Application Note

Onsight Connect Network Requirements V6.1

Librestream

1 Onsight Connect Service Network Requirements

1.1 Onsight Connect Overview

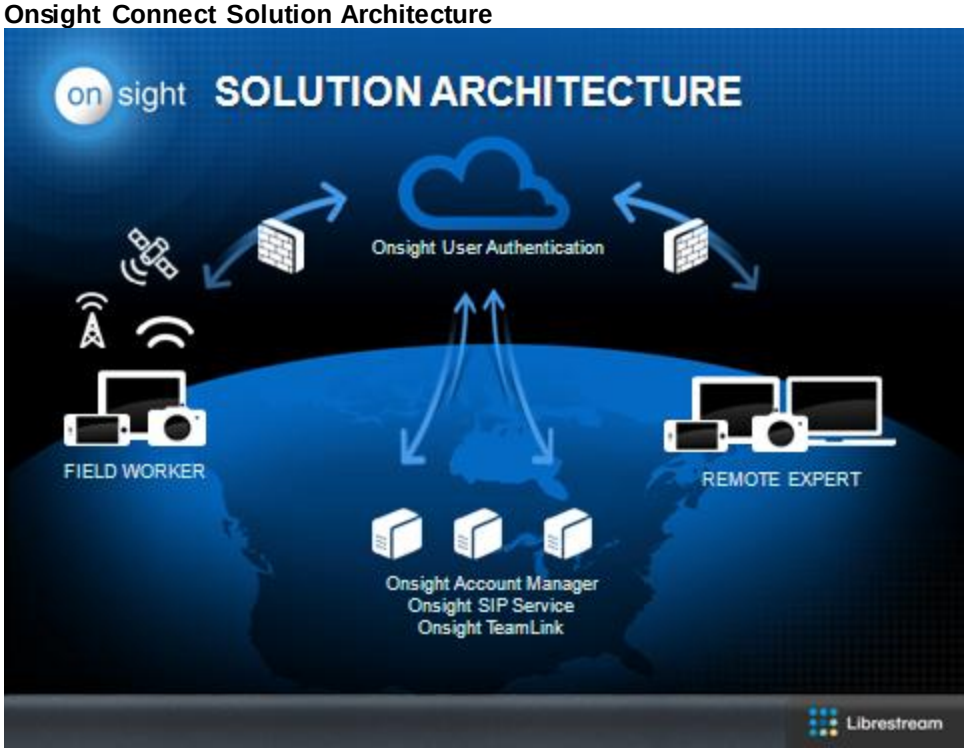
This document provides a description of the network requirements for Onsight Connect on a Local Area Network and on the Internet.

Onsight Connect relies on the HTTPS protocol for communication between the Onsight endpoints and the Onsight Connect Service. All communication is encrypted using SSL. When a user logs in to their Onsight endpoint they are authenticated against their user credentials by the Onsight Connect service. Once the Onsight user is authenticated their endpoint automatically receives configuration settings from the Onsight Connect service and they can begin using Onsight Connect. Onsight Connect only handles user authentication and configuration of the Onsight endpoint all other aspects of Media collaboration is handled by the SIP Service.

HTTPS uses TCP port 443

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

Onsight Connect Solution Architecture



List of Required Network Protocols:

1. SIP (TCP 5060)
2. SIP-TLS (TCP 5061)
3. HTTPS (TCP 443)
4. HTTP (TCP 80)
5. Audio/Video/Data (UDP)
6. STUN (UDP port 3478)*
7. Cisco Presence: client configuration web service (TCP 8443)

For details on setting up Onsight Connect refer to the ***Onsight Account Manager User Manual***.
*Only used if TeamLink is enabled.

