Avaya Solution & Interoperability Test Lab

Application Notes for configuring ASC EVOIPneo active V5.0 from ASC Technologies AG to interoperate with Avaya Aura® Communication Manager R7.0 and Avaya Aura® Application Enablement Services R7.0 - Issue 1.0

Abstract

These Application Notes describe the configuration steps for ASC EVOIPneo active to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. ASC EVOIPneo active from ASC Technologies AG integrates with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using single step conferencing implemented via DMCC over TSAPI.

Readers should pay attention to Section 2, in particular the scope of testing as outlined in Section 2.1 as well as the 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 describe the compliance tested configuration of ASC EVOIPneo active V5.0 from ASC Technologies AG with Avaya Aura® Communication Manager R7.0 and Avaya Aura® Application Enablement Services R7.0 to record telephone conversations.

ASC EVOIPneo active 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 to capture the audio and call details for recording agent calls. ASC EVOIPneo active 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 EVOIPneo active. 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 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 EVOIPneo active (ASC) to carry out call recording in a variety of scenarios using DMCC with Aura® Application Enablement Services (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 Conference
- Supervised Conference
- Forwarded Calls
- Feature Calls
- Inbound Calls to Communication Manager Agents
- Serviceability Testing

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

2.2. Test Results

All functionality and serviceability test cases were completed successfully.

Please note that the tested versions used in Section 4 for this test were the latest GA versions that could be used with this solution because of the following:

- Communication Manager 7.0.1 with patch 23012 does not allow **H.323 Registrations** with Application Enablement Services 7.0. A fix has been put in place in Application Enablement Services 7.0.1. ASC Technologies currently use H.323 virtual stations for recording using **RTP port redirection**.
- Application Enablement Services 7.0.1(any build) does not allow **RTP port redirection**. ASC Technologies use this method for the virtual station used by the recorder. An open ticket is being worked to fix this issue.

Both of the above issues are Avaya issues and are not issues with the ASC EVOIPneo active recorder.

2.3. Support

Technical support can be obtained for ASC EVOIPneo active as follows:

Email:	hq@asctechnologies.com
Website:	www.asctechnologies.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 EVOIPneo active is connected to the LAN and recording is performed using the Single Step Conference feature of Communication Manager using DMCC provided by AES.

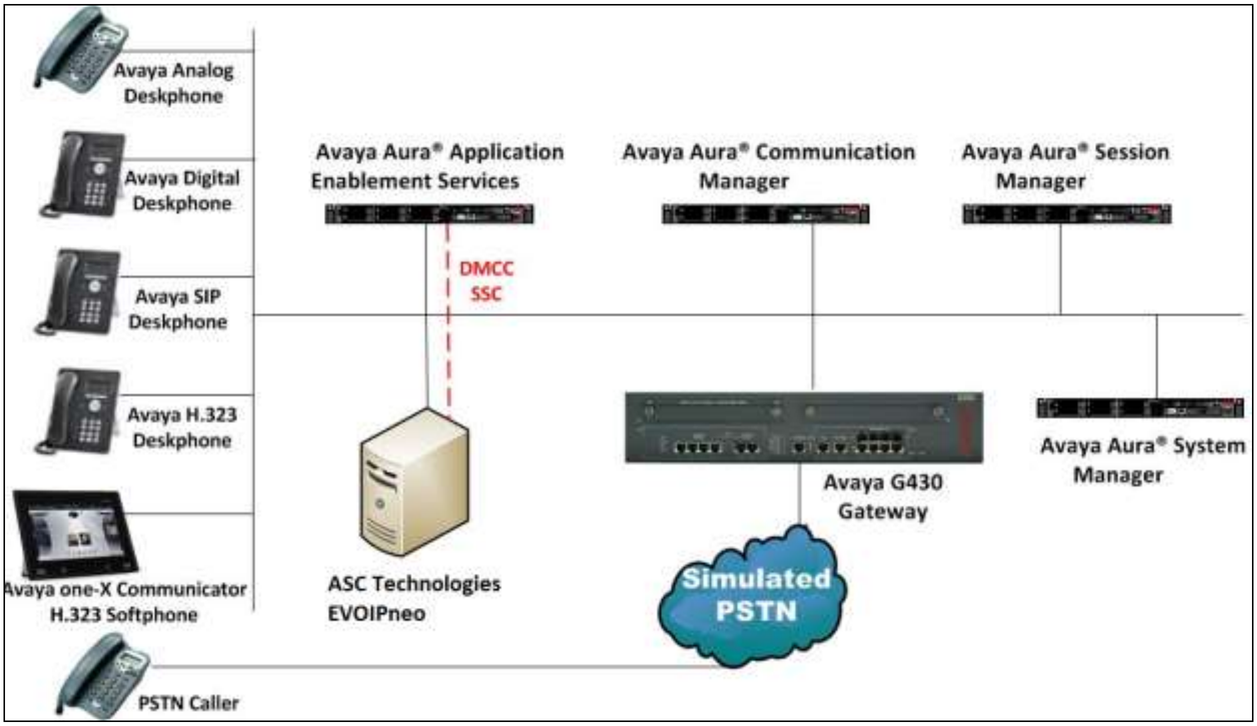

Avaya Analog Deskphone
Avaya Digital Deskphone
Avaya SIP Deskphone
Avaya H.323 Deskphone
Avaya one-X Communicator H.323 Softphone
PSTN Caller
Avaya Aura® Application Enablement Services
DMCC SSC
ASC Technologies EVOIPneo
Avaya Aura® Communication Manager
Avaya Aura® Session Manager
Avaya G430 Gateway
Avaya Aura® System Manager
Simulated PSTN

Figure 1: Avaya Aura® Communication Manager with Avaya Aura® Application Enablement Services, and ASC EVOIPneo active

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 a virtual server	7.0.1.0 Build – 7.0.0.0.16266 Software Update Revision Number: 7.0.1.0.064859 Feature Pack 1
Avaya Aura® Communication Manager running on a virtual server	R17x.00.0.441.0 Version CM 7.0.0.3.0.441.22856
Avaya Aura® Session Manager running on a virtual server	7.0.1.0.701007
Avaya Aura® Application Enablement Services running on a virtual server	7.0.0.0.0.13-1
Avaya G430 Gateway	37.21.0
Avaya 9641g Series Deskphone	96x1 H.323 Release 6.6029
Avaya 9611g Series Deskphone	96x1 H323 Release 6.6.029
Avaya 9611g Series Deskphone	96x1 SIP Release 7.0.0-080615
Avaya 9641g Series Deskphone	96x1 SIP Release
Avaya one-X® Agent	2.5.58020.0
Avaya one-X® Communicator	6.2.11.03-SP11
Avaya 2420 Digital Deskphone	NA
ASC EVOIPneo active running on MS Windows Server 2012 R2	V5.0
ASC POWERplay running on MS Windows Server 2012 R2	V5.0

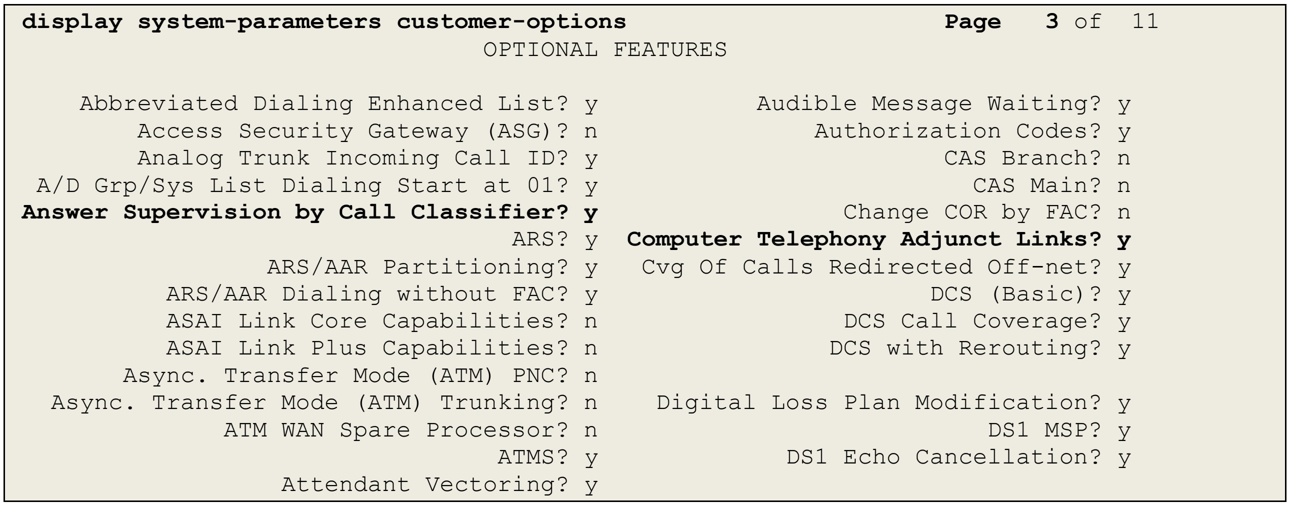
5. Configure Avaya Aura® Communication Manager

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
Answer Supervision by Call Classifier? y                 Change COR by FAC? n
                                  ARS? y  Computer Telephony Adjunct Links? y
                 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 (**Aes71624**).

```
display node-names ip                                              Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
SM100               10.10.40.34
Aes71624            10.10.16.24
default             0.0.0.0
g430                10.10.40.15
procr               10.10.16.27
```

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      Enabled      Local        Local        Remote       Remote
  Type                     Node         Port         Node         Port
AESVCS         y           procr        8765
```

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

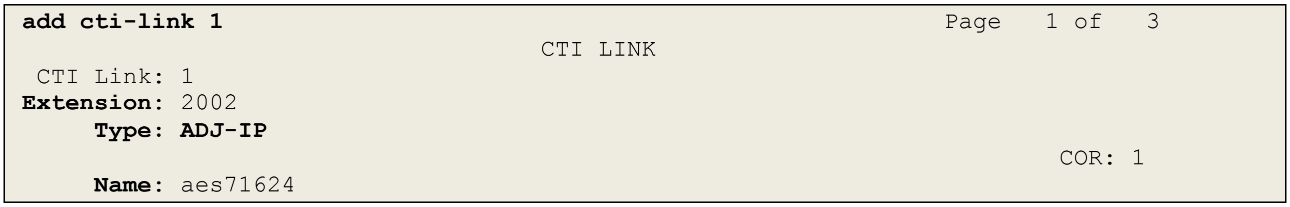
- **AE Services Server**: Name obtained from the AES server, in this case **aes71624**.
- **Password**: Enter a password to be administered on the AES server.
- **Enabled**: Set to **y**.

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        Password          Enabled    Status
                   Server
      1:        aes71624           ********          y          idle
      2:
      3:
```

5.4. Configure CTI Link for TSAPI Service

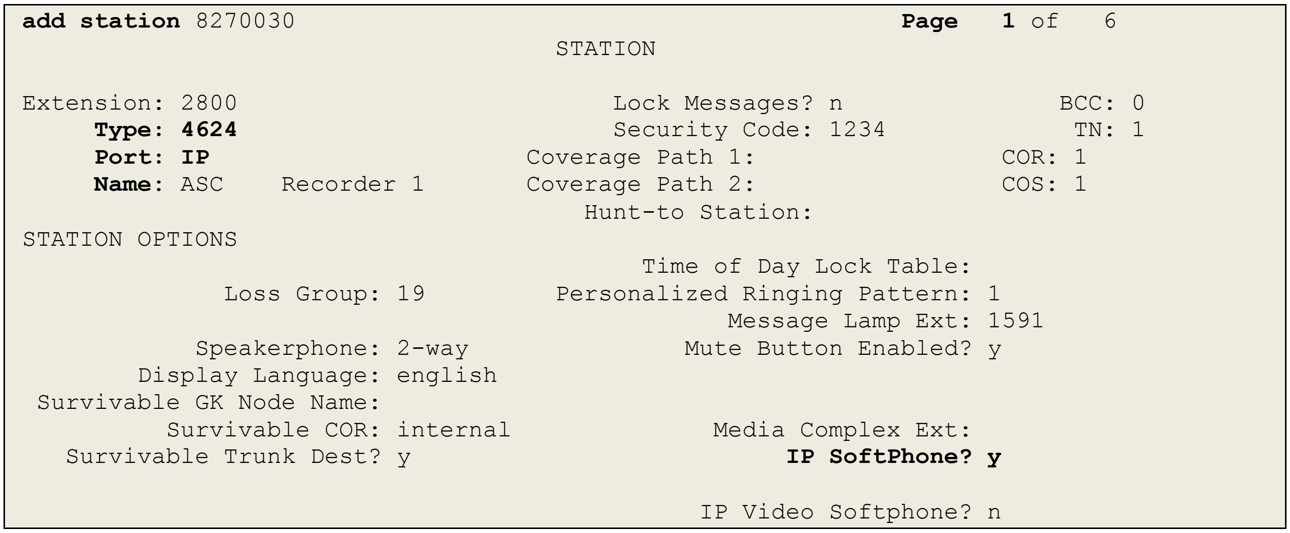
Add a CTI link using the **add cti-link n** command. Enter an available extension number in the **Extension** field. Enter **ADJ-IP** in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.



```
add cti-link 1                                                  Page   1 of   3
                                    CTI LINK
 CTI Link: 1
Extension: 2002
     Type: ADJ-IP
                                                                        COR: 1
     Name: aes71624
```

5.5. Configure Virtual Stations

ASC EVOIPneo active 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 8270030                                          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
                                           Time of Day Lock Table:
              Loss Group: 19         Personalized Ringing Pattern: 1
                                                 Message Lamp Ext: 1591
            Speakerphone: 2-way                Mute Button Enabled? y
        Display Language: english
 Survivable GK Node Name:
          Survivable COR: internal              Media Complex Ext:
   Survivable Trunk Dest? y                          IP SoftPhone? y

