



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Configuring Avaya Aura® Communication Manager R6.3 and Avaya Aura® Application Enablement Services R6.3 to Interoperate with ASC Telecom ASC EVOIPneo active - Issue 1.0**

## **Abstract**

These Application Notes describe the configuration steps for ASC telecom ASC EVOIPneo active for Avaya Aura (with CM & AES) to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. ASC telecom ASC EVOIPneo active for Avaya Aura (with CM & AES) integrates with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using single step conferencing implemented via DMCC over TSAPI.

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 describe the compliance tested configuration using ASC EVOIPneo active for Avaya Aura (with CM & AES) with Avaya Aura® Communication Manager R6.3 and Avaya Aura® Application Enablement Services R6.3 (AES).

ASC EVOIPneo active for Avaya Aura (with CM & AES) (ASC) uses Avaya Aura® Communication Manager's Single Step Conferencing (SSC) feature via the Device, Media, and Call Control (DMCC) service provided by the Avaya Aura® Application Enablement Services (AES) to capture the audio and call details for recording agent calls. ASC EVOIPneo active for Avaya Aura (with CM & AES) uses the Avaya Aura® Application Enablement Services DMCC service to register a pool of virtual IP softphones that are used as "recorders". Target agents, whose calls are to be recorded, are configured on the ASC server. When a target agent places or receives a call, SSC is used to conference in a "recorder" to capture the audio stream and call details.

The ASC EVOIPneo active for Avaya Aura (with CM & AES) is fully integrated into a LAN (Local Area Network), and includes easy-to-use Web based application that works with Java to retrieve telephone conversations from a comprehensive long-term calls database.

## 2. General Test Approach and Test Results

The interoperability compliance testing evaluated the ability of ASC telecom to carry out call recording in a variety of scenarios using DMCC with AES and Communication Manager.

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 test included both feature functionality and serviceability testing. The feature functionality testing focused on placing and recording calls in different call scenarios with good quality audio recordings and accurate call records. The tests included:

- Inbound Calls
- Outbound Calls
- Call Hold
- Blind Transfer
- Consultative Transfer
- Blind 3-way Conference
- Supervised Conference
- Forwarded Calls
- No Answer, Engaged, Unobtainable
- Inbound Calls to Communication Manager Agents
- Failover Testing

The serviceability testing focused on verifying the ability of ASC to recover from disconnection and reconnection to the Avaya solution.

## 2.2. Test Results

All functionality and serviceability test cases were completed successfully.

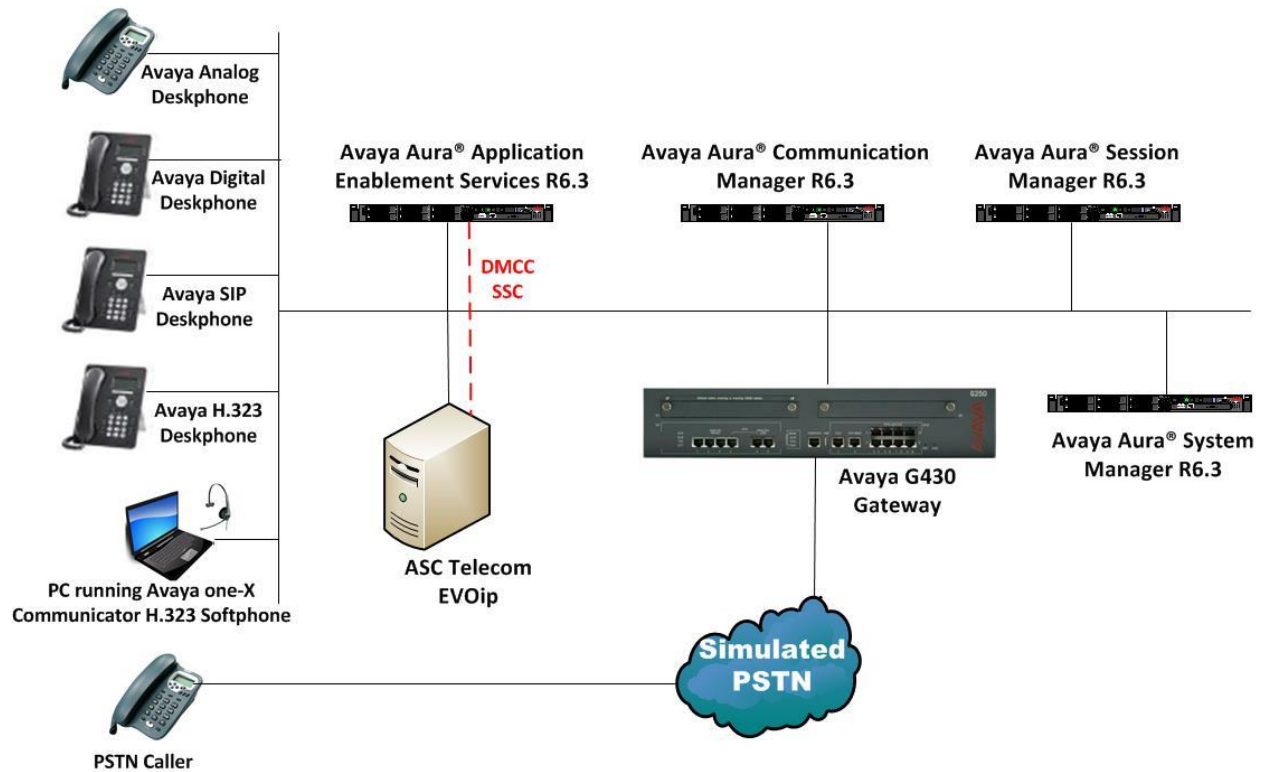
## 2.3. Support

Technical support can be obtained for ASC telecom as follows:

- Email: [hq@asctelecom.com](mailto:hq@asctelecom.com)
- Website: [www.asctelecom.com](http://www.asctelecom.com)
- Phone: +49 6021 5001-0

### 3. Reference Configuration

**Figure 1** shows the network topology during interoperability testing. Communication Manager with an Avaya G430 Media Gateway was used as the hosting PBX. ASC call recording component is connected to the LAN and recording is performed using the Single Step Conference feature of Communication Manager using DMCC provided by AES.



**Figure 1: Avaya Aura® Communication Manager with Avaya Aura® Application Enablement Services, and ASC telecom ASC EVOIPneo active for Avaya Aura (with CM & AES) configuration**

## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® System Manager running on Avaya S8800 Server	System Manager 6.3.0 - FP2 Build No. - 6.3.0.8.5682-6.3.8.1814 Software Update Revision No: 6.3.3.5.1719
Avaya Aura® Communication Manager running on Avaya S8800 Server	R6.3 SP1 R016x.03.0.124.0
Avaya Aura® Application Enablement Services running on Avaya S8800 Server	R6.3 Build No - 6.3.0.0.212-0
Avaya G430 Gateway	R6.3
Avaya Analog deskphone	N/A
Avaya Digital deskphone	N/A
Avaya 96xx/96x1 Series Deskphone	96xx H.323 Release 3.1 SP2
Avaya 96xx/96x1 Series Deskphone	96xx SIP Release 2.6 SP3
Avaya one-X® Communicator running H.323 Firmware	R6.1
ASC EVOIPneo active for Avaya Aura (with CM & AES) running on Windows 2012 R2 Server	R3.0
ASC POWERplay Web running on Mozilla Firefox	R3.0

## 5. Configure Avaya Aura® Communication Manager

The information provided in this section describes the configuration of Communication Manager relevant to this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**.

The configuration illustrated in this section was performed using Communication Manager System Administration Terminal (SAT).

### 5.1. Verify System Features

Use the **display system-parameters customer-options** command to verify that Communication Manager has permissions for features illustrated in these Application Notes. On **Page 3**, ensure that **Answer Supervision by Call Classifier?** is set to **y** and **Computer Telephony Adjunct Links?** is set to **y** as shown below.

display system-parameters customer-options		Page	3 of	11
OPTIONAL FEATURES				
Abbreviated Dialing Enhanced List?	y	Audible Message Waiting?	y	
Access Security Gateway (ASG)?	n	Authorization Codes?	y	
Analog Trunk Incoming Call ID?	y	CAS Branch?	n	
A/D Grp/Sys List Dialing Start at 01?	y	CAS Main?	n	
<b>Answer Supervision by Call Classifier?</b>	<b>y</b>	Change COR by FAC?	n	
ARS?	y	<b>Computer Telephony Adjunct Links?</b>	<b>y</b>	
ARS/AAR Partitioning?	y	Cvg Of Calls Redirected Off-net?	y	
ARS/AAR Dialing without FAC?	y	DCS (Basic)?	y	
ASAI Link Core Capabilities?	n	DCS Call Coverage?	y	
ASAI Link Plus Capabilities?	n	DCS with Rerouting?	y	
Async. Transfer Mode (ATM) PNC?	n			
Async. Transfer Mode (ATM) Trunking?	n	Digital Loss Plan Modification?	y	
ATM WAN Spare Processor?	n	DS1 MSP?	y	
ATMS?	y	DS1 Echo Cancellation?	y	
Attendant Vectoring?	y			

## 5.2. Display Node Names for Avaya Aura® Application Enablement Services Connectivity

Display the **procr** IP Address by using the command **display node-names ip** and noting the IP address for the **procr** and AES (**aes63vmpg**).

display node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
SM100	10.10.40.34	
<b>aes63vmpg</b>	<b>10.10.40.30</b>	
default	0.0.0.0	
g430	10.10.40.15	
<b>procr</b>	<b>10.10.40.31</b>	

## 5.3. Configure AE service for Avaya Aura® Application Enablement Services Connectivity

To administer the transport link to AES use the **change ip-services** command. On **Page 1** add an entry with the following values:

- **Service Type:** should be set to **AESVCS**.
- **Enabled:** set to **y**.
- **Local Node:** set to the node name assigned for the **procr** in **Section 5.2**
- **Local Port:** retain the default value of **8765**.

change ip-services		Page 1 of 4
IP SERVICES		
Service Type	Enabled	Local Node
AESVCS	y	procr

Go to **Page 4** of the **ip-services** form and enter the following values:

- **AE Services Server:** Name obtained from the AES server, in this case **aes62vmpg**.
- **Password:** Enter a password to be administered on the AES server.
- **Enabled:** Set to **y**.

**Note:** The password entered for **Password** field must match the password on the AES server in **Section 6.2**. The **AE Services Server** should match the administered name for the AES server, this is created as part of the AES installation, and can be obtained from the AES server by typing **uname -n** at the Linux command prompt.

change ip-services		Page 4 of 4
AE Services Administration		
Server ID	AE Services Server	Password
1:	<b>aes63vmpg</b>	*****
2:		
3:		

## 5.4. Configure CTI Link for TSAPI Service

Add a CTI link using the **add cti-link n** command. Enter an available extension number in the **Extension** field. Enter **ADJ-IP** in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

```
add      cti-link 1                               Page   1 of   3
                                         CTI LINK
CTI Link: 1
Extension: 2002
      Type: ADJ-IP
                                         COR: 1
Name: aes63vmpg
```

## 5.5. Configure Virtual Stations

ASC uses the Single Step Conferencing method to conference “recorders” with the agent calls in order to capture the call audio. Use the command **add station** to configure a station for each of the recording pool stations. On **Page 1** enter a descriptive **Name** and **Security Code**, set the **Port** to **IP**, set the **Type** to **4624** and set **IP SoftPhone** to **y**. Repeat according to the maximum number of call to be recorded simultaneously. These extensions can also be configured on ASC for the playback of recordings. Configure sufficient stations to accommodate for the maximum number of simultaneous recording playback channels required.

```
add station 2800                               Page   1 of   6
                                         STATION
Extension: 2800                                Lock Messages? n          BCC: 0
      Type: 4624                                Security Code: 1234       TN: 1
      Port: IP                                Coverage Path 1:         COR: 1
      Name: ASC      Recorder 1                Coverage Path 2:         COS: 1
                                         Hunt-to Station:
STATION OPTIONS
      Loss Group: 19                        Time of Day Lock Table:
      Speakerphone: 2-way                    Personalized Ringing Pattern: 1
      Display Language: english                Message Lamp Ext: 1591
Survivable GK Node Name:                      Mute Button Enabled? y
      Survivable COR: internal                  Media Complex Ext:
      Survivable Trunk Dest? y                  IP SoftPhone? y
                                         IP Video Softphone? n
```



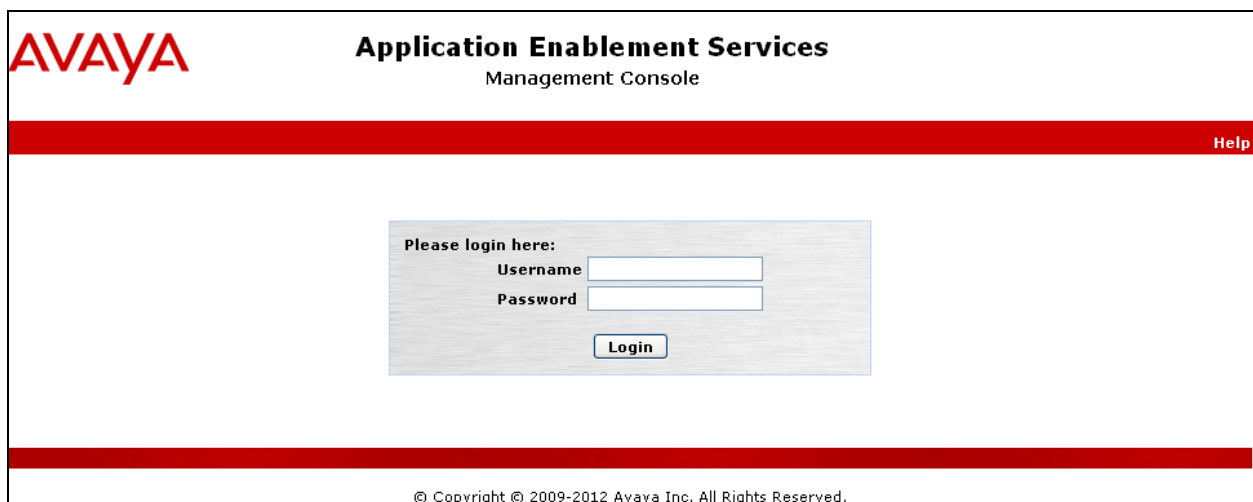
## 6. Configure Avaya Aura® Application Enablement Services

This section provides the procedures for configuring Application Enablement Services. The procedures fall into the following areas:

- Verify Licensing
- Create Switch Connection
- Administer TSAPI link
- Create CTI User
- Enable CTI Link User
- Identify Tlinks
- Enable DMCC ports

### 6.1. Verify Licensing

To access the maintenance console, enter **https://<ip-addr>** as the URL in an Internet browser, where <ip-addr> is the active IP address of AES. The login screen is displayed, log in with the appropriate credentials and then select the **Login** button.



