



## White Paper

### Enterprise Deployment Guide for the Onsight Mobile Collaboration System V1.2

# Table of Contents

<b>INTRODUCTION</b>	<b>3</b>
PREREQUISITES	3
ADDITIONAL RESOURCES	3
<b>STAGE 0: NETWORK ARCHITECTURE</b>	<b>4</b>
NETWORK ARCHITECTURE EXAMPLE	4
SECURITY	5
SIP SERVER	5
FIREWALL TRAVERSAL	6
VPN	6
OMS WEB SERVICE	7
NETWORK ARCHITECTURE CHECKLIST	7
ADDITIONAL RESOURCES	7
<b>STAGE 2: ONSIGHT MANAGEMENT SUITE CONFIGURATION</b>	<b>7</b>
OMS INSTALLATION AND CONFIGURATION	7
OMS FIREWALL SETUP	8
CREATE CONFIGURATION PACKAGES	8
CREATE USER / CONTACT LISTS	8
CREATE MEDIA CONFIGURATION PACKAGES	8
CERTIFICATE PACKAGES	9
LICENSE MANAGEMENT – ONSIGHT EXPERT	9
OMS CONFIGURATION CHECKLIST	9
ADDITIONAL RESOURCES	9
<b>STAGE 3: CONFIGURING THE ONSIGHT DEVICES</b>	<b>10</b>
CONNECT ONSIGHT DEVICES TO THE NETWORK	10
COMPLETE MANUAL CONFIGURATION REQUIREMENTS	10
ONSIGHT DEVICE DISCOVERY	10
OMS SOFTWARE UPDATE JOB	10
CONFIRM CORRECT CONFIGURATION	10
PACKAGE AND SHIP	10
ONSIGHT DEVICE CONFIGURATION CHECKLIST	11
ADDITIONAL RESOURCES	11
<b>STAGE 4: CONFIGURING THE ONSIGHT EXPERT DESKTOPS</b>	<b>11</b>
ONSIGHT EXPERT INSTALLATION	11
ONSIGHT EXPERT DISCOVERY	11
ONSIGHT EXPERT ACTIVATION	11
OMS SOFTWARE UPDATE JOB	12
CONFIRM CORRECT CONFIGURATION	12
ONSIGHT EXPERT CONFIGURATION CHECKLIST	12
ADDITIONAL RESOURCES	12
<b>STAGE 5: USER TRAINING</b>	<b>13</b>
<b>FOR MORE INFORMATION</b>	<b>13</b>

## Introduction

The purpose of this document is to provide a high level overview of the basic requirements for the Onsight system and outline the typical stages involved in a mid to large scale deployment.

The following topics will be covered:

- Network Architecture review
- Typical infrastructure requirements such as a SIP server, firewall considerations, and network topology
- Onsight Management Suite (OMS) centralized administration software including Onsight endpoint configuration packages, contact lists and Onsight Expert licensing
- Onsight mobile device (OD) staging including wireless network set-up and centralized configuration
- Onsight Expert (OE) software deployment across an enterprise
- End user training recommendations

## Prerequisites

1. Onsight software and license activation keys are available for deployment.
2. The SIP Server Installation and configuration is complete.
3. The Onsight Devices are on premise and a staging area is available. *Note: Each OD will need to be connected to the network and correctly configured manually to receive the initial OMS configuration packages.*