1.2 Onsight Connect Servers

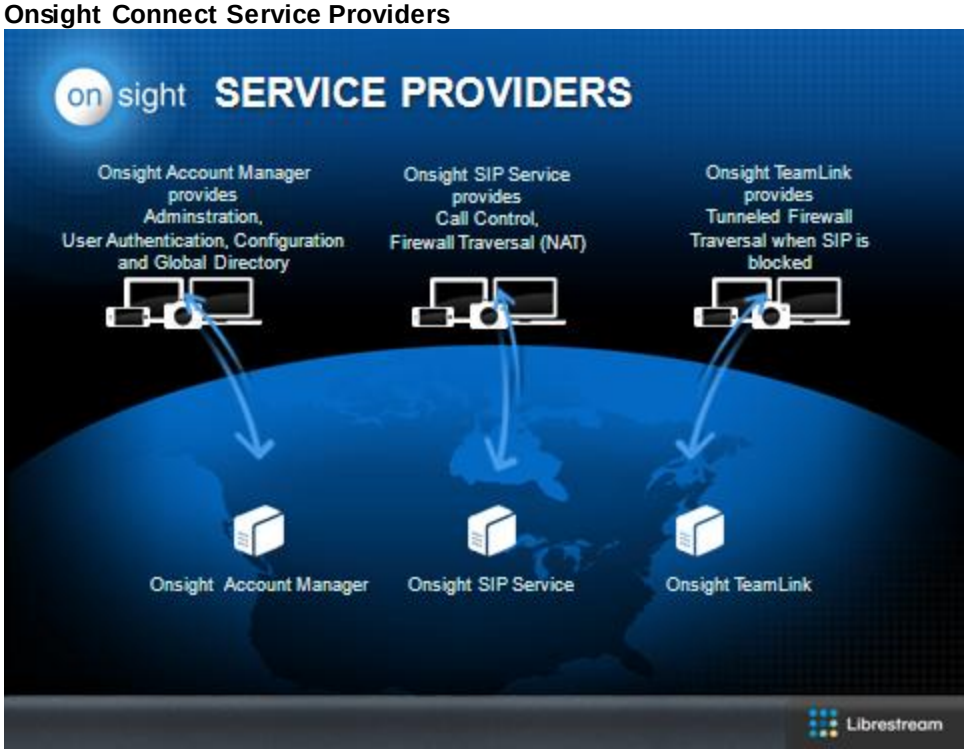
Onsight Connect is delivered in the cloud by Cloud hosted Servers to make it easier for users to access the software. Video recordings and images captured with Onsight are not streamed through or stored in the Onsight Connect Server.

Cloud data storage is limited to the user account information and global contact list, accessible only to the assigned Onsight users.

The optional Onsight TeamLink and Onsight SIP services stream media but do not store any video recordings or images in the cloud. Customers who are concerned about content security with these optional services can enable AES 128-key encryption and secure call control with SIP-TLS.

- onsight.librestream.com (50.57.49.192)
- siphost.librestream.com (64.4.89.118)
- teamlink10.librestream.com (50.57.93.169)

Onsight Connect Service Providers

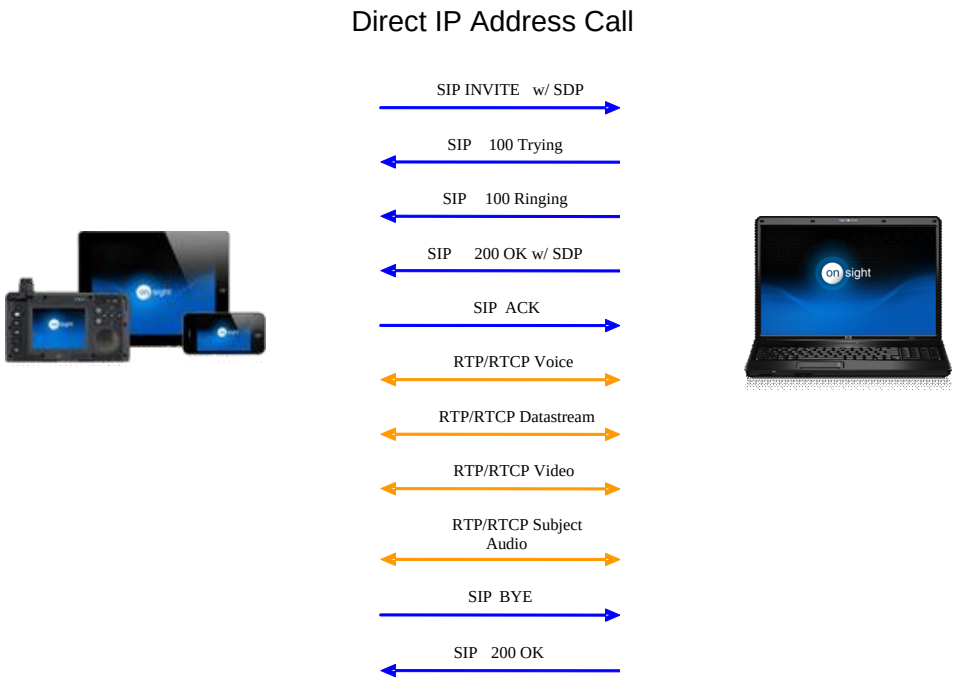


1.2.1 SIP Overview

Onsight Connect uses Session Initiation Protocol (SIP) to establish an audio and video communication session between endpoints. Communication can occur directly between the Onsight Endpoints when they are on the same LAN or it can occur via a SIP Proxy Server when they exist on different networks.

