



LifeSize[®] UVC Access[™] Deployment Guide

LifeSize UVC Access

LifeSize UVC Access is a standalone H.323 gatekeeper that provides services such as address translation and admission control, bandwidth management and routing management for H.323 calls to gateways, video communications systems and MCUs. LifeSize recommends using LifeSize UVC Access in deployments of LifeSize UVC Transit.

The guide is divided into these sections:

Planning	Presents deployment considerations.	Planning LifeSize UVC Access Deployment
Deploying	Describes tasks to configure the service for H.323 calls.	Deploying LifeSize UVC Access
Maintaining	Describes how to back up, restore, and reset the system and how to troubleshoot issues.	Maintaining LifeSize UVC Access

Related documentation is available from lifesize.com/support.

Section 1: Planning LifeSize UVC Access Deployment

LifeSize UVC Access is most commonly deployed in the LAN with the H.323 video communications systems registered to it. When deployed with LifeSize UVC Transit Client, LifeSize UVC Access must be deployed in the same LAN as LifeSize UVC Transit Client. When deployed with LifeSize UVC Transit Server alone, LifeSize UVC Access must be deployed in the DMZ.

If you deploy LifeSize UVC Access in a 1:1 static NAT, callers outside of your network must use the public IP address of LifeSize UVC Access to place calls to your video systems. Additionally, when you deploy LifeSize UVC Access with LifeSize UVC Transit in a 1:1 static NAT, the two servers must use each other's public IP address.

For more information about deploying LifeSize UVC Access with a new or existing deployment of LifeSize UVC Transit, including network diagrams for the various options, refer to the planning section of the *LifeSize UVC Transit Deployment Guide*.

Deploying LifeSize UVC Access in the DMZ with NAT

If you use 1:1 static NAT for LifeSize UVC Access, ensure **Use public address** is selected in **Configuration : H323** on LifeSize UVC Access. Configure the private IP address for LifeSize UVC Access during the initial configuration or in console mode. Specify the static NAT IP address for LifeSize UVC Access in **Configuration : Server : Signaling server public address**. When static NAT is configured, the public and private addresses appear on the LifeSize UVC Access dashboard.

Configuring Ports

The following firewall ports must be open to incoming traffic through the LAN:

- H.225 UDP port 1718 (This port is required only if you enable gatekeeper auto discovery. Open this port for multicast traffic from video communications systems.)
- H.225 UDP port 1719
- H.225 TCP port 1720
- H.245 TCP ports 37000 to 41105
- DNS port 53
- NTP port 123
- SNMP port 162
- SYSLOG port 514

For a complete description of firewall configuration details refer to the firewall section of the *LifeSize UVC Transit Deployment Guide*. Settings are identical to those for LifeSize UVC Transit Server deployed in the DMZ alone, without LifeSize UVC Transit Client.

Configuring H.460 Support

If your devices need H.460 support, deploy LifeSize UVC Transit with LifeSize UVC Access. H.460 clients must connect directly to LifeSize UVC Transit Server, which forwards call signaling to LifeSize UVC Access.

For more information about deploying LifeSize UVC Access with LifeSize UVC Transit, refer to the planning section of the *LifeSize UVC Transit Deployment Guide*.

Section 2: Deploying LifeSize UVC Access

Deploying LifeSize UVC Access includes the following tasks:

Complete installation and initial configuration.	Initial Configuration
Check for software updates and upgrade to the latest versions to ensure they are compatible.	<i>LifeSize UVC Platform Deployment Guide</i>
<i>Optional:</i> To receive calls in the Annex O format (username@domain), create H.323 local domains and DNS SRV RR records.	Annex O Dialing
If you intend to use authentication, create a user account in LifeSize UVC Access for each video system and MCU in your private network.	Creating User Accounts
Name the gatekeeper and configure authentication options.	Configuring Authentication
Configure zones to control per call and total bandwidth usage between registered devices	Configuring Zones
Configure call routing between devices.	Configuring Call Routing

Initial Configuration

1. Install the LifeSize UVC Platform hardware or virtual machine according to the instructions in the *LifeSize UVC Platform Installation Guide*.
2. Log in to the LifeSize UVC Platform interface and activate LifeSize UVC Access. Refer to the *LifeSize UVC Platform Deployment Guide*.
3. Complete the initial configuration for LifeSize UVC Access. Read more at [Enabling LifeSize UVC Access](#).
4. *Optional:* Enable auto discovery. Read more at [LifeSize UVC Access Auto Discovery](#).
5. *Optional:* To use Annex O dialing, create DNS entries.

