



Avaya Solution & Interoperability Test Lab

Application Notes for CCT Deutschland GmbH ContactPro® 6.0 using Client JavaScript SDK and Avaya Aura® Device Services 8.0.2, Avaya Aura® Web Gateway 3.8.1 - Issue 1.0

Abstract

These Application Notes contain instructions for CCT ContactPro® 6.0 using Client JavaScript SDK to successfully interoperate with Avaya Aura® Environment 8.1.3.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1**, as well as 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 configuration steps required for CCT ContactPro® from CCT, to interoperate with Avaya Aura® Device Services 8.0.2, Avaya Aura® Web Gateway 3.8.1 and the Avaya platform, as listed in **Section 4**.

The CCT ContactPro® solutions offer a variety of integrations into the Avaya call center environment, supporting different Avaya platforms to interact for multimedia agents as well as for voice only agents. CCT ContactPro® is a solution for agent desktops in an Avaya call center environment focused on voice and multimedia such as email and webchat. CCT ContactPro® can be installed with enabled Presence Services and integrated Customer Data and empowers agents to efficiently serve customers by allowing the agents have full call control from the agent's screen.

CCT ContactPro® 6 includes a software application that serves as a softphone running as a browser application. CCT ContactPro® 6 solution integrated with Avaya Client JavaScript SDK for voice call control and audio to register as WebRTC endpoints with Avaya Aura® Web Gateway and Avaya Aura® Session Manager.

2. General Test Approach and Test Results

Interoperability testing contained functional tests mentioned in **Section 2.1**. All test cases were performed manually. The general test approach was to validate successful handling of inbound skillset/VDN calls using ContactPro Web Client. This was performed by calling inbound to a VDN and/or outbound from the elite call center using ContactPro to answer calls. Where applicable, agent actions were performed using the ContactPro Agent Client.

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 CCT ContactPro® 6 solution utilized enabled securities capabilities with HTTPS/SRTP. And the DMCC interface between Avaya systems and the CCT ContactPro® 6 solution did not include use of any specific encryption features as requested by CCT.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. Feature testing included the validation of the following:

- **Registration** - Successful registration of CCT ContactPro® 6 with Avaya Aura® Device Services (AADS) and Avaya Aura® Web Gateway (AAWG).
- **Agent state change**– Login, Ready/Not Ready using ContactPro Agent.
- **Inbound and Outbound Calls** between CCT ContactPro® 6 Web client and Avaya SIP, H.323, and digital telephones. Calls between Contact Pro client and PSTN endpoints. Calls with G.711, OPUS codec support and negotiation, with and without media shuffling. Calls with SRTP enabled and disabled. DTMF transmission.
- **Hold/Transfer/Conference** – Place callers on hold and transfer and conference using ContactPro Agent.
- **Serviceability** - The serviceability testing focused on verifying the ability of CCT ContactPro® 6 Web client to recover from adverse conditions, such as disconnecting/reconnecting the network to ContactPro Server.

2.2. Test Results

The testing was successful. All test cases passed.

2.3. Support

Support for CCT products can be obtained as follows:

WEBSITE

www.cct-solutions.com

CONTACT

Phone: +49 69 7191 4969 0

Email: contact@cct-solutions.com

SUPPORT

Hotline: +49 821 455152 455

Email: helpdesk@cct-solutions.com

CCT Solutions

Deutschland GmbH

Tilsiter Str. 1

60486, Frankfurt am Main

Germany

Phone +49 69 7191 4969 0

CCT Software LLC

1801 N.E. 123rd Street, Suite 314

North Miami, 33181 FL

United States of America

Phone +1 786 738 5253

3. Reference Configuration

Figure 1 illustrates a sample configuration that consists of Avaya products and the CCT ContactPro® 6.

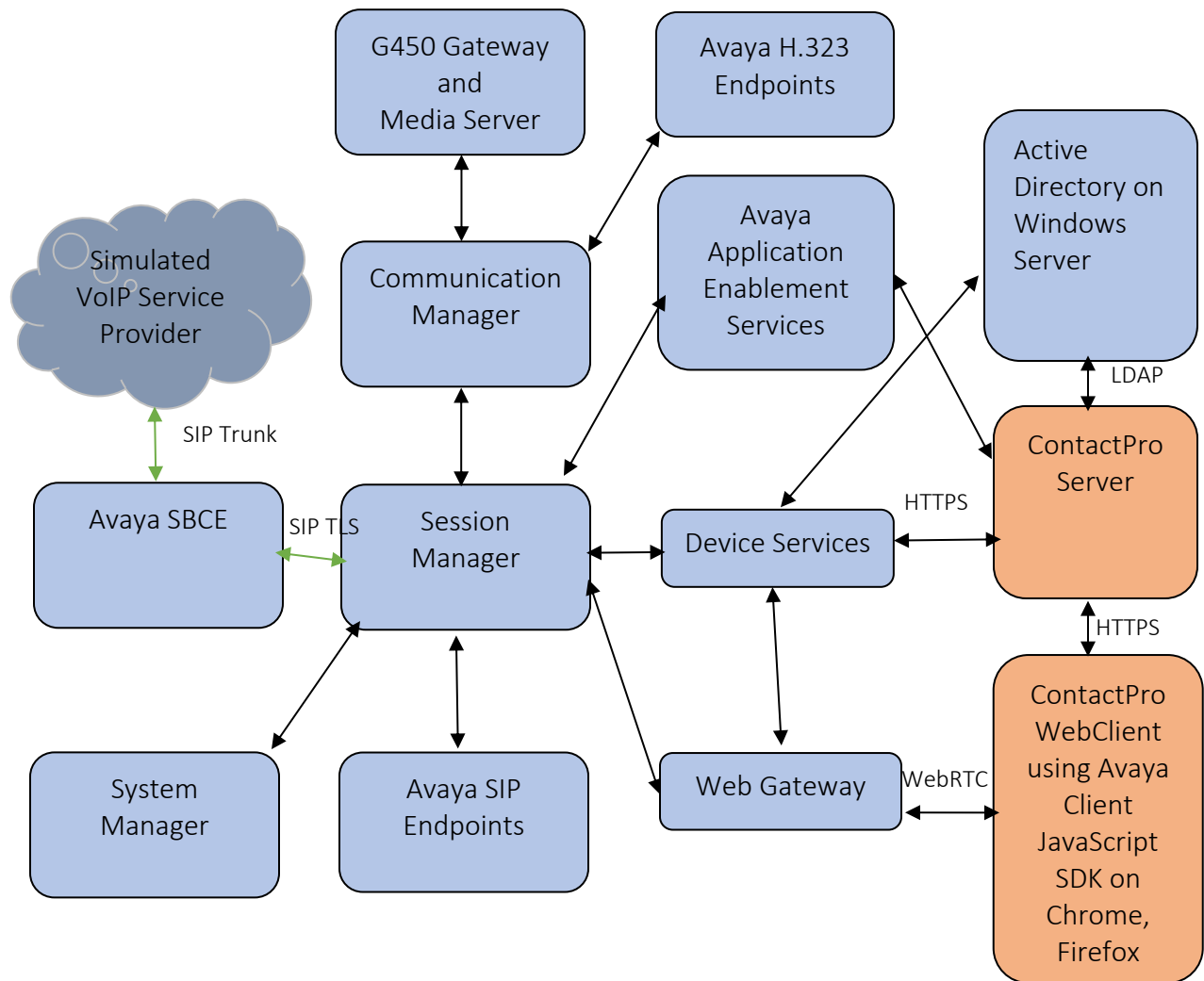


Figure 1: Test Configuration for CCT ContactPro® and the Avaya Platform.

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 in Virtual Environment	8.1.3.0
Avaya Aura® Session Manager in Virtual Environment	8.1.3.0
Avaya Aura® Communication Manager in Virtual Environment	8.1.3.0
Avaya G450 Media Gateway	41.16.30
Avaya Aura® Media Server in Virtual Environment	8.0.2.43
Avaya Session Border Controller for Enterprise in Virtual Environment	8.1.1.0
Avaya Client SDK for JavaScript	4.12
Avaya Aura® Device Services	8.0.2
Avaya Aura® Web Gateway	3.8.1
Avaya 9608G & 9641G IP Deskphone (H.323)	6.8
Avaya IX Workplace	3.16.0
Avaya 9641 & 9621 IP Deskphone (SIP)	7.1.9
Avaya J159	4.0.7
CCT ContactPro® Server	6.0

5. Administer users on Windows Server Active Directory

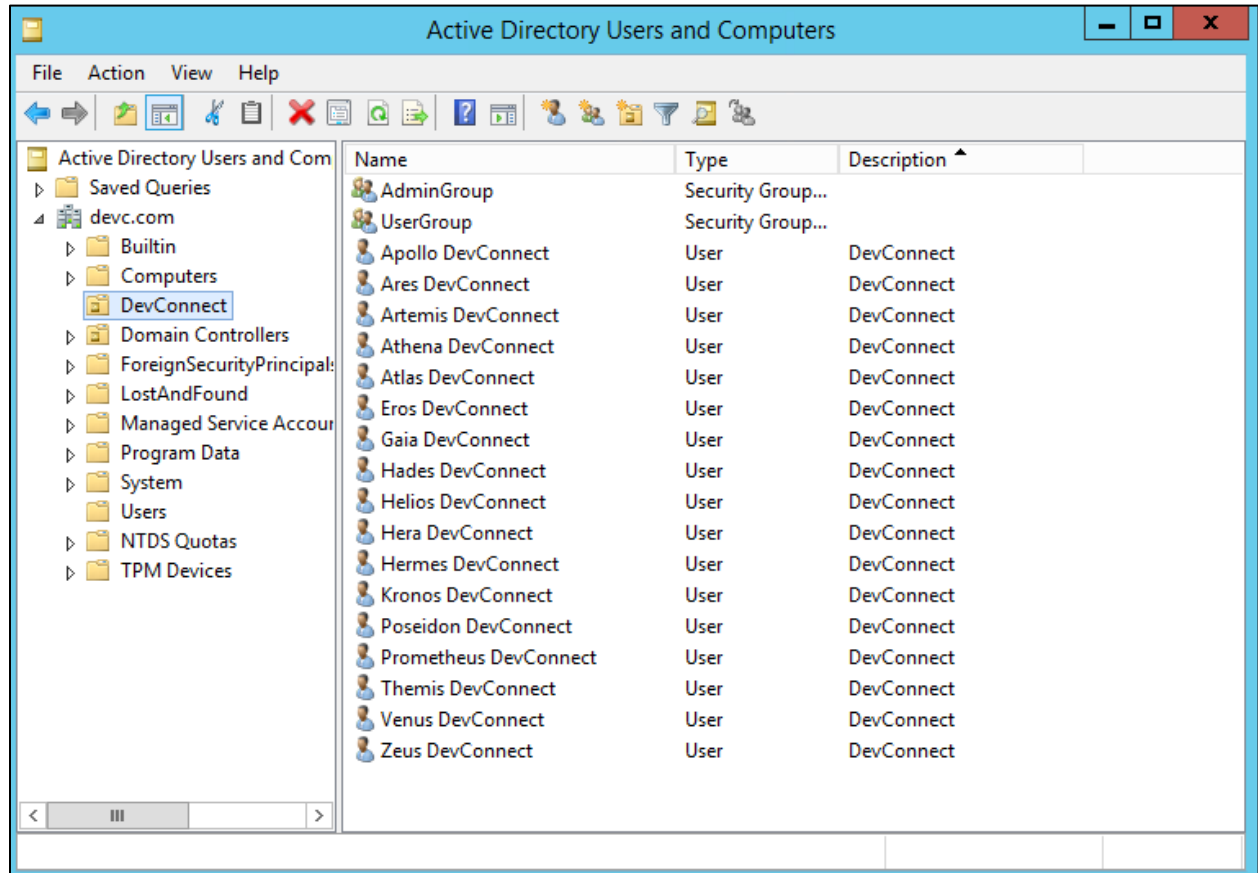
These Application Notes assume Active Directory and a domain are already in place. The screenshot below displays an Active Directory user administered with required fields **Telephone number**, **E-mail** and **Description**. All users should use same **Description**.

The screenshot shows the 'Zeus DevConnect Properties' dialog box with the 'General' tab selected. The dialog box contains the following fields and values:

Field	Value
First name	Zeus
Initials	
Last name	DevConnect
Display name	DevConnect, Zeus
Description	DevConnect
Office	
Telephone number	72017
E-mail	Zeus@devc.com
Web page	

The 'Other...' buttons are visible next to the 'Telephone number' and 'Web page' fields. The 'OK', 'Cancel', 'Apply', and 'Help' buttons are at the bottom of the dialog box.

Below is a list of **Active Directory** users that were created for this compliance testing:



6. Configure Avaya Aura® System Manager

This section provides the procedures for configuring Avaya Aura® Environment. It is implied that a working Avaya Aura® Environment, which includes System Manager, Session Manager, Communication Manager, Media Server, Device Services and a Web Gateway, is already in place with the necessary licensing. For all other provisioning information, such as initial installation and configuration, please refer to the product documentation in **Section 13**.

