Avaya Solution & Interoperability Test Lab

Application Notes for ASC EVOIPneo active V7.0 from ASC Technologies AG to interoperate with Avaya Aura® Communication Manager R10.1 and Avaya Aura® Application Enablement Services R10.1 - 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 V7.0 from ASC Technologies AG with Avaya Aura® Communication Manager R10.1 and Avaya Aura® Application Enablement Services R10.1 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 Avaya Aura® Application Enablement Services to capture the audio and call details for recording agent calls. ASC EVOIPneo active uses 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 Avaya Agent for Desktop.
- **Serviceability testing** - The behavior of ASC EVOIPneo under different simulated LAN 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.

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.

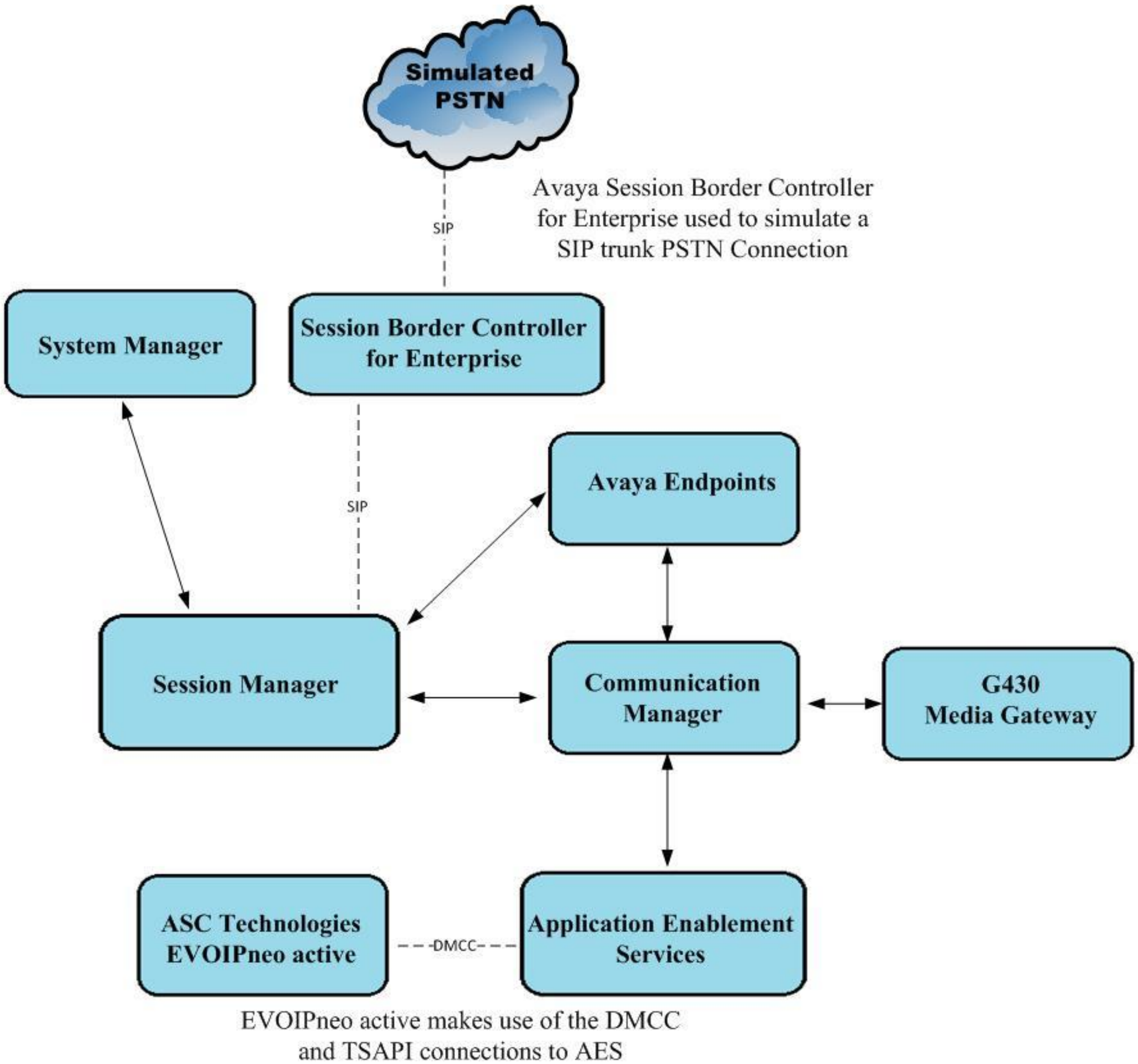


Figure 1: Avaya Aura® Communication Manager with Avaya Aura® Application Enablement Services, and ASC EVOIPneo active

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	10.1.0.0 Build No. – 10.1.0.0.537353 SW Update Revision No: 10.1.0.0.0614254
Avaya Aura® Session Manager	10.1 Build No. – 10.1.0.0.1010105
Avaya Aura® Communication Manager	10.1.0.1.0-SP1 Update ID 01.0.974.0-27372
Avaya Aura® Application Enablement Services	10.1.0 Build 10.1.0.2.0.12-0
Avaya Session Border Controller for Enterprise	8.1.3.0-31-21052
Avaya G430 Media Gateway	41.16.0/1
Avaya J100 Series H.323 Deskphone	6.8304
Avaya J100 Series SIP Deskphone	4.0.7.1.5
Avaya 9408 Digital Phone	2.00
Avaya Agent for Desktop	2.0.6.23.3005
Avaya Workplace for Windows	3.28.0.73
Avaya DECT Handsets	3725 DH4 (R3.3.11) 3720 DH3 (R3.3.11)
ASC EVOIPneo active running on MS Windows Server 2019	V7.0
ASC POWERplay Pro running on MS Windows 10 PC	V7.0

Note: All Avaya and ASC equipment were running on Virtual Servers.

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 IP addresses by using the command **display node-names ip** and noting the IP address for the **procr** and the AES.

```
display node-names ip                                         Page   1 of   2
                                 IP NODE NAMES
    Name              IP Address
SM100               10.10.40.12
aespri101x          10.10.40.16
aessec101x          10.10.40.46
g450                10.10.40.15
procr               10.10.40.13
```

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   3

                                   IP SERVICES
 Service      Enabled      Local        Local       Remote       Remote
  Type                     Node         Port        Node         Port
AESVCS          y          procr        8765
```

Go to **Page 3** of the **ip-services** form and enter the following values:

- **AE Services Server:** Name obtained from the AES server, in this case **aespri101x**.
- **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** Error! Reference source not found.. 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:        aespri101x          ********           y         in use
      2:        aessec101x          ********           y         in use
      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: 3990
     Type: ADJ-IP
                                                                    COR: 1
     Name: aespri101x
```

5.5. Configure H.323 Stations for Single Step Conference

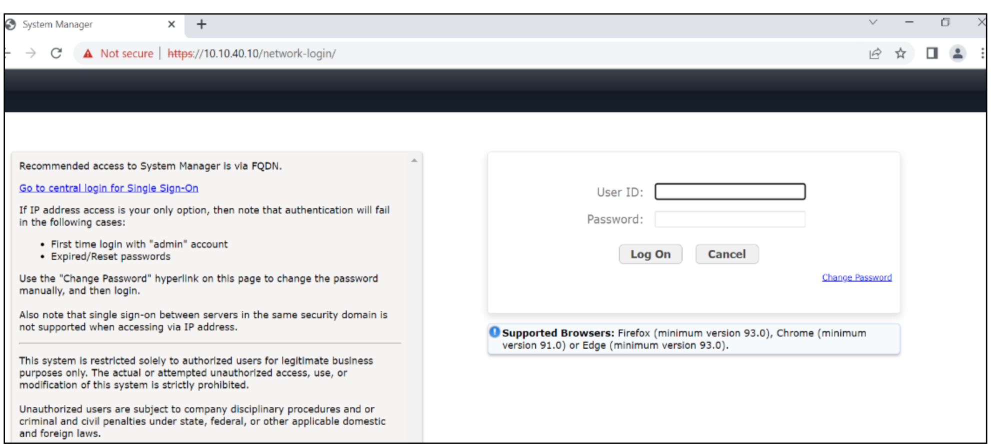
No changes were made during compliance testing for and H.323 stations that were tested. The screen below shows an example of a H.323 phone that was tested.

```
display station 3001                                            Page   1 of   6
                                     STATION

Extension: 3001                             Lock Messages? n
BCC: 0
     Type: 9608                         Security Code: 1234             TN: 1
     Port: S00101                       Coverage Path 1:               COR: 1
     Name: H323 3001                    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: 3001
            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
```

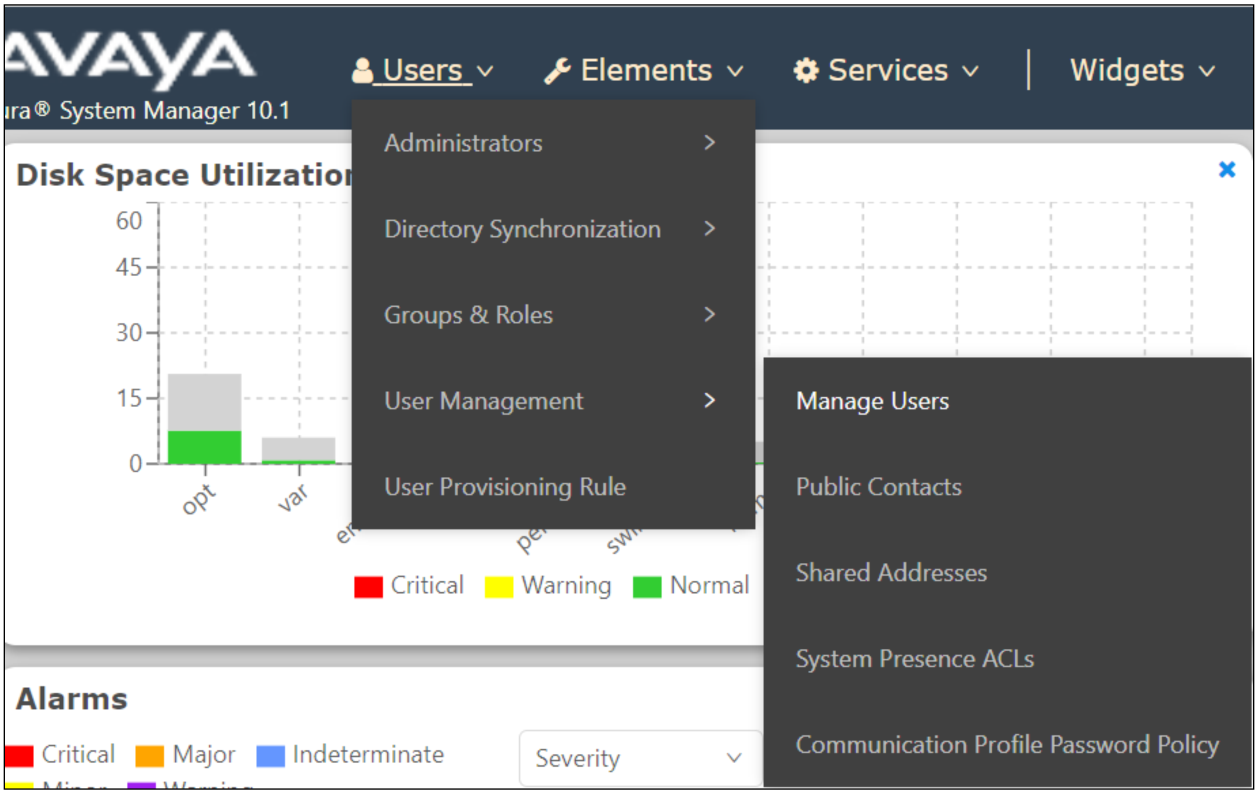
5.6. Configure SIP Stations for Single Step Conference

Each Avaya SIP endpoint or station that needs to be monitored for call recording will need to have the correct Class of Restriction assigned. Changes to SIP phones on Communication Manager must be carried out from System Manager. Access the System Manager using a Web Browser by entering **http://<FQDN >/network-login**, where **<FQDN>** is the fully qualified domain name of System Manager or the IP address of System Manager can be used as an alternative to the FQDN. Log in using appropriate credentials.

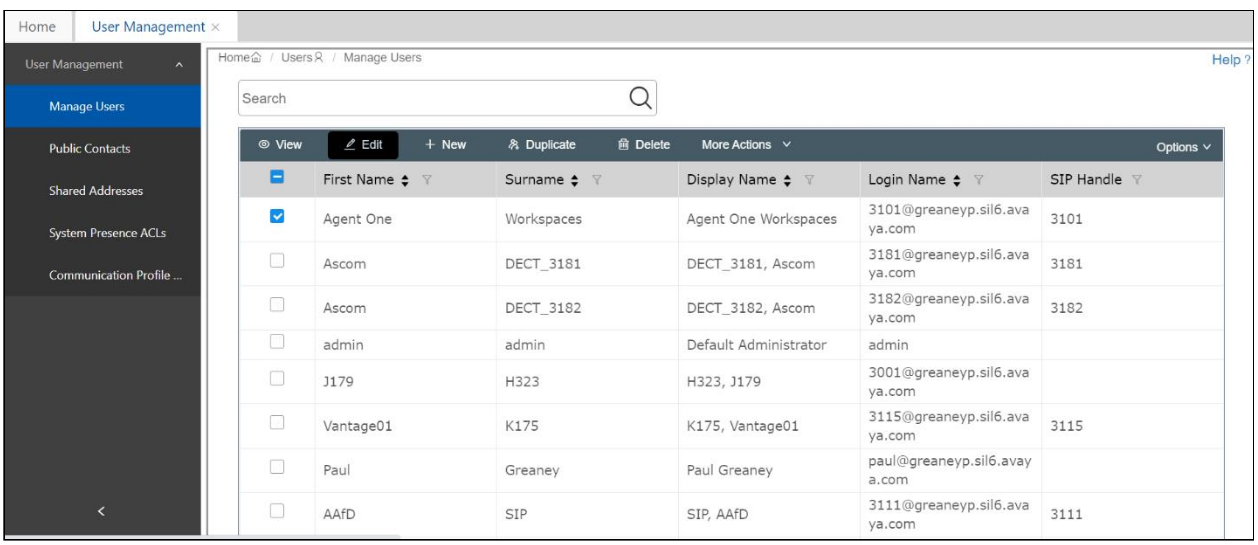
Note: The following shows changes to a SIP extension and assumes that the SIP extension has been programmed correctly and is fully functioning.



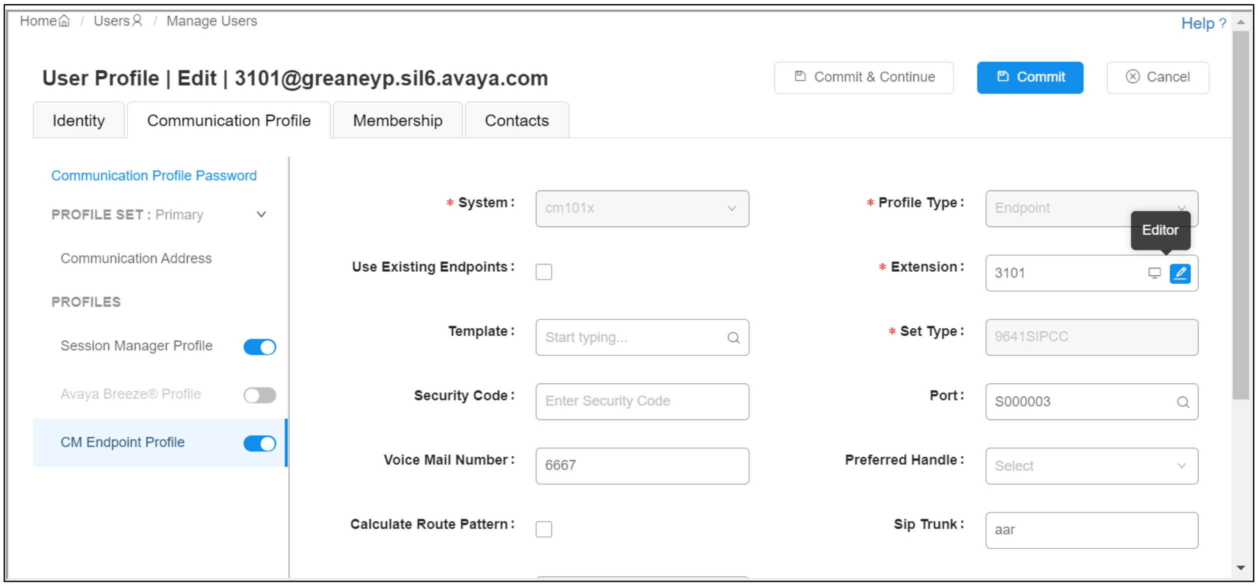
From the home page, click on **Users → User Management → Manage Users**, as shown below.



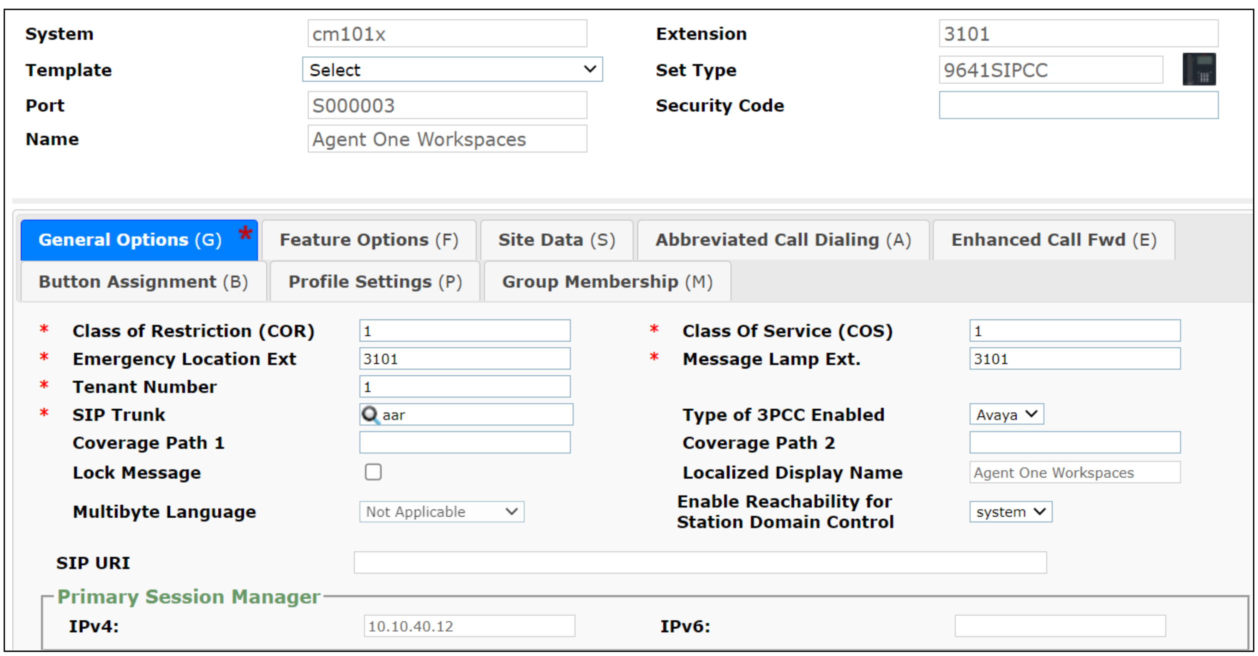
Click on **Manager Users** in the left window. Select the station to be edited and click on **Edit**.



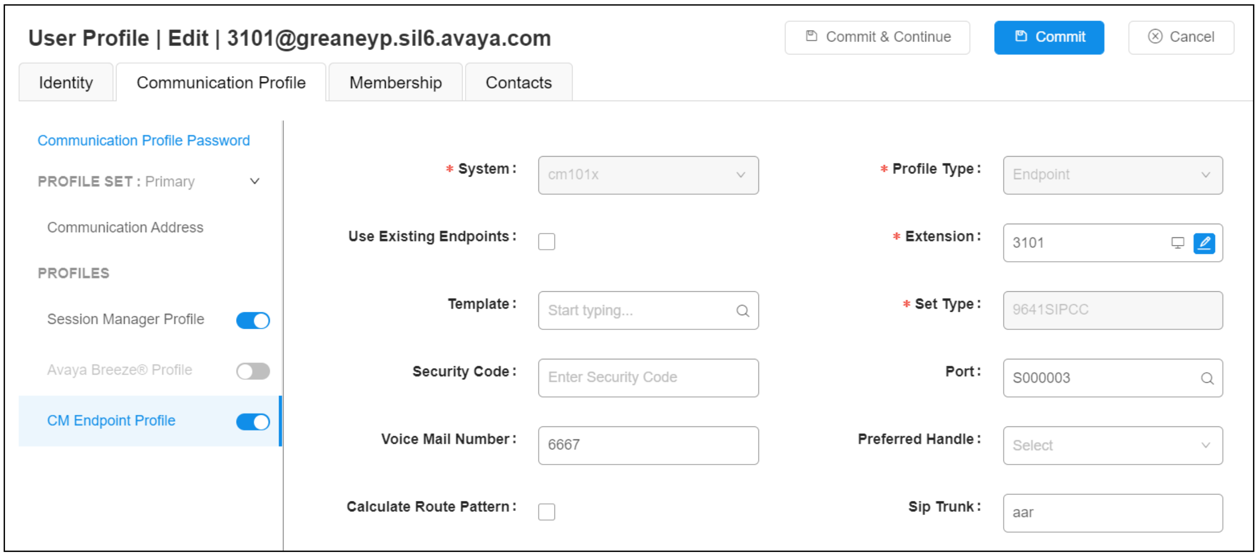
Click on the **CM Endpoint Profile** tab in the left window. Click on **Endpoint Editor** to make changes to the SIP station.



In the **General Options** tab, ensure that **Type of 3PCC Enabled** is set to **Avaya**. Click on **Done** at the bottom of the screen once this is set (not shown).



Click on **Commit** once this is done to save the changes.



