ON SIGHT

APP NOTES

TeamLink and Firewall Detect

July 2016

LIBRESTREAM

Table of Contents

Document Revision
Librestream
Onsight Connect Network Requirements
Doc #: 400218-03
July 2016

1. Overview

This document provides a description of TeamLink services for Onsight Connect clients. Firewall Detect is a feature included in each client that tests whether the Firewall allows network traffic to the Onsight servers.

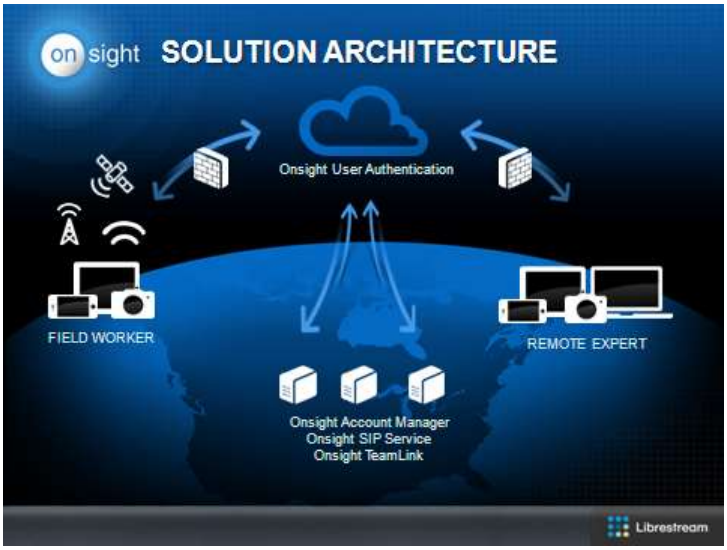
1.1 When is TeamLink Used?

Onsight TeamLink is for situations when it is not possible to open SIP and Media ports on the Firewall, in these cases TeamLink is used to tunnel all SIP and Media traffic encapsulated in HTTPS packets to a TeamLink Server. The TeamLink Server proxies all traffic to the SIP and Media Servers 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).

TeamLink is not used to communicate with Onsight Account Manager. TeamLink is only used for SIP and Media Call Control.

Direct communication with the SIP Server is the preferred method of establishing communication between Onsight endpoints. Whenever possible the firewall should be configured to allow direct communication to the SIP and Media Servers.

1.2 Onsight Connect Solution Architecture



Onsight Connect consist of 3 distinct services; 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.

*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.

1.3 Three Stages of Onsight Connectivity

1.3.1 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.

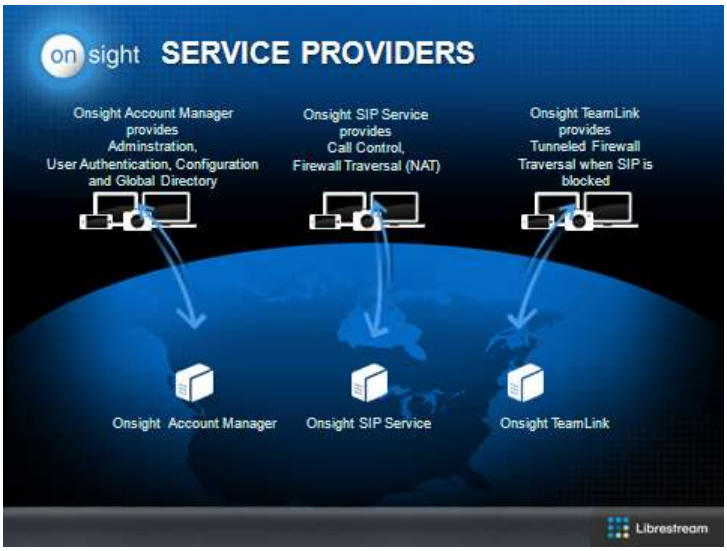
1.3.2 Onsight Connect SIP Registration

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.

1.3.3 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.

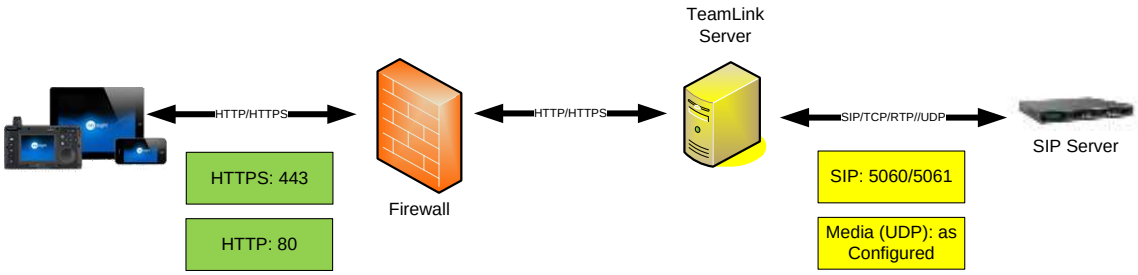
Onsight Connect Service Providers



2. Web (HTTP/S) Proxy Configuration

Onsight Connect and TeamLink use HTTPS to communicate with the Onsight Connect service and tunnel SIP and Media 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 Onsight URIs to a Proxy white list at your location.