## Additional Resources

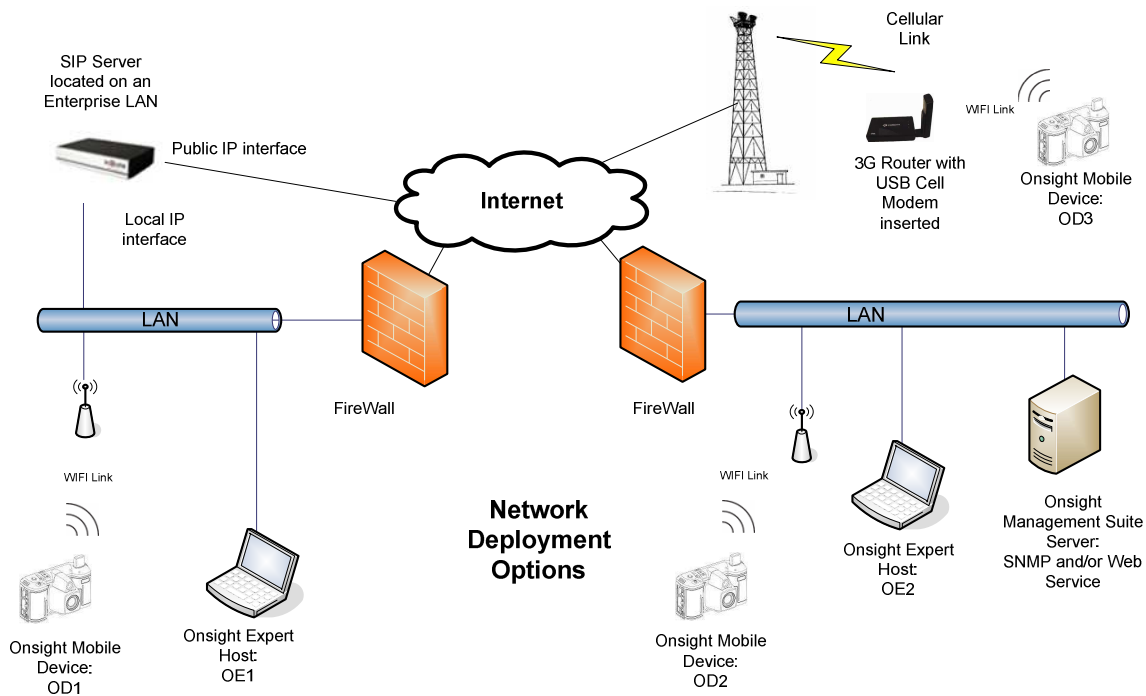
For further information regarding prerequisites consult the Onsight Management Suite, Onsight Device and Onsight Expert User Manuals.

## Stage 0: Network Architecture

The Onsite system uses Session Initiation Protocol (SIP) to establish audio and video sessions between Onsite Endpoints (Onsite Devices and Onsite Expert desktops). The session is established using TCP for the SIP protocol, Audio and Video media is sent using UDP packets, and a SIP Server is required to manage the traffic between the endpoints. The existing network architecture must be configured to permit the Onsite Endpoints to communicate with the SIP Server.

Involvement of the IT department is essential in ensuring a smooth deployment. Decisions on network security and deployment require their knowledge and in most cases approval before connecting the Onsite system to the network.

### Network Architecture Example



The key to ensuring that Onsite Endpoints can communicate with each other is access to the SIP Proxy Server. All SIP traffic can be restricted based on destination i.e. only allow originating SIP/Media traffic to the SIP Server. These requirements are described in more detail in Stage 1.

## Stage 1: Infrastructure Readiness

During the first stage, you will complete the corporate infrastructure set-up and confirm the corporate policy decisions. For example, the central IT group will need to open SIP and Media ports on the Firewall (destined specifically to the SIP Server) and confirm security policy decisions for the Onsite system.

### Security

Onsite provides many enterprise security options to safeguard the media and communication. These options include:

- User Authentication
- Configuration Access Control
- WiFi Security
- Media Encryption
- SIP-TLS Encryption
- Virtual Private Network
- Privacy (disables video and image saving)
- Firewall/NAT Traversal
- FIPS 140-2 Encryption

These options should be reviewed to confirm the features and options your enterprise would like to use. If your organization selects SIP-TLS encryption, you will need to install the SIP Server certificate on the Onsite Endpoints in the later deployment stages.

For more information see:

[http://www.librestream.com/Brochures/Whitepapers/Onsite\\_Security\\_Overview\\_v1.2.pdf](http://www.librestream.com/Brochures/Whitepapers/Onsite_Security_Overview_v1.2.pdf)

### SIP Server

When the Onsite Endpoints are located on different networks and SIP traffic must cross Firewall/NAT borders, a SIP Server is required to manage the traffic between the endpoints. The SIP Server also allows an URI addressing scheme (format: user@sip.com) to simply contact lists.

You will need the following SIP information for the next stage of deployment:

1. SIP server address
2. URI
3. User name and password
4. Authentication Transport Setting

Note: Using IP addresses to call the Onsite Endpoints directly is possible when the endpoints exist on a routable network i.e. WAN. However this approach is not recommended in a medium to large deployment due to the difficulty in managing IP addresses that may change regularly with DHCP addressing schemes.