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 **Section7.4.1**. Note the **Security Code** and ensure that **IP SoftPhone** is set to **y**.

```
add station 33001                                            Page   1 of   6
                                     STATION

Extension: 33001                       Lock Messages? n               BCC: 0
     Type: 9620                        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: 33001
            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

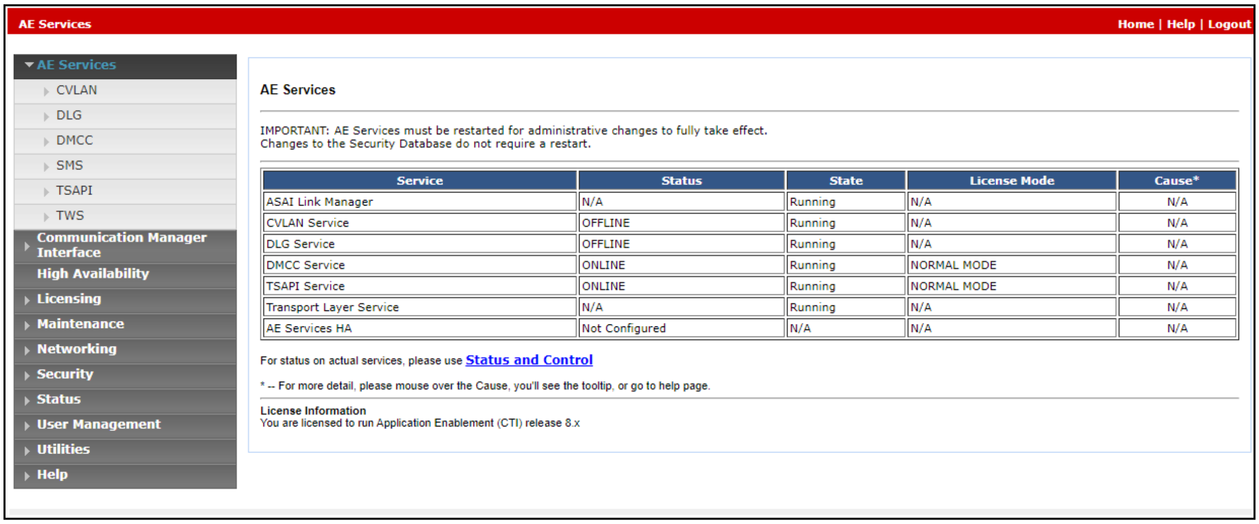
This section provides the procedures for configuring AES. The procedures fall into the following areas:

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

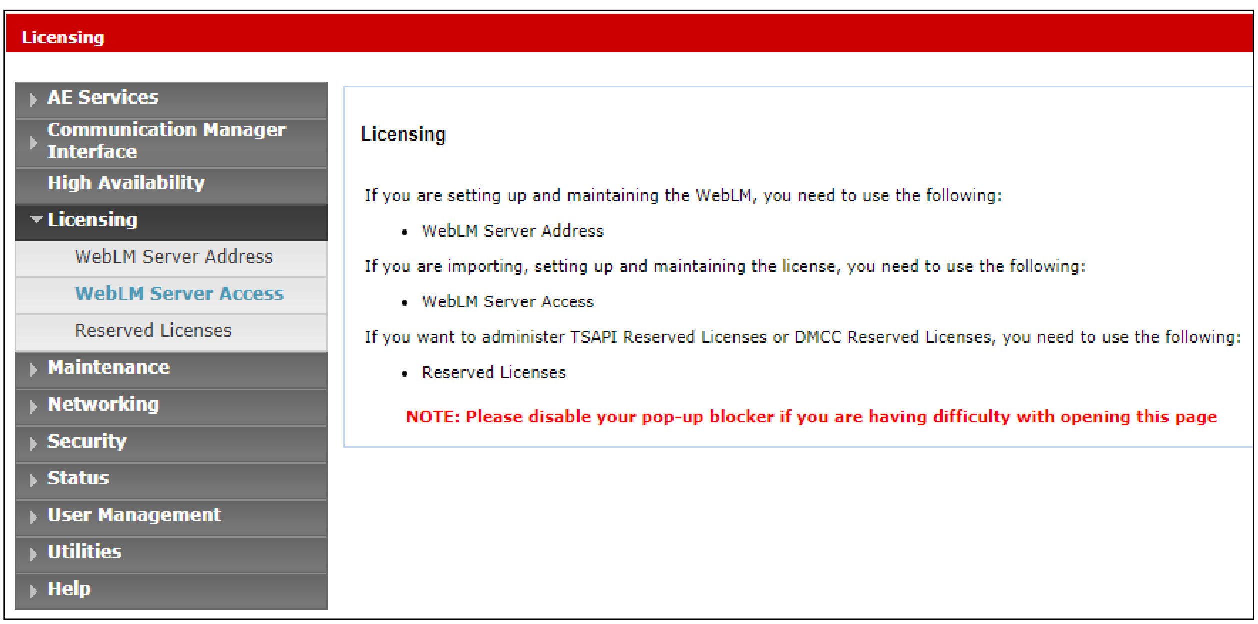
6.1. Verify Licensing

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.

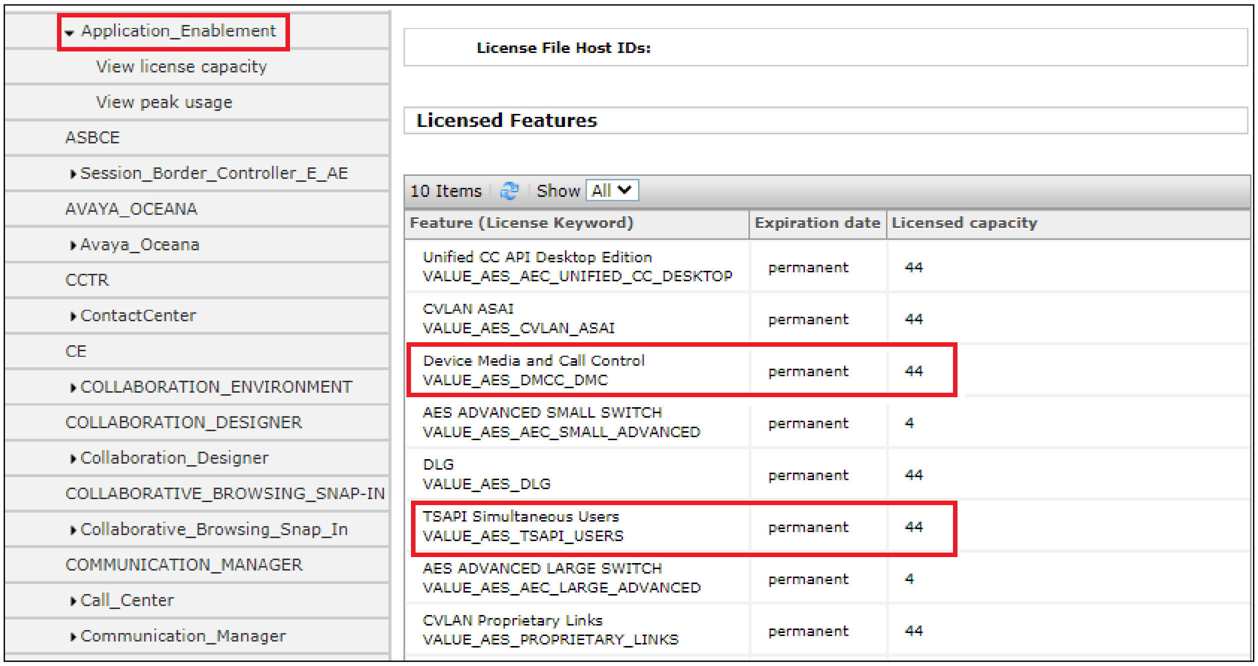
The Application Enablement Services Management Console appears displaying the **Welcome to OAM** screen (not shown). Select **AE Services** and verify that the TSAPI and DMCC Services are licensed by ensuring that **TSAPI Service** and **DMCC Service** are in the list of **Services** and that the **License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



The TSAPI and DMCC licenses are user licenses issued by the Web License Manager to which the Application Enablement Services server is pointed to. From the left window open **Licensing** and click on **WebLM Server Access** as shown below.

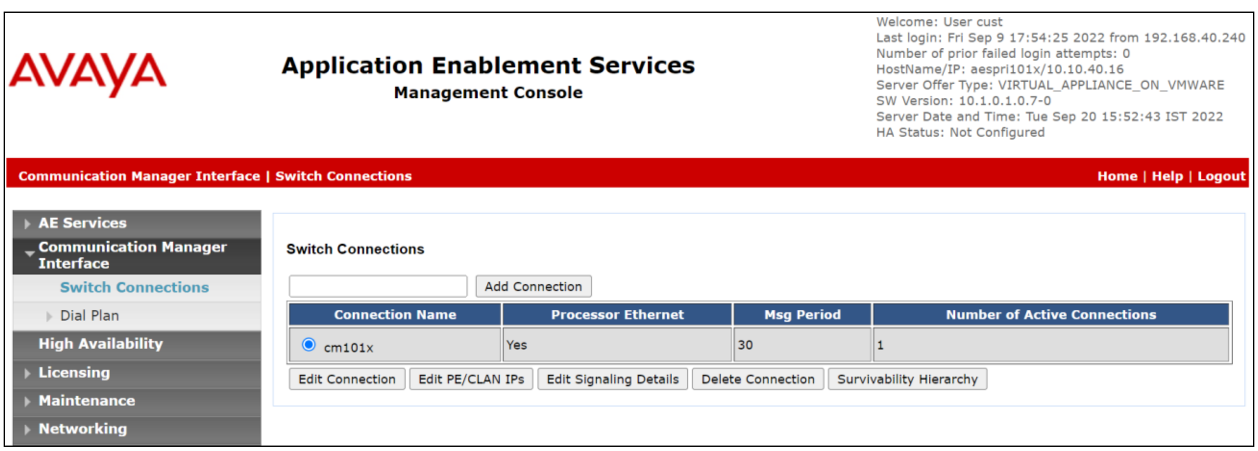


The following screen shows the available licenses for **TSAPI** and **DMCC** users.

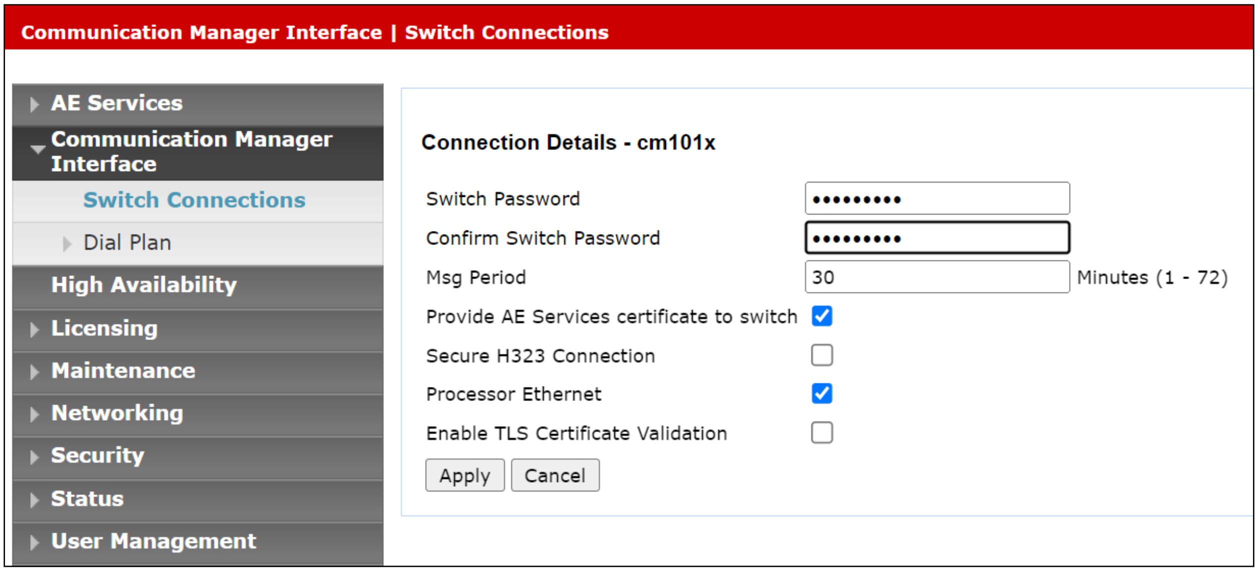


6.2. Create Switch Connection

Typically, the connection between the AES and Communication Manager is setup as part of the initial installation and would not usually be outlined in these Application Notes. Due to the nature of this particular setup with two connections from Communication Manager to two separate AES's the switch connection will be displayed on this section. From the AES Management Console navigate to **Communication Manager Interface → Switch Connections**, the connection to Communication Manager should be present as shown below but if one is not present one can be added by clicking on **Add Connection**.