If your organization does not manage its domain names, ask your Internet Service Provider (ISP) to do so. Refer to [Annex O Dialing](#) for more information.

6. Ensure that you can access the LifeSize UVC Access interface from your private network.

In a browser, enter the IP address or fully qualified domain name of LifeSize UVC Access on HTTPS.

`https://lifesize_UVC_access_IP_address`

`https://access.example.com`

7. Log in to LifeSize UVC Access. The default administrator credentials for LifeSize UVC Platform and all enabled services are:

Username: *administrator*

Password: *admin123*

Enabling LifeSize UVC Access

1. Open a browser and log in to the LifeSize UVC Platform. The default administrator credentials are:

Username: *administrator*

Password: *admin123*

NOTE You can create other administrator accounts. Refer to step 4 in this procedure.

2. Ensure an IP address is available for configuring LifeSize UVC Access.
 - a. Navigate to **System Settings : IP Addresses : Edit**.
 - b. Click **Add address**.
 - c. Enter the new IP address.

NOTE Press Tab to instruct the server to enter the remaining values, or enter each remaining value. Review any values entered by the server.

- d. Click **Apply Changes**.

3. Enable LifeSize UVC Access:

NOTE You must activate a license for LifeSize UVC Access before performing these steps. Refer to the *LifeSize UVC Platform Deployment Guide*.

- a. Navigate to **Operations and Maintenance : Applications enabled - Edit**.
- b. In **Enable new applications**, select **Access**.
- c. Select the IP address.
- d. Click **Enable Application**.

NOTE If LifeSize UVC Access is deployed in the DMZ or Internet, alone or with LifeSize UVC Transit Server, callers outside of your network must use the public IP address of LifeSize UVC Access to place calls to your video communications systems.

4. *Optional:* Create an administrator account for LifeSize UVC Access.
 - a. Navigate to **User Management : Users - Add**.
 - b. Enter a username and password.
 - c. Click **Save**.
 - d. In **Access Server Permissions**, select **Access Administrator**.
 - e. Click **Save**.

Annex O Dialing

This section applies to a standalone instance of LifeSize UVC Access. If you are using LifeSize UVC Access in conjunction with LifeSize UVC Transit, refer to the LifeSize UVC Transit documentation for instructions on how to enable Annex O dialing.

LifeSize UVC Access handles Annex O dialing (username@domain) to other gatekeepers and video communications devices automatically by looking up the H.323 DNS SRV records for the external systems with fallback to DNS records. Refer to the documentation for third party devices to enable them to receive Annex O calls.

To enable video systems to receive H.323 calls in Annex O format, complete the following steps:

1. Configure an H.323 local domain on LifeSize UVC Access in **Configuration : H.323 : Local Domains**.
2. Create an H.323 DNS SRV record for each domain you would like accessible from external devices. For example:

_Service._Proto.Name	TTL	Class	Priority	Weight	Port	Target
_h323ls._udp.example.com	3600	IN	0	0	1719	<Access IP address>
_h323cs._tcp.example.com	3600	IN	0	0	1720	<Access IP address>

3. Configure the local video communications systems with H.323 names without the domain extension. External video communications systems connect with the dial string <H.323 name@domain>.

If all calls go through LifeSize UVC Access or LifeSize systems, your H.323 domain does not have to resolve through DNS. LifeSize UVC Access acts as the gatekeeper for the domains. Use its IP address as the target in H.323 SRV records.

Configuring Authentication

You can configure authentication for H.225 RAS messages and Q.931 signaling messages (including SETUP messages).

