Avaya Solution & Interoperability Test Lab

Application Notes for configuring ASC EVOIPneo active V6.0 from ASC Technologies AG to interoperate with Avaya Aura® Communication Manager R8.0 and Avaya Aura® Application Enablement Services R8.0 - 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 V6.0 from ASC Technologies AG with Avaya Aura® Communication Manager R8.0 and Avaya Aura® Application Enablement Services R8.0 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.

DMCC works by allowing software vendors to create soft phones, in memory on a recording server, and use them to monitor and record other phones. This is purely a software solution and does not require telephony boards or any wiring beyond a typical network infrastructure

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 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.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Avaya systems and ASC EVOIPneo did not include use of any specific encryption features. ASC EVOIPneo can connect to the Avaya system using a secure connection, but this was not used on this occasion.

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/Outbound calls** – Test call recording for inbound and outbound calls to the Communication Manager to and from PSTN callers
- **Hold/Transferred/Conference calls** – Test call recording for calls transferred to and in conference with PSTN callers.
- **EC500 Calls/Forwarded calls** - Test call recording for calls terminated on Avaya DECT handsets using EC500.
- **Feature calls** - Test call recording for calls that are parked or picked up using Call Park and Call Pickup.
- **Calls to Elite Agents** – Test call recording for calls to Communication Manager agents logged into one-X® Agent.
- **Serviceability testing** - The behavior of ASC EVOIPneo under different simulated failure conditions.

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. The following observations were noted.

1. Blind Conference from PSTN calling into H323 conferencing in another H323 or SIP the AES is sending duplicate conference events. ASC can work around this issue and Avaya are investigating this scenario.
2. An issue was observed with Call Park as the second leg of the un-parked call was not being recorded if a feature access code is used to park the call. If a call park button is used, then there is no issue. ASC were able to implement a work around for this and Avaya are investigating the issue.

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 G450 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.

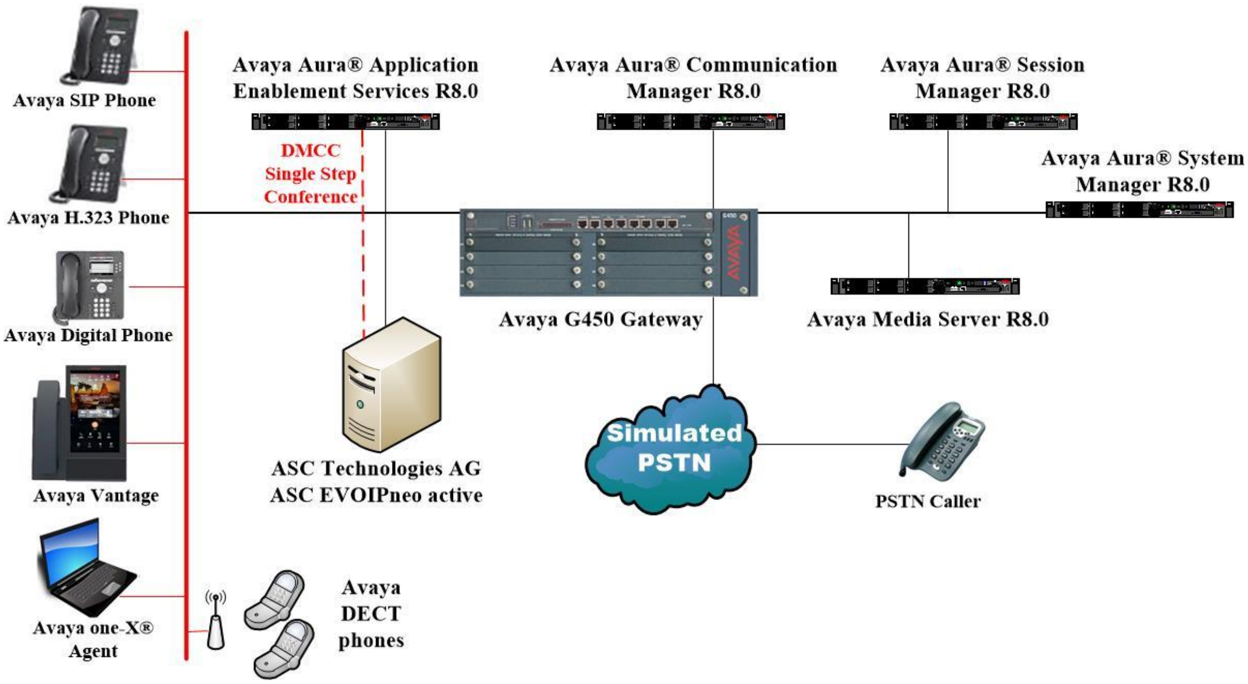

Avaya SIP Phone
Avaya H.323 Phone
Avaya Digital Phone
Avaya Vantage
Avaya one-X® Agent
Avaya DECT phones
Avaya Aura® Application Enablement Services R8.0
DMCC Single Step Conference
Avaya Aura® Communication Manager R8.0
Avaya Aura® Session Manager R8.0
Avaya Aura® System Manager R8.0
Avaya G450 Gateway
Avaya Media Server R8.0
ASC Technologies AG ASC EVOIPneo active
Simulated PSTN
PSTN Caller

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 Virtual Server	System Manager 8.0.1.0 Build No. – 8.0.0.0.931077 Software Update Revision No: 8.0.1.0.038826 Feature Pack 1
Avaya Aura® Session Manager running on Virtual Server	Session Manager R8.0 FP1 Build No. – 8.0.1.0.801007
Avaya Aura® Communication Manager running on Virtual Server	R018x.00.0.822.0 R8.0.1.0.0 – FP1 Update ID 00.0.822.0-25031
Avaya Aura® Application Enablement Services running on Virtual Server	R8.0 Build No – 8.0.0.0.0.6-0
Avaya G450 Gateway	41.10.1 /1
Avaya Media Server running on a Virtual Server	R8.0.0.150
Avaya 9608 H323 Deskphone	96x1 H323 Release 6.6.115
Avaya 1616-I H323 Deskphone	Ha1616ua1_3110A
Avaya J179 H323 Deskphone	96x1 H323 Release 6.7.002U
Avaya 9641 SIP Deskphone	96x1 SIP Release 7.1.2.0.14
Avaya J129 SIP Deskphone	SIP 1.0.0.0.0.43
Avaya Vantage Equinox	1.0.0.2
Avaya 9408 Digital Deskphone	2.0
Avaya one-X® Agent	R2.5.8
Avaya DECT Handsets	3725 DH4 (R3.3.11) 3720 DH3 (R3.3.11)
ASC EVOIPneo active running on MS Windows Server 2016	V6.0
ASC POWERplay Pro running on MS Windows Client	V6.0

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 **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. Note procr IP Address for Avaya Aura® Application Enablement Services Connectivity

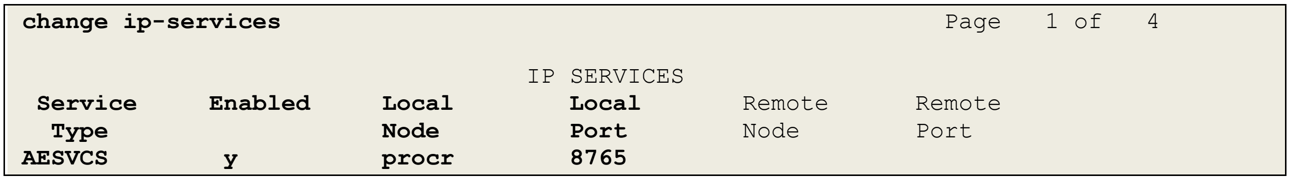
Display the procr IP address by using the command **display node-names ip** and note the IP address for the **procr** and AES (**aes80vmpg**).

```
display node-names ip                                           Page   1 of   2
                                IP NODE NAMES
    Name              IP Address
SM100               10.10.40.34
aes80vmpg           10.10.40.56
default             0.0.0.0
g450                10.10.40.15
procr               10.10.40.59
```

5.3. Configure Transport Link 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**.

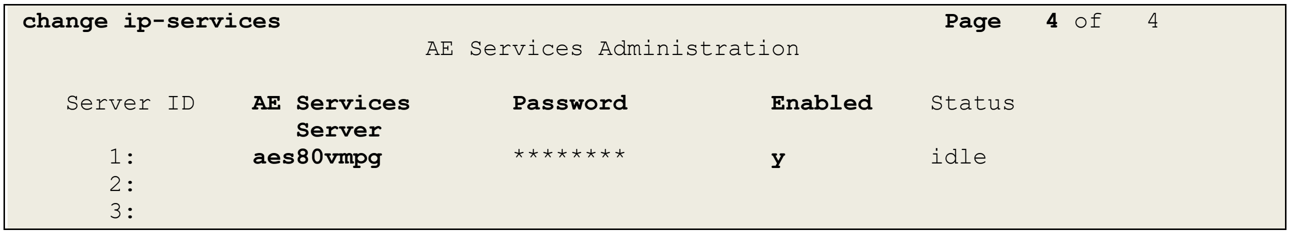


```
change ip-services                                              Page   1 of   4

                                   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 **aes80vmpg**.
- **Password:** Enter a password to be administered on the AES server.
- **Enabled:** Set to **y**.

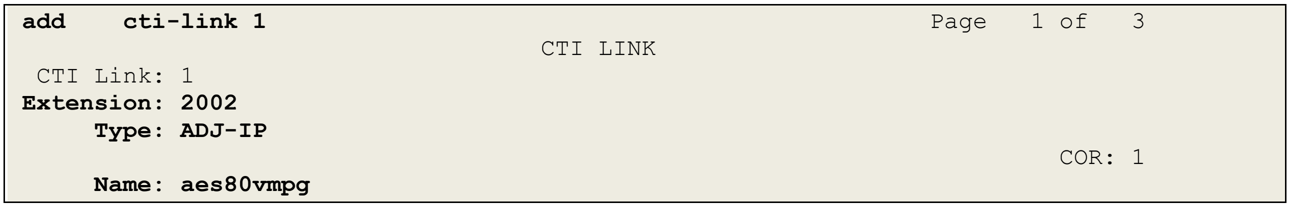
Note: The password entered for **Password** field must match the password on the AES server in **Section 6.2**. The **AE Services Server** should match the administered name for the AES server; this is created as part of the AES installation, and can be obtained from the AES server by typing **uname –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:        aes80vmpg         ********          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: aes80vmpg
```

5.5. Configure H323 Stations for Single Step Conference

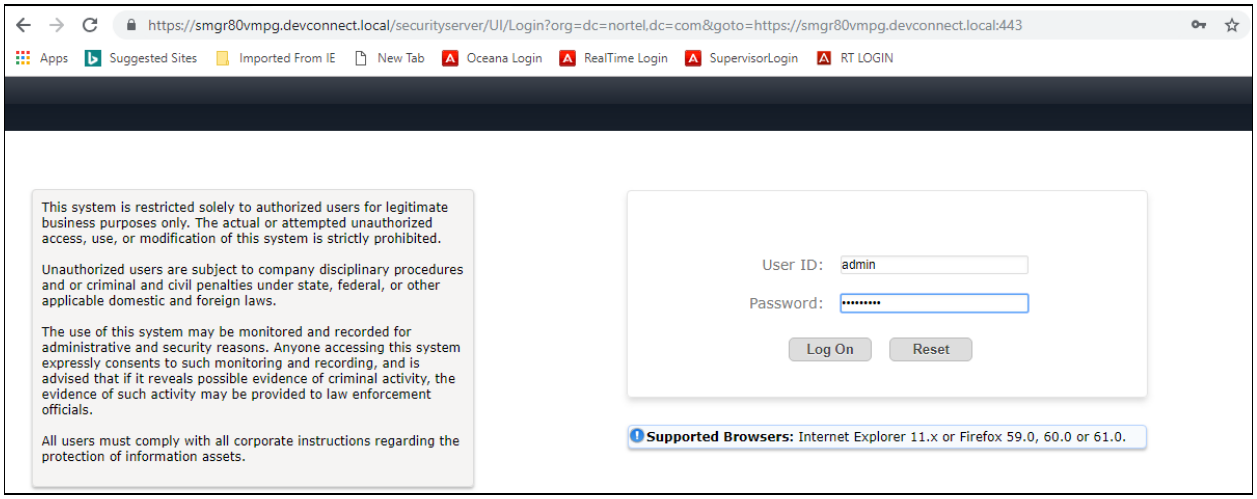
No changes were made during compliance testing for and H.323 stations that were tested. The screen below shows an example of a H.323 phone that was tested.

```
diaplay station 2000                                            Page   1 of   6
                                     STATION

Extension: 2000                             Lock Messages? n            BCC: 0
     Type: 9608                           Security Code: 1234         TN: 1
     Port: S00101                         Coverage Path 1:            COR: 1
     Name: H323 2000                      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: 2000
            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? n

                                                   IP Video Softphone? n
                                 Short/Prefixed Registration Allowed: default
```

5.6. Configure SIP Stations for Single Step Conference

Any SIP extension that is to be recorded requires some configuration changes to allow call recording using service observation. Changes of SIP phones on Communication Manager must be carried out from System Manager. Access the System Manager using a web browser by entering **http://<FQDN >/SMGR**, where **<FQDN>** is the fully qualified domain name of System Manager or **http://<IP Address >/SMGR**. Log in using appropriate credentials.

Note: The following shows changes a SIP extension and assumes that the SIP extension has been programmed correctly and is fully functioning.


https://smgr80vmpg.devconnect.local/securityserver/UI/Login?org=dc=nortel,dc=com&goto=https://smgr80vmpg.devconnect.local:443
Apps
Suggested Sites
Imported From IE
New Tab
Oceana Login
RealTime Login
SupervisorLogin
RT LOGIN

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

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

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

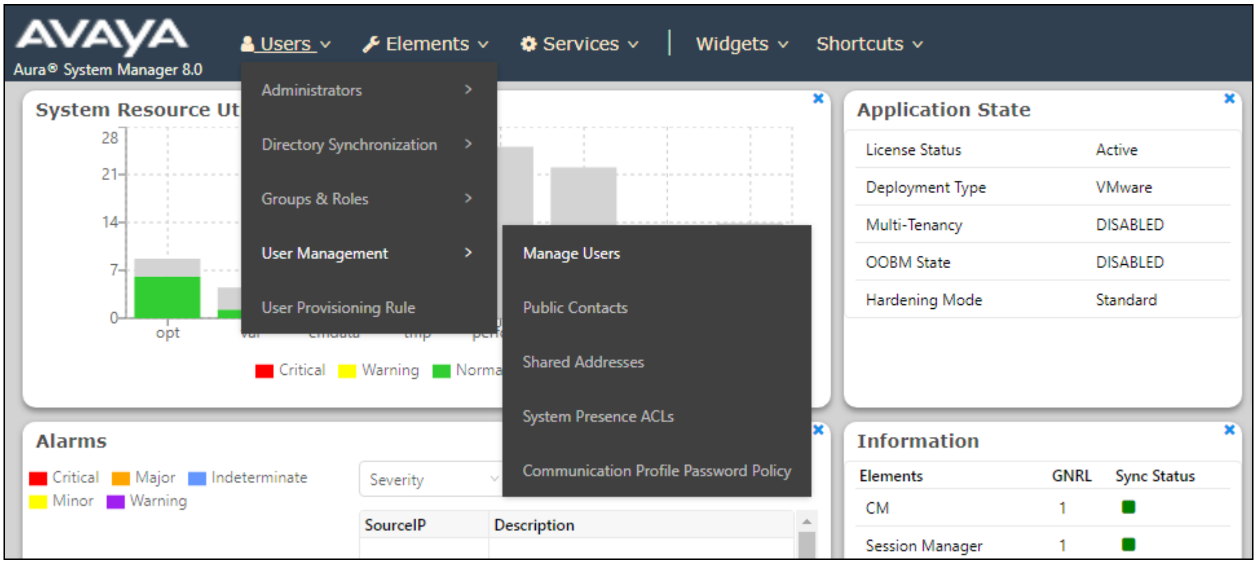
All users must comply with all corporate instructions regarding the protection of information assets.

User ID: admin

Password: ••••••••

Supported Browsers: Internet Explorer 11.x or Firefox 59.0, 60.0 or 61.0.

From the home page click on **Users → User Management → Manage Users** as highlighted below.



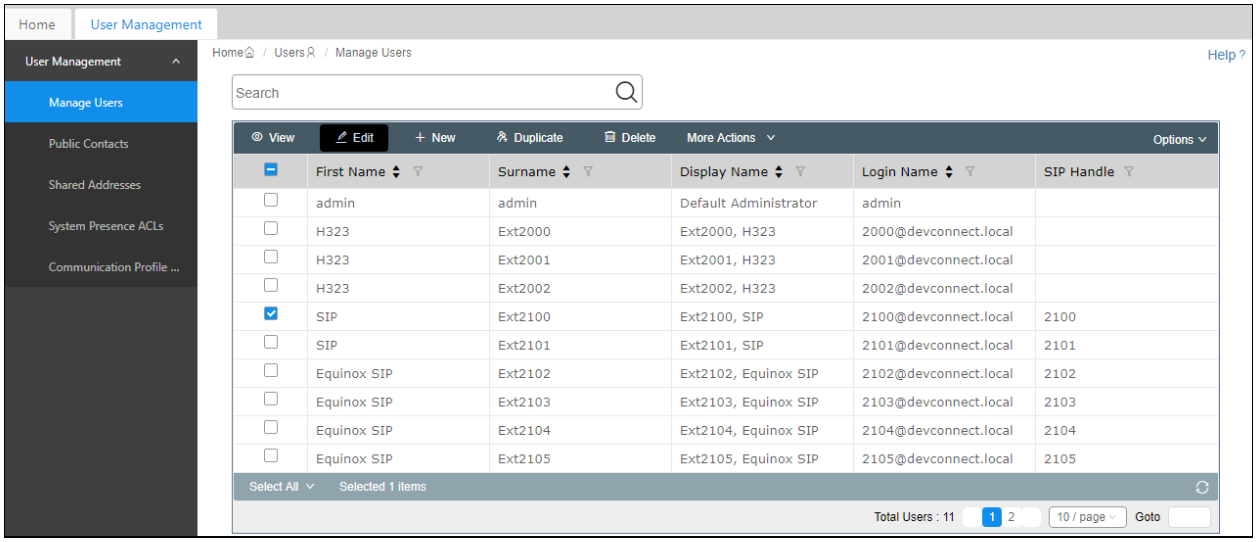
Application State

License Status	Active
Deployment Type	VMware
Multi-Tenancy	DISABLED
OOBM State	DISABLED
Hardening Mode	Standard

Information

Elements	GNRL	Sync Status
CM	1	🟩
Session Manager	1	🟩

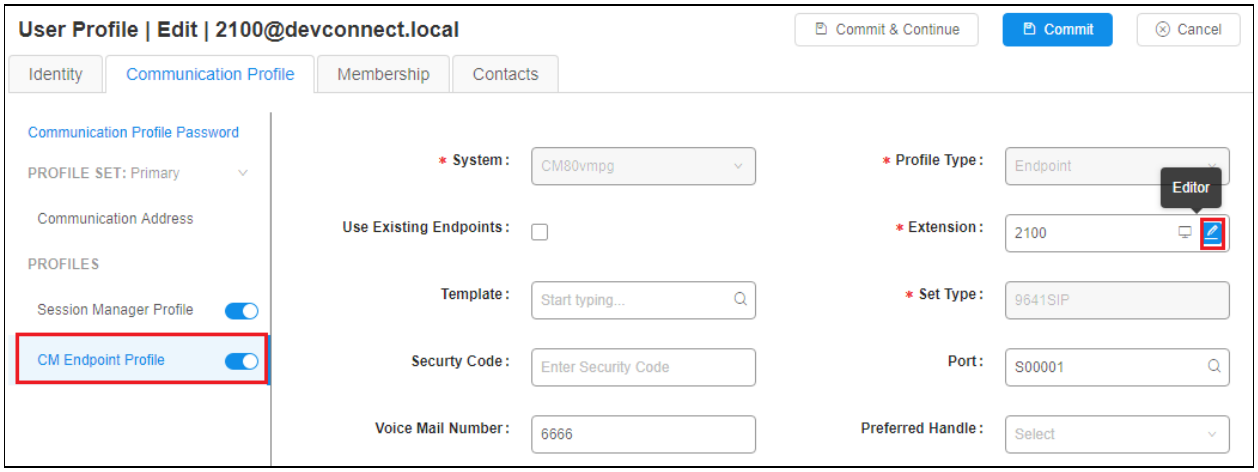
Select the station to be edited and click on **Edit**. The example below shows that SIP extension **2100** is selected.



	First Name	Surname	Display Name	Login Name	SIP Handle
☐	admin	admin	Default Administrator	admin	
☐	H323	Ext2000	Ext2000, H323	2000@devconnect.local	
☐	H323	Ext2001	Ext2001, H323	2001@devconnect.local	
☐	H323	Ext2002	Ext2002, H323	2002@devconnect.local	
☑	SIP	Ext2100	Ext2100, SIP	2100@devconnect.local	2100
☐	SIP	Ext2101	Ext2101, SIP	2101@devconnect.local	2101
☐	Equinox SIP	Ext2102	Ext2102, Equinox SIP	2102@devconnect.local	2102
☐	Equinox SIP	Ext2103	Ext2103, Equinox SIP	2103@devconnect.local	2103
☐	Equinox SIP	Ext2104	Ext2104, Equinox SIP	2104@devconnect.local	2104
☐	Equinox SIP	Ext2105	Ext2105, Equinox SIP	2105@devconnect.local	2105

To set the password for the SIP extension click on **Communication Profile Password** in the left window and set the password in the main window (not shown here).

Click on the **CM Endpoint Profile** in the left window. Click on the **Editor** icon in the main window.



User Profile | Edit | 2100@devconnect.local

Communication Profile Password

PROFILE SET: Primary

Communication Address

PROFILES

Session Manager Profile

CM Endpoint Profile

* System : CM80vmpg

Use Existing Endpoints : □

Template : Start typing...