1.2.2 Direct IP Calling

When both Onsight endpoints exist on the same LAN they can communicate directly using the IP address of each Onsight endpoint as the ***contact address*** to route traffic between each other. Table 2.1 describes the source ports for the SIP and UDP traffic involved in an Onsight Collaboration session.
TCP port 5060 is used for the SIP Protocol and UDP ports 6000 – 6200 are used for Media (audio, video, and data).



The Onsight Connect will attempt to open the following Source ports on the PC to initiate sending traffic to the Onsight Device:

Default Source Ports for SIP, RTP, RTCP*
SIP (TCP): random
Video (RTP/RTCP): 6000/6001
Subject audio (RTP/RTCP): 6002/6003
Voice (RTP/RTCP): 6004/6005
Data (RTP): 6006

**Each RTP stream has an RTCP stream associated with it, e.g. video happens over RTP 6000, and its associated RTCP stream is over 6001. RTCP provides statistics on the RTP stream.*

However, if these ports are already in use on a PC, Onsight Connect will increment the source port until it finds a free one. So the possible range of UDP source ports starts at 6000 and is determined by availability of UDP ports on the Onsight Connect Host PC.

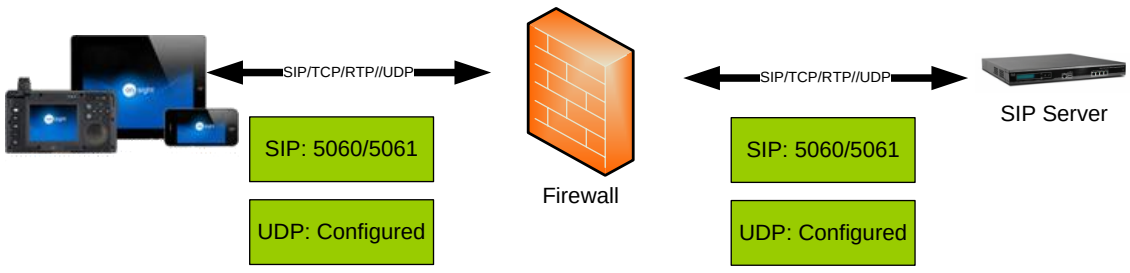
The Onsight Device will always use these source ports (6000/6001, 6002/6003, 6004/6005, 6006) because it is a closed system.

Destination Ports when using Direct IP Calls:

The destination ports are usually the same so that the video stream's source port is 6000 and it is sending to destination port 6000 on the Onsight Device. (They're both on the same LAN and communication directly with each other.) The SIP destination port is always 5060 or 5061 (for SIP-TLS).

1.2.3 Direct SIP Server Registration

Firewall/NAT traversal is required to establish a session when the endpoints are not located on the same LAN. This is accomplished by using a SIP Server. Each endpoint registers to the SIP Server which is typically located outside of the Firewall. The SIP Server acts as a proxy and directs SIP messaging and data traffic between the endpoints.
Each endpoint is assigned a unique Uniform Resource Identifier (URI) by the SIP Server which is used as the ***contact address*** for the endpoint. Its format is user@sipdomain.com.



When the Onsight endpoints are registered to the SIP Server, both the Onsight Device and Onsight Connect for PC can initiate calls by calling the ***contact address*** (URI) of the other endpoint.

The Onsight Connect for PC Software will attempt to open the following Source ports on the PC to initiate sending traffic to the SIP Server:

Default Source Ports for SIP, RTP, RTCP			
Transport	**Protocol**	**Source Port**	**Destination Port**
SIP	TCP	Random	5060/5061
Video	RTP/RTCP (UDP)	6000/6001	Dictated by SIP Server
Subject Audio	RTP/RTCP (UDP)	6002/6003	Dictated by SIP Server
VoIP	RTP/RTCP (UDP)	6004/6005	Dictated by SIP Server
Data	RTP (UDP)	6006	Dictated by SIP Server

**Each RTP stream has an RTCP stream associated with it, e.g. video happens over RTP 6000, and its associated RTCP stream is over 6001. RTCP provides statistics on the RTP stream.*

