Contents

1 Introduction .................................................................................................................. 6
  1.1 How to Use this Guide ............................................................................................ 7
    1.1.1 Commands ........................................................................................................ 8
    1.1.2 Management and network interfaces ................................................................. 8
  1.2 Application Programming Interface ...................................................................... 9

2 General Concepts & Prerequisites ........................................................................... 10
  2.1 Prerequisites ........................................................................................................... 10
    2.1.1 DNS configuration ............................................................................................ 10
    2.1.2 Security certificates ......................................................................................... 10
    2.1.3 Firewall configuration ...................................................................................... 10
    2.1.4 Remote Syslog server ..................................................................................... 10
    2.1.5 Network Time Protocol Server ....................................................................... 11
    2.1.6 Call Detail Record Support ............................................................................. 11
    2.1.7 Host name ......................................................................................................... 12
    2.1.8 Other requirements .......................................................................................... 12
    2.1.9 Acano X series server-specific prerequisites ................................................... 13
    2.1.10 Virtualized deployment-specific prerequisites ............................................... 13
  2.2 General Points about Acano solution Components ............................................. 14
    2.2.1 Support for Lync clients ................................................................................... 14
    2.2.2 Deploying Acano clients .................................................................................. 14
    2.2.3 Acano Web Bridge ........................................................................................... 16
    2.2.4 Acano TURN Server ....................................................................................... 16
    2.2.5 Diagnostics and Troubleshooting ................................................................... 16
  2.3 General Points about Scalability & Resilience ..................................................... 16
    2.3.1 Example using “combined” servers ................................................................ 17
  2.4 Scalability and Resilience Components ................................................................ 18
    2.4.1 Example using split deployments and geo-distribution ................................. 19
    2.4.2 coSpace database concepts .............................................................................. 21

3 Configuring the MMP ................................................................................................. 22
  3.1 Creating and Managing MMP and Web Admin Interface User Accounts .......... 22
  3.2 Upgrading Software ............................................................................................... 22
  3.3 Checking the Web Admin Interface for HTTPS Access ....................................... 23
  3.4 Configuring the Call Bridge Listening Interface .................................................. 24
  3.5 Configuring the XMPP server ................................................................................ 24

4 Configuring the coSpace Databases ......................................................................... 27
  4.1 coSpace Database on a Separate Server .............................................................. 27
    4.1.1 Requirements for a coSpace database on a separate server ......................... 27
    4.1.2 Deploying a coSpace database on a separate server ...................................... 27
  4.2 Deploying Certificates on the coSpace Database and Call Bridge Servers ........ 28
  4.3 Selecting the Master coSpace Database for a Cluster ......................................... 28
  4.4 Attaching other Database Instances to the coSpace Database Cluster .............. 29
  4.5 Connecting Remote Call Bridges to the coSpace Database Cluster ................... 31
  4.6 Upgrading the database schema .............................................................................. 32
11.4.2 VCS configuration .................................................................................................................. 70
11.4.3 Acano solution configuration .................................................................................................. 70
11.5 Integrating Acano Clients with SIP and Lync Clients ............................................................. 71
11.6 Lync Edge Server Integration .................................................................................................. 71
11.6.1 Lync Edge Call Flow ........................................................................................................... 71
11.6.2 Configuration for using Lync Edge ....................................................................................... 72
11.7 Lync Federation ....................................................................................................................... 74

12 LDAP Configuration .................................................................................................................. 75
12.1 Why use LDAP? ....................................................................................................................... 75
12.2 Acano Solution Settings ......................................................................................................... 75
12.3 Example .................................................................................................................................. 78
12.4 More Information on LDAP Field Mappings ......................................................................... 80

13 Additional Security Considerations & QoS ............................................................................. 81
13.1 Common Access Card (CAC) integration .................................................................................. 81
13.2 Online Certificate Status Protocol (OCSP) ............................................................................. 81
13.3 FIPS ....................................................................................................................................... 81
13.4 TLS Certificate Verification ...................................................................................................... 82
13.5 User Controls ........................................................................................................................... 82
13.6 Firewall Rules ......................................................................................................................... 82
13.7 DSCP ..................................................................................................................................... 82

Appendix A DNS Records Needed for a Scalable and Resilient Acano Solution ......................... 84
Appendix B Ports Required for a Scalable and Resilient Deployment ............................................ 86
Appendix C Unclustering ................................................................................................................ 90
Unclustering Call Bridges ................................................................................................................ 90

Appendix D Example of Configuring a Static Route from a Lync Front End Server ............... 91
Lync Configuration Changes ........................................................................................................... 91
Acano Solution Configuration ......................................................................................................... 92

Appendix E API Examples ............................................................................................................. 93
Creating an Outbound Dial Plan Rule for a Specific Call Bridge in a Cluster ............................. 93
Setting up Web Bridges on the Call Bridge ..................................................................................... 95
Creating Web Bridge Customization on a Call Bridge ................................................................. 96
Setting up Turn Servers on a Call Bridge ...................................................................................... 97
Creating a coSpace with the API .................................................................................................... 98
Creating a coSpace Member for a coSpace ................................................................................... 98
Creating Call Leg Profiles ............................................................................................................. 99

Figures
Figure 1: Combined vs. split Core & Edge deployments ................................................................. 6
Figure 2: Overview of guides covering the Acano solution.......................................................... 8
Figure 3: Example Call flow diagram ......................................................................................... 15
Figure 4: Simplest scaled and resilient configuration ................................................................. 17
Figure 5: Simple deployment showing connections .................................................................. 19
Figure 6: Split Core and Edge servers showing new location of XMPP server ......................... 20
Figure 7: Multi Core & Edge server deployment ....................................................................... 20
Figure 8: Co-located Call Bridges are automatically connected ................................................ 29
Figure 9: Attaching coSpace databases ....................................................................................... 30
Figure 10: Example of coSpace database clustering and Call Bridge connections ...................... 32
Figure 11: Mesh configuration for SIP Call Control ................................................................. 37
Figure 12: Geographical configuration example for SIP Call Control ....................................... 37
Figure 13: Trunk and Load Balancer listening ports in a split deployment ................................. 41
Figure 14: Load balancers configured in a split deployment ...................................................... 44
Figure 15: Web Bridges configured in a split deployment ......................................................... 48
Figure 16: TURN server public IP address ............................................................................... 50
Figure 17: TURN servers configured in a split deployment ........................................................ 52
Figure 18: Two PC Clients making calls to different coSpaces in a combined deployment ........ 53
Figure 19: Two PC Clients making calls to different coSpaces in a split deployment ................ 54
Figure 20: Two Call Bridges calling coSpace A in a combined deployment ............................. 56
Figure 21: Two Call Bridges calling coSpace A in a split deployment ....................................... 57
Figure 22: Example media flows and views when PC Clients dial into coSpace A in a combined deployment .................................................................................................................. 58
Figure 23: Example media flows and views when PC Clients dial into coSpace A in a split deployment ....................................................................................................................................... 59
Figure 24: Example solution for dial plan configuration ............................................................ 60
Figure 25: Example of SIP video endpoints calling into an Acano Server hosted calls ............ 61
Figure 26: Example Lync clients calling into Acano server hosted meetings .......................... 65
Figure 27: Example of SIP video endpoints and Lync clients calling into Acano server hosted meetings ........................................................................................................................................ 66
Figure 28: Example of SIP video endpoints and Lync clients in calls ....................................... 69
Figure 29: Call Bridge to Lync Edge Server Call Flow ............................................................. 72
Figure 30: Ports that must be open in an Acano solution deployment ........................................ 86
Figure 31: Additional ports required to be open in an Acano multiple deployment solution deployment ........................................................................................................................................ 87
# Introduction

**Note:** This version of the Deployment guide has a number of sections related to certificates removed and therefore has been slightly reorganized. The information is now in a new Certificates Guidelines document for the scalability & resilience deployment solution. See section 1.1.

This document covers the Acano solution deployed as a scalable and resilient solution. It provides an overview of how the Acano solution provides these features when you deploy more than one Acano server. The servers can be Acano X3 or X2 servers, be hosted on virtual machines (VM) or be a combination; the term “Acano server” in this document covers all.

This document discusses the concepts, requirements and how to deploy this type of architecture. By deploying more than one host server as described here you can configure:

- Several components of the same type to work as one resilient “unit”; for example if one Call Bridge goes down, meetings can be hosted on the other(s)
- Scalability (increased capacity); for example, one meeting can be hosted across Call Bridges if one does not have enough capacity to host all the participants. (As a general principle, when possible, each meeting is hosted on a single Call Bridge)
- Efficiency; the Acano solution decides which components to use to provide effective and efficient meetings; for example, participants calling into a meeting from different locations can use different components while keeping the user experience of a simpler deployment

When deploying for scalability and resilience, use the API rather than the Web Admin Interface when possible: in some cases it is a necessity, and instructions are provided in this document.

- Install the Acano X series server or virtualized solution following the appropriate Installation Guide
- Each Acano server can host all the components of the Acano solution or be an Edge or Core server (part of a “split deployment”)

![Figure 1: Combined vs. split Core & Edge deployments](image)

**Figure 1: Combined vs. split Core & Edge deployments**
1.1 How to Use this Guide

This guide follows on from the appropriate Installation Guide(s) (see the figure below)—and assumes that you have completed the instructions there already.

The guide provides two examples, the smallest resilient deployment configuration that we recommend and a more comprehensive example.

This deployment guide is intended to be read and acted upon in the order provided. Between versions 76-1040-03-C and 76-1040-03-D information on certificates has been moved to a new Certificate Guidelines document for the scalability & resilience solution; for example the previous appendix C and D.

In addition within the body of the document, sections about certificates have been reduced to one step and a reference to the new document; section 3 Creating and Installing Certificates no longer exists and information in it for each component has been moved to another section so that all the Web Bridge configuration (for example) is together. This provides one place for all certificate information, another for the configuration relating to each component and reduces duplication.

In addition to this deployment guide and the Certificate Guidelines, the reference material shown in the figure below can be found at the Acano Documentation & software page. If you need any technical assistance with the configuration, or you want to report a suspected bug, email support@acano.com.
1.1.1 Commands

In this document, commands are shown in black and must be entered as given—replacing any parameters in <> brackets with your appropriate values. Examples are shown in blue and must be adapted to your deployment.

1.1.2 Management and network interfaces

There are two layers to the Acano solution: a Platform and an Application.

- The Platform is configured through the Mainboard Management Processor (MMP). The MMP is used for low level bootstrapping and configuration via its a command line interface.

  Note: On the Acano X series servers the MMP can be accessed via the serial Console port or using SSH on the Ethernet interface labeled Admin. In the virtualized deployment the MMP is accessed on virtual interface A.

- The Application runs on this managed platform with configuration interfaces of its own. The application level administration (call and media management) is done via the Call Bridge’s Web Admin Interface which can be configured to run on any one of the Ethernet interfaces.

On the Acano X series servers there are five physical Ethernet interfaces labeled Admin, A, B, C and D. In the virtualized deployment one Ethernet interface (A) is created but up to three more can be added (B, C and D).
Introduction

Note: There is no physical separation between the media interfaces A-D on an X series server but the Admin interface is physically separate. Each interface is configured independently at the IP level. IP forwarding is not enabled in either the Admin or host IP stack.

See the appropriate (Acano X series or virtualized deployment) Installation Guide for details.

1.2 Application Programming Interface

The Acano solution supports an Application Programming Interface (API). The API uses HTTPS as a transport mechanism and is designed to be scalable in order to manage the potentially very large numbers of active calls and coSpaces available in the Acano solution.

The API includes LDAP server access methods for adding, configuring and modifying LDAP servers and support for multi-tenancy for searching calls through an additional Tenant ID. Other additions include posting to coSpace message boards, the ability to filter the set of active call legs to just those experiencing "alarm" conditions (for example, packet loss or excessive jitter) and the ability to retrieve system-wide status values.

Multi-tenancy means that groups of users can be entirely segmented within the solution as required by service provider deployments e.g. users will only be able to meet, assign users to coSpaces, and search in the directory within the same configured customer groups.

Refer to the Acano API Reference guide for more details.
2 General Concepts & Prerequisites

2.1 Prerequisites

The list of items you need prior to installing and configuring the Acano solution in a typical customer environment is given below; some of these items can be configured beforehand:

2.1.1 DNS configuration

The Acano solution needs a number of DNS SRV and A records. See this appendix for a full list but specific records are also mentioned elsewhere.

DNS names can be configured to resolve to multiple IP addresses with priority and weighting to each. In advanced configurations, the result of the DNS resolution can be set up to be dependent on the location of the requestor.

2.1.2 Security certificates

You will need to generate and install X.509 certificates and keys for Acano services which use TLS; for example, Call Bridge, Web Admin Interface (the Call Bridge’s interface), Web Bridge, the XMPP server and the Load balancer if used.

The new Certificates Guidelines for scalable and resilient deployments contains both background information on certificates and instructions, including how to generate self-signed certificates using the Acano solution’s MMP commands. These certificates are useful for testing your configuration in the lab. However, in a production environment we strongly recommend using certificates signed by a Certificate Authority (CA).

Instructions that were previously in this guide concerning certificates have been removed and replaced by a single step referencing the new guide.

Note: If you self-sign a certificate, you may see a warning message when you use it that the service is untrusted. To avoid these messages re-issue the certificate and have it signed by a trusted CA: this can be an internal CA unless you want public access to this component.

2.1.3 Firewall configuration

See the appendix on Ports required for a summary of the firewall changes you may need to make, and the section on Firewall rules

2.1.4 Remote Syslog server

Configure the Acano solution to use one or more remote Syslog servers to store the log files because they contain more detailed logging than is available on an Acano server’s own internal log page. (These details are valuable when troubleshooting). All host servers (combined, Edge and Core) should be configured to send debug information to a Syslog server. This can be to a single Syslog server or to multiple servers; however, if you are using any form of clustering then all servers must use the same Syslog server to aid troubleshooting. Remember to look in the logs for all the Acano servers involved in your issue.
Note: The Syslog server uses TCP not UDP.

Follow the instructions below on each Acano server to define a Syslog server.

1. SSH into the MMP and log in.

2. Enter the following command, `syslog server add <server address> [port]`
   
   Examples:
   ```
   syslog server add syslog01.example.com 514
   syslog server add 192.168.3.4 514
   ```

3. Enable the Syslog server by entering:
   ```
   syslog enable
   ```

4. Optionally, if you want to send the audit log to a Syslog server follow these steps.

   (The audit log facility records configuration changes and significant low-level events. For example, changes made to the dial plan or coSpace configuration via the Web Admin Interface or the API are tracked in this log file, and tagged with the name of the user that made the change. The file is also available via SFTP.)

   a. Create a user with the audit role.
      ```
      user add <username> (admin|crypto|audit|appadmin)
      ```
      ```
      user add audituser audit
      ```

   b. Log out of the MMP and log back in with the newly created user account.

   c. Enter the command (this command can only be run by a user with the audit role):
      ```
      syslog audit add <servername>
      ```
      ```
      syslog audit add audit-server.example.org
      ```

   Note: Normally Syslog files are overwritten in time but you can permanently store system and audit log files using the new `syslog rotate <filename>` and `syslog audit rotate <filename>` commands. See the MMP Command Reference.

2.1.5 Network Time Protocol Server

Configure one or more Network Time Protocol (NTP) servers to synchronize time between the Acano components and ensure that timings in the logs are consistent:

On each Acano server:

1. If necessary, SSH into the MMP and log in.

2. To set up an NTP server, type:
   ```
   ntp server add <domain name or IP address of NTP server>
   ```

   To find the status of configured NTP servers: type `ntp status`

   See the MMP command reference for a full list of `ntp` commands.

2.1.6 Call Detail Record Support

The Acano solution generates Call Detail Records (CDRs) internally for key call-related events, such as a new SIP connection arriving at the server, or a call being activated or deactivated. It can be configured to send these CDRs to a remote system to be collected and analyzed. There
is no provision for records to be stored on a long-term basis on the Acano solution, nor any way to browse CDRs on the Acano server. If you are using Acano Manager, it must be your CDR receiver. Both Acano servers should use the same CDR receiver.

The CDR system can be used in conjunction with the API, with the call ID and call leg IDs values being consistent between the two systems to allow cross referencing of events and diagnostics.

The CDR receiver is defined in the Web Admin Interface of each Acano server; see the Acano solution CDR Guide for more information.

2.1.7 Host name

The hostname must be set for each Acano server:

3. If necessary, SSH into the MMP and log in.

4. Type:
   ```sh
   hostname <name>
   hostname london1
   hostname mybox.example.com
   ```

5. Type:
   ```sh
   reboot
   ```

Note: A reboot is required after issuing this command.

2.1.8 Other requirements

- Access to an LDAP server to import users. From R1.6 this can be an Active Directory server or an OpenLDAP server.

  You must have an LDAP server to use the Acano solution. User accounts are imported from the LDAP server. You can create user names by importing fields from LDAP as described later. The passwords are not cached on the Acano solution, a call is made to the LDAP server when an Acano client authenticates, and therefore passwords are managed centrally and securely on the LDAP server.

- Decision on a dial plan to use to reach calls hosted on the Call Bridge. The dial plan will depend on your environment; that is whether you are making one or more of the following types of call: Lync, SIP (including voice) or Acano client calls. Instructions for deploying this dial plan are given in this document. Dial plans for scalable and resilient deployment must be set up via the API.

- Access to one or more of the following to test the solution: Lync clients, SIP endpoints phones and/or Acano clients as appropriate.