Librestream has tested Onsight with the following SIP servers:

- The InGate SIParator
  - A Firewall/NAT-Session Border Controller with a built-in SIP Proxy Service.
  - For more information on the configuration of InGate with Onsight see: [http://www.librestream.com/Brochures/Whitepapers/Librestream\\_InGate\\_QSG.pdf](http://www.librestream.com/Brochures/Whitepapers/Librestream_InGate_QSG.pdf)
- Tandberg Video Communication Server (VCS)

In addition, Librestream also provides a SIP hosting service for enterprises that do not plan to implement their own SIP servers internally. For more information on the SIP Hosting Service Requirements, see

[http://www.librestream.com/Brochures/Whitepapers/Librestream\\_FireWall\\_Requirements.pdf](http://www.librestream.com/Brochures/Whitepapers/Librestream_FireWall_Requirements.pdf)

## Firewall Traversal

The corporate firewall must be configured to allow SIP Protocol and media traffic. The following ports are required to allow Onsight SIP and Media traffic to a SIP Proxy 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 SIParator. SIP-TLS provides encrypted SIP messages and requires the installation of certificates on the Onsight endpoints.
- UDP Media Ports: e.g. 58024 – 58523. This range is configurable on the SIP Server and allows the following RTP/RTCP streams:
  - Video
  - Voice
  - Subject Audio
  - Data

For more information see the Firewall Traversal Application Note:

[http://www.librestream.com/Brochures/Whitepapers/Librestream\\_FireWall\\_Requirements.pdf](http://www.librestream.com/Brochures/Whitepapers/Librestream_FireWall_Requirements.pdf)

## VPN

If your network architecture for deploying the Onsight system includes VPN access to your network, you must ensure the supported VPN methods are configured on your VPN Server. The Onsight Device supports L2TP/IPSec.

For more information, see the Onsight Device VPN Application Note at

[http://www.librestream.com/Brochures/Whitepapers/AppNote-VPN\\_OD\\_setup\\_v1.1.pdf](http://www.librestream.com/Brochures/Whitepapers/AppNote-VPN_OD_setup_v1.1.pdf)

A VPN connection allows an OD to connect from a 3<sup>rd</sup> Party network to the SIP Server through the native Enterprise LAN without needing to make Firewall changes at the 3<sup>rd</sup> Party network. However, VPN traffic must be allowed at the 3<sup>rd</sup> Party network.

### **Onsight Management Suite Web Service**

Depending on the placement of the OMS Server within your Network Topology, you may need to configure port forwarding on the network Firewall/Router for the OMS Web Service option. This port forwarding is required to allow the external Onsight endpoints to contact the server.

### **Network Architecture Checklist**

- SIP Server is installed/configured
- Firewall ports have been configured to allow SIP and Media traffic
- VPN Server is configured (Optional – not mandatory)
- Decisions made on Onsight security methods
- Install Firewall/Router Port forwarding established for the OMS Web Service

### **Additional Resources**

For further information regarding SIP Registration Setup consult the Onsight Device and Onsight Expert User Manuals and/or review the Application Notes identified above.

## **Stage 2: Onsight Management Suite Configuration**

The OMS software is used by central administrators to manage all the Onsight endpoints. In this second stage, the OMS software should be installed, licensed and used to create initial packages to push to Onsight endpoints. With OMS, the Administrator has the ability to manage each endpoint and set the features that are available to the users without Administrative privileges.

### **OMS Installation and Configuration**

1. Install OMS on a server that meets the defined specifications in the OMS user manual. This software will run for 60 days before the license activation key must be installed.
2. Before you start using OMS, you should activate the software and determine if you want to use OMS as a Web Service and/or SNMP management. You will need this decision prior to configuring the Onsight Endpoints.
  - a. Typically SNMP is sufficient when all endpoints are located on the same LAN. The Remote Web Service option is used when Onsight Endpoints are located outside the network, e.g. Field Technicians, but still need access to the

OMS Service for updates. The SNMP and Remote Web Service options can be run concurrently.

3. If you are planning to use the Remote Web Service option, set-up an Onsite Expert Custom Install Package in OMS. This function creates an XML file that will automatically configure the Server URI and Encryption key for the Onsite Expert installation in Stage 4.