Security Code : Enter Security Code

Voice Mail Number : 6666

* Profile Type : Endpoint

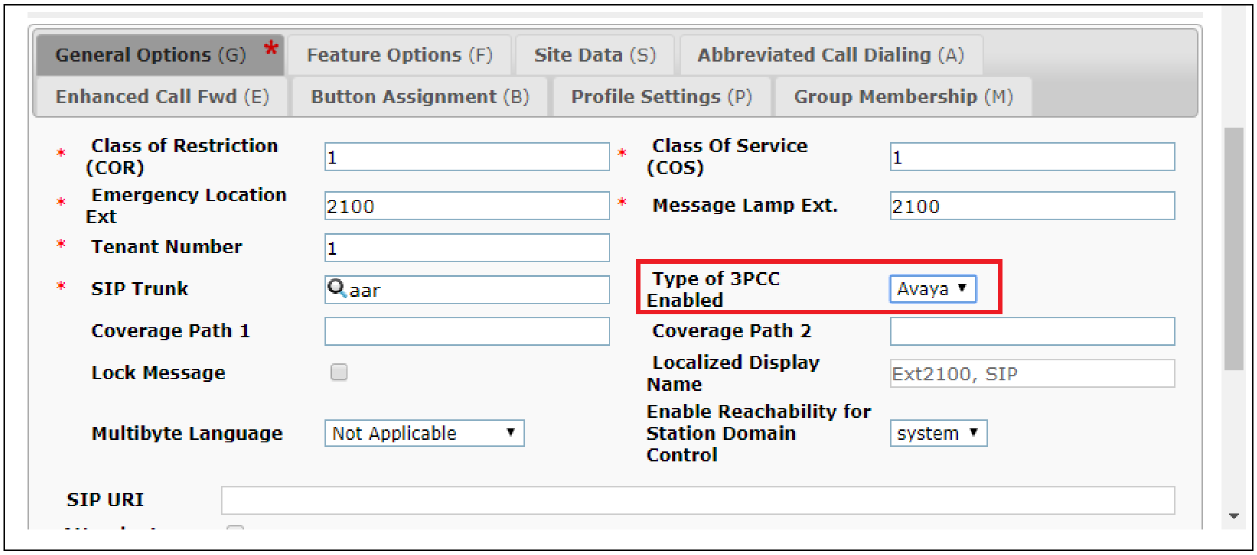
* Extension : 2100

* Set Type : 9641SIP

Port : S00001

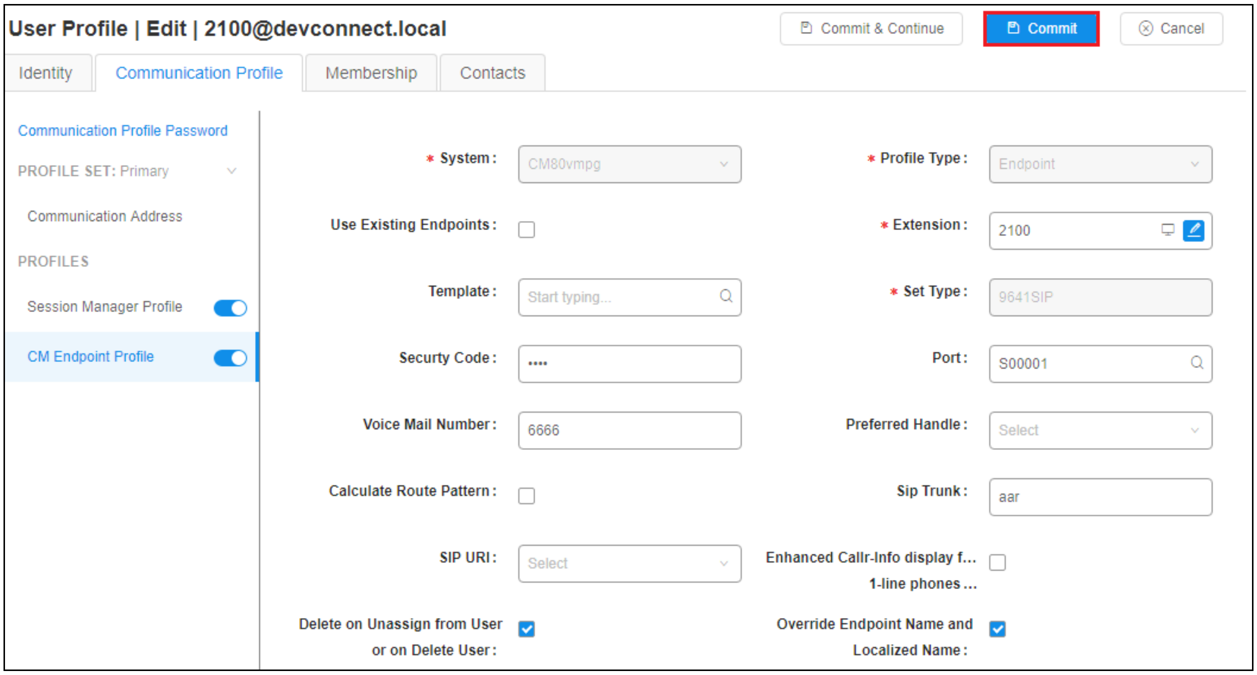
Preferred Handle : Select

Ensure that **Type of 3PCC Enabled** is set to **Avaya**. Click on the **Feature Options** tab after that. Ensure that both the **Class of Restriction (COR)** and the **Class of Service (COS)** are set correctly. Scroll up or down and click on **Done** (not shown).



* Class of Restriction (COR)	1	* Class Of Service (COS)	1
* Emergency Location Ext	2100	* Message Lamp Ext.	2100
* Tenant Number	1		
* SIP Trunk	aar	Type of 3PCC Enabled	Avaya
Coverage Path 1		Coverage Path 2	
Lock Message	□	Localized Display Name	Ext2100, SIP
Multibyte Language	Not Applicable	Enable Reachability for Station Domain Control	system
SIP URI			

Click on **Commit**, as shown.



User Profile | Edit | 2100@devconnect.local

* System : CM80vmpg

* Profile Type : Endpoint

Use Existing Endpoints : □

* Extension : 2100

Template : Start typing...

* Set Type : 9641SIP

Securty Code : ••••

Port : S00001

Voice Mail Number : 6666

Preferred Handle : Select

Calculate Route Pattern : □

Sip Trunk : aar

SIP URI : Select

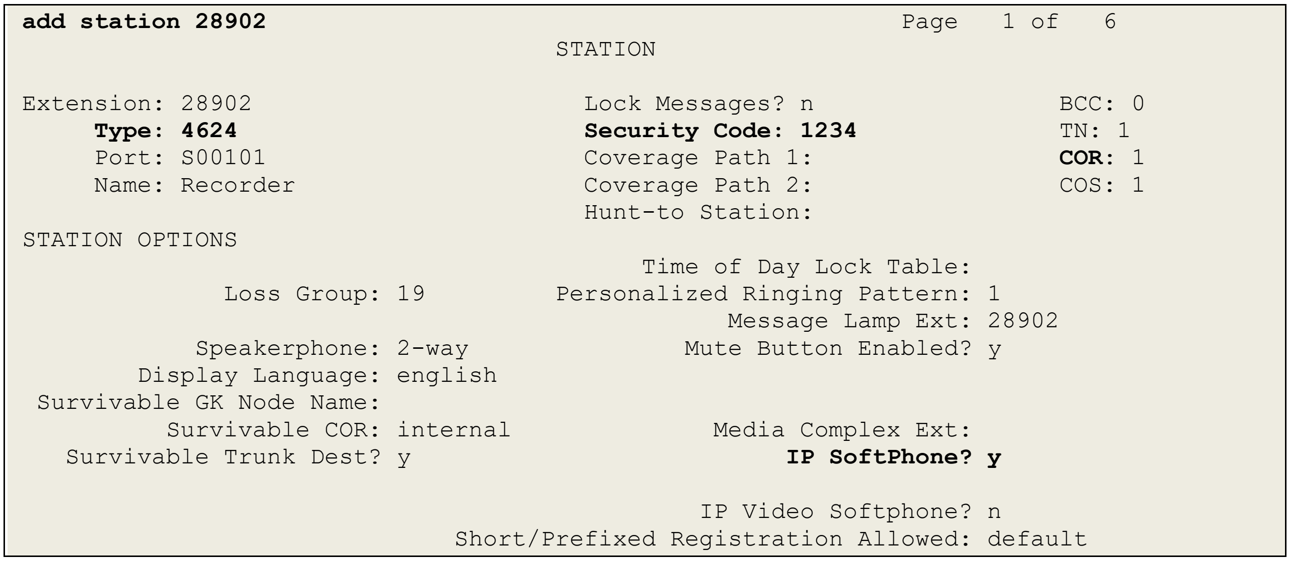
Enhanced Callr-Info display f... 1-line phones ... □

Delete on Unassign from User or on Delete User : ☑

Override Endpoint Name and Localized Name : ☑

5.7. Configure Virtual Stations for Single Step Conference

Add virtual stations to allow ASC EVOIPneo active record calls using Single Step Conference. Type **add station x** where x is the extension number of the station to be configured also note this extension number for configuration required in **Section 7.4.1**. Note the **Security Code** and ensure that **IP SoftPhone** is set to **y**.



```
add station 28902                                            Page   1 of   6
                                     STATION

Extension: 28902                       Lock Messages? n                 BCC: 0
     Type: 4624                        Security Code: 1234               TN: 1
     Port: S00101                      Coverage Path 1:                 COR: 1
     Name: Recorder                    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: 28902
            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
                              Short/Prefixed Registration Allowed: default
```

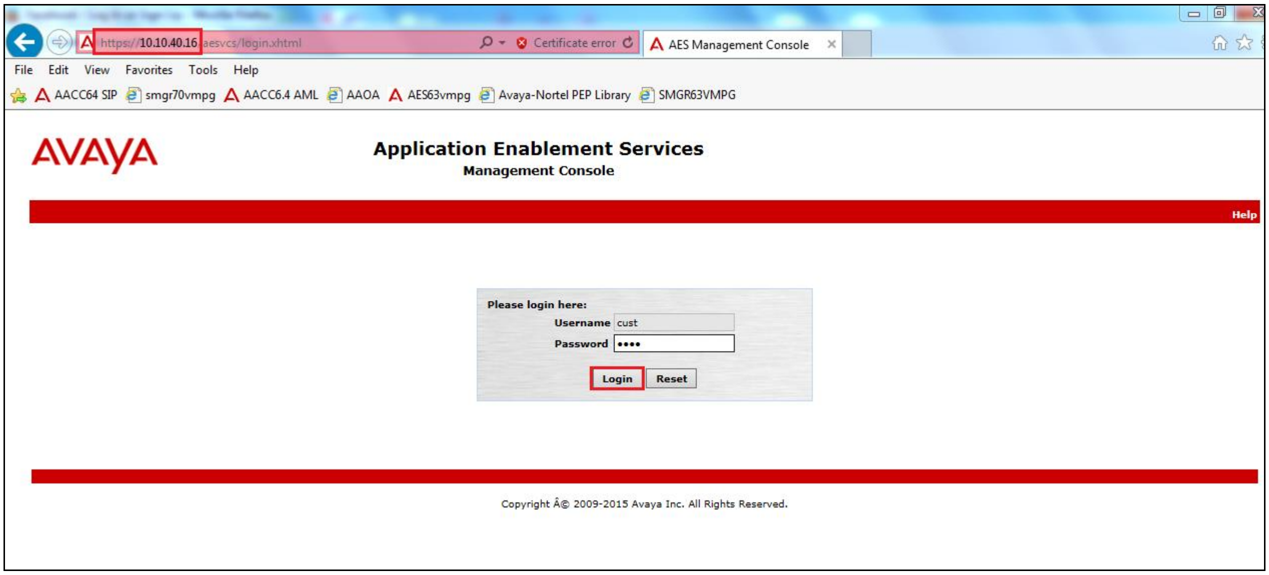
6. Configure Avaya Aura® Application Enablement Services

This section provides the procedures for configuring AES. The procedures fall into the following areas:

- Verify Licensing
- Create Switch Connection
- Administer TSAPI link
- Identify Tlinks
- Configure Networking Ports
- Create CTI User
- Configure Security Database

6.1. Verify Licensing

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



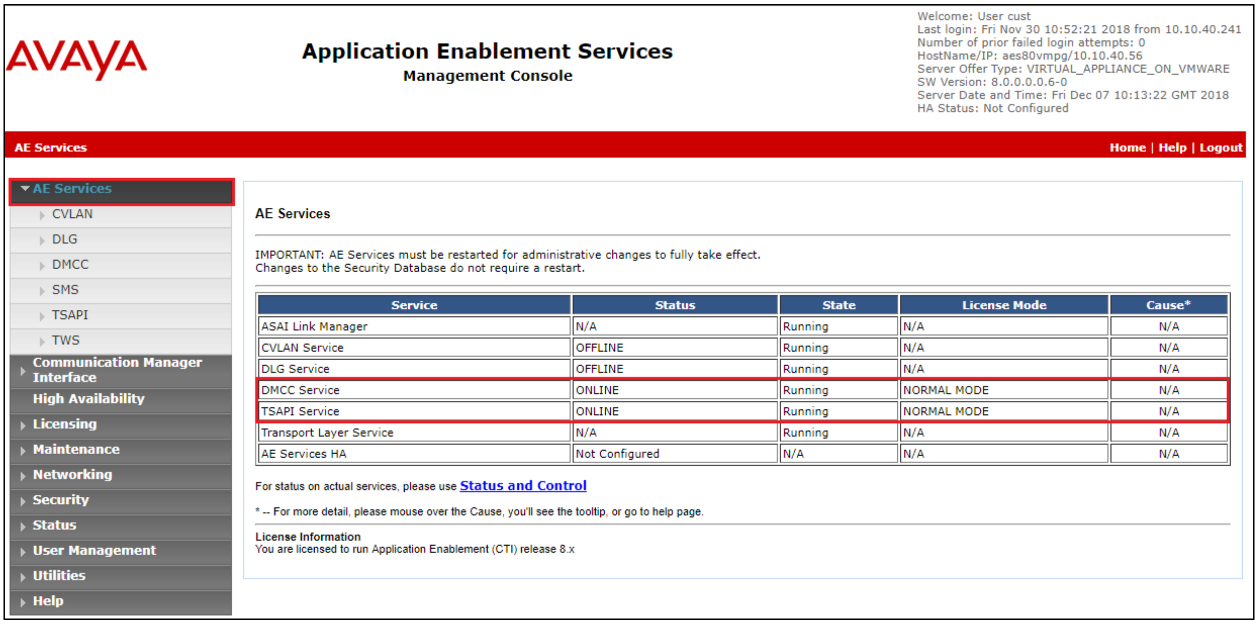
Please login here:

Username cust

Password ••••

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** and **DMCC Service** are licensed by ensuring 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: Fri Nov 30 10:52:21 2018 from 10.10.40.241
Number of prior failed login attempts: 0
HostName/IP: aes80vmpg/10.10.40.56
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.0.0.0.0.6-0
Server Date and Time: Fri Dec 07 10:13:22 GMT 2018
HA Status: Not Configured

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	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

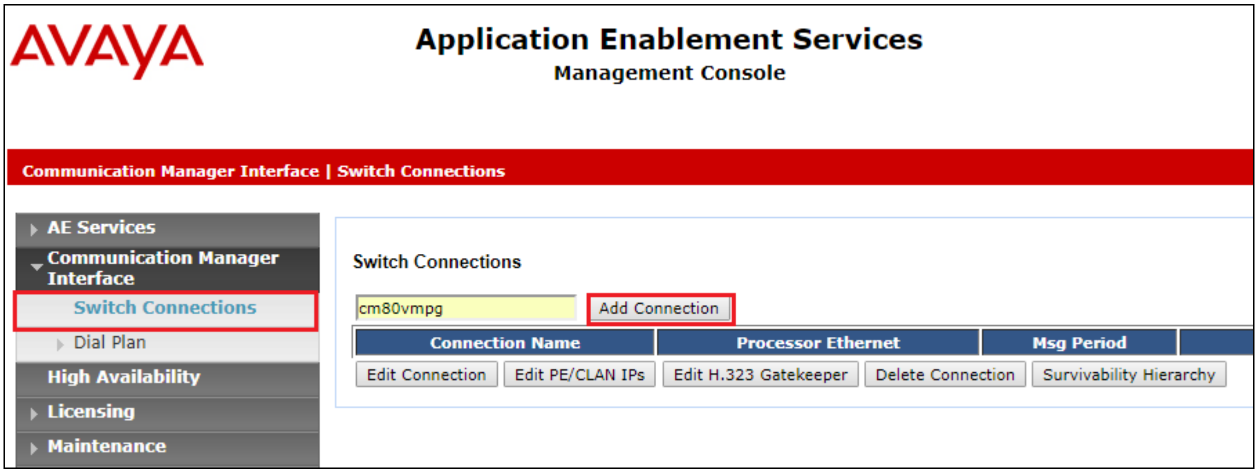
For status on actual services, please use Status and Control

* -- 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 8.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 a name for the Switch Connection to be added and click the **Add Connection** button.

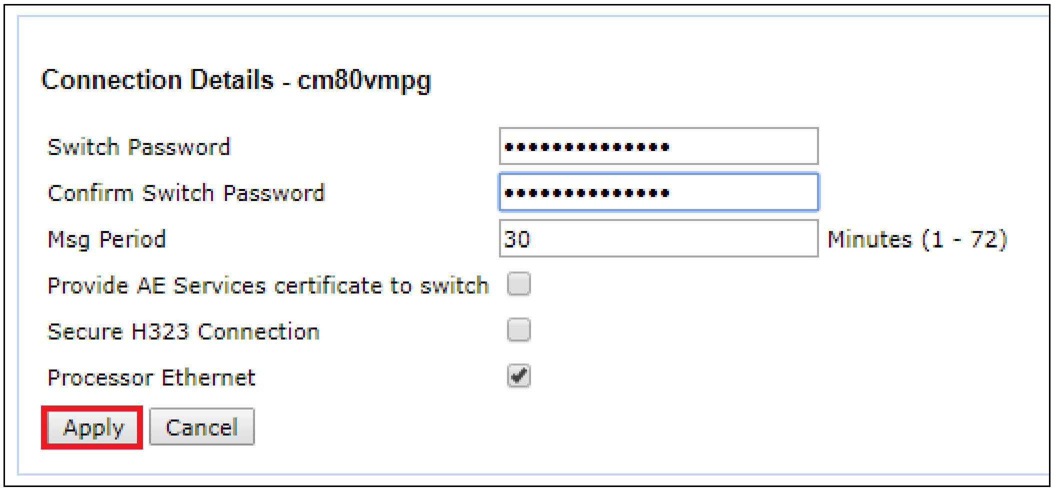


Switch Connections

cm80vmpg

Connection Name	Processor Ethernet	Msg Period

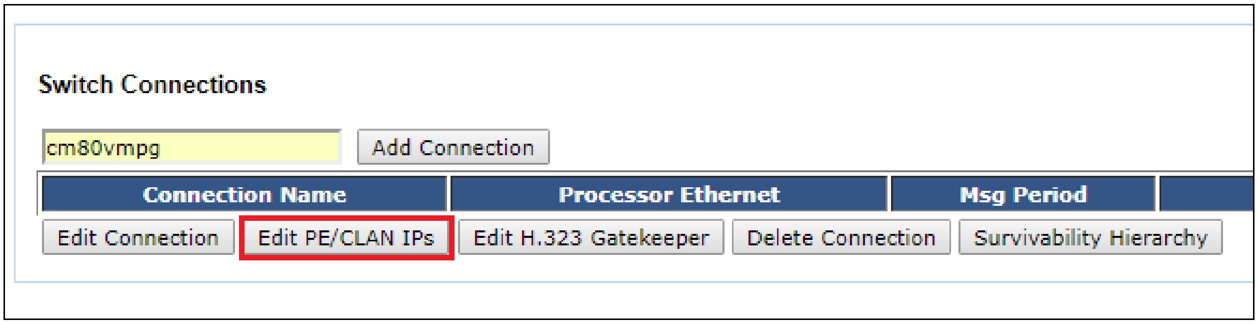
In the resulting screen enter the **Switch Password**; the Switch Password must be the same as that entered into Communication Manager AE Services Administration screen via the **change ip-services** command, described in **Section 5.3**. Default values may be accepted for the remaining fields. Click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



Connection Details - cm80vmpg

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 PE/CLAN IPs** button.

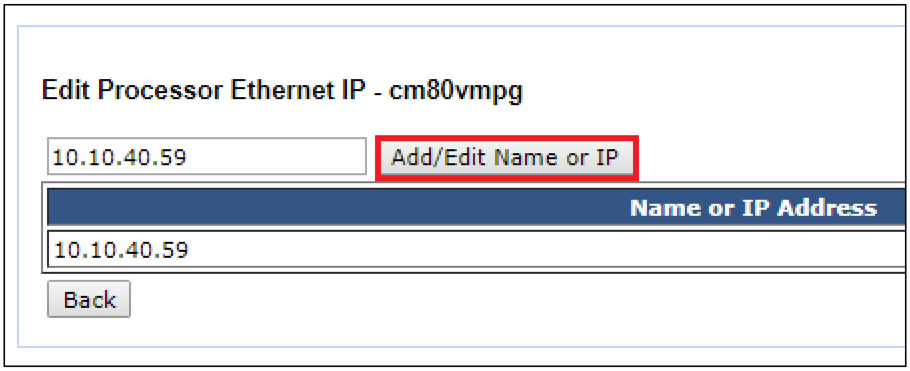


Switch Connections

cm80vmpg

Connection Name	Processor Ethernet	Msg Period

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.



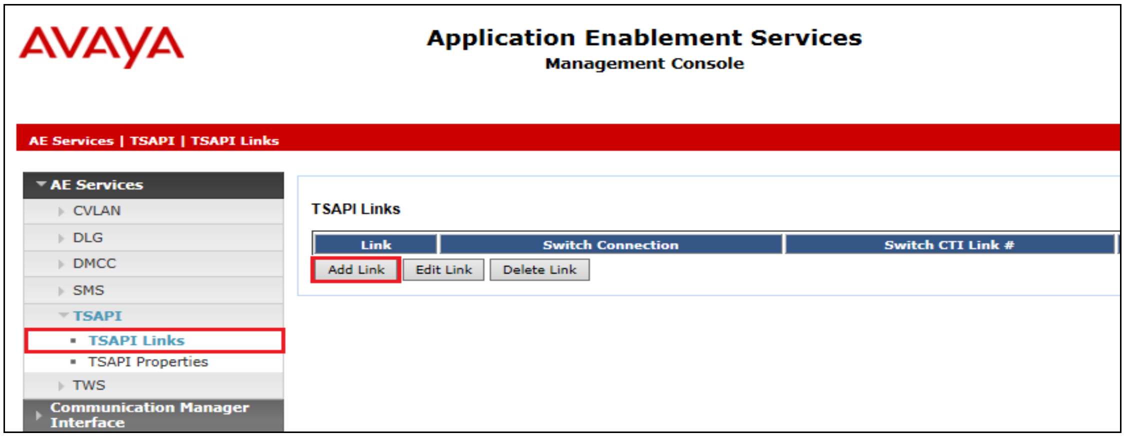
Edit Processor Ethernet IP - cm80vmpg

10.10.40.59

Name or IP Address
10.10.40.59

6.3. Administer TSAPI link

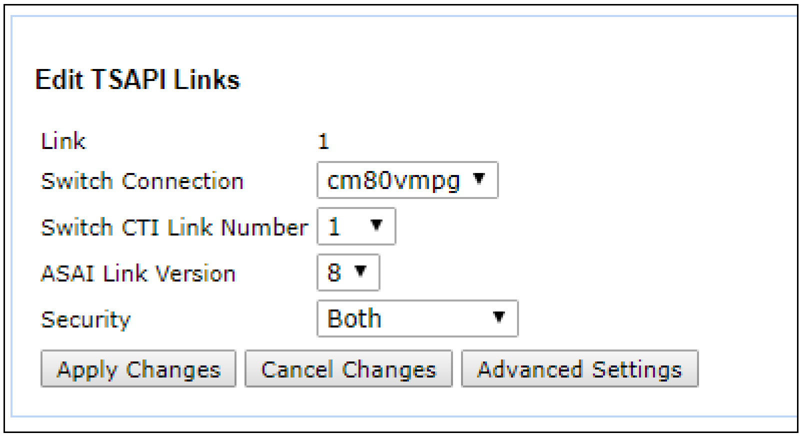
From the Application Enablement Services Management Console, select **AE Services** → **TSAPI** → **TSAPI Links**. Select **Add Link** button as shown in the screen below.