- Access to a SIP Call Control platform if you intend to make SIP calls (for example, using Cisco VCS) to make dial plan configuration changes. The changes required to set up these SIP trunks (e.g. resilient trunks from a device such as Cisco VCS into one or more Call Bridges) are given in this document.

Note: Information on setting up the SIP Trunk to a Cisco Unified Communications Manager (CUCM), the Avaya CM and Polycom DMA has been removed from appendices in this version of the Deployment guide. The information is now in a new Third Party Call Control Guide available on acano.com/support.
Note: You can use other call control devices not listed in the Third Party Call Control Guide.

- If you intend to integrate with an audio deployment, access to a Voice Call Control device and this device must be attached to a PBX; it is not possible to connect an Acano server directly to a PBX.

- If deploying in a Lync environment, access to the Lync Front End (FE) server to make dial plan configuration changes there. The changes required are given in this document.

The Acano solution R1.6 integrates with more than one Lync Front End (FE) server: for the incoming (Lync to Acano) direction, each Lync FE pool can be configured to point to a DNS record that resolves to multiple Call Bridges. Failover happens via DNS; Lync will try each result in turn. For geographic distribution, we assume that the Lync FE pools are geographically distributed and the most logical approach is to point each Lync FE pool to a different set of Acano Call Bridges co-located in the same region.

For the outgoing direction, via DNS the Acano dial plan can be configured to resolve to multiple Lync FE servers or the Lync Director. Each Acano region can be configured to point to a different FE pool.

Any production environment which also has a Lync deployment requires certificates that are trusted by the Lync FE server.

2.1.9 Acano X series server-specific prerequisites

- A suitable environment: refer to the Hardware/Environmental Data Sheet for details on the required power and cooling.

- The Acano X series server has two power modules, and country-specific power cables are supplied for the AC power supplies. At installation you must connect both cables to a power supply socket to implement power supply redundancy (or even to separate power supplies), but the server will work with just a single power unit connected.

- 2U of rack space if using the rack mounting kit; 3U of rack space if installing on a shelf.

- A minimum of two Ethernet links:
  - One for the MMP (labeled Admin on the back of the Acano Server). The speed can be 100M or 1G.
  - One for a media interface (there are four labeled A to D). The speed can be 1G or 10G.

IP addresses can be configured statically or automatically via DHCP or SLAAC/DHCPv6. Ethernet links will operate at the speed of the network switch; the switch port should be set to auto negotiate speed. If you are using a speed of 10G be sure to use the appropriate cable. See the Acano solution X series Server Installation Guide for full details.

2.1.10 Virtualized deployment-specific prerequisites

- A qualified host server with some specific resources. See the Acano solution Virtualized Deployment Installation Guide for full details.

- A license for the XMPP server(s). The license for the XMPP server is shipped with Acano Servers (X1, X2 and X3) but a license is required if you are enabling an XMPP server on a virtual host server. The license is tied to the MAC address and therefore cannot be moved from server to server – email support@acano.com with the MAC address.
2.2 General Points about Acano solution Components

2.2.1 Support for Lync clients
You can use both Lync 2010 and 2013 clients connected to a Lync 2010 or 2013 server.
The Acano solution uses:

- the RTV codec transcoding up to 1080p with the 2010 Lync Windows client and 2011 Lync Mac clients
- the RTV codec and H.264 with the 2013 Lync Windows client

Lync 2010 and 2013 clients can share content. The Acano solution transcodes the content from native Lync RDP into the video format used by other participants in the meeting and sends it as a separate stream. Lync clients receive content from the meeting in the main video.
The Lync FE Server will need a Trusted SIP Trunk configured to route calls originating from Lync endpoints through to the SIP video endpoints i.e. to route calls with destination in the SIP video endpoint domain through to the Call Bridge.
The SIP Call Control will require configuration changes to route calls destined to the Lync client domain to the Call Bridge so that SIP video endpoints can call Lync clients.
The dial plan routes Lync calls between these two domains in both directions.
The Acano solution includes support for Lync Edge to enable Lync clients outside of your firewall to join coSpaces.

2.2.2 Deploying Acano clients
If you are using any of the Acano clients you need to enable the XMPP server (combined deployments) or the Load Balancer, trunk and XMPP server (split deployments), refer to the sections on XMPP Server configuration and Deploying the trunk and Load Balancer. If you are not using the Acano PC Client, iOS Client for iPhone and iPad, Mac or WebRTC Client, disregard all sections referring to the XMPP server.
The Load Balancer provides a single point of contact for Acano clients in split deployments. It listens on an external interface and port (as described in the XMPP client SRV record) for incoming connections. Equally, the Load Balancer accepts incoming TLS connections from the XMPP server over which it can multiplex TCP connections from external clients. This creates a TLS trunk between the Core and the Edge.
The Load Balancer does not require a license.
The following diagram shows example control and media flows during an Acano client call in a split deployment.
Figure 3: Example Call flow diagram

Notes on the figure:

The following ports must be open:

- UDP Port 3478 from Call Bridge to TURN server (for TURN)
- UDP Port 50000-51000 from Call Bridge to TURN server (for media)
- TCP Port 443 (HTTPS) from Call Bridge to Web Bridge (for guest login)

* Although the range between the TURN server and the external Acano clients is shown as 32768-65535, currently only 50000-51000 is used. A wider range is likely to be required in future releases.
Internal clients connect directly to the XMPP server on port 5222 and media connects directly between the Acano client and the Call Bridge.

External Acano clients establish a control connection to the Load Balancer (black line). Media can go directly from the Acano client to the Call Bridge (dashed blue line) or be relayed via the TURN server if required (blue line).

Both internal and external Acano clients use ICE/TURN to find suitable candidates for connectivity and choose the best: in the case of internal clients this will always be the local host candidates on the internal network.

The necessary ports need to be open on the firewall between Core and Edge components to allow the media UDP traffic to pass (UDP ports 32768 - 65535) and the trunk between the Load Balancer and the XMPP server. The Web Bridge uses port 443 (and optionally port 80).

Separate internal and external SRV records for the XMPP service need to be configured, directed to the two interfaces on the Core server/virtualized server that the XMPP server is listening on. The Call Bridge to XMPP connection should also use the XMPP server’s internal address.

### 2.2.3 Acano Web Bridge

If you are using the Acano WebRTC Client you will need to enable and configure the Acano Web Bridge, refer to the section on configuring the Web Bridges. Acano WebRTC Client works on HTML5-compliant browsers and uses the WebRTC standard for video and audio. For a list of tested devices see the Acano solution Support FAQs document.

### 2.2.4 Acano TURN Server

To use Acano clients separated from the Acano solution by a firewall or NAT you need to enable the TURN server, refer to the section on configuring the TURN servers. The TURN server provides firewall traversal technology.

### 2.2.5 Diagnostics and Troubleshooting

In addition to using a Syslog server it is also possible to enable additional SIP tracing using the Logs > Call Diagnostics page in the Web Admin Interface. These logs may be useful when investigating call setup failure issues for SIP endpoints and should be disabled at all other times. To prevent the verbose logging being enabled for longer than necessary, it automatically shuts off after a choice of 1 minute, 10 minutes or 30 minutes. Refer to the Acano Support FAQs on the Acano website for more troubleshooting information.

### 2.3 General Points about Scalability & Resilience

For scalability and resilience the Acano solution can be deployed with:

- Multiple combined servers (Acano X series servers, virtualized servers or a combination). The location of these servers will depend on your requirements, possibly one at each point of presence—although this is not a requirement

  When scaling to a large deployment, it is not necessary (and not always recommended) to have every component enabled on every instance: this is discussed more fully later.
- Multiple Edge and/or Core servers (Acano X series servers, virtualized servers or a combination). The location of these Edge and Core servers will depend on your requirements, possibly co-locating Core and Edge servers in the same data center—although this is not a requirement.

- In a large split deployment it is not necessary, or even desirable, to have the same number of Edge and Core servers. For example, one Call Bridge can manage multiple Web Bridges; those Web Bridges can be reachable externally with a single DNS name resolving to potentially multiple separate units.

2.3.1 Example using “combined” servers

There are many topologies in which to deploy the Acano solution but a simple example is shown below: this provides resilience and double the capacity of a single host server solution.

![Diagram showing two host servers each with all the components enabled except for the XMPP server on the New York Acano Server, and a third host server with just a coSpace database that is likely to be a virtualized (VM) host. The location of this host is immaterial to the deployment. For a coSpace database VM host we recommend:

- Enabling hyper-threading
- Not changing any of the default ESXi system parameters

(Be sure you have the license file for the VM host loaded.)

Note: The third database instance is recommended for stability; while it is theoretically possible to have a database cluster of two, a third database aids failover.

Such an implementation can therefore provide:

- Consideration of geographic location
Resilience because if any one component is unavailable at the time that a call starts, its “partner” will be used

Similarly, if a component becomes unavailable during a call, while the call will drop for any PC/WebRTC Client using it — if the participant calls in again, a new call with a new route will be established and the participant can re-join the call remaining unaware of the new route.

Ability to scale by using both Call Bridges seamlessly

### 2.4 Scalability and Resilience Components

Looking at the previous figure and the communication between servers further:

- The three coSpace database servers are clustered using the MMP as described [later](#).
  - In R1.6, the coSpace databases are run in a different operational mode to that in previous releases. (Therefore, if you are upgrading to R1.6, you must take a backup before upgrading)
  - Clustered databases have their contents synchronized
- Each coSpace database can be on the same server as one of the Call Bridges (recommended in most deployments), on a separate virtualized server or as shown in the previous figure, on a combination

#### Notes:

In a large deployment with several Core servers, it is not necessary to have a coSpace database instance for every Call Bridge; rather we recommend one at every point of presence (POP). (For example, you may want the database in a local data center where you can control physical access but require Call Bridges around the world.

- The two Call Bridges are clustered using the Web Admin Interface as described later. In addition, they are aware of the TURN server and Web Bridge on the other host server, and the XMPP server on the London host. They also connect to the coSpace database cluster to read from and write to it

#### Note:
Clustered Call Bridges cannot use the same coSpace database (or database cluster) as a non-clustered Call Bridge.

Each Call Bridge provides CDRs for the call legs that it is hosting. Each CDR identifies the coSpace ID so you can identify the same meeting on different Call Bridges by collecting together calls with the same coSpace ID

- The two Web Bridges are configured using the API as described [later](#)
  - The Web Bridge services can be configured to have a single DNS A record externally. However, when configuring the Web Bridges on the Call Bridge(s) there must be a unique hostname or IP address for each Web Bridge configured on the Call Bridge(s). Put another way, each Web Bridge must be uniquely identifiable by every Call Bridge

- The TURN servers are configured via the API as described [later](#)
- The TURN servers can be configured either by hostname (with one hostname resolving to potentially multiple servers via DNS) or by IP address. This configuration is stored in the shared coSpace database.

- The Acano clients are always monitoring TURN servers in the background via their connections to an XMPP server. When a call starts, the client is sent a list of available TURN servers but will have already chosen the best TURN server for each interface: therefore, when joining a call there is no additional delay in choosing a TURN server. Acano reserves the right to change and enhance the algorithms used.

  ▶ The XMPP server is configured using the MMP as described later.

---

**Note:** You may have multiple XMPP servers in your deployment, providing each XMPP server is in a different domain to the other XMPP servers.

Therefore the previous figure becomes the following when connections are shown.

---

**Figure 5:** Simple deployment showing connections

---

**2.4.1 Example using split deployments and geo-distribution**

The figure below shows the single split deployment with components rearranged for scalability and resilience. Note that the XMPP server moves to the core server and there is a new component – the Load Balancer – on the Edge server.

---

**Note:** As used by Acano clients, XMPP requires a persistent connection from the client to the XMPP server. From R1.6 the XMPP should be run on a Core server if you have security concerns; therefore there is a following requirement to have a new Edge component – the Load Balancer – to provide this connection to the clients.
The Load Balancer provides a single point of contact for Acano clients and the XMPP server. It listens on an external interface and port (as described in the XMPP client SRV record) for incoming connections. Equally, the Load Balancer accepts incoming TLS connections from the XMPP server over which it can multiplex TCP connections from external clients. This creates a TLS trunk between the Core and the Edge. More than one Edge server can trunk to the XMPP server.

The Load Balancer does not require a license.

The Web Bridge and Call Bridge are configured using a DNS A record, and the XMPP server has associated XMPP SRV records.

Connections between the Call Bridge on the Core server and the Web Bridge and TURN servers on the Edge servers use same ports as in previous releases: that is, 443 and 3478 respectively.

This deployment can be scaled in a number of ways, for example see the figure below. The Hong Kong Core server currently hosts the coSpace database; New York and London use external coSpace databases.

Figure 6: Split Core and Edge servers showing new location of XMPP server

Figure 7: Multi Core & Edge server deployment
2.4.2 coSpace database concepts

- All inter-database communication between database cluster peers is handled through SSL for security and compression.
- Within a coSpace database cluster, only one database is used at any time by all the Call Bridges; this is the “master” All reads and writes are performed on this database instance.
- This master database’s contents are replicated to the “slaves/hot-standbys” for resilience: this is indicated in the figures in the chapter on databases.
- In case of master failure, a slave database will be "promoted" to being the new master, and other slaves will reregister with the new master database. After the failure has been corrected, the old master will assign itself as a slave and will also register with the new master:
  - Loss of power to the master database results in that database reverting to being a slave on startup.
  - Loss of all network connectivity to and from the master database results in that database becoming a slave when connectivity is restored.
- In cases where a network partition occurs, any database that can see less than half of the total number in the cluster will not be promoted to being a master database. Likewise, any existing master that cannot see more than half of the cluster databases will be demoted to a slave. This ensures that multiple masters are not created, and that the coSpace databases’ contents remain consistent across the cluster.
- If the network is split equally; then for safety, the database cluster reverts to containing no masters. This situation can also occur if the network is partitioned into three or more disconnected pieces in which no one piece contains more than half the databases.

CAUTION: In cases where no master can be elected, the system administrator must reinitalize the cluster. This can be done by following the initialization and attachment steps described later in this section. For this reason, while you can have a cluster of 2, we recommend having at least 3 databases when using database clustering.

- When a Call Bridge can only see slave databases it continues to operate (reading from a slave database), but will not be able to perform any database writes. This includes modification operations via the API, coSpace modifications via an Acano client, client login via XMPP and LDAP sync. SIP calls will operate as normal.
- In order for a Call Bridge and a database to communicate, the two must be running the compatible database schemas. In a single-node (non-clustered) system, the Call Bridge automatically upgrades the database schema to the latest version when it first boots. However in the clustered scenario, this process has been made manual to allow greater control of when the upgrade occurs — as described later in this document.
- There are two important time factors:
  - Time after becoming isolated for a master to revert to being a slave: 5-6 seconds
  - Time after master goes down for a slave to become the master: 10-15 seconds
3 Configuring the MMP

The Acano solution components are configured using the MMP.

3.1 Creating and Managing MMP and Web Admin Interface User Accounts

You should have created a MMP administrator user account on each Acano server; if so, go on to the next section unless you want to set up additional accounts. The same account is used to access the Web Admin Interface.

(If you do not have these MMP administrator user accounts, you will have to use the emergency admin recovery procedure detailed in the appropriate Installation Guide.)

You can create additional user accounts for the MMP that have admin level rights using the MMP add user command user add <account name> <role>.

1. SSH into the MMP.
2. Add an admin level user account, for example:
   ```bash
   user add adminuser2 admin
   ```
3. Enter the password you want to use for this account twice in order to complete the account creation.

   On login the user will be forced to configure a new password.

Note: For additional user accounts with other roles and the full range of user commands, see the Acano solution MMP Command Reference Guide.

3.2 Upgrading Software

The Acano X series servers ship with the latest release available at the time of shipment but may not be up-to-date. Equally, if you downloaded the OVF ZIP file for the virtualized deployment some days ago, we advise you to check on the partner section of the Acano website whether a later version is available, and if so, upgrade before you start testing. The following instructions apply to both types of deployment and should be checked on each Acano server:

1. To find out which version the Acano solution is running, SSH into the MMP, log in and type:
   ```bash
   version
   ```
2. To upgrade, first download the updated .img file from your Acano reseller.

   NOTE: Ensure that you install the correct image file for your type of deployment; that is either the Acano X series server upgrade file or the virtualized server image file; each is clearly labeled. Note that you may need to rename the file to upgrade.img before going on to step 3.

3. Use a SFTP client to upload a new image to the MMP, for example using a command line SFTP client (where 10.1.x.y is an IP address or domain name):

   For example:
4. Then to complete the upgrade, connect via SSH to into the MMP and type:
   
   ```
   upgrade
   ```
   
   Allow 10 minutes for the solution to restart.

5. To verify that the upgrade was successful, SSH into the MMP, log in and type the following command to verify that you are now running the version that you intended to:
   
   ```
   version
   ```

### 3.3 Checking the Web Admin Interface for HTTPS Access

The Web Admin Interface is the Call Bridge’s user interface. You should have set up the certificate for the Web Admin Interface (by following one of the Installation Guides). If you have not, do so now.

1. The port for the Web Admin Interface is 443 **UNLESS** you configured the Web Admin Interface access on the same interface as the Web Bridge. Then set the default TCP port to a non-standard port such as 445 to allow the Web Bridge to function on TCP port 443 with the command.

   ```
   webadmin listen admin 445
   ```

   Note: the Admin interface does not exist on the VM server, so assuming you are using interface A for web admin, then the `webadmin` command becomes:

   ```
   webadmin listen a 445
   ```

2. To test that you can access the Web Admin Interface, type your equivalent into your web browser: `https://acanoserver.example.com`

   If it works, proceed to next section.

