DevConnect Program

Application Notes for Cleric Respond-2 with Avaya Aura® Communication Manager 10.1.3 and Avaya Aura® Application Enablement Services 10.1.3 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Cleric Respond-2 to interoperate with Avaya Aura® Communication Manager 10.1.3 and Avaya Aura® Application Enablement Services 10.1.3.

The compliance testing focused on the voice integration of Cleric Respond-2 with Avaya Aura® Communication Manager via the Avaya Aura® Application Device, Media and Call Control (DMCC) Application Programming Interface.

Readers should pay attention to **Section 2,** in particular the scope of testing as outlined in **Section 2.1** as well as any 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.

1. Introduction

These Application Notes describe the configuration steps required for Cleric Respond-2 to interoperate with Avaya Aura® Communication Manager 10.1.3 and Avaya Aura® Application Enablement Services 10.1.3.

The compliance testing focused on the integration of Cleric Respond-2 with Communication Manager via the Application Enablement Services Device, Media, and Call Control (DMCC) Application Programming Interface.

Cleric Respond-2 is a highly visual Ambulance Command and Control / NHS 111 Call Centre computer aided dispatch application. Cleric Respond-2 can monitor agent states and Vector Directory Numbers (VDNs) in the emergency response centre using DMCC of Avaya Aura® Application Enablement Services.

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 Cleric Response-2 successfully monitoring agents'states and calls placed to Vector Directory Numbers (VDNs) from the PSTN, analog phones, digital phones, and IP phones (SIP and H.323) on Avaya Aura® 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 this Application Note, the interface between Avaya systems and Cleric Respond-2 did not include use of any specific encryption features as requested by Cleric.

2.1. Interoperability Compliance Testing

The interoperability Compliance test included feature and serviceability testing. Feature testing monitored agents and calls placed to Vector Directory Numbers (VDNs) and the following:

- **Agent State Changes** – Login, Ready/Not Ready, AUX, After Call Work.
- **Inbound Calls** from Avaya SIP, H.323, and digital telephones, PSTN endpoints.
- **Hold/Transfer/Conference**
- **Serviceability -** The serviceability testing focused on verifying the ability of Cleric Respond-2 to recover from adverse conditions, such as disconnecting/reconnecting the network to Cleric Respond-2.

2.2. Test Results

The testing was successful. All test cases passed.

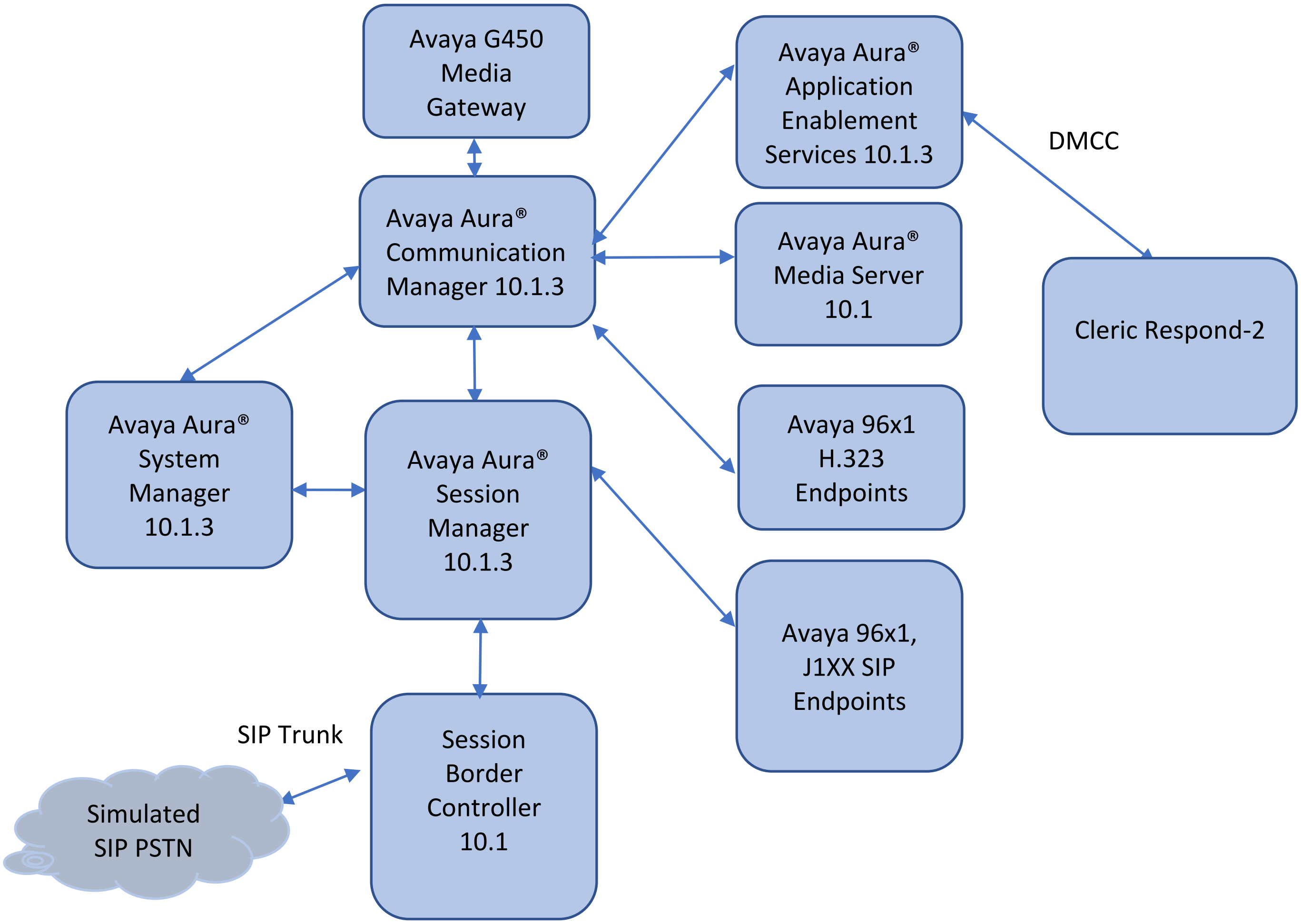
2.3. Support

Technical support can be obtained for the Cleric Respond-2 solution as follows:

Tel: (+44) 01260 270433
Email: support@cleric.co.uk
Web: https://cleric.co.uk/customers/support/

3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**. The detailed administration of basic connectivity between Communication Manager and Application Enablement Services is not the focus of these Application Notes and will not be described.



Avaya G450 Media Gateway
Avaya Aura® Application Enablement Services 10.1.3
DMCC
Avaya Aura® Communication Manager 10.1.3
Avaya Aura® Media Server 10.1
Cleric Respond-2
Avaya Aura® System Manager 10.1.3
Avaya Aura® Session Manager 10.1.3
Avaya 96x1 H.323 Endpoints
Avaya 96x1, J1XX SIP Endpoints
SIP Trunk
Simulated SIP PSTN
Session Border Controller 10.1

Figure 1: Compliance Testing Configuration

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	10.1.3
Avaya Aura® Session Manager in Virtual Environment	10.1.3
Avaya Aura® Communication Manager in Virtual Environment	10.1.3
Avaya G450 Media Gateway	42.22.0
Avaya Aura® Media Server in Virtual Environment	10.1.0 SP4
Avaya Aura® Application Enablement Services in Virtual Environment	10.1.3
Avaya Session Border Controller	10.1
Avaya 9621G & 9641G IP Deskphone (SIP)	7.1.8
Avaya J159 & J179 IP Deskphone (H.323)	6.8.5.3
Avaya J159, J179 IP Deskphone (SIP)	4.1.1
Avaya Agent for Desktop	2.0.6.26.3001
Cleric Respond-2	4.7.120

5. 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
- Administer vectors and VDNs

5.1. 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.

```
change system-parameters customer-options                      Page   4 of  12
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? y          Audible Message Waiting? y
        Access Security Gateway (ASG)? y              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.)
```

Navigate to **Page 7** and verify that the **Vectoring (Basic)** customer option is set to “y”.

```
change system-parameters customer-options                       Page   7 of  12
                         CALL CENTER OPTIONAL FEATURES

                          Call Center Release: 10.1

                                ACD? y                          Reason Codes? y
                       BCMS (Basic)? y               Service Level Maximizer? n
         BCMS/VuStats Service Level? y             Service Observing (Basic)? y
  BSR Local Treatment for IP & ISDN? y     Service Observing (Remote/By FAC)? y
                  Business Advocate? n              Service Observing (VDNs)? y
                    Call Work Codes? y                             Timed ACW? y
      DTMF Feedback Signals For VRU? y                     Vectoring (Basic)? y
                   Dynamic Advocate? n                 Vectoring (Prompting)? y
       Expert Agent Selection (EAS)? y             Vectoring (G3V4 Enhanced)? y
                            EAS-PHD? y              Vectoring (3.0 Enhanced)? y
                   Forced ACD Calls? n     Vectoring (ANI/II-Digits Routing)? y
               Least Occupied Agent? y     Vectoring (G3V4 Advanced Routing)? y
          Lookahead Interflow (LAI)? y                     Vectoring (CINFO)? y
Multiple Call Handling (On Request)? y      Vectoring (Best Service Routing)? y
    Multiple Call Handling (Forced)? y                  Vectoring (Holidays)? y
  PASTE (Display PBX Data on Phone)? y                 Vectoring (Variables)? y
        (NOTE: You must logoff & login to effect the permission changes.)
```

5.2. 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
                                                                     COR: 1

