



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.

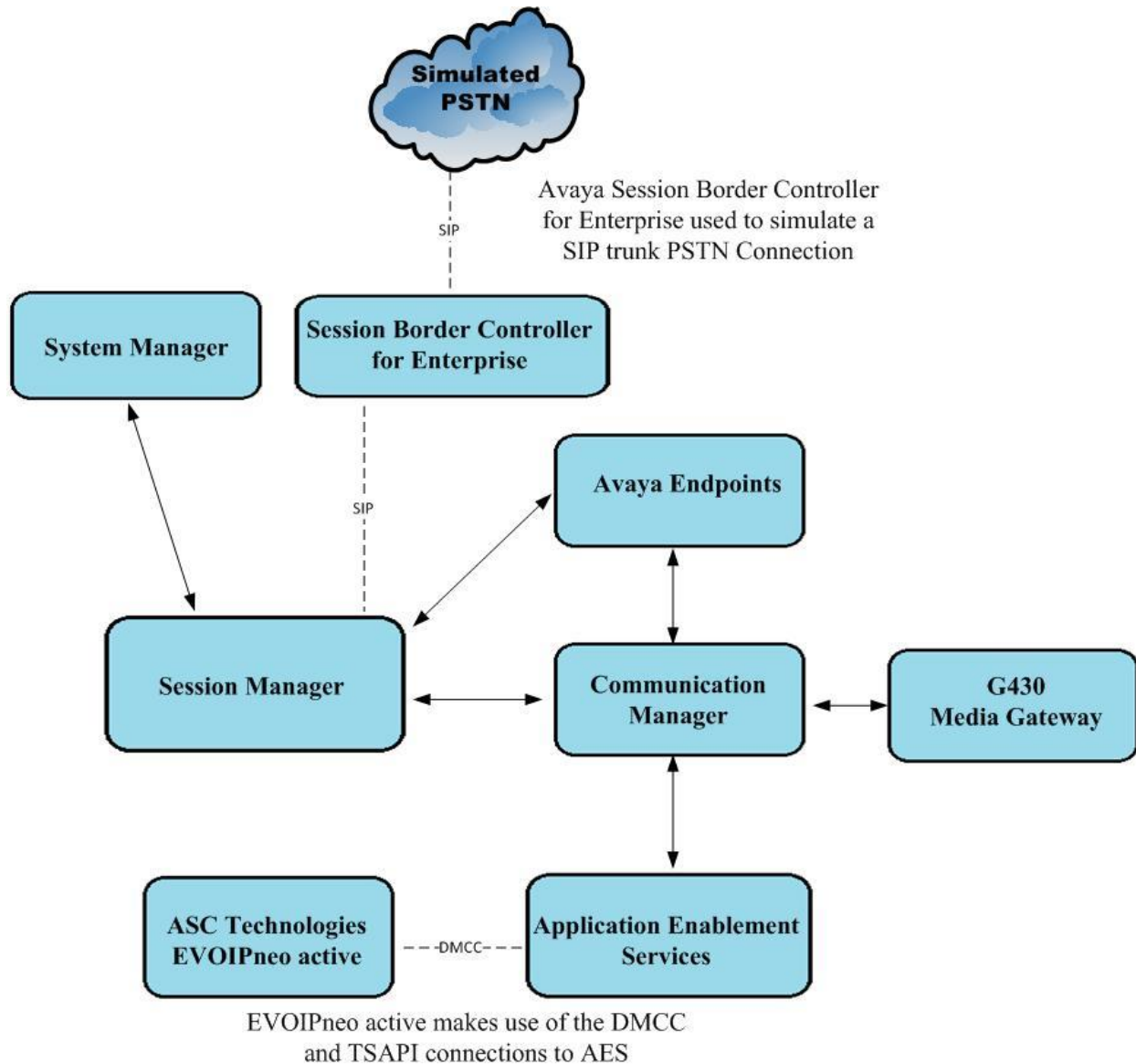


Figure 1: Avaya Aura® Communication Manager with Avaya Aura® Application Enablement Services, and ASC EVOIPneo active

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	Digital Loss Plan Modification?	y
Async. Transfer Mode (ATM) Trunking?	n	DS1 MSP?	y
ATM WAN Spare Processor?	n	DS1 Echo Cancellation?	y
ATMS?	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 Server	Password	Enabled	Status
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

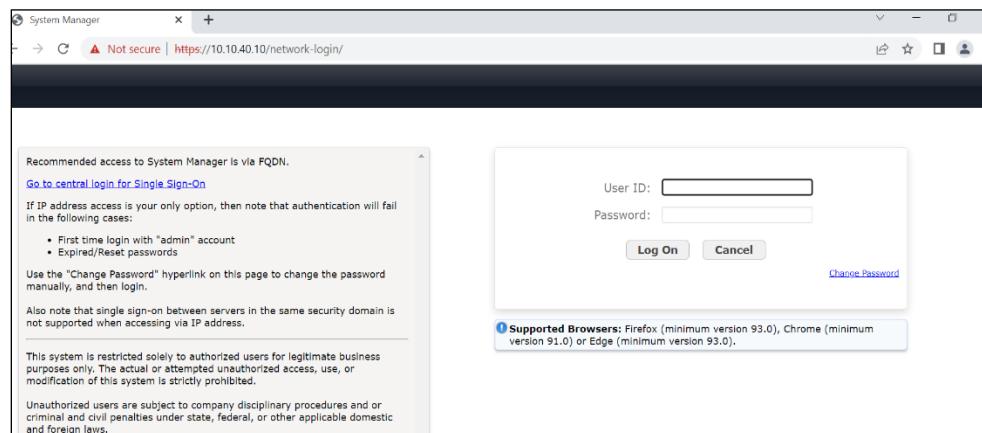
No changes were made during compliance testing for and H.323 stations that were tested. The screen below shows an example of a H.323 phone that was tested.

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		
Loss Group: 19	Time of Day Lock Table:	
	Personalized Ringing Pattern: 1	
Speakerphone: 2-way	Message Lamp Ext: 3001	
Display Language: english	Mute Button Enabled? y	
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	

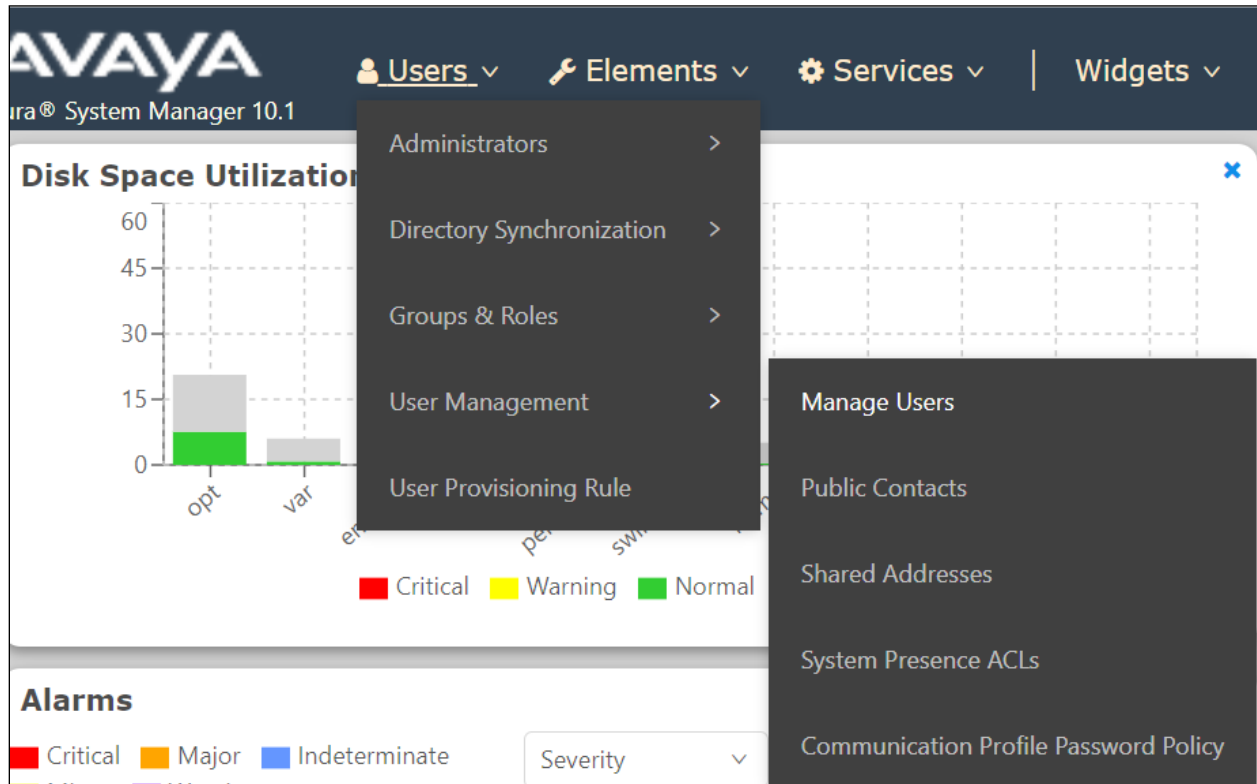
5.6. Configure SIP Stations for Single Step Conference

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.