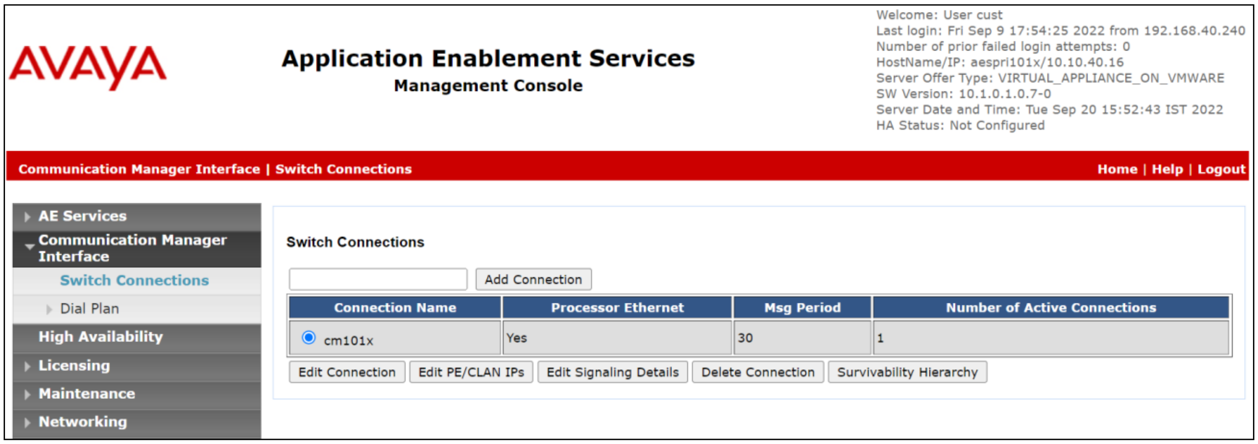


In the resulting screen, enter the **Switch Password**; the Switch Password must be the same as that entered into Communication Manager AE Services Administration screen via the **change ip-services** command, described in **Section** Error! Reference source not found.. **Secure H323 Connection** was left unticked, as shown below. Click **Apply** to save changes.

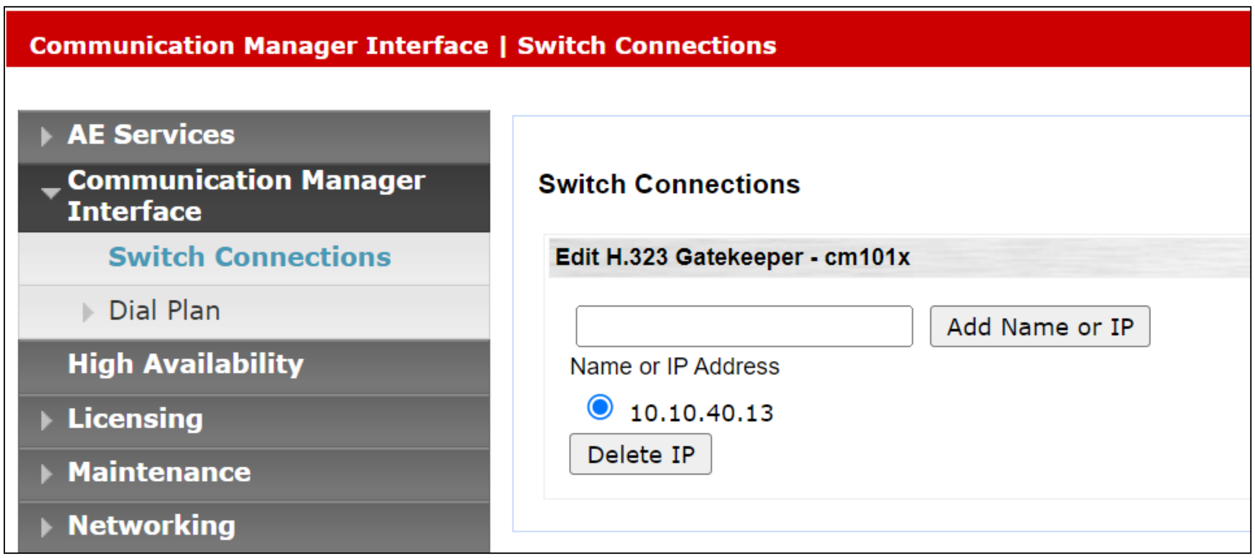


From the **Switch Connections** screen, select the radio button for the recently added switch connection and select the **Edit PE/CLAN IPs** button (not shown), see screen at the bottom of the previous page. In the resulting screen, enter the IP address of the procr as shown in **Section** Error! Reference source not found. that will be used for the AES connection and select the **Add/Edit Name or IP** button.

Clicking on **Edit Signaling Details** below brings up the H.323 Gatekeeper page.

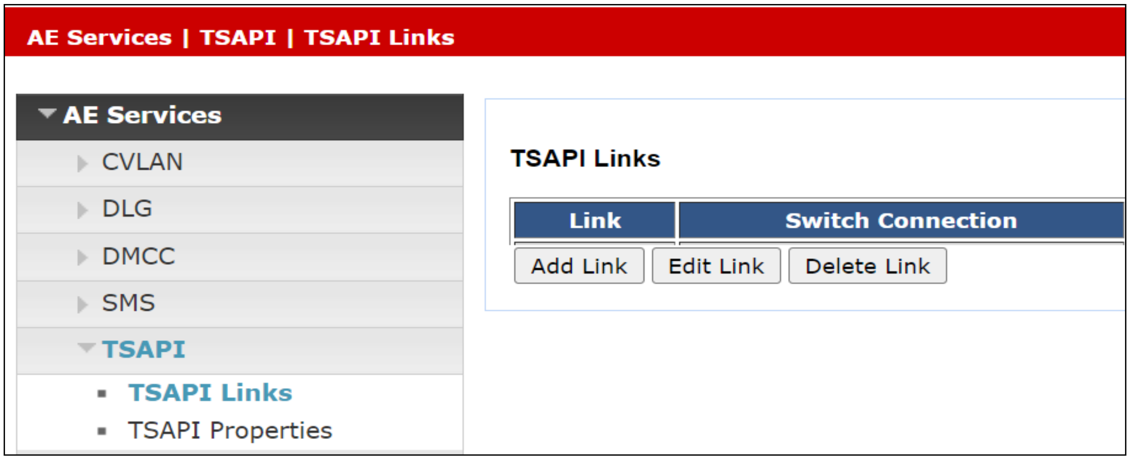


The IP address of Communication Manager is set for the **H.323 Gatekeeper**, as shown below.



6.3. Administer TSAPI link

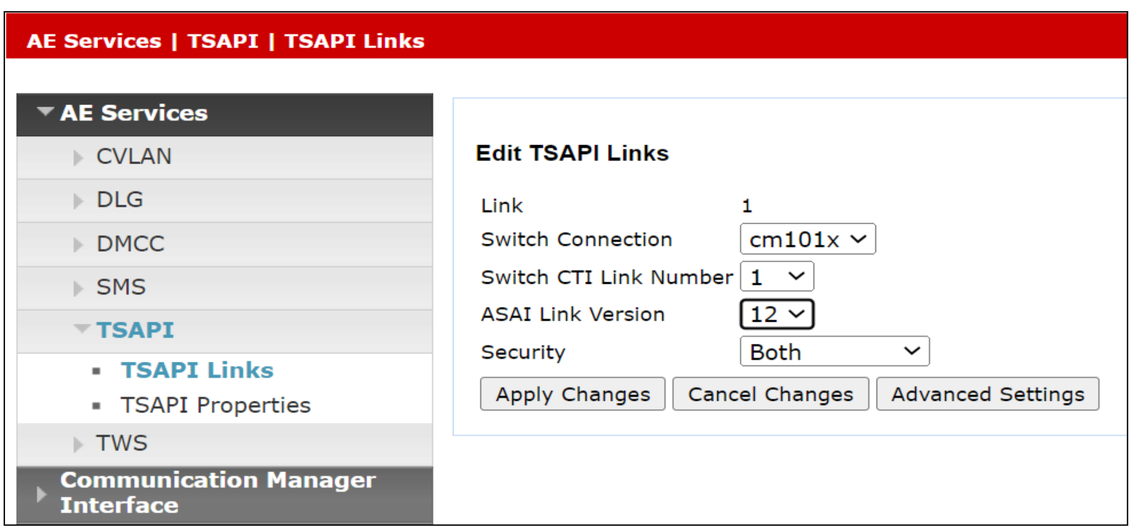
From the Application Enablement Services Management Console, select **AE Services** → **TSAPI** → **TSAPI Links**. Select **Add Link** button as shown in the screen below.



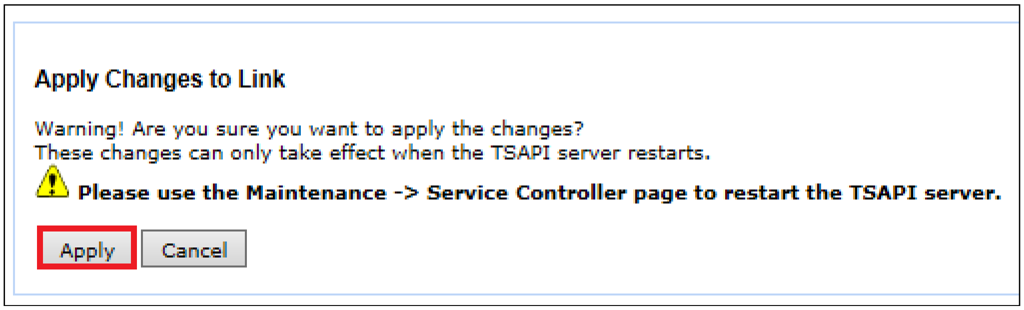
On the **Add TSAPI Links** screen (or the **Edit TSAPI Links** screen to edit a previously configured TSAPI Link as shown below), enter the following values:

- **Link:** Use the drop-down list to select an unused link number.
- **Switch Connection:** Choose the switch connection **cm101x**, 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 (the latest version available should be chosen).
- **Security:** This can be left at the default value of **both**.

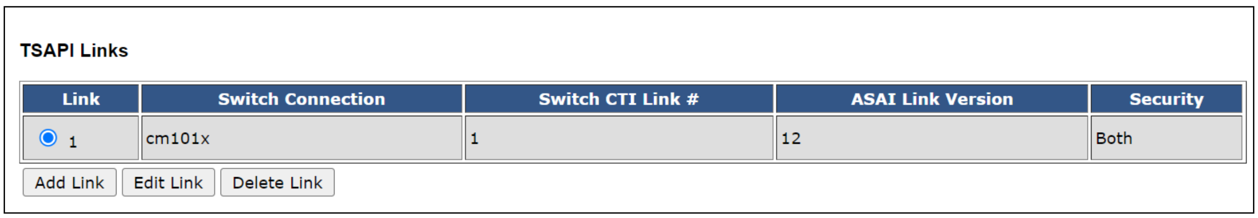