     Name: aes140
```

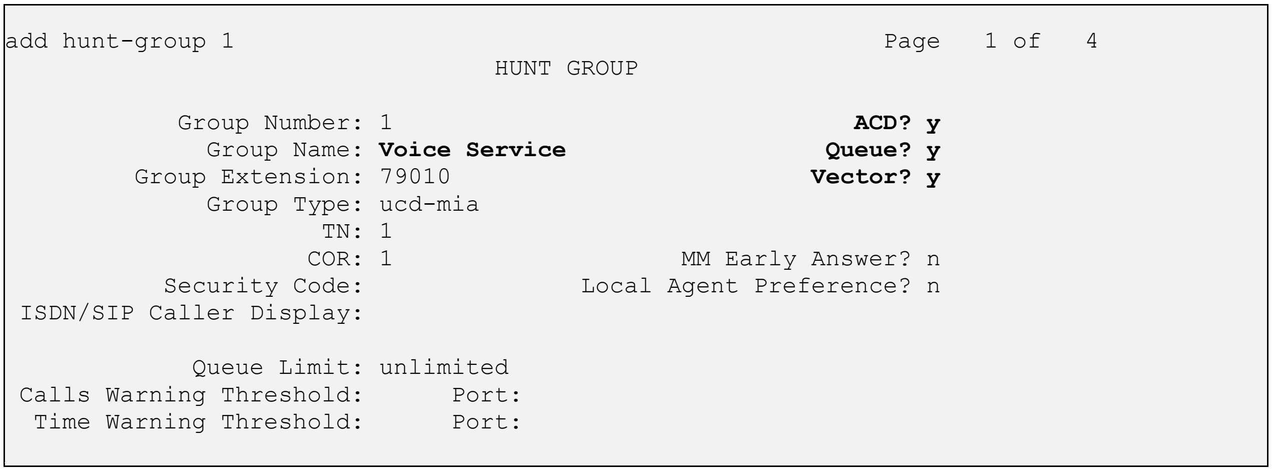
5.4. Administer Hunt Group and Agent

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

- Hunt Group
- Agent

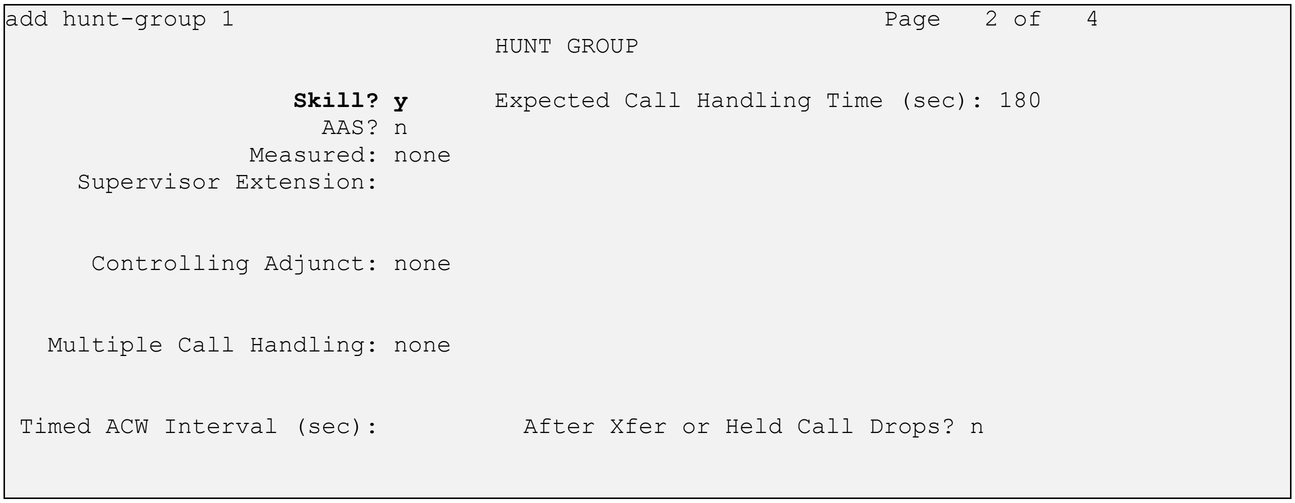
5.4.1. Add Hunt Group

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: 79010                            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.

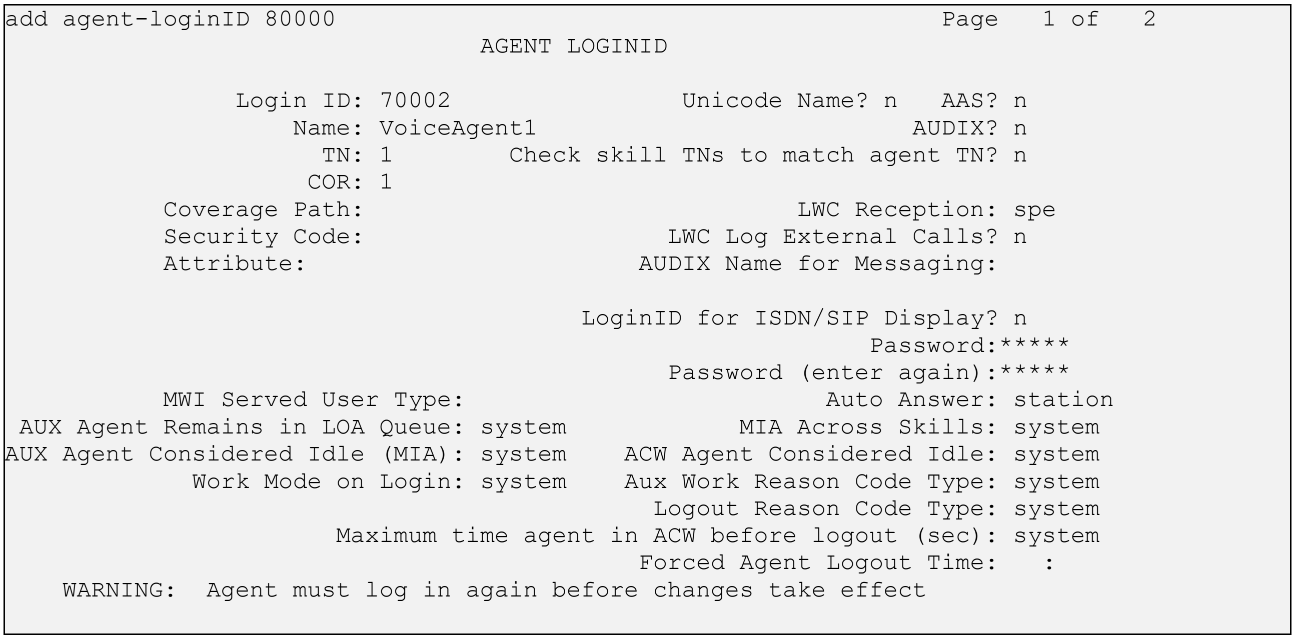


```
add hunt-group 1                                            Page   2 of   4
                                  HUNT GROUP

                    Skill? y      Expected Call Handling Time (sec): 180
                      AAS? n
                 Measured: none
     Supervisor Extension:


      Controlling Adjunct: none


   Multiple Call Handling: none


 Timed ACW Interval (sec):          After Xfer or Held Call Drops? n
```

5.4.2. Add Agent

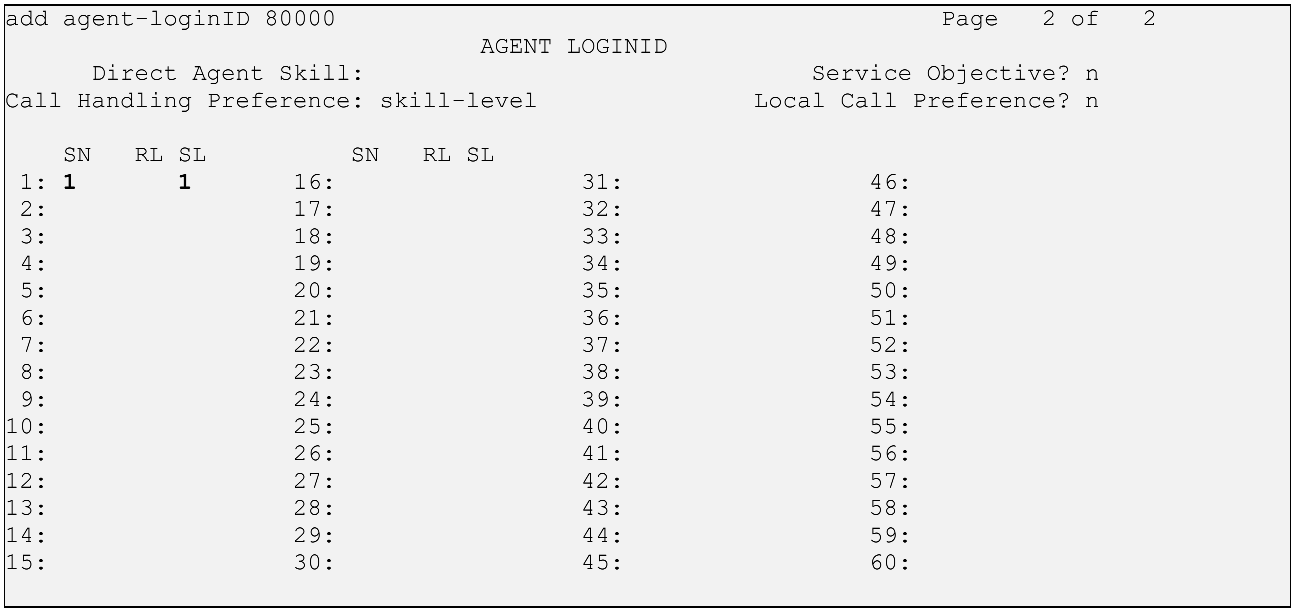
In the compliance testing, the agents 80000 and 80001 were created.

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



```
add agent-loginID 80000                                          Page   1 of   2
                                 AGENT LOGINID

                Login ID: 70002                Unicode Name? n   AAS? n
                    Name: VoiceAgent1                          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
           Attribute:                       AUDIX Name for Messaging:

                                        LoginID for ISDN/SIP Display? n
                                                            Password:*****
                                              Password (enter again):*****
           MWI Served User Type:                         Auto Answer: station
 AUX Agent Remains in LOA Queue: system            MIA Across Skills: system
AUX Agent Considered Idle (MIA): system    ACW Agent Considered Idle: system
             Work Mode on Login: 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 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 80000                                          Page   2 of   2
                                 AGENT LOGINID
      Direct Agent Skill:                               Service Objective? n
Call Handling Preference: skill-level               Local Call Preference? n