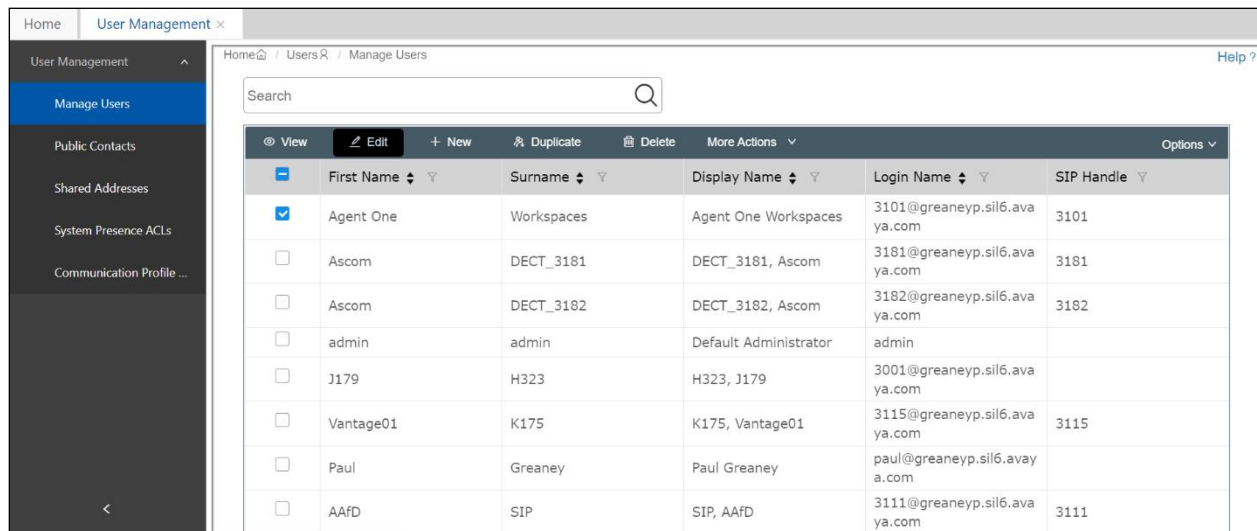
Note: The following shows changes to a SIP extension and assumes that the SIP extension has been programmed correctly and is fully functioning.



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.

Home / Users / Manage Users

User Profile | Edit | 3101@greanep.sil6.avaya.com

Commit & Continue Commit Cancel

Identity Communication Profile Membership Contacts

Communication Profile Password

PROFILE SET : Primary

Communication Address

PROFILES

Session Manager Profile

Avaya Breeze® Profile

CM Endpoint Profile

* System : cm101x

* Profile Type : Endpoint

Use Existing Endpoints :

* Extension : 3101

Template : Start typing...

* Set Type : 9641SIPCC

Security Code : Enter Security Code

Port : S000003

Voice Mail Number : 6667

Preferred Handle : Select

Calculate Route Pattern :

Sip Trunk : aar

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).

System cm101x

Extension 3101

Template Select

Set Type 9641SIPCC

Port S000003

Security Code

Name Agent One Workspaces

General Options (G) Feature Options (F) Site Data (S) Abbreviated Call Dialing (A) Enhanced Call Fwd (E)

Button Assignment (B) Profile Settings (P) Group Membership (M)

* Class of Restriction (COR) 1

* Emergency Location Ext 3101

* Tenant Number 1

* SIP Trunk aar

Coverage Path 1

Lock Message

Multibyte Language Not Applicable

* Class Of Service (COS) 1

* Message Lamp Ext. 3101

Type of 3PCC Enabled Avaya

Coverage Path 2

Localized Display Name Agent One Workspaces

Enable Reachability for Station Domain Control system

SIP URI

Primary Session Manager

IPv4: 10.10.40.12

IPv6:

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

User Profile | Edit | 3101@greanep.sil6.avaya.com

Commit & Continue

Commit

Cancel

Identity

Communication Profile

Membership

Contacts

Communication Profile Password

PROFILE SET : Primary

Communication Address

PROFILES

Session Manager Profile

Avaya Breeze® Profile

CM Endpoint Profile

* System :

cm101x

* Profile Type :

Endpoint

Use Existing Endpoints :

* Extension :

3101

Template :

Start typing...

* Set Type :

9641SIPCC

Security Code :

Enter Security Code

Port :

S000003

Voice Mail Number :

6667

Preferred Handle :

Select

Calculate Route Pattern :

Sip Trunk :

aar

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 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

Loss Group: 19

Time of Day Lock Table:

Personalized Ringing Pattern: 1

Message Lamp Ext: 33001

Mute Button Enabled? y

Speakerphone: 2-way

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

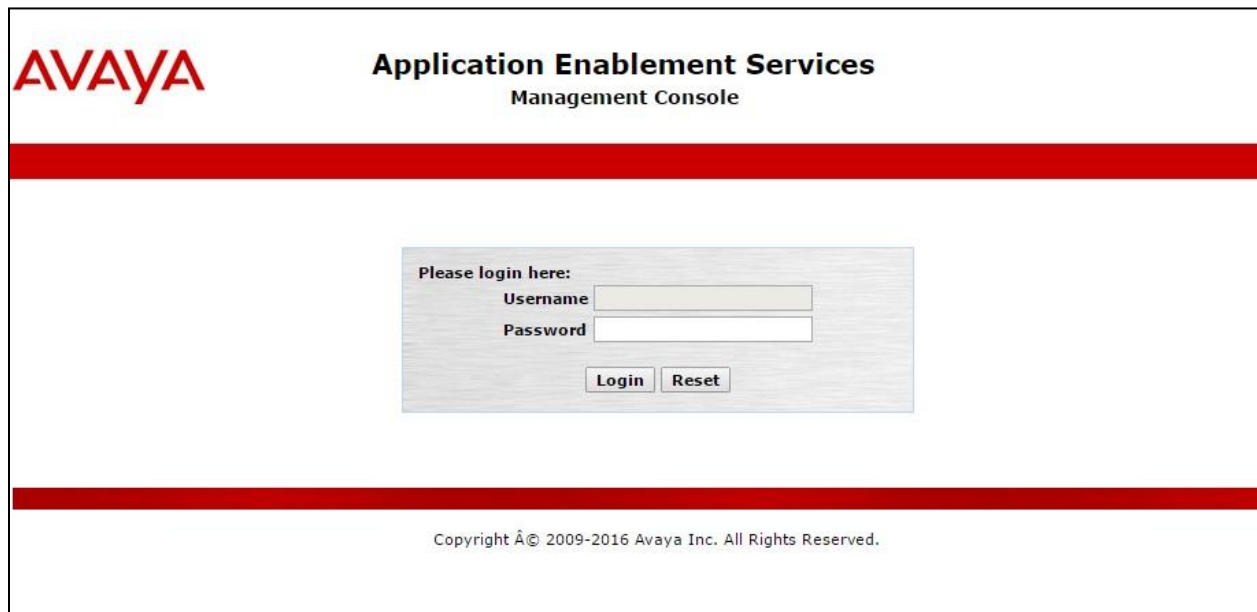
6. Configure Avaya Aura® Application Enablement Services

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 screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" is displayed in a large, bold font, with "Management Console" in a smaller font below it. A thick red horizontal bar spans the width of the page below the header. In the center of the page is a light gray rectangular box containing the login form. The form has the text "Please login here:" followed by two input fields: "Username" and "Password". Below these fields are two buttons: "Login" and "Reset". Another thick red horizontal bar is located at the bottom of the page, just above the footer. The footer text, "Copyright © 2009-2016 Avaya Inc. All Rights Reserved.", is centered at the very bottom.

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 screenshot shows the 'AE Services' page in the management console. On the left is a navigation menu with options like CVLAN, DLG, DMCC, SMS, TSAPI, TWS, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The 'Licensing' option is selected. The main content area displays a table of services and their status.

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

Below the table, there is a note: 'For status on actual services, please use [Status and Control](#)'. A footnote states: '* -- For more detail, please mouse over the Cause, you'll see the tooltip, or go to help page.' License information at the bottom indicates the system is licensed for Application Enablement (CTI) release 8.x.

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 screenshot shows the 'Licensing' page. The left navigation menu has 'Licensing' selected. The main content area provides instructions for setting up and maintaining the WebLM. It lists three scenarios: setting up/maintaining WebLM, importing/setting up/maintaining the license, and administering reserved licenses. A red note at the bottom asks users to disable their pop-up blocker.

Licensing

If you are setting up and maintaining the WebLM, you need to use the following:

- WebLM Server Address

If you are importing, setting up and maintaining the license, you need to use the following:

- WebLM Server Access

If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:

- Reserved Licenses

NOTE: Please disable your pop-up blocker if you are having difficulty with opening this page

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

▼ Application_Enablement

View license capacity

View peak usage

ASBCE

▶ Session_Border_Controller_E_AE

AVAYA_OCEANA

▶ Avaya_Oceana

CCTR

▶ ContactCenter

CE

▶ COLLABORATION_ENVIRONMENT

COLLABORATION_DESIGNER

▶ Collaboration_Designer

COLLABORATIVE_BROWSING_SNAP-IN

▶ Collaborative_Browsing_Snap_In


COMMUNICATION_MANAGER

▶ Call_Center

▶ Communication_Manager

License File Host IDs:

Licensed Features

10 Items  Show

All ▼

Feature (License Keyword)	Expiration date	Licensed capacity
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	44
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	44
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	44
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	4
DLG VALUE_AES_DLG	permanent	44
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	44
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	4
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	44

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**.

