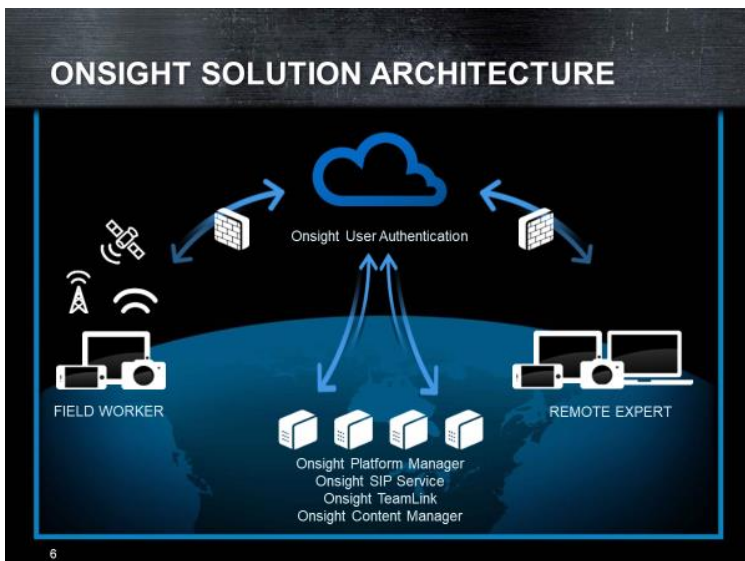
Onsite Connect Services consists of 3 distinct functions: Onsite Platform Manager (OPM), Onsite SIP Service, and Onsite TeamLink.

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

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

Onsite 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 Onsite endpoint. This method is only recommended when it is not possible to traverse the Firewall using the standard SIP ports.

1.1 Onsite Connect Solution Architecture



Your Enterprise Firewall and/or Web Proxy must allow traffic to onsight.librestream.com, Onsite 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 Onsite Endpoints have accurate date and time set to allow authentication.