Enter the authentication settings for LifeSize UVC Access in **Configuration : H.323 : Configuration**.

Label	Description
Gatekeeper ID	Name of the gatekeeper. The default is <i>LifeSize UVC Access</i> .
RAS authentication Q.931 authentication	Default is <i>None</i> . Select from the following: <ul style="list-style-type: none"> <i>Alias</i> - Caller must have a user account on the gatekeeper. This option prevents unregistered devices from calling a device registered to the gatekeeper. <i>Prefix</i> - Accepts calls with the specified prefix. <i>H.235</i> - Caller must have a user account with the correct H.235 password. This option prevents unregistered devices from calling a device registered to the gatekeeper.
Authentication prefix	Enter the prefix to use for prefix authentication. Multiple prefixes must be separated by the character.

Creating User Accounts

If LifeSize UVC Access is configured with alias or H.235 authentication, create a user account in LifeSize UVC Access for each video communications system, MCU, or instance of desktop devices that makes or receives calls. At a minimum, a registered device must have a numeric extension.

Create user accounts for LifeSize UVC Access in **Configuration : Users**. Enter the following information for each new user account.

Label	Description
H.323 extension	Required for H.323 calls. 50 numeric characters maximum.
H.323 name	An optional alphanumeric alias for the H.323 user. 50 characters maximum. Do not use the full domain name (@domain). Configure the domain in Configuration : H.323 : Local Domains .
Password	50 alphanumeric characters maximum. This is required for H.235 authentication.
Disabled	Use this option to temporarily prevent this device from registering to LifeSize UVC Access, rather than removing the device registration completely. Note: If you disable LifeSize Bridge when H.235 authentication is enabled, the device and all its conferences are disabled.

Except where noted, you can use alphanumeric characters, the period, the underscore, the tilde, and the dash. Unicode characters are not supported. Click **Show Advanced Settings** for more optional fields. The new account appears in **Configuration : Users**.

LifeSize UVC Access Auto Discovery

Auto discovery allows H.323 terminals and gateways to discover LifeSize UVC Access through 224.0.1.41:1718. To enable auto discovery in LifeSize UVC Access, navigate to **Configuration : H.323 : Advanced** and select **H.323 gatekeeper discovery**.

NOTE Auto discovery fails if the H.323 terminal or gateway uses a broadcast address and port.

Line Hunting

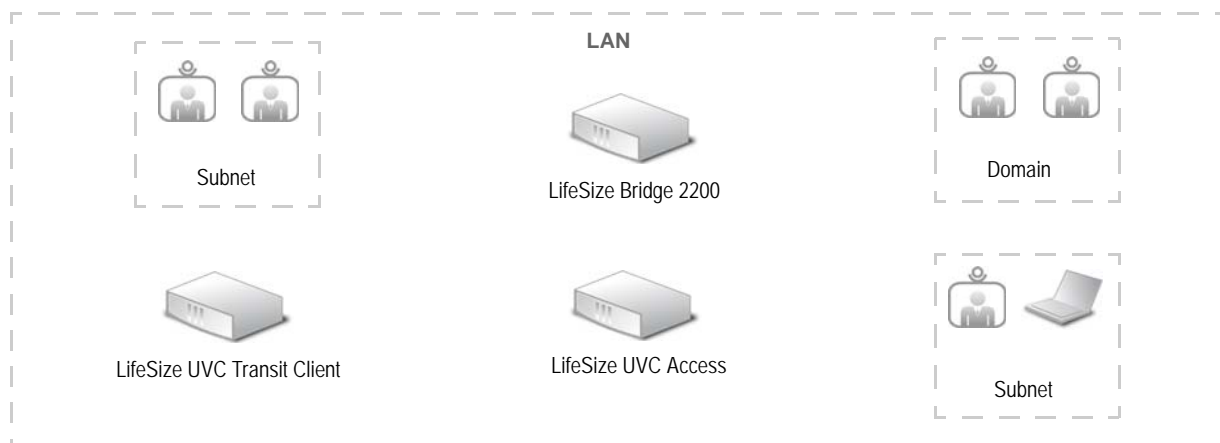
LifeSize UVC Access supports multiple gateways registered to it with the same prefix. When an incoming call uses a prefix that matches more than one gateway, LifeSize UVC Access chooses a gateway according to the following priority:

1. LifeSize UVC Access randomly selects a matching gateway.
2. If the call routed to the randomly selected gateway fails, LifeSize UVC Access tries another gateway that matches the prefix, until the call succeeds. If routing through all the gateways fails, the call fails.