3. If you cannot reach the Web Admin Interface:
   a. Sign into the MMP, type the following and look at the output:

   ```
   webadmin
   ```

   The last line of the output should say "webadmin running".

   b. If it does not there is a configuration problem with your Web Admin Interface. Check that you have enabled it by typing:

   ```
   webadmin enable
   ```

   c. The output of the `webadmin` command should also tell you the names of the certificates you have installed, e.g. `webadmin.key` and `webadmin.crt`.

   ```
   webadmin.key
   webadmin.crt
   ```

   Note: They should the same names of the certificates you uploaded previously.

   Assuming these are the names then type:

   ```
   pki match webadmin.key webadmin.crt
   ```

   This will check that the key and certificate match.
d. If you are still experiencing issues, troubleshoot the problem as explained in the Certificates guidelines document.

### 3.4 Configuring the Call Bridge Listening Interface

The Call Bridge needs a key and certificate pair that is used to establish TLS connections with SIP Call Control devices and with the Lync Front End (FE) server. If you are using Lync, this certificate will need to be trusted by the Lync FE server.

The command `callbridge listen <interface>` allows you to configure a listening interface (chosen from A, B, C or D). By default the Call Bridge listens on no interfaces, see the MMP Command Reference.

Configure listening interfaces on each Call Bridge as follows:

1. Create and upload the certificate as described in the Certificate guidelines document.
2. Sign into the MMP and configure the Call Bridge to listen on interface A.
   ```
   callbridge listen a
   ```

   **Note:** Call Bridge must be listening on a network interface that is not NAT’d to another IP address, because Call Bridge is required to convey the same IP that is configured on the interface in SIP messages when talking to a remote site.

3. Configure the Call Bridge to use the certificates by using the following command so that a TLS connection can be established between the Lync FE server and the Call Bridge, for example:
   ```
   callbridge certs callbridge.key callbridge.crt
   ```
   The full command and using a certificate bundle as provided by your CA, is described in the Certificate guidelines document.

4. Restart the Call Bridge interface to apply the changes.
   ```
   callbridge restart
   ```

### 3.5 Configuring the XMPP server

If you are using any of the Acano clients including the WebRTC Client you now need to configure the XMPP server and then enable it. Otherwise, skip this section.

**Note:** If you had the XMPP server configured before upgrading to R1.6, some of the configuration will be lost on upgrade. There is also a new Domain field. Therefore, follow these instructions to ensure that you have a valid configuration.

1. Follow the instructions in section 6.1 to set the DNS records for the XMPP server
2. Sign in to the MMP and generate the private key and certificate using the information in the Certificate guidelines document. Upload the certificates to the server hosting the XMPP server.

On Acano X series servers the XMPP license key file (license.dat) is pre-installed; check it is visible in the list of files. (The example below may look different to your SFTP client). If it is
missing contact support@acano.com with the serial number of your X series server.

On a virtualized deployment, you must upload license.dat yourself (using SFTP). If you have not done so already, contact support@acano.com with one of the MAC addresses assigned to the VM to obtain this file. See the Virtualized deployment specific pre-requisites.

The XMPP server can be configured to listen on any subset of the four media interfaces and ignore connections from any interface in the complement.

1. Establish a SSH connection to the MMP and log in.
2. To configure the XMMP server to use one or more interfaces enter the following command:
   
   ```
   xmpp listen <interface whitelist>
   
   The following is an example where interface is set to interface A and B.
   ```
   
   ```
   xmpp listen a b
   ```
3. Assign the certificate and private key files that were uploaded earlier, using the command:
   
   ```
   xmpp certs <key-file> <crt-file>
   ```
   
   see the Certificate guidelines for further information
4. Configure the XMPP server with the following command:
   
   ```
   xmpp domain <domain name>
   ```
   
   The following is an example where domain-name is example.com.
   ```
   xmpp domain example.com
   ```
5. Enable the XMPP service:
   
   ```
   xmpp enable
   ```
6. To allow a Call Bridge to access the XMPP server securely (after configuration), provide a component name for the Call Bridge to use to authenticate e.g. example_component:
   
   ```
   xmpp callbridge add <component name>
   ```
   for example
   ```
   xmpp callbridge add cb_london
   ```
   A secret is generated; for example, you see:
   ```
   acano>xmpp callbridge add cb_london
   Added callbridge: Secret: aB45d98asdf9gabgAb1
   ```
   
   Note: Each Call Bridge requires a unique component name so that all the Call Bridges can connect to the XMPP server at the same time.
7. Note the domain, component and secret generated in the previous steps because they are required later when you configure the Call Bridge access to the XMPP server (so that the Call Bridge will present the authentication details to the XMPP server).

   (If you lose the details, use the MMP `xmpp callbridge list` command to display them.)
4 Configuring the coSpace Databases

You do not need to create or enable coSpace databases as happens for other components: an empty coSpace database is created on every host server when you install the Acano solution image on the server.

However, it is important to understand the way in which a coSpace database cluster works because it is different to other clusters in the Acano solution. Follow the instructions in this section to create the cluster(s). Unless otherwise noted, these instructions apply equally to combined or split deployments.

Note: If a WAN optimiser is deployed between clustered database nodes, it may prevent keep-alive checks from completing, causing errors to appear in logs. In cases where a WAN optimiser is being used between cluster nodes, it is important to ensure that all keep alive traffic is sent in a timely manner.

Please consult your WAN optimiser documentation about how to either disable this functionality between specific IP addresses, or for options that control which optimisations are applied.

4.1 coSpace Database on a Separate Server

4.1.1 Requirements for a coSpace database on a separate server

Note: This section is applicable only if you choose to use one or more external databases.

The coSpace database host server has modest CPU requirements but requires large storage and memory. We do not mandate a qualified VM host but recommend:

- Four vCPUs, 8GB RAM and 100GB data store
  (The OVF will be set to these parameters so that they are the defaults post-deployment)
- Sandy Bridge (or later) class Intel processors (e.g. E5-2670 or E5-2680 v2)
- The data store should reside on either a high IO per second SAN or local SSD storage
- The data must reside on the same vdisk as the OS

The Dell R620 which we currently qualify for the Core virtualized server could be used but will require a local SSD if a high performance SAN is not available.

It should be possible to run other VMs on the same host server, if desired.

We do not have any operational statistics yet, but we are gathering information.

4.1.2 Deploying a coSpace database on a separate server

1. Install the Acano solution image on to each of the external database host servers. An empty database is set up automatically.
2. This host server still requires certificates – see the next section.
4.2 Deploying Certificates on the coSpace Database and Call Bridge Servers

Note: In any production environment, you must use encryption on database traffic. This is achieved by using certificates. However, for testing (and only for testing) you can skip this section.

**CAUTION**: These instructions can only be run on a disabled database cluster. If you have already set up a coSpace database cluster you must run the `database cluster remove` command on every server in the cluster, then run the commands in this section before recreating the cluster using the steps in the following sections.

coSpace database clustering uses public/private key encryption for both confidentiality and authentication, with a single, shared Certificate Authority (CA). Because the database clustering is not user-accessible, the certificates can be signed by a local CA. Refer to the [Certificate guidelines](#) document for information on creating, uploading and assigning certificates and certificate bundles to the database cluster.

4.3 Selecting the Master coSpace Database for a Cluster

To deploy a coSpace database cluster, decide which will be the master database (that is, the coSpace database instance that will be used by all Call Bridges initially). If you have been deploying without scalability, initially the database master must be the current coSpace database so that no data is lost. Therefore this coSpace database will be co-located with a Call Bridge.

Note: A single coSpace database can be a “cluster” in that it can have one or more Call Bridges using it (“attached” to it). However, there is no resilience.

1. On the server with the coSpace database that will start as the master, sign in to the MMP.
2. Enter the following command to select the interface for this coSpace database cluster:
   ```bash
   database cluster localnode <interface>.
   
   database cluster localnode a
   ```

   The `<interface>` can be in the following formats
   - `[a|b|c|d|e]` - the name of the interface (the first IPv6 address is preferred, otherwise the first IPv4 address is chosen) e.g. `database cluster localnode a`
   - `ipv4:[a|b|c|d|e]` - the name of the interface restricted to IPv4 (the first IPv4 address is chosen) e.g. `database cluster localnode ipv4:a`
   - `ipv6:[a|b|c|d|e]` - the name of the interface restricted to IPv6 (the first IPv6 address is chosen) e.g. `database cluster localnode ipv6:a`
   - `<ipaddress>` - a specific IP address, can be IPv4 or IPv6 e.g. `database cluster localnode 10.1.3.9`
3. Enter the MMP command: `database cluster initialize` and press Y in response to the prompt to initialize this coSpace database as the master for this database cluster.

   ```
   database cluster initialize
   WARNING!!!
   Are you sure you wish to initialize this node as a new database cluster? (Y/n)
   The contents of this node's database will become the master version of the database in the new cluster.
   Initialization started...
   ```

   This triggers a restart of the local Call Bridge and takes approximately 30 seconds.

4. Check that the initialization completed correctly by entering the following command until the Status is reported as Enabled:

   ```
   database cluster status
   ```

   You should see messages similar to:

   ```
   Status: Initializing
   Nodes: 10.1.2.3 (me)      : Connected Master
   Interface                : a
   ```

   And later if you re-run the status command:

   ```
   Status: Enabled
   Nodes: 10.1.2.3 (me)      : Connected Master
   Interface                : a
   ```

4.4 Attaching other Database Instances to the coSpace Database Cluster

Note: These server(s) can have an empty database and do not need to have a co-located Call Bridge e.g. virtualized servers set up to be external databases only. (As mentioned previously, these host servers require the dbcluster certificates and keys.)
**CAUTION**: The contents of the coSpace database currently on this server (if any) will be destroyed.

1. Attach other servers hosting a database that you want to be part of this database cluster.
   a. On each such server set the listening interface using the following command (interface can be in any of the formats listed previously in this section):
      ```
      database cluster localnode <interface>.
      acano> database cluster localnode a
      Interface updated
      ```
   b. “Attach” this database to the master using the command
      ```
      database cluster join <master hostname/IP>
      ```
      and then use the `database cluster status` command to monitor the progress, as shown below.

![Figure 9: Attaching coSpace databases](image)

**Note**: A hostname can be used in the `database cluster join <master hostname/IP>` command below but it will be replaced by the IP address of the interface specified for the master.

The attach command pulls a full copy of the coSpace master database onto this server, and therefore may take some time depending on the connection speed. For an empty database, this operation is expected to take approximately 30 seconds.
This triggers a restart of the local Call Bridge (if there is one).

c. Verify that the master coSpace database is aware of the attached coSpace database by entering the database cluster status command in the MMP of the master coSpace database host server. (This information should have propagated automatically within 10 seconds of the join command completing.)

```
10.1.2.8 (me)      : Connected Slave
Interface          : a
acano> database cluster status
Status              : Enabled
Nodes:
    10.1.2.3       : Connected Master
    10.1.2.8 (me)  : Connected Slave
Interface          : a
```

```
acano> database cluster status
Status              : Enabled
Nodes:
    10.1.2.3 (me)  : Connected Master
    10.1.2.8       : Connected Slave
Interface          : a
```

### 4.5 Connecting Remote Call Bridges to the coSpace Database Cluster

Call Bridges that are co-located with a coSpace database (master or slave) are automatically connected to the coSpace database cluster that the co-located coSpace database is part of.

---

**Note:** Put another way, the `database cluster connect` command below does not have to be run if `database cluster initialize` or `database cluster join` has already been run on this host server, and it is already listed in the list of nodes when `database cluster status` is run. See the figure below.

```
“Connection” means that the Call Bridge knows how to access all the coSpace databases in the cluster; therefore it does not matter which coSpace database’s address is used to connect. (The actual database that is read from/written to is the current master).
```

1. Sign in to the MMP of the Core server with an unconnected Call Bridge and issue the command `database cluster connect <hostname/IP>`. The hostname or IP address can be for any coSpace database in the cluster.

```
acano> database cluster connect 10.1.2.3
WARNING!!!
Are you sure you wish to connect this node to an existing database cluster? (Y/n)
Connecting started...
```

This triggers the Call Bridge on this Core Server to restart.

---

**Note:** Unlike the attach command used in the previous section, the connect command does not delete any existing coSpace database on the server hosting this Call Bridge. Therefore
if you use the command on a Core server with an existing local database then the contents of the database are not destroyed, but the local coSpace database is invisible until this server’s Call Bridge is disconnected from the cluster.

Figure 10: Example of coSpace database clustering and Call Bridge connections

4.6 Upgrading the database schema

Note: This section does not apply when you first set up database clustering, but these steps must be run after every subsequent Core server software update; otherwise the Call Bridges and coSpace databases may be out-of-step with regards to the database schema.

The upgrade path for a clustered system is:

1. Upgrade each database node one by one, ensuring each node is up and the `database cluster status` command reports full connection to the cluster, BEFORE upgrading the next one.
   
   At this stage `database cluster status` should report healthy on all nodes, but the Call Bridges will not be operating correctly and will show database errors.

2. Use the command `database cluster status` to identify the master node.

3. Log into this master node’s MMP and issue the command `database cluster upgrade_schema`

4. Verify that the operation was successful by using `database cluster status`.
   
   A status of Enabled means success, whereas Error indicates an issue.
5 Deploying the Call Bridges

Unless otherwise noted, these instructions apply equally to combined or split deployments.

5.1 Setting up the Call Bridges’ certificates

The Call Bridge needs a key and certificate pair that is used to establish TLS connections with SIP call control devices and with the Lync Front End server.

If you are using Lync, this certificate will need to be trusted by the Lync FE Server; the best way to achieve this is to sign the certificate on the CA server that has issued the certificates for the Lync FE Server.

Follow the instructions in the Certificate guidelines document for information on creating, uploading and assigning certificate to Call Bridges.

5.2 Setting up the Call Bridges

If you have not already done so, on each Call Bridge:

1. Configure the Call Bridge’s listening interface

   The command `callbridge listen <interface>` allows you to configure a listening interface (chosen from A, B, C or D). By default, the Call Bridge listens on no interfaces. A full list of commands is in the MMP Command Reference Guide.

   Configure listening interfaces as follows:

   a. Configure the Call Bridge to listen on interface A.
      
      `callbridge listen a`

   b. Configure the Call Bridge to use the security certificates (created previously) by typing the following (so that a TLS connection can be established between the Lync FE server and the Acano Call Bridge):
      
      `callbridge certs callbridge.key callbridge.crt`

      The full command and using a certificate bundle as provided by your CA, is described in the Certificate guidelines document.

   c. Restart the Call Bridge to apply the changes.
      
      `callbridge restart`

---

Note: You will need to add the Call Bridge certificate to every Web Bridge’s trust store after you’ve configured the Web Bridges, as described in the Certificate guidelines document.
5.3 Clustering Call Bridges

Within your Acano deployment, you can enable Call Bridge clustering which will allow multiple Call Bridges to operate as a single entity and scale beyond the capacity of any single Call Bridge.

You have a choice whether to setup the Call Bridges in the cluster to link peer-to-peer, or for calls to route via call control devices between the clustered Call Bridges.

Linking Call Bridges peer-to-peer:
- reduces call complexity as the call will go from Call Bridge A to Call Bridge B directly, with nothing in the middle to interfere with the routing of the call.
- reduces load on the call control device, and frees up resources to handle calls that need to route through the call control device. This may be important if the call control device is licensed on a per call basis.

Routing via call control device(s):
- creates a consistent call flow for your Acano and Local SIP devices. This can make network configuration a little simpler, particularly if there are firewalls between networks with fixed "allow rules" which only allow calls routed through call control devices.

How calls are routed in deployments with clustered Call Bridges is determined by the Peer Link SIP domain field (see below) and the dial plan (see section 5.5).

Follow these instructions to cluster Call Bridges:

Note: The instructions in this section assume that:
- all the coSpace databases are running as a cluster
- all the Call Bridges that will form part of the cluster are configured as standalone Call Bridges
- all the Call Bridges have been connected to the coSpace database cluster

On every Call Bridge that will be part of the Call Bridge cluster:
1. Sign in to the Web Admin Interface and go to Configuration > Cluster.
2. In the Call Bridge Identity section, enter a unique name for that Call Bridge (e.g. "London-Core1") and click Submit.
3. Enter a Peer link bit rate, the per call rate in which servers will connect at in a distributed call (optional)

On one Call Bridge that will be part of the cluster:
4. Sign in to the Web Admin Interface and go to Configuration > Cluster. In the Clustered Call Bridges table:
   a. Add an entry for this Call Bridge, using the Unique Name of this Call Bridge entered in step 2.
   b. Add the Address by which the Web Admin Interface of the Call Bridge can be reached from other servers in the cluster via HTTPS. This address will be used for management messaging e.g. Participant lists. Note: Weadmin can be set to listen on the Admin interface as well as interfaces A through D.
   c. Leave the Peer Link SIP Domain blank unless you have call control devices between your Call Bridges. If you leave the field blank then the address of the outbound SIP call
Deploying the Call Bridges

will be in the form of a random URI generated by the Call Bridge followed by the IP address of the Call Bridge that it is linking to (for example randomURI@10.10.10.10). If you specify the Peer Link SIP Domain then, that is what will be used when calling to a remote server for a Peer call. You can have it route to your call control device if you have set up an Outbound Rule that matches the Peer Link SIP Domain. If routing through an existing call control, it is recommended to use a unique domain or each servers’ FQDN for the Peer link SIP domain. This ensures no accidental call loops that would likely occur if using the same domain on all.

d. Click Add.

e. Repeat steps 4a to 4c for each Call Bridge that will be part of the cluster, entering the unique name for each Call Bridge that you set up in step 2.

