



Application Note

**Firewall Requirements for the OnSight
Mobile Collaboration System and
Hosted Librestream SIP Service
v5.0**

1	FIREWALL REQUIREMENTS FOR ONSIGHT MOBILE VIDEO COLLABORATION SYSTEM AND HOSTED SIP SERVICE.....	3
1.1	Overview.....	3
1.2	Endpoint Registration to SIP Server	3
2	FIREWALL REQUIREMENTS – ALLOWING SIP TRAFFIC	3
2.1	Firewall Diagram.....	5
2.2	Example Firewall Configuration.....	6
3	ONSIGHT: NETWORK PROTOCOLS AND PORTS	7
3.1	Network Protocols and Ports Table	7
4	ONSIGHT ENDPOINT SIP SERVER CALLS THROUGH FIREWALLS	8
4.1	Session Initiation Protocol – Communication Exchange.....	8
5	ONSIGHT TEAMLINK HTTP TUNNELING SERVICE	9
5.1	TeamLink Encapsulation.....	9
5.2	Firewall Detect.....	9
6	POTENTIAL ISSUES:	10
6.1	TeamLink Firewall Detect Limitations.....	10
6.2	Cisco SIP Aware	10
7	SIP SERVICE CHECK LIST	11

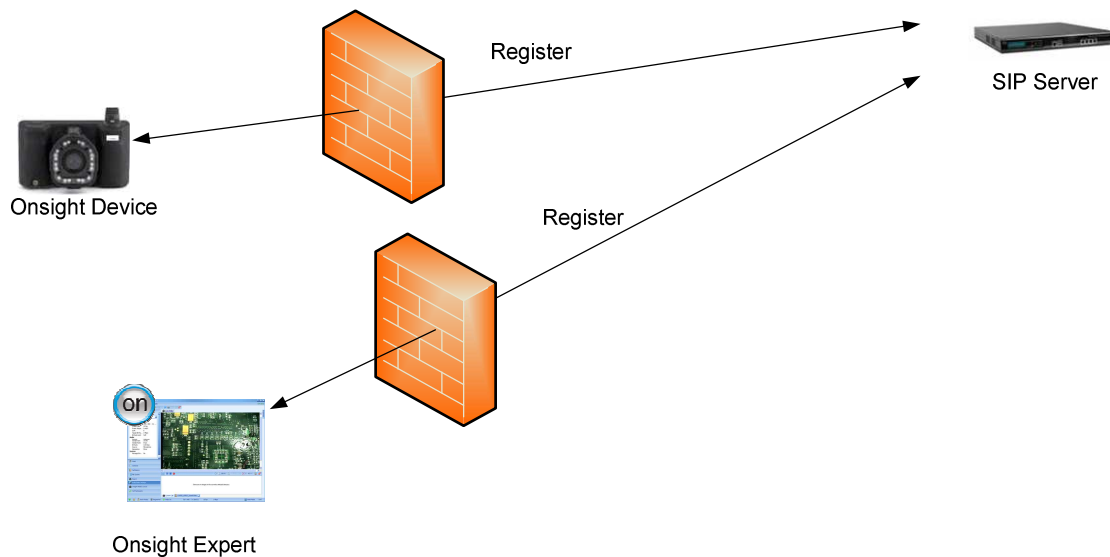
1 Firewall Requirements for Onsight Mobile Video Collaboration System and Hosted SIP Service

1.1 Overview

This document provides a high level description of the firewall configuration required to allow communication for the Onsight Mobile Video Collaboration system as well as the hosted Librestream SIP Service.

The Onsight Mobile Video Collaboration System uses Session Initiation Protocol (SIP) to establish audio and video communication sessions between endpoints. Firewall traversal is required to establish a session when the endpoints are not located on the same LAN. This is accomplished by using a SIP Proxy Server. Each endpoint registers to the SIP Server which is located outside of the Firewall. The SIP Server acts as a proxy and directs SIP messaging and data traffic between the endpoints.

1.2 Endpoint Registration to SIP Server



When the Onsight endpoints are registered to the SIP Server, both the Onsight Devices and the Onsight Experts can initiate calls.

