



## Application Note

**Onsight TeamLink: Firewall Tunneling Service**

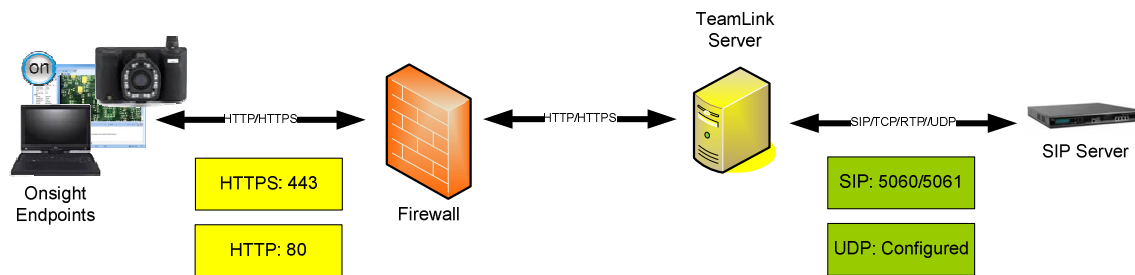
# Table of Contents

Onsight TeamLink Overview .....	2
Transmission Security .....	2
Direct SIP Server Communication .....	2
Onsight TeamLink Configuration.....	3
TeamLink Settings.....	3
Firewall Detection.....	4
Example: Onsight Endpoints perform Firewall Detect Test.....	4
Firewall Detect Preferences.....	5
Firewall Detect Advanced Settings .....	5
Firewall Detection Status .....	6
Order of Precedence Summary.....	8
Potential Issues.....	9
Latency on Poor Networks.....	9
False SIP Negatives from Firewall Detect .....	9
Cisco VCS Expressway Pairs .....	9
Proxy Settings.....	10

## Onsight TeamLink Overview

Librestream's innovative Onsight TeamLink capability immediately connects teams across networks without needing to open SIP and UDP firewall ports. It provides a quick and easy method for Onsight to connect across networks that prevent standard SIP calls as a result of their firewalls. This option can greatly simplify the Onsight experience, especially when teams need to urgently connect with customers or suppliers across various networks.

In these cases, as long as HTTP (port 80) or HTTPS (port 443) traffic is allowed through the firewall, the Onsight TeamLink Server (OTLS) can quickly connect Onsight collaborators across firewalls that typically restrict SIP/Media traffic. If you can browse the Internet, you can most likely connect Onsight collaborators without making any adjustments. The Onsight TeamLink traffic flow is depicted below.



### ***Transmission Security***

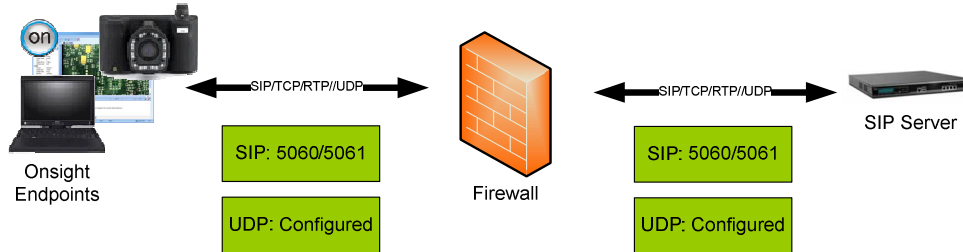
Onsight TeamLink acts as a proxy. The Onsight mobile devices and Onsight Expert client endpoints send all SIP and media traffic encapsulated in the HTTP or HTTPS protocol. Onsight TeamLink forwards the SIP and media traffic to the SIP Server and automatically negotiates the connection.

Onsight supports the SIP-TLS security method and AES128 bit content encryption to provide end to end security over the transmission. In addition, an enterprise has the option to disable Onsight TeamLink or restrict it to just HTTPS (TCP 443) if there are any concerns about HTTP (TCP port 80) connections.

### **Direct SIP Server Communication**

The ideal method to establish an Onsight collaboration session is direct communication with the SIP Server. This method sends all traffic directly to the SIP Server, which can optimize performance. In this case, the network firewall must allow traffic for the required SIP and UDP ports. As mentioned previously, it may be challenging to get the required firewall ports open to allow this connection. In that case, the Onsight TeamLink method is the best approach.