This feature is available only for registered gateways. Gateways specified through **Configuration : H323 : Gateway Routing** are not supported.

Configuring Zones

By default, all devices belong to the Default Zone, and conform to the default configuration for call duration, bandwidth per call, and total bandwidth, among others. You can partition your network into different custom zones, and then apply rules to calls within those zones and between zones. You cannot rename the Default Zone, although you can adjust the other parameters.



A zone can have one or multiple members and can be defined in the following ways:

- by subnet
- by IP address
- by H.323 extension
- by H.323 name
- by DNS hostname

Most commonly, zones are defined to encompass multiple members. However, you can define a single device as its own zone. For example, you can define a zone to have as its one member, the IP address of LifeSize UVC Transit Client. All outbound calls to the Internet that pass through the client are then bound by the zone bandwidth rules.

Likewise, you can define a neighboring gatekeeper as a zone, such that all calls to that gatekeeper are bound by a specific bandwidth rule. This only applies to calls directly between the two gatekeepers. If the call passes through LifeSize UVC Transit, the rule for LifeSize UVC Transit applies.

NOTE LifeSize UVC Access can only manage zones in the network in which it is deployed. When deployed in the DMZ with LifeSize UVC Transit Server, it cannot manage zones in the LAN, except by H.323 extensions or aliases.

Adding a New Zone

Create zones for LifeSize UVC Access in **Configuration : Zones**.

1. Click **Add zone** and enter the following information for each zone:

Parameter	Description
Zone name	The zone name must be unique and limited to alphanumeric characters.
Bandwidth Limits	Use the default zone settings, no limits, or specific limits for this zone. If you set specific call bandwidth limits and a call exceeds them, it is downspeeded to the limit you specify in Auto downspeed bandwidth .
Intrazone call bandwidth	Appears when you choose Use specified zone settings for Bandwidth Limits . Enter a bandwidth limit in Kb/s for a single call within a zone.
Intrazone total bandwidth	Appears when you choose Use specified zone settings for Bandwidth Limits . Enter a bandwidth limit in Kb/s for all calls within a zone.
Interzone call bandwidth	Appears when you choose Use specified zone settings for Bandwidth Limits . Enter a bandwidth limit in Kb/s for a single call to other zones.
Interzone total bandwidth	Appears when you choose Use specified zone settings for Bandwidth Limits . Enter a bandwidth limit in Kb/s for all calls to another zone.

Parameter	Description
Auto downspeed bandwidth	Appears when you choose Use specified zone settings for Bandwidth Limits . Enter a bandwidth limit in Kb/s for calls after the total bandwidth limit for interzone or intrazone calls is exceeded. If set to zero, LifeSize UVC Access rejects any calls after total interzone or intrazone bandwidth limits are reached. Note: After upgrading from a version that did not offer this option, the value is set to half of the lowest total call bandwidth setting.
Call blocking	Use the default zone setting, disable time blocking, block all outgoing calls, or block calls at certain specified times. If you choose Use specified time intervals , you will be prompted to specify the interval after clicking to add the zone.
Authentication	Use the device's configured authentication for the call, or disable authentication for the zone.
Call restriction	Use the default zone setting, block calls to unregistered devices, or allow calls to unregistered devices.
Maximum call time	Use the default zone setting, no limit, or specify a limit for this zone.
Maximum call time limit	This option appears only if you choose to apply a limit in Maximum call time . Enter the maximum call time in seconds for this zone.