Application Enablement Services

Management Console

Welcome: User cust

Last login: Fri Sep 9 17:54:25 2022 from 192.168.40.240

Number of prior failed login attempts: 0

HostName/IP: aespri101x/10.10.40.16

Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE

SW Version: 10.1.0.1.0.7-0

Server Date and Time: Tue Sep 20 15:52:43 IST 2022

HA Status: Not Configured

Communication Manager Interface | Switch Connections

Home | Help | Logout

AE Services

Communication Manager Interface

Switch Connections

Dial Plan

High Availability

Licensing

Maintenance

Networking

Switch Connections


Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> cm101x	Yes	30	1

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.

Name or IP Address	Status
10.10.40.13	In Use

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



Application Enablement Services
Management Console

Welcome: User cust
Last login: Fri Sep 9 17:54:25 2022 from 192.168.40.240
Number of prior failed login attempts: 0
HostName/IP: aespri101x/10.10.40.16
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.0.1.0.7-0
Server Date and Time: Tue Sep 20 15:52:43 IST 2022
HA Status: Not Configured

Communication Manager Interface | Switch ConnectionsHome | Help | Logout

▶ AE Services

▼ Communication Manager Interface

Switch Connections

▶ Dial Plan

High Availability

▶ Licensing

▶ Maintenance

▶ Networking

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> cm101x	Yes	30	1

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

Communication Manager Interface | Switch Connections

▶ AE Services

▼ Communication Manager Interface

Switch Connections

▶ Dial Plan

High Availability

▶ Licensing

▶ Maintenance

▶ Networking

Switch Connections

Edit H.323 Gatekeeper - cm101x

Name or IP Address

☒ 10.10.40.13

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.

The screenshot shows the 'AE Services | TSAPI | TSAPI Links' page. On the left, a sidebar lists 'AE Services' (CVLAN, DLG, DMCC, SMS) and 'TSAPI' (TSAPI Links, TSAPI Properties). The main content area is titled 'TSAPI Links' and contains a table with two columns: 'Link' and 'Switch Connection'. Below the table are three buttons: 'Add Link', 'Edit Link', and 'Delete Link'.


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**.

The screenshot shows the 'Edit TSAPI Links' screen. The sidebar is similar to the previous screen but includes 'TWS' and 'Communication Manager Interface' under 'TSAPI'. The main content area is titled 'Edit TSAPI Links' and contains the following fields: 'Link' (set to 1), 'Switch Connection' (set to cm101x), 'Switch CTI Link Number' (set to 1), 'ASAI Link Version' (set to 12), and 'Security' (set to Both). At the bottom are three buttons: 'Apply Changes', 'Cancel Changes', and 'Advanced Settings'.

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.**

Apply Cancel

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

TSAPI Links				
Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
<input checked="" type="radio"/> 1	cm101x	1	12	Both
<div>Add Link Edit Link Delete Link</div>				

6.4. Identify Tlinks

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

Security | Security Database | Tlinks

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▼ Security

▶ Account Management

▶ Audit

▶ Certificate Management

▶ Enterprise Directory

▶ Host AA

▶ PAM

▼ Security Database

▪ Control

▪ CTI Users

▪ Devices

▪ Device Groups

▪ **Tlinks**

▪ Tlink Groups

▪ Worktops

Tlinks
Tlink Name
☒ AVAYA#CM101X#CSTA#AESPRI101X
☐ AVAYA#CM101X#CSTA-S#AESPRI101X

Delete Tlink

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**.

▶ AE Services			
▶ Communication Manager Interface			
High Availability			
▶ Licensing			
▶ Maintenance			
▼ Networking			
AE Service IP (Local IP)			
Network Configure			
Ports			
TCP/TLS Settings			
▶ Security			
▶ Status			
▶ User Management			
▶ Utilities			
▶ Help			

Ports

CVLAN Ports			Enabled	Disabled
Unencrypted TCP Port	9999		<input checked="" type="radio"/>	<input type="radio"/>
Encrypted TCP Port	<input type="text" value="9998"/>		<input checked="" type="radio"/>	<input type="radio"/>

DLG Port	TCP Port	5678		
----------	----------	------	--	--

TSAPI Ports			Enabled	Disabled
TSAPI Service Port	450		<input checked="" type="radio"/>	<input type="radio"/>
Local TLINK Ports				
TCP Port Min	1024			
TCP Port Max	1039			
Unencrypted TLINK Ports				
TCP Port Min	<input type="text" value="1050"/>			
TCP Port Max	<input type="text" value="1065"/>			
Encrypted TLINK Ports				
TCP Port Min	<input type="text" value="1066"/>			
TCP Port Max	<input type="text" value="1081"/>			

DMCC Server Ports			Enabled	Disabled
Unencrypted Port	<input type="text" value="4721"/>		<input checked="" type="radio"/>	<input type="radio"/>
Encrypted Port	<input type="text" value="4722"/>		<input checked="" type="radio"/>	<input type="radio"/>
TR/87 Port	<input type="text" value="4723"/>		<input checked="" type="radio"/>	<input type="radio"/>

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.

User Management | User Admin

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).

High Availability	* User Id	asc
▶ Licensing	* Common Name	asc
▶ Maintenance	* Surname	asc
▶ Networking	User Password
▶ Security	Confirm Password
▶ Status	Admin Note	
▼ User Management	Avaya Role	None ▼
▶ Service Admin	Business Category	
▼ User Admin	Car License	
▪ Add User	CM Home	
▪ Change User Password	Css Home	
▪ List All Users	CT User	Yes ▼
▪ Modify Default Users	Department Number	
▪ Search Users	Display Name	
▶ Utilities	Employee Number	
▶ Help	Employee Type	
	Enterprise Handle	
	Given Name	
	Home Phone	
	Home Postal Address	


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.



The screenshot shows a web-based configuration interface. On the left is a vertical navigation menu with the following items: 'AE Services', 'Communication Manager Interface', 'High Availability', 'Licensing', 'Maintenance', 'Networking', 'Security' (expanded), 'Account Management', 'Audit', 'Certificate Management', 'Enterprise Directory', 'Host AA', 'PAM', 'Security Database' (expanded), 'Control' (selected), and 'CTI Users'. The main content area on the right is titled 'SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services'. It contains two checkboxes: 'Enable SDB for DMCC Service' (unchecked) and 'Enable SDB for TSAPI Service, JTAPI and Telephony Web Services' (checked). Below these checkboxes is an 'Apply Changes' button.

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**.

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▼ Security

▶ Account Management

▶ Audit

▶ Certificate Management

▶ Enterprise Directory

▶ Host AA

▶ PAM

▼ Security Database

▪ Control

▣ CTI Users

▪ List All Users

▪ Search Users

CTI Users

User ID	Common Name	Worktop Name	Device ID
<input checked="" type="radio"/> asc	asc	NONE	NONE
<input type="radio"/> nice1	nice1	NONE	NONE
<input type="radio"/> paul1	paul1	NONE	NONE
<input type="radio"/> paul2	paul2	NONE	NONE
<input type="radio"/> sytel	Sytel	NONE	NONE

EditList All

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

Edit CTI User

User Profile:

User IDasc

Common Nameasc

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

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.

Maintenance | Service Controller

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▼ Maintenance

Date Time/NTP Server

▶ Security Database

Service Controller

▶ Server Data

▶ Networking

▶ Security

▶ Status

Service Controller

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

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

Start

Stop

Restart Service

Restart AE Server

Restart Linux

Restart Web Server

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

Maintenance | Service Controller

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▼ Maintenance

Date Time/NTP Server

▶ Security Database

Service Controller

▶ Server Data

Restart AE Server

Warning! Are you sure you want to restart?
Restarting will cause all existing connections to be dropped and associations lost.