Direct SIP Server communication traffic flow is typically Onsite Endpoint > Firewall/NAT > SIP Server. This requires that the SIP and UDP ports are allowed on the firewall to the destination address of the SIP Server. Again, if the ports are not open, Onsite TeamLink provides an alternative method to connect Onsite endpoints.

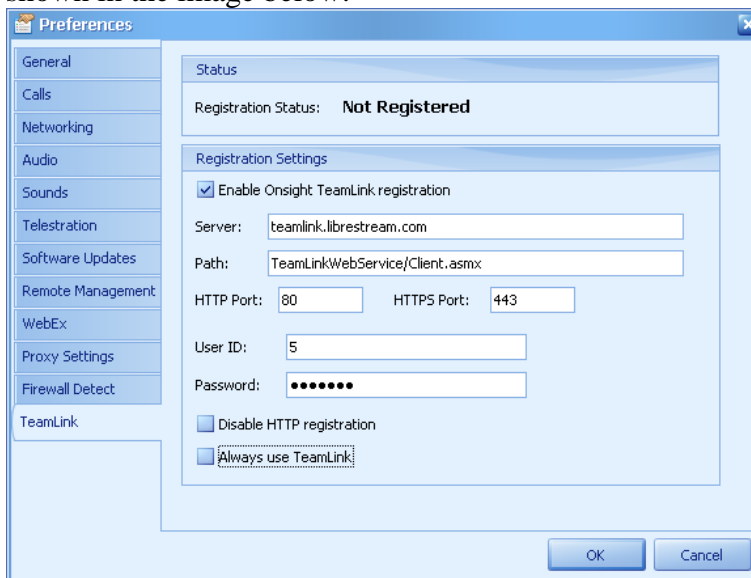


## Onsite TeamLink Configuration

There are two areas involved in the configuration of the Onsite TeamLink tunneling service – TeamLink settings and Firewall Detect settings.

### TeamLink Settings

To connect to TeamLink the Onsite endpoint must be configured with the information shown in the image below:



**Note:** Contact Librestream if you do not already have an Onsite TeamLink User ID and Password.

The following table describes each of the fields shown above.

Registration Status	Reports TeamLink registration status
Server	Onsight TeamLink IP address or Domain name (provided by Librestream)
Path	the path to the OTLS on the host Server
HTTP port	the port used by TeamLink to receive HTTP traffic
HTTPS port	the port used by TeamLink to receive HTTPS traffic
User ID	the Onsight TeamLink user ID (provided by Librestream)
Password	the Onsight TeamLink user account password (provided by Librestream)
Disable HTTP registration	Disables HTTP so that only HTTPS is used to register to the OTLS. HTTP may not be desired since it is unencrypted.
Always use TeamLink	Only register to the SIP Server via OTLS

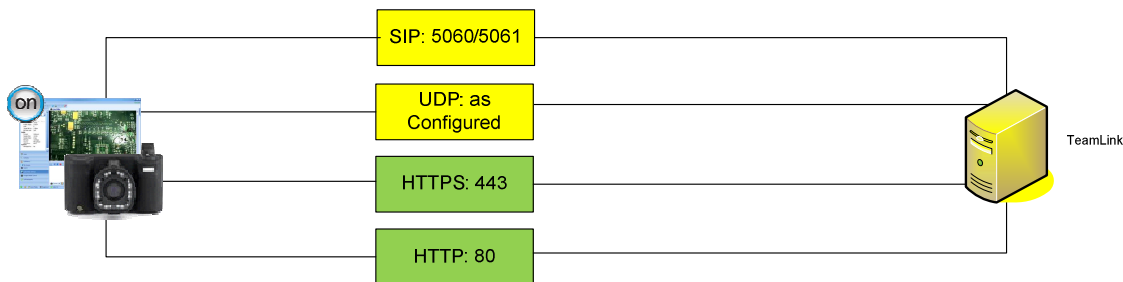
## Firewall Detection

The second component to configure for Onsight TeamLink is the Firewall Detect settings. However, if the default settings are acceptable, there is no additional configuration required.

