# Lifesize Communicator Traversal Server Administration Guide

Version 1.0

June 2010

#### Copyrights and Trademarks

Portions of the LifeSize Software and/or documentation ("Software") are the copyrighted material of LifeSize Communications Corporation, © 1994-20010. The Software may also contain copyrighted materials licensed to LifeSize by (i) Paradial AS © 2008 – 2009; (ii) Vanguard Software Solutions Inc. © 1995-2009; (iii) Nalperion Inc., © 2008 – 2009; and (iv) Intel Corporation © 2007 – 2009. Use of the Software is subject to the terms of the applicable End User License Agreement ("EULA") included with the Software. All rights reserved. LifeSize, the LifeSize logos, LifeSize Systems, LifeSizeVOS, LifeSize Communicator, LifeSize Communicator Communicator, LifeSize C2 Unified, LifeSize Communicator Desktop, LifeSize Communicator Integrator, LifeSize Communicator Conference, LifeSize Communicator Traversal Server, LifeSize Communicator Connect, LifeSize Communicator Command, LifeSize Communicator Media Engine, vBrief, Shareboard, and World on the Desktop are trademarks or registered trademarks of LifeSize Communications Corporation. All other names used are the trademarks of their respective owners.

LifeSize's products are manufactured under the certain US and International patents a complete list of which can be view at: <http://www.LifeSize.com/company/default.aspx?id=74>. Other pending published patent applications maybe relevant. Portions of the LifeSize Software is manufactured under the AVC Patent Portfolio license. Additional information may be obtained from MPEG LA, L.L.C. See <a href="http://www.mpegla.com">http://www.mpegla.com</a>.

In addition, portions of the Software may contain copyrighted material ("Freeware") of the following copyright holders and their contributors ("Copyright Holders"): the RSA Data Security, Inc. MD5 Message-Digest Algorithm; Apache Software Foundation (<http://www.apache.org>) - © 1999-2000 The Apache Software Foundation; Computing Services at Carnegie Mellon University (<http://www.cmu.edu/computing/>) - © 2001 Carnegie Mellon University; OpenLDAP Foundation - © 1998-2003 The OpenLDAP Foundation; © 1996, 1998-2000 The Regents of the University of California © 2001-2003, Networks Associates Technology, Inc.; © 2001-2003, Cambridge Broadband Ltd.; © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A.; © 2003-2006, Sparta, Inc.; © 2004, Cisco, Inc and Information Network Center of Beijing University of Posts and Telecommunications; © Fabasoft R&D Software GmbH & Co KG, 2003 oss@fabasoft.com, Author: Bernhard Penz; ©2006, Yahoo! Inc.; © 1998 by the Massachusetts Institute of Technology; © 1996 - 2008, Daniel Stenberg, <daniel@haxx.se>; © 1998, 1999, 2000 Thai Open Source Software Center Ltd and Clark Cooper; © 2001, 2002, 2003, 2004, 2005, 2006 Expat maintainers; Boost Software License - Version 1.0 - August 17th, 2003 (www.boost.org); 1998-2008 The OpenSSL Project; ©1998, 1999, 2000 Thai Open Source Software Center Ltd and Clark Cooper; © 2001, 2002, 2003, 2004, 2005, 2003, 2004, 2005, 2006 Expat maintainers; ©1998-2008 The OpenSSL Project; © 2002-2003, Jean-Marc Valin/Xiph.Org Foundation; © Microsoft Corporation.

Permission is hereby granted by the Copyright Holders, free of charge, to any person obtaining a copy of Software to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to strict adherence to the following conditions:

- (i) The above copyright notice, listing each Copyright Holder, and this permission notice along with the disclaimer notice in (iii) below shall be included in all copies or substantial portions of the Freeware.
- (ii) The Freeware is provided by the Copyright Holders "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED, INCLUDING ANY WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR PERFORMANCE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

(iii) Disclaimer Notice - Redistribution and use of this software in source and binary forms, with or without modification, is permitted provided that the following conditions are met:

\* Redistributions must retain the above copyright notice, the below list of conditions and disclaimers in all copies.

\* The name of the Copyright Holders may not be used to endorse or promote products derived from this software without specific prior written permission of the Copyright Holders.

#### **Version Information**

# **Table of Contents**

Prerace
Terminology
About This Edition
Audience
What's In This Guide7
Documentation Conventions
Technical Support Information
The LifeSize Communicator Traversal Server
Hardware and Software requirements
Java Runtime Environment (JRE)
Network Requirements
DNS Configuration
Additional Requirements
Installation Process
Running the installation wizard
Check LifeSize Communicator Traversal Server services
Verify Connection to Signaling Server
Uninstalling
DNS entries
Firewall Rules
Firewall Rules: LifeSize Communicator Traversal Server (DMZ) to the Internet
Firewall Rules: LifeSize Communicator Traversal Server (DMZ) to the Corporate LAN 17
The Operation & Maintenance Web interface
Server Status (Home)
List Tunnelled Clients
Server Configuration
Database Configuration
Media Engine Configuration
STUN Server
TURN Server
SIP Configuration
SIP Registrar Settings
Registered SIP Users
SIP/H.323 Routing
Cluster Configuration
Event Reporting
SNMP Traps
Call Status
Conferences
H.323 Configuration
Logging
O&M Certificates

Installing O&M Certificates	30
Call End Reasons	
Third-party Software Licensing	
SSL Certificates	
Introduction	
1. Prepare information	
2. Create key pairs and certificate signing requests	
3. Order certificates from a Certificate Authority (CA)	
4. Install the signed certificates in LifeSize Communicator Traversal Server	
5. Verify installation	
6. Backup	
Troubleshooting	39
Appendix A: Configuring multiple IP addresses on a single NIC	41
Index	

# Preface

This guide describes how to install and administer Version 1.0 of the LifeSize Communicator Traversal Server, which extends your LifeSize user base by allowing LifeSize Communicator Endpoint clients to connect and call across firewall boundaries.

# Terminology

Terms used to distinguish products and features are described below:

Communicator Endpoint	The LifeSize Communicator client application that runs on each end user's machine. This could be Communicator or Communicator Unified-Microsoft OCS Edition.
Communicator Traversal Server	A service that acts as a central hub, enabling firewall traversal. The Communicator Traversal Server is comprised of the Media Server and the Signaling Server.
Media Server	Part of the LifeSize Communicator Traversal Server, the Media Server handles the transport of voice and video data.
RealTunnel Server (RTS)	The LifeSize Communicator Traversal Server bundles a third- party product called Paradial RealTunnel Server, or RTS. Any reference to the "RealTunnel Server" or "RTS" in scripts, file names, and user interfaces can be taken to mean the LifeSize Communicator Traversal Server.
Signaling Server	Part of the LifeSize Communicator Traversal Server, the Signaling Server process handles the transport of signaling data, including registrations and call setup. Sometimes referred to as the Proxy Server.

# **About This Edition**

This document describes the installation and administration requirements for Version 1.0 of the LifeSize Communicator Traversal Server.

Basic installation, initial configuration, and ongoing routine administration of standard LifeSize Systems are described in the following document:

• LifeSize Communicator Administration Guide

It is recommended that you read the *LifeSize Communicator Administration Guide* before reading the present document.

## Audience

The procedures in this guide should be performed by system installers with experience in installing and configuring LifeSize systems and with knowledge of networking and firewalls.

## What's In This Guide

Chapter 1 introduces the LifeSize Communicator Traversal Server.

Chapter 2 describes procedures for installing the LifeSize Communicator Traversal Server. Chapter 3 describes procedures for administering the LifeSize Communicator Traversal Server using the web-based administration tool.

Chapter 4 describes the procedure for installing SSL certificates on the LifeSize Communicator Traversal Server.

## **Documentation Conventions**

LifeSize documents use the following specific conventions and contrasting typefaces and sizes to clarify the subject matter:

monospace	Computer terms such as file and directory names, system prompts, output displays, folder names, and entries in text files.
monospace bold	Command line text or dialog text field entries that the user types.
italics	Variable names or values that you must supply when entering commands.
Sans Serif Type	References to graphic user interface features: menu items and options; dialog tab names, text entries, options, and buttons; toolbar icon names.

## **Technical Support Information**

If for some reason you encounter a problem with your LifeSize system, refer to the LifeSize Support Agreement included in the material you received when your LifeSize system was delivered.