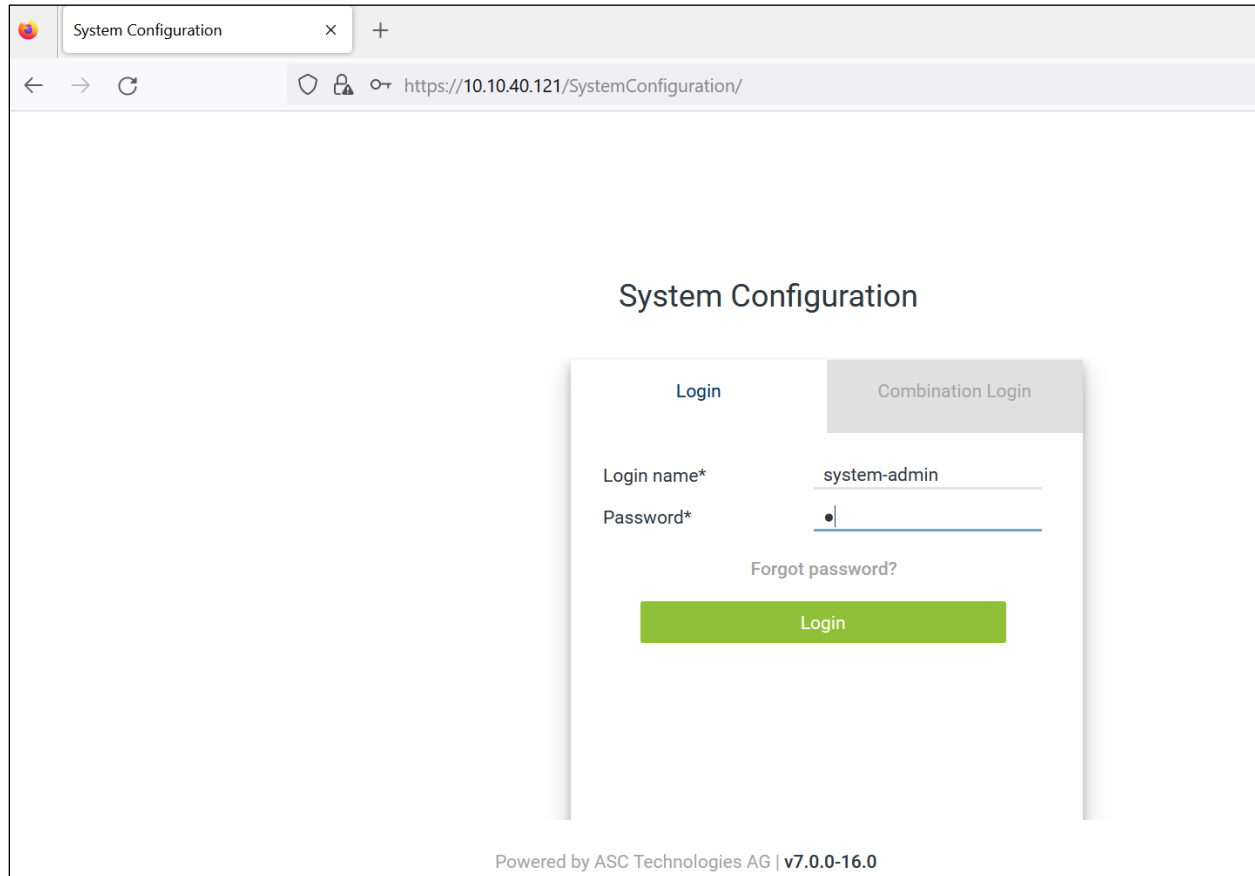
Restart

Cancel

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.

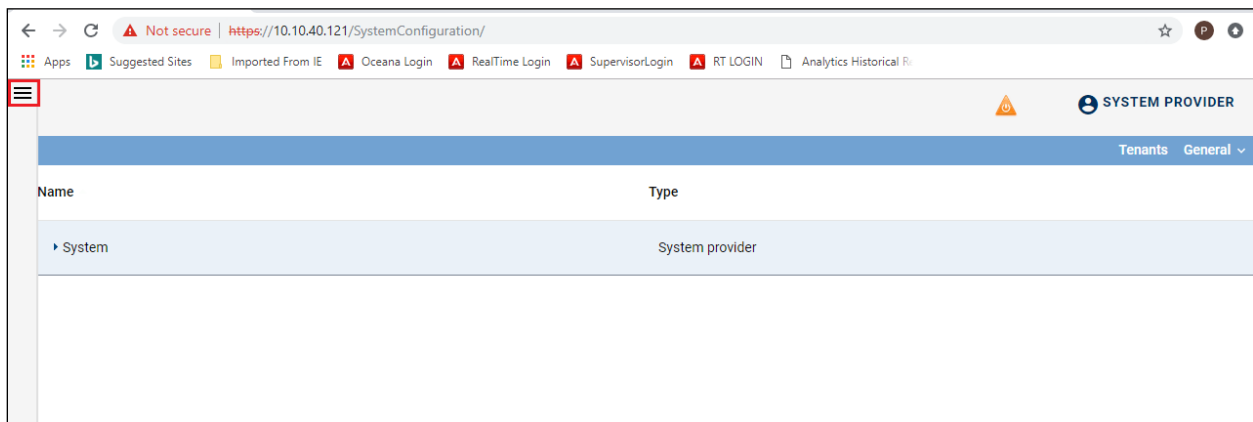
Using Mozilla Firefox open a web session to **https://<ServerIP>/SystemConfiguration**. Enter the proper username and password and click on **Login**.



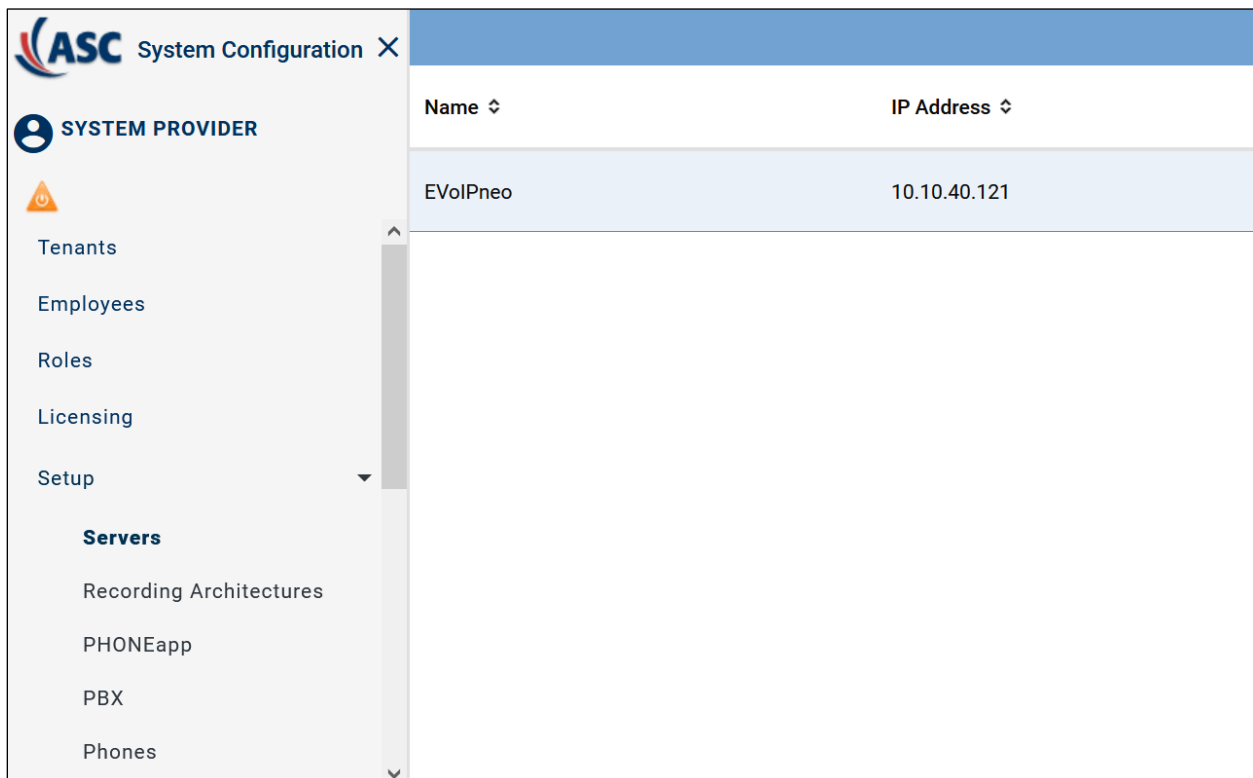
The screenshot shows a web browser window with the title "System Configuration". The address bar displays the URL "https://10.10.40.121/SystemConfiguration/". The main content area features a "System Configuration" heading and a login form. The form has two tabs: "Login" (selected) and "Combination Login". Under the "Login" tab, there are two input fields: "Login name*" with the value "system-admin" and "Password*" with a masked password. Below these fields is a link for "Forgot password?". A green "Login" button is positioned at the bottom of the form. At the very bottom of the page, a footer reads "Powered by ASC Technologies AG | v7.0.0-16.0".

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.

The screenshot shows a web application window titled "EVolPneo". On the left, a table lists server entries with columns "Name" and "IP Address". The entry "EVolPneo" with IP "10.10.40.121" is selected. On the right, a configuration panel for the selected server is shown with tabs: "Details*", "Usage*", "Media Streamer", and "Replay Server Address Mapping". The "Details*" tab is active, displaying fields for "Name" (EVolPneo), "Configured IP address" (10.10.40.121), "IP address*" (a dropdown menu showing 10.10.40.121), and "Server location" (a dropdown menu showing "Please choose..."). A "Help" icon is visible in the top right of the configuration panel.

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.

The screenshot shows the same web application window, but now the "Usage*" tab is active in the configuration panel. It contains several sections: "API Server" with a checked checkbox for "API server" and a text field for "API server name*" containing "apitest"; "Storage expansions" with a table header showing "Path" and "Server" and a message "No records found"; a checkbox for "Replay via phone"; and "Recording Control/Key Management" with a checkbox for "Recording control/Live Streaming", a dropdown for "Recording architecture" showing "Please choose...", and a checkbox for "Neo key management". At the bottom of the configuration panel are "Save" and "Reset" buttons. The left table remains the same, and the bottom of the screen shows pagination information: "Rows per page 50", "1 - 1 of 1", and navigation arrows.

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

Name	IP Address
EVolPneo	10.10.40

Usage*

Replay

☒ Replay server

Replay server*replaytest

WebSocket port*12345
(max. 5 characters)

API server*

Name	Connection Status
EVolPneo	OK

Virtualization

☐ VM without Trusted License

SaveReset

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**.