1.2 Three Stages of Onsite Connectivity

1.2.1 Onsite Endpoint Authentication

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

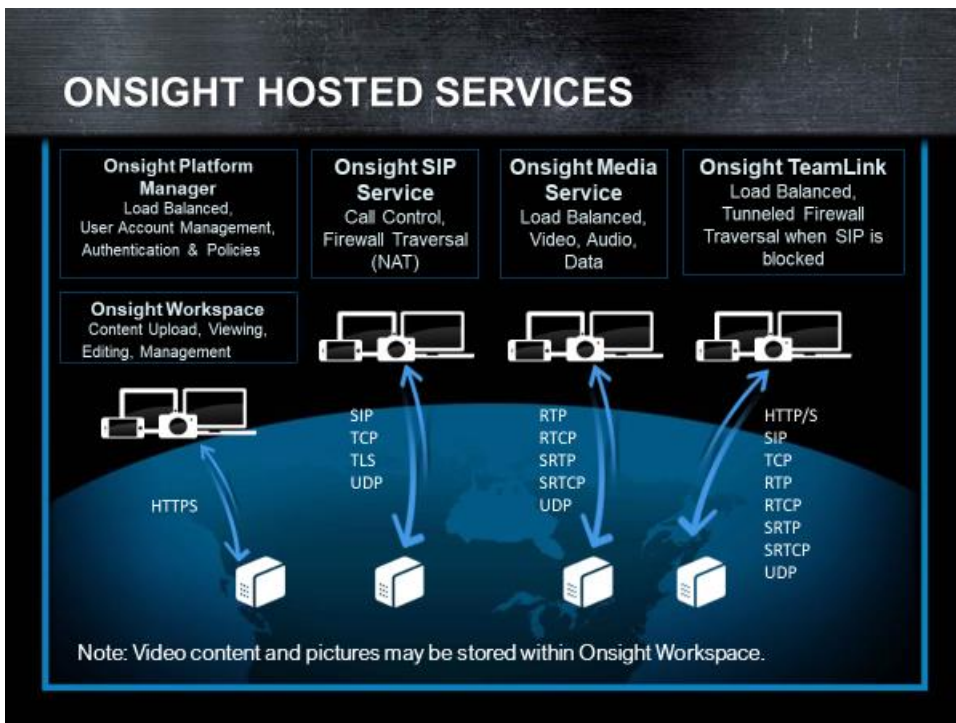
1.2.2 Onsite Connect SIP Registration

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

1.2.3 Onsite TeamLink Registration (Optional)

The Onsite Endpoint has the option of using Onsite 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 Onsite 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.

Onsite Connect Service Providers



2. Web (HTTP/S) Proxy Configuration

Onsite Connect and TeamLink use HTTPS (HTTP is optional) to communicate with the Onsite Connect service and tunnel SIP traffic. It is 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 Onsite 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 to allow an Onsite endpoint to connect to the Onsite Service, SIP and Media Servers.

There are 4 basic Firewall scenarios:

Definitions:

Onsite Service = onsite.librestream.com (Onsite Platform Manager)

Onsite SIP Service = Librestream's Hosted SIP Service

Enterprise SIP Service = Customer's private SIP Infrastructure (Cisco VCS or alternative)

Migrate across Firewall = Onsite endpoints connect both inside and outside the Enterprise network.

Onsite Connect including Onsite SIP Service (TeamLink - enabled) - The Customer requires onsite.librestream.com with sip.librestream.com and TeamLink Connectivity. In this scenario, the Onsite Endpoint is migrating inside and outside the Customer's 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.
Firewall Detect Test Server: SIP Server - Full (sip.librestream.com).

Onsite Connect including Onsite SIP Service (TeamLink - not required) - The Customer requires onsite.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 do not migrate across the Firewall or will operate in an unrestricted hosted environment.
Firewall Detect Test Server: not applicable.

Onsite Connect with Enterprise SIP Service (TeamLink - enabled) - The Customer uses onsite.librestream.com and their private SIP Infrastructure but also uses TeamLink. This requires onsite.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.
Firewall Detect Test Server: SIP Server – Basic (Customer's private SIP Server).

Onsite Connect with Enterprise SIP Service (TeamLink - not required) - The Customer requires onsite.librestream.com but uses their own SIP infrastructure. This will require onsite.librestream.com being added to either the Firewall Rules or

the Proxy White List. There is no need to use TeamLink since endpoints do not migrate across the Firewall or will operate in an unrestricted hosted environment.

Firewall Detect Test Server: SIP Server – Basic (Customer's SIP Server).

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

3.2.4 Table: Onsite Required Ports and Protocols

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

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

The following table lists Transport, Ports and Protocols used by TeamLink Services.

3.2.5 Table: TeamLink Required Ports and Protocols

Transport	Ports	Protocols
TCP	5060	SIP
TCP	5061	SIP-TLS
TCP	443	HTTPS
TCP	80	HTTP
UDP	58024, 58523	STUN
UDP	3478	STUN

The following table lists the IP addresses for Onsite Platform Manager, Onsite 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 Onsite Hosted Service. They must be accessible from the network via the Firewall or Proxy.

3.2.6 Table: Onsite Hosted Servers

Server		
Proxy White List (wild card) ¹	*.librestream.com	
Onsite 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
Onsite Workspace		
workspace.librestream.com		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:

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 Onsite 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 Onsite 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).

3.2.7 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, HTTP, HTTPS

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. Onsite Endpoint SIP Server Registration

Onsite Endpoints support the ability to configure both a Public and Private SIP Server. The Public server is used when the Onsite 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 Onsite 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 Onsite 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 Onsite endpoint registers to it. If the Private server does not respond, the Onsite endpoint will attempt to register to the Public server.