2. Click **Add**.
3. If you choose **Use specified time intervals** in **Call blocking**, click **Add call blocking time intervals** in the **Call Blocking page**.
4. Enter the day, start, and end time of the interval and click **Add**. The call blocking time interval appears in the call blocking time interval table. Repeat the process to add more time intervals.
5. When you have finished adding call blocking time intervals, click **Next**. You can click **Next** without adding any call blocking time intervals and add them later.
6. Specify members of the zone by selecting a **Member type** and specifying the appropriate identifiers.

Member Type	Identifiers
Subnet	Enter an IP address and IP mask to define the subnet. The mask must start with 255, and end with 0, 128, 192, 224, 240, 248, 252, or 255.
IP address	Enter an IP address.
H.323 extension	Enter a pattern of H.323 extensions using digits, +, and the wildcard ? for a single digit, and the wildcard * for a series of non-zero digits.
H.323 name	Enter a pattern of H.323 names using alphanumeric characters, +, and the wildcard ? for a single character, and the wildcard * for a series of characters.
DNS hostname	Enter a hostname in the form <i>example.com</i> .

7. Click **Add**. The new member type appears in the member type table. Repeat the process to add more member types.
8. Click **OK**, when finished adding member types.

Managing Zones

When your zones are configured, you can view them in a grid. Each cell lists the per call bandwidth, a colored icon, and the total call bandwidth for calls from the row's zone to the column's zone. If the zone is the same in the row and column, those numbers represent intrazone limits.

Icon	Meaning	Actions
	The limits shown are the effective limits based on the zone settings.	Click on the zone and add an override rule for calls between these zones only.
	Override rules are set for calls in this direction between these zones.	Click on the zone to edit or remove the override rule.
	Calls are blocked between these zones. This icon does not appear for zones with specified call blocking intervals.	Click on the zone to edit the call blocking settings.

Use the **Grid** view to create, edit, or remove zone to zone override settings.

Use the **List** view to edit zone settings.

NOTE If you use the **Search** option, you must leave the **Zones** page and then click on the **Zone** tab to see all the zones in the **List** view.

Use the **Zone members** view to add, edit, or delete zone members.

Examples of Calls Using Zone Rules

The following table shows the settings for the calls in the following examples:

Zones	Members	Intrazone Per Call Bandwidth	Intrazone Call Total Bandwidth	Interzone Per Call Bandwidth	Interzone Call Total Bandwidth	Downspeed Bandwidth
A	A1, A2, A3	2,000 Kb/s	4,000 Kb/s	1,000 Kb/s	2,000 Kb/s	512 Kb/s
B	B1, B2, B3	4,000 Kb/s	8,000 Kb/s	1,500 Kb/s	3,000 Kb/s	1000 Kb/s

Per Call Examples

Calls from A1 to A2 can have a maximum bandwidth of 2000 Kb/s. Calls from A1 to B1 can have a maximum a bandwidth of 1000 Kb/s.

Calls from B1 to A1 can have a maximum bandwidth of 1000 Kb/s, because the lowest interzone bandwidth rule applies unless you have applied an override rule.

Calls from B1 to B2 can have a maximum a bandwidth of 4000 Kb/s

Override Example

From the **Grid** view, apply an override rule by clicking on the cell with row Zone B, column Zone A and set the call bandwidth to 3000 Kb/s.

Calls from A1 to B1 can have a maximum bandwidth of 1000 Kb/s. Calls from B1 to A1 can have a maximum bandwidth of 3000 Kb/s

Total Bandwidth Example

Concurrent calls from A1 to B1, and from A2 to B2 consume 2000 Kb/s total bandwidth. Adding a call from A3 to B3 will downspeeded the new call bandwidth to 512 Kb/s.

Determining and Applying Zone Membership

When you specify membership in a zone by multiple types of identification, some systems may be included in multiple zones. In such cases, membership is determined by the following priority:

1. H.323 Extension
2. H.323 Name
3. DNS host name
4. IP address
5. Subnet

The bandwidth and call parameters take effect when calls are placed. The zone of the caller and the zone of the recipient are determined and the zone rules of the caller are applied to the call.

