ON SIGHT

APP NOTE

Onsight Connect Service
Enterprise Deployment Guide

July 2016

LIBRESTREAM

Table of Contents

Document Revision
APP NOTE
Enterprise Deployment guide
Doc #: 400278-01
July 2016

Overview

The purpose of this document is to provide an overview of the stages involved in a mid to large scale deployment of Onsight Connect.

The following Deployment stages will be discussed:

- Network Infrastructure
  - Required infrastructure such as a Wireless Access Points, SIP server, and firewall considerations.
- Onsight Account Manager
  - Configuration
  - Software Installation
- Training for Onsight Connect end users
- Work Process Adoption
- Where does Onsight Connect fit into current processes and workflows
  - Changing work habits to include Onsight Connect as a valuable tool
    - How will adopting the new tool affect Metrics for employee evaluation?
- What situations benefit from Onsight Connect?
  - Problem resolution through collaboration
  - Inspection, Maintenance, Repair
  - Consultation
  - Training

Stage 1: Network Infrastructure

Both the Wireless and Wired network infrastructure need to be configured to allow for and optimize continuously streaming video.

Network Infrastructure Checklist

- ☑ Wireless Infrastructure supports video streaming
- ☑ Network policy allows and is configured for the required network protocols
- ☑ Security policy is defined
- ☑ SIP Server is installed/configured
  - SIP Accounts for Onsight Connect users are configured
- ☑ Proxy configuration
- ☑ Firewall ports have been configured to allow SIP and Media traffic
- ☑ Decisions made on Onsight security methods
- ☑ Install Firewall/Router Port forwarding established for the OMS Web Service

Infrastructure Readiness

Confirm the exiting network infrastructure can support the Onsight Connect deployment:

- Onsight Connect for Windows requires Ethernet or Wireless connections. Ethernet is recommended.
- Onsight Devices require Wireless network connections for mobility.

- Wireless network coverage must provide reliable signal quality and bandwidth to support streaming Audio/Video. Adding extra Wireless Access Points in areas of little or no coverage may be required.

- A Wireless Site Survey will identify areas that require upgrades or additional Wireless network infrastructure.

For guidance on wireless network requirements please refer to the white paper – *Wireless Network Considerations* available at http://www.librestream.com/support .

Required Network Protocols

The existing network infrastructure must be configured to permit the Onsight Endpoints to communicate with the required Cloud Services.

- *Onsight Connect requires an HTTPS (TCP port 443) connection to the Onsight Connect Service for user authentication and endpoint configuration.*
- *Onsight Connect requires a SIP (TCP port 5060/5061)) connection to a SIP Service for making calls across the internet.*
- *TeamLink requires an HTTP/S (TCP port 443 or 80) connection to the Cloud Service to provide tunneled SIP connections to the SIP Service.*
- *Firewall detect requires STUN (UDP port 3478) connection to the Cloud Service to determine SIP connectivity for TeamLink.*
- *Sessions between Onsight Endpoints require Media streams for Audio/Video/Data (UDP port range dependent on the SIP Service provider).*

For complete details on the required network protocols please refer to the application note – *Onsight Connect Network Requirements* available at http://www.librestream.com/support/knowbase.html.

SIP Server

When the Onsight 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 URI addressing (format: user@sipdomain.com) to simplify contact lists.

- *Each Onsight Connect User requires a unique SIP account on the SIP Server.*
- *SIP Server Address, SIP URI, Authentication Transport, Authentication name and password are required when setting up users in Onsight Account Manager.*

Librestream has tested Onsight Connect with the following SIP servers:

- Onsight SIP Service
- Cisco Video Communication Server (VCS)
- The InGate SIParator

Librestream provides a SIP Hosting Service for Enterprises that do not plan to deploy their or own SIP Servers or as a temporary service while their SIP Server is deployed.

For more information on SIP Server Requirements see the Application Note:
http://www.librestream.com/Brochures/Whitepapers/AppNote_Librestream_Network_Requirements_v5.1.pdf

Firewall Traversal

When registering directly to a Public SIP Service, the 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-TLS TCP: 5061
  - SIP-TLS encryption is the recommended protocol for SIP messaging on the SIP Server. SIP-TLS provides encrypted SIP messages and requires the installation of certificates on the Onsight endpoints.
- SIP TCP/UDP: 5060
  - The Onsight Endpoints can use SIP TCP 5060 for SIP messaging but the option to use SIP UDP 5060 is recommended. SIP TCP is not encrypted, using it in conjunction with Media encryption is not recommended. Use SIP-TLS whenever media encryption is required.
- UDP Media Ports: e.g. 15000 – 65000. This range is configurable on the SIP Server and allows the following RTP/RTCP streams:
  - Video
  - Voice
  - Subject Audio
  - Data

For more information on Firewall Traversal see the Onsight Connect Network Requirements Application Note:
http://www.librestream.com/Brochures/Whitepapers/AppNote_Onsight_Connect_Network_Requirements_400210-04_revA.pdf

TeamLink can tunnel SIP and Media traffic through the Firewall using HTTPS port 443.

