LifeSize® Bridge™ 2200
Administrator Guide

Installing the LifeSize Bridge Utility

The LifeSize Bridge Utility manages LifeSize Bridge 2200 from your Mac or PC. You can create and manage conferences, configure system and user experience preferences, and perform diagnostics and maintenance using the utility.

Ensure that your system meets the following requirements prior to installing the utility.

Operating System	Requirements
Windows	Intel® Pentium III or faster processor Microsoft Windows XP Home, Professional, or Tablet PC Edition with Service Pack 2 or 3, Windows Server 2003, Windows Vista Home Premium, Business, Ultimate, or Enterprise (including 64-bit editions) with Service Pack 1, or Windows 7 RAM: 1 GB required, 2 GB recommended
Mac	Intel Core™ Duo or faster processor Mac OS X v10.4, v10.5, or v10.6 RAM: 1 GB required, 2 GB recommended
Linux	Intel Pentium III or faster processor Fedora Core 12, Ubuntu 9.10, or openSUSE® 11.2 RAM: 1 GB required, 2 GB recommended

NOTE   Windows 2000, Mac PowerPC, and 64-bit Linux are not supported by Adobe AIR 2 and are, therefore, unsupported with the LifeSize Bridge Utility.

To install the utility, enter the IP address of your LifeSize Bridge (by default, 169.254.1.1) in a browser. You are prompted to install Adobe AIR and the LifeSize Bridge Utility.

NOTE   The system on which you are installing the utility must be connected to the Internet during installation of Adobe AIR. This is only necessary the first time you launch the utility and if Adobe AIR is not already installed.

When you receive automatic notification of updates to the utility, you can install them immediately or download and install them at a later time.

NOTE   For the most current product information refer to the documentation and release notes at lifesize.com/support.

Getting Started with the LifeSize Bridge Utility

The LifeSize Bridge Utility enables administrators to manage all aspects of conferences and the system. Two types of user accounts are available.

- The **user** account, default password of *user*, can access the Scheduler only.

- The **admin** account, default password of *admin*, can access all areas of the utility.

LifeSize recommends that you protect the user and administrator preferences with a secure password. Change passwords from **Preferences : Passwords**. Passwords must be a minimum of five characters.

When logging in, you can select HTTPS from the login screen to enable secure communications.

Terminology

The following terms are used in this document to describe the LifeSize Bridge features. These terms may differ from terms used with other LifeSize video communications systems. Familiarize yourself with these terms to best understand the capabilities of your LifeSize Bridge.

call	Individual participant who joins a conference.
conference	Conference with multiple participants, hosted by the bridge.
expanded conference	Conference hosting up to 48 participants; a license key is required for this feature. Read more at Updating License Keys.
cascaded conference	Conference in which a multipoint control unit (MCU) hosts a combination of participant MCUs and single participants. Refer to Configuring Conference Types.
on demand conference	Conference that is not scheduled in advance, does not have a scheduled start time, and is always live.
temporary conference	On demand conference that is removed two minutes after the last participant exits the call. A temporary conference can only be created from the Virtual Operator by selecting *Allow users to create conferences*.
scheduled conference	Conference that is planned in advance and includes a specific start and end time.
active	State of the conference after the first participant has joined.
live	A conference is live when the start time occurs, or when an on demand conference has been initiated; participants need not have joined for the conference to be live.
port	Refers to both Ethernet ports to which you connect your bridge, as well as conference connection ports, which determine the number of simultaneous participants that can be hosted on a single conference.

Navigating the Utility

The IP address of the system to which you are logged in and the version of software you are running appear in the title bar of your browser. System information appears at the top of the utility. Mouse over the text and icons for more information:

Scheduled	Number of live scheduled conferences.
Ports	Number of scheduled ports.
On Demand	Number of on demand conferences.
Active	Number of live conferences with participants.
Operator	Number of participants interacting with the Virtual Operator.
Calls	Total number of connected calls.
	Number of connected video calls.
	Number of connected voice calls.
Available	The number of remaining ports, not active or not scheduled.
	A shortcut to **Diagnostics : System Health**, providing a quick view of your system, temperature, and fan status. This icon changes color to identify the health of the system.
H.323	A shortcut to **Preferences : H.323**. This text changes color to identify the status of the protocol connection.
SIP	A shortcut to **Preferences : SIP**. This text changes color to identify the status of the Session Initiation Protocol (SIP) connection.
FIPS	Indicates that FIPS-140-2 (**Preferences : Security : FIPS**) is enabled.
	A shortcut to **Preferences : Network**. This icon changes color to identify the status of the network connection for each configured Ethernet port; the port number also appears on this icon.
	A shortcut to **Preferences : Network**. This icon changes color to identify the status of the redundant ports, if network port redundancy is enabled.

Click the buttons beneath your system information to schedule and manage calls, set preferences, and perform diagnostics and maintenance.

Scheduling Conferences

Manage conferences from the calendar view of conferences in the Scheduler. You can view all conferences by day, week, or month.

Allocating Ports

You can create both scheduled and on demand conferences.

- Scheduled conferences have a specific start and end time, and ports are allocated by participant.

- On demand conferences have no start or end times, and no allocated ports. They use any available port not scheduled or active.

On demand conferences include all attributes of scheduled conferences except start and end times and recurrence settings. This conference begins if required ports are available when the first participant attempts to join.

The Scheduler manages the scheduling of ports and ensures there are no conflicts with the available ports. Each participant in a conference uses one port. You can choose 2 through 16 ports for the conference, and additionally select 16 ports and then select **Expand** to accommodate up to 48 participants.

NOTE   **Expand** is available only for scheduled conferences, if all ports are available, and if a license for this feature is available. Read more about Expanding Your Conference.

Up to eight conferences can be active at one time. Scheduled conferences take priority over on demand conferences. Therefore, if you create 2 two-way scheduled conferences and 10 on demand conferences, only 6 of the on demand conferences can become active, consisting of two participants in each. In this scenario, attempts to join the remaining on demand conferences are rejected and the caller receives a busy signal.

If two active, scheduled conferences are using 4 ports and 6 ports, respectively, 10 ports are scheduled, leaving 6 ports available for on demand conferences. If a scheduled conference requiring 3 ports becomes active, the longest running on demand conference(s) terminates to free the necessary 3 ports for the scheduled conference.

You can create up to 40 on demand conferences. On demand conferences are listed in a separate view in the Scheduler, to the left of the calendar view. If you have reached the maximum number, the ⊕ button is disabled.