The Firewall Detect Test *automatically* tests the firewall status of Onsight mobile devices and Onsight Expert desktop clients. Depending on the results of the automated test, Onsight calls will connect through SIP, HTTPS or HTTP protocols without any IT intervention required.

The Firewall Detect Test sends SIP, UDP, HTTP, and HTTPS test packets *directly to the TeamLink Server* to determine if the ports are open on the Firewall. If a reply for each packet type is not received the port is marked as unavailable.

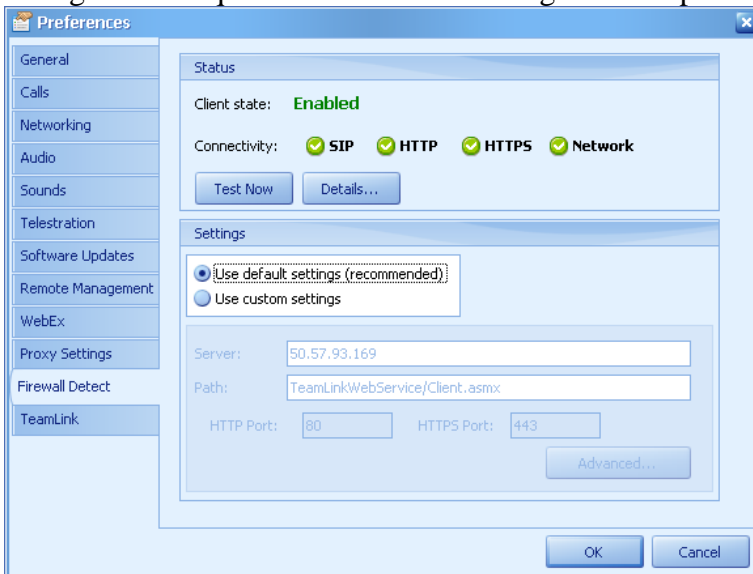
## Example: Onsight Endpoints perform Firewall Detect Test



Both the SIP and UDP ports must be opened for the SIP connectivity test to pass and be reported as 'Enabled'.

## Firewall Detect Preferences

The initial Firewall Detect configuration screen is shown below. There is no configuration required if the default settings are acceptable.



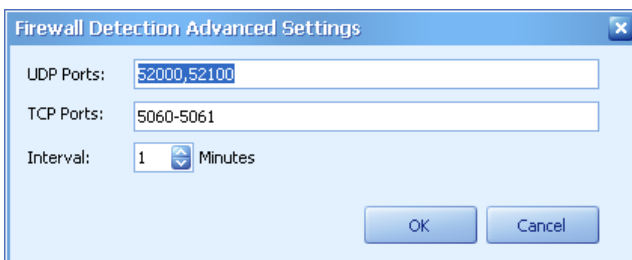
The following table describes each of the fields shown above.

Client state	indicates state of the Firewall Detect client
Connectivity	indicates connection method status
Test Now	runs the Firewall Detect test
Details	displays Firewall Test results
Use default settings	uses the TeamLink default port settings for the Firewall Detect Test, e.g. HTTP (TCP port 80)
Use custom settings	if custom port settings are required to run the Firewall Detect Test
Advanced	set the custom UDP, TCP ports and test interval for Firewall Detect Test

## Firewall Detect Advanced Settings

To customize the Firewall Detect ports, select 'Use custom settings'. You can then configure the ports to test if your enterprise is not using the standard ports for HTTP (i.e. TCP 80) or HTTPS (i.e. TCP 443).

Press the 'Advanced...' button to enter the custom UDP and TCP ports for SIP and media traffic on the firewall. The following screen will be displayed.