Once completed, select **Apply Changes**.



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



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



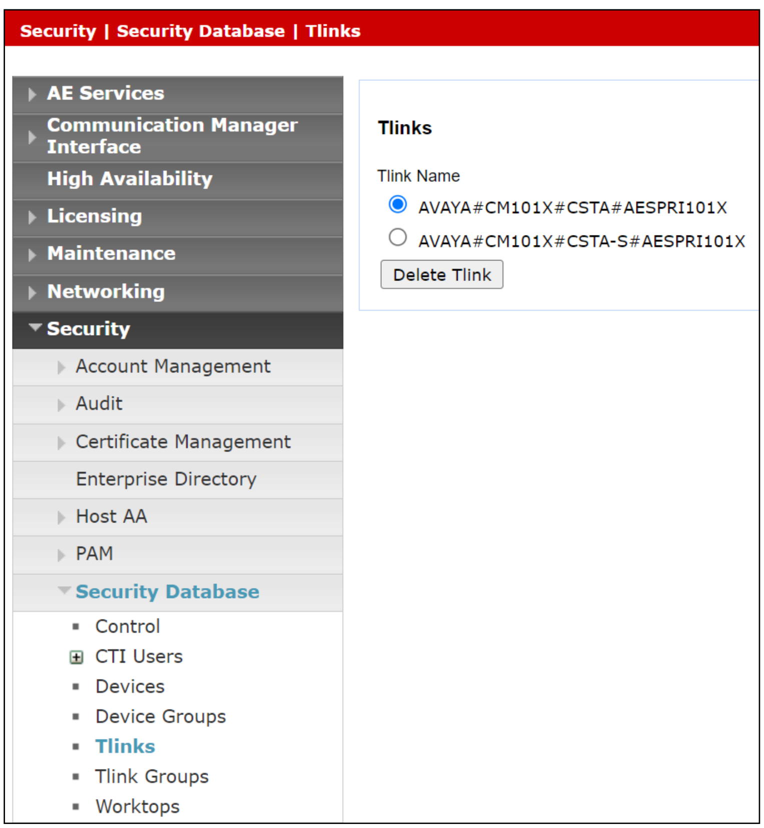
TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
1	cm101x	1	12	Both

Add Link | Edit Link | Delete Link

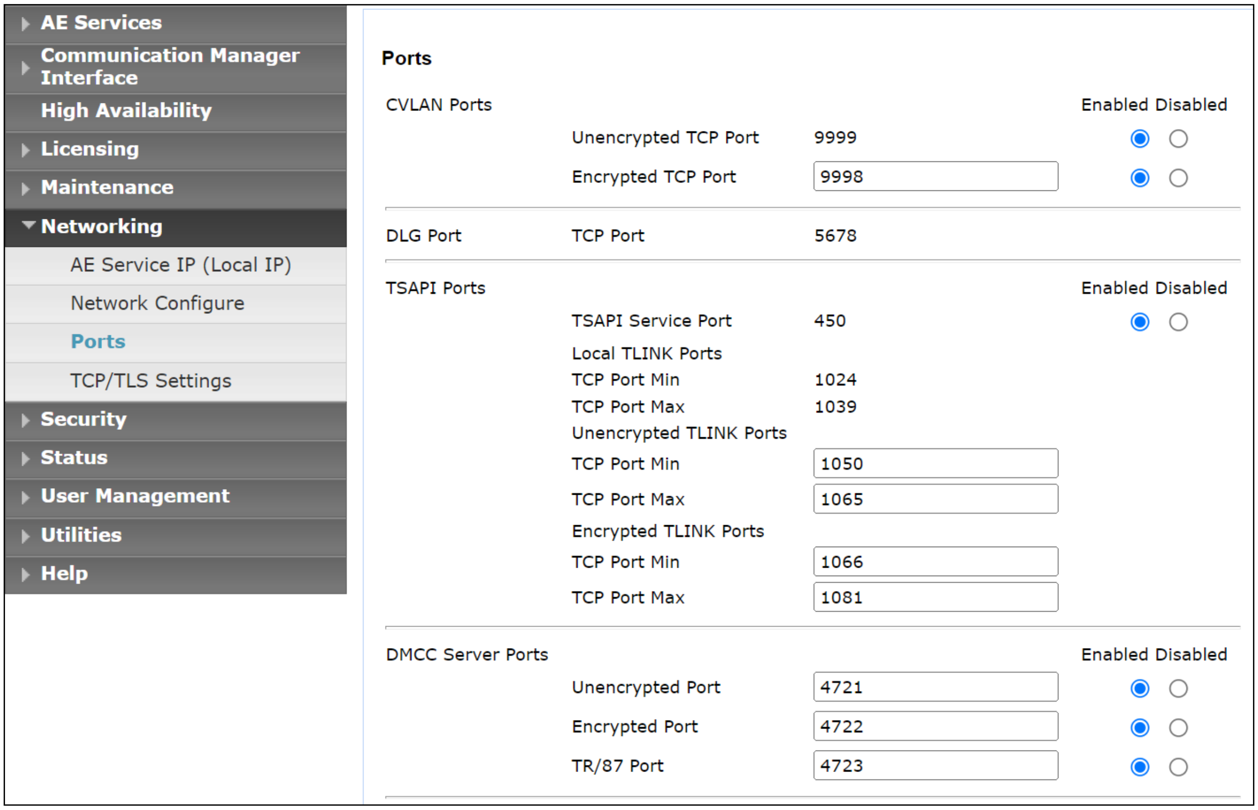
6.4. Identify Tlinks

Navigate to **Security → Security Database → Tlinks**. Verify the value of the **Tlink Name**.



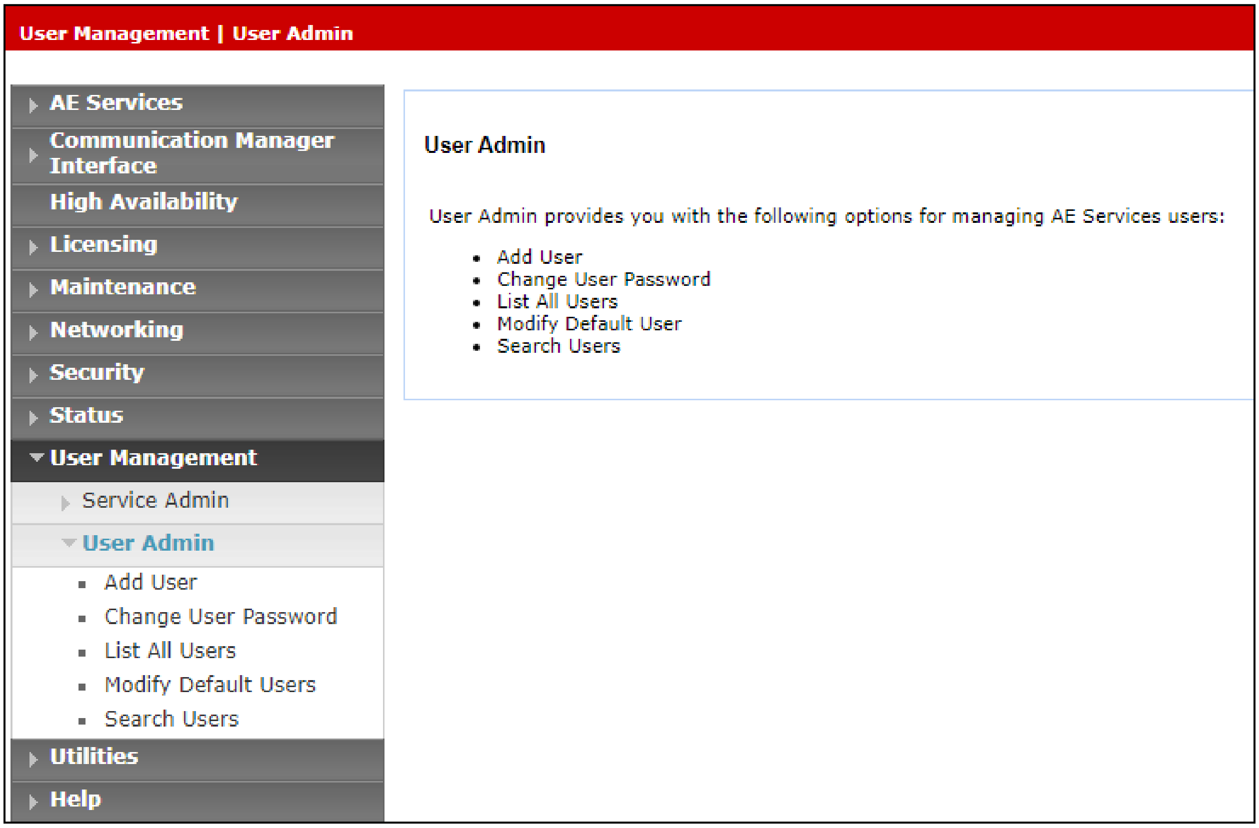
6.5. Configure Networking Ports

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**.



6.6. Create Avaya CTI User

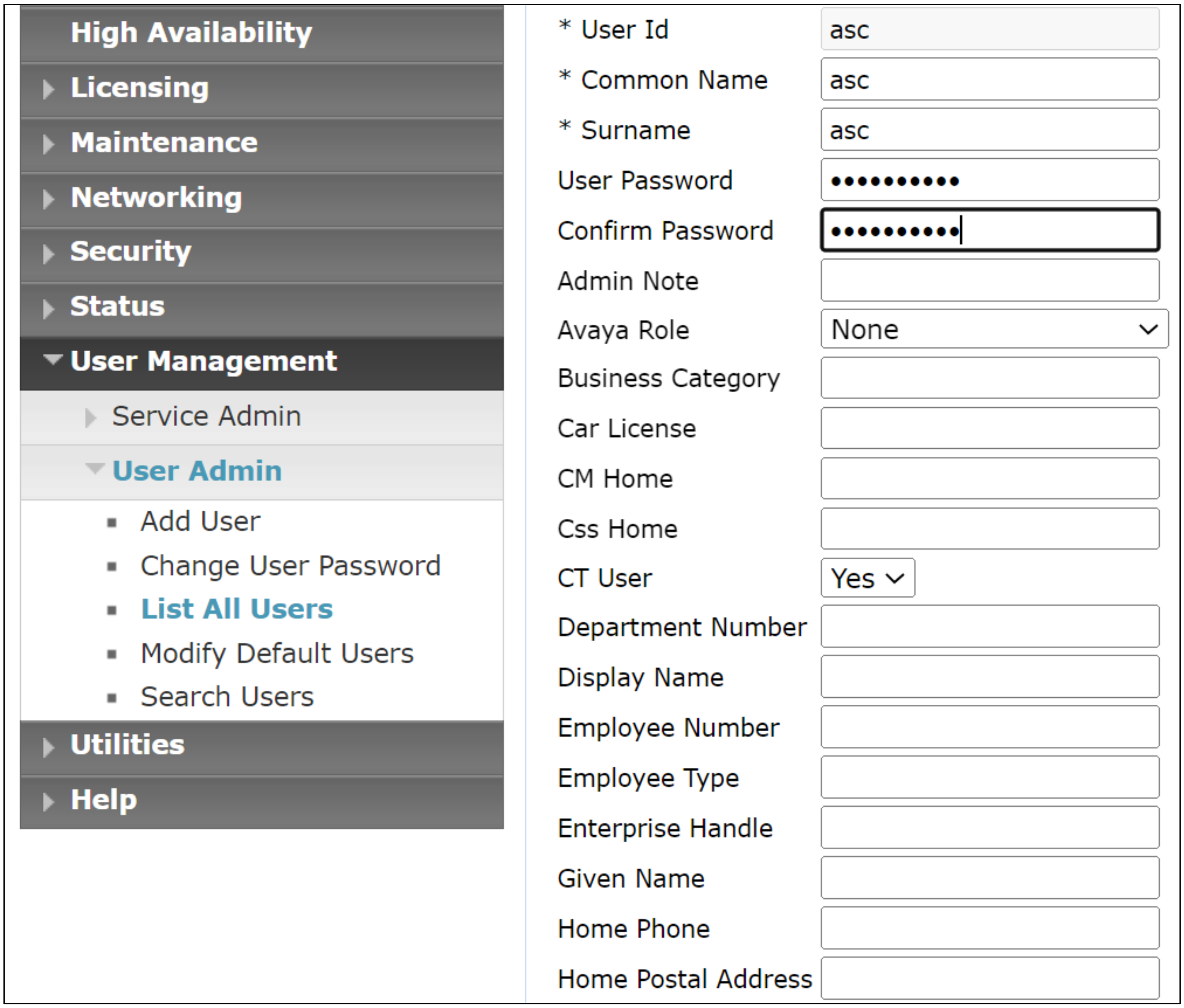
A User ID and password needs to be configured for the ASC EVOIPneo active to communicate as a TSAPI client with the Application Enablement Services server. Navigate to the **User Management → User Admin** screen then choose the **Add User** option.



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).



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

6.7. Configure Security

The CTI user and the database security are set here under **Security Database**.

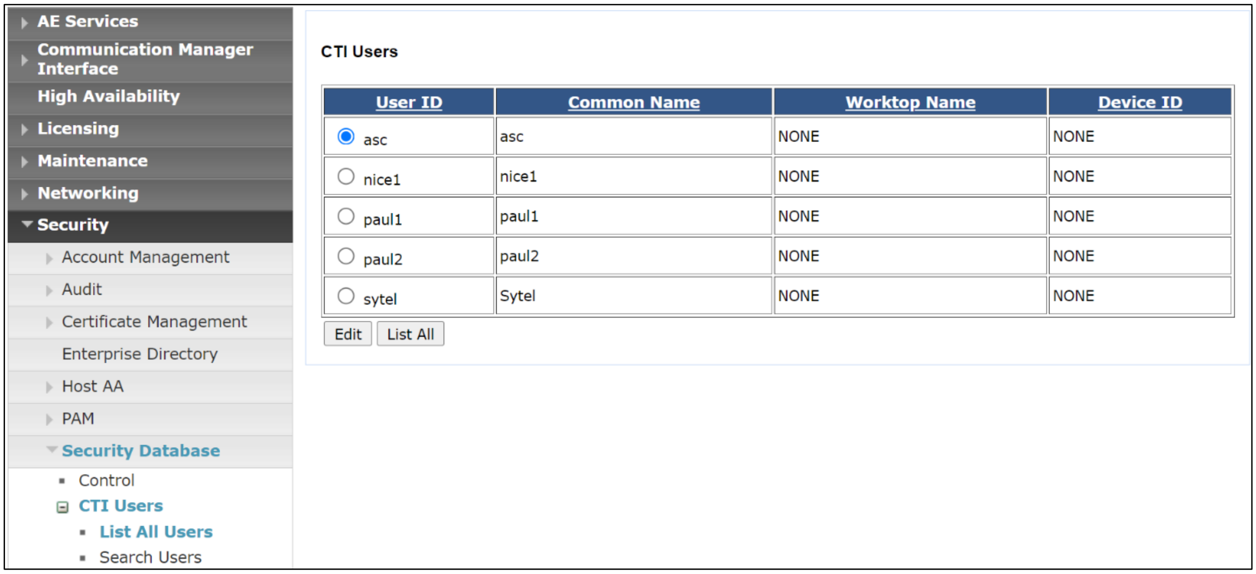
6.7.1. Configure Database Control

Open **Control** and ensure that the **SDB Control** is set as shown below.

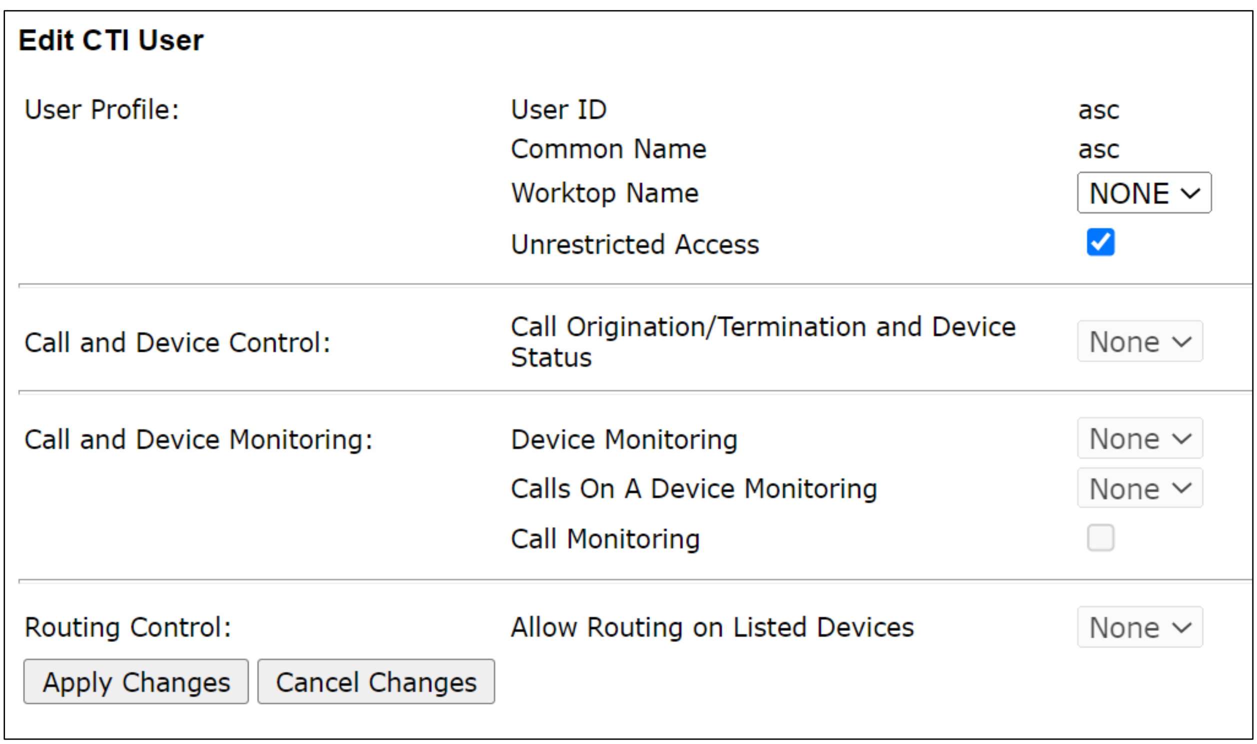
Note: The AES Security Database (SDB) provides the ability to control a user's access privileges. The SDB stores information about Computer Telephony (CT) users and the devices they control. The DMCC service, the TSAPI service, and Telephony Web Services use this information for permission checking. Please look to **Section 10** for more information on this.

6.7.2. Associate Devices with CTI User

Navigate to **Security → Security Database → CTI Users → List All Users**. Select the CTI user added in **Section 6.6** and click on **Edit Users**.

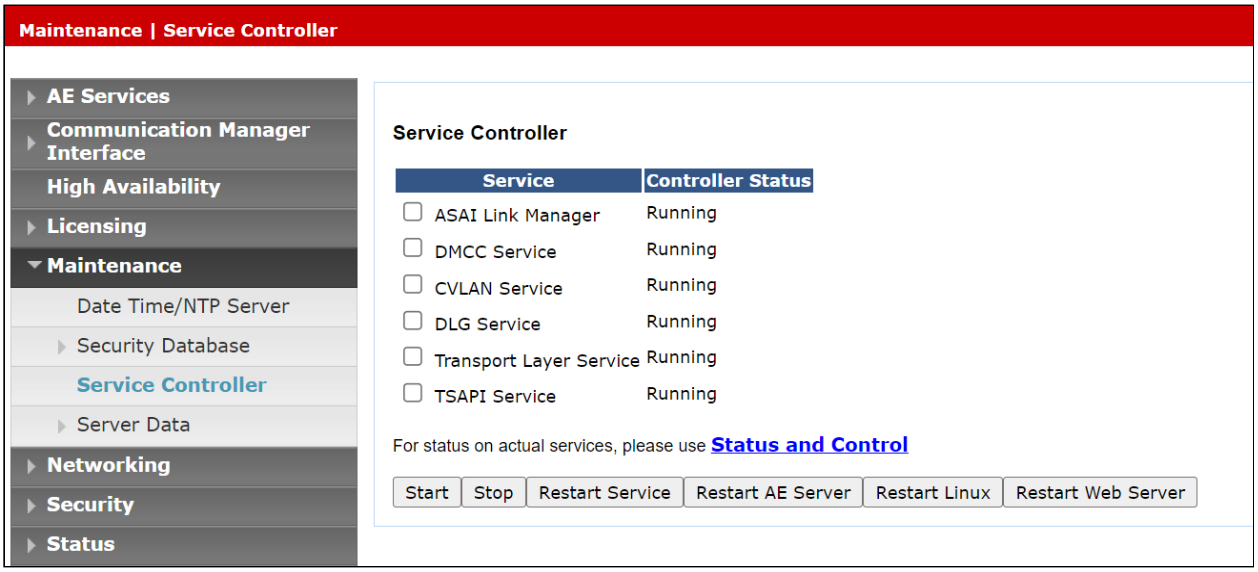


In the main window ensure that **Unrestricted Access** is ticked. Once this is done click on **Apply Changes**.

