Avaya Solution & Interoperability Test Lab

Application Notes for configuring CaféX Supervisor Assist with Avaya Aura® Communication Manager R6.3 and Avaya Aura® Application Enablement Services R6.3 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for CaféX Supervisor Assist 1.9.0 to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using Device, Media and Call Control (DMCC).

Readers should pay attention to Section 2, in particular the scope of testing as outlined in Section 2.1 as well as the observations noted in Section 2.2, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration steps required for CaféX Supervisor Assist 1.9.0 to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using the Device, Media and Call Control (DMCC) Application Programming Interface (API).

CaféX Supervisor Assist can make contact center agents more effective by providing live coaching during customer calls. From anywhere on any Web browser, supervisors can listen to customer conversations, text chat with agents, see agents' desktops and even highlight or click through sections for enhanced real-time interaction.

This document focuses on integration to Avaya Aura® Application Enablement Services using DMCC. CaféX Supervisor Assist implements DMCC to provide Computer Telephony Integration (CTI) call control and monitoring functionality and application programming interfaces to end user business applications.

DMCC works by allowing software vendors to create soft phones, in memory on a server, and use them to monitor and Service Observe other phones. This is purely a software solution and does not require telephony boards or any wiring beyond a typical network infrastructure. The DMCC API associated with the AES server monitors the digital and VoIP extensions. The application uses the AE Services DMCC service to register itself as a device with the ability to Service Observe at the target extension. When Supervisor Assist joins a call, the application automatically receives the call's aggregated RTP media stream via the recording device and observes the call.

2. General Test Approach and Test Results

The general test approach was to validate the ability of Supervisor Assist to correctly and successfully connect to Application Enablement Services in order to monitor various Communication Manager endpoints using the Communication Manager Service Observe feature.

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.

2.1. Interoperability Compliance Testing

Interoperability compliance testing consisted of using Supervisor Assist to verify successful observation of a variety of calls to endpoints.

- Observing basic calls to and from agent phones.
- Observing Transferred, Conference and Forwarded calls to agent phones.
- Observing basic calls to and from one-X® Agent.
- Observing Transferred, Conference and Forwarded calls to one-X® Agent.
- Serviceability testing, by simulation LAN failures for various devices in the solution.

2.2. Test Results

Almost all test cases were executed successfully. The following issues were observed.

1. While observing an agent phone, a call is transferred into the agent phone. Once the transfer has been completed, the Service Observe drops and the agent shows as "Idle". This issue does not happen when transferring from a H323 phone into a SIP phone.
2. While observing a one-X® Agent when making a Supervised Transfer out to another VDN or extension. Once the Supervised Transfer has been completed the Service Observe drops and the agent shows as "Idle". There is no issue when using Blind Transfer.

2.3. Support

For technical support on CaféX Supervisor Assist products, please visit the website at http://www.cafex.com/ or contact an authorized CaféX representative at info@cafex.com.

3. Reference Configuration

Figure 1 below shows Avaya Aura® Communication Manager R6.3, serving both SIP and H.323 endpoints with an Avaya G450 Media Gateway and an Avaya Aura® Application Enablement Services R6.3 hosted on VMware providing a DMCC interface to which the CaféX Supervisor Assist application connects. Avaya Aura® Session Manager R6.3 provides the point of registration for Avaya SIP endpoints. Avaya Aura® System Manager Server provides a means to manage and configure Session Manager. All of these applications were hosted on VMware ESXi 5.5 infrastructure.

The agent PC's run the CaféX Agent software and the supervisor PC runs the CaféX Supervisor software. This software is run from the CaféX Supervisor Assist sever as shown below.

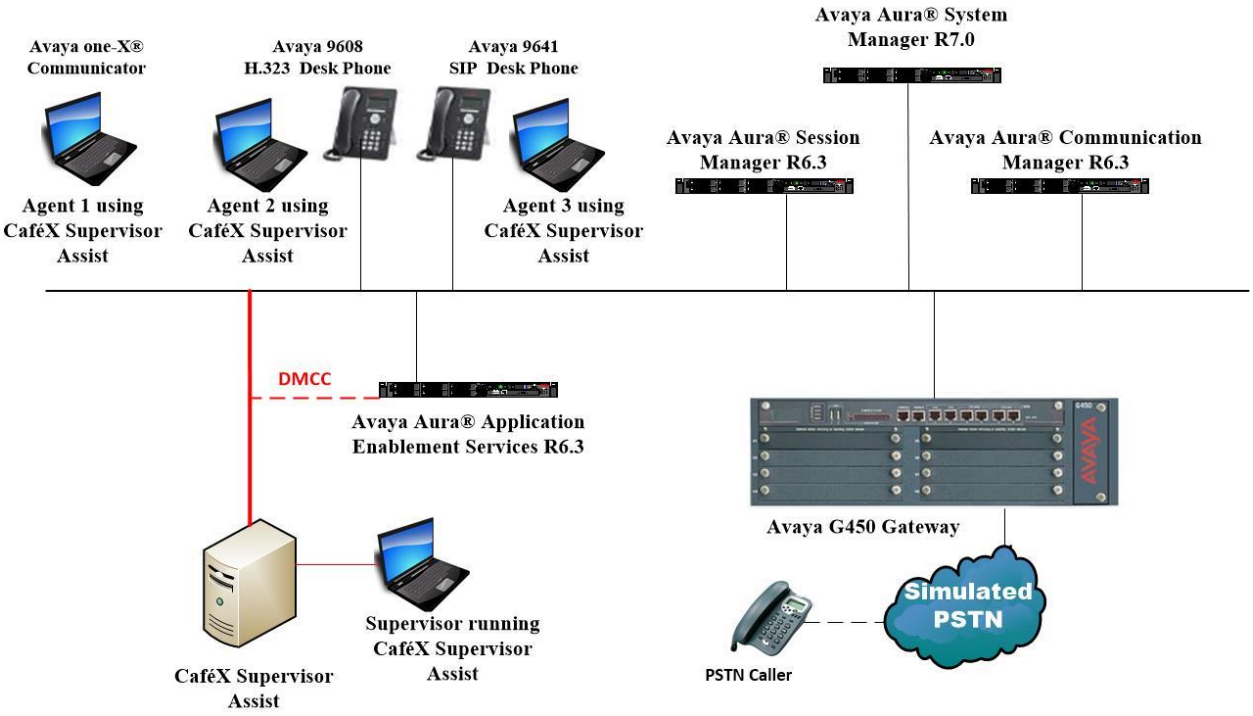


Figure 1: Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services with CaféX Supervisor Assist solution

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya Aura® System Manager running on a virtual server	System Manager 7.0.1.0 Build No. - 7.0.0.0.16266 Software Update Revision No: 7.0.1.0.064859 Feature Pack 1
Avaya Aura® Communication Manager running on a virtual server	R6.3 R016x.03.0.124.0 03.0.124.0-22038
Avaya Aura® Application Enablement Services running on a virtual server	R6.3 SP3 Build No – 6.3.3.3.10-0
Avaya Aura® Session Manager running on a virtual server	Session Manager R 6.3 SP14 Build No. – 6.3.14.0.631402
Avaya G450 Gateway	37.19.0 /1
Avaya 9608 H323 Deskphone	96x1 H323 Release 6.6.028
Avaya 9608 SIP Deskphone	96x1 SIP Release 7.0.0.39
Avaya one-X® Agent	2.5
CaféX Supervisor Assist	1.9.0

5. Configure Avaya Aura® Communication Manager

The configuration and verification operations illustrated in this section are performed using the Communication Manager System Access Terminal (SAT). The information provided in this section describes the configuration of Communication Manager for this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation as referenced in **Section 10**. The configuration operations described in this section can be summarized as follows:

- Configure Interface to Avaya Aura® Application Enablement Services.
- Configure Class of Restriction.
- Configure Existing Agent Extensions.
- Configure DMCC Stations.

5.1. Configure Interface to Avaya Aura® Application Enablement Services

The following sections illustrate the steps required to create a link between Communication Manager and Application Enablement Services.

5.1.1. Verify System Features

Use the **display system-parameters customer-options** command to verify that Communication Manager has permissions for features illustrated in these Application Notes. On **Page 3**, ensure that **Computer Telephony Adjunct Links?** is set to **y** as shown below.

```
display system-parameters customer-options                    Page   3 of  11
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? y          Audible Message Waiting? y
        Access Security Gateway (ASG)? n              Authorization Codes? y
        Analog Trunk Incoming Call ID? y                      CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? y                        CAS Main? n
Answer Supervision by Call Classifier? y                 Change COR by FAC? n
                                ARS? y  Computer Telephony Adjunct Links? y
                ARS/AAR Partitioning? y  Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? y                      DCS (Basic)? y
          ASAI Link Core Capabilities? n                DCS Call Coverage? y
          ASAI Link Plus Capabilities? n               DCS with Rerouting? y
       Async. Transfer Mode (ATM) PNC? n
  Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? y
              ATM WAN Spare Processor? n                          DS1 MSP? y
                                ATMS? y            DS1 Echo Cancellation? y
                  Attendant Vectoring? y
```

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

Display the procr IP address by using the command **display node-names ip** and noting the IP address for the **procr** and AES (**aes63vmpg**).

```
display node-names ip                                          Page   1 of   2
                                  IP NODE NAMES
    Name                 IP Address
SM100                  10.10.40.12
aes63vmpg              10.10.40.30
default                0.0.0.0
G450                   10.10.40.15
procr                  10.10.40.13
```

5.1.3. Configure Transport Link for Avaya Aura® Application Enablement Services Connectivity

To administer the transport link to AES use the **change ip-services** command. On **Page 1** add an entry with the following values:

- **Service Type:** Should be set to **AESVCS**.
- **Enabled:** Set to **y**.
- **Local Node:** Set to the node name assigned for the procr in **Section 5.1.2**.
- **Local Port:** Retain the default value of **8765**.

```
change ip-services                                             Page   1 of   4

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

Go to **Page 4** of the **ip-services** form and enter the following values:

- **AE Services Server:** Name obtained from the AES server, in this case **aes70vmpg**.
- **Password:** Enter a password to be administered on the AES server.
- **Enabled:** Set to **y**.

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

```
change ip-services                                             Page   4 of   4
                           AE Services Administration

   Server ID    AE Services       Password          Enabled    Status
                   Server
      1:        aes63vmpg         ********          y          idle
      2:
      3:
```

5.1.4. Configure CTI Link for TSAPI Service

Add a CTI link using the **add cti-link n** command, where n is the n is the cti-link number as shown in the example below this is **1**. Enter an available extension number in the **Extension** field. Enter **ADJ-IP** in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

```
add cti-link 1                                                Page   1 of   3
                                    CTI LINK
 CTI Link: 1
Extension: 7999
     Type: ADJ-IP
                                                                      COR: 1
     Name: aes63vmpg
```

5.2. Configure Class of Restriction

The Class of Restriction must allow **Can be Service Observed** and **Can be Service Observer** to allow Supervisor Assist to work. Type **change cor X** where X is the class of service to be changed. Ensure that **Can be Service Observed** and **Can be Service Observer** are both set to **y** as shown below. This COR will then be assigned to all the agents and supervisors using Supervisor Assist.