Your support agreement may specify for you to call your system administrator, LifeSize- trained technical contacts in your organization, an authorized LifeSize reseller, an authorized LifeSize service center, or LifeSize. If in doubt, call LifeSize technical support at one of the numbers below:

- In the U.S.A. and Canada, call X.XXX.XXX.XXXX
- In all other international areas, call + X.XXX.XXX.XXXX
- Send e-mail via the Internet to helpdesk@LifeSize.com

# **Chapter 1: Introduction**

This chapter introduces the LifeSize Communicator Traversal Server, including its uses and features, and describes typical deployment scenarios.

# The LifeSize Communicator Traversal Server

The LifeSize Communicator Traversal Server provides a high-quality firewall traversal solution, extending your LifeSize user base by allowing LifeSize Communicator Endpoints to connect and call across firewall boundaries.

The LifeSize Communicator Traversal Server is scalable, easy to deploy, and requires minimal or no firewall changes, depending on the configuration used. Up to 500 simultaneous video calls at call rates up to 1Mbps are supported per host server, and multiple LifeSize Communicator Traversal Servers are supported for additional scalability, performance, and redundancy.

For end-users, the LifeSize Communicator Traversal Server enables one-click calling and conferencing with remote users, customers and partners. No VPN connection is required for LifeSize Communicator Endpoints. Remote users place calls as they would normally; users need no additional training to place calls that use firewall traversal.

From the administrator or IT manager's perspective, benefits include leveraging existing LifeSize infrastructure that may already be deployed in the enterprise. And, because a VPN tunnel is not required when the LifeSize Communicator Tunnel is deployed, an enterprise can allow customers and partners to make LifeSize calls into the enterprise without granting them full LAN access. The LifeSize Communicator Traversal Server transparently determines the best way to connect videoconference calls, regardless of the type of firewall, network configuration, multivendor hardware, or varying security policies.

The LifeSize Communicator Traversal Server firewall and NAT traversal solution implements current industry standards for best performance, including the following:

- STUN/STUN RELAY (TURN)/ICE for firewall traversal of SIP-based communications
- Uses Direct UDP paths where possible and reverts to tunneled operation when necessary
- HTTPS tunneled signaling and media are supported

LifeSize Communicator Traversal Server enables various call scenarios, including:

- A remote LifeSize Communicator Endpoint calling an internal LifeSize Communicator Endpoint
- A remote LifeSize Communicator Endpoint calling another remote LifeSize Communicator Endpoint
- Multiparty calls that include internal LifeSize Communicator Endpoints and external LifeSize Communicator Endpoints.

The LifeSize Communicator Tunnel selects the most efficient communication method based on how participants in a call or a conference are connected; direct connection for users on the same network, and STUN, TURN, or relaying through UDP, TCP and HTTPS for other network scenarios. LifeSize Communicator Traversal Server can also be configured to meet specific customer security requirements, such as always tunneling over HTTPS in order to achieve desired security levels.

A typical deployment is shown in the diagram below:



This diagram shows a mobile or home user's LifeSize Communicator Endpoint behind a firewall, perhaps provided by a home router, and another LifeSize Communicator Endpoint behind a firewall at a partner or customer location. Both are able to connect to LifeSize Communicator Endpoints within the enterprise LAN through the LifeSize Communicator Traversal Server that is deployed in the enterprise's DMZ. Remote LifeSize Communicator Endpoints can also participate in multi-party conference calls by connecting through the LifeSize Communicator Traversal Server to the LifeSize Communicator Multipoint Server (MCU).

The LifeSize Communicator Traversal Server is typically deployed in the enterprise's DMZ, with two IP addresses that are routable from the public Internet and from the corporate LAN, without Network Address Translation (NAT). This aspect of the deployment is shown in the diagram below:



**Note:** In the case of traffic between the LifeSize Communicator Traversal Server and the corporate LAN (Local Area Network), there must be no network address translation in either direction, that is, for connections from the LifeSize Communicator Traversal Server to the LAN and for connections from the LAN to the LifeSize Communicator Traversal Server. It is common for DMZ routers to NAT all traffic coming from the corporate LAN. Special configuration of the router's "rules list" may be required so that DMZ traffic is not NATted, while all other traffic going to the Internet is NATted.

Also note that, not only can there be no NAT between the LifeSize Communicator Traversal Server and the LifeSize infrastructure, as described above, but there can be no more than one NAT between a remote endpoint and the LifeSize Communicator Traversal Server. Since home users may already have NAT on their home firewall devices, there cannot be an additional NAT in the DMZ to the LifeSize Communicator Traversal Server. The diagram above shows a deployment where the LifeSize Communicator Traversal Server is accessible from the Internet, so that home users (without using VPN) can make LifeSize calls through firewalls into the enterprise.

The LifeSize Communicator Traversal Server can also be used when a firewall separates two corporate divisions. The basic principal is the same, but the left side of the diagram would be a subsidiary corporate LAN rather than the public Internet, while the right side of the diagram would be the primary corporate LAN. The Communicator Traversal Server would reside on the same side of the firewall as the LifeSize Communicator Server.

# **Chapter 2: Installation and Configuration**

This chapter explains how to install and configure the LifeSize Communicator Traversal Server. The LifeSize Communicator Traversal Server system comprises two server processes:

- The Signaling Server handles the transport of signaling data: registrations, call setup, and Operation and Maintenance services.
- The Media Server handles the transport of actual voice and video data.

## Hardware and Software requirements

You can install LifeSize Communicator Traversal Server on a Windows server. The host computer must meet these requirements:

Resource	Requirements
Operating system	Windows Server 2003 or later
CPU	Dual processor 2.0 GHz or higher, 1.0 GHz FSB (Front Side Bus)
Memory	2.0 GB or higher, 500MHz RAM
Disk space	40GB available
Network interface	Single, 1 Gbps full-duplex Ethernet TCP/IP local network connection.
Privileges	Administrator "root" privileges are required for installation.

The Signaling Server and the Media Engine are normally installed on the same machine. The operating system must be configured to handle two public IP addresses on one network card (NIC). See Appendix A for more information. *Do not* use two different NICs on the same machine as a way of obtaining two IP addresses.

Please note carefully the above requirement: you must configure two public IP addresses on a single network interface card (NIC). The Communicator Traversal Server installation will fail if this requirement is not met.

If your requirements include keeping the service in operation in case of restarts—for instance, during software upgrades—then a high-availability setup is necessary. This requires at least two LifeSize Communicator Tunnel Signaling Servers and two Media Engines.

## Java Runtime Environment (JRE)

The Sun Java Runtime Environment (JRE), Version 1.5 or later, is required on the host machine where you run the LifeSize Communicator Traversal Server. Windows JRE 1.5 is automatically installed during installation of the LifeSize Communicator Traversal Server.

## **Network Requirements**

This section describes network requirements of the LifeSize Communicator Traversal Server, specifically IP addresses, ports, and DNS configuration.

**Note**: The IP address of the LifeSize Communicator Traversal Server should be reachable from both sides of the firewall, that is, from hosts on the public Internet and on the enterprise's intranet. Typically, the LifeSize Communicator Traversal Server will be deployed in the enterprise's DMZ.

## **DNS Configuration**

For a publicly available service, the LifeSize Communicator Signaling Servers and LifeSize Communicator Media Servers need to have public addresses that are registered in the global DNS service. For more information see DNS entries.

## **Additional Requirements**

The following are additional requirements for LifeSize Communicator Traversal Server installation:

- License file for each server component (received separately from LifeSize Support).
- SSL certificates—temporary demo certificates are included in the packages.

# **Installation Process**

Here is an overview of the steps involved with installing the LifeSize Communicator Traversal Server on a Windows-based host machine:

- Obtain the installer file, LifeSize-Communicator-Traversal-Server-Setup.msi.
- Obtain license keys for the LifeSize Communicator Traversal Server from LifeSize support. There is one license key file for the Signaling Server (proxyserver.lic) and another file for the Media Engine (me.lic). Copy the files to a location on the host machine before running the installation.
- Run the installation wizard to install the LifeSize Communicator Traversal Server.
- Verify the connection between the two components of the LifeSize Communicator Traversal Server, the Signaling Server and the Media Server.

After installing and verifying connectivity between the LifeSize Communicator Traversal Server components, see DNS entries and Firewall Rules 1516for further configuration information.