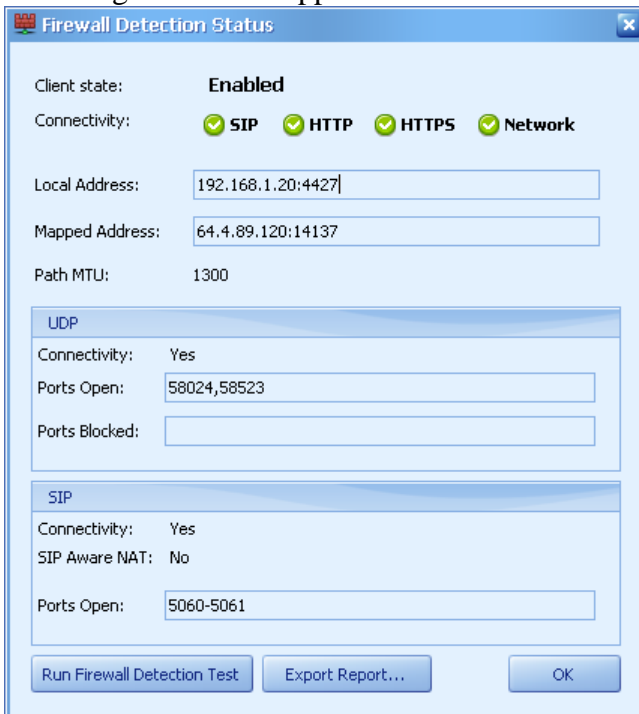


The following table describes each of the fields in the screens shown above.

Use default settings	Use the default TeamLink Server configuration
UDP Ports	Manually set the UDP ports to be tested for Media
TCP Ports	Manually set the TCP ports to be tested for SIP
Interval	Enter the minutes between test runs

## Firewall Detection Status

For a summary of all the Firewall Detect settings and status, select 'Details...' and the following screen will appear.



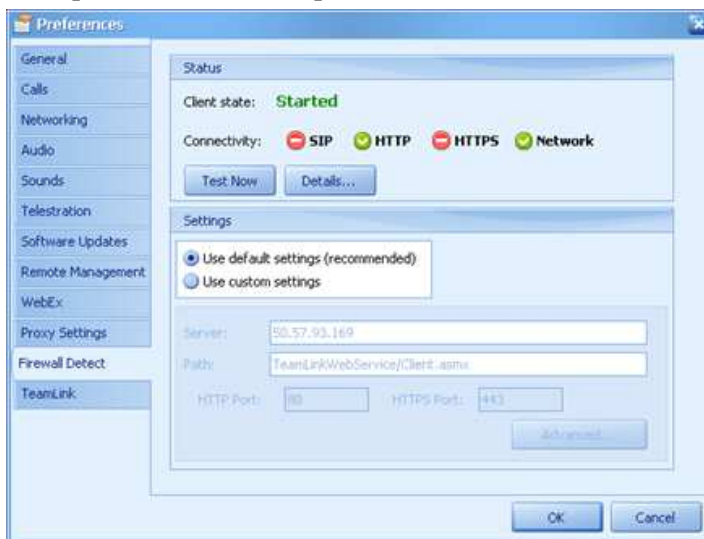
The following table describes each of the fields shown above.

Client state	Indicates whether Firewall Detect is active
Connectivity	Reports the Status of the SIP Registration methods and Network. Connection Method is Open/Network is connected Connection Method is Disabled Connection Method is Blocked
Local Address	Reports the Local IP address of the Host PC running Onsite Expert
Mapped Address	Reports the external IP address of the Firewall the PC sits behind
Path MTU	Reports the size of the Maximum Transmission Unit for the Host PC
UDP Connectivity	Reports the status of the listed UDP ports on the Firewall
SIP Connectivity	Reports the status of the listed TCP ports on the Firewall

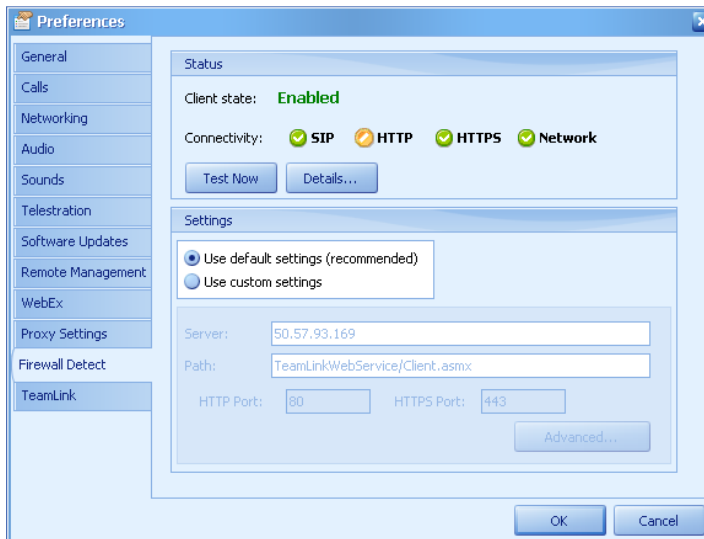
The UDP test checks the ports used for the media such as audio, video and data. For efficiency, set the boundaries of the port range you would like to test as in the example above by separating them by commas e.g. 52000, 52100. Testing a complete range e.g. 52000 – 52100 could take an excessive amount of time.

