Avaya Solution & Interoperability Test Lab

Application Notes for Enghouse Interactive Attendant Console 6.0 to interoperate with Avaya Aura® Communication Manager R6.3 and Avaya Aura® Session Manager R6.3 - Issue 1.0

Abstract

These Application Notes describe the configuration steps required Enghouse Interactive Attendant Console 6.0 to interoperate with Avaya Aura® Communication Manager R6.3 and Avaya Aura® Session Manager R6.3.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes outline the steps necessary to configure Enghouse Interactive Attendant Console to interoperate with Avaya Aura® Communication Manager R6.3 via Avaya Aura® Session Manager R6.3. Enghouse Interactive Attendant Console provides a Computer Telephony Interface (CTI) to PBX environments that do not support a traditional Third-Party Call Control API or Protocol. Instead, the Attendant Console implements a Back-to-Back User Agent (B2BUA) model where customer and agent call legs are directed from the PBX to the Attendant Console, where they are controlled via a conference bridge. In addition, the Attendant Console enables a set of Media Control APIs to be supported by CTI Connect for these PBXs. These PBXs can be used to support applications such as Self-service IVR.

CTI Connect Media Gateway 8.1 introduces support for an equivalent SIP Trunk interface to Avaya Aura® Communication Manager via Avaya Aura® Session Manager.

The Attendant Console supports two types of CTI Connect channel:

- **Route Channel** – a CTC application can use this channel to play media to the caller, receive notification of DTMF key presses, receive audio input and route the call to a new destination on the PBX.
- **Device channel** – The Attendant Console joins the inbound call in a conference with the PBX Extension that was associated with the "To:" header. A Device Channel may be used to initiate an outbound call on behalf of the PBX extension. In this case, a call leg will be established from the Media Gateway to the extension and then conferenced with the outbound leg to the IP-PBX which will route it to the appropriate destination.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise voice network using Communication Manager. The Attendant Console Communicates with the Communication Manager using a SIP trunk via session Manager. See **Figure 1** for a network diagram. A Dial plan was configured on Communication Manager to route calls to queues on Attendant Console. Calls placed to these queues are automatically bridged to the telephone the Attendant is using for answering purposes.

Note: During compliance testing an Avaya H.323 9640G was used as the attendant's telephone.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

The interoperability compliance testing included feature and serviceability testing. The serviceability testing introduced failure scenarios to see the Attendant Console could resume after a link failure with Communication Manager/Session Manager. The testing included:

- Incoming internal and external calls
- Outgoing internal and external calls
- Re-queuing calls
- Hold/Release
- Supervised and unsupervised transfer with answer
- Directing calls to busy extensions
- Call queuing and retrieval

2.2. Test Results

Tests were performed to verify interoperability between Enghouse Interactive Attendant Console and Avaya Communication Manager. The tests were all functional in nature and performance testing was not included. All the test cases passed successfully with one observation. Enghouse Interactive Attendant Console can only initiate a 3 way conference.

2.3. Support

For technical support for Enghouse Interactive products, please use the following web link.
https://mysupport.enghouseinteractive.com

Enghouse Interactive can also be contacted as follows.

Phone:	+44(0)870 220 2205 (EMEA)
:	+1 800.657.1530 (Americas)
E-mail:	Support@Datapulse.com

3. Reference Configuration

Figure 1 illustrates the network topology used during compliance testing. The Avaya solution consists of a Communication Manager, which has a SIP Trunk connection to the CTI Connect Server via Session Manager. An Avaya H.323 telephone was used as the Attendant telephone during compliance testing. System Manager was used to configure Session Manager. Digital and H.323 telephones were configured on the Communication Manager to generate outbound/inbound calls to/from the PSTN. A QSIG trunk was configured to connect to the PSTN.

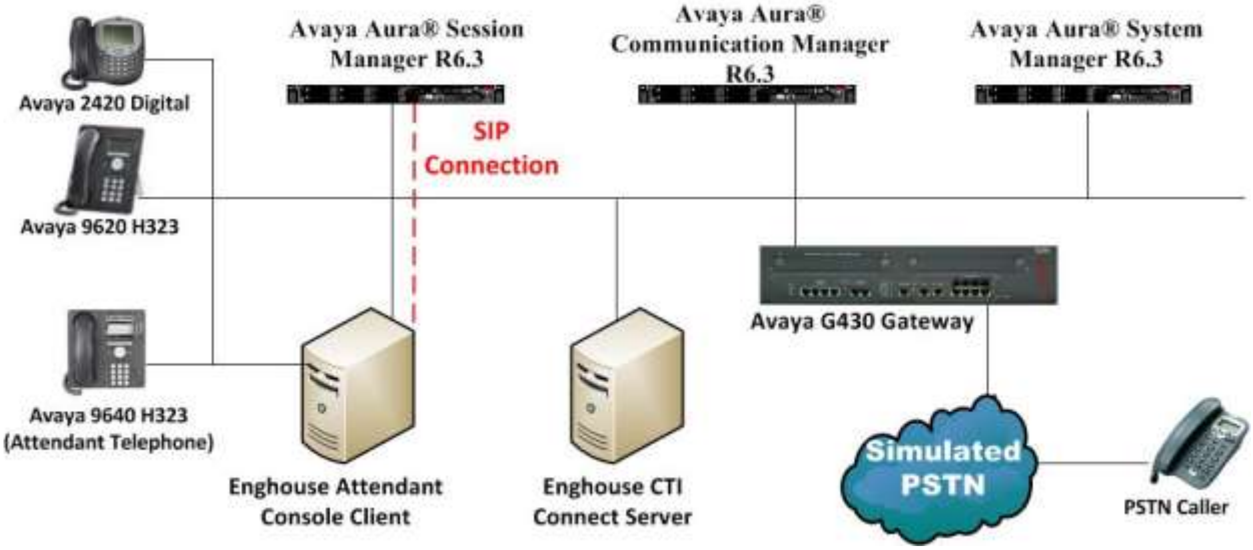

Avaya 2420 Digital
Avaya 9620 H323
Avaya 9640 H323
(Attendant Telephone)
Avaya Aura® Session Manager R6.3
SIP Connection
Avaya Aura® Communication Manager R6.3
Avaya Aura® System Manager R6.3
Avaya G430 Gateway
Enghouse Attendant Console Client
Enghouse CTI Connect Server
Simulated PSTN
PSTN Caller

Figure 1: Avaya and Enghouse Interactive Reference Configuration

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Avaya Equipment	Software / Firmware Version
Avaya Aura® Communication Manager	R6.3 Build R016x.03.0.124.0
Avaya Aura® Session Manager	R6.3.7 Software Update 6.3.7.0.637008
Avaya Aura® System Manager	R6.3.7 Build 6.3.0.8.5682-6.3.8.2826 Update 6.3.5.52017
Avaya G430 Media Gateway Module MM710 (DSP MP20)	Version 36.7.0/1 Version HW04 FW021
Avaya Media Gateway DSP module	MP20 FW 132
Avaya 96xx IP phones 9640G 9620D Avaya 2420 Digital phone	 3.1.05S 3.1.01S Rel 6.0, FWV 6
Enghouse Interactive Equipment	**Software / Firmware Version**
CTI Connect Media Gateway Attendant Console server both running on Microsoft Windows 2008 R2 SP1 Server	Version 8.1 Version 6.0.0.6
Attendant Console client running on Microsoft Windows 7 Enterprise SP1	Version 6.0.0.6

5. Configure Avaya Aura® Communication Manager

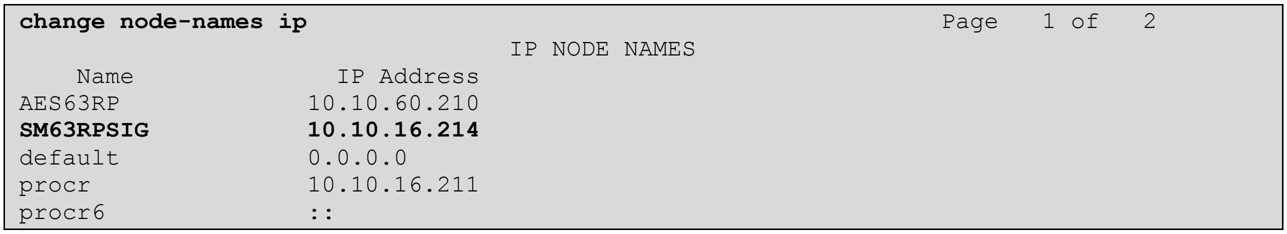
Configuration and verification operations on the Communication Manager illustrated in this section were all performed using Avaya Site Administrator Emulation Mode. The information provided in this section describes the configuration of the Communication Manager for this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**.

It is implied a working system is already in place. The configuration operations described in this section can be summarized as follows: (Note: during Compliance Testing all inputs not highlighted in Bold were left as Default)

- Configure Session Manager Node
- Configure Signaling-Group (for information only)
- Configure Trunk Group (for information only)
- Configure Route Pattern
- Configure dialplan analysis

5.1. Configure Session Manager Node

For the Communication Manager to communicate with the Session Manager a node must be configured. The screen shot below shows **SM63RPSIG** with IP address **10.10.16.214** was used.
Note: 10.10.16.214 IP address of the Session Manager SIP Signaling Interface.