## Running the installation wizard

- 1. Log in to the host machine as Administrator.
- 2. Double-click the installer file, LifeSize-Communicator-Traversal-Server-Setup.msi, to start the installation wizard.
- 3. After accepting the license agreement, choose a destination folder for the LifeSize Communicator Traversal Server, or click Next to accept the default location.
- 4. On the IP Address Assignment screen, choose the network adapter to use for the Tunnel Server and configure two IP addresses, one for Signaling and one for Media.
  - The Network Adapter dropdown menu shows all available network adapters on the host server.
  - You must choose a unique IP address for each field.
- 5. Create a password. LifeSize Communicator Endpoints will use this password to access the LifeSize Communicator Traversal Server.
- 6. Specify the location where you stored the Signaling Server and Media Server license files obtained from LifeSize support.

A runtime license is required for both the Signaling component and the Media component of the Traversal Server. During installation, the license files are copied to a license directory in the LifeSize Communicator Traversal Server program directory. This protects the license files and allows LifeSize Support to easily update your licenses at a later date.

- 7. Click Install to begin installing LifeSize Communicator Traversal Server program files.
- 8. After program files are installed, click Install Certificate to start the Certificate Import wizard.

You administer the LifeSize Communicator Traversal Server using the web browser-based Operation and Maintenance interface. The interface is protected by a security certificate and is only accessible after you install the client certificate in your browser.

- 9. The File to Import screen of the wizard shows the location of the demo certificate supplied with the LifeSize Communicator Traversal Server. If you have your own security certificate, browse to that file and select it, then click Next.
- 10. On the password screen, enter demo as the private key password for the demo certificate. Leave other options deselected and click Next.
- 11. On the Install Certificate page, click Next.
- 12. Click Finish to complete the Certificate Import wizard.
- 13. Click Finish to complete the LifeSize Communicator Traversal Server installation.

The installer creates a shortcut to the web interface on the desktop and in the Start menu program list.

## **Check LifeSize Communicator Traversal Server services**

Installation creates two Windows services that run on the host machine: LifeSize Communicator Traversal Server - Signaling, and LifeSize Communicator Traversal Server - Media.

To verify that both services were successfully started after installation, do the following:

- 1. Choose Start > Programs > Administrative Tools > Services.
- 2. Locate the two LifeSize Communicator Traversal Server services and check that the status for both is **Started**.

The default startup value for both services is Automatic. Both services are set to restart as the recovery option in the event of a service failure.

## Verify Connection to Signaling Server

To confirm that installation was successful, verify that the Media Engine is connected to the Signaling Server and has the expected version number.

 Double-click the LifeSize Communicator Traversal Server Admin Tool shortcut on the host machine desktop, or choose Start > Programs > LifeSize > LifeSize Communicator Traversal Server Admin Tool.

The Admin Tool opens by default on the Real Tunnel Server Status page.

2. In the Server Status (lower) section of the page, check the Media Engine Version and Media Engines values.

## Uninstalling

- 1. Choose Start > Settings > Control Panel, then double-click Add or Remove Programs.
- 2. Locate LifeSize Communicator Traversal Server in the list of installed programs and click Remove.

**Note**: The Communicator Traversal Server uninstaller removes all installed files and registry entries except the license files. The program directory structure is not deleted.

## **DNS** entries

The domain name of the LifeSize Communicator Traversal Server must be resolvable by the LifeSize Communicator Endpoint (the LifeSize Communicator client application). For a publicly available service, signaling and media servers need to have public addresses that are registered in the global DNS service. For companies that do not manage their own domain names, please ask your Internet Service Provider (ISP) to do this.

The DNS entries chosen for the servers must match the name in the SSL certificate (see SSL Certificates on page 33Error! Bookmark not defined.).

Example:

pxs1.somecompany.com me1.somecompany.com

for the Signaling Server for the Media Engine

## **Firewall Rules**

The tables in this section provide details about firewall rules and port requirements for these connections:

- 1. Firewall Rules: LifeSize Communicator Traversal Server (DMZ) to the Internet
- 2. Firewall Rules: LifeSize Communicator Traversal Server (DMZ) to the Corporate LAN

## Firewall Rules: LifeSize Communicator Traversal Server (DMZ) to the Internet

Open firewall ports between the LifeSize Communicator Traversal Server and the public Internet are shown in the next two tables. The first table shows minimum requirements, where all traffic is tunneled to the LifeSize Communicator Traversal Server (TCP mode). The second table shows requirements for optimized quality, where traffic is relayed through the LifeSize Communicator Traversal Server (UDP mode).

# Minimum requirements: all traffic is tunneled to Communicator Traversal Server (TCP mode):

Rule	Source	Source Port	Destination	Destination	Protocol	Usage Description
				Port		
1	Internet	Dynamic Port	LifeSize	443	TCP	Remote LifeSize
	(Remote	1024-65534	Communicator			Communicator Endpoint
	LifeSize		Traversal Server			connects to the LifeSize
	Desktops)					Communicator Traversal
						Server through HTTPS. Port
						443 used for signaling and
						media traffic.

#### Quality optimization: traffic is relayed through LifeSize Communicator Traversal Server (UDPmode):

Rule	Source	Source Port	Destination	Destination Port	Protocol	Usage Description
1	Internet (Remote	Dynamic Port 1024–65534	LifeSize Communicator	45100-45900	UDP	Remote LifeSize Communicator Endpoint
	LifeSize Desktops)		Traversal Server			media uses UDP to connect to LifeSize Communicator Traversal Server which relays media to other call participants (inc. MCU if applicable)

# Firewall Rules: LifeSize Communicator Traversal Server (DMZ) to the Corporate LAN

Open firewall ports between the LifeSize Communicator Traversal Server and the corporate LAN are:

Rule	Source	Source Port	Destination	Destination Port	Protocol	Usage Description
1	LifeSize Communicator Endpoints [LAN]	5060-5069	LifeSize Communicator Traversal Server	5060	UDP	SIP signaling traffic for call control.
2	LifeSize Communicator Traversal Server	45100-45900	LifeSize Communicator Endpoints [LAN]	4200-4299	UDP	Audio and video traffic from the LifeSize Communicator Traversal Server to the LifeSize Communicator Endpoint.
3	LifeSize Communicator Endpoints [LAN]	4200-4299	LifeSize Communicator Traversal Server	45100-45900	UDP	Audio and video traffic from the LifeSize Communicator Endpoint to the LifeSize Communicator Traversal Server.
4	LifeSize Communicator Traversal Server	45100-45900	LifeSize Communicator Conference MCU	7460-7600	UDP	Audio and video traffic from the LifeSize Communicator Traversal Server to the MCU.
5	LifeSize Communicator Conference MCU	7460–7600	LifeSize Communicator Traversal Server	45100-45900	UDP	Audio and video traffic from the MCU to the LifeSize Communicator Traversal Server.
6	LifeSize Communicator Traversal Server	45100-45900	H.323 Endpoint	Varies by Endpoint	UDP	Audio and video traffic from the LifeSize Communicator Traversal Server to the H.323 Endpoint

# Chapter 3: LifeSize Communicator Traversal Server Administration

This section describes the tools and procedures for performing ongoing administration of the LifeSize Communicator Traversal Server once it is installed and configured, as well as settings you may need to alter immediately after installation.

# The Operation & Maintenance Web interface

The Communicator Traversal Server is managed and monitored using a web-based administration tool called the **Operation & Maintenance Web interface**, also referred to in this document as the **O&M interface**. To access the O&M interface, point a Web browser to https://localhost:8181 on the machine where LifeSize Communicator Traversal Server (or, more specifically, the Signaling Server) is running.

If you are accessing the O&M interface remotely, use the hostname of the machine in place of localhost in the URL, e.g., <u>https://pxsi.somecompany.com:8181</u>.

**Note:** To use the O&M interface, you must install the **oam.pfx** certificate in your Web browser. Demo certificates are provided with the installation and instructions for installing certificates is provided in the installation section.

The O&M interface is used to perform most administrative operations for the LifeSize Communicator Traversal Server. If you find that you have altered data in the Web panel incorrectly but have not clicked the **Set** button for that data item, remember that a refresh on the Web page will get back your previous settings.

**Note:** For each setting that you modify in the O&M interface, you must click the **Set** button to apply your changes. There are no master **Save** buttons that will apply all of the changes made on a page with a single click. Navigating away from the page without first clicking **Set** will discard any changes that have note been saved using the **Set** button.

The URL, https://localhost:8181, opens the Server Server Status page of the O&M interface. You can also access this page by clicking **Home** in the left hand navigation pane.

Note: Each page of the O&M interface uses the same navigation links for selecting a page to view.

## Server Status (Home)

The **Server Status** page gives an overview of the status of the Signaling Server, and includes two main sections, **Event Status** and **Server Status**. These are described below.