The image shows the login screen for the Avaya Application Enablement Services Management Console. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" is displayed in a large, bold font, with "Management Console" in a smaller font below it. A thick red horizontal bar spans the width of the page, with the word "Help" in white text on the right side. In the center of the page is a light gray rectangular box containing the login form. The form has the text "Please login here:" followed by two input fields: "Username" and "Password". Below these fields is a "Login" button. At the bottom of the page, a thin red horizontal bar is present, and below it, the copyright notice "© Copyright © 2009-2012 Avaya Inc. All Rights Reserved." is displayed.

The Application Enablement Services Management Console appears displaying the **Welcome to OAM** screen (not shown). Select **AE Services** and verify that the TSAPI Service is licensed by ensuring that **TSAPI Service** is in the list of services and that the **License Mode** is showing **NORMAL MODE**. If not, contact an Avaya support representative to acquire the proper license for your solution.

**AVAYA** Application Enablement Services Management Console

Welcome: User craft  
Last login: Wed Dec 12 10:45:16 2012 from 192.168.10.209  
Number of prior failed login attempts: 0  
HostName/IP: aes62vmppg.devconnect.local/10.10.40.10  
Server Offer Type: SWONLY  
SW Version: r6-2-0-18-0  
Server Date and Time: Thu Dec 20 11:51:08 UTC 2012

**AE Services** Home | Help | Logout

▼ AE Services

- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▶ TSAPI
- ▶ TWS
- ▶ Communication Manager Interface
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▶ Status

**AE Services**

IMPORTANT: AE Services must be restarted for administrative changes to fully take effect. Changes to the Security Database do not require a restart.

Service	Status	State	License Mode	Cause*
ASAI Link Manager	N/A	Running	N/A	N/A
CVLAN Service	ONLINE	Running	NORMAL MODE	N/A
DLG Service	OFFLINE	Running	N/A	N/A
DMCC Service	ONLINE	Running	NORMAL MODE	N/A
<b>TSAPI Service</b>	<b>ONLINE</b>	<b>Running</b>	<b>NORMAL MODE</b>	N/A
Transport Layer Service	N/A	Running	N/A	N/A

For status on actual services, please use [Status and Control](#)

\* -- For more detail, please mouse over the Cause, you'll see the tooltip, or go to help page.

## 6.2. Create Switch Connection

From the AES Management Console navigate to **Communication Manager Interface** → **Switch Connections** to set up a switch connection. Enter in a name for the Switch Connection to be added and click the **Add Connection** button.

**AVAYA** Application Enablement Services Management Console

Welcome: User craft  
Last login: Thu Nov 14 10:22:12 2013 from 10.10.40.140  
Number of prior failed login attempts: 16  
HostName/IP: AES63VMPPG  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 6.3.0.0.212-0  
Server Date and Time: Tue Dec 3 15:33:26 UTC 2013

**Communication Manager Interface | Switch Connections** Home | Help | Logout

▼ AE Services

- ▶ Communication Manager Interface
- Switch Connections**
- ▶ Dial Plan
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

**Switch Connections**

CM63VMPPG Add Connection

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections

Edit Connection Edit PE/CLAN IPs Edit H.323 Gatekeeper Delete Connection Survivability Hierarchy

In the resulting screen enter the **Switch Password**, the Switch Password must be the same as that entered into Communication Manager AE Services Administration screen via the **change ip-services** command, described in **Section 5.3** Default values may be accepted for the remaining fields. Click **Apply** to save changes.

**AVAYA** Application Enablement Services Management Console

Welcome: User craft  
Last login: Thu Nov 14 10:22:12 2013 from 10.10.40.140  
Number of prior failed login attempts: 16  
HostName/IP: AES63VMPG  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 6.3.0.0.212-0  
Server Date and Time: Tue Dec 3 15:35:47 UTC 2013

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services  
Communication Manager Interface  
Switch Connections  
Dial Plan  
Licensing  
Maintenance  
Networking  
Security  
Status  
User Management  
Utilities  
Help

Connection Details - CM63vmpg

Switch Password: [Redacted]  
Confirm Switch Password: [Redacted]  
Msg Period: 30 Minutes (1 - 72)  
SSL: ☒  
Processor: Ethernet ☒  
Apply Cancel

From the **Switch Connections** screen, select the radio button for the recently added switch connection and select the **Edit CLAN IPs** button (not shown). In the resulting screen, enter the IP address of the **procr** as shown in **Section 5.2** that will be used for the AES connection and select the **Add Name or IP** button.

**AVAYA** Application Enablement Services Management Console

Welcome: User craft  
Last login: Thu Nov 14 10:22:12 2013 from 10.10.40.140  
Number of prior failed login attempts: 16  
HostName/IP: AES63VMPG  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 6.3.0.0.212-0  
Server Date and Time: Tue Dec 03 15:36:31 UTC 2013

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services  
Communication Manager Interface  
Switch Connections  
Dial Plan  
Licensing  
Maintenance  
Networking  
Security  
Status  
User Management  
Utilities  
Help

Edit Processor Ethernet IP - CM63vmpg

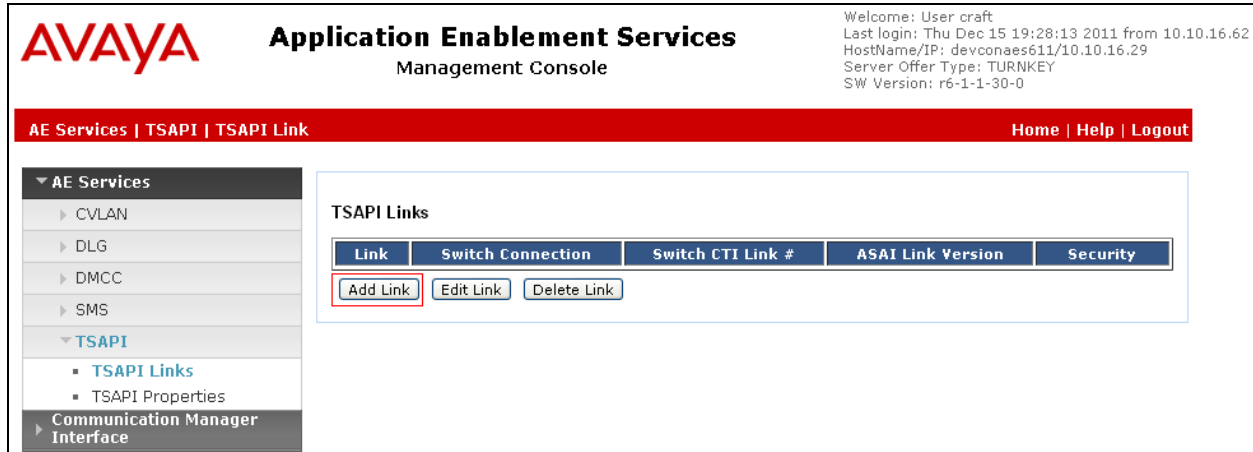
10.10.40.31 Add/Edit Name or IP

Name or IP Address	Status
10.10.40.31	In Use

Back

### 6.3. Administer TSAPI link

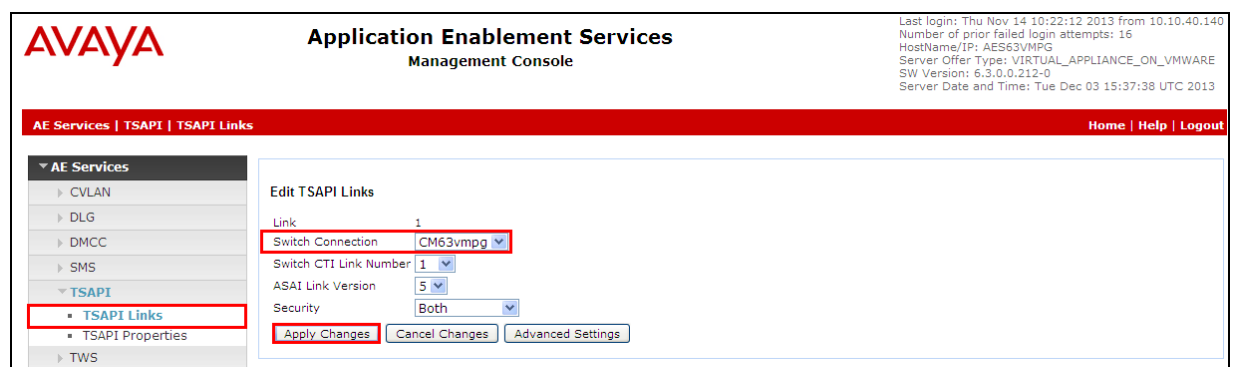
From the Application Enablement Services Management Console, select **AE Services** → **TSAPI** → **TSAPI Links**. Select **Add Link** button as shown in the screen below.



On the **Add TSAPI Links** screen, enter the following values:

- **Link:** Use the drop-down list to select an unused link number.
- **Switch Connection:** Choose the switch connection **CM63VMPG**, which has already been configured in **Section 6.2**, from the drop-down list.
- **Switch CTI Link Number:** Corresponding CTI link number configured in **Section 5.4** which is **1**.
- **ASAI Link Version:** This can be left at the default value of **5**.
- **Security:** This can be left at the default value of **both**.

Once completed, select **Apply Changes**.



Another screen appears for confirmation of the changes. Choose **Apply**.

**AVAYA Application Enablement Services Management Console**

Welcome: User craft  
Last login: Thu Dec 15 19:28:13 2011 from 10.10.16.62  
HostName/IP: devconaes611/10.10.16.29  
Server Offer Type: TURNKEY  
SW Version: r6-1-1-30-0

**AE Services | TSAPI | TSAPI Link** Home | Help | Logout

**▼ AE Services**

- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▼ TSAPI**
  - **TSAPI Links**
  - TSAPI Properties
- ▶ Communication Manager Interface

**Apply Changes to Link**

Warning! Are you sure you want to apply the changes?  
These changes can only take effect when the TSAPI server restarts.  
Please use the Maintenance -> Service Controller page to restart the TSAPI server.

When the TSAPI Link is completed, it should resemble the screen below.

**AVAYA Application Enablement Services Management Console**

Last login: Tue Dec 3 15:32:14 2013 from 10.10.40.225  
Number of prior failed login attempts: 17  
HostName/IP: AES63VMPG  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 6.3.0.0.212-0  
Server Date and Time: Tue Dec 03 16:34:53 UTC 2013

**AE Services | TSAPI | TSAPI Links** Home | Help | Logout

**▼ AE Services**

- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▼ TSAPI**
  - **TSAPI Links**
  - TSAPI Properties

**TSAPI Links**

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
1	CM63vmppg	1	5	Both

The TSAPI Service must be restarted to effect the changes made in this section. From the Management Console menu, navigate to **Maintenance → Service Controller**. On the Service Controller screen, tick the **TSAPI Service** and select **Restart Service**.

**AVAYA Application Enablement Services Management Console**

Welcome: User craft  
Last login: Thu Dec 15 19:28:13 2011 from 10.10.16.62  
HostName/IP: devconaes611/10.10.16.29  
Server Offer Type: TURNKEY  
SW Version: r6-1-1-30-0

**Maintenance | Service Controller** Home | Help | Logout

**▼ AE Services**

- ▶ Communication Manager Interface
- ▶ Licensing
- ▼ Maintenance**
  - ▶ Date Time/NTP Server
  - ▶ Security Database
  - Service Controller**
  - ▶ Server Data
- ▶ Networking
- ▶ Security
- ▶ Status
- ▶ User Management

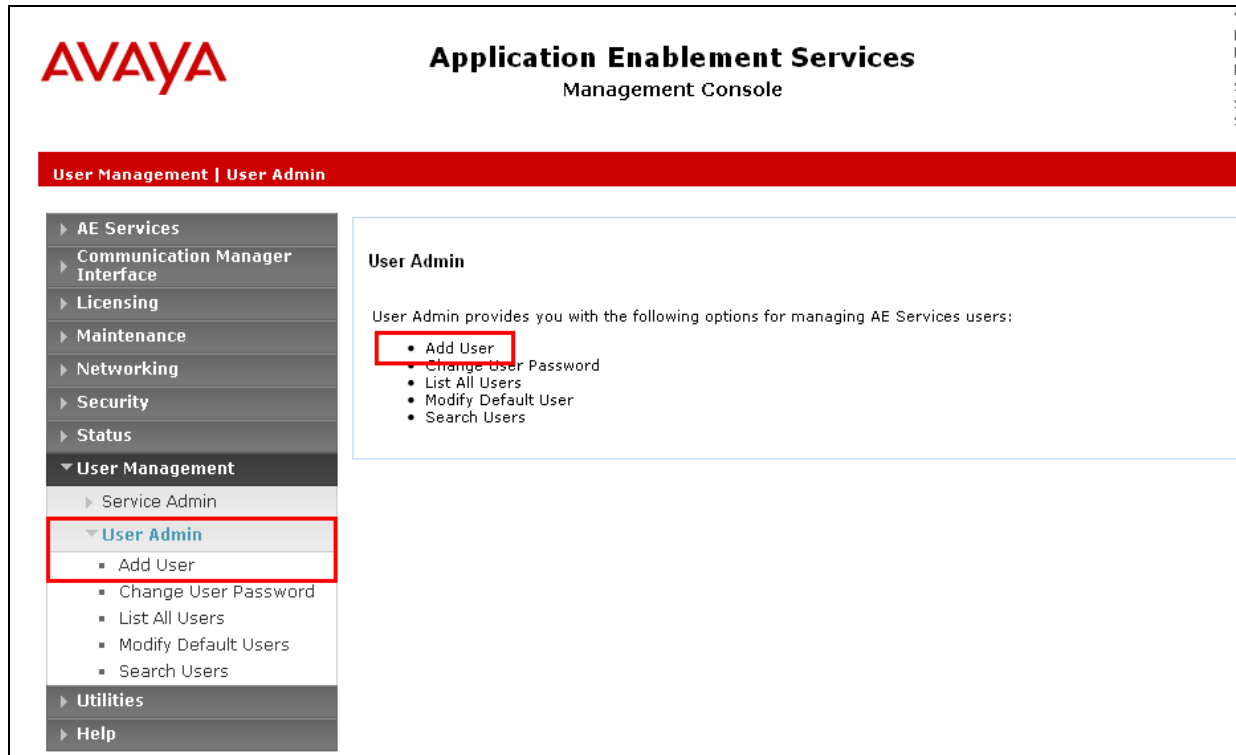
**Service Controller**

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input type="checkbox"/> DMCC Service	Running
<input type="checkbox"/> CVLAN Service	Running
<input type="checkbox"/> DLG Service	Running
<input type="checkbox"/> Transport Layer Service	Running
<input checked="" type="checkbox"/> <b>TSAPI Service</b>	Running

For status on actual services, please use [Status and Control](#)

## 6.4. Create Avaya CTI User

A User ID and password needs to be configured for the ASC server to communicate as a TSAPI client with the Application Enablement Services server. Navigate to the **User Management** → **User Admin** screen then choose the **Add User** option.



