



White Paper

**Security Overview for the Onsight Mobile
Collaboration System v5.0**



Librestream

ONSIGHT MOBILE VIDEO COLLABORATION SYSTEM – SECURITY OVERVIEW	2
Onsight Mobile Video Collaboration System Features:	2
USER AUTHENTICATION	3
Onsight Mobile Device Security	3
Onsight Expert Application	3
CONFIGURATION ACCESS CONTROL	3
WI-FI SECURITY	4
FIPS 140-2 ENCRYPTION	5
ONSIGHT MEDIA ENCRYPTION	5
SIP-TLS SIGNALING ENCRYPTION	6
Protected Information	6
SIP-TLS Certificates	6
InGate SIParator	7
Tandberg VCS	7
VIRTUAL PRIVATE NETWORK	7
Onsight Mobile Device: VPN	7
Supported Onsight Device VPN Configuration Options	8
Onsight Expert: VPN	10
PRIVACY	10
FIREWALL/NAT TRAVERSAL	10
FireWall	10
Network Address Translation	12
Onsight TeamLink Server	12
Firewall Detect	0

Onsight Mobile Video Collaboration System – Security Overview

This document outlines the security features supported by the Onsight mobile video collaboration system. It gives a brief overview of the methods used to provide a secure communication link between the Onsight endpoints. The combination of methods used will depend on the security policy of an enterprise.

Onsight Mobile Video Collaboration System Features:

1. **User Authentication:**
Manage access to the Onsight device and Onsight Expert application.
2. **Configuration Access Control:**
Control access to the device configuration menus.
3. **WiFi Security:**
Configure wireless network access.
4. **Media Encryption:**
Encrypt real-time media traffic.
5. **SIP-TLS encryption:**
Encrypt Session Initiation Protocol traffic.
6. **FIPS 140-2 Encryption**
Encrypt Wireless traffic to FIPS-120 standard for government agencies.
7. **Virtual Private Network:**
Establish secure network connections from remote locations to an Enterprise VPN Server.
8. **Privacy:**
Prevent the recording/storage of video (mpeg4) and still images (jpeg).
9. **FireWall/NAT Traversal:**
 - a. FireWall Traversal and Network Address Translation solutions.
10. **TeamLink HTTP/S Tunneling Server**

User Authentication

A password protected user account is required to access the Onsight Device and the Onsight Expert application. The system administrator creates the list of valid user accounts and initial passwords. The administrator can also determine the minimum acceptable password length using Onsight Management Suite (OMS) to manage the devices.

Onsight Mobile Device Security

When the Onsight mobile device is powered up, the user is presented with the User Authentication Screen. A user must select their Username from the drop-down list and enter the corresponding password to gain access to the Onsight mobile device.

The device can be configured to allow Auto Login to the device on boot up. This is configurable by the device administrator.

Onsight Expert Application

The Onsight Expert user must enter a user name/password to login to the application. The default Administrator account is admin/admin. It is recommended that the Administrator's password be changed on the first login.

Onsight Expert can be configured to allow Auto Login in when the application is launched. This is configurable by the Administrator.

Configuration Access Control

Configuration Access Control* allows an administrator to grant or deny access to selective features. For example, a user may be allowed access to Wi-Fi Security configuration but be locked out of Call Control - SIP Settings.

The options for Configuration Access Control are:

- Open (any valid user can modify the setting);
- Admin (only admin users can modify the setting);
- Locked (no user can modify the setting directly from the device, OMS must be used).

*Requires Onsight Management Suite (OMS) to configure the device remotely.

Wi-Fi Security

Wi-Fi Security governs authentication of the wireless device to the network and encryption of the data over the wireless connection. Wireless network configuration settings must be obtained from your Network Administrator in order to connect to a security enabled Access Point.