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

5. Onsite TeamLink HTTP/S Tunneling Service

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 Onsite 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 Onsite 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 tests are only active if TeamLink is enabled.** The test is conducted by sending test traffic to a **Test Server**, one of either: the TeamLink server or the Onsite SIP Server. The destination is dependent on configuration of the Onsite 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 Onsite Endpoint assumes the ports are also open to the SIP Server. That is, if SIP ports are open to the **Test Server** the Onsite Endpoint attempts to SIP register **directly** to the SIP Server; if SIP ports are closed the Onsite 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 TeamLink Servers to properly determine when using TeamLink is required.

5.3.8 TeamLink - SIP Detection Method

TeamLink will behave according to the SIP Detection Method that is configured on the endpoint. The following tables show the ports when sending traffic to the targeted servers. The Targeted Server is specified by the SIP Detection Method.

If any portion of the TeamLink test fails, then Onsight Connect will default to using TeamLink as the communication method.

TeamLink will determine if it is able to access the targeted servers as determined by the configured SIP Detection method (Full, Basic or TeamLink). If it cannot, TeamLink will tunnel all SIP and Media traffic through the Firewall to the TeamLink Servers.

TeamLink Test Behavior

- Proxy Settings – if enabled, HTTP port 80 is not allowed by TeamLink and is not tested.
- TeamLink 'Allow HTTP Registration' – if enabled TCP port 80 is part of the TeamLink test, if not, it's excluded.
- SIP ports 5060 and 5061 are tested regardless of which SIP transport is selected (TCP or TLS) for the client.

What causes Teamlink test failures?

- The presence of a SIP AWARE NAT on the network will cause the TeamLink test to fail.
- Blocked ports

5.3.9 Which SIP Detection Method do I use?

SIP Server Full

This is used when you are using the Onsight SIP Service, sip.librestream.com. This is the default configuration when using Onsight Connect. The Corporate Firewall must allow communication as outlined in the table below.

SIP Server Full – Targeted Server: sip.librestream.com	
sip.librestream.com	STUN, SIP, SIP-TLS, UDP
tcm.librestream.com	HTTP, HTTPS

5.3.10 Table: Onsight Required Ports and Protocols

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

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

The following table lists Transport, Ports and Protocols used by TeamLink Services.

5.3.11 Table: TeamLink Required Ports and Protocols

Transport	Ports	Protocols
TCP	5060	SIP
TCP	5061	SIP-TLS
TCP	443	HTTPS
TCP	80	HTTP
UDP	58024, 58523*	STUN
UDP	3478	STUN

*These ports are tested but the full range of 15000 – 65000 must be allowed on the Firewall.

Endpoint Behaviour:

Behind the Corporate Firewall the TeamLink will contact sip.librestream.com and tcm.librestream.com and determine if TeamLink is needed. The test should pass and all SIP and Media communication should be directed to the sip and media servers. The assumption is that all the required ports have been opened on the Corporate Firewall.

Outside of the Corporate Firewall TeamLink may or may not be able to contact sip.librestream.com and tcm.librestream.com directly. If the test passes, direct communication is used, if the test fails, TeamLink is the method of communication.

SIP Server Basic

This is used when you are using the Onsite SIP Service, sip.librestream.com. The Corporate Firewall must allow communication as outlined in the table below. This is not recommended for most installations since it doesn't test for SIP AWARE NAT or the Media ports. The Corporate Firewall must allow communication as outlined in the table below.

SIP Server Basic – Targeted Server: sip.librestream.com (or a private server)	
sip.librestream.com (or the customer's private SIP Server)	SIP, SIP-TLS, STUN (UDP is not included in this test.)
tcm.librestream.com	HTTP, HTTPS

*excludes UDP 58024, 58523 and SIP AWARE NAT test.

Endpoint Behaviour:

Behind the Corporate Firewall the endpoint will contact sip.librestream.com and tcm.librestream.com and determine if TeamLink is needed. The test should pass and all SIP and Media communication will be direct to the sip and media servers. The assumption is that all the required ports have been opened on the Corporate Firewall.