    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:
11:                 26:                 41:                 56:
12:                 27:                 42:                 57:
13:                 28:                 43:                 58:
14:                 29:                 44:                 59:
15:                 30:                 45:                 60:
```

Repeat this section to add another agent 80001.

5.5. 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. 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
```

6. Configure Avaya Aura® Application Enablement Services

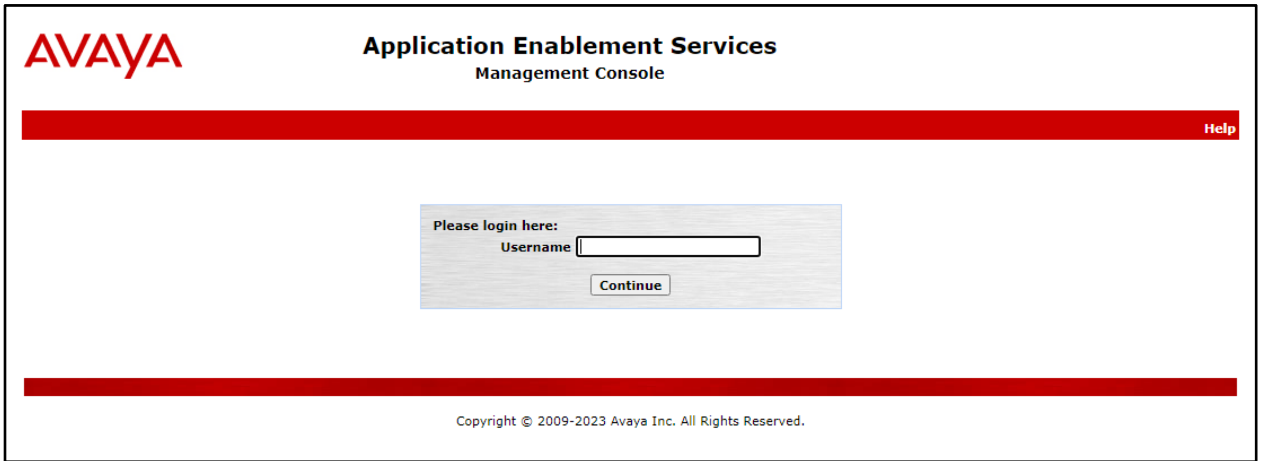
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

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

6.1. Launch OAM Interface

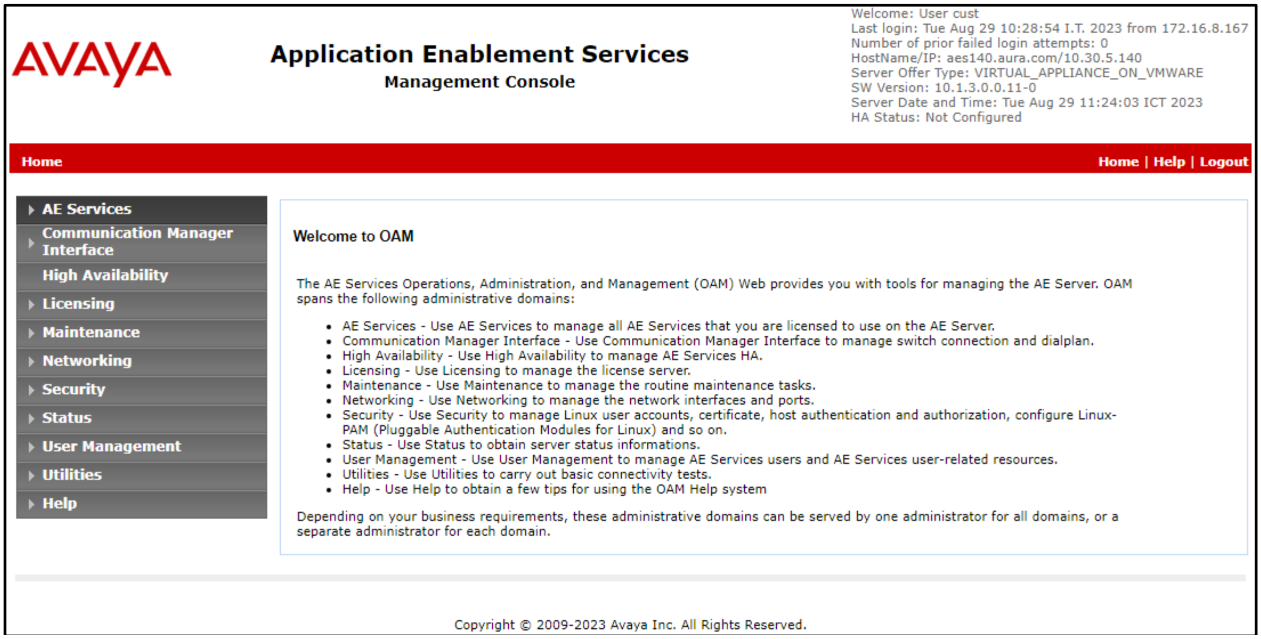
Access the OAM web-based interface by using the URL “https://ip-address” in an Internet browser window, where **ip-address** is the IP address of the Application Enablement Services server.

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


Application Enablement Services
Management Console

Copyright © 2009-2023 Avaya Inc. All Rights Reserved.

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



Welcome: User cust
Last login: Tue Aug 29 10:28:54 I.T. 2023 from 172.16.8.167
Number of prior failed login attempts: 0
HostName/IP: aes140.aura.com/10.30.5.140
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.0.0.11-0
Server Date and Time: Tue Aug 29 11:24:03 ICT 2023
HA Status: Not Configured

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:

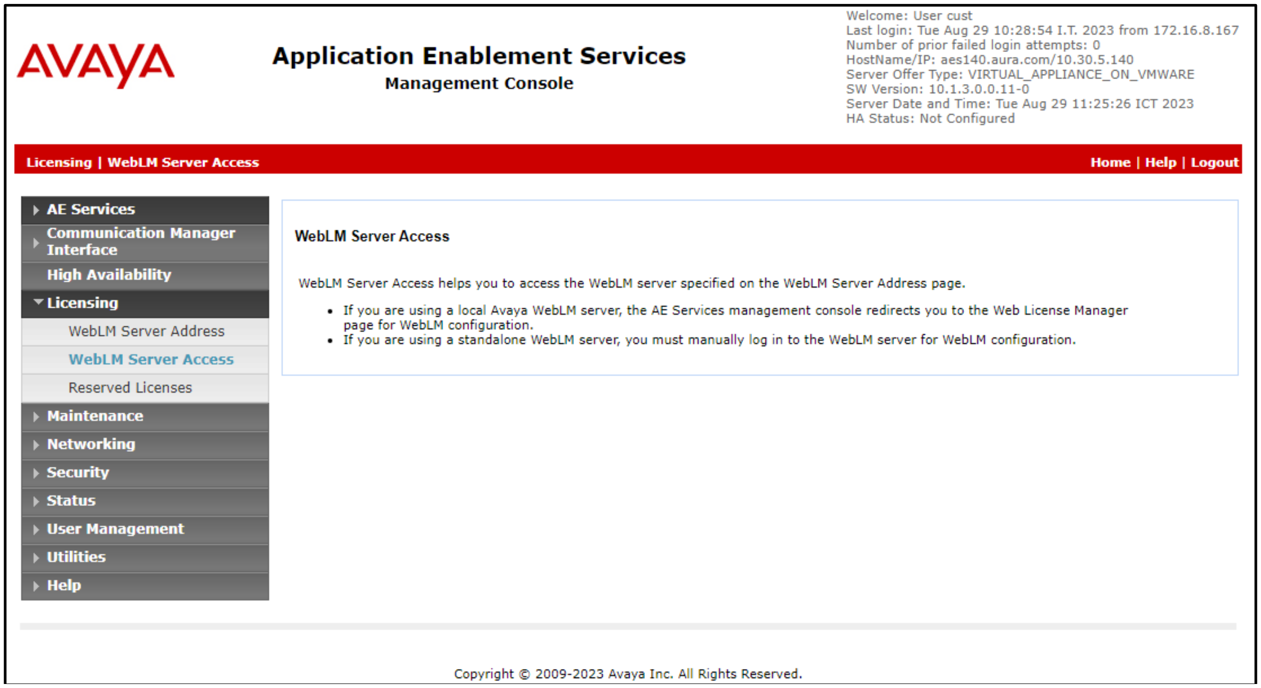
- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- High Availability - Use High Availability to manage AE Services HA.
- Licensing - 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 © 2009-2023 Avaya Inc. All Rights Reserved.

6.2. 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).



Welcome: User cust
Last login: Tue Aug 29 10:28:54 I.T. 2023 from 172.16.8.167
Number of prior failed login attempts: 0
HostName/IP: aes140.aura.com/10.30.5.140
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.0.0.11-0
Server Date and Time: Tue Aug 29 11:25:26 ICT 2023
HA Status: Not Configured