Onsight supports the following Wi-Fi Security protocols:

- WLAN Network Authentication:
 - WPA*
 - WPA-PSK
 - WPA2*, **
 - WPA2-PSK
 - Open – Not Recommended but preferred over ‘Shared’
 - Shared – Not Recommended

- WLAN Data Encryption:
 - AES 128 bit**
 - TKIP
 - WEP (40 and 128 bit) – Not Recommended
 - Disabled – i.e. Encryption and Authentication is off, Not Recommended.

- 802.1X Authentication*
 - EAP-TLS (Requires a User and Certificate Authority certificate)
 - PEAP-MSCHAPv2 (User Name\Password based authentication)
 - PEAP-GTC (User Name\Passcode(PIN+Token)\FixedPasscode)

- X.509 certificate* formats:
 - .cer
 - .pfx, .p12
 - .pvk

* Requires a RADIUS Authentication Server e.g. Microsoft’s Internet Authentication Service (IAS) or FreeRADIUS (OpenSource).

** WPA2 with AES encryption is the highest level of security under the IEEE 802.11i standard. The IEEE 802.11i standard specifies security methods for wireless networks.

FIPS 140-2 Encryption

The Onsight Wi-Fi traffic can be encrypted (up to AES-256) by a Fortress FIPS certified Access Point and the Onsight FIPS option using the integrated Fortress Secure Client.

Librestream has integrated the Fortress FIPS 140-2 software client within its line of Onsight mobile devices. When customers use the FIPS-enabled Onsight device with the Fortress line of FIPS 140-2 compliant mesh solutions, the video, audio and data sent from the Onsight mobile devices meet the rigorous transmission security requirements of defense and other government agencies.

FIPS is a set of standards that describe document processing, provide standard algorithms for searching and provide other information processing standards for security modules used to protect government networks. For more information regarding NIST and FIPS visit: <http://www.nist.gov>.

This solution requires Fortress Hardware to be installed as part of the Wireless infrastructure for your enterprise. E.g. ES520.

Onsight Media Encryption

Media encryption between the Onsight endpoints is provided using Secure RTP (SRTP) with AES-128 bit encryption (RFC3711 compliant).

When Onsight Media Encryption is enabled, the SIP signaling between the SIP Server and the Onsight endpoints should also be encrypted (using SIP-TLS). If SIP-TLS is not employed, i.e. SIP is used as the Authentication Transport, the encryption keys will be sent as unencrypted open text over the network. SIP-TLS ensures an encrypted key exchange occurs between the endpoints.

Note: Unless the Onsight endpoints are registered to a SIP Registrar such as the InGate SIParator using SIP-TLS, the Media encryption keys will be passed as open text in the SIP protocol when Media Encryption mode is enabled.

Media encryption is enabled on the Onsight Expert under File\Preferences\Security\Media Encryption Mode and on the Onsight mobile device under Configuration\Security\Encryption\Encryption Mode.

SIP-TLS Signaling Encryption

SIP-TLS requires the authentication of the SIP client and SIP Proxy Servers (required for Firewall/NAT traversal) before a connection can be established. Based on public key cryptography, TLS encryption relies on digital certificates. The authentication exchange works like this:

1. The SIP client connects to the SIP server.
2. The SIP client requests a TLS session from the server.
3. The server replies with a valid public certificate.
4. The client validates the certificate.
5. The client and server exchange session keys.
6. The session keys encrypt and decrypt data for the session.

Once the authenticated session is established all SIP packets are encrypted between the client and the server. (RFC 2246 defines TLS.) “Media encryption mode” must also be enabled on the Onsite endpoints in order to send encrypted data.

Protected Information

All session information for a call is passed in the SIP Protocol. Using SIP-TLS for the Authentication transport encrypts and therefore protects this information.

What information does SIP-TLS protect?

1. LAN IP address Scheme
2. Calling information: caller and called party
3. SIP URI
4. Port Address Allocation on the Firewall
5. Vendor equipment
6. Session Description Protocol – describes Media Codecs and addressing

SIP-TLS Certificates

The SIP client must have certificate of either the SIP Server or the Certificate Authority that signed the SIP Server’s certificate installed. The Network Administrator will issue the certificates required for SIP-TLS Authentication.