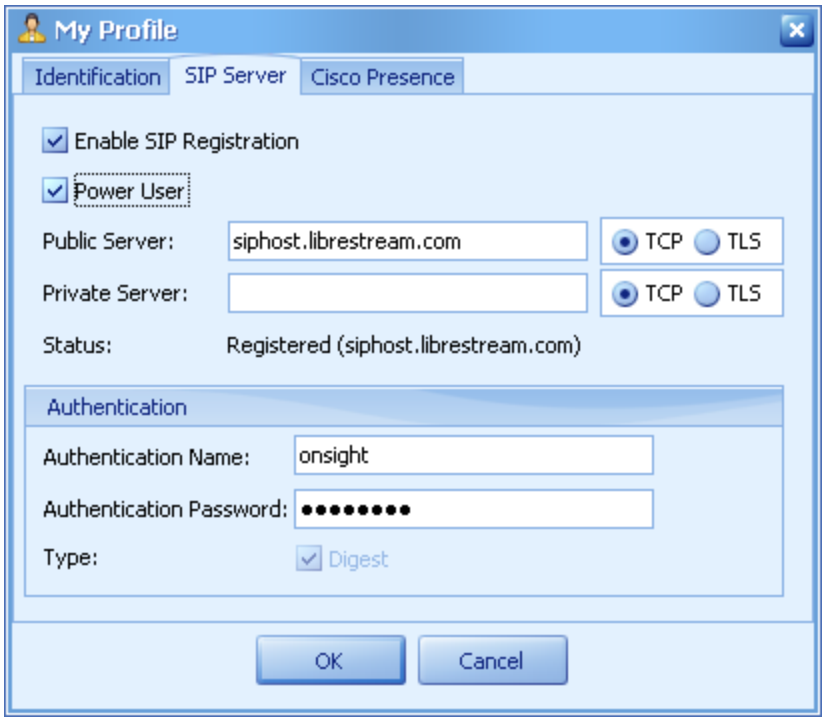
However, if these ports are already in use on a PC, Onsight Connect will increment the source port until it finds a free one. So the possible range of UDP source ports starts at 6000 and is determined by availability of UDP ports on the Onsight Connect Host PC.
The Onsight Device will always use these source ports (6000/6001, 6002/6003, 6004/6005, 6006) because it is a closed system and no other processes has access to them.

Destination Ports when using a SIP SERVER:
When using a SIP Server the destination ports are in the range configured on the SIP Server for the RTP and RTCP traffic, this is because the SIP Server has directed Onsight Connect to send to these ports. These ports must be opened on the Firewall.
Both the RTP and RTCP are in the range that has been configured on the SIP Server, this range is determined by the SIP Server Administrator and is based on the number of concurrent calls that need to be supported. Note that SIP traffic is still sent to the destination ports of 5060 or 5061.

From Onsight Connect's point of view, it is only sending and receiving traffic to the SIP Server.

1.2.4 Public/Private SIP Server Pair

As of v6.1, the SIP Server configuration supports listing two SIP Servers for SIP Registration. The Public Server resides outside of the Firewall and is accessible by the SIP endpoint when it is also outside the Firewall. The Private Server is located behind the Firewall on a private network, the SIP endpoint is also on the private network when it registers to the Private Server.



Firewall detection is used to determine the availability of the Public Server and potential connectivity methods (i.e. Direct SIP vs. TeamLink Proxy SIP).

If a Private server is specified, the Onsight software will use the SIP OPTIONS method (rather than Firewall detection) to determine if the Private server is available. The SIP OPTIONS method allows a SIP endpoint to query another SIP endpoint or a proxy server as to its capabilities. If the Private server responds to the SIP OPTIONS method, SIP registration will be attempted to the internal server. If it is not, registration will be attempted to the external server (based on the results of the Firewall detection tests).

2 Onsight: Network Protocols and Local Ports

2.1 Network Protocols and Local Ports Table

This table describes the protocols and Local ports used by Onsight Connect for SIP messaging and data transfer between Onsight Endpoints. For the SIP protocol the source port on the originating endpoint is random, the destination port is TCP 5060. The calling endpoint will try to open the UDP ports as listed in the following table. If a UDP port is already in use on the system the Onsight endpoint will increment the UDP port by one until it finds an open port. The port number will increment until a maximum of 6200. The UDP Media traffic will always be in the port range of 6000 to 6200 when both endpoints exist on the same LAN. (Note that for each RTP stream there is an associated RTCP stream with the exception of the Data stream.)
When two endpoints are using a SIP Server to communicate the UDP destination ports will be in the range dictated by the SIP Server configuration, however the UDP source ports should be in the 6000 to 6200 range.

Note that the Firewall/NAT will change source ports as the traffic exits the Local Area Network and is sent over the internet.