If you call a video communication device that is not registered to LifeSize UVC Access, and the device does not belong to a zone other than the default zone, the device is considered external. If the calling device belongs to the default zone, too, then the interzone bandwidth limits are used instead of the intrazone bandwidth limits (if the bandwidth mode is configured to use limits).

Authentication takes effect on registration requests. The zone of the registering video system, gateway or MCU is determined and the authentication mode of the zone is applied.

NOTE For DNS host names, zone membership is determined only for the recipient, and it takes effect only if you dial `usr@dnsname` or `@dnsname`. For all other membership parameters, the membership is determined by information in the RAS signaling.

Neighboring Gatekeeper Examples

Example 1: To place calls using the H.323 extensions of the neighboring video systems and apply specific zone rules, define an H.323 route and a zone with the appropriate H.323 extension as a zone member.

Dial string	200
Neighboring gatekeeper	1.2.3.4
H.323 route	20 -> 1.2.3.4
Zone member	20*

Example 2: To place calls using the IP address of the neighboring gatekeeper and apply specific zone rules, define a zone with the appropriate IP address as a zone member.

Dial string	1.2.3.4##200
Neighboring gatekeeper	1.2.3.4
Zone member	1.2.3.4

LifeSize UVC Transit Client Example

To place calls to any external device via LifeSize UVC Transit Client and apply specific zone rules, define a zone with the appropriate H.323 name as a zone member.

Dial string	19##122.166.122.40
LifeSize UVC Transit Client	1.2.3.4
LifeSize UVC Transit Client Outbound Prefix	19
Zone member	19*

Gateway Example

To place calls using the H.323 extensions of video systems via a gateway and apply specific zone rules, define a gateway route and a zone with the appropriate H.323 extension as a zone member.

Dial string	2001
Gateway	1.2.3.4
Gateway route	20* -> 1.2.3.4
Zone member	20*

Call Blocking

From the **Zones** list view, click on **Call Blocking** for a zone. Choose **Use default zone setting**, **Disable time blocking**, **Block all outgoing calls**, or **Use specified time intervals**. If you choose **Use specified time intervals**, click **Add call blocking time intervals** and add day and time intervals during which calls are blocked.

From the **Grid** view, you can add call blocking override settings. Click on a cell, and click **Add override rule between zones**. Choose the call blocking mode and click **Save**. If you chose **Use specified time intervals**, click **Add call blocking time intervals**, and specify call blocking time intervals.

Ensure that you have set the time and date settings in **System Settings** in the **Platform Administration** page to the correct time and time zone.

NOTE If you receive the *Failed to add call blocking* error message, ensure that the start time of the interval precedes the end time of the interval.

Configuring Call Routing

You can configure prefixes for neighboring gatekeepers, prefixes for gateways and MCUs, and rules for rewriting extension numbers for registered devices (Direct Inward Dialing).

NOTE LifeSize UVC Transit Servers, gateways, MCUs and neighboring gatekeepers can register multiple video communications systems in a bulk registration. If the license limit for registered clients is reached during a bulk registration, those registrations are accepted, but no new bulk registrations are accepted, and LifeSize UVC Access raises an event stating that the license must be updated to accommodate more license seats.

Configuring Prefixes for Neighboring Gatekeepers

Create prefixes for neighboring gatekeepers in LifeSize UVC Access in **Configuration : H.323 : Routing**. The prefix can be numeric for calls using numbers, or alphanumeric for calls using Annex O dialing, *user@host*. Calls starting with the prefix are routed to the configured gatekeeper. Enter the following information for each neighboring gatekeeper:

Label	Description
H.323 prefix	Enter a numeric prefix or domain to identify the gatekeeper.
H.323 gatekeeper	Enter the IP address of the neighboring gatekeeper.
Username	If the gatekeeper requires authentication, enter the username.
Password	If the gatekeeper requires authentication, enter the password.

Configuring H.323 Phone Routing

LifeSize UVC Access can modify the incoming E.164 numbers (standard telephone numbers) to correspond to the extension of registered devices or dial plans of external gatekeepers (Direct Inward Dialing). Configure the translation rules in LifeSize UVC Access in **Configuration : H.323 : Phone routing**.