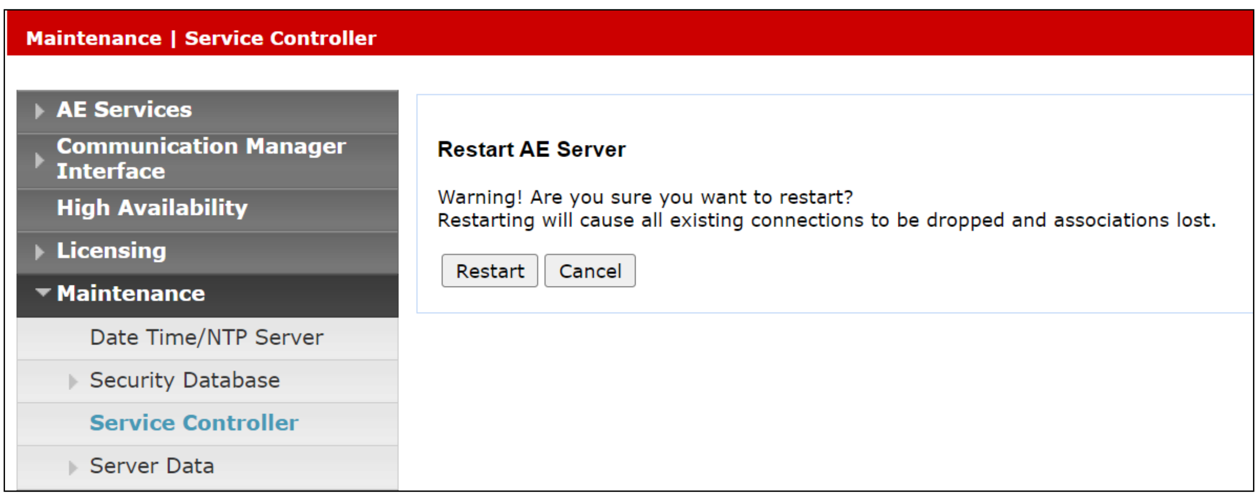


6.8. Restart AE Server

Once everything is configured correctly, it is best practice to restart AE Server (if possible), this will ensure that the new connections are brought up correctly. Click on the **Restart AE Server** button at the bottom of the screen.



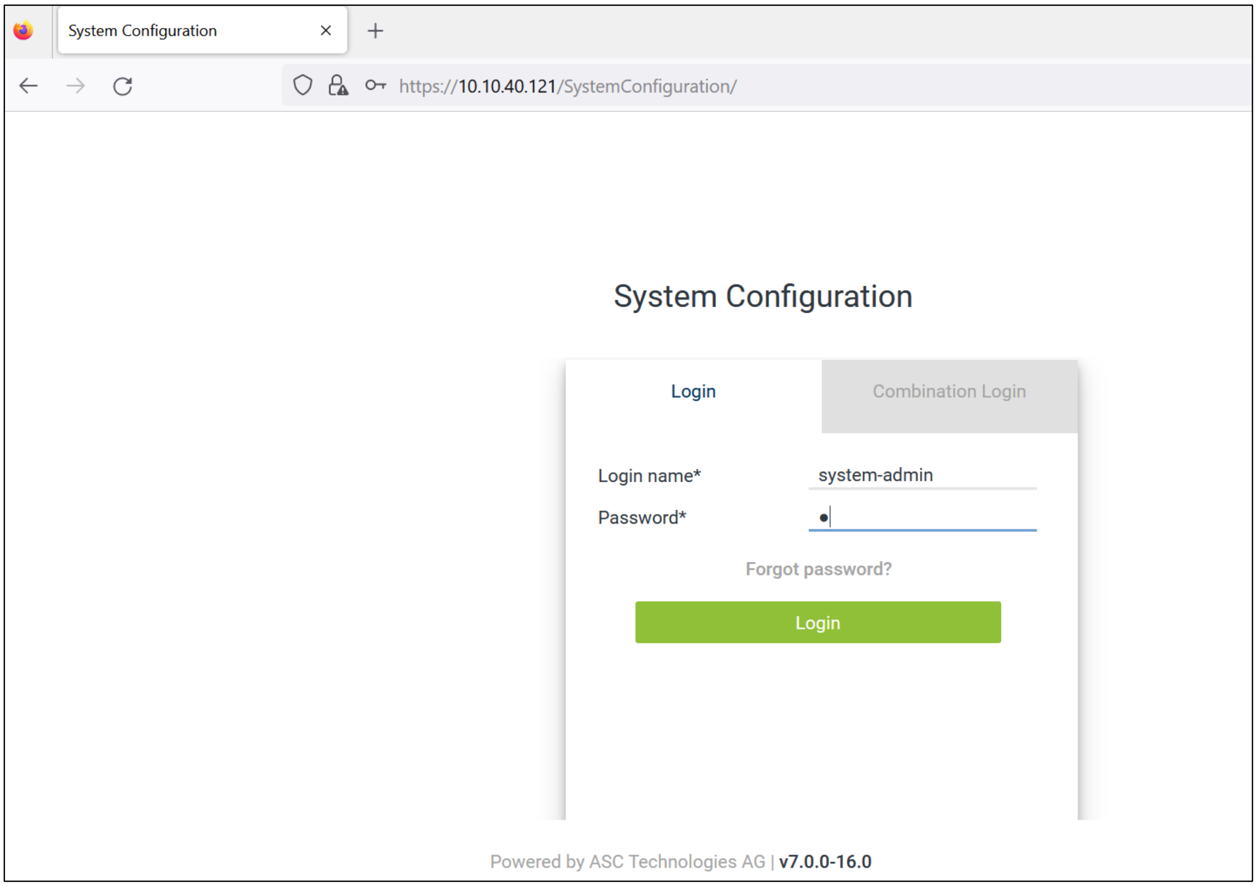
A message confirming the restart will appear, click on **Restart** to proceed.



7. Configure ASC EVOIPneo active

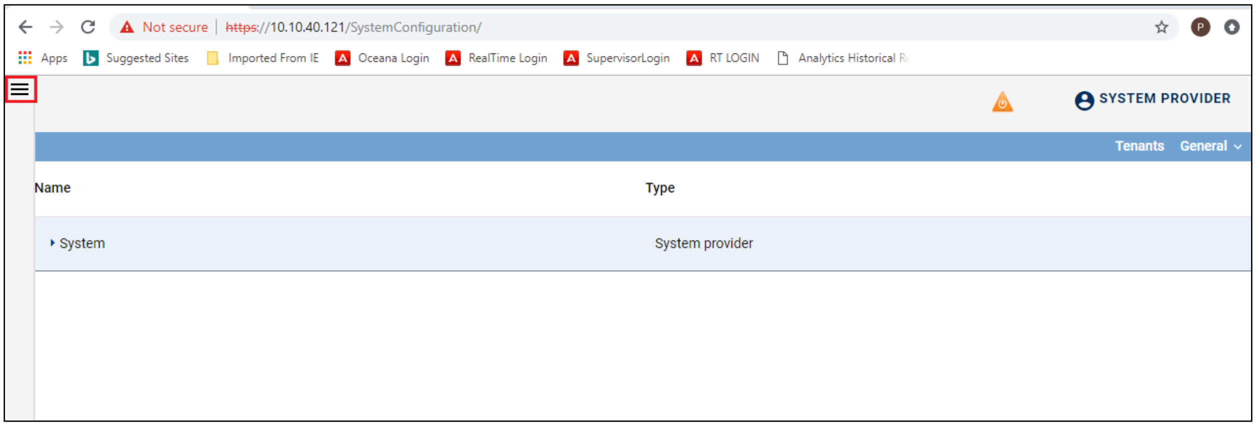
The configuration of the ASC EVOIPneo active is achieved by opening a web session connecting to that servers IP address. Mozilla Firefox is the supported web browser.

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

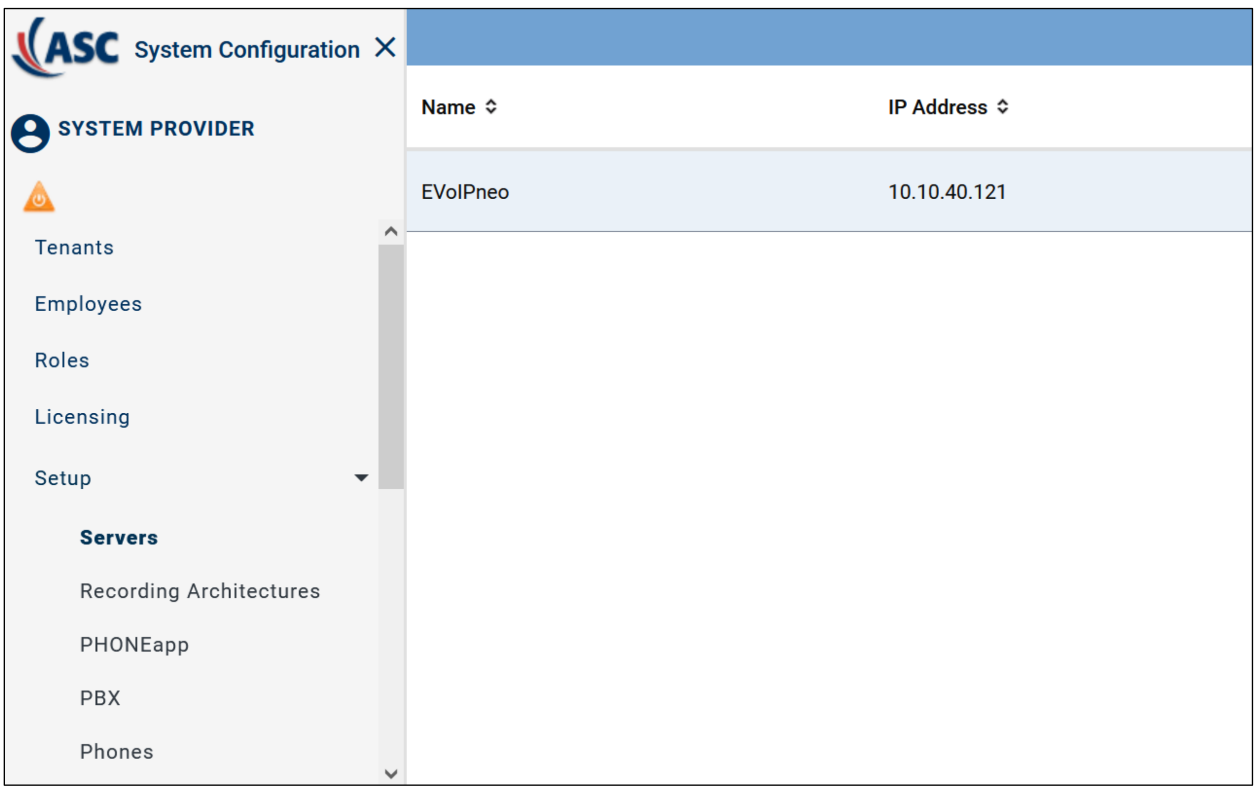


7.1. Configure Server

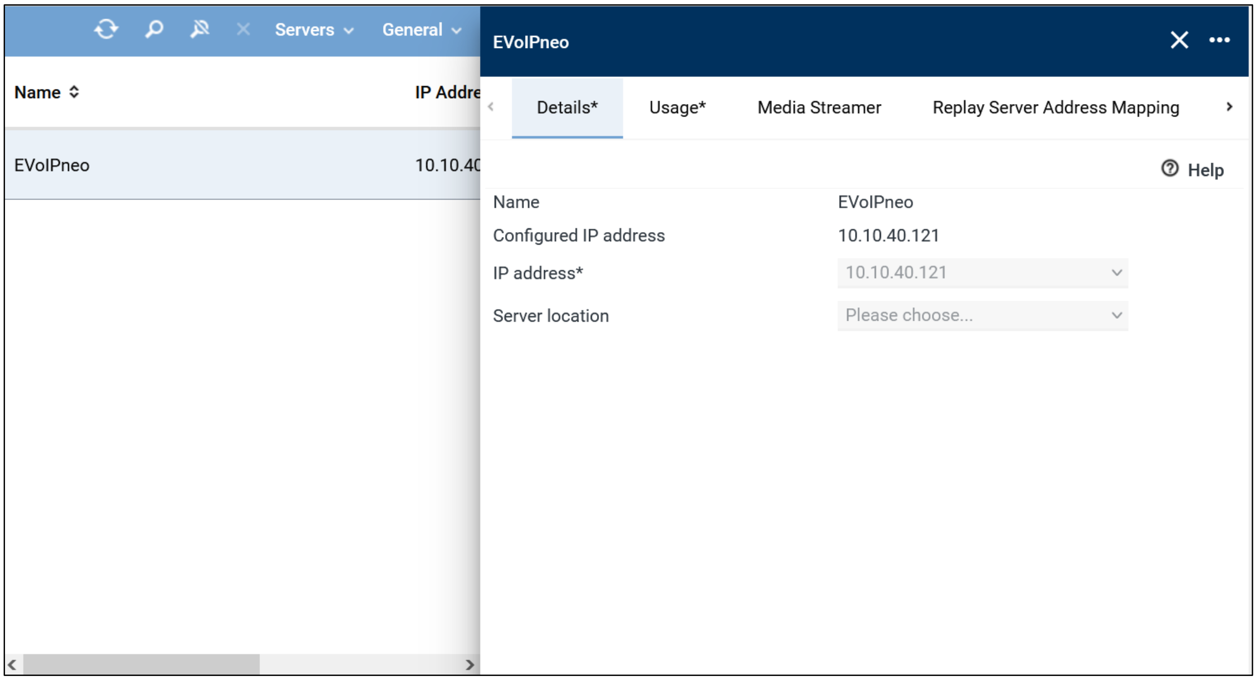
Expand the menu by clicking on the tab highlighted at the top left of the screen.



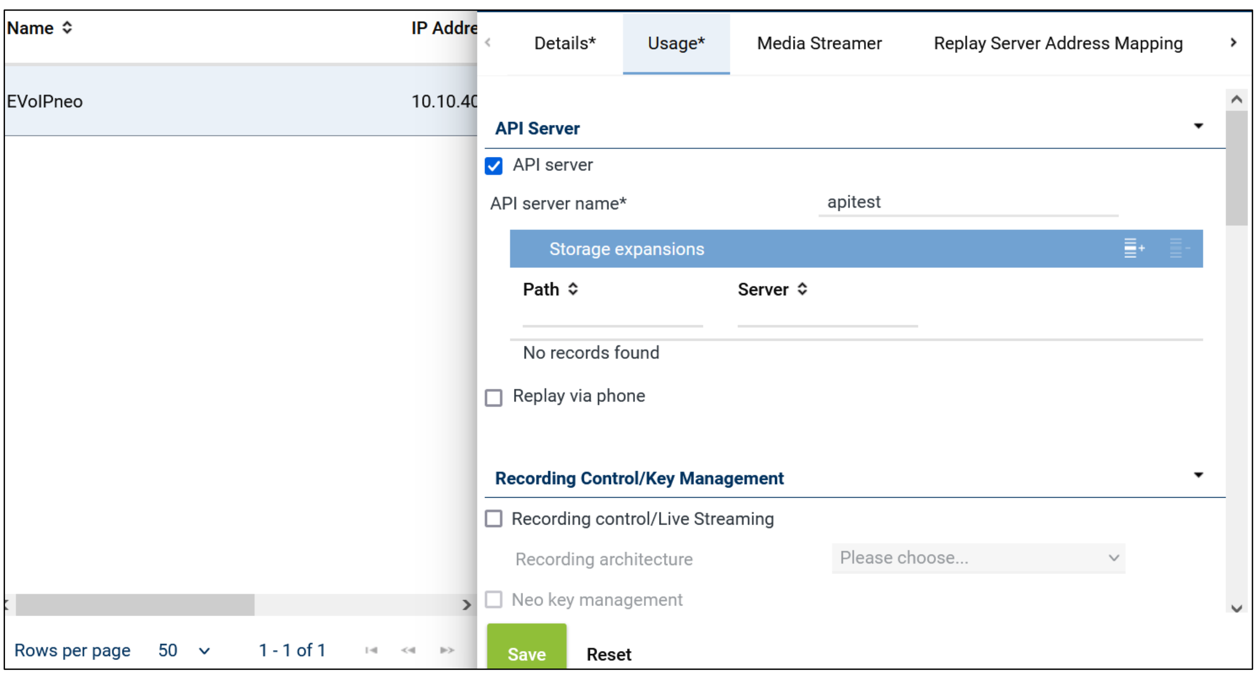
Navigate to **Setup → Servers** in the left window. Click on the Server shown in the main window.



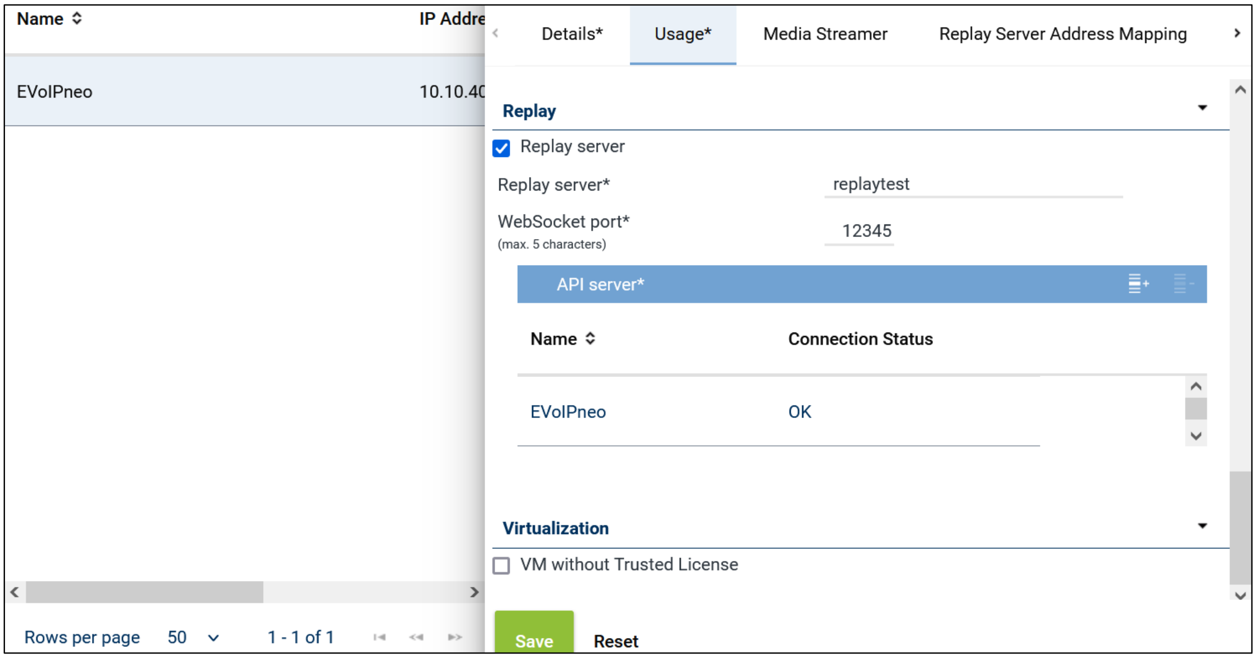
The **Details** tab shows the **Name** and **IP address** of the server.



Click on the **Usage** tab in the right window. Ensure that **Data Storage** (not shown) and **API server** boxes are ticked. Scroll down to the bottom of the screen.

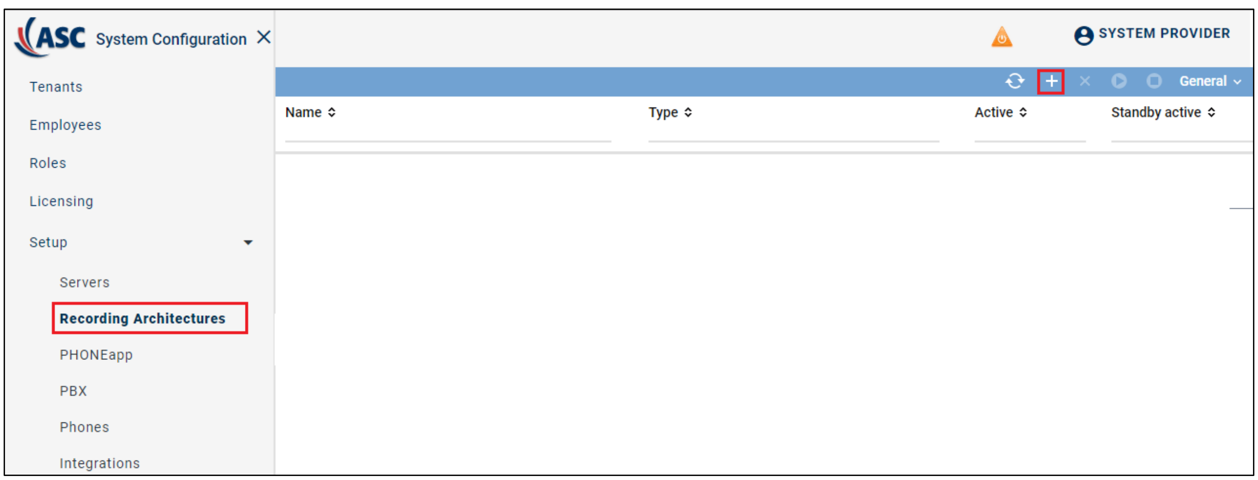


Ensure that the **Replay** server box is ticked and click on **Save** at the bottom of the screen.

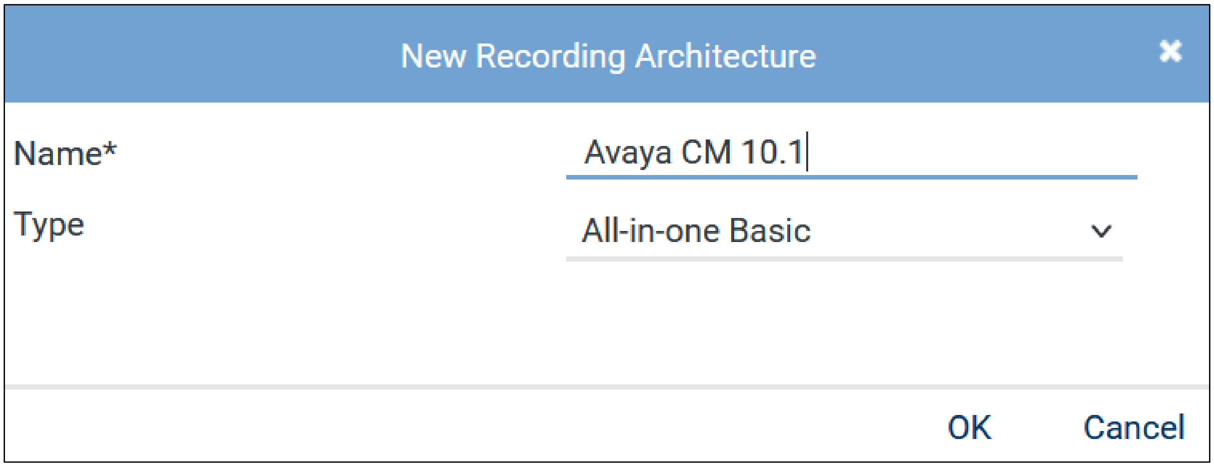


7.2. Configure Recording Architecture

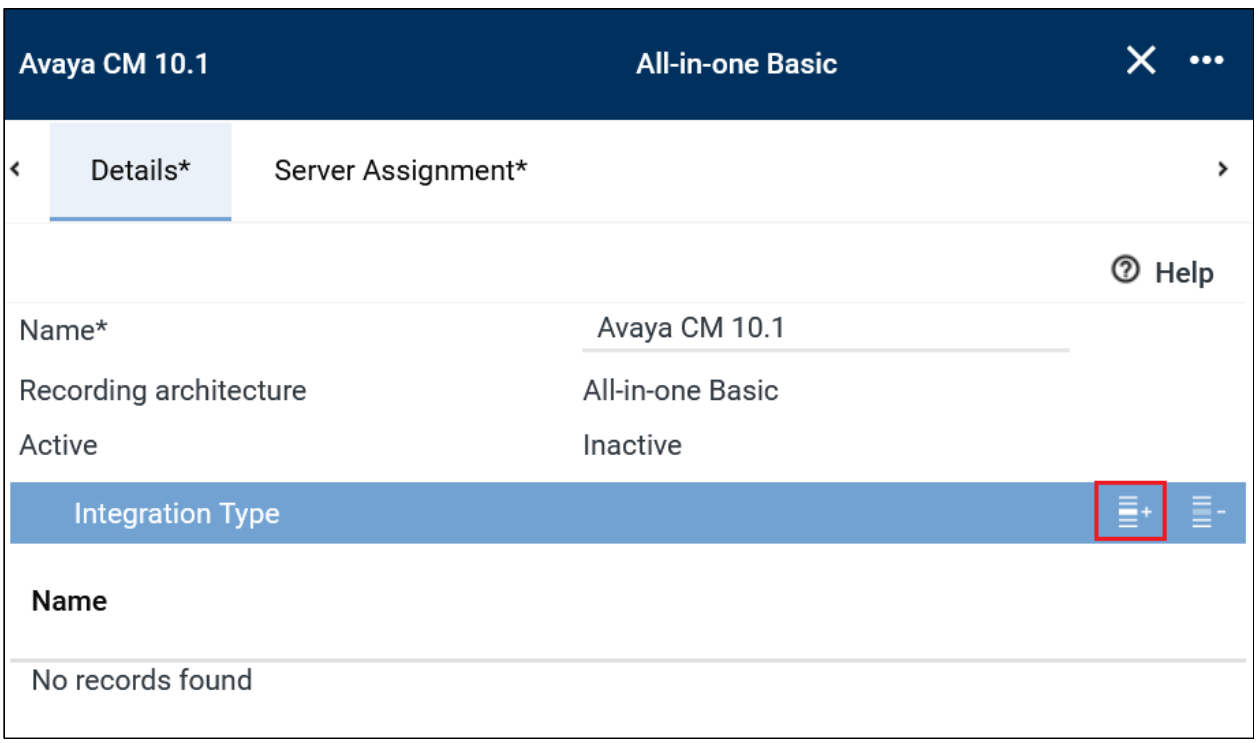
Navigate to **Setup → Recording Architectures** in the left window and click on the **+** icon to add a **New Recording Architecture**.



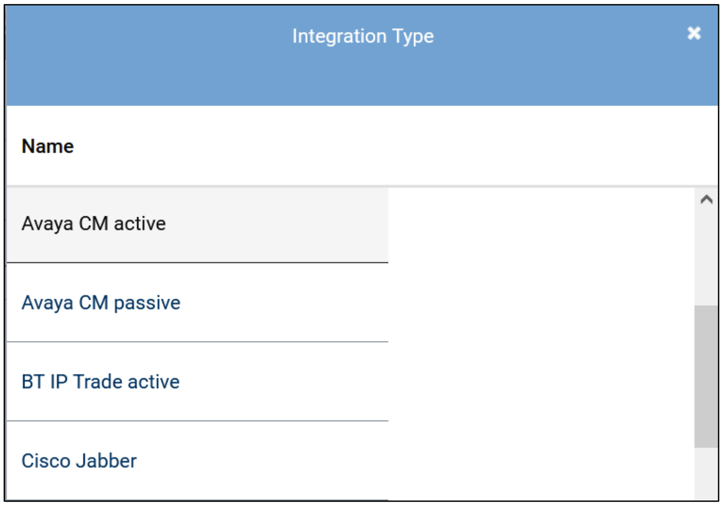
Enter a suitable **Name** and select **All-in-one Basic** as the **Type**, as shown below, click on **OK** once complete.



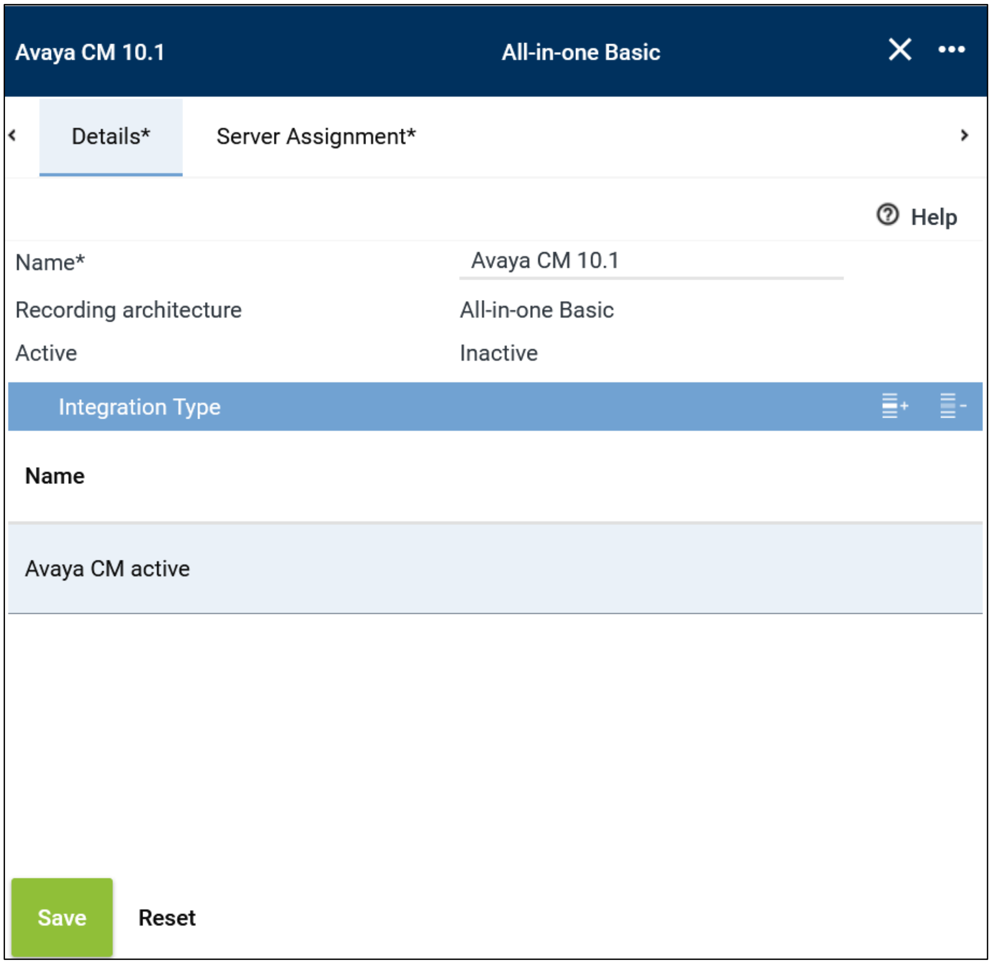
Click on the **Add** icon highlighted on the right side of the screen below.



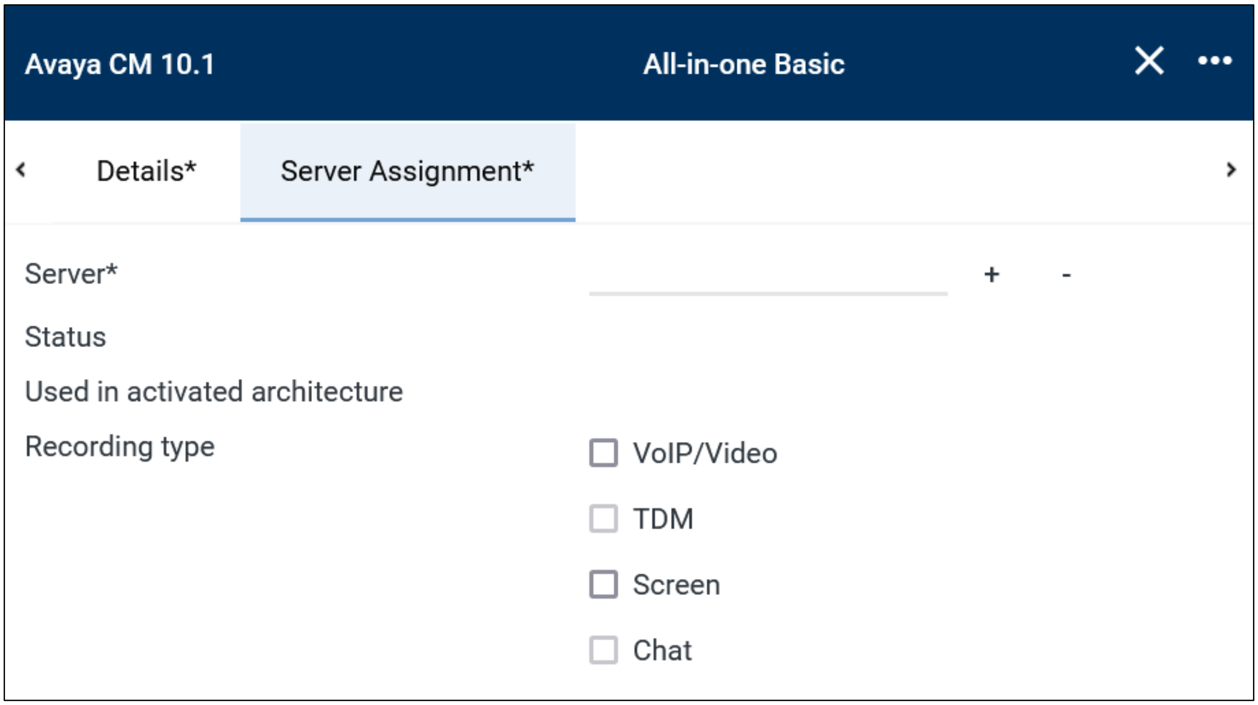