Table 2.1: Onsight Connect Source Ports

Category	Protocol	SRC Port(s)	Notes	Detail [3,8]	
SIP Signaling	TCP[5]	Random[2]	Direct IP Calls[6]	PC/Device sends SIP/TCP pkts out with SRC=x and DST=5060	PC/Device receives SIP/TCP pkts with SRC=5060 and DST=x
SIP Signaling	TCP	Random[2,3]	SIP proxy server based calls	PC/Device sends SIP/TCP pkts out with SRC=x and DST=5060/5061	PC/Device receives SIP/TCP pkts with SRC=5060/5061 and DST=x
Video	RTP/RTCP	6000/6001[1]	H.264 MPEG4 H.263+	PC/Device sends RTP/RTCP/UDP pkts out with SRC=6000-6001 and DST=y	PC/Device receives RTP/RTCP/UDP pkts with SRC=y and DST=6000-6001
Subject Audio	RTP/RTCP	6002/6003[1,2]	G.711 GSM6.10	PC/Device sends RTP/RTCP/UDP pkts out with SRC=6002-6003 and DST=y	PC/Device receives RTP/RTCP/UDP pkts with SRC=y and DST=6002-6003
Voice	RTP/RTCP	6004/6005[1]	Two-way voice	PC/Device sends RTP/RTCP/UDP pkts out with SRC=6004-6005 and DST=y	PC/Device receives RTP/RTCP/UDP pkts with SRC=y and DST=6004-6005
Data	RTP/RTCP[3]	6006[1]	Status, control, data, etc.	PC/Device sends RTP/RTCP/UDP pkts out with SRC=6006 and DST=y	PC/Device receives RTP/RTCP/UDP pkts with SRC=y and DST=6006
STUN[7]	UDP	Random	Firewall Detect – Mapped address	PC/Device sends UDP pkts out with SRC=x and DST=3478	PC/Device receives UDP pkts with SRC=3478 and DST=x
HTTPS/HTTP	TCP	Random[5]	TeamLink	PC/Device sends TCP pkts out with SRC=x and DST=443/80	PC/Device receives UDP pkts with SRC=443/80 and DST=x

1. The SRC ports shown are the first choice when a call is established. If a requested port is in use on the PC, the port number will increment (to a limit of 6200) until an available port is located. The Device will not have conflicts and will use the ports shown.
2. 'x' are random ports determined during SIP negotiation.
3. Send DST port is 5060 or 5061 if TLS is enabled.
4. 'y' are ports determined by the SIP proxy server during call negotiation usually from a limited range configured by the SIP proxy server administrator.
5. TeamLink will use either HTTPS or HTTP to proxy SIP traffic and Media depending on the Onsight endpoints configuration.
6. Direct IP Calls are calls made between Onsight endpoints using the IP address as the address of the contact, in comparison SIP Calls are made using the SIP URI as the address of the contact.
7. Only used by the Firewall Detect test if TeamLink is enabled.

3 Firewall Requirements – Allowing SIP Traffic

The following ports must be opened to allow SIP and Media traffic to the SIP Server and/or TeamLink Server:

- SIP TCP/UDP: 5060 (The Onsight endpoints use SIP TCP 5060 by default but the option to use SIP UDP 5060 is provided.)
- SIP-TLS TCP 5061 (Optional, but required if using TLS encryption for SIP messaging on the SIP Server. SIP-TLS provides encrypted SIP messages and requires the installation of certificates on the Onsight endpoints.)
- UDP Media Ports (see NOTE 1). The range of media ports allows the following RTP/RTCP streams:
    - Video
    - Voice
    - Subject Audio
    - Data
- HTTPS/HTTP/STUN for TeamLink

NOTE 1:

- Each connection between the Onsight Device and Onsight Connect endpoints will require 16 UDP ports, 8 for each endpoint: 4 RTP and 4 RTCP.
- The SIP Server passes RTP (video/audio/subject audio/data) streams and their associated RTCP streams over the UDP Media Ports. Each stream sends and receives on the same port number.
- The range of UDP ports that must be opened for Media traffic is dependent on the configuration of the SIP Server. The SIP Server dictates which UDP ports will be used during a session by an endpoint.
- See Section 4.1 for a diagram showing the SIP, RTP and RTCP stream flow.

3.1 Sample Firewall Configuration

The following sample configuration allows internal IP addresses to send (and receive) SIP (TCP 5060 and 5061) messages, data (UDP 58024 - 58523), HTTP (TCP 80), HTTPS (TCP 443), and STUN (UDP 3478) to the hosted Librestream servers at siphost.librestream.com, onsight.librestream.com and teamlink10.librestream.com.

The firewall can be configured to allow any internal IP address to send/receive on the required ports.

ACTION *Permit or Deny*	**Source IP Address** *IP Address, Hostname that INITIATES*	**Destination** *IP Address, Hostname*	**IP Type** *UDP or TCP*	**Protocol / Port #** *Media Port Range*
PERMIT	192.168.1.X (DHCP)	siphost.librestream.com (64.4.89.118)	UDP	58024-58523
PERMIT	192.168.1.X (DHCP)	siphost.librestream.com (64.4.89.118)	TCP	5060 - 5061
PERMIT	192.168.1.X (DHCP)	onsight.librestream.com (50.57.49.192)	TCP	80, 443
PERMIT	192.168.1.X (DHCP)	teamlink10.librestream.com (50.57.93.169)	UDP	58024-58523
PERMIT	192.168.1.X (DHCP)	teamlink10.librestream.com (50.57.93.169)	TCP	5060 - 5061
PERMIT	192.168.1.X (DHCP)	teamlink10.librestream.com (50.57.93.169)	TCP	80, 443
PERMIT	192.168.1.X (DHCP)	teamlink10.librestream.com (50.57.93.169)	UDP	3478