Creating a Conference

1. To create an on demand conference, click ➕ below the list of On Demand Conferences.

    To create a scheduled conference, open the Scheduler and double-click the desired date for the conference, or right-click the date and choose **Create Conference**.

    > NOTE   If all ports are in use or allocated to scheduled conferences, you cannot create a new conference from the Virtual Operator.

    To create a cascaded conference, refer to Configuring Conference Types.

2. Select **Auto** to automatically assign an ID to the conference. Clear the check box to assign a specific conference ID.

    > NOTE   If you specify a conference ID that is already in use, the system substitutes an alternate value. You cannot modify the conference IDs of live conferences.

3. Enter a name for the conference.

4. *Optional*: Enter a description of the conference.

5. *Optional*: Enter a password that users must enter to join the conference. Select **Display Password** to include the password in the meeting invitation. Passwords must be 20 characters or less, numbers only.

6. Select **All Day** or adjust the time frame for the start and end date and time.

7. For recurring conferences, select how often to repeat. Recurring conferences are indicated in the Scheduler by 🔄 .

8. Choose the number of ports to allocate for the conference. For up to 48 participants in a scheduled conference, choose 16 ports and select **Expand**.

    > NOTE   **Expand** is available for scheduled conferences only, if all ports are available, and if a license for this feature is available. Read more at Updating License Keys.

9. To set additional preferences, click **Show Details** to change the following values:

Preference	Description	Default Value
Conference Type	Refer to Configuring Conference Types for more information.	Standard
Language	The language in which the user interface text and voice prompts appear.	English (US)
Self View	The view from a participant's own camera appears on their screen.	Off
Speaker Order	The most recent speaker appears in the prominent window.	On
Status Indicators	Status icons appear on the user interface.	On

Preference	Description	Default Value
Announcements	Voice prompts and system sounds indicate the current system status or action required.	On
Navigation	Control the interface using touch tones or far end camera control.	Touch tones
Text Inset	How far the text is offset from the sides of the screen.	7%
Default Layout	The default layout to use for the conference.	Auto
Participants	A list of participants to add to a conference when it becomes live. In a scheduled conference, these participants are dialed when the conference becomes live. In an on demand conference, all participants are dialed when one participant dials the conference, making it live. You can also trigger the conference from the Call Manager by clicking 📞➡. If you prefer that participants must dial in individually, do not define any participants in this list.	no default
Participant Bitrate	The bit rate for each participant in the conference.	Auto
Security	Encryption level used for the conference. *Auto* allows both encrypted and unencrypted calls. *Strict* connects encrypted calls only.	Auto
Resolution	The video resolution used for the conference. The default is 720p60.	Auto
Video Codecs	Customize the default video codec order, or allow the system to choose automatically.	Auto
Audio Codecs	Customize the default audio codec order, or allow the system to choose automatically.	Auto
Presentations	The ability to display data from a PC or secondary input.	On
Presentation Codecs	Customize the default presentation codec order, or allow the system to choose automatically.	Auto

10. Click **Save** to make the changes and close the dialog box.

NOTE   Not all options are available during active conferences or for expanded conferences.

You can also manage conference restrictions from **Preferences : Scheduler**.

Conference ID Bounds	Choose the number of digits the system will allow for a conference ID. The default is 4. Also specify the minimum and maximum allowable numbers. Minimum default: 1000. Maximum default: 9999.
Maximum On Demand Conferences	Enter the maximum number of on demand conferences the system will manage. The default is 40.
Expired Conference Removal Time	Choose the length of time for the system to store expired conferences. The default is 3 months.

Troubleshooting Scheduling Failures

Message	Action
The conference has no name.	Enter a name for the conference in the **Event Information.**
No available ports for requested time.	Select a time for the conference when the required number of ports is available.
All conference IDs are in use.	Change the range of possible conference IDs in **Preferences : Scheduler** to allow the system to assign a unique ID.
Exceeded maximum number of on demand conferences.	Increase the value for **Maximum On Demand Conferences** in **Preferences : Scheduler.**
Scheduler file not found. The system may be corrupt.	Restart the LifeSize Bridge Utility.

Expanding Your Conference

You can add up to 48 participants to a scheduled conference by selecting 16 ports and then selecting **Expand**. The **Expand** check box does not appear if all 16 ports are not available, if a license key is not available for this feature, or if a 16 way conference is live. No other conferences can be created during this time. Read Creating a Conference for specific instructions. Participants of an expanded conference are unable to control the conference or change the layout. The default layout shows video from the last 8 active speakers. Change layouts from the Scheduler to show fewer or additional participants.

A license key is required to expand the conference beyond 16 participants. The **Expand** check box does not appear if no license is available. Contact your LifeSize reseller or LifeSize Technical Services to obtain the expanded conference license key.

Configuring Conference Types

Configuring Cascaded Conferences

You can allow a conference to host other conferences as participants. The host conference can include MCU and non-MCU participants. Participant MCUs cannot host other MCUs. A scheduled cascaded conference can host up to 16 participant MCUs. An on demand cascaded conference can host up to 15 participant MCUs.

1. Determine the host MCU and note its IP address.

2. Configure conferences on each participant MCU.

   a. From a participant LifeSize Bridge Utility, create a scheduled or on demand conference. Refer to Scheduling Conferences.

   b. Click **Show Details**.

   c. From **Conference Type**, select *Cascading Participant*.

   d. Click **Add Participant**, enter the host MCU's number and change **Participant Type** to *Host MCU*.

   e. Add other participants as required.

   f. Note the conference ID.

   NOTE   For third party MCUs, create the conference and add non-MCU participants only. Configure the layout to full screen and active talker. The participant conference must be able to accept a call from the host.

   ---

3. Configure a conference on the host LifeSize Bridge.

   a. From the host LifeSize Bridge Utility, create a conference.

   b. Click **Show Details**.

   c. For **Conference Type**, select *Cascading Host.*

   d. Click **Add Participant** and add each participant MCU number and change **Participant Type** to *Participant MCU*. The dial string you enter as the participant MCU number must specify the participant conference you created in step 2.

   e. Add other participants as required.

Participant MCUs send the last talker on their conference to the host conference, and participants on the participant conference can view only the layout sent from the host MCU.

NOTE   Third party MCUs produce infinitely cascaded video to the host until one of their participants joins.

SIP Presentations are not supported on third party MCUs.

Configuring a Lecture Conference

Use lecture type to specify a participant who always appears in the main window regardless of who is speaking.

When creating the conference, click **Show Details : Conference Type : Lecture** and change one participant's type to *Lecturer*.