## **Event Status**

This section shows an overview of important events reported by the server. The administrator should pay special attention to events marked "Severe" and "Warning" as these may indicate a serious problem with the server.

## Server Status

**Proxy Server Version** is the version of the Signaling Server.

Media Engine Version is the version of the active Media Engine.

Public Address is the public address of the Signaling Server.

**Master Server Address** is the public address of the master Signaling Server. This address is not visible if no master server address is configured

Current Time is the time of the machine where the Signaling Server is running.

**Running Time** indicates how long the Signaling Server has been running since last restart, in hours:minutes:seconds.

Startup Time indicates when the Signaling Server was started.

**License Expire Date** indicates when the license for the Signaling Server will expire. It is important to pay attention to this parameter since the Signaling Server will terminate when the license is expired. Please notify LifeSize Support several weeks in advance before the license expires to extend the license.

Media Engines indicates if the defined Media Engines are connected.

Connected Clients indicates connected (tunnelled) client status.

Local Current Calls indicates current calls in the Signaling Server.

**Global Current Calls** indicates concurrent calls in the total system. This parameter is displayed only when the Signaling Server is part of a cluster configuration.

Public SSL Certificate expiry date indicates when the SSL certificate expires.

## **List Tunnelled Clients**

All the connected Communicator Traversal Server clients are shown here with the information for each as described below.

User ID is the SIP/H323 user ID the user is logged into as the SIP client.

**Country** is the country the LifeSize firewalled client is connected from.

**Region** is the region in the world the LifeSize firewalled client is connected from.

Version is the software version ID of the firewall traversal library.

RealTunnel ID is the internal LifeSize Communicator Traversal Server user ID.

Client ID is the name and IP address of the computer the LifeSize firewalled client is installed on.

Port is the server port the LifeSize firewalled client is connected on.

Public Address is the public address of the LifeSize firewalled client.

**Proxy Address** is the address of the HTTP(-S) proxy if used.

**Proxy Auth** is the authentication scheme used in the HTTP-proxy.

**NAT** is the NAT-type of the LAN where the LifeSize firewalled client is running.

**Type** is the type of the SIP-client.

Duration tells how long the LifeSize firewalled client has been connected.

## **Server Configuration**

Set Basic Signaling Server parameters on this screen.

Restart Signaling Server will restart the Signaling Server.

Restart all media servers will restart all Media Engines connected to this Signaling Server.

Note: For the fields below, be sure to click the **Set** button to save the new settings for any field you have modified.

**Signaling Server public address:** This address will be advertised to other hosts. *Do not change this value*.

**Signaling Server ports** Enable or disable ports 443 (standard HTTPS), 444, and 80. *Do not change this value*.

## **Database Configuration**

This panel configures how end-user transactions are authenticated. Three kinds of transactions are authenticated: Tunnel connections, SIP transactions by the registrar (see SIP Configuration on page 2323) and Stun Relay allocations (see TURN Server on page 2323). All three use the same authentication method.

Note: Currently, LifeSize only supports Fixed Authentication.

Database Mode: Requires restart of the server	<ul> <li>No database</li> <li>Connect directly to database</li> <li>Cuse master signalling server as database</li> </ul>	Set
Authentication Settings		
Changing these settings requires restart of the server		
Authentication mode:		Set
Fixed Reseword Configuration		
Password for Fixed Authentication:	avistar	Set
RADIUS Configuration		
Local authentication password:	C Digest (RFC 4590) Sterman Draft	Set
Shared Secret:	null	Set
Radius Server Remove/Add		
Custom authentication plugin		
Main class name of the plugin: Requires restart of the server		Set

**Database Mode:** The **Database Mode** should be set to No database so that the LifeSize Communicator Traversal Server will authenticate all users with the same password.

Authentication Mode: Should be set to Fixed so that the LifeSize Communicator Traversal Server will authenticate all users with the same password.

**Password for Fixed Authentication:** Enter the password that will be used by all LifeSize Communicator Endpoints for firewall traversal. LifeSize Communicator Endpoints will enter this password in the Firewall Traversal settings for their particular LifeSize Communicator Endpoint.

Optionally, modify the password on the Database Configuration page and click the **Set** button. If you change the **Password for Fixed Authentication**, you must restart the Signaling Server (in the Tunnel configuration panel) to make your change take effect.

Local authentication password: Not applicable. Database authentication mode is not supported.

Shared Secret: Not applicable. RADIUS authentication mode is not supported.

Main class name of the plugin: Not applicable. Plugin authentication mode is not supported.

## **Media Engine Configuration**

Use this screen to configure options for types of media that can pass through the Media Engine.

## **Multi TCP Configuration**

Multi TCP is a way to optimize media traffic over TCP by using more than one TCP connection per media stream. It generally improves the media quality in congested networks, but can also cause the RTP packets to be received out of order, so it works best with clients with good sequence control and jitter buffers for received media packets.

Enable multi-TCP on audio: Enables or disables multi-TCP on audio.

**Enable multi-TCP on video:** Enables or disables multi-TCP on video. *Leave the two multi-TCP settings above with their default values, disabled.* 

#### **Media Configuration**

**Enable application sharing in PXS:** Enables or disables application sharing. **Allow direct media between clients:** Enables or disables direct media between LifeSize Communicator Traversal Server clients.

## Media Relay

The LifeSize Communicator Traversal Server Signaling Server can relay RTP/UDP media for SIP clients without LifeSize Communicator Traversal Server clients. For users behind relaxed NAT devices (allowing UDP traffic out) this is an attractive option, as the LifeSize Communicator Traversal Server client is not needed. You can control the level of media relay:

All: All calls routed through this Signaling Server is relayed, regardless of whether they need it or not. This leads to excessive relaying, so it only should be set for testing purposes.

Non-ICE: All calls that are routed through this server not using ICE will be relayed.

**All NAT:** Media is relayed for all users in need, when either the calling or called client is behind NAT (and do not handle traversal on their own).

**Local users:** Same as All NAT, except we only relay for the authenticated users local to this registrar.

None: Set to disable UDP relay completely.

These settings will not affect the behavior for calls to or from a tunneling client.

Allow direct media for UDP registrations behind the same public address: Checking this box will lead to more efficient media between clients on the same local network, but can cause media to fail on complex local networks with internal firewalls or NAT devices. It makes sense to enable this on an enterprise server if you know there is only one NAT device on the local network. ISP-like installations serving many unknown NATs should keep this disabled.

## **Media Engines**

Added Media Engines should always display "yes" in the Connected column, that is, they should be connected. If not, check that the address, port and secret-token values correspond to the values in the me.cfg file. If the primary Media Engine is out-of-service, the Signaling Server will automatically try to use the secondary Media Engine (i.e. secondary Media Engines servers as backup).

Add a Media Engine by providing appropriate data in the editable fields of the bottom row of the **Media Engines** table. Complete the following fields and click the **Add** button:

**Connect Address:** The connect-address, i.e. the address the Signaling Server shall use when connecting to the Media Engine.

**Port:** The port the Signaling Server shall use when connecting to the Media Engine. Please use default port.

**Public Address:** The public-address used as media-address for clients. This address is normally the same as the connect-address, but if the Media Engine is protected by a NAT, the public-address used in the NAT shall be inserted here. This address must be resolvable by DNS.

**Internal address:** In a normal scenario this field is not in use. The internal-address is the mediaaddress for components on the internal LANs where the Media Engine is installed. Note that if this parameter is specified all non-tunneled clients will use this address for media, i.e. all clients on public internet must be tunneled, so use this parameter with care.

**Password:** The password used for authentication of the Signaling Server at the Media Engine. The corresponding secret token is configured in the me.cfg file located on the Media Engine server.

Click the **Add** button when adding a Media Engine. Added Media Engines are placed in the Media Engine table. The first Media Engine listed in the table will be the primary Media Engine.

## **STUN Server**

The LifeSize Communicator Traversal Server servers include both a STUN (RFC 3489) server and a STUN Relay (previously known as TURN) server, both available to the LifeSize Communicator

Traversal Server clients and external clients. Any firewalls in front of the server should open these ports as well. All of the ports on this page require a restart before a new value takes effect.