4 Onsight Endpoint SIP Server calls through Firewalls

The Onsight endpoints (Onsight Connect for PC, Onsight Devices, iPad and iPhones) must register with the SIP Server. Any calls between the Onsight Endpoints are managed by the SIP Server. Onsight endpoints can call directly to each other using IP addresses but they must be on the same LAN, as soon as you cross a Firewall you must use a SIP Server to manage the calls. Note: There is an option on some SIP Servers to allow two endpoints located behind the same Firewall/NAT to send data directly between each other, but normally all data traffic is routed through the SIP Server.

4.1 SIP Server – Public vs. Private

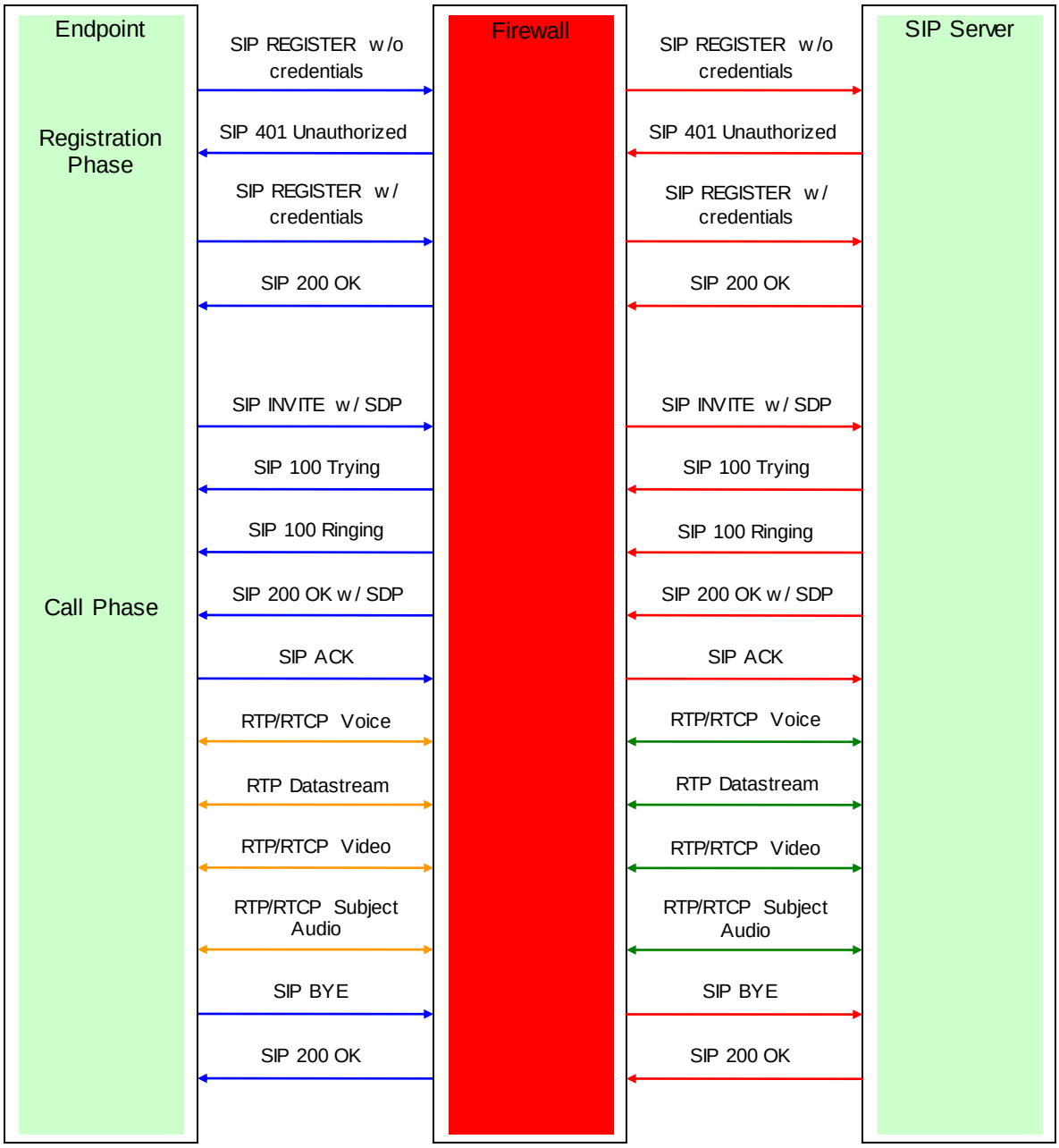
Onsight Endpoints support the ability to configure both a Public and Private SIP Server. The Public server is used when the Onsight endpoint is located outside the Firewall and must connect to a SIP Server that has a Public interface e.g. Cisco VCS Expressway. The Private Server is

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. The method used to register to the Public Server will depend on the results of the Firewall Detect test, see Section 6.1 for details.