The procedures include the following areas:

- Create User Provisioning Rules on System Manager
- LDAP Sync Configuration

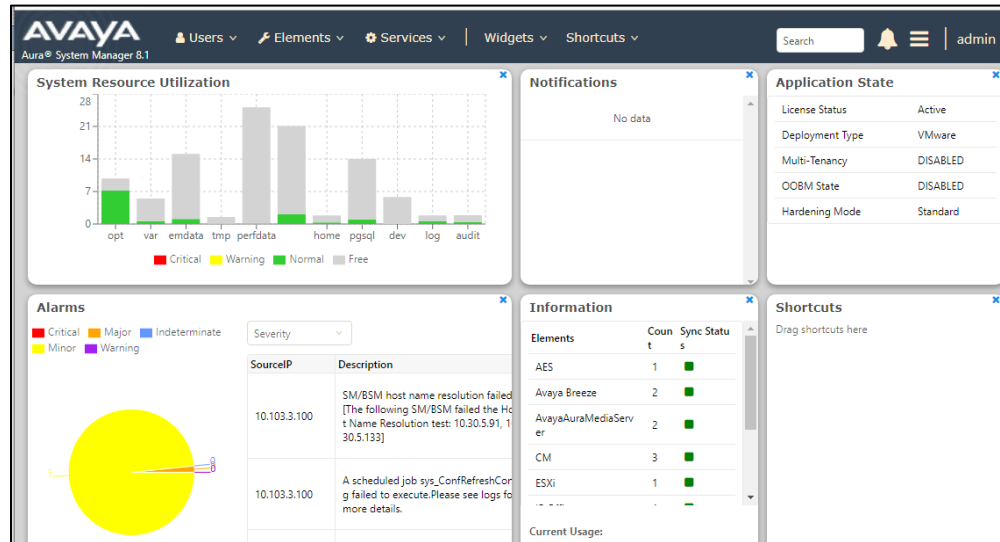
6.1. Create User Provisioning Rules on System Manager

A user provisioning rule includes a master communication profile template and a set of provisioning rules. A user provisioning rule enables predefined templates that consist of user attributes found in the communication profile of the user. In the user provisioning rule, the administrator specifies the following information to provision the user:

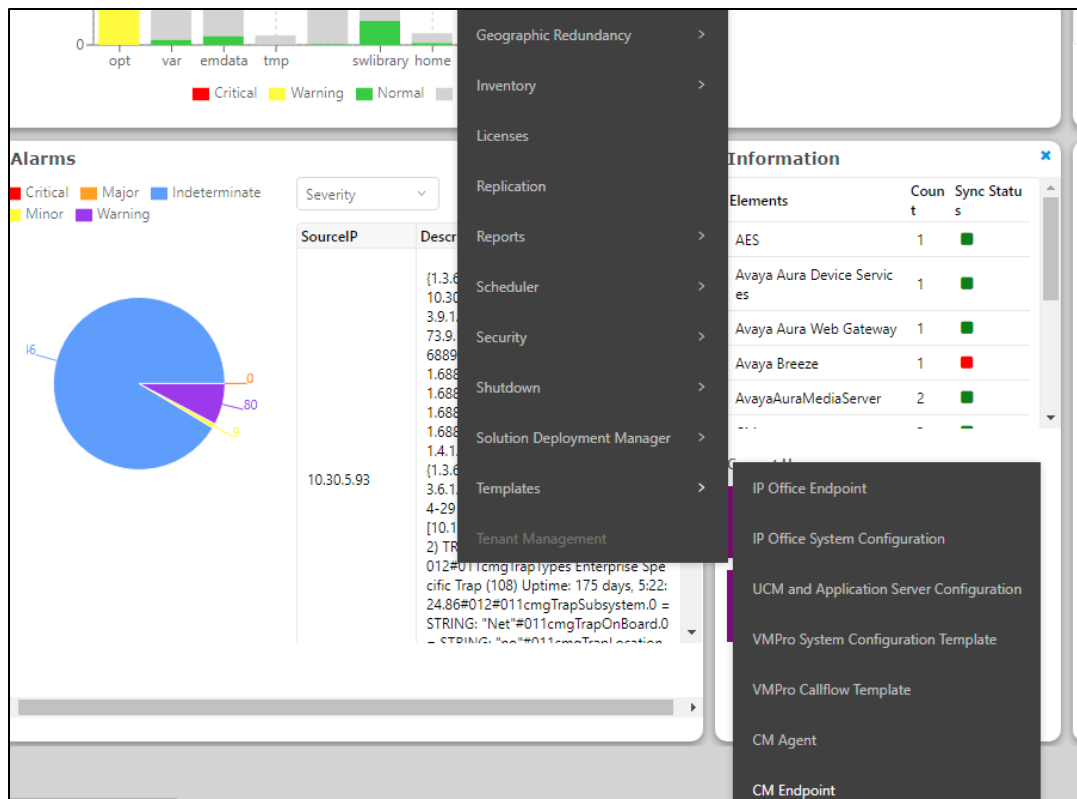
- Basic information that includes the communication profile password, time zone, and language preference.
- The communication system that the user must use, for example, Communication Manager.
- The method to assign or create a communication profile for the user, for example, by assigning the next available extension for Communication Manager.

Configuration of User Provisioning Rules and is performed via Avaya Aura® System Manager. Access the System Manager Administration web interface by entering the System Manager (SMGR) URL in a web browser. Log in using appropriate credentials.

Once logged in, the following screen is displayed.



Select **Services** → **Templates** → **CM Endpoint**.



On **Endpoint Templates** page, select **CM 8.1** and press **New** to create new **Custom templates**.

The screenshot displays the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.1', and tabs for 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The left sidebar shows a list of templates, with 'CM Endpoint' highlighted. The main content area is titled 'Endpoint Templates' and features a search bar. Below the search bar, there is a section for 'Supported Feature Server Versions' with a table of 10 items. The table has columns for 'System Type' and 'Software Version'. The row for 'CM 8.1' is selected. Below the table, there is a 'Select : All, None' option. At the bottom, there is a section for 'Custom templates (C)' and 'Default templates (D)'. The 'Custom Templates List' section shows a 'New' button highlighted with a red box, along with other buttons like 'View', 'Edit', 'Duplicate', 'Delete', and 'Upgrade'. The table below the buttons is empty, showing '0 Items' and a 'Show All' dropdown. The table headers are 'Name', 'Set Type', 'Owner', and 'Version'. A message at the bottom states: 'No Endpoint templates found. Select Feature Server Version(s) and click on show'.

	System Type	Software Version
<input type="checkbox"/>	CM	5.0
<input type="checkbox"/>	CM	5.1
<input type="checkbox"/>	CM	5.2
<input type="checkbox"/>	CM	6.0
<input type="checkbox"/>	CM	6.2
<input type="checkbox"/>	CM	6.3
<input type="checkbox"/>	CM	7.0
<input type="checkbox"/>	CM	7.1
<input type="checkbox"/>	CM	8.0
<input checked="" type="checkbox"/>	CM	8.1


Name	Set Type	Owner	Version
No Endpoint templates found. Select Feature Server Version(s) and click on show			

On **New Endpoint Template** page, choose **J179CC** as the **Set Type**. Select **Template Name**, **Class of Restriction (COR)**, **Class of Service (COS)** and **SIP Trunk** as below. Change **Type of 3PCC Enabled** to **Avaya**.

New Endpoint Template

* Set Type

J179CC ▼



* Template Name

ContactProCC

System Type

CM

Version

8.1

General Options (G) *

Feature Options (F)

Site Data (S)

Abbreviated Call Dialing (A)

Enhanced Call Fwd (E)

Button Assignment (B)

Profile Settings (P)

* Class of Restriction (COR)

1

* SIP Trunk

aar

Emergency Location Ext

* Tenant Number

1

Coverage Path 2

Enable Reachability for Station Domain Control

system ▼

* Class Of Service (COS)

1

Type of 3PCC Enabled

Avaya ▼

Message Lamp Ext.

Coverage Path 1

Lock Message

☐

* Required

Select **Feature Option (F)** tab and enable **IP Softphone**.

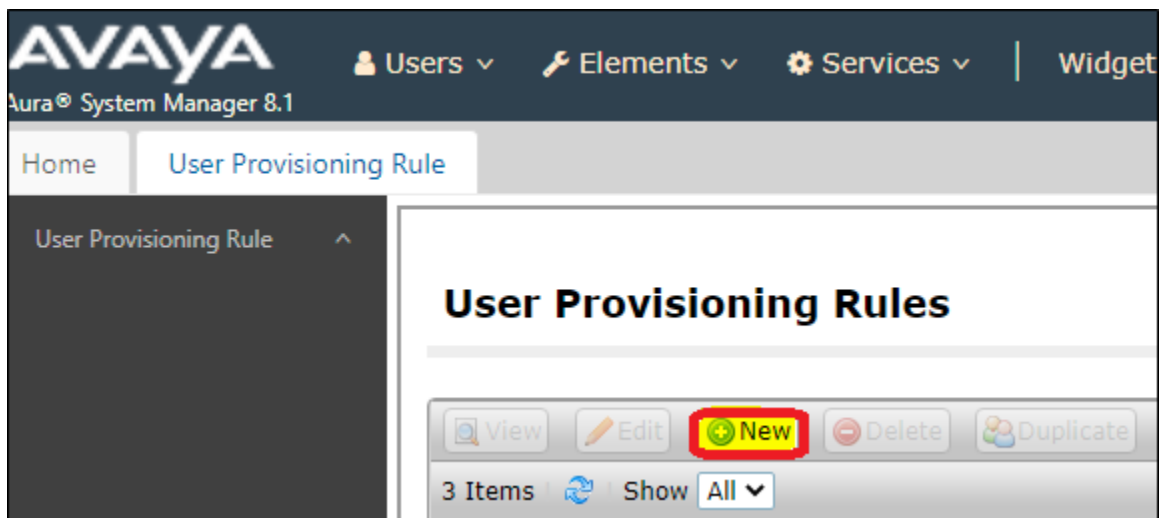
General Options (G) *	Feature Options (F)	Site Data (S)	Abbreviated Call Dialing (A)	Enhanced Call Fwd (E)
<div> <div>Button Assignment (B)</div> <div>Profile Settings (P)</div> </div>				
Active Station Ringing single ▾		Auto Answer none ▾		
MWI Served User Type None ▾		Coverage After Forwarding system ▾		
Per Station CPN - Send Calling Number None ▾		Display Language english ▾		
IP Phone Group ID <input type="text"/>		Hunt-to Station <input type="text"/>		
Remote Soft Phone Emergency Calls as-on-local ▾		Loss Group 1 <input type="text"/>		
LWC Reception spe ▾		Survivable COR internal ▾		
AUDIX Name <input type="text"/>		Time of Day Lock Table None ▾		
EC500 State enabled ▾		Location <input type="text"/>		
Voice Mail Number <input type="text"/>		Bridging Tone for This Extension no ▾		
Music Source <input type="text"/>				
Features <div> <div> <input type="checkbox"/> Always Use <input type="checkbox"/> IP Audio Hairpinning <input type="checkbox"/> Bridged Call Alerting <input type="checkbox"/> Bridged Idle Line Preference <input checked="" type="checkbox"/> Coverage Message Retrieval <input checked="" type="checkbox"/> Direct IP-IP Audio Connections <input checked="" type="checkbox"/> Survivable Trunk Dest <input type="checkbox"/> Bridged Appearance Origination Restriction <input checked="" type="checkbox"/> Restrict Last Appearance <input type="checkbox"/> Turn on mute for remote off-hook attempt <input type="checkbox"/> IP Hoteling </div> <div> <input type="checkbox"/> Idle Appearance Preference <input checked="" type="checkbox"/> IP SoftPhone <input checked="" type="checkbox"/> LWC Activation <input type="checkbox"/> CDR Privacy <input type="checkbox"/> Precedence Call Waiting <input type="checkbox"/> H.320 Conversion <input type="checkbox"/> IP Video Softphone <input type="checkbox"/> Per Button Ring Control </div> </div>				

Select the **Button Assignment** tab, and select **Button Feature** as below:

Endpoint Configurations		Button Configurations			
Favorite	Button Label	Button Feature	Argument-1	Argument-2	Argument-3
1 <input type="checkbox"/>		call-appr			
2 <input type="checkbox"/>		call-appr			
3 <input type="checkbox"/>		call-appr			
4 <input type="checkbox"/>		agnt-login			
5 <input type="checkbox"/>		None			
6 <input type="checkbox"/>		None			
7 <input type="checkbox"/>		None			
8 <input type="checkbox"/>		None			

Click **Commit** to save this Endpoint Template.

Back to SMGR Dashboard, select **Users** → **User Provisioning Rule**, click **New** to create new User Provisioning Rule.