```
change cor 1                                                  Page   1 of  23
                             CLASS OF RESTRICTION

               COR Number: 1
          COR Description: Default_PG

                      FRL: 0                                  APLT? y
  Can Be Service Observed? y            Calling Party Restriction: none
Can Be A Service Observer? y             Called Party Restriction: none
        Time of Day Chart: 1         Forced Entry of Account Codes? n
         Priority Queuing? n                  Direct Agent Calling? y
     Restriction Override: none         Facility Access Trunk Test? n
     Restricted Call List? n                   Can Change Coverage? n

            Access to MCT? y              Fully Restricted Service? n
Group II Category For MFC: 7              Hear VDN of Origin Annc.? n
         Send ANI for MFE? n               Add/Remove Agent Skills? n
            MF ANI Prefix:                Automatic Charge Display? n
Hear System Music on Hold? y   PASTE (Display PBX Data on Phone)? n
                         Can Be Picked Up By Directed Call Pickup? y
                                      Can Use Directed Call Pickup? y
                                      Group Controlled Restriction: inactive
```

5.3. Configure Existing Agent Extensions

Each agent that is to be monitored must have the Class of Restriction (COR) set to that in **Section 5.2**. Type **change station X**, where X is the station that needs to be changed. Ensure that the **COR** is set to that created in **Section 5.2**.

```
change station 2016                                          Page   1 of   5
                                    STATION

Extension: 2016                          Lock Messages? n               BCC: 0
     Type: 9608                          Security Code: 1234             TN: 1
     Port: S00000                      Coverage Path 1:                 COR: 1
     Name: EXT7000                     Coverage Path 2:                 COS: 1
                                       Hunt-to Station:               Tests? y
STATION OPTIONS
                                            Time of Day Lock Table:
              Loss Group: 19          Personalized Ringing Pattern: 1
                                                  Message Lamp Ext: 7000
           Speakerphone: 2-way                 Mute Button Enabled? y
         Display Language: english                  Button Modules: 0
 Survivable GK Node Name:
          Survivable COR: internal                Media Complex Ext:
   Survivable Trunk Dest? y                            IP SoftPhone? y
                                                 IP Video Softphone? n
                                Short/Prefixed Registration Allowed: yes
                                                 Customizable Labels? Y
```

5.4. Configure DMCC Stations

A DMCC station must be created with a Service Observe button; this will be used by the Supervisor Assist application to observe various agents. Use the command, add station x, where x is the extension number of the station to be added. In the example below used for compliance testing, a **9640** type station was added. Ensure that the **COR** is set to that configured in **Section 5.2**.

```
add station 28800                                            Page   1 of   5
                                    STATION

Extension: 28800                         Lock Messages? n               BCC: 0
     Type: 9640                          Security Code: 1234             TN: 1
     Port: S00123                      Coverage Path 1:                 COR: 1
     Name: cafexDMCC1                  Coverage Path 2:                 COS: 1
                                       Hunt-to Station:               Tests? y
STATION OPTIONS
               Location:                     Time of Day Lock Table:
              Loss Group: 19          Personalized Ringing Pattern: 1
                                                  Message Lamp Ext: 28800
           Speakerphone: 2-way                 Mute Button Enabled? y
         Display Language: english                  Button Modules: 0
 Survivable GK Node Name:
          Survivable COR: internal                Media Complex Ext:
   Survivable Trunk Dest? y                            IP SoftPhone? y

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

Data Restriction is set to **n**, there are no other specific changes required on **Page 2**, these are the default values.

```
add station 28800                                          Page   2 of   5
                                    STATION
FEATURE OPTIONS
           LWC Reception: spe              Auto Select Any Idle Appearance? n
         LWC Activation? y                           Coverage Msg Retrieval? y
  LWC Log External Calls? n                                  Auto Answer: none
            CDR Privacy? n                              Data Restriction? n
   Redirect Notification? y                     Idle Appearance Preference? n
 Per Button Ring Control? n                   Bridged Idle Line Preference? n
   Bridged Call Alerting? n                       Restrict Last Appearance? y
  Active Station Ringing: single
                                                        EMU Login Allowed? n
       H.320 Conversion? n          Per Station CPN - Send Calling Number?
      Service Link Mode: as-needed                     EC500 State: enabled
        Multimedia Mode: enhanced                  Audible Message Waiting? n
    MWI Served User Type:                        Display Client Redirection? n
             AUDIX Name:                        Select Last Used Appearance? n
                                                  Coverage After Forwarding? s
                                                    Multimedia Early Answer? n
 Remote Softphone Emergency Calls: as-on-local Direct IP-IP Audio Connections? y
  Emergency Location Ext: 28800         Always Use? n IP Audio Hairpinning? n
```

There are no specific changes required on **Page 3**, these are the default values.

```
add station 28800                                          Page   3 of   5
                                    STATION

             Conf/Trans on Primary Appearance? n
   Bridged Appearance Origination Restriction? n    Offline Call Logging? y


               Call Appearance Display Format: disp-param-default
                            IP Phone Group ID:
Enhanced Callr-Info Display for 1-Line Phones? n

                              ENHANCED CALL FORWARDING
                                    Forwarded Destination         Active
 Unconditional For Internal Calls To:                                n
                   External Calls To:                                n
          Busy For Internal Calls To:                                n
                   External Calls To:                                n
      No Reply For Internal Calls To:                                n
                   External Calls To:                                n

            SAC/CF Override: n
```

On **Page 4** a Service Observe button needs to be added. This is done below by changing button **4** to **serv-obsrv**. Note that any button will work here, button 4 was chosen for compliance testing.

```
add station 28800                                          Page   4 of   5
                                    STATION
 SITE DATA
      Room:                                            Headset? n
      Jack:                                            Speaker? n
     Cable:                                           Mounting: d
     Floor:                                       Cord Length: 0
   Building:                                        Set Color:

ABBREVIATED DIALING
     List1:                    List2:                    List3:




BUTTON ASSIGNMENTS
 1: call-appr                          5:
 2: call-appr                          6:
 3: call-appr                          7:
 4: serv-obsrv                         8:

    voice-mail
```

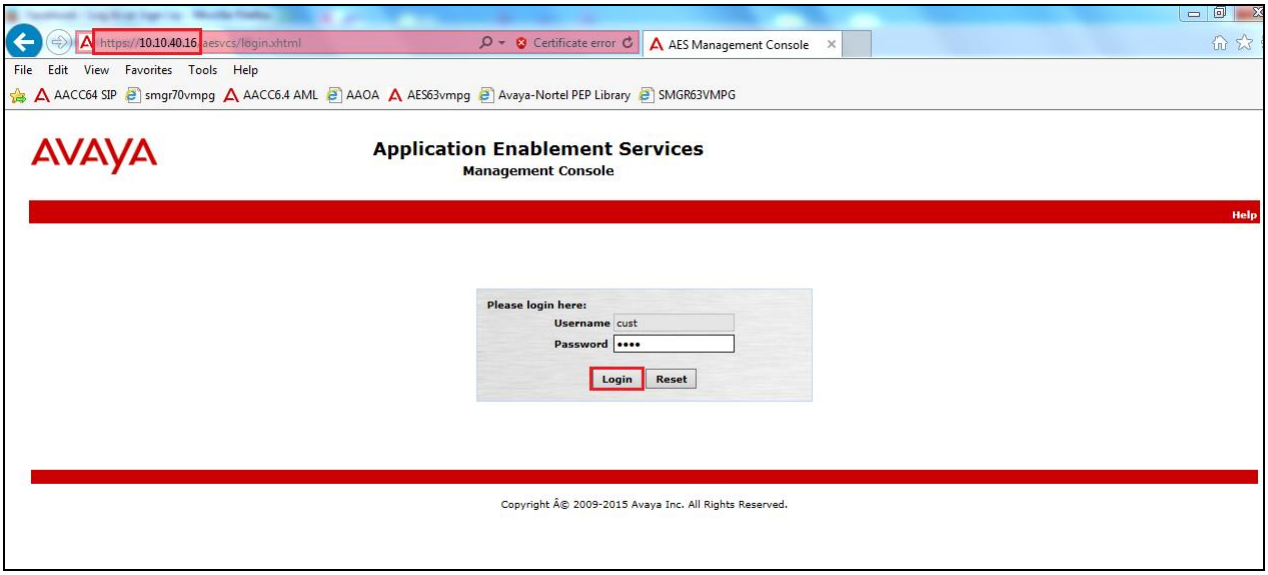
6. Configure Avaya Aura® Application Enablement Services