Sharing Presentations

Users can share data during a call through a secondary H.239 media channel, typically from a laptop or personal computer that is connected to the appropriate input on the participating LifeSize system.

By default, presentation codecs are automatically selected. You can customize the codecs and the order in which they are attempted in a conference from either **Create New Conference** or **Event Information**. Click **Show Details**, and select *Custom* for **Presentation Codecs**. Then choose the codecs to add to the custom list, and drag them to the desired order.

The Call Manager indicates the status of a presentation in progress 🖼 .

Managing Conferences

The Call Manager automatically updates as conferences become live or expire, and as calls connect and terminate. The first column in the Call Manager identifies whether the conference is scheduled 🖼 or on demand ▶ . Click ▼ next to the conference to view additional details about the conference:

📞	Identifies the participant as a voice call.
👤	Identifies the participant as a video call.
⬅	Identifies the participant as an incoming call.
➡	Identifies the participant as an outgoing call.
🎤 🔇	Identifies the received audio as unmuted or muted. LifeSize devices only.
🔒	Identifies the participant or conference as encrypted.

Options in the second column depend on whether you are viewing a single call or controlling all participants in the conference. Following are the actions you can take:

📞➡	In live conferences with no participants, dial the participants when the conference becomes live.
🔊 🔇	Toggle the audio transmission.
👤 🚫	Toggle the video transmission.
▦	Change the video layout. Select a layout from the dialog. Refer to Managing Layouts.
🔒	The video layout for a participant or the conference is locked. Refer to Locking a Video Layout.
⚙	Change the user experience settings. Refer to Creating a Conference.

Display the following audio, video, and presentation statistics for a call, including both transmit and receive data:

- resolution
- codec
- bandwidth
- frame rate
- maximum jitter
- average jitter
- packet loss

You can increase or decrease the value in the **Refresh Interval** box and click **Refresh** to update the number of seconds to refresh the values.

Add a participant to the live conference. (Disabled if the conference has reached full capacity.)

Terminate the call or conference.

The remaining column in the Call Manager provides detailed information about the conference:

- name and ID of the conference

- conference state

- number of allocated ports

- number of participants

- start and end time of the conference (scheduled conferences only)

- protocol (the registration status for the conference with the respective gateway or registrar)

Individual calls display the following:

- call state (for example, dialing, connecting, busy, unreachable, etc.)

- system name, IP address, and number

- encoder and decoder

- protocol used

- vendor information for the system (and software version number)

State indicates the conference's registration status with the communication protocol. The following values may appear:

expiring	The conference is about to exceed its scheduled time.
expired	The conference has exceeded its scheduled time and will be removed.
unregistered	Your system is currently not registered with an H.323 gatekeeper or SIP server.
registering	Your system is attempting to register with the H.323 gatekeeper or SIP server.
registered	Your system successfully registered with the H.323 gatekeeper or SIP server.
registration failed	The registration failed. Click **Register** to retry.
unknown error	An unknown error occurred preventing registration. Click **Register** to retry.

Modifying Conferences

You can configure most conference attributes, including:

- conference name and description
- password
- ports
- start and end dates and times
- if recurring, how often to repeat and when to end
- ports
- language
- self view, speaker order, status indicators, announcements, and navigation options
- text inset
- default layout (choosing a different layout automatically locks the layout when a participant joins)
- participants in the conference and their bit rate
- moving participants from one conference to another
- security
- resolution
- video, audio, and presentation codecs
- presentations status

> NOTE   Changing any of these options from the Virtual Operator during a call does not affect participants in the active call.

Multiple instances of LifeSize Bridge Utility can manage the same schedule. If you add, modify, or delete a conference, the change automatically appears in a second instance of the utility.

You can modify conferences in the following ways:

Set the minimum and maximum limits for conference IDs	**Preferences : Scheduler**	Choose the number of digits and the minimum and maximum range.
Edit or remove an on demand conference	**Scheduler**	Highlight the conference name you want to modify or delete, and double-click, right-click, or click ✏. NOTE: A limited set of edit options are available for active conferences to ensure uninterrupted connectivity.

| Add participants to a conference	**Call Manager**	Click ⊕. Enter the participant's *Number*, specify the call *Type*, *Protocol*, and *Bitrate*. You cannot add a participant MCU to a cascaded conference using this method. NOTE: When the conference has no available capacity, ⊕ is disabled.
Move participants from one conference to another	**Call Manager**	You can drag participants from one conference in the Call Manager to another. The participant immediately drops from the current conference and joins the other conference. If you move a participant sharing a presentation, the presentation immediately ends.
Specify when to remove expired conferences from the Scheduler	**Preferences : Scheduler**	The default is 3 months.
Modify or delete recurring conferences	**Scheduler or Call Manager**	Choose to edit or delete a single instance or all instances in the series.
Cut, copy, paste, or drag	**Scheduler**	You can drag a conference to a new time. You can copy and paste a conference to a new date and time. A new ID is assigned. You can also copy and paste an on demand conference to be a scheduled conference and the reverse. By default, an on demand conference copied to a scheduled conference becomes an all day conference; however, you can edit the conference details to adjust this result.

Managing Layouts

The following illustrations show the number and order of layouts available for each possible call scenario. Layout rotation is determined by the maximum number of video participants allocated for the conference.

Participants appear in the order in which they join the conference. When new participants join the conference after all available spaces in the current layout are filled, the layout changes to the next best fitting layout. The layout also changes to the best fit as participants exit the conference, unless manually changed by the user.

With only one participant in a conference, the full screen view becomes the first layout in the rotation.