Enter following information:

User Provision Rule Name	Same as Active Directory Description in Section 5 . In this case " DevConnect "
SIP Domain	Select a SIP Domain from Drop down list, devconnect.com
Presence/IM Domain	Select a Presence/IM Domain from Drop down list, devconnect.com
Communication Profile Password	Enter a Password
Confirm Password	Enter Password again
User Phone Number last ... digits for Extension	Enter digits length for Communication Extension, In this case " 5 "
Prefix for Avaya E164 Handle	+848333
Language Preference	Select Language Preference in drop down list
Time Zone	Select Time Zone in drop down list

New User Provisioning Rule

Basic *

Communication Profile

* User Provisioning Rule Name:

DevConnect

Description:

SIP Domain:

devconnect.com

Presence/IM Domain:

devconnect.com

Auto Generate Communication Profile Password:

☐

Communication Profile Password:

Confirm Password:

Generate

Use Phone Number last

5

digits for Extension

Prefix for Avaya E164 Handle:

+848333

Language Preference:

English (United States)

Time Zone:

(+7:0)Bangkok, Hanoi, Jakarta,

Select the **Communication Profile** tab.

New User Provisioning Rule

Basic *

Communication Profile

☐ Session Manager Profile ▶

☐ Avaya Breeze® Profile ▶

☐ CM Endpoint Profile ▶

☐ Presence Profile ▶

☐ IP Office Endpoint Profile ▶

*Required

Enable **Session Manager Profile** and enter the **Primary Session Manager**, **Origination Application Sequence**, **Termination Application Sequence** and **Home Location** relevant to the implementation.

☒ **Session Manager Profile** ▼

SIP Registration

* Primary Session Manager:

DevConnect-SMSIP ▼

Secondary Session Manager:

(None) ▼

Survivability Server:

Start typing... ▼

Max. Simultaneous Devices:

1 ▼

Block New Registration When
Maximum Registrations
Active?:

☐

Application Sequences

Origination Application
Sequence:

CM93-AppSeq ▼

Termination Application
Sequence:

CM93-AppSeq ▼

Emergency Calling Application Sequences

Emergency Calling Application
Sequences:

(None) ▼

Emergency Calling Application
Sequences:

(None) ▼

Call Routing Settings

* Home Location:

SaiGon ▼

Conference Factory Set:

(None) ▼

Call History Settings

Enable Centralized Call
History?:

Select ▼

Scroll down the page and enable the **CM Endpoint Profile** section. Select the Communication Manager system from the **System** drop down box, select **Endpoint** as the **Profile Type**, enter the **Extension Range** number you wish to use, select **ContactProCC** as the **Template** and select **Security Code** as **Extension/Reverse Extension**.

☒ **CM Endpoint Profile**

* System: CM93

Profile Type: Endpoint

Use Next Available Extension: ☒

Extension Range: 70000:70999

Template: ContactProCC

Security Code: Reverse Extension

Preferred Handle: Avaya SIP

Delete Endpoint on Unassign of Endpoint from User or on Delete User: ☒

Override Endpoint Name: ☒

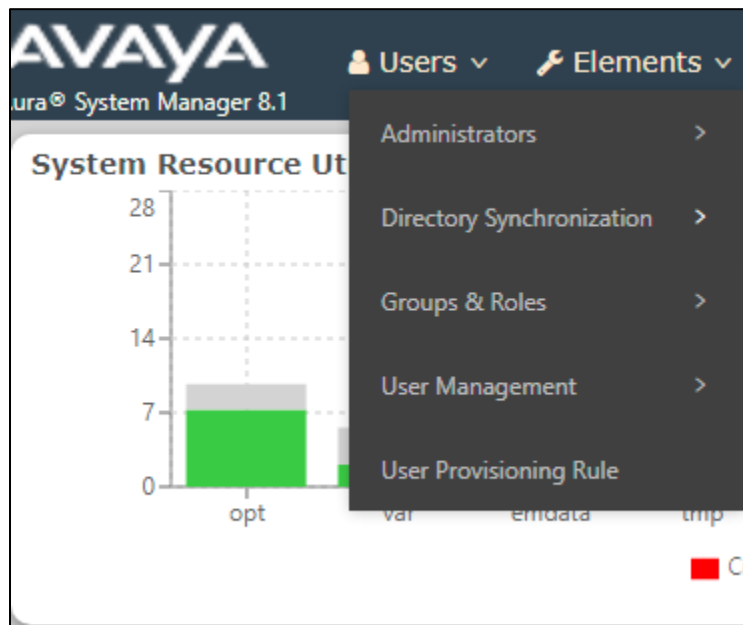
Allow H.323 and SIP Endpoint Dual Registration: ☐

Click **Commit** to save **User Provisioning Rule**. The new User Provisioning Rule is shown in list below.

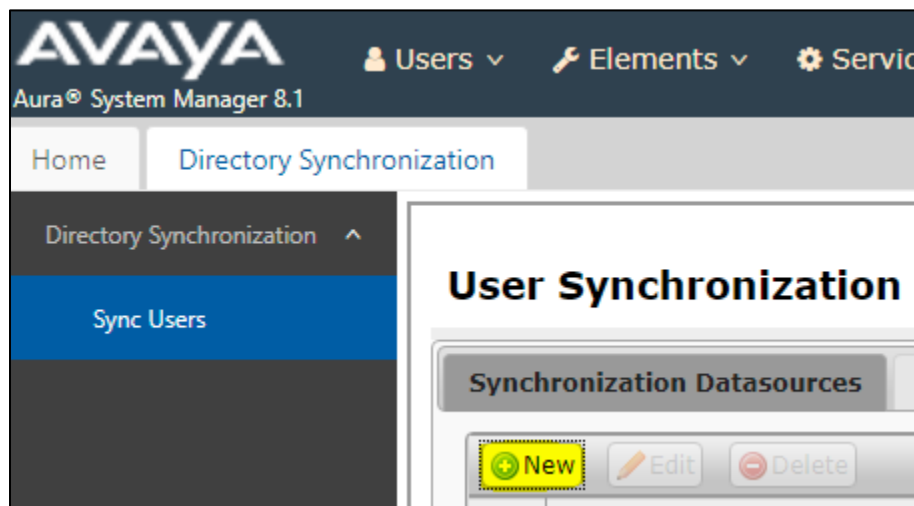
User Provisioning Rules		
<div> <div>View Edit New Delete Duplicate</div> <div>3 Items Show All</div> </div>		
<input type="checkbox"/>	Name	SIP Domain
<input type="checkbox"/>	DevConnect	devconnect.com
<input type="checkbox"/>	DevConnect-CM96	devconnect.com
<input type="checkbox"/>	DevConnect-CM93	devconnect.com
Select : All, None		

6.2. LDAP Sync Configuration

On the SMGR page, click on **Directory Synchronization** under the **Users** menu.



On the **User Synchronization** page, click **New** to create a data source for **System Manager** to synchronize with Active Directory.



On the **New User Synchronization Datasource** page, enter the required **Directory Parameters**.

Datasource Name	Create a name to identify the LDAP Directory Server. This name will be required to create a sync job, i.e AD143
Host	IP Address or host name of the directory server you want to sync users with, i.e 10.30.5.143
Principal	LDAP Directory Server username that has write permissions to create/update users, i.e gnguyenanh@devc.com
Password	Password of the Principal (username above) to access LDAP Directory Server.
Port	LDAP Directory Server port number to enable System Manager connectivity. Default values are 389 for nonSSL connection and 636 for SSL connection.
Base Distinguished Name	Base DN is an element that works in conjunction with the search scope. It's the tree from which users are synced. The sub trees are not considered for syncing the users, i.e ou=DevConnect,dc=devc,dc=com
LDAP User Schema	Schema defines the object classes. The object class definitions define the list of attributes that must contain values and the list of attributes that may contain values. Definitions differ depending on your LDAP Directory Server. Default value is inetOrgPerson .
Search Filter	Search filter provides a mechanism for defining the criteria for matching entries in a LDAP search operation.
Use SSL	Checkbox to use SSL.
Allow Deletions	Checkbox to have System Manager delete previously sync users that have been deleted in the LDAP Directory Server.
Allow Null values in LDAP	The option to allow null values to be inserted by System Manager in LDAP.

Edit User Synchronization Datasource

Directory Parameters

* Datasource Name

* Host

* Principal

* Password

* Port

* Base Distinguished Name

* LDAP User Schema

* Search Filter

Use SSL ☒

Allow Deletions ☒

Allow Null values in LDAP ☐

Click **Test Connection**. If the parameters that you enter are correct, the **New User Synchronization Datasource** page will expand to enable the administration of **Attribute Parameters**.

Allow Null values in LDAP ☐

Attribute Parameters

<input type="text"/>	->	<input type="text" value="sourceUserKey"/>
<input type="text"/>	->	<input type="text" value="loginName"/>
<input type="text"/>	->	<input type="text" value="surname"/>
<input type="text"/>	->	<input type="text" value="givenName"/>
<input type="text"/>	->	<input type="text" value="displayName"/>

Configure the five mandatory attribute mappings. These attributes are grayed out and can only be synced from the LDAP Directory Server to System Manager.

objectGUID	->	sourceUserKey
userPrincipalName	->	loginName
sn	->	surname
givenName	->	givenName
displayName	->	displayName

Click **Add Mapping** to configure optional attribute mappings:

telephoneNumber	->	Phone Number	Remove
description	+	User Provisioning Rule	Remove
mail	->	Microsoft Exchange Handle	Remove

Save Cancel

Click **Save** to save **User Synchronization Datasource**.

User Synchronization

Synchronization Datasources Active Synchronization Jobs Synchronization Job History

+ New Edit Delete

	Name	Host	Search Filter
<input type="radio"/>	AD143	10.30.5.143	userPrincipalName=*

Select : None

From **User Synchronization** page, select the **Active Synchronization Jobs** tab and then click on the **Create New Job** button.

User Synchronization

Synchronization Datasources **Active Synchronization Jobs** Synchronization Job History

+ Create New Job

Name	Next Execution Time	Recurring Interval	Action
DirectorySyncCleanupJob	January 31, 2021 1:18:31 PM +07:00	Recursive	Delete Job

To immediately start the synchronization, choose the **Datasource Name** and click **Run Job**.

New User Synchronization Job

Datasource Name

AD143 ▼

Schedule job for future execution
☐

Run Job

Cancel

On the **User Synchronization** page, and then click on the **Synchronization Job History** tab. Click on **View Job Summary** to view the details of the synchronization job.

User Synchronization					
Synchronization Datasources Active Synchronization Jobs Synchronization Job History					
36 Items					
Name	Start Time	End Time	Status	Job Result	Action
AD143	December 15, 2020 5:28:43 PM +07:00	December 15, 2020 5:28:43 PM +07:00	COMPLETED	View Job Summary	Delete Job
AD143	November 9, 2020 12:04:40 PM +07:00	November 9, 2020 12:04:52 PM +07:00	COMPLETED	View Job Summary	Delete Job
AD143	November 6, 2020 7:46:04 PM +07:00	November 6, 2020 7:46:10 PM +07:00	COMPLETED	View Job Summary	Delete Job
AD143	November 3, 2020 4:34:41 PM +07:00	November 3, 2020 4:35:57 PM +07:00	COMPLETED	View Job Summary	Delete Job
AD79	November 3, 2020 4:07:28 PM +07:00	November 3, 2020 4:07:40 PM +07:00	COMPLETED	View Job Summary	Delete Job
AD79	November 3, 2020 4:04:47 PM +07:00	November 3, 2020 4:05:19 PM +07:00	COMPLETED	View Job Summary	Delete Job
AD79	June 29, 2020 2:58:16 PM +07:00	June 29, 2020 2:58:30 PM +07:00	COMPLETED	View Job Summary	Delete Job
AD79	June 11, 2020 1:36:58 AM +07:00	June 11, 2020 1:37:44 AM +07:00	COMPLETED	View Job Summary	Delete Job
AD79	April 29, 2020 11:47:57 AM +07:00	April 29, 2020 11:48:29 AM +07:00	COMPLETED	View Job Summary	Delete Job
AD79	April 29, 2020 11:46:02 AM +07:00	April 29, 2020 11:46:33 AM +07:00	COMPLETED	View Job Summary	Delete Job
AD79	April 29, 2020 11:45:16 AM +07:00	April 29, 2020 11:45:16 AM +07:00	COMPLETED	View Job Summary	Delete Job
AD55	April 29, 2020 5:00:00 AM +07:00	April 29, 2020 5:00:00 AM +07:00	COMPLETED	View Job Summary	Delete Job
AD79	April 28, 2020 10:04:24 AM +07:00	April 28, 2020 10:04:24 AM +07:00	COMPLETED	View Job Summary	Delete Job
AD55	April 28, 2020 10:04:15 AM +07:00	April 28, 2020 10:04:15 AM +07:00	COMPLETED	View Job Summary	Delete Job
AD55	April 28, 2020 5:00:01 AM +07:00	April 28, 2020 5:00:07 AM +07:00	COMPLETED	View Job Summary	Delete Job

The **Job Results** are shown below:

Job Results		
Added	17	▼
Modified	0	
Deleted	0	
Unchanged	0	
Failed	0	
Total records processed	17	

7. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager. The procedures include the following areas:

- Verify license
- Administer CTI link
- Administer hunt group and agent

7.1. Verify License

Log into the System Access Terminal to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the “display system-parameters customer-options” command to verify that the **Computer Telephony Adjunct Links** customer option is set to “y” on **Page 4**. If this option is not set to “y”, then contact the Avaya sales team or business partner for a proper license file.

display system-parameters customer-options

Page 4 of 12

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?	y	DCS Call Coverage?	y
ASAI Link Plus Capabilities?	y	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		

(NOTE: You must logoff & login to effect the permission changes.)