Note: If you are using SNMP, you will need to select the SNMP Device Discovery function within OMS after the Onsite Endpoints have been configured with the SNMP information.

### **OMS Firewall Setup**

The Firewall/Router must forward incoming web service request from the Onsite Endpoints to the OMS Server in order for Onsite Endpoints to communicate with OMS when outside the Enterprise LAN/WAN.

### **Create Configuration Packages**

You can use OMS to create configuration packages to push specific settings to your Onsite Endpoints. Within the Configuration packages, you can centrally manage options such as bandwidth limitations, security policies, battery life settings, etc. for the Onsite Endpoints. You can set-up one or multiple package for Onsite Expert desktops and Onsite Devices if there is differentiation based on criteria such as location.

1. Create Onsite Expert Configuration package(s).
2. Create Onsite Device Configuration package(s).

Note: Make sure that your packages include the SNMP or Remote Web Service configuration information as well as the correct day/time information.

### **Create User / Contact Lists**

Using OMS, you can create User and Contact lists to send to all the Onsite Endpoints. You can create different lists for groups (e.g. by department or by region) to send specific lists to different groups of Onsite Endpoints. .

### **Create Media Configuration Packages**

The Onsite Endpoints ship with three preconfigured media settings including:

- High (720 x 480 resolution, 10 fps, target 1Mb/sec bandwidth)
- Medium (528 x 368 resolution, 10 fps, target 400 Kb/sec)
- Low (320 x 240 resolution, 10 fps, target 250 Kb/sec)

You may wish to distribute additional standard media configurations to your Onsite Endpoints. For example, if your use case involves high motion, you may wish to set-up and push out an option that includes 30 frames per second (fps).

### **Certificate Packages**

If you are using SIP-TLS, you can create a package to push out the certificate to your Onsite Endpoints.

### **License Management – Onsite Expert**

To activate the Onsite Expert software, the end users can manually enter Activation Keys or you can automate the process. To automate in OMS, you would do the following:

1. Import or enter the Activation Keys within OMS
2. In Stage 4, you will create an Onsite Expert Activation Job in OMS to push out to the Onsite Expert desktops

Note: You can also create an Onsite Expert Custom Install Package file (as described earlier) that includes the Activation Key. However, this approach is not typical for large scale deployments, as you would need to create a custom file for each user.

### **OMS Configuration Checklist**

- Install, Activate and Configure OMS
- Create Onsite Expert Custom Install file if using Remote Web Service
- Create Onsite Device and Onsite Expert Configuration packages
- Create User/Contact list(s)
- Create Media Configurations, if desired
- Create Certificate packages, if SIP-TLS used
- Enter the Onsite Expert Activation Keys
- Distribute the login account information to the end users, (User name and passwords) in order for them to be able to login to the endpoints.

### **Additional Resources**

Refer to the OMS User Manual for more details on package creation and deployment.

## **Stage 3: Configuring the Onsite Devices**

### **Connect Onsite Devices to the Network**

The Onsite Device *must* be powered on, connected to an AC power supply and connected to either a Wireless network or through Ethernet to receive package updates from the OMS server.

The Onsite Device *must* be manually configured to connect to the Wireless Network. If using an Ethernet connection with an Onsite 2000 device, you will need to attach the I/O sled to the bottom of the device in order to connect the cable. The Ethernet connection requires no further configuration.

### **Complete Manual Configuration Requirements**

1. Connect OD to the network
2. Configure OD with either the SNMP Community details or the Remote Web Service information to allow OMS communication to the device
3. Make sure the Onsite Devices have the correct Date/Time

### **Onsite Device Discovery**

After the Onsite Devices are connected to the network and manually configured, OMS must perform the ‘SNMP Discovery’ to create the list of Managed Endpoints.

### **OMS Software Update Job**

In OMS, create a Software Update Job that includes the configuration packages, user/contact lists, etc. that you want to push out to the Onsite Devices. You can create multiple Software Update Jobs to select specific packages for groups of Onsite Devices, if desired.

Note: these packages may take a few minutes to reach all the Onsite endpoints.