STUN Server Configuration		
STUN Server ports		
Port one:	3478	iet
Port two:	34501	iet
Remote STUN Server ports Media Engine STUN Port:	34501	iet
TURN Server Changing these settings requires restart of the server		
Enable TURN Server:	۲ ۲	iet
TURN port:	3560	iet
TURN port on MediaEngine:	3560 5	iet
Enable redirect based on TURN client location:	2	et

**STUN Server ports:** Displays the UDP ports used for the STUN servers. A STUN server requires two ports on the primary server, plus a third port on another IP address for checking the network connection. The Signaling Server is always the primary STUN server, while the primary Media Engine is used as the secondary STUN server. The recommended port is 3478. **Remote STUN Server ports:** Sets the STUN port on the Media Engine, and should correspond to what's set in its configuration file; or 34501 if nothing is set.

## **TURN Server**

These settings control the behavior of the TURN server. TURN requests require authentication, with the same user ID and password as used with LifeSize firewalled clients, such as the LifeSize Communicator Endpoint. The Signaling Server authenticates these, and lets the Media Engine do the actual relaying of media, so the clients need to support redirection of TURN requests.

Enable TURN Server: If this is unchecked, the TURN server is disabled.

TURN Port: The server port (UDP/TCP) for TURN used on the Signaling Server.

TURN Port on Media Engine: The server port for TURN used on the Media Engine.

**Enable redirect based on TURN client location:** Like the tunneling connections, the TURN clients can be directed to the TURN server closest to them, to reduce the latency and give better media quality in a call. If checked, the TURN requests are matched against the regions defined in 2.11, and the clients may be redirected to the matching servers if the current server is not closest.

## **SIP Configuration**

Use this screen to configure various SIP parameters:

**Use the public address in SIP signaling:** This checkbox selects which IP address the server will use as its own in SIP signaling. If deployed behind a NAT, the server is configured with its public address. Check this box unless the other SIP servers are on the same private network. If the server is not deployed through a NAT or the public address isn't set, the checkbox will be disabled.

**SIP ports:** The standard SIP port is 5060. It is recommended that you keep this value. If modified, you will need to restart the Signaling Server for this parameter to take effect.

**Max UDP packet size:** The Signaling Server can receive and send SIP over TCP. If UDP messages get bigger than the maximum transmission unit (MTU), they will be fragmented, and there is a risk they will not be received correctly by all hosts. To avoid UDP fragmentation, the server sends outbound requests over TCP if they exceed a certain size. This size should be 200 bytes less than the known MTU; or 1300 bytes if the MTU is unknown. Note that if a particular transport is enforced in the routing table, this setting will not take effect.

**Incoming Redirect Messages:** This parameter controls how the LifeSize Communicator Traversal Server Signaling Server acts on incoming redirect (3xx) messages; for example a redirect server can send a "302 Moved Temporarily" in response to an INVITE, with the address of the client. The default behavior is to recurse and send a new INVITE to the new location. If disabled (unchecked), the server will send this redirect message upstream to the calling client, which can again perform the redirection.

**Home Routing:** If the checkbox is checked, the LifeSize Communicator Traversal Server Signaling Server will route requests from non-local users to their home proxy rather than to the destination. This is used to preserve home-based services and authentication, for example. It has no effect for users who are local on this server (the registrar is enabled).

**Domain Registration Policy:** A LifeSize Communicator Traversal Server server provides resources (processor power, bandwidth) to the users, and you may want to restrict the usage of this to certain user groups. In this field you can set up a set of SIP domains the users are allowed to log on to through this server; registrations towards all other domains will be rejected. Local users (if registrar is enabled) will always be allowed regardless of this setting. The local users will still be able to call and receive calls from other domains. If this field is empty, registrations will be allowed towards all domains.

## **SIP Registrar Settings**

Use this screen to configure locally managed domains, security and trusted remote domains.

#### **SIP** domains

These tables contain domains or prefixes that are considered "local" for SIP handling. The server will look up users with these domain names (or phone numbers starting with these digits) in the database, and not route on domain name. For these to be callable from other systems, one should add these domains to DNS for this host.

#### **Security level**

Full: All requests are authenticated.

**Medium:** All requests are authenticated, except from the tunneled clients connected to this proxy server, where only REGISTER is authenticated.

**Registration:** Allow requests from the REGISTERED (and authenticated) address, otherwise LifeSize Communicator Traversal Server authenticates.

None: No requests are authenticated.

## **Trusted hosts**

Adds a set of hostnames or IP Addresses (with optional SIP port) for the trusted hosts. These will not be challenged for password authentication, and require a database user entry.

**Proxy Mode:** The proxy mode will affect the routing between SIP users on external hosts or on other SIP servers. We will always forward from or to users on this Signaling Server. External requests can either be handled by redirect or forward, depending on the radio button chosen here.

## **Registered SIP Users**

This screen presents a table of all SIP users registered in the database, with information about the contact address, registration and expiry times. The columns in the table are defined as follows:

**SIP URI:** The SIP user ID registered.

**Alias:** An optional second identifier per user, typically used for incoming calls from the PSTN. **Expires:** The lifetime of this expiry. If the client does not register again before this time, it will be unregistered.

Contact: The IP address and port the client is registered on, as reported in the contact header.

**Unregister:** The operator can clear this registration manually by pressing this button. The client will still believe it is registered, but won't receive any calls. Note that this does not block the user from registering again.

If UDP Relay is enabled in the SIP Configuration page's Media Relay, the clients connected through a firewall/NAT device will be shown in a table named "Direct Registrations from clients behind NAT."

## **Proxy Registrations**

This table shows the current proxy registrations, registrations from clients connecting through SIP from behind a NAT. They may or may not be registered on the local registrar, if there is one within the same server.

SIP URI: The SIP ID (address-of-record) of the user registered.

Public Address: The public address used to contact this user.

Private Address: The private address (on the LAN) the client is registered from.

Protocol: The transport protocol used when registering, UDP or TCP.

**Relay:** Whether this client needs relay assistance for calls.

**Registered:** The time when the user first registered.

Last seen: The time of the last registration.

Rate: The re-registration frequency, in seconds.

Expires: The time when this registration will expire, if not refreshed.

## SIP/H.323 Routing

Use this screen to configure routing for SIP/H.323. This screen is not applicable for the current release of the LifeSize Communicator Traversal Server, since SIP/H.323 routing is not supported in this version.

## **Cluster Configuration**

Configures how several Signaling Servers interact in a LifeSize Communicator Traversal Server cluster.

**Read world table file:** A feature used to override the standard IP address-to-country mapping. This feature is rarely used.

**Enable redirect when clients connect:** Used to redirect tunneled clients to other Signaling Servers. Should be enabled in all normal production systems. If disabled, tunneled clients will not be redirected to other Signaling Servers.

**Master Proxy server address:** The address of the master Signaling Server. This address shall be set correctly in all systems that use more than one Signaling Server. This address is normally the address of the Signaling Server where the SIP registrar is enabled and where the database is accessed. If no such features are enabled, the administrator shall select one Signaling Server as a master.

## Servers

Enter the name and host address of each Signaling Server in the cluster in this table. It is up to the system administrator to choose good logical names for the servers. The addresses to the servers are usually the host addresses for the Signaling Servers on the LAN. Entries are added in the last row by clicking the **Add** button.

If your deployment includes more than one server, this list needs to be configured on all servers in order to enable redirect.

## Regions

Regions define which Signaling Server shall be used for different regions in the world. This feature should not be used unless your Communicator Traversal Server deployment includes several clusters in a widespread geographical area.

## **Event Reporting**

Configures and displays event status in the Signaling Server.

**Mail Configuration:** Configures where a mail shall be sent when events are registered in the Signaling Server.

Outgoing SMTP server: The outgoing SMTP server address.

Mail username: The username to use to authenticate at the SMTP server.

Mail password: The password to use to authenticate at the SMTP server.

**Mail Recipients:** Mail addresses of the recipients separated by a comma (user1@acme.com, user2@acme.com).

Trap Receiver: Configures where traps are sent when events are registered in the Signaling Server.

Trap Receiver address: The address of the trap receiver.

Event Table: Shows the history of events on this server.

Event table size: The maximum number of events stored in the table.

The event table displays the following columns:

**#:** The event number.

Event Name: The logic name of the event.

**Severity:** The severity of the event (corresponds to log level for each event; see [link to Logging topic]

Info: A textual explanation of the event.

Raised: The timestamp when the event was raised.

Cleared: The timestamp when the event was cleared.

**Customer ID:** The id of the customer.

Key: A unique id of the event.

Local Address: The address of the host of the event.

Action: Defines possible actions to handle the event.

Events displayed on white backgrounds are active, events displayed on grey background are cleared.