InGate SIParator

The InGate SIParator supports SIP-TLS traffic between the endpoints and the SIParator. This requires an X.509 certificate to be installed on all endpoints using SIP-TLS. SIP-TLS encrypts the SIP messaging between the InGate SIParator and the OnSight endpoint.

“InGate SIParator monitors the SIP signaling port (5060) and applies routing rules and process policies to only the SIP Protocol traffic, where all other UDP/TCP traffic will be discarded and not forwarded to the IP-PBX. In addition, the InGate SIParator/Firewall will dynamically open and close media ports based on the negotiated SIP Traffic, by carefully monitoring the Media Ports negotiated and responding and routing media accordingly.” – InGate Security Best Practices Ver 2.pdf.

The SIParator does not enforce the SIP-TLS requirement for encrypted streams between OnSight Endpoints, it is therefore possible to use SIP with Media encryption. However as stated in the OnSight Media Encryption section, the encryption keys will be passed as open text in the SIP packet if SIP-TLS is not used. Therefore SIP-TLS is the recommended Authentication Transport for use with Media Encryption.

Using Secure Real-time Transport Protocol (SRTP) the media stream is encrypted between the two endpoints making the media stream secure from eavesdropping and Hijacking.

Tandberg VCS

The Tandberg VCS is a SIP Registrar that supports the SIP-TLS protocol as well. The VCS enforces the SIP-TLS requirement for encrypted streams. ***This means that a stream will not be encrypted unless the OnSight endpoints have registered to the VCS using SIP-TLS.***

Virtual Private Network

The OnSight Expert and OnSight Mobile device can operate over a VPN network connection.

OnSight Mobile Device: VPN

The VPN connection allows the device to connect to a remote enterprise LAN and make direct IP calls or register locally to a SIP Proxy Server and call other endpoints using a SIP URI.

The Onsight mobile device can establish a secure VPN connection to a remote VPN server using the following methods.

1. L2TP/IPSec: IPSec provides a secure channel, L2TP provides the tunnel.
2. PPTP

Supported Onsight Device VPN Configuration Options

Security Page:

Data Encryption Checkbox - this setting determines whether Microsoft Point-To-Point Encryption (MPPE) will be negotiated in the Compression Control Protocol (CCP) negotiations when setting up the Point to Point Protocol (PPP) link. CCP is a Network Control Protocol (NCP).

Use Extensible Authentication (EAP) checkbox + combo box - this uses the selected EAP type for PPP authentication. This authentication protocol is negotiated via the Link Control Protocol (LCP) when establishing the PPP link.

Unencrypted Password (PAP) checkbox - this enables the negotiation of Password Authentication Protocol (PAP) authentication in the LCP PPP setup. PAP basically sends a clear-text Username and Password pair to be authenticated by the server.

Challenge Handshake Authentication Protocol (CHAP) checkbox - this enables the negotiation of CHAP authentication in the LCP PPP setup. CHAP involves the authenticator sending an arbitrary string to be MD5 hashed along with the password, session ID, and unhashed username. The password is used to create the encrypted hash of the challenge, and acts as a shared secret between client and server, so no clear text password is sent.

Microsoft CHAP (MS-CHAP) checkbox - this enables the negotiation of MS-CHAP authentication in the LCP PPP setup.

Microsoft CHAP version 2 (MS-CHAP-v2) checkbox - this enables the negotiation of MS-CHAP-v2 authentication in the LCP PPP setup. This is considered more secure than MS-CHAP-v1.

Preview Username and Password checkbox - if this checkbox is set, when attempting to connect to a VPN, the username/password dialog will always be shown. If this is deselected, cached credentials will be used from a previous successful authentication attempt, and the dialog will not be shown. If there are no previous credentials (no successful prior connections), the dialog will still be shown.

General TCP/IP Page:

Use Server Assigned IP Address checkbox + textbox - if checked, the server will assign an IP address for this VPN connection from its VPN address pool. If this is unchecked, the user can enter a desired static IP address to use.