If only one of the Public or Private Server settings are configured, the Onsight endpoint will attempt to register to it based on the results of the Firewall Detect test.

4.2 Session Initiation Protocol – Communication Exchange



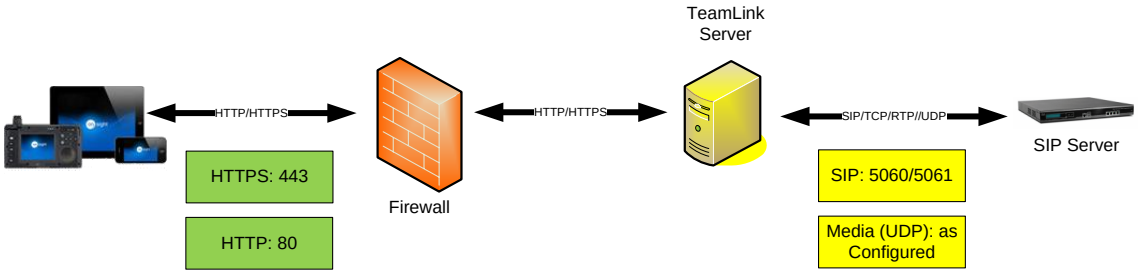
5 Onsight TeamLink HTTP/S Tunneling Server

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 HTTP/S 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 uses existing open ports on the Firewall, TCP 443 for HTTPS (or TCP 80 for HTTP if configured).

5.1 TeamLink Encapsulation

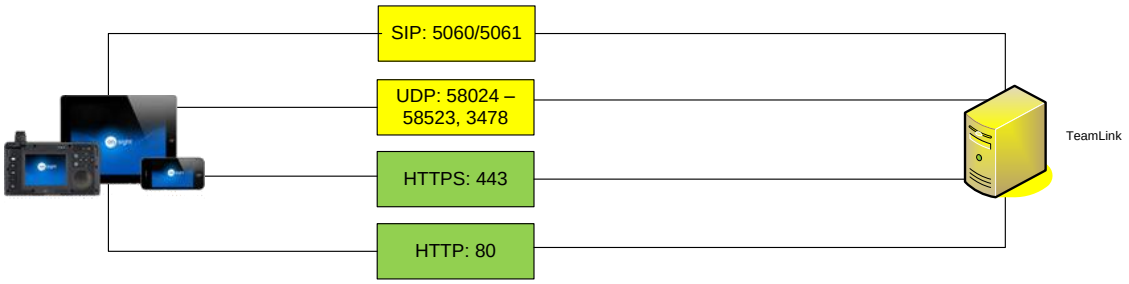
When using TeamLink the Onsight Endpoint will encapsulate SIP (TCP) and Media (RTP/RTCP/UDP) traffic in either HTTP or HTTPS protocol packets. The TeamLink Server receives these packets and strips off the HTTP/HTTPS encapsulation before forwarding them to the SIP Server. The SIP Server will send responses to the TeamLink Server. TeamLink encapsulates the packets before sending them back to the Onsight Endpoint.



5.2 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 the TeamLink server i.e. the test server.
If the Firewall test detects that the local firewall ports are open to the TeamLink server, then the Onsight Endpoint assumes the ports are also open to the SIP Server. That is, if SIP ports are open to TeamLink, 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.

Firewall Detect determines the best method of SIP Registration based on the results of the port teststo the TeamLink server. If your Enterprise allows direct SIP registration to the SIP server and has endpoints that will migrate from inside the Firewall to outside, Firewall Detect will provide the most accurate results if the Enterprise's Firewall allows traffic to Teamlink over the following ports:



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 Hosted 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 TeamLink Server by the Onsight Endpoint. STUN is also used to test UDP ports 58024 and 58523.