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

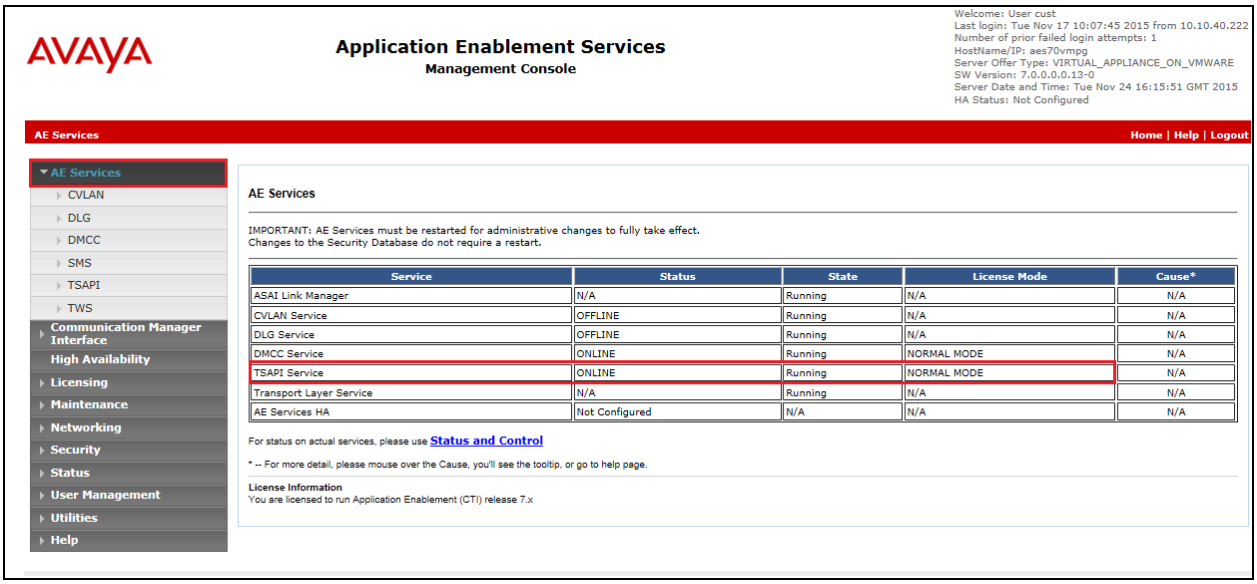
- Verify Licensing.
- Create Switch Connection.
- Administer TSAPI link.
- Enable TSAPI & DMCC Ports.
- Create CTI User.
- Associate Devices with CTI User.

6.1. Verify Licensing

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

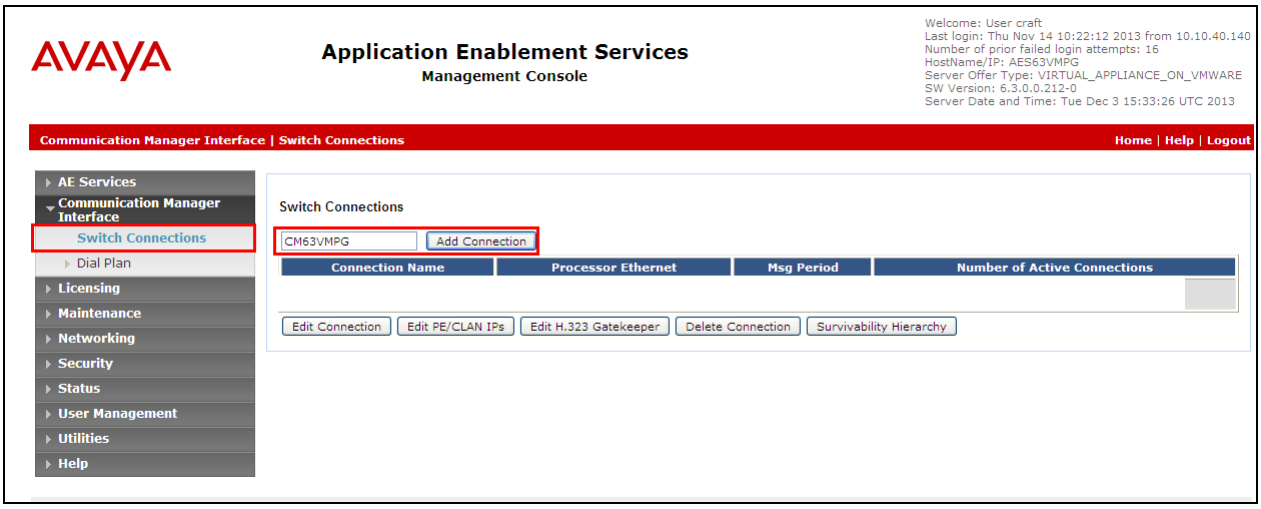


The Application Enablement Services Management Console appears displaying the **Welcome to OAM** screen (not shown). Select **AE Services** and verify that the TSAPI Service is licensed by ensuring that **TSAPI Service** is in the list of **Services** and that the **License Mode** is showing **NORMAL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

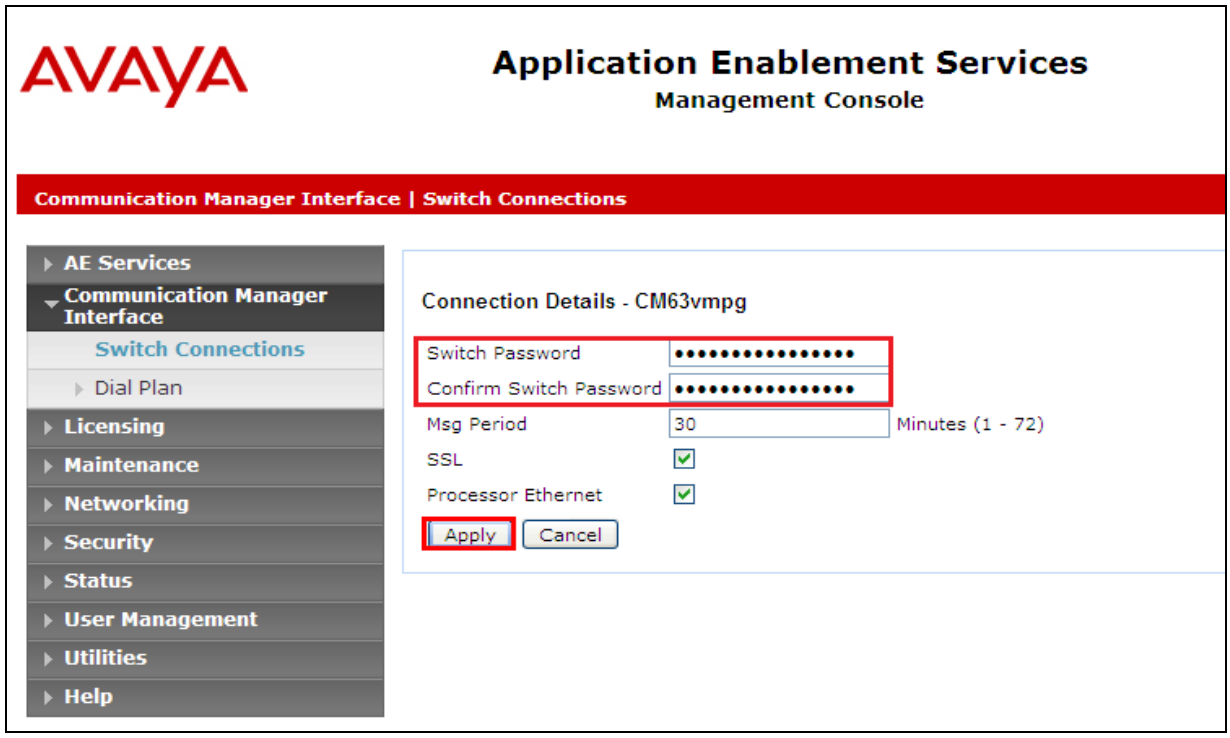


6.2. Create Switch Connection

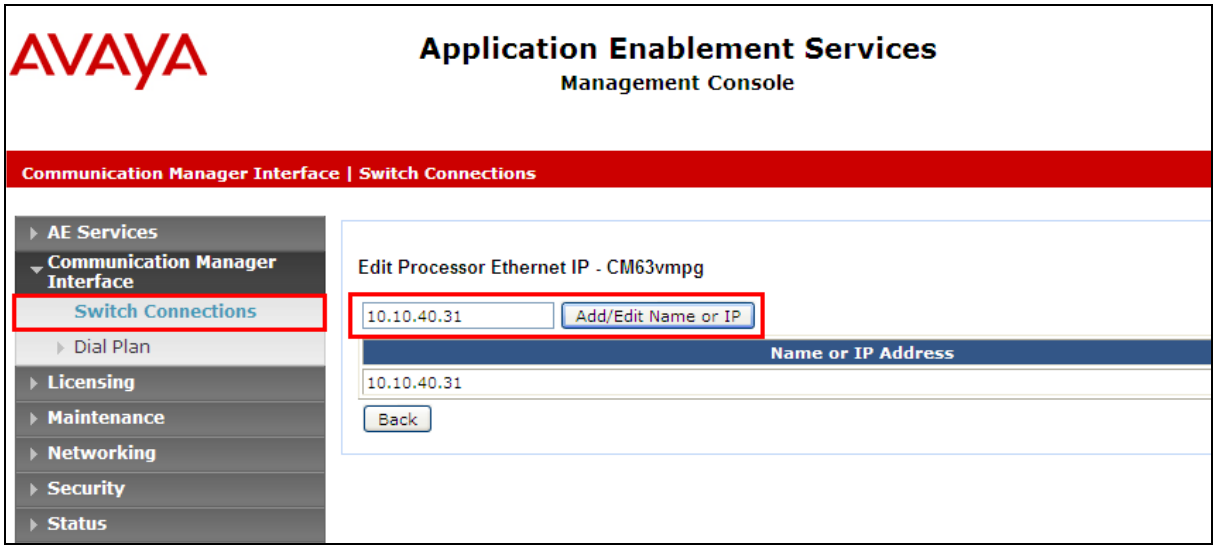
From the AES Management Console navigate to **Communication Manager Interface** → **Switch Connections** to set up a switch connection. Enter a name for the Switch Connection to be added and click the **Add Connection** button.



In the resulting screen enter the **Switch Password**; the Switch Password must be the same as that entered into Communication Manager AE Services Administration screen via the **change ip-services** command, described in **Section 5.1.3**. The remaining fields should show as below. Click **Apply** to save changes.