7.2. Administer CTI Link

Add a CTI link using the **add cti-link n** command, where **n** is an available CTI link number. Enter an available extension number in the **Extension** field. Note that the CTI link number and extension number may vary. 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: 79999			
Type: ADJ-IP			
Name: aes95			
			COR: 1

7.3. Administer Hunt Group and Agent

This section shows the steps required to add a new service or skill on Communication Manager. Services are accessed by calling a Vector Directory Number (VDN), which points to a vector. The vector then points to a hunt group associated with an agent. Agent can use ContactPro as agent desktops for handling incoming and outgoing calls with WebRTC voice through Avaya Aura® Web Gateway (AAWG).

The following sections give step by step instructions on how to add the following.

- Hunt Group
- Agent

7.3.1. Add Hunt Group

To add a new skillset or hunt group type, **add hunt-group x**, where **x** is the new hunt group number. For example, hunt group **1** is added for the **Voice Service** queue. Ensure that **ACD**, **Queue** and **Vector** are all set to **y**. Also, that **Group Type** is set to **ucd-mia**.

add hunt-group 1		Page 1 of 4
HUNT GROUP		
Group Number: 1	ACD? y	
Group Name: Voice Service	Queue? y	
Group Extension: 87000	Vector? y	
Group Type: ucd-mia		
TN: 1		
COR: 1	MM Early Answer? n	
Security Code:	Local Agent Preference? n	
ISDN/SIP Caller Display:		
Queue Limit: unlimited		
Calls Warning Threshold:	Port:	
Time Warning Threshold:	Port:	

On **Page 2** ensure that **Skill** is set to **y** as shown below.

add hunt-group 1		Page 2 of 4
HUNT GROUP		
Skill? y	Expected Call Handling Time (sec): 180	
AAS? n		
Measured: none		
Supervisor Extension:		
Controlling Adjunct:		
Multiple Call Handling: none		
Timed ACW Interval (sec):	After Xfer or Held Call Drops? n	

7.3.2. Add Agent

In the compliance testing, the agents 80001 and 80002 were created.

To add a new agent, type **add agent-loginID x**, where x is the login id for the new agent.

```
add agent-loginID 80001                                     Page 1 of 3
AGENT LOGINID
Login ID: 80001                                             AAS? n
Name: Voice Agent                                           AUDIX? n
TN: 1                                                       Check skill TNs to match agent TN? n
COR: 1
Coverage Path:                                             LWC Reception: spe
Security Code:                                             LWC Log External Calls? n
AUDIX Name for Messaging:
LoginID for ISDN/SIP Display? n
Password:
Password (enter again):
Auto Answer: station
MIA Across Skills: system
ACW Agent Considered Idle: system
Aux Work Reason Code Type: system
Logout Reason Code Type: system
Maximum time agent in ACW before logout (sec): system
Forced Agent Logout Time: :
WARNING: Agent must log in again before changes take effect
```

On **Page 2**, add the required skills. Note that the skill **1** is added to this agent so when a call for **Voice Service** is initiated, the call is routed correctly to this agent.

```
add agent-loginID 80001                                     Page 2 of 3
AGENT LOGINID
Direct Agent Skill:                                         Service Objective? n
Call Handling Preference: skill-level                       Local Call Preference? n

SN  RL SL      SN  RL SL      SN  RL SL      SN  RL SL
1: 1      1      16:      31:      46:
2:      17:      32:      47:
3:      18:      33:      48:
4:      19:      34:      49:
5:      20:      35:      50:
6:      21:      36:      51:
7:      22:      37:      52:
8:      23:      38:      53:
9:      24:      39:      54:
10:     25:      40:      55:
```

Repeat this section to add another agent 80002.

7.4. Administer Vectors and VDNs

Add a vector using the **change vector n** command, where **n** is a vector number. Note that the vector steps may vary, and below is a sample vector used in the compliance testing.

```
change vector 1                                     Page 1 of 6

                                CALL VECTOR

    Number: 1                                Name: VoiceService
Multimedia? n      Attendant Vectoring? n      Meet-me Conf? n      Lock? n
    Basic? y      EAS? y      G3V4 Enhanced? y      ANI/II-Digits? y      ASAI Routing? y
    Prompting? y      LAI? y      G3V4 Adv Route? y      CINFO? y      BSR? y      Holidays? y
    Variables? y      3.0 Enhanced? y
01 wait-time      2      secs hearing silence
02 queue-to      skill 1      pri t
03 wait-time      2      secs hearing silence
04 stop
05
06
07
08
09
10
11
12

                                Press 'Esc f 6' for Vector Editing
```

Add a VDN using the **add vdn n** command, where **n** is an available extension number. Enter a descriptive Name and the vector number from above for **Destination**. Retain the default values for all remaining fields.

```
change vdn 88000                                     Page 1 of 3

                                VECTOR DIRECTORY NUMBER

                                Extension: 88000                                Unicode Name? n
                                Name*: Voice VDN
                                Destination: Vector Number      1
                                Attendant Vectoring? n
                                Meet-me Conferencing? n
                                Allow VDN Override? n
                                COR: 1
                                TN*: 1
                                Measured: none      Report Adjunct Calls as ACD*? n

                                VDN of Origin Annc. Extension*:
                                1st Skill*:
                                2nd Skill*:
                                3rd Skill*:

SIP URI:

* Follows VDN Override Rules
```

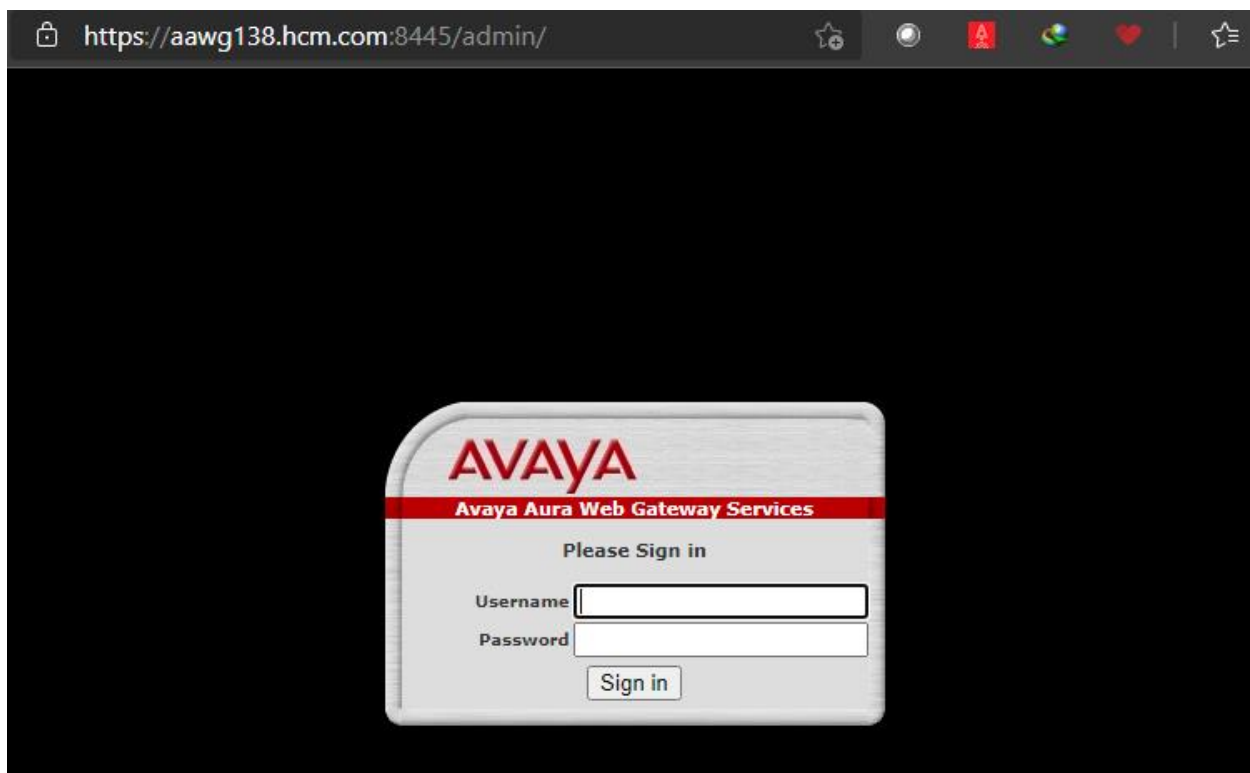
8. Configure Avaya Aura® Web Gateway

The Avaya Aura® Web Gateway (AAWG) server acts as a gateway to CCT ContactPro® web using JSDK clients utilizing WebRTC signaling and media. This section provides the procedures for configuring Avaya Aura® Web Gateway. It assumes that AAWG is already installed and basic configuration steps have been performed. The procedures include the following areas:

- Launch AAWG web admin.
- Verify General Network Settings.
- Verify LDAP Configuration.
- Assign locations to AAWG.
- Configured Media Settings for Audio.

8.1. Launch AAWG web admin

Access the AAWG web admin interface by using the URL “https://**ip-address**:8445/admin” in an Internet browser window, where **ip-address** is the IP address of the AAWG server. Log in using the appropriate credentials.



8.2. Verify General Network Settings

In System Overview, verify AAWG connect successfully to LDAP Configuration, Device Services, System Manager, and Media Services with status **Connected**.

Avaya Aura Web Gateway Services

System Overview

General Network Settings

- System Manager
- Device Services
- Location
- LDAP Configuration
- Media Services

Equinox Conferencing

External Access

Logs Management

Licensing

Security Settings

Advanced

System Overview

Deployment Type

Team Engagement

Solution Servers

Required Server	Status
LDAP Configuration	Connected
Device Services	Connected
System Manager	Connected
Media Services	Connected

Service Control

10.30.5.138 Restart

Node Status

IP Address	FQDN	Service Status
10.30.5.138	aawg138.hcm.com	STARTED

8.3. Verify LDAP Configuration

In the left panel, go to **General Network Settings → LDAP Configuration**, verify that Base Context DN is the point where users created in the Active Directory, (in this case: **ou=DevConnect, dc=devc, dc=com**). Verify **UID Attribute ID** is configured as **sAMAccountName**.

The screenshot shows the 'ActiveDirectory_2012' configuration window. The 'Enterprise-Directory Type' is set to 'ActiveDirectory_2012'. The 'Provenance Priority' is 1. The 'Authentication Domain' is 'devc.com'. The 'Server Address and Credentials' section is expanded, showing the following settings:

- Secure LDAP: ☐
- *Address: 10.30.5.143
- *Bind DN: Administrator@devc.com
- Base Context DN: ou=DevConnect,dc=devc,dc=com
- *Role Filter: (&(objectClass=group)(meml
- Roles Context DN: ou=DevConnect,dc=devc,dc=com
- Role Attribute is DN: false
- Search Scope: Subtree
- Administrator Role: AdminGroup
- Auditor Role:
- Services Maintenance and Support Role:
- Language used in Directory: English (en)
- Active Users Search Filter: (!!(userAccountControl:1.2.84
- Windows Authentication: None
- *Port: 389
- *Bind Credential:
- *UID Attribute ID: sAMAccountName
- *Role Attribute ID: cn
- Role Name Attribute:
- Allow Empty Passwords: false
- Role Recursion: false
- User Role: UserGroup
- Services Administrator Role:
- Security Administrator Role:
- Last Updated Time Attribute ID: whenChanged

Buttons at the bottom: Test Connection, Save, Cancel, Modify Attribute Mappings.

8.4. Assign locations to Avaya Aura® Web Gateway

Select **General Network Settings → Location**, choose AAWG Location in drop down list, in this case **SaiGon**, then click **Save**.

The screenshot shows the 'Web Gateway Locations' configuration window. It contains the following text:

Assign a location to each Avaya Aura® Web Gateway.
A Web Gateway location represents a grouping of one or more Web Gateways.

Below the text is a table with two columns: 'Address' and 'Location'.