In the **Add User** screen shown below, enter the following values:

- **User Id** - This will be used by the ASC Server in **Section 7.4**.
- **Common Name** and **Surname** - Descriptive names need to be entered.
- **User Password** and **Confirm Password** - This will be used with the **User Id** in **Section 7.4**.
- **CT User** - Select **Yes** from the drop-down menu.

Complete the process by choosing **Apply** at the bottom of the screen (not shown).

<ul style="list-style-type: none"><li>▶ Licensing</li><li>▶ Maintenance</li><li>▶ Networking</li><li>▶ Security</li><li>▶ Status</li><li>▼ User Management<ul style="list-style-type: none"><li>▶ Service Admin</li><li>▼ User Admin<ul style="list-style-type: none"><li>▪ Add User</li><li>▪ Change User Password</li><li>▪ <a href="#">List All Users</a></li><li>▪ Modify Default Users</li><li>▪ Search Users</li></ul></li></ul></li><li>▶ Utilities</li><li>▶ Help</li></ul>	* User Id	asc
	* Common Name	asc
	* Surname	asc
	User Password	
	Confirm Password	
	Admin Note	
	Avaya Role	None ▼
	Business Category	
	Car License	
	CM Home	
	Css Home	
	CT User	Yes ▼
	Department Number	
	Display Name	
	Employee Number	
	Employee Type	
	Enterprise Handle	
	Given Name	
Home Phone		
Home Postal Address		
Initials		

The next screen will show a message indicating that the user was created successfully (not shown).

## 6.5. Enable Unrestricted Access for CTI User

Navigate to the **CTI Users** screen by selecting **Security** → **Security Database** → **CTI Users** → **List All Users**. Select the user that was created in **Section 6.4** and select the **Edit** option.

The screenshot shows the Avaya Application Enablement Services Management Console. The left sidebar contains a navigation menu with the following items: AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, Security (expanded), Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, Security Database (expanded), Control, CTI Users (expanded), List All Users (highlighted), Search Users, and Devices. The main content area is titled 'CTI Users' and displays a table with the following data:

User ID	Common Name	Worktop Name
<input checked="" type="radio"/> asc	asc	NONE
<input type="radio"/> presence	presence	NONE

Below the table are two buttons: 'Edit' and 'List All'. The 'Edit' button is highlighted with a red box. In the top right corner, there is a welcome message: 'Welcome: User: [blank]', 'Last login: Tue Feb 18', 'Number of prior failed HostName/IP: AES63V', 'Server Offer Type: VII', 'SW Version: 6.3.0.0.2', and 'Server Date and Time'.

The **Edit CTI User** screen appears. Check the **Unrestricted Access** box and **Apply Changes** at the bottom of the screen.

The screenshot shows the 'Edit CTI User' screen. The left sidebar is the same as in the previous screenshot, with 'List All Users' highlighted. The main content area is titled 'Edit CTI User' and contains the following fields:

- User Profile: User ID (ctiuser), Common Name (ctiuser), Worktop Name (NONE), and Unrestricted Access (checked).
- Call and Device Control: Call Origination/Termination and Device Status (None).
- Call and Device Monitoring: Device Monitoring (None), Calls On A Device Monitoring (None), and Call Monitoring (unchecked).
- Routing Control: Allow Routing on Listed Devices (None).

At the bottom of the screen are two buttons: 'Apply Changes' and 'Cancel Changes'. The 'Apply Changes' button is highlighted with a red box.

A screen (not shown) appears to confirm applied changes to CTI User, choose **Apply**. This CTI user should now be enabled.



## 6.6. Identify Tlinks

Navigate to **Security** → **Security Database** → **Tlinks**. Verify the value of the **Tlink Name**. This will be needed to configure the ASC server in **Section 7.4**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header features the Avaya logo and the title "Application Enablement Services Management Console". Below this is a red navigation bar with the text "Security | Security Database | Tlinks". On the left, a sidebar menu lists various services: AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, Security, Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, Security Database, Control, CTI Users, Devices, Device Groups, and Tlinks. The "Tlinks" item is highlighted with a red box. The main content area is titled "Tlinks" and contains a "Tlink Name" section with two radio button options: "AVAYA#CM63VMPG#CSTA#AES63VMPG" (selected) and "AVAYA#CM63VMPG#CSTA-S#AES63VMPG". A "Delete Tlink" button is also present.

## 6.7. Enable DMCC ports

In order to enable DMCC for call recording navigate to **Networking→Ports→DMCC Server Ports**.

- Enable DMCC **Unencrypted Port**
- Enable DMCC **Encrypted Port**
- Enable DMCC **TR/87 Port**

Click on **Apply Changes** at the bottom of the screen (not shown).

Networking   Ports			
<b>Ports</b>			
CVLAN Ports			Enabled Disabled
	Unencrypted TCP Port	9999	<input checked="" type="radio"/> <input type="radio"/>
	Encrypted TCP Port	<input type="text" value="9998"/>	<input checked="" type="radio"/> <input type="radio"/>
DLG Port		TCP Port	5678
TSAPI Ports			Enabled Disabled
	TSAPI Service Port	450	<input checked="" type="radio"/> <input type="radio"/>
	Local TLINK Ports		
	TCP Port Min	1024	
	TCP Port Max	1039	
	Unencrypted TLINK Ports		
	TCP Port Min	<input type="text" value="1050"/>	
	TCP Port Max	<input type="text" value="1065"/>	
	Encrypted TLINK Ports		
	TCP Port Min	<input type="text" value="1066"/>	
	TCP Port Max	<input type="text" value="1081"/>	
DMCC Server Ports			Enabled Disabled
	Unencrypted Port	<input type="text" value="4721"/>	<input checked="" type="radio"/> <input type="radio"/>
	Encrypted Port	<input type="text" value="4722"/>	<input checked="" type="radio"/> <input type="radio"/>
	TR/87 Port	<input type="text" value="4723"/>	<input checked="" type="radio"/> <input type="radio"/>

Once this change is made a restart of the AE Server is required. Navigate to **Maintenance** → **Service Controller**. In the main screen select **Restart AE Server** highlighted.

**AVAYA** **Application Enablement Services**  
Management Console

**Maintenance | Service Controller**

Left Sidebar:

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ Licensing
- ▼ **Maintenance**
- ▶ Date Time/NTP Server
- ▶ Security Database
- Service Controller**
- ▶ Server Data
- ▶ Networking
- ▶ Security
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

**Service Controller**

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input type="checkbox"/> DMCC Service	Running
<input type="checkbox"/> CVLAN Service	Running
<input type="checkbox"/> DLG Service	Running
<input type="checkbox"/> Transport Layer Service	Running
<input type="checkbox"/> TSAPI Service	Running

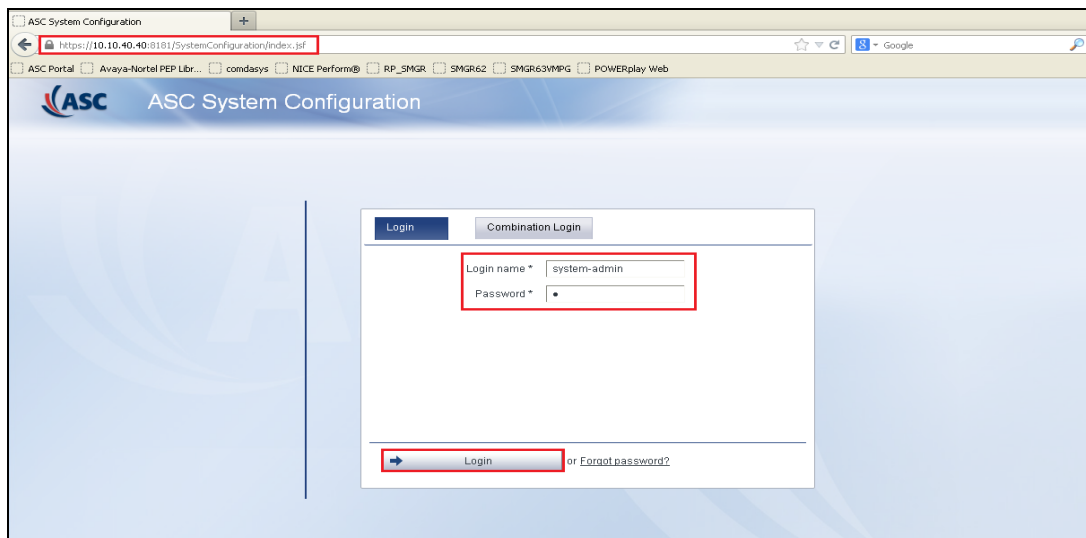
For status on actual services, please use [Status and Control](#)

Buttons: Start Stop Restart Service **Restart AE Server** Restart Linux Restart Web Server

## 7. Configure ASC telecom ASC EVOIPneo active

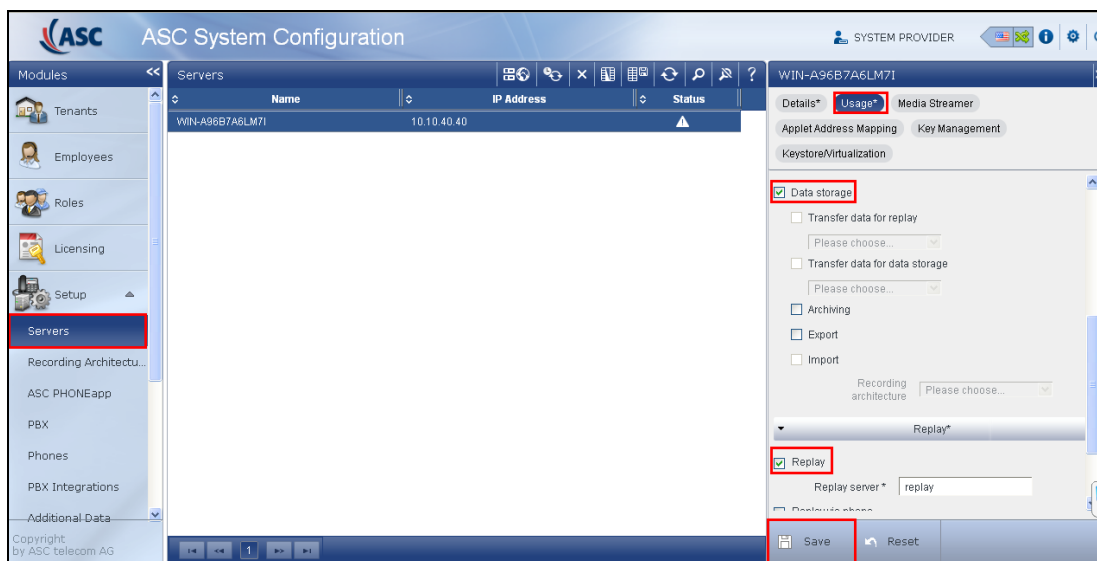
The configuration of the ASC server is achieved by opening a web session connecting to that servers IP address. Mozilla Firefox is the supported web browser.

Using Mozilla Firefox open a web session to **https://<ServerIP>:8181/SystemConfiguration/**. Enter the proper username and password and click on **Login**.



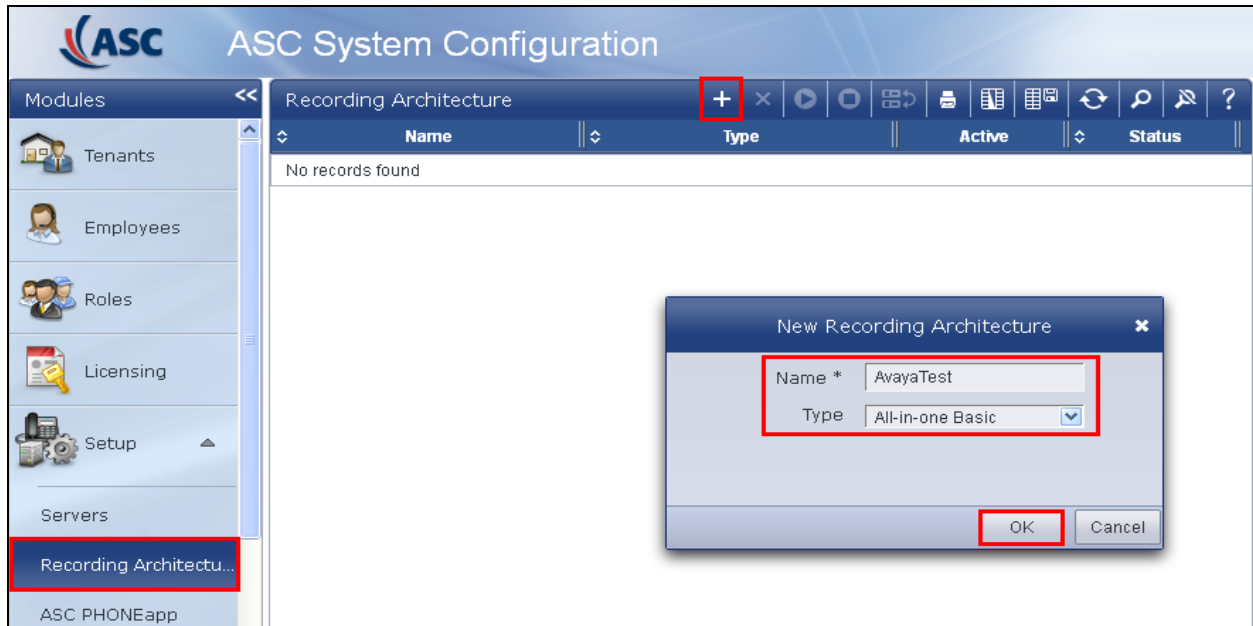
### 7.1. Configure Server

Navigate to **Setup → Servers** in the left window and click on the **Usage** tab in the right window. Ensure that **Data Storage** and **Replay** boxes are ticked and click on **Save** at the bottom of the screen.