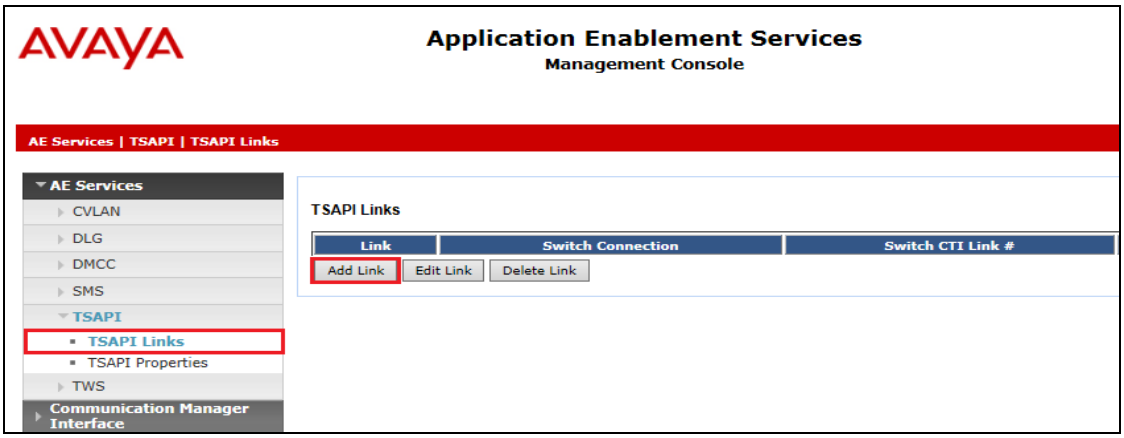


From the **Switch Connections** screen, select the radio button for the recently added switch connection and select the **Edit PE/CLAN IPs** button (not shown, see screen at the bottom of the previous page. In the resulting screen, enter the IP address of the procr as shown in **Section 5.1.2** that will be used for the AES connection and select the **Add/Edit Name or IP** button.



6.3. Administer TSAPI link

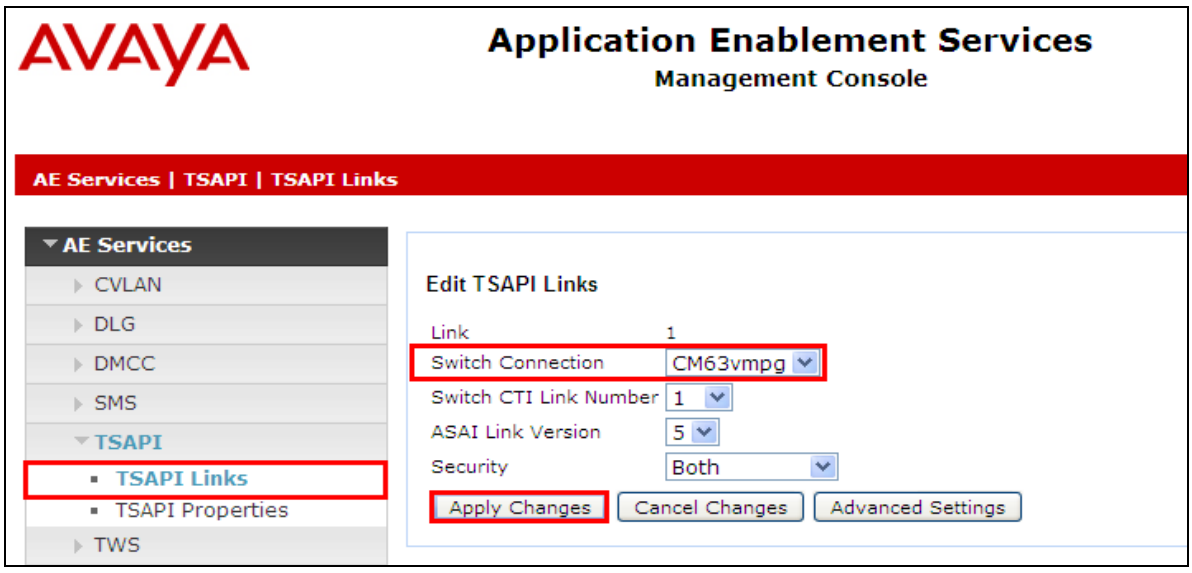
From the Application Enablement Services Management Console, select **AE Services → TSAPI → TSAPI Links**. Select **Add Link** button as shown in the screen below.



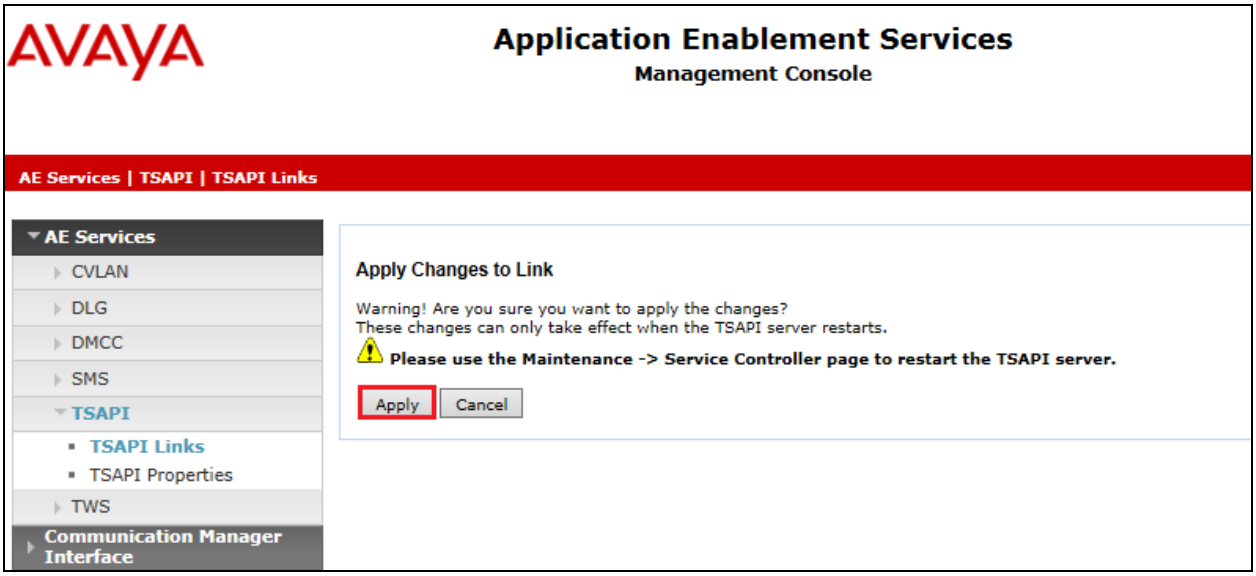
On the **Add TSAPI Links** screen (or the **Edit TSAPI Links** screen to edit a previously configured TSAPI Link as shown below), enter the following values:

- **Link:** Use the drop-down list to select an unused link number.
- **Switch Connection:** Choose the switch connection **cm63vmpg**, which has already been configured in **Section 6.2** from the drop-down list.
- **Switch CTI Link Number:** Corresponding CTI link number configured in **Section 5.1.4** which is **1**.
- **ASAI Link Version:** This can be left at the default value of **5**.
- **Security:** This can be left at the default value of **both**.

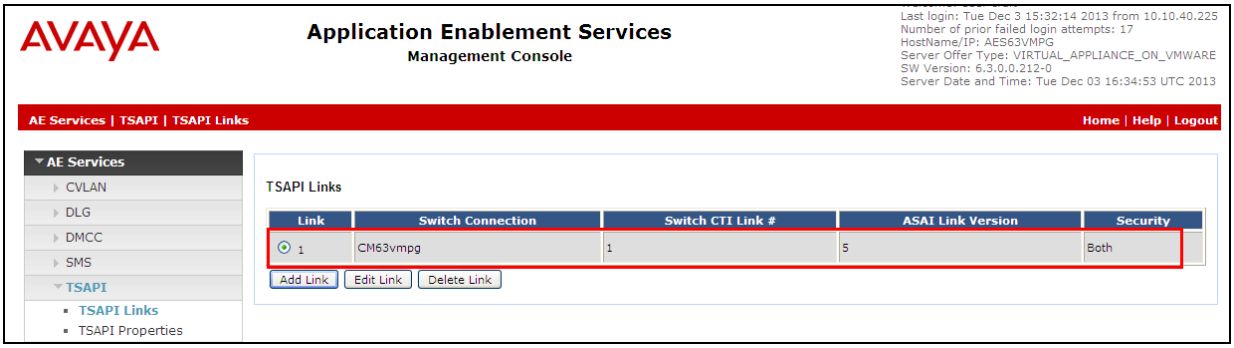
Once completed, select **Apply Changes**.