WebLM Server Access

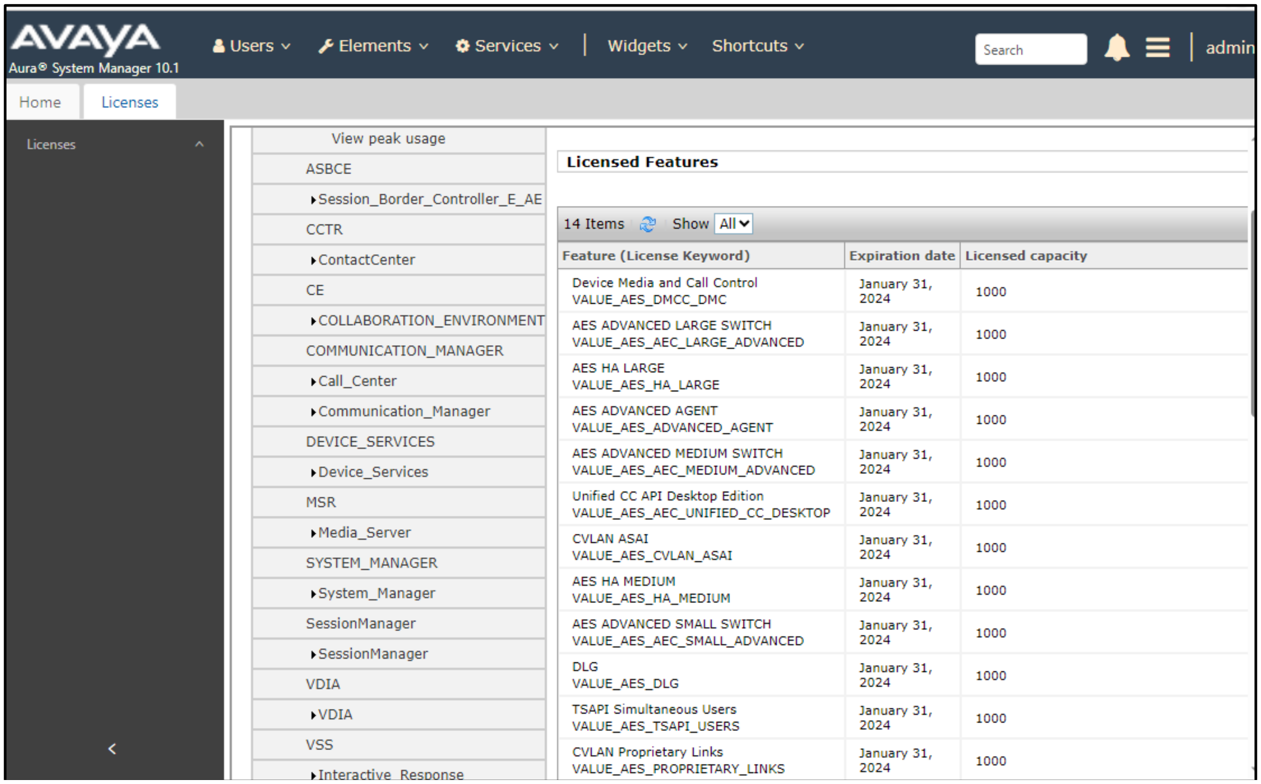
WebLM Server Access helps you to access the WebLM server specified on the WebLM Server Address page.

- If you are using a local Avaya WebLM server, the AE Services management console redirects you to the Web License Manager page for WebLM configuration.
- If you are using a standalone WebLM server, you must manually log in to the WebLM server for WebLM configuration.

Copyright © 2009-2023 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 **Device Media and Call Control**, as shown below.



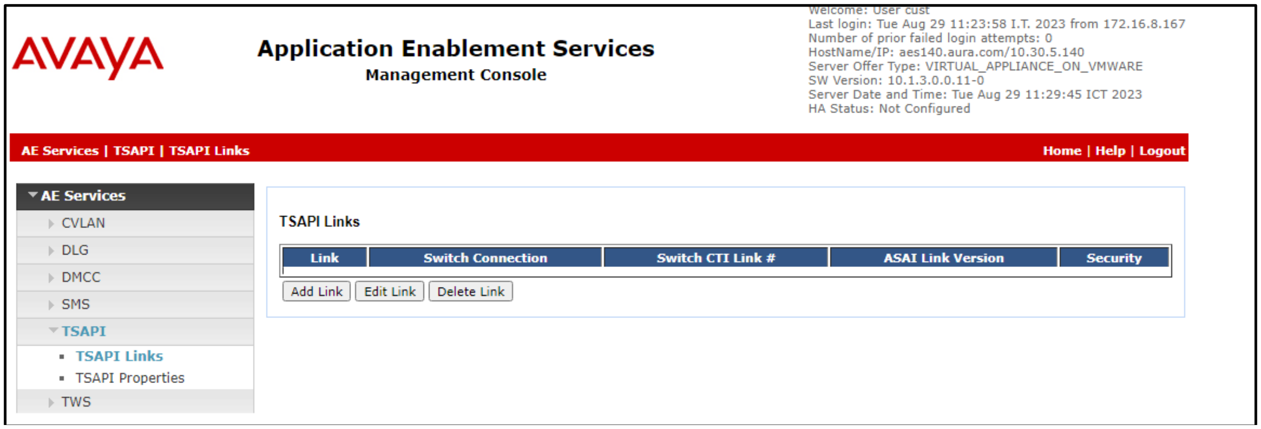
Licensed Features

14 Items Show All

Feature (License Keyword)	Expiration date	Licensed capacity
Device Media and Call Control VALUE_AES_DMCC_DMC	January 31, 2024	1000
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	January 31, 2024	1000
AES HA LARGE VALUE_AES_HA_LARGE	January 31, 2024	1000
AES ADVANCED AGENT VALUE_AES_ADVANCED_AGENT	January 31, 2024	1000
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	January 31, 2024	1000
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	January 31, 2024	1000
CVLAN ASAI VALUE_AES_CVLAN_ASAI	January 31, 2024	1000
AES HA MEDIUM VALUE_AES_HA_MEDIUM	January 31, 2024	1000
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	January 31, 2024	1000
DLG VALUE_AES_DLG	January 31, 2024	1000
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	January 31, 2024	1000
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	January 31, 2024	1000

6.3. 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**.



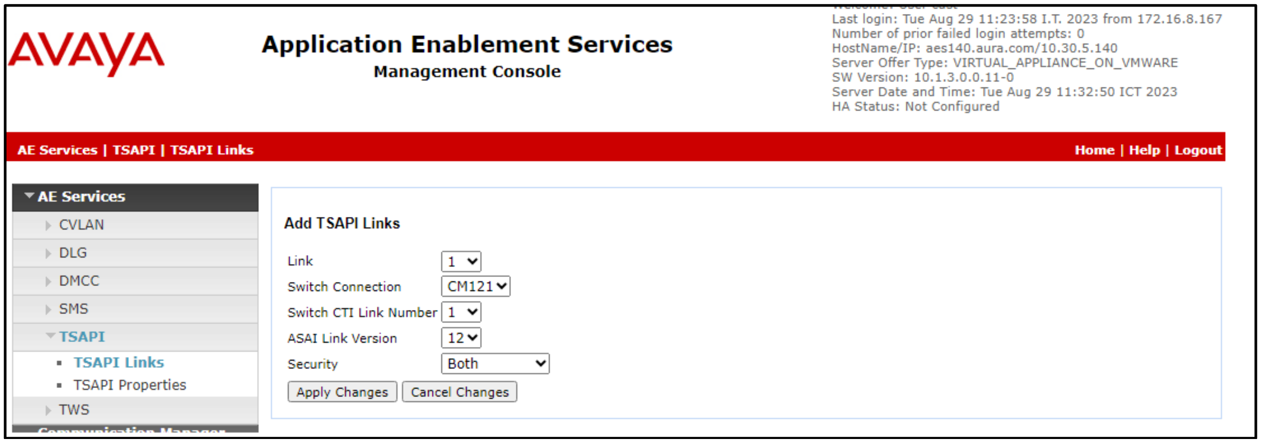
Welcome: User cust
Last login: Tue Aug 29 11:23:58 I.T. 2023 from 172.16.8.167
Number of prior failed login attempts: 0
HostName/IP: aes140.aura.com/10.30.5.140
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.0.0.11-0
Server Date and Time: Tue Aug 29 11:29:45 ICT 2023
HA Status: Not Configured

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security

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

The **Link** field is only local to the Application Enablement Services 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 **CM121** is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields.



Last login: Tue Aug 29 11:23:58 I.T. 2023 from 172.16.8.167
Number of prior failed login attempts: 0
HostName/IP: aes140.aura.com/10.30.5.140
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.0.0.11-0
Server Date and Time: Tue Aug 29 11:32:50 ICT 2023
HA Status: Not Configured

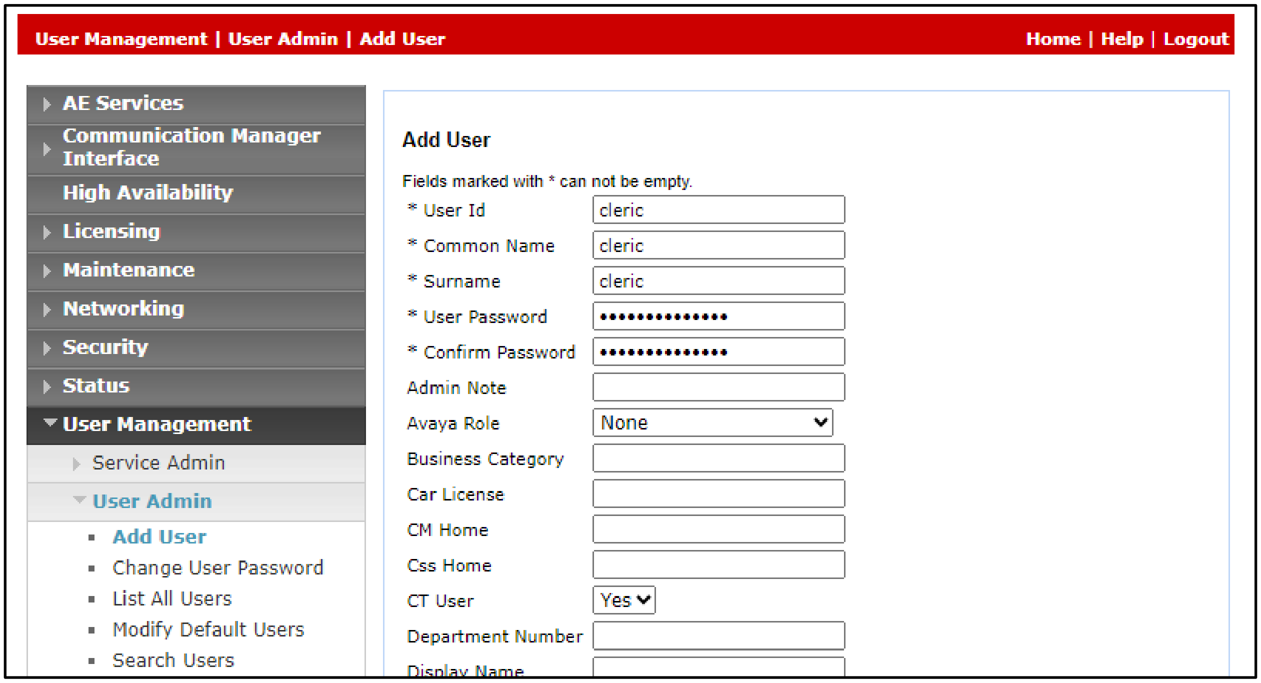
Add TSAPI Links

Link	1
Switch Connection	CM121
Switch CTI Link Number	1
ASAI Link Version	12
Security	Both