2 Firewall Requirements – Allowing SIP Traffic

The following ports must be opened to allow SIP and data traffic to the Librestream SIP Server:

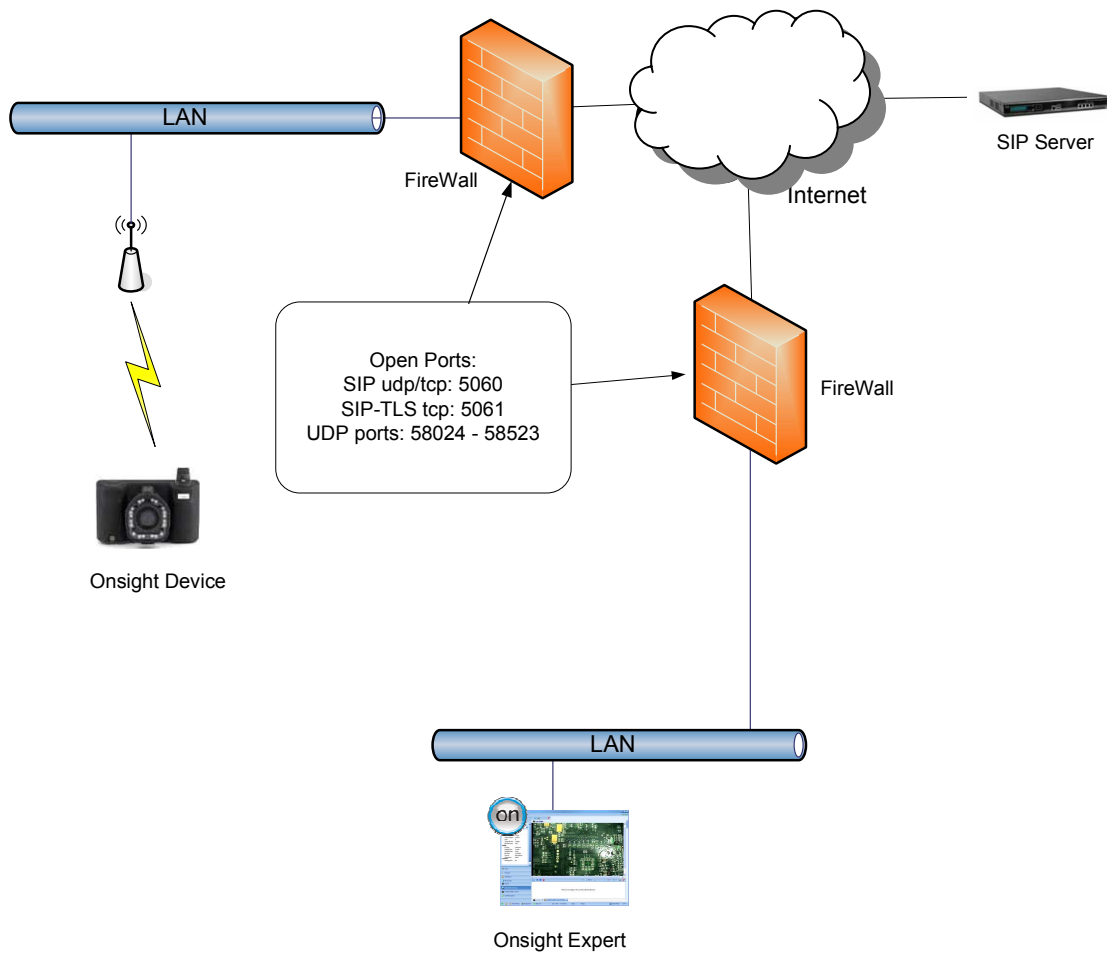
- SIP TCP/UDP: 5060 (The Onsight endpoints use SIP TCP 5060 by default but the option to use SIP UDP 5060 is provided.)