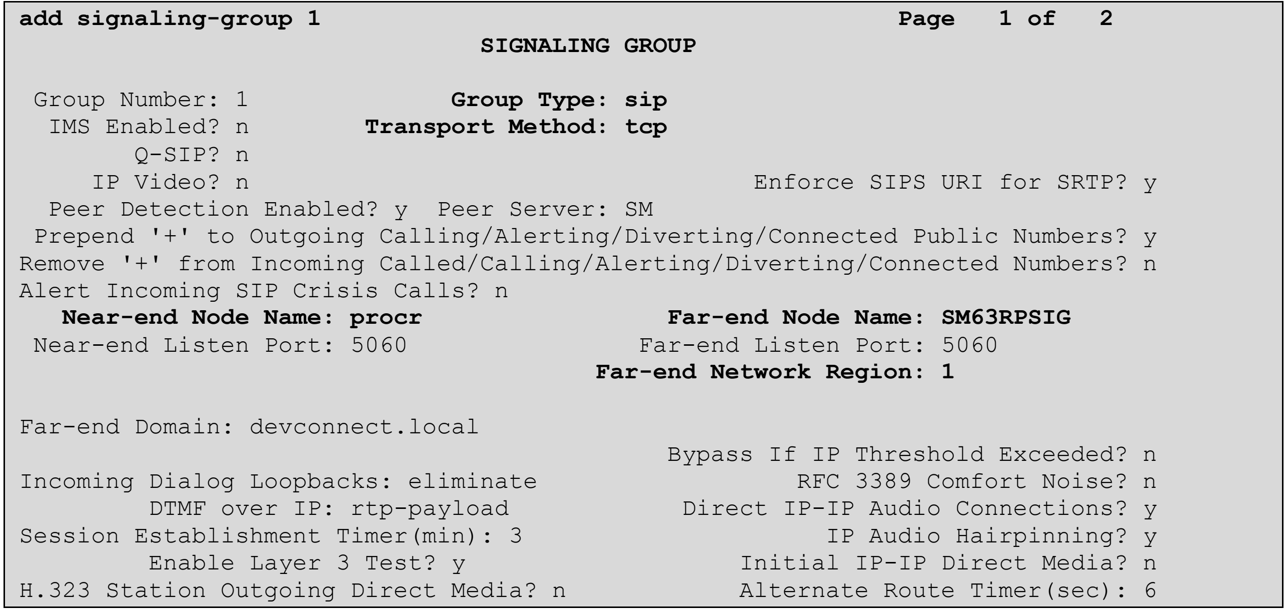
```
change node-names ip                                                Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
AES63RP             10.10.60.210
SM63RPSIG           10.10.16.214
default             0.0.0.0
procr               10.10.16.211
procr6              ::
```

5.2. Configure Signaling Group

A signaling group is required before a trunk-group can be configured. Use the **add signaling-group** command followed by next available signaling-group number to configure the following:

- **Group Type:** Enter **sip**
- **Transport Method** Enter **tcp**
- **Near-end Node Name:** Enter **procr**
- **Far-end Node Name:** Enter **SM63RPSIG** (Session Manager Node as configured in **Section 5.1**)
- **Far-end Network Region:** Enter the appropriate Network region (i.e. **1**)
- **Far End Domain:** Enter the appropriate Domain

Page 1



```
add signaling-group 1                                    Page   1 of   2
                                SIGNALING GROUP

 Group Number: 1              Group Type: sip
  IMS Enabled? n        Transport Method: tcp
        Q-SIP? n
     IP Video? n                                  Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr                  Far-end Node Name: SM63RPSIG
 Near-end Listen Port: 5060                 Far-end Listen Port: 5060
                                         Far-end Network Region: 1

Far-end Domain: devconnect.local
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload             Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? y
         Enable Layer 3 Test? y                    Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n             Alternate Route Timer(sec): 6
```

5.3. Configure Trunk Group

This section describes the Trunk Group configuration used during compliance testing. Use the **add trunk-group** command followed by next available Group number and configure the following:

- **Group Type:** Enter **sip**
- **Group Name:** Enter an informative name for the trunk (i.e. **To SM6.3 SIP)**
- **TAC** Enter a TAC number (i.e. **701)**
- **Service Type:** Enter **public-ntwrk**
- **Signaling Group:** Enter the Signaling Group number as configured in **Section 5.2**
- **Number of Members:** Enter the number of channels required to connect to the Session Manger (during compliance testing 30 channels were used)

Page **1**

```
add trunk-group 1                                            Page   1 of  21
                                TRUNK GROUP

Group Number: 1                    Group Type: sip           CDR Reports: y
  Group Name: To SM6.3 SIP                COR: 1        TN: 1        TAC: 701
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 1
                                                     Number of Members: 30
```

Go to page 3 and enter **private** for **Numbering format**.

```
add trunk-group 1                                            Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y



                     Numbering Format: private
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n


                                Modify Tandem Calling Number: no


Show ANSWERED BY on Display? y
```

5.4. Configure Route Pattern

Enter the command **change route-pattern 1** where route pattern 1 is used to route calls between Communication Manager and Session Manager. Enter an identifying **Pattern Name**. In the **Grp No** field enter the Trunk Group number as configured in **Section 5.3**.

```
change route-pattern 1                                            Page   1 of   3
                    Pattern Number: 1    Pattern Name: to SMs
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                                DCS/ IXC
    No          Mrk Lmt List Del  Digits                                    QSIG
                             Dgts                                           Intw
 1: 1    0                                                                n   user
 2:                                                                       n   user
 3:                                                                       n   user
 4:                                                                       n   user
 5:                                                                       n   user
 6:                                                                       n   user

    BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: y y y y y n  n            rest                                          none
 2: y y y y y n  n            rest                                          none
 3: y y y y y n  n            rest                                          none
 4: y y y y y n  n            rest                                          none
 5: y y y y y n  n            rest                                          none
 6: y y y y y n  n            rest                                          none
```

5.5. Configure Dialplan

There a number of ways to configure Dial plans, during compliance testing ARS was used. CTI Connect was configured with two queue numbers - 4700 was used for the Internal queue and 4701 was used for the External queue. Enter the command **change ars analysis 47** as shown below. Any 4 digit number beginning with 47 was routed to Route Pattern 1 (as configured in **Section 5.4**) and then in turn routed to CTI Connect via Session Manager.

```
change ars analysis 47                                              Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location: all           Percent Full: 0

          Dialed           Total     Route     Call    Node   ANI
          String          Min  Max   Pattern   Type    Num    Reqd
    47                    4    4      1        pubu           n
```

6. Configuring Avaya Aura® Session Manager

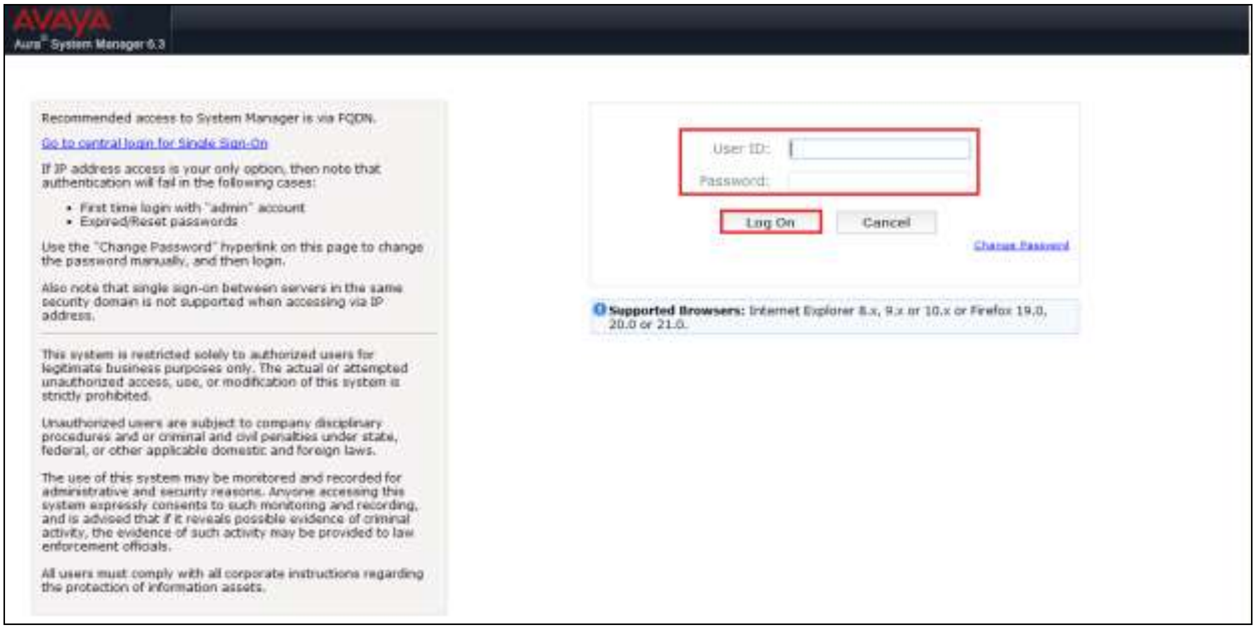
A number of configurations are required to enable Communication Manager to route calls to CTI connect and vice versa. All configurations of Session Manager are performed using System Manager. The configuration operations described in this section can be summarized as follows:

- Logging on to System Manager
- Create CTI Connect as a SIP Entity
- Create an Entity Link for CTI Connect
- Create a Routing Policy for CTI Connect
- Create a Dial Pattern for CTI Connect

Note: It is implied a working system is already in place including a Domain (**devconnect.local**) and a Location (**DevConnectRP**). During compliance testing a SIP Entity and an Entity Link for the Communication Manager were created. Also a Routing Policy and a Dial Pattern to route calls to the Communication Manager were created and are outside the scope of these Application Notes.

6.1. Logging on to Avaya Aura® System Manager

Log on by accessing the browser-based GUI of System Manager, using the URL "http://<fqdn>/SMGR" or "http://<ip-address>/SMGR", where:
"<fqdn> is the fully qualified domain name of the System Manager or the"<ipaddress>" is the IP address of System Manager.
Once the System Manager web page opens, log in with the appropriate credentials.



Recommended access to System Manager is via FQDN.