On the **Add TSAPI Links** screen (or the **Edit TSAPI Links** screen to edit a previously configured TSAPI Link as shown below), enter the following values:

- **Link:** Use the drop-down list to select an unused link number.
- **Switch Connection:** Choose the switch connection **cm80vmpg**, 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 should correspond with the Communication Manager version.
- **Security:** This can be left at the default value of **both**.

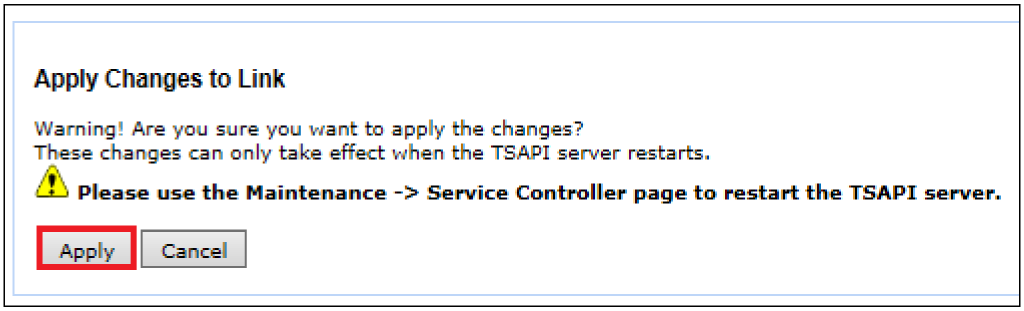
Once completed, select **Apply Changes**.



Edit TSAPI Links

Link	1
Switch Connection	cm80vmpg
Switch CTI Link Number	1
ASAI Link Version	8
Security	Both

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

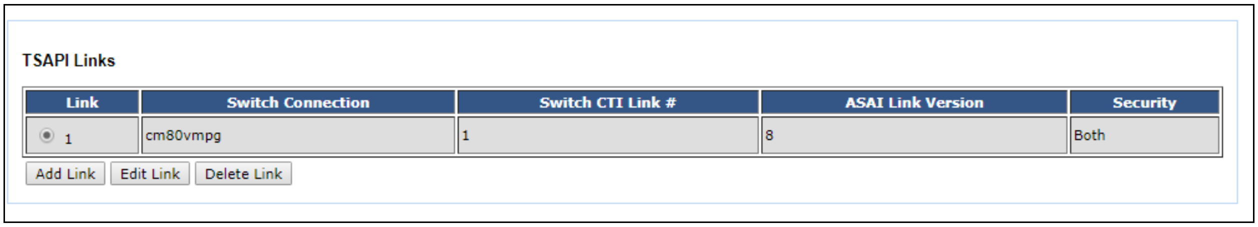


Apply Changes to Link

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.**

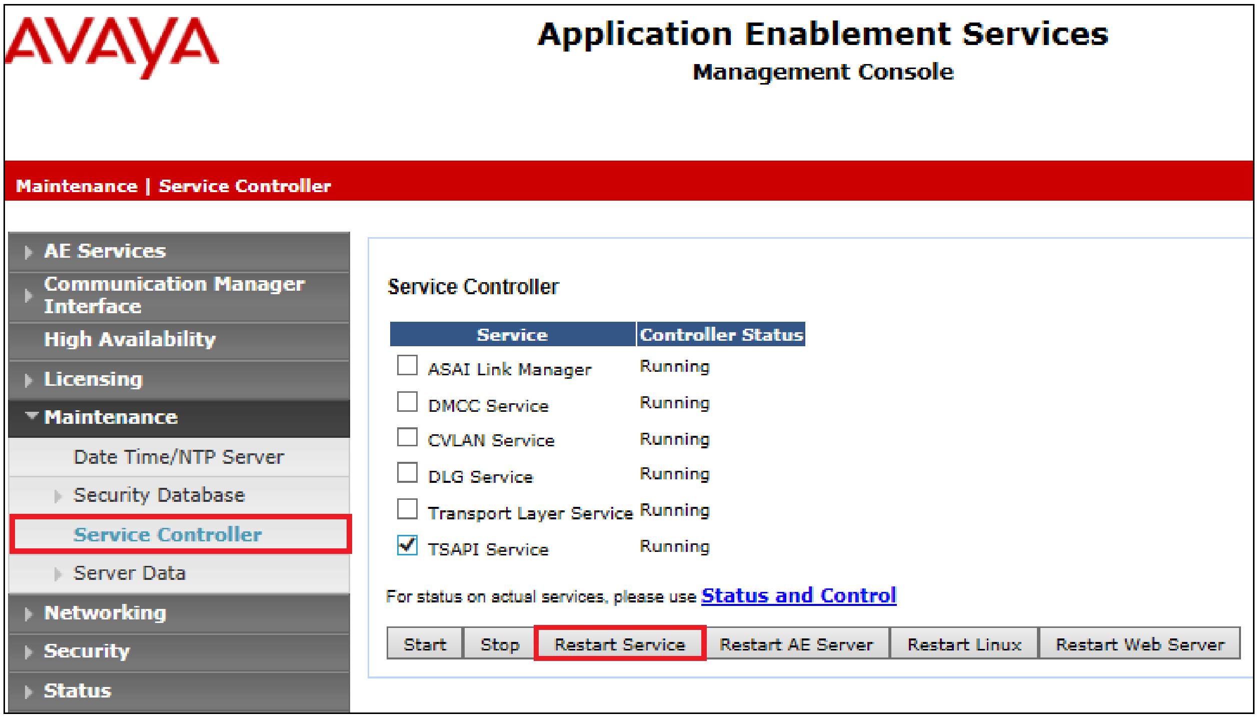
When the TSAPI Link is completed, it should resemble the screen below.



TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
● 1	cm80vmpg	1	8	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**.



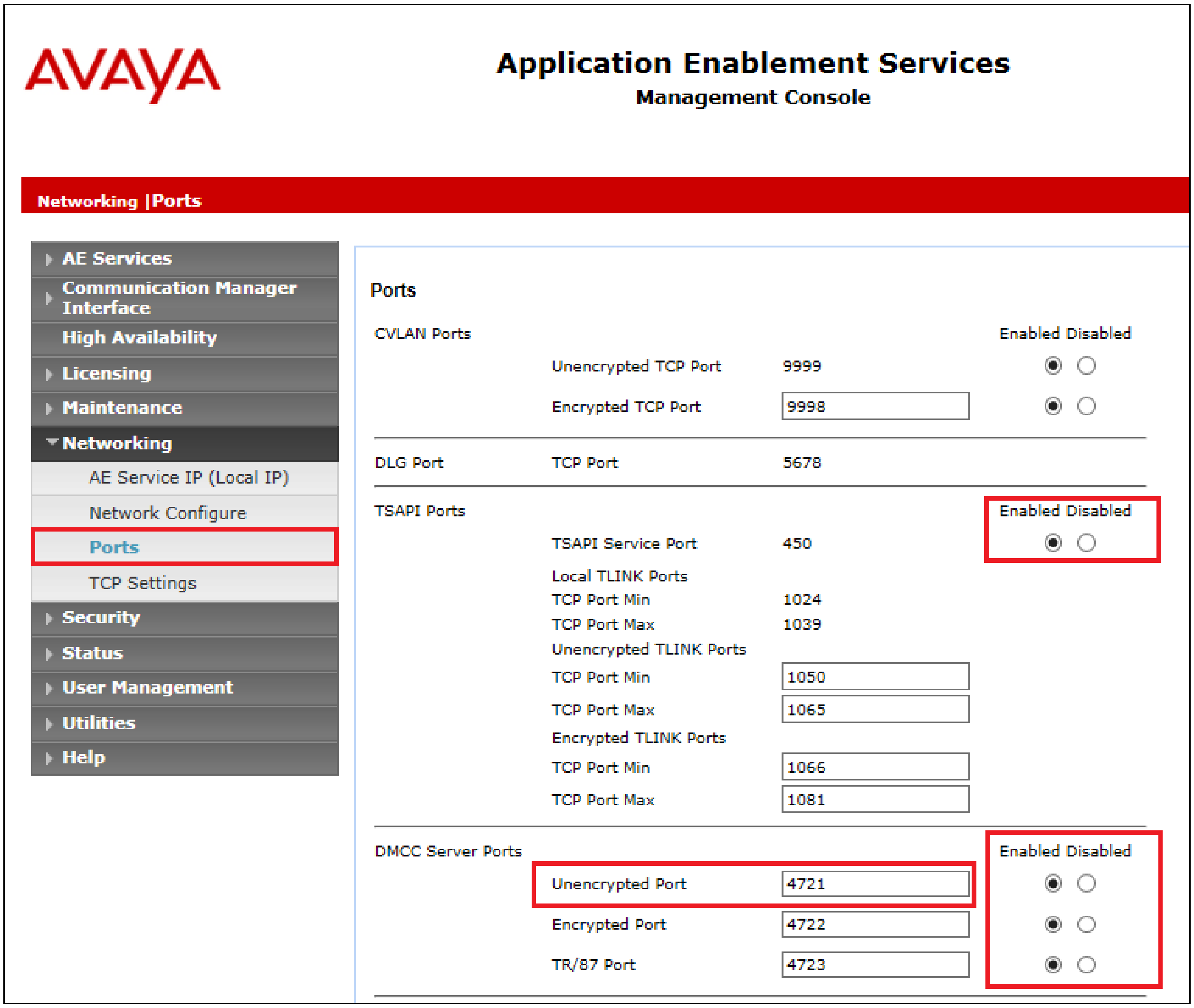
Service Controller

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. Configure Networking Ports

To ensure that TSAPI and DMCC ports are enabled, navigate to **Networking → Ports**. Ensure that the TSAPI ports are set to **Enabled** as shown below. Ensure that the **DMCC Server Ports** are also **Enabled** and take note of the **Unencrypted Port 4721** which will be used later in **Section 7.4.1**.

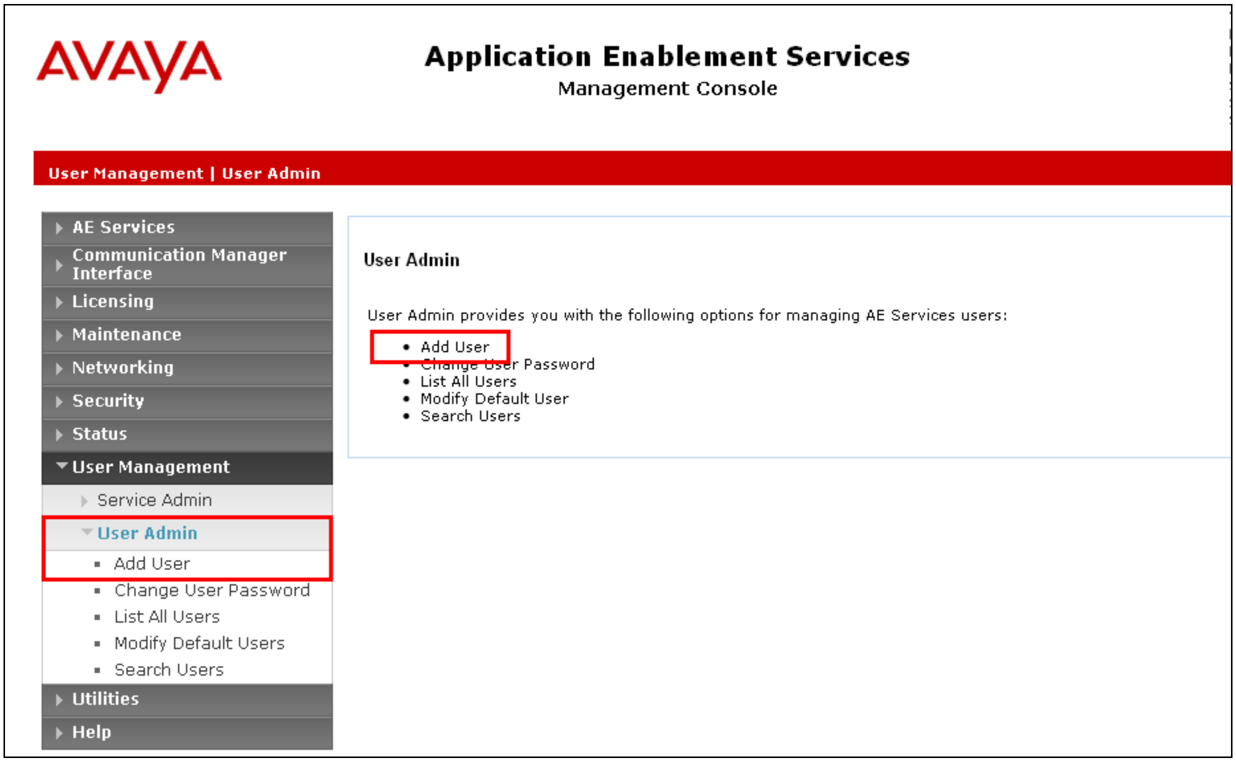


Ports

			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	●	○

6.5. 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

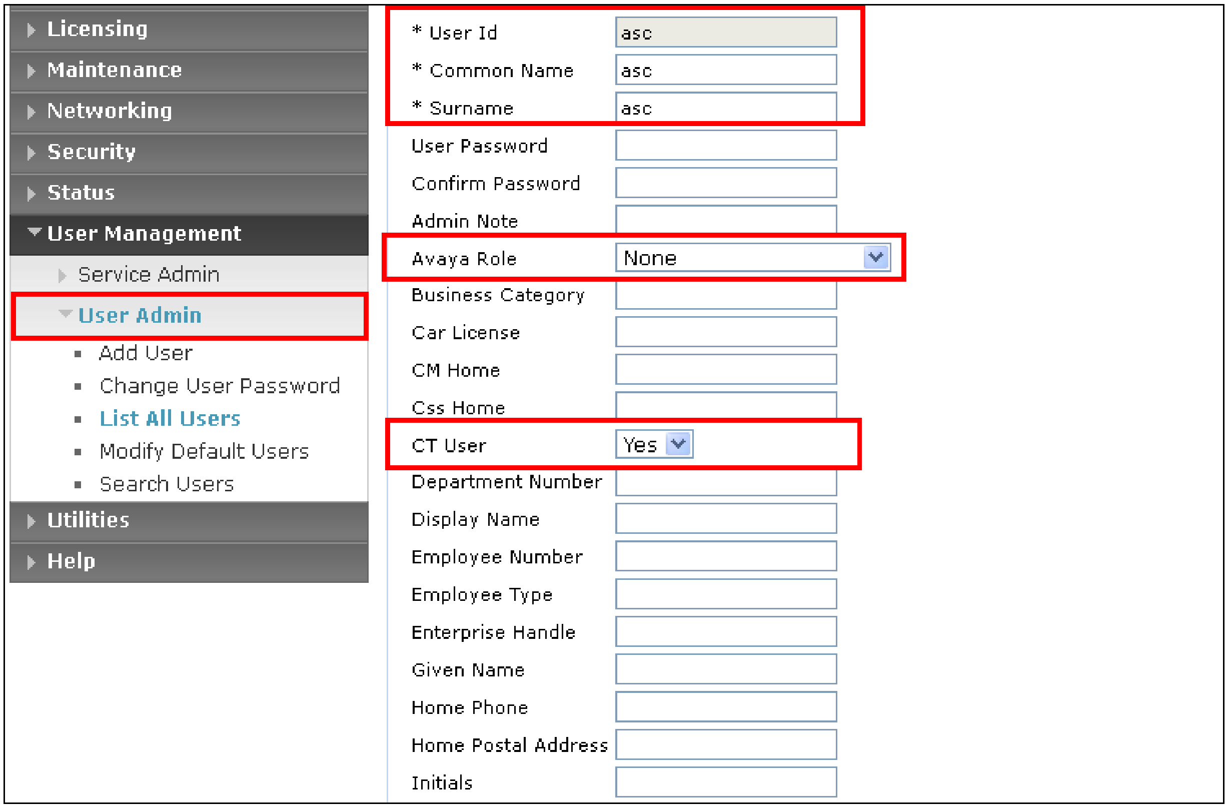
User Admin provides you with the following options for managing AE Services users:

- 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).

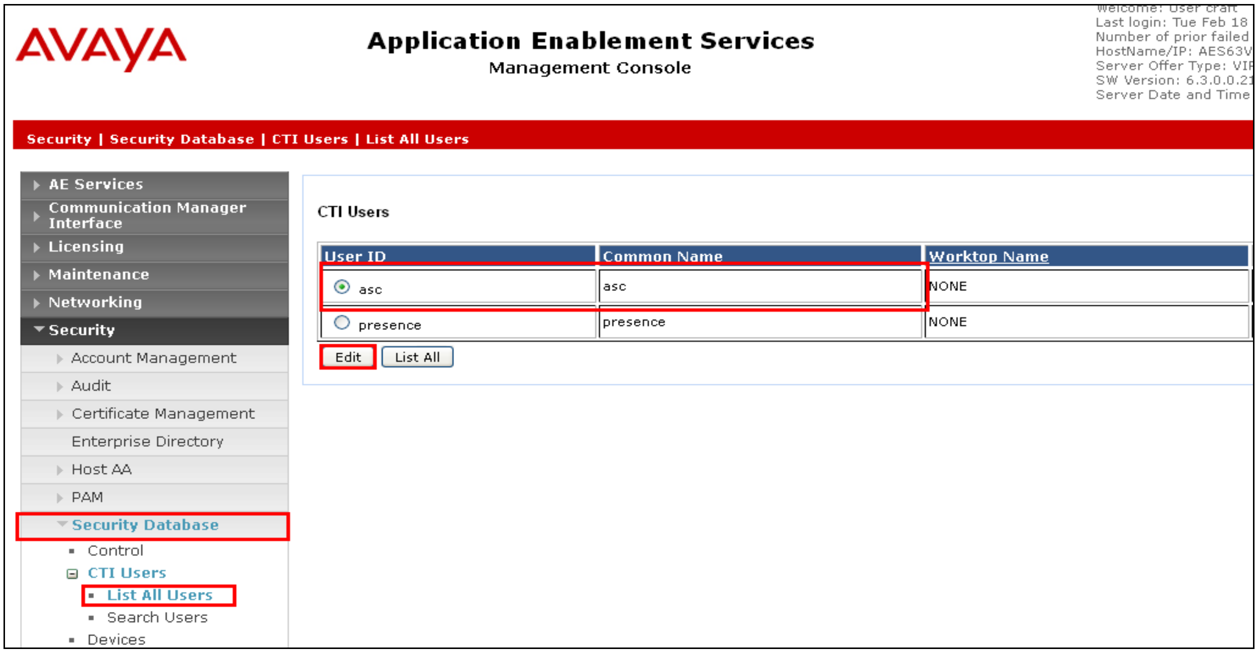


* User Id	asc
* Common Name	asc
* Surname	asc
User Password	
Confirm Password	
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes
Department Number	
Display Name	
Employee Number	
Employee Type	
Enterprise Handle	
Given Name	
Home Phone	
Home Postal Address	
Initials	

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

6.6. 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.

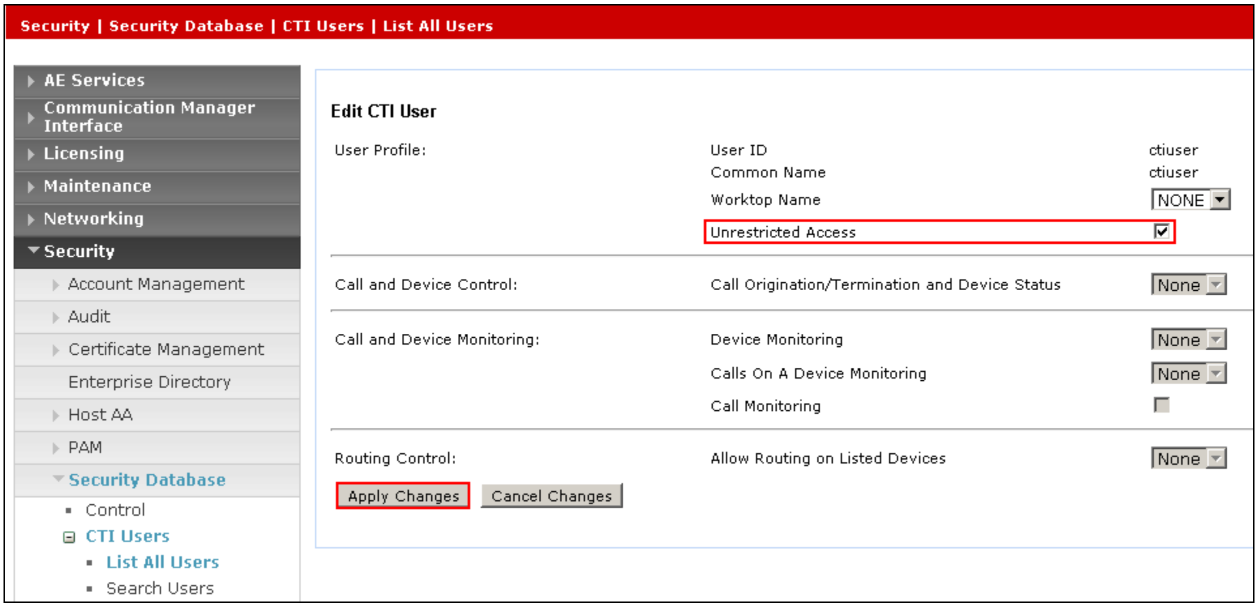


CTI Users

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

Edit | List All

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



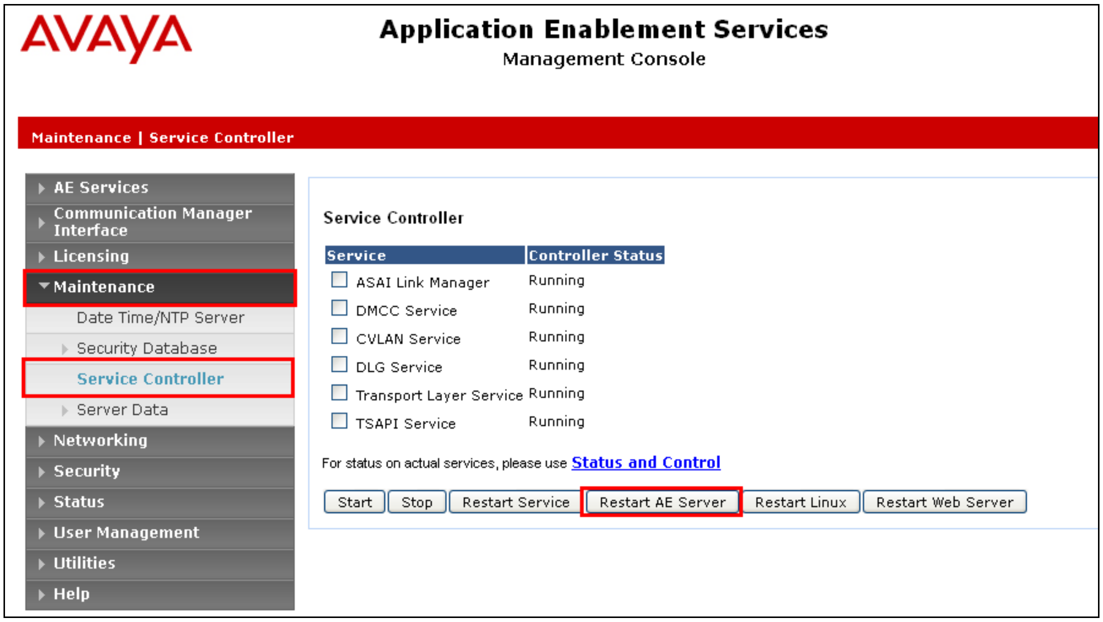
Edit CTI User

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

Apply Changes | Cancel Changes

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

Once all the necessary changes are made it is a good idea to restart of the AE Server. Navigate to **Maintenance → Service Controller**. In the main screen select **Restart AE Server** highlighted.