The SIP test will check for TCP ports 5060 and 5061 and it will test for SIP aware Firewalls. The SIP Aware NAT test is a SIP header test looking for Public IP addresses being inserted in the SIP header in place of private LAN IP addresses. When a SIP Aware NAT is present it can cause confusion for the SIP Server so it is best to use SIP-TLS as the transport. SIP-TLS will encrypt the SIP headers and make these unavailable for inspection by the SIP Aware NAT.

**Example: SIP and HTTPS ports are blocked to the TeamLink Server**



**Example: SIP and HTTPS are available. HTTP was disabled and will not be used.**



## Order of Precedence Summary

Onsight TeamLink will determine the optimal method based on the results of the Firewall Detect test. If SIP is available, Onsight endpoint will connect directly to the SIP Server. However if SIP is not available, the Onsight endpoint will use either HTTPS or HTTP to tunnel the SIP traffic to the TeamLink Server.

1. SIP / UDP	<p>The first choice is to connect using SIP if both the SIP and UDP ports are open.</p> <p>SIP: if confirmed as open, the Onsight endpoint can register directly to a SIP Server such as the InGate SIParator or Cisco Video Communication Server (VCS).</p> <p>UDP: if confirmed as open, the Onsight endpoint can send Media traffic directly to a SIP Server.</p> <p>Both SIP and UDP must be open to use direct SIP registration.</p>
2. HTTPS	<p>The second choice is to connect using HTTPS if port 443 is open and the Onsight TeamLink CA certificate is installed on the Onsight endpoint. Thawte is the CA for the TeamLink Server certificate.</p> <p>Note: This certificate is included in the V5.0 upgrade for the Onsight Mobile (Device) software.</p> <p>If confirmed as open, the Onsight endpoint can register to Onsight TeamLink and proxy all SIP and UDP media traffic through it.</p>
3. HTTP	<p>The third choice is to connect using HTTP if port 80 is open.</p> <p>If confirmed as open, the Onsight endpoint can register to Onsight TeamLink and proxy all SIP and UDP Media traffic through it.</p>

## Potential Issues

### Latency on Poor Networks

Streaming video over TCP port 80 or 443 can introduce latency. Librestream has implemented an innovative approach to overcome this latency, but in situations where network reliability is poor and available bandwidth is low, there may be a noticeable effect.

In these situations, Librestream recommends adjusting the Onsite media configurations to decrease the bandwidth load. If that isn't sufficient, it is worthwhile to go through the process required to open the SIP and UDP firewall ports.

### False SIP Negatives from Firewall Detect

It is possible to get a false negative from the Firewall Detection Test for the SIP test. This false negative may occur in the following situation.

The Onsite TeamLink server will not 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 Onsite TeamLink server as the destination. If the Firewall blocks SIP to OTLS but allows SIP to another unknown SIP Server, the test result will report 'SIP blocked'. In this case, the OTLS should be added to the Firewall White List on your network to allow traffic to it.

Note: the term 'unknown SIP Server' is meant only to indicate that OTLS is unaware of the SIP Server in terms of Firewall Detect.