ASC System Configuration

Tenants
Employees
Roles
Licensing
Setup
Servers
Recording Architectures
PHONEapp
PBX
Phones
Integrations

SYSTEM PROVIDER

NameTypeActiveStandby active

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*

Avaya CM 10.1

Type

All-in-one Basic

OK

Cancel

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

Avaya CM 10.1

All-in-one Basic

×

⋮

Details*

Server Assignment*

?

Help

Name*

Avaya CM 10.1

Recording architecture

All-in-one Basic

Active

Inactive

Integration Type

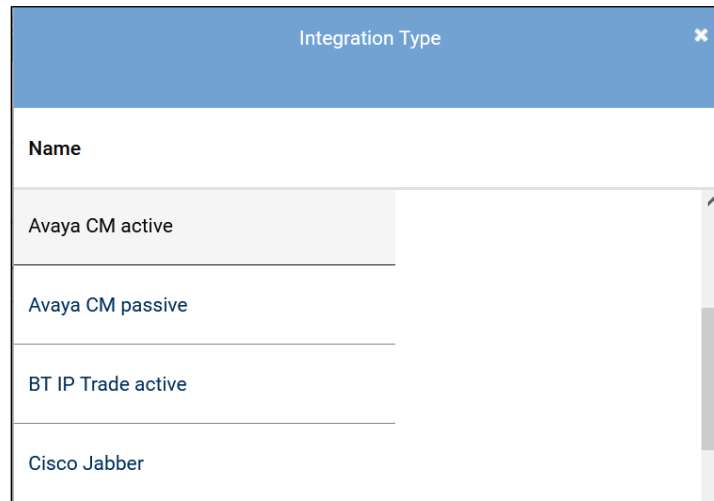
≡ +

≡ -

Name

No records found

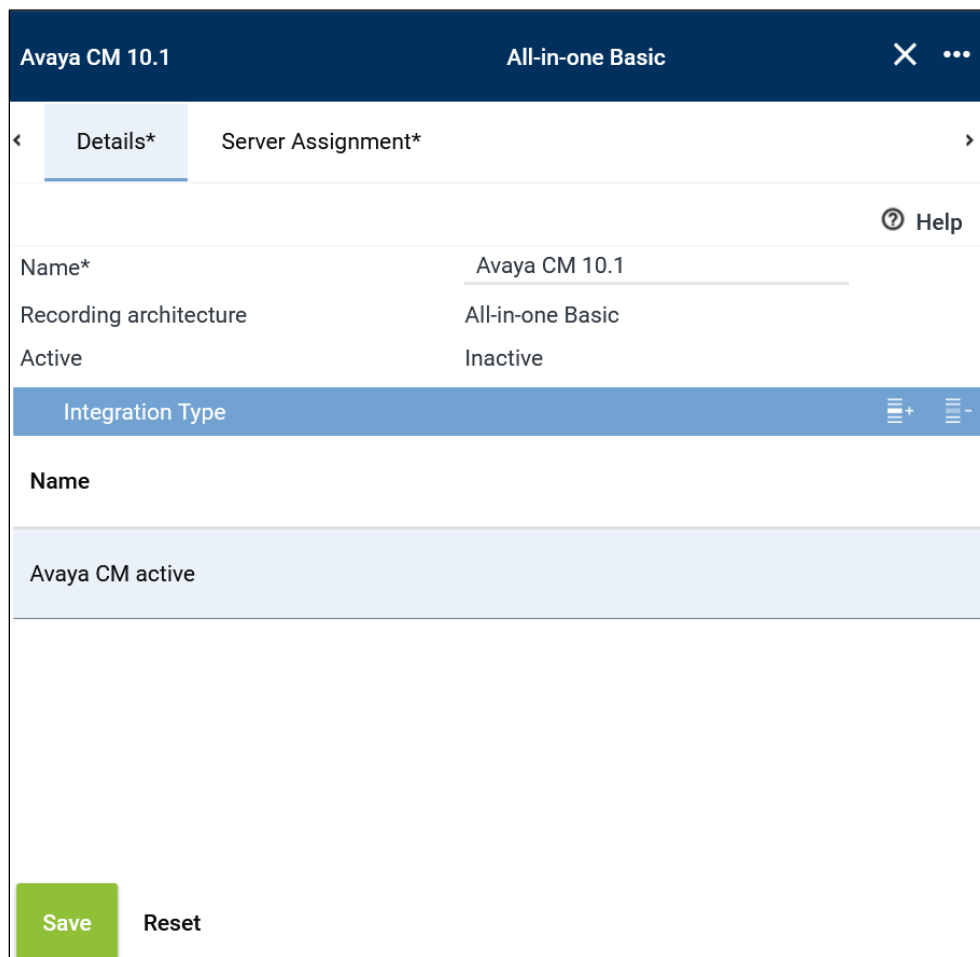
A screen is opened showing the **Integration Type** that is present depending on license. Select **Avaya CM active** and click on **Add** at the bottom of this screen (not shown).



The image shows a dialog box titled "Integration Type" with a close button (X) in the top right corner. Inside the dialog, there is a list of integration types. The first item, "Avaya CM active", is highlighted with a light gray background. Below it are "Avaya CM passive", "BT IP Trade active", and "Cisco Jabber". A vertical scrollbar is visible on the right side of the list.

Integration Type
Avaya CM active
Avaya CM passive
BT IP Trade active
Cisco Jabber

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



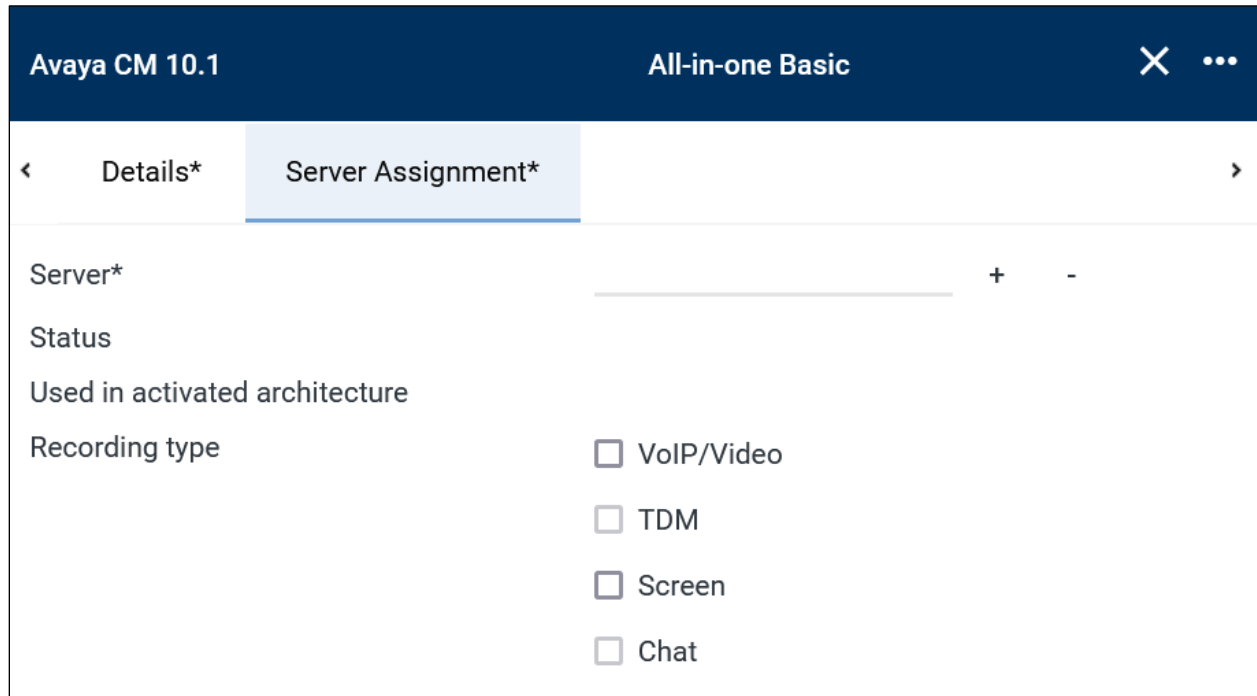
The image shows a configuration screen for "Avaya CM 10.1" under the "All-in-one Basic" license. The screen has a dark blue header with the title and license name, and a close button (X) and a menu button (three dots). Below the header, there are two tabs: "Details*" and "Server Assignment*", with "Details*" being the active tab. A "Help" button (question mark icon) is located in the top right corner of the main content area. The main content area contains a form with the following fields:

- Name***: Avaya CM 10.1
- Recording architecture**: All-in-one Basic
- Active**: Inactive

Below the form, there is a section titled "Integration Type" with a blue header and a list of integration types. The first item, "Avaya CM active", is highlighted with a light blue background. At the bottom of the screen, there are two buttons: "Save" (green) and "Reset" (gray).