The Clustered Call Bridges table should now have one entry for every Call Bridge that will be part of the cluster, and the Unique Name in the Call Bridge Identity section identifies which Call Bridge this is.

The information in the Clustered Call Bridges table is replicated to every Call Bridge in the cluster. Therefore, you can now go to any Call Bridge server, sign in to the Web Admin Interface and go to Configuration > Cluster to see the status of all the clustered Call Bridges.

The Call Bridge cluster is now setup, and the clustered Call Bridges will share the same dial plan (Inbound, Outbound and Call Forwarding dial plan rules). You now need to check that the dial plan uses the same addresses as those entered in the Clustered Call Bridges table. See the section on dial plans.

5.4 Lync Account Information

For Call Bridge integration with Lync Edge, we recommend that you configure each Call Bridge with its own login account so that there are no conflicts. For each Lync call to or from that Call Bridge, we request TURN resources from the Lync Edge using that account. Until that call is disconnected, that resource is considered "Used" from a Lync point of view. Lync will only allow up to 12 TURN allocations per user account; therefore, with 1 registration, only 12 calls are possible. If you shared that one account across multiple Call Bridges, you would only be allowed 12 Lync calls in total across all Call Bridges, not just the 1.
Configure each Call Bridge independently for this reason and so that each regional Call Bridge uses a local regional Lync Edge (where available). Use the normal dial plan outbound rules to determine if a call is a Lync call and to configure where to send it.

### 5.5 Dial Plan Information

This section discusses setting up a dial plan for scalable and resilient deployments: inbound dial plan rules, outbound dial plan rules and call forwarding rules. The specific dial plan rules you require and their priority depend on your deployment, not only the topology of the Acano solution but also of your third party call control platform(s) and whether you prefer to use local resources or want to load balance calls.

From R1.6 the dial plan is stored on the coSpace database server therefore you can amend the dial plan from any Call Bridge in the Call Bridge cluster. Also you can see the full dial plan in the Web Admin Interface of any Call Bridge but we recommend setting up the dial plan using the API because this provides more flexibility. Outbound dial plan rules must be configured via the API for clustered Call Bridges. See the appendix of examples later.

For example, you may want every Call Bridge in a cluster to use the same outbound dial plan, but this will not allow for geographic differences. To account for location and topology you can mix rules that apply to all Call Bridges with those that are specific to one Call Bridge – which you specify in the API. For example, you may want calls placed to +01 numbers to always be made from a Call Bridge in the US.

To match this API addition there is a new column called Call Bridge Scope in the **Configuration > Outbound Calls** page in R1.6 (after Beta 3): you cannot edit this column in the Web Admin Interface, it simply shows you what was set in the API. Specifically it does not show which Call Bridge a rule applies to if the rule is Call Bridge-specific.

Note: Call Bridge Scope of All is equivalent to the API scope setting of global, while the Call Bridge Scope of One is equivalent to a scope of callbridge in the API.

When setting the dial plan rules, ensure that:

- Outbound dial plan entries for calls are either valid for all Call Bridges in the cluster i.e. have a Call Bridge Scope of All in the Web Admin Interface, or that rules with a setting of One are completely defined using the API to specify the Call Bridge that the rule applies to
- The configured Incoming dial plan for SIP calls covers the set of domains that will be routed to any Call Bridge in the cluster from outside the cluster

Note: Inter-peer calls between Call Bridges will be placed using the outbound dial plan rules on the initiating Call Bridge. Therefore you may need to add outbound dial plan rules if the calls are to IP addresses in order to place the call direct to the other Call Bridge, rather than via a SIP proxy. However, your existing outbound dial plan rules may already cover inter-peer calling if you are using domain dialing.

Note: Inter-peer signaling between Call Bridges uses HTTPS.

Note: Outgoing calls with the same dial plan rule priority will favor local call control device over one in another geographical location.
5.5.1 Examples

These examples use a Cisco VCS but the concepts are independent of Call Control device.

In the simplest case, a single VCS is trunked to a single Acano server (and therefore a single Call Bridge) to provide integration with SIP endpoints. In a larger deployment of multiple Call Bridges across multiple data centres more thought must be given to the dial plan.

Example #1: One option is to configure a cluster of VCSs to forward calls to the cluster of Call Bridges. This provides resiliency because any VCS can route a call to any Call Bridge in the Acano solution (see the figure below). Likewise the Acano solution can route calls from any Call Bridge to any VCS.

![Mesh configuration for SIP Call Control](image1.png)

Figure 11: Mesh configuration for SIP Call Control

Example #2: If you have a geographically distributed call control system then you can choose to selectively trunk these VCSs to Call Bridges that are local to them. For example VCSs in London can be trunked to London-based Call Bridges and New York-based VCSs can be trunked to New York-based Call Bridges. This ensures that media does not travel between data centres unnecessarily, and if you have a conference that spans locations there is a single peer-link between Call Bridges to minimize bandwidth usage between data centres.

![Geographical configuration example for SIP Call Control](image2.png)

Figure 12: Geographical configuration example for SIP Call Control
6 Deploying the XMPP Server

Unless otherwise noted, these instructions apply equally to combined or split deployments. These deployment instructions assume that you have already followed the appropriate Acano Solution Installation Guide.

Note: XMPP server clustering released as a beta feature in Release 1.6, is being replaced with a revised feature in a future release. Please be advised that the configuration will be different from that previously documented. The current XMPP cluster configuration has been removed from the deployment guide. Until this feature is ready, only enable one XMPP server per domain in your Acano solution.

CAUTION: If you have enabled an XMPP server on an Edge server and you now intend to move it to a Core server, then you need to do the following steps in the order provided:
- disable the XMPP server(s) on the Edge server using the `xmpp disable` MMP command
- enable XMPP server(s) on the Core server (see the first two sections below)
- enable the Load Balancer on the Edge server (see later in this document)
This does not apply if you have not enabled XMPP servers or if you are only using combined host servers.

6.1 Configuring DNS Records for the XMPP Server

Note: the remainder of this section assumes that you have already followed the steps in section 3.5 to configure the XMPP server.

DNS SRV records are required for any location in which it is desired to access the XMPP service. Depending on the configuration of your deployment, these can include internal DNS records within the LAN which resolve directly to the XMPP server, or public DNS records which resolve to the Load Balancer in the DMZ.

Note: You can configure the DNS resolver(s) to return values which are not configured in DNS servers or which need to be overridden; custom Resource Records (RRs) can be configured using the `dns rr` command which will be returned instead of querying DNS servers. However, this has the disadvantage that when you start adding additional XMPP servers you must add these records on each server. See the MMP Command Reference for details.

1. Create DNS A records for the fully qualified domain name (FQDN) of the XMPP service’s host server and set it to the IP Address of the interface that the XMPP server is configured to listen on.

   In order to enable client connections, including use of the WebRTC Client, an `_xmpp-client._tcp` record is required. On a typical deployment, this will resolve to port 5222. Inside the LAN, if the core server is directly routable, it can resolve to the XMPP service running on the core server. For example:

   ```
   _xmpp-client._tcp.example.com could have the following SRV records:
   _xmpp-client._tcp.example.com 86400 IN SRV 10 50 5222 core1.
   ```
example.com

In locations where it is not possible to route to the core server, XMPP traffic should instead be handled by the Load Balancer, running on an Edge server. From the example above:

```plaintext
_xmpp-client._tcp. example.com 86400 IN SRV 10 60 5222 edge1.example.com.
_xmpp-client._tcp. example.com 86400 IN SRV 10 20 5222 edge2.example.com.
_xmpp-client._tcp. example.com 86400 IN SRV 10 20 5222 edge3.example.com.
```

where edge1.example.com is in the DMZ, and therefore accessible from the Internet.

If multiple geographically distributed edge servers are available, GeoDNS can be used in order to tell clients to favor Edge servers close to them.

The XMPP service can federate with any other standards-compliant XMPP service. In order to enable this create an _xmpp-server._tcp SRV record, usually resolving to port 5269. Because XMPP federation will usually be across the Internet, typically these records are only required to point to servers available in the DMZ. For example:

```plaintext
_xmpp-server._tcp. example.com 86400 IN SRV 10 60 5269 edge1.example.com.
_xmpp-server._tcp. example.com 86400 IN SRV 10 20 5269 edge2.example.com.
_xmpp-server._tcp. example.com 86400 IN SRV 10 20 5269 edge3.example.com.
```

Note: The 60 and 20 in the above examples are priorities. DNS SRV records have a priority field and clients try those servers with the lowest priority first. In addition there is a weight field (within a given priority, if we have e.g. weight 2, 1, 1 the client will choose the server with weight 2 50% of the time, and each of the weight 1 servers 25% of the time).

2. Test the above with the following commands:
   - `nslookup -q=srv _xmpp-server._tcp.example.com`
   - `nslookup -q=srv _xmpp-client._tcp.example.com`

### 6.2 Connecting Call Bridges to the XMPP Server

1. To allow a Call Bridge to access the XMPP server:
   a. Sign to the Call Bridge’s Web Admin Interface and go to Configuration > General.
   b. Complete the fields in the XMPP Server Settings section and save your configuration.
      i. Unique Call Bridge name (this is the component name set up previously): `cb_london` (no domain part is required, as shown)
      ii. Domain (this is the XMPP server domain set up previously): `example.com`
      iii. Server Address: localhost:5223
Notes:

If you are using DNS to locate the XMPP servers it is not necessary to configure the server address.

If you are using a two Acano Server deployment or a split virtual deployment use the IP address of the Edge server/virtualized server.

- Shared Secret = the component secret generated in earlier by the mmp command
- If the Authentication Suffix was previously configured to a value other than * (star) then this field is shown. It should be configured = * (star)

See the Acano solution MMP Command Reference for details of the xmpp callbridge commands.

6.3 Deploying the Trunk and the Load Balancer

The Core server creates a TLS connection to the Edge server. They mutually authenticate, and the Edge server starts to listen on port 5222 for incoming client XMPP connections. A client XMPP connection is serviced by the Load Balancer and relayed to the Core server using the TLS trunk.

Note the direction of traffic: the Core server connects out from the internal network to the Edge server in the DMZ—which is the natural direction of traffic as far as firewalls are concerned and convenient if the internal network uses NAT.
6.3.1 Configuring the Edge Server Load Balancer

To configure the Load Balancer you need:

- Key and the corresponding certificate (and perhaps a bundle of CA-signed and intermediate certificates) for the trunk TLS connection
- Bundle of trusted certificates for authentication of the trunk connections
- Network interfaces and ports to use for public connections
- Network interface and port to use for trunk connections
- Simple name (tag) for the Edge server

1. Sign in to the MMP of the Edge server.

2. Create an Edge instance, using the command:

```
loadbalancer create <tag>
```

If the tag for the Edge server is "LondonEdge", type:

```
loadbalancer create londonEdge
```

3. Configure the necessary keys and certificates for the trunk TLS connections as well as the trust bundle to specify which Core servers are authorized to create trunks to this Edge server. If the Core server presents any of the certificates in this bundle when creating the TLS connection, then the connection succeeds. If the trust bundle contains a valid chain of certificates, with the presented certificate issued by the end of the chain, then authentication succeeds. Otherwise, the connection will be rejected.

```
loadbalancer auth <tag> <key-file> <cert-file> <bundle-file>
```
Deploying the XMPP Server

e.g. if the bundle of trusted certificates is named "trust.pem" and the certificate and key file are called "edge.pem" and "edge.key", then

```
loadbalancer auth londonEdge edge.key edge.pem trust.pem
```

4. Configure the trunk interface and port, using:

```
loadbalancer trunk <tag> <iface>:<port>
```

e.g. if trunk connections will be allowed on interface A, port 4999, then type:

```
loadbalancer trunk londonEdge a:4999
```

5. Configure the public interface and port (for accepting client connections), using

```
loadbalancer public <tag> <iface:port whitelist>
```

e.g. if client connections are to be allowed on B, port 5222, then type:

```
loadbalancer public londonEdge b:5222
```

6. In a common Edge server deployment, the Web Bridge is also enabled and needs to make use of a trunk. To allow this, configure the loopback as a public interface, e.g.

```
loadbalancer public londonEdge b:5222 lo:5222
```

7. Enable the trunk, using:

```
loadbalancer enable <tag>
```

e.g.

```
Load Balancer enable LondonEdge
```

---

**Note:** The public port is not opened until there are trunks to service connections.

To see the full list of trunk commands, see the Acano solution MMP Reference.

### 6.3.2 Deploying a TLS Trunk between Core and Edge Servers

To configure a trunk you need:

- Key and the corresponding certificate for the trunk TLS connection
- Bundle of trusted certificates for authentication of the trunk connections
- Domain name or IP address of the Edge server to trunk to
- Edge port to trunk to
- Service which will use the trunk (i.e. XMPP) or the port used by the service
- Simple name (tag) for the trunk

1. Sign in to the Core Server’s MMP.
2. Create a trunk instance, using the command:

```
trunk create <tag> <port/service name>
```

If the tag for the trunk is "trunktoLondonEdge", type:

```
trunk create trunktoLondonEdge xmpp
```

3. Configure the private key and certificate used to authenticate to the Edge server, and the trusted certificates which may be presented by the Edge server to the core server:

```
trunk auth <tag> <key-file> <cert-file> <trust-bundle>
```
Deploying the XMPP Server

e.g. if the private key is acano.key and the corresponding public key is acano.crt, and if the trust bundle file is bundle.pem, then type:

```
trunk auth trunktoLondonEdge acano.key acano.crt bundle.pem
```

Note that the public key used here must be present in the trust bundle for the Edge server.

If the Edge server public certificate is in the trust bundle, then authentication (at the trunk side) will succeed. If there is a chain of certificates in the trust bundle with the Edge server certificate issued by the end of the chain, then authentication will succeed. Otherwise, authentication of the Edge server fails.

4. Configure the Edge server that this trunk will connect to, using:

```
trunk edge <tag> <edge name/ip address> [default port]
```

e.g. if the Edge server name is london1.example.com using port 4999, then type:

```
trunk edge trunktoLondonEdge edge1.example.com 4999
```

Note: If the domain name resolves to multiple IP addresses, a connection will be attempted to all.

5. Enable the trunk, using:

```
trunk enable <tag>
```

e.g.

```
trunk enable trunktoLondonEdge
```

To see the full list of trunk commands, see the Acano solution MMP Command Reference.
Figure 14: Load balancers configured in a split deployment
7 Configuring Web Bridges

Unless otherwise noted, these instructions apply equally to combined or split deployments.

Note: While you can still configure one Web Bridge via the Web Admin Interface, if you have multiple Web Bridges we strongly suggest that you use only the API to configure them all, as described below. (An example using the POSTMAN tool is provided later.)

7.1 Setting up the Web Bridges via the API

1. Using the API on one Call Bridge, create a /webBridges/<web bridge id> node for each Web Bridge.
   a. For example, for each Web Bridge access the API as usual.
   b. POST to the Call Bridge’s /webBridges node with the following values replaced by your values – each Web Bridge requires a unique URL:
      - url = https://join.example.com
      - resourceArchive= https://www.example.com/customization1_zip.zip

Note: You do NOT need to sign into the Web Admin Interface Configuration > General to configure the Guest Account Jid Domain field. This field only applies to single Web Bridges configured on this page.

7.2 Installing the Web Bridge Certificate

Note: If you are not using the Acano WebRTC Client, skip this section.

The Web Bridge is used by the Acano WebRTC client. If you are testing this client follow the steps below on the Edge server.

1. Create DNS A record for the Web Bridge and set it to the IP Address of the Ethernet interface you want the Web Bridge to listen on.
2. Create a certificate and private key for the Web Bridge (using the FQDN defined in DNS A record as the Common Name). See the previous section for instructions.
   - Private key can use the .key extension (example: webbridge.key)
   - Certificate can use the .crt extension (example: webbridge.crt)

Note: The Web Bridge supports HTTPS. It will forward HTTP to HTTPS if configured to use “http-redirect”. See later.

3. Upload the certificate file to the MMP via SFTP.
7.3 Adding the Call Bridge Certificate to the Web Bridge Trust Store

The Web Bridge allows configuration of guest logins and image customizations to be pushed from a Call Bridge (see the next section). It is important for the security of the deployment that configuration is only accepted from Call Bridges that are trusted.

Trust between Call Bridge and Web Bridge is established by providing the Web Bridge with the public certificate of the Call Bridge. The Web Bridge can use this to challenge the Call Bridge to prove by cryptographic means that it is the owner of the certificate. Technically, client certificate authentication in TLS is used. If the Call Bridge cannot prove that it is the owner of one of the trusted certificates, the Web Bridge will not accept configuration.

1. In split deployments the Call Bridge certificate needs to be copied from the Core server to the Edge server before you use the `webbridge trust <callbridge_cert>` command on the Edge server.

   On the Acano Core server running Call Bridge server run:

   ```
   46cano>callbridge
   Listening interfaces : a
   Key file : callbridge.key
   Certificate file : callbridge.cer
   ```

   Use SFTP to copy (in this example) “callbridge.cer” from the Core server to the Edge running Web Bridge. Then on the Edge server add the certificate to the Web Bridge trust store:

2. Add the certificate to the Web Bridge’s Trust store using one of the following

   - If you only have one Call Bridge and multiple Web Bridges, sign in to each Web Bridge and add the Call Bridge certificate to each Web Bridge’s trust store using:
     ```
     acano>webbridge disable
     acano>webbridge trust callbridge.cer
     acano>webbridge enable
     SUCCESS: Key and certificate pair match
     SUCCESS: webbridge enabled
     ```

   - If you have several Call Bridges with the same Call Bridge certificate on each Call Bridge then add this Call Bridge certificate to each Web Bridge’s trust store using:
     ```
     acano>webbridge disable
     acano>webbridge trust callbridge.cer
     acano>webbridge enable
     SUCCESS: Key and certificate pair match
     SUCCESS: webbridge enabled
     ```

   - If you have several Call Bridges with different certificate files:
     i. Combine all of their certificates into one trust bundle in one of the following ways:

        - Linux or UNIX-like Operating Systems:
          ```
          cat cert1.crt cert2.crt cert3.crt > yourDomain.ca-bundle
          ```

        - Windows or DOS:
copy cert12.crt + cert2.crt + cert3.crt yourDomain.ca-bundle

yourDomain.ca-bundle’ is only a placeholder file name: use an appropriate name for your deployment.