Address	Location
aawg138.hcm.com	SaiGon

A dropdown menu is open for the 'Location' column, showing the following options:

- SaiGon
- NhaTrang
- HaNoi

Buttons at the bottom: Save, Cancel.

Scroll down the page, assign all locations to AAWG by press **Add All** and press **Save**.

Location Assignments and Priorities

Assign and prioritize locations for each web gateway location.
All web gateways in a location use the servers in the assigned server locations.

Web Gateway Location: SaiGon

Input Location

No data available in table

Add

Add All

Remove

Up

Down

Assigned Locations

SaiGon

NhaTrang

HaNoi

Save

Cancel

NAQ; Reviewed
SPOC 8/13/2021

Solution & Interoperability Test Lab Application Notes
©2021 Avaya Inc. All Rights Reserved.

30 of 52
CP6Aura8

8.5. Configure Media Settings for Audio

Select **Advanced** → **Media Settings** → **Audio**, Select **SIP Audio Codecs** and **WebRTC Audio Codecs** as show below:

The screenshot shows the 'Audio' configuration window. At the top, it says 'Select codec preferences for SIP and WebRTC clients.' Below this, there are two sections: 'SIP Audio Codecs' and 'WebRTC Audio Codecs'. In the 'SIP Audio Codecs' section, a dropdown menu is set to 'Custom'. Below it is a list of codecs: Opus Wideband, G722, G722.1_32K, G722.1_24K, G711MU, G711A, G726, and G729a. There are 'Add' and 'Remove' buttons next to the dropdown. In the 'WebRTC Audio Codecs' section, there is a list of codecs: Opus, G711A, and G711MU. It also has 'Add' and 'Remove' buttons. At the bottom, there is a 'WebRTC Audio Codec' dropdown and an 'OPUS Profile' dropdown set to 'Wide Band'. 'Save' and 'Cancel' buttons are at the bottom right.

Select **Security Settings** → **Session Security**, configure **Session Security** as below to enable SRTP for SIP Sessions.

The screenshot shows the 'Session Security' configuration window. It starts with the instruction 'Select the required SIP and SRTP security policy for sessions.' There are two policy options: 'Best Effort' (selected) and 'Enforced'. Below this is the 'Cipher Support' section, which says 'Select the ciphers that you want to support for media encryption.' There are four checkboxes: 'AES_CM_256_HMAC_SHA1_80 enabled' (checked), 'AES_CM_256_HMAC_SHA1_32 enabled' (unchecked), 'AES_CM_128_HMAC_SHA1_80 enabled' (checked), and 'AES_CM_128_HMAC_SHA1_32 enabled' (unchecked). 'Save' and 'Cancel' buttons are at the bottom right.

9. Configure Avaya Aura® Application Enablement Services

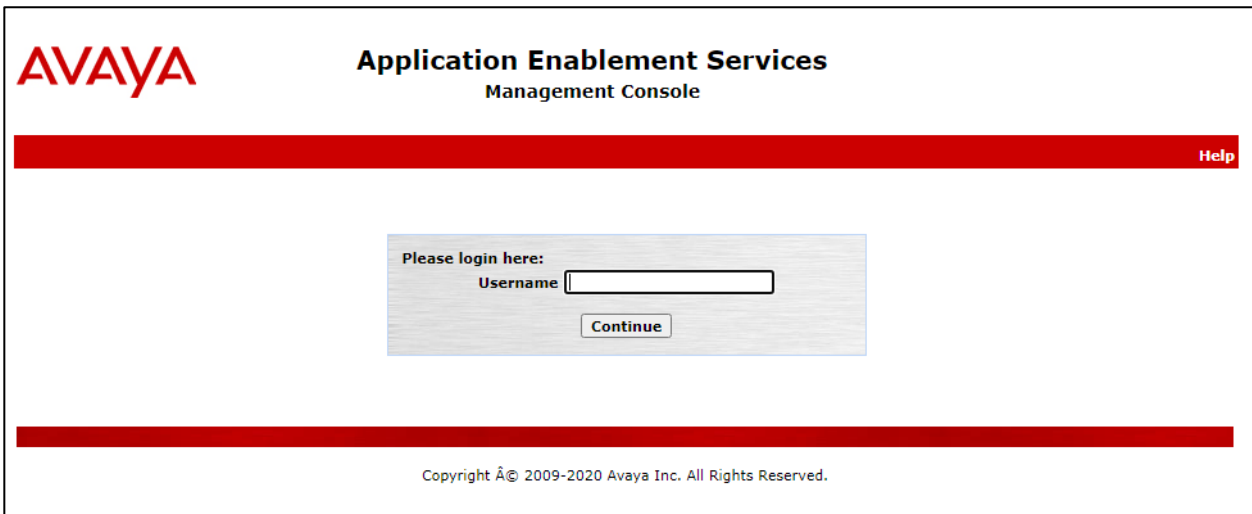
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer Avaya user
- Administer security database
- Restart services
- Obtain Tlink name

9.1. Launch OAM Interface


Access the OAM web-based interface by using the URL “https://ip-address” in an Internet browser window, where **ip-address** is the IP address of the Application Enablement Services server.

The **Please login here** screen is displayed. Log in using the appropriate credentials.



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" and "Management Console" is displayed. A red horizontal bar spans the width of the page, with a "Help" link on the right. In the center, there is a login box with the text "Please login here:" and "Username" followed by a text input field. Below the input field is a "Continue" button. At the bottom of the page, a red horizontal bar is present, and below it, the copyright notice "Copyright © 2009-2020 Avaya Inc. All Rights Reserved." is displayed.

The **Welcome to OAM** screen is displayed next.



Application Enablement Services Management Console

Welcome: User cust
Last login: Thu Feb 18 14:36:40 2021 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.0.0.25-0
Server Date and Time: Mon Feb 22 17:38:46 ICT 2021
HA Status: Not Configured

Home

Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

Welcome to OAM

The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:


- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- High Availability - Use High Availability to manage AE Services HA.
- Licensing - Use Licensing to manage the license server.
- Maintenance - Use Maintenance to manage the routine maintenance tasks.
- Networking - Use Networking to manage the network interfaces and ports.
- Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.
- Status - Use Status to obtain server status informations.
- User Management - Use User Management to manage AE Services users and AE Services user-related resources.
- Utilities - Use Utilities to carry out basic connectivity tests.
- Help - Use Help to obtain a few tips for using the OAM Help system

Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain.

Copyright © 2009-2020 Avaya Inc. All Rights Reserved.

9.2. Verify License

Select **Licensing** → **WebLM Server Access** in the left pane, to display the applicable WebLM server log in screen (not shown). Log in using the appropriate credentials and navigate to display installed licenses (not shown).

**Application Enablement Services**
Management Console

Welcome: User cust
Last login: Thu Feb 18 14:36:40 2021 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.0.0.25-0
Server Date and Time: Mon Feb 22 17:39:12 ICT 2021
HA Status: Not Configured

LicensingHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

High Availability

▼ Licensing

WebLM Server Address

WebLM Server Access

Reserved Licenses

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

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

Copyright © 2009-2020 Avaya Inc. All Rights Reserved.

Select **Licensed products** → **APPL_ENAB** → **Application_Enablement** in the left pane, to display the **Licensed Features** screen in the right pane.

Verify that there are sufficient licenses for **TSAPI Simultaneous Users**, as shown below. The TSAPI license is used for device monitoring.

AVAYA Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ Widgets ▾ Shortcuts ▾

Search 🔍

Home Licenses

Licenses

- WebLM Home
- Install license
- Licensed products
- APPL_ENAB
- ▼ Application_Enablement
 - View license capacity
 - View peak usage
- ASBCE
- ▶ Session_Border_Controller_E_AE
- AVAYAAURAWEBGATEWAY
- ▶ AVAYAAURAWEBGATEWAY
- AVP
- ▶ AVP
- CCTR
- ▶ ContactCenter
- CE
- ▶ COLLABORATION_ENVIRONMENT
- COMMUNICATION_MANAGER
- ▶ Call_Center
- ▶ Communication_Manager
- ▶ Dialog_Designer
- IPO
- ▶ IP_Office
- MESSAGING
- ▶ Messaging
- MSR

Application Enablement (CTI) - Release: 8 - SID: 10503000 Standard Li

You are here: Licensed Products > Application_Enablement > View License Capacity

License installed on: September 6, 2019 4:38:44 PM +07:00

License File Host IDs: V7-67-C3-CF-17-1A-01

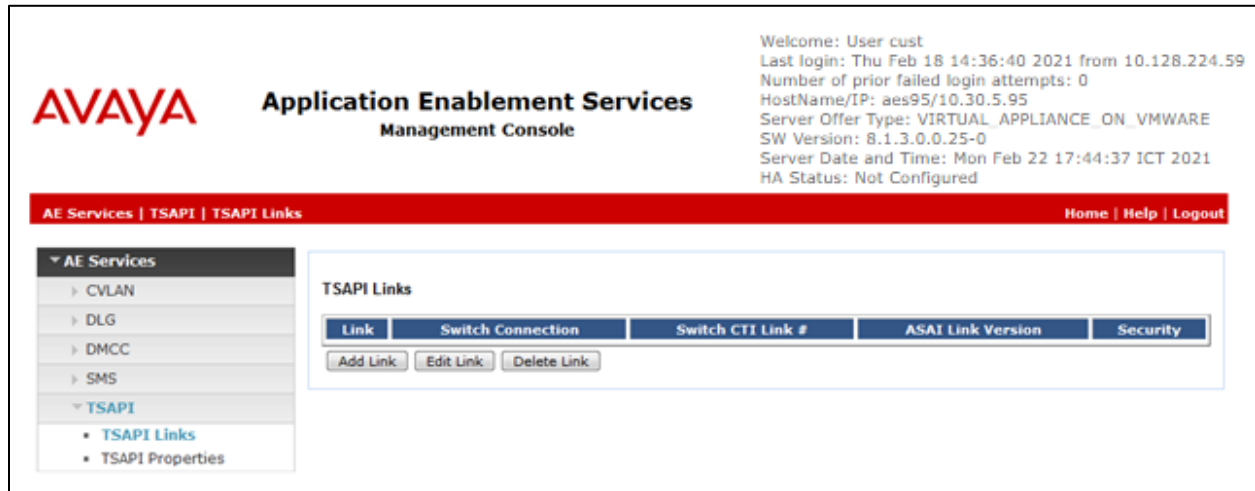
Licensed Features

13 Items Show All ▾

Feature (License Keyword)	Expiration date	Licensed capacity
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	100
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	100
AES HA LARGE VALUE_AES_HA_LARGE	permanent	100
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	100
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	100
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	100
AES HA MEDIUM VALUE_AES_HA_MEDIUM	permanent	100
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	100
DLG VALUE_AES_DLG	permanent	100
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	100
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	100

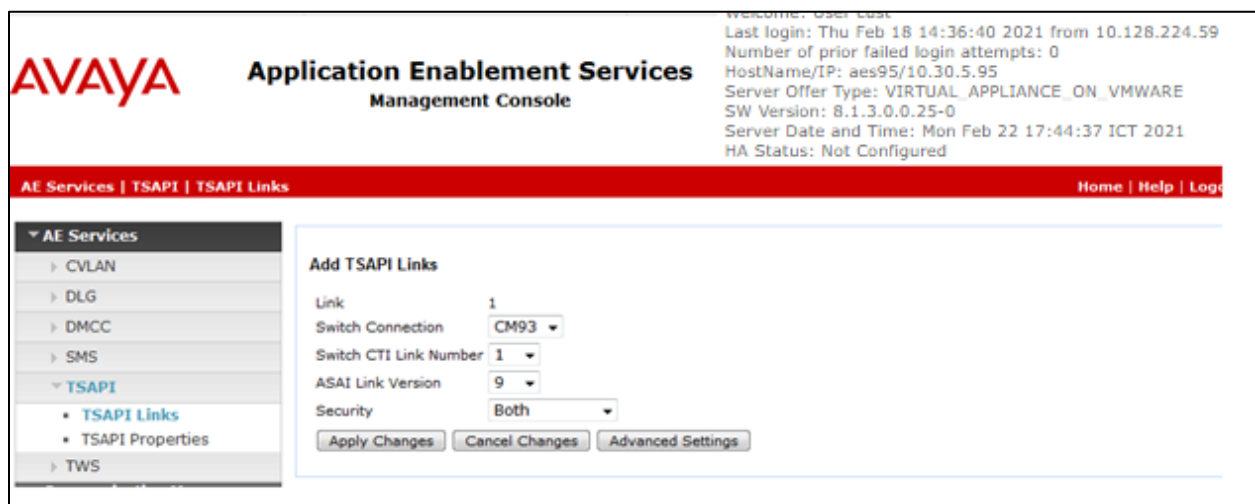
9.3. Administer TSAPI Link

Select **AE Services** → **TSAPI** → **TSAPI Links** from the left pane of the **Management Console**, to administer a TSAPI link. The **TSAPI Links** screen is displayed, as shown below. Click **Add Link**.