## **SNMP** Traps

Certain events can be forwarded as SNMP traps. To enable SNMP traps, specify the hostname and port of a trap receiver. For example, if you have installed HP-OpenView on 292.168.0.53, and it uses the default SNMP port 162, set the following trap receiver:

292.168.0.53:162

If the trap receiver field is empty, SNMP traps are disabled. If you change the trap receiver field, you must restart before the change takes effect.

Currently the following SNMP traps can be sent:

#### **Connection Lost:**

1: Lost connection to MediaEngine

#### Congestion:

- 1: Max Call Limit Reached
- 2: Max number of conferences exceeded
- 3: Max Connected Communicator Traversal Server Clients

#### LicenseExpired:

1: Problem with license file

#### **Restart:**

1: The Signaling Server was (re)started

#### ConfigurationError:

1: Bad SIP route configuration

2: Failed to load authentication plug-in

#### DatabaseProblem:

1: Failed to connect to database

2: Failed to read conferences in database

#### CertificateProblem:

- 1: Public SSL certificate is not yet valid
- 2: Public SSL certificate expires in one day
- 3: Public SSL certificate expires in 4 weeks
- 4: Public SSL certificate has expired

Please refer the LifeSize Communicator Traversal Server MIB file for details: realtunnel-MIB.my

## **Call Status**

Informative information about both current and present calls is displayed. Successful calls are displayed in white, and failed calls are red.

**Max concurrent calls:** The maximum number of concurrent calls permitted. This parameter can be set up to the value which is limited by the license configuration.

#### **Active Calls**

This table displays information on all active calls in three sections, with the following columns:

#### **Originating Side of Call**

#: call number.

User ID: The address of record created by the originating user.

RealTunnel ID: The LifeSize Communicator Traversal Server user ID of the originating user.

Public Address: The public IP address of the originating user. Country: The country of the originating user.

#### **Terminating Side of Call**

User ID: The address of record created by the terminating user.

**RealTunnel ID:** The LifeSize Communicator Traversal Server user id of the terminating user.

Public Address: The public IP address of the terminating user.

Country: The country of the terminating user.

#### **Common Info**

**Duration**: The duration of the call in seconds. **Call ID:** The unique call ID.

#### **Closed Calls**

In the Closed Calls table, the columns displaying call information correspond to those in the Active Calls table. In addition, the first column (# call number) can be clicked to view more detailed information on the selected call.

## Conferences

This screen is not applicable. LifeSize provides its own conferencing functionality.

## **H.323 Configuration**

This screen is not applicable. Firewall-traversed H.323 is not supported in this release of the LifeSize Communicator Traversal Server.

## Logging

A comprehensive logging tool is included for identifying problems and system bugs. Remember that a high log level increases CPU usage and lowers the disk lifetime.

**Level of logged messages:** It is possible to set the log level here. Remember to click the **Set** button after selecting a log level. Note that a high log level increases CPU usage. The default setting normally shouldn't be modified, except when reproducing a problem before sending logs to LifeSize Support.

Select the log groups to exclude: Choose All, None, or desired log groups (possible by toggling on or off desired log groups). Remember to click the Apply button when done. The default setting normally shouldn't be modified.

## **Current log files**

To inspect a log file, download either the original file or a zipped version (useful on slow connections) by clicking the appropriate link. The most recent file is the one with the lowest index.

## **O&M** Certificates

The O&M interface pages can be protected using SSL (HTTPS). This requires a set of SSL certificates. A server certificate is used on the web server and a client certificate is used in the web browser (required only when client authentication is enabled). A new installation of Communicator Traversal Server will contain a set of demo certificates. You should replace these demo certificates with customer-specific certificates for optimal security. Use the **O&M Certificates** page to create new certificates.

On a new installation, the O&M Certificates page appears as follows:

The first section of the page allows you to download the existing certificates.

- Root certificate
- Client certificate

These certificates are required to access the O&M web pages. Download and distribute these certificates to those that need access.

**Note:** On some systems it will not be possible to download the original root and client certificates. However, when new certificates are installed they will appear as expected in the Current O&M certificates section.

#### **Create new certificates**

This section allows you to replace the current O&M certificates with new certificates. You enter the following information to embed in the new client certificate:

- Country code (two letters)
- Name of organization
- Certificate Name
- Password to protect the client certificate

Click **Create** to generate certificates. The page changes to a new state, "Certificates created, but not activated." Before you can activate the new certificates on the server, you must install them in your web browser.

#### Installing O&M Certificates

1. Install the new root certificate in the web browser by following the browser-specific procedure for SSL certificate installation. (If installing the demo certificate, you can begin the procedure by double-clicking oam.pfx.)

Once the new root and client certificates are successfully installed in your web browser on the Signaling Server machine, you are ready to activate the new certificates on the server.

2. Click Activate, then OK to confirm the restart.

The Signaling Server is restarted and will now use the new certificates. The new certificates must be verified before they are committed. This verification step is necessary to ensure that you can access the O&M pages after activating the new certificates. If verification is not performed within 3 minutes the server reverts back to the old certificates.

3. To verify the certificate, open the O&M web pages in a new browser window. You must quit and open a new browser window since the browsers often cache certificate information.

This completes the certificate upgrade process.

It is important to download the root and client certificates and store them in a safe place. *Avoid the situation where the new client certificate is installed on a single computer*. If the computer experiences hard drive failure, the O&M interface will be inaccessible.

## **Call End Reasons**

The O&M interface call status page displays a list of calls with their end reasons. The list of all call end reasons is provided below.

Reason	Description
UNKNOWN	Unknown reason
NORMAL	Call terminated normally
USER_UNREG	The user unregistered during a call
USER_FORCED_UNREG	The user was forced unregistered (signed in from another location,
	or unregistered by operator)
PXC_CONN_LOST	The signaling connection to the client was lost
MESSAGE_IN_BAD_STATE	Got a message in bad state
RESERVE_MEDIA_FAILED	Failed reserving media. Most often seen if the Signaling Server isn't
	connected to the Media Engine.
JOIN_MEDIA_FAILED	Failed joining media. Most often seen if the Signaling Server isn't
	connected to the Media Engine.
IO_FAIL_SENDING_MSG	IO failure sending a message
NO_RESPONSE_TO_INVITE	Got no response to Invite
INVITE_REJECTED	Invite was rejected
ME_TUN_CONN_FAIL	Tunnel connection failed towards Media Engine
NO_RESPONSE_TO_OK	No ACK following a 200 ok
BAD_SDP	Trouble decoding the SDP in SIP message, or a 415 Unsupported
	Media Type received
FORCED_DOWN_UNREGD	Call forced down as user unregistered
TUNNEL_DOWN	Signaling connection lost during media transfer
CONN_FAILED_IN_PXS	Failed to connect two users in PXS (Signaling Server)
CALL_ENDED_BY_ME	The call was ended by Media Engine (most likely if it detected a lost
	TCP connection from the client)
PXS_LOST_CONN_TO_ME	The PXS (Signaling Server) lost connection to ME
CALL_REL_TIMEOUT	The call was released due to a timeout
BAD_SIP_MESSAGE	The recipient SIP user didn't like the request (typically received a
	4xx response not otherwise covered on INVITE)
SIP_AUTHENTICATION_FAILURE	A SIP server required authentication, but none or bad authentication data was sent
SIP_USER_NOT_FOUND	The (external) user wasn't found (on receipt of 404 Not Found on
	INVITE)
EXTERNAL_SERVER_UNAVAILABLE	The external server was temporary unavailable (received 500 Server
	Internal Error, 501 Not Implemented, or 503 Service Unavailable
	from external server)
USER_BUSY	The user is busy and can't accept more calls (486 Busy Here or 600
	Busy Everywhere received)
EXTERNAL_TIMEOUT	A request towards an external server timed out
USER_REJECTED	The user declined the call (received 603 Decline from called party)
HANGING_CALL	BW usage is null over a long time
CLIENT_CONNECTION_LOST	Signaling connection to client lost (from the server)
USER_TEMPORARILY_UNAVAILABLE	The user was temporary unavailable, probably not logged on
NOT_END_TO_END_MEDIA	All signaling was okay, but we didn't get media end-to-end both
	ways
INCOMPATIBLE_MEDIA	We couldn't find a single compatible codec in SDP
OAM_CLOSED	Call was forced down by operator
REFERRED_OUT	Call was referred out by another user. Only used for conference calls

CONFERENCE_OWNER_LEFT	The conference owner left an ad-hoc conference. Only used for
	conference calls
ME_LOST_CONN_TO_CLIENT	The media-engine lost connection to the client
FAILED_TO_SET_ME_FORMATS	Failed to set media-formats in ME. Only used for conference calls
ME_TUN_CONN_LOST	Connection to media-engine lost
FAILED_TO_CONN_USERS	Failed to connect users
MEDIA_FAILED_SIP_OK	Failed to create connection to media-engine (but the INVITE was
	accepted)
CALLER_CANCELLED	The caller cancelled the call before anyone answered (most probably
	the called party didn't answer)
MAX_CALL_CAP_REACHED	The max-call capacity in the PXS (Signaling Server) has been reached
SOCKET_FAILURE	The call failed due a local socket/network failure

## **Third-party Software Licensing**

The LifeSize Communicator Traversal Server makes use of parts of the following Tandberg patent applications necessary in order to implement the ITU standards H.460.18 and H.460.19:

- U.S. Patent Application No. 10/332.785
- U.S. Patent Application No. 10/432.468
- U.S. Patent Application No. 11/008.150

The list and copyright statements of licensed third-party software is included with the distributed software, in the file readme\_pxs.txt.