- 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 Onsite endpoints.)
- UDP Media Ports (see NOTE 1). The range of media ports allows the following RTP/RTCP streams:
 - Video
 - Voice
 - Subject Audio
 - Data

NOTE 1:

- 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. E.g. Video sends and receives on UDP port 6000.
- Each connection between the Onsite Device and Onsite Expert endpoints will require 16 UDP ports, 8 for each endpoint: 4 RTP and 4 RTCP.
- The range of UDP ports that must be opened for Media traffic are: **UDP 58024-58523**. This is the configured UDP Media port range on the Librestream SIP Hosting Server.
- See Section 4.1 for a diagram showing the SIP, RTP and RTCP stream flow.

2.1 Firewall Diagram



2.2 Example Firewall Configuration

The following sample configuration allows 3 specific IP addresses to send (and receive) SIP (TCP and UDP) messages and data (UDP) to the hosted Librestream SIP server at IP address 64.4.89.118 (siphost.librestream.com). The firewall could also be configured to allow any internal IP address to send/receive on the required ports.

ACTION	Source IP Address	Destination	IP Type	Protocol / Port #
<i>Permit or Deny</i>	<i>IP Address, Hostname that INITIATES</i>	<i>IP Address, Hostname</i>	<i>UDP or TCP</i>	<i>Media Port Range</i>
PERMIT	192.168.1.1 (DHCP)	64.4.89.118 or siphost.librestream.com	UDP	58024-58523
PERMIT	192.168.1.2 (DHCP)	64.4.89.118 or siphost.librestream.com	UDP	58024-58523
PERMIT	192.168.1.3 (DHCP)	64.4.89.118 or siphost.librestream.com	UDP	58024-58523
PERMIT	192.168.1.1 (DHCP)	64.4.89.118 or siphost.librestream.com	TCP	5060 - 5061
PERMIT	192.168.1.2 (DHCP)	64.4.89.118 or siphost.librestream.com	TCP	5060 - 5061
PERMIT	192.168.1.3 (DHCP)	64.4.89.118 or siphost.librestream.com	TCP	5060 - 5061
PERMIT	192.168.1.1 (DHCP)	64.4.89.118 or siphost.librestream.com	UDP	5060
PERMIT	192.168.1.2 (DHCP)	64.4.89.118 or siphost.librestream.com	UDP	5060
PERMIT	192.168.1.3 (DHCP)	64.4.89.118 or siphost.librestream.com	UDP	5060

3 Onsite: Network Protocols and Ports

3.1 Network Protocols and Ports Table

This table describes the protocols and ports used by the Onsite Mobile Collaboration System for SIP messaging and data transfer.

Category	Protocol	SRC Port(s)	Notes	Detail ^{3,8}	
SIP Signaling	TCP ⁵	Random ⁷	Used for calls that do not use a SIP proxy server	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 ⁷	SIP proxy server based calls	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
Video	RTP	6000/6001 ²		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	6002/6003 ²		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	6004/6005 ^{2,1}	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 ⁴	6006 ^{2,6}	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