When using TeamLink the Onsight Endpoint will encapsulate SIP (TCP) and Media (RTP/RTCP/UDP) traffic in HTTPS protocol packets. The TeamLink Server receives these packets and strips off the HTTPS encapsulation before forwarding them to the SIP (and Media Servers). The SIP Server will send responses to the TeamLink Server. TeamLink encapsulates the packets before sending them back to the Onsight Endpoint.
When TeamLink is enabled Onsight Endpoints will first contact a TeamLink Cluster Manager (TCM) which will assign a TeamLink Server to the endpoint. The Onsight Endpoint will then register to the TeamLink Server.



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.*

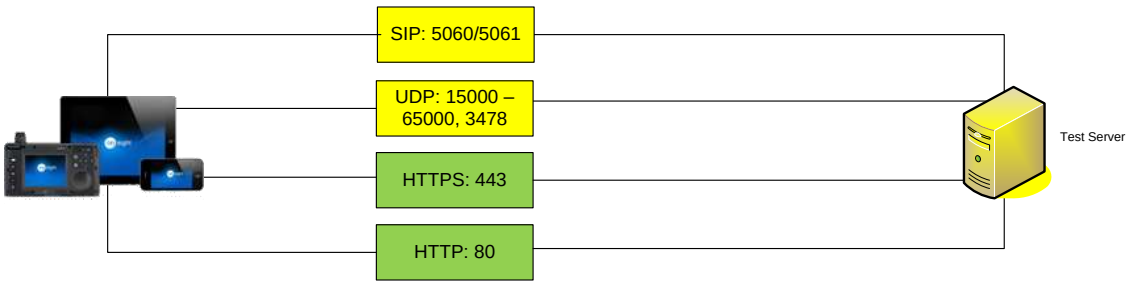
Direct SIP Traffic is not sent through a Web Proxy, it is only routed through a Web Proxy when TeamLink is enabled and the connection method is HTTPS or HTTP. The Firewall Detect test determines the suitable connection method: SIP, HTTPS or HTTP, depending on the results of the Firewall test.

3. Firewall 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.

If the Firewall test detects that the local firewall ports are open to the Test server, then the Onsight Endpoint sends SIP and Media traffic directly to SIP and Media Servers. If ports are determined to be closed the Onsight Endpoint will use TeamLink to register to the SIP Server indirectly.

Firewall Detect determines the best method of SIP Registration based on the results of the Firewall port tests.:



The tested range of SIP, HTTP, HTTPS and UDP ports is configured on the Onsight Endpoint by Librestream. They are based on the required ports for Librestream's Onsight SIP Service.

The Firewall Detect Test uses Session Traversal Utilities for NAT (STUN) protocol to determine the mapped Public IP address of the Firewall. STUN traffic is sent to UDP destination port 3478 of the Test Server by the Onsight Endpoint. STUN is also used to test UDP ports 58024 and 58523.

TeamLink, won't correctly interpret the Firewall Detect test if the Firewall has been configured to block SIP and Media ports to either the TCM or TeamLink server but allow HTTP/S. This may result in the use of TeamLink's HTTPS tunneling when it is not required. This is because the SIP ports are tested using either TCM or TeamLink as the destination. If the Firewall blocks SIP to either this will be reported as 'SIP blocked' even though the Firewall may allow SIP packets to a specific SIP Server.

3.3.4 Firewall Detect – Test Server Options:

Firewall detection occurs through different paths depending on the configuration of the Onsight Client. The configuration is controlled by the OAM Client Policy under Firewall Detect-SIP Detection Method.

Firewall Detect Tests are only run when TeamLink is enabled.

TeamLink is under Cluster management control (tcm.librestream.com). This means each endpoint contacts the cluster manager and is then assigned to a TeamLink Cluster Manager (TCM). The Cluster Manager assigns the Onsight Client a TeamLink server dynamically. At that point the Onsight Client connects to the TeamLink server directly.