6.4. Administer Cleric 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.



Add User

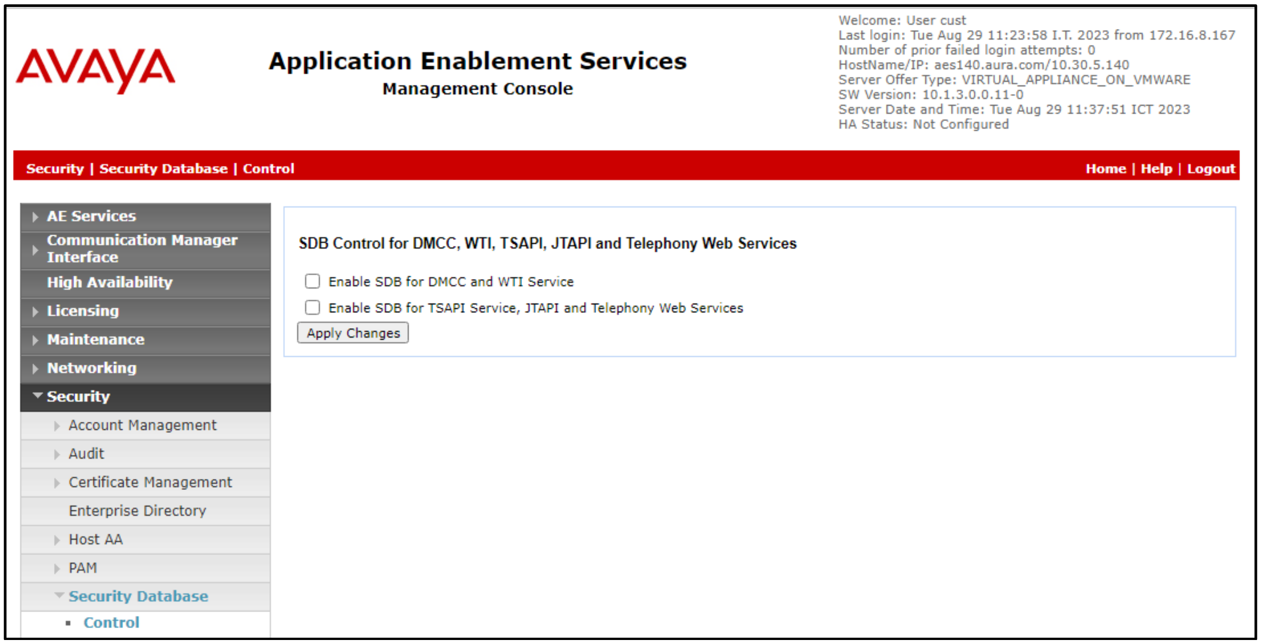
Fields marked with * can not be empty.

* User Id	cleric
* Common Name	cleric
* Surname	cleric
* User Password	••••••••••••••
* Confirm Password	••••••••••••••
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes
Department Number	
Display Name	

6.5. 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] to configure access privileges for the Avaya user from **Section 6.4.**



Welcome: User cust
Last login: Tue Aug 29 11:23:58 I.T. 2023 from 172.16.8.167
Number of prior failed login attempts: 0
HostName/IP: aes140.aura.com/10.30.5.140
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.0.0.11-0
Server Date and Time: Tue Aug 29 11:37:51 ICT 2023
HA Status: Not Configured

SDB Control for DMCC, WTI, TSAPI, JTAPI and Telephony Web Services

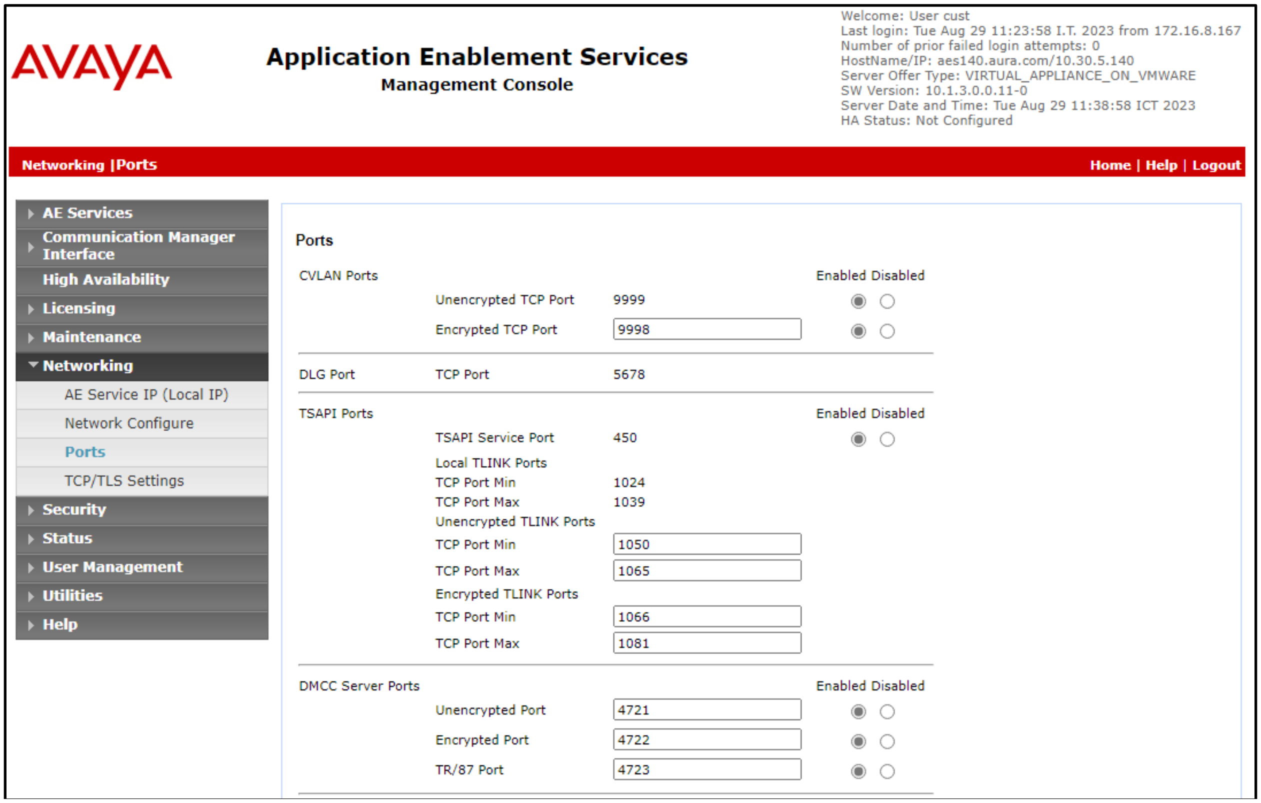
□ Enable SDB for DMCC and WTI Service

□ Enable SDB for TSAPI Service, JTAPI and Telephony Web Services

6.6. Administer Ports

Select **Networking → Ports** from the left pane, to display the **Ports** screen in the right pane.

In the **DMCC Server Ports** section, select the radio button for **Unencrypted Port** under the **Enabled** column, as shown below. Retain the default values in the remaining fields.



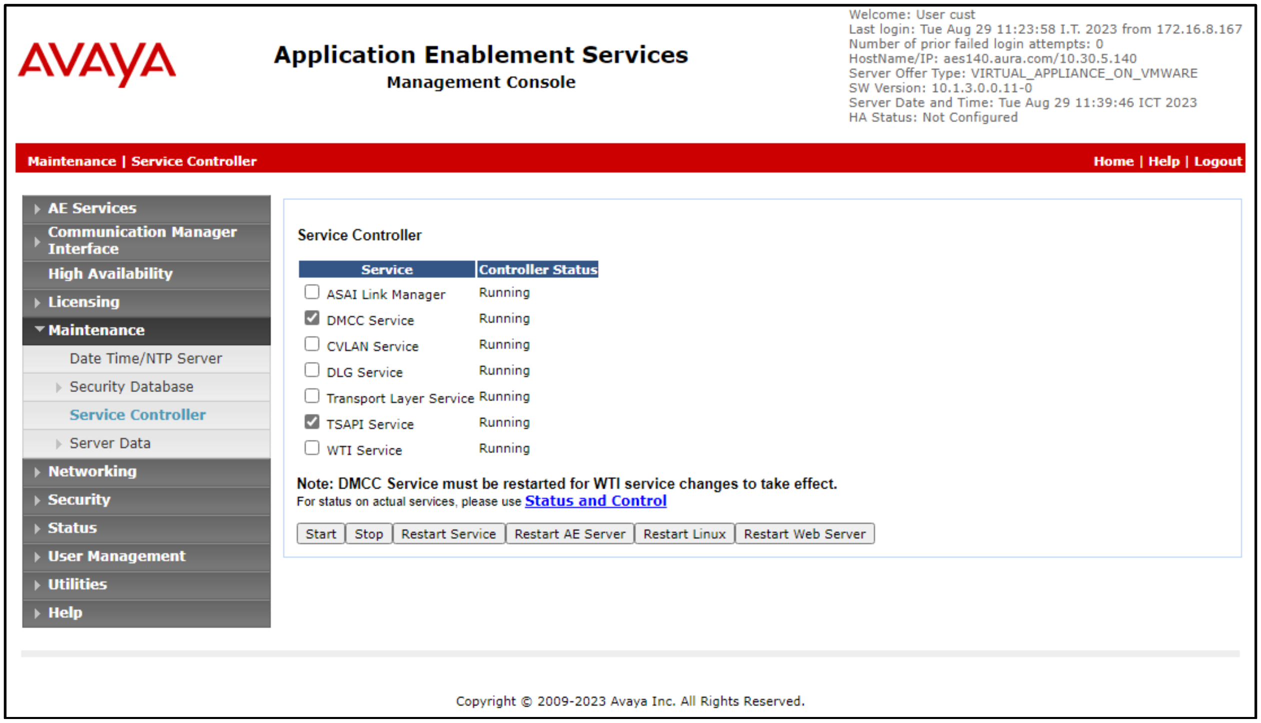
Welcome: User cust
Last login: Tue Aug 29 11:23:58 I.T. 2023 from 172.16.8.167
Number of prior failed login attempts: 0
HostName/IP: aes140.aura.com/10.30.5.140
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.0.0.11-0
Server Date and Time: Tue Aug 29 11:38:58 ICT 2023
HA Status: Not Configured