Service Controller

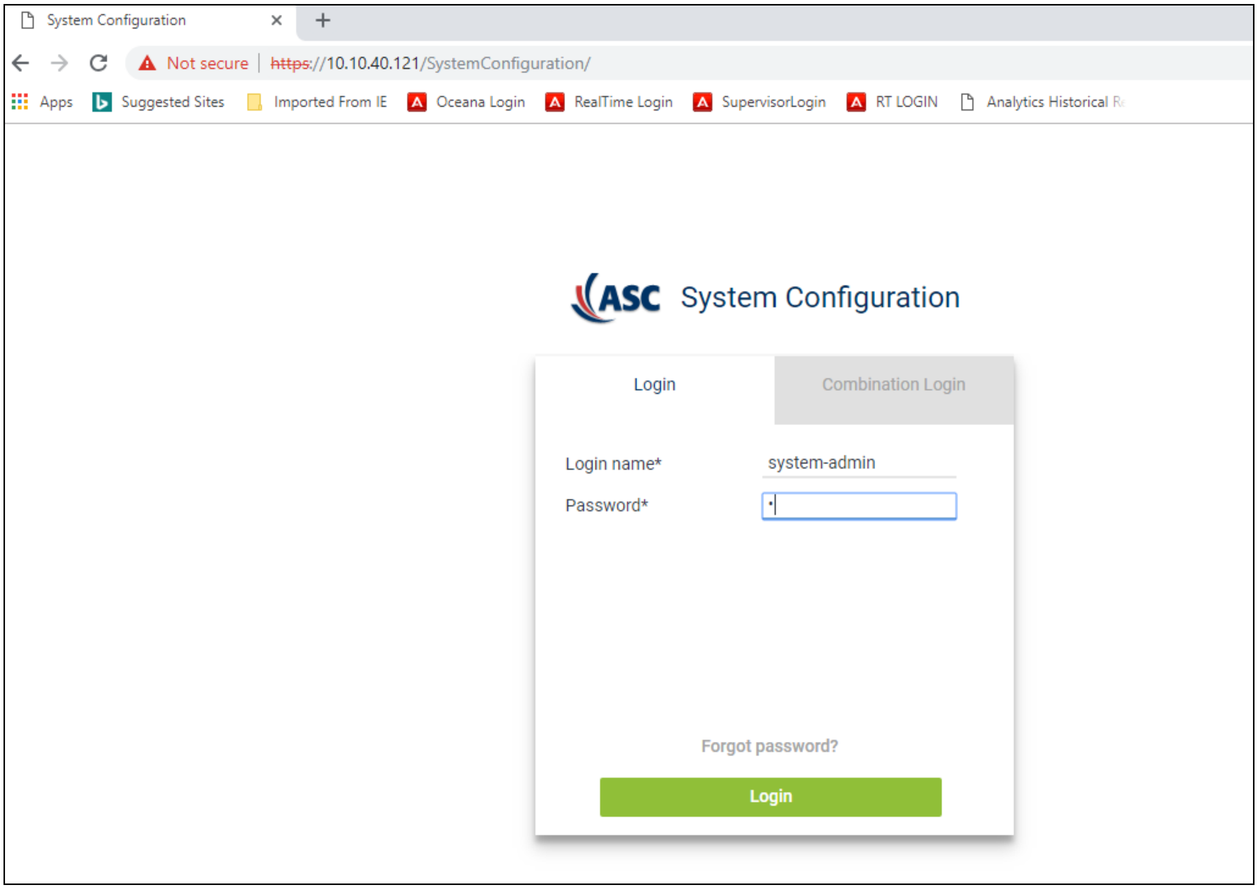
Service	Controller Status
□ ASAI Link Manager	Running
□ DMCC Service	Running
□ CVLAN Service	Running
□ DLG Service	Running
□ Transport Layer Service	Running
□ TSAPI Service	Running

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**.

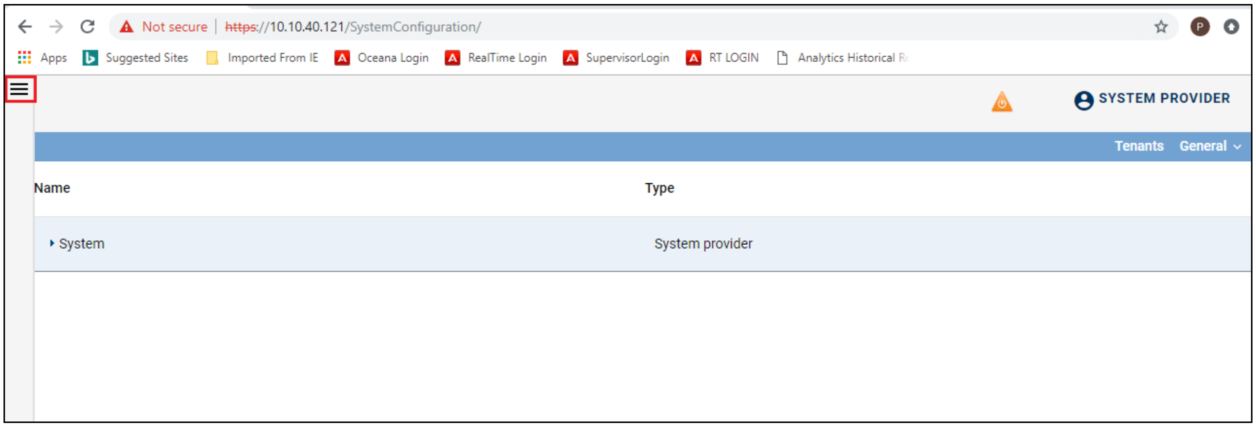


Login name* system-admin

Password* •

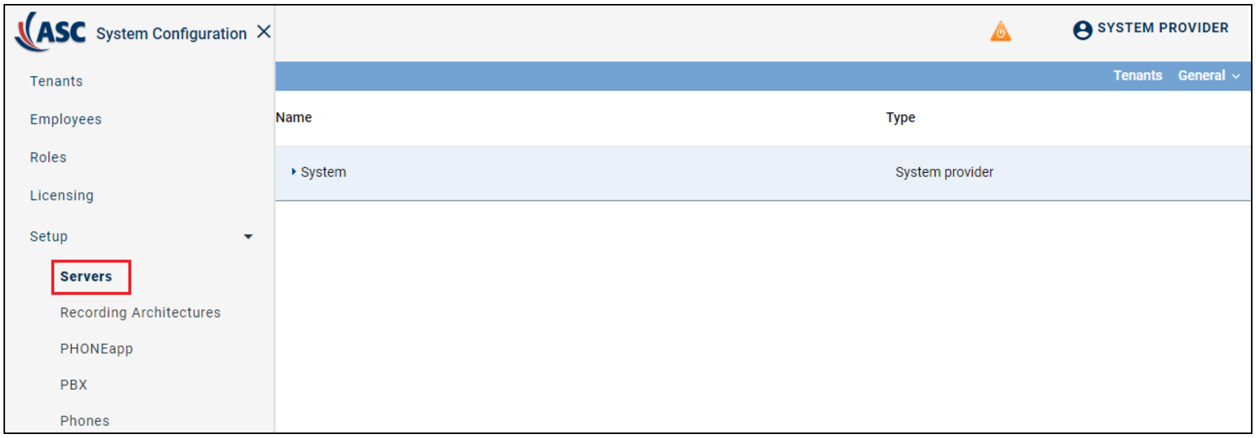
7.1. Configure Server

Expand the menu by clicking on the tab highlighted at the top left of the screen.



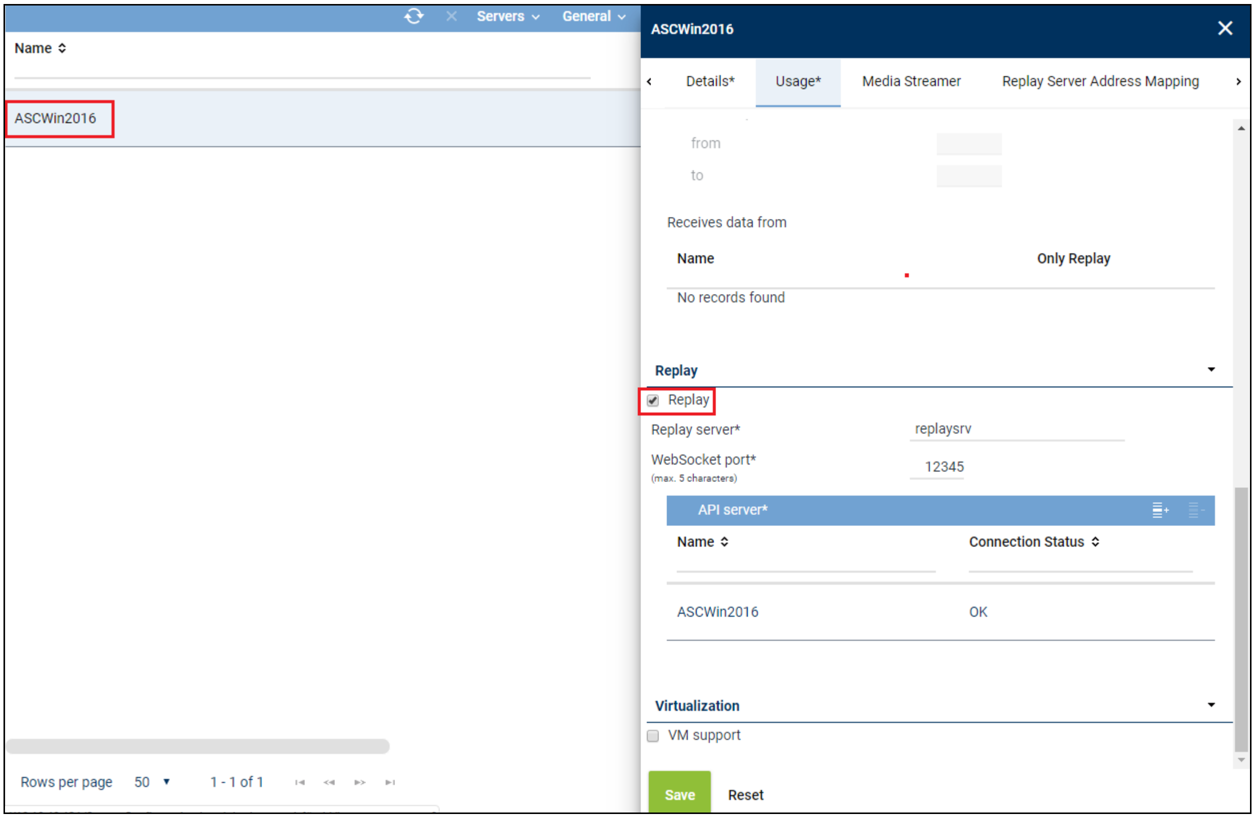
Name	Type
System	System provider

Navigate to **Setup → Servers** in the left window.



Name	Type
System	System provider

Click on the **Usage** tab in the right window. Ensure that **Data Storage** (not shown) and **Replay** boxes are ticked and click on **Save** at the bottom of the screen.



Servers General

Name

ASCWin2016

Rows per page 50 1 - 1 of 1

ASCWin2016

Details* Usage* Media Streamer Replay Server Address Mapping

from

to

Receives data from

Name	Only Replay
No records found	

Replay

☑ Replay

Replay server* replaysrv

WebSocket port* (max. 5 characters) 12345

API server*

Name	Connection Status
ASCWin2016	OK

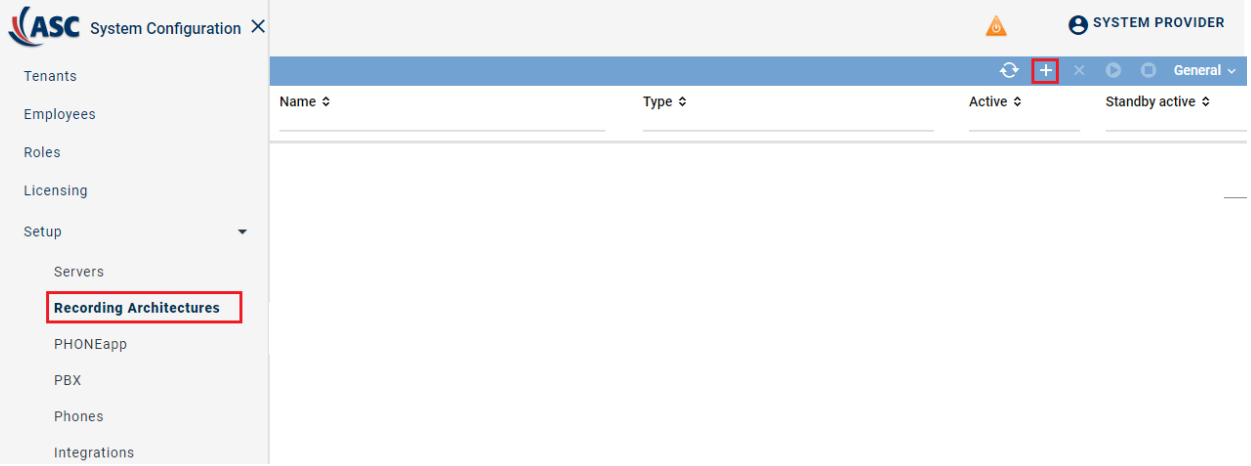
Virtualization

□ VM support

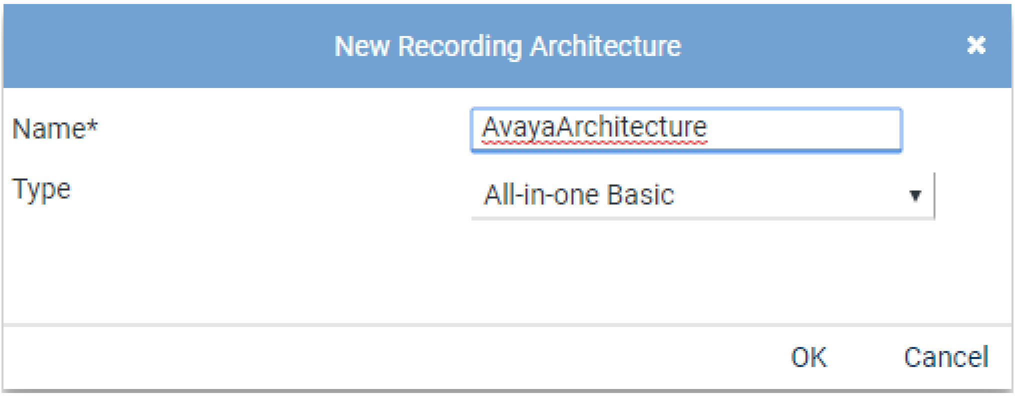
Save Reset

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**.



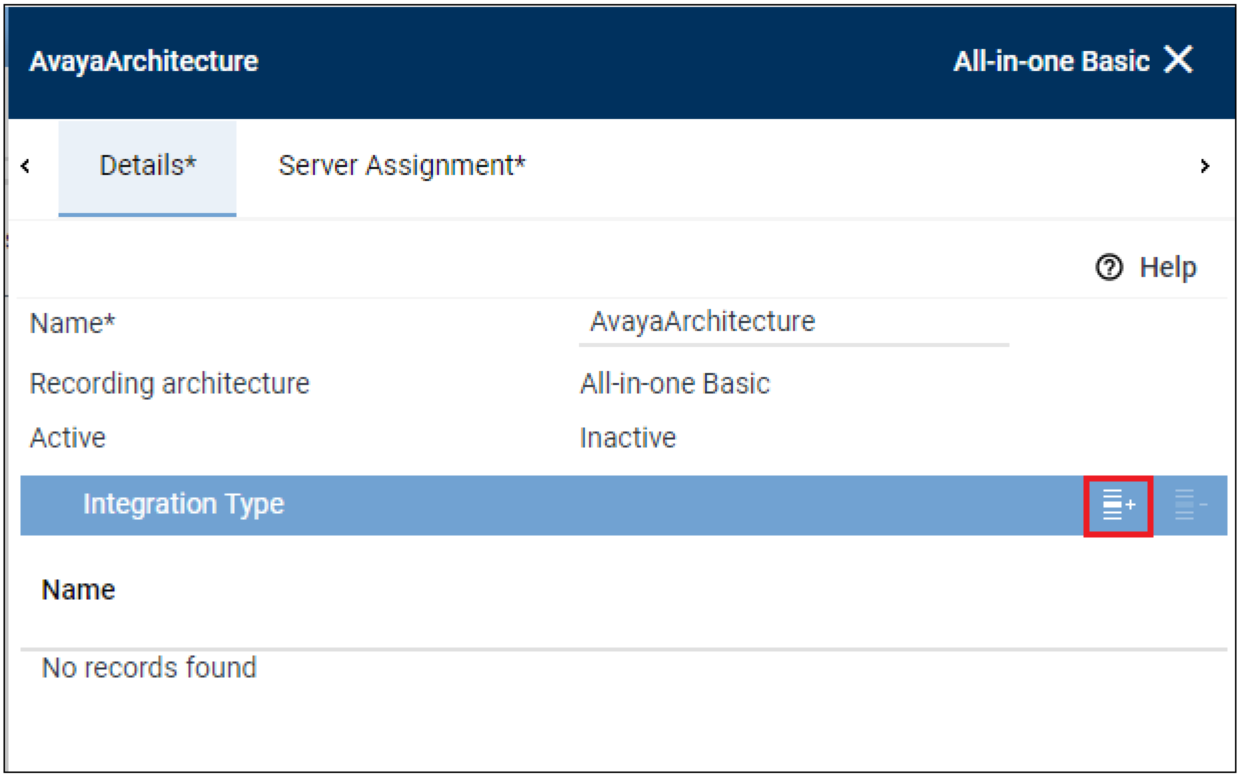
Enter a suitable **Name** and select **All-in-one Basic** as the **Type**, as shown below, click on **OK** once complete.


New Recording Architecture

Name* AvayaArchitecture

Type All-in-one Basic

Click on the **Add** icon highlighted on the right side of the screen below.


AvayaArchitecture — All-in-one Basic

Name* AvayaArchitecture

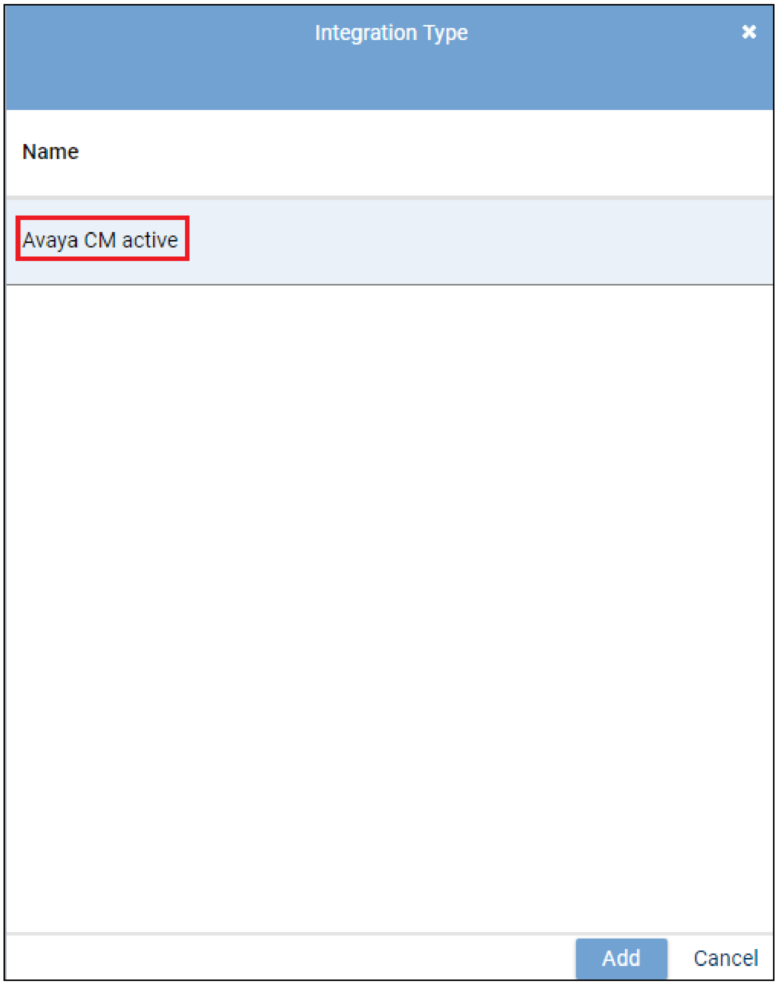
Recording architecture All-in-one Basic

Active Inactive

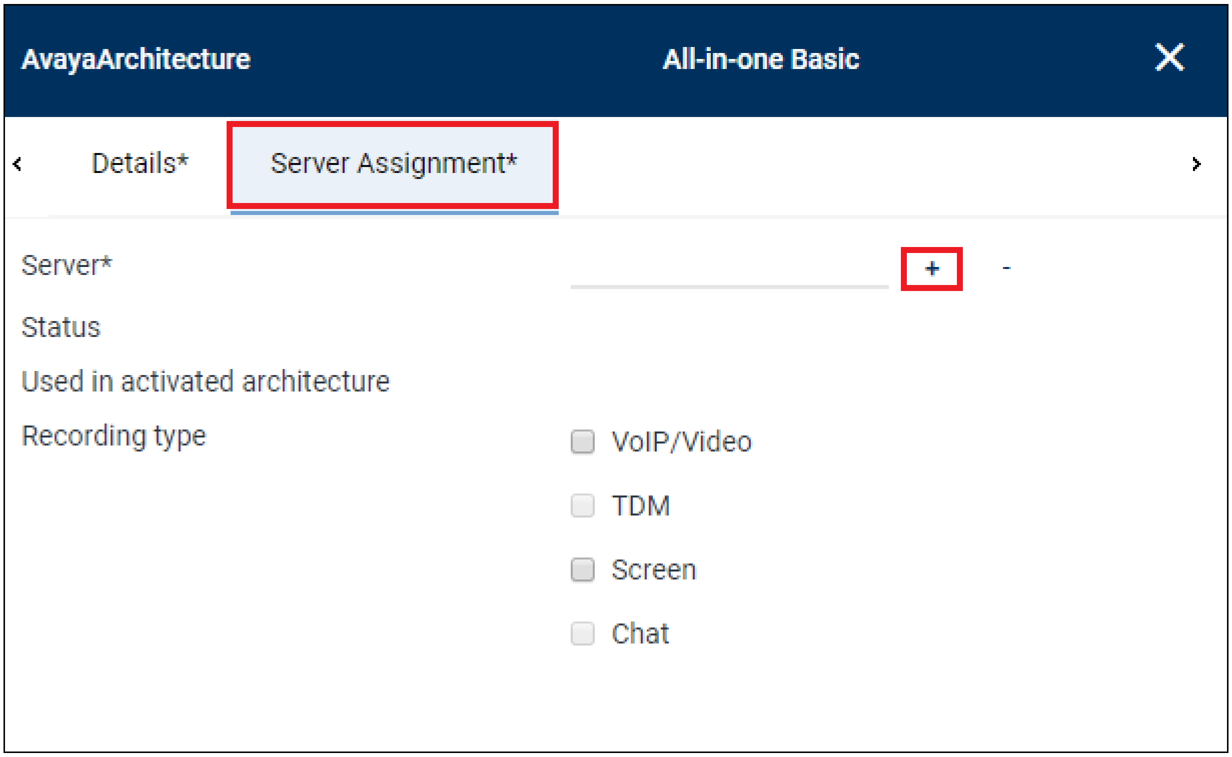
Integration Type

Name
No records found

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.