                                               IP Video Softphone? n
```

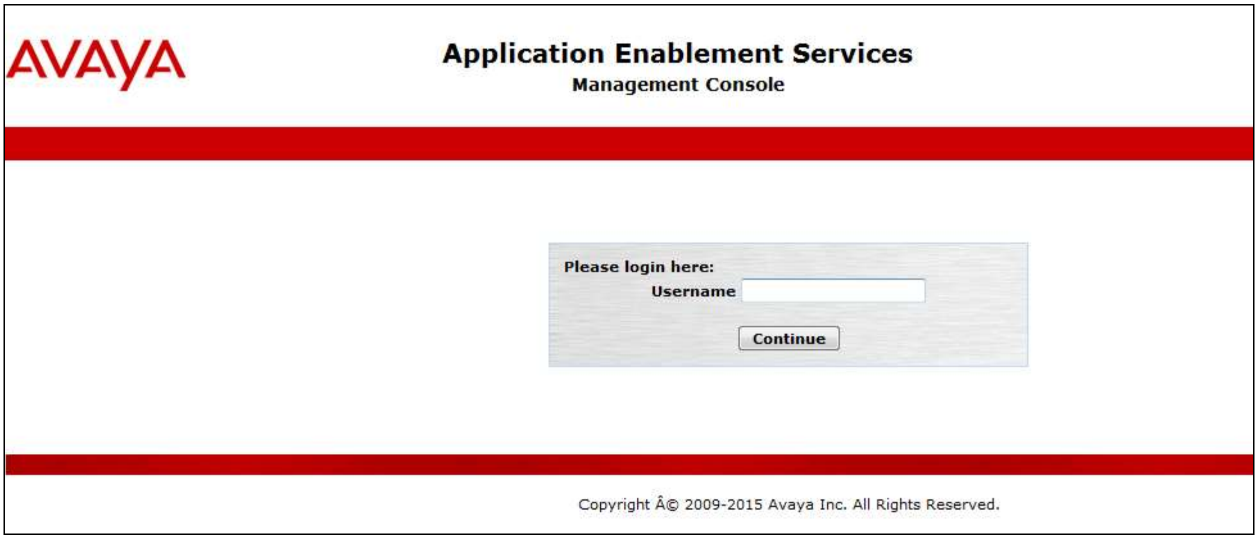
6. Configure Avaya Aura® Application Enablement Services

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

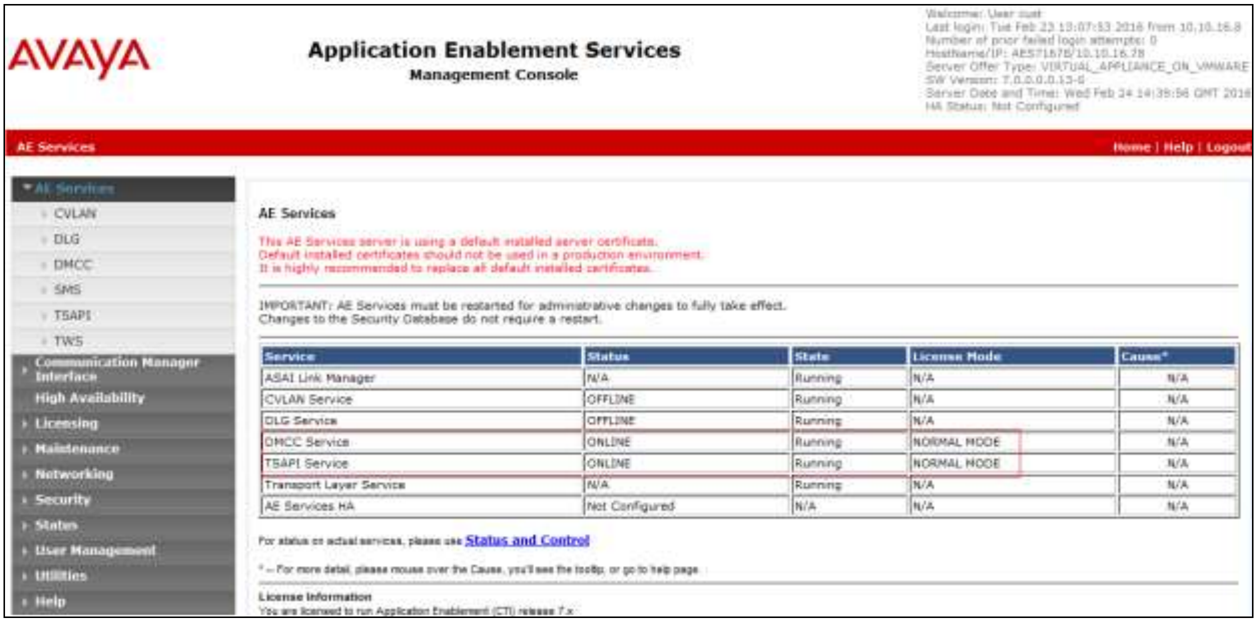
To access the maintenance console, enter **https://<ip-addr>** as the URL in an Internet browser, where <ip-addr> is the active IP address of AES. The login screen is displayed, enter the appropriate credentials and then select the **Login** button.


Application Enablement Services
Management Console

Please login here:
Username

Copyright Â© 2009-2015 Avaya Inc. All Rights Reserved.

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.



Welcome: User cust
Last login: Tue Feb 23 13:07:53 2016 from 10.10.16.8
Number of prior failed login attempts: 0
HostName/IP: AES7167B/10.10.16.78
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.0.0.0.13-6
Server Date and Time: Wed Feb 24 14:39:56 GMT 2016
HA Status: Not Configured

AE Services

This AE Services server is using a default installed server certificate.
Default installed certificates should not be used in a production environment.
It is highly recommended to replace all default installed certificates.

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	OFFLINE	Running	N/A	N/A
DLG Service	OFFLINE	Running	N/A	N/A
DMCC Service	ONLINE	Running	NORMAL MODE	N/A
TSAPI Service	ONLINE	Running	NORMAL MODE	N/A
Transport Layer Service	N/A	Running	N/A	N/A
AE Services HA	Not Configured	N/A	N/A	N/A

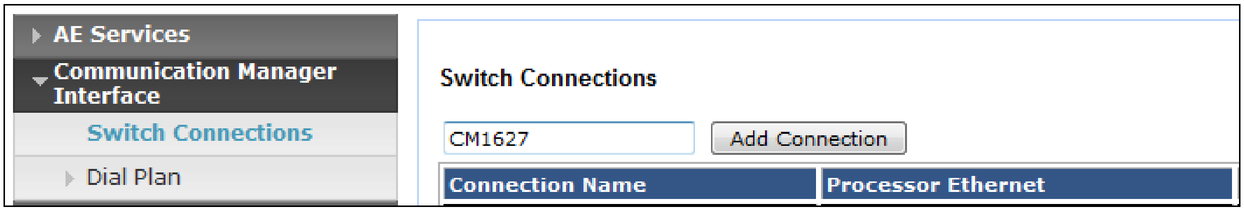
For status on actual services, please use Status and Control

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

License Information
You are licensed to run Application Enablement (CTI) release 7.x

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.

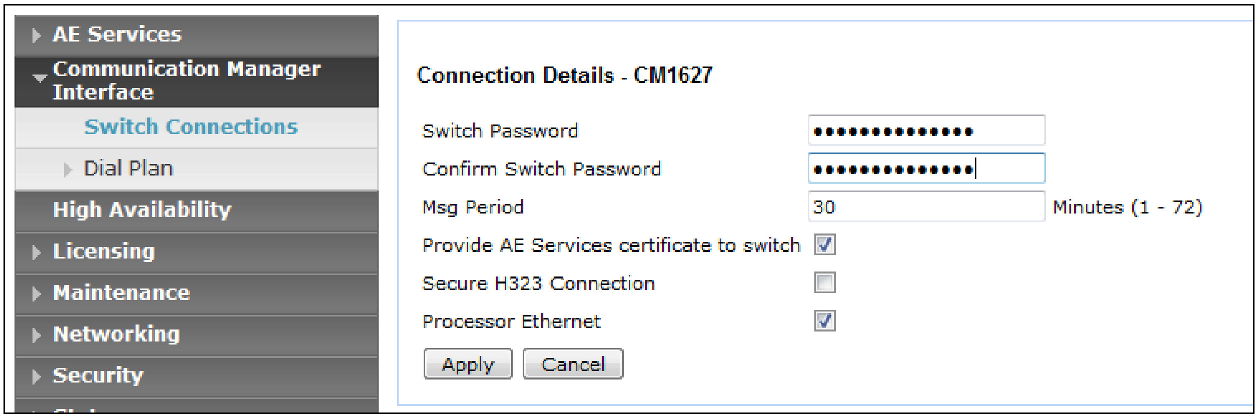


Switch Connections

CM1627

Connection Name	Processor Ethernet

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.



Connection Details - CM1627

Switch Password ••••••••••••••

Confirm Switch Password ••••••••••••••

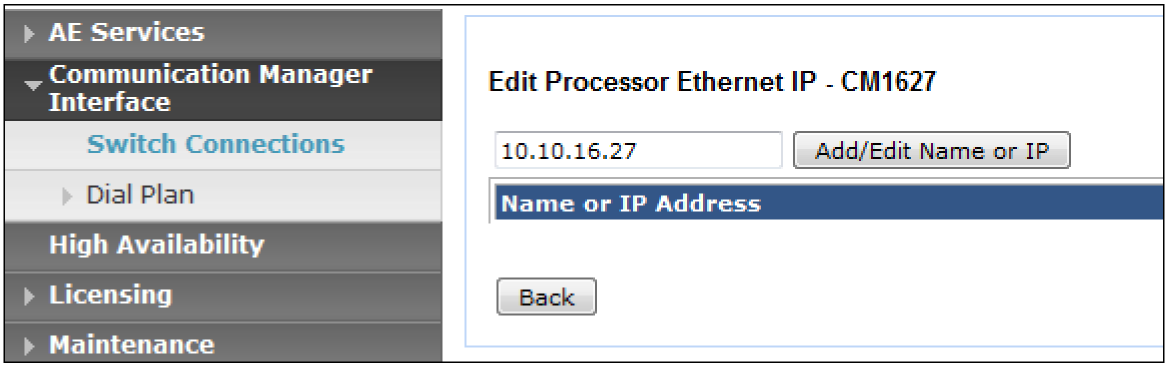
Msg Period 30 Minutes (1 - 72)

Provide AE Services certificate to switch ☑

Secure H323 Connection ☐

Processor Ethernet ☑