Ports

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

6.7. Restart Services

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



Welcome: User cust
Last login: Tue Aug 29 11:23:58 I.T. 2023 from 172.16.8.167
Number of prior failed login attempts: 0
HostName/IP: aes140.aura.com/10.30.5.140
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.0.0.11-0
Server Date and Time: Tue Aug 29 11:39:46 ICT 2023
HA Status: Not Configured

Service Controller

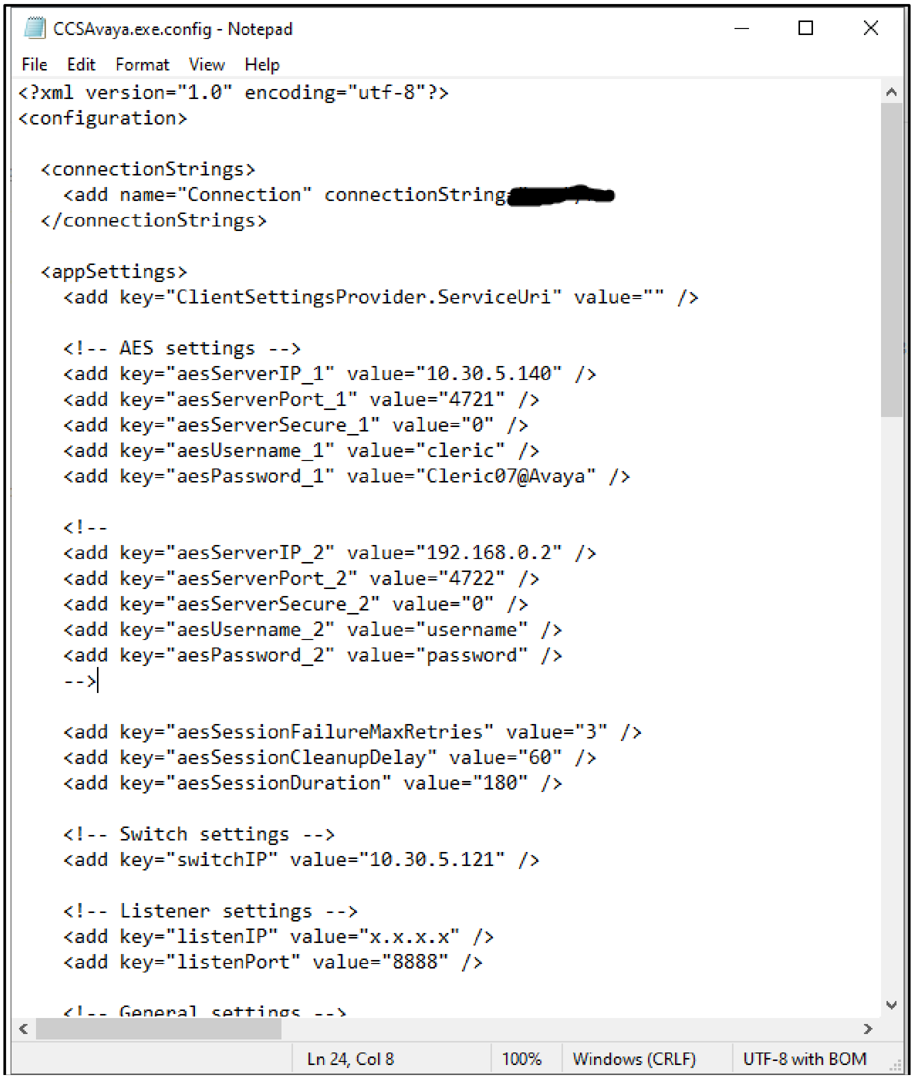
Service	Controller Status
□ ASAI Link Manager	Running
☑ DMCC Service	Running
□ CVLAN Service	Running
□ DLG Service	Running
□ Transport Layer Service	Running
☑ TSAPI Service	Running
□ WTI Service	Running

Note: DMCC Service must be restarted for WTI service changes to take effect.
For status on actual services, please use Status and Control

7. Configure Cleric Respond-2 Server

This section provides the procedures for configuring Cleric Respond-2 Server. It is implied a working Cleric Respond-2 is already in place successfully with the necessary licensing.
Go to CCSA folder (e.g., C:\CCSAvaya\CCSAvaya). Open the CCSAvaya.exe.config file and modify the following settings:

AES Settings
aesServerIP_1: Enter AES IP address, in this case 10.30.5.140
aesServerPort_1: Enter AES DMCC port, in this case 4721 with Unencrypted Port
aesServerSecure_1: Select 0 for Unencrypted
aesUsername_1: Enter cleric user created in **Section 0**
aesPassword_1: Enter password for cleric user in **Section 0**
Switch Settings
switchIP_1: Enter Communication Manager IP address.



```
<?xml version="1.0" encoding="utf-8"?>
<configuration>

  <connectionStrings>
    <add name="Connection" connectionString[redacted]
  </connectionStrings>

  <appSettings>
    <add key="ClientSettingsProvider.ServiceUri" value="" />

    <!-- AES settings -->
    <add key="aesServerIP_1" value="10.30.5.140" />
    <add key="aesServerPort_1" value="4721" />
    <add key="aesServerSecure_1" value="0" />
    <add key="aesUsername_1" value="cleric" />
    <add key="aesPassword_1" value="Cleric07@Avaya" />

    <!--
    <add key="aesServerIP_2" value="192.168.0.2" />
    <add key="aesServerPort_2" value="4722" />
    <add key="aesServerSecure_2" value="0" />
    <add key="aesUsername_2" value="username" />
    <add key="aesPassword_2" value="password" />
    -->

    <add key="aesSessionFailureMaxRetries" value="3" />
    <add key="aesSessionCleanupDelay" value="60" />
    <add key="aesSessionDuration" value="180" />

    <!-- Switch settings -->
    <add key="switchIP" value="10.30.5.121" />

    <!-- Listener settings -->
    <add key="listenIP" value="x.x.x.x" />
    <add key="listenPort" value="8888" />

    <!-- General settings -->
```

8. Verification Steps

This section provides the tests that can be performed to verify correct configuration of Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services and Cleric Respond-2 solution.

8.1. 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 5.2**. **as shown below**.

```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

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

1     12       no    aes140           established   14       14
```

Enter the command **list agent-loginID** and verify that agents **80000** and **80001,** shown in **Section 5.4.2,** are logged into Skill 1 via extension **70010** and **70009**, respectively.

```
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 Skil/Lv

80000         Voice Agent    70010                                 1   lvl
                 1/01     /       /       /       /       /       /

80001         Voice Agent1   70009                                 1   lvl
                 1/01     /       /       /       /       /       /
```

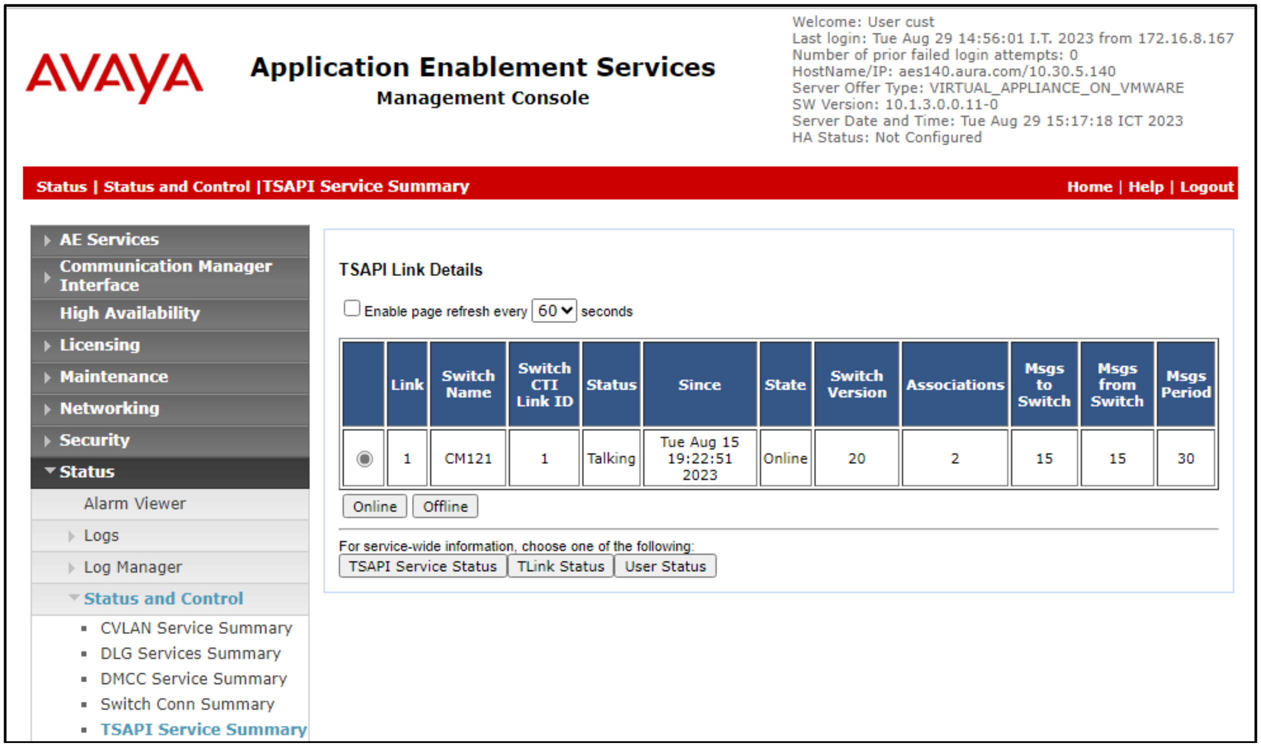
Enter the command **status station 70010** and on **Page 7** verify that the agent is logged into the appropriate skill.

```
status station 70010                                              Page   7 of   7
                                   ACD STATUS

 Grp/Mod  Grp/Mod  Grp/Mod  Grp/Mod  Grp/Mod  Grp/Mod  Grp/Mod
  1/AUX      /        /        /        /        /        /    On ACD Call? no
```

8.2. 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 6.3,** and that the **Associations** column reflects the total number of agents, in this case “**2**.