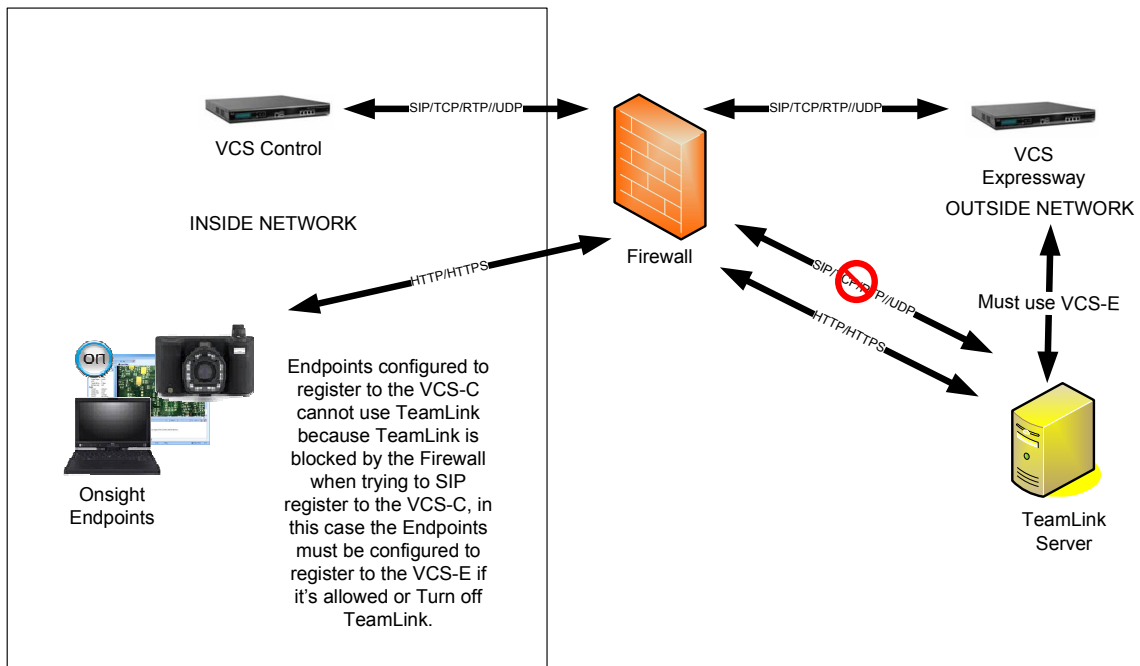
Example: An existing customer already has firewall rules to allow SIP/UDP to a certain SIP Server. If there are no similar rules on the firewall defined for the Onsite TeamLink server, the firewall detection algorithms on the OD/OE will report that SIP is not available and use HTTPS or HTTP tunneling by default. Librestream recommends that existing and new customers should apply firewall rules for SIP/UDP for both the Onsite TeamLink server and the existing SIP Server; *otherwise they should disable Onsite TeamLink when inside the firewall.*

### Cisco VCS Expressway Pairs

Onsite TeamLink won't detect VCS Expressway/Control pairs (outside the firewall and inside the firewall respectively). Depending on configuration, SIP calls may fail because of the Onsite endpoint's SIP Profile Settings. TeamLink cannot SIP register on behalf of the Onsite endpoint to a VCS control that is behind a Firewall. Even though Onsite's Firewall Detect status reports that HTTP/HTTPS is available, SIP registration will not be available through TeamLink and therefore SIP calls will not be possible.

**Simply stated TeamLink can only proxy SIP traffic if the SIP Server it is contacting has a Public interface.** VCS Controls are typically located behind a Firewall and/or in a DMZ and do not have a Public interface. Onsite endpoints outside the Firewall must register to the VCS Expressway that is located outside the Firewall.

Example: 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 Onsite Endpoints' 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. *Librestream recommends that you disable the OTLS configuration when behind the firewall and enable the OTLS configuration when on the outside of the firewall.*



## Proxy Settings

If Proxy Settings are configured on the Onsite endpoint, Onsite TeamLink traffic will be directed to your enterprise's Proxy Server. The Proxy Server must be configured to allow HTTP/S tunneling.

The use of the Proxy Server might impact video quality due to heavy loads on the Proxy Server adding additional latency to the media streams.

In this case the traffic flow would be Onsite Expert > Enterprise Proxy Server > Enterprise Firewall > OHTS > SIP Server.

## **Web Proxy Authentication**

Some Web Proxy Servers may require client authentication before allowing access to proxy services. Currently TeamLink does not support authentication with Web Proxy Servers.

To work around this issue, if possible the Web Server Proxy needs to be configured to allow TeamLink traffic without requiring authentication from the Onsite Endpoint. Alternatively, the native SIP/Media ports can be used by disabling TeamLink, this however requires the Firewall to allow traffic on these ports to the SIP Server. See the Network Requirements application note at [www.librestream.com/Support](http://www.librestream.com/Support).