Contents

1 Introduction ........................................................................................................................................ 3
  1.1 How to Use this Guide ................................................................................................................. 3
    1.1.1 Commands ............................................................................................................................. 4

2 Example of Configuring a SIP Trunk to CUCM ............................................................................. 5
  2.1 Prerequisites .................................................................................................................................. 5
  2.2 Acano solution Configuration ....................................................................................................... 5
  2.3 CUCM Configuration ..................................................................................................................... 6
    2.3.1 Uploading the certificate to the trust store ............................................................................... 6
    2.3.2 Creating a security profile ........................................................................................................ 7
    2.3.3 Creating a SIP profile ............................................................................................................... 7
    2.3.4 Creating a SIP trunk .................................................................................................................. 7
    2.3.5 Configuring the dial plan for outbound calls ........................................................................... 8
    2.3.6 Testing ..................................................................................................................................... 9

3 Configuring a SIP Trunk to an Avaya CM ..................................................................................... 10
  3.1 Configuration Summary ................................................................................................................ 10
  3.2 Acano Server Configuration ......................................................................................................... 10
  3.3 Avaya CM Configuration .............................................................................................................. 11

4 Configuring a Polycom DMA for the Acano solution ................................................................... 16
  4.1 Setting up the External SIP Peer .................................................................................................. 16
  4.2 Creating the Dial Rule ................................................................................................................... 19

Figures

Figure 1: Installation and deployment documentation.......................................................................... 3
1 Introduction

This document provides examples of how to configure the Acano solution to work with third party call control devices. These may need to be adapted.

It applies equally to all deployment topologies, whether deployed on Acano X series servers or virtual host, and in both single and scaled/resilient deployments. The term Acano server in this document means either a Acano X series server or one running on a virtual host.

1.1 How to Use this Guide

This guide is referenced from the appropriate Deployment Guide (see the figure below). Follow the section or sections that are relevant to the third party call control platform(s) that you use. In addition to this guide, the 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.

![Acano solution documentation diagram](image-url)
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.
2 Example of Configuring a SIP Trunk to CUCM

This appendix provides an outline how to set up a SIP Trunk between the Acano Core and a Cisco Unified Communications Manager (CUCM).

Important Note: Acano strongly advises you to seek the advice of your local CUCM server administrator on the best way to implement the equivalent on your server’s configuration if you are not that person.

2.1 Prerequisites

This section assumes that you have:

- You have specified a listening interface using the MMP `callbridge listen` command
- If you will use TLS, you have configured certificates to use with the `callbridge certs` command

Note: CUCM has some requirements on what TLS certificates it will accept. You should ensure that the certificate on the Acano server has the SSL Client and SSL server purposes enabled. This is done during the certificate signing stage: instead of "CertificateTemplate:WebSever" create and use a different template.

Use openSSL to see whether the existing certificate is OK; for example:

`openssl x509 -in <certificatename> -noout -text -purpose`

The important lines in the output are "SSL client" and "SSL server" which must have a Yes, for example:

Certificate purposes:
- SSL client : Yes
- SSL client CA : No
- SSL server : Yes

See the Deployment Guides for more details.

2.2 Acano solution Configuration

1. In the Web Admin Interface, go to Configuration > Outbound Calls.
2. In the blank row, for Domain, enter the domain that will be matched for calls that need to be sent to CUCM.
3. For SIP Proxy to Use, do one of the following:
   - Leave this field blank and the server will perform a DNS SRV lookup for the called domain using `_sip._tls.<yourcucmdomain>.com`. If this fails to resolve the server will try a lookup using TCP an then UDP.
   - Enter the CUCM FQDN and the server will perform a DNS SRV lookup for that defined domain.
Note: If this fails to resolve the server will try a lookup using TCP an then UDP. The server will then perform a DNS A record lookup for the Host entered if the above SRV lookup fails to resolve using TLS, TCP or UDP.

- Enter the IP address of your CUCM

4. For Local Contact Domain, enter the domain that you route to your Acano server, e.g. acano.yourcompany.com. (The only case in which this field should be set is when setting up a trunk to Lync; otherwise it should be left blank.)