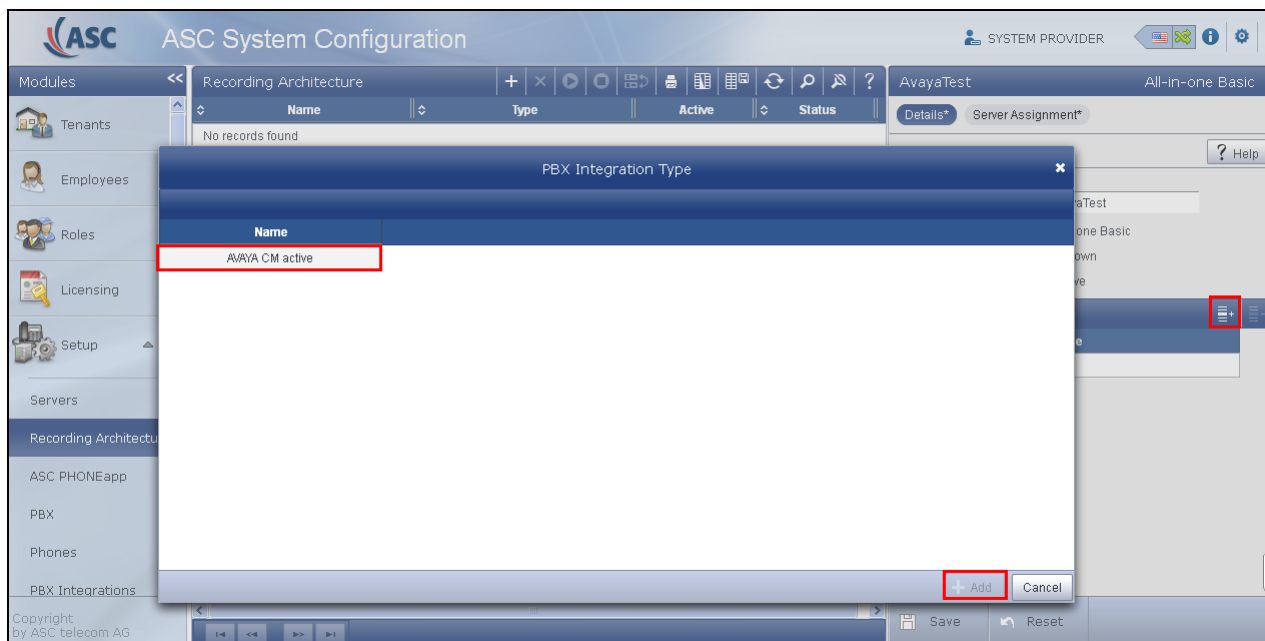


## 7.2. Configure Recording Architecture

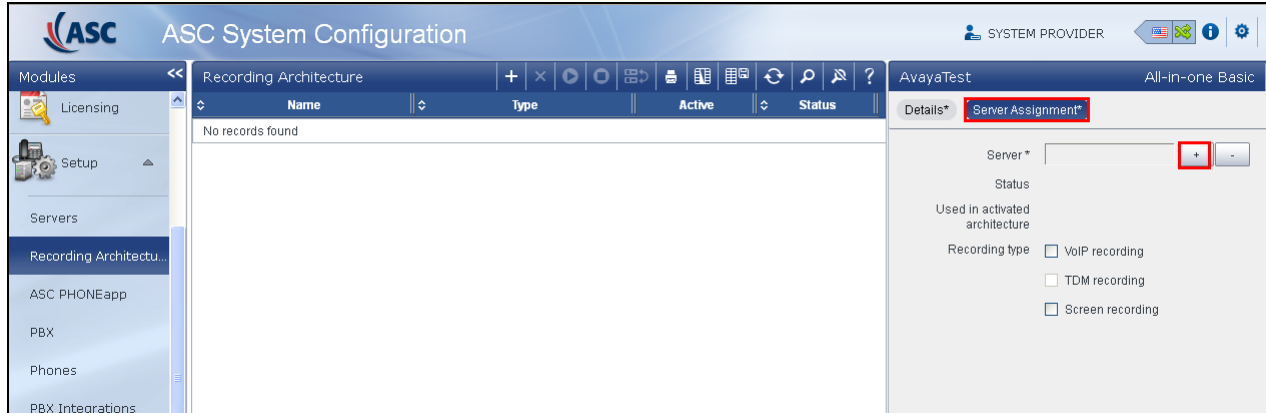
Navigate to **Setup** → **Recording Architecture** in the left window and click on the + icon to add a **New Recording Architecture**. Enter a suitable **Name** and select **All-in-one-Basic** as shown below, click on **OK** once complete.



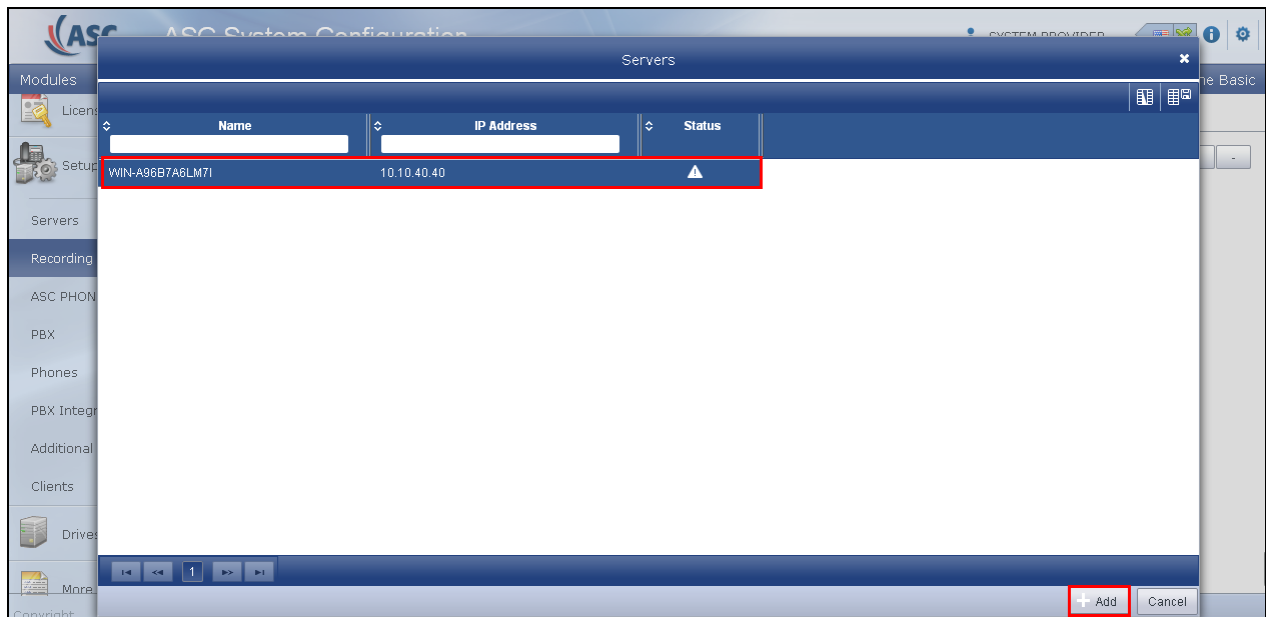
Click on the **Add** icon highlighted on the right side of the screen below. A screen is opened showing the **PBX Integration Type** that is present, license depending, select this and click on **Add** at the bottom of this screen.



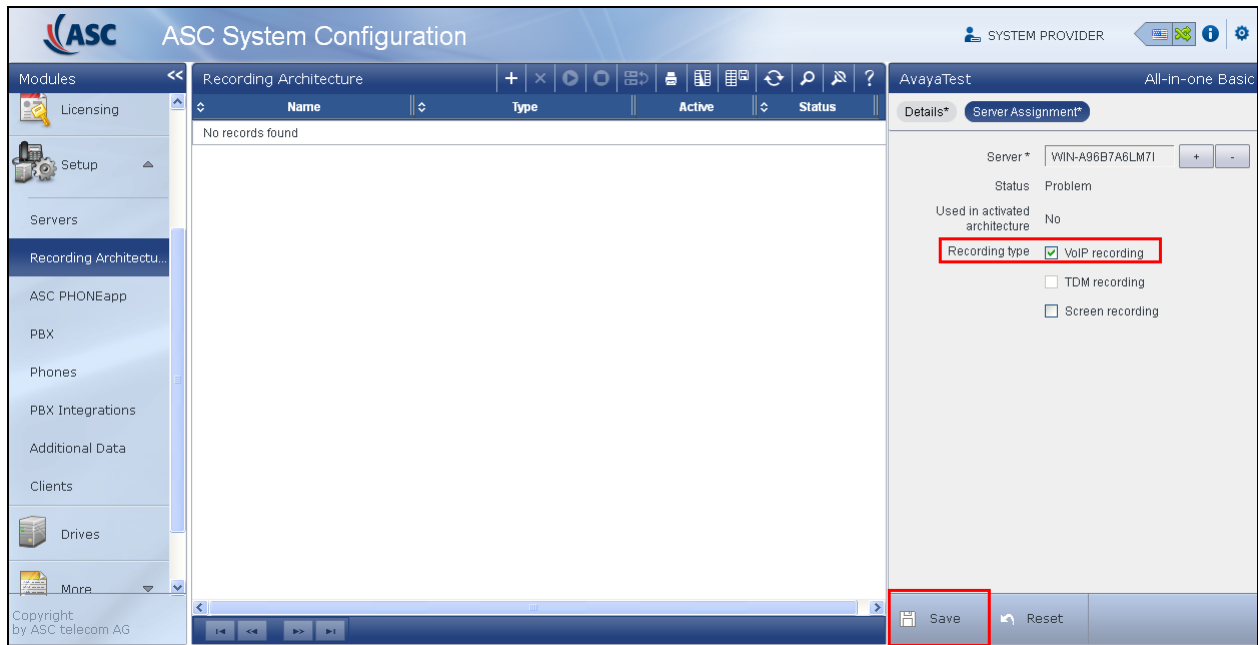
Click on the **Server Assignment** tab highlighted and click on the + icon to add a server.



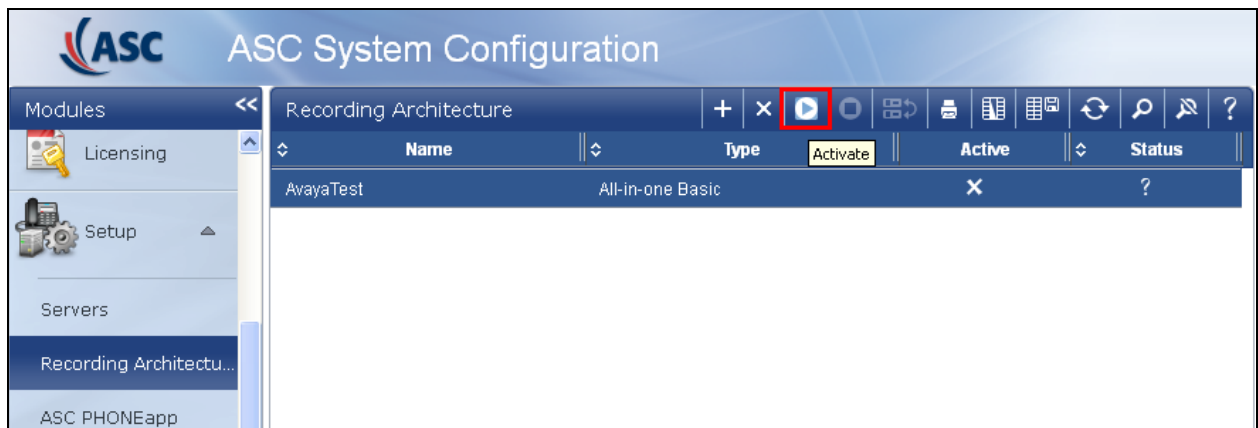
Select the server (added during the installation) and click on **Add** at the bottom of the screen.



Ensure that **VoIP recording** is ticked as shown and click on **Save** at the bottom of the screen.

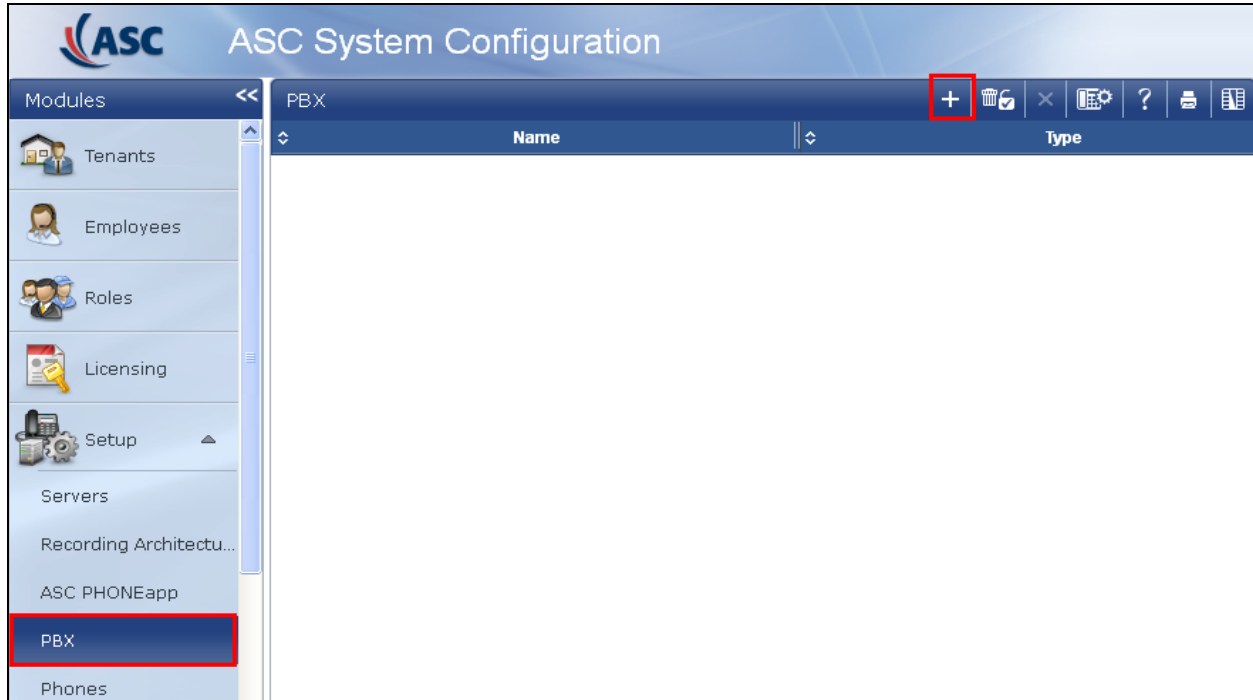


Once this Recording Architecture is added it must be activated by clicking on the **Activate** icon highlighted below.