Integration Type
Avaya CM active

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



Avaya CM 10.1 All-in-one Basic

< Details* Server Assignment* >

Server* _____ + -

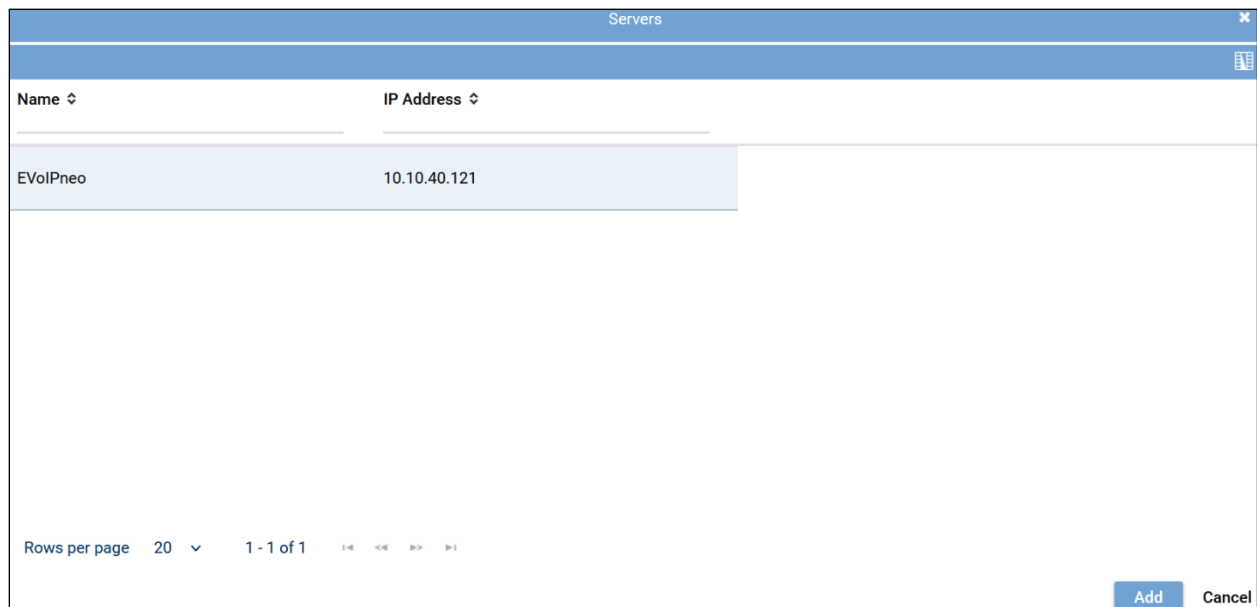
Status

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.



Servers	
Name ↕	IP Address ↕
EVoIPneo	10.10.40.121

Rows per page 20 ▾ 1 - 1 of 1 < << >> >

Add Cancel

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

Avaya CM 10.1

All-in-one Basic

✕ ...

< Details*

Server Assignment*

>

Server*

EVolPneo

+

-

Used in activated architecture

Yes

Recording type

☒ VoIP/Video

☐ TDM

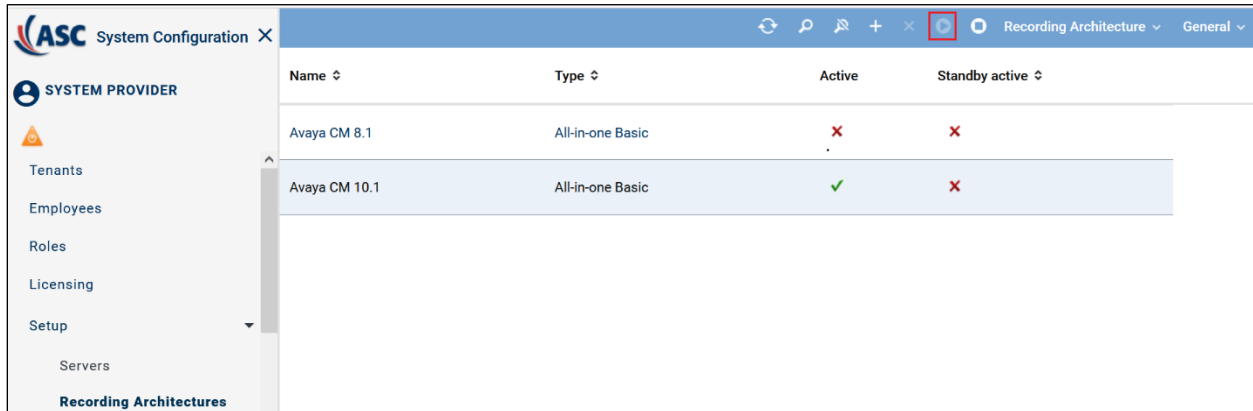
☐ Screen

☐ Chat

Save

Reset

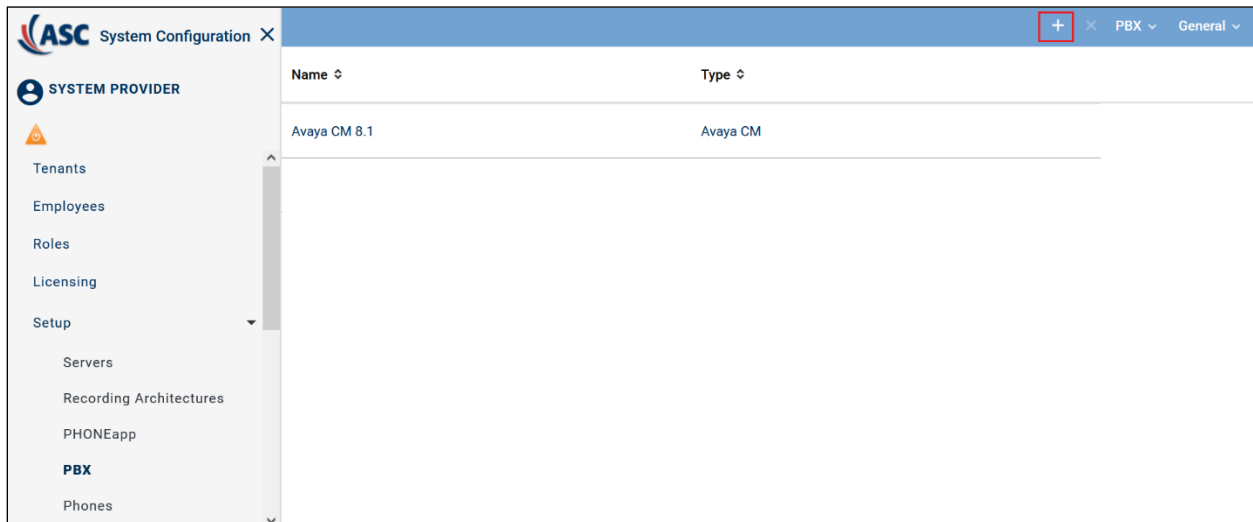
Once this Recording Architecture is added it must be activated by clicking on the **Activate** icon highlighted below.



Name	Type	Active	Standby active
Avaya CM 8.1	All-in-one Basic	✗	✗
Avaya CM 10.1	All-in-one Basic	✓	✗

7.3. Add PBX

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



Name	Type
Avaya CM 8.1	Avaya CM

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

Avaya CM 10.1

×

⋮

Details*

PHONEapp Configuration

Web Service

Name*

Avaya CM 10.1

PBX type

Avaya CM

Maximum length of extensions

4

▼

Country code

☒ Select from list

Ireland (353)

▼

☐ Enter manually

Area code*

91

Net code*

1234

Non Phone IPs

No records found

Add

Delete

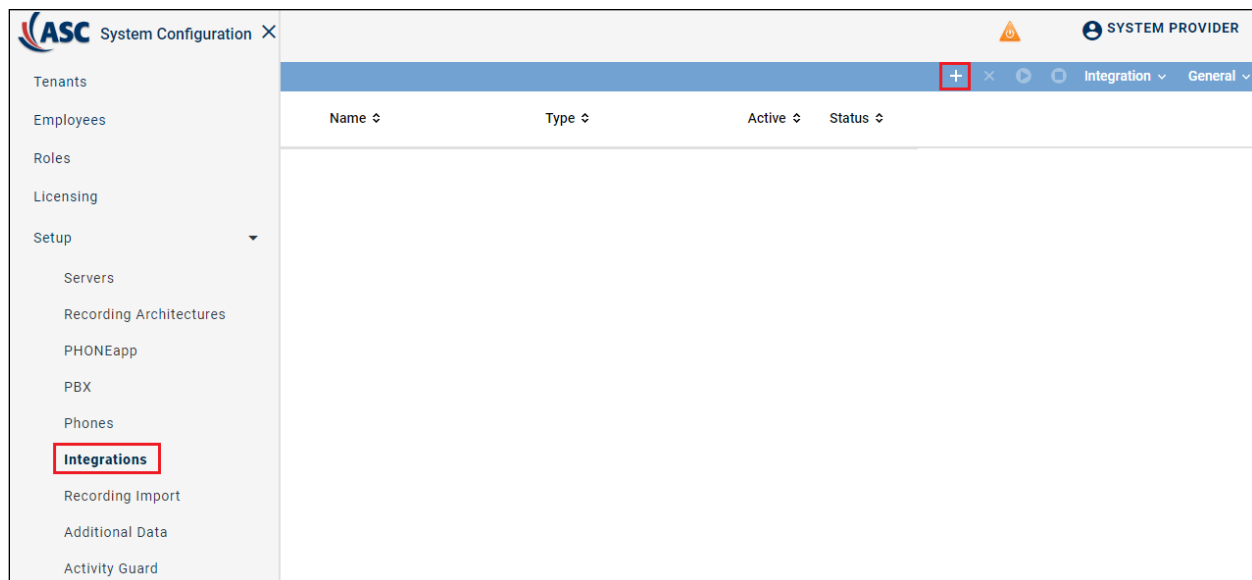
IPs to be ignored

Save

Reset

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.