Go to central login for Single Sign-On

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

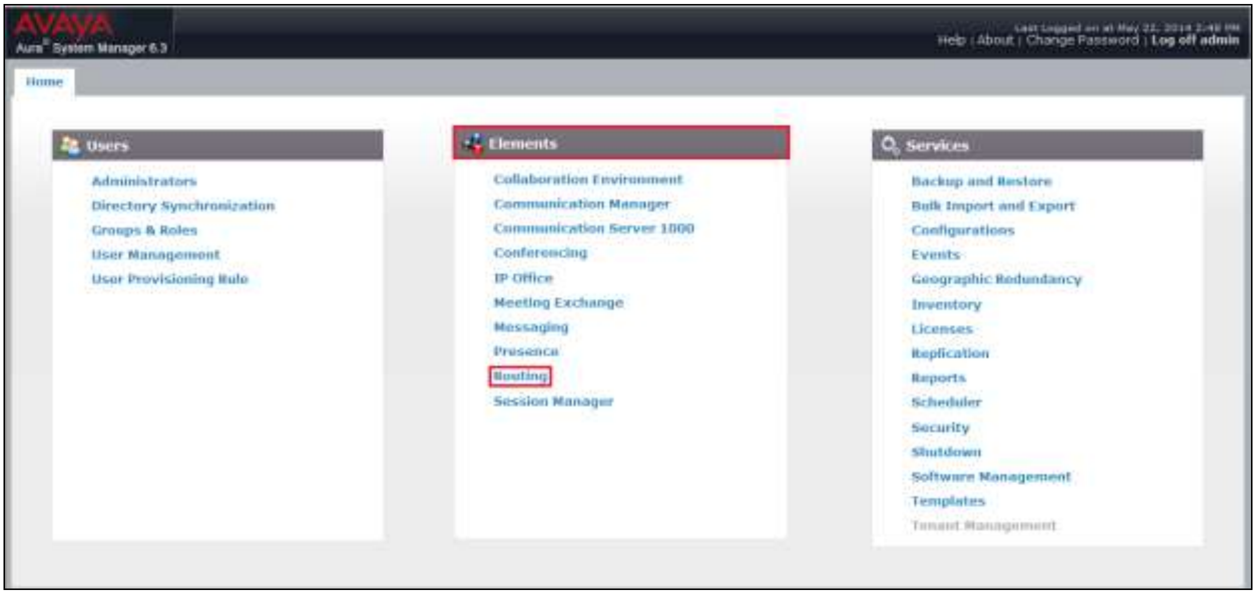
The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

Supported Browsers: Internet Explorer 8.x, 9.x or 10.x or Firefox 19.0, 20.0 or 21.0.

6.2. Create CTI Connect as a SIP Entity

Once logged in select the **Routing** Link under the **Elements** column.



A SIP Entity must be added for CTI Connect. To add a SIP Entity, select **SIP Entities** on the left panel menu and then click on the **New** button (not shown).

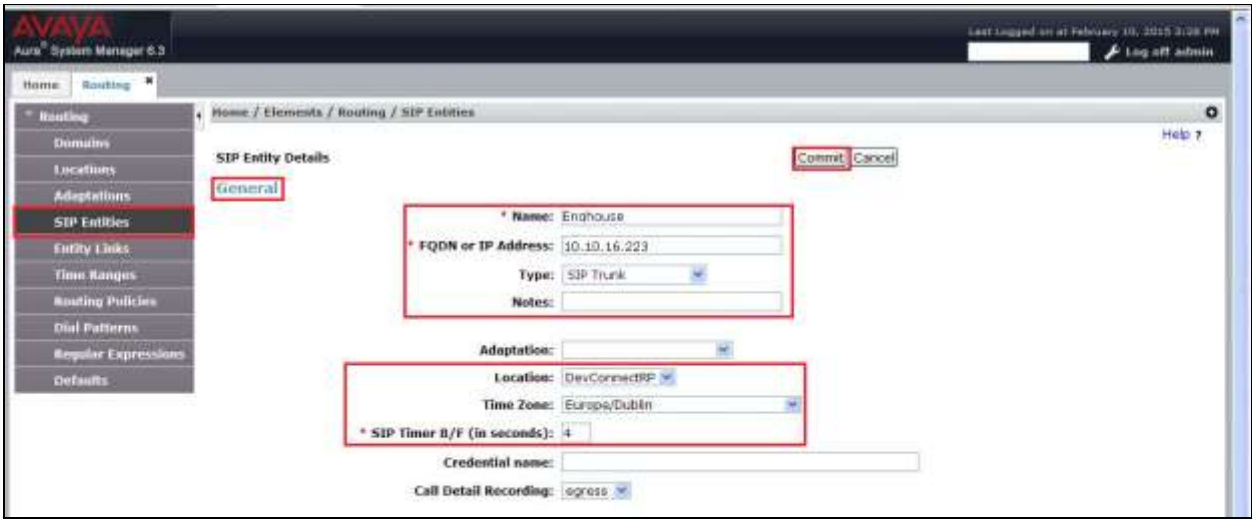
Note: A SIP Entity was already configured for Communication Manager.

Enter the following for ACS SIP Entity:
Under **General:**

- **Name** Enter an informative name (e.g., **Enghouse**)
- **FQDN or IP Address** Enter the IP address of the signalling interface on CTI connect
- **Type** Select **SIP Trunk** from the dropdown box
- **Location** Select the required Location (i.e. **DevConnectRP**) from the dropdown box
- **Time Zone** Select time zone for this location from the dropdown box
- **SIP Timer** Enter **4**

Once the correct information is entered click the **Commit** Button

Note: During compliance testing **Adaptation** was left blank.



SIP Entity Details

* Name: Enghouse
* FQDN or IP Address: 10.10.16.223
Type: SIP Trunk
Notes:

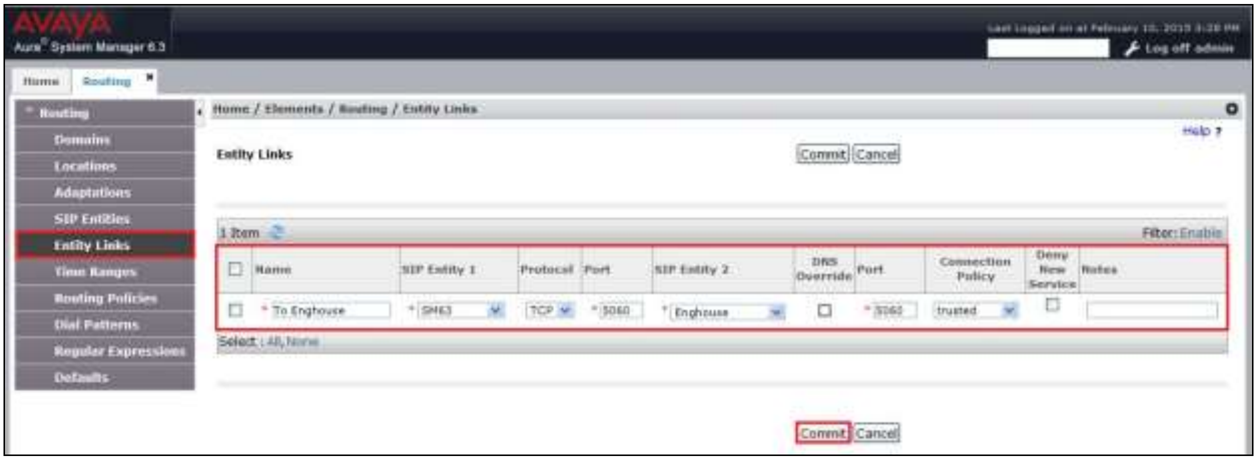
Adaptation:
Location: DevConnectRP
Time Zone: Europe/Dublin
* SIP Timer B/F (in seconds): 4
Credential name:
Call Detail Recording: egress

6.3. Create an Entity Link for CTI Connect

The SIP trunk between Session Manager and CTI Connect Server requires an Entity Link. To add an Entity Link, select **Entity Links** on the left panel menu and click on the **New** button (not shown), and enter the following:

- **Name** An informative name, (e.g. **To Enghouse**)
- **SIP Entity 1** Select **SM63** from the **SIP Entity 1** dropdown box
- **Protocol** Select **TCP** from the Protocol drop down box
- **Port** Enter **5060**
- **SIP Entity 2** Select **Enghouse** from the **SIP Entity 2** dropdown box (configured in **Section 7.2**)
- **Port** Enter **5060** as the Port
- **Connection Policy** Select **Trusted** from the **Connection Policy** dropdown

Click **Commit** to save changes. The following screen shows the Entity Links used.



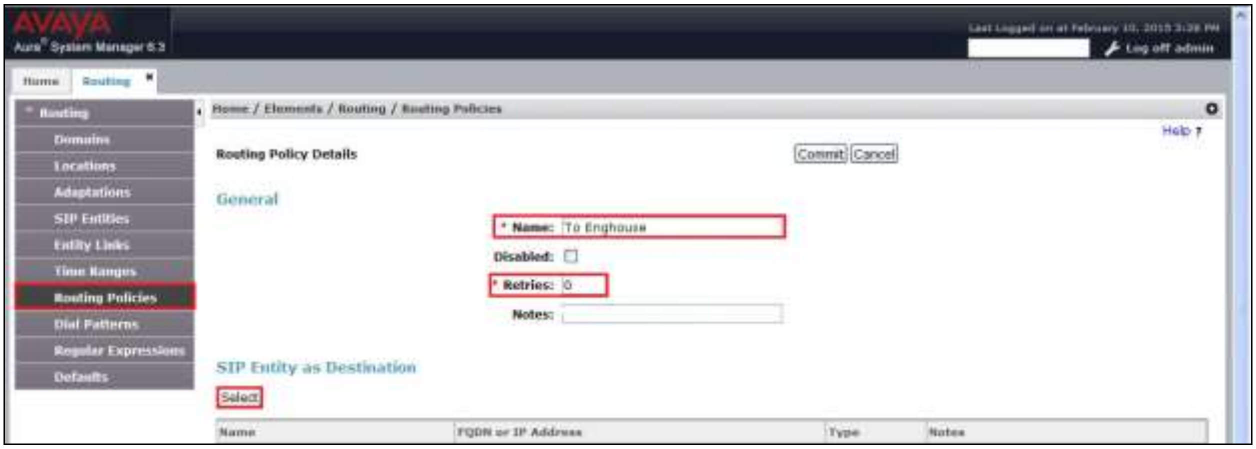
Entity Links

1 Item

□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
□	* To Enghouse	* SM63	TCP	* 5060	* Enghouse	□	* 5060	trusted	□	

6.4. Create a Routing Policy for CTI Connect

Create routing policies to direct calls to CTI Connect. To add a routing policy, select **Routing Policies** on the left panel menu and then click on the **New** button (not shown). In **Routing Policy Details** enter an informative name in the **Name** field (example, **To Enghouse**) and enter **0** in the **Retries** field**.** In **SIP Entity as Destination,** click **Select**.