A screen is opened showing the **Integration Type** that is present depending on license. Select **Avaya CM active** and click on **Add** at the bottom of this screen (not shown).



The new Integration is added as shown below, click on the **Server Assignment** tab.

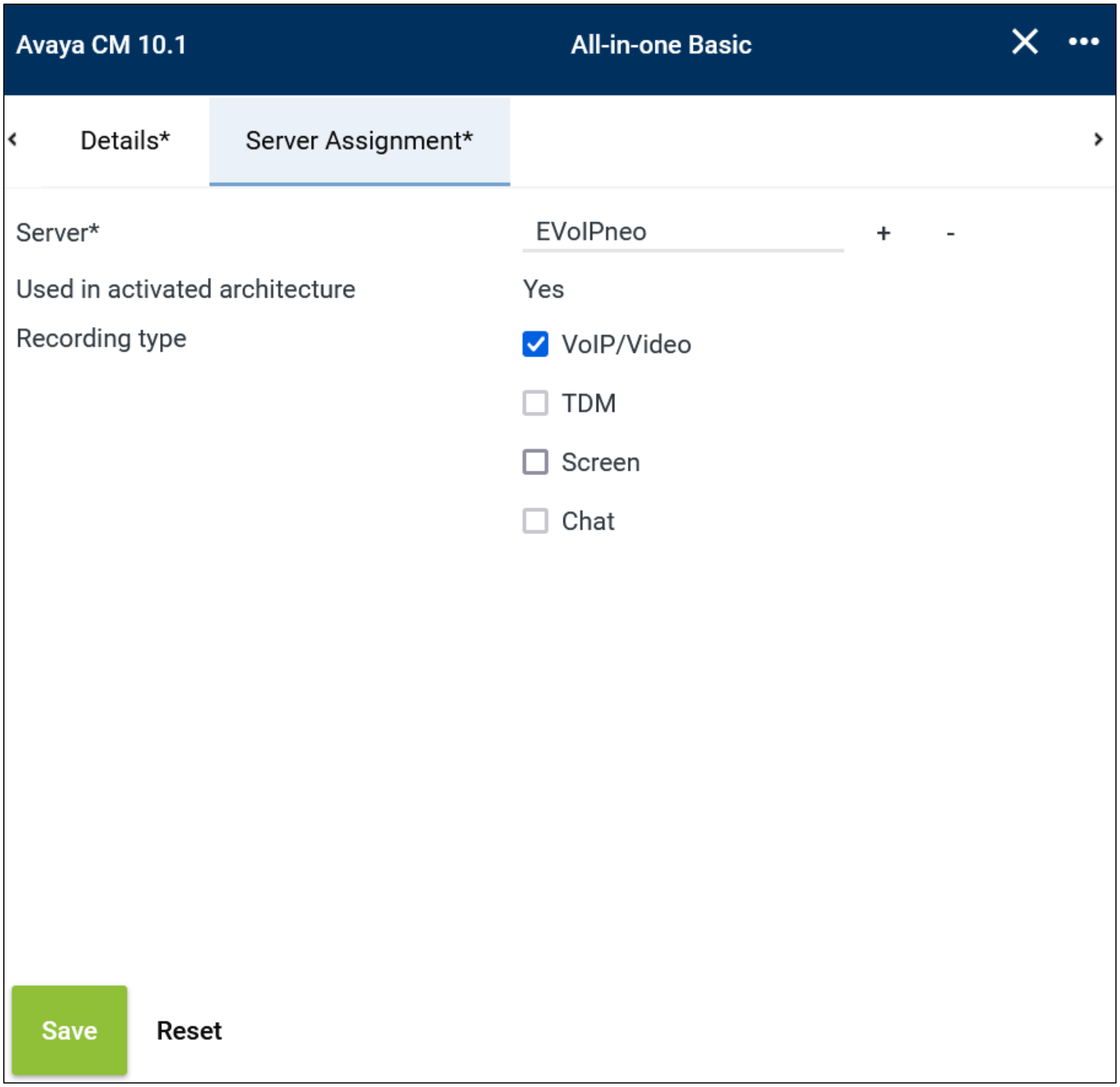


Click on the **Server Assignment** tab highlighted and click on the **+** icon to add a server.

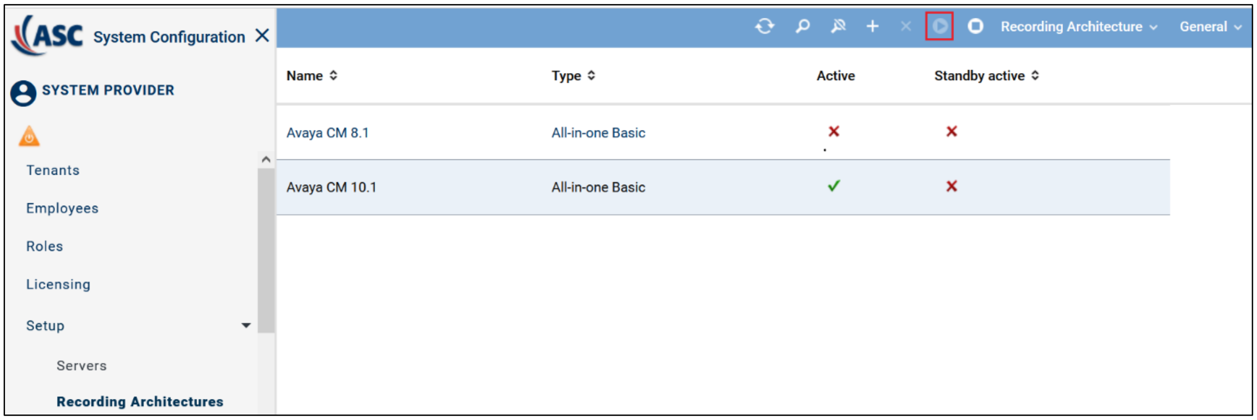


Select the server (added during the installation) and click on **Add** at the bottom of the screen.

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

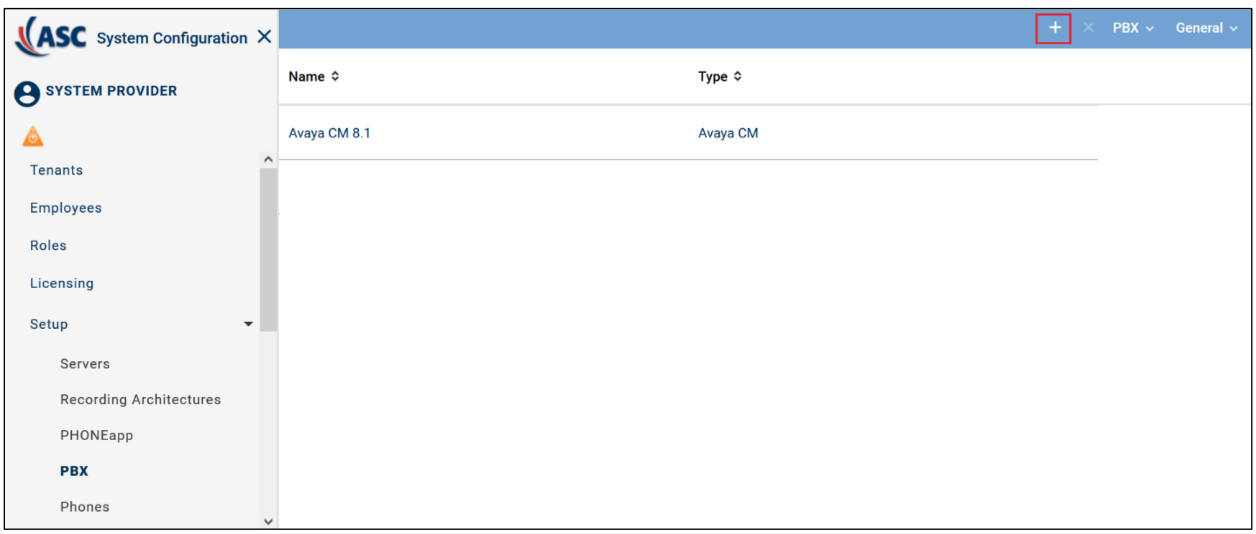


Once this Recording Architecture is added it must be activated by clicking on the **Activate** icon highlighted below.

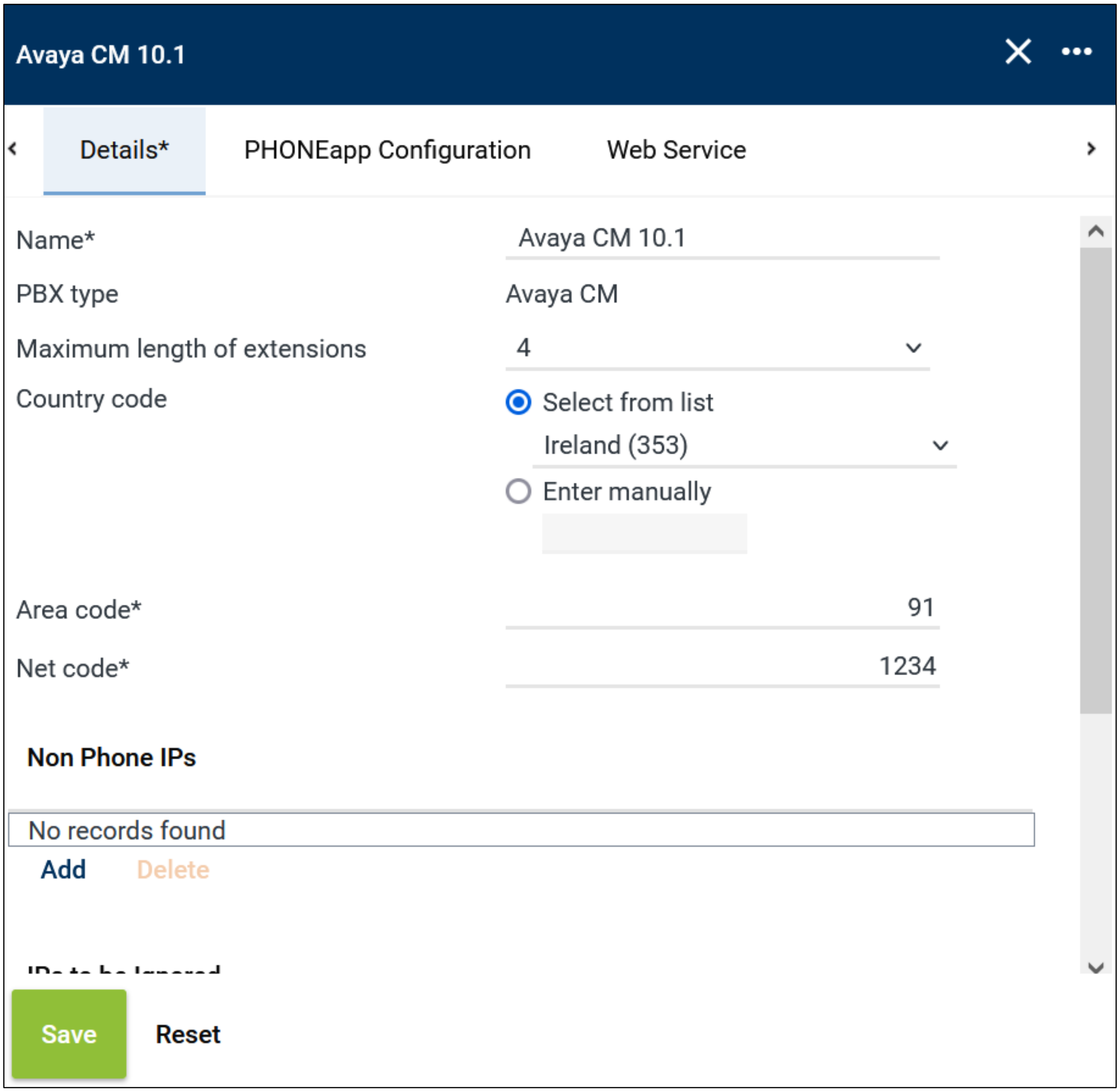


7.3. Add PBX

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

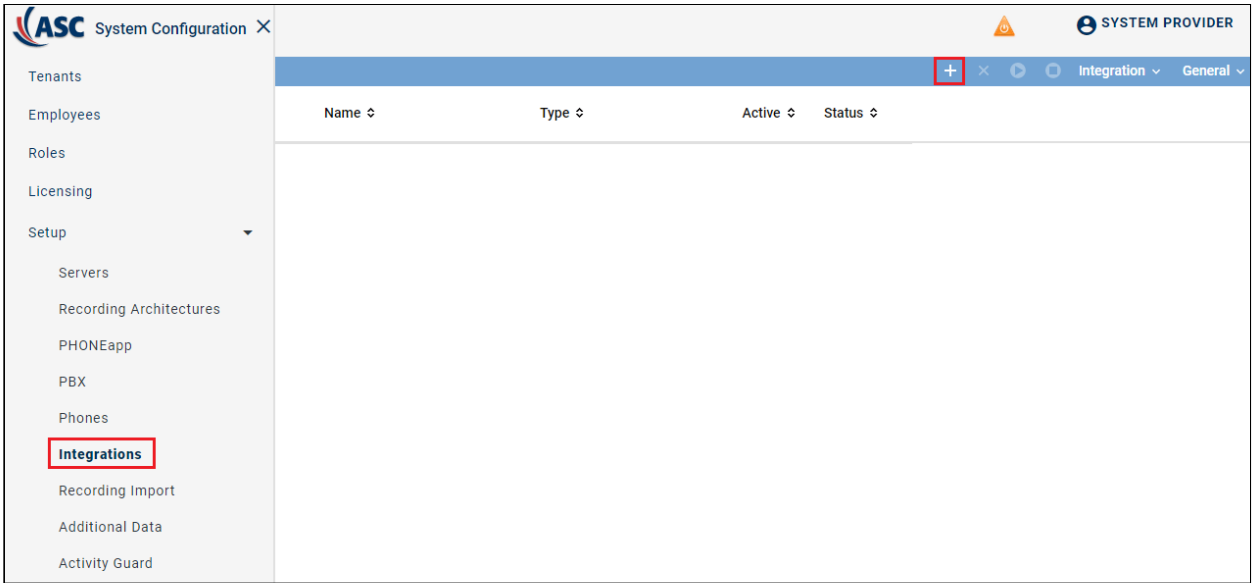


Enter the telephony details as shown and click on **Save** at the bottom of the screen.

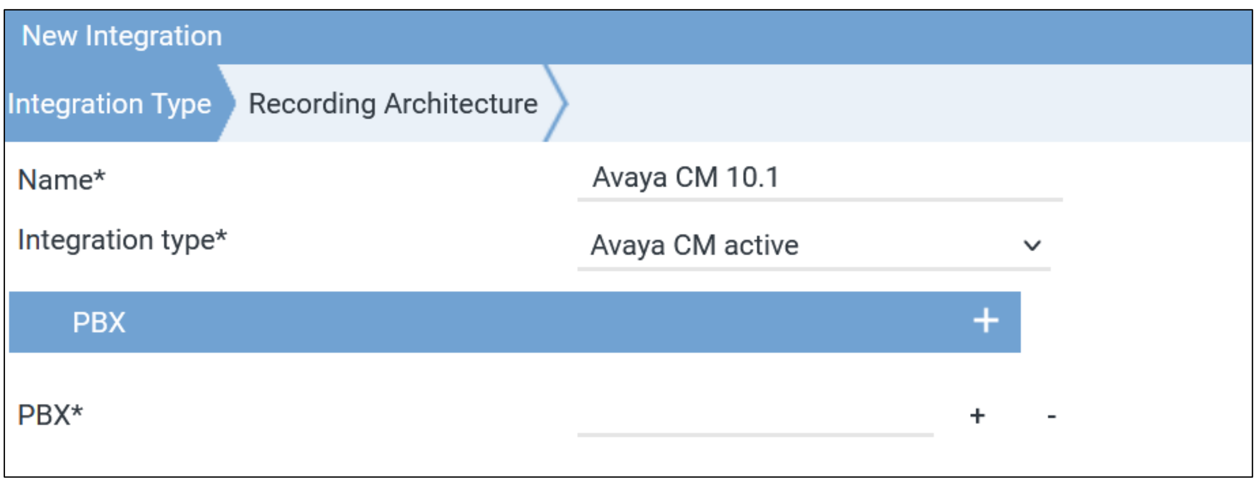


7.4. Integrations

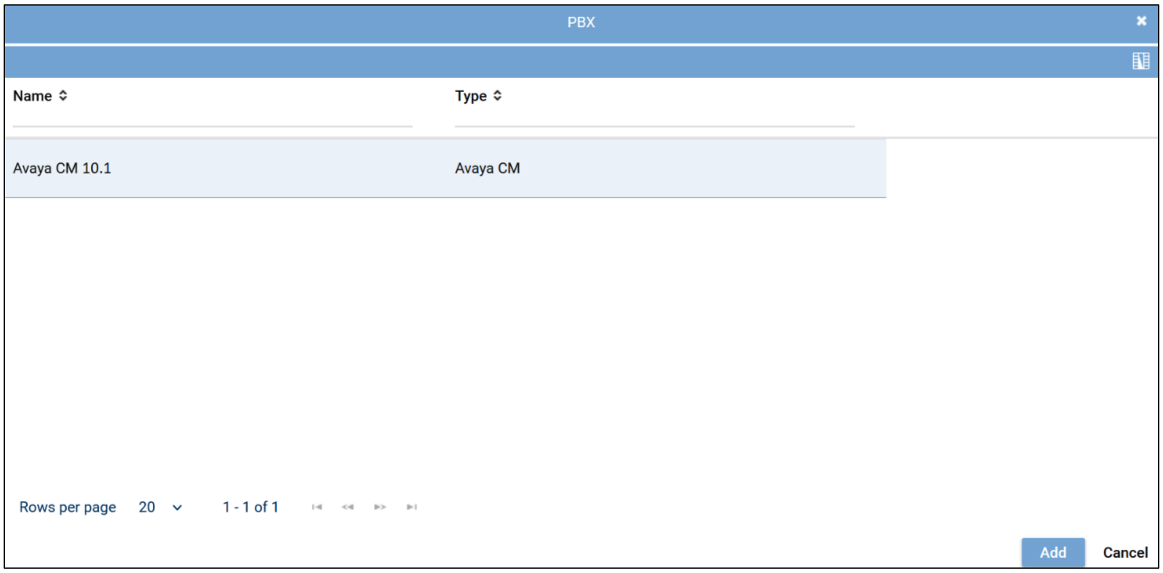
Navigate to **Setup → Integrations** in the left window and click on the **+** icon at the top of the main window to add or create a new Integration.



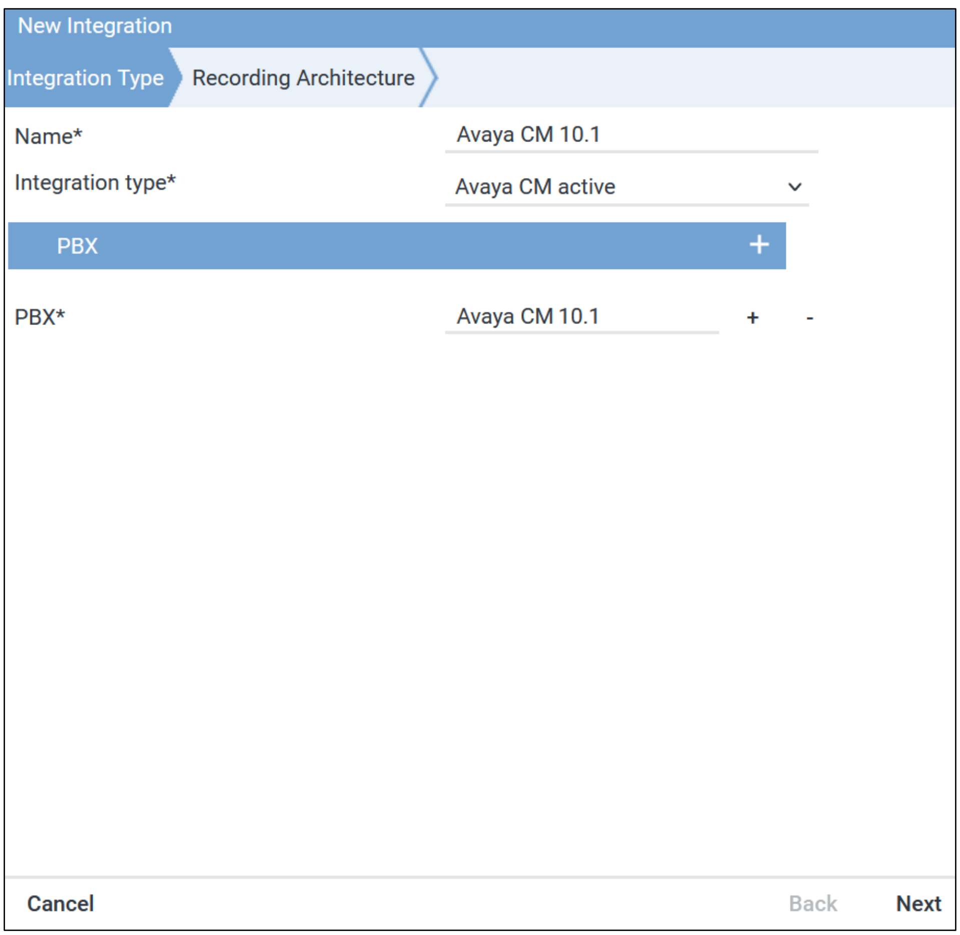
In the right window enter a suitable **Name** and select the **Avaya CM active** as the **Integration type**. Click on the Add Icon **+** next to **PBX** as shown below.



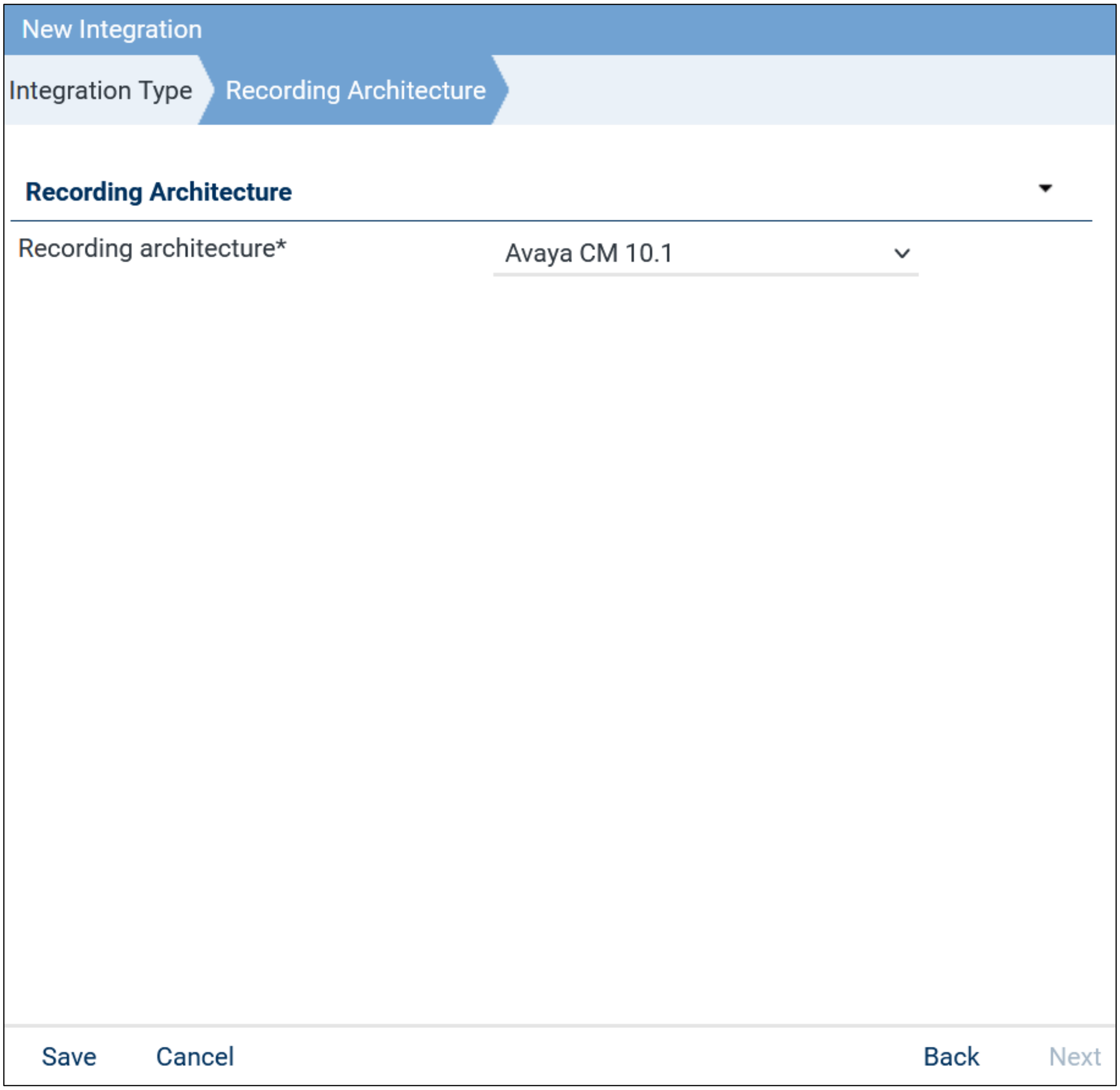
Select the PBX, this was created in **Section 7.3**, click on **Add** at the bottom of the screen.



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

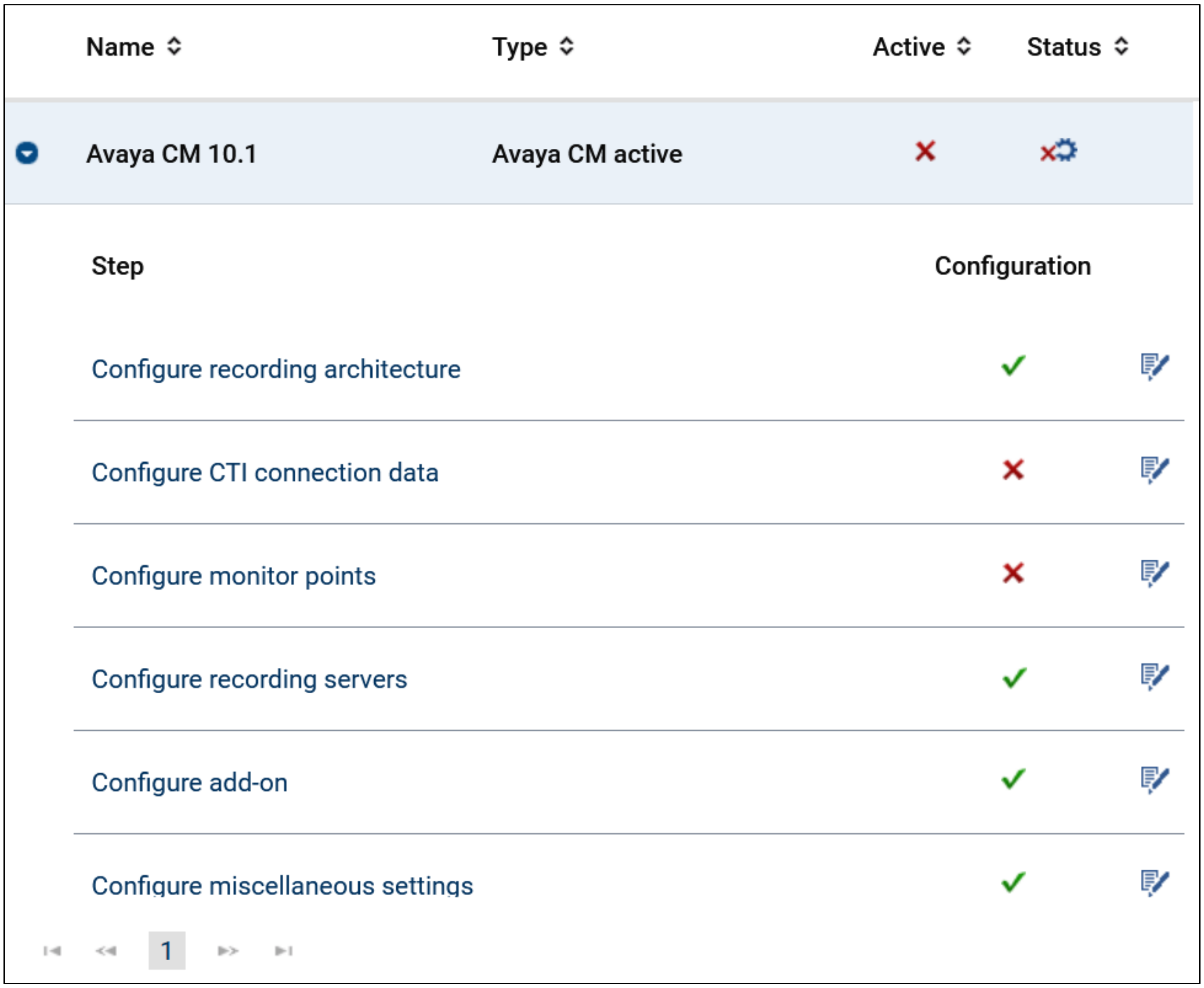


Select the **Recording architecture** created in **Section 7.2** and click on **Save**.



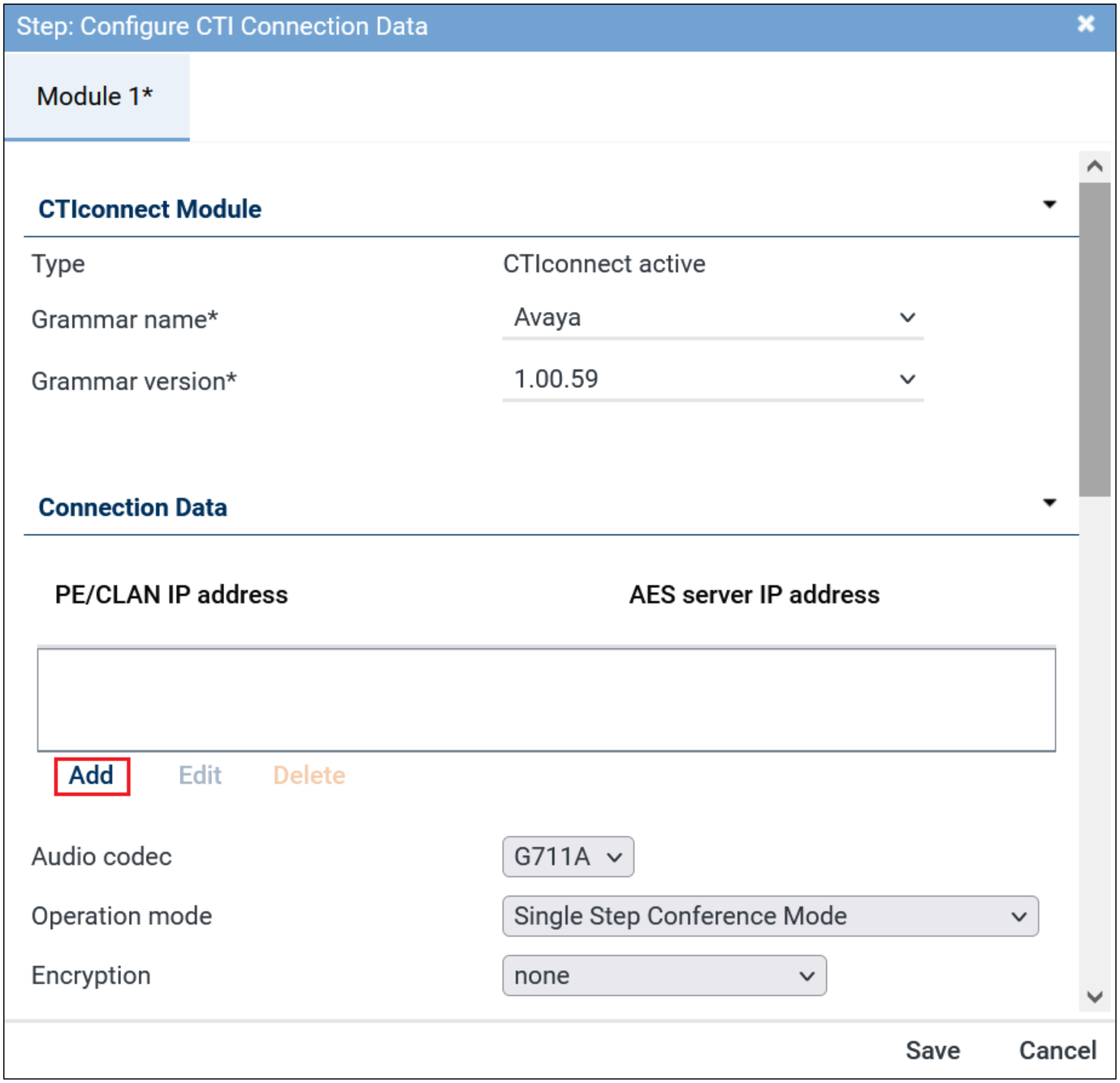
Once saved click on the Maximize icon. There are two steps left to configure before the system is ready.

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

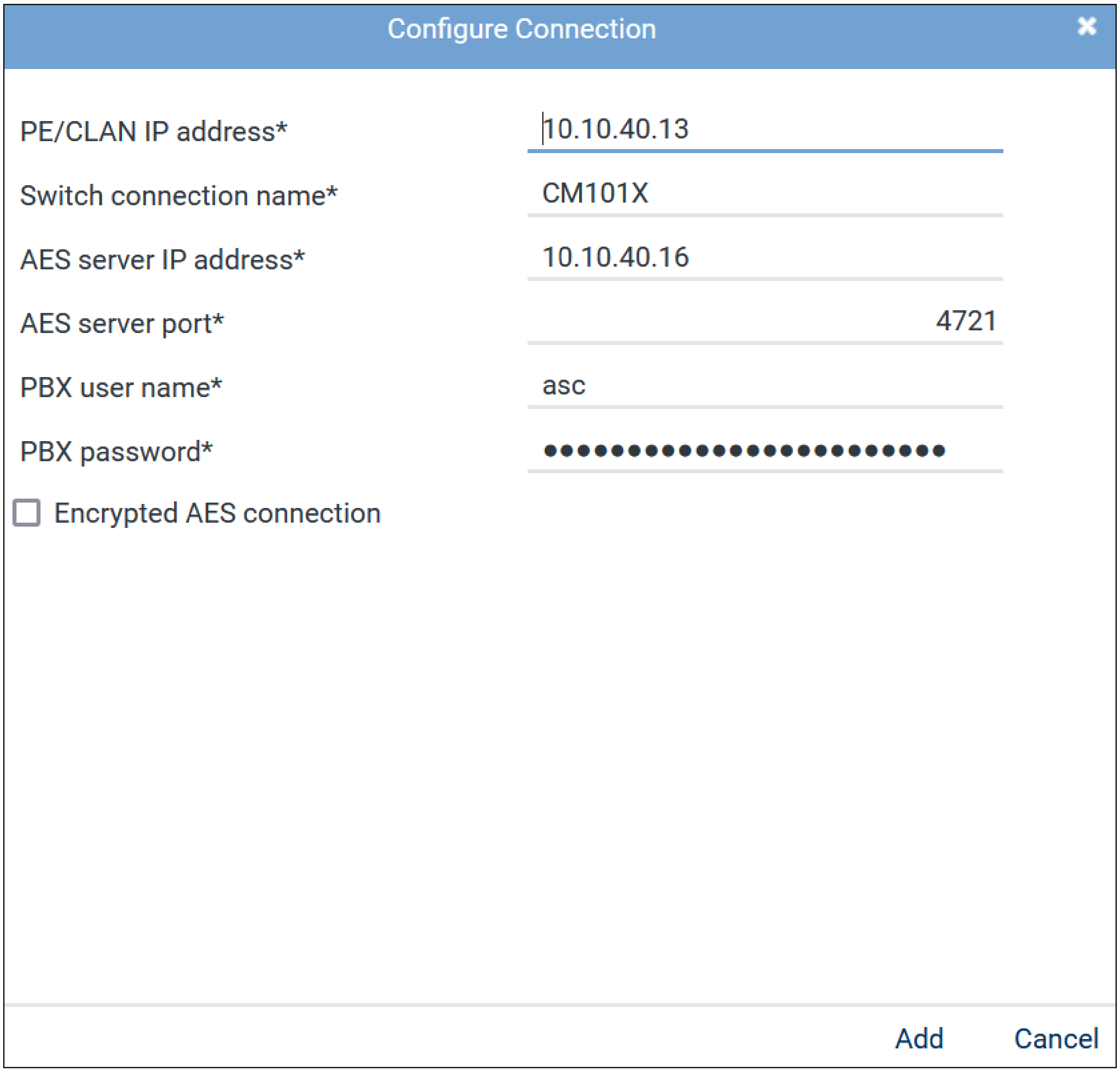