5. For Local From Domain, enter the domain that you want the call to be seen as coming from (the Caller ID).

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

6. For Trunk Type select Standard SIP.
7. Set the Priority as necessary.
8. Select Add new.

### 2.3 CUCM Configuration

Note: Our testing has been done on trunks without MTP configured. Therefore:

- Disable MTP if this will not negatively affect your deployment
  Turning off MTP might have a negative impact on your deployment only if you are using SCCP phones and there are call scenarios in which sending DTMF to the Acano solution is required

- If the above is not a valid implementation, you may need to increase the MTP capacity on the CUCM depending on the number of simultaneous calls

An overview of the steps required on CUCM is:

1. If you will use TLS, then upload a certificate to the trust store.
2. If you will use TLS, create a security profile.
3. Create a SIP profile.
4. Create the SIP trunk.
5. Configure the dial plan for outbound calls.
6. Test.

Each step is described in more detail in the sections below.

#### 2.3.1 Uploading the certificate to the trust store

If the SIP trunk type will be TLS, follow these steps; otherwise go on to the next section.

1. Go to Cisco Unified OS Administration and log in.
3. Select **Upload Certificate/Certificate Chain**.
4. Complete the fields as follows:
5. Enter the Certificate Name as CallManager-trust and type in a Description.
6. Click **Choose File** to find your certificate. This can be the root certificate or the Acano server’s certificate.
7. Click **Upload File**.

### 2.3.2 Creating a security profile

If the trunk will be TCP, then use CUCM’s default security profile called Non Secure SIP Trunk when you create the SIP Trunk. To use TLS, or something other than the standard security profile, follow these steps:

1. Go to Cisco Unified CM Administration and log in again.
2. Go to **System > Security > SIP Trunk Security Profile** and click **Add New**.
3. Complete the fields as follows:
   - Name = Type in a name e.g. "Acano Server Encrypted TLS SIP trunk"
   - Device Security Mode = Encrypted
   - Incoming Transport Type = TLS
   - Outgoing Transport Type = TLS
   - X.509 Subject Name: The X509 subject name of the certificate installed on the Acano Call Bridge (usually the FQDN of the Acano server)
   - Incoming Port: 5061
4. Click **Save**.

### 2.3.3 Creating a SIP profile

CUCM comes with a profile called Standard SIP Profile For TelePresence Conferencing

1. In Cisco Unified CM Administration, go to **Device > Device Settings > SIP Profile** and click **Add New**.
2. Configure the fields as appropriate.
3. Click **Save**.

### 2.3.4 Creating a SIP trunk

1. In Cisco Unified CM Administration, go to Device >Trunk and click Add New.
2. Configure these fields:
   - Trunk Type = SIP trunk
   - Device Protocol = SIP
   - Trunk Service Type = None(Default)
3. Click **Next**.
4. As a minimum, complete these fields:
   - **Device name** = Type in a name e.g. Acanoserver (no spaces allowed)
   - **Device pool** = The pool you want your device to belong to (as configured in **System > Device Pool** in CUCM)
   - **SRTP Allowed** = Select if you want media encryption (we only do media encryption if the trunk is TLS)
   - **Inbound Calls > Calling Search Space** = default
   - **Outbound Calls > Calling Party Transformation CSS** = Select as appropriate
   - **Sip Information > Destination Address** = The destination address e.g. `acanoserver.acano.com` or an IP address.
   - **Sip Information > Destination Port** = 5060 for TCP or 5061 for TLS
   - **SIP Trunk Security Profile** = As in Creating a Security profile above. (Either the security profile that you created or "Non Secure SIP Trunk" if this trunk will be a TCP.)
   - **SIP Profile** = As in Creating a SIP profile above.
   - **Normalization Script** = "vcs-interop" if available. (Only necessary if SRTP will be used. Even if you do not have a VCS, the Acano solution has the same interop issues that VCS would have, and therefore this script is suitable for a trunk to the Acano Core also.)

5. Click **Save**.

### 2.3.5 Configuring the dial plan for outbound calls

You can configure number based routing e.g. 7xxx to Acano or domain based routing e.g. `@mydomain.acano.com` to the Acano server. In both cases this is done through the Cisco Unified CM Administration interface. Follow the relevant example here:

#### Domain based routing example

To route all calls to `@mydomain.acano.com` to the Acano Call Bridge, in the Cisco Unified CM Administration interface:

1. Go to **Call Routing > Sip Route Pattern**.
2. Click **Add New**.
3. Complete the following:
   - **Pattern usage** = domain routing
   - **IPv4 pattern** = something like `mydomain.acano.com`
   - **Description** = anything you want
   - **Route partition** = see below
   - **SIP trunk / route list** = the trunk you have already configured