# **SSL Certificates**

This section explains how to add an SSL certificate to the LifeSize Communicator Traversal Server to insure that the server is reachable via HTTPS for clients behind firewalls.

## Introduction

Secure Sockets Layer (SSL) is an internet standard for authentication, encryption and integrity of TCP connections. Firewalls and web proxies typically require that web servers identify themselves using public certificates when setting up HTTPS connections with web browsers. Some firewalls and web proxies are more restricted and require that the server certificate is signed by a trusted Certificate Authority (CA).

Installing a trusted public certificate on the LifeSize Communicator Traversal Server ensures that the service will work for users on almost all types of networks.

To obtain a public certificate, follow these steps (each step is discussed in the sections that follow):

- 1. Prepare information:
  - Domain name for the LifeSize Communicator Traversal Server service
  - Organization name
  - Unit within organization
  - Locality/City
  - State/province
  - Country
  - Email contact
- 2. Create key pairs and certificate signing request
- 3. Order SSL certificate from a CA
- 4. Install signed certificate on LifeSize Communicator Traversal Server
- 5. Verify installation
- 6. Backup

## 1. Prepare information

The identity of the server and its owner must be present in the certificate. You must know the domain name for the server before you order the certificate. You can use two kinds of certificates with the LifeSize Communicator Traversal Server:

- One SSL/TLS certificate per server
- A wildcard SSL/TLS certificate

The wildcard certificate can be used for all servers in an organization's domain. Changing the hostnames of existing servers will not break certificate compatibility as long as the domain name isn't modified. Example: If ordering a wildcard certificate for company.com, changing from

sigX.company.com to sigY.company.com will not break certificate compatibility for a wildcard certificate.

If your organization changes the DNS entries for your LifeSize Communicator Traversal Servers when you are using non-wildcard certificates, you must obtain and install a new certificate.

#### Domain name for the LifeSize Communicator Traversal Server service

Example: If the Signaling Server and Media Engine are installed on computers with DNS entries signaling1.company.com and media1.company.com, respectively, then your two choices for certificate names are as follows:

Ordering two certificates with name fields:

- signaling1.company.com
- medial.company.com

Or using a single wildcard certificate with name field:

• \*.company.com

#### **Organization name**

The organization name must match with the information stored in the public domain name registry.

#### Unit within organization

Describes which unit within the organization is responsible for this certificate.

#### Locality/City, State/Province and Country

Address/location of the organization/unit.

#### **E-mail contact**

This e-mail address that will be visible in the certificate, for instance, <u>info@company.com</u>.

#### 2. Create key pairs and certificate signing requests

You create the certificate signing request (CSR) and key pair using tools located in the PCT (Paradial Certificate Tool) distribution. Unzip pct.zip somewhere on your hard drive. Enter the information described in the previous section in a configuration file in the PCT distribution. The country name codes referred to below are available here:

http://en.wikipedia.org/wiki/ISO\_3166

1. Open <PCT>/pd.cfg in a text editor. Locate the following section:

[ req_distinguished_name ] countryName countryName_default countryName_min countryName_max	= Country Name (2 letter code) = UK = 2 = 2
stateOrProvinceName	= State or Province Name (full name)
stateOrProvinceName_default	= London
localityName	= Locality Name (eg, city)
localityName_default	= London
0.organizationName	= Organization Name (eg, company)
0.organizationName_default	= MyCompany Ltd

organizationalUnitName	= Organizational Unit Name (eg, section)
organizationalUnitName_default	= IP Telephony
commonName	= Common Name (eg, YOUR name)
commonName_max	= 64
emailAddress	= Email Address
emailAddress_max	= 64
emailAddress_default	= <u>info@mycompany.co.uk</u>

2. Edit all the parameters that end with \_default. Enter the correct information for your company:

countryName_default	= UK
stateOrProvinceName_default	= London
localityName_default	= London
0.organizationName_default	= MyCompany Ltd
organizationalUnitName_default	= IP Telephony
organizationalUnitName_default	= IP Telephony
emailAddress_default	= <u>info@mycompany.co.uk</u>

- 3. Open a command shell and change directories to the PCT folder.
- 4. Create keys and CSR.

If you are ordering a wildcard certificate then you need to perform this step only once. For non-wildcard certificates, please perform this step once for each server/ DNS entry.

For wildcard execute:

openssl req -newkey rsa:1024 -keyout key.pem -out csr.pem -config pd.cfg

For non-wildcard, replace X with hostname, e.g. key sig1.pem, and then execute:

```
openssl req -newkey rsa:1024 -keyout key_X.pem -out csr_X.pem -config pd.cfg
```

Whenever the \_x extension is used in the remaining part of this document, a certificate is meant, regardless of if it is a non-wildcard or a wildcard certificate.

5. Follow these steps:

```
enter password (write down this password)
re-type password
Press enter to confirm "Country Name"
Press enter to confirm "State or Province Name"
Press enter to confirm "Locality Name"
Press enter to confirm "Organization Name"
Press enter to confirm "Organization Unit Name"
Enter the domain name for the certificate in "Common Name", i.e.
"*.company.com"
Press enter to confirm "Email Address"
```

- 6. Create a non-password-protected key file. openssl rsa -in key\_X.pem -out keynp\_X.pem
- 7. Store all key, csr files, and passwords in a safe place. If you lose the key files or forget the passwords, you will not be able to use the certificates ordered (see next section).

## 3. Order certificates from a Certificate Authority (CA)

Order a (wildcard) SSL certificate from a CA of your choice. Not all CAs support wildcard certificates. www.instantssl.com is a CA that supports wildcard certificates.

The order process is typically initiated from a web page. The certificate signing request (CSR) is provided along with contact information.

The CA verifies the company information provided in the order and in the CSR. An approval is also requested from the registered domain contact person for your domain. It is a good idea to find out who this is and tell him that he will probably receive such an email from the CA. If verification succeeds, you will receive the signed certificate by e- mail (after payment, of course). The CA will also pass on the CA and related chained CA certificates.

Store and name the signed certificates returned from the CA as follows (in <pct- folder>):

- cert.pem (if you ordered a wildcard certificate)
- cert\_X.pem (if you ordered one certificate per server)

where x is the name of the corresponding server. It is important to be systematic when dealing with these files since it is very easy to make a mistake if you handle more than one or two servers.

## 4. Install the signed certificates in LifeSize Communicator Traversal Server

LifeSize Communicator Traversal Server cannot directly use the signed certificates received from the CA. The Tunnel Server requires the following files:

- roots.pem (both servers)
- server\_public\_cert.pem (Signaling Server)
- cert.pem (media server)
- keynp.pem (media server)

In the descriptions below it is assumed that the received certificates are stored as cert\_X.pem corresponding to key\_X.pem and csr\_X.pem.

#### a) Create roots.pem

Create a text file roots.pem and insert the contents of all CA certificates that were used by your CA when signing the certificates. This file is the same on all servers.

#### b) Create server\_public\_cert.pem

Repeat the following step for all certificates, cert\_X.pem. Create a text file server\_public\_cert\_X.pem and insert the contents of key\_X.pem and cert\_X.pem. This is only needed for signaling servers.