The **Add TSAPI Links** screen is displayed next.


The **Link** field is only local to the Application Enablement Services server and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection **CM93** is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 7.2**. Retain the default values in the remaining fields.



9.4. Administer CCT User

Select **User Management** → **User Admin** → **Add User** from the left pane, to display the **Add User** screen in the right pane.

Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password**, and **Confirm Password**. For **CT User**, select **Yes** from the drop-down list. Retain the default value in the remaining fields.

 **Application Enablement Services**
Management Console

Welcome: User cust
Last login: Wed Apr 7 16:47:18 2021 from 10.128.224.163
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.0.0.25-0
Server Date and Time: Tue Apr 13 18:31:39 ICT 2021
HA Status: Not Configured

User Management | User Admin | List All UsersHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▼ User Management

▶ Service Admin

▼ User Admin

▪ Add User

▪ Change User Password

▪ List All Users

▪ Modify Default Users

▪ Search Users

▶ Utilities

▶ Help

Edit User

* User Id

cct

* Common Name

cct

* Surname

cct

User Password

••••••••

Confirm Password

Admin Note

Avaya Role

None ▼

Business Category

Car License

CM Home

Css Home

CT User

Yes ▼

Department Number

Display Name

Employee Number

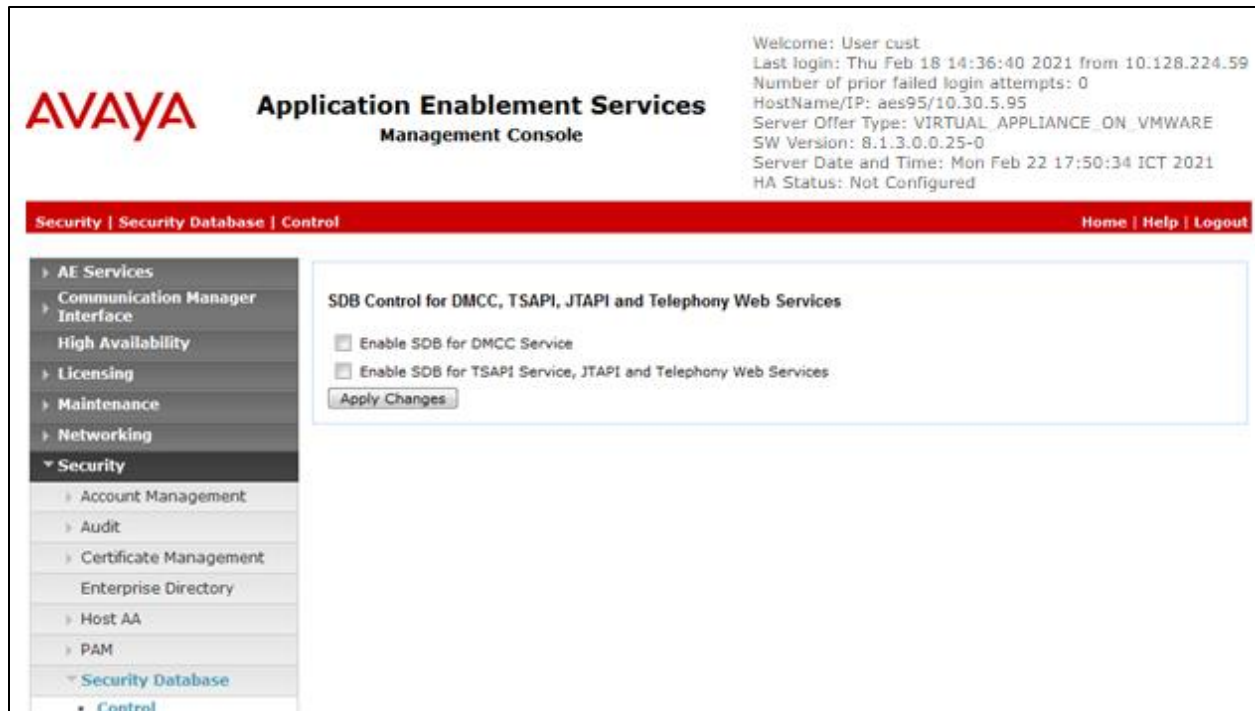
Employee Type

Enterprise Handle

9.5. Administer Security Database

Select **Security** → **Security Database** → **Control** from the left pane, to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane. Uncheck both fields below.

In the event that the security database is used by the customer with parameters already enabled, then follow reference [4] in **Section 13** to configure access privileges for the CCT user from **Section 9.4**.



9.6. Restart Services

Select **Maintenance** → **Service Controller** from the left pane, to display the **Service Controller** screen in the right pane. Check **TSAPI Service** and click **Restart Service**.

The screenshot displays the Avaya Application Enablement Services Management Console. The left sidebar contains a navigation menu with the following items: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance (selected), Date Time/NTP Server, Security Database, Service Controller (highlighted in blue), Server Data, Networking, Security, Status, User Management, Utilities, and Help. The main content area is titled 'Service Controller' and features a table with two columns: 'Service' and 'Controller Status'. The table lists several services, all of which are 'Running'. The 'TSAPI Service' is selected with a checked checkbox. Below the table, there is a note: 'For status on actual services, please use [Status and Control](#)'. At the bottom of the main area, there is a row of buttons: Start, Stop, Restart Service, Restart AE Server, Restart Linux, and Restart Web Server.

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

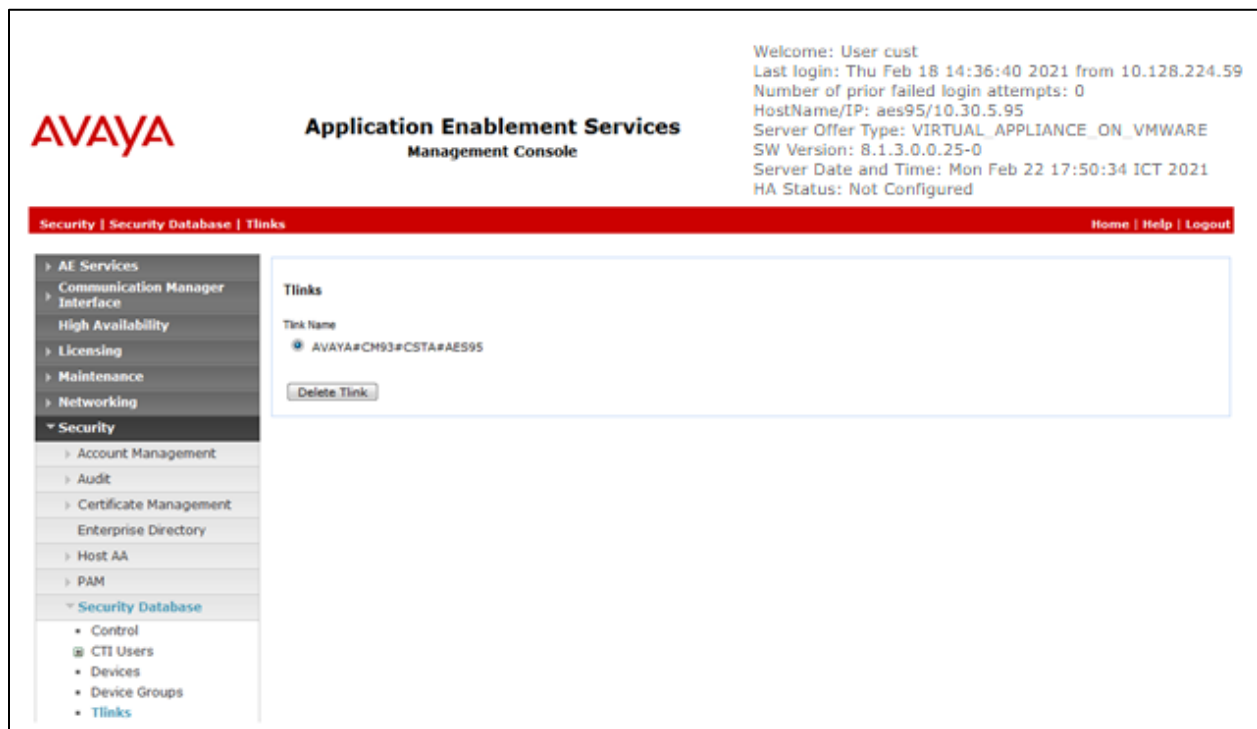
For status on actual services, please use [Status and Control](#)

Start Stop Restart Service Restart AE Server Restart Linux Restart Web Server

9.7. Obtain Tlink Name

Select **Security** → **Security Database** → **Tlinks** from the left pane. The **Tlinks** screen shows a listing of the Tlink names. A new Tlink name is automatically generated for the TSAPI service. Locate the Tlink name associated with the relevant switch connection, which would use the name of the switch connection as part of the Tlink name. Make a note of the associated Tlink name, to be used later for configuring ContactPro.

In this case, the associated Tlink name is **AVAYA#CM93#CSTA#AES95**. Note the use of the switch connection **CM93** from **Section 9.3** as part of the Tlink name.



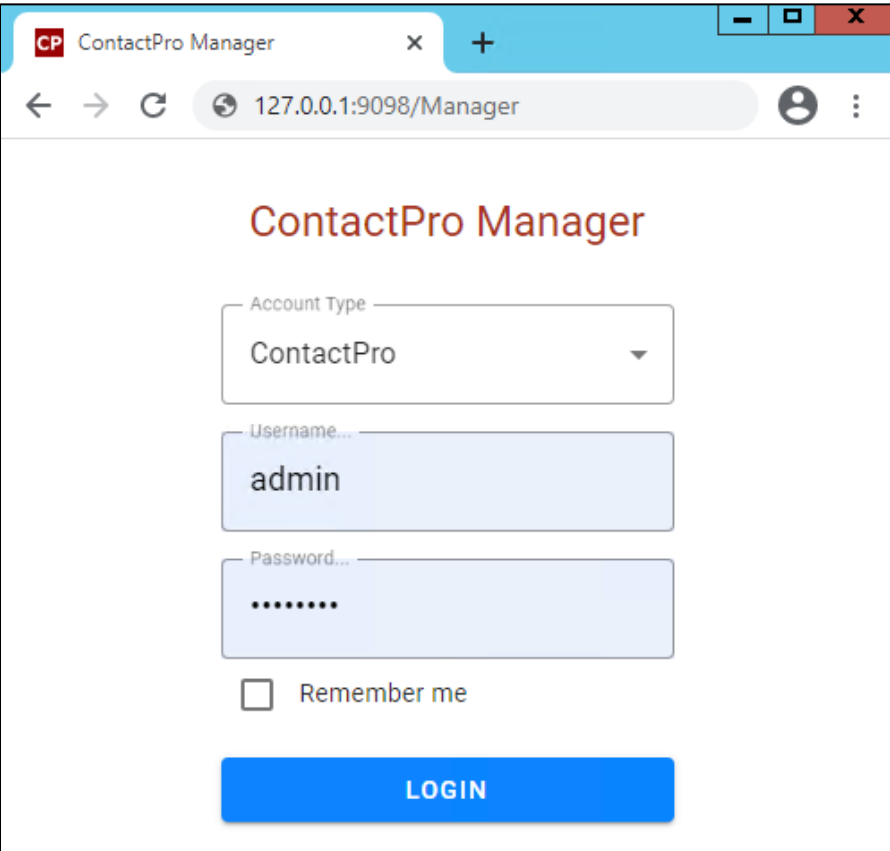
10. Configure CCT ContactPro® Server

It is implied a working CCT ContactPro® Server is already in place and connect to AES successfully with the necessary licensing.

10.1. Configure Users with CCT ContactPro® Manager

Access the CCT ContactPro® Manager web-based interface by using the URL <https://fqdn:39098> or http://ip-address_or_fqdn:9098 in an Internet browser window, where **fqdn** is the dns name of the ContactPro server or **ip-address** is the IP address of the ContactPro server.