Label	Description
Matching expression	<p>This is the formula for converting the expression you expect to receive from the calling device. The matching expression can contain digits, +, ?, and *.</p> <p>? is a wildcard and is not included in the result expression.</p> <p>* matches one or more digits and the matching digits are placed in the result expression. Any character after the * (including additional *s) is ignored. * can appear anywhere in the result expression.</p> <p>Dashes (-) are removed from numbers and expressions.</p> <p>+ is a matching digit (+44* does not match 44*), but can only be present first in a number or result expression.</p>
Result expression	<p>This defines the output of the expression modification. Use * anywhere in the expression. All characters the * character matched from the input dial string are inserted.</p>

DID (PBX mode) Example

External calls use a prefix or exchange with an extension, where internal devices use just the extension. Remove the prefix or exchange.

External Dial String	Internal Extension	Matching Expression	Result Expression
22181801	1801	2218*	*
555-1209	1209	555*	*

Breakout Prefix Example

Recognize 9 as a breakout prefix to international calls over a gateway at IP address 1.2.3.4. Remove the prefix 9, add the prefix 00 and route to 1.2.3.4.

Original Dial String	Resultant Dial String	Matching Expression	Result Expression
991555	0091555@1.2.3.4	9*	00*@1.2.3.4

Configuring Routing to Gateways and MCUs

Route calls with known prefixes to gateways and MCUs that are not registered to LifeSize UVC Access in **Configuration : H.323 : Gateway routing**. Enter the following information for the gateway or MCU.

Label	Description
Prefix	Enter a numeric prefix to identify the gateway or MCU.
Address	Enter the IP address of the gateway or MCU.

Direct IP Dialing without Outbound Prefix

If you are using LifeSize UVC Access with LifeSize UVC Transit Server and LifeSize UVC Transit Client, any video communications system registered to LifeSize UVC Access can dial unregistered public systems without prefixes.

From LifeSize UVC Access navigate to **Configuration : H.323 : Configuration** and select **Route outgoing public calls through UVC Transit Client**. This feature is enabled by default.

Example Dial Strings

When this feature is enabled, dial the IP address of the public system. When the feature is disabled, you must use a dial string of the following form:

<outbound prefix>##< Public system IP address>.

CAUTION Prepending the prefix directly onto the IP address may produce a valid but incorrect IP address and the call fails.

Section 3: Maintaining LifeSize UVC Access

Maintenance Mode

To perform maintenance and configuration, you must first enter maintenance mode in **Maintenance : Maintenance Mode : Enter maintenance mode**. Maintenance mode puts the service into a suspended state and prevents new calls from connecting and new devices from registering. **Enter maintenance mode** waits until the last current call ends and then enters maintenance mode. The **Force maintenance mode** option immediately disconnects all current calls, deregisters all devices, and enters maintenance mode.

Back Up, Restore, Reset

From maintenance mode in LifeSize UVC Access, navigate to **Maintenance : System** and select *Back Up*, *Restore*, or *Reset* to create a backup file, restore from a backup file, or reset the service to factory defaults, respectively.

Troubleshooting and Diagnostics

Following are common issues that you may encounter with LifeSize UVC Access.

Issue	Workaround
Previous version of the interface persists after upgrade.	Clear the browser cache to load the new interface.
Invalid DNS configuration.	LifeSize UVC Access may fail to function properly if it is not configured to use a valid, available DNS server. Ensure that you have properly configured the DNS settings on LifeSize UVC Platform and that the DNS server is available.
Calls and registrations fail with H.235 authentication.	Check that your NTP server setting is valid.