5. Click **Save**.

#### Numeric dialing example

This basic example routes everything starting with a 7 to the Acano solution. In the Cisco Unified CM Administration interface:

1. Go to **Call routing > Route/Hunt > Route Pattern**.
2. Click **Add New**.

3. Complete the following:
   - Route pattern = 7. (The ! means anything. The dot is useful for a later option below.)
   - Route partition = the route partition you want this rule to belong to - see the note below
   - Description = any appropriate text
   - Gateway/route list = the trunk you have already configured
   - Route this pattern = ensure that this option is selected

Further down the page you can set various transforms e.g. in the Discard Digits field you can select PreDot to strip off the leading 7 in our example.

4. Click **Save**.

---

**Note on route partitions:**
Various dial plan rules are attached to a route partition and a calling search space (CSS) comprises a list of route partitions. You can have a different CSS for different people, each phone, or trunk.
When a call is made CUCM goes through each route partition in the CSS until it finds one that has a matching rule.

---

2.3.6 **Testing**

Make some test calls.
3 Configuring a SIP Trunk to an Avaya CM

This appendix provides an example of setting up a SIP trunk between the Acano server and the Avaya Communications Manager (Avaya CM) in order to use the Avaya CM and may need to be adapted.

**Important Note:** Acano strongly advises you to seek the advice of your local Avaya CM administrator on the best way to implement the equivalent on your server’s configuration if you are not that person.

Note: Avaya CM is an Avaya PBX, so calls will be audio only, however, the Acano solution does not impose this restriction on interoperability with Avaya: therefore a call defined to be type ‘avaya’ in the Acano solution does not imply that the call is audio-only.

### 3.1 Configuration Summary

This example deployment assumes that:

- This audio connection between Avaya CM and Acano is accessed via dialing a prefix 49
- The assigned IVR digits for the Acano server are 8320; that is a user from the Avaya environment will dial 498320 to access the Acano server IVR
- A DID extension 5328 to route to this same number and allow for PSTN dial-in to the Acano server
- Avaya Software Version: CM6 R016x.00.1.510.1 Update: 19940

### 3.2 Acano Server Configuration

1. Log in to the Web Admin Interface and go to Configuration > General.
2. For IVR Numeric ID, enter 8320.

   ![IVR Configuration](image)

   These digits will be passed from the Avaya CM to the Acano server, and then routed to the Acano IVR.
3. Click **Submit**.
4. Go to Configuration > Outbound Calls.
5. Add a dial plan entry for the Avaya CM – see the example below.

The highlighted IP address below matches the C-LAN or Processor Ethernet address on the CM side and represents the CM interface used in the Signaling Group created later.
6. Click **Add New**.

### 3.3 Avaya CM Configuration

1. Add a node name for the Acano signaling interface.

   ![IP NODE NAMES]

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acano</td>
<td>192.168.110.51</td>
</tr>
<tr>
<td>App1-ANH</td>
<td>10.22.4.38</td>
</tr>
</tbody>
</table>

2. Add an Avaya Signaling Group with the following:
   - **Group Type** = SIP
   - **Near-end Node Name** = C-LAN or Processor Ethernet interface indicated in the dial plan setting in the previous section
   - **Far-end Node Name** = Node name for the Acano signaling interface created above.
   - **Port settings for both Near-end and Far-end** = 5060
   - **Far-end Domain** = SIP domain associated with the Acano server
   - **Direct IP-IP Audio Connections** = n. This ensures that all traffic from the Avaya CM comes from the Near-end Node
3. Add an Avaya Trunk Group with the following:
   - Group Type = SIP
   - Direction = two way
   - Service Type = tie
   - Additional settings may vary, but see the examples below for possible configuration
### Configuring a SIP Trunk to an Avaya CM

#### Group Type: sip

#### TRUNK PARAMETERS

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Page Line Retrieval?</td>
<td>n</td>
</tr>
<tr>
<td>Redirect On OPTIN Failure</td>
<td>5000</td>
</tr>
<tr>
<td>SCCAM?</td>
<td>y</td>
</tr>
<tr>
<td>Preferred Minimum Session Refresh Interval (sec)</td>
<td>600</td>
</tr>
<tr>
<td>Disconnect Supervision - In?</td>
<td>y</td>
</tr>
<tr>
<td>Out?</td>
<td>y</td>
</tr>
<tr>
<td>XSSIP Treatment?</td>
<td>auto</td>
</tr>
<tr>
<td>Delay Call Setup When Accessed Via IGA?</td>
<td>n</td>
</tr>
</tbody>
</table>