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/Edit Name or IP** button.



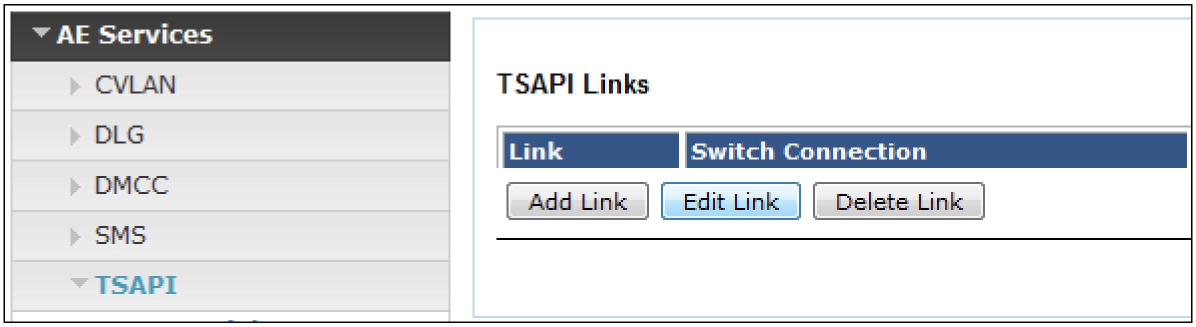
Edit Processor Ethernet IP - CM1627

10.10.16.27

Name or IP Address

6.3. Administer TSAPI link

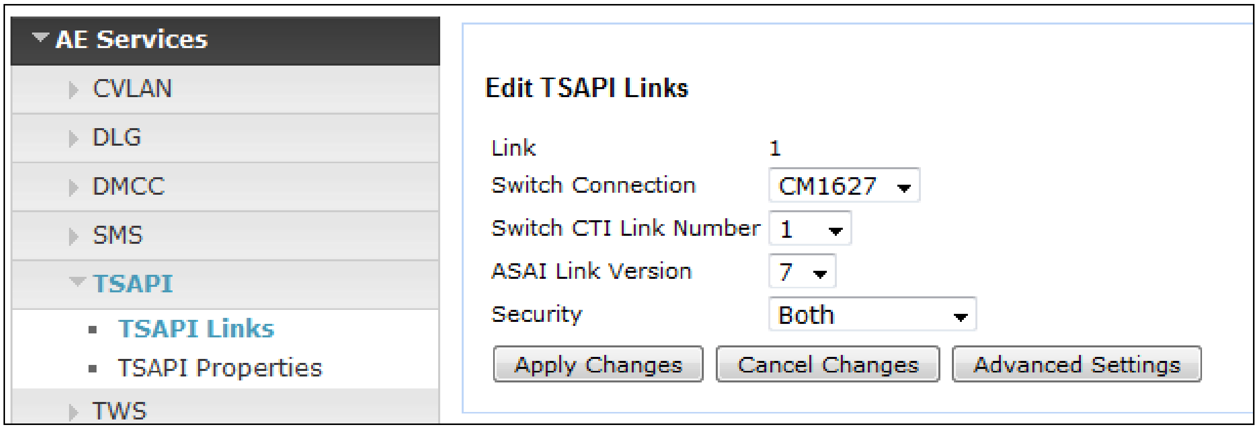
From the Application Enablement Services Management Console, select **AE Services** → **TSAPI** → **TSAPI Links**. Select **Add Link** button as shown in the screen below.



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 **CM1627**, 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 **7**.
- **Security:** select **Both** from the drop down.

Once completed, select **Apply Changes**.

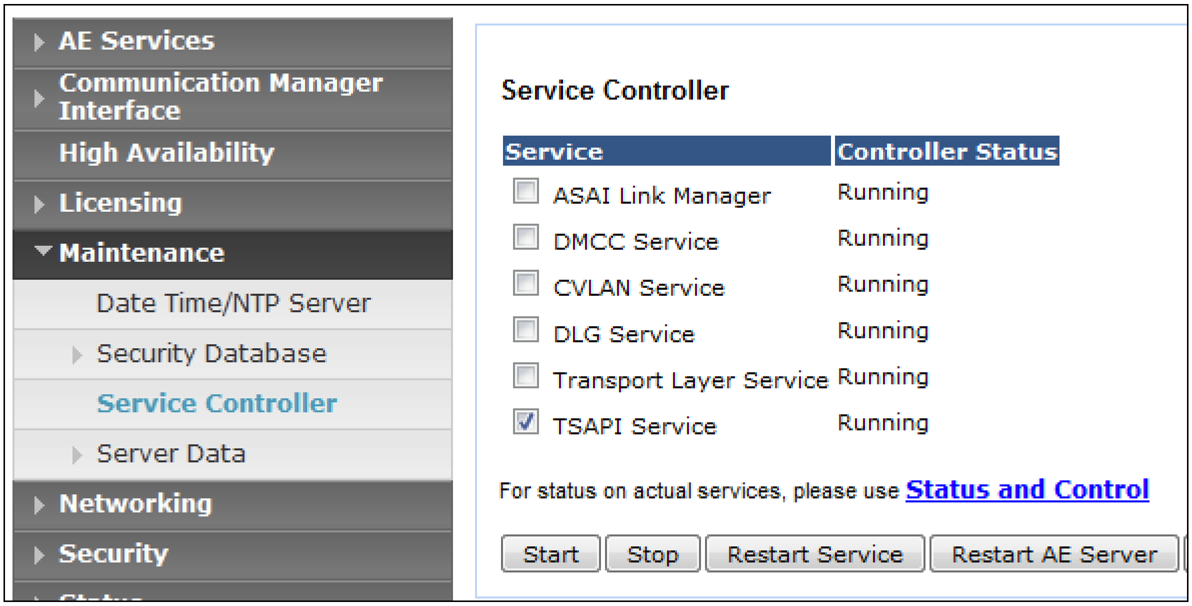


Edit TSAPI Links

Link	1
Switch Connection	CM1627
Switch CTI Link Number	1
ASAI Link Version	7
Security	Both

Another screen appears for confirmation of the changes. Choose **Apply** (not shown).

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**.



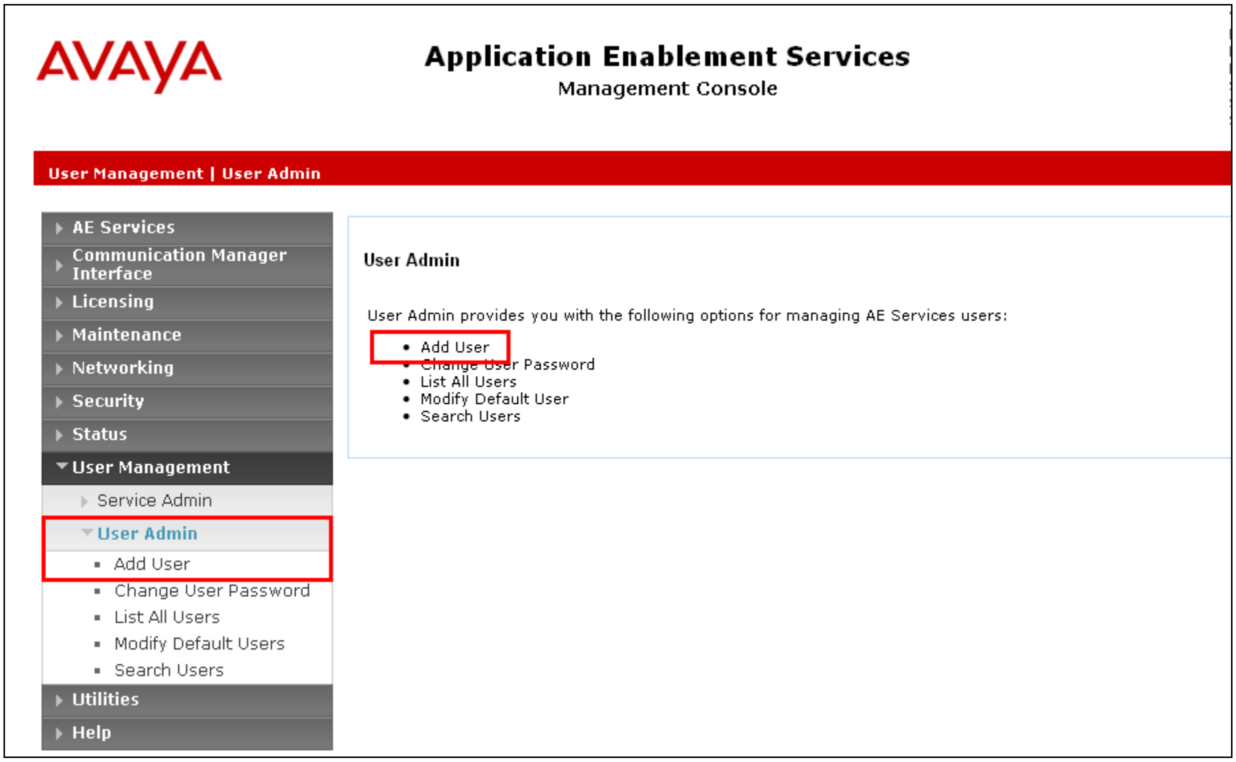
Service Controller

Service	Controller Status
□ ASAI Link Manager	Running
□ DMCC Service	Running
□ CVLAN Service	Running
□ DLG Service	Running
□ Transport Layer Service	Running
☑ TSAPI Service	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 EVOIPneo active 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.



User Admin

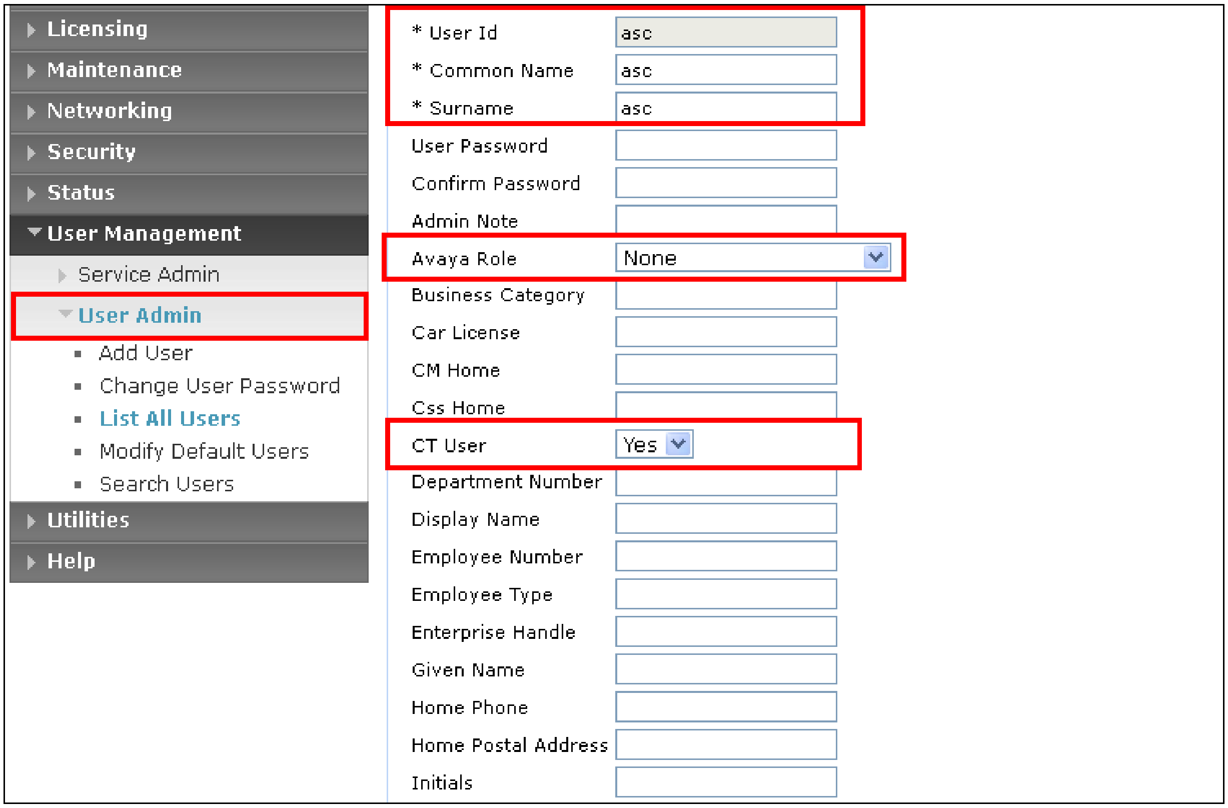
User Admin provides you with the following options for managing AE Services users:

- Add User
- Change User Password
- List All Users
- Modify Default User
- Search Users

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 7.4.1**. This value must be filled in.
- **CT User -** Select **Yes** from the drop-down menu.

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

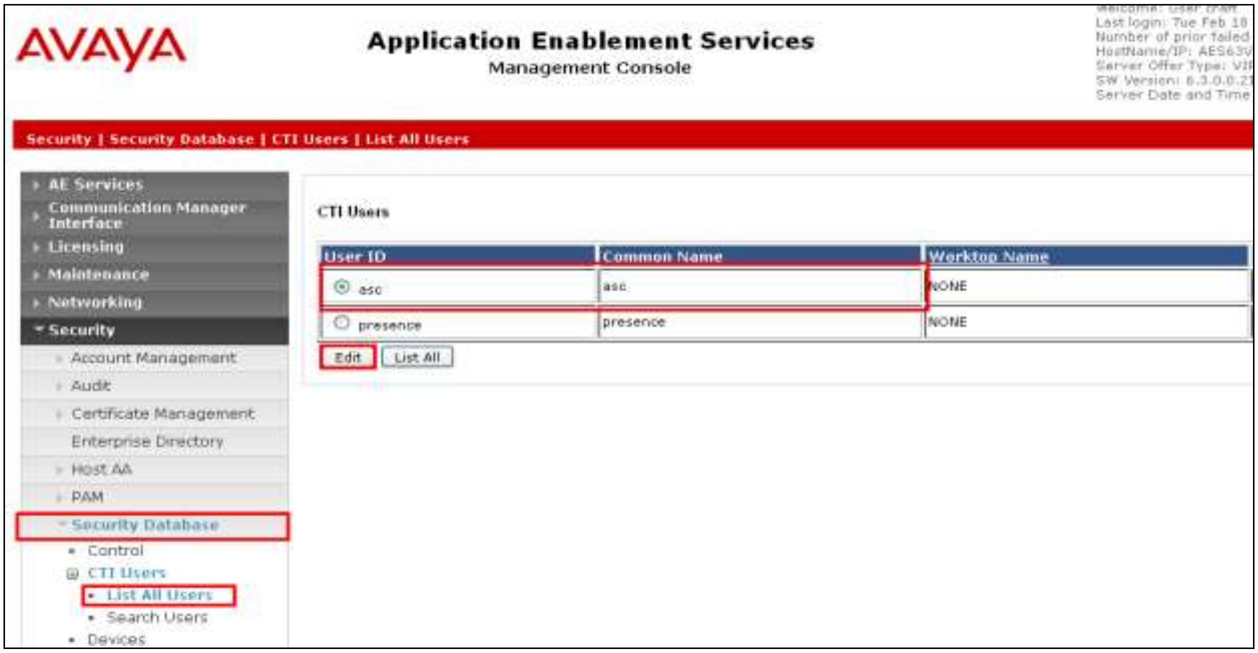


* User Id	asc
* Common Name	asc
* Surname	asc
User Password	
Confirm Password	
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes
Department Number	
Display Name	
Employee Number	
Employee Type	
Enterprise Handle	
Given Name	
Home Phone	
Home Postal Address	
Initials	

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

6.5. Enable Unrestricted Access for CTI User

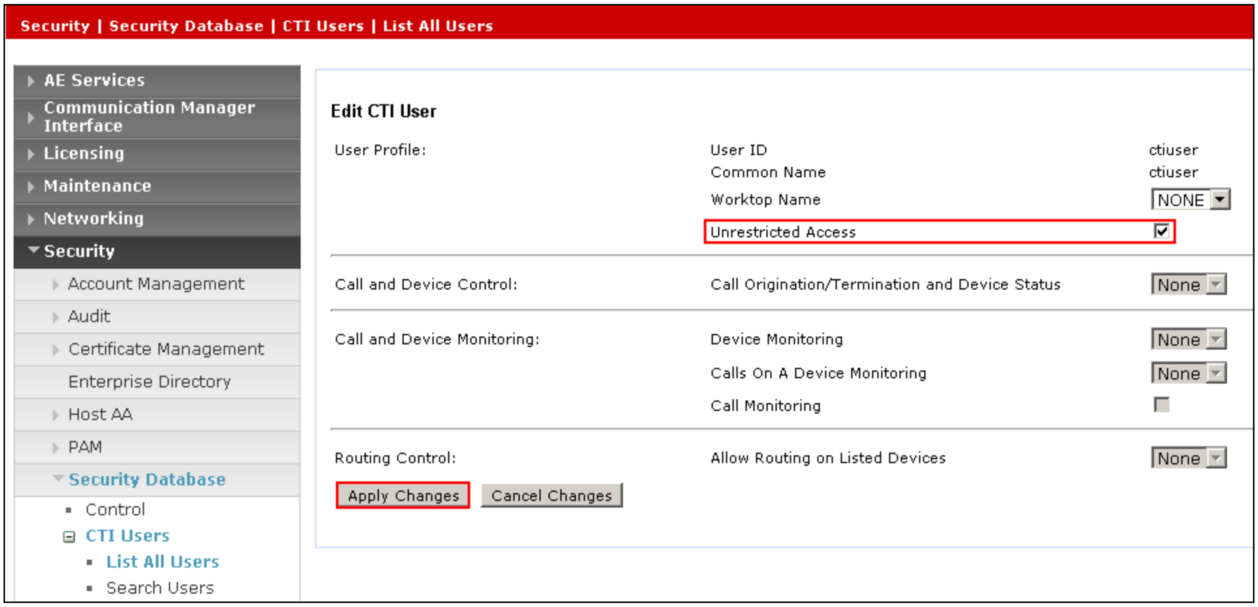
Navigate to the **CTI Users** screen by selecting **Security** → **Security Database** → **CTI Users** → **List All Users**. Select the user that was created in **Section 6.4** and select the **Edit** option.