#### c) Install the keys, certificate and CA certificates in Signaling Server.

For each signaling server X copy:

- roots.pem
- server\_public\_cert\_X.pem

to

```
/usr/paradial/ProxyServer.
```

Rename files:

```
• cd /usr/paradial/ProxyServer
```

• mv server\_public\_cert\_X.pem server\_public\_cert.pem

```
Update password in proxyserver.cfg. Example:
```

```
[Tunnel]
:
sslPassword=pwd123
```

#### d) Install the keys, certificate and CA certificates in media server.

For each media server x copy:

```
• roots.pem
```

```
• keynp_X.pem
```

```
• cert_X.pem
```

to

```
/usr/paradial/MediaEngine.
```

Rename files (only necessary for non-wildcard certificates):

- cd /usr/paradial/MediaEngine
- mv keynp\_X.pem keynp.pem
- mv cert\_X.pem cert.pem

Restart servers and verify that they are functioning normally.

## 5. Verify installation

You can verify that the certificates are correctly installed using the procedure described below. The free OpenSSL tool is available with most Linux distributions, and is available on both signaling and Media Servers from Paradial. The Windows version of OpenSSL is bundled with PCT. Note that the servers must be running in order to verify the installation.

The following commands use Linux file name conventions. The file roots.pem contains the CA certificates.

- 1. Log in to the Signaling Server as root.
- 2. Go to the Signaling Server directory /usr/paradial/ProxyServer
- 3. Verify Signaling Server certificates. Execute the following command: openssl s\_client -quiet -connect sig1.company.com:443 -ssl3 -cipher NULL-MD5 -CAfile roots.pem Press Control-C to exit the test client.
- 4. Verify Media Server certificates. Execute the following command: openssl s\_client -quiet -connect media1.company.com:443 -ssl3 -cipher NULL-MD5 -CAfile roots.pem

Press Control-C to exit the test client.

#### **Example printout 1: Certificates OK**

CONNECTED(00000003) depth=2 /C=US/O=GTE Corporation/OU=GTE CyberTrust Solutions, Inc./CN=GTE CyberTrust Global Root verify return:1

depth=1 /C=GB/O=Comodo Limited/OU=Comodo Trust Network/OU=Terms and Conditions of use: http:// www.comodo.net/repository/OU=(c)2002 Comodo Limited/CN=Comodo Class 3 Security Services CA verify return:1

depth=0 /C=NO/2.5.4.17=0165/ST=Oslo/L=Oslo/2.5.4.9=Nordahl Brunsgate 22/2.5.4.18=8702 Youngstorget/O=Paradial AS/OU=IT/OU=PremiumSSL Wildcard/CN=\*.Communicator Traversal Server.com verify return:1

A certificate chain of three certificates are received from the Signaling Server. The root CA (depth=2) is GTE CyberTrust Global Root. The intermediate CA (depth=1) is Comodo Class 3 Security Services CA. The server certificate (depth=0) is \*.Communicator Traversal Server.com. All three certificates are verified without any error messages.

#### **Example printout 2: Expired certificate**

```
CONNECTED(0000003)
depth=2 /C=US/O=GTE Corporation/CN=GTE CyberTrust Root
verify return:1
depth=1 /C=GB/O=Comodo Limited/OU=Comodo Trust Network/OU=Terms and Conditions of use: http://
www.comodo.net/repository/OU=(c)2002 Comodo Limited/CN=Comodo Class 3 Security Services CA
verify return:1
depth=0 /C=N0/2.5.4.17=0165/ST=Oslo/L=Oslo/2.5.4.9=Nordahl Brunsgate 22/2.5.4.18=8702 Youngstorget/O=Paradial
```

AS/OU=IT/OU=PremiumSSL Wildcard/CN=\*.Communicator Traversal Server.com

```
verify error:num=10:certificate has expired notAfter=Mar 8 23:59:59 2005 GMT verify return:1
```

In this example the verification of the server certificate (depth=0) fails because the certificate has expired.

#### 6. Backup

Back up all the files (keys, certificates and passwords) that were installed on the LifeSize Communicator Traversal Server(s). These files are needed in case of a software re-installation (due to hardware crash, or for other reasons).

## Troubleshooting

Here is a list of the most common errors people make when creating/installing new SSL certificates:

#### 1. Forgot to set new SSL password

When generating a new key pair, you need to specify a password. This password must be entered in proxyserver.cfg.

Example:

proxyserver.cfg:

[Tunnel] : sslPassword=pwd123

#### 2. Used wrong cipher when testing SSL certificates

The command line used for testing the certificates include a -<cipher> parameter. Forgetting to set this will give a warning that SSL handshake has failed (on the Signaling Server only). See example printout below.

Example error printout : Missing cipher spec

```
CONNECTED(0000003)
depth=2 /C=US/O=GTE Corporation/CN=GTE CyberTrust Solutions, Inc./CN=GTE CyberTrust Global Root
verify return:1
depth=1 /C=GB/O=Comodo Limited/OU=Comodo Trust Network/OU=Terms and Conditions of use: http://
www.comodo.net/repository/OU=(c)2002 Comodo Limited/CN=Comodo Class 3 Security Services CA
verify return:1
depth=0 /C=NO/2.5.4.17=0165/ST=Oslo/L=Oslo/2.5.4.9=Nordahl Brunsgate 22/2.5.4.18=8702 Youngstorget/O=Paradial
AS/OU=IT/OU=PremiumSSL Wildcard/CN=*.Communicator Traversal Server.com
```

verify return:1

24533:error:1409E0E5:SSL routines:SSL3\_WRITE\_BYTES:ssl handshake failure:s3\_pkt.c:529:

#### 3. Key and certificate are not matching

The certificate that is returned from the CA must be paired with the correct key file. To verify which key belongs to which certificate, use these commands:

#### Print key details:

>openssl rsa -text -in key.pem [Enter pass phrase] Private-Key: (1024 bit) modulus:

```
    00:ac:1c:53:c2:7b:61:31:e4:48:bd:4d:3f:1f:e9: 1b:d5:cd:7d:fa:bf:78:73:1f:b5:fd:30:e9:6a:32:
    4a:e3:84:d6:9e:2c:02:78:66:b7:ed:55:a3:ce:73: 39:e7:84:25:01:63:b7:eb:fa:6c:5a:c2:59:6a:c6:
    24:c0:a4:98:b2:60:be:5e:81:2e:bb:9a:01:d5:d6: b9:65:6c:4b:ff:a7:a4:54:92:8c:0e:79:3d:c6:d9: fc:95:7e:ba:c4:1c:ff:9f:a3:49:be:70:19:18:2a:
    1b:d5:cd:7d:fa:bf:78:73:1f:b5:fd:30:e9:6a:32: f0:1e:e4:03:e3:54:62:6c:5b
    publicExponent: 65537 (0x10001)
    privateExponent:
    79:85:32:ba:b1:a4:a9:b6:76:89:7a:7e:24:88:d1: c7:7e:e5:01:63:a9:a7:17:6f:c6:ca:7f:34:25:38:
    ...
```

## 4. Blank lines or whitespace in certificate files

Verify that there are no blank lines in any of these files:

- roots.pem (both servers)
- server\_public\_cert.pem (Signaling Server)
- cert.pem (media server)
- keynp.pem (media server)

# Appendix A: Configuring multiple IP addresses on a single NIC

Standard LifeSize Communicator Traversal Server configurations require two IP addresses on a single network interface card (NIC). The following instructions cover how to configure two IP addresses on a single card.

To configure two IP addresses on a single NIC, follow these steps:

- 1. On the host machine, choose Start > Settings > Control Panel.
- 2. Double-click Network Connections.
- 3. Right-click the Local Area Connection icon for the NIC you want to configure, then click **Properties**.
- 4. In the Properties dialog box, select the TCP/IP protocol, then click Properties.
- 5. On the General tab, verify that Use the following IP address is selected. Click Advanced.
- 6. In the Advanced Settings dialog, IP addresses section, click Add.
- 7. Enter the IP address and subnet mask for the second IP address, then click Add.
- 8. Both IP addresses should now appear in the Advanced Settings dialog. Click OK.
- 9. Click **OK** to save the TCP/IP properties and the Local Area Connection properties.

## Index

## A

active calls, 28

## С

call end reason list, 31 call status, 28

## D

DNS Configuration, 13

## E

event reporting, 26

## L

LifeSize Communicator Traversal Server about, 8 database configuration, 20 firewall rules, 16 installing, 13 requirements, 12 services, 14 logging, 29

## Ν

network interface card (NIC), configuring, 41

## 0

O&M certificates, 30 Operation & Maintenance Web interface, 18

#### S

SIP configuration, 23 registar, settings, 24 users, 25 SNMP trap forwarding, 27 SSL certificates about, 33 installing, 36 troubleshooting, 39 verifying, 37 STUN server, 22

## Т

TURN server, 23