The screenshot shows the 'New Integration' form. At the top, there are two tabs: 'Integration Type' and 'Recording Architecture'. The 'Integration Type' tab is active. Below the tabs, there are two input fields: 'Name*' with the value 'Avaya CM 10.1' and 'Integration type*' with the value 'Avaya CM active' and a dropdown arrow. Below these fields, there is a blue button labeled 'PBX' with a '+' icon next to it. At the bottom, there is a 'PBX*' field with a '+' and '-' icon next to it.

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

Name	Type
Avaya CM 10.1	Avaya CM

Rows per page: 20 | 1 - 1 of 1 | < > << >>

Add **Cancel**

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

New Integration

Integration Type | Recording Architecture

Name* Avaya CM 10.1

Integration type* Avaya CM active

PBX +

PBX* Avaya CM 10.1 + -

Cancel **Back** **Next**

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

New Integration

Integration Type

Recording Architecture

Recording Architecture

Recording architecture*

Avaya CM 10.1

▼

Save




















Cancel

Back

Next

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

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

Name ↕	Type ↕	Active ↕	Status ↕
 Avaya CM 10.1	Avaya CM active		
Step		Configuration	
Configure recording architecture			
Configure CTI connection data			
Configure monitor points			
Configure recording servers			
Configure add-on			
Configure miscellaneous settings			
  1  			

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**.

Step: Configure CTI Connection Data

Module 1*

CTIconnect Module

Type	CTIconnect active
Grammar name*	Avaya
Grammar version*	1.00.59

Connection Data

PE/CLAN IP address	AES server IP address
<div></div>	
<div><div>Add</div><div>Edit</div><div>Delete</div></div>	
Audio codec	G711A
Operation mode	Single Step Conference Mode
Encryption	none

Save

Cancel

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**.

Configure Connection

PE/CLAN IP address*

10.10.40.13

Switch connection name*

CM101X

AES server IP address*

10.10.40.16

AES server port*

4721

PBX user name*

asc

PBX password*

☐ Encrypted AES connection

Add

Cancel

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

Step: Configure CTI Connection Data

Module 1*

PE/CLAN IP address	AES server IP address
10.10.40.13	10.10.40.16

Add

Edit

Delete

Audio codec

G711A

Operation mode

Single Step Conference Mode

Encryption

none

Softphone Extension

No records found.

Add

Delete

Extensions to be Ignored

No records found.

Add

Delete

Save

Cancel

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)

33001-33005

Replace existing list of extensions

Add

Cancel

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*

33003
33004
33005

Add

Delete

Extensions to be Ignored ↕

No records found.

Add

Delete

☒ Activate password

Password*

••••





















Additional Data

Save

Cancel

7.4.2. Configure monitor points

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

Name ↕	Type ↕	Active ↕	Status ↕
 Avaya CM 8.1	Avaya CM active		
 Avaya CM 10.1	Avaya CM active		
Step		Configuration	
Configure recording architecture			
Configure CTI connection data			
Configure monitor points			
Configure recording servers			
Configure add-on			
  1  			

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

Step: Configure Monitor Points ✕	
Extension Monitor Points	Attendant extension monitor points
Extension ▲	Active ⇅
3020	✓
3050	✓
3101	✓
3110	✓
3111	✓
Add Active/Inactive Delete	

Enter the extensions to be monitored or recorded. Below shows the extension added as described in **Section 5.5**, 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)

☐ Replace existing list of extensions

AddCancel

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.

Step: Configure Monitor Points

Extension Monitor Points

Attendant extension monitor points

Extension ▲

Active ⇅

3001	✓
3020	✓
3050	✓
3101	✓
3110	✓
3111	✓

Add







Active/Inactive

Delete

Save

Cancel

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

Name ⇅	Type ⇅	Active ⇅	Status ⇅
▼ Avaya CM 10.1	Avaya CM active	✓	✓
Step		Configuration	
Configure recording architecture		✓	
Configure CTI connection data		✓	
Configure monitor points		✓	
Configure recording servers		✓	
Configure add-on		✓	
Configure miscellaneous settings		✓	
◀◀ 1 ▶▶ ▶▶			

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 aescvcs cti-link**. Verify the **Service State** of the CTI link is **established**.

status aescvcs cti-link							
AE SERVICES CTI LINK STATUS							
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs 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**.

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

AE Services

Communication Manager Interface

High Availability

Licensing

Maintenance

Networking

Security

Status

Alarm Viewer

Logs

Log Manager

Status and Control

CVLAN Service Summary

DLG Services Summary

DMCC Service Summary

Switch Conn Summary

TSAPI Service Summary

TSAPI Link Details

☐ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input checked="" type="radio"/>	1	cm101x	1	Talking	Thu Oct 27 17:28:27 2022	Online	20	6	15	15	30

OnlineOffline

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

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

Status | Status and Control | DMCC Service Summary

Home | Help | Logout

AE Services

Communication Manager Interface

High Availability

Licensing

Maintenance

Networking

Security

Status

Alarm Viewer

Logs

Log Manager

Status and Control

CVLAN Service Summary

DLG Services Summary

DMCC Service Summary

Switch Conn Summary

TSAPI Service Summary

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)

Generated on Fri Oct 28 15:34:24 IST 2022

Service Uptime: 2 days, 3 hours 59 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 11

Number of Existing Devices: 5

Number of Devices Created Since Service Boot: 45

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	0F3BF2F18418019CB FC7A0D9FAD67292-12	asc	cmapiApplication	10.10.40.121	XML Unencrypted	5

Terminate Sessions

Show Terminated Sessions

Item 1-1 of 1

1 Go

8.3. Verify ASC EVOIPneo active services are running

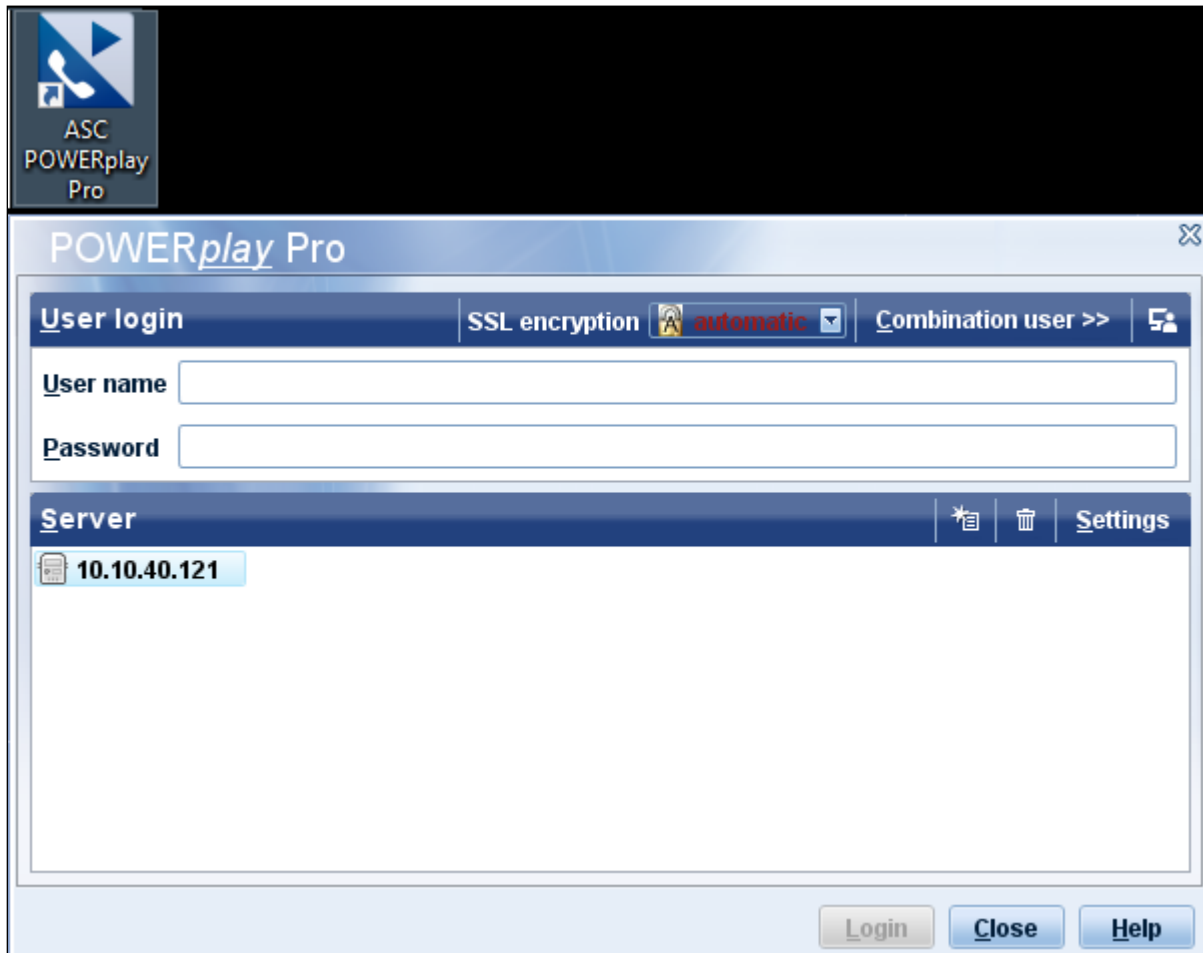
Open services.exe and ensure that the correct ASC services are running. Below is a list of services that were running during the compliance testing.