CTI Users

User ID	Common Name	Worktop Name
● asc	asc	NONE
○ presence	presence	NONE

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



Edit CTI User

User Profile:	User ID	ctiuser
	Common Name	ctiuser
	Worktop Name	NONE
	Unrestricted Access	☑
Call and Device Control:	Call Origination/Termination and Device Status	None
Call and Device Monitoring:	Device Monitoring	None
	Calls On A Device Monitoring	None
	Call Monitoring	□
Routing Control:	Allow Routing on Listed Devices	None

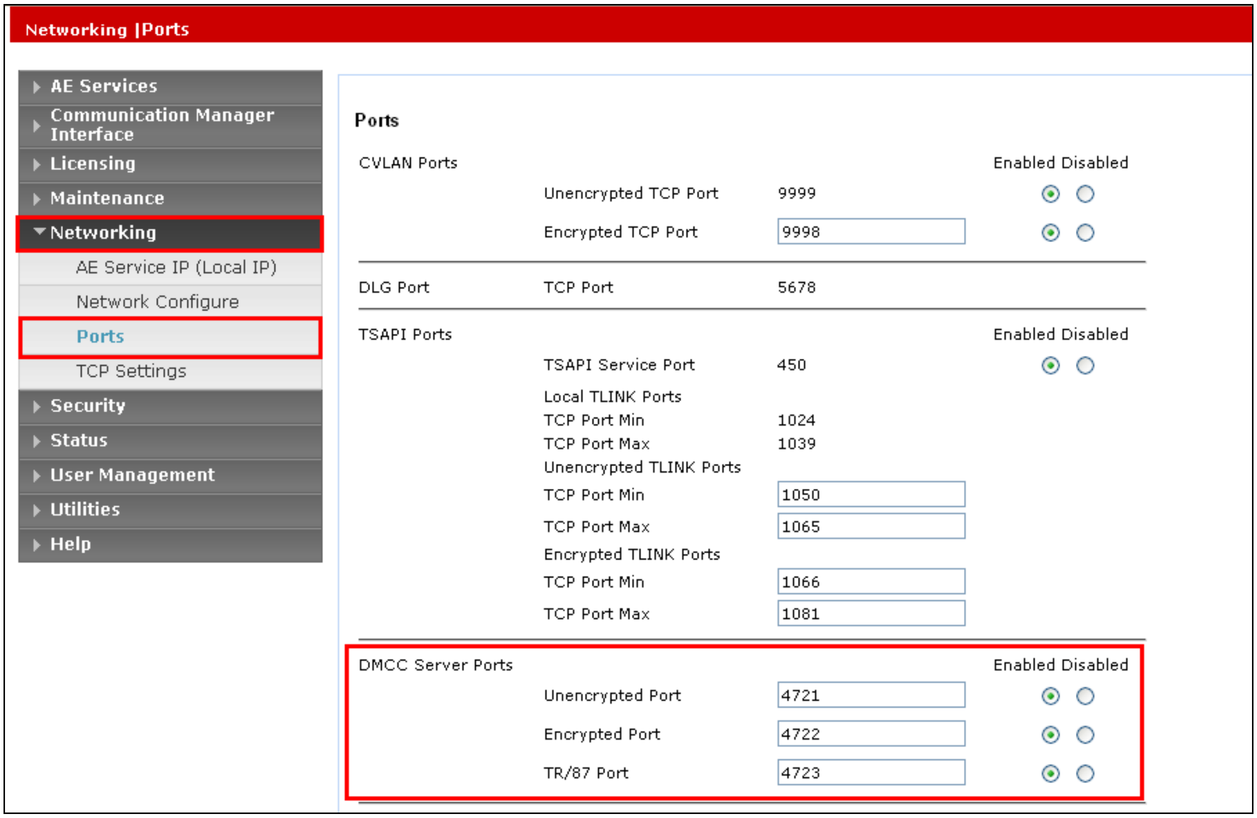
A screen (not shown) appears to confirm applied changes to CTI User, choose **Apply**. This CTI user should now be enabled.

6.6. 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**

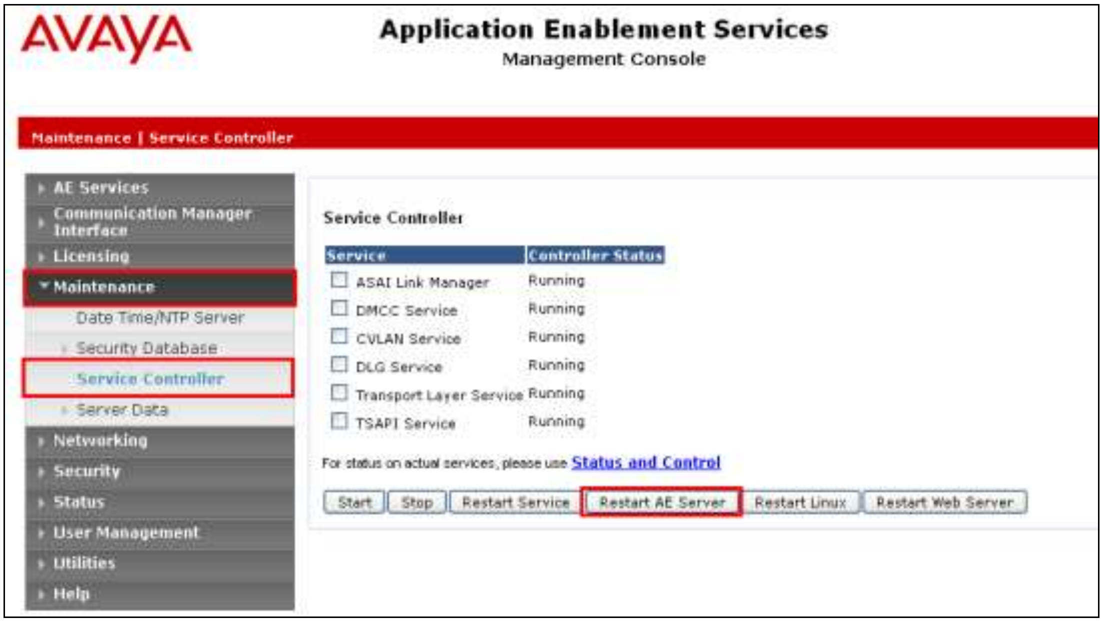
Click on **Apply Changes** at the bottom of the screen (not shown).



Ports

			Enabled	Disabled
CVLAN Ports				
	Unencrypted TCP Port	9999	●	○
	Encrypted TCP Port	9998	●	○
DLG Port	TCP Port	5678		
TSAPI Ports				
	TSAPI Service Port	450	●	○
	Local TLINK Ports			
	TCP Port Min	1024		
	TCP Port Max	1039		
	Unencrypted TLINK Ports			
	TCP Port Min	1050		
	TCP Port Max	1065		
	Encrypted TLINK Ports			
	TCP Port Min	1066		
	TCP Port Max	1081		
DMCC Server Ports				
	Unencrypted Port	4721	●	○
	Encrypted Port	4722	●	○
	TR/87 Port	4723	●	○

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.



Service Controller

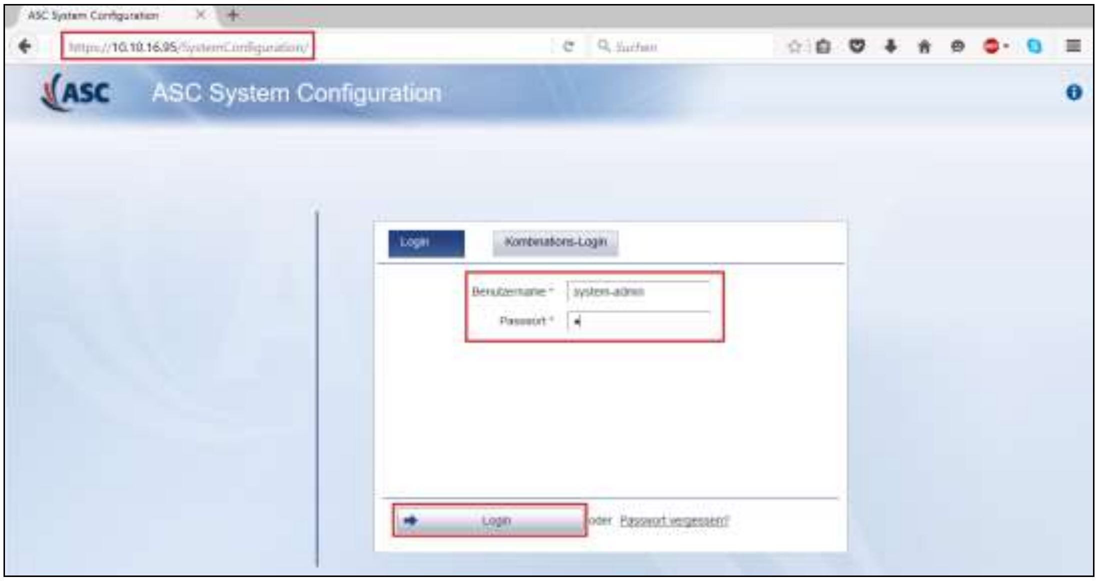
Service	Controller Status
□ ASAI Link Manager	Running
□ DMCC Service	Running
□ CVLAN Service	Running
□ DLG Service	Running
□ Transport Layer Service	Running
□ TSAPI Service	Running

For status on actual services, please use Status and Control

7. Configure ASC EVOIPneo active

The configuration of the ASC EVOIPneo active 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>/SystemConfiguration**. Enter the proper username and password and click on **Login**.



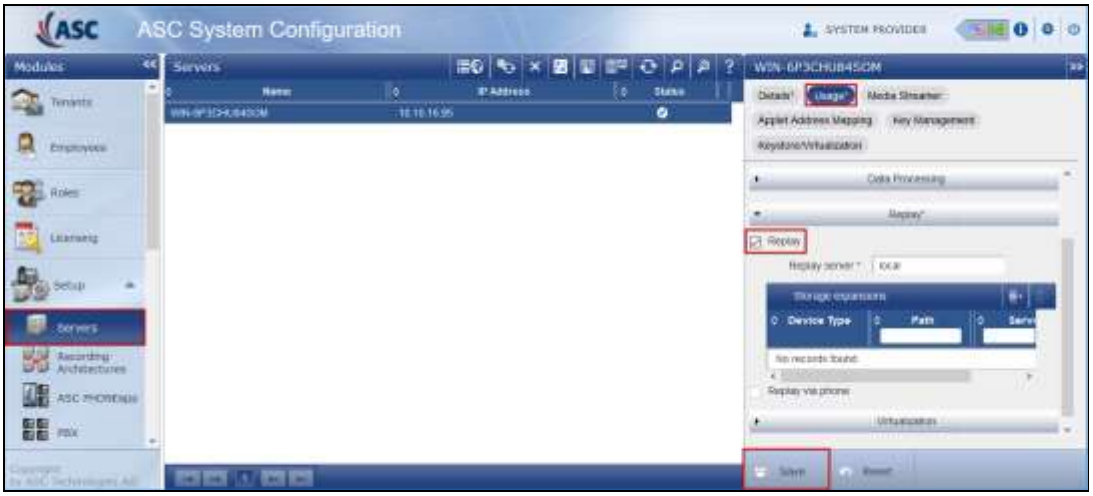
https://10.10.16.95/SystemConfiguration/

Benutzername * system-admin

Passwort *

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.



Name	IP Address	Status
WIN-6P3CHUB4SOM	10.10.16.95	✓

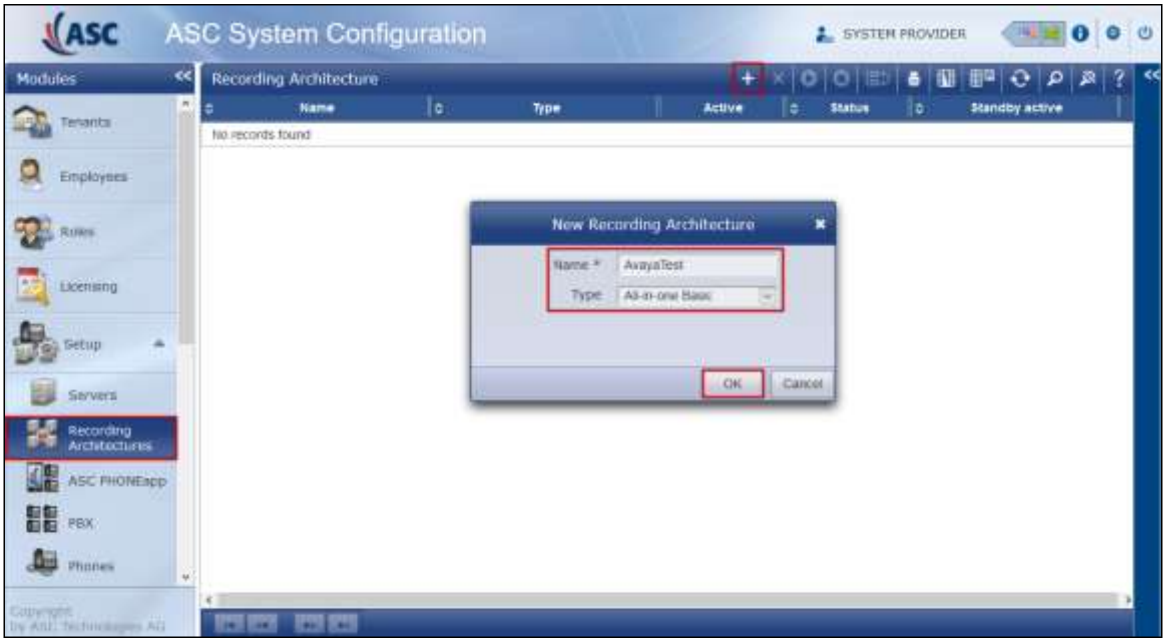
☑ Replay

Replay server * local

□ Replay via phone