If up to two maximum participants are allocated for the conference, the following layouts are available:
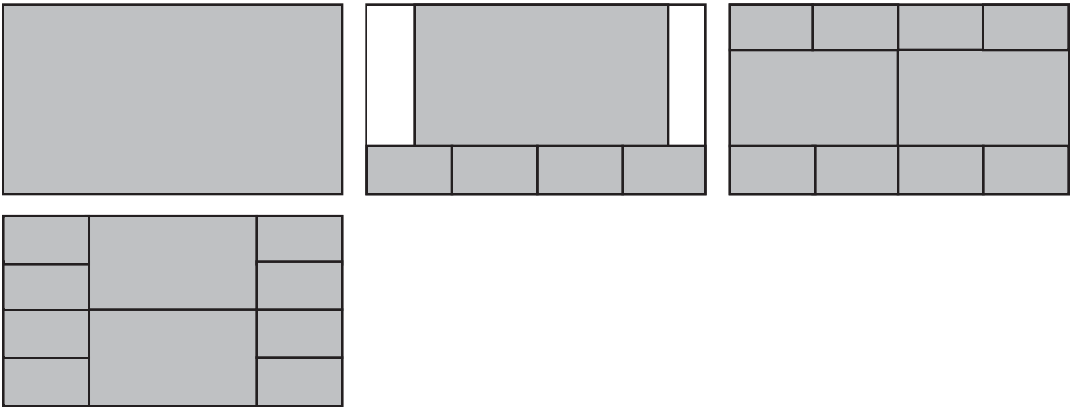
If three maximum participants are allocated for the conference, the following layouts are available:
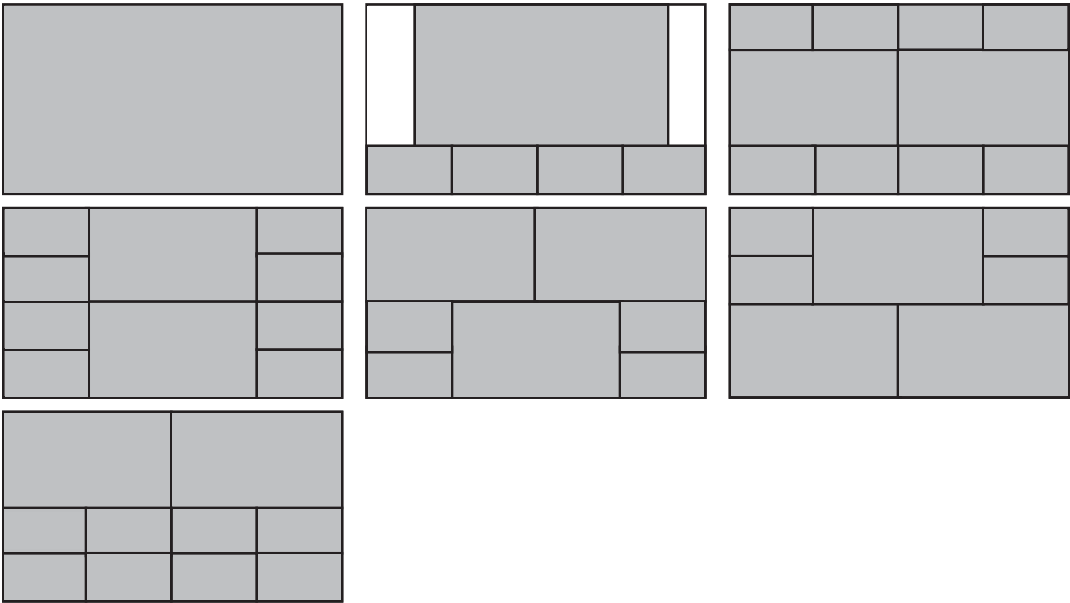
If four maximum participants are allocated for the conference, the following layouts are available:
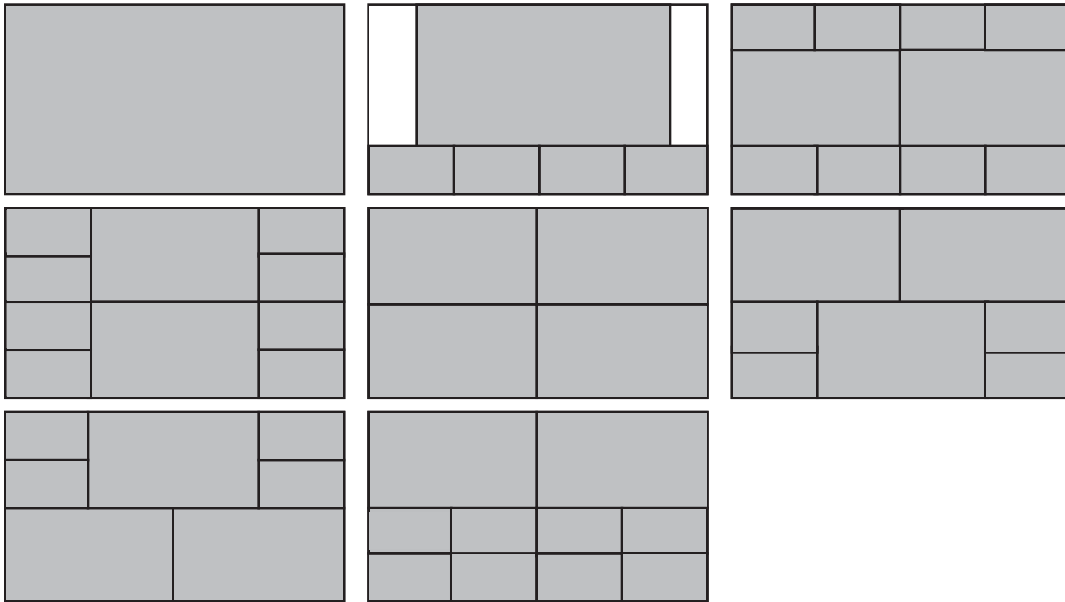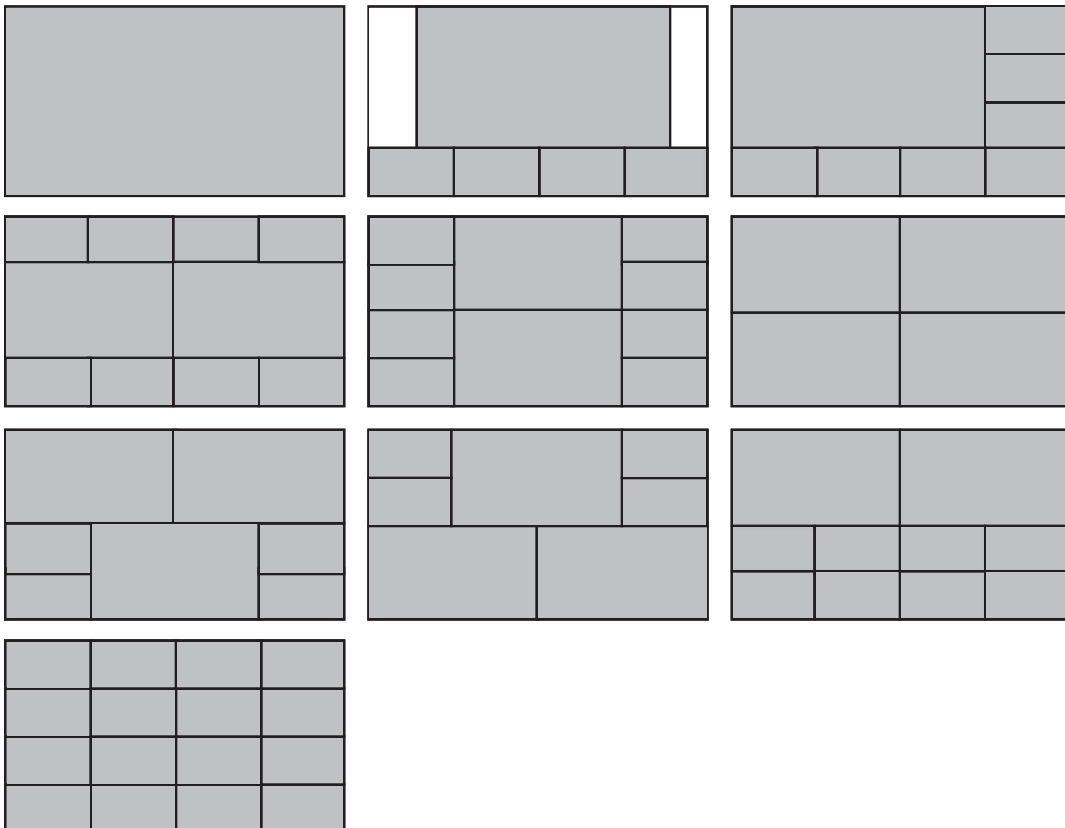
If 5 to 7 maximum participants are allocated for the conference, the following layouts are available:

If 8-16 maximum participants are allocated for the conference, the following layouts are available:
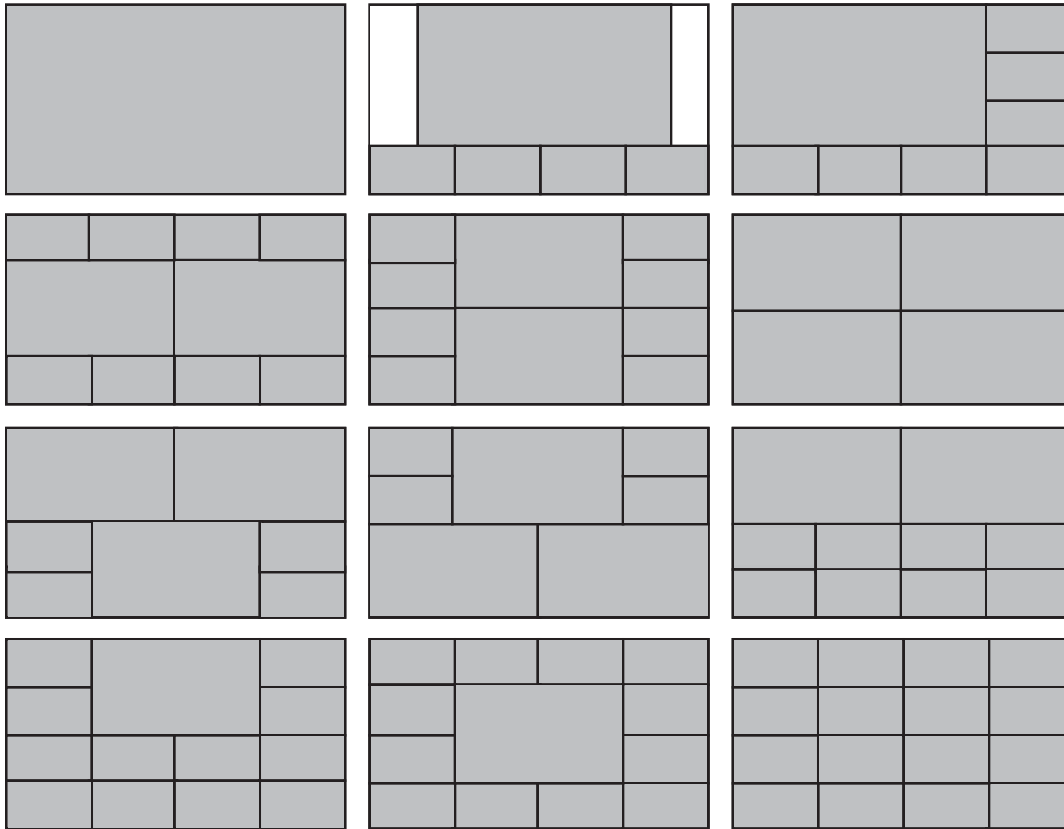
If only one participant is connected, the setting for **Self View** is ignored until a second caller joins the conference. **Self View** is disabled by default.

Changing Layouts for an Individual Call

1. From the Call Manager, select the call whose layout you want to change.

2. Click ⬛⬛▤ .

    The available layouts appear for that call. The current layout appears highlighted in green.

3. Choose the desired layout.

4. If speaker order is not disabled, the layout change takes effect immediately. Otherwise you must click **Apply**.

5. Click **Close**.

Customizing How Participants Appear in Layouts

You can choose to disable speaker ordering and instead drag particular participants into particular windows for the duration of the call. You can customize participant positions in the master layout of the conference or in layouts of individual participants.

1. From the Call Manager, select the conference or participant whose layout you want to change.

2. Click .

   The available layouts appear for that conference or participant.

3. Choose the desired layout.

4. Click **Disable Speaker Order**.

5. Drag participants from one window in a layout to another or replace participants in layout windows with participants not currently visible in the layout. Click **Clear All** to remove all participants from the layout and then drag participants into the layout.

6. Click **Apply**.

Locking a Video Layout

From the Call Manager, select the conference whose layout you want to change.

7. Click .

8. Choose the desired layout.

9. Choose lock.

10. Click **Close**.

To ensure new participants joining a call are locked, choose a default layout and lock it for the conference instead of locking individual callers.

NOTE   The layout in expanded conferences and for participant MCUs in a cascaded conference is always locked and cannot be unlocked.

Configuring Preferences

Changes to preferences that may cause a call to disconnect or the system to restart display a notification. These preferences are unavailable if calls are in progress. Changes to these preferences must occur when the system is idle. Schedule a maintenance window to make these changes by creating a conference that uses all ports and has a password that is not shared.

Configuring the System Date and Time

The system date and time are automatically set if one of the following conditions exists:

- The **DHCP** preference (in **Network**) is set to *Enabled*, and the DHCP server can pass an NTP server address to your system.

- You specify the hostname or IP address of an NTP server in **NTP Server Hostname**.

> NOTE   The value you specify for **NTP Server Hostname** is used in addition to any NTP server address that a DHCP server passes to your system.

View or configure the date and time of the system as follows:

Current System Time	Shows the current system time, relative to the system's configured time zone.
System Time	Configure the current time on your system relative to the system's configured time zone.
Time Zone	Configure the time zone of your system.
Current NTP Server	Shows the currently configured NTP server. This value can be set manually or specified by DHCP.
NTP Server Hostname	Configure the NTP server of your system.