Routing Policy Details

* Name: To Enghouse

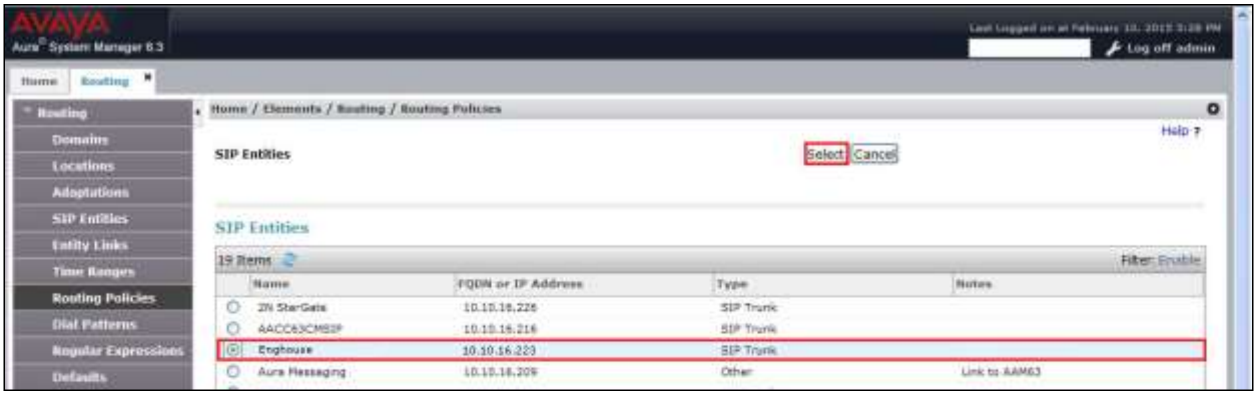
Disabled: □

* Retries: 0

Notes:

Name	FQDN or IP Address	Type	Notes

Once the SIP Entity List screen opens, check the **Enghouse** radio button. Click on the **Select** button to confirm the chosen options and then return to the **Routing Policies Details** screen and select **Commit** button (not shown) to save.



SIP Entities

SIP Entities

19 Items

	Name	FQDN or IP Address	Type	Notes
○	2N StarGate	10.10.16.226	SIP Trunk	
○	AACC63CMSIP	10.10.16.216	SIP Trunk	
●	Enghouse	10.10.16.223	SIP Trunk	
○	Aura Messaging	10.10.16.209	Other	Link to AAM63

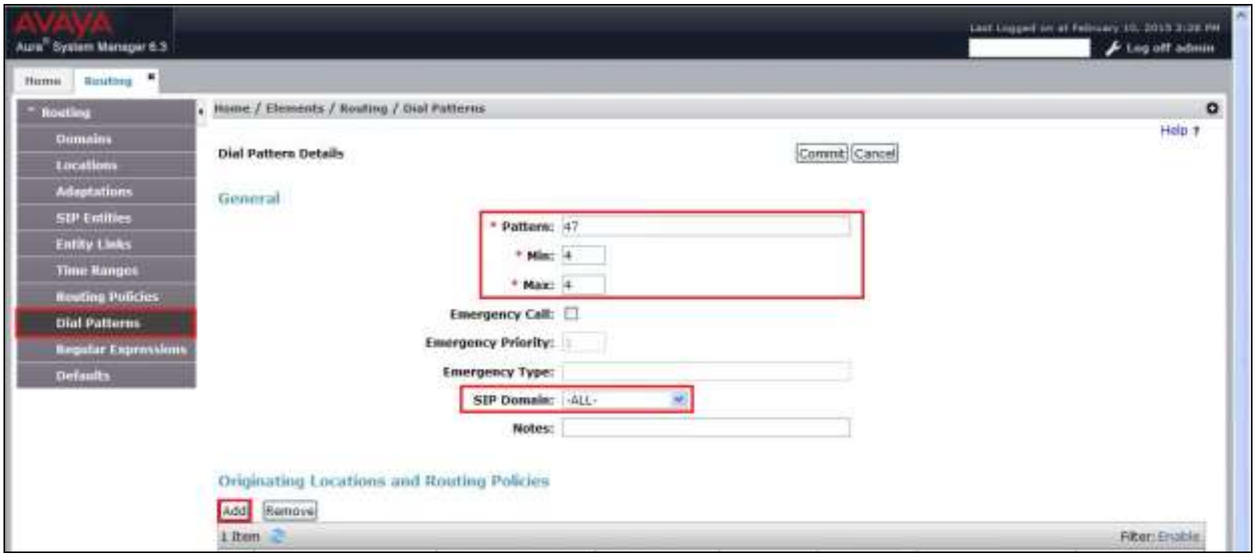
6.5. Create a Dial Pattern for CTI Connect

A dial pattern must be created on Session Manager to route calls to and from CTI Connect. During testing numbers beginning with **47** were sent to CTI Connect. To configure the CTI Connect Dial Pattern select **Dial Patterns** on the left panel menu and then click on the **New** button (not shown).

Under **General** carry out the following for each number:

- **Pattern** Enter **47**
- **Min** Enter **4** as the minimum length of dialed number
- **Max** Enter **4** as the maximum length of dialed number
- **SIP Domain** Select **All** from the drop down box

Click the **Add** button in **Originating Locations and Routing Policies**.



Dial Pattern Details

General

* Pattern: 47

* Min: 4

* Max: 4

Emergency Call: □

Emergency Priority: 1

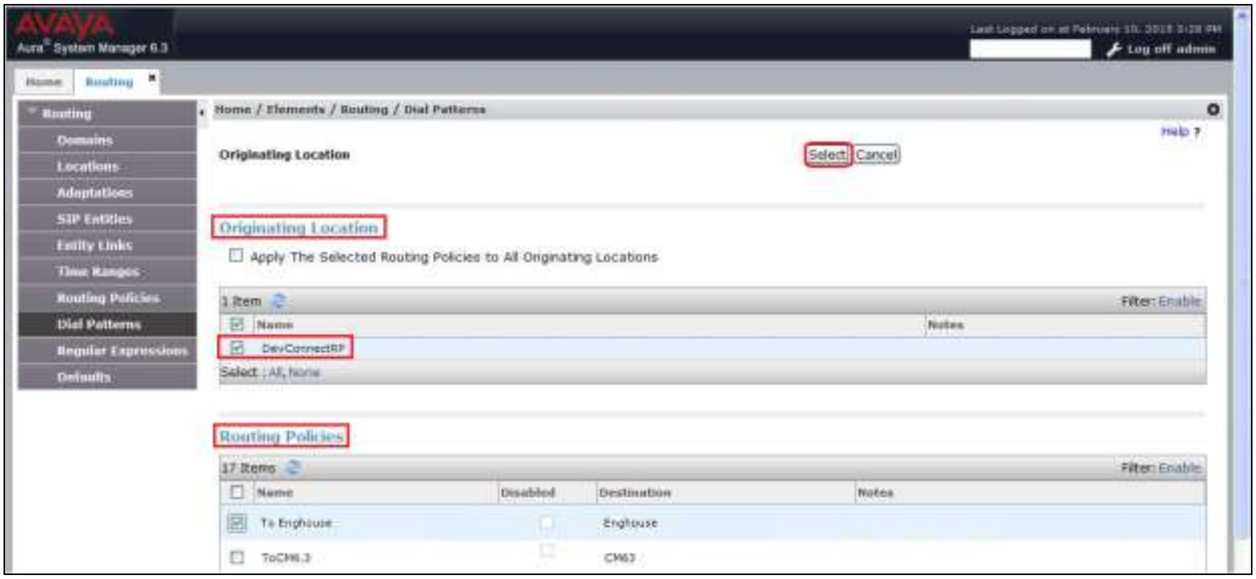
Emergency Type:

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

In **Originating Location** check the **DevConnectRP** check box. Under **Routing Policies** check the **To Enghouse** check box. Click on the **Select** button to confirm the chosen options and then be returned to the Dial Pattern screen (shown previously), select **Commit** button (not shown) to save.



Originating Location

Originating Location

□ Apply The Selected Routing Policies to All Originating Locations

1 Item — Filter: Enable

☑	Name	Notes
☑	DevConnectRP	

Select : All, None

Routing Policies

17 Items — Filter: Enable

□	Name	Disabled	Destination	Notes
☑	To Enghouse	□	Enghouse	
□	ToCM6.3	□	CM63	

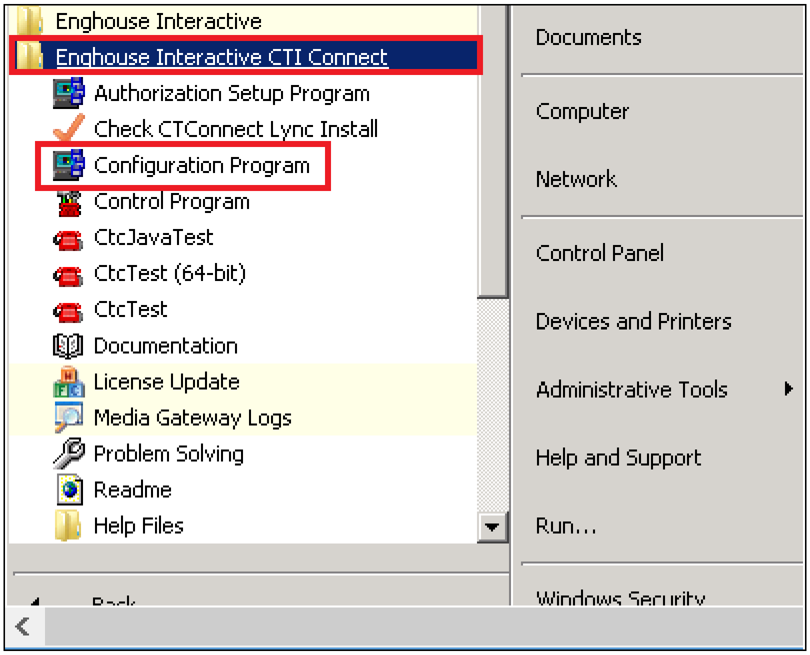
7. Configure CTI Connect server

This section shows how to configure CTI Connect server to successfully connect to Session Manager in order to make and receive calls to telephone sets on Communication Manager. The installation of the CTI Connect server software is assumed to be completed and the CTI Connect services are up and running. The steps to configure the CTI Connect server are as follows:

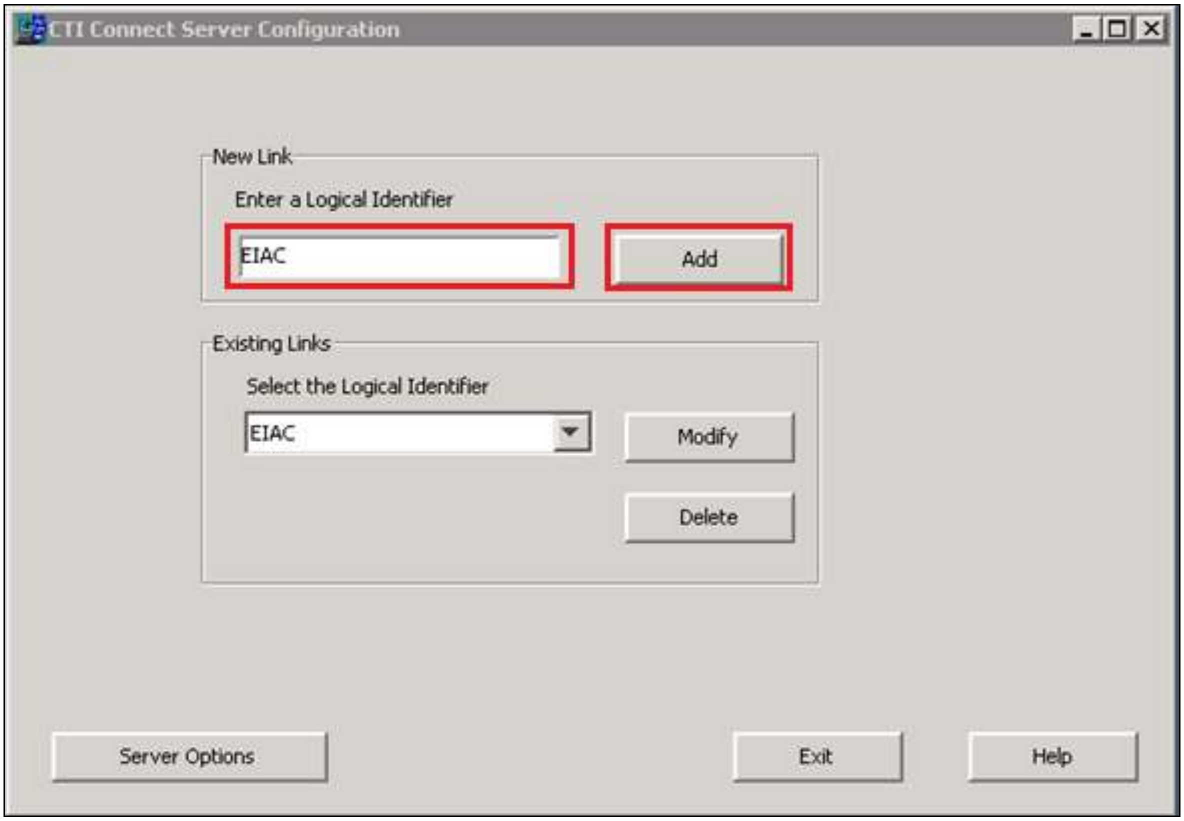
- Configure CTI Connect Configuration Program
- Turn on Link State

7.1. Configure CTI Connect Configuration Program

On the CTI Connect server launch the **Configuration Program** select **Start** → **All Programs** → (not shown) **Enghouse Interactive CTI Connect** →**Configuration Program**.



In the subsequent window, enter the **Logical Identifier** (i.e. EIAC, which is mandatory and cannot be anything different) and click on the **Add** button.



CTI Connect Server Configuration

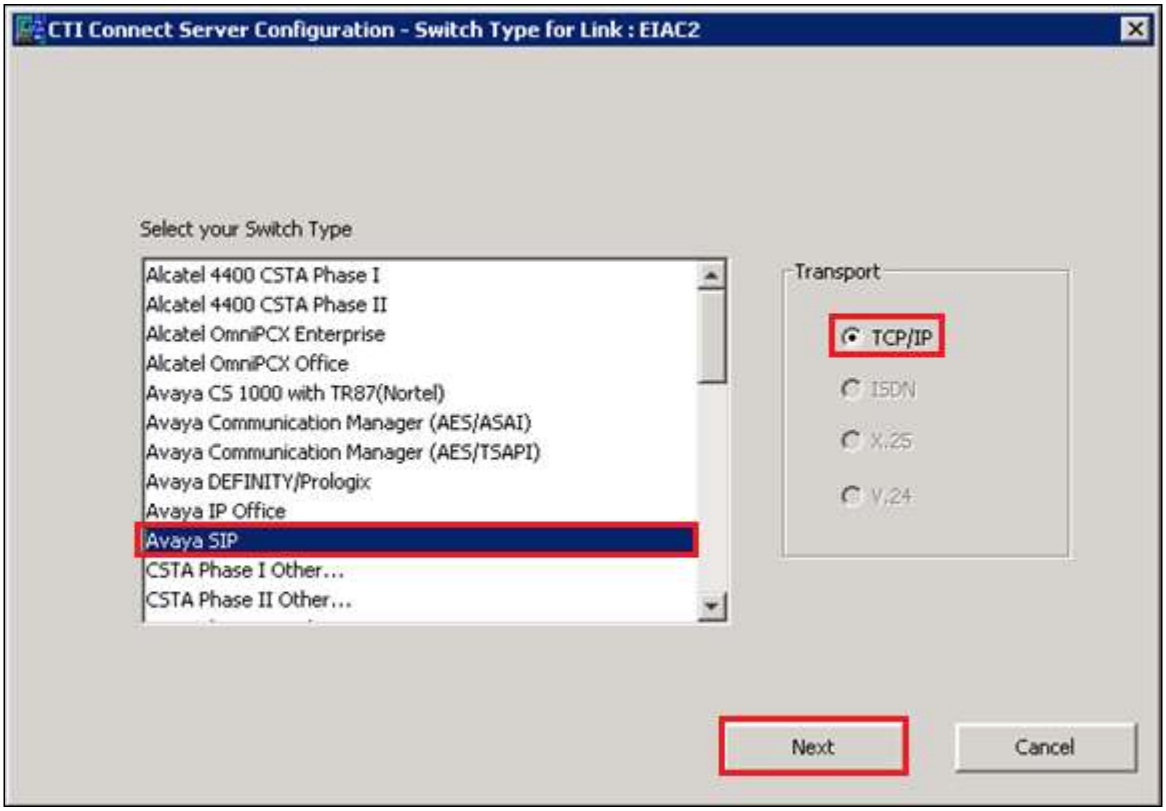
New Link

Enter a Logical Identifier: EIAC

Existing Links

Select the Logical Identifier: EIAC

In the subsequent window click on the **TCP/IP** radio button and select **Avaya** SIP from the **Select your Switch Type** pane followed by the **Next** button to continue.



CTI Connect Server Configuration - Switch Type for Link : EIAC2

Select your Switch Type

- Alcatel 4400 CSTA Phase I
- Alcatel 4400 CSTA Phase II
- Alcatel OmniPCX Enterprise
- Alcatel OmniPCX Office
- Avaya CS 1000 with TR87(Nortel)
- Avaya Communication Manager (AES/ASAI)
- Avaya Communication Manager (AES/TSAPI)
- Avaya DEFINITY/Prologix
- Avaya IP Office
- Avaya SIP
- CSTA Phase I Other...
- CSTA Phase II Other...

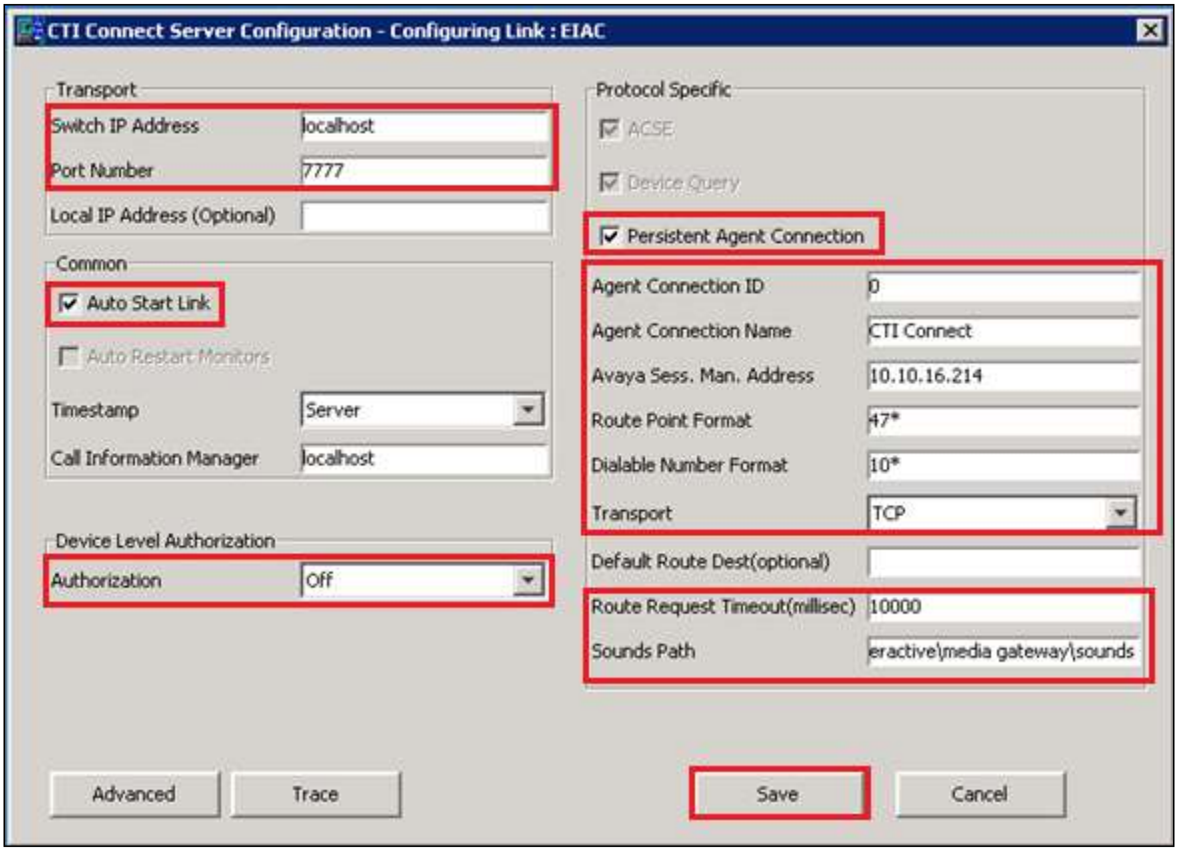
Transport

● TCP/IP
○ ISDN
○ X.25
○ V.24

In the subsequent window enter the following settings:

• **Switch IP Address**	Enter **localhost**
• **Port Number**	Enter **7777**
• **Auto start Link**	Tick the check box
• **Authorization**	Select **Off** from the dropdown list
• **Persistent Agent connection**	Tick the check box
• **Agent Connection ID**	Enter **0**
• **Agent connection Name**	Enter **CTI Connect**
• **Avaya Sess. Man. Address**	Enter the IP address of the Session Manager as seen in **Section 5.1**
• **Route Point Format**	Enter **47*** (see **Section 6.5**)
• **Dialable Number Format**	Enter the number range of Communication Manager (i.e. **10***, any number beginning with 10 will be sent to Communication Manager via Session Manager)
• **Transport**	Select **TCP** from the dropdown list
• **Route Request Timeout**	Enter **10000**
• **Sound Path**	Enter the path where the voice prompts are stored

Click on the **Save** button to continue.