- Windows 7 command line
  type cert1.pem  cert2.pem > combined.pem

- Manually combine the certificates using Notepad or Notepad++. There must be no spaces on the first certificates “end certificate” line and the second (and further certificates) “begin certificate” line but there MUST be a carriage return at the end of the file. They MUST also be in Base64 encoded format.

ii. Then deploy that certificate bundle on each Web Bridge with the command:
  webbridge trust <crt-bundle>

See the figure below for the current setup on a split deployment.

7.4 Web Bridge Customization

Customization is described in the Acano solution Customization document. From R1.6, WebRTC Client customization has changed in some details and additional customization is possible; but some new features require you to purchase a license key.

Note that customization of Web Bridges (the WebRTC Client landing page) is different between API-configured and Web Admin Interface-configured Web Bridges.

- When using the API (the recommended method) you configure the resourceArchive which is also a URI but points to a .zip file which can contain the two files you used to configure via the Web Admin Interface (the logo and the background image file). See the example later.

- Via the Web Admin Interface Configuration > General page, you configure a custom background image and custom login logo by specifying URIs in the Custom Background Image URI and Custom Login Logo URI fields
Configure Web Bridges

**Figure 15: Web Bridges configured in a split deployment**
7.5 Acano Client and WebRTC Client Information

Not all the features of the Acano solution R1.6 can be tested with Acano clients earlier than v1.3.x – and we strongly recommend upgrading to this client version as they become available. As an absolute minimum, use Acano clients v1.1.x and later because only these clients are multi-TURN server aware.

When a PC Client user calls in:
1. The client does a XMPP SRV lookup to locate the Load Balancer within the cluster to use. By employing a number of rules, a Load Balancer is chosen.
2. The Call Bridge chosen for this call sends the client a list of TURN servers to use.
3. When a call starts, the PC client receives a list of TURN servers to choose from (those configured on the Call Bridge). The PC Client queries the set of possible TURN servers and chooses one based on availability, location and TURN server load.

The Load Balancer and TURN server used for a call do not have to be co-located.

When a WebRTC Client calls in:
1. The user’s web browser performs a simple DNS A record lookup to choose a Web Bridge.
2. The Web Bridge supplies the address of the TURN server for the WebRTC client to use.

The Web Bridge, Load Balancer and TURN server used for a call do not have to be co-located.

7.5.1 Enabling HTTP redirect and the Web Bridge

The Web Bridge supports HTTPS. It will forward HTTP to HTTPS if configured to use “http-redirect”.

1. Enable HTTP redirect with the following command:
   `webbridge http-redirect enable`

2. If required set the ClickOnce location and the Windows MSI, Mac OSX DMG and iOS installers which are presented to WebRTC users:
   `webbridge clickonce <url>
   webbridge msi <url>
   webbridge dmg <url>
   webbridge ios <url>

   **Note:** If you only use browsers that support WebRTC (e.g. Chrome) you do not need to set these download locations because browser functionality will be used for guest access to coSpaces. However, if you use browsers that do not (e.g. IE, Safari) then configure these locations so that when the Acano solution detects the device being used (iOS device, Mac, or PC) it can redirect you to the configured client download link for that device and prompt to install the correct Acano client so that you can join the meeting. After installation, you are connected to the coSpace as a Guest. (Firefox support is currently in beta.)

3. Enable the Web Bridge with the following command:
   `webbridge enable`
8 Configuring the TURN Servers

Unless otherwise noted, these instructions apply equally to combined or split deployments.

Note: While you can still configure a single TURN server via the Web Admin Interface, we strongly suggest that if you have multiple TURN servers you use only the API to configure them, as described below. An example using the POSTMAN tool is provided later.

1. Configure and enable each TURN server.
   a. If necessary, SSH into the MMP.
   b. Configure the XMPP server with the following command:
      ```
      turn credentials <username> <password> <realm>
      ```
      The following is an example where username is myusername, the password is mypassword and it uses the realm example.com.
      ```
      turn credentials myusername mypassword example.com
      ```
   c. If the TURN server located behind a NAT, set the public IP Address that the TURN Server will advertise using:
      ```
      turn public-ip <ip address>
      ```

      Note: If the TURN server has a public IP address rather than being NAT’ed (see the figure below and its notes), this step is not required.

![Diagram of TURN server in DMZ with NAT and public IP address]

**Figure 16: TURN server public IP address**

Note: * Although the port range between the TURN server and the external clients is shown as 32768-65535, currently only 50000-51000 is used. The required range is likely to be larger in future releases.

The following is an example where a public IP address is set to 5.10.20.99
Configuring the TURN Servers

d. Configure the TURN Server to listen on a specific interface using:
   ```
   turn listen <interface whitelist>
   ```
   The following is an example where the interface list is set to interface C but you can specific more than one interface
   ```
   turn listen c
   ```

e. Enable the TURN server with the following command:
   ```
   turn enable
   ```

2. Using the API, set up either a /turnServer/<turn Server id> node for each TURN server on the Call Bridge, or have one node with the DNS record pointing to multiple instances.

   For example, access the API as usual. Then for each TURN server POST to the Call Bridge’s /turnServers node with the following parameter values replaced by your values:

   - `serverAddress = edge1.example.com`
   - `clientAddress = edge1.example.com`
   - `username = fred`
   - `password = password`
   - `type = Acano`

   See the figure over page for the completed deployment.
Figure 17: TURN servers configured in a split deployment
9 coSpaces and User Experience

Note: this chapter describes resilient deployments with XMPP server clustering. The XMPP server cluster feature will be available in a future release.

coSpaces can be created via API calls to any Call Bridge in the cluster, and these coSpaces are visible to all Call Bridges connected to this cluster. An example using the POSTMAN tool is provided later.

- coSpace naming is the same as in previous releases
- A coSpace’s configuration (access methods, URI, passcode(s) etc.) is the same for every member of that coSpace

The two figures below each show two PC Client calls to different coSpaces in a split deployment. This figure demonstrates that:

- All Call Bridges read from the same coSpace database instance irrespective of location
- The control and media routes (and therefore the component instances used) vary depending on the client location. This can involve more than one point of presence – as in the call from the PC Client in London using a TURN server and Load Balancer in a different location

Figure 18: Two PC Clients making calls to different coSpaces in a combined deployment
Figure 19: Two PC Clients making calls to different coSpaces in a split deployment
The following two figures show that when a meeting is hosted on more than one Call Bridge, (a distributed meeting) these Call Bridges exchange the necessary audio and video streams so that each is aware of every participant:

- Joining a meeting in the coSpace is the same experience for every participant regardless of where they are located or which components they use; that is, it is as though the coSpace was hosted on a single Call Bridge
- However, the in-call experience including the layout that each participant sees will depend on the settings for their call leg (set via the API) and who is speaking/the previous speaker—as in a meeting hosted on one Call Bridge

Participants see continuous presence for all participants in the same meeting who are connected to the same Call Bridge as themselves and up to four participants on each of the distributed links to the other Call Bridges.

**Example 1** Participant 1 is on Call Bridge A along with participants 2, 3 and 4. Participants 5, 6, 7 and 8 are on Call Bridge B and participants 9, 10, 11 and 12 are on Call Bridge C. If participant 1 selects the layout to be “all equal” he sees the other 11 participants (numbers 2 through 12).

**Example 2** Participant 1 is on Call Bridge A along with participants 2 and 3. Participants 4, 5, 6 and 7 are on Call Bridge B and participants 8, 9, 10, 11 and 12 are on Call Bridge C. If participant 1 selects the layout to be “all equal” he should see participants 2 to 7 from Call Bridges A and B along with the four most recent speakers from participants 8, 9, 10, 11 and 12 from Call Bridge C.

Whenever a Call Bridge receives a call from an endpoint it queries the other Call Bridge to see whether it already has an instantiation of the coSpace. If it does, a link is established between the two Call Bridges and you end up with a distribution link between them. If more endpoints join the call on either Call Bridge, the link starts to send active participant video streams between the two Call Bridges. When the last endpoint leaves on either side of the distributed call, the link from that Call Bridge to the other one is torn down, and the call is no longer distributed.
Figure 20: Two Call Bridges calling coSpace A in a combined deployment
Figure 21: Two Call Bridges calling coSpace A in a split deployment

Example views and media flows are shown in the two figures below with four participants in a coSpace.
Figure 22: Example media flows and views when PC Clients dial into coSpace A in a combined deployment
Figure 23: Example media flows and views when PC Clients dial into coSpace A in a split deployment
10 Dial Plan Configuration – SIP Endpoints

10.1 Introduction

In order for the Acano solution to be integrated in a SIP, Lync and voice environment, connections need to be set up from the SIP Call Control, Voice Call Control and Lync FE Server components to the Acano solution as shown in Figure 1 above. Changes to the call routing configuration on these devices are required in order to route the calls that require the Acano solution for interoperability correctly to it.

This example (see the figure below) assumes a company deployment which has a mix of SIP video endpoints, Lync clients and IP phones: the Acano solution enables connectivity between Lync clients and SIP video endpoints, and between Lync clients and IP phones.

The SIP video endpoints are configured on a domain called vc.example.com and the Lync clients on example.com. You will need to adapt the example, as appropriate.

Note: Although this figure and subsequent diagrams in this Deployment Guide use an Acano X series deployment as the example, the instructions apply equally to virtualized deployments.

Figure 24: Example solution for dial plan configuration
As shown in the figure above, the Lync FE server needs a Trusted SIP Trunk to the Acano solution, configured to route calls originating from Lync clients through to Acano coSpaces, Acano client users (native and WebRTC) and also SIP video endpoints. The subdomains vc.example.com and acano.example.com should be routed through this trunk from the Lync server to the Acano solution.

The SIP Call Control platform needs a SIP trunk set up to route calls to the example.com domain (for Lync Clients) and acano.example.com (for coSpaces and Acano clients) to the Acano solution.

The Acano solution requires a dial plan to route calls to example.com to the Lync FE server and vc.example.com to the SIP Call Control platform.

The configuration required for the total solution is built up step-by-step below and therefore, to plan your own installation, work through the steps in the order provided adapting the example as appropriate.

**10.2 SIP Endpoints Dialing a Call on the Acano Solution**

As a starting point, consider using only SIP video endpoints and the configuration on the VCS and Acano solution to direct and host calls for these endpoints.

Figure 25: Example of SIP video endpoints calling into an Acano Server hosted calls
10.2.1 SIP call control configuration

This example assumes the SIP Call Control is a Cisco VCS but similar steps are required on other Call Control devices. See the Third Party Call Control Guide.

Set up a zone to route calls to the Acano solution by logging into the VCS as an administrator and following the steps below.

1. Go to VCS Configuration > Zones > New.
2. Create the zone with the following:
   - H.323 Mode = Off.
   - SIP Mode = On
   - SIP Port = 5060 (5061 if using TLS)
   - SIP Transport = TCP or TLS, as appropriate
   - SIP Accept Proxyied Registrations = Allow
   - Authentication Policy = Treat as authenticated
   - SIP Authentication Trust Mode = Off
   - Peer 1 Address = the IP address of the Call Bridge

10.2.2 VCS search rule configuration

Add a search rule on the VCS to route calls to the Acano solution by following the steps below (e.g. to route any video endpoint call to a call on the Acano solution using the call prefix 88).

1. Go to VCS Configuration > Dial Plan > Search rules.
2. Give the rule a suitable name, e.g. VC EPs to Acano.
3. Set the following:
   - Source = Any
   - Request Must Be Authenticated = No
   - Mode = Alias pattern match
   - Pattern Type = Regex
   - Pattern String = .*@acano.example.com
   - Pattern Behavior = Leave
   - On Successful Match = Stop
   - Target = the zone you created for the Acano solution.

10.2.3 Creating a coSpace on the Acano solution

Create a coSpace on the Acano solution for endpoints to dial into as follows:

1. Sign in to the Web Admin Interface.
2. Go to Configuration > CoSpaces.
3. Add a coSpace with:
10.2.4 Adding a dial plan rule on the Acano solution

1. Still in the Web Admin Interface, go to Configuration > Outbound Calls and add a dial plan rule with the following details:
   a. Domain = vc.mycompany.com
   b. SIP Proxy = the IP address or FQDN of your VCS
   c. Local Contact Domain = Note: The local contact domain field should be left blank unless setting up a trunk to Lync (as in section 11.1.2).
   d. Local From Domain = acano.mycompany.com
   e. Trunk Type=Standard SIP.

SIP video endpoints can now dial into a call 88001 hosted on the Acano solution by dialing 88001@acano.mycompany.com

10.3 Media Encryption for SIP Calls

The Acano solution supports media encryption for SIP connections including Lync calls.

This is configured in the Configuration > Call settings page in the Web Admin Interface and allows encryption to be Required, Allowed or Disabled for SIP calls made to or from the Acano solution. Additionally, you can choose whether changes to this setting will apply to SIP calls already in progress (Apply to Active Calls button) or just future calls by using the Submit button at the end of the Call Settings page.

1. Sign in to the Web Admin Interface and go to Configuration > Call settings.
2. Select the appropriate SIP Media Encryption setting (Required, Allowed or Disabled).
3. Click either Submit or Apply to Active calls.

Note: The SIP Encryption field in the Web Admin Interface Configuration > Outbound Calls page allows you to set the behavior for each Outbound Calls dial rule. This separates the control and media encryption behaviour, allowing a TLS control connection to be used in the absence of media encryption, for example. (You can also control SIP control message behavior via the API (see the API Reference guide.)

10.4 Enabling TIP Support

If you use endpoints such as the cisco CTS range, you require the new TIP protocol support available in R1.6. Enable it as follows:

1. In the Web Admin Interface go to Configuration > Call Settings and in the SIP Settings section, set TIP (Telepresence Interoperability Protocol) calls to Enabled.
2. Set both SIP Bandwidth Settings to at least 4000000.

3. Click **Submit**.

**10.5 IVR Configuration**

You can configure an Interactive Voice Response (IVR) to use to manually route to pre-configured calls. Incoming calls can be routed to the IVR where callers are greeted by a prerecorded voice message inviting them to enter the ID number of the call or coSpace that they want to join. Video participants will see a welcome splash screen with the Acano logo. After entering the ID users are routed to the appropriate call or coSpace, or prompted to enter a PIN if the call or coSpace has one. (Callers are disconnected after the third incorrect call ID.)

If you intend to use an IVR follow these instructions:

1. Sign into the Web Admin Interface and go to **Configuration > General**.
2. Configure the following:
   - **IVR Numeric ID** = numeric call ID that users call to reach the IVR
   - **IVR Telephone Number** = external phone number that users have to call to reach the IVR
3. Configure the appropriate routing on your SIP Call Control to ensure that calls to the numbers set in the previous step are routed to the Acano Server.

Note: In R1.6 there is a new Target IVR settings in the Web Admin Interface **Configuration > Inbound Calls** page.
11 Dial Plan Configuration – Integrating Lync

11.1 Lync Clients Dialing into a Call on the Acano solution

This section provides the equivalent of the previous section but for Lync endpoints joining a meeting hosted on the Acano solution. It uses the same call number/URI: adapt the example as appropriate.

![Diagram showing Lync clients calling into Acano server hosted meetings](image)

**Figure 26: Example Lync clients calling into Acano server hosted meetings**

11.1.1 Lync Front End Server configuration

To route calls originating from Lync clients to the Acano solution:

1. Add a Lync static route pointing to the Acano solution matching domain acano.example.com. See the [Appendix with an example](#) for details.

11.1.2 Adding a dial plan rule on the Acano solution

1. Sign in to the Web Admin Interface and go to **Configuration > Outbound Calls**.
2. Set up a dial plan rule with:
   a. Domain = `mycompany.com`
   b. SIP Proxy = the IP address or FQDN of your Lync FE pool or server
c. Local contact domain = callbridge.acano.mycompany.com

Note: The local contact domain field should contain the Fully Qualified Domain Name (FQDN) for the Acano server. It should only be set if setting up a trunk to Lync.

d. Trunk Type = Lync

e. Local From Domain = acano.mycompany.com

f. Leave SIP Proxy to Use blank

Lync clients can now dial into a call 88001 hosted on the Acano solution by dialing 88001@mycompany.com.

11.2 Integrating SIP Endpoints and Lync Clients

To allow both SIP video endpoints and Lync clients to dial into the same meeting, carry out the configuration in both of the previous sections.

Then both SIP video endpoint users and Lync client users can dial <call_id>@acano.example.com to enter the same call.

![Figure 27: Example of SIP video endpoints and Lync clients calling into Acano server hosted meetings](image)

11.3 Web Admin Interface Configuration Pages that Handle Calls

Before going on to expand the examples in the previous sections, it is necessary to understand how the Acano solution determines how to handle each call.