Configuring Your Network

To configure preferences that affect how your system functions with other servers and devices on your local network, modify the **Network** preferences.

Controlling Ethernet ports	Enable or disable each of the four Ethernet ports. Disable the ports that you are not using. Selecting the port shows the status, current IP address, and subnet mask for the port. You can configure one port at a time or configure up to four network ports for port redundancy.
Specifying DHCP or a locally configured IP address	DHCP dynamically allocates and assigns IP addresses. Enable DHCP (if a DHCP server is present) by selecting **Use DHCP**. If you disable DHCP, enter the locally configured IP address and subnet mask (used to partition the IP address into a network and host identifier).
Specifying network speed	If you do not select **Auto negotiate speed and duplex settings**, ensure that the values match the speed and duplex configured on your network switch. LifeSize recommends that you set **Auto negotiate speed and duplex settings** unless your network specifically requires a fixed speed or duplex setting. NOTE: If your Ethernet switch is configured for half duplex, you may experience poor quality video when placing calls greater than 512 kb/s. Change your Ethernet switch configuration to a setting other than half duplex when selecting **Auto negotiate speed and duplex settings**.
Specifying a VLAN ID	If you have static virtual local area networks (VLANs) configured, you can configure your LifeSize system to apply a VLAN tag to outgoing packets and accept incoming tagged packets only if they have the same VLAN identifier. Specify the VLAN identifier of the VLAN to which the system is assigned. The value range is 1 through 4094.
Network Port Redundancy	Select the check box to enable redundancy, specify the ports you are using, and specify the type of port redundancy. The port status, current IP address, and subnet mask for all enabled ports appears. Read more at Configuring Network Port Redundancy.
Default Gateway	Specify the default gateway.
Specifying the hostname and DNS servers	Enter the hostname of the system and the IP addresses to configure domain name service (DNS) servers. Enter the domain names to search when resolving hostnames. DNS translates names of network nodes into addresses; specify this preference to use DNS to resolve the hostnames to IP addresses. NOTE: A system cannot detect a change to its IP address from a change in networks from a wiring closet or through software, such as a change to a router configuration.
Restricting reserved ports	By default, LifeSize systems communicate through TCP and UDP ports in the range 60000 - 64999. You can restrict the range of UDP and TCP ports that are available for communication. LifeSize recommends that the range you choose, if other than a subset of the default range, begins with a port number greater than 10000. A minimum of 128 ports must be open regardless of the call type or number of participants.
Configuring QoS	Set Quality of Service (QoS) preferences according to the settings in your network. You can specify DiffServ (differentiated services) or IntServ (integrated services) values for audio, video, and data packets. You can also set the IntServ Type of Service (ToS) preference. By default, **Network QoS** and **IntServ ToS** are set to *None*. The range for DiffServ values is 0 - 63. The range for IntServ values is 0-7.
Adjusting the MTU of video packets	Video packets that exceed the maximum transmission unit (MTU) size for any router or segment along the network path may be fragmented or dropped, resulting in poor quality video at the receiving device. You can set the MTU of video packets that your LifeSize system sends. The default value is 1440 bytes. The valid range is 900 -1500 bytes.

Configuring Network Port Redundancy

Enable network port redundancy to configure and combine up to four Ethernet ports into a single connection.

1. Click ⬚ at the top of the utility or navigate to **Preferences : Network**.

2. Select **Enable Network Port Redundancy**.

3. Select the type of port redundancy bond.

Active Backup	The default. Only one port is active. Another port becomes active if the current port fails.
802.3ad	Creates groups that share the same speed and duplex settings.
Adaptive Transmit	Outgoing traffic is distributed evenly; does not require switch support.
Balanced Round Robin	Packets are transmitted in sequential order across available ports.
Balanced XOR	Packets are transmitted based on MAC address. The same port is selected for each destination MAC address.
Broadcast	Each port transmits the same signal.

4. Select the network interface to configure for each of the four redundant ports.

5. Click **Save**.

Configuring Your Firewall

If your LifeSize system communicates with other systems through a firewall, you must configure your firewall to allow incoming and outgoing traffic to the system through the following ports:

*   TCP port 1720 (for H.323 call setup)

*   UDP port 5060 (for SIP call setup)

*   TCP port 5060 (for SIP call setup if TCP signaling is enabled for SIP calls)

*   TCP port 5061 (for TLS signaling in SIP calls if TLS signaling is enabled)

*   Reserved TCP and UDP ports (default range 60000 - 64999)

*   80 (HTTP) and 443 (HTTPS) for administration ports

Configuring Protocols

You can also identify the status of H.323 and SIP services, network interface status, and system health from the system information at the top of the utility. Clicking any of these icons displays the preferences for these items, which you can then modify.

Configuring H.323

By default, LifeSize Bridge supports the H.323 protocol for placing and receiving video and voice calls. To disable support for H.323 calls, clear **Enable H.323** in **Preferences : H.323 : General**.

NOTE   If both **H.323** and **SIP** are *disabled*, a message indicates that calls cannot be placed or received.

When H.323 is enabled, you can specify an H.323 name or extension to use when placing a call. The H.323 name and extension identify the device to the gatekeeper. Any registered device can dial another using this name and extension. The **H.323 Name** preference is an optional value that is used when a gatekeeper is configured and requires the system to register with an H.323 ID. If the gatekeeper administrator assigns an H.323 ID for the system, enter that ID for **H.323 Name**. The **H.323 Extension** preference is an optional value that is used when a gatekeeper is configured and requires the system to register with an E.164 number or extension. If the gatekeeper administrator assigns an E.164 number or extension for the system, enter that number for **H.323 Extension**.

Set the **Gatekeeper ID** only if the gatekeeper requires it (for example, configurations with multiple gatekeepers). The **Gatekeeper ID** must match the gatekeeper ID configured for the gatekeeper to which the system is registering. Select **Enable Gatekeeper Authentication** to enable authentication and enter the authentication username and password.

Set **Gatekeeper Mode** to *Auto* to have the system automatically discover a gatekeeper. You can also set **Gatekeeper Mode** to *Manual* to specify the IP address and port for the primary gatekeeper.

When you click **Save**, icons appear in the status bar to indicate the status of the registration process. The yellow icon appears when your system is attempting to register. If the registration fails, the red icon appears.

Configuring SIP

By default, support for SIP is enabled. To configure SIP as the protocol to use for placing calls, select the **Enable SIP** check box in **Preferences : SIP : General** and configure the SIP preferences.