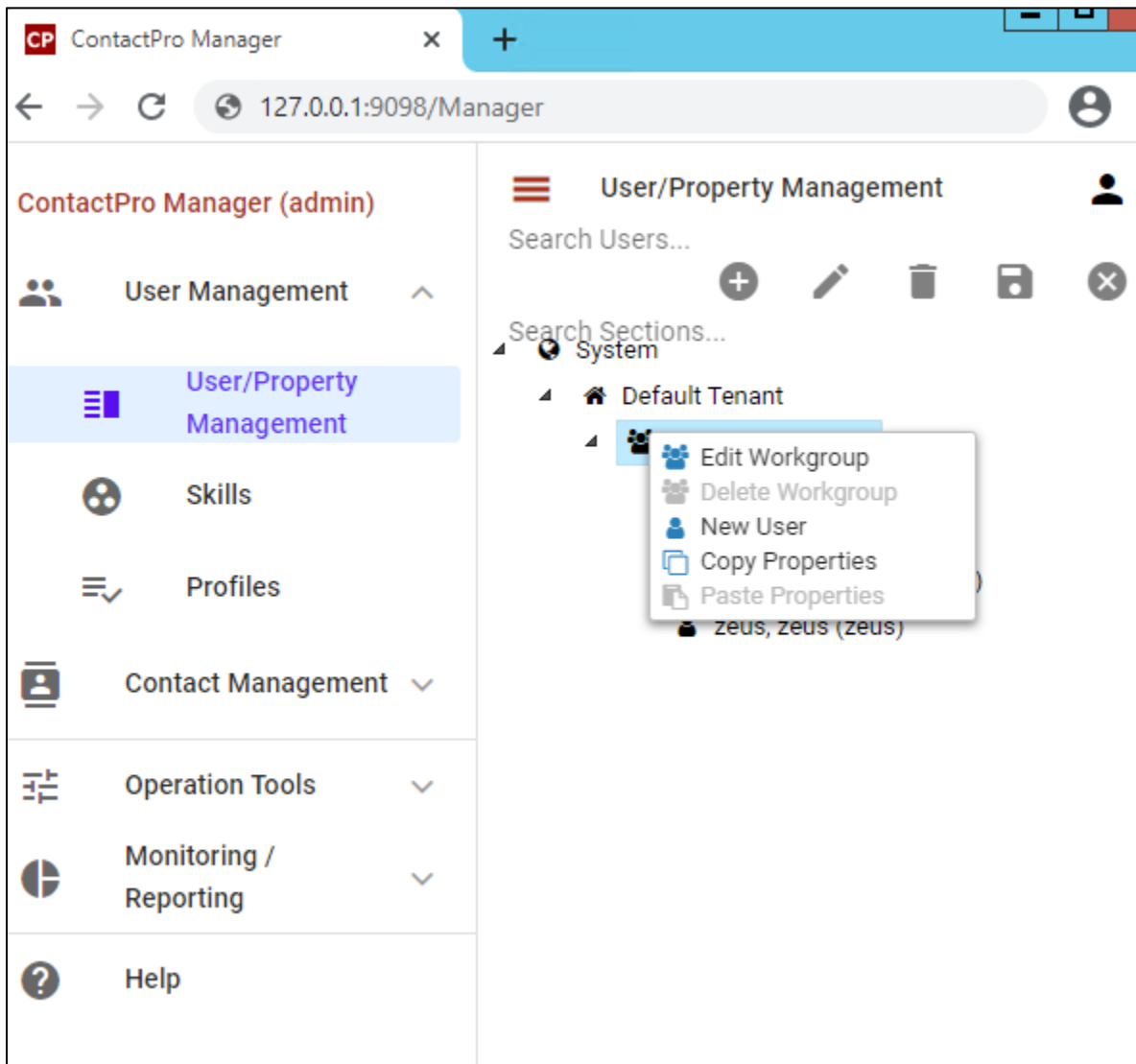
The Login screen is displayed. Log in using the appropriate credentials.



The screenshot shows a web browser window titled "ContactPro Manager". The address bar displays "127.0.0.1:9098/Manager". The main content area features the "ContactPro Manager" title in red. Below the title is a login form with the following elements:

- An "Account Type" dropdown menu with "ContactPro" selected.
- A "Username..." text input field containing the text "admin".
- A "Password..." text input field with masked characters (dots).
- A checkbox labeled "Remember me" which is currently unchecked.
- A blue "LOGIN" button at the bottom of the form.

Right click on a **Workgroup** then click **New User** to create new employee for every ContactPro Client user.



The following fields are required.

- Username (This is the **Agent ID** such as that created in **Section 7.3.2** for example)
- First Name
- Last Name
- Password

Add User

Username* zeus	Title
First Name* zeus	Last Name* zeus
Phone	Email
Active Directory Username zeus	CRM Username

Role
Agent

Agent Profile

☐ Overwrite Current Skills With Agent Profile

Password

Min. password length: 8
Min. number of characters: 1
Min. number of numbers: 0
Min. number of special Characters: 0

☐ Change Password On Login

Agent ID 80001	Agent Password *****
Station 72017	Station Password *****

Capacity Email 1	Capacity WebChat 1	Capacity Outbound 1	Capacity SMS 1	Capacity Total 1
---------------------	-----------------------	------------------------	-------------------	---------------------

ADD **CANCEL**

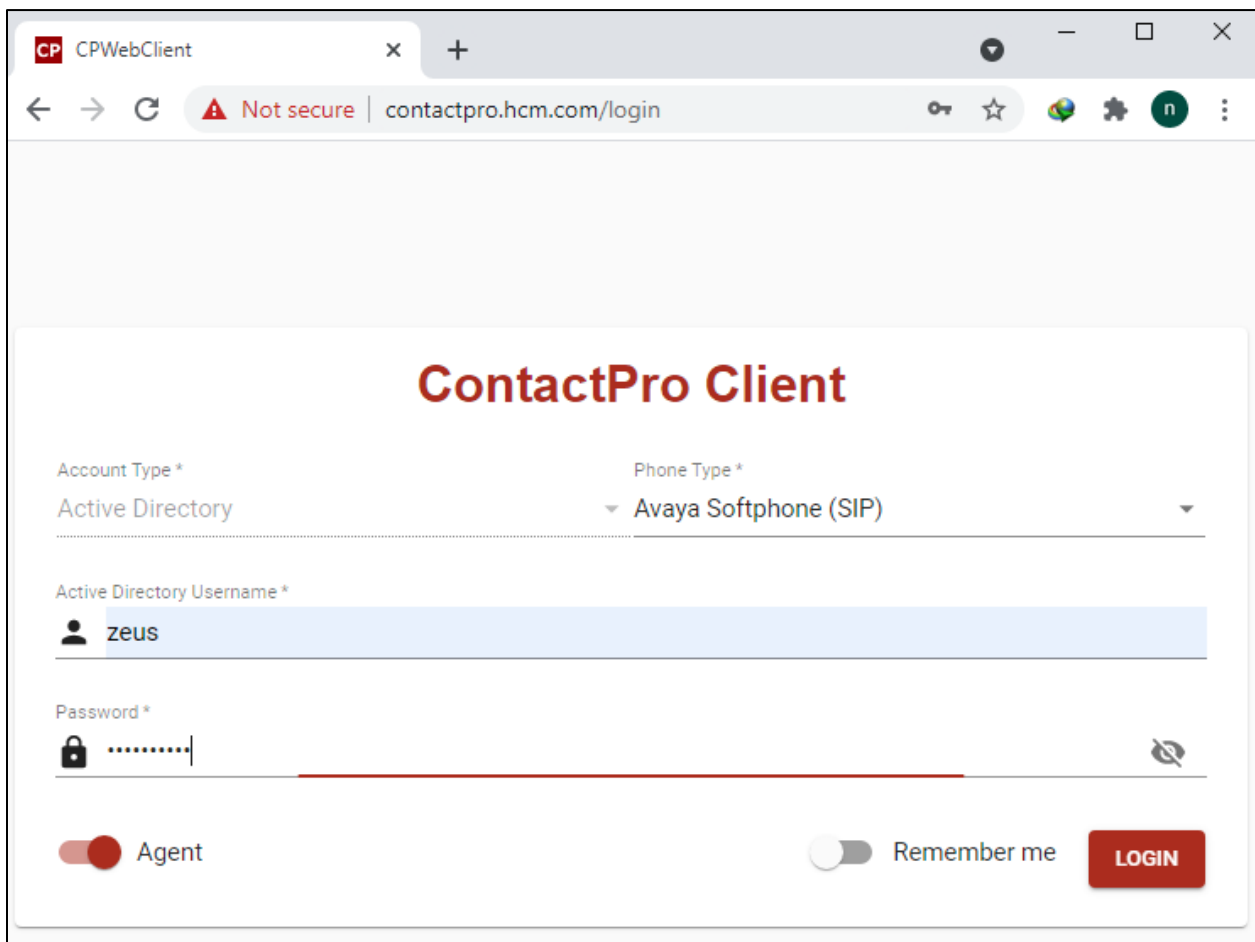
Create employees under different workgroups in different tenants. This allows you to easily manage different Properties for different **Tenants** or **Workgroups** or each individual **Employee**. NOTE: Do not need to duplicate properties. You only need to configure what's different compared to the upper level which could be either the **Top System Level**, **Tenant** or **Workgroup** level.

11. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Application Enablement Services and ContactPro Client.

11.1. Verify login of ContactPro Client

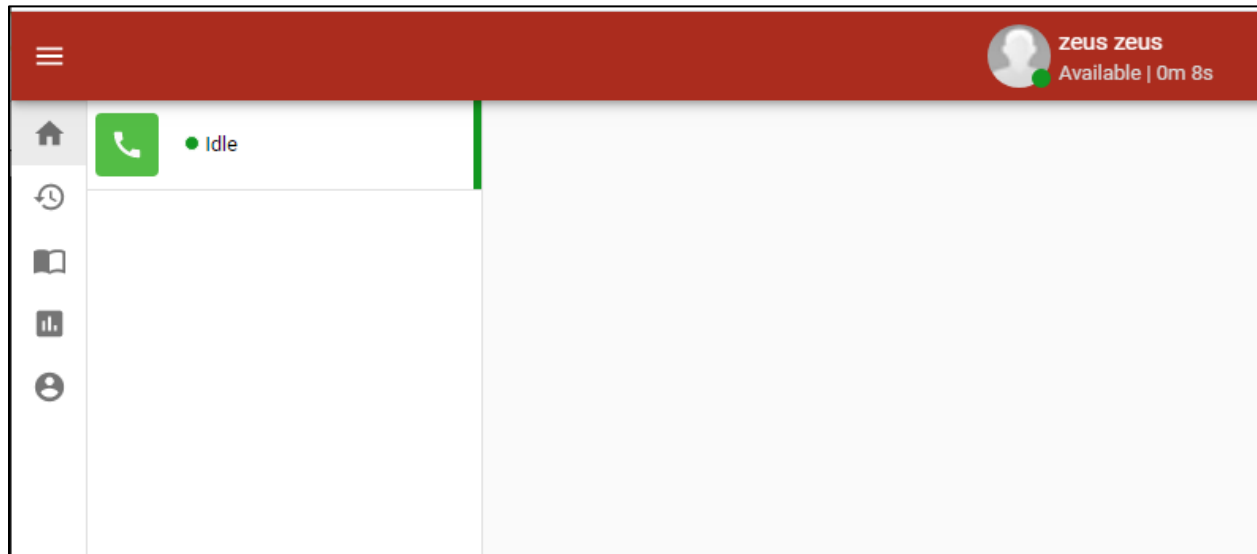
From the Client PC open the Chrome Web browser access ContactPro Web Client URL:



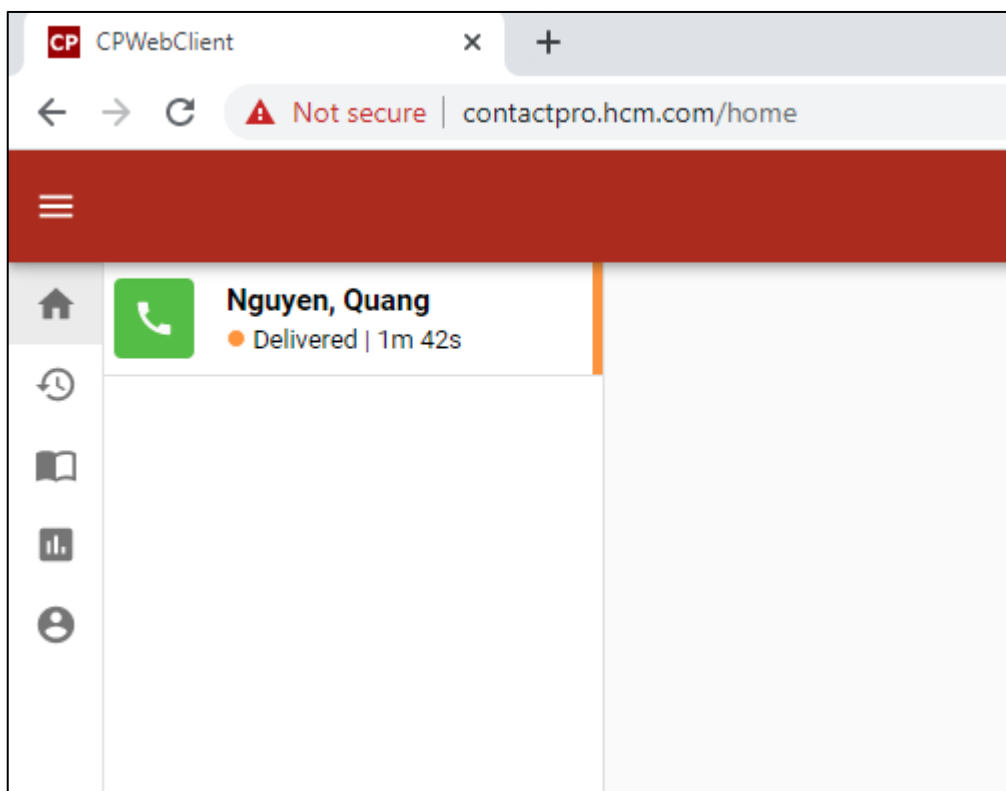
The screenshot shows a Chrome browser window with the tab labeled 'CPWebClient'. The address bar displays 'contactpro.hcm.com/login' with a 'Not secure' warning. The page title is 'ContactPro Client'. The login form includes the following fields and controls:

- Account Type ***: A dropdown menu with 'Active Directory' selected.
- Phone Type ***: A dropdown menu with 'Avaya Softphone (SIP)' selected.
- Active Directory Username ***: A text input field containing the username 'zeus'.
- Password ***: A password input field with masked characters '.....' and a toggle icon to show/hide the password.
- Agent**: A toggle switch that is currently turned on (red).
- Remember me**: A toggle switch that is currently turned off (grey).
- LOGIN**: A red button to submit the login information.