Firewall Detect Matrix:

IP Type	Protocol / Port #	Destination	Result	
UDP or TCP	*Port Range under Test*	*IP Address, Hostname*	*Open*	*Closed*
UDP	3478	teamlink10.librestream.com (50.57.93.169)	Public IP Address of the Firewall is discovered; the remaining port tests are run	Public IP Address of Firewall cannot be determined; the remaining port tests are aborted. TeamLink tunneling is enabled
TCP	5060 - 5061	teamlink10.librestream.com (50.57.93.169)	Direct SIP Server Registration is attempted	SIP Registration is proxied through TeamLink
UDP	58024-58523	teamlink10.librestream.com (50.57.93.169)	Media streams are sent directly to the SIP Server	Media streams are tunneled through TeamLink
TCP	80, 443	teamlink10.librestream.com (50.57.93.169)	TeamLink registration and HTTP/S tunneling are enabled	TeamLink is blocked, can't register to TeamLink

If Firewall Detect determines that all ports are blocked to TeamLink, including HTTPS and HTTP, Onsight Connect will attempt to register directly to the SIP Server.

6 Web (HTTP/S) Proxy Configuration

Web Proxies act as an intermediary between a client and the internet. When a client requests a resource from the internet, e.g. a PC browser requests a web page, the Web Proxy requests it on the client's behalf.

Because both Onsight Connect and TeamLink use HTTP/S protocols to communicate with the Onsight Connect service and tunnel SIP traffic it is possible that it will be routed through an internal Web (HTTP/S) Proxy at your location.

Onsight Endpoints can be configured to use the Web Proxy at your location. Proxy Settings options include: No Proxy, Use System Settings, or Manual Proxy configuration. Onsight Connect also supports Proxy Authentication.

On a PC, the Onsight Connect option, 'Use System Settings' will use the client's Proxy configuration found under ***Control Panel-Internet Properties-Connections-LAN Settings***.

Onsight Connect Devices, e.g. 2500 or 2000, support Manual Proxy configuration and Authentication.

Onsight for iOS Devices supports 'Use System Settings' and 'Manual'. If 'Use System Settings' is selected the proxy configuration will be used from the currently selected Wireless Network configuration under ***Settings***.

Your Enterprise's Web Proxy must allow traffic to the both Onsight.librestream.com and TeamLink (teamlink10.librestream.com).

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. Recall that the Firewall Detect test determines the suitable connection method: SIP, HTTPS or HTTP, depending on the results of the Firewall test.*

7 Potential Issues:

7.1 TeamLink Firewall Detect Limitations

The firewall detection implementation of TeamLink and the Onsight Connect endpoints have these known issues:

1. TeamLink won't correctly interpret firewalls that have been configured to block SIP and Media ports to TeamLink but allow HTTP/S. This may result in the use of TeamLink's HTTP/HTTPS tunneling when it is not required. This is because the SIP ports are tested using the TeamLink Server as the destination. If the Firewall blocks SIP to TeamLink this will be reported as 'SIP blocked' even though it allows SIP to an 'unknown' SIP Server.

(Note: the term 'unknown SIP Server' is meant only to indicate that TeamLink is unaware of the SIP Server in terms of Firewall Detect.)

2. CUCM is not supported and would not work without an alternative firewall traversal mechanism.

CASE 1:
An existing customer already has firewall rules to allow SIP/UDP to a certain SIP Server. If there are no similar rules on the firewall defined for the TeamLink, the Firewall Detect Test will report that SIP is not available and use tunneling by default.
Recommendation is that existing and new customers should apply firewall rules for SIP/UDP for both the TeamLink and the existing SIP Server; *otherwise they should disable the TeamLink configuration when inside the firewall*.

CASE2:
Customers with Cisco Unified Communications Manager (CUCM). CUCM installations are generally always behind the firewall. In this case, since the TeamLink server is in the cloud, it cannot contact CUCM and will not be able to tunnel.

7.2 Cisco SIP Aware

Cisco Routers have a SIP aware feature that is enabled by default. It rewrites header information in the SIP packets with respect to source addressing for the SIP packet, which confuses the SIP Server and must be turned OFF in order for the SIP Server communication to work correctly.

Example Commands To turn OFF Cisco SIP aware:

- show fixup sip 5060
- no fixup protocol sip 5060

Or

- no ip nat service sip udp port 5060
- no ip nat service sip tcp port 5060

Alternatively, the Onsight endpoints can be configured to use SIP-TLS for the Authentication transport. This requires a certificate to be installed on the endpoints. SIP-TLS encrypts the SIP messaging headers and therefore the headers are ignored by the SIP aware feature of the Cisco router.

8 Onsight Connect Service Check List

- ☑ Firewall ports have been configured to allow Onsight Connect Service and SIP Registration
- ☑ Onsight devices are connected to the network (WiFi or Ethernet)
- ☑ Onsight Account Manager has been configured with Users, Client Policies and SIP Account information:
  - SIP server address
  - URI
  - User name and password
  - Authentication Transport Setting
- ☑ Install Certificates (if necessary, for SIP-TLS)

☑ If required, TeamLink has been enabled

For further information regarding Onsight Connect Setup consult the Onsight Connect User Manuals.