In **Preferences : SIP : Identification**, enter the username, SIP server authorization name, and password for the device, if required. The authorization username and password are the values the LifeSize system uses for authentication; these values are required only if the registrar or proxy require authentication.

You can enable the SIP registrar or a proxy and configure proxy settings. SIP devices use register settings to dynamically register their current location.

When you click **Save**, the status bar indicates the status of the registration process with the SIP server. SIP appears when your system is trying to register with the SIP server. If the registration fails, SIP appears. If the registration fails, click **Register** to retry.

Ports

By default, UDP and TCP signaling are enabled and cannot be disabled. The default port for each is 5060, but you can change either to a non-zero value.

By default, the TLS signaling port is 0, which disables TLS signalling. Enter a non-zero value, customarily 5061, to enable TLS signalling. Select **Enable the SIP registrar** and register to a SIP registrar. Direct SIP TLS calls are not supported.

If you enable TLS signaling, the system attempts to use Secure Real-time Transport Protocol (SRTP) for media encryption in SIP calls. If the far side supports SRTP, the media is encrypted.

NOTE   The system reboots if you change any port value and click **Save**.

Configuring the Virtual Operator

Use the Virtual Operator to create and connect to conferences.

1. Access **Preferences : Virtual Operator**.

2. Select the check box to enable the operator.

3. Enter a name for the operator, which will appear in the caller ID and redial lists. (The default is **Virtual Operator**.)

4. Select a language.

5. Select *Touch Tones* or *Camera Control* as the default navigation method.

6. To create a **temporary conference** from the Virtual Operator, check *Allow users to create conferences*. This allows users interacting with the Virtual Operator to create an on demand conference that is removed two minutes after the last participant exits the call.

Controlling Remote Administration

By default, remote access to a LifeSize system through the web (HTTP) or SSH is enabled. To change remote access through these mechanisms, configure **Preferences : Security**.

NOTE   Disabling HTTP immediately disconnects you from the system, and you are no longer able to manage the system from the web. If you select *Disabled* for this preference, you are prompted to confirm the change. You can re-enable HTTP from the console using the `set http enabled` command. Refer to the *LifeSize Bridge Installation Guide* for more information about running commands from the console.

Enabling FIPS 140-2 Security

LifeSize Bridge 2200 supports the Federal Information Processing Standard (FIPS) 140-2 (Level 1), a US government computer security standard. By default, FIPS security is disabled. When you enable FIPS 140-2 (**Preferences : Security : FIPS)**, the following occurs:

• The system reboots.

• FIPS appears at the top of the utility after the system reboots.

• **System Upgrade**, **System Save**, and **System Restore** are disabled in **Maintenance**.

• **Add**, **Delete**, and **Update** buttons are disabled on the **License Keys** page.

• **Preferences : SIP : TLS Signaling Port** is removed.

• In the **Add Participant** dialog, the protocol selection is removed.

Diagnostic Tools

Call Records

Diagnostics : Call Records displays the call history of the system, including:

- system name and IP address

- conference ID

- start time and duration

- call direction

- protocol

- dialed and actual bandwidths

- the reason for disconnection

You can export this data to an XML file by clicking **Save Records**. Click **Refresh** to reload the current call records. Select the maximum number of call records, up to 2000, to store in **Preferences : Diagnostics**. Possible reasons for disconnection are as follows:

Normal disconnect	The call was terminated correctly.
User busy	The caller was unreachable.
Unreachable destination	The call could not connect to the other party.
Destination rejection	The call was rejected and could not connect.
Call deflection	The call request was redirected.
In conference	Another call is in progress.
No bandwidth	The bandwidth necessary for the call is unavailable.
Security denied	Incompatible security support.
TCS rejected	Terminal Capability Set (TCS) failed.
Local failure	The call disconnected due to a subsystem failure.
Unreachable GK	The system could not register with the gatekeeper; gatekeeper was unavailable or the gatekeeper IP address was invalid.
No GK resource	The gatekeeper is unavailable.
No GW resource	The system could not register with the gateway.
Invalid address	The IP address was invalid.
Called party not registered	The called participant is unregistered and unreachable.
Caller not registered	The caller is unregistered and cannot connect to the call.
Max calls exceeded	The maximum number of calls has been reached.
Audio resource unavailable	Audio is unavailable to complete the call.

Select **Show TX/RX Details** to display the transmit and receive data for audio and video codecs.

System Health

From **Diagnostics : System Health** you can view the status of the system, temperature, and fans, and determine whether the system has experienced critical errors.

The current running temperature is color coded accordingly:

Green	normal operating temperature
Yellow	approaching critical temperature
Red	system overheated or shut down due to overheating

Fan status for the four fans is color coded accordingly:

Green	normal
Red	stalled or failed

These values are read only. You cannot adjust fan speed.

System Information

Diagnostics : System Information displays details about your system, including serial numbers and versions.

You can export this data to a text, HTML, or XML file by clicking the corresponding button.

System Logs

From **Preferences : Diagnostics**, enter the hostname or IP address of your system log server. Then choose the log level for each of the subsystems.

NOTE   Choosing verbose or debug can adversely affect the performance of the system.

From **Diagnostics : System Logs** you can filter the current log and save the current view to your computer. Logs are color coded by level:

Verbose	White
Debug	Blue
Info	Green
Warning	Yellow
Error	Orange
Failure, Critical, Alert, Panic	Red

Select the check boxes on the left to choose which subsystem data to view or export. Select the levels at the top to choose which level of the logs to display.

System Reboot

The system reboots when you complete any of the following tasks:

- Manually reboot the system (**Diagnostics : System Reboot**).

- Reset the system to its default state (**Maintenance : System Reset**).

- Revert the system to the previous state (**Maintenance : System Revert**).

- Restore the system to a saved state (**Maintenance : System Restore**).

- Change the **VLAN ID** preference (**Preferences : Network : VLAN ID**).

- Change TCP reserved ports (**Preferences : Network : Reserved Ports**).

- Change the UDP signaling port, enable or disable TCP or TLS signaling, or change the TCP or TLS signaling ports.

- Upgrade the system software (**Maintenance : System Upgrade**).

- Change IP address.

- Change protocol and network preferences; these are disabled if calls are in progress. Schedule a maintenance window to make these changes by creating a conference that uses all ports and has a password that is not shared.

You may need to reboot a system that fails to connect calls. To reboot the system, click in **Diagnostics : System Reboot**.

If calls are in progress, you are prompted to continue or cancel. Press **Continue** to disconnect the calls and complete the reboot.