IP Header Compression checkbox - enables negotiation of Protocol field compression and Address/control field compression in LCP PPP setup.

Software Compression - this setting determines whether Microsoft Point-To-Point Compression (MPPC) will be negotiated in the Compression Control Protocol (CCP) negotiations when setting up the Point to Point (PPP) link. MPPC compresses the data contained in the PPP packets.

Name Servers Page:

Use server assigned IP addresses checkbox + textboxes - if checked the server will assign IP addresses for the client to use for DNS and WINS servers. If it is unchecked, the user can enter his/her own IP addresses to use for these servers.

IPSEC Page (Only available for L2TP/IPSEC VPN):

Certificate authentication radio-button - If this option is selected, the client will use a certificate to provide a shared secret when initiating the IPsec Security Associate (SA) in phase 1 of the IPsec establishment process. A root certificate must also be present in the Trusted Store for the Onsite device to authenticate the server and complete the SA.

Pre-Shared Key radio-button + checkbox - If this option is selected, a shared string can be used to provide the shared secret when initiating the IPsec SA in phase 1 of IPsec. Generally considered less secure and scalable, but avoids the need to set up a PKI and import certificates to devices.

Onsight Expert: VPN

The Onsight Expert will operate across an active VPN connection on the Host PC. However, when the VPN is operating in split-tunneling mode, special attention should be paid to the method of SIP registration. The proper address should be used for the preferred method of connection to the SIP Server, i.e. registering to the Public IP address or the local interface of the Server through the VPN connection. This is a configuration policy that should be defined by your Network Administrator.

Privacy

The Privacy option allows an Administrator to disallow recording/storage of video and still images on the device and Host PC of the Onsight Expert application. The participants in the session will only be able to view Live Streaming Video and Still Images. Once the session ends no record of video or still images remain. This feature is most likely to be employed in a healthcare setting.

FireWall/NAT Traversal

FireWall

The Onsight Mobile Collaboration System uses Session Initiation Protocol (SIP) to establish communication links between the Onsight Device and Onsight Expert endpoints. SIP traffic must be allowed to pass through an enterprise's Firewall in order for endpoints to communicate. The Onsight system can use a VoIP Firewall (Session Border Controller) called the 'InGate SIParator' to manage SIP/RTP traffic.

All endpoints wishing to communicate with each other register to the SIParator. This SIP Server acts as a proxy directing SIP and Media traffic between the endpoints. The Onsight endpoint communicates directly to the SIP Server, which in turn passes the traffic on to the intended recipient. The SIParator itself is a Firewall device that only processes SIP/RTP traffic.

An enterprise's Firewall must be configured to allow SIP and RTP traffic to and from a specific SIParator. The SIParator acts a Proxy server redirecting traffic between endpoints.

This means that a Firewall needs to only allow traffic to a specific IP address on the required SIP/RTP ports i.e. the SIParator.

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

- SIP TCP/UDP: 5060 (The Onsite endpoints use SIP TCP 5060 by default but the option to use SIP UDP 5060 is provided.)
- SIP-TLS TCP 5061 (required when using TLS encryption for SIP messaging on the SIPerator. 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 data streams:
 - Video
 - Voice
 - Subject Audio
 - Data

NOTE 1: The SIP Server passes video/audio/subject audio/data over the UDP Media Ports. The ports that must be opened for Media traffic are dependent on the SIP Server configuration. E.g. If the SIP Server is configured to pass Media over UDP ports 58024-58523 then the FW must allow traffic on these ports. The typical range of UDP Media ports is 58024 to 60999; this can be reduced to a smaller subset.