7.4.1. Configure CTI connection data

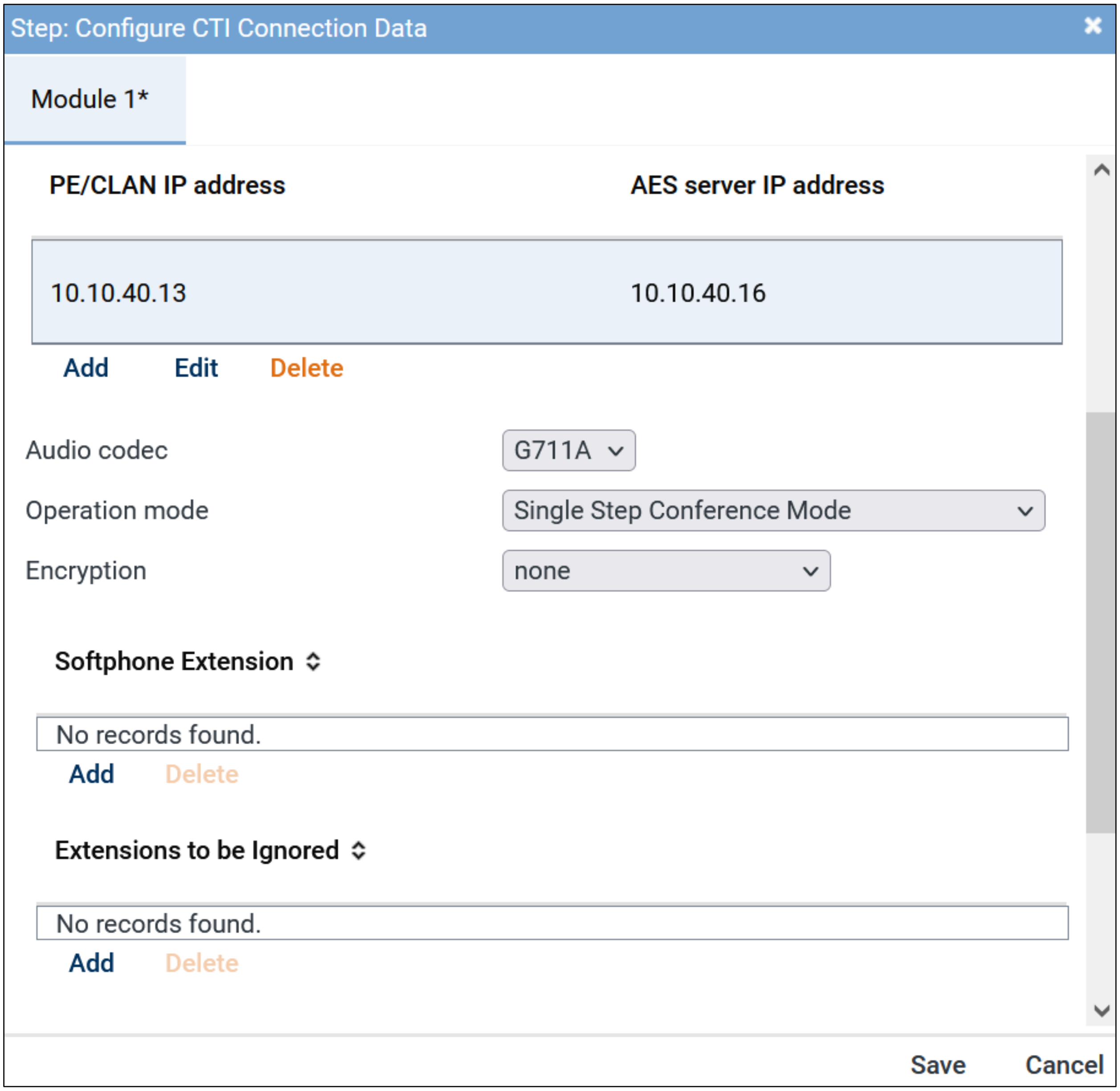
Click on the edit icon next to **Configure CTI connection data** (not shown). Click on **Add** under **PE/CLAN IP address – AES server IP address**. The **Audio Codec**, the **Operation mode** and **Encryption** are also set here. **G711A** was set for the Audio Codec and **Single Step Conference** was selected for the operation mode. No encryption was used, so this was set to **none**.



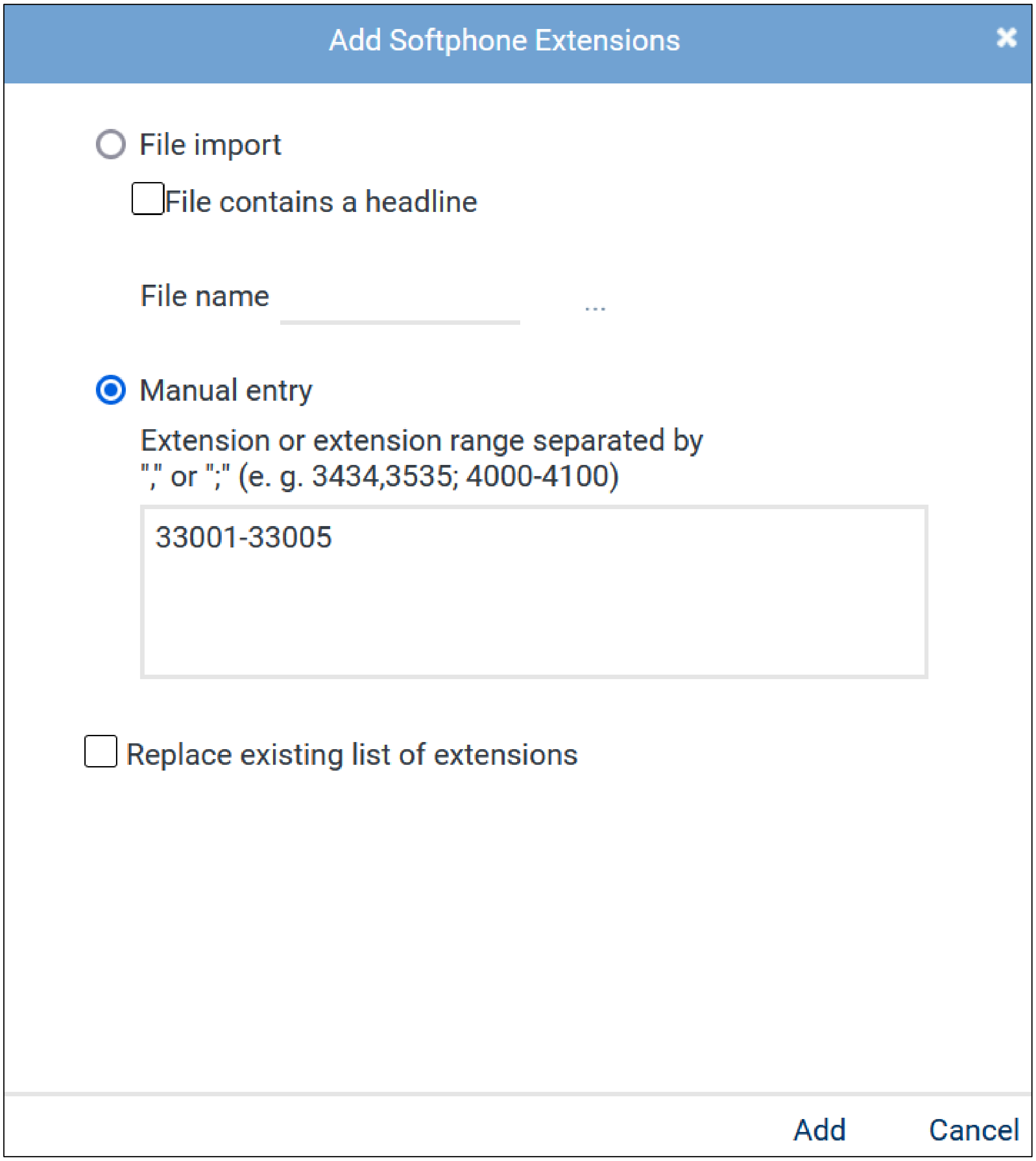
Enter the Communication Manager IP Address and the AES information which can be obtained from **Section 6.5**. Click on **Add** once complete. Note in the screen shot below the **PE/CLAN IP address** will be that of the **procr** address displayed in **Section 5.2**.



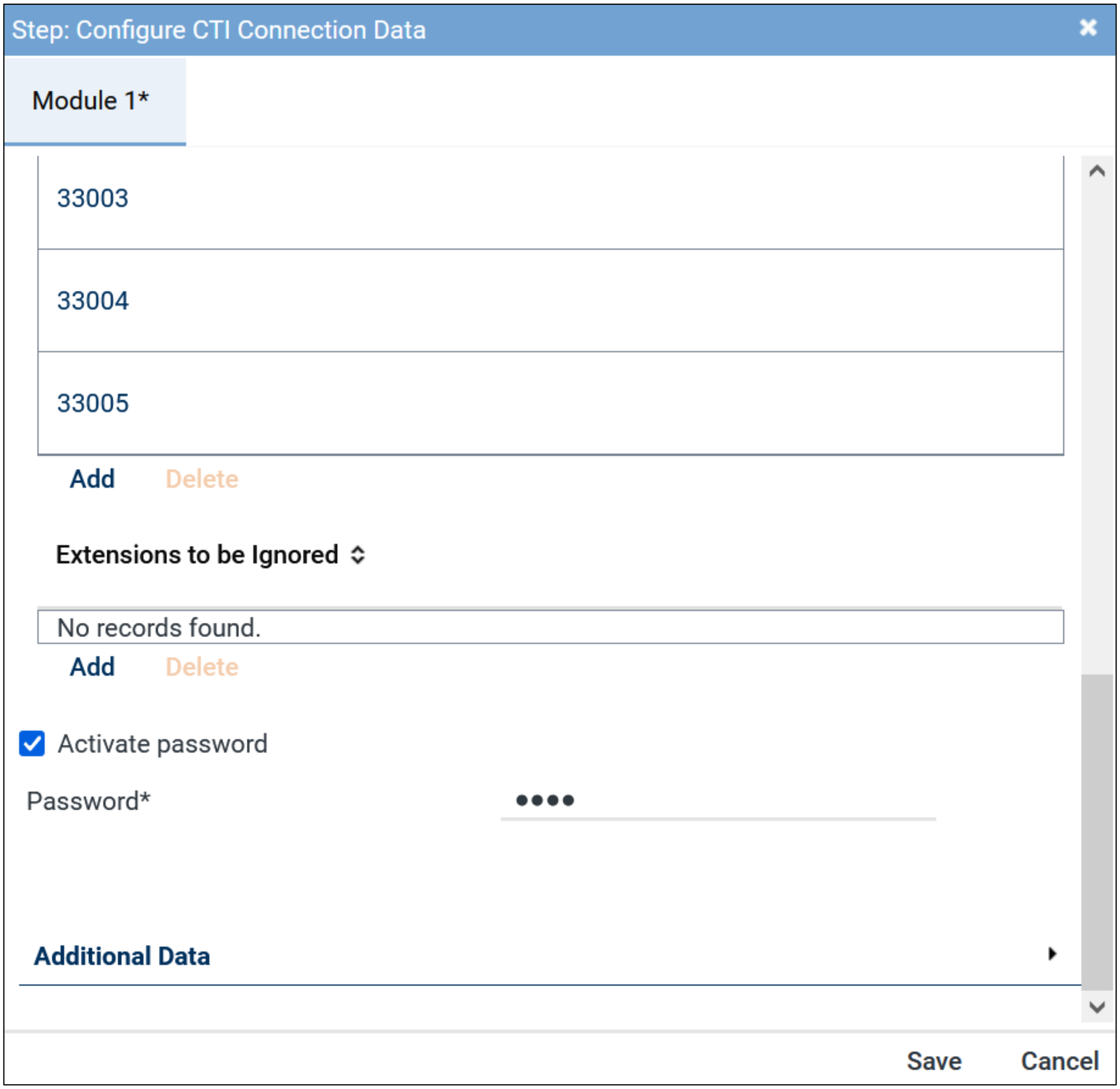
On the same screen, in the right window, select **Add** under **Softphone Extension**.



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

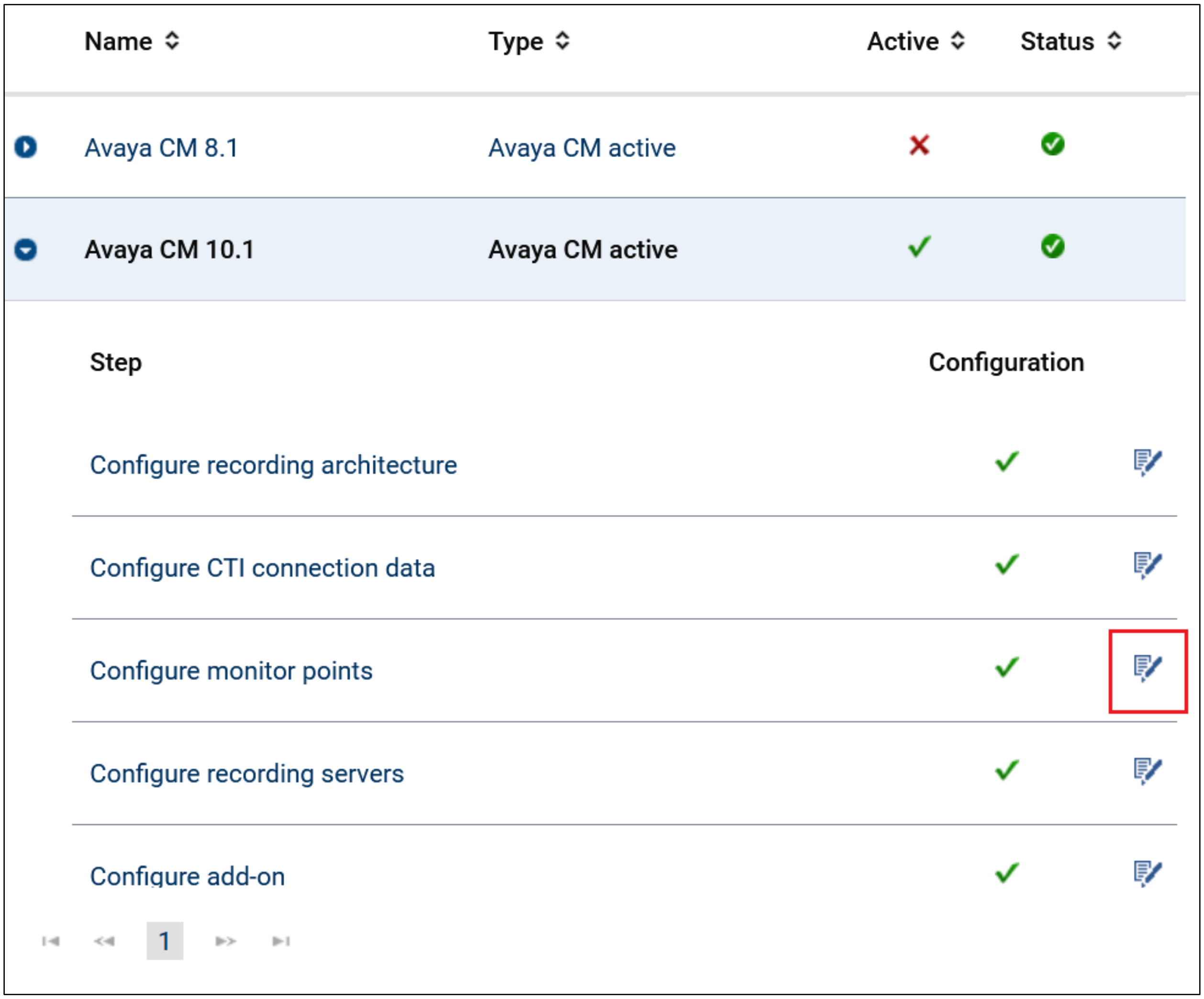


Click on **Activate password** and enter the password for the virtual stations created in **Section 5.5**. Click on **Save** at the bottom of the screen once complete.

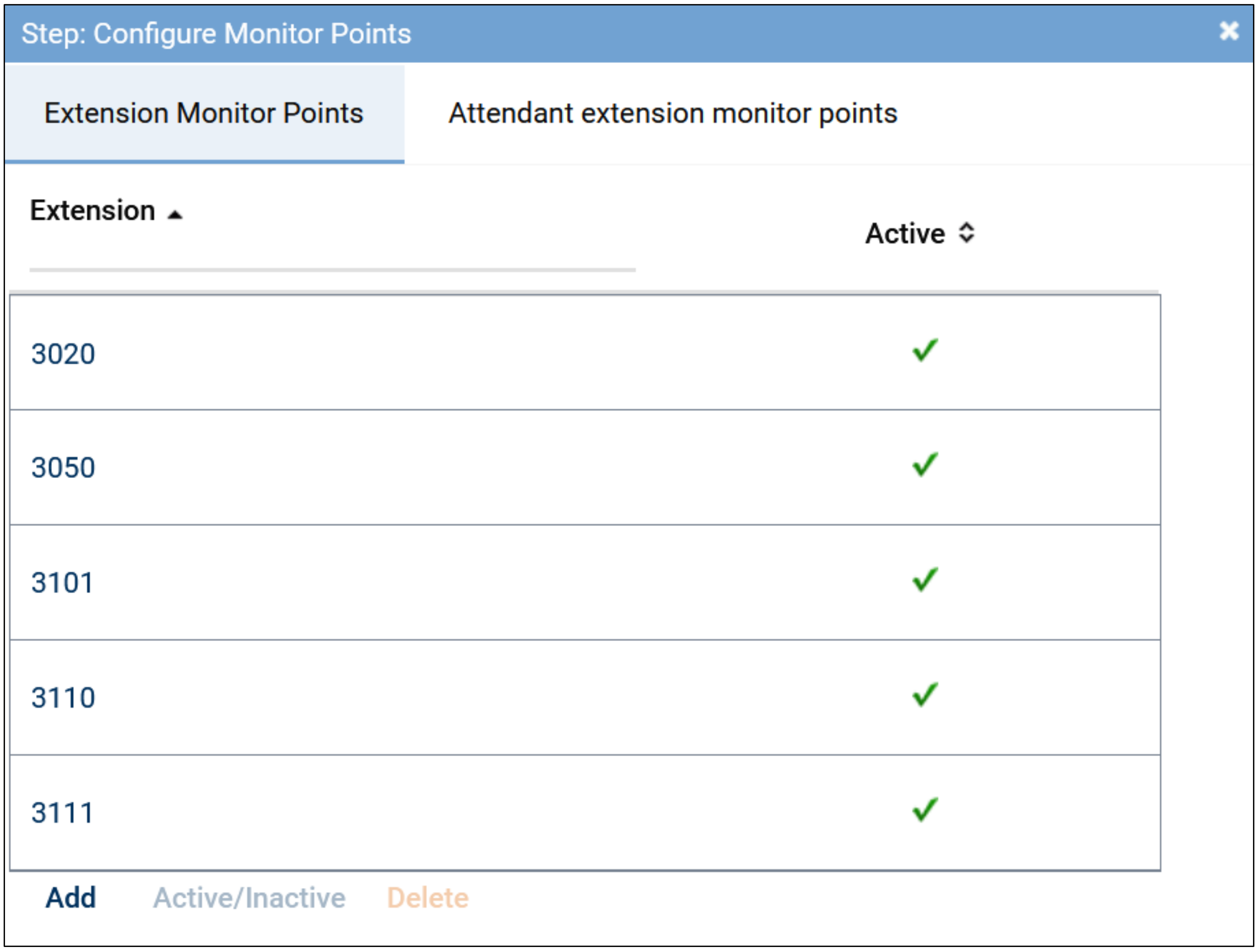


7.4.2. Configure monitor points

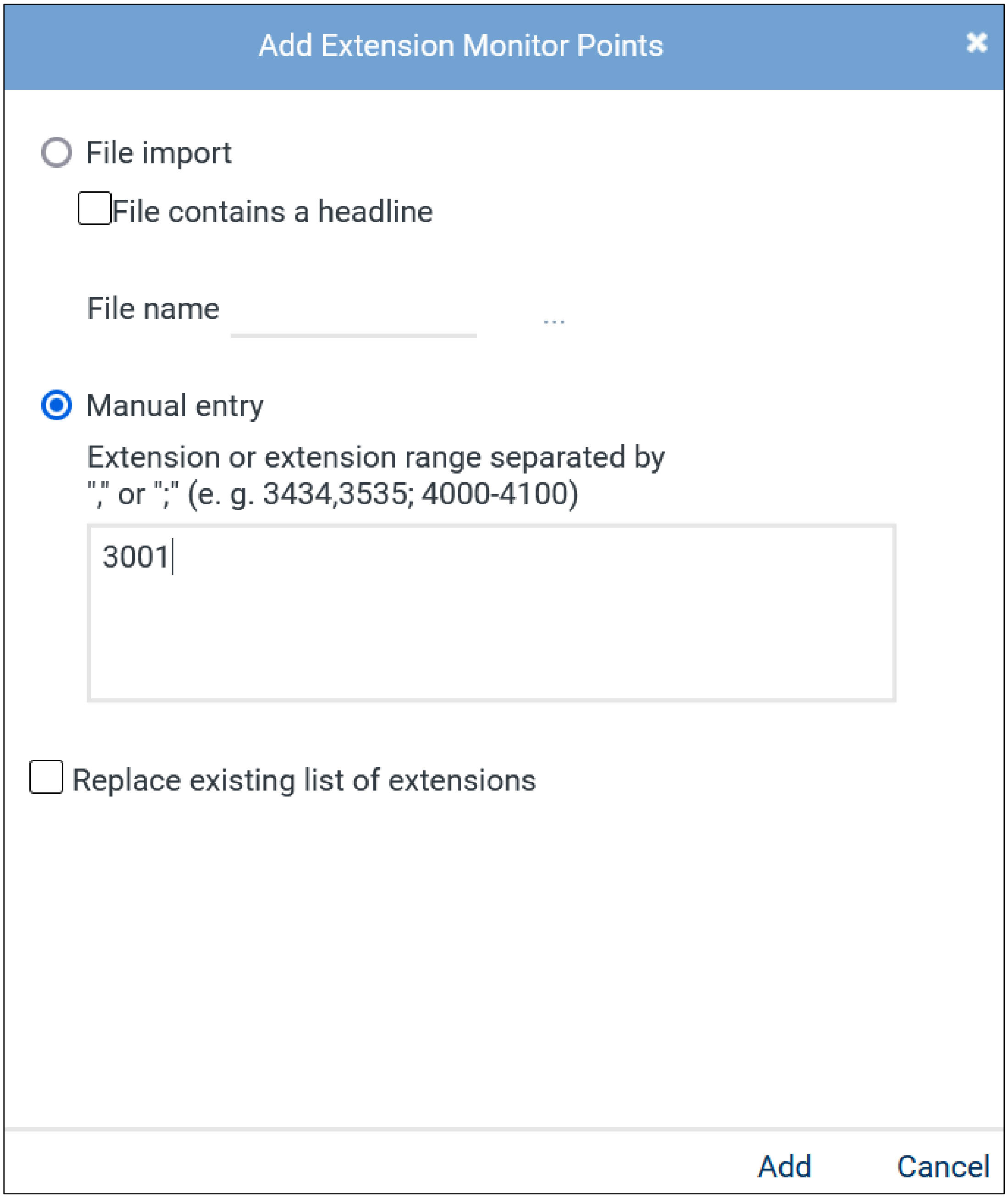
Click on the edit icon next to **Configure monitor points**.



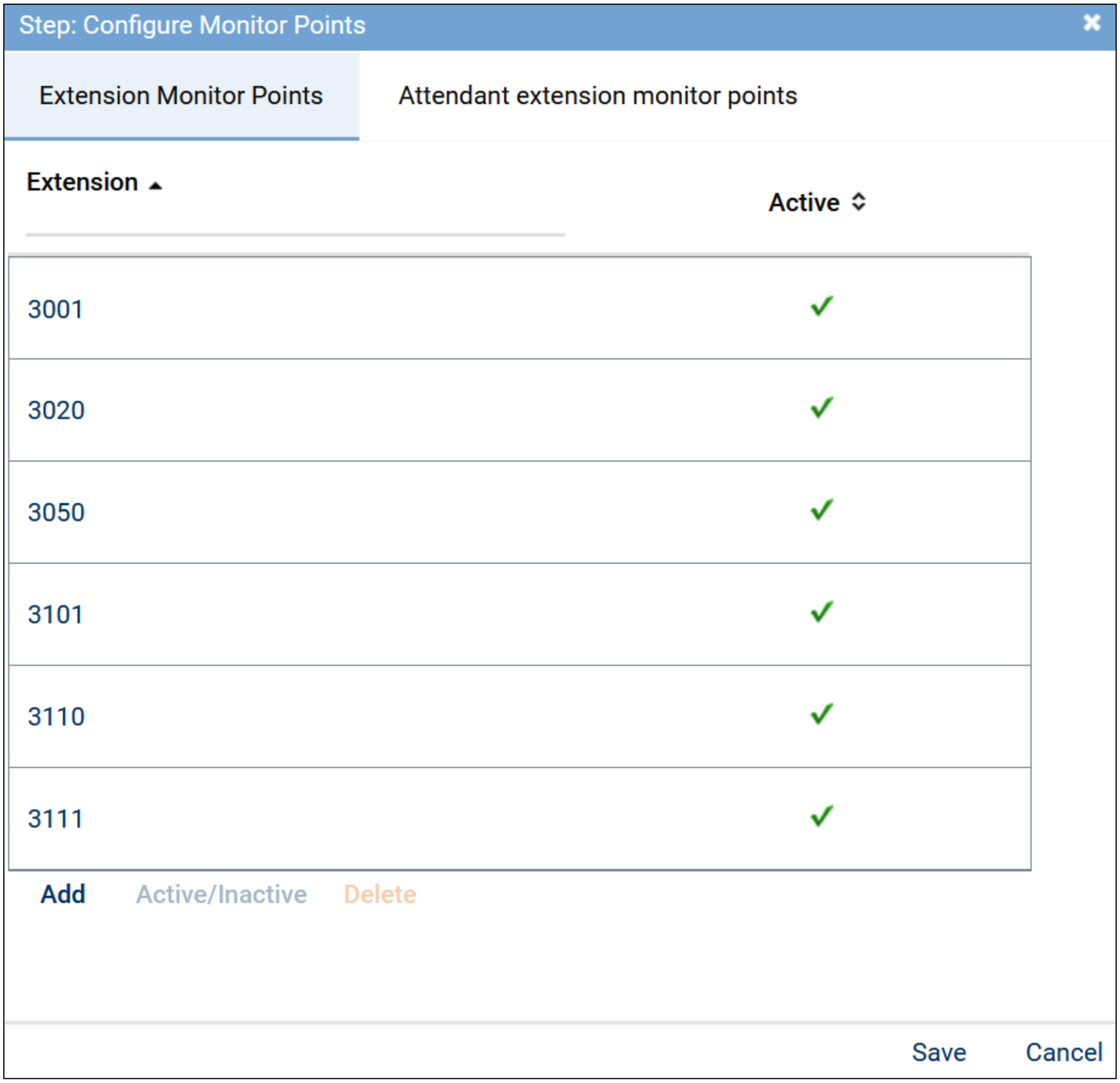
Some extensions are already added. To add another extension, click on **Add** at the bottom of the window.



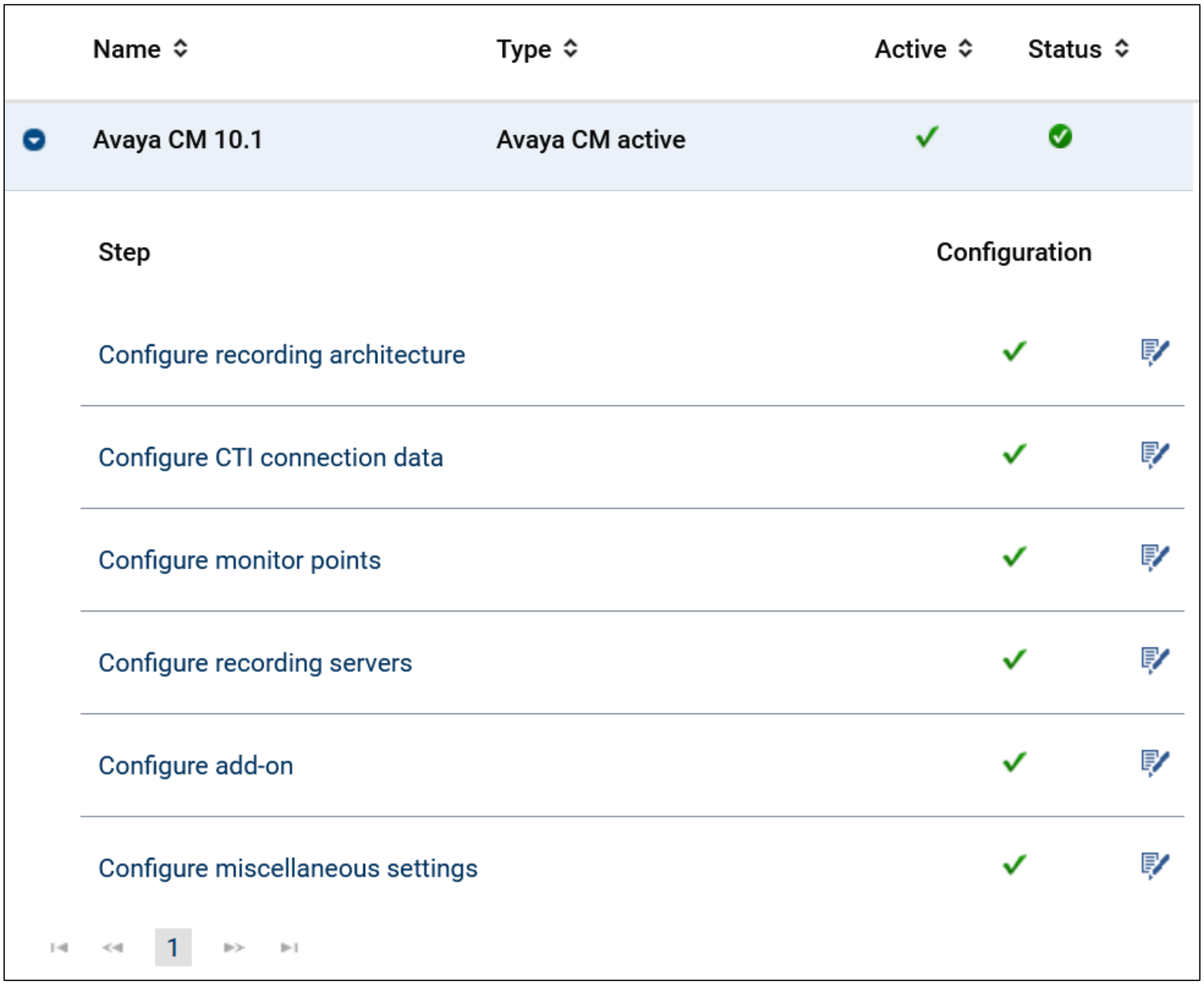
Enter the extensions to be monitored or recorded. Below shows the extension added as described in **Section 5.5**, click on **Add** once complete.



The new extension added is shown at the top of the screen. Once all the required extensions to be monitored are added, click on **Save** at the bottom of the screen.



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



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.**

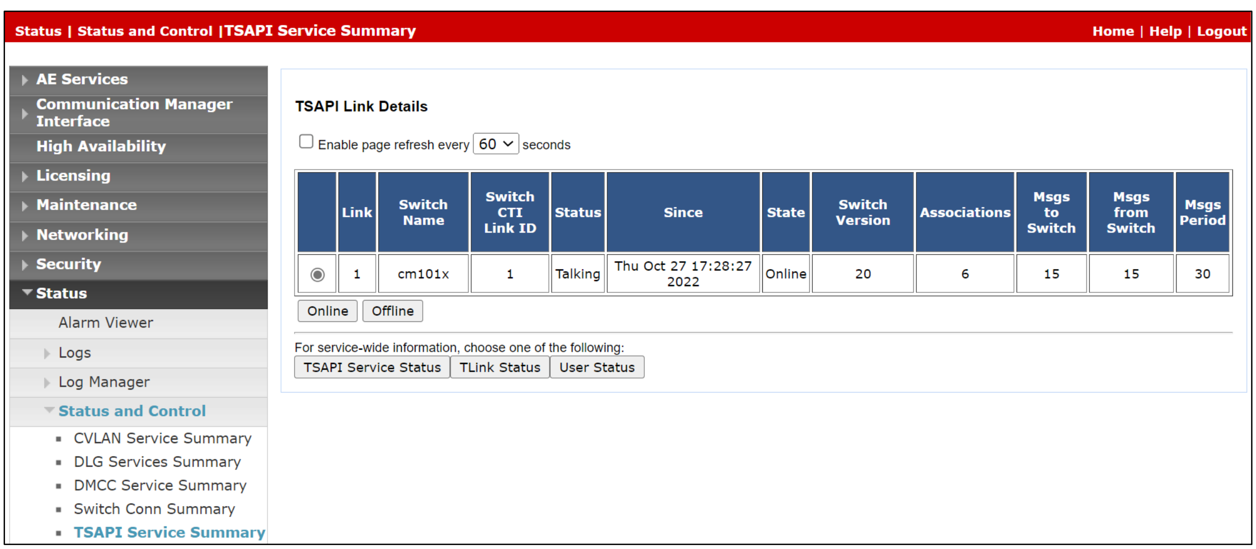
```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