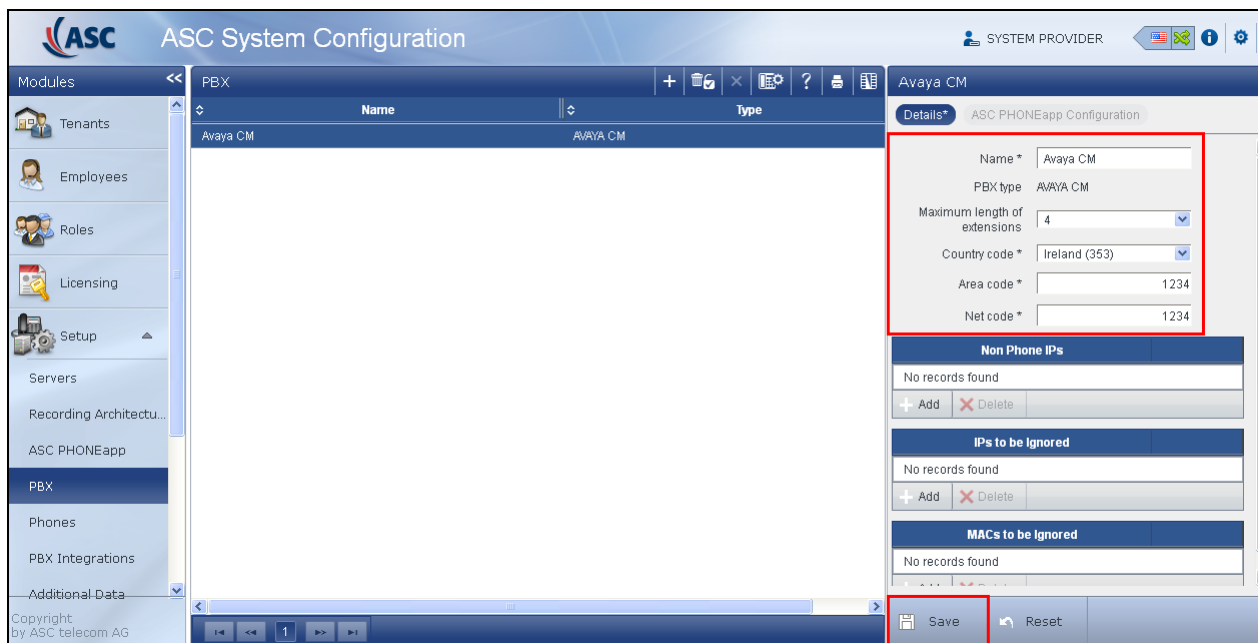


### 7.3. Add PBX

Navigate to **Setup** → **PBX** in the left window and click on the + icon at the top of the main window to add or create a new PBX.



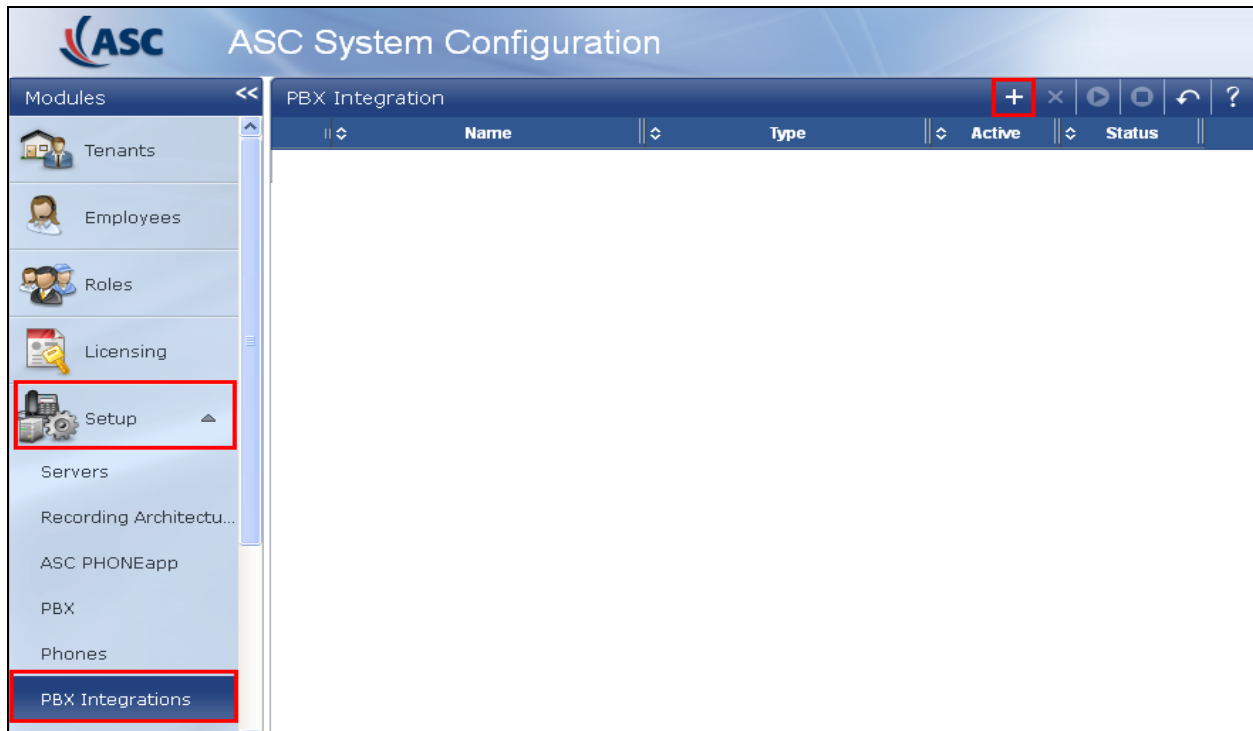
Enter the telephony details as shown in the right window and click on **Save** at the bottom of the screen.



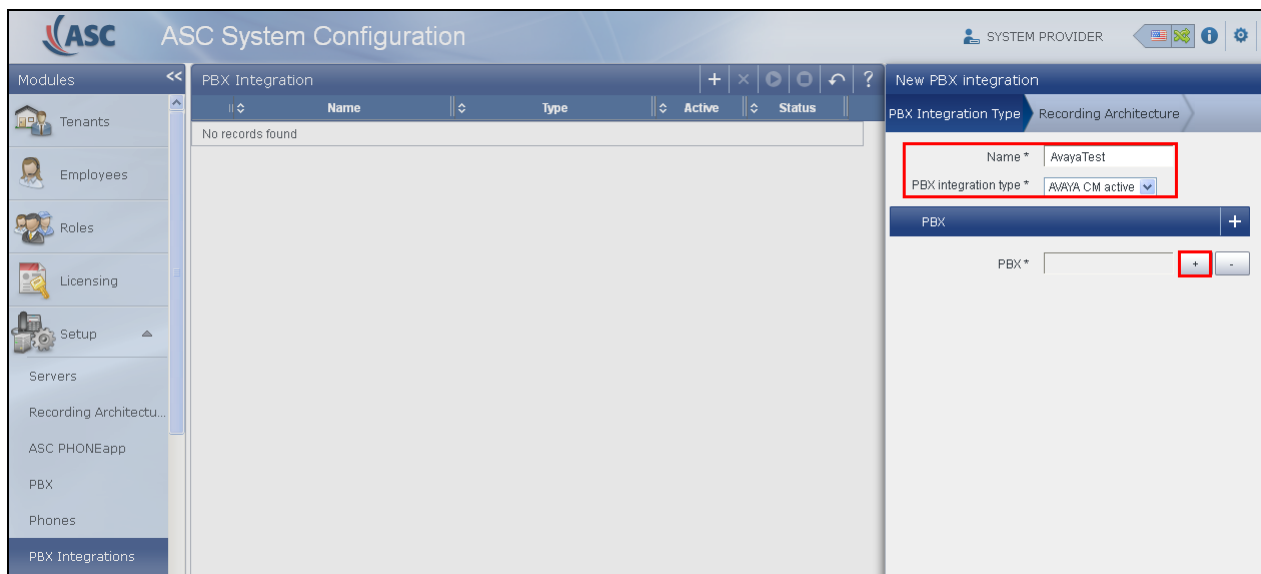


## 7.4. PBX Integrations

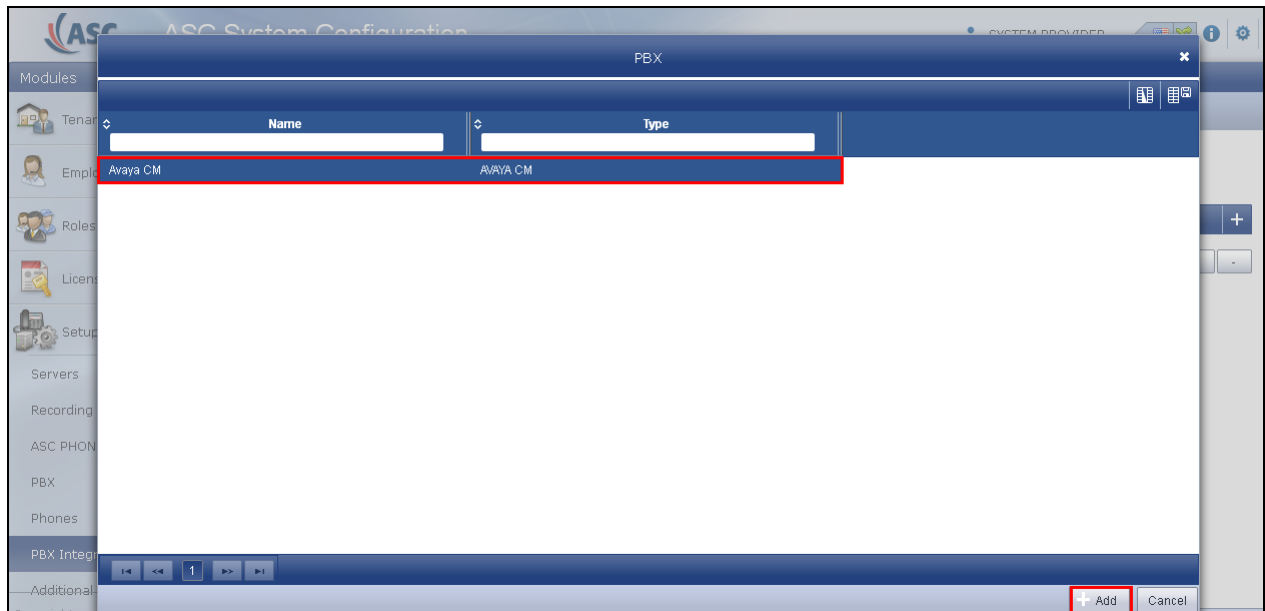
Navigate to **Setup** → **PBX Integrations** in the left window and click on the + icon at the top of the main window to add or create a new PBX Integration.



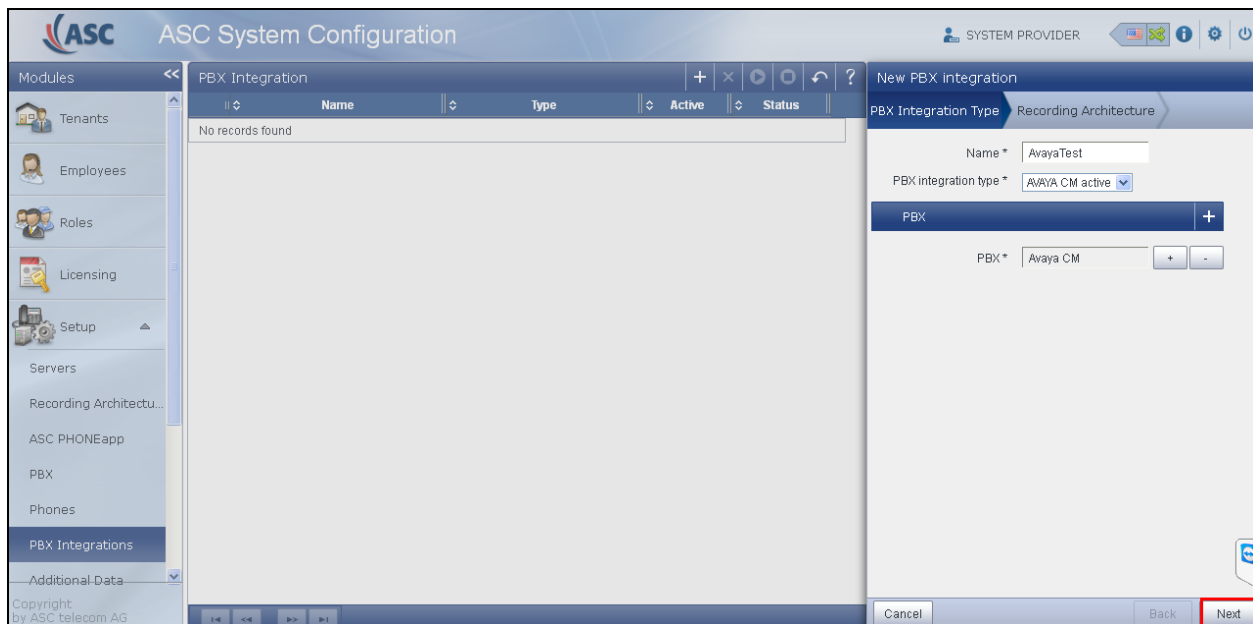
In the right window enter a suitable **Name** and select the **AVAYA CM active** as the **PBX Integration type**. Click on the Add Icon + next to **PBX** as shown below.



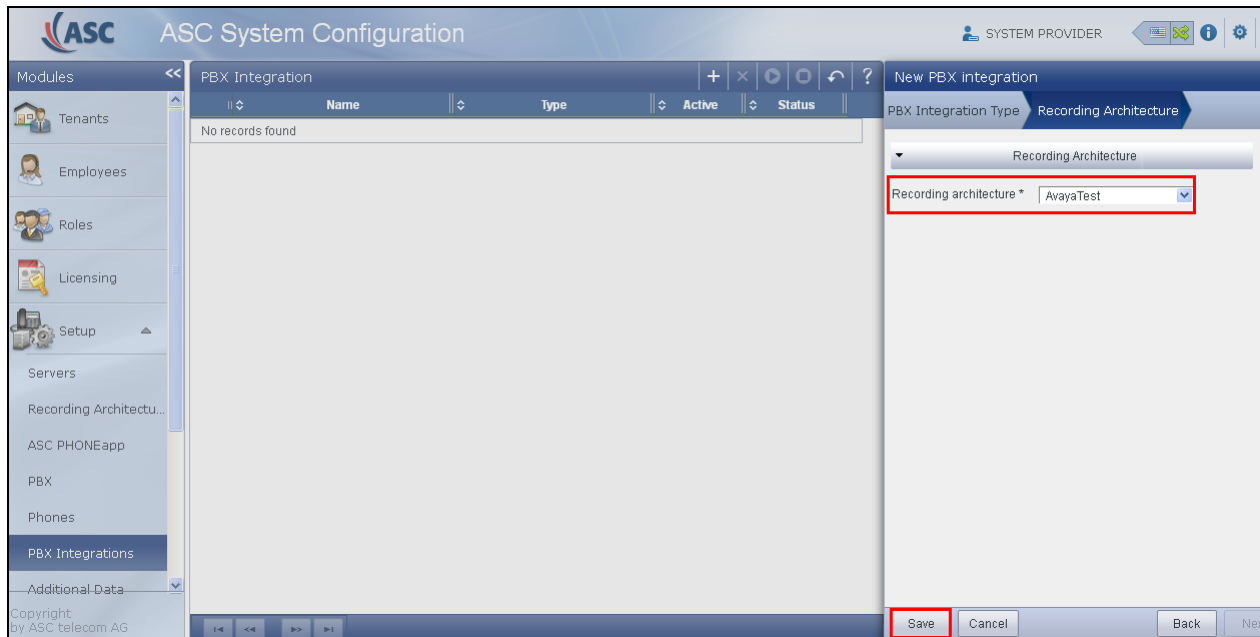
Select the PBX, this was created in **Section 7.3**, click on **Add** at the bottom of the screen.