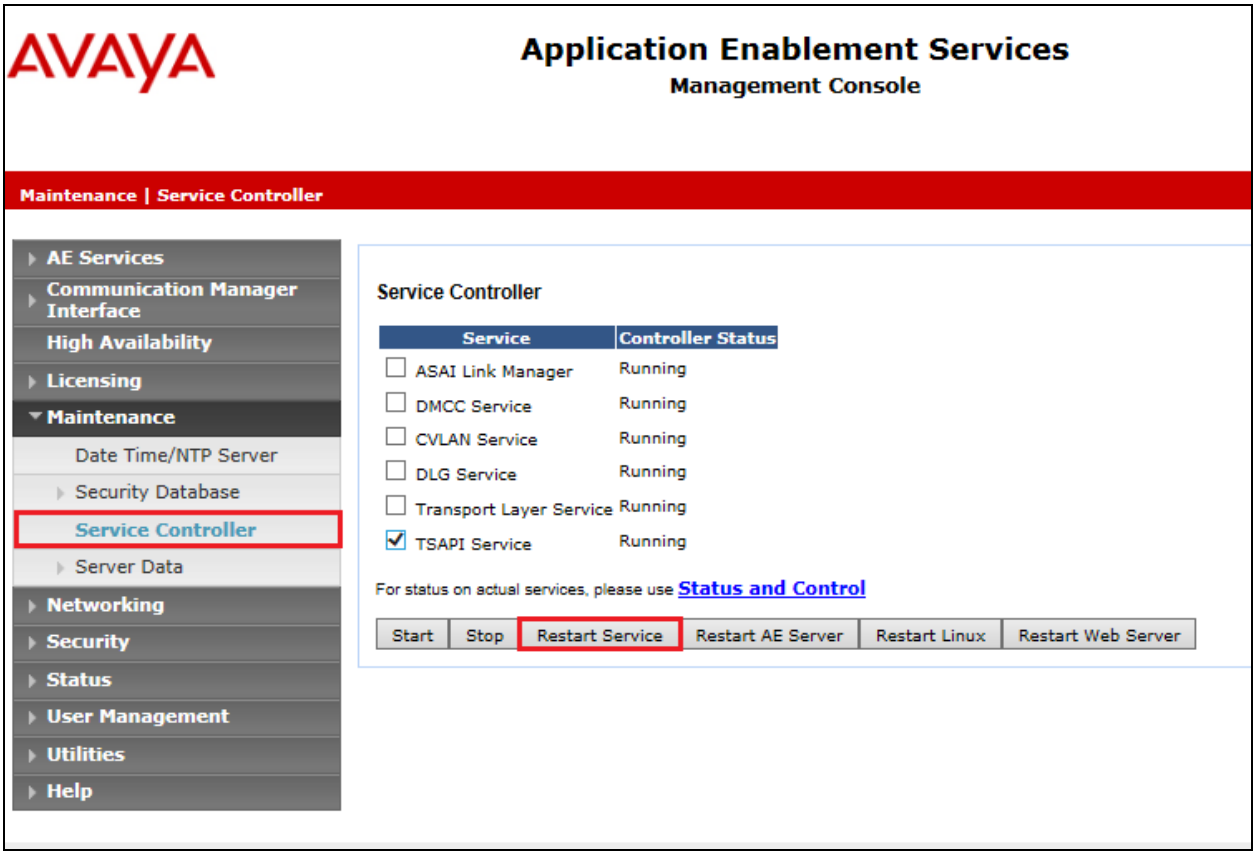
Another screen appears for confirmation of the changes made. Choose **Apply**.



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

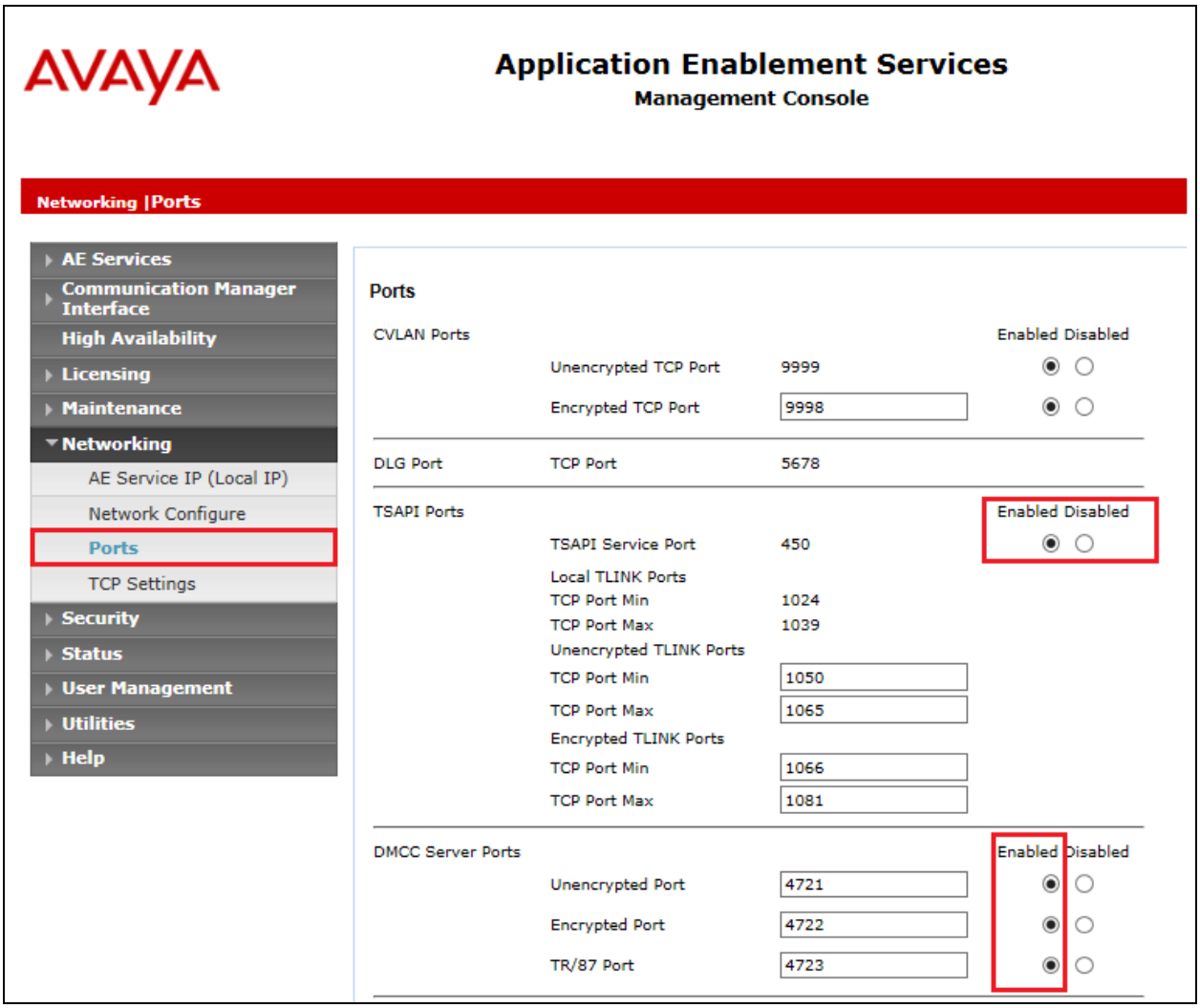


The TSAPI Service must be restarted to effect the changes made in this section. From the Management Console menu, navigate to **Maintenance → Service Controller**. On the Service Controller screen, tick the **TSAPI Service** and select **Restart Service**.



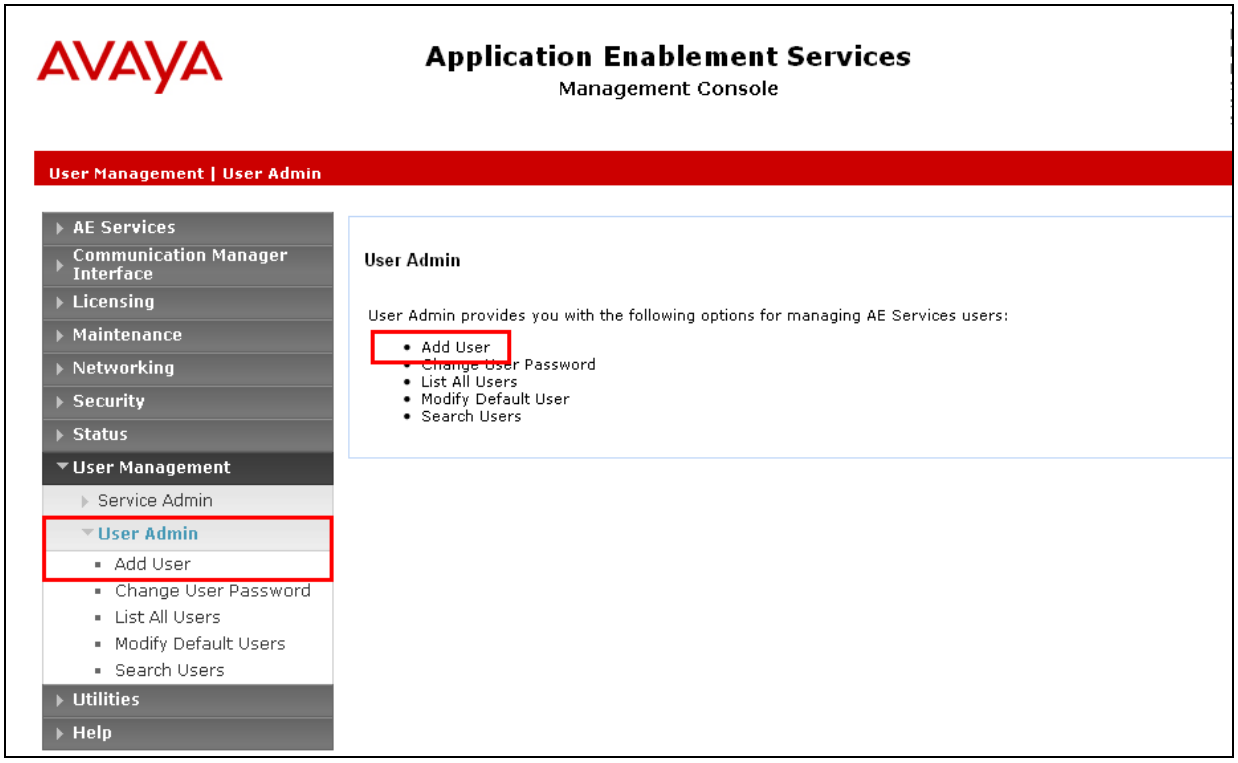
6.4. Enable DMCC and TSAPI Ports

To ensure that TSAPI ports are enabled, navigate to **Networking → Ports**. Ensure that the both the DMCC TSAPI ports are set to **Enabled** as shown below.