CTI Connect Server Configuration - Configuring Link : EIAC

Transport
Switch IP Address: localhost
Port Number: 7777
Local IP Address (Optional):

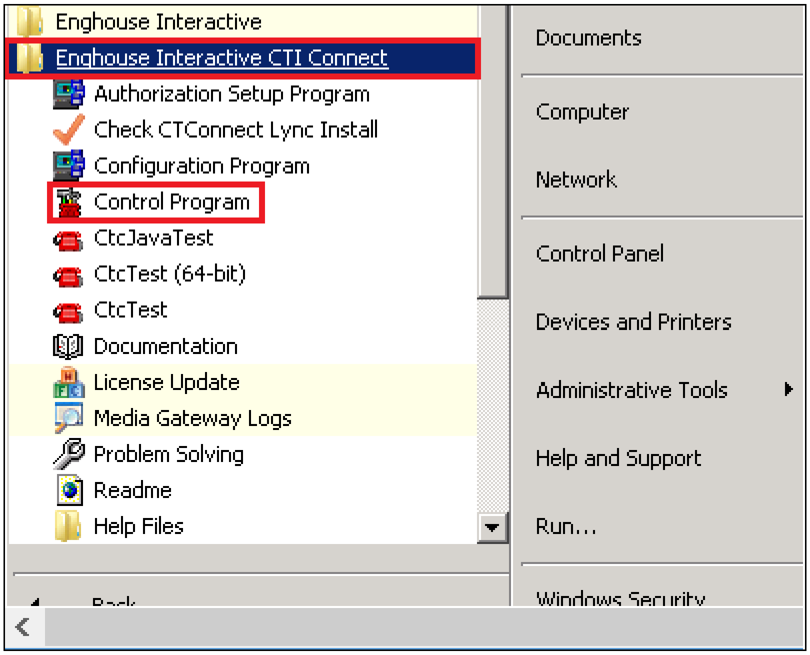
Common
☑ Auto Start Link
☐ Auto Restart Monitors
Timestamp: Server
Call Information Manager: localhost

Device Level Authorization
Authorization: Off

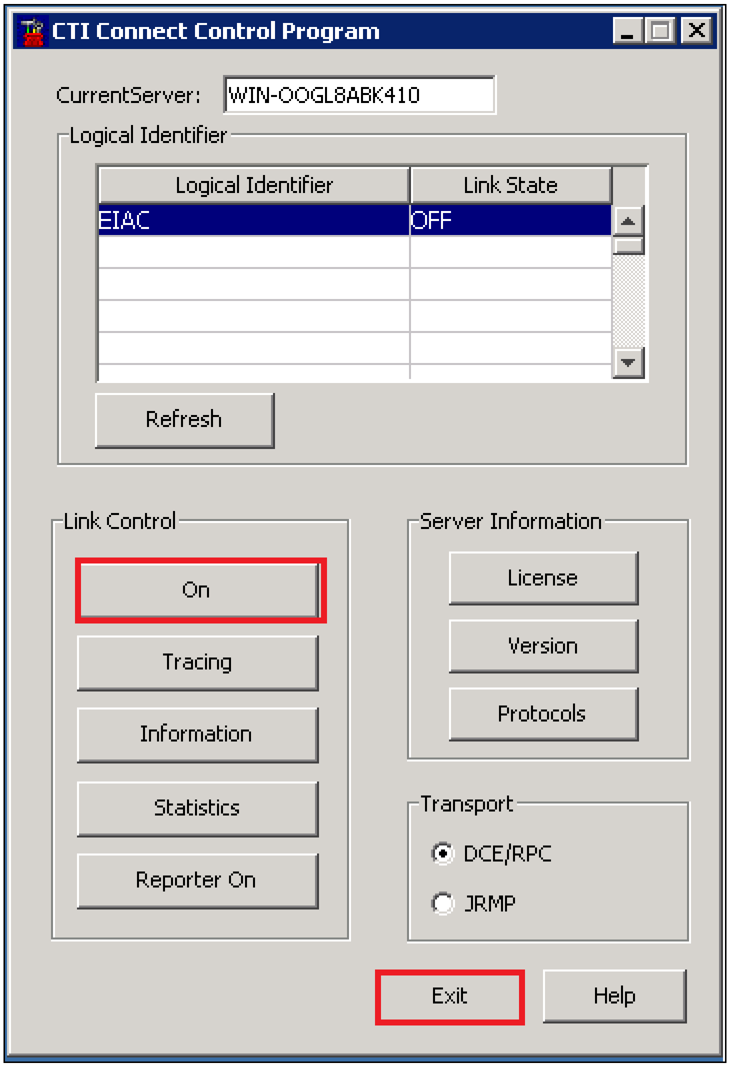
Protocol Specific
☑ ACSE
☑ Device Query
☑ Persistent Agent Connection
Agent Connection ID: 0
Agent Connection Name: CTI Connect
Avaya Sess. Man. Address: 10.10.16.214
Route Point Format: 47*
Dialable Number Format: 10*
Transport: TCP
Default Route Dest(optional):
Route Request Timeout(millisec): 10000
Sounds Path: eractive\media gateway\sounds

7.2. Turn on Link State

To turn on the Link State go to **Control Program** select **Start → All Programs →** (not shown) **Enghouse Interactive CTI Connect →Control Program**.



In the subsequent window click the **On** button, wait for the state to change and then **Exit**.



CTI Connect Control Program

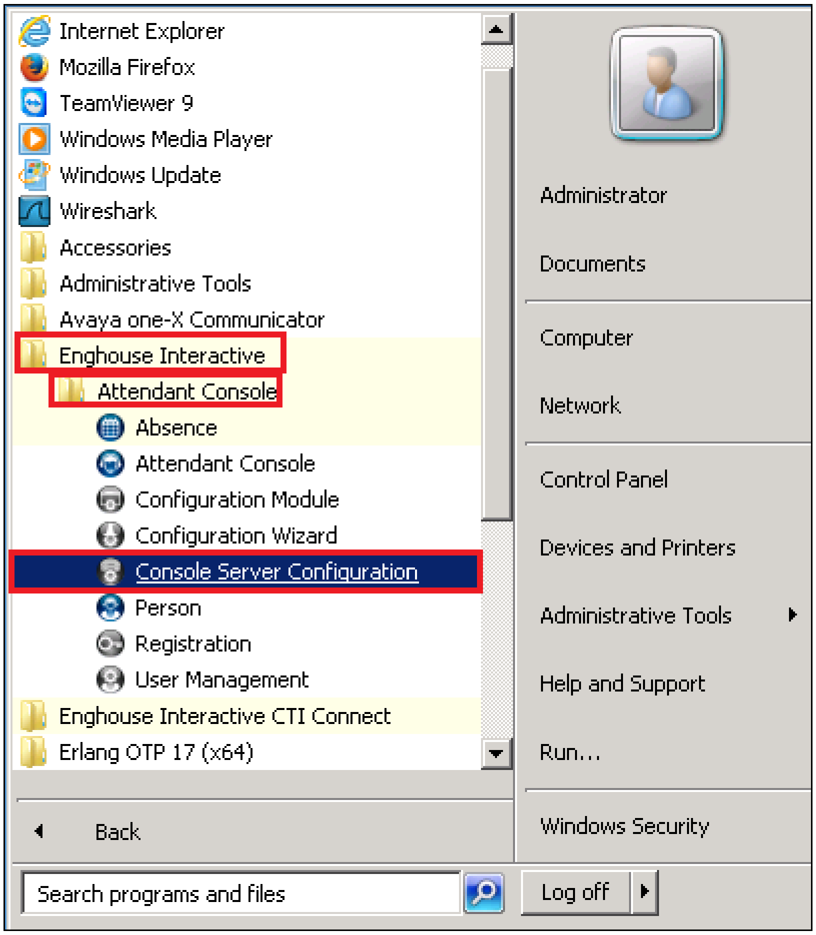
CurrentServer: WIN-OOGL8ABK410

Logical Identifier	Link State
EIAC	OFF

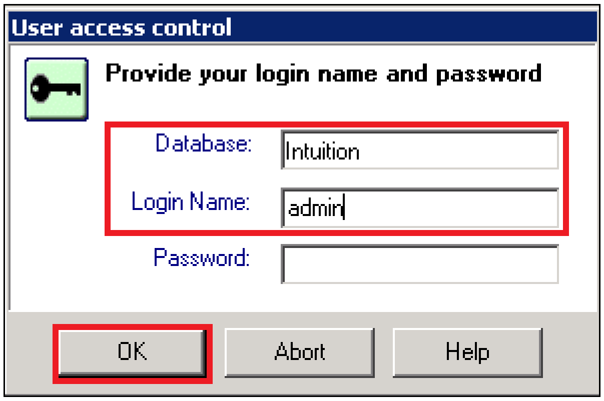
Transport: ● DCE/RPC ○ JRMP

8. Configure Console server

This section shows how to configure Enghouse Interactive Console server. To launch the **Console Server Configuration** select **Start** → **All Programs** → (not shown) **Enghouse Interactive** → **Attendant Console** → **Console Server Configuration**.