Outside of the Corporate Firewall the TeamLink test may or may not be able to contact sip.librestream.com and tcm.librestream.com directly. If the test passes, direct communication is used, if the test fails, TeamLink is the method of communication. A false positive test may occur if the endpoint can contact sip.librestream.com and tcm.librestream.com but since the media ports aren't tested, direct communication may fail during a call. I.E. if the media ports are blocked TeamLink will not detect this during the test.

TeamLink

This is used when you are using a private SIP Server such as a Cisco VCS. Third Party SIP Servers do not respond to the Firewall Detect Test so the test must be run against TeamLink Servers. Use this method when you have Mobile users who will access your SIP Servers from unknown network environments e.g. Guest Network from a Partner or 3rd Party Vendor. If your Mobile user can't access pass the Firewall Detect test at a remote location, they will use TeamLink to tunnel all SIP and Media to your SIP Server. The Corporate Firewall must allow communication as outlined in the table below.

Endpoint Behaviour:

Behind the Corporate Firewall the endpoint will contact the TeamLink servers and determine if TeamLink is needed. The test should pass and all SIP and Media communication will be direct to the sip and media servers. The assumption is that all the required ports have been opened on the Corporate Firewall.

Outside of the Corporate Firewall the TeamLink test may or may not be able to contact the TeamLink servers to test all ports. If the test passes, direct communication is used, if the test fails, TeamLink is the method of communication. The assumption is that if the TeamLink test fails we will still be able to use HTTPS/HTTP to contact TeamLink.

TeamLink – Targeted Server: TeamLink*.librestream.com	
Any one of the following TeamLink servers will be targeted:	
TeamLink Load balancer	HTTP, HTTPS
tcm.librestream.com	54.200.211.44 54.201.116.193 54.149.122.186 54.149.14.174 54.149.178.194 54.191.206.117
Teamlink cluster managers	STUN, HTTP, HTTPS, SIP, SIP-TLS, UDP
tcm1.librestream.com	54.200.203.117
tcm2.librestream.com	54.213.116.106
tcm3.librestream.com	54.218.72.77

TeamLink - Private Server Pool

TeamLink can be configured to bypass the TeamLink Load balancer and always register to the same TeamLink Server, this is referred to as a Private Server Pool. When an endpoint is configured this way the TeamLink test will run against the private TeamLink Server.

Endpoint Behaviour:

Behind the Corporate Firewall the endpoint will contact the TeamLink server, only one server will be involved in the test to determine if TeamLink is needed. The test should pass and all SIP and Media communication will be direct to the sip and media servers. The assumption is that all the required ports have been opened on the Corporate Firewall.

Outside of the Corporate Firewall the TeamLink test may or may not be able to contact the TeamLink server to test all ports. If the test passes, direct communication is used, if the test fails, TeamLink is the method of communication. The assumption is that if the TeamLink test fails we will still be able to use HTTPS/HTTP to contact TeamLink.

TeamLink – Private Server Pool	
TeamLink Servers	STUN, HTTP, HTTPS, SIP, SIP-TLS, UDP
teamlink1.librestream.com	54.200.207.108
teamlink2.librestream.com	future
teamlink3.librestream.com	future
teamlink4.librestream.com	54.200.203.116
teamlink5.librestream.com	future
teamlink6.librestream.com	future
teamlink7.librestream.com	future
teamlink10.librestream.com	54.201.6.72

*The load balancers, onsite.librestream.com and tcm.librestream.com, are not targeted during the Firewall Detect Test.

Note: The default configuration of Onsite Connect for Firewall detect will NOT test HTTP port 80 due to these settings:

1. Proxy - enabled within Onsite Connect, i.e. it is set to 'Use System Settings' or 'Manual'. This forces the use of HTTPS port 443.
2. TeamLink – 'Allow HTTP Registration' is set to 'Off', again this forces the use of HTTPS port 443.

ICMP message starts each Firewall Detect test to TCM-LB and TCM-MGR.