Click on Next at the bottom right of the screen to continue.

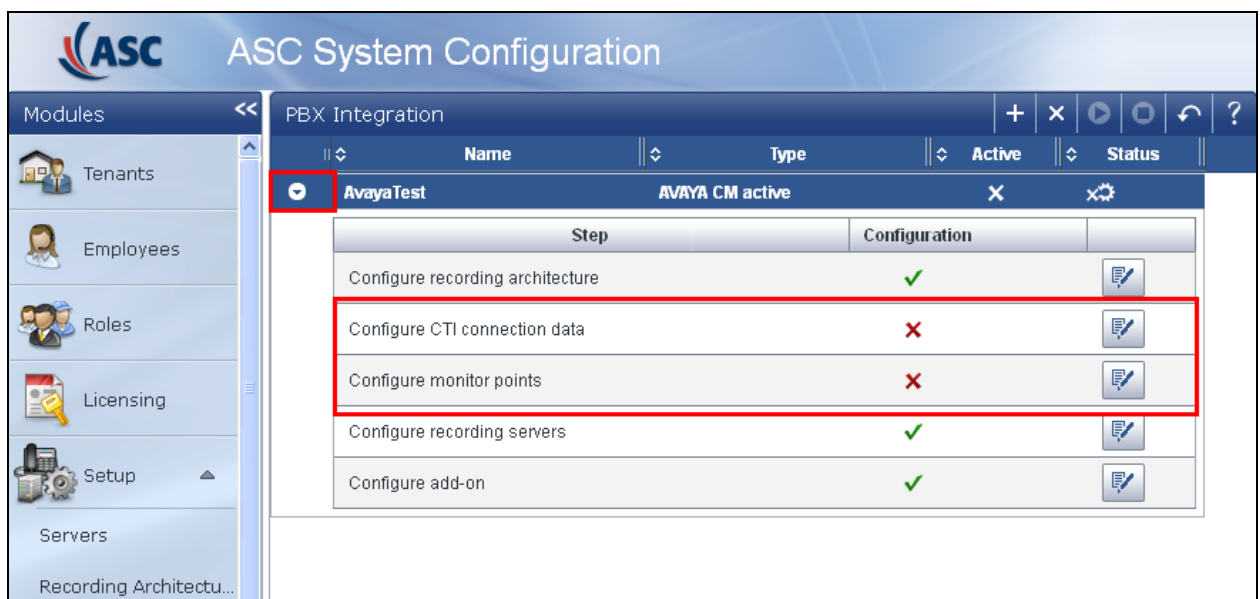


Select the Recording architecture, created in **Section 7.2**, and click on **Save**.



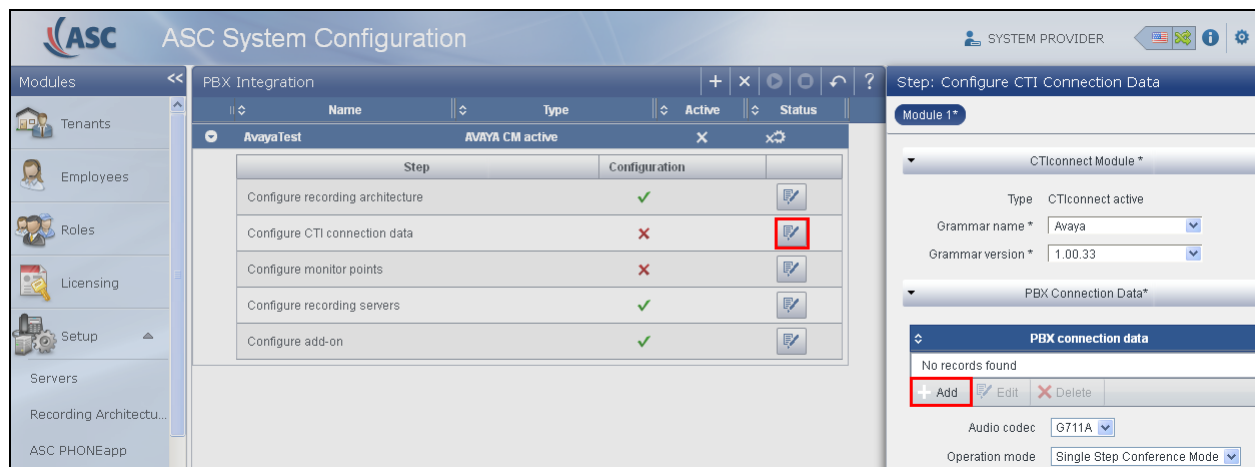
Once saved click on the Maximize icon . There are two steps left to configure before the system is ready.

1. **Configure CTI connection data.**
2. **Configure monitor points.**

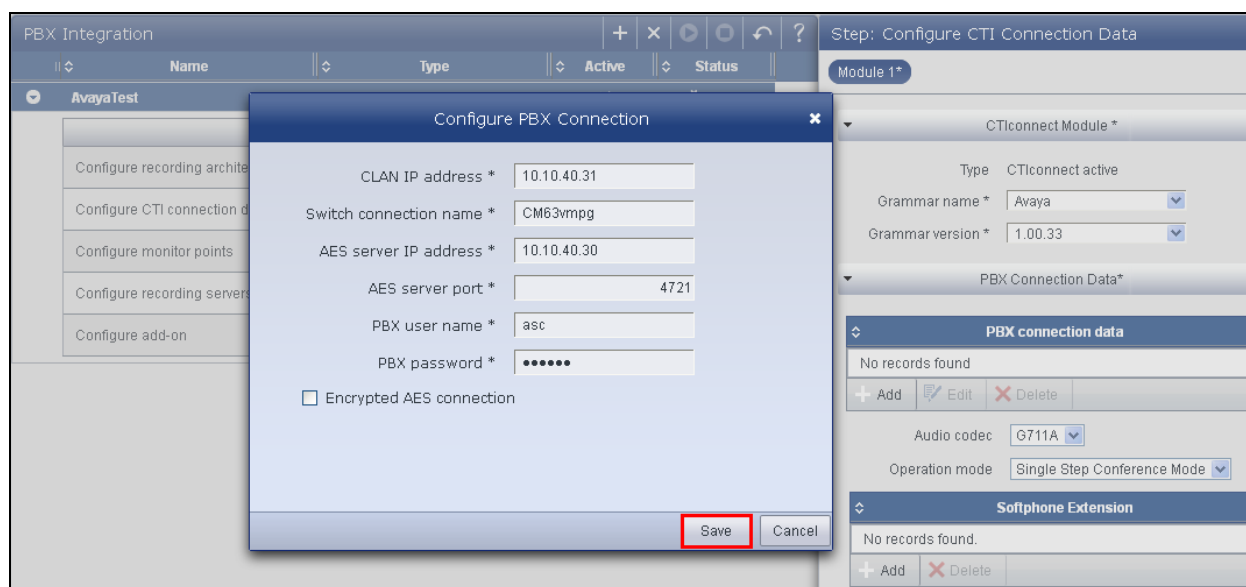


### 7.4.1. Configure CTI connection data

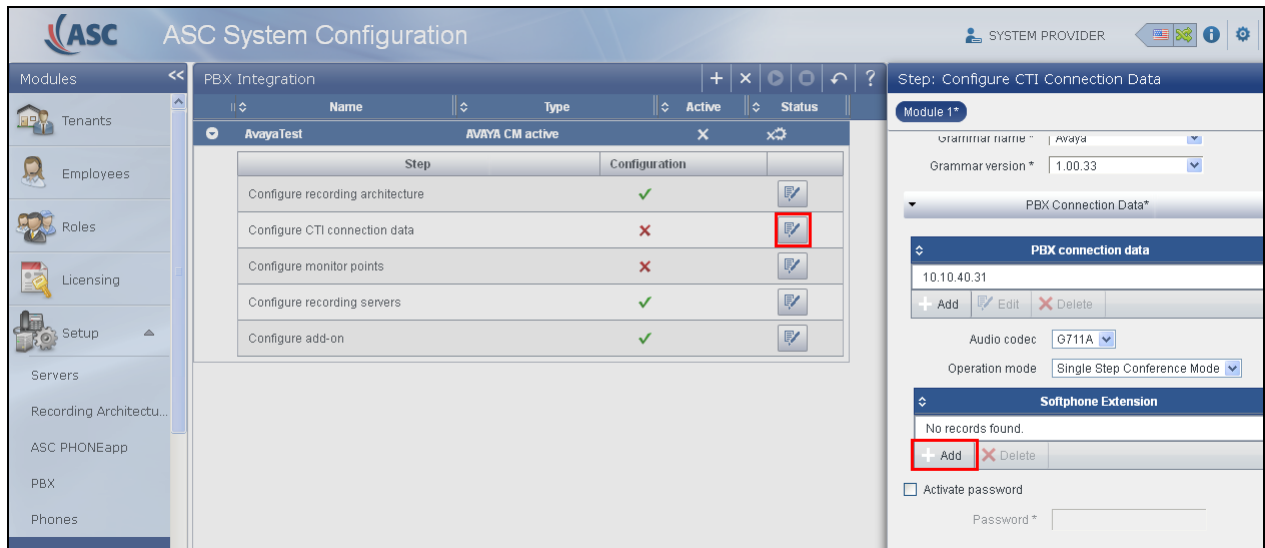
Click on the edit icon next to **Configure CTI connection data**. Click on **+Add** under **PBX connection data** in the right window.



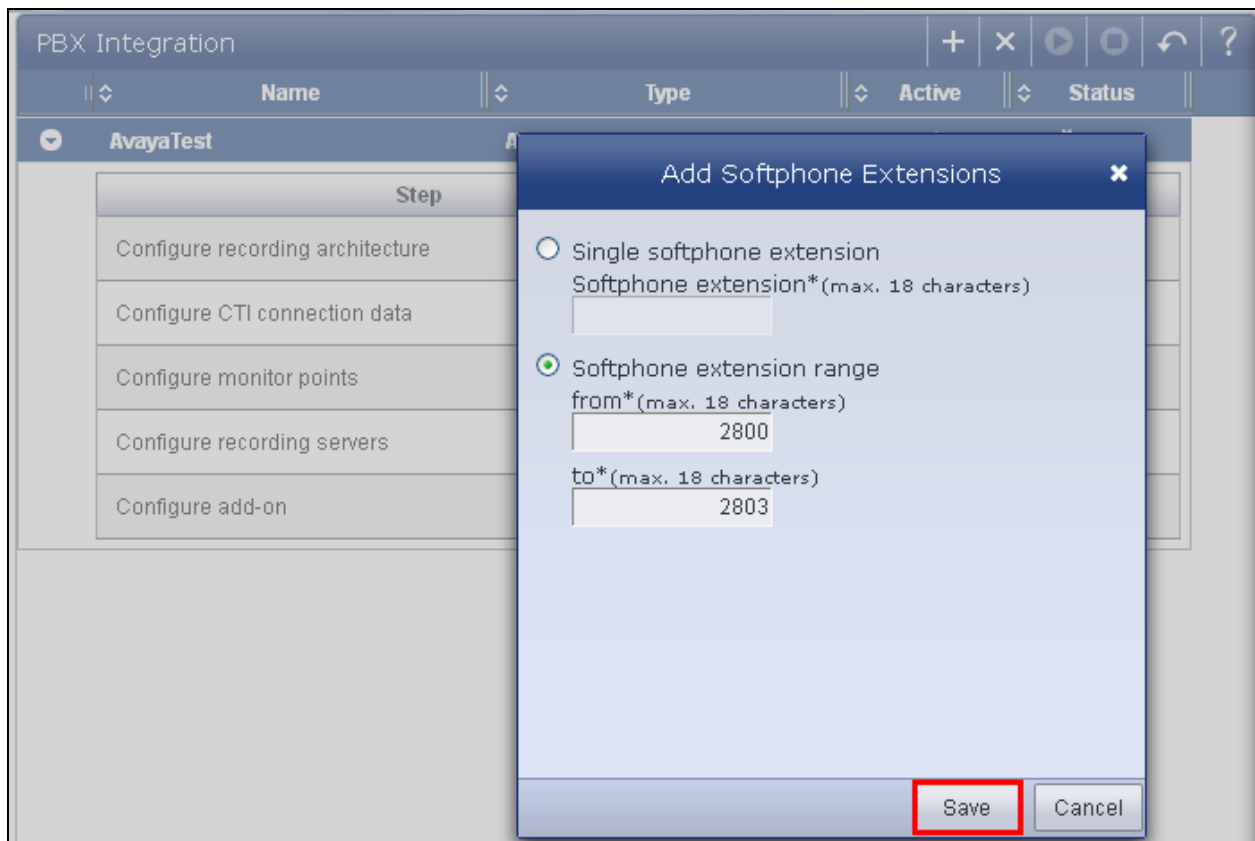
Enter the Communication Manager and AES information. This information can be obtained from **Sections 5&6**. Click on **Save** once complete. Note in the screen shot below the **CLAN IP address** will be that of the **procr** address displayed in **Section 5.2**.



On the same screen, in the right window, select **+Add** under **Softphone Extension**.



Enter the virtual extension numbers created in **Section 5.5**.



Click on **Activate password** and enter the password for the virtual stations created in **Section 5.5**. Click on **Save** at the bottom of the screen once complete.

ASC System Configuration

SYSTEM PROVIDER

Modules: PBX Integration

Name	Type	Active	Status
AvayaTest	AVAYA CM active		
Step Configuration			
Configure recording architecture		✓	
Configure CTI connection data		✗	
Configure monitor points		✗	
Configure recording servers		✓	
Configure add-on		✓	

Step: Configure CTI Connection Data

Module 1\*

PBX connection data

10.10.40.31

+ Add Edit Delete

Audio codec: G711A

Operation mode: Single Step Conference Mode

Softphone Extension

2800

2801

2802

2803

+ Add Delete

☒ Activate password

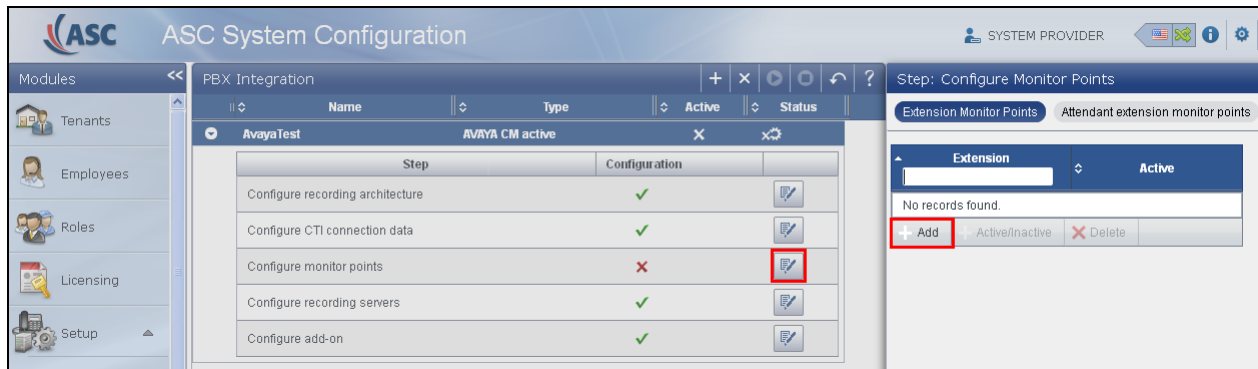
Password \* .....