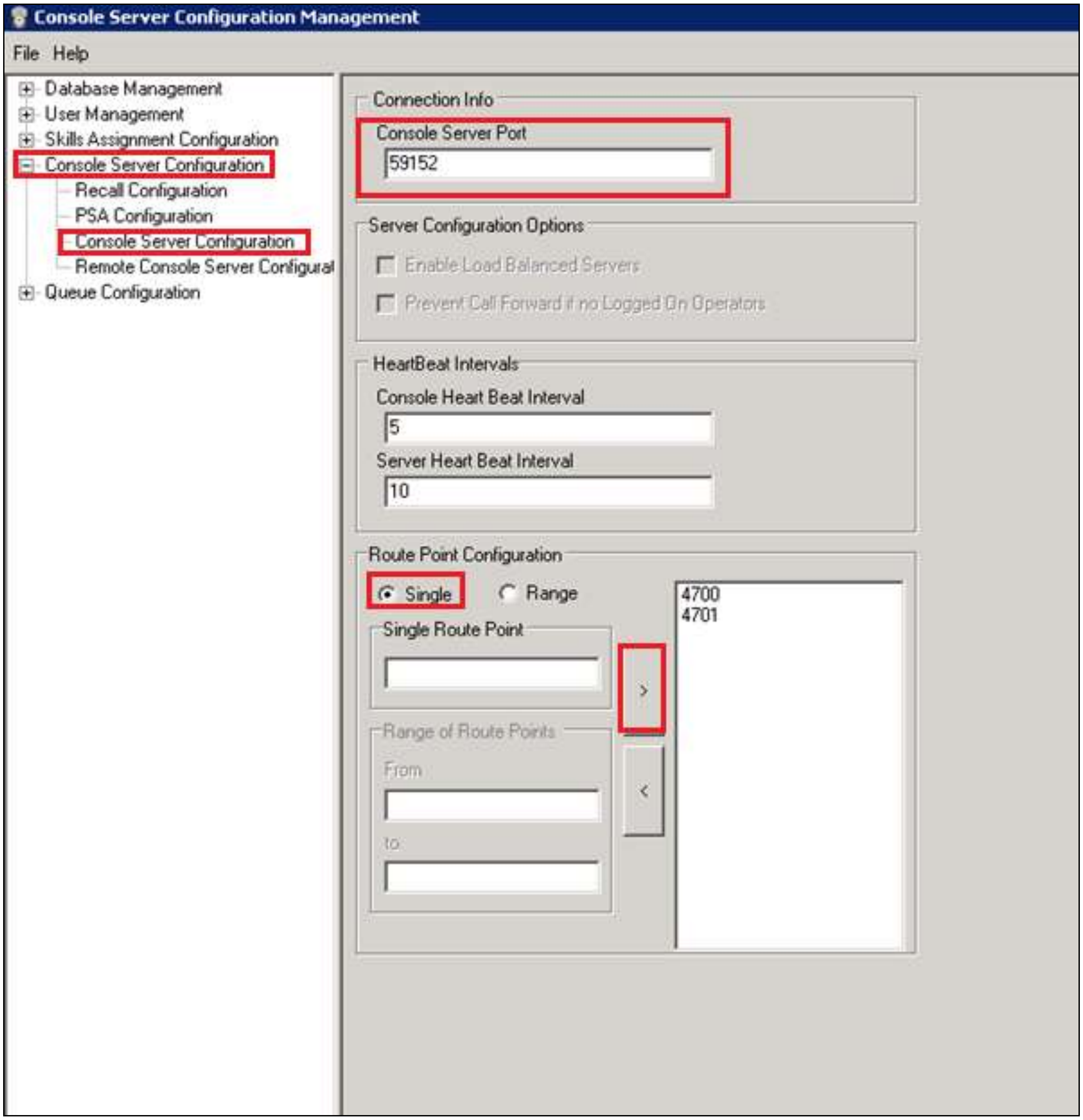
In the subsequent window enter **Intuition** in the **Database** field, **admin** in the **Login Name** field and click on the **OK** button.
Note: No Password is required.



Database: Intuition
Login Name: admin
Password:

8.1. Add Route Points for Queue

In the subsequent window navigate to **Console Server Configuration** → **Console Server Configuration**. In the **console Server Port** enter **59152**. Click the **Single** radio button. In the **Single Route Point** field enter the required Queue numbers. (In the example below **4700** and **4701** were added.



Console Server Port: 59152

☐ Enable Load Balanced Servers

☐ Prevent Call Forward if no Logged On Operators

Console Heart Beat Interval: 5

Server Heart Beat Interval: 10

● Single ○ Range

4700
4701

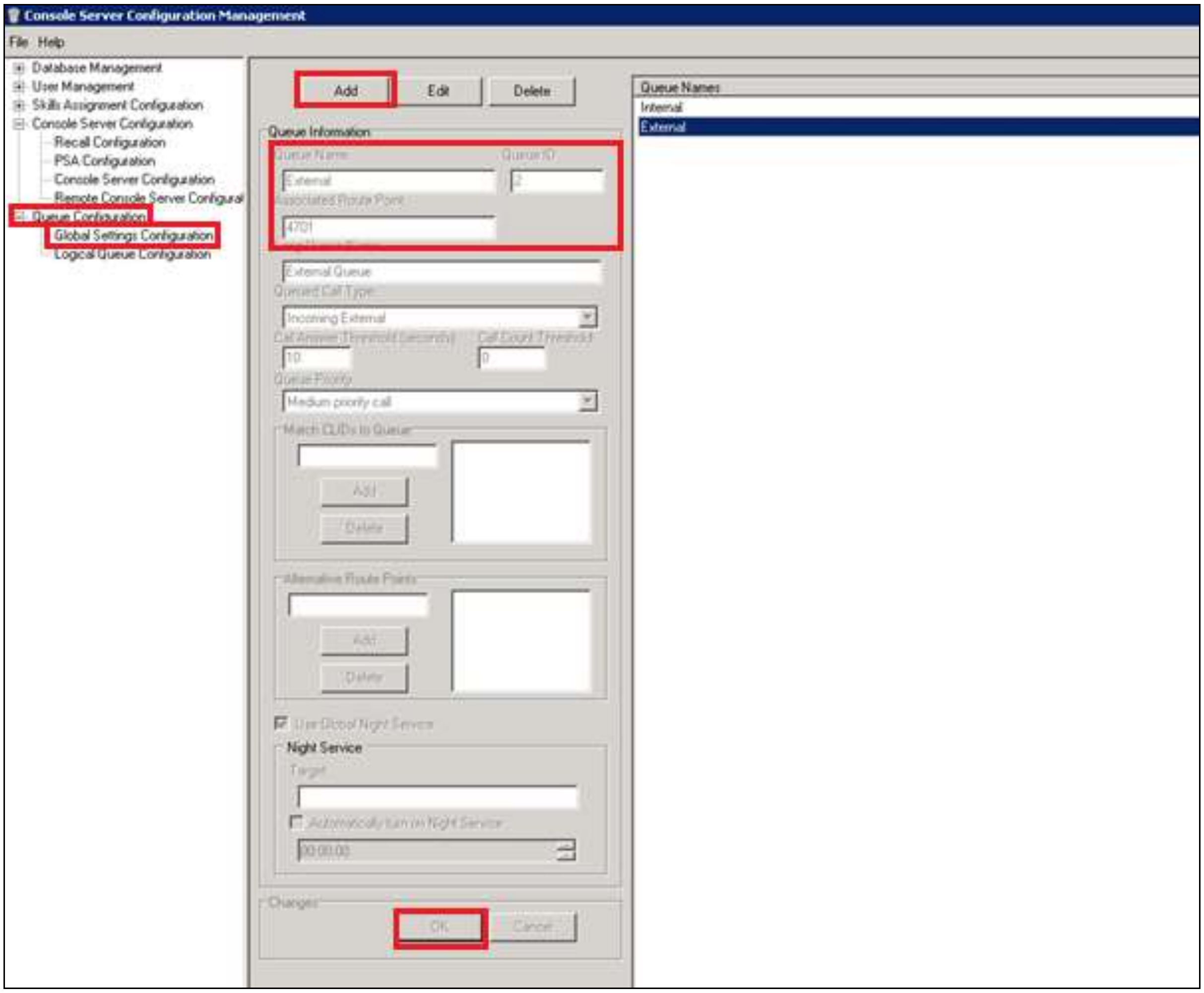
Console Server Configuration Management
File Help
Database Management
User Management
Skills Assignment Configuration
Console Server Configuration
Recall Configuration
PSA Configuration
Console Server Configuration
Remote Console Server Configurat
Queue Configuration
Connection Info
Server Configuration Options
HeartBeat Intervals
Route Point Configuration
Single Route Point
Range of Route Points
From
to
>
<

8.2. Add Queues

In the example below the **External** queue is configured. To add the Queues navigate to **Queue Configuration → Global Settings Configuration** and enter the following:

Queue Name	Enter **External**
Queue ID	Enter **2**
Associated Route Point	Enter **4701**

Click on the **Add** button. Repeat for the internal queue, where 4700 is the **Associated Route Point** and the **Queue ID** is **1**. When complete and click on the **OK** button.



Queue Name: External

Queue ID: 2

Associated Route Point: 4701

[illegible]: External Queue

Queued Call Type: Incoming External

Call Answer Threshold (seconds): 10

Call Count Threshold: 0

Queue Priority: Medium priority call

☑ Use Global Night Service

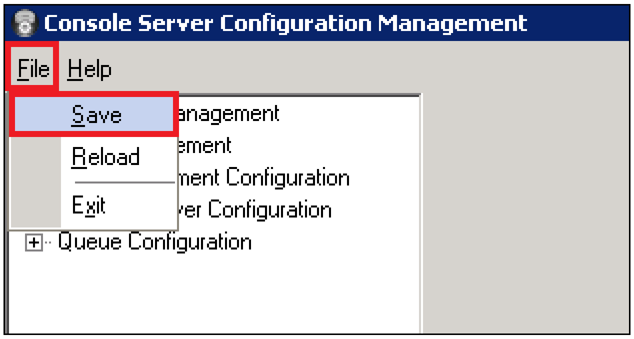
Target:

☐ Automatically turn on Night Service

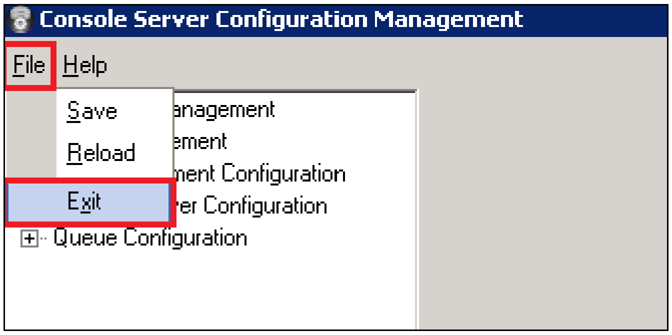
00:00:00

Queue Names: Internal, External

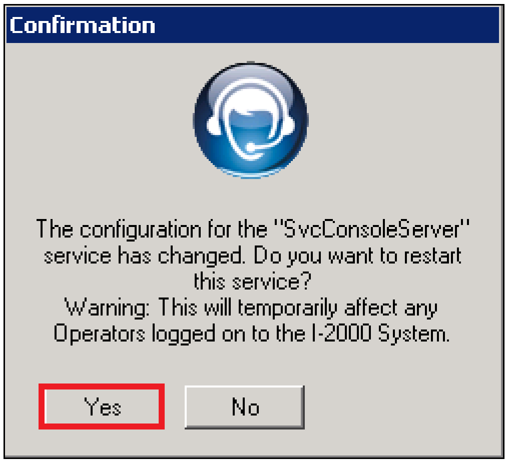
To save the configuration click on **File** followed by **Save**.



