ON SIGHT

RELEASE NOTES

Onsight Connect for Librestream Devices
Software Version 7.1.6

July 2016

LIBRESTREAM

Table of Contents

Document Revision

Name of Librestream Software Onsight Connect

Overview

This document includes the Onsight Connect for Librestream Devices (2500/2000/1000) software release notes for Major Revision number 7 including a description of new features, resolved issues and a list of Known Issues.

All releases of Onsight Connect software have been validated with their concurrent release of Onsight software products and are compatible with the previous revision of all Onsight products.

The Onsight operations-driven video collaboration system provides interactive video, audio, images and telestration to immediately connect remote teams, suppliers and customers. Using Onsight Connect, teams can collaborate fully across distant locations to quickly solve problems, monitor projects and improve overall communication.

Recommended Equipment/Infrastructure

This section documents the recommended equipment to be used with Librestream's Onsight Devices.

SD/SDHC Memory Card
- SD/SDHC Memory cards used with Onsight must have a speed grade of Class 10 (or higher) or meet the following performance requirements:
    - Minimum write speed: 9.0 MB/sec
    - Minimum read speed: 10.0 MB/sec
    - The SanDisk Ultra-II series of SD and SDHC cards have been tested and are recommended. Other brands that meet the performance requirements should also be acceptable.
- Important Notes:
    - Non-SDHC format SD cards larger than 2GB are not compatible with Onsight and may result in poor or incorrect performance.
    - The SD card must be formatted in the Onsight Device before first use. Cards not formatted using the Onsight Device may have insufficient performance.
    - The Onsight Device does not support SDHC cards greater than 32GB.

802.11 Radio Infrastructure
- Librestream recommends the use of Symbol, Cisco, Fortress and Honeywell 802.11g wireless infrastructure equipment with the Onsight system. In limited testing, other brands of 802.11 equipment have not shown significant Issues or issues; however, Librestream has not conducted sufficient testing to ensure compatibility in all cases.
    - Important Notes:
    - Disable "Aggressive Load Balancing" on Cisco Wireless LAN Controllers to allow reliable roaming. (Note: Cisco makes the same recommendation when using Cisco Wireless IP phones).

NAT/Firewall Traversal
Librestream recommends the use of its hosted Onsight SIP Service or Cisco Video Communication Server (VCS) for NAT and firewall traversal. In conjunction with these products, the Onsight TeamLink service can provide further NAT and firewall traversal capabilities by tunneling through HTTP and HTTPS ports. Please contact Librestream for further information.

Software Release Notes for Onsight Connect Version 7.1.6.7

Changes and Improvements since Previous Version

- Onsight Connect for Librestream Devices now supports TLS v1.2.

    - Note: TLS 1.0 and TLS 1.1 are deprecated but are still supported.

- gSOAP v2.8.27 support added.

- Privacy for images and recordings can be controlled separately.

- WebEx Collaboration Meeting Room (CMR) support.

- Fixed #12038: Direct SIP registration is no longer attempted when already registered to TeamLink.

- Various minor fixes and improvements.

Software Release Notes for Onsight Connect Version 7.0.11.8

Changes and Improvements since Previous Version

- Fixed Ref#11554: Client Policies applying Bandwidth Control are now applied correctly on the for the Onsight user account.

- OpenSSL v1.0.1m update.

- Various minor fixes and improvements.

Software Release Notes for Onsight Connect Version 7.0.10.8

New Features

Setup Wizard

Onsight Rugged Smart Cameras now include a Setup Wizard for simplified configuration of wireless networks, date and time, and certificates.

HD Compatibility

Onsight Rugged Smart Cameras can participate in calls with HD capable endpoints however they do not support HD quality resolutions therefore cannot send or receive 1080p or 720p video configurations. HD media profiles will be disabled when the 2500 is connected to an HD capable device.

Touch Tone Keypad

Onsight Rugged Smart Cameras can now participate in conference bridge calls that require you to enter a Conference ID. The TOUCH TONE KEYPAD provides DTMF tones allowing you to enter the code and join the conference bridge.