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



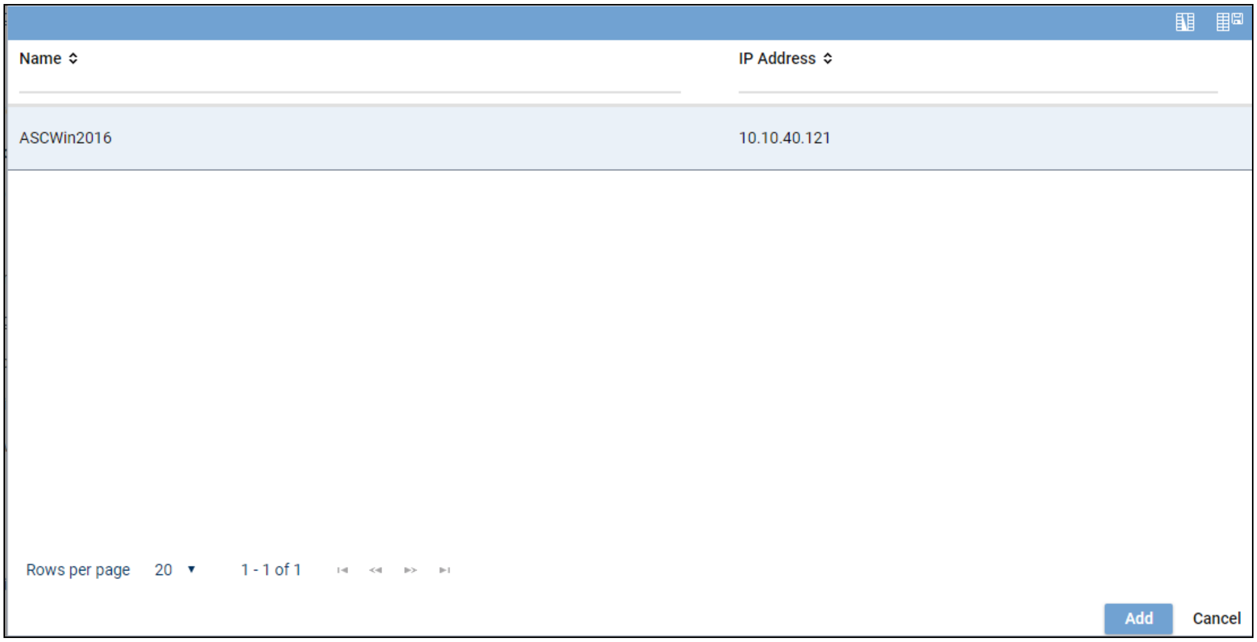
Server*

Status

Used in activated architecture

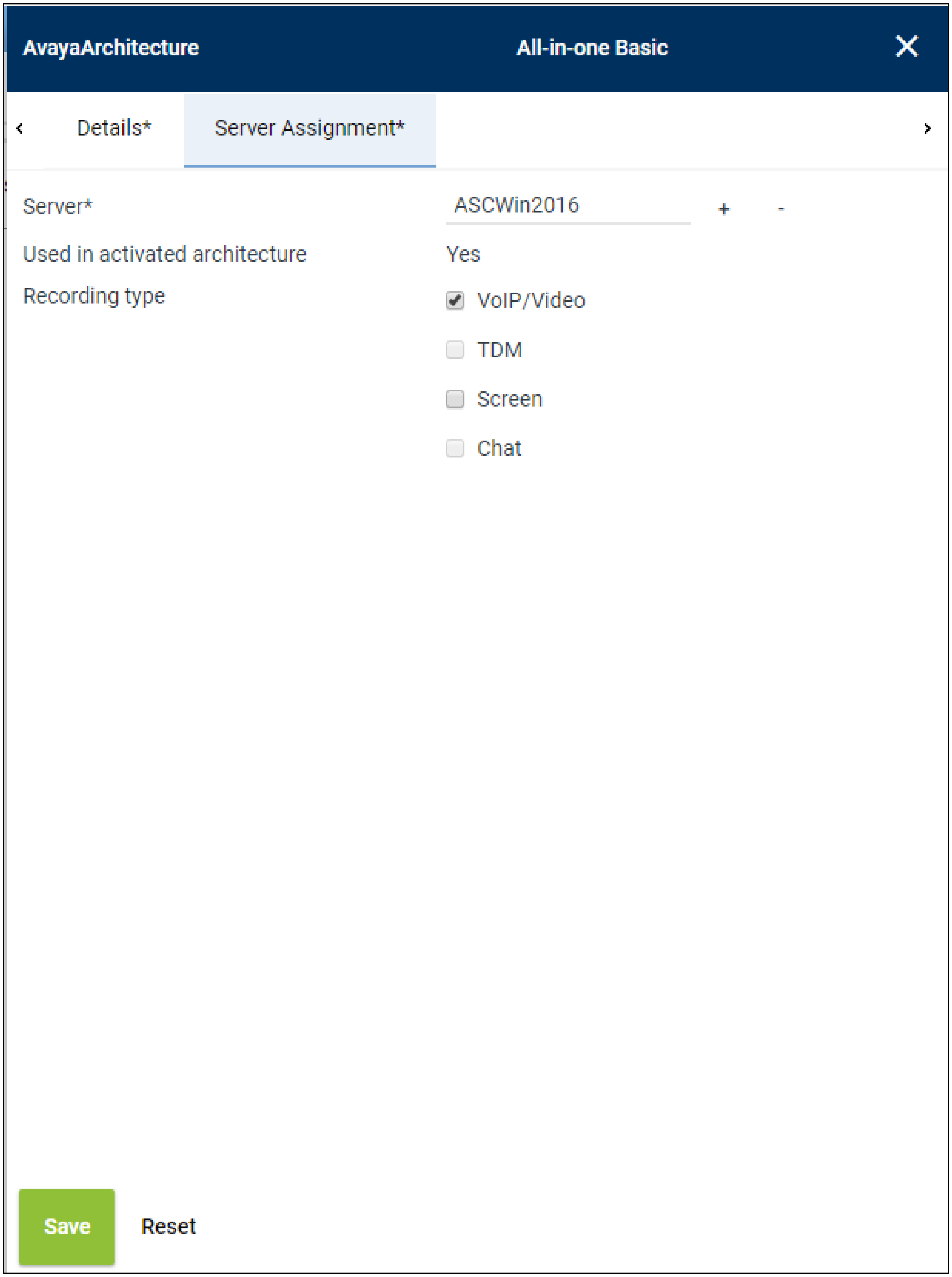
Recording type
□ VoIP/Video
□ TDM
□ Screen
□ Chat

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



Name	IP Address
ASCWin2016	10.10.40.121

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

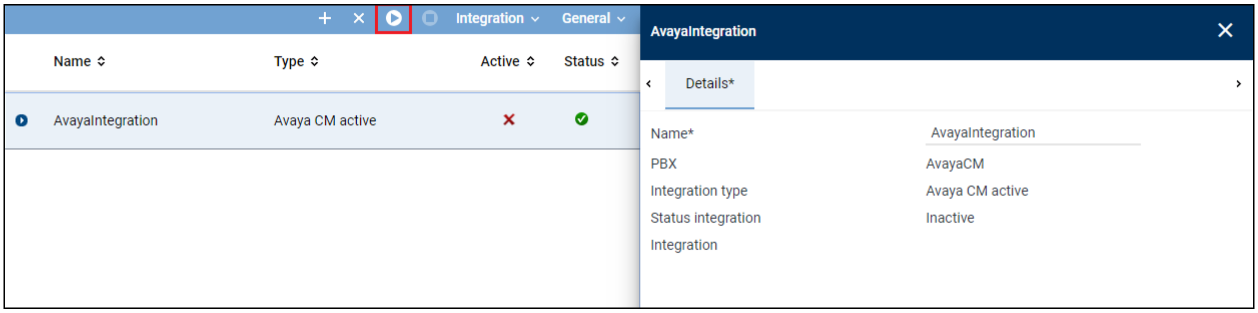


Server* ASCWin2016

Used in activated architecture Yes

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.

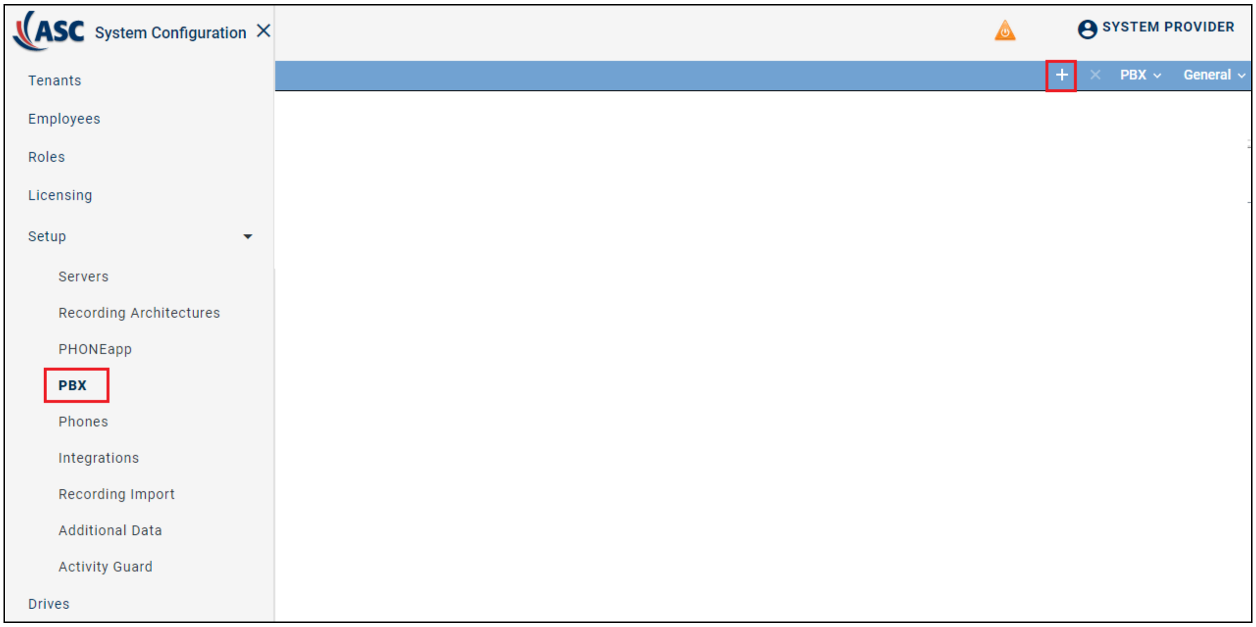


Name	Type	Active	Status
AvayaIntegration	Avaya CM active	✗	✓

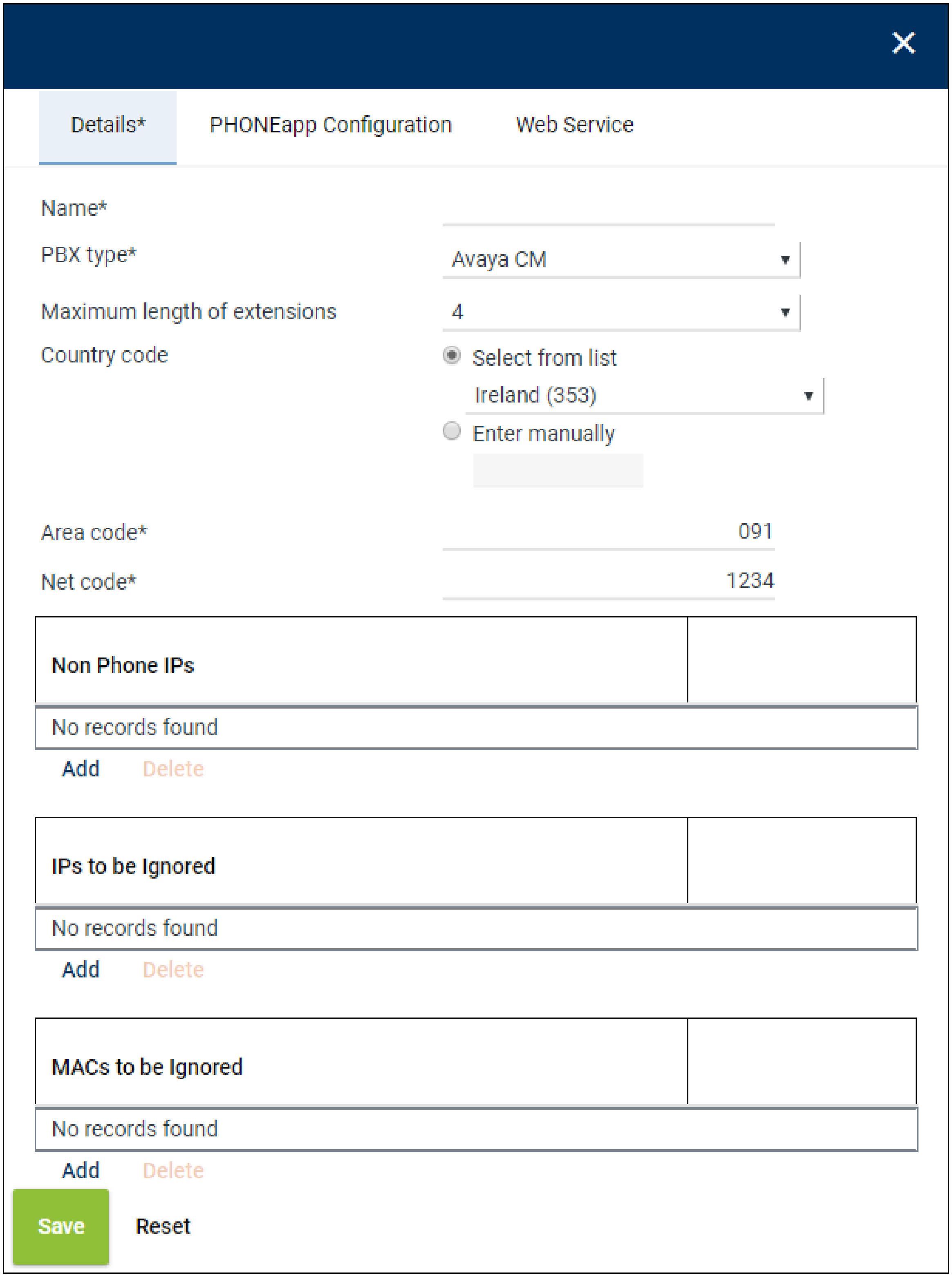
Name*	AvayaIntegration
PBX	AvayaCM
Integration type	Avaya CM active
Status integration	Inactive
Integration	

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*

PBX type* Avaya CM

Maximum length of extensions 4

Country code
● Select from list
Ireland (353)
○ Enter manually

Area code* 091

Net code* 1234

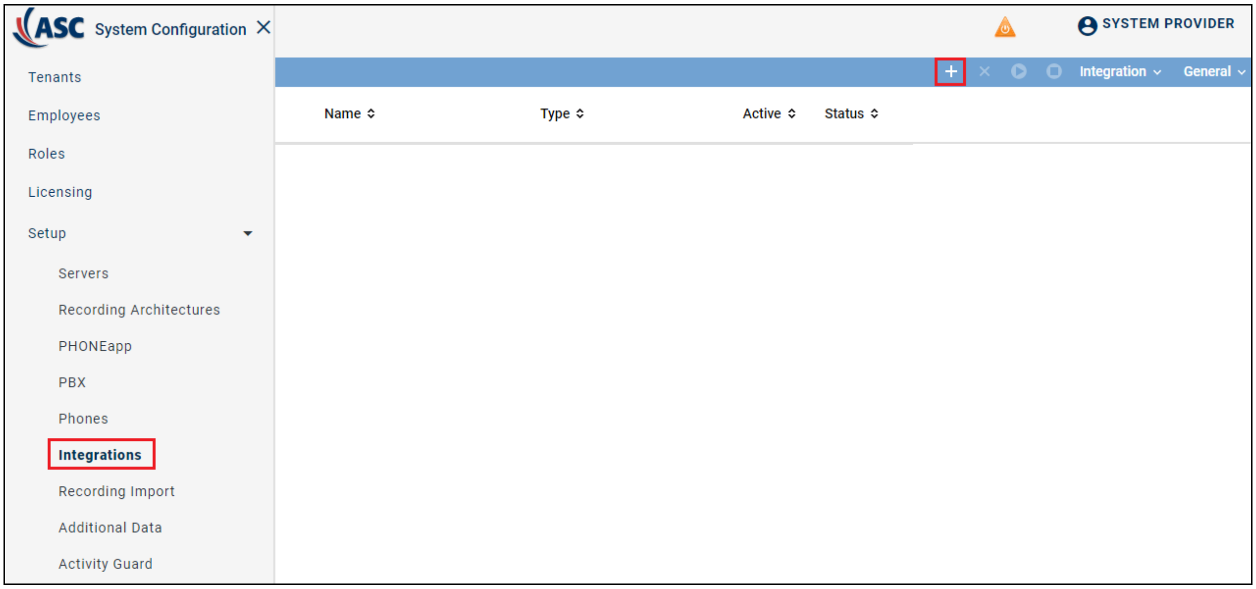
Non Phone IPs
No records found

IPs to be Ignored
No records found

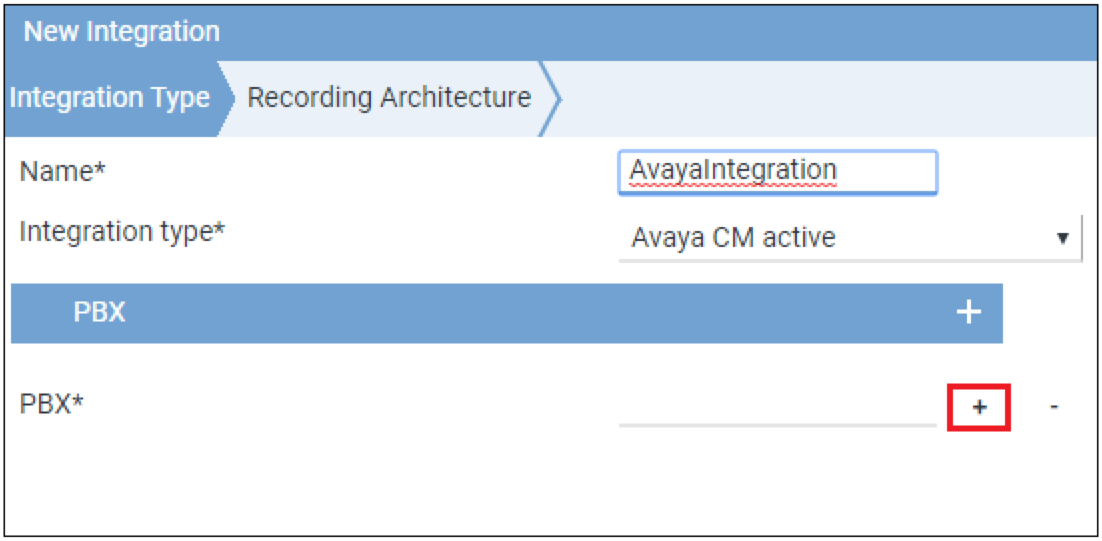
MACs to be Ignored
No records found

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.



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.