NOTE   If the user interface is not responding and you are unable to reboot the system, press the Reset button on the front of the system. Do not attempt to restart your system by unplugging the power cord.

Maintaining Your System

System upgrade, license key, and system reset options are available from the **Maintenance** page.

You can schedule a maintenance window in which to manage the system, and change preferences that may require a system reboot. Some preferences are unavailable if calls are in progress.

Create a maintenance window by scheduling a conference that uses all ports and has a password that is not shared.

Saving a System Configuration

1. Navigate to **Maintenance : System Reset**.

2. Click ⬤ .

3. Choose a location to save the configuration file and then click **Save**.

NOTE   Scheduler data is not saved in this process.

Restoring a System Configuration

1. Ensure that a current, saved configuration file exists before performing a restore.

NOTE   Configuration preferences and options vary across software releases. Restoring a system configuration using a file saved from a different software release can produce unexpected results. Only restore a configuration that was saved from the same software release.

---

2. Hang up all calls connected to the system. If calls are connected when you perform a restore, a dialog box prompts you to continue or cancel the restore. If you continue, the system restore process terminates the calls.

3. Navigate to **Maintenance : System Reset**.

4. Click ⬤ .

NOTE   You must have a current system configuration saved prior to executing the system restore function or you will be unable to return to the previous state.

---

5. Click **Continue** and choose the file to which to restore the system.

   The system reboots and a dialog box indicates that the restore succeeded.

Resetting the System

1. Navigate to **Maintenance : System Reset**.

2. Click   .

3. Enter the reason for the reset and click **Yes** to confirm setting the system to its default state.

    The system automatically reboots.

Reverting the System to an Alternate Image

1. Navigate to **Maintenance : System Reset**.

2. Click   .

3. Enter the reason for reverting the system.

4. Optionally, select **Reset to defaults?** to reset the system to default values.

5. Click **Yes**.

    The system automatically reboots.

Updating License Keys

Software upgrades require that a current license key be installed on the system. A current license key for upgrades is available when a maintenance agreement for the system is in effect. The license key table in **Maintenance : License Keys** lists the expiration date of the license key.

Expanding a conference up to 48 participants also requires an expanded conference license key. Contact your LifeSize reseller or LifeSize Technical Services to obtain one.

During a software upgrade, if no license key is installed on a system or the installed key has expired, the system attempts to contact the LifeSize license key server to check the license key status. You can check for updates to license keys in the LifeSize Bridge Utility if your system has HTTP access through port 80 to the LifeSize license key server. If your system does not have this access, refer to Installing a License Key Manually.

Checking for License Key Updates in the Utility

1. Navigate to **Maintenance : License Keys**.

2. Click **Update**.

   If the update is successful, **Success** appears and the current license keys and their expiration dates appear.

If the update fails, one of the following messages indicates the cause of the failure:

- License key format invalid

- License expired

- Internal system error

- Verification failed

- Validation failed

- No serial number found for this system

- No licenses found for this system

- License key server busy. Try again.

Ensure a current maintenance agreement for the system is in effect and ensure you have entered the key correctly.

Installing a License Key Manually

1. Click **Download Software** on lifesize.com/support.

2. Log in to your support account. On your first visit, create the account.

3. Follow the instructions to obtain a license key.

4. Open a separate browser window and access the LifeSize Bridge Utility.

5. Navigate to **Maintenance : License Keys**.

6. Click and paste the license key that you obtained in step 3.

7. Click **Add**.

Upgrading your System Software

Before you upgrade your system software, ensure that the system meets the following prerequisites:

*   A current license key for upgrading exists on the system. The expiration date for the upgrade license appears in **Maintenance : License Keys**. Read more at Updating License Keys.

NOTE	An upgrade fails if a current license key does not exist on the system. If a current license key does not exist, contact your authorized LifeSize Partner to renew your maintenance agreement. The renewal process can take 24 to 48 hours.

*   Terminate all calls prior to upgrading. Create a maintenance window by scheduling a conference that uses all ports and has a password that is not shared.

1. Click **Download Software** on lifesize.com/support.

2. Log in to your support account. On your first visit, create the account.

3. Follow the instructions to find the software version you want for your product, and download it to a local directory on your system.

4. Access the LifeSize Bridge Utility.

5. Click **Maintenance : System Upgrade**.

6. Browse for the upgrade file you downloaded in step 3.

    The system validates the file. To re-validate the same file or if you manually entered a path to a file, click **Validate** for the verification to occur.

7. If the validation succeeds and your upgrade requires you to reset the system to the original default settings, select **Reset to Default State**.

8. Click **Upgrade Now.**

    The upgrade can take several minutes; do not disrupt the upgrade process. During an upgrade, a status screen appears. Keep the utility window open to monitor the upgrade process. If you close the window before the file upload completes, the upload is cancelled. If you close the window after the file upload completes, the upgrade process continues, but you are no longer able to monitor the upgrade process.

    A system upgrade status message appears when the upgrade is complete and the system automatically reboots.

    If the software you are attempting to install is an older version than what is currently installed, the button appears as **Downgrade Now**.

9. Your system is ready to use. If you selected **Reset to Default State** in step 7, you must first reconfigure your system.

Troubleshooting Upgrade Failures

If attempts to upgrade software fail, follow these steps:

1. Ensure you have a valid upgrade image.

2. Reboot the system.

3. Attempt the upgrade again.

4. If a second attempt fails, note the error code returned.

5. If problems persist, contact LifeSize Technical Services or your LifeSize Partner.

Upgrade Error Codes

Following are the error codes you may receive when an upgrade fails.

Problem	Description
Upgrade script failed	After the image has been successfully uploaded, the system runs an upgrade script for final processing. This error indicates a failure in that script.
Unknown error	The upgrade failed for undetermined reasons.
Upgrade in progress	An upgrade is already in progress. The system only supports one upgrade at a time.
Bad upgrade file format	The upgrade image is corrupt and unusable. This typically occurs due to a bad image or errors during upload to the device.
Invalid signature	The encryption signature is invalid. This typically occurs if the image is corrupt or compromised.
Missing required file	The system was unable to run the upgrade script. This typically occurs due to a bad image or errors during upload to the device.
Upgrade license expired	A current license key for upgrading the system software does not exist on the device. Contact your LifeSize Partner to renew your maintenance agreement.
The system is busy	Resources were unavailable to perform the upgrade.
Must reset to defaults to install this upgrade	The upgrade requires a reset. Select the **Reset to Default Values** check box before proceeding with the upgrade.