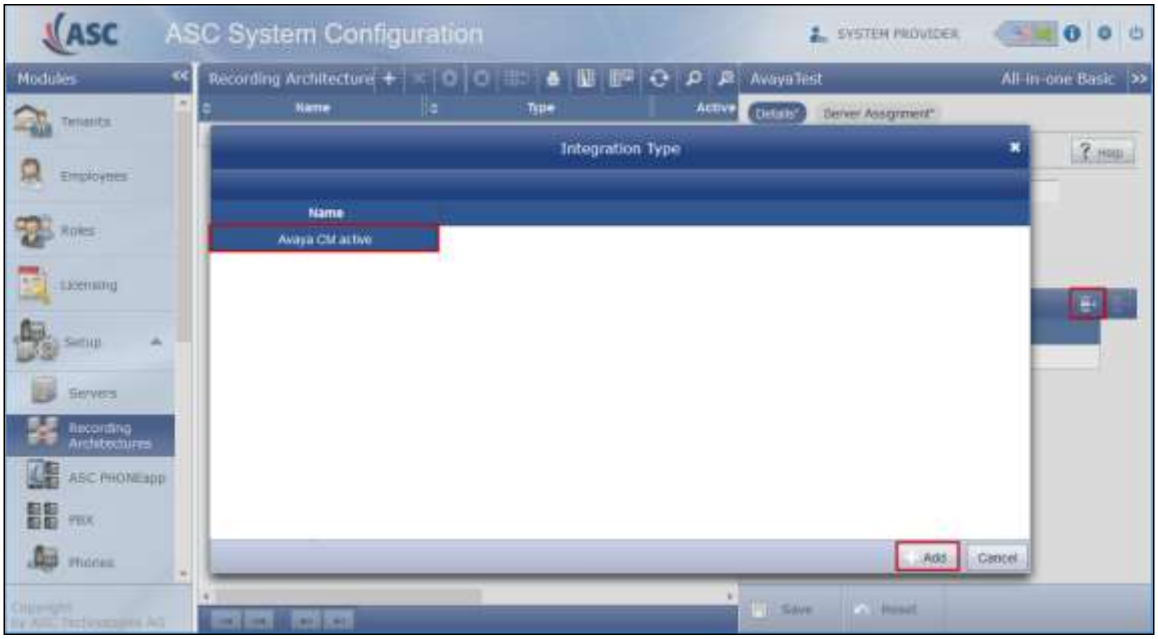
7.2. Configure Recording Architecture

Navigate to **Setup → Recording Architectures** 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.



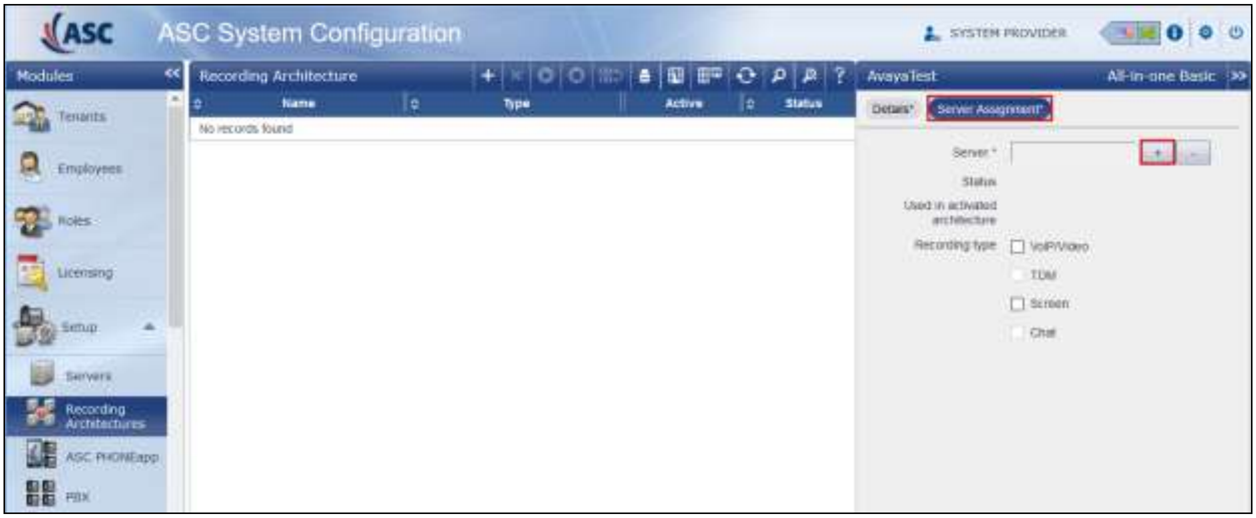
Name *: AvayaTest
Type: All-in-one Basic

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

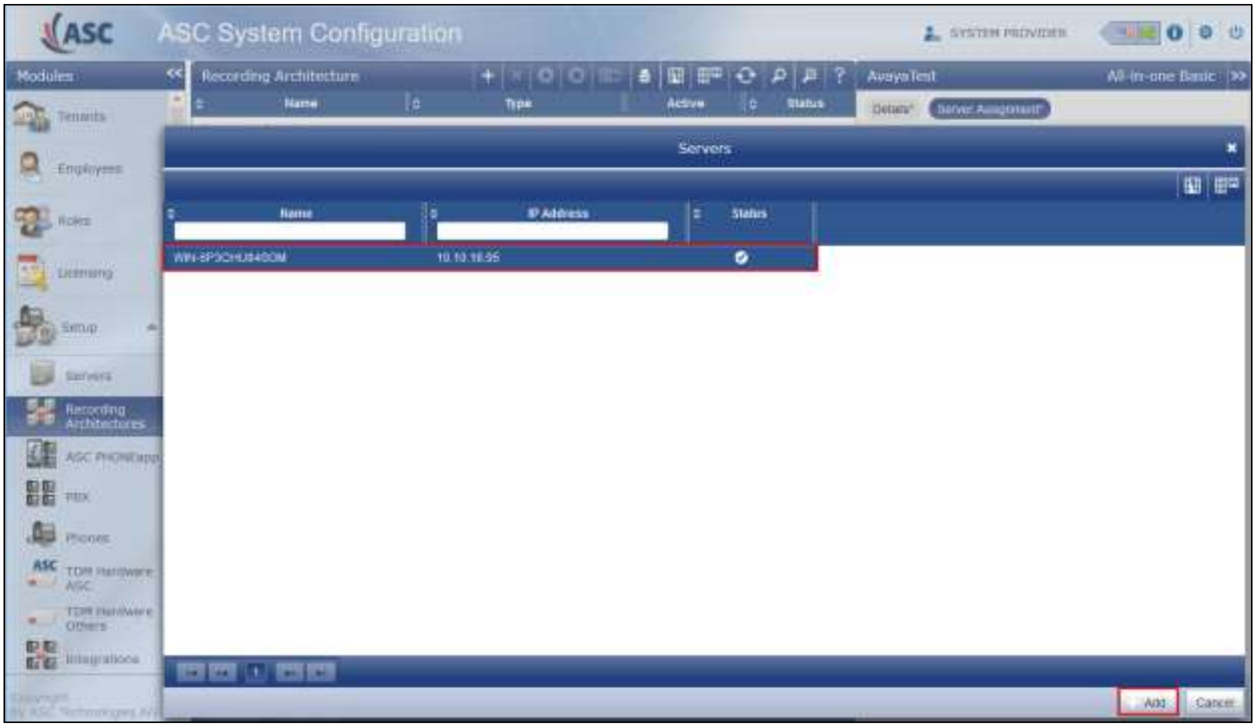


Name: Avaya CM active

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

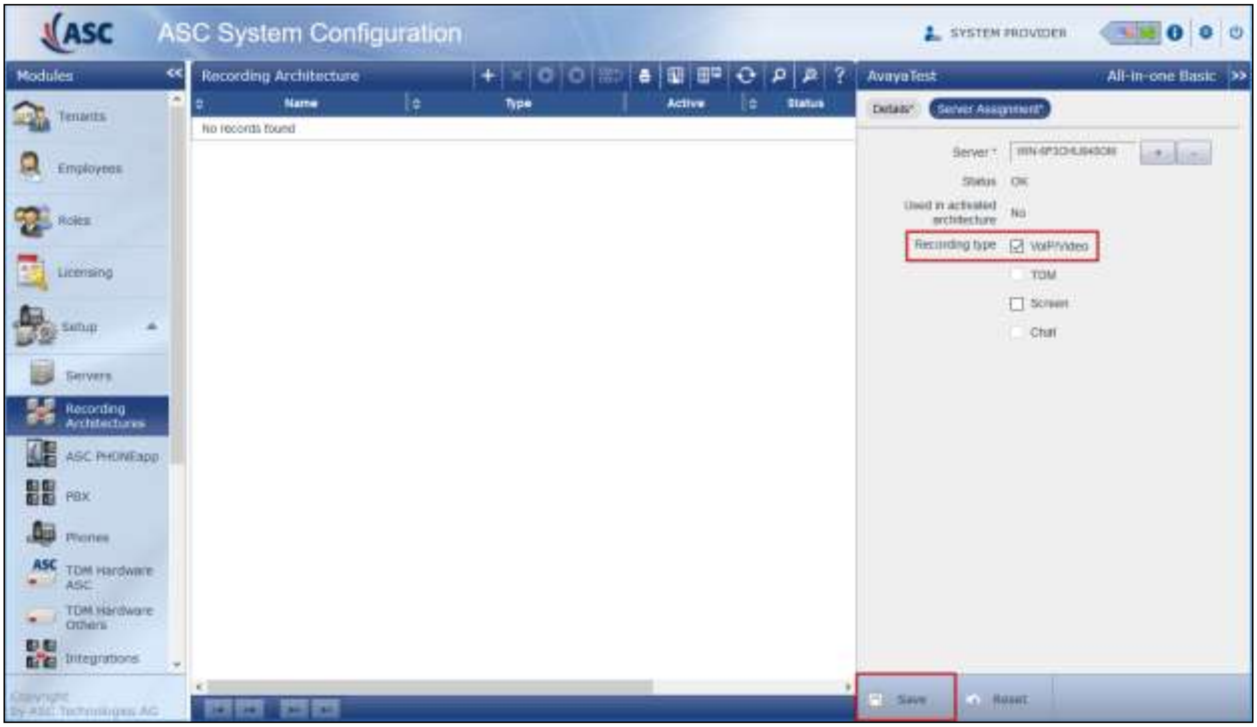


Select the server (added during the installation) and click on **Add** at the bottom of the screen.



Name	IP Address	Status
WIN-8P3CHU840OM	10.10.16.95	✓

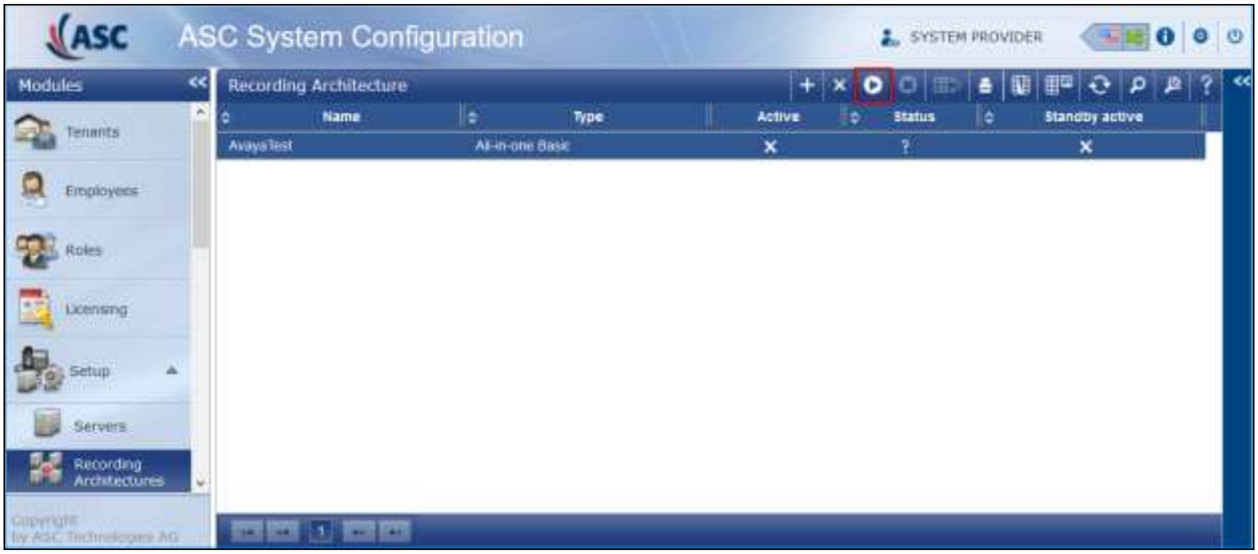
Ensure that **VoIP/Video r**ecording type is ticked as shown and click on **Save** at the bottom of the screen.



No records found

Server *: WIN-6P3CHL84SOM
Status: OK
Used in activated architecture: No
Recording type: ☑ VoIP/Video
□ TDM
□ Screen
□ Chat

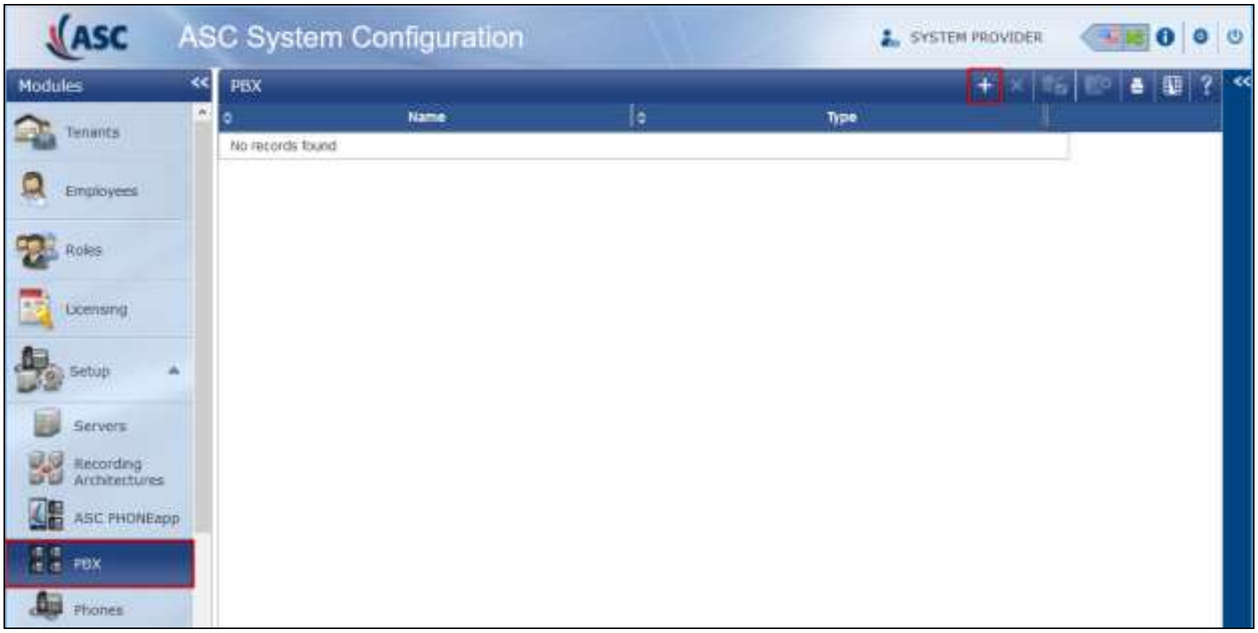
Once this Recording Architecture is added it must be activated by clicking on the **Activate** icon highlighted below.



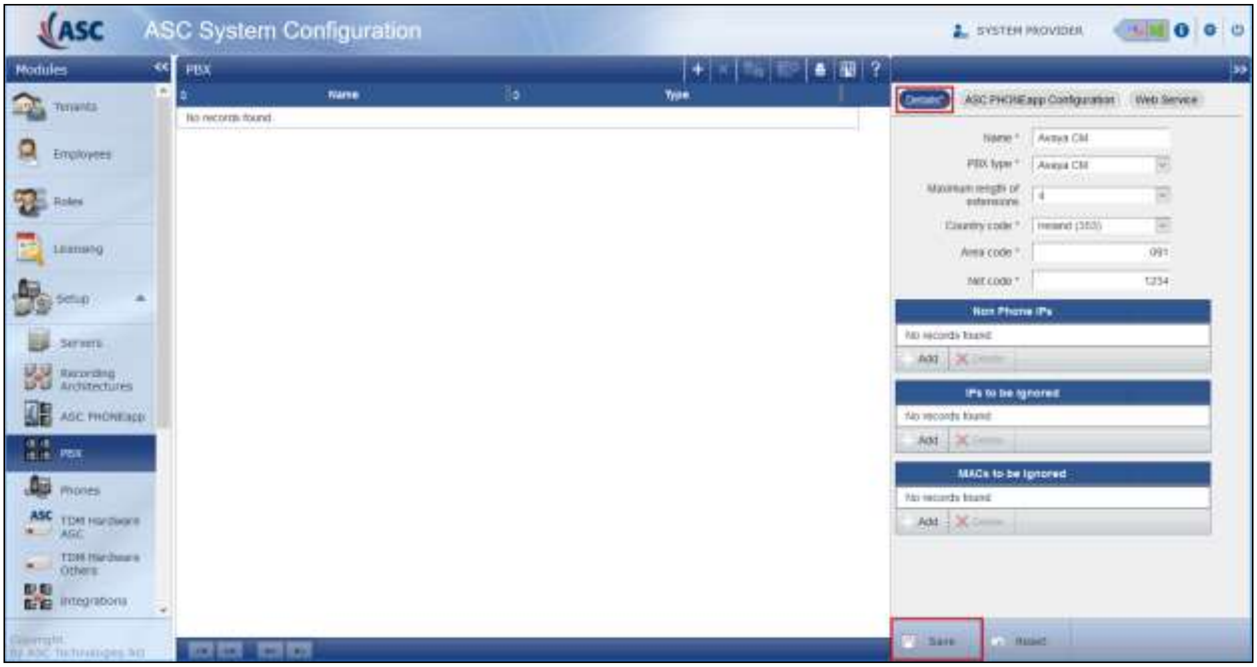
Name	Type	Active	Status	Standby active
AvayaTest	All-in-one Basic	✕	?	✕

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.



Name *	Avaya CM
PBX type *	Avaya CM
Maximum length of extensions	4
Country code *	Ireland (353)
Area code *	091
Net code *	1234

Non Phone IPs

No records found

Add | Delete

IPs to be ignored

No records found

Add | Delete

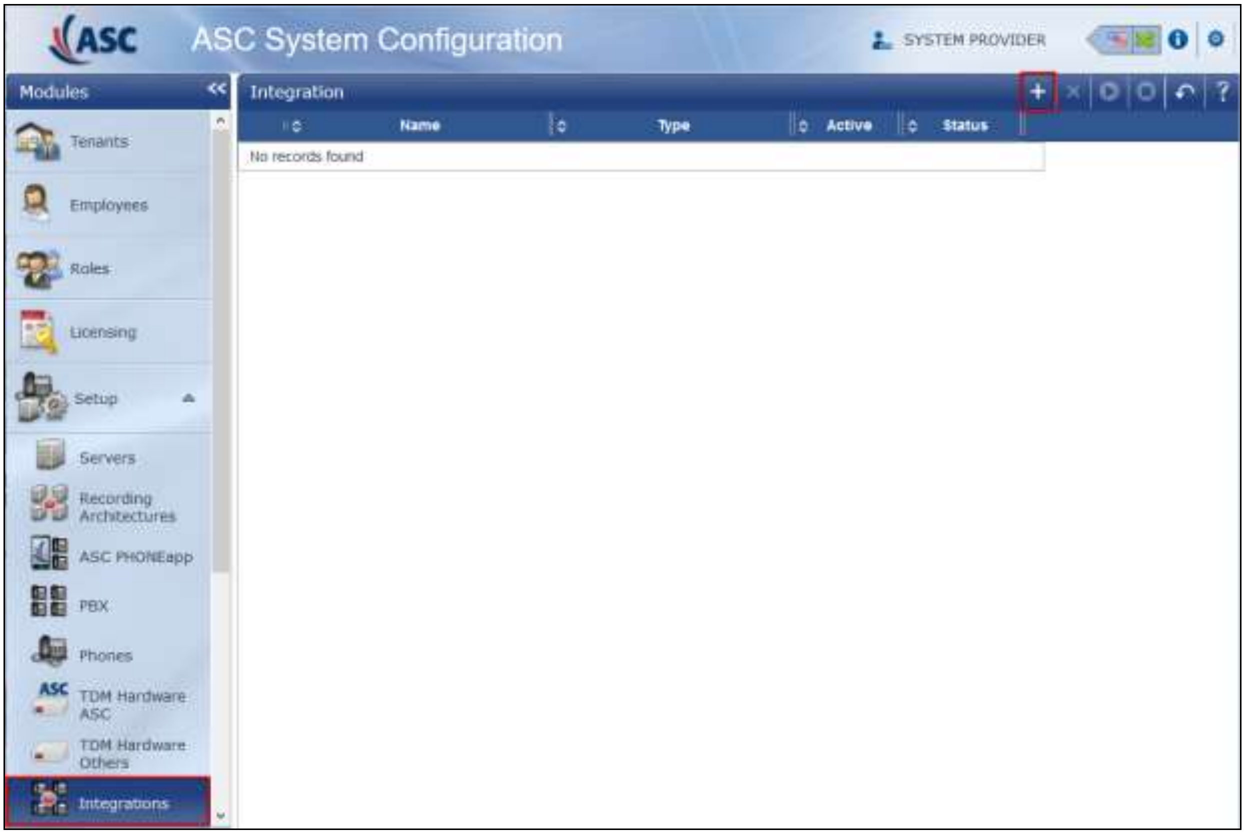
MACs to be ignored

No records found

Add | Delete

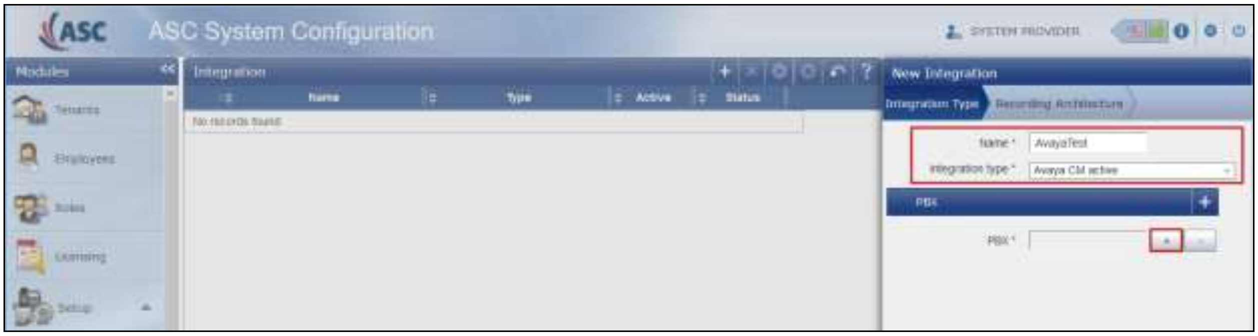
7.4. Integrations

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



No records found

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



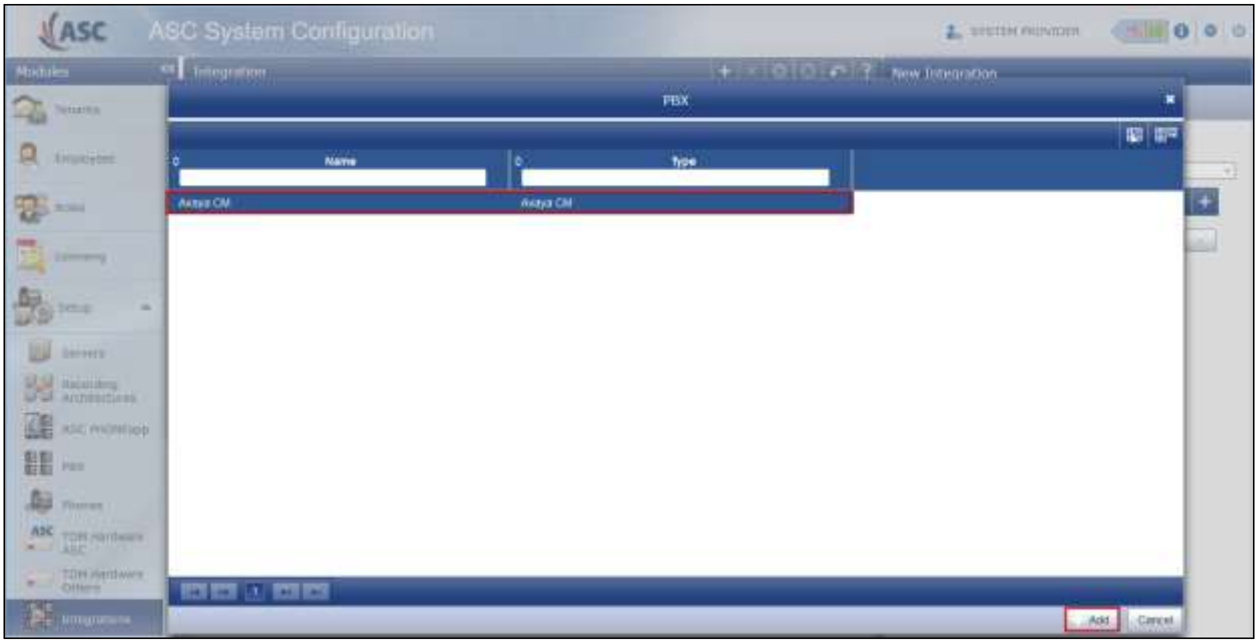
No records found

Name * AvayaTest

Integration type * Avaya CM active

PBX *

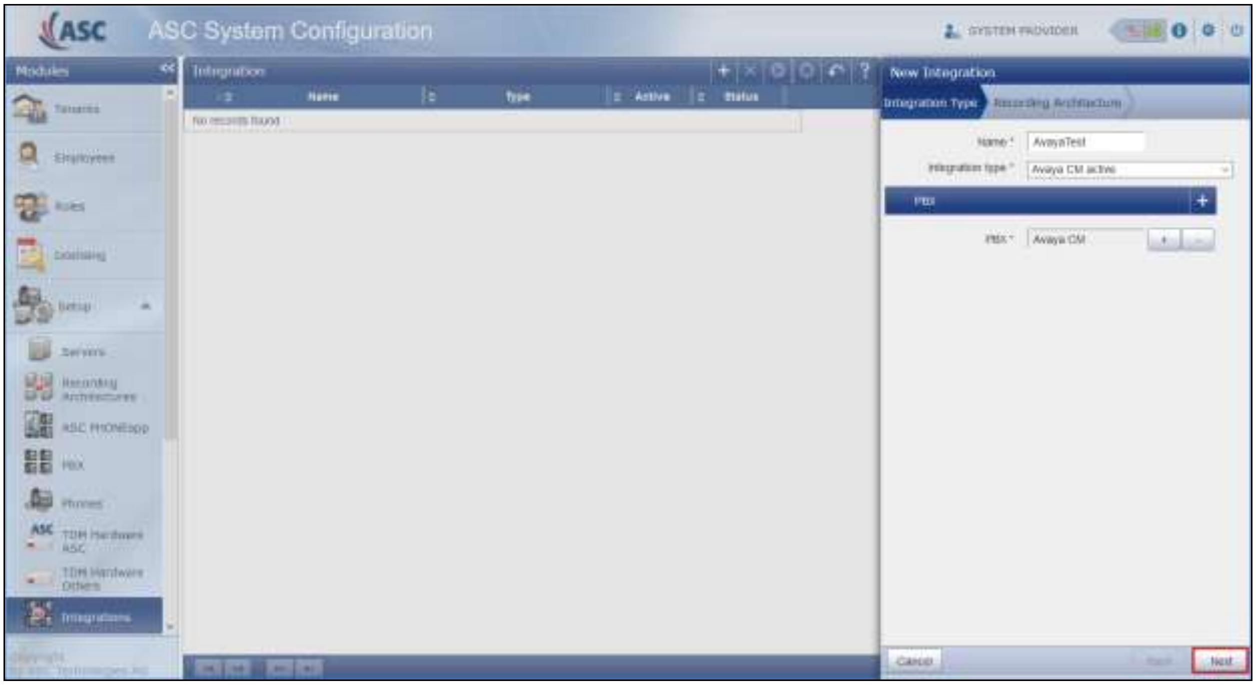
Select the PBX, this was created in **Section 7.3**, click on **Add** at the bottom of the screen.



PBX

Name	Type
Avaya CM	Avaya CM

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



New Integration

Integration Type › Recording Architecture

Name *: AvayaTest

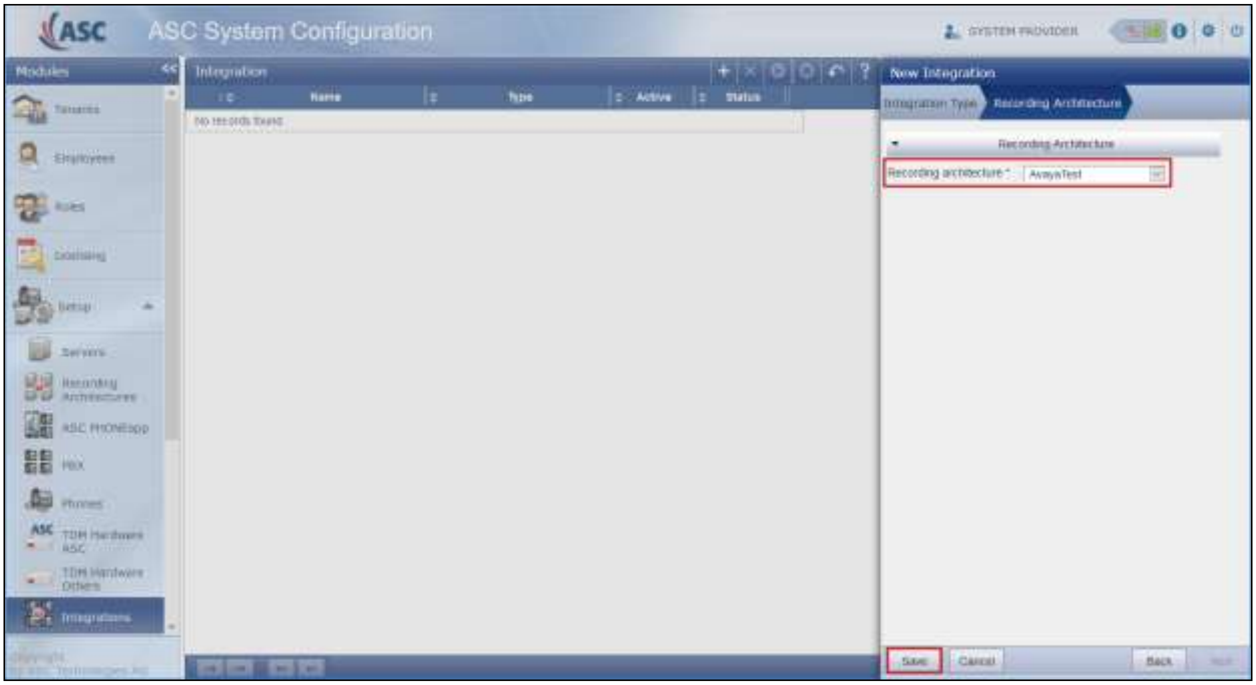
Integration type *: Avaya CM active

PBX