Two configuration pages in the Web Admin Interface control how the Acano solution behaves for incoming and outgoing calls: Outbound Calls and Incoming Calls pages. The Outbound Calls page is for outbound calls; the Incoming calls page determines whether incoming calls are rejected. If they are not rejected, but matched and forwarded, then information about how to forward them is required and the Incoming Calls page has two tables — one to configure
matching/rejection and the other to configure the forwarding behavior. This section provides an overview of these two pages which are then used in the next section to configure the Acano Server to act as a gateway between SIP and Lync calls.

### 11.3.1 Outbound Calls page

The Outbound Calls page allows you to configure an appropriate dial plan comprising a number of dial plan rules. The dial plan controls the routing of outbound calls. Each entry/rule in the dial plan matches on the Domain of the outgoing call (see below) and determines which SIP proxy to use (or whether it is a direct call).

The Local Contact Domain is the domain that will be used for the contact URI for calls using this rule. The Local From Domain is the domain the call uses as its originator ID/Caller ID.

#### CAUTION: From R1.2 there has been the ability to configure an explicit contact domain to be used: if you are using Lync, we suggest that you use the Local Contact Domain. If you are not using Lync we recommend that the Local Contact Domain field is left blank to avoid unexpected issues with the SIP call flow.

![Outbound calls table]

<table>
<thead>
<tr>
<th>Domain</th>
<th>SIP proxy to use</th>
<th>Local contact domain</th>
<th>Local from domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>lync.example.com</td>
<td>&lt;none; call directly&gt;</td>
<td>example.com</td>
<td>example.com</td>
</tr>
<tr>
<td>&lt;match all domains&gt;</td>
<td>10.1.1.77</td>
<td>example.com</td>
<td>example.com</td>
</tr>
</tbody>
</table>

Usually, you set up rules to route calls out to third party SIP control devices such as Cisco VCS, Avaya Manager or Lync servers. Therefore, there are currently three types of SIP trunks you can configure: Standard SIP, Lync and Avaya.

Note: A common use of the Acano solution is with an Avaya PBX; these calls will be audio-only. However, the Acano solution does not impose this restriction on interoperability with Avaya products (some of which support video also): therefore a call of type of ‘avaya’ does not imply that the call is audio-only.

Dial plan rules are tried in the order of the Priority values. In the current Acano solution version only one match is possible for a call and even if there would be other matches in lower priority rules they will not be reached; therefore the Priority is important.
CAUTION: The default Encryption behavior mode is Auto. This does not match pre-R1.2 behavior. Previously, all "Lync" outbound dialing rules would automatically use Encrypted mode; therefore you need to ensure that these rules are explicitly set to Encrypted mode to prevent the Call Bridge attempting to use unencrypted TCP for these connections in the event of the TLS connection attempt failing.

11.3.2 Incoming Call page: call matching

The top table in the Incoming Call page is the Call Matching table. The rules defined in the Call Matching table govern how the Acano solution handles incoming SIP calls. Any call routed to the Acano Server on any domain can be tested for a match for Acano client users or for preconfigured coSpaces on that server.

The example Call matching rule below seeks to match all calls coming in on the acano.example.com domain to both Acano users and coSpaces.

For example, if the incoming call was to name.cospace@acano.example.com and there was a configured coSpace called name.coSpace the call would be routed to the coSpace with that name. If the incoming call was to firstname.lastname@acano.example.com the call would be routed to that user with that first and last name.

Alternatively, you can choose not to route calls to users or coSpaces on a per domain basis; that is, you can use one incoming domain for coSpaces and another for users.

After a rule is executed rules further down the list are ignored for the call.

If all Call matching rules fail, the next table (Call Forwarding) is used as described in the next section.

Note1: Matching for coSpace and/or users is only done on the part of the URI before the @.

Note2: You cannot configure more than one rule with same destination.

Note3: If the Domain is left blank in a rule, the rule matches any call. If no match is found then the Call Forwarding table is used.

11.3.3 Call forwarding

If a call fails to match any of the rules in the Call Matching table in the Incoming Calls page, the call will be handled according to the Call Forwarding table. In this table you can have rules decide whether to reject the call outright or to forward the call in bridge mode. Rules can overlap, and include wildcards. You order rules using the Priority value; higher numbered rules are tried first.

By defining rules, you decide whether to forward the call or not. It might be appropriate to “catch” certain calls and reject them.
For calls that will be forwarded, you can rewrite the Lync destination domain using the Forwarding Domain. A new call is created to the specified domain.

The example Call forwarding rule below forwards calls for the domain lync.example.com and the routing is determined by the call routing rules.

<table>
<thead>
<tr>
<th>Domain matching pattern</th>
<th>Priority</th>
<th>Forward</th>
<th>Caller ID</th>
<th>Rewrite domain</th>
<th>Forwarding domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>lync.example.com</td>
<td>50</td>
<td>forward</td>
<td>pass through</td>
<td>no</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>reject</td>
<td>use dial plan</td>
<td>no</td>
<td></td>
</tr>
</tbody>
</table>

If none of the Domain Matching Patterns matches the domain of an incoming call that was not matched in the Call Matching section, the call is terminated.

### 11.4 Adding Calls between Lync Clients and SIP Video Endpoints

This section assumes the configuration described in the two dial plan configuration sections has been completed. It expands the example to allow Lync and SIP video endpoints to call each other in a call using the Acano server as a gateway to transcode the video and audio (see the figure below).

Note: The Outbound Calls page was used previously to set up a SIP trunk from the Acano server to the Cisco VCS. In order to configure the Acano server to act as a "point-to-point bridge" between Lync and SIP environments, you need to configure call forwarding as described in this section and also set up a SIP trunk from the Acano Server to other SIP call control devices you are using such as the Lync FE server and Cisco VCS, CUCM, Avaya CM or Polycom DMA (see the appropriate appendix).

![Diagram showing call flow](image-url)

**Figure 28:** Example of SIP video endpoints and Lync clients in calls
In this example:

- A Lync user can dial `<name>@vc.example.com` to set up a call with a SIP video endpoint who is `<name>@vc.example.com`.
- A SIP video endpoint can dial `<name>@example.com` to set up a call with a Lync endpoint who is `<name>@example.com`.

Adapt the example as appropriate.

11.4.1 Lync Front End Server configuration

To allow Lync clients to call SIP video endpoints:

1. Add a Lync static route pointing to the Acano solution for `vc.example.com`.

11.4.2 VCS configuration

To route SIP video endpoint calls to Lync clients:

1. Add a search rule on the VCS to route calls with the suffix `@example.com` to the Acano solution.

11.4.3 Acano solution configuration

Perform the following steps so that all calls to the Acano solution that are not matched to Acano users or coSpaces are forwarded.

1. Sign in to the Web Admin Interface and go to Configuration > Incoming Calls.
2. In the Call Forwarding section, add a new rule as follows:
   - Domain Matching Pattern = *
     Wildcards are permitted in any part of a domain matching pattern.
     (Unmatched calls with a domain that matches this pattern are forwarded using this rule.)
   - Priority: To ensure that this rule is always used, its priority should be the highest of any rules configured (any value, including 0, is acceptable if there are no other forwarding rules configured).
     (Rules are checked in order of priority; highest priority first. If two Domain Matching Patterns would match a destination domain the rule with the higher priority is used.)
   - Forward = forward
     (If you select Reject calls that matched the Domain Matching Pattern are not forwarded but terminate.)
   - Rewrite Domain = no
     The call will be forwarded using the domain that was called.
     (If you select yes here, you must then complete the Forward Domain. The original domain will be replaced with the one you enter in Forward Domain before the call is forwarded.)
3. Click Add new.

SIP video endpoints can now call Lync clients by dialing `<name>@example.com`, and Lync clients can call SIP video endpoints by dialing `<endpoint>@vc.example.com`. 
11.5 Integrating Acano Clients with SIP and Lync Clients

Refer to the LDAP Configuration and Configuring the XMPP server sections for instructions about configuring your Acano solution to use the Acano clients.

If you are using the same LDAP configuration to create both your Lync accounts and Acano clients, problems may occur if a user tries to call a Lync client when using the Acano solution as a gateway because the user may end up calling your Acano XMPP client. The Acano Configuration > Incoming Calls page has a table of rules (Call Matching section) to prevent this.

For example, assume you have an account fred@example.com on the Acano solution. I also have a fred@lync.example.com account on my Lync FE server. If a call arrives at the Acano solution and no Call Matching rules are configured, the Acano solution will ignore the domain and the call will go to the Acano solution’s fred@example.com account. In other words, dialing fred@xxxx will ignore xxxx and see if there is a user “fred” locally.

This is problematic because a user trying to call the Lync address fred@lync.example.com using the Acano solution as a gateway will end up in a call with the Acano XMPP client logged in as fred@example.com. If the same LDAP structure has been used to create both the Acano solution’s and the Lync’s user accounts, this will be a common problem.

The solution is to configure the Incoming Calls page with the Domain Name field set to something distinct from the domain that the Lync FE server uses. In the example above, a sensible choice for the Domain Name field would be example.com. Then, a call to fred@example.com will reach the Acano client but a call to fred@lync.example.com or fred@xxxx will not. Instead, if the Call Forwarding section is set up, the Acano solution forwards the call on.

11.6 Lync Edge Server Integration

11.6.1 Lync Edge Call Flow

To establish a call from the Acano Server to the Lync Edge server (see the figure below):

1. The Acano Call Bridge makes a “register” SIP call to the Lync Front End server.
2. The “register” is acknowledged.
3. The Call Bridge sends a “subscribe” to the Lync Front End server.
4. The Front End server returns the URI of the media relay authentication server (MRAS). (The Lync Edge Server acts as a MRAS.)

5. (and 6) Call Bridge contacts the MRAS over SIP to get the Edge information for the call. The call media then flows directly between the Call Bridge and Edge’s TURN server on UDP port 3478 and returns from Edge server to the Call Bridge on a port in the ephemeral range above.

Therefore the following ports need to be opened in the firewall for the media between Call Bridge and the Edge server: UDP 3478 outgoing and 32768-65535 incoming.

11.6.2 Configuration for using Lync Edge

To use a Lync Edge server, log in to the Web Admin Interface, go to Configuration > General and configure the Lync Edge Settings. (When a Lync Edge server is configured, it takes the
TURN / ICE role for Lync calls, and so at some level is an alternative to the TURN Server Settings above.)

You also need to create a Lync user client account to set up the Acano Lync Server Edge configuration.

Follow these steps to set up the Acano solution to use the Lync Edge server:

1. Ensure that you have the appropriate DNS records in place; see the appendix on DNS records for the full requirements.

2. Create a new user in your LDAP directory, just as you would any other user in your directory, i.e. firstname="acano", second name = “edge”.

3. Login into the user manager on your Lync Server and create a Lync Client user from the user you created in the previous step. Do thus in the same way as you would any other user to enable them to use Lync. Using the example name above create a Lync client user called acano.edge@lync.example.com

4. Sign in to the Web Admin Interface, and go to Configuration > General. Configure the Lync Edge Settings by entering the Lync Front End Server Address (or a host name that resolves to this). For Username enter the Lync client user name created in the previous step.

5. Complete the Number of Registrations field, if necessary.

   This field overcomes a feature of the Lync Edge server that limits the number of simultaneous calls that it will run for one registered device. By entering a number greater than 1, the Call Bridge will make that number of registrations, thereby increasing the number of simultaneous calls that the Acano solution can make out through the Lync Edge Server.

   Entering a number greater than 1 adds a number to the end of your Lync Edge username and registers with the resulting username. For example, if you configured Username as edgeuser@example.com and set Number of Registrations to 3, you will need to create the following users in your Lync environment so that they can be used with the Edge server;

   edgeuser1@example.com
   edgeuser2@example.com
   edgeuser3@example.com

   We recognize that this requires some administrative overhead; however it is due to a limitation of the Lync Edge server as explained above.

   Leave the Number of Registrations blank to only make a single registration as edgeuser@example.com.

---

Note: The Acano solution supports Lync content (presentations contributed over RDP) from external Lync clients whose media arrives via the Lync Edge server. In addition, coSpace (URIs) now report back as busy or available based on how many participants are currently in the coSpace so that Lync clients that have Acano coSpaces in their favorites can see the coSpace status.

Note: Acano clients continue to use the Acano TURN Server even if a Lync Edge server is configured.

Note: If you have a Lync Edge server configured, all Lync calls will use that server for ICE candidate gathering and external media connectivity. If you do not have a Lync Edge server configured, Lync calls handled by the Acano solution will use any configured TURN server.
11.7 Lync Federation

Acano solution R1.6 adds support for federation with Microsoft Lync. This allows calls to be made from the Acano server to any Lync domain and vice versa.

To allow inbound calls you must:

1. create the DNS SRV record _sipfederationtls._tcp.domain.com that points to the FQDN of the Acano server. This step is required as Call Bridge will need to have a public IP, and NAT is not supported in this scenario.

2. add a DNS A record that resolves the FQDN of the Acano server to a public IP address.

3. upload a certificate and certificate bundle to the Acano server that complies with the following:
   a. the certificate must have the FQDN as the CN, or if using a certificate with a SAN list then ensure that the FQDN is also in the SAN list. Note: if the certificate contains a SAN list, then Lync will ignore the CN field and only use the SAN list.
   b. the certificate must be signed by a real CA.
   c. the certificate bundle must contain the Root CA’s certificate and all intermediate certificates in the chain in sequence, so that a chain of trust can be established.

   **Note:** for more information on certificates refer to the Introduction in the [Acano Certificate Guidelines](#).

4. Open the appropriate Firewall ports as stated in the [Acano Deployment Guide](#) for example: TCP 5061, UDP 3478, UDP 32768-65535, TCP 32768-65535

For outbound calls from Acano:

1. create an outbound dial rule, leave the Domain and SIP proxy fields blank, and set Trunk type as Lync. Also set the appropriate Local contact domain and the Local from domain fields.
12 LDAP Configuration

Note: The Acano solution supports multiple LDAP servers via the API: the Web Admin Interface only allows you to configure one. See the LDAP Methods section in the API Reference.

You must have an LDAP server to use the Acano solution. User accounts are imported from the LDAP server. You can create user names by importing fields from LDAP as described in this section. The passwords are not cached on the Acano solution, a call is made to the LDAP server when an Acano client authenticates, and therefore passwords are managed centrally and securely on the LDAP server.

12.1 Why use LDAP?

Using LDAP to configure the Acano solution is a powerful and scalable way to set up your environment: defining your organization’s calling requirements within the LDAP structure minimizes the amount of configuration required on the Acano solution.

The solution uses the concept of filters, rules and templates (which will be expanded in future releases).

Filters allow you to separate users into groups, for example:

- Everyone in the HR department
- Staff at grade 11 and above
- Job title = ‘director’
- People whose surname starts with ‘B’

Then rules (actions) can be applied on these groups, for example:

- Give users in this group the ability to create new coSpaces
- Associate users in this group to one or more existing coSpaces, e.g. the 'HR managers CoSpace’
- Create a personal coSpace for each user in this group
- Apply a template to this group of users

Templates define things such as which default layout to use, or what maximum call rate is allowed. For example, if a new employee joins the organization as a manager with a grade >11, just based on his job title or grade he can be set up automatically with a personal coSpace, have the ability to create new coSpaces, have a 4Mbps call rate and be assigned to the “all managers” coSpace. In contrast, another new joiner with job title "temp” might be configured with a default call rate of 500kbps.

12.2 Acano Solution Settings

This example assumes you are using Microsoft Active Directory (AD).

To set up the Acano solution to work with AD, follow these steps:

1. Sign in to the Web Admin Interface and go to Configuration > Active Directory.
2. Configure the connection to the LDAP server in the first section with the following:
   - **Address** = this is the IP address of your LDAP server
   - **Port** = usually 636
   - **Username** = the Distinguished Name (DN) of a registered user. You may want to create a user for this purpose
   - **Password** = the password for the user name you are connecting as
   - **Secure Connection** = select this setting for a secure connection

   For Example:
   - **Address**: 100.133.2.44
   - **Port**: 636
   - **Username**: cn=Fred Bloggs,cn=Users,OU=Sales,dc=YourCompany,dc=com
   - **Password**: password

   Note: The Acano solution supports secure LDAP. By default the LDAP server runs on port 636 for secure communications and port 389 for insecure communications. The Acano solution supports both but we recommend using 636. Note that you must select Secure Connection (see above) for communications to be secure: using port 636 alone is not enough.