Security

Onsight Connect provides enterprise security options to safeguard the media and communication. These options include:

- Onsight Connect Service User Authentication (HTTPS TCP:443)
- Wireless Security (802.11 a/b/g/n)
- Media Encryption (AES-128)
- SIP-TLS Encryption (AES-128)
- Proxy Authentication support
- Privacy (disables video and image saving)
- FIPS 140-2 Encryption

These options should be reviewed by the stakeholders to confirm the features and options your Enterprise would utilize.

For more information see: http://www.librestream.com/Brochures/Whitepapers/Onsight_Security_Overview_v1.2.pdf

Stage 2: Onsight Account Manager

Onsight Account Manager (OAM) is the central management system for configuring the Onsight Connect endpoints. The Onsight Account Administrator is assigned by your organization and configures the settings using the Onsight Account Manager Web interface located at https://www.onsight.librestream.com.

Group Client Policy, Security, and Endpoint Settings should be configured before adding users to the system.

For complete details on using Onsight Account Manager refer to the OAM User Manual at http://www.librestream.com/support/knowbase.html.

Configuring Onsight Connect for Windows

Onsight Connect for Windows Installation

When a user is added to the Onsight system they receive a Welcome email from Onsight Account Manager. Download, install and login information is included in the email.

The Onsight Connect for Windows software is also available for download from Librestream's Software download page. Enterprises typically store the Installation package on a network drive and distribute it 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. Once installed they login to Onsight Connect using the credentials received in the Welcome Email.

Configuring Onsight Connect for iOS and Android

Onsight Connect for Smartphones (iOS and Android) is controlled by configuring Group Client Policy using OAM. Users are free to download the app from the Apple App Store or Google Play Store however they must have a valid user account in order to login. Smartphone users can be configured to use the application in either Expert or Field mode. See the OAM User Manual for details.

Configuring Onsight Devices

Connect Onsight Devices on the Network

All Onsight Devices must have a network connection in order to contact the Onsight Connect Service and place calls:

- Onsight Connect for Windows will use the PC's existing network connection.
- Onsight for iOS will use the existing iPhone or iPad's network connection. This will include wifi or 3G/4G.
- Onsight Devices, e.g. 2500n, must be configured to connect to the network using either wireless or Ethernet connections. Wireless is the preferred method for mobility.

The Onsight Devices must be manually configured to connect to the Wireless Network before being able to contact the Onsight Connect Service.

For Ethernet connectivity attach an I/O sled to the Onsight Rugged Smart Phone.

For complete details on using configuring Onsight Devices refer to the Onsight Account Service Setup Guide at http://www.librestream.com/support/knowbase.html.

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.

Onsight Account Manager Checklist

- ☑ Your Onsight Administrator has been assigned and has received their Welcome email from Onsight Account Manager.
- ☑ You have obtained the required number of license subscriptions to support your deployment of Onsight Connect users.
- ☑ SIP Service arrangements have been made to provide SIP accounts to your Onsight Connect users.
- ☑ If downloading Onsight Connect for Windows directly from the Onsight Connect Server is not preferred, Set-up a central location for users to access the Onsight Connect for Windows installation
- ☑ Perform test calls with a sample of the Onsight Connect for Windows users, a subset of users can be added initially to facilitate initial testing.
- ☑ Add all users to Onsight Account Manager.
- ☑ Create Groups and Configure Client Policy for all Users based on Group membership.

Additional Resources
Refer to http://www.librestream.com/support/knowbase.html for more details.

Stage 3: User Training

After the Onsight Endpoints are configured and available for use it is important to train the end users on how to use the Onsight system effectively as an Operations based 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
    - Searching the Global Directory
    - Making Calls
    - Still Image Sharing
    - Streaming Video (Live and Recorded)
    - Recording Video
    - Etc.
2. Hands on Practice
3. Best Practices

Onsight User Training Checklist

- ☑ User accounts have been created and Welcome emails received by all users.
- ☑ Onsight Connect software has been installed by all users.
- ☑ After training users understand how to do the following:
    a. Login
    b. Search the global directory
    c. Place a call
    d. Share video, still images and recordings
    e. Change media configurations
    f. End call
- ☑ Users have been instructed when to use video calls.
- ☑ Users understand who to contact if issues arise.

Stage 4: Work Process Adoption

Successful Adoption of Onsight Connect relies on:

- Defining a work process that outlines how to use Onsight Connect
- Identifying Use Cases where the Onsight Connect can leverage expertise within your enterprise. i.e. when to make video calls
- Identifying who to call
- Identify to whom to report any issues

For More Information

Please contact Librestream at information@librestream.com.