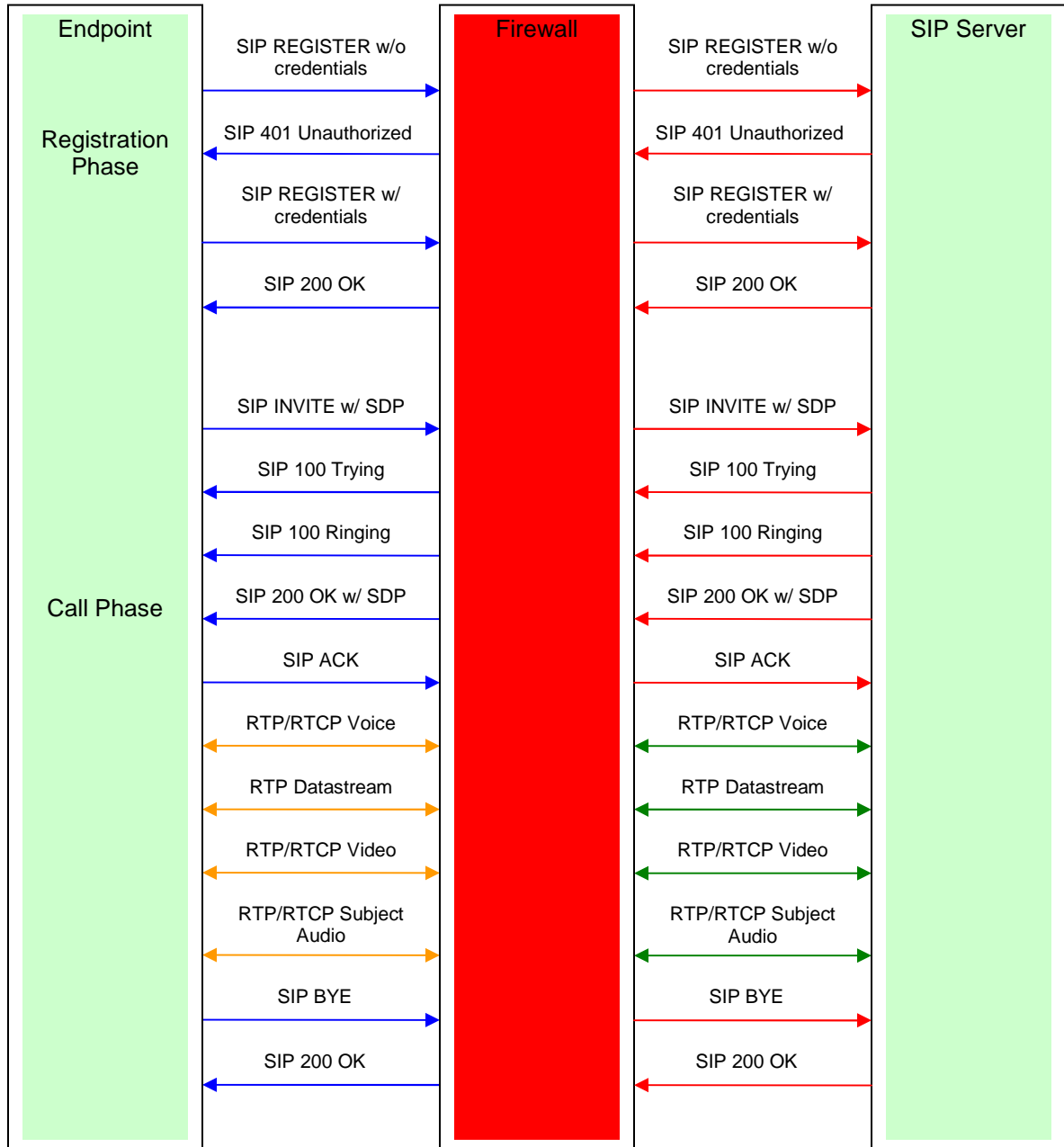
1. Device OS 2.34 (and lower) used random ports. PC Application 2.5.1 (and lower) used random ports.
2. The SRC ports shown are the first choice when a call is established. If a requested port is in use on the PC, the port number will increment (to a limit of 6200) until an available port is located. The Device will not have conflicts and will use the ports shown.
3. 'x' are random ports determined during SIP negotiation.
4. Device OS 2.xx used UDP. PC Application 2.x.x used UDP.
5. Optionally configurable as UDP.
6. Device OS 3.76 (and lower) used port 8888. PC Application 3.1.2 (and lower) used port 8888.
7. Send DST port is 5060, or 5061 if TLS is enabled.
8. 'y' are ports determined by the SIP proxy server during call negotiation usually from a limited range configured by the SIP proxy server administrator.

4 Onsite Endpoint SIP Server calls through Firewalls

The Onsite endpoints (Onsite Device or Onsite Expert) must register with the Librestream SIP Server. Any calls between the Onsite Endpoints are managed by the SIP Server.