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 CTIConnectForMitellC...			Manual	Local Syste...	
ASC CTIConnectForMitellM...	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...	

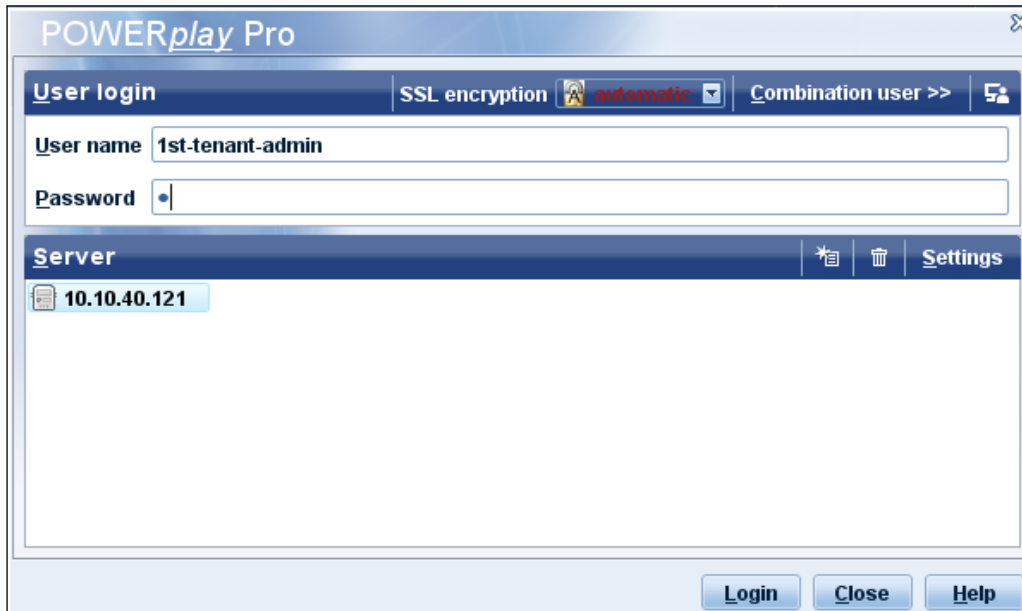
8.4. Verify ASC EVOIPneo active Capture and Playback

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 **POWERplay Pro** window appears as shown below.

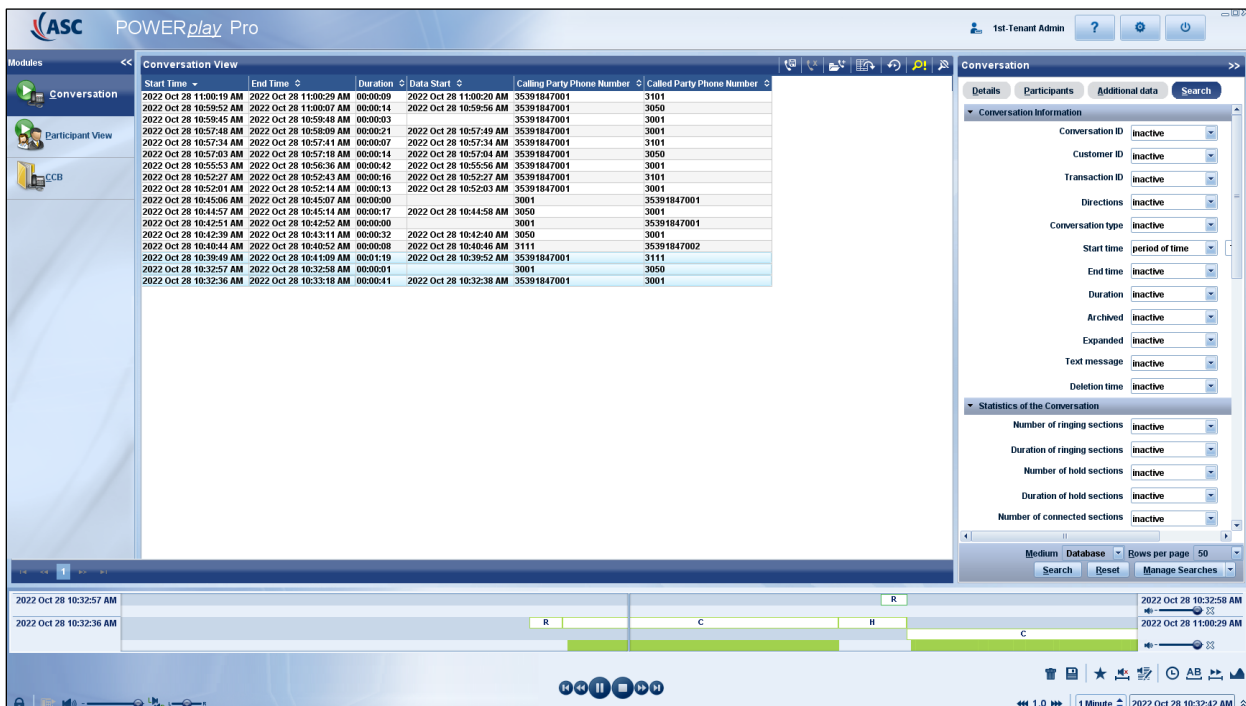


Enter the appropriate **User name** and **Password** and click on **Login**.



The image shows the 'POWERplay Pro' login window. It has a title bar with the application name and a close button. Below the title bar, there's a 'User login' section with fields for 'User name' (containing '1st-tenant-admin') and 'Password' (with a masked input). To the right of the password field, there's a status for 'SSL encryption' set to 'automatic' and a link for 'Combination user >>'. Below the login fields is a 'Server' section showing the IP address '10.10.40.121'. At the bottom right, there are three buttons: 'Login', 'Close', and 'Help'.

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.



The image shows the 'POWERplay Pro' 'Conversation View' window. The title bar includes the 'ASC' logo, the application name, and the user '1st-Tenant Admin'. The left sidebar has icons for 'Conversation', 'Participant View', and 'CCB'. The main area displays a table of conversation records. The table has columns for 'Start Time', 'End Time', 'Duration', 'Data Start', 'Calling Party Phone Number', and 'Called Party Phone Number'. The bottom of the window features a playback control bar with a timeline, play/pause buttons, and a volume icon. The right sidebar contains a 'Conversation' panel with various filters and statistics.

Start Time	End Time	Duration	Data Start	Calling Party Phone Number	Called Party Phone Number
2022 Oct 28 11:00:19 AM	2022 Oct 28 11:00:29 AM	00:00:09	2022 Oct 28 11:00:20 AM	35391847001	3101
2022 Oct 28 10:59:52 AM	2022 Oct 28 11:00:07 AM	00:00:14	2022 Oct 28 10:59:56 AM	35391847001	3050
2022 Oct 28 10:59:45 AM	2022 Oct 28 10:59:48 AM	00:00:03		35391847001	3001
2022 Oct 28 10:57:48 AM	2022 Oct 28 10:58:09 AM	00:00:21	2022 Oct 28 10:57:49 AM	35391847001	3001
2022 Oct 28 10:57:34 AM	2022 Oct 28 10:57:41 AM	00:00:07	2022 Oct 28 10:57:34 AM	35391847001	3101
2022 Oct 28 10:57:03 AM	2022 Oct 28 10:57:18 AM	00:00:14	2022 Oct 28 10:57:04 AM	35391847001	3050
2022 Oct 28 10:55:53 AM	2022 Oct 28 10:56:36 AM	00:00:42	2022 Oct 28 10:55:56 AM	35391847001	3001
2022 Oct 28 10:52:27 AM	2022 Oct 28 10:52:43 AM	00:00:16	2022 Oct 28 10:52:27 AM	35391847001	3101
2022 Oct 28 10:52:01 AM	2022 Oct 28 10:52:14 AM	00:00:13	2022 Oct 28 10:52:03 AM	35391847001	3001
2022 Oct 28 10:45:06 AM	2022 Oct 28 10:45:07 AM	00:00:00		3001	35391847001
2022 Oct 28 10:44:57 AM	2022 Oct 28 10:45:14 AM	00:00:17	2022 Oct 28 10:44:58 AM	3050	3001
2022 Oct 28 10:42:51 AM	2022 Oct 28 10:42:52 AM	00:00:00		3001	35391847001
2022 Oct 28 10:42:39 AM	2022 Oct 28 10:43:11 AM	00:00:32	2022 Oct 28 10:42:40 AM	3050	3001
2022 Oct 28 10:40:44 AM	2022 Oct 28 10:40:52 AM	00:00:08	2022 Oct 28 10:40:46 AM	3111	35391847002
2022 Oct 28 10:39:49 AM	2022 Oct 28 10:41:09 AM	00:01:19	2022 Oct 28 10:39:52 AM	35391847001	3111
2022 Oct 28 10:32:57 AM	2022 Oct 28 10:32:58 AM	00:00:01		3001	3050
2022 Oct 28 10:32:36 AM	2022 Oct 28 10:33:18 AM	00:00:41	2022 Oct 28 10:32:38 AM	35391847001	3001

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

©2022 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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