6. Connectivity Summary

Configure the firewall to allow the following connections based on your Onsite Platform Manager policies for SIP and TeamLink.

6.4 Default Configuration

The following is required when using Onsite Connect including Onsite SIP Services.

6.4.1 Onsite User Authentication and Authorization

Server		
Proxy White List (wild card) ¹	*.librestream.com	
Onsite 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	TCP, 443, HTTPS

6.4.2 Onsite SIP and Media Services

SIP Servers		
sip.librestream.com	54.213.166.17	UDP, 3478, STUN* UDP, 58024, STUN* UDP, 58523, STUN* TCP, 5060, SIP TLSv1.2, 5061, SIP

*Required if TeamLink is enabled

Media Servers	
54.200.152.202	UDP, 15000 – 65000, RTP, RTCP
54.201.34.23	UDP, 15000 – 65000, RTP, RTCP
54.213.38.103	UDP, 15000 – 65000, RTP, RTCP
54.218.75.97	UDP, 15000 – 65000, RTP, RTCP
54.213.75.101	UDP, 15000 – 65000, RTP, RTCP
54.200.248.252	UDP, 15000 – 65000, RTP, RTCP

6.4.3 TeamLink (SIP Detection Method: SIP Server Full)

TeamLink – Targeted Server: TeamLink*.librestream.com		
Any one of the following TeamLink servers will be targeted:		
TeamLink Load balancer		

tcm.librestream.com	54.200.211.44 54.201.116.193 54.149.122.186 54.149.14.174 54.149.178.194 54.191.206.117	TCP, 80, HTTP TCP, 443, HTTPS
---------------------	--	----------------------------------

TeamLink Servers		
teamlink1.librestream.com	54.200.207.108	TCP, 80, HTTP TCP, 443, HTTPS
teamlink2.librestream.com	future	Same as above
teamlink3.librestream.com	future	Same as above
teamlink4.librestream.com	54.200.203.116	Same as above
teamlink5.librestream.com	future	Same as above
teamlink6.librestream.com	future	Same as above
teamlink7.librestream.com	future	Same as above
teamlink10.librestream.com	54.201.6.72	Same as above

6.5 Private SIP Server Configuration

The following configuration is required when using Onsight Connect with a Private SIP Server.

6.5.1 Onsight User Authentication and Authorization

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	TCP, 443, HTTPS

6.5.2 Private SIP and Media Services

SIP Servers		
sip.yourcompany.com udp.yourcompany.com	addresses	TCP, 5060, SIP TLSv1.2, 5061, SIP UDP, port range, RTP, RTCP

6.5.3 TeamLink (SIP Detection Method: TeamLink)

TeamLink – Targeted Server: TeamLink*.librestream.com		
Any one of the following TeamLink servers will be targeted:		
TeamLink Load balancer		

tcm.librestream.com	54.200.211.44 54.201.116.193 54.149.122.186 54.149.14.174 54.149.178.194 54.191.206.117	TCP, 80, HTTP TCP, 443, HTTPS
Teamlink cluster managers	STUN, HTTP, HTTPS, SIP, SIP- TLS, UDP	
tcm1.librestream.com	54.200.203.117	UDP, 3478, STUN UDP, 58024, STUN UDP, 58523, STUN TCP, 80, HTTP TCP, 443, HTTPS TCP, 5060, SIP TLSv1.2, 5061, SIP
tcm2.librestream.com	54.213.116.106	Same as above
tcm3.librestream.com	54.218.72.77	Same as above

TeamLink Servers		
teamlink1.librestream.com	54.200.207.108	TCP, 80, HTTP TCP, 443, HTTPS
teamlink2.librestream.com	future	
teamlink3.librestream.com	future	
teamlink4.librestream.com	54.200.203.116	
teamlink5.librestream.com	future	
teamlink6.librestream.com	future	
teamlink7.librestream.com	future	
teamlink10.librestream.com	54.201.6.72	

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

7. For More Information

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