Additional Data

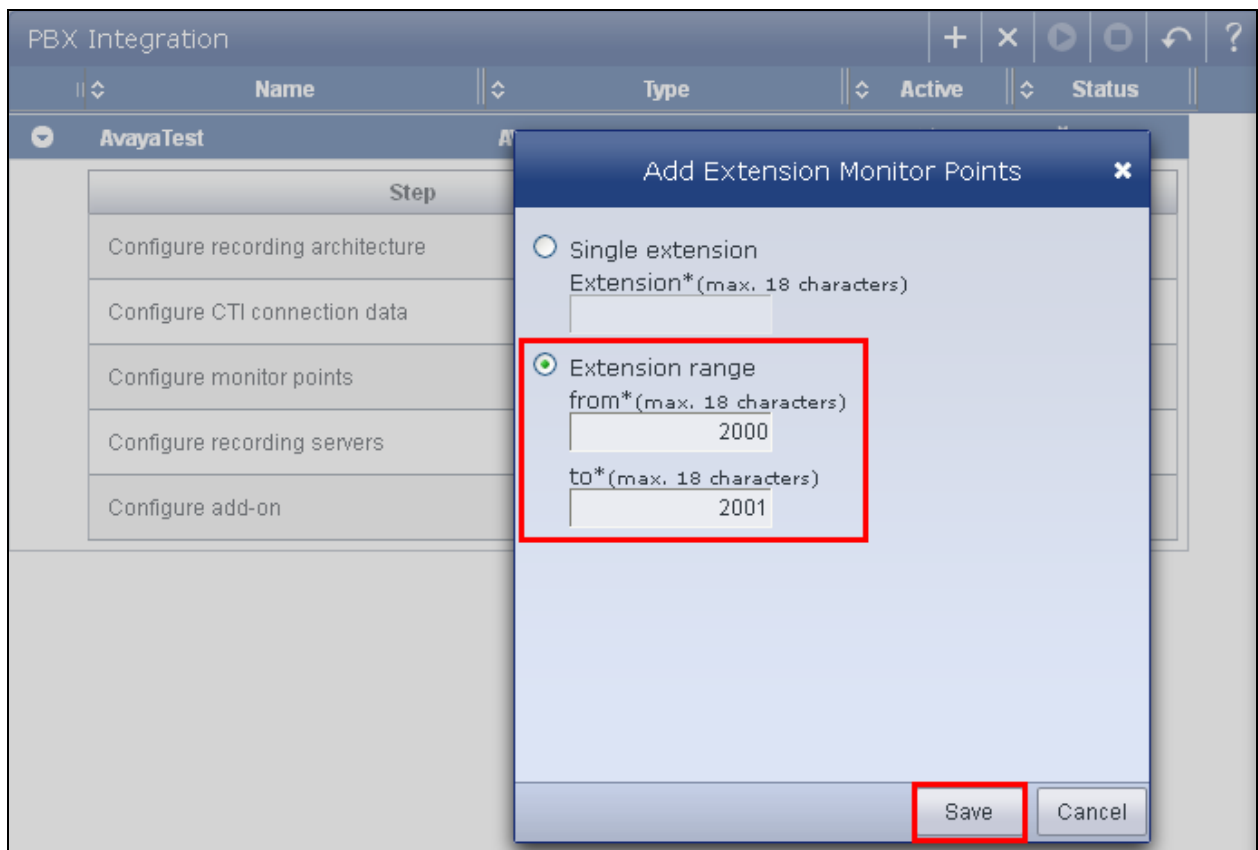
Save Cancel

## 7.4.2. Configure monitor points

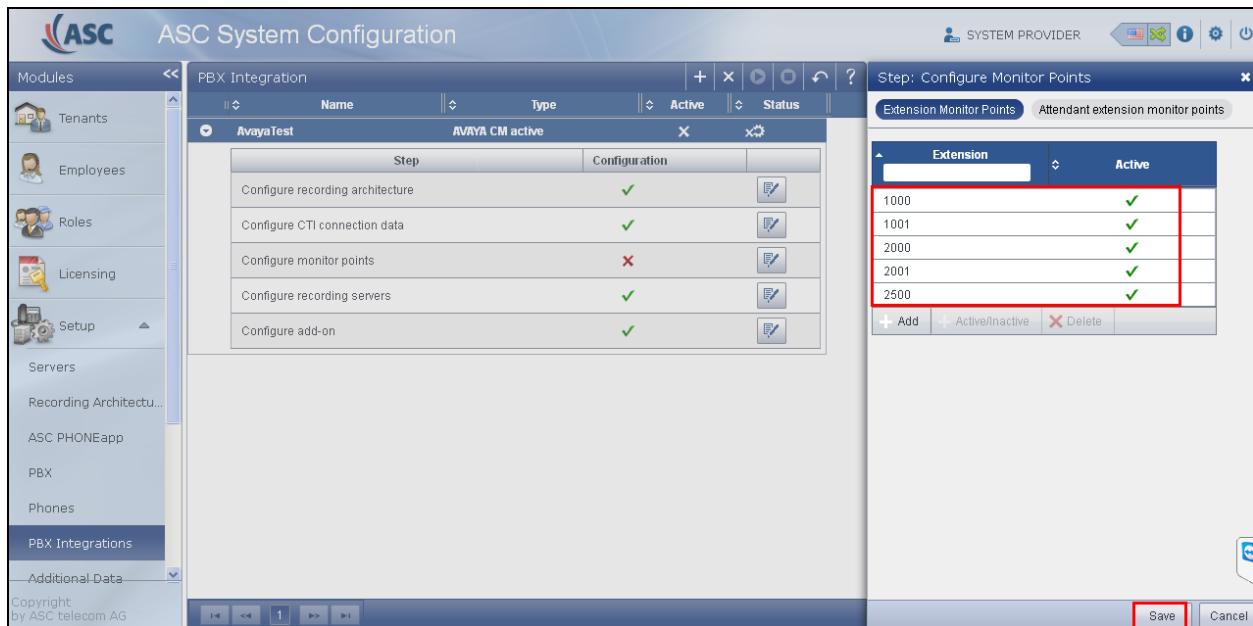
Click on the edit icon next to **Configure Monitor points**. Click on **+Add** in the right window.




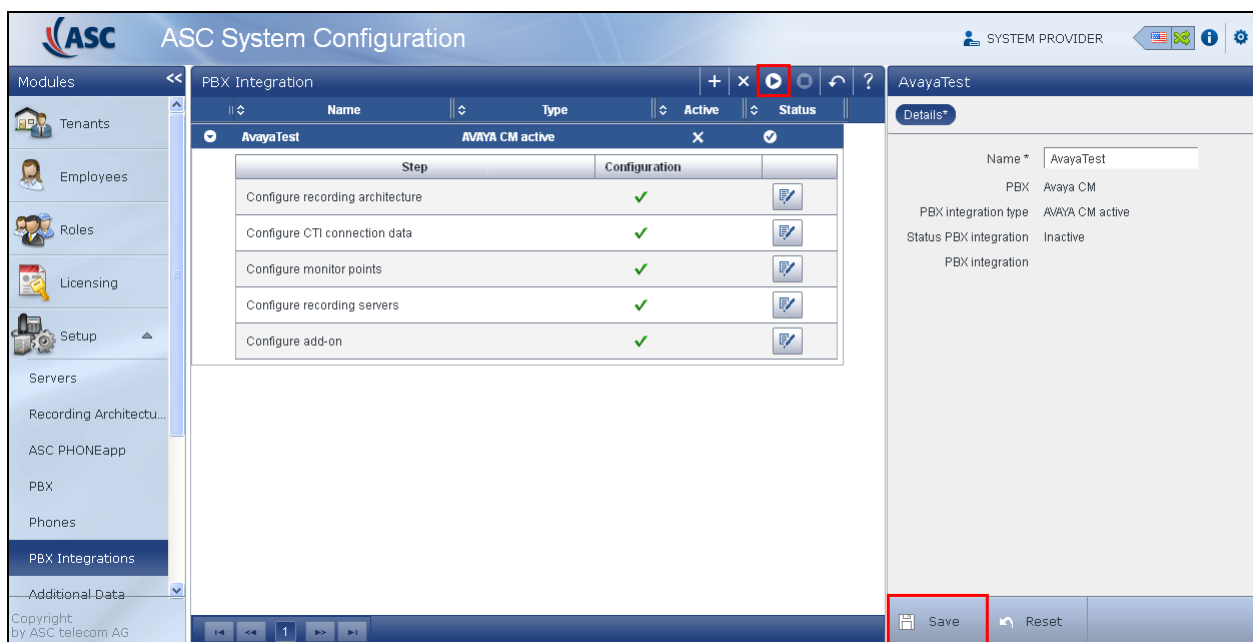
Enter the extensions to be monitored or recorded and click on **Save** once complete.



The extensions that will be recorded show in the right window. Once complete click on **Save** at the bottom of the screen.



Click on **Save** at the bottom of the screen and this completes the setup for the PBX Integration. This new PBX Integration now needs to be activated by pressing on the Activate icon  highlighted in the screen below. This will enable recording to begin.





## 8. Verification Steps

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

### 8.1. Verify Avaya Aura® Communication Manager CTI Service State

The following steps can validate that the communication between Communication Manager and AES is functioning correctly. Check the AESVCS link status with AES by using the command **status aesvcs cti-link**. Verify the **Service State** of the CTI link is **established**.

status aesvcs cti-link						
AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	4	no	aes63vmpg	established	18	18

### 8.2. Verify TSAPI Link and DMCC

#### 8.2.1. Verify TSAPI Link

On the AES Management Console verify the status of the TSAPI link by selecting **Status** → **Status and Control** → **TSAPI Service Summary** to display the **TSAPI Link Details** screen. Verify the status of the TSAPI link by checking that the **Status** is **Talking** and the **State** is **Online**.

**AVAYA**

**Application Enablement Services**  
Management Console

Welcome: User craft  
Last login: Thu Feb 20 11:01:32 2014 from 192.168.10.222  
Number of prior failed login attempts: 33  
HostName/IP: AES63VMPG  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 6.3.0.0.212-0  
Server Date and Time: Thu Feb 20 11:14:02 UTC 2014

Status | Status and Control | TSAPI Service Summary

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

Log Manager

▶ Logs

▼ Status and Control

■ CVLAN Service Summary

■ DLG Services Summary

■ DMCC Service Summary

■ Switch Conn Summary

■ TSAPI Service Summary

TSAPI Link Details

☐ Enable page refresh every 60 seconds

Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
1	CM63vmpg	1	Talking	Tue Feb 18 11:21:49 2014	Online	16	5	15	15	30

For service-wide information, choose one of the following:

### 8.2.2. Verify Avaya Aura® Application Enablement Services DMCC Service

The following steps are carried out on AES to validate that the communication link between AES and the ASC server is functioning correctly. Verify the status of the DMCC service by selecting **Status → Status and Control → DMCC Service Summary**. The **DMCC Service Summary – Session Summary** screen is displayed as shown below. It shows a connection to the ASC server, IP address **10.10.40.40**. The **Application** is shown as **cmapiApplication**, and the **Far-end Identifier** is given as the IP address **10.10.40.40** as expected. The **User** is shown as the user created for the CTI user for ASC Server, in this case **asc**.

**AVAYA**

**Application Enablement Services**  
Management Console

Welcome: User craft  
Last login: Tue Feb 18 12:51:12 2014 from 10.10.40.222  
Number of prior failed login attempts: 31  
HostName/IP: AES63VMPG  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 6.3.0.0.212-0  
Server Date and Time: Thu Feb 20 11:02:19 UTC 2014

Status | Status and Control | DMCC Service SummaryHome | Help | Logout

AE Services

Communication Manager Interface

Licensing

Maintenance

Networking

Security

Status

Alarm Viewer

Log Manager

Logs

Status and Control

CVLAN Service Summary

DLG Services Summary

DMCC Service Summary

Switch Conn Summary

TSAPI Service Summary

DMCC Service Summary - Session Summary

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)  
Generated on Thu Feb 20 11:02:04 UTC 2014  
Service Uptime: 1 days, 23 hours 38 minutes  
Number of Active Sessions: 1  
Number of Sessions Created Since Service Boot: 3  
Number of Existing Devices: 4  
Number of Devices Created Since Service Boot: 8

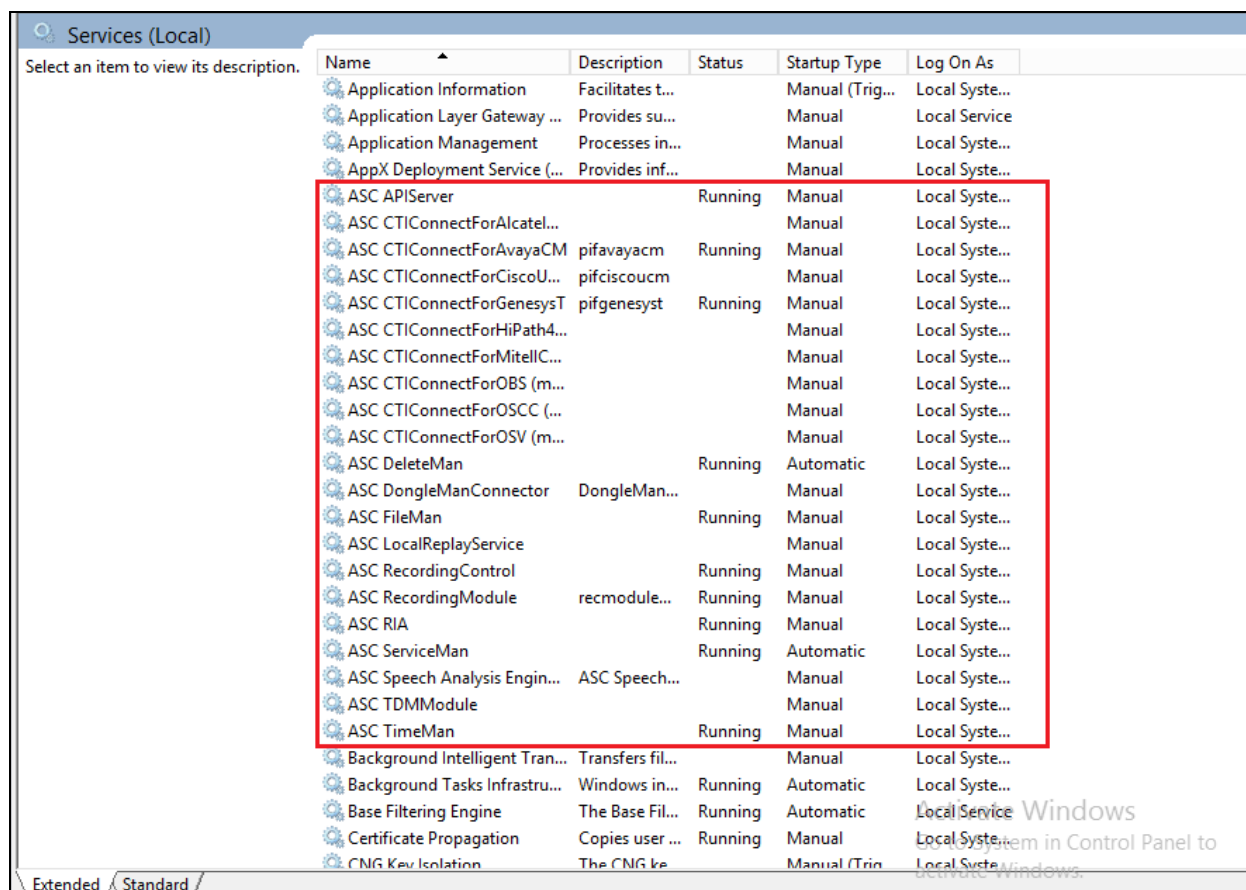
	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	480296D71BABBBD11 560CC61BE9C0470-2	asc	cmapiApplication	10.10.40.40	XML Unencrypted	4

[Terminate Sessions](#) [Show Terminated Sessions](#)

Item 1-1 of 1

### 8.3. Verify ASC EVOIPneo active for Avaya Aura (with CM & AES) services are running

Open services.exe and ensure that the correct ASC services are running. Below is a list of services that were running during the compliance testing.