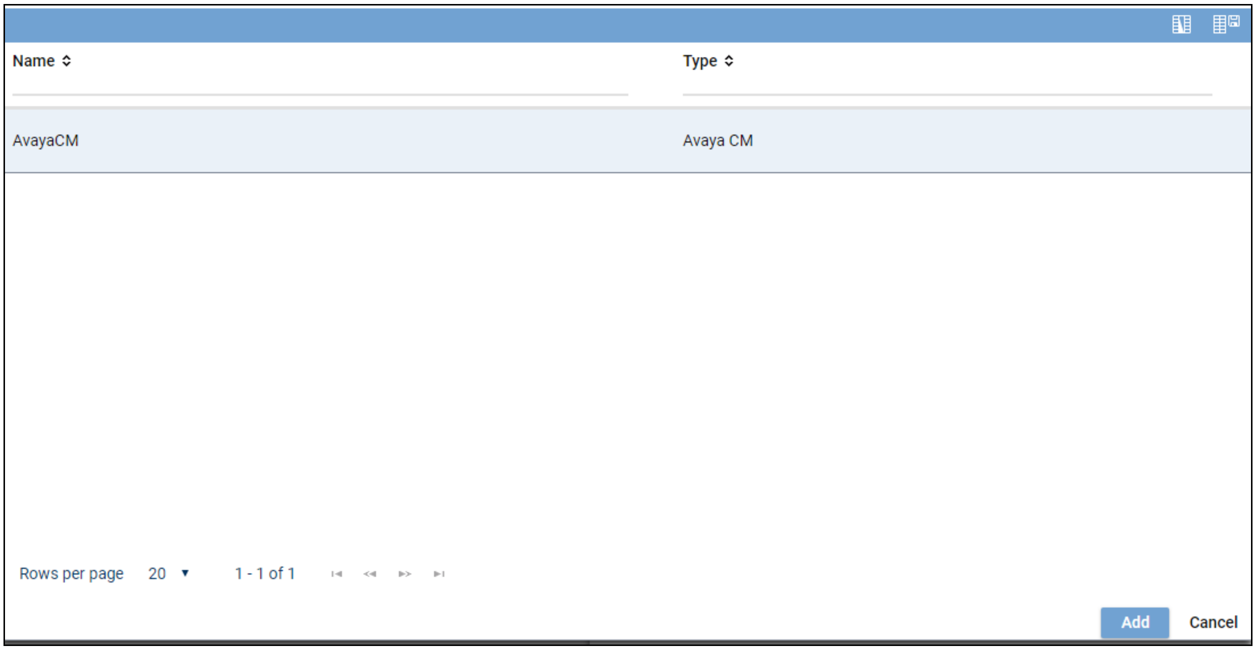


Name* AvayaIntegration

Integration type* Avaya CM active

PBX*

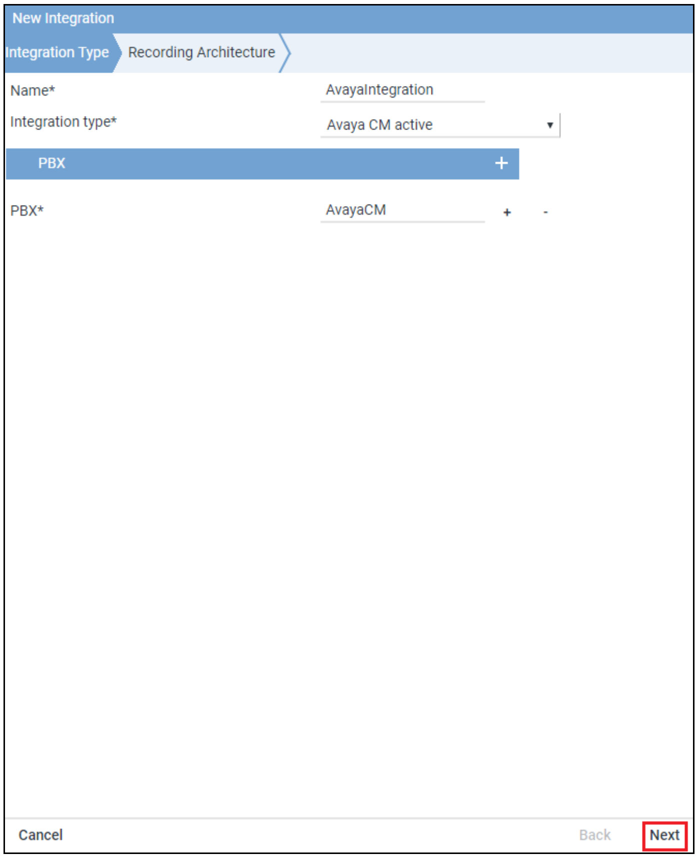
Select the PBX, this was created in **Section 7.3**, click on **Add** at the bottom of the screen.



Name	Type
AvayaCM	Avaya CM

Rows per page 20 1 - 1 of 1

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



New Integration

Integration Type › Recording Architecture

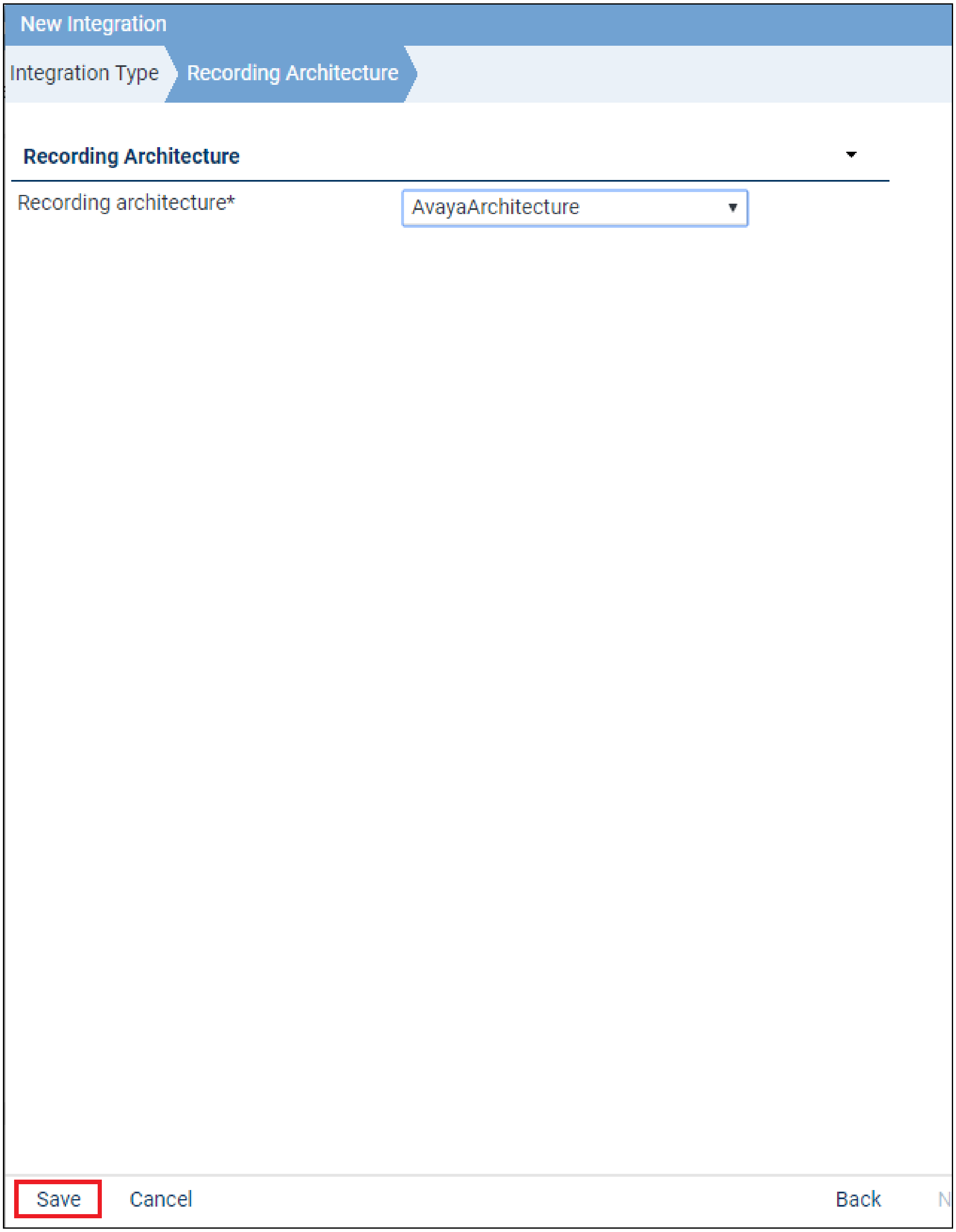
Name* AvayaIntegration

Integration type* Avaya CM active

PBX

PBX* AvayaCM

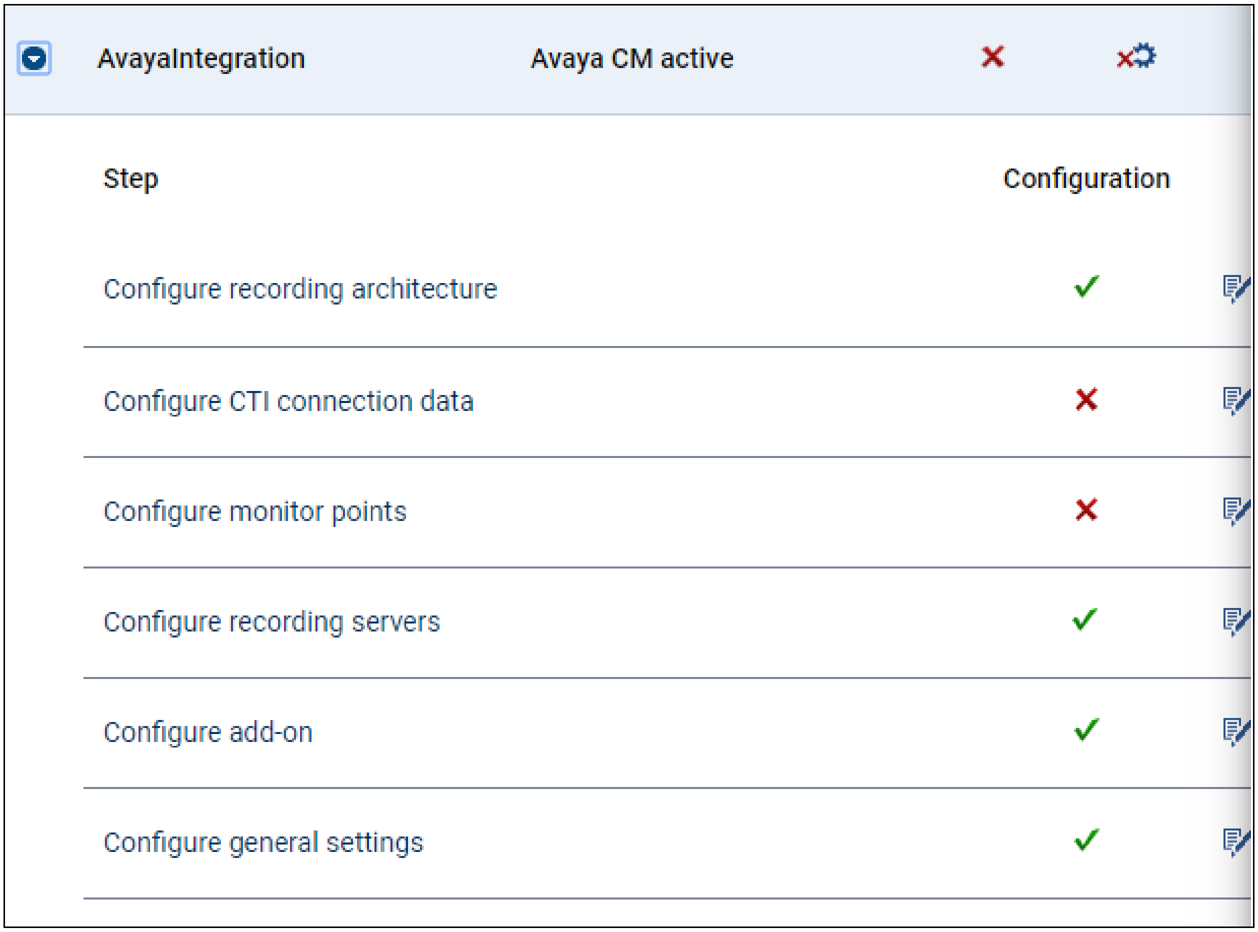
Select the Recording architecture, created in **Section 7.2**, and click on **Save**.



Recording architecture* AvayaArchitecture

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**.

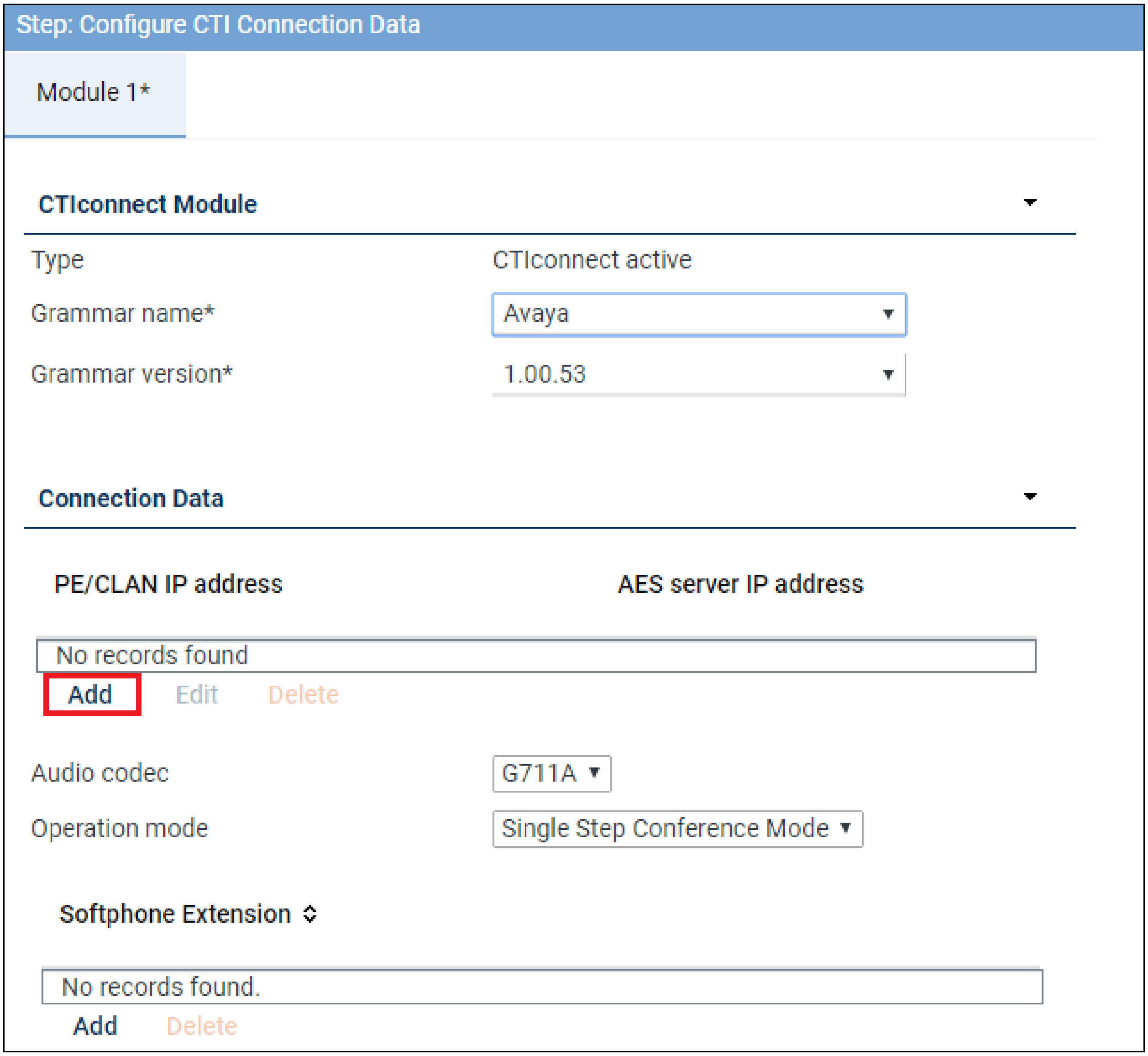


AvayaIntegration Avaya CM active ✗ ✗⚙

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

7.4.1. Configure CTI connection data

Click on the edit icon next to **Configure CTI connection data** (not shown). Click on **+Add** under **PE/CLAN IP address – AES server IP address**.



Step: Configure CTI Connection Data

Module 1*

CTIconnect Module

Type: CTIconnect active

Grammar name*: Avaya

Grammar version*: 1.00.53

Connection Data

PE/CLAN IP address | AES server IP address

No records found

Add Edit Delete

Audio codec: G711A

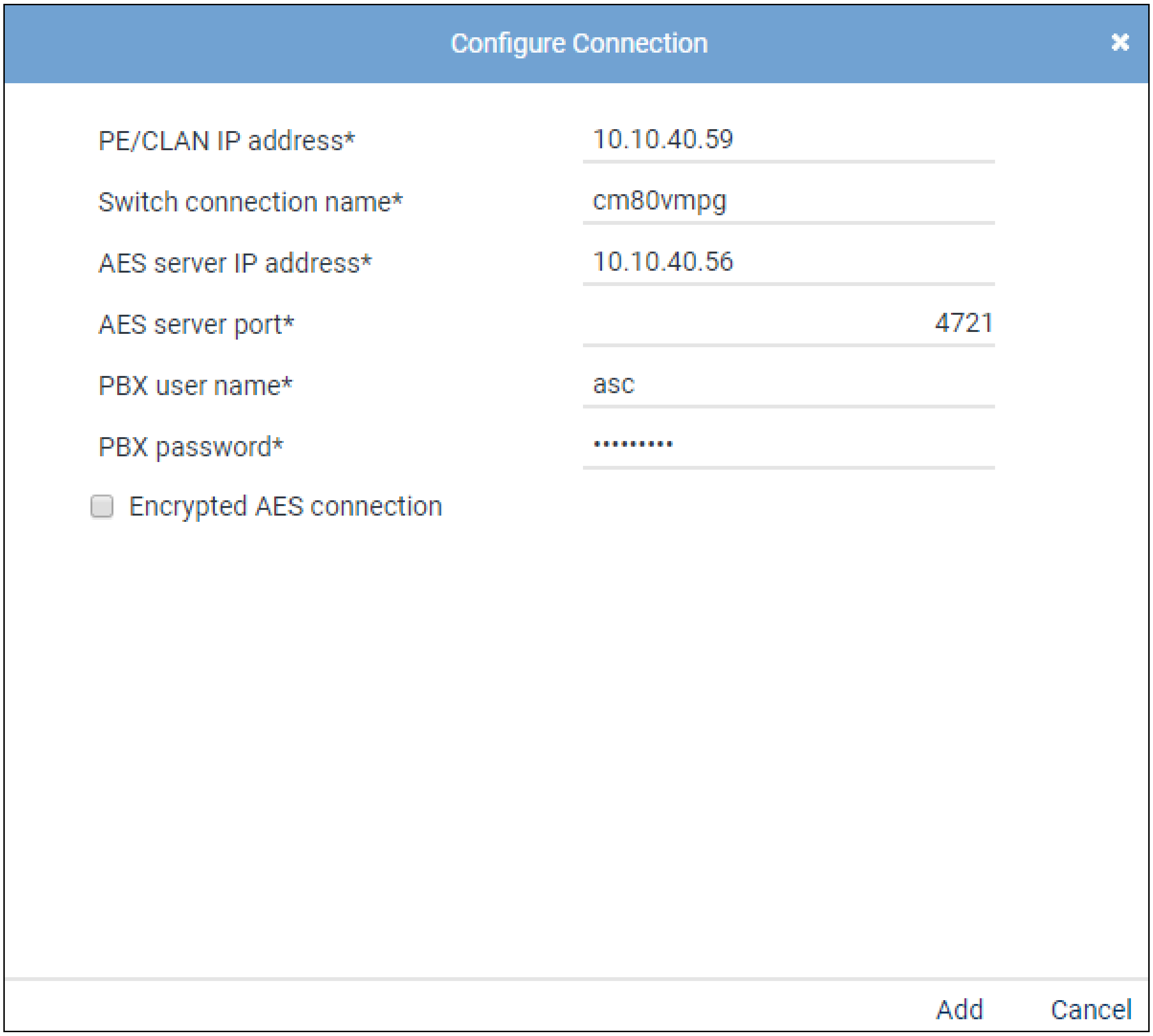
Operation mode: Single Step Conference Mode

Softphone Extension

No records found.

Add Delete

Enter the Communication Manager IP Address and the AES information which can be obtained from **Section 6.5**. 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**.