PBX *: Avaya CM

Name	Type	Active	Status
No records found			

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

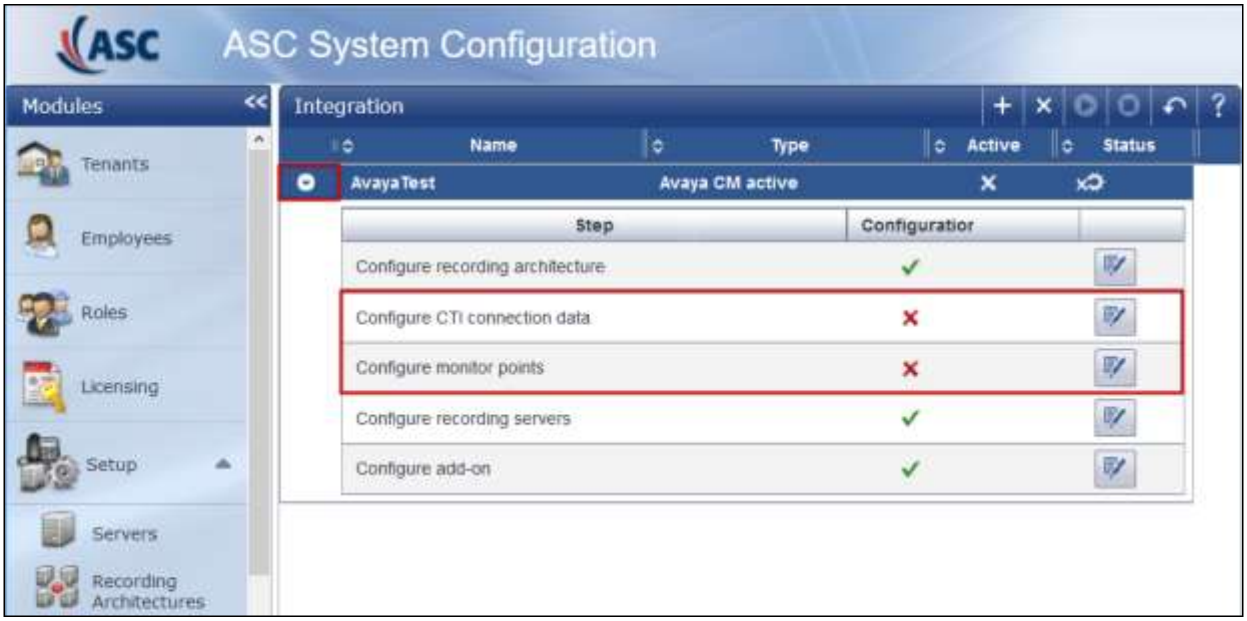


Recording Architecture

Recording architecture *: AvayaTest

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**.

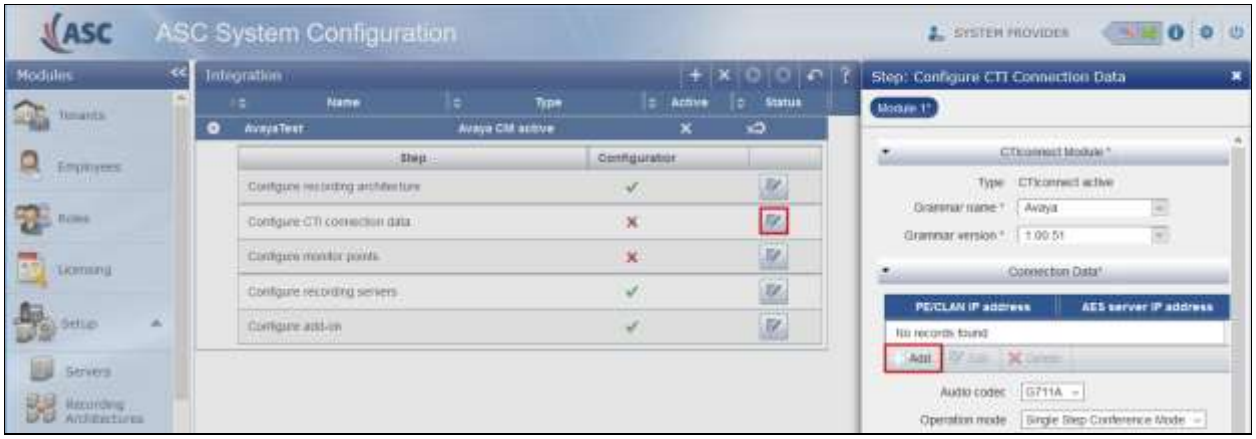


Name	Type	Active	Status
AvayaTest	Avaya CM active	✗	✗

Step	Configuration
Configure recording architecture	✓
Configure CTI connection data	✗
Configure monitor points	✗
Configure recording servers	✓
Configure add-on	✓

7.4.1. Configure CTI connection data

Click on the edit icon next to **Configure CTI connection data**. Click on **+Add** under **PE/CLAN IP address – AES server IP address** in the right window.



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	✓

CTIconnect Module *

Type: CTIconnect active

Grammar name *: Avaya

Grammar version *: 1.00.51

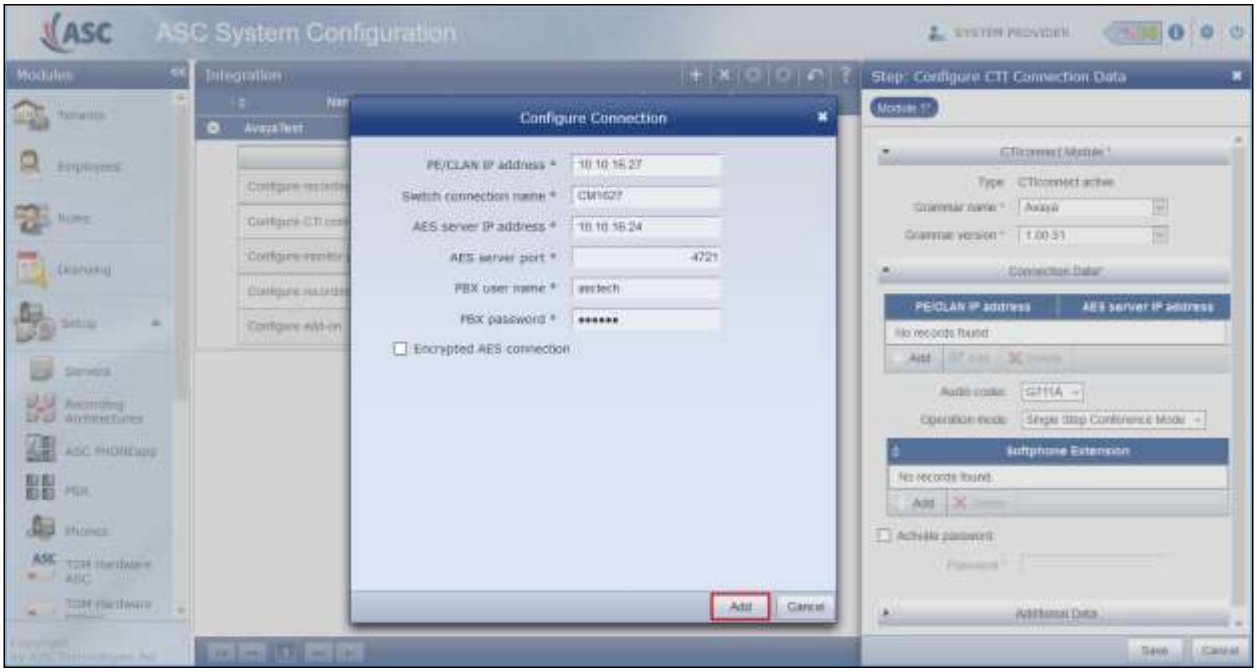
Connection Data*

PE/CLAN IP address	AES server IP address
No records found	

Audio codec: G711A

Operation mode: Single Step Conference Mode

Enter the Communication Manager IP Address and the AES information which can be obtained from **Section 6.4**. Click on **Add** once complete. Note in the screen shot below the **PE/CLAN IP address** will be that of the **procr** address displayed in **Section 5.2**.



Configure Connection

PE/CLAN IP address *: 10.10.16.27

Switch connection name *: CM1627

AES server IP address *: 10.10.16.24

AES server port *: 4721

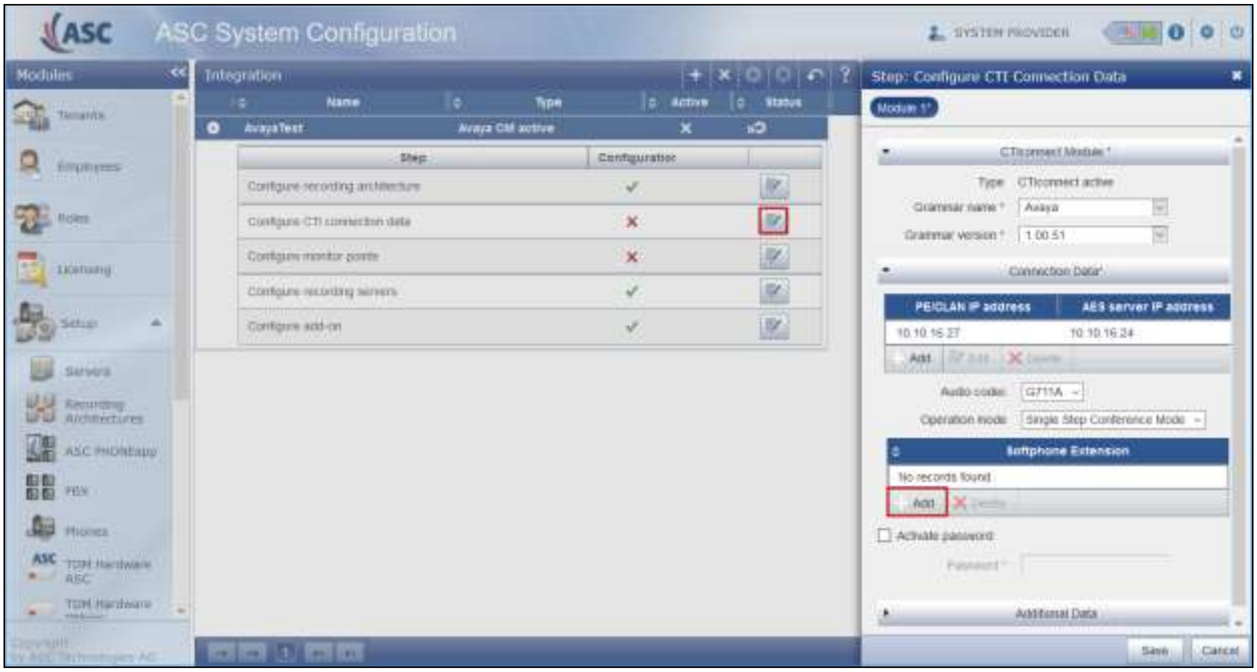
PBX user name *: asctech

PBX password *: ••••••

☐ Encrypted AES connection

Add Cancel

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



Step: Configure CTI Connection Data

Module 1*

CTIconnect Module *

Type CTIconnect active

Grammar name * Avaya

Grammar version * 1.00.51

Connection Data*

PE/CLAN IP address	AES server IP address
10.10.16.27	10.10.16.24

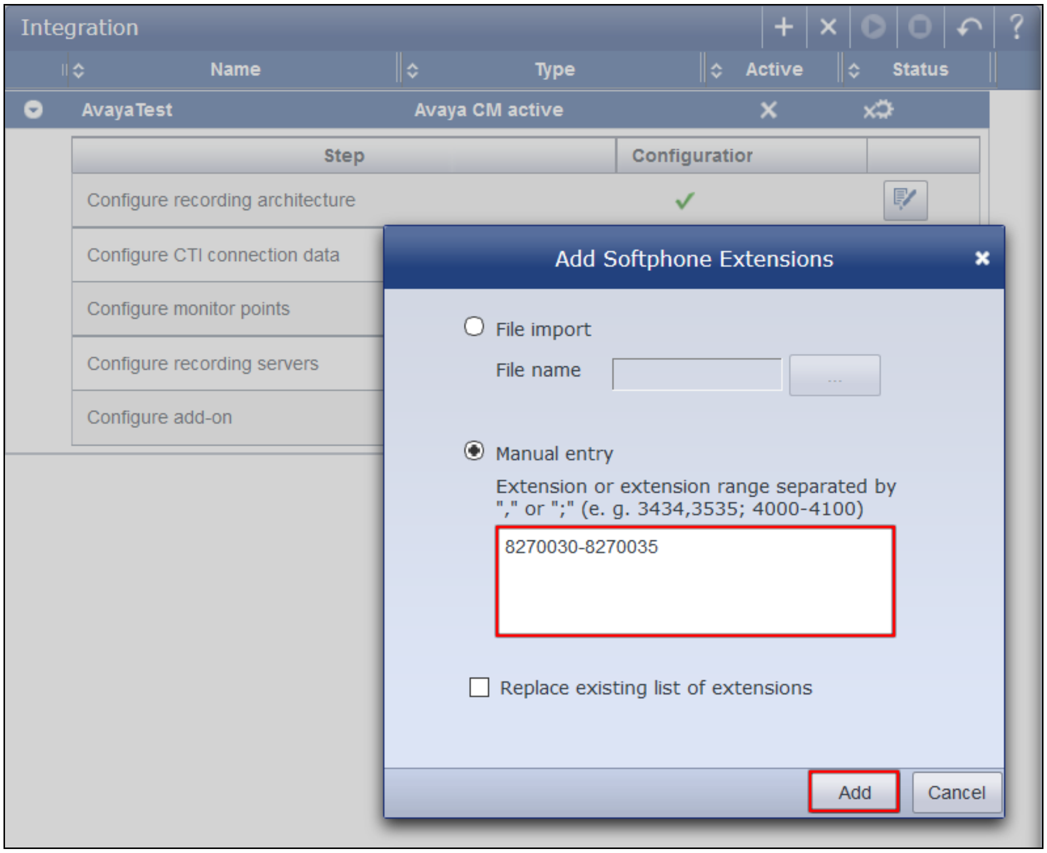
Audio codec G711A

Operation mode Single Step Conference Mode

Softphone Extension

No records found

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



Add Softphone Extensions

○ File import

File name

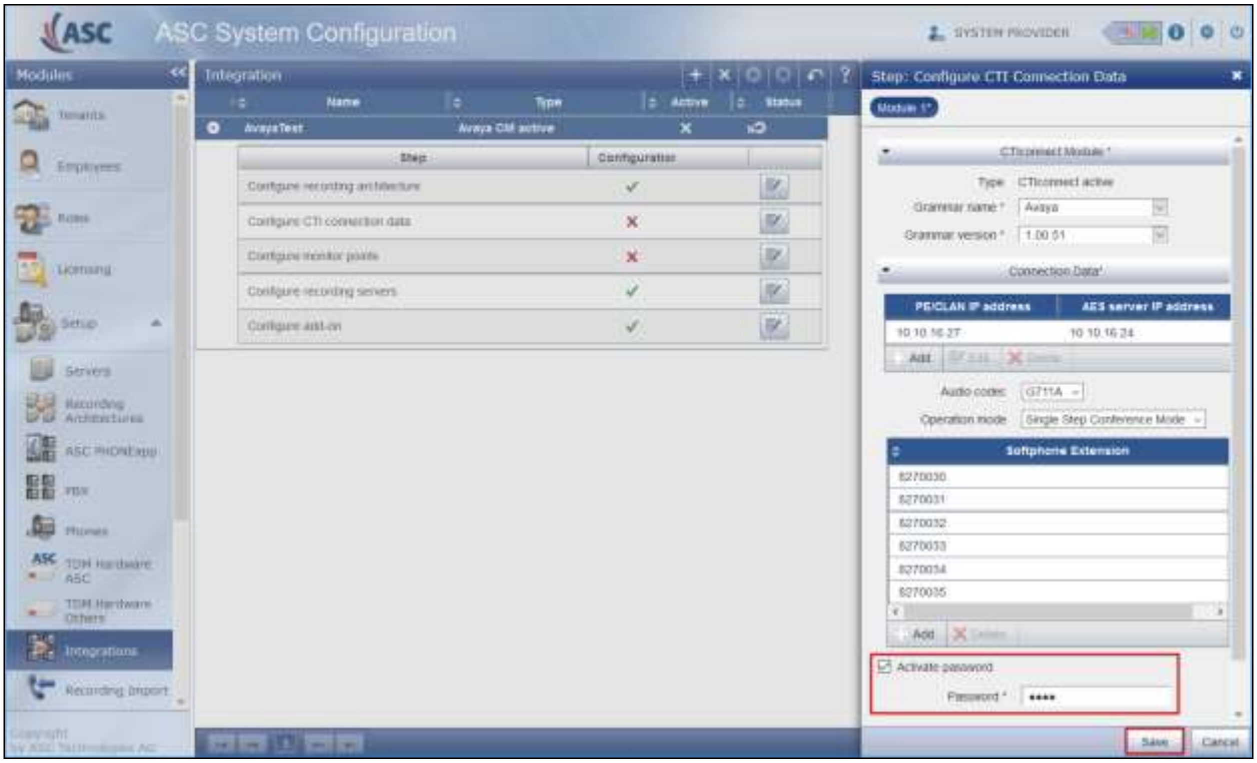
● Manual entry

Extension or extension range separated by "," or ";" (e. g. 3434,3535; 4000-4100)