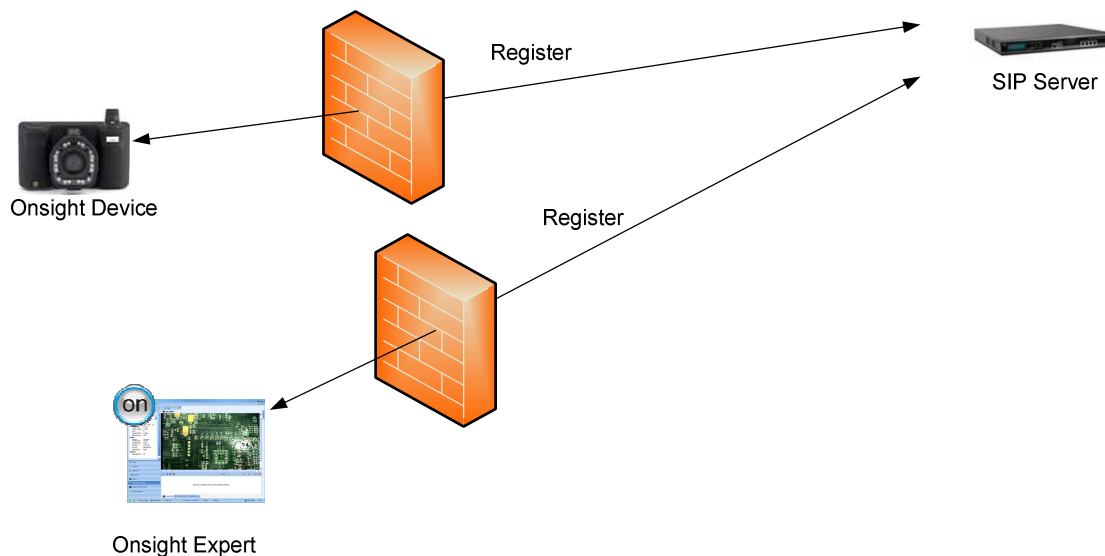


Figure 1: SIP Registration

The Onsite Mobile Collaboration System is also compatible with the Tandberg Video Communication Server (VCS). The VCS is also a SIP Proxy border controller that allows video streaming across Firewalls.

Network Address Translation

Network Address Translation allows a pool of devices on a LAN to share a single Public IP address on the Internet. The Onsite endpoints receive IP Addresses on their local area network; these are either manually assigned static IP addresses or assigned using a Dynamic Host Configuration Protocol (DHCP) Server. When the Onsite endpoint sends traffic through the Firewall to the SIP Proxy (e.g. SIParator), the local IP address is translated to the Public IP address of the Firewall. When the Endpoint registers to the SIP Server it uses the Enterprise's Firewall Public IP as the Source IP address. This makes it possible for the SIP Server to send packets back to the Onsite Endpoint that sits behind the Firewall. The Enterprise's Firewall knows to redirect the incoming traffic to the Onsite Endpoint using NAT addressing.

This means that a Firewall needs to only allow traffic to/from a specific IP address on the required SIP/RTP ports i.e. the SIP Server.

Some Firewalls have 'SIP Aware' features that insert the Public IP address of the source Firewall into the SIP Header of the SIP packets being sent to the SIP Proxy Server (e.g. SIParator). This behavior confuses the SIP Server and it must be disabled on the Firewall or SIP-TLS must be used so that SIP headers are encrypted and therefore untouched by the SIP Aware feature.

E.g. these commands are used on a Cisco router to turn off the 'SIP Aware' feature:

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

Onsite TeamLink Server

TeamLink encapsulates SIP and UDP Media traffic in HTTP or HTTPS protocol packets so that an endpoint can SIP register and pass UDP Media traffic through a Firewall using existing open ports, specifically TCP 80 and TCP 443. The TeamLink Server receives all packets and forwards them to the SIP Server on behalf of the endpoint.

It is recommended that Onsite endpoints using TeamLink enable HTTPS, SIP-TLS and Media Encryption.

Firewall Detect

The Firewall Detect feature is active when TeamLink has been enabled on an endpoint. Firewall Detect determines what ports are open on the Firewall by sending test packets to the configured TeamLink server. Based on the results the endpoint will then select the best method for registering to the SIP Server. The Order of Precedence is SIP Server, HTTPS then HTTP.