PE/CLAN IP address* 10.10.40.59

Switch connection name* cm80vmpg

AES server IP address* 10.10.40.56

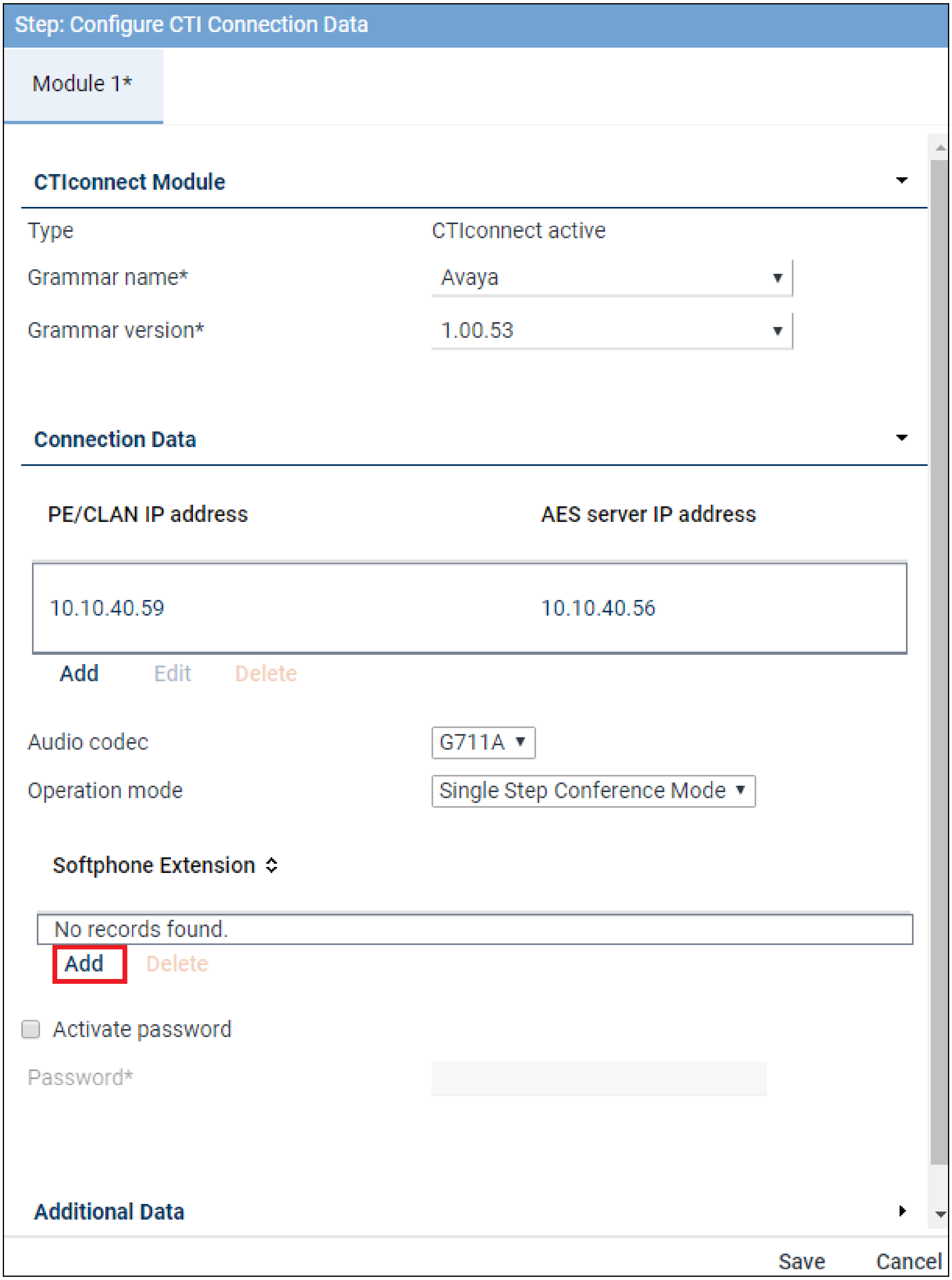
AES server port* 4721

PBX user name* asc

PBX password* ••••••••••

□ Encrypted AES connection

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*	1.00.53

Connection Data

PE/CLAN IP address	AES server IP address
10.10.40.59	10.10.40.56

Audio codec	G711A
Operation mode	Single Step Conference Mode

Softphone Extension

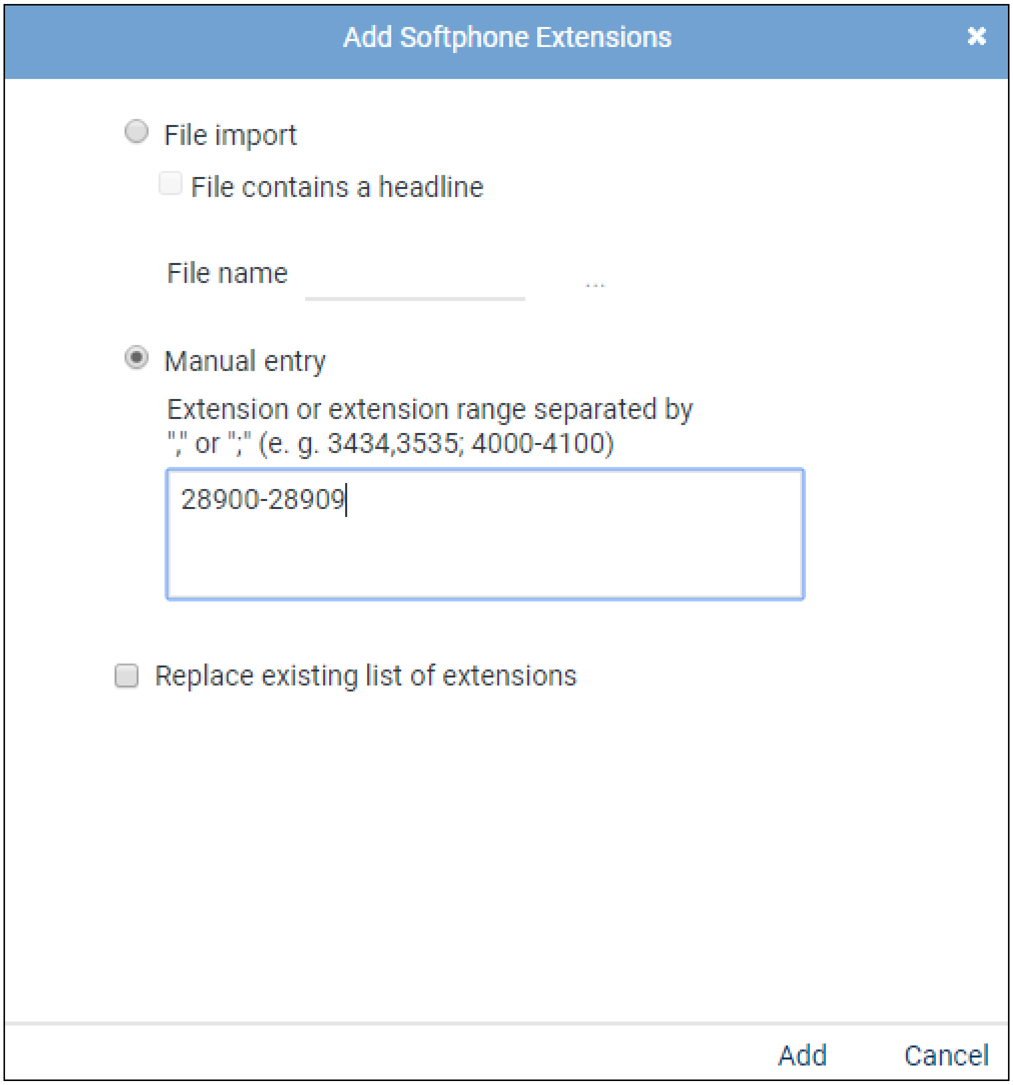
No records found.

□ Activate password

Password*

Additional Data

Enter the virtual extension numbers created in **Section 5.7**.



Add Softphone Extensions

○ File import

□ File contains a headline

File name ...

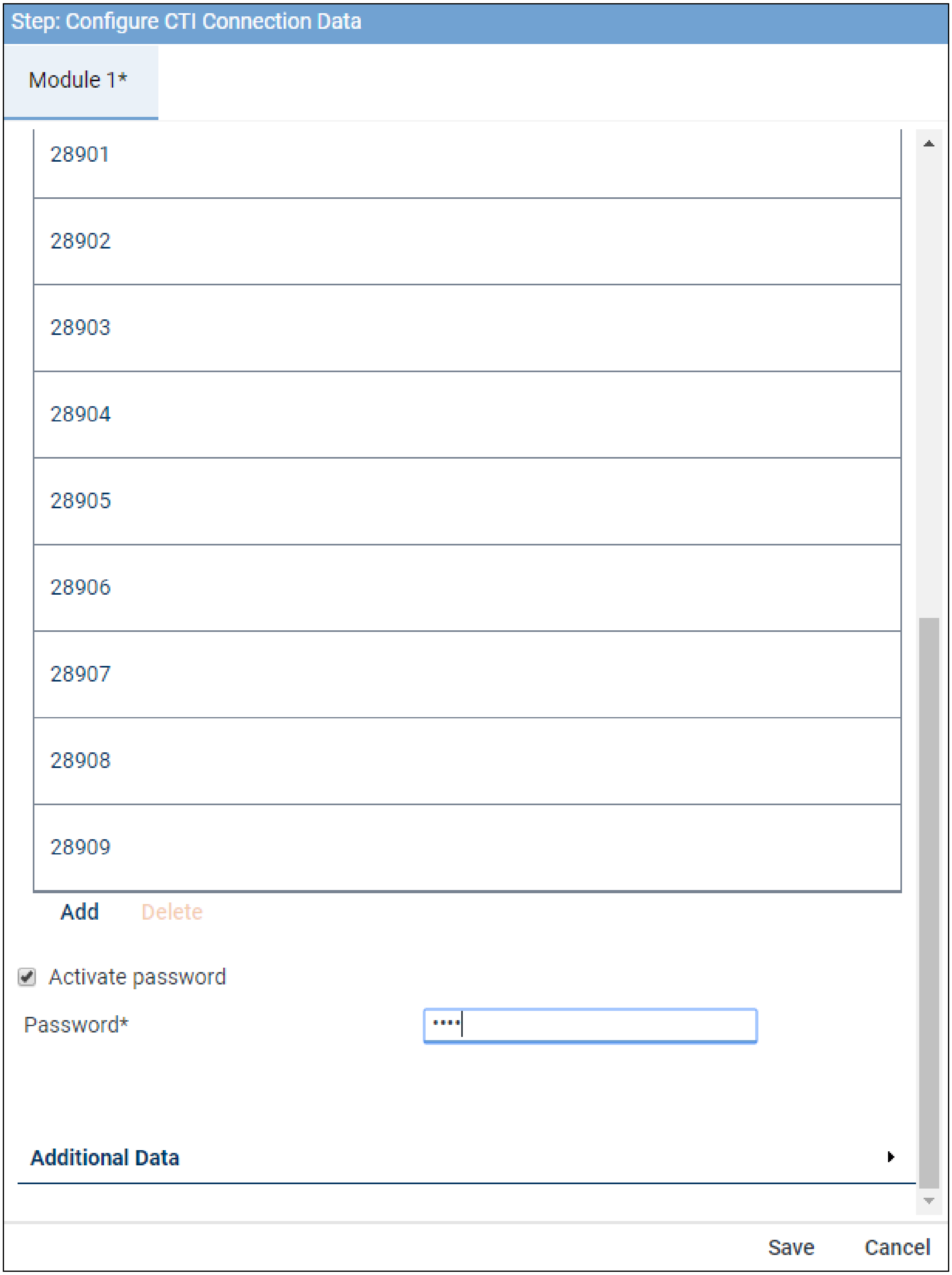
● Manual entry

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

28900-28909

□ 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.



Step: Configure CTI Connection Data

Module 1*

28901

28902

28903

28904

28905

28906

28907

28908

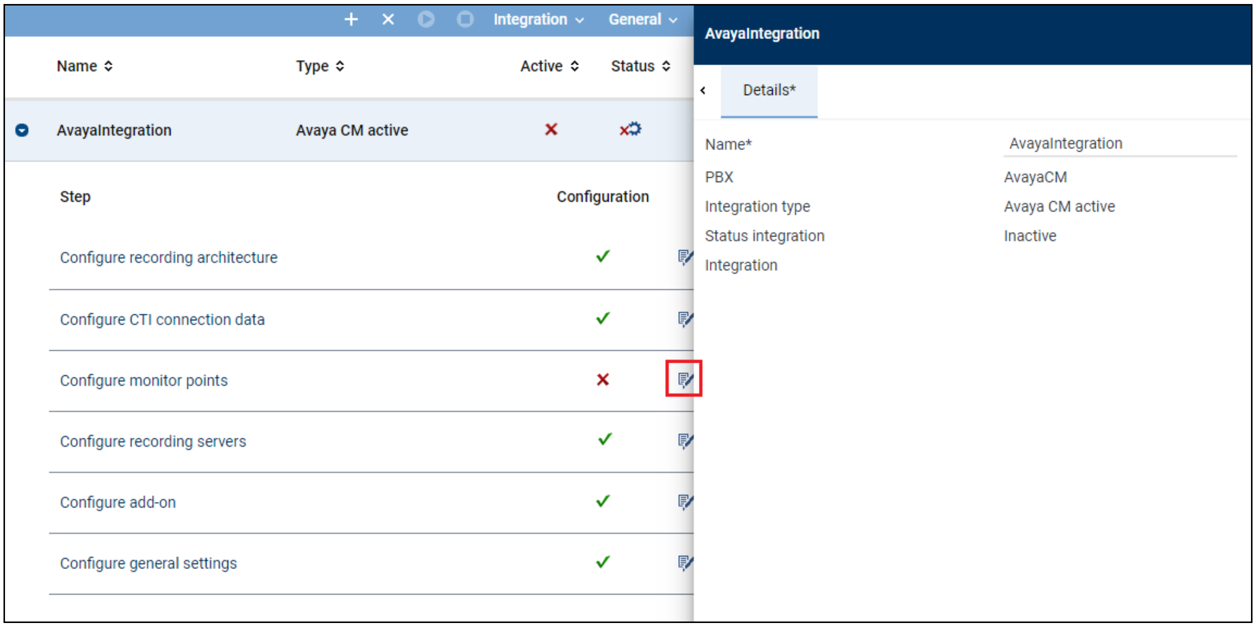
28909

☑ Activate password

Password* ••••

7.4.2. Configure monitor points

Click on the edit icon next to **Configure monitor points**.



Name	Type	Active	Status
AvayaIntegration	Avaya CM active	✗	✗

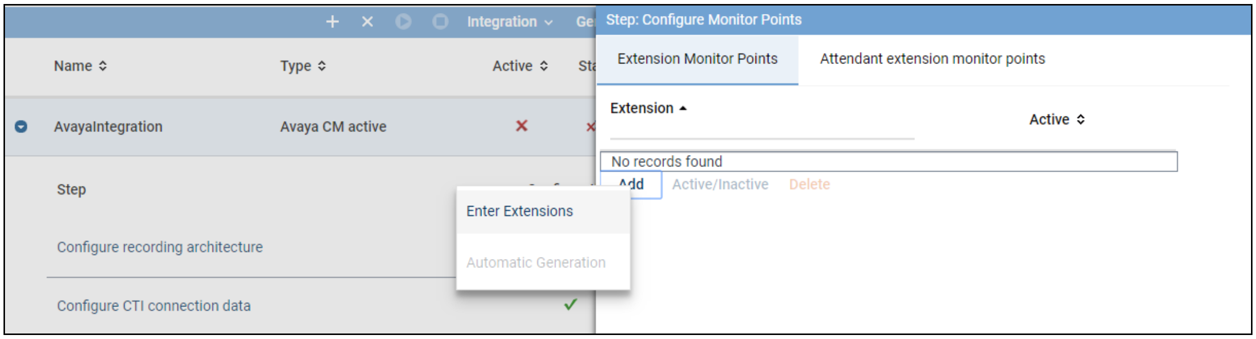
Step	Configuration
Configure recording architecture	✓
Configure CTI connection data	✓
Configure monitor points	✗
Configure recording servers	✓
Configure add-on	✓
Configure general settings	✓

AvayaIntegration

Details*

Name*	AvayaIntegration
PBX	AvayaCM
Integration type	Avaya CM active
Status integration	Inactive
Integration	

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
AvayaIntegration	Avaya CM active	✗

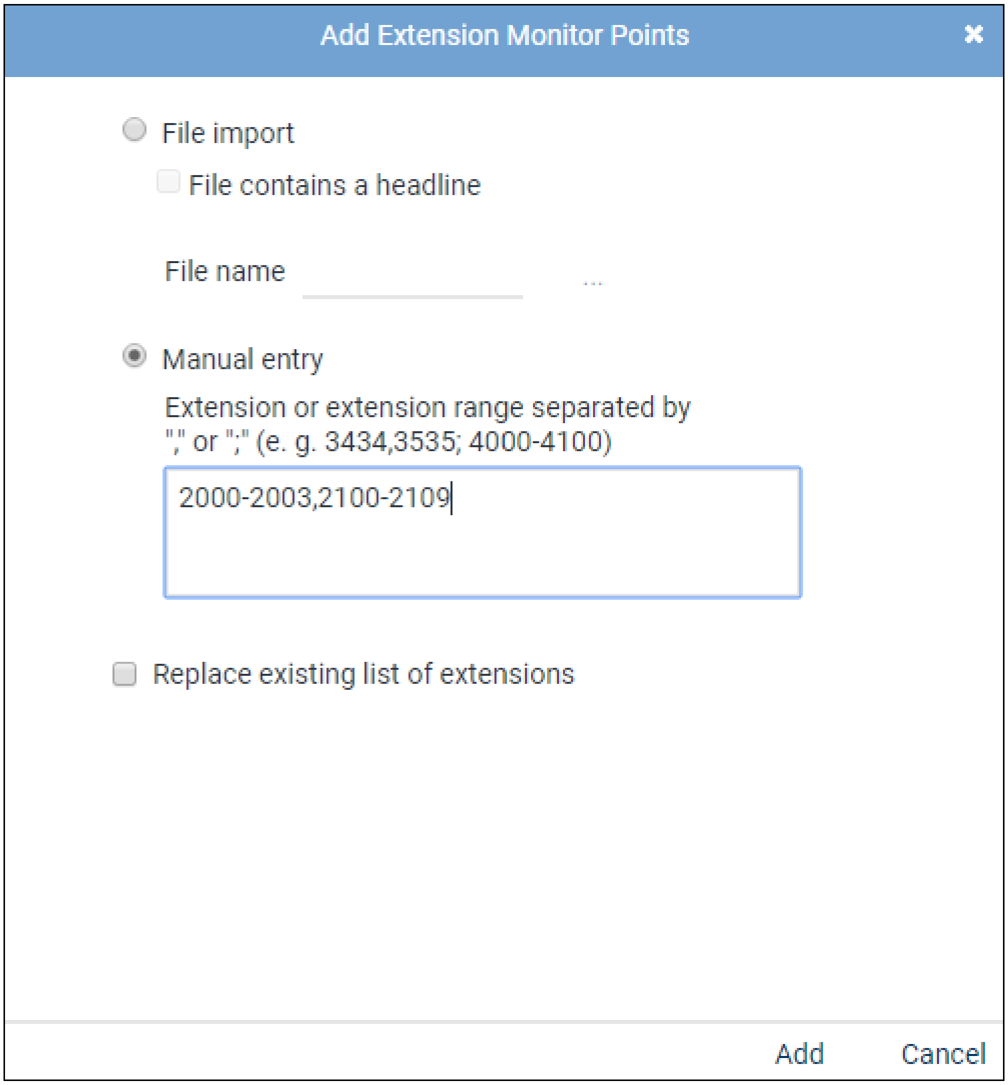
Step
Configure recording architecture
Configure CTI connection data

Step: Configure Monitor Points

Extension Monitor Points | Attendant extension monitor points

Extension	Active
No records found	

Enter the extensions to be monitored or recorded (**Section 5.5** and **Section 5.6**) and click on **Add** once complete.



Add Extension Monitor Points

○ File import

□ File contains a headline

File name

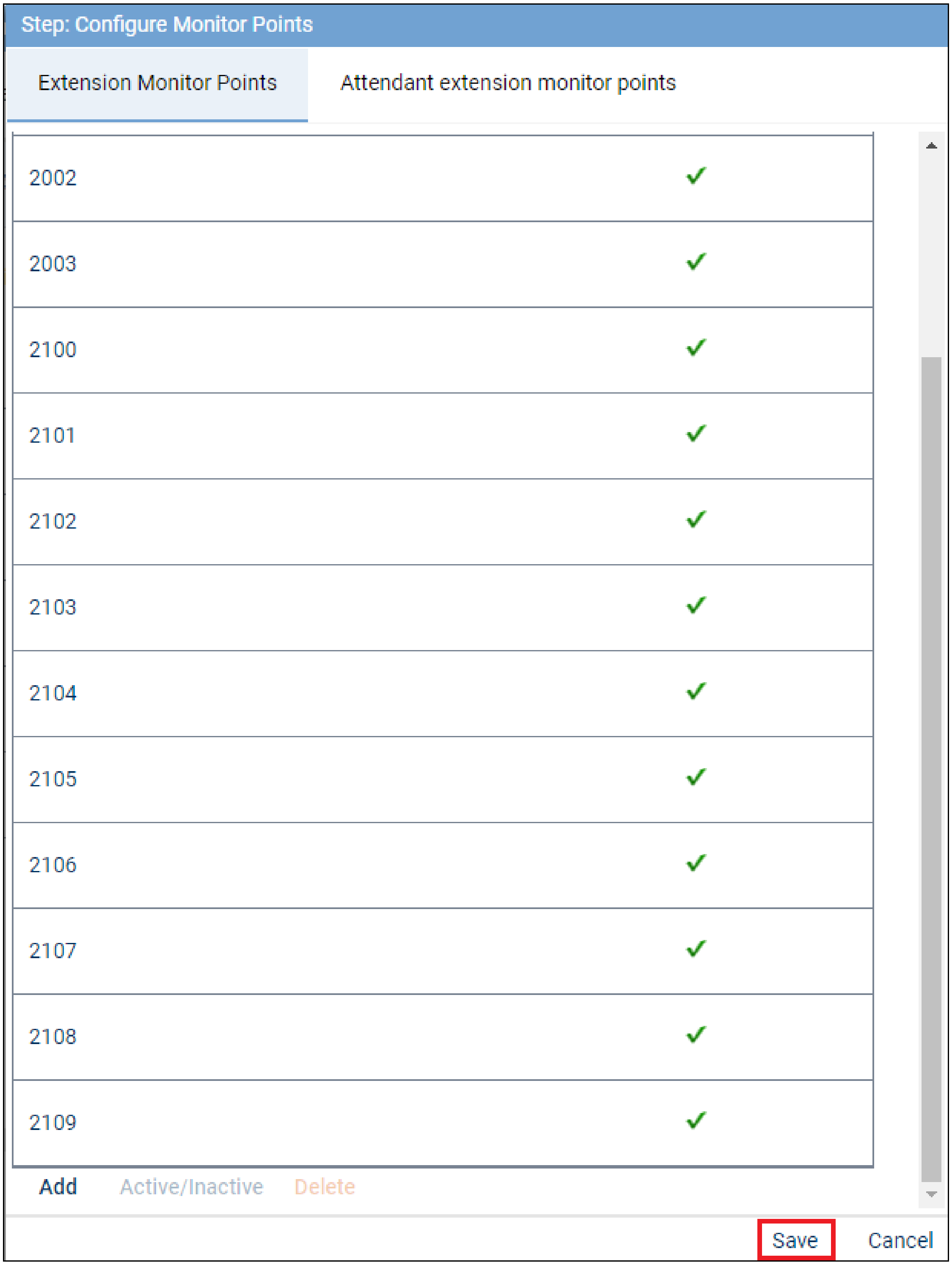
● Manual entry

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

2000-2003,2100-2109

□ Replace existing list of extensions

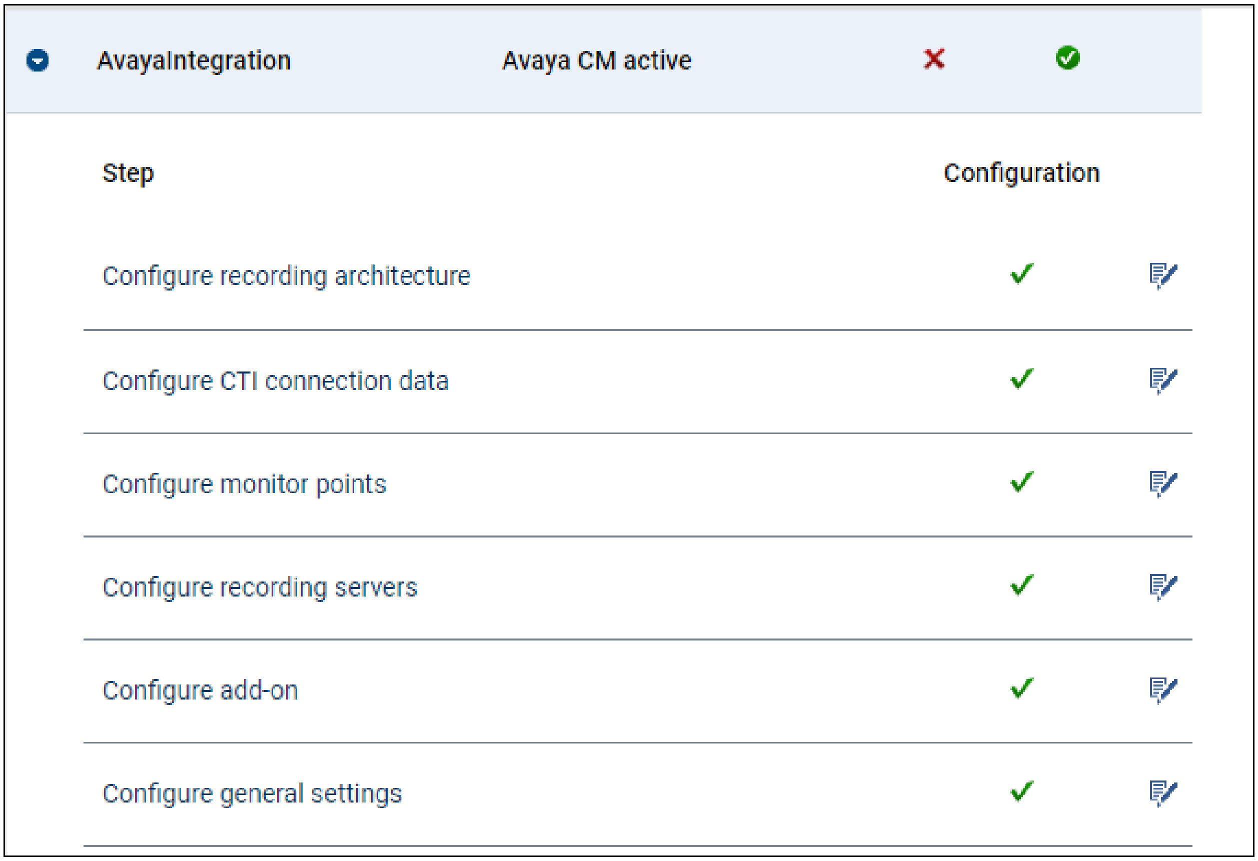
The extensions that will be recorded show in the right window. Once complete click on **Save** at the bottom of the screen.