8270030-8270035

□ Replace existing list of extensions

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.



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*

CTIconnect Module *

Type: CTIconnect active
Grammar name *: Avaya
Grammar version *: 1.00.01

Connection Data*

PE/CLAN IP address	AES server IP address
10.10.16.27	10.10.16.24

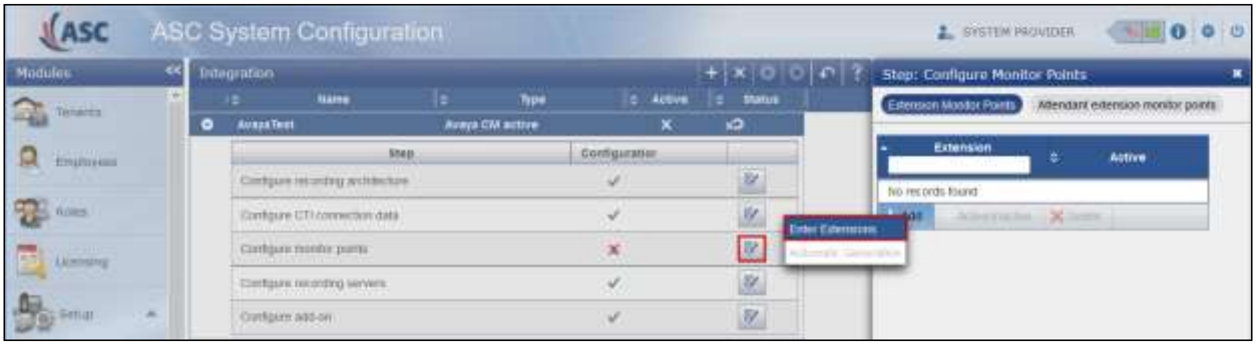
Audio codec: G711A
Operation mode: Single Step Conference Mode

Softphone Extension
6270030
6270031
6270032
6270033
6270034
6270035

☑ Activate password
Password *: ****

7.4.2. Configure monitor points

Click on the edit icon next to **Configure monitor points**. Click on **+Add** in the right window, this brings up a new mini-window next to it where **Enter Extensions** is selected.

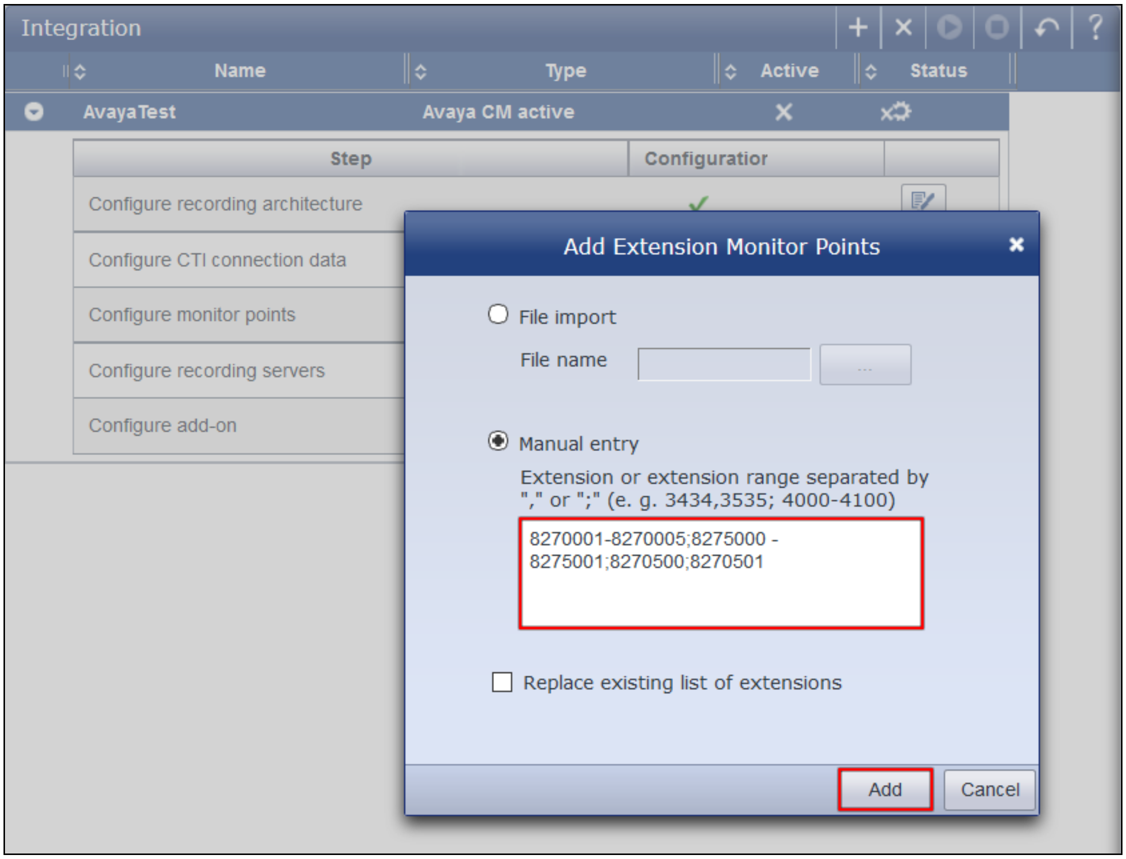


Name	Type	Active	Status
AvayaTest	Avaya CM active	✕	

Step	Configuration
Configure recording architecture	✓
Configure CTI connection data	✓
Configure monitor points	✗
Configure recording servers	✓
Configure add-on	✓

Extension	Active
No records found	

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



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	

Add Extension Monitor Points

○ File import

File name

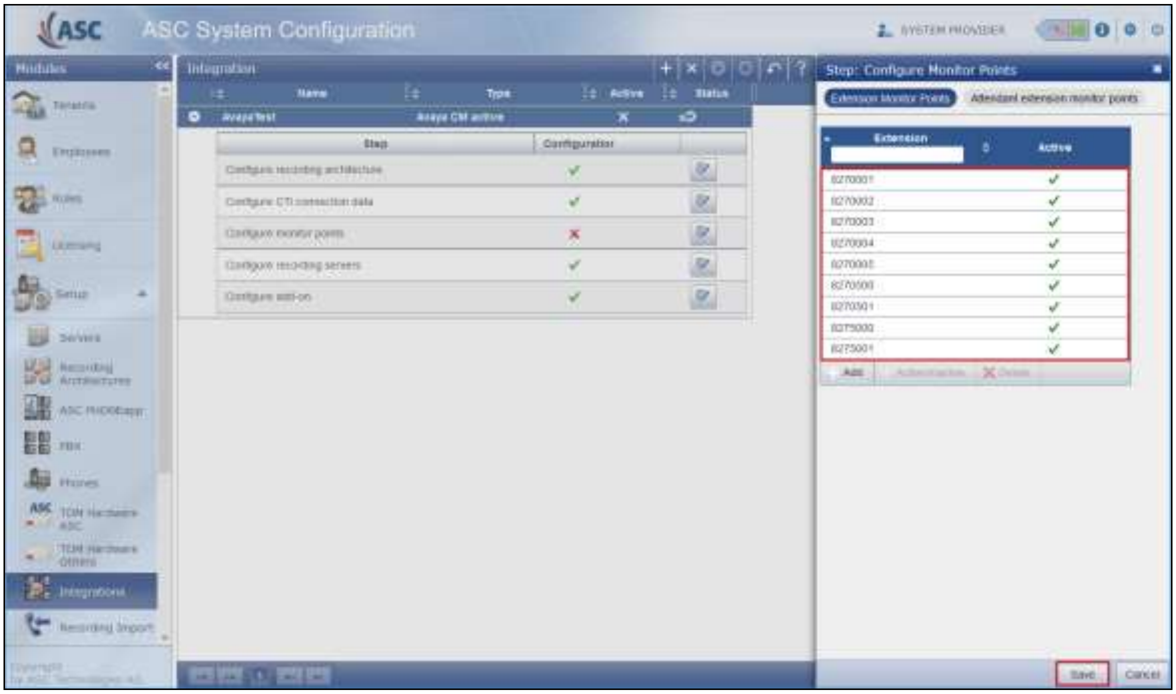
● Manual entry

Extension or extension range separated by "," or ";" (e. g. 3434,3535; 4000-4100)

8270001-8270005;8275000 - 8275001;8270500;8270501

□ Replace existing list of extensions

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

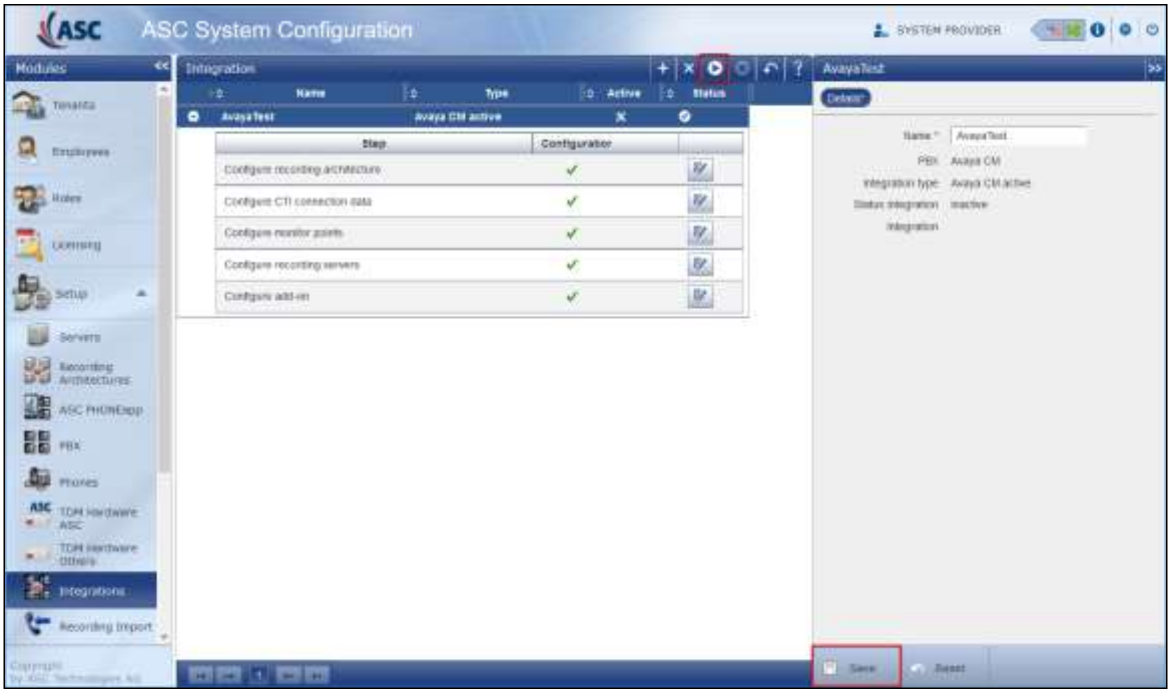


Name	Type	Active	Status
AvayaTest	Avaya CM active	✗	

Step	Configuration
Configure recording architecture	✓
Configure CTI connection data	✓
Configure monitor points	✗
Configure recording servers	✓
Configure add-on	✓

Extension	Active
8270001	✓
8270002	✓
8270003	✓
8270004	✓
8270005	✓
8270500	✓
8270501	✓
8275000	✓
8275001	✓

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



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	✓

Name *: AvayaTest
PBX: Avaya CM
Integration type: Avaya CM active
Status integration: inactive
Integration

8. Verification Steps

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

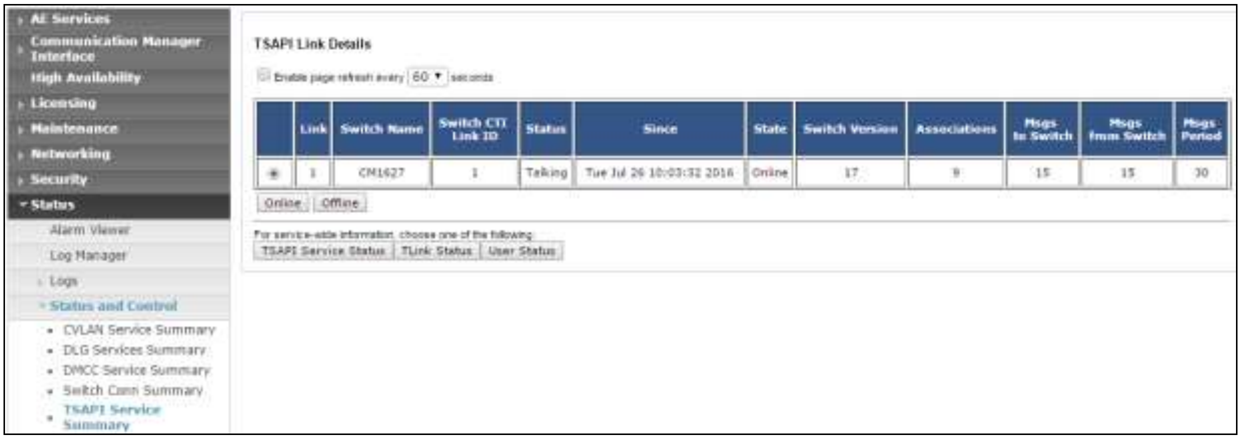
```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