3. The Import Settings control which users should be imported.
   - **Base Distinguished Name** = the node in the LDAP tree from which to import users. The following is a sensible choice for base DN to import users
     - `cn=Users,dc=sales,dc=YourCompany,dc=com`
   - **Filter** = a filter expression that must be satisfied by the attribute values in a user's LDAP record. The syntax for the Filter field is described in rfc4515.
     - A rule for importing people into the main coSpace database might reasonably be 'import anyone with an email address', and this is expressed by the following filter:
       - `mail=*`

     For testing purposes you may want to import a named user and a group of test users whose mail address starts with "test"; for example:
     - `(|(mail=fred.bloggs*)(mail=test*))`

     If you wanted to import everyone apart from one named user, use this format:
     - `(! (mail=fred.bloggs*))`

     To import users that belong to a specific group, you can filter on the `memberOf` attribute. For example:
     - `memberOf=cn=apac,cn=Users,dc=Example,dc=com`

     This imports both groups and people that are members of the APAC group. To restrict to people, use:
Using an extensible matching rule (LDAP_MATCHING_RULE_IN_CHAIN / 1.2.840.113556.1.4.1941), it is possible to filter on membership of any group in a membership hierarchy (below the specified group); for example:

`(&(memberOf:1.2.840.113556.1.4.1941:=cn=apac,cn=Users,dc=Example,dc=com)(objectClass=person))`

Other good examples which you can adapt to your LDAP setup include:

- Filter that adds all Person and User except the ones defined with a !
  `((&(objectCategory=person)(objectClass=user)(!(cn=Administrator))((cn=Guest))))
   (!(cn=krbtgt)))`

- Filter that adds same as above (minus krbtgt user) and only adds if they have a sAMAccountName
  `(&(objectCategory=person)(objectClass=user)(!(cn=Administrator))
   (!(cn=Guest)))((sAMAccountName=*))`

- Filter that adds same as above (Including krbtgt user) and only adds if they have a sAMAccountName
  `(&(objectCategory=person)(objectClass=user)(!(cn=Administrator))
   (!(cn=Guest)))((cn=krbtgt))((sAMAccountName=*))`

- This filter only imports specified users within (|( tree
  `((&(objectCategory=person)(objectClass=user)(|(cn=accountname)(cn=
    anotheraccountname)))
   ((cn=accountname)|(cn=anotheraccountname)))
   
   Global Catalog query to import only members of specified security group (signified
   with =cn=xxxxx
  `(&(memberOf:1.2.840.113556.1.4.1941:=cn=groupname,cn=Users,dc=example,dc=com)(objectClass=person))`)

4. Set up the Field Mapping Expressions

The field mapping expressions control how the field values in the Acano solution’s user records are constructed from those in the corresponding LDAP records. Currently, the following fields are populated in this way:

- Display Name
- User name
- coSpace Name
- coSpace URI user part (i.e. the URI minus the domain name)
- coSpace Secondary URI user part (optional alternate URI for coSpace)
- coSpace call id (unique ID for coSpace for use by WebRTC client guest calls)

Field mapping expressions can contain a mixture of literal text and LDAP field values, as follows:

`$<LDAP field name>$`

As an example, the expression
$sAMAccountName$@example.com

Generates:
fred@example.com

For more information see the section on LDAP field mappings.

Note: Each imported user must have a unique XMPP user ID (JID), constructed using the JID field in the Field Mapping Expressions section of the Configuration > Active Directory. In order to construct a valid JID, any LDAP attribute used in the JID field mapping expression must be present in each LDAP record that is to be imported. To ensure that only records that have these attributes present are imported, we recommend that you include presence filters (i.e. those of the form (attribute name=*)) using a ‘&’ (AND) in the Filter field under Import Settings for each attribute used in the JID field mapping expression.

For example, suppose your JID field mapping expression is $sAMAccountName$@company.com, and you wish to import users who are members of the group cn=Sales,cn=Users,dc=company,dc=com, an appropriate import filter would be

(&memberOf=cn=Sales,cn=Users,dc=company,dc=com)(sAMAccountName=*))

5. To synchronize with AD, select Sync now or activate the synchronization by using the appropriate API call (see the Acano solution API Reference).

   Note that you must manually resynchronize whenever entries in the LDAP server change.

6. View the result of the synchronization by going to Status > Users.

It is possible to choose whether to use OU separation when importing from the LDAP server. In the Web Admin Interface, go to Configuration > Active Directory and select Restrict Search to Searcher OU to enable the search only within the OU of the user account.

12.3 Example

You want to assign a coSpace to a particular group of users and a Call ID for this coSpace using an 88 prefix in front of the regular telephone number.

1. Create the group in the LDAP structure called “cospace” and assign the required members to that group.

2. Use the following filter which uses the extensible matching rule (LDAP_MATCHING_RULE_IN_CHAIN / 1.2.840.113556.1.4.1941) to find all the users that are a member of the “cospace” group:

   (&(memberOf:1.2.840.113556.1.4.1941:=cn=cospace,cn=Users,dc=lync,dc=example,dc=com)(objectClass=person))
3. Then synchronizing a particular user in the directory called:
   - cn = Fred Blogs
   - TelephoneNumber = 7655
   - sAMAccountName = fred.blogs

creates the following coSpace which can be viewed on the Status > Users page.

<table>
<thead>
<tr>
<th>Name</th>
<th>XMPP id</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fred Blogs</td>
<td><a href="mailto:fred.blogs@xmpp.example.com">fred.blogs@xmpp.example.com</a></td>
</tr>
</tbody>
</table>

And the following coSpace that can be viewed on the Configuration > coSpace page.

<table>
<thead>
<tr>
<th>Name</th>
<th>URI user part</th>
</tr>
</thead>
<tbody>
<tr>
<td>fred.blogs</td>
<td>fred.blogs.cospace</td>
</tr>
</tbody>
</table>
12.4 More Information on LDAP Field Mappings

This section provides additional information for LDAP field mappings that you set up for the Acano solution.

Parts of an LDAP field value can be substituted by means of a sed-like construction, as follows:

`${<LDAP field name}>|'/<regex>/'<replacement format>/'<option>'$

1. `<option>` can be `g`, to replace every match of `<regex>` with `<replacement format>`, or blank to match only the first
2. parts of `<regex>` can be tagged for use in `<replacement format>` by enclosing them in round brackets
3. tagged matches can be referenced in `<replacement format>` as `\x` where `x` is a digit from 0 to 9. Match 0 corresponds to the entire match, and matches 1-9 the 1st to 9th tagged sub-expressions
4. single quotes inside the substitution expression must be escaped with a backslash, as must backslash characters themselves
5. any character other than a single quote, a backslash, or the digits 0-9 can be used in place of the forward slash that separates the components of the substitution expression
6. if the separating character is to be used as a literal within the expression, it must be escaped with a backslash

As an example, the following would convert

`firstname.lastname@test.example.com`

addresses into

`firstname.lastname@xmpp.example.com JIDs`

`$mail|'@test/@xmpp/'$

and the following would remove every lower case 'a' from the user's full name

`$cn|'/a//g'$

A sensible set of expressions for use might be:

- **Full name:** `$cn$
- **JID:** `$mail|'@test/@xmpp/'$
- **CoSpace URI:** `$mail|'@.*//'.$cospace$
- **CoSpace dial-in number:** `$ipPhone$


13 Additional Security Considerations & QoS

A number of security issues have already been discussed (e.g. certificates) but the Acano solution R1.6 offers a number of additional functions for securing your deployment. These are described in this section.

13.1 Common Access Card (CAC) integration

The Common Access Card (CAC) is used as an authentication token to access computer facilities. The CAC contains a private key which cannot be extracted but can be used by on-card cryptographic hardware to prove the identity of the card holder. The Acano solution R1.6 supports administrative logins to the SSH and Web Admin Interface using CAC.

The MMP commands available are (also see the MMP Command Reference)

- `cac enable|disable [strict]`: enables/disables CAC mode with optional strict mode removing all password-based logins
- `cac issuer <ca cert-bundle>`: identifies trusted certificate bundle to verify CAC certificates
- `cac ocsp certs <key-file> <crt-file>`: identifies certificate and private key for TLS communications with OCSP server, if used
- `cac ocsp responder <URL>`: identifies URL of OCSP server
- `cac ocsp enable|disable`: enables/disables CAC OCSP verification

13.2 Online Certificate Status Protocol (OCSP)

OCSP is a mechanism for checking the validity and revocation status of certificates. The MMP can use OCSP to work out whether the CAC used for a login is valid and, in particular, has not been revoked.

13.3 FIPS

You can enable a FIPS 140-2 level 1 certified software cryptographic module, then cryptographic operations are carried out using this module and cryptographic operations are restricted to the FIPS approved cryptographic algorithms.

The MMP commands to use are (also see the MMP Command Reference guide)

- `fips enable|disable`, enables/disables the FIPS-140-2 mode cryptography for all cryptographic operations for network traffic. After enabling or disabling FIPS mode, a reboot is required
- `fips`, displays whether FIPS mode is enabled
- `fips test`, runs the built-in FIPS test
13.4 TLS Certificate Verification
You can enable Mutual Authentication for SIP and LDAP in order to validate that the remote certificate is trusted. When enabled, the Call Bridge will always ask for the remote certificate (irrespective of which side initiated the connection) and compare the presented certificate to a trust store that has been uploaded and defined on the server.

The MMP commands available are (also see the MMP Command Reference guide):

- `tls <sip|ldap> trust <crt bundle>`: defines Certificate Authorities to be trusted
- `tls <sip|ldap> verify enable|disable|ocsp`: enables/disables certificate verification or whether OCSP is to be used for verification
- `tls <sip|ldap>`: displays current configuration

13.5 User Controls
Admin users can:

- Reset another user’s password
- Set the maximum number of characters that can be repeated in a user’s password – and there are a number of other user password rule additions
- Limit MMP access by IP address
- Disable MMP accounts after configurable idle period

13.6 Firewall Rules
In R1.6 the MMP supports the creation of simple firewall rules for both the media and admin interfaces. Note that this is not intended to be a substitute for a full standalone firewall solution and therefore is not detailed here.

Firewall rules must be specified separately for each interface. See the MMP Command Reference for full details and examples.

**CAUTION**: We recommend using the serial console to configure the firewall, because using SSH means that an error in the rules would make the SSH port inaccessible. If you must use SSH then ensure that an `allow ssh` rule is created for the ADMIN interface before enabling the firewall.

13.7 DSCP
You can enable DSCP tagging for the different traffic types on the Acano server (see the MMP Command Reference).

1. Sign in to the MMP and set the DSCP values as required.
2. Go to **Configuration > Call Settings** and set the DSCP Mode as follows:
   - In a non-AS SIP environment, select Use Normal Values
   - In an AS SIP environment, select Use Assured Values
Note: DSCP tagging is for all packets being sent from the Acano solution only. For PC Client DSCP tagging, Group Policy must be used to define desired DSCP values because Windows controls this, and normal user accounts have no permissions to set DSCP.
## Appendix A  DNS Records Needed for a Scalable and Resilient Acano Solution

Note: Verify that no A or SRV records already exist for any Acano servers before defining the records below.

<table>
<thead>
<tr>
<th>Type</th>
<th>Example</th>
<th>Resolves to</th>
<th>Resilience considerations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRV(*)</td>
<td>_xmpp-client._tcp.example.com</td>
<td>The A record xmpp.example.com below. Usually this is port 5222.</td>
<td>One SRV record can be created for each XMPP server/Load Balancer such that multiple results are returned in response to a DNS lookup. Clients choose a destination for XMPP traffic based on the priority and weight information.</td>
<td>Used by clients to login. The SRV record must correspond to the domain used in your XMPP usernames.</td>
</tr>
<tr>
<td>SRV(*)</td>
<td>_xmpp-server._tcp.example.com</td>
<td>The A record xmpp.example.com below. Usually this is port 5269.</td>
<td>One SRV record can be created for each XMPP server/Load Balancer such that multiple results are returned in response to a DNS lookup. Clients choose a destination for XMPP traffic based on the priority and weight information.</td>
<td>Used to federate between XMPP servers. The SRV record must correspond to the domain used in your XMPP usernames.</td>
</tr>
<tr>
<td>A</td>
<td>xmpp.example.com</td>
<td>IP address of either the XMPP server or a Load Balancer which is configured to trunk to the XMPP server.</td>
<td>One A record per XMPP server or Load Balancer.</td>
<td></td>
</tr>
<tr>
<td>A /</td>
<td>join.example.com</td>
<td>IP address of Web Bridge</td>
<td>One A and/or AAAA record per Web Bridge. The decision on which Web Bridge your browser uses is made by your web browser. Normally the choice is random.</td>
<td>This record is not used by the Acano solution directly; however, it is common practice to provide an end user with an FQDN to type into the browser which resolves to the Web Bridge. There is no restriction or requirement on the format of this record.</td>
</tr>
<tr>
<td>AAAA</td>
<td>join.example.com</td>
<td>IP address of Web Bridge</td>
<td>One A and/or AAAA record per Web Bridge. The decision on which Web Bridge your browser uses is made by your web browser. Normally the choice is random.</td>
<td>This record is not used by the Acano solution directly; however, it is common practice to provide an end user with an FQDN to type into the browser which resolves to the Web Bridge. There is no restriction or requirement on the format of this record.</td>
</tr>
<tr>
<td>A /</td>
<td>ukedges.example.com</td>
<td>IP addresses of any</td>
<td>Each Core server in a given datacenter should be listed.</td>
<td>Used in split deployments.</td>
</tr>
</tbody>
</table>

_Acano solution: Scalability & Resilience Deployment R1.6 76-1040-03-Kb_
<table>
<thead>
<tr>
<th>Type</th>
<th>Example</th>
<th>Resolves to</th>
<th>Resilience considerations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAAA</td>
<td>nyedges.example.com</td>
<td>local Load Balancers</td>
<td>trunk to only the Edge servers within that datacenter. In our example, ukedges.example.com would return the IP address of all Load Balancers within the UK datacenter</td>
<td>only by the Core server to create a trunk to a Load Balancer running on the Edge server</td>
</tr>
<tr>
<td>A / AAAA</td>
<td>ukcore1.example.com</td>
<td>IP address of the Call Bridge</td>
<td>One record per Call Bridge. Each Call Bridge must have a unique FQDN</td>
<td>Used by the Lync FE server to contact the Call Bridge</td>
</tr>
<tr>
<td></td>
<td>nycore1.example.com</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A / AAAA</td>
<td>ukcore1admin.example.com</td>
<td>IP address of the MMP interface</td>
<td>One record per Web Admin Interface. Each MMP interface must have a unique FQDN</td>
<td>This record it is used purely for admin purposes; when system administrators prefer a FQDN to remember for each MMP interface</td>
</tr>
<tr>
<td></td>
<td>ukedge1admin.example.com</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>nycore1admin.example.com</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix B  Ports Required for a Scalable and Resilient Deployment

The following diagram labels the links on which ports need to be open and shows which firewall is concerned.

Figure 30: Ports that must be open in an Acano solution deployment
**Ports Required for a Scalable and Resilient Deployment**

![Diagram of Acano solution: Scalability & Resilience Deployment](image)

**Figure 31: Additional ports required to be open in an Acano multiple deployment solution deployment**

The following ports are required by the Call Bridge.

<table>
<thead>
<tr>
<th>Function</th>
<th>Destination Port</th>
<th>Type</th>
<th>Direction</th>
<th>Used on Link(s)</th>
<th>Configurable?</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>80</td>
<td>TCP</td>
<td>Incoming</td>
<td>M</td>
<td>MMP</td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
<td>TCP</td>
<td>Incoming</td>
<td>M, N</td>
<td>MMP (for N)</td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
<td>TCP</td>
<td>Outgoing</td>
<td>E</td>
<td></td>
</tr>
<tr>
<td>SIP UDP</td>
<td>5060</td>
<td>UDP</td>
<td>Both</td>
<td>I, T</td>
<td></td>
</tr>
<tr>
<td>SIP TCP</td>
<td>5060</td>
<td>TCP</td>
<td>Both</td>
<td>I, T</td>
<td></td>
</tr>
<tr>
<td>SIP TLS</td>
<td>5061</td>
<td>TCP</td>
<td>Both</td>
<td>I, K, T</td>
<td></td>
</tr>
<tr>
<td>SIP BFCP</td>
<td>32768-65535</td>
<td>UDP</td>
<td>Incoming</td>
<td>II, T</td>
<td></td>
</tr>
<tr>
<td>SIP BFCP</td>
<td>1024-65535 #</td>
<td>UDP</td>
<td>Outgoing</td>
<td>II, T</td>
<td></td>
</tr>
<tr>
<td>TURN</td>
<td>3478</td>
<td>UDP</td>
<td>Outgoing</td>
<td>D, O</td>
<td></td>
</tr>
<tr>
<td>TURN</td>
<td>443</td>
<td>TCP</td>
<td>Outgoing</td>
<td>O</td>
<td></td>
</tr>
<tr>
<td>STUN/RTP</td>
<td>32768-65535</td>
<td>UDP</td>
<td>Incoming</td>
<td>D, I, II, JJ, K,</td>
<td></td>
</tr>
<tr>
<td>STUN/RTP</td>
<td>32768-65535</td>
<td>UDP</td>
<td>Incoming</td>
<td>O, T</td>
<td></td>
</tr>
<tr>
<td>STUN/RTP</td>
<td>1024-65535 #</td>
<td>UDP</td>
<td>Outgoing</td>
<td>II, JJ, K</td>
<td></td>
</tr>
<tr>
<td>STUN/RTP</td>
<td>32768-65535</td>
<td>UDP</td>
<td>Outgoing</td>
<td>D, T</td>
<td></td>
</tr>
<tr>
<td>RDP</td>
<td>32768-65535</td>
<td>TCP</td>
<td>Incoming</td>
<td>KK</td>
<td></td>
</tr>
<tr>
<td>RDP</td>
<td>1024-65535++</td>
<td>TCP</td>
<td>Outgoing</td>
<td>KK</td>
<td></td>
</tr>
<tr>
<td>LDAP/LDAPS</td>
<td>389/636</td>
<td>TCP</td>
<td>Outgoing</td>
<td>H</td>
<td>Web Admin Interface</td>
</tr>
<tr>
<td>DNS</td>
<td>53</td>
<td>UDP</td>
<td>Outgoing</td>
<td>G</td>
<td></td>
</tr>
<tr>
<td>XMPP/Secure XMPP</td>
<td>5223 +</td>
<td>TCP</td>
<td>Outgoing</td>
<td>U</td>
<td>Web Admin Interface</td>
</tr>
<tr>
<td>CDR</td>
<td>Set in Web Admin Interface</td>
<td>TCP</td>
<td>Outgoing</td>
<td>N</td>
<td>Web Admin Interface</td>
</tr>
</tbody>
</table>
Ports Required for a Scalable and Resilient Deployment

| Database cluster / replication ports | 5432 | TCP | Both | S |
| XMPP cluster (not currently available) | 3999 | TCP | Both | R |
| Call Bridge cluster | 443 | TCP | Both | T |

+ this port is not required if the Call Bridge and XMPP server are on the same Core server but for deployments with multiple Core servers, each Call Bridge must be able to reach all of the XMPP servers for resilience.