### **Confirm Correct Configuration**

After the Software Update Job is complete, test a sample of Onsite Devices to confirm the settings are correct before they are shipped to the users. A typical test would be to login as a user, confirm SIP registration, and conduct a test call.

### **Package and Ship**

The Onsite devices are typically sold with an accessory kit that includes a hard carrying case, spare battery, SD card, spare stylus and headset. Place the OD and DC power adapter back into the hard carrying case and confirm that the accessories are there prior to shipping.

## Onsight Device Configuration Checklist

- Connect the Onsight Devices to the network
- Complete the manual configuration requirements for each OD
- Create the 'Software Update Job' in OMS for the Onsight Devices
- Perform the SNMP Device Discovery within OMS, if SNMP is used
- Test a sample of the Onsight Devices
- Package and Ship the Devices to the End Users

## Additional Resources

Refer to the Onsight Device User Manual for more details.

Refer to the OMS User Manual for more details on Onsight endpoint configuration, package creation and deployment.

## Stage 4: Configuring the Onsight Expert Desktops

### Onsight Expert Installation

The Onsight Expert software is typically stored on a network drive and distributed to the appropriate staff via a link to this central storage location. The recipient would typically run the software install from the network folder in order to install it on their computer. The OE software will run in trial mode for 60 days prior to requiring an activation key.

Onsight Expert Custom Installs can be made using the 'Create Onsight Expert Custom Install' feature. The Custom install allows automatic configuration of Web Service. See the OMS User Guide for details.

### Onsight Expert Discovery

If you are using SNMP for OMS, follow the SNMP set-up instructions in the Onsight Management Suite User Guide. From OMS, you must then perform the 'SNMP Discovery' to create the list of Managed Endpoints.

### Onsight Expert Activation

To license Onsight Expert, users can enter the Activation Keys manually as described in Stage 2 or you can automate the process through OMS.

- If you are using OMS, you should have already entered the Activation Keys in Stage 2.

- In this stage, you will Create Onsite Expert Activation Job in OMS. This action will automatically push the Activation Keys to the Onsite Expert clients you select.

Using OMS to distribute the Onsite Expert Activation Keys in this manner is the recommended method. You can also activate each Onsite Expert desktop separately through the Custom Install option that is described in Stage 2.

Note: The Onsite Expert application must be running on its host PC in order to receive updates from the OMS.

### **OMS Software Update Job**

In OMS, create a Software Update Job that includes the configuration packages, user/contact lists, etc. that you want to push out to the Onsite Expert desktops. You can create multiple Software Update Jobs to select specific packages for groups of Onsite Expert desktops, if desired.

Note: these packages may take a few minutes to reach all the Onsite endpoints.

### **Confirm Correct Configuration**

After the Software Update Job is complete, test a sample of Onsite Expert desktops to confirm the correct settings before they are approved for use by the users. A typical test would be to login as a user, confirm SIP registration, and conduct a test call.

### **Onsite Expert Configuration Checklist**

- Set-up a central location for users to access the Onsite Expert installation
- Complete the Onsite Expert Activation Job through OMS
- Configure SNMP Community on the Expert
- Create the 'Software Update Job' in OMS for the Onsite Expert desktops
- Perform test calls with a sample of the Onsite Expert users

### **Additional Resources**

Refer to the Onsite Expert User Manual for more details.

Refer to the OMS User Manual for more details on Onsite endpoint configuration, package creation and deployment.

## Stage 5: User Training

After the Onsite Endpoints are configured and available for use it is important to train the end users on how to use the Onsite system effectively as a collaboration tool. Librestream can provide end user training online or onsite, if required. If the training is provided online, it can be recorded and provided to you for future use.

A sample of the important initial topics is outlined below.

1. Basic System training
  - How to Login
  - Making Calls
  - Still Image Sharing
  - Streaming Video (Live and Recorded)
  - Recording Video
  - Etc.
2. Review Best Practices
3. Identify Use Cases where the Onsite mobile collaboration system can leverage expertise within your enterprise.

## For More Information

Librestream Technologies Inc.  
895 Waverley, Suite 110  
Winnipeg, Manitoba  
Canada, R3T 5P4  
Phone: 1-800-849-5507 / +1-204-487-0612  
Fax: +1-204-487-0914  
[www.librestream.com](http://www.librestream.com)  
[info@librestream.com](mailto:info@librestream.com)