Note: There is an option on the SIP Server 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 Session Initiation Protocol – Communication Exchange



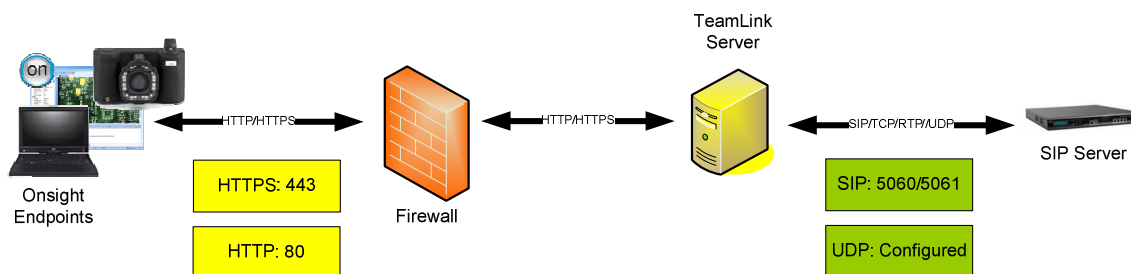
5 Onsight TeamLink HTTP Tunneling Service

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 HTTP/S packets to an 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 80 for HTTP and TCP 443 for HTTPS.

Librestream will provide TeamLink accounts upon request. This information is entered on the Onsight Endpoint to allow registration with the TeamLink Server.

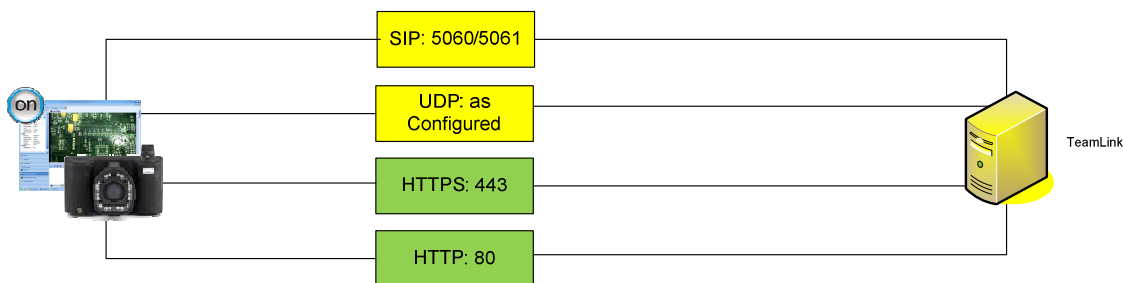
5.1 TeamLink Encapsulation

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 open ports on the Firewall and determines the best method for SIP Registration. If SIP ports are open the Onsight Endpoint will SIP register directly to the SIP Server, if SIP ports are closed the Onsight Endpoint will use TeamLink to SIP register by proxy, using TeamLink, to the SIP Server.



*Firewall Detection Settings: The tested range of TCP, HTTP, HTTPS and UDP ports can be configured within the Onsight Endpoint.

6 Potential Issues:

6.1 TeamLink Firewall Detect Limitations

The firewall detection implementation of TeamLink and the OE/OD clients have these known issues:

1. TeamLink won't detect firewalls that have already been configured to work with unknown SIP Servers which may result in the use of 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 but allows it to another unknown SIP Server this will be reported as 'SIP blocked'. (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. TeamLink won't detect VCS Expressway/Control pairs and depending on configuration, SIP calls may fail.
3. 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 detection algorithms on the OD/OE 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: A customer has a VCS Expressway and VCS Control pair. In this case the TeamLink may report that SIP is not available when behind the firewall and tunneling may not work if the SIP settings are pointing to the VCS Control. Customers in this configuration already have to re-point the SIP settings to the VCS Express or VCS Control when they cross from one side of the firewall to the other. *It is recommended that you disable the TeamLink configuration when behind the firewall and enable the TeamLink configuration when on the outside of the firewall.*

CASE3: Customers with Cisco Unified Communications Manager (CUCM). The CUCM installations we've seen do not have any firewall/NAT traversal mechanisms and are generally always behind the firewall. In this case, since the TeamLink is in the cloud, it cannot contact the CUCM and will not be able to tunnel.

6.2 Cisco SIP Aware

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

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 Onsite 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.

7 SIP Service Check List

- Firewall ports have been configured
- Onsite devices are connected to the network (WiFi or Ethernet)
- Endpoints have been configured with 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.
- TeamLink accounts have been configured
 - Server, Path, User ID, Password
 - HTTP Port, HTTPS Port

For further information regarding SIP Registration Setup consult the Onsite mobile device and Onsite Expert User Manuals.