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

1          12     no      aespri101x           established  865      865
```

8.2. Verify TSAPI Link and DMCC

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

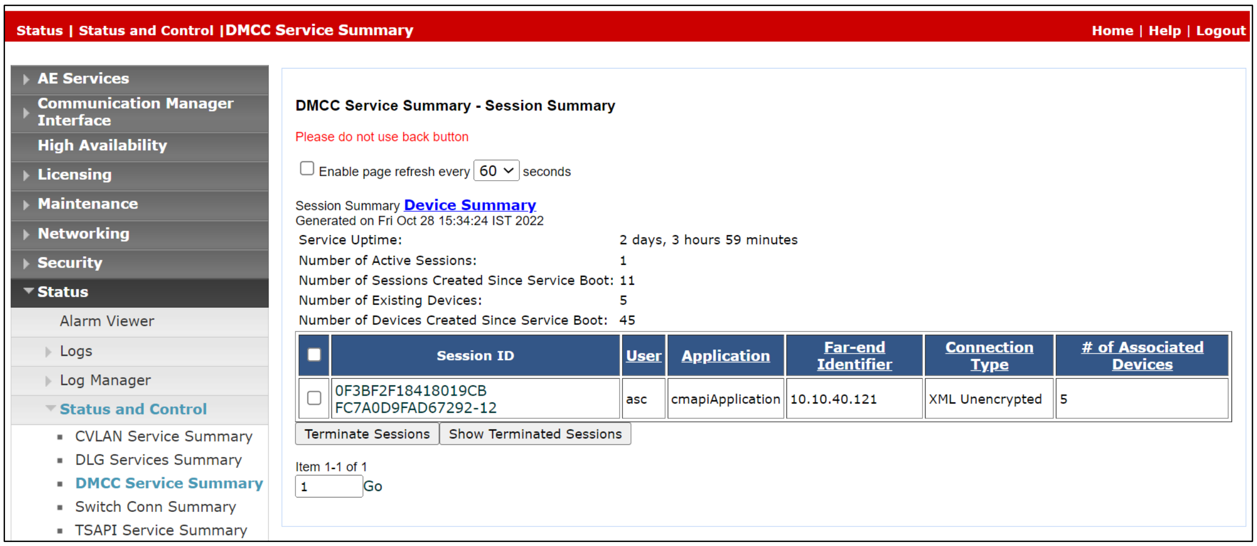
8.2.1. Verify TSAPI Link

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**.



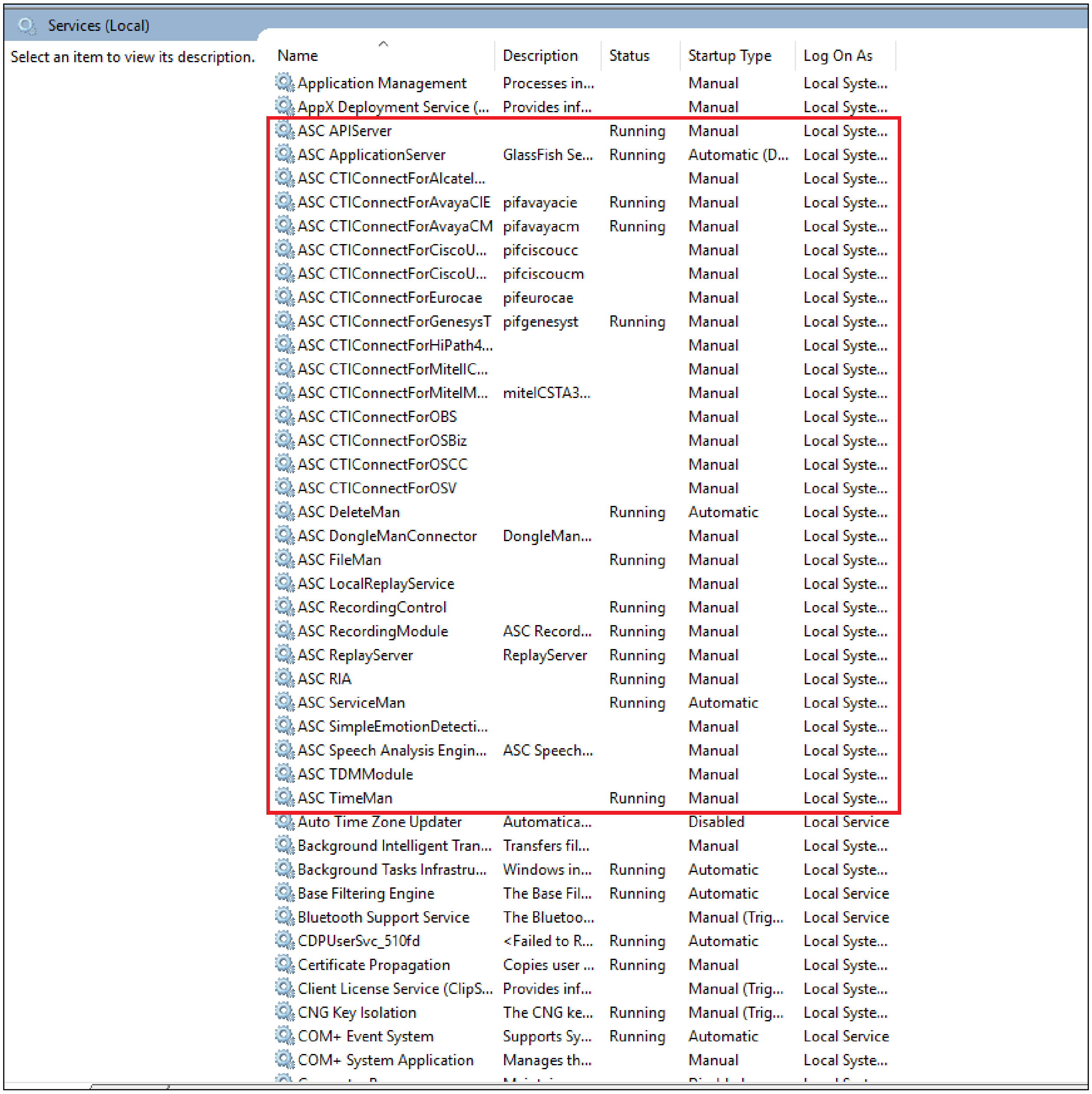
8.2.2. Verify Avaya Aura® Application Enablement Services DMCC Service

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. This user is monitoring five devices on Communication Manager, i.e., the five virtual stations that are used for Single Step Conference.



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)

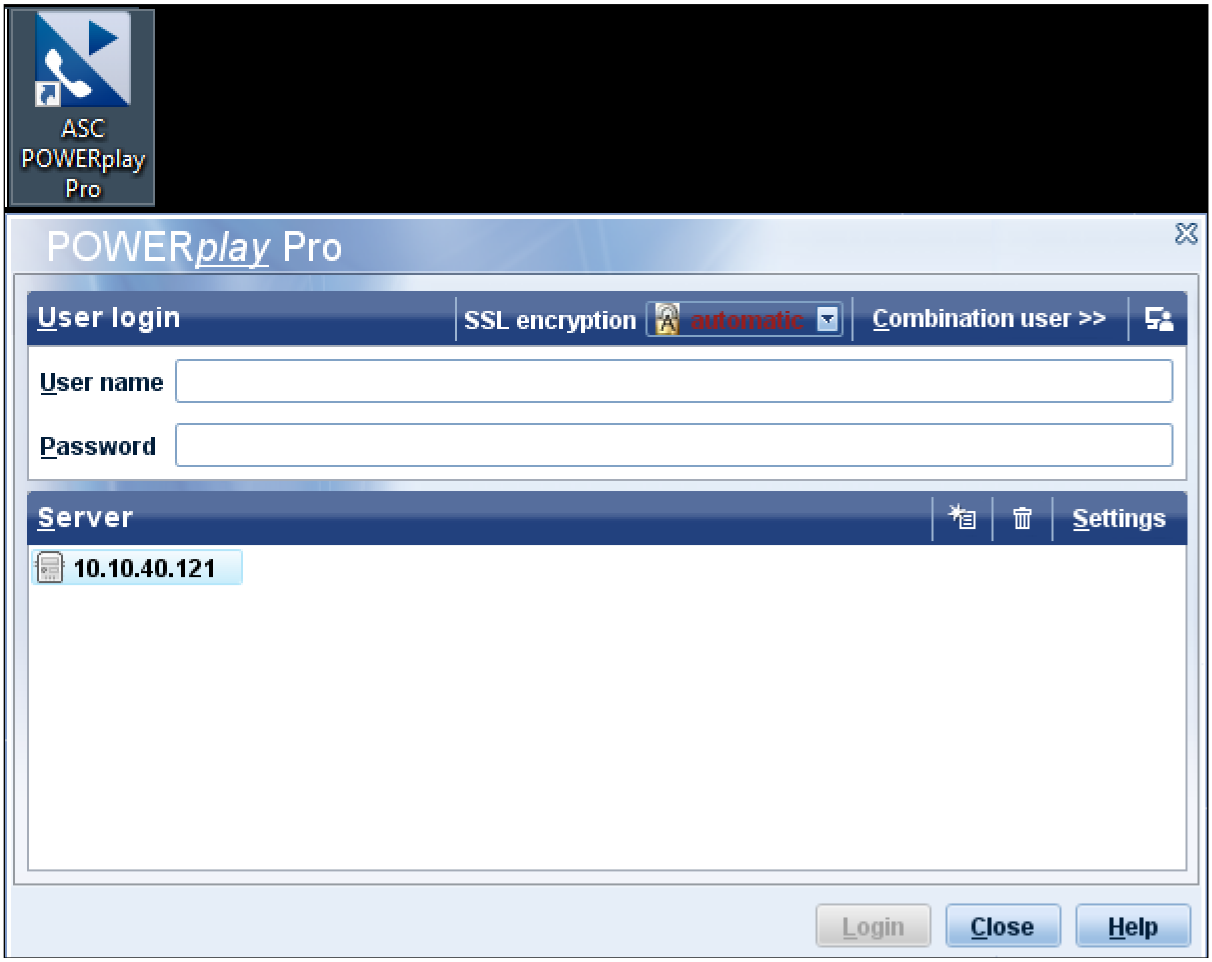
Select an item to view its description.

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...

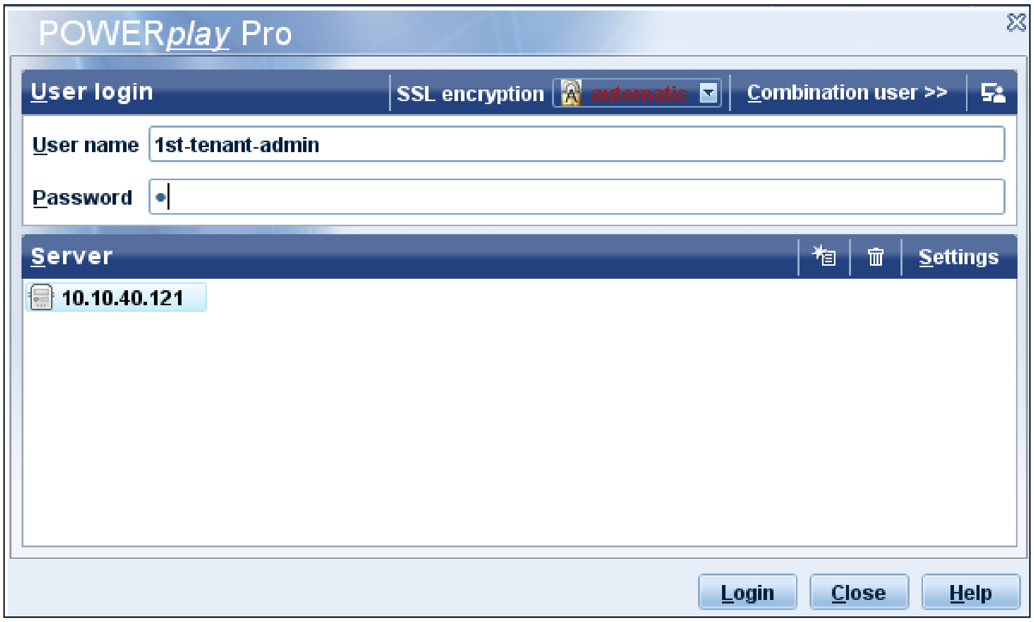
8.4. Verify ASC EVOIPneo active Capture and Playback

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

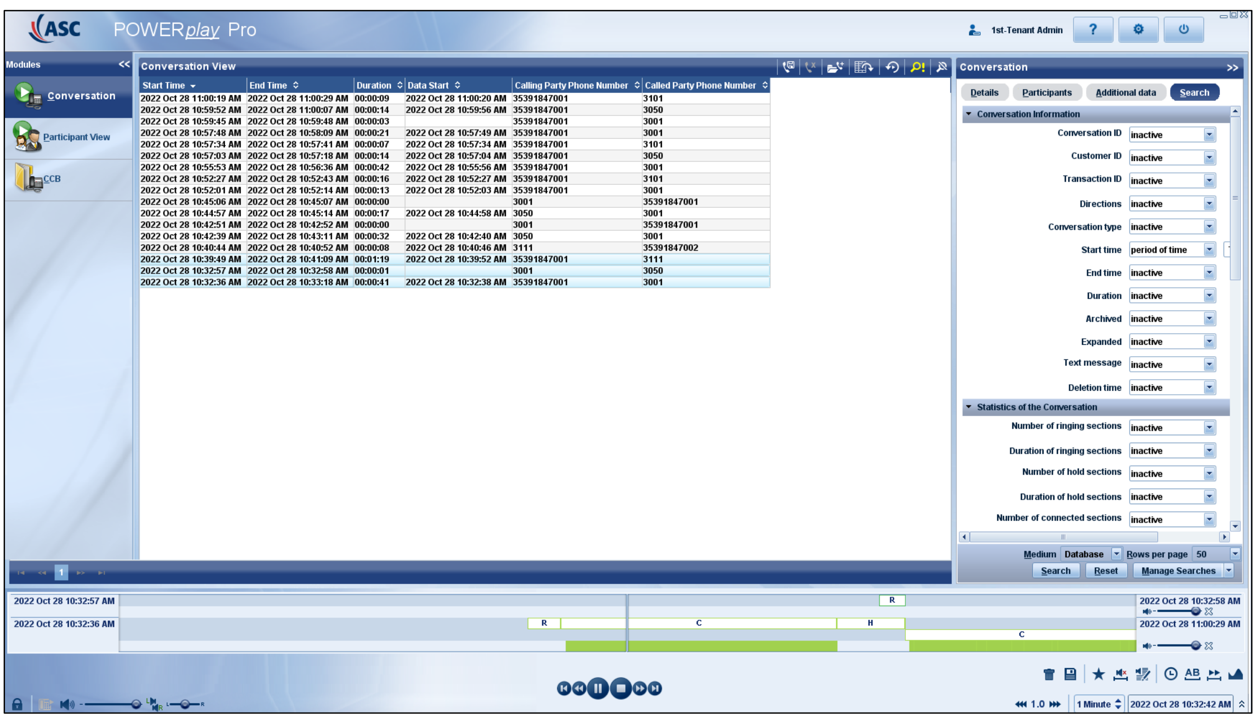
Double click on the shortcut icon and the **POWER*play* Pro** window appears as shown below.



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



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.



9. Conclusion

These Application Notes describe the configuration steps required for ASC EVOIPneo active V7.0 from ASC Technologies AG to successfully interoperate with Avaya Aura® Communication Manager R10.1 using Avaya Aura® Application Enablement Services R10.1. All feature functionality and serviceability test cases were completed successfully.

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*. Release 10.1, Issue 1, December 2021.

[2] *Administering Avaya Aura® Application Enablement Services*. Release 10.1.x, Issue 4, April 2022.

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.