Application Enablement Services
Management Console

Welcome: User cust
Last login: Tue Aug 29 14:56:01 I.T. 2023 from 172.16.8.167
Number of prior failed login attempts: 0
HostName/IP: aes140.aura.com/10.30.5.140
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.0.0.11-0
Server Date and Time: Tue Aug 29 15:17:18 ICT 2023
HA Status: Not Configured

TSAPI Link Details

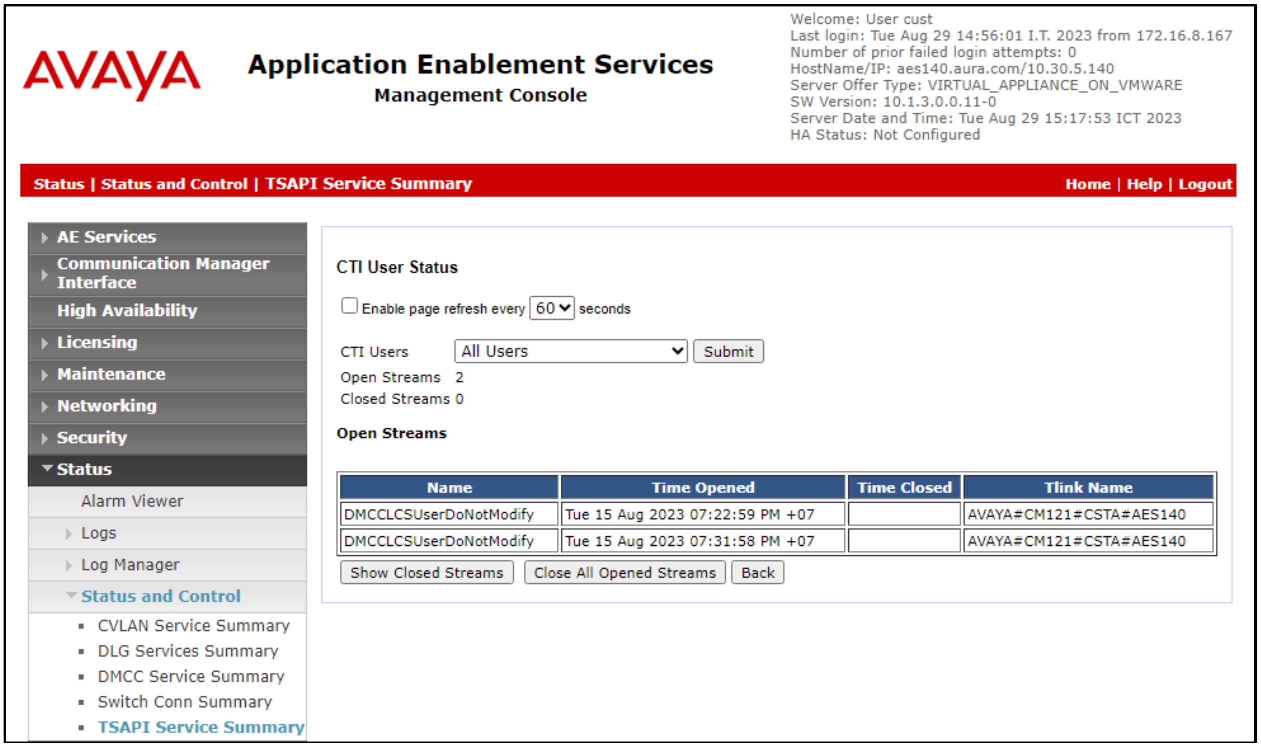
□ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
●	1	CM121	1	Talking	Tue Aug 15 19:22:51 2023	Online	20	2	15	15	30

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

8.4. Verify Avaya Aura® Application Enablement Services

The following steps are carried out on the Application Enablement Services to ensure that the communication link between Communication Manager and the Application Enablement Services server is functioning correctly. Verify the status of the TSAPI service by selecting **Status → Status and Control → TSAPI Service Summary → User Status.** The **Open Streams** section of this page displays open stream created by the **Avaya** user with the **Tlink**.



Welcome: User cust
Last login: Tue Aug 29 14:56:01 I.T. 2023 from 172.16.8.167
Number of prior failed login attempts: 0
HostName/IP: aes140.aura.com/10.30.5.140
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.0.0.11-0
Server Date and Time: Tue Aug 29 15:17:53 ICT 2023
HA Status: Not Configured

CTI User Status

□ Enable page refresh every 60 seconds

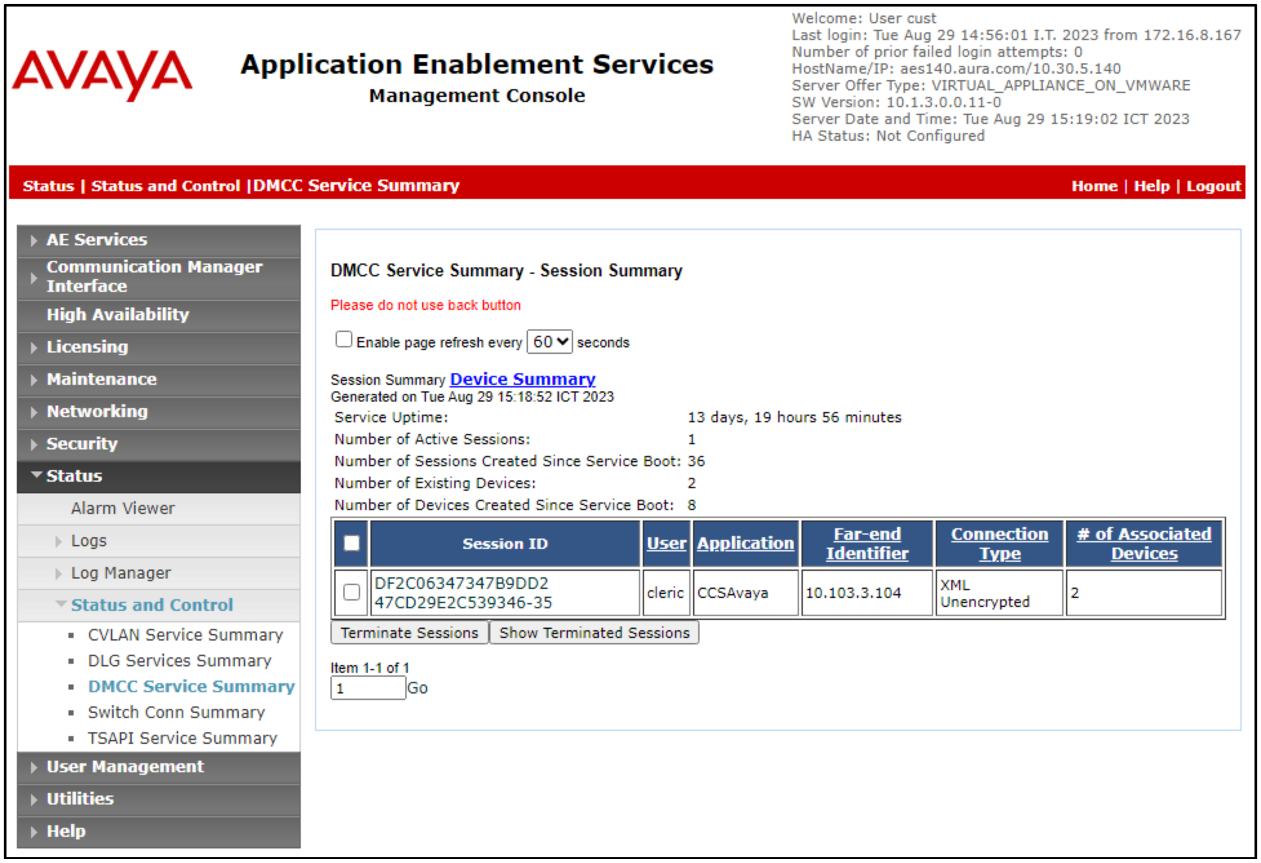
CTI Users: All Users
Open Streams 2
Closed Streams 0

Open Streams

Name	Time Opened	Time Closed	Tlink Name
DMCCLCSUserDoNotModify	Tue 15 Aug 2023 07:22:59 PM +07		AVAYA#CM121#CSTA#AES140
DMCCLCSUserDoNotModify	Tue 15 Aug 2023 07:31:58 PM +07		AVAYA#CM121#CSTA#AES140

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 **cleric** username from **Section 6.5**



Welcome: User cust
Last login: Tue Aug 29 14:56:01 I.T. 2023 from 172.16.8.167
Number of prior failed login attempts: 0
HostName/IP: aes140.aura.com/10.30.5.140
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.0.0.11-0
Server Date and Time: Tue Aug 29 15:19:02 ICT 2023
HA Status: Not Configured