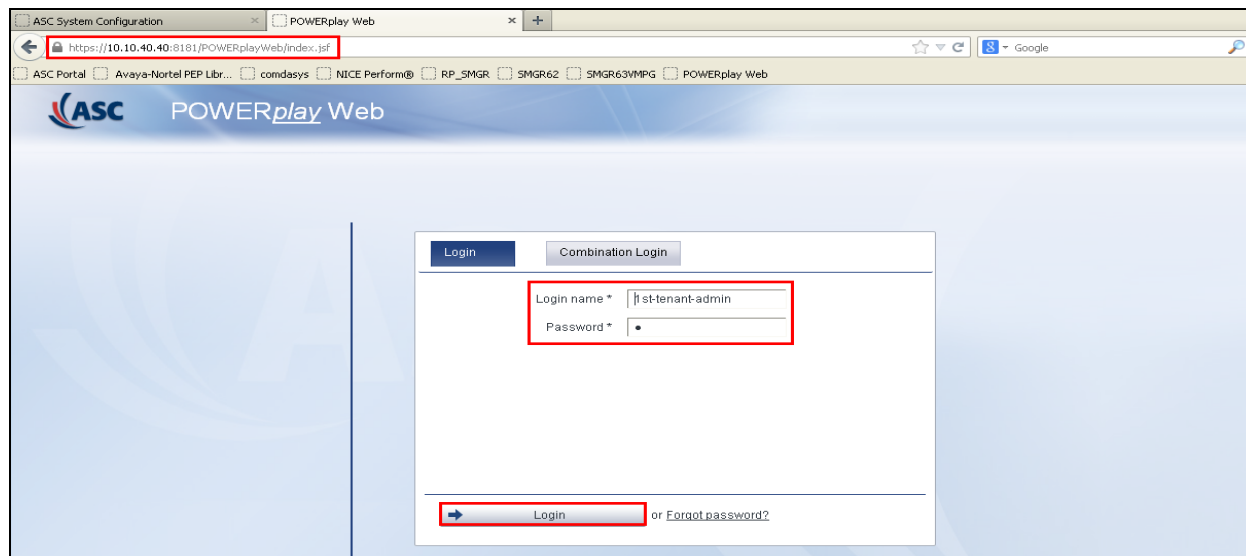


Name	Description	Status	Startup Type	Log On As
Application Information	Facilitates t...		Manual (Trig...	Local Syste...
Application Layer Gateway ...	Provides su...		Manual	Local Service
Application Management	Processes in...		Manual	Local Syste...
AppX Deployment Service (...)	Provides inf...		Manual	Local Syste...
ASC API Server		Running	Manual	Local Syste...
ASC CTIConnectForAlcatel...			Manual	Local Syste...
ASC CTIConnectForAvayaCM...	pifavayacm	Running	Manual	Local Syste...
ASC CTIConnectForCiscoU...	pifciscouc...		Manual	Local Syste...
ASC CTIConnectForGenesysT...	pifgenesys...	Running	Manual	Local Syste...
ASC CTIConnectForHiPath4...			Manual	Local Syste...
ASC CTIConnectForMitellC...			Manual	Local Syste...
ASC CTIConnectForOBS (m...			Manual	Local Syste...
ASC CTIConnectForOSCC (...)			Manual	Local Syste...
ASC CTIConnectForOSV (m...			Manual	Local Syste...
ASC DeleteMan		Running	Automatic	Local Syste...
ASC DongleManConnector	DongleMan...		Manual	Local Syste...
ASC FileMan		Running	Manual	Local Syste...
ASC LocalReplayService			Manual	Local Syste...
ASC RecordingControl		Running	Manual	Local Syste...
ASC RecordingModule	recmodule...	Running	Manual	Local Syste...
ASC RIA		Running	Manual	Local Syste...
ASC ServiceMan		Running	Automatic	Local Syste...
ASC Speech Analysis Engin...	ASC Speech...		Manual	Local Syste...
ASC TDMMModule			Manual	Local Syste...
ASC TimeMan		Running	Manual	Local Syste...
Background Intelligent Tran...	Transfers fil...		Manual	Local Syste...
Background Tasks Infrastru...	Windows in...	Running	Automatic	Local Syste...
Base Filtering Engine	The Base Fil...	Running	Automatic	Local Service
Certificate Propagation	Copies user ...	Running	Manual	Local Syste...
CNG Key Isolation	The CNG ke		Manual (Trin	Local Syste...

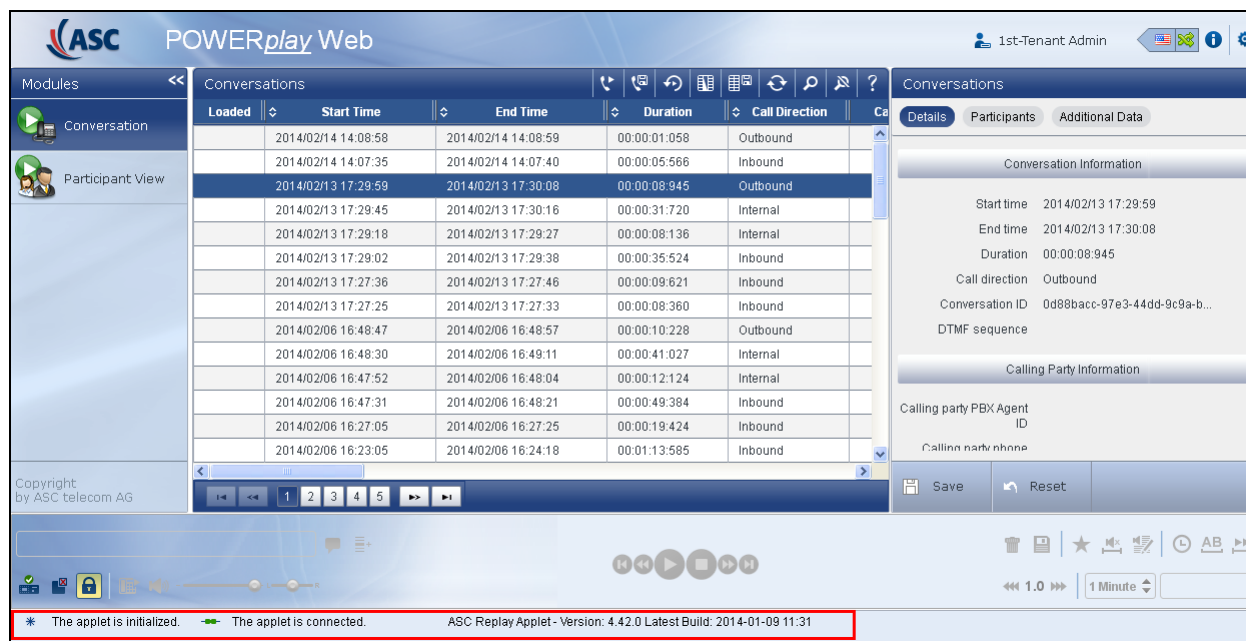
## 8.4. Verify ASC EVOIPneo active for Avaya Aura (with CM & AES) Capture and Playback


The playback of ASC recordings is achieved by opening a web session connecting to that servers IP address. Mozilla Firefox is the supported web browser.

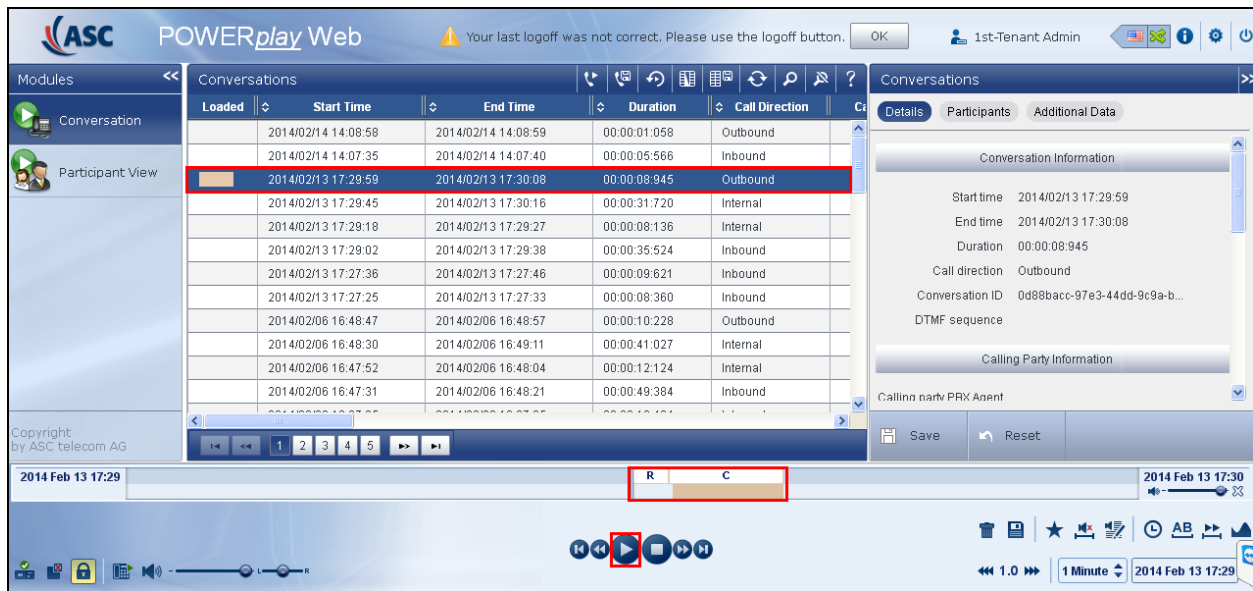
Using Mozilla Firefox open a web session to <https://<ServerIP>:8181/PowerPlayWeb/>. Enter the proper username and password and click on Login.



The following screen appears and the Java applet loads automatically. There may be a message asking to activate this on the first instance, if so click on Yes to continue (not shown).



Double-Click on the recording to be played and click on the Play icon  at the bottom of the screen to play back the recording.



The screenshot displays the ASC POWERplay Web interface. The main window shows a list of conversations with columns for Loaded, Start Time, End Time, Duration, and Call Direction. A red box highlights a specific conversation row. To the right, a detailed view of the selected conversation is shown, including Conversation Information (Start time, End time, Duration, Call direction, Conversation ID, DTMF sequence) and Calling Party Information. At the bottom, there is a playback control bar with a play button highlighted by a red box.

Loaded	Start Time	End Time	Duration	Call Direction
	2014/02/14 14:08:58	2014/02/14 14:08:59	00:00:01:058	Outbound
	2014/02/14 14:07:35	2014/02/14 14:07:40	00:00:05:566	Inbound
	2014/02/13 17:29:59	2014/02/13 17:30:08	00:00:08:945	Outbound
	2014/02/13 17:29:45	2014/02/13 17:30:16	00:00:31:720	Internal
	2014/02/13 17:29:18	2014/02/13 17:29:27	00:00:08:136	Internal
	2014/02/13 17:29:02	2014/02/13 17:29:38	00:00:35:524	Inbound
	2014/02/13 17:27:36	2014/02/13 17:27:46	00:00:09:621	Inbound
	2014/02/13 17:27:25	2014/02/13 17:27:33	00:00:08:360	Inbound
	2014/02/06 16:48:47	2014/02/06 16:48:57	00:00:10:228	Outbound
	2014/02/06 16:48:30	2014/02/06 16:49:11	00:00:41:027	Internal
	2014/02/06 16:47:52	2014/02/06 16:48:04	00:00:12:124	Internal
	2014/02/06 16:47:31	2014/02/06 16:48:21	00:00:49:384	Inbound

Conversation Information:

- Start time: 2014/02/13 17:29:59
- End time: 2014/02/13 17:30:08
- Duration: 00:00:08:945
- Call direction: Outbound
- Conversation ID: 0d88bacc-97e3-44dd-9c9a-b...
- DTMF sequence:

Calling Party Information:

Calling party PRX Agent

Save Reset

2014 Feb 13 17:29

R C

2014 Feb 13 17:30

1 Minute 2014 Feb 13 17:29

## 9. Conclusion

These Application Notes describe the configuration steps required for ASC telecom ASC EVOIPneo active for Avaya Aura (with CM & AES) to successfully interoperate with Avaya Aura® Communication Manager R6.3 using Avaya Aura® Application Enablement Services R6.3. All feature functionality and serviceability test cases were completed successfully as outlined in **Section 2.2**.

## 10. Additional References

This section references the Avaya and ASC product documentation that are relevant to these Application Notes.

Product documentation for Avaya products may be found at <http://support.avaya.com>.

- [1] *Administering Avaya Aura® Communication Manager*, Document ID 03-300509
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Document ID 555-245-205
- [3] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide Release 6.3*

Product documentation for ASC telecom can be obtained as follows:

- Email: [hq@asctelecom.com](mailto:hq@asctelecom.com)
- Website: [www.asctelecom.com](http://www.asctelecom.com)
- Phone: +49 6021 5001-0

---

**©2014 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. 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](mailto:devconnect@avaya.com).