To exit **Console Server Configuration** click on **File** followed by **Exit**.



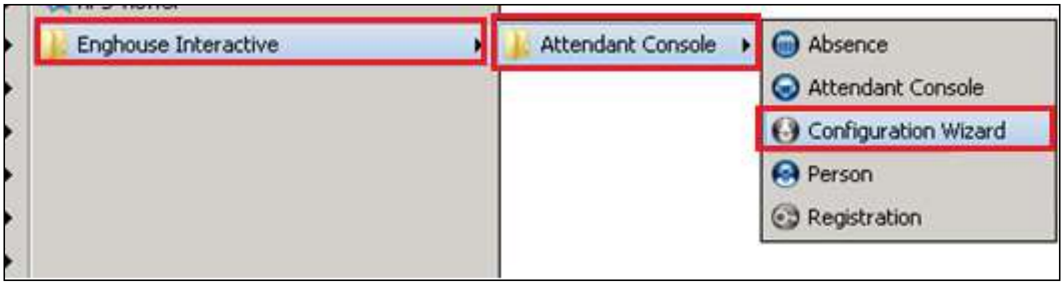
After exiting click on the **Yes** button in the subsequent **Confirmation** window to restart the Console server.


Confirmation

The configuration for the "SvcConsoleServer" service has changed. Do you want to restart this service?
Warning: This will temporarily affect any Operators logged on to the I-2000 System.

9. Configure Attendant Console Client

This section shows how to configure Enghouse Interactive CTI Connect Attendant Console Client. The installation of the Attendant Console Client software is assumed to be completed To configure Attendant Console client click on **Start →Programs →** (not shown) **Enghouse Interactive → Attendant Console → Configuration Wizard**.



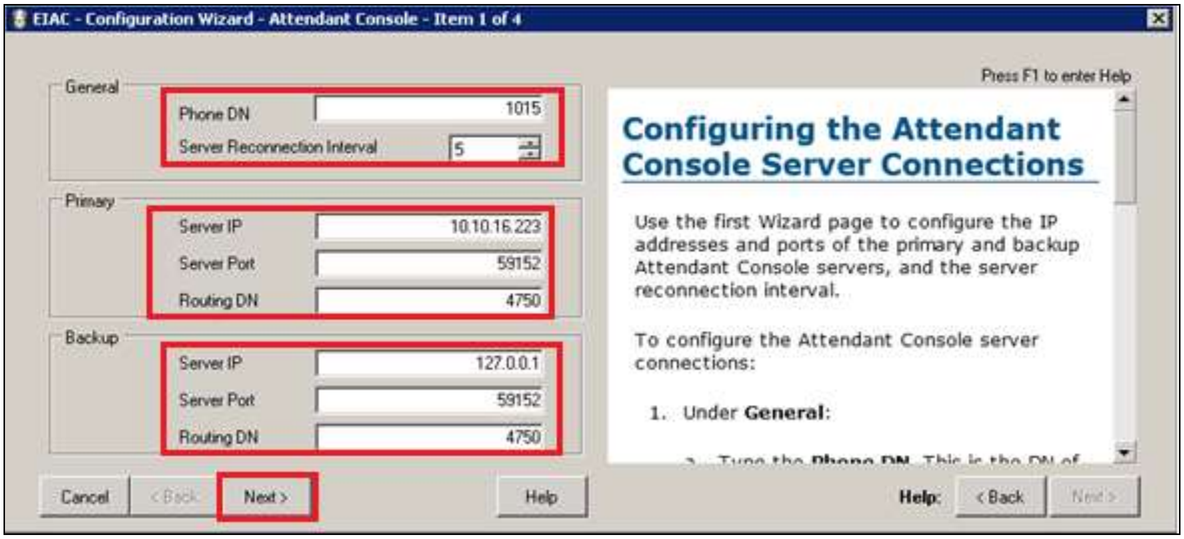
When the **Configuration Wizard** opens enter the following:

• **Phone DN**	Enter the extension of the telephone configured on the Communication Manager to act as the Attendant telephone. (i.e. **1015**)
• **Server Reconnection Interval**	Enter **5**
• **Server IP**	Enter the IP address of the CTI Connect Server
• **Server Port**	Enter **59152**
• **Routing DN**	Enter **4750** (this is an internal number used for the agent using the Attendant client)

Backup (if no Backup server is available configure the following:

• **Server IP**	Enter **127.0.0.1**
• **Server Port**	Enter **59152**
• **Routing DN**	Enter **4750**

Click on the **Next** button (3 times, not shown) button to continue followed by the **Finish** button.


EIAC - Configuration Wizard - Attendant Console - Item 1 of 4

General
Phone DN: 1015
Server Reconnection Interval: 5

Primary
Server IP: 10.10.16.223
Server Port: 59152
Routing DN: 4750

Backup
Server IP: 127.0.0.1
Server Port: 59152
Routing DN: 4750

Press F1 to enter Help

Configuring the Attendant Console Server Connections

Use the first Wizard page to configure the IP addresses and ports of the primary and backup Attendant Console servers, and the server reconnection interval.

To configure the Attendant Console server connections:

1. Under **General**:

   a. Type the **Phone DN**. This is the DN of

10. Verification

This section provides the tests that can be performed to verify correct configuration of the Avaya and Enghouse Interactive solution.

10.1. Verify the signaling group status

Using the SAT terminal, enter the **status signaling-group <n>** command, where **<n>** is the number of the SIP signaling group which connects to Session Manager. Verify that the **Group State** is **in-service**.

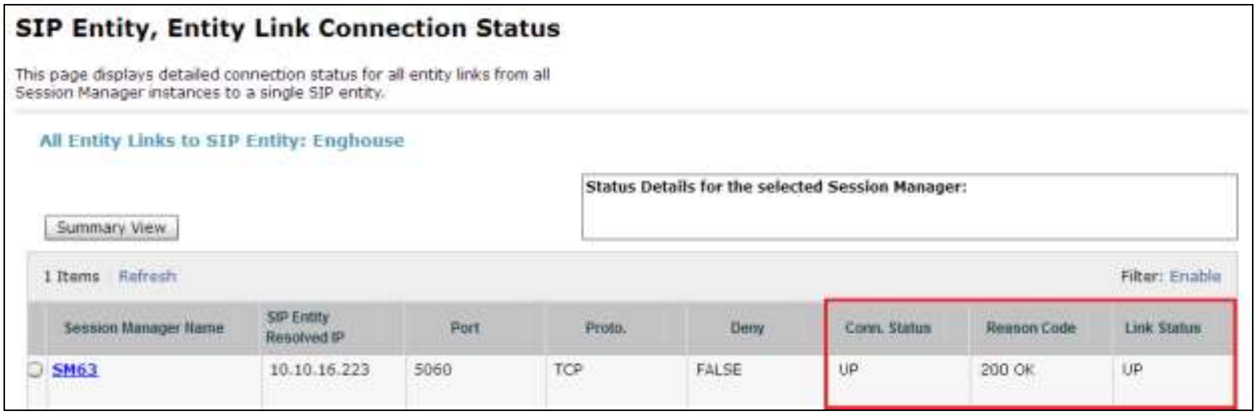
```
status signaling-group 1
                         STATUS SIGNALING GROUP

        Group ID: 1
      Group Type: sip

     Group State: in-service
```

10.2. Verify the SIP Entity Link status for Attendant Console

From System Manager select **Session Manager** from under the **Elements** column, not shown. When the **Session Manager** tab opens select **System Status** followed by **SIP Entity Monitoring**, then click on **Enghouse** SIP Entity (not shown) created in **Section 6.2**, ensure that the **Conn. Status** is **Up**, the **Reason Code** is **200OK** and the **Link Status** is **Up**.



SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

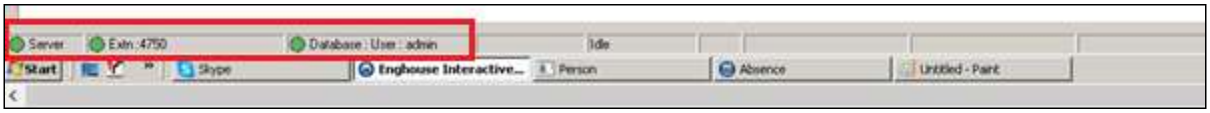
All Entity Links to SIP Entity: Enghouse

Status Details for the selected Session Manager:

Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
○ SM63	10.10.16.223	5060	TCP	FALSE	UP	200 OK	UP

10.3. Verify Attendant Console

Login to a Attendant Console client using the appropriate credentials (not shown) and verify the **Server**, **Extn** and **Database** icons are green as per the screenshot below.



11. Conclusion

A full and comprehensive set of feature and functional test cases were performed during Compliance testing. Enghouse Interactive Attendant Console 8.1 is considered compliant with Avaya Aura® Communication Manager 6.3 and Avaya Aura® Session Manager 6.3. All test cases have passed and met the all objectives with one observation as outlined in **Section 2.2**.

12. Additional References

These documents form part of the Avaya official technical reference documentation suite. Further information may be had from *http://support.avaya.com* or from the local Avaya representative.

[1] *Administering Avaya Aura® Communication Manager, Release 6.3, Document Number 03-300509, Issue 9.0.*

[2] *Administering Avaya Aura® Session Manager, Release 6.3*

[3] *Administering Avaya Aura® System Manager, Release 6.3*

Product Documentation for Enghouse Interactive AB can be obtained in the installed software or at: https://mysupport.enghouseinteractive.com

The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.