CTI   Version     Mnt   AE Services      Service       Msgs     Msgs
Link              Busy     Server         State        Sent     Rcvd

1         4       no      aes71624       established   18       18
```

8.2. Verify TSAPI Link and DMCC

This section will verify both the TAPI and DMCC links between the AES and Communication Manager.

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**.



TSAPI Link Details

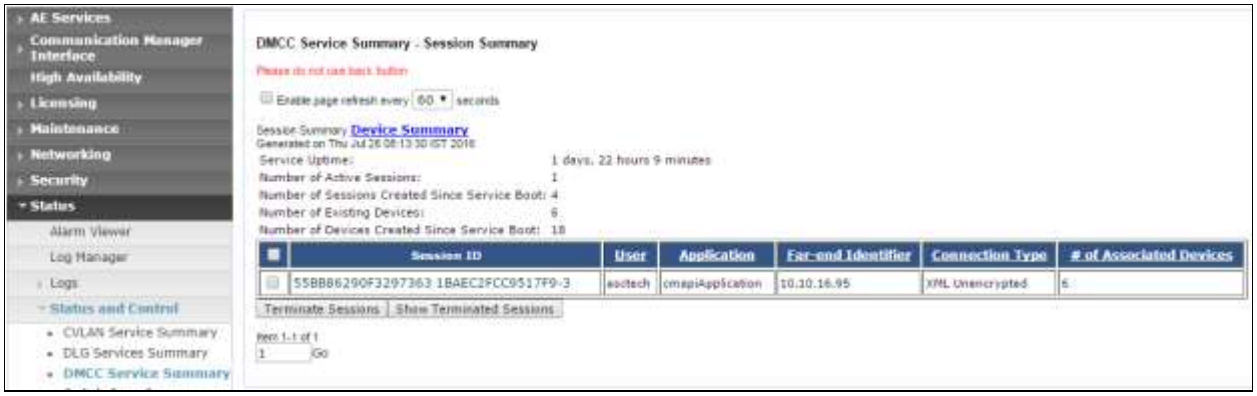
□ Enable page refresh every 60 ▾ seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
●	1	CM1627	1	Talking	Tue Jul 26 10:03:32 2016	Online	17	9	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 **10.10.16.95**. The **Application** is shown as **cmapiApplication,** and the **Far-end Identifier** is given as the IP address **10.10.16.95** as expected. The **User** is shown as the user created for the CTI user for ASC Server.



DMCC Service Summary - Session Summary

Please do not use back button

□ Enable page refresh every 60 ▾ seconds

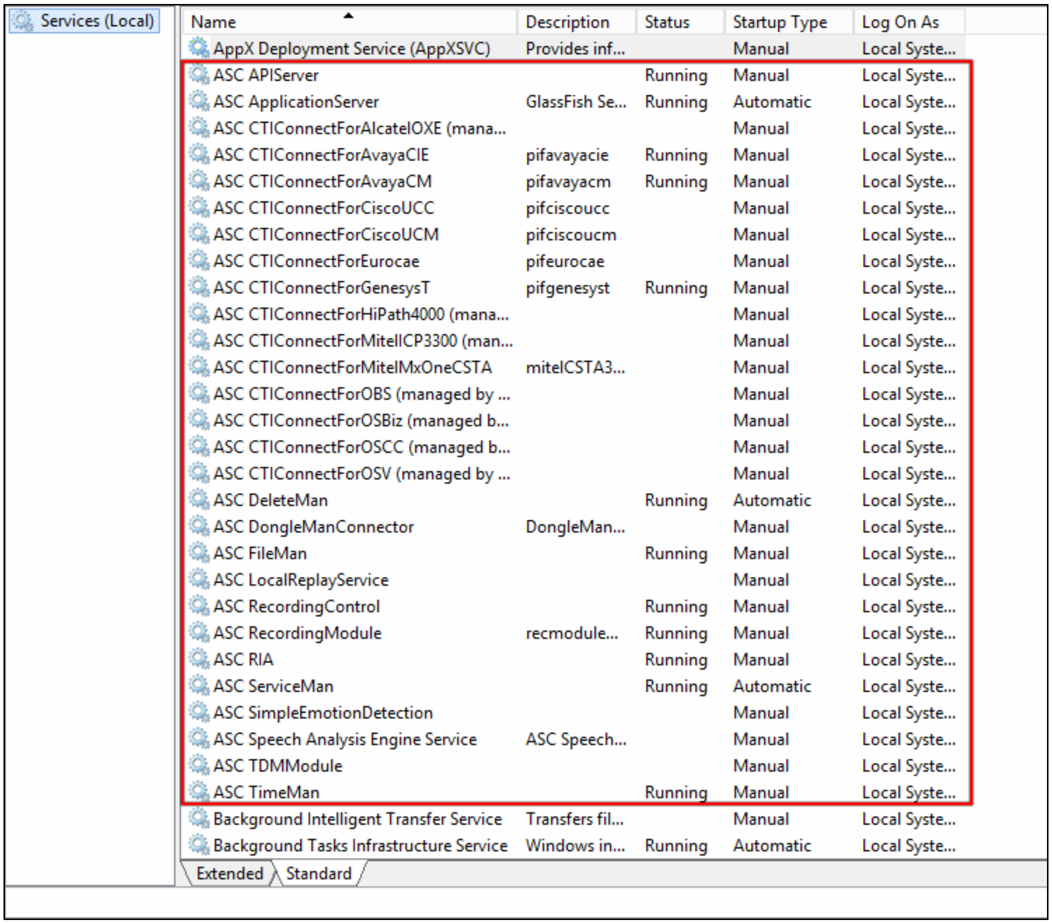
Session Summary Device Summary
Generated on Thu Jul 28 08:13:30 IST 2016

Service Uptime:	1 days, 22 hours 9 minutes
Number of Active Sessions:	1
Number of Sessions Created Since Service Boot:	4
Number of Existing Devices:	6
Number of Devices Created Since Service Boot:	18

■	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
□	55BB8629OF3297363 1BAEC2FCC9517F9-3	asctech	cmapiApplication	10.10.16.95	XML Unencrypted	6

8.3. Verify ASC EVOIPneo active 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.

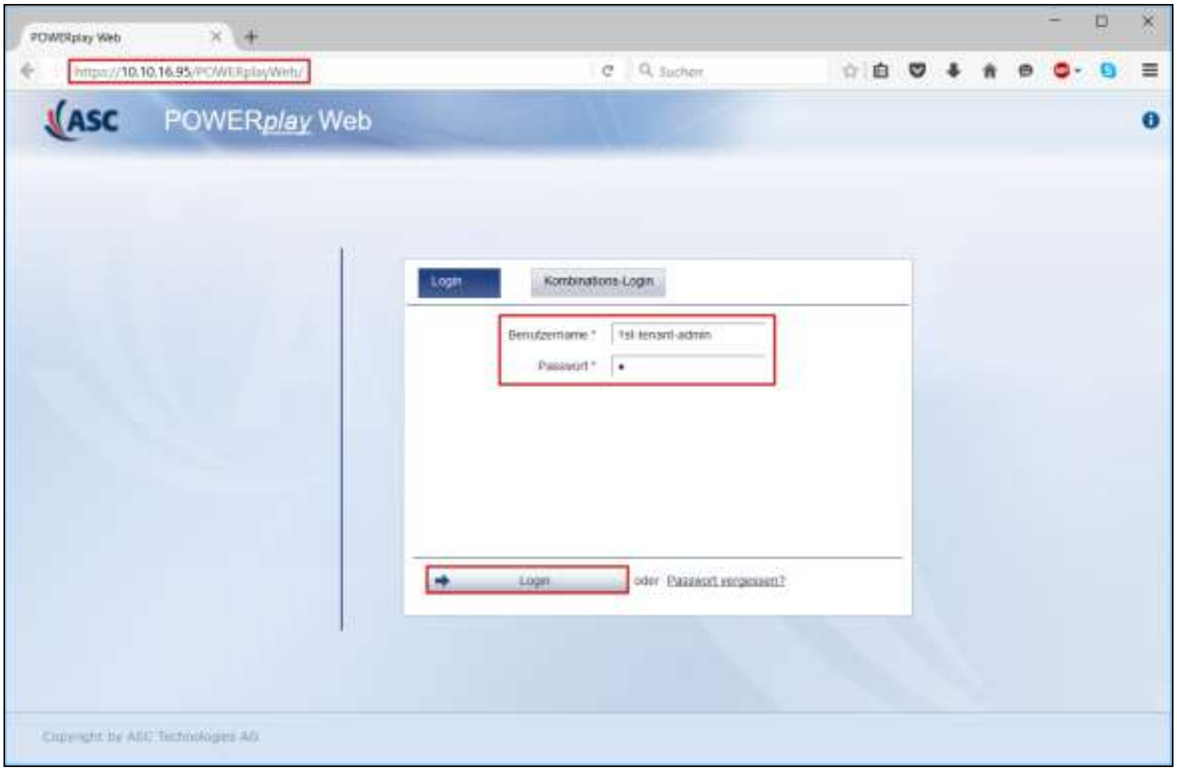


Name	Description	Status	Startup Type	Log On As
AppX Deployment Service (AppXSVC)	Provides inf...		Manual	Local Syste...
ASC APIServer		Running	Manual	Local Syste...
ASC ApplicationServer	GlassFish Se...	Running	Automatic	Local Syste...
ASC CTIConnectForAlcatelOXE (mana...			Manual	Local Syste...
ASC CTIConnectForAvayaCIE	pifavayacie	Running	Manual	Local Syste...
ASC CTIConnectForAvayaCM	pifavayacm	Running	Manual	Local Syste...
ASC CTIConnectForCiscoUCC	pifciscoucc		Manual	Local Syste...
ASC CTIConnectForCiscoUCM	pifciscoucm		Manual	Local Syste...
ASC CTIConnectForEurocae	pifeurocae		Manual	Local Syste...
ASC CTIConnectForGenesysT	pifgenesyst	Running	Manual	Local Syste...
ASC CTIConnectForHiPath4000 (mana...			Manual	Local Syste...
ASC CTIConnectForMitelICP3300 (man...			Manual	Local Syste...
ASC CTIConnectForMitelMxOneCSTA	mitelCSTA3...		Manual	Local Syste...
ASC CTIConnectForOBS (managed by ...			Manual	Local Syste...
ASC CTIConnectForOSBiz (managed b...			Manual	Local Syste...
ASC CTIConnectForOSCC (managed b...			Manual	Local Syste...
ASC CTIConnectForOSV (managed by ...			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 SimpleEmotionDetection			Manual	Local Syste...
ASC Speech Analysis Engine Service	ASC Speech...		Manual	Local Syste...
ASC TDMModule			Manual	Local Syste...
ASC TimeMan		Running	Manual	Local Syste...
Background Intelligent Transfer Service	Transfers fil...		Manual	Local Syste...
Background Tasks Infrastructure Service	Windows in...	Running	Automatic	Local Syste...

8.4. Verify ASC EVOIPneo active 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>/POWERplayWeb/.**
Enter the proper username and password and click on Login.

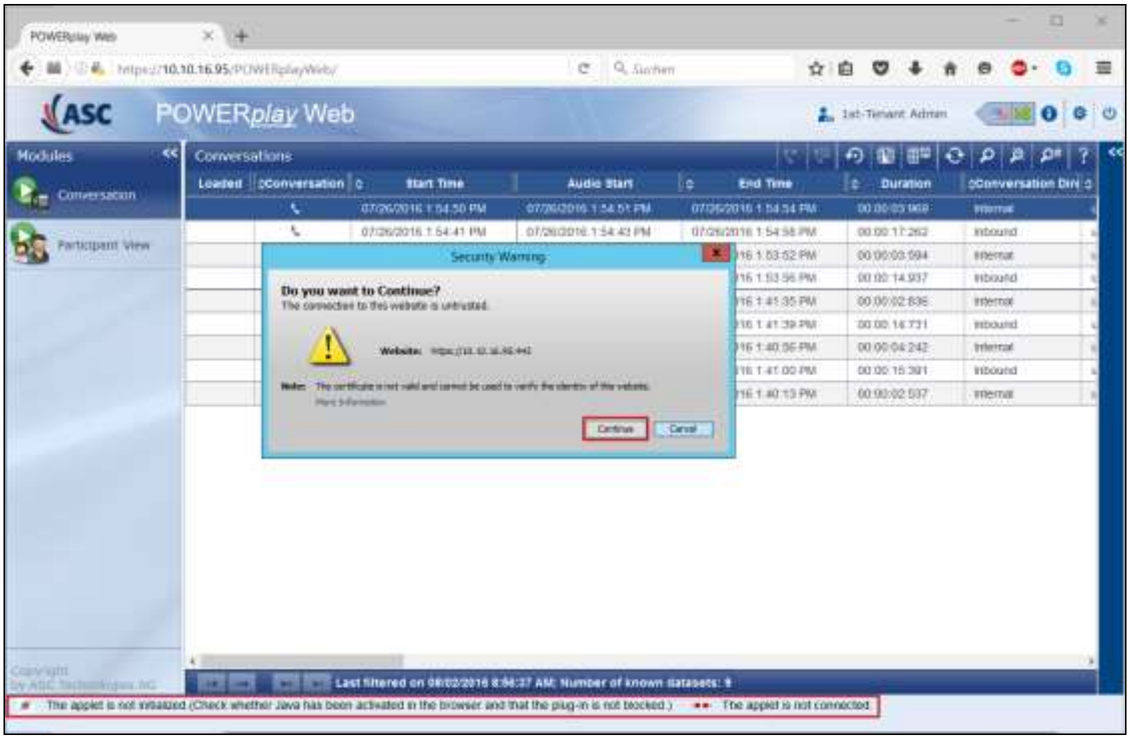


https://10.10.16.95/POWERplayWeb/

Benutzername * 1sl-tenant-admin

Passwort * •

The following screen appears. A window may open such as below if the site is untrusted, click on **Continue** and the Java applet loads automatically. There may also be a message asking to activate this on the first instance, if so click on **Yes** to continue (not shown).



Loaded	Conversation	Start Time	Audio Start	End Time	Duration	Conversation Dir
	☎	07/26/2016 1:54:50 PM	07/26/2016 1:54:51 PM	07/26/2016 1:54:54 PM	00:00:03.968	Internal
	☎	07/26/2016 1:54:41 PM	07/26/2016 1:54:43 PM	07/26/2016 1:54:58 PM	00:00:17.262	Inbound
				16 1:53:52 PM	00:00:03.594	Internal
				16 1:53:56 PM	00:00:14.937	Inbound
				16 1:41:35 PM	00:00:02.836	Internal
				16 1:41:39 PM	00:00:14.731	Inbound
				16 1:40:56 PM	00:00:04.242	Internal
				16 1:41:00 PM	00:00:15.391	Inbound
				16 1:40:13 PM	00:00:02.537	Internal

Security Warning

Do you want to Continue?
The connection to this website is untrusted.

Website: https://10.10.16.95:443

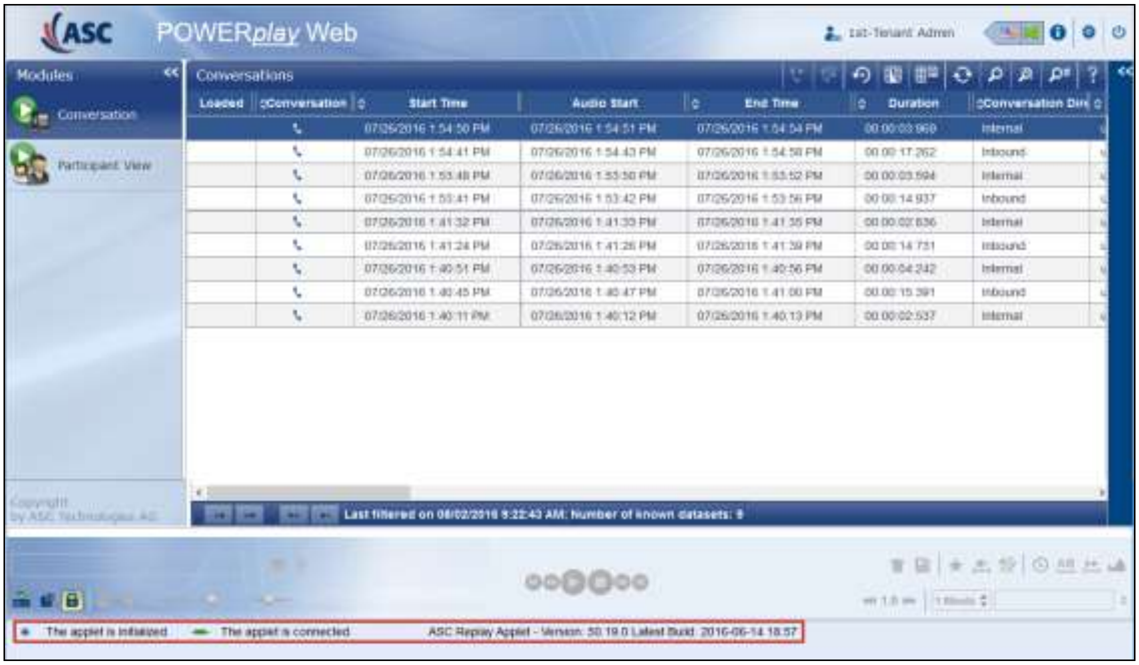
Note: The certificate is not valid and cannot be used to verify the identity of this website.
More Information

Continue Cancel

Last filtered on 08/02/2016 8:56:37 AM; Number of known datasets: 9

The applet is not initialized (Check whether Java has been activated in the browser and that the plug-in is not blocked.) The applet is not connected

Once the applet is loaded the following message will appear at the bottom of the screen. **The applet is initialized** and **The applet is connected**.

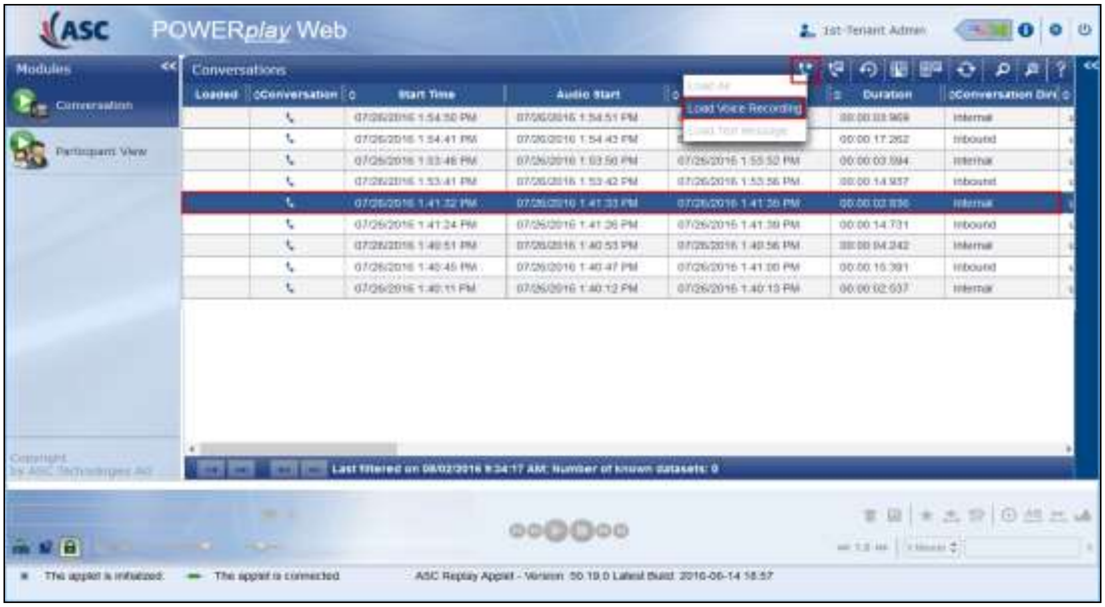


Loaded	Conversation	Start Time	Audio Start	End Time	Duration	Conversation Dir
	☎	07/26/2016 1:54:50 PM	07/26/2016 1:54:51 PM	07/26/2016 1:54:54 PM	00:00:03.968	Internal
	☎	07/26/2016 1:54:41 PM	07/26/2016 1:54:43 PM	07/26/2016 1:54:58 PM	00:00:17.262	Inbound
	☎	07/26/2016 1:53:48 PM	07/26/2016 1:53:50 PM	07/26/2016 1:53:52 PM	00:00:03.594	Internal
	☎	07/26/2016 1:53:41 PM	07/26/2016 1:53:42 PM	07/26/2016 1:53:56 PM	00:00:14.937	Inbound
	☎	07/26/2016 1:41:32 PM	07/26/2016 1:41:33 PM	07/26/2016 1:41:35 PM	00:00:02.836	Internal
	☎	07/26/2016 1:41:24 PM	07/26/2016 1:41:26 PM	07/26/2016 1:41:39 PM	00:00:14.731	Inbound
	☎	07/26/2016 1:40:51 PM	07/26/2016 1:40:53 PM	07/26/2016 1:40:56 PM	00:00:04.242	Internal
	☎	07/26/2016 1:40:45 PM	07/26/2016 1:40:47 PM	07/26/2016 1:41:00 PM	00:00:15.391	Inbound
	☎	07/26/2016 1:40:11 PM	07/26/2016 1:40:12 PM	07/26/2016 1:40:13 PM	00:00:02.537	Internal

Last filtered on 08/02/2016 9:22:43 AM; Number of known datasets: 9

The applet is initialized The applet is connected ASC Replay Applet - Version: 50.19.0 Latest Build: 2016-06-14 18:57

Select the recording to be played back. Right click on the icon highlighted at the top of the screen and select **Load Voice Recording**.

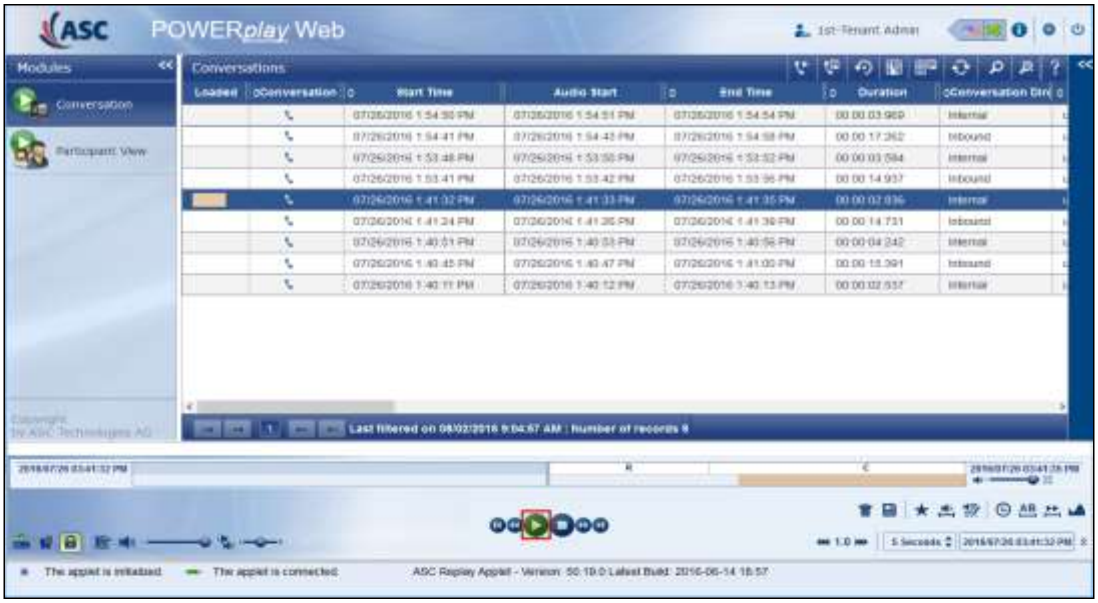


Loaded	Conversation	Start Time	Audio Start		Duration	Conversation Dir
	☎	07/26/2016 1:54:50 PM	07/26/2016 1:54:51 PM		00:00:03.969	Internal
	☎	07/26/2016 1:54:41 PM	07/26/2016 1:54:43 PM		00:00:17.262	Inbound
	☎	07/26/2016 1:53:48 PM	07/26/2016 1:53:50 PM	07/26/2016 1:53:52 PM	00:00:03.594	Internal
	☎	07/26/2016 1:53:41 PM	07/26/2016 1:53:42 PM	07/26/2016 1:53:56 PM	00:00:14.937	Inbound
	☎	07/26/2016 1:41:32 PM	07/26/2016 1:41:33 PM	07/26/2016 1:41:35 PM	00:00:02.836	Internal
	☎	07/26/2016 1:41:24 PM	07/26/2016 1:41:26 PM	07/26/2016 1:41:39 PM	00:00:14.731	Inbound
	☎	07/26/2016 1:40:51 PM	07/26/2016 1:40:53 PM	07/26/2016 1:40:56 PM	00:00:04.242	Internal
	☎	07/26/2016 1:40:45 PM	07/26/2016 1:40:47 PM	07/26/2016 1:41:00 PM	00:00:15.391	Inbound
	☎	07/26/2016 1:40:11 PM	07/26/2016 1:40:12 PM	07/26/2016 1:40:13 PM	00:00:02.537	Internal

Last filtered on 08/02/2016 9:34:17 AM: Number of known datasets: 0

The applet is initialized. The applet is connected. ASC Replay Applet - Version: 50.19.0 Latest Build: 2016-06-14 18:57

Click on the Play icon at the bottom of the screen to play back the recording.



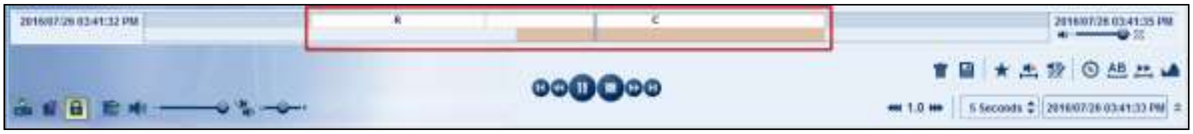
Loaded	Conversation	Start Time	Audio Start	End Time	Duration	Conversation Dir
	☎	07/26/2016 1:54:50 PM	07/26/2016 1:54:51 PM	07/26/2016 1:54:54 PM	00:00:03.969	Internal
	☎	07/26/2016 1:54:41 PM	07/26/2016 1:54:43 PM	07/26/2016 1:54:58 PM	00:00:17.262	Inbound
	☎	07/26/2016 1:53:48 PM	07/26/2016 1:53:50 PM	07/26/2016 1:53:52 PM	00:00:03.594	Internal
	☎	07/26/2016 1:53:41 PM	07/26/2016 1:53:42 PM	07/26/2016 1:53:56 PM	00:00:14.937	Inbound
	☎	07/26/2016 1:41:32 PM	07/26/2016 1:41:33 PM	07/26/2016 1:41:35 PM	00:00:02.836	Internal
	☎	07/26/2016 1:41:24 PM	07/26/2016 1:41:26 PM	07/26/2016 1:41:39 PM	00:00:14.731	Inbound
	☎	07/26/2016 1:40:51 PM	07/26/2016 1:40:53 PM	07/26/2016 1:40:56 PM	00:00:04.242	Internal
	☎	07/26/2016 1:40:45 PM	07/26/2016 1:40:47 PM	07/26/2016 1:41:00 PM	00:00:15.391	Inbound
	☎	07/26/2016 1:40:11 PM	07/26/2016 1:40:12 PM	07/26/2016 1:40:13 PM	00:00:02.537	Internal

Last filtered on 08/02/2016 9:04:57 AM : Number of records 9

2016/07/26 03:41:32 PM 2016/07/26 03:41:35 PM 2016/07/26 03:41:32 PM

The applet is initialized. The applet is connected. ASC Replay Applet - Version: 50.19.0 Latest Build: 2016-06-14 18:57

This will play through the recording as shown below.



2016/07/26 03:41:32 PM 2016/07/26 03:41:35 PM 2016/07/26 03:41:33 PM

9. Conclusion

These Application Notes describe the configuration steps required for ASC EVOIPneo active V5.0 from ASC Technologies AG to successfully interoperate with Avaya Aura® Communication Manager R7.0 using Avaya Aura® Application Enablement Services R7.0. All feature functionality and serviceability test cases were completed successfully, with any issues and observations noted in **Section 2.2**.

10. Additional References

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

Product documentation for Avaya products may be found at *https://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 7.0*

Product documentation for ASC Technologies AG can be obtained as follows:

Email:	hq@asctechnologies.com
Website:	www.asctechnologies.com
Phone:	+49 6021 5001-0

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.