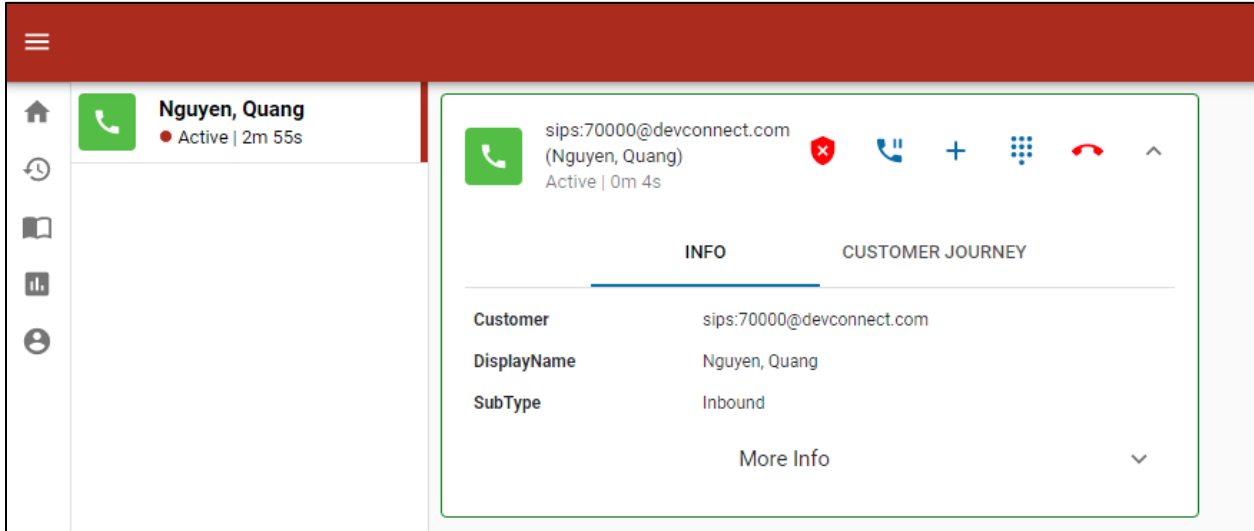
Enter LDAP user credentials already created in **Section 5** and press **Login** with **Agent** enabled. After logging in successfully, ContactPro is shown below:



Place a call to VDN/Hunt Group. Verify that ContactPro Client can receive incoming call:



Answer the call by press on incoming call name panel.



11.2. Verify Avaya Aura® Communication Manager

On Communication Manager, verify status of the administered CTI link by using the **status aesvcs cti-link** command. Verify that the **Service State** is **established** for the CTI link number administered in **Section 7.2**, as shown below.

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS

CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	9	no	Aes95	established	14	14

Enter the command **list agent-loginID** verify that agent **80001** shown in **Section 5.2.4** is logged-in to extension **72017**.

```
list agent-loginID
```

AGENT LOGINID

Login ID	Name	Extension	Dir Agt	AAS/AUD	COR Ag	Pr	SO
	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv
80001	Voice Agent	72017			1	lv1	
	2/01	/	/	/	/	/	/

Enter the command **status station 72017** and on **Page 7** verify that the agent is logged-in to the appropriate skill.

status station 72017							Page 7 of 7
ACD STATUS							
Grp/Mod	Grp/Mod	Grp/Mod	Grp/Mod	Grp/Mod	Grp/Mod	Grp/Mod	
2/AI	/	/	/	/	/	/	On ACD Call? no

11.3. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify the status of the TSAPI link by selecting **Status → Status and Control → TSAPI Service Summary** from the left pane. The **TSAPI Link Details** screen is displayed.

Verify the **Status** is “Talking” for the TSAPI link administered in **Section 9.3**.

Status | Status and Control | TSAPI 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

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	CM93	1	Talking	Thu Jul 8 10:16:09 2021	Online	18	0	15	15	30

Online
Offline

For service-wide information, choose one of the following:
TSAPI Service Status
TLink Status
User Status

Verify the status of the DMCC link by selecting **Status → Status and Control → DMCC Service Summary** from the left pane. The **DMCC Service Summary – Session Summary** screen is displayed.

Verify the **User** column shows action sessions with the CCT username from **Section 9.4**.



Application Enablement Services

Management Console

Welcome: User cust
 Last login: Tue Apr 13 18:46:09 2021 from 10.128.224.59
 Number of prior failed login attempts: 0
 HostName/IP: aes95/10.30.5.95
 Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
 SW Version: 8.1.3.0.0.25-0
 Server Date and Time: Tue Apr 13 19:22:22 ICT 2021
 HA Status: Not Configured

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
- ▶ User Management
- ▶ Utilities
- ▶ Help

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)
 Generated on Tue Apr 13 19:22:12 ICT 2021

Service Uptime: 90 days, 23 hours 36 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 40

Number of Existing Devices: 0

Number of Devices Created Since Service Boot: 21

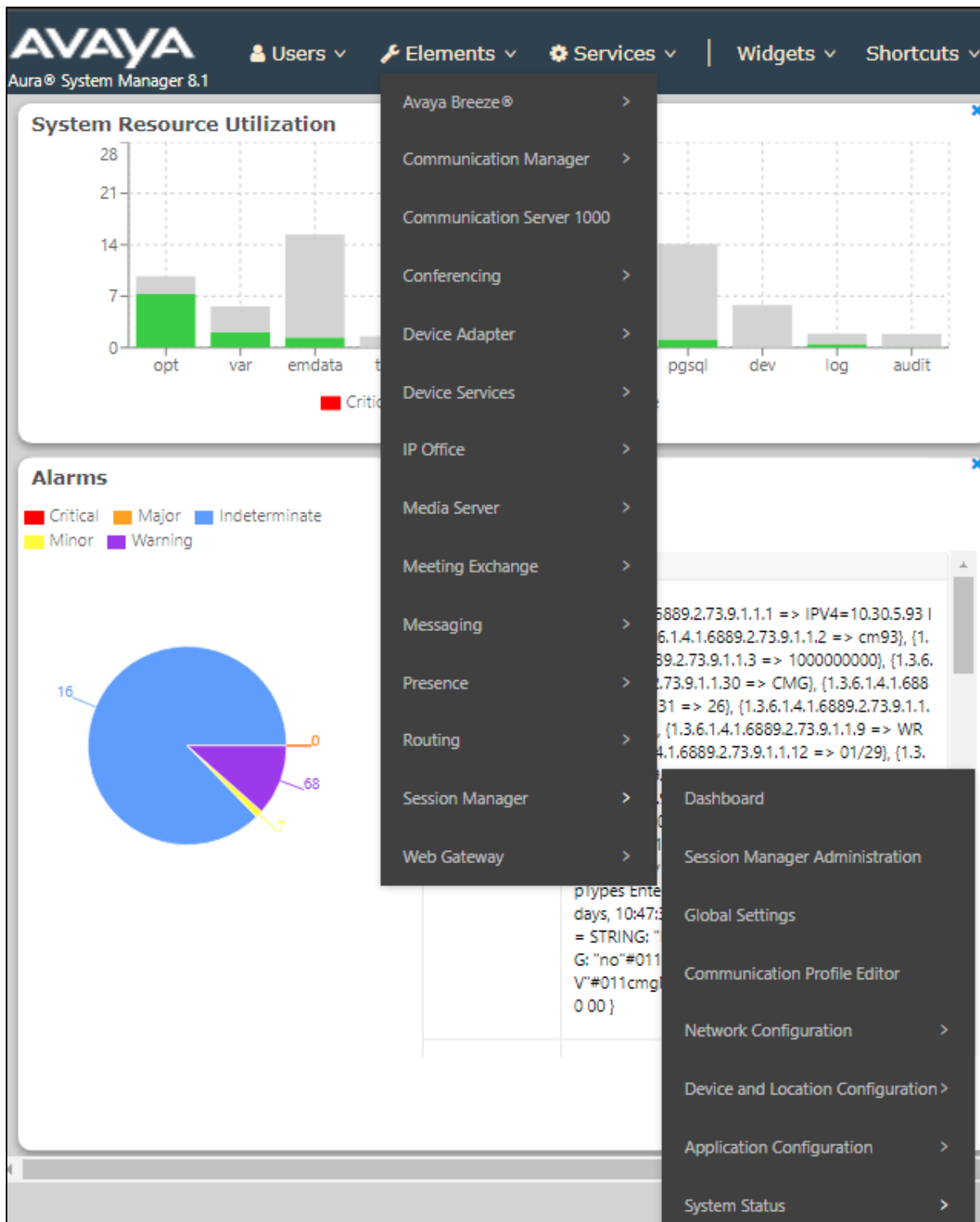
■	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	6FC3A7C0650D5BF39 672B00EF8430175-135162	cct	CCT AES Connector	10.103.3.223	XML Unencrypted	0

Terminate Sessions
Show Terminated Sessions

Item 1-1 of 1
1 Go

11.4. Verify User Registrations on SMGR

From the SMGR Dashboard, go to **Elements** → **Session Manager** → **System Status**.



Select **User Registrations** in left pannel, and verify the user is logged in using the Web Gateway IP Address.

AVAYA Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾

Home Session Manager

Session Manager Ad...

Global Settings

Communication Pro...

Network Configur... ▾

Device and Locati... ▾

Application Confi... ▾

System Status ▴

SIP Entity Monit...

Managed Band...

Security Modul...

SIP Firewall Stat...

Registration Su...

User Registratio...

Session Counts

User Registrations

Select rows to send notifications to devices. Click on Details column for complete registration status.

View ▾ Default Export Force Unregister AST Device Notifications: Reboot Reload ▾ Failback As of 5:13

55 Items Show 15 ▾

<input type="checkbox"/>	Details	Address ▾	First Name	Last Name	Actual Location	IP Address	Remote Office	Share
<input type="checkbox"/>	► Show	72017@devconnect.com	Zeus	DevConnect	SaiGon	10.30.5.138	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	► Show	71015@devconnect.com	Ext7	BT	---	172.27.130.3	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	► Show	71014@devconnect.com	Ext6	BT	---	172.27.130.3	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	► Show	71013@devconnect.com	Ext5	BT	---	172.27.130.3	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	► Show	71012@devconnect.com	Ext4	BT	---	172.27.130.3	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	► Show	71010@devconnect.com	Ext2	BT	---	172.27.130.3	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	► Show	71009@devconnect.com	Ext1	BT	---	172.27.130.3	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	► Show	70001@devconnect.com	Ku	Go	---	10.128.224.164	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	► Show	70000@devconnect.com	Quang	Nguyen	---	10.128.224.212	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	► Show	---	Eros	DevConnect	---	---	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	► Show	---	tran1	Linh	---	---	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	► Show	---	Poseidon	DevConnect	---	---	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	► Show	---	Tran2	Linh	---	---	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	► Show	---	Fernando	Torres	---	---	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	► Show	---	Usopp	OP	---	---	<input type="checkbox"/>	<input type="checkbox"/>

Select : All, None

12. Conclusion

CCT Deutschland GmbH ContactPro 6.0 solution was able to successfully interoperate with Avaya Aura® Environment 8.1.3, which consists of Avaya Aura® Device Services 8.0.2, Avaya Aura® Web Gateway 3.8.1 and the Avaya platform, as listed in **Section 4**. All test cases passed successfully.

13. Additional References

Documentation related to Avaya can be obtained from <https://support.avaya.com>.

- [1] *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 8, Nov 2020
- [2] *Administering Avaya Aura® Session Manager*, Release 8.1.x, Issue 8, Feb 2021
- [3] *Administering the Avaya Aura® Web Gateway*, Release 3.8 Issue 2, July 2020
- [4] *Administering Avaya Aura® Application Enablement Services*, Release 8.1.x, Issue 8, Feb 2021
- [5] *Administering Avaya Aura® Device Services*, Release 8.0.2, Issue 4, June 2020

©2021 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.