DMCC Service Summary - Session Summary

Please do not use back button

□ Enable page refresh every 60 seconds

Session Summary Device Summary
Generated on Tue Aug 29 15:18:52 ICT 2023

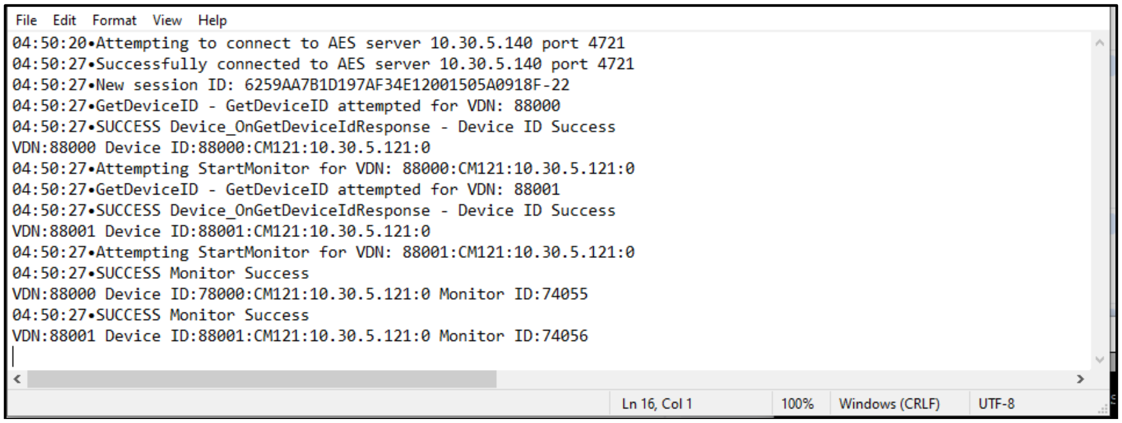
Service Uptime:	13 days, 19 hours 56 minutes
Number of Active Sessions:	1
Number of Sessions Created Since Service Boot:	36
Number of Existing Devices:	2
Number of Devices Created Since Service Boot:	8

■	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
□	DF2C06347347B9DD2 47CD29E2C539346-35	cleric	CCSAvaya	10.103.3.104	XML Unencrypted	2

Item 1-1 of 1
1

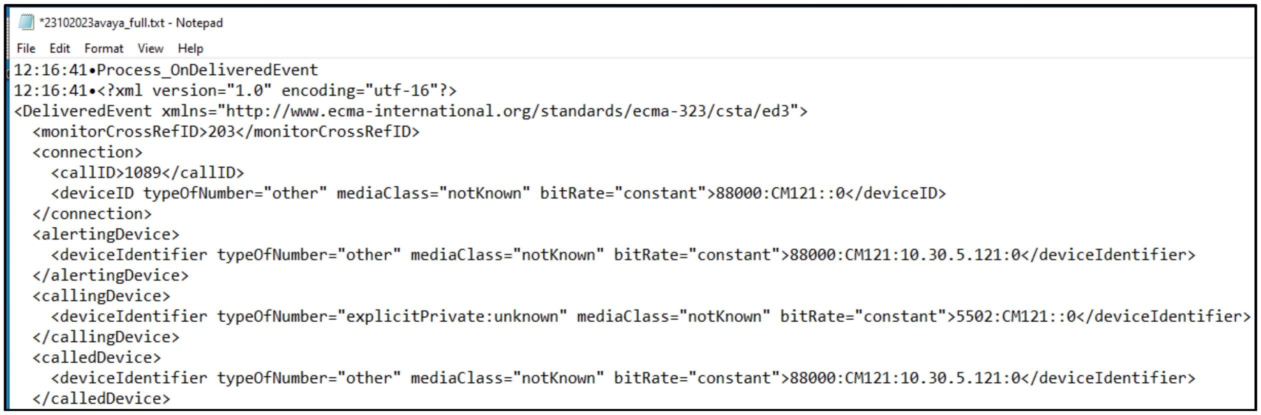
8.5. Verify Cleric Respond-2

On Cleric Respond-2 Server, go to CCSAvaya Logs folder (e.g., C:\CCSAvaya\Logs). Verify that all VDNs are already monitored successfully.



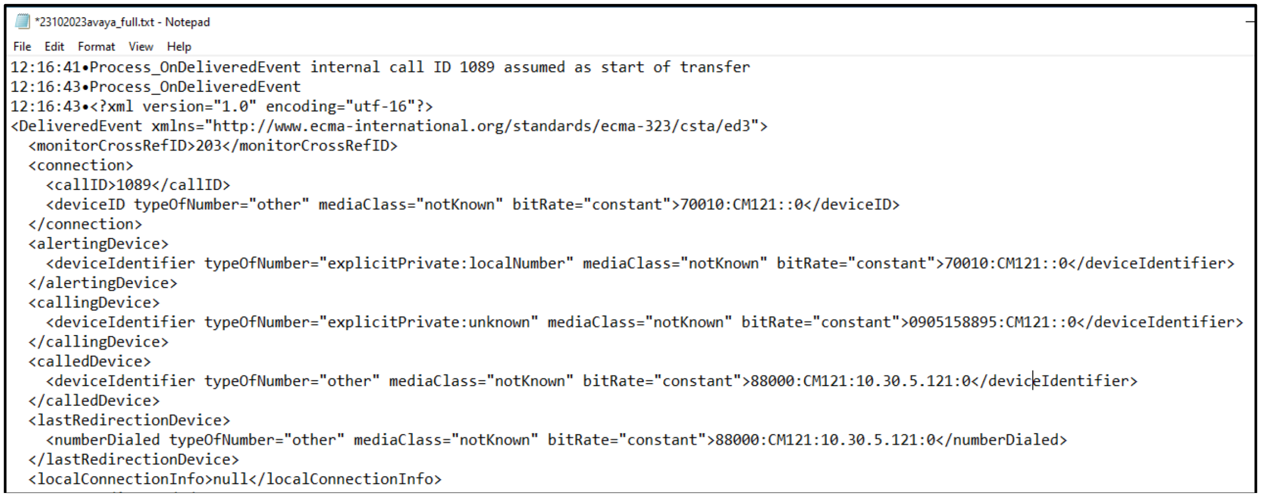
```
04:50:20•Attempting to connect to AES server 10.30.5.140 port 4721
04:50:27•Successfully connected to AES server 10.30.5.140 port 4721
04:50:27•New session ID: 6259AA7B1D197AF34E12001505A0918F-22
04:50:27•GetDeviceID - GetDeviceID attempted for VDN: 88000
04:50:27•SUCCESS Device_OnGetDeviceIdResponse - Device ID Success
VDN:88000 Device ID:88000:CM121:10.30.5.121:0
04:50:27•Attempting StartMonitor for VDN: 88000:CM121:10.30.5.121:0
04:50:27•GetDeviceID - GetDeviceID attempted for VDN: 88001
04:50:27•SUCCESS Device_OnGetDeviceIdResponse - Device ID Success
VDN:88001 Device ID:88001:CM121:10.30.5.121:0
04:50:27•Attempting StartMonitor for VDN: 88001:CM121:10.30.5.121:0
04:50:27•SUCCESS Monitor Success
VDN:88000 Device ID:78000:CM121:10.30.5.121:0 Monitor ID:74055
04:50:27•SUCCESS Monitor Success
VDN:88001 Device ID:88001:CM121:10.30.5.121:0 Monitor ID:74056
```

Make an incoming call to VDN and verify it shows in the CCSAvaya log.



```
12:16:41•Process_OnDeliveredEvent
12:16:41•<?xml version="1.0" encoding="utf-16"?>
<DeliveredEvent xmlns="http://www.ecma-international.org/standards/ecma-323/csta/ed3">
  <monitorCrossRefID>203</monitorCrossRefID>
  <connection>
    <callID>1089</callID>
    <deviceID typeOfNumber="other" mediaClass="notKnown" bitRate="constant">88000:CM121::0</deviceID>
  </connection>
  <alertingDevice>
    <deviceIdentifier typeOfNumber="other" mediaClass="notKnown" bitRate="constant">88000:CM121:10.30.5.121:0</deviceIdentifier>
  </alertingDevice>
  <callingDevice>
    <deviceIdentifier typeOfNumber="explicitPrivate:unknown" mediaClass="notKnown" bitRate="constant">5502:CM121::0</deviceIdentifier>
  </callingDevice>
  <calledDevice>
    <deviceIdentifier typeOfNumber="other" mediaClass="notKnown" bitRate="constant">88000:CM121:10.30.5.121:0</deviceIdentifier>
  </calledDevice>
```

Verify the call transfer to agent 80000 on station 70010.



```
12:16:41•Process_OnDeliveredEvent internal call ID 1089 assumed as start of transfer
12:16:43•Process_OnDeliveredEvent
12:16:43•<?xml version="1.0" encoding="utf-16"?>
<DeliveredEvent xmlns="http://www.ecma-international.org/standards/ecma-323/csta/ed3">
  <monitorCrossRefID>203</monitorCrossRefID>
  <connection>
    <callID>1089</callID>
    <deviceID typeOfNumber="other" mediaClass="notKnown" bitRate="constant">70010:CM121::0</deviceID>
  </connection>
  <alertingDevice>
    <deviceIdentifier typeOfNumber="explicitPrivate:localNumber" mediaClass="notKnown" bitRate="constant">70010:CM121::0</deviceIdentifier>
  </alertingDevice>
  <callingDevice>
    <deviceIdentifier typeOfNumber="explicitPrivate:unknown" mediaClass="notKnown" bitRate="constant">0905158895:CM121::0</deviceIdentifier>
  </callingDevice>
  <calledDevice>
    <deviceIdentifier typeOfNumber="other" mediaClass="notKnown" bitRate="constant">88000:CM121:10.30.5.121:0</deviceIdentifier>
  </calledDevice>
  <lastRedirectionDevice>
    <numberDialed typeOfNumber="other" mediaClass="notKnown" bitRate="constant">88000:CM121:10.30.5.121:0</numberDialed>
  </lastRedirectionDevice>
  <localConnectionInfo>null</localConnectionInfo>
```

9. Conclusion

These Application Notes describe the configuration steps required for Cleric Respond-2 to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. All feature and serviceability test cases were completed successfully**.**

10. Additional References

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

Product documentation for Avaya products may be found at *http://support.avaya.com*.

1. *Administering Avaya Aura® Communication Manager*, Release 10.1.x, Issue 6, June 2023
2. *Administering Avaya Aura® Session Manager*, Release 10.1.x, Issue 6, June 2023
3. *Administering Avaya Aura® System Manager*, Release 10.1.x, Issue 6, June 2023
4. *Administering Avaya Aura® Application Enablement Services*, Release 10.1.x, Issue 9, June 2023

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.