++ Exact range depends on configuration on Lync server

# Exact range depends on far end

The following ports are used by MMP

<table>
<thead>
<tr>
<th>Function</th>
<th>Destination Port</th>
<th>Type</th>
<th>Direction</th>
<th>Used in Link(s)</th>
<th>Configurable?</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH</td>
<td>22</td>
<td>TCP</td>
<td>Incoming</td>
<td>M</td>
<td></td>
</tr>
<tr>
<td>Syslog</td>
<td>514</td>
<td>TCP</td>
<td>Outgoing</td>
<td>F</td>
<td>MMP</td>
</tr>
<tr>
<td>NTP</td>
<td>123</td>
<td>UDP</td>
<td>Outgoing</td>
<td>L</td>
<td></td>
</tr>
<tr>
<td>SNMP</td>
<td>161</td>
<td>UDP</td>
<td>Outgoing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SNMP</td>
<td>162</td>
<td>UDP</td>
<td>Outgoing</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The following ports are used by the Web Bridge

<table>
<thead>
<tr>
<th>Function</th>
<th>Destination Port</th>
<th>Type</th>
<th>Direction</th>
<th>Used in Link(s)</th>
<th>Configurable?</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>80</td>
<td>TCP</td>
<td>Incoming</td>
<td>B</td>
<td>MMP</td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
<td>TCP</td>
<td>Incoming</td>
<td>B</td>
<td>MMP</td>
</tr>
<tr>
<td>XMPP</td>
<td>5222</td>
<td>TCP</td>
<td>Outgoing</td>
<td>A, B</td>
<td></td>
</tr>
<tr>
<td>Load Balancer</td>
<td>5222</td>
<td>TCP</td>
<td>Outgoing</td>
<td>V</td>
<td></td>
</tr>
</tbody>
</table>

The following ports are used by the XMPP Server

<table>
<thead>
<tr>
<th>Function</th>
<th>Destination Port</th>
<th>Type</th>
<th>Direction</th>
<th>Used in Link(s)</th>
<th>Configurable?</th>
</tr>
</thead>
<tbody>
<tr>
<td>XMPP Client</td>
<td>5222</td>
<td>TCP</td>
<td>Incoming</td>
<td>J</td>
<td></td>
</tr>
<tr>
<td>XMPP Server</td>
<td>5269 + 4999**</td>
<td>TCP</td>
<td>Both</td>
<td>Q</td>
<td>MMP</td>
</tr>
<tr>
<td>Trunk</td>
<td>5999**</td>
<td>TCP</td>
<td>Outgoing</td>
<td>CC</td>
<td>MMP</td>
</tr>
</tbody>
</table>
The following ports are used by the Load Balancer

<table>
<thead>
<tr>
<th>Function</th>
<th>Destination Port</th>
<th>Type</th>
<th>Direction</th>
<th>Used in Link(s)</th>
<th>Configurable?</th>
</tr>
</thead>
<tbody>
<tr>
<td>XMPP Client</td>
<td>5222</td>
<td>TCP</td>
<td>Incoming</td>
<td>A</td>
<td>MMP</td>
</tr>
<tr>
<td>XMPP Server</td>
<td>5269</td>
<td>TCP</td>
<td>Both</td>
<td>Q</td>
<td>MMP</td>
</tr>
<tr>
<td>XMPP Server</td>
<td>5223</td>
<td>TCP</td>
<td>Incoming</td>
<td>U</td>
<td>MMP</td>
</tr>
<tr>
<td>Trunk</td>
<td>4999**</td>
<td>TCP</td>
<td>Incoming</td>
<td>C</td>
<td>MMP</td>
</tr>
<tr>
<td>Trunk</td>
<td>5999**</td>
<td>TCP</td>
<td>Incoming</td>
<td>CC</td>
<td>MMP</td>
</tr>
</tbody>
</table>

The following ports are used by the TURN Server

<table>
<thead>
<tr>
<th>Function</th>
<th>Destination Port</th>
<th>Type</th>
<th>Direction</th>
<th>Used in Link(s)</th>
<th>Configurable?</th>
</tr>
</thead>
<tbody>
<tr>
<td>STUN</td>
<td>3478</td>
<td>UDP</td>
<td>Incoming</td>
<td>A, B, D</td>
<td></td>
</tr>
<tr>
<td>STUN RTP</td>
<td>32768-65535*</td>
<td>UDP</td>
<td>Incoming</td>
<td>A, B, D</td>
<td></td>
</tr>
</tbody>
</table>

Note: * Although the range between the TURN server and the external Acano clients is shown as 32768-65535, currently only 50000-51000 is used. A wider range is likely to be required in future releases.

Note: ** These ports are user-defined and are only used for the trunk from the Core server to the Load Balancer on the Edge server.
Appendix C  Unclustering

Unclustering Call Bridges

It is possible to have some Call Bridges clustered and accessing a database cluster; however any Call Bridges that are not in the Call Bridge cluster cannot access the clustered databases and will use a local database.

1. Remove a Call Bridge from the cluster:
   a. On that Call Bridge’s Core Server sign in to the Web Admin Interface and go to Configuration > Cluster.
   b. Select the check box next to the Call Bridge’s entry and click Delete.
      This takes that Call Bridge out of the Call Bridge cluster.

2. Then remove the co-located database (if any) from the database cluster.
   a. Sign in to the Call Bridge server’s MMP.
   b. Enter the database cluster remove command.
      The coSpace database is disconnected from the database cluster and the coSpace database cluster’s contents are no longer accessible to the Call Bridge on this Core server; however the original database contents become accessible again. (Note that they may be out of date compared to the contents of the clustered databases.)

3. Remove the component connection from the Call Bridge Web Admin Interface: to do this, delete the XMPP server details on the Configuration > General page. (If this step is missed the XMPP server may continue to use that Call Bridge for authentication despite it no longer having a connection to the database cluster.)
Appendix D  Example of Configuring a Static Route from a Lync Front End Server

Important Note: This appendix provides an example to be used as a guideline and is not meant to be an explicit set of instructions for you to follow. Acano strongly advises you to seek the advice of your local Lync server administrator on the best way to implement the equivalent on your server’s configuration.

1. Ensure that you have installed certificates on the Acano solution to trust the Lync server – as described earlier in this document.

Lync Configuration Changes

2. Optionally, enable HD720p on Lync as follows (if you want HD calls from Lync because the default is VGA):
   a. Open the Lync Server Management Shell,
   b. Enable support for HD720P Lync calls with:
      ```bash
      Set-CsMediaConfiguration -MaxVideoRateAllowed Hd720p15M
      ```
3. Add the trusted application and static routes to the Acano solution with the following five commands:
   ```bash
   New-CsTrustedApplicationPool -Identity acano-trust -ComputerFqdn fqdn.acanoserver.com -Registrar fqdn.lyncserver.com -site 1 -RequiresReplication $false -ThrottleAsServer $true -TreatAsAuthenticated $true
   ```
   Replacing
   - acano-trust with a name of your choice
   - fqdn.acanoserver.com with the FQDN of the Acano solution
   - fqdn.lyncserver.com with your Lync FE Server or Pool FQDN
   ```bash
   New-CsTrustedApplication -ApplicationId acano-application -TrustedApplicationPoolFqdn acano-trust -Port 5061
   ```
   Replacing
   - acano-application with name of your choice
   - acano-trust with name used above
   ```bash
   $x=New-CsStaticRoute -TLSRoute -Destination "fqdn.acanoserver.com" -MatchUri "something.com" -Port 5061 -UseDefaultCertificate $true
   ```
   Replacing
   - fqdn.acanoserver.com with your FQDN of the Acano solution
• something.com with the URI match of your choosing, possibly acano.yourcompany.com if that is the domain used for all Acano calls

Set-CsStaticRoutingConfiguration -Identity global -Route @(Add=$x)
Enable-CsTopology

This command enables the new topology. Users may have to logout and login again to update to the new HD720p setting, all other settings are automatic and should work within a few minutes.

**Acano Solution Configuration**

4. In the Web Admin Interface go to Configuration > Outbound Calls

5. In the blank row, for Domain, enter the Lync domain that will be matched for calls that need to be sent to Lync

6. For SIP Proxy to Use, do one of the following:
   a. Leave this field blank and the server will perform a DNS SRV lookup for the called domain using _sipinternaltls._tcp.<yourlyncdomain>.com
   b. Enter the Front End Pool (or Lync sip domain) and the server will first perform a DNS SRV lookup for that defined domain using _sipinternaltls._tcp.<yourlyncdomain>.com and then perform a DNS A record lookup for the Host entered if the SRV lookup fails to resolve
   c. Enter the IP address of your Lync Front End server

7. For Local Contact Domain, enter the FQDN of your Acano solution. (The only case in which this field should be set is when setting up a trunk to Lync; otherwise it should be left blank.)

8. For Local From Domain, enter the domain that you want the call to be seen as coming from (the Caller ID) e.g. acano.yourcompany.com

   Note: If you leave Local From Domain blank, the domain used for the Caller ID defaults to that entered as the Local Contact Domain.

9. For Trunk Type, select Lync.

10. Select Add New.

   After completion you should be able to call from the Lync environment to the Acano solution and from the Acano solution to Lync.
Appendix E  API Examples

The examples in this appendix use the POSTMAN API tool. There are others that you can use. The examples do not use all the parameters that are possible for these API methods; see the MMP Command Reference for additional details.

Note: You will need to enter a login account and password for the API in POSTMAN. This is not called out as a separate step in the examples below but must be entered before you click Send.

Creating an Outbound Dial Plan Rule for a Specific Call Bridge in a Cluster

This requires a POST method to the “/outboundDialPlanRules” node.

1. Set the following (see the screenshot below):
   a. Assuming that the Call Bridge IP address is 192.168.3.77, then the Post URL is https://192.168.3.77/api/v1/outboundDialPlanRules.
   b. If the domain to match in order to apply the dial plan rule is acanopartners.com, then this is added in body message. This is the only mandatory parameter.
   c. Set the method as POST
   d. Click Send. (Required for every API call.)

   ![API Method](image1)

   If POST operation is successful, 200OK status is seen in the reply.

2. A GET method will find the new rule’s outboundDialPlanRule ID and display it in the reply.

   ![outboundDialPlanRule ID](image2)
From screenshot above, you see that the outboundDialPlanRule ID is ea3f5cd1-7b5b-4d80-af5f-ffff2362d0f.

3. Note this ID.

4. Perform a GET operation on the “/callBridges” node to find the IDs of all the Call Bridges.
   
   If GET operation is successful, 200OK status is seen.

5. Scroll down and note the Call Bridge ID that you want the outboundDialPlanRule to apply to.
   
   In this example, we use Call Bridge ukcore2 with ID = 0ce50c9e-c92b-43f8-9f79-69e638a9c098

6. Apply the outboundDialPlanRule using a PUT method on the “/outboundDialPlanRules/" node.
   
   a. PUT URL is https://192.168.3.77/api/v1/outboundDialPlanRules/ea3f5cd1-7b5b-4d80-af5f-ffff2362d0f. This is the ID from step 2 above.

   b. Body parameters are
   
   localFromDomain=acanohome.com
   
   sipProxy=abc.acanopartners.com
   
   trunkType=sip
   
   priority=70
   
   failureAction=continue
   
   sipControlEncryption=auto
   
   scope=callbridge
   
   callBridge=0ce50c9e-c92b-43f8-9f79-69e638a9c098

   These parameters are entered as one long strong concatenated with ampersands (&) as shown below
If the API call is successful, 200OK status is seen.

7. To verify that the rule now applies, use a GET method on the “/outboundDialPlanRules/<outboundDialPlanRule ID>” node where the node ID is ea3f5cd1-7b5b-4d80-af5f-ffff2362d0f as before.

You also see the new rule in the Web Admin Interface. Note the “Call Bridge Scope” column entry of “one” means this rule only applies to a specific Call Bridge, not all Call Bridges.

**Setting up Web Bridges on the Call Bridge**

This requires a POST method on the “/webBridges” node for the appropriate Call Bridge.

1. Use the following:
   a. Set the POST method
   b. URL is https://192.168.3.77/api/v1/webBridges/ (assuming the same Call Bridge that was used in the previous example)
   c. Body message is “url=https://ukedge1join.acanohome.com” where ukedge1join.acanohome.com is the FQDN used to reach to the Web Bridge.
d. Click **Send**.

2. Verify that the Web Bridge is configured using GET method on the “/webBridges” node.
   a. URL is https://192.168.3.77/api/v1/webBridges/.

3. The new Web Bridge ID is shown in the reply (see the example above). You need the ID in the following example.

**Creating Web Bridge Customization on a Call Bridge**

We use the WebBridge ID of 89fb1f38-c5cf-42df-a58f-caa06eaed32a from the previous example.

This requires a PUT method on the “/webBridges/<webBridge ID>” node.

1. Enter the following:
   a. Set the method as PUT.
   b. URL is https://192.168.3.77/api/v1/webBridges/89fb1f38-c5cf-42df-a58f-caa06eaed32a.
   c. Body message is “resourceArchive=http://192.168.1.188/webrtcbranding/Uxbridge-colo.zip” which defines the path to the resource archive containing the customization files.
   d. Click **Send**.
2. Verify that the PUT method was successful by retrieving the Web Bridge node details with a GET method on the "/webBridges/<webBridge ID>" node.
   a. URL is https://192.168.3.77/api/v1/webBridges/89fb1f38-c5cf-42df-a58f-caa06eae32a. If GET operation is successful, the 200OK status is seen and the resourceArchive parameter is displayed (as shown below).

   ![Web Bridge Node Details](image)

**Setting up Turn Servers on a Call Bridge**

This requires a POST method on the "/turnServers" node.

1. Enter the following:
   a. Set the method as POST
   b. URL is https://192.168.3.77/api/v1/turnServers/
   c. Body messages is (ampersands concatenate parameters as in an earlier example)
      "serverAddress=192.168.7.66&clientAddress=200.100.1.66&username=turnuser&password=acano&type=acano",
   d. Click Send.
2. Verify the success and retrieve the Turn Server’s ID with a GET method on the 
“/turnServers/” node.
3. Retrieve the Turn Server’s details with a GET method on the “/turnServers/<turnServer ID>” 
node.
   a. URL is https://192.168.3.77/api/v1/turnServers/e545f4c4-56f2-45ab-be36- 
      ef5aa64db55e.

Creating a coSpace with the API
This requires a POST method on the “/coSpaces” node.
1. Enter the following:
   a. Set the method as POST
   b. URL is https://192.168.3.77/api/v1/coSpaces
   c. Body message is
      “name=acanouser1’coSpace&uri=12345678.cospace&secondaryUri=acanouser1.coSpa 
      ce&callId=12345678&passcode=1111&tenant=d326e4e9-a927-4514-bbab- 
e36262373f73”.
   d. Click Send.

Creating a coSpace Member for a coSpace
This requires a POST method on the “/coSpaces/<coSpace ID>/coSpaceUsers” node.
1. Enter the following
   a. Set the method as POST
b. URL is https://192.168.3.77/api/v1/coSpaces/49967952-83d1-4d7b-8dd6-1688aec6cb5d/coSpaceUsers

c. Body message is
   "userJid=aacanouser1@acanohome.com&canDestroy=true&canAddRemoveMember=true&canChangeName=false&canChangeUri=false&canChangeCallId=false&canChangePasscode=true&canPostMessage=true&canRemoveSelf=false&canDeleteAllMessages=true"

d. Click **Send**.

### Creating Call Leg Profiles

This example creates two callLegProfiles, one for hosts and the other for guests. Both require a POST operation to the `/callLegProfiles` node.

1. To create the host callLegProfile with the host default layout of all equal, enter the following:
   a. Set method to POST.
   b. URL is https://192.168.3.77/api/v1/callLegProfiles
   c. Body message is "defaultLayout=allEqual"
   d. Click **Send**.

2. To create the guest callLegProfile so that guests are disconnected automatically 10 seconds after host leaves the meeting, enter the following:
   a. Set method to POST
   b. URL is https://192.168.3.77/api/v1/callLegProfiles
   c. Body message is
      "needsActivation=true&defaultLayout=speakerOnly&deactivationMode=disconnect&deactivationModeTime=10"
   d. Click **Send**.
3. Create an access method for hosts using a POST method on the “/coSpaces/<coSpace ID>/accessMethods” node.
   a. Set method to POST.
   b. URL is https://192.168.3.77/api/v1/coSpaces/ 49967952-83d1-4d7b-8dd6-1688aec6cb5d/accessMethods
   c. Body message is “uri=12345678.cospace&callID=12345678&callLegProfile=6afd72da-c824-47d5-a78b-fb0c8817d4”.
   d. Click Send.

4. Create an access method for guests using a POST method on the “/coSpaces/<coSpace ID>/accessMethods” node.
   a. Set method to POST.
   b. URL is https://192.168.3.77/api/v1/coSpaces/ 49967952-83d1-4d7b-8dd6-1688aec6cb5d/accessMethods
   c. Body message is “uri=87654321.cospace&callID=87654321&callLegProfile= f3d8515a-8eb5-46e6-8c08-172b6ad2a8b5”.
   d. Click Send.
5. Test this configuration; you should see the following behavior.
   - All guests join the coSpace by dialing 87654321
   - You (and others) can join the coSpace as the host by dialing 12345678.
   - All guests cannot see any video streams or hear any audio until a host joins.
   - All guests are disconnected in 10 seconds after the last host leaves the meeting.