SHA-2 Certificate Support

Onsight Rugged Smart Cameras have added support for X.509 Certificates with SHA-2 signatures. This is required for access to Onsight Connect Web servers.

Changes and Improvements since Previous Version

Usability
- Various minor fixes and improvements.

Known Issues

In PEAP-GTC mode if there aren't any preferred networks configured, the available networks list is blank on startup until forcing a refresh. #8066
Onsight 2500 with 802.11b/g radio units (not applicable to 2500n - 802.11 a/b/g/n radio units) unable to get a valid IP address when connecting to a network that uses Hidden SSID with PEAP GTC. The work around is to use 802.1X Authentication with WEP. Affects the Following Onsight Device models: Model, System Board Number(s) MCD2500-N05, 300057-03_revB MCD2500-N06, 300057-03_revB MCD2500-R05, 300057-03_revB or 300085-02_revA MCD2500-R06, 300057-03_revB or 300085-02_revA MCD2500-R07, 300057-03_revB or 300085-02_revA Users can view the System Board Number under Configuration\Information\Versions. #8063
It is possible for the Firewall Detect test to report that the SIP ports are disabled even though a Firewall rule has been enabled to allow SIP traffic to a specific SIP Server address. This is due to the fact that the Firewall Detect test uses the TeamLink server as the destination address for all ports being tested. Since the TeamLink server has not been added to the Firewall rule as an allowed destination the Firewall Detect test reports the SIP ports are disabled. This will result in the Onsight software using TeamLink instead of sending SIP/Media traffic directly to the SIP Server. Ref#7240
Onsight mobile devices must have their date and time set accurately to be able to authenticate using HTTPS to the Onsight Connect Service. Ref#7166
Onsight Devices MCD1000/MCD2000/MCD2500-(N05, N06, R05, R06, and R07) may not be able to connect with Cisco AP's presenting CCKM as an encryption option. When CCKM is enabled, the Onsight Device may not operate with WPA2 but will operate with WPA. Note that Access Points that enable combinations of WPA and WPA2 with '802.1X and CCKM' will work as long as the encryption for WPA and WPA2 are identical. However, the Onsight Device will only connect using WPA even though both WPA and WPA2 are enabled on the Access Point. Eg. AP Security Settings: AP with WPA-TKIP and WPA2-TKIP: Onsight Device will connect with WPA-TKIP AP with WPA-TKIP and WPA2-AES: Onsight Device fails to connect Ref#5394
Selecting UDP for SIP messaging only affects direct IP calls. Registered SIP calls will always use TCP for SIP messaging. Ref #4956
The side-tone feature does not work with Bluetooth headsets. Ref#5508

Some hotspots may be incompatible with the Hotspot Login feature. Retry with different settings under the Configuration->Network->Hotspot Login->Browser Compatibility Mode option. Ref#5794
Device may not properly disconnect from an AP when out of range. Manual disconnect is required. Ref#5873
Selecting an S-Video In standard on the Onsight Device that does not match the standard of the S-Video input may result in distorted video to other participants. In this case the Onsight Device must be reconfigured for the correct standard and the Onsight Device restarted. Ref #5307
Connecting a live S-Video signal to the Onsight Device while the device is starting or restarting may result in distorted video to other participants. It is recommended not to have a powered S-Video source connected to the Onsight Device during device start up. Ref #5318
When an EAP 802.1x Authenticated Preferred Network is created (pushed out to the device via the Onsight Management Suite or created locally), the EAP authentication settings for the Preferred Network will only be preserved for the user that is logged in at the time the Preferred Network was installed/created on the device. Workaround is to log in as every other user and re-enter the EAP authentication settings. Ref #4322.
When a Preferred Network uses IEEE 802.11X Authentication with Username/Password and the Respond Automatically checkbox is checked, the Username/Password dialog may also be incorrectly suppressed for VPN connections that use Username/Password type authentication. It is recommended that the Respond Automatically checkbox remains unchecked unless you have 802.1X authentication issues. Ref #4321.

For More Information

If you need Release Notes for an earlier version, please contact Librestream at support@librestream.com.