#### TRUNK FEATURES

<table>
<thead>
<tr>
<th>Feature</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACA Assignment?</td>
<td>n</td>
</tr>
<tr>
<td>Measured:</td>
<td>none</td>
</tr>
<tr>
<td>Maintenance Tests?</td>
<td>y</td>
</tr>
<tr>
<td>Numbering Format:</td>
<td>public</td>
</tr>
<tr>
<td>UUI Treatment:</td>
<td>service-provider</td>
</tr>
<tr>
<td>Replace Restricted Numbers?</td>
<td>n</td>
</tr>
<tr>
<td>Replace Unavailable Numbers?</td>
<td>n</td>
</tr>
<tr>
<td>Modify Tandem Calling Number?</td>
<td>no</td>
</tr>
<tr>
<td>Show ANSWERED BY on Display?</td>
<td>y</td>
</tr>
<tr>
<td>DSN Term?</td>
<td>n</td>
</tr>
</tbody>
</table>
4. Add an Avaya Route Pattern to routes calls to trunk group 105 and delete the first two digits (deletes the prefix digits 49).
5. Add a Uniform Dial Plan to provide a routing for a 6-digit number with a prefix of 49. These calls must be set to be routed to AAR tables in Avaya.

6. Add an AAR setting to route all calls of 6 digits in length and beginning with 49 (i.e. 498320) to route pattern 105 (the Acano Trunk Group).

7. Assign an Extension and DID.
   Optionally, in the Uniform Dial Plan you can add a setting for a DID extension (in this example, x5328) to route a call via digits 498320 to the Acano server.
4 Configuring a Polycom DMA for the Acano solution

For calls from a Polycom DMA environment to the Acano solution, create an External SIP Peer on the Polycom DMA that will point to the Acano solution, and then configure a Dial Rule on the Polycom DMA that will direct calls to it.

The following is an example of configuring the Acano solution for the Polycom DMA, and may need to be adapted. Follow the instructions in the Deployment guides to set up a dial plan rule that points to the Polycom DMA server in the Web Admin Interface Configuration > Outbound Calls page. Also ensure that the correct ports are open (Incoming/Outgoing UDP 32768-65535 – RTP).

**Important Note:** Acano strongly advises you to seek the advice of your local Polycom server administrator on the best way to implement the equivalent on your server’s configuration if you are not that person.

4.1 Setting up the External SIP Peer

On the Polycom DMA:

1. Go to Network > External SIP Peer > Add (see right)
2. In the External SIP Peer page configure the following (see below):
   a. Name: Acano
   b. Description: a meaningful phrase, possibly Acano IP Peer
   c. Next hop Address: IP Address of Acano Call Bridge
   d. Port: 5060
   e. User Route Header: selected
   f. Type: Other
   g. Transport Type: TCP
3. Leave the Domain List page blank (see below).

4. In the Postliminary page Header Options section configure the following (see below):
   a. Copy All Parameters: Checked
   b. Format: Use original request's To

5. In the Postliminary page Request URI options section configure the following (see below):
   a. Format: Original user, configured peer's Destination Network or next hop address
6. In the Authentication page configure the following (see below):
   a. Authentication: Pass authentication
   b. Proxy authentication: Pass Proxy authentication

7. Click Save.
4.2 Creating the Dial Rule

In the Polycom DMA:

1. Go to **Admin > Call Server > Dial Rules > Add** (see right).

2. In the Edit Dial Rule for Authorized Calls page, configure the following (see below):
   a. Description: Acano <Description of pattern>

3. Select **Enabled**.

4. Select the Acano SIP Peer in the left pane and click the arrow to move it to the Selected SIP Peers.

5. In the Preliminary page create a string to represent how calls will match this rule (see below). Consult the DMA Admin Guide for more detail. The example below matches any call that begins with a 6 and sends it to the Acano solution.

   ```java
   if(!DIAL_STRING.match(/sip:6/))
   {
     return NEXT_RULE;
   }
   
   6. Click **OK**.
You should now be able to dial from any SIP-enabled Polycom DMA endpoint to the Acano solution using the rule created.