Call Status Page

In LifeSize UVC Access, navigate to **Status : Calls : All calls** to view active and ended calls. Click **Ended calls** to view ended and failed calls. The following details are available for a call:

Order	Call number.
Caller ID	Name of the caller.
Caller IP address	Public address of the device or the address of a remote gatekeeper if the internal address is hidden.
Recipient ID	Name of the called device.
Recipient IP address	IP address of the called device. This may also be the address of a remote gatekeeper.
Duration	Length of the call.
Status	Active or inactive.
Details	Includes additional information about the call, including the originating and terminating user IDs, IP addresses, and client types, and details about the originating and terminating media.

You can download call detail records (CDRs) for all calls. A new CDR file is created for each day at the time a call fails. Files are not created if no calls are placed. The newest call appears first in the UI. To access the CDRs, follow these steps:

1. Navigate to **Status : Calls : All calls**.
2. Download a compressed file, `cdr.tar.gz`, containing all CDR files for each day.
3. Use the REST API to retrieve all CDR records for a specified date using the following URL:

`https://uvcaccess-signaling-ip/uvcaccess/v1/callstatus/YYYY:MM:DD`

NOTE Knowledge about scripting and REST is required for using this interface. For example, you can use the 'curl' command and python for parsing the JSON output:

```
curl -k --basic -u administrator:admin123 https://10.93.1.133/access/v1/
callstatus/2012:11:20 | python -mjson.tool
{
  "call_list": [
    {
```

```

"call_active_status": "Inactive",
"call_failed": false,
"call_id": "24de5be473fd11dab1470013fa03e483",
"count": 1,
"duration": "0:0:23",
"originating_address": "10.93.1.34",
"originating_clienttype": "LifeSize Express 220 4.11.4.23",
"originating_endreason": "USERS_DISCONNECT",
"originating_userid": "400u",
"protocol": "H.323",
"start_time": "2012:11:20-16:45:18",
"terminating_address": "10.93.1.50",
"terminating_clienttype": "LifeSize Express 220 4.11.4.23",
"terminating_endreason": "NORMAL",
"terminating_userid": "10.93.1.133:1720"
}
],
"call_status": {
"active_call_count": 0,
"placed_call_count": 1
}
}
}
Events

```

LifeSize UVC Access can send email or SNMP traps when certain events occur. To configure these notification options, navigate to **Configuration : Events**.

Email Event Notification

SMTP server	The outgoing SMTP server address.
Username	Authenticates at the SMTP server.
Password	Authenticates at the SMTP server.
Recipients	The mail address of the recipients (separated by a comma).

SNMP Trapping Events

Trap receiver address	The IP address of the SNMP trap receiver.
------------------------------	---

Viewing Events on LifeSize UVC Access

To view events on the server, navigate to **Status : Events**.

Field	Description
Order	Event number.
Event name	Logical name of the event.
Severity	Severity of the event (corresponds to the log level for each event). Refer to Log Files .
Information	Textual explanation of the event.
Time of event	Timestamp when the event was raised.
Customer ID	ID of the customer.
Clear	Clears the event.

Log Files

LifeSize UVC Access logs events to a file for download.

Navigate to **Configuration : Logs** for controls to set the log levels and indicate the system log host.

Navigate to **Status : Logs** for a list of available log files.

LifeSize Technical Services may instruct you to download and send these files to LifeSize for analysis.

Copyright Notice

©2013 Logitech, and its licensors. All rights reserved.

LifeSize Communications, a division of Logitech, has made every effort to ensure that the information contained in this document is accurate and reliable, but assumes no responsibility for errors or omissions. Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless noted. This document contains copyrighted and proprietary information which is protected by United States copyright laws and international treaty provisions. No part of the document may be reproduced or transmitted, in any form or by any means, electronic or mechanical, for any purpose, without the express written permission from LifeSize Communications.

Trademark Acknowledgments

LifeSize, the LifeSize logo and other LifeSize marks, are registered trademarks or trademarks of Logitech. All other trademarks are the property of their respective owners.

Patent Notice

For patents covering LifeSize® products, refer to lifesize.com/support/legal.

Contacting Technical Services

LifeSize Communications welcomes your comments regarding our products and services. If you have feedback about this or any LifeSize product, please send it to feedback@lifesize.com. Refer to lifesize.com/support for additional ways to contact LifeSize Technical Services.