Step: Configure Monitor Points
Extension Monitor Points
Attendant extension monitor points

2002	✓
2003	✓
2100	✓
2101	✓
2102	✓
2103	✓
2104	✓
2105	✓
2106	✓
2107	✓
2108	✓
2109	✓

Add
Active/Inactive
Delete
Save
Cancel

All the configuration should be showing green now as displayed below.



AvayaIntegration Avaya CM active ✗ ✓

Step	Configuration	
Configure recording architecture	✓	✎
Configure CTI connection data	✓	✎
Configure monitor points	✓	✎
Configure recording servers	✓	✎
Configure add-on	✓	✎
Configure general settings	✓	✎

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.**

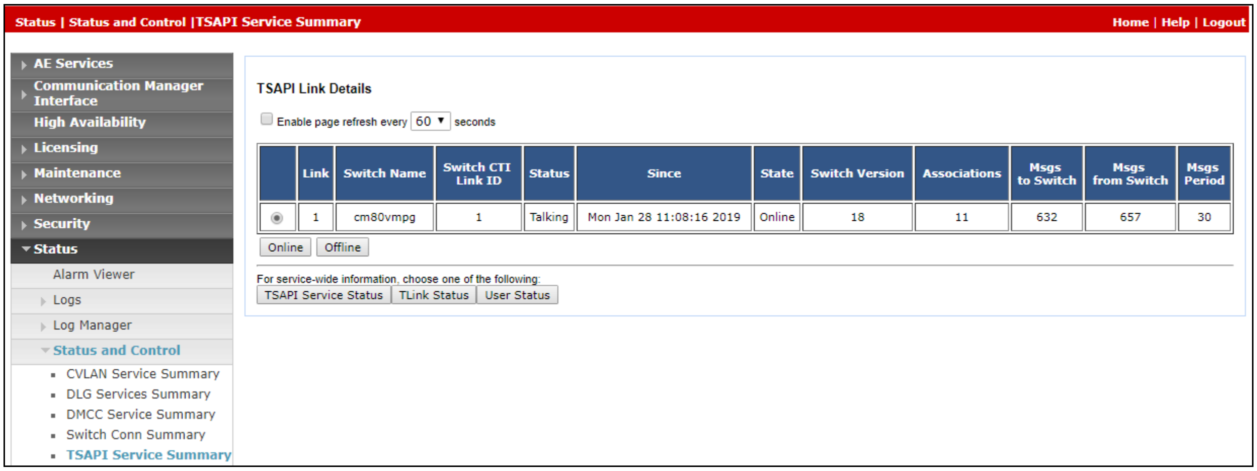
```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

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

1          8      no        aes80vmpg      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	cm80vmpg	1	Talking	Mon Jan 28 11:08:16 2019	Online	18	11	632	657	30

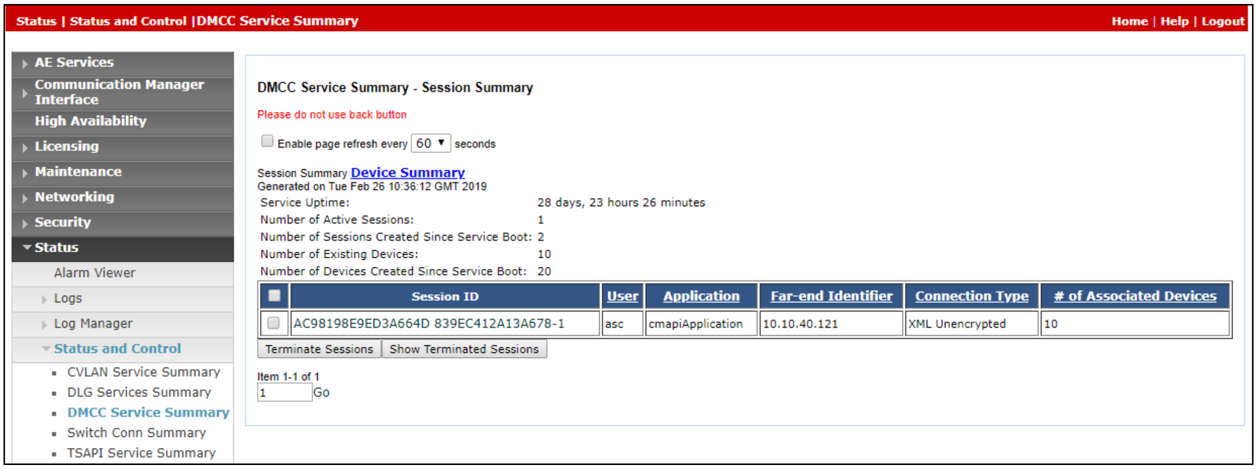
Online Offline

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

TSAPI Service Status TLink Status User Status

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 **10.10.40.121**. The **Application** is shown as **cmapiApplication,** and the **Far-end Identifier** is given as the IP address **10.10.40.121** 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 Tue Feb 26 10:36:12 GMT 2019

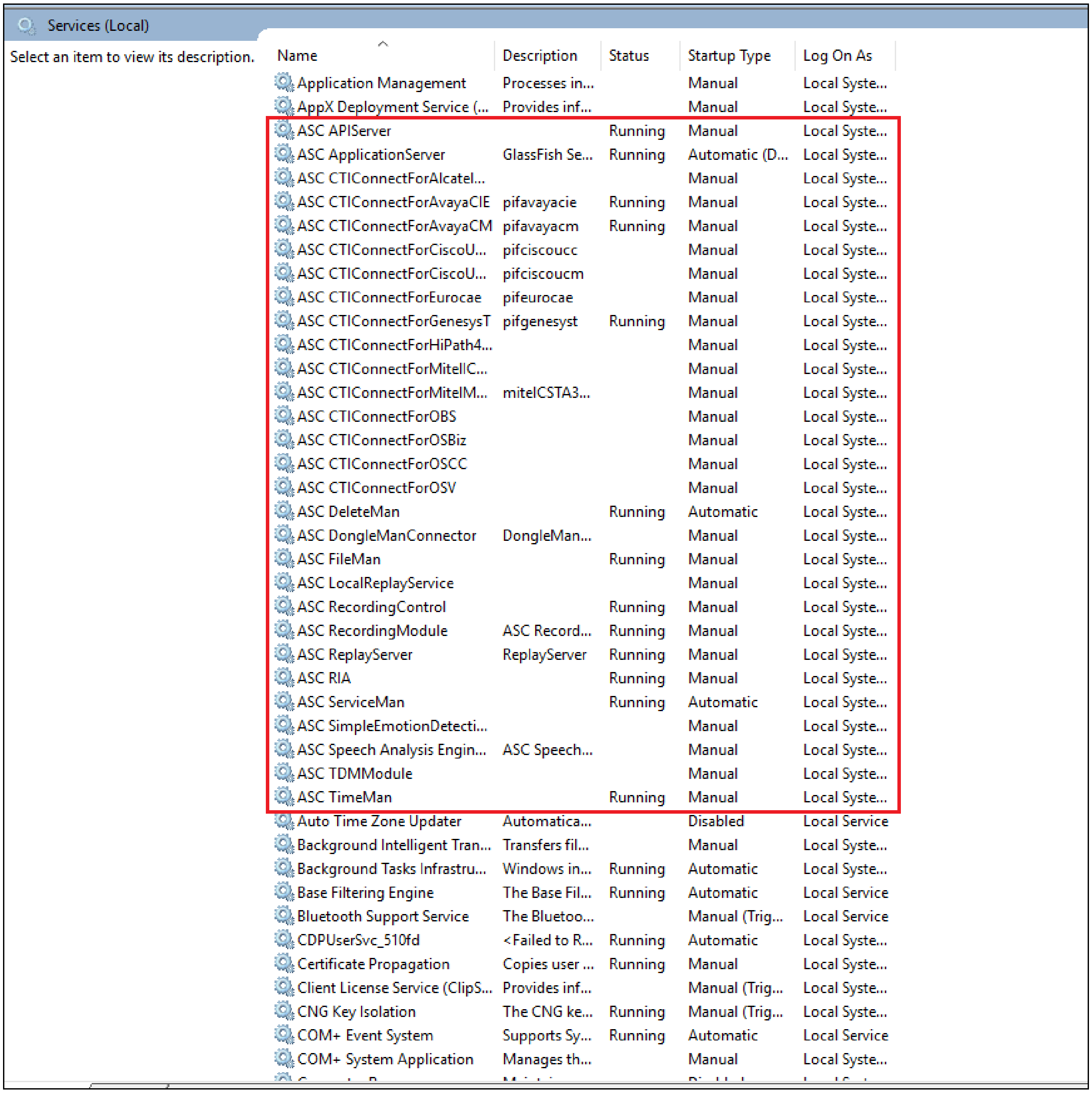
```
Service Uptime:                           28 days, 23 hours 26 minutes
Number of Active Sessions:                1
Number of Sessions Created Since Service Boot: 2
Number of Existing Devices:               10
Number of Devices Created Since Service Boot:  20
```

□	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
□	AC98198E9ED3A664D 839EC412A13A678-1	asc	cmapiApplication	10.10.40.121	XML Unencrypted	10

Item 1-1 of 1
1 Go

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.



Services (Local)

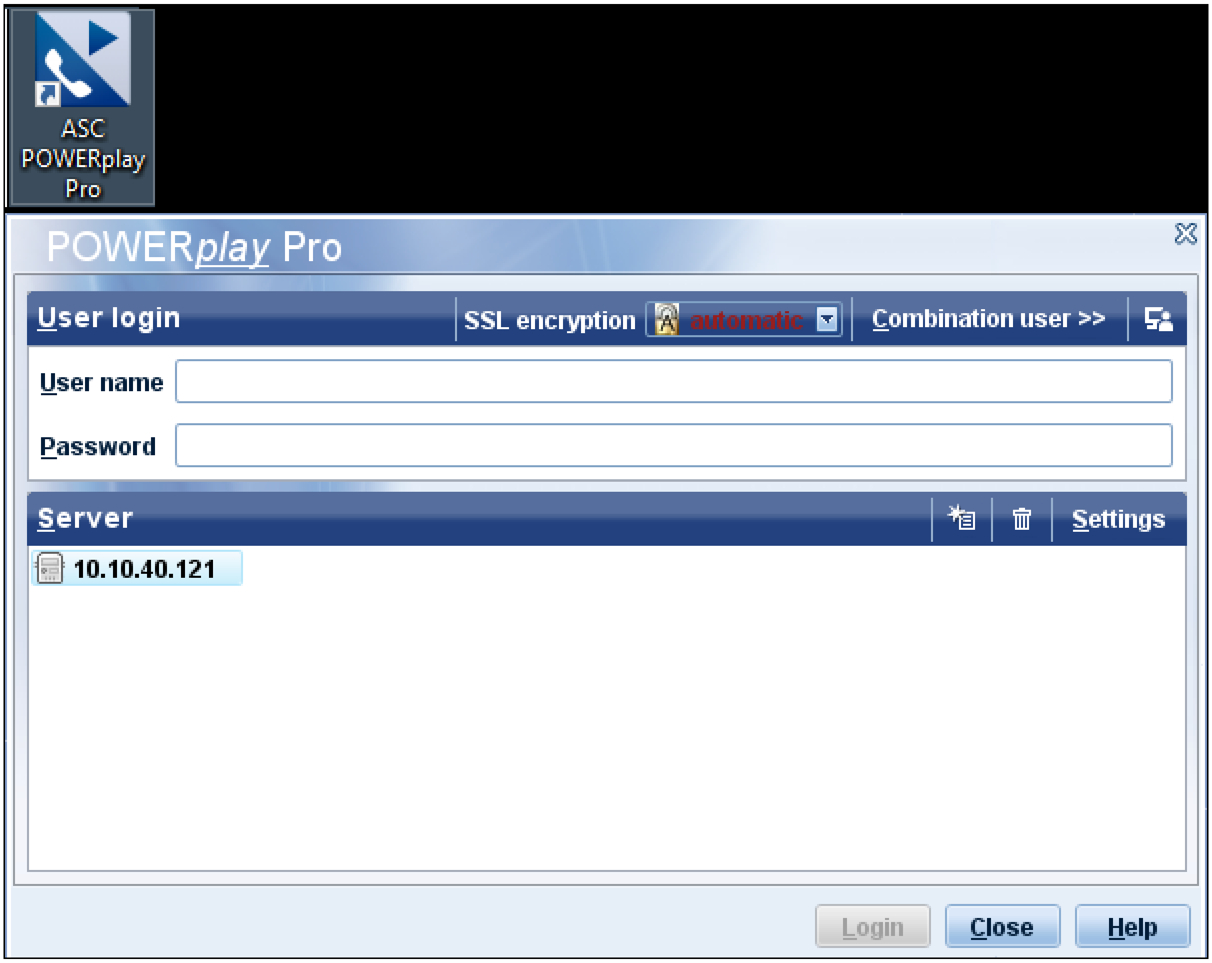
Select an item to view its description.

Name	Description	Status	Startup Type	Log On As
Application Management	Processes in...		Manual	Local Syste...
AppX Deployment Service (...	Provides inf...		Manual	Local Syste...
ASC APIServer		Running	Manual	Local Syste...
ASC ApplicationServer	GlassFish Se...	Running	Automatic (D...	Local Syste...
ASC CTIConnectForAlcatel...			Manual	Local Syste...
ASC CTIConnectForAvayaCIE	pifavayacie	Running	Manual	Local Syste...
ASC CTIConnectForAvayaCM	pifavayacm	Running	Manual	Local Syste...
ASC CTIConnectForCiscoU...	pifciscoucc		Manual	Local Syste...
ASC CTIConnectForCiscoU...	pifciscoucm		Manual	Local Syste...
ASC CTIConnectForEurocae	pifeurocae		Manual	Local Syste...
ASC CTIConnectForGenesysT	pifgenesyst	Running	Manual	Local Syste...
ASC CTIConnectForHiPath4...			Manual	Local Syste...
ASC CTIConnectForMitelIC...			Manual	Local Syste...
ASC CTIConnectForMitelM...	mitelCSTA3...		Manual	Local Syste...
ASC CTIConnectForOBS			Manual	Local Syste...
ASC CTIConnectForOSBiz			Manual	Local Syste...
ASC CTIConnectForOSCC			Manual	Local Syste...
ASC CTIConnectForOSV			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	ASC Record...	Running	Manual	Local Syste...
ASC ReplayServer	ReplayServer	Running	Manual	Local Syste...
ASC RIA		Running	Manual	Local Syste...
ASC ServiceMan		Running	Automatic	Local Syste...
ASC SimpleEmotionDetecti...			Manual	Local Syste...
ASC Speech Analysis Engin...	ASC Speech...		Manual	Local Syste...
ASC TDMModule			Manual	Local Syste...
ASC TimeMan		Running	Manual	Local Syste...
Auto Time Zone Updater	Automatica...		Disabled	Local Service
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
Bluetooth Support Service	The Bluetoo...		Manual (Trig...	Local Service
CDPUserSvc_510fd	<Failed to R...	Running	Automatic	Local Syste...
Certificate Propagation	Copies user ...	Running	Manual	Local Syste...
Client License Service (ClipS...	Provides inf...		Manual (Trig...	Local Syste...
CNG Key Isolation	The CNG ke...	Running	Manual (Trig...	Local Syste...
COM+ Event System	Supports Sy...	Running	Automatic	Local Service
COM+ System Application	Manages th...		Manual	Local Syste...

8.4. Verify ASC EVOIPneo active Capture and Playback

The playback of ASC recordings is achieved by running an application called **ASC POWERplayPro** from a local PC.

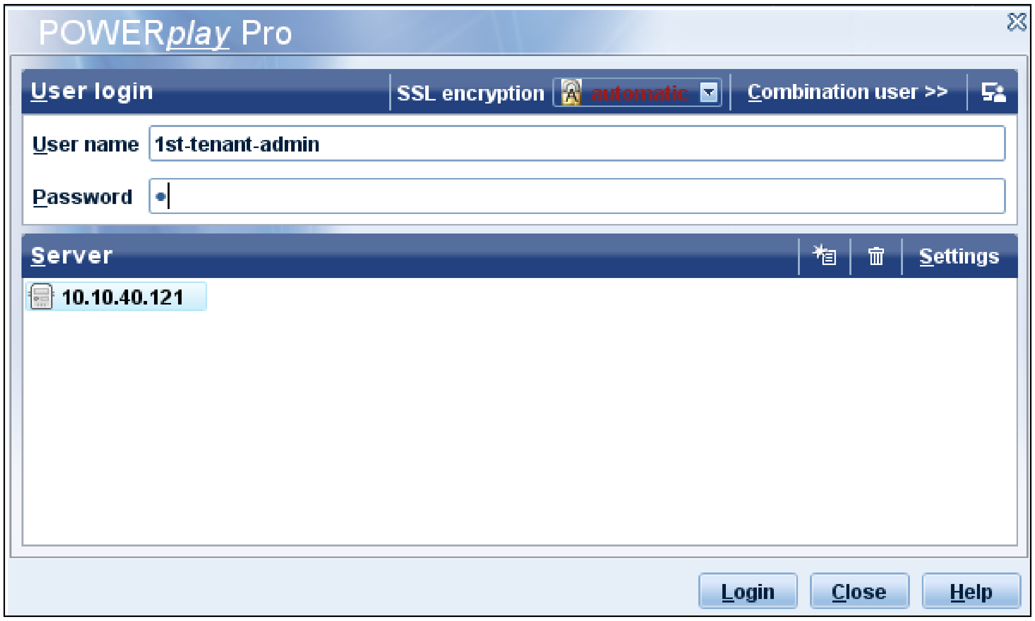
Double click on the shortcut icon and the **POWER*play* Pro** window appears as shown below.



SSL encryption automatic

10.10.40.121

Enter the appropriate **User name** and **Password** and click on **Login**.

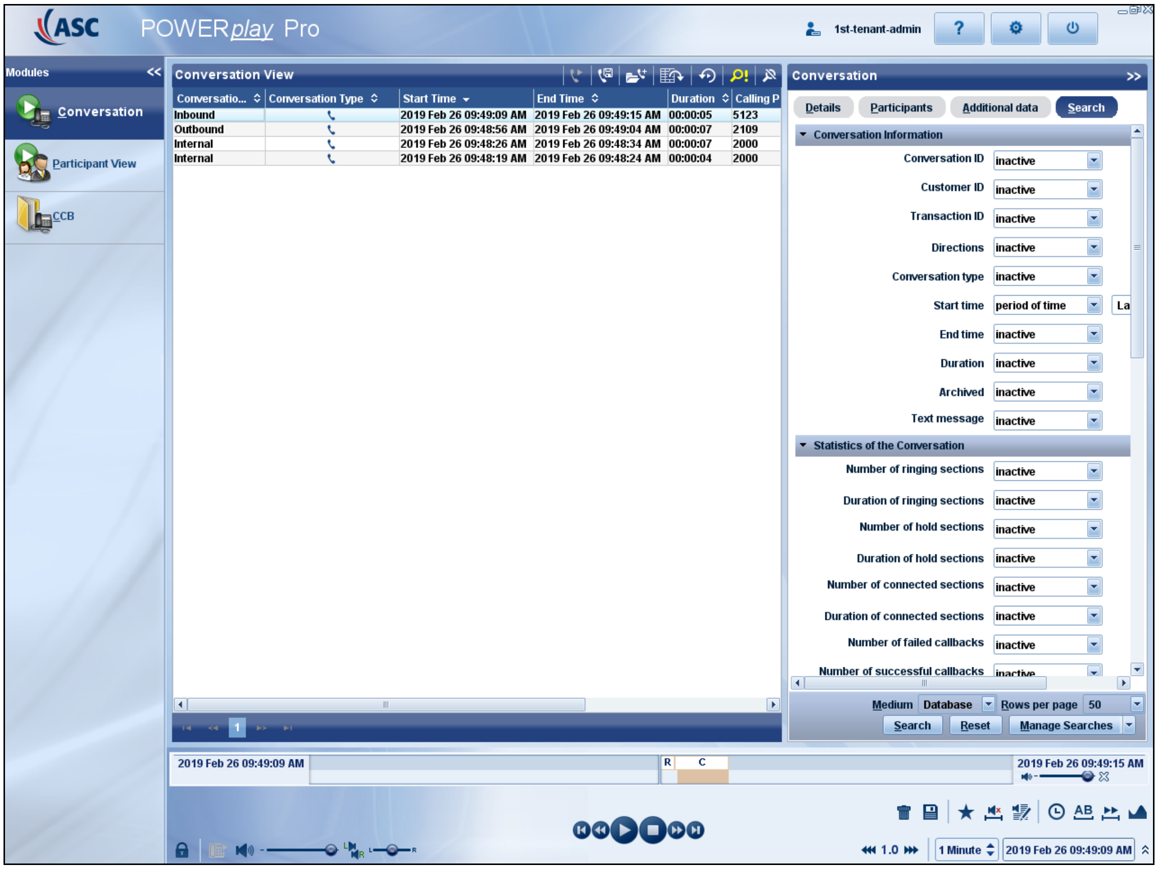


User name: 1st-tenant-admin

Password: •

10.10.40.121

The following window is opened with any recordings appearing in the main window. By highlighting a recording this can be played back at the bottom of the screen.



Conversatio...	Conversation Type	Start Time	End Time	Duration	Calling P
Inbound	☎	2019 Feb 26 09:49:09 AM	2019 Feb 26 09:49:15 AM	00:00:05	5123
Outbound	☎	2019 Feb 26 09:48:56 AM	2019 Feb 26 09:49:04 AM	00:00:07	2109
Internal	☎	2019 Feb 26 09:48:26 AM	2019 Feb 26 09:48:34 AM	00:00:07	2000
Internal	☎	2019 Feb 26 09:48:19 AM	2019 Feb 26 09:48:24 AM	00:00:04	2000

Conversation Information

Conversation ID	inactive
Customer ID	inactive
Transaction ID	inactive
Directions	inactive
Conversation type	inactive
Start time	period of time
End time	inactive
Duration	inactive
Archived	inactive
Text message	inactive

Statistics of the Conversation

Number of ringing sections	inactive
Duration of ringing sections	inactive
Number of hold sections	inactive
Duration of hold sections	inactive
Number of connected sections	inactive
Duration of connected sections	inactive
Number of failed callbacks	inactive
Number of successful callbacks	inactive

2019 Feb 26 09:49:09 AM

2019 Feb 26 09:49:15 AM

2019 Feb 26 09:49:09 AM

9. Conclusion

These Application Notes describe the configuration steps required for ASC EVOIPneo active V6.0 from ASC Technologies AG to successfully interoperate with Avaya Aura® Communication Manager R8.0 using Avaya Aura® Application Enablement Services R8.0. 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 8.0*

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.