6.5. Create CTI User

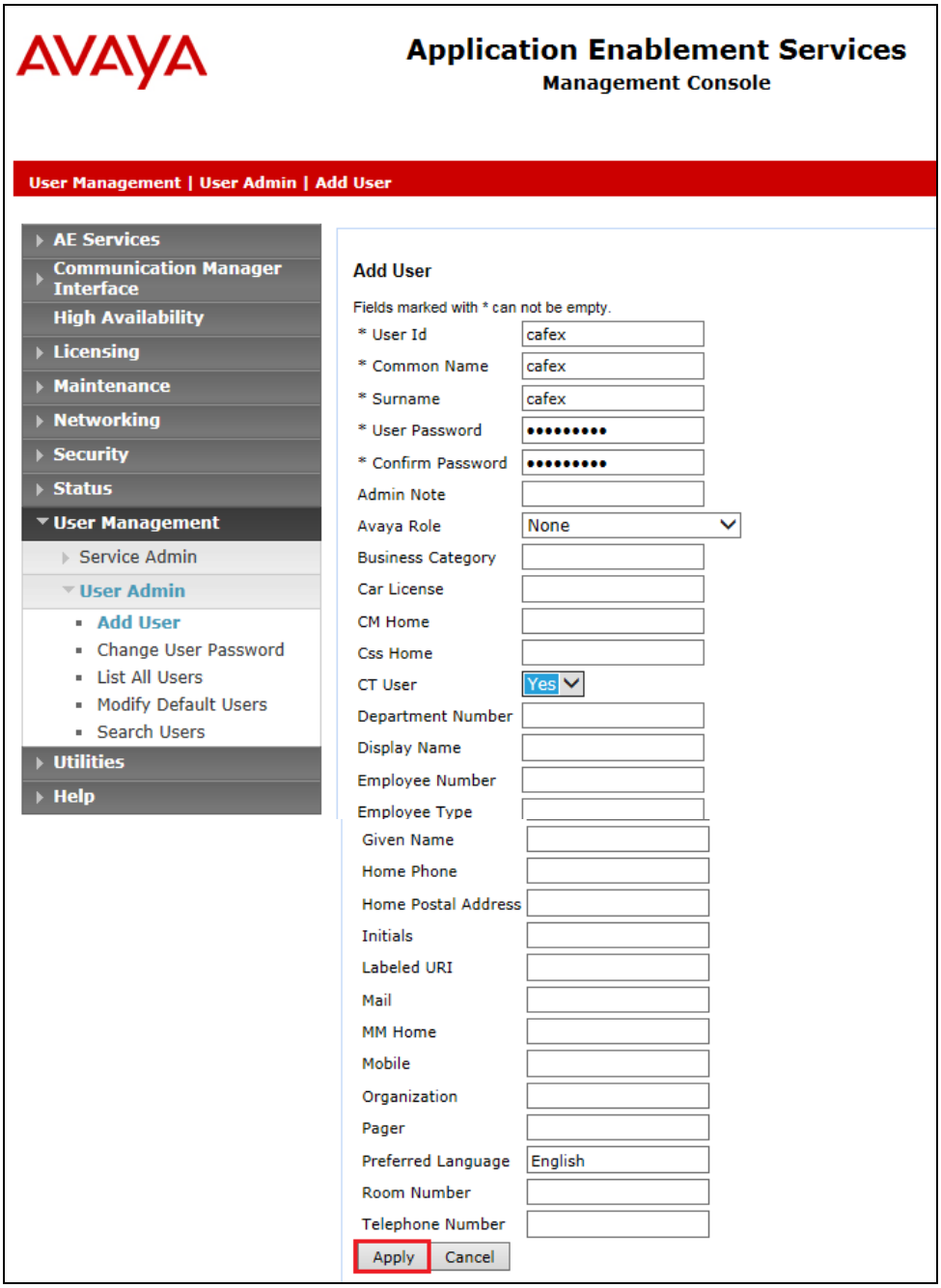
A user ID and password needs to be configured for the Supervisor Assist application to communicate with the Application Enablement Services server. Navigate to the **User Management → User Admin** screen then choose the **Add User** option.



In the **Add User** screen shown below, enter the following values:

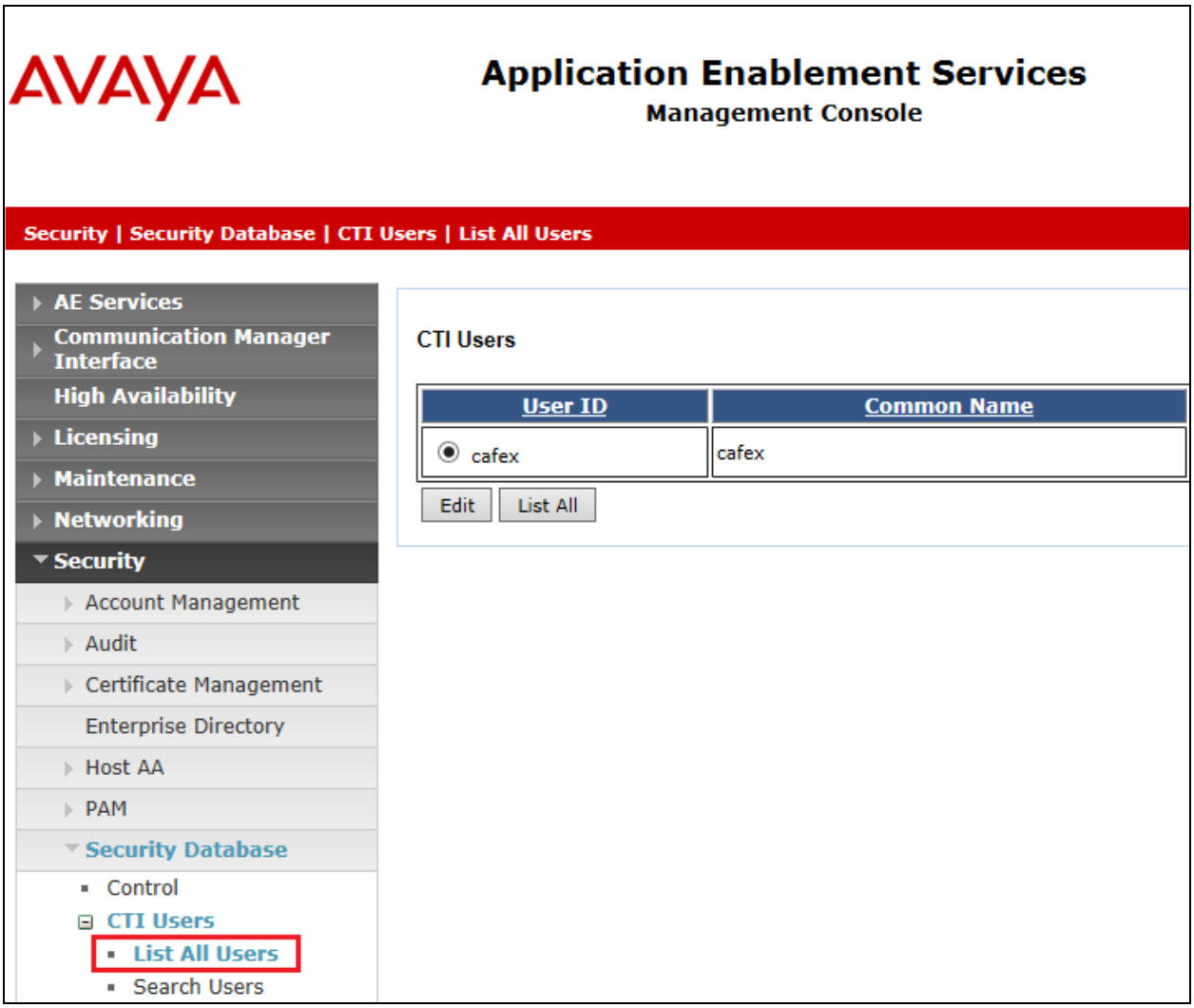
- **User Id** - This will be used by the Supervisor Assist setup in **Section 7.2**.
- **Common Name** and **Surname** - Descriptive names need to be entered.
- **User Password** and **Confirm Password** - This will be used with Supervisor Assist setup in **Section 7.2**.
- **CT User** - Select **Yes** from the drop-down menu.

Click on **Apply Changes** at the bottom of the screen.

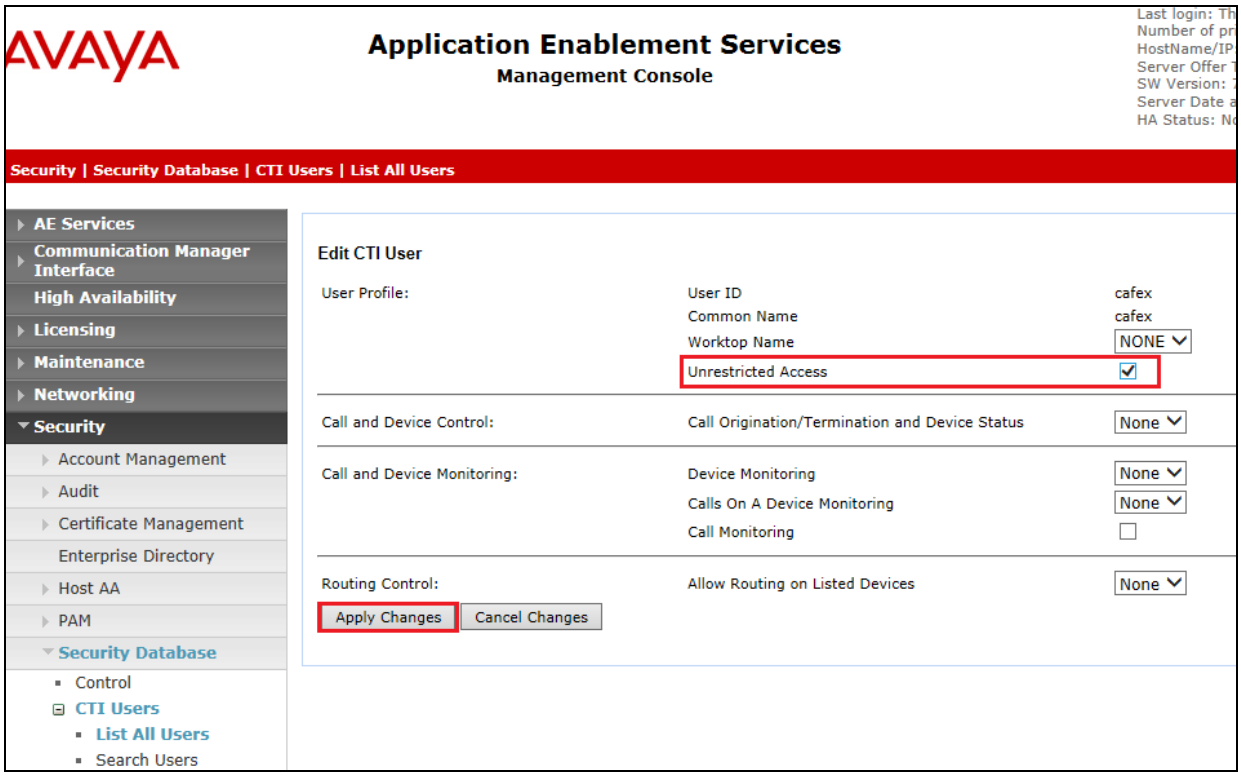


6.6. Associate Devices with CTI User

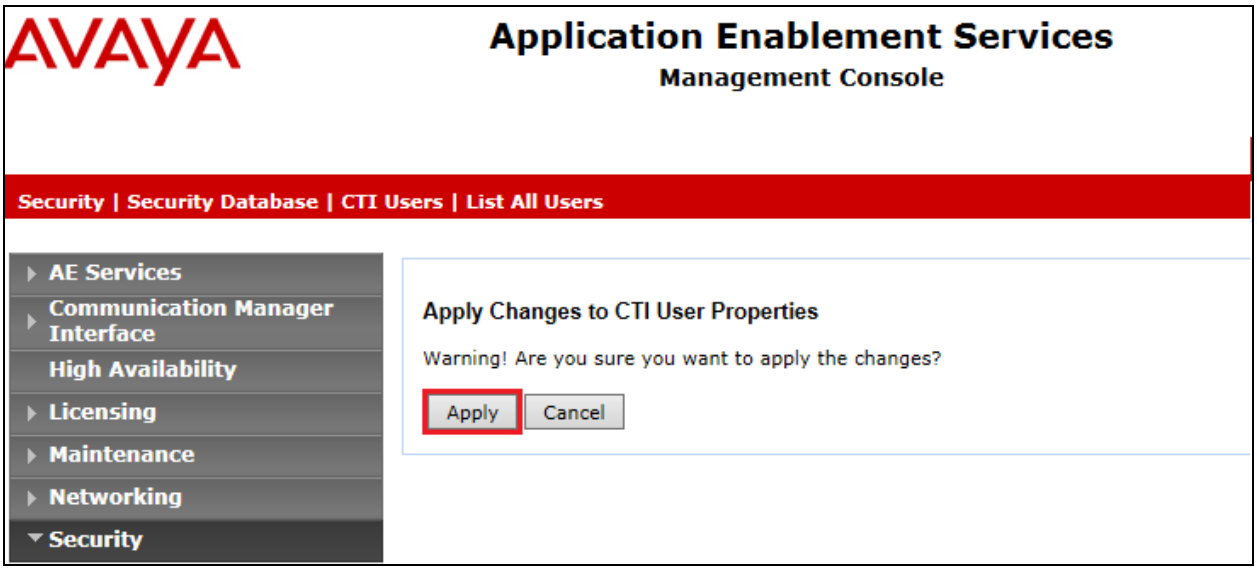
Navigate to **Security → Security Database → CTI Users → List All Users**. Select the CTI user added in **Section 6.5** and click on **Edit**.



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



Click on **Apply** when asked again to **Apply Changes**.



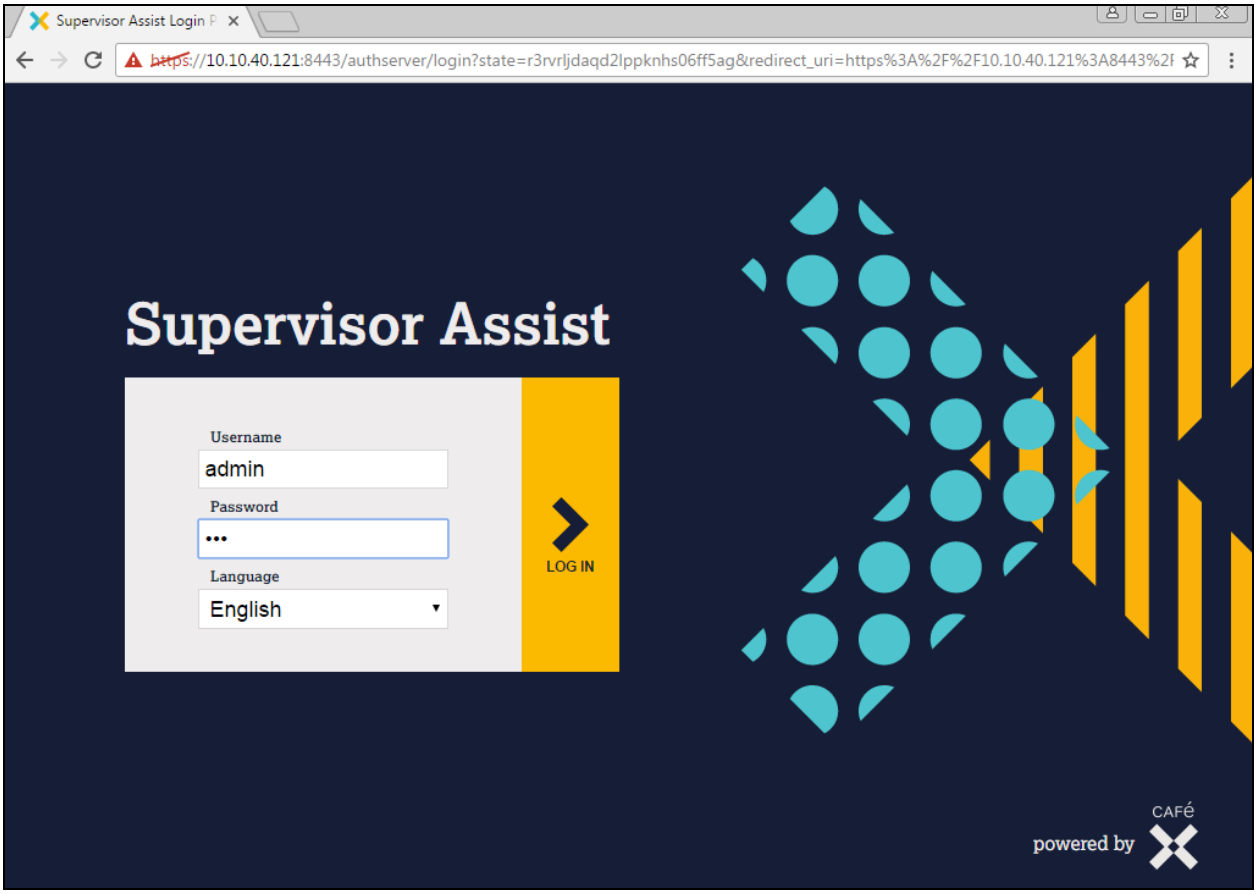
7. Configure CaféX Supervisor Assist

This section provides the procedures for configuring Supervisor Assist. The procedures include the following areas:

- Launch configuration program.
- Administer link to AES.

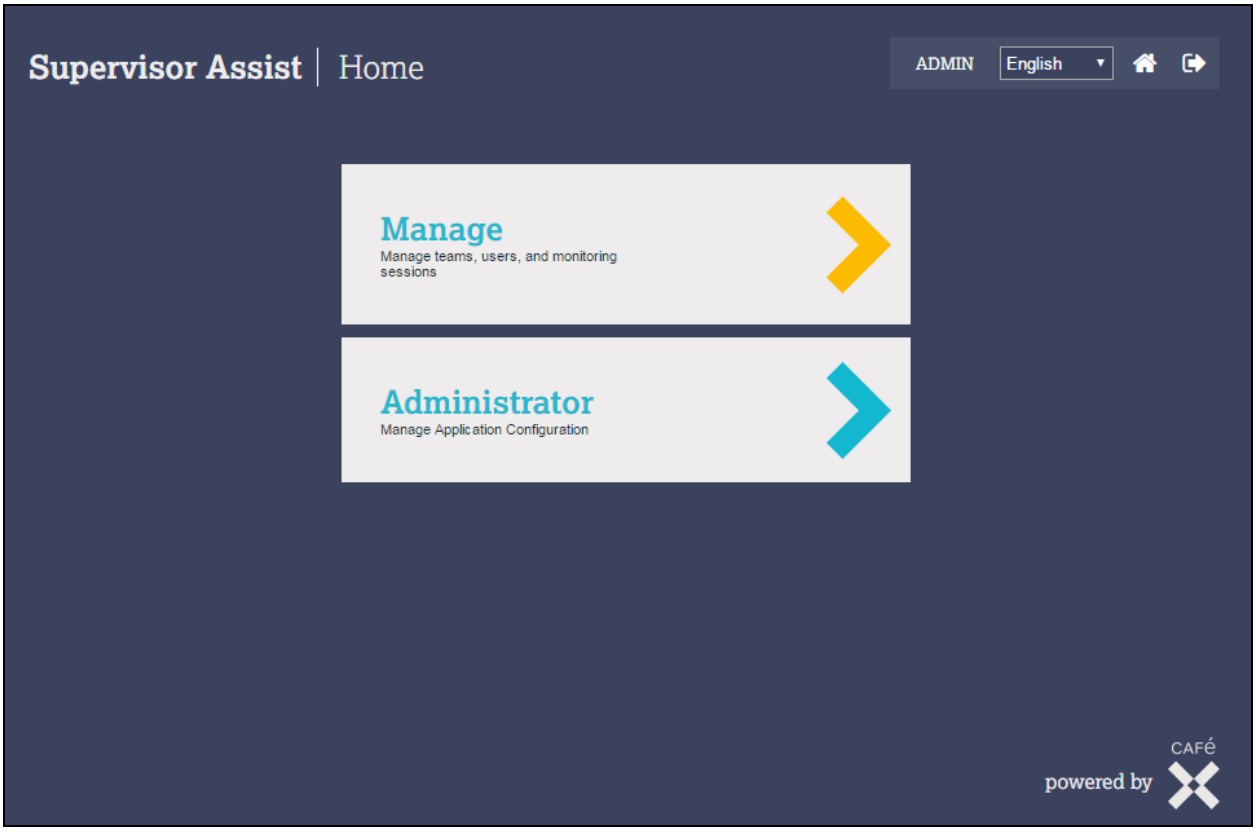
7.1. Launch configuration program

Supervisor Assist uses a GUI based configuration program to configure the DMCC connection between the Supervisor Assist server and Application Enablement Services. From the Supervisor Assist server, launch the configuration program by opening the Chrome web browser to **https://<Server IP>:8443/sa**. This will open the window as shown below, enter the appropriate credentials and click on **LOG IN**.

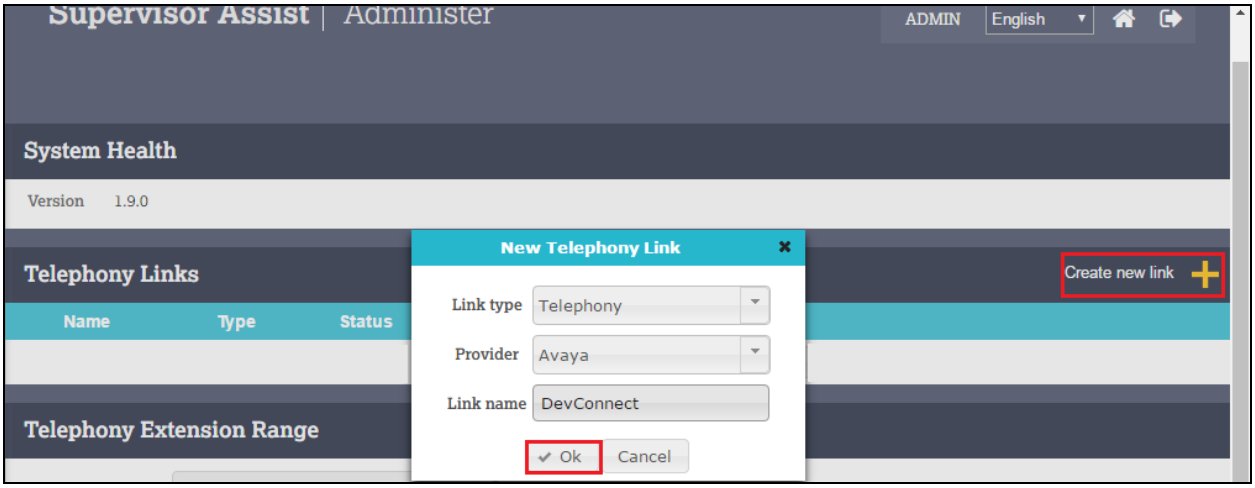


7.2. Administer Link to AES

The **Supervisor Assist Home** screen is displayed, click on **Administrator**.

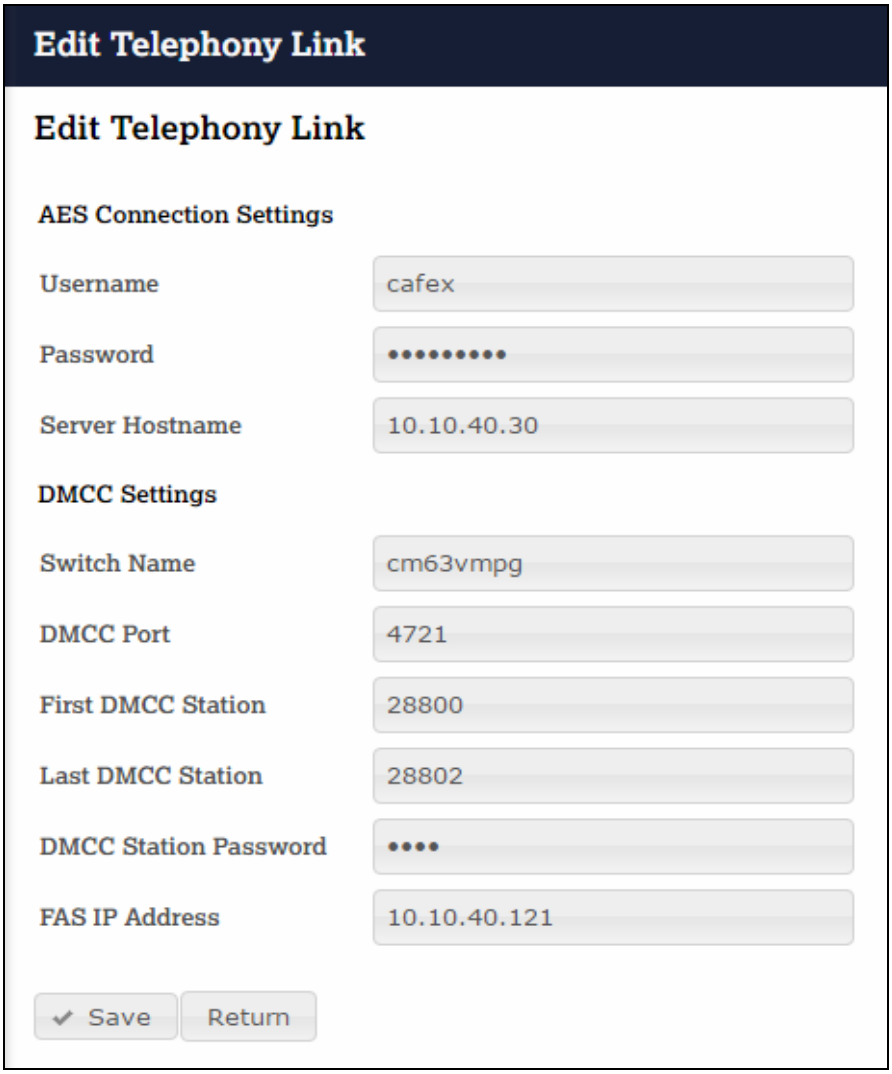


Click on **Create new link**. A new window opens where the Link type, Provider and Link name are chosen. Fill in the details as shown below where the **Link type** is **Telephony**, the **Provider** is **Avaya** and a suitable name is given for the **Link name**.

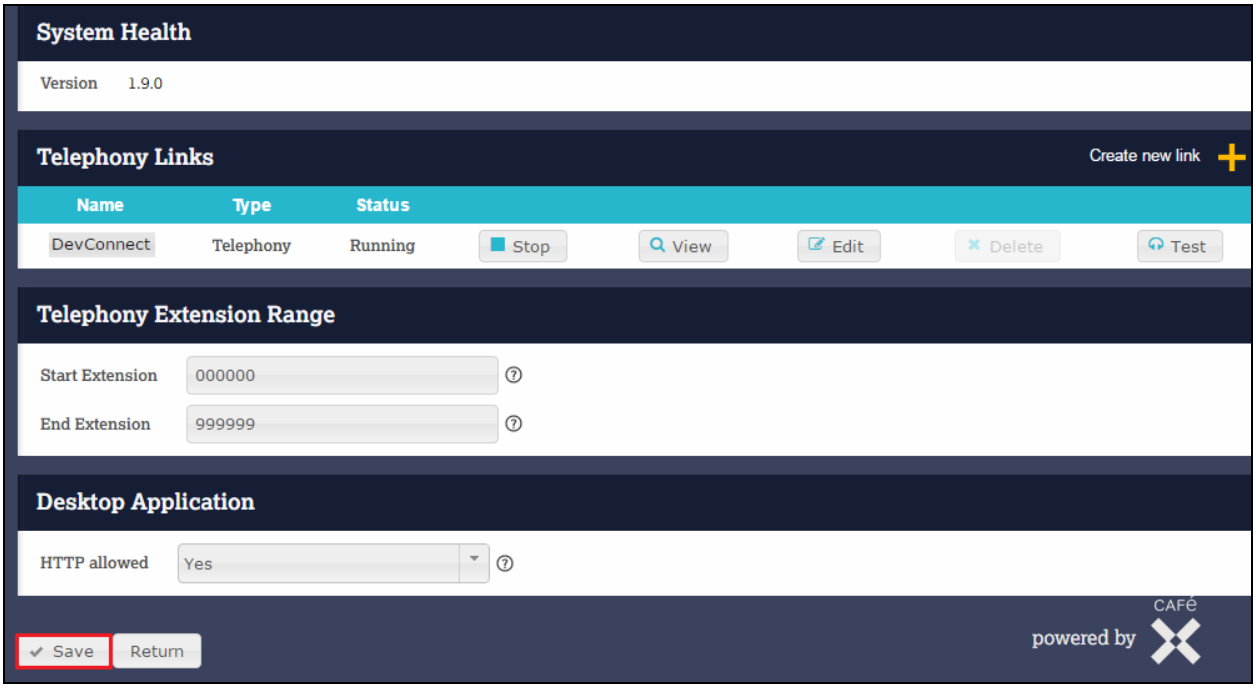


Enter the following values for the specified fields, and retain the default values in the remaining fields. Click **Save** when done.

- **Username -** enter the CT User configured in **Section 6.5**.
- **Password -** enter CT User **Password** configured in **Section 6.5**.
- **Server Hostname** – enter the IP address of Application Enablement Services, in this case **10.10.40.30**.
- **Switch Name -** enter the Communication Manager switch name obtained in **Section 6.2**.
- **DMCC Port** – enter the port number for the DMCC as per **Section 6.4**.
- **First DMCC Station** – enter the first DMCC station created, found in **Section 5.4**.
- **Last DMCC Station** - enter the last DMCC station created.
- **DMCC Password** – enter the password for all DMCC stations, they must be all the same, this password can be found in **Section 5.4**.
- **FAS IP Address** – enter the IP address of the Supervisor Assist server.



Once the information in the previous page has been filled in the **Start Extension** and **End Extension** are filled in as shown as well as the **HTTP allowed**. Click on **Save** to complete the connection to the AES.



8. Verification Steps