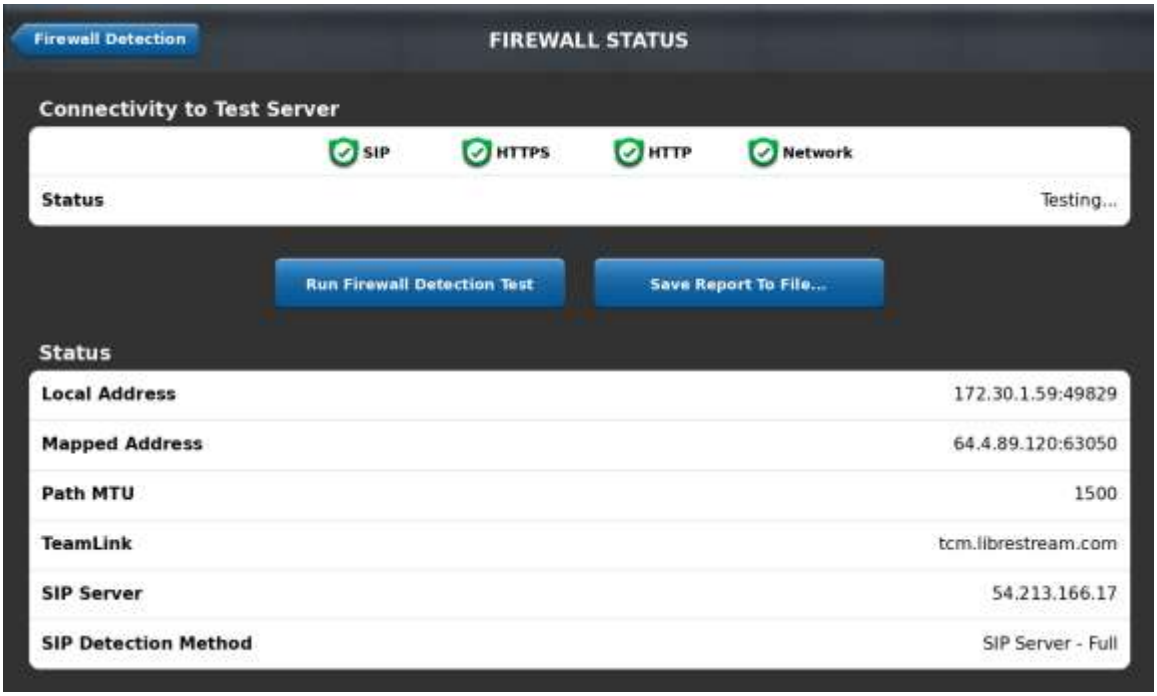
TCM communication:

A. HTTP/HTTPS tests are done directly to the configured TeamLink Cluster Manager server.
B. SIP tests are done according to the following:
   1. If a private SIP server is configured, a simple OPTIONS ping test will be done to the configured private SIP server.
   2. If SIP Detection Method is configured to be SIP Server – Full. Then the Onsight client will interrogate the configured public SIP server with a full SIP/STUN test.
   3. If SIP Detection Method is configured to be SIP Server – Basic. Then the Onsight client will interrogate the configured public SIP server with a simple OPTIONS ping test.
   4. If SIP Detection Method is configured to be TeamLink. Then the Onsight client will interrogate the configured TeamLink Cluster Manager server with a full SIP/STUN test.

Customers who are using 3rd party SIP Servers must use the SIP Server – Basic method for SIP Detection. The 3rd Party SIP Server must respond to SIP OPTIONS requests in order for the Firewall Detect Test to function correctly.

3.3.5 Firewall Detection Status

For a summary of all the Firewall Detect settings and status, select 'Details…' and the following screen will appear.



The following table describes each of the fields shown above.

Client state	Indicates whether Firewall Detect is active
Connectivity	Reports the Status of the SIP Registration methods and Network. Connection Method is Open/Network is connected Connection Method is Disabled Connection Method is Blocked
Local Address	Reports the Local IP address of the Host PC running Onsight Connect for PC
Mapped Address	Reports the external IP address of the Firewall the PC sits behind
Path MTU	Reports the size of the Maximum Transmission Unit for the Host PC
TeamLink Server	TeamLink Load Balancer
SIP Server	SIP Registration Server
SIP Detection Method	SIP test method for Firewall Detect
UDP Connectivity	Reports the status of the listed UDP ports on the Firewall
SIP Connectivity	Reports the status of the listed TCP ports on the Firewall

The UDP test checks the ports used for the media such as audio, video and data. For efficiency, set the boundaries of the port range you would like to test as in the example above by separating them by commas e.g. 58024, 58523. Testing a complete range e.g. 58024 – 58523 could take an excessive amount of time.

The SIP test will check for TCP ports 5060 and 5061 and it will test for SIP aware Firewalls. The SIP Aware NAT test is a SIP header test looking for Public IP addresses being inserted in the SIP header in place of private LAN IP addresses. When a SIP Aware NAT is present it can cause confusion for the SIP Server so it is best to use SIP-TLS as the transport. SIP-TLS will encrypt the SIP headers and make these unavailable for inspection by the SIP Aware NAT.

4. Allowing SIP Traffic - Firewall Requirements

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 and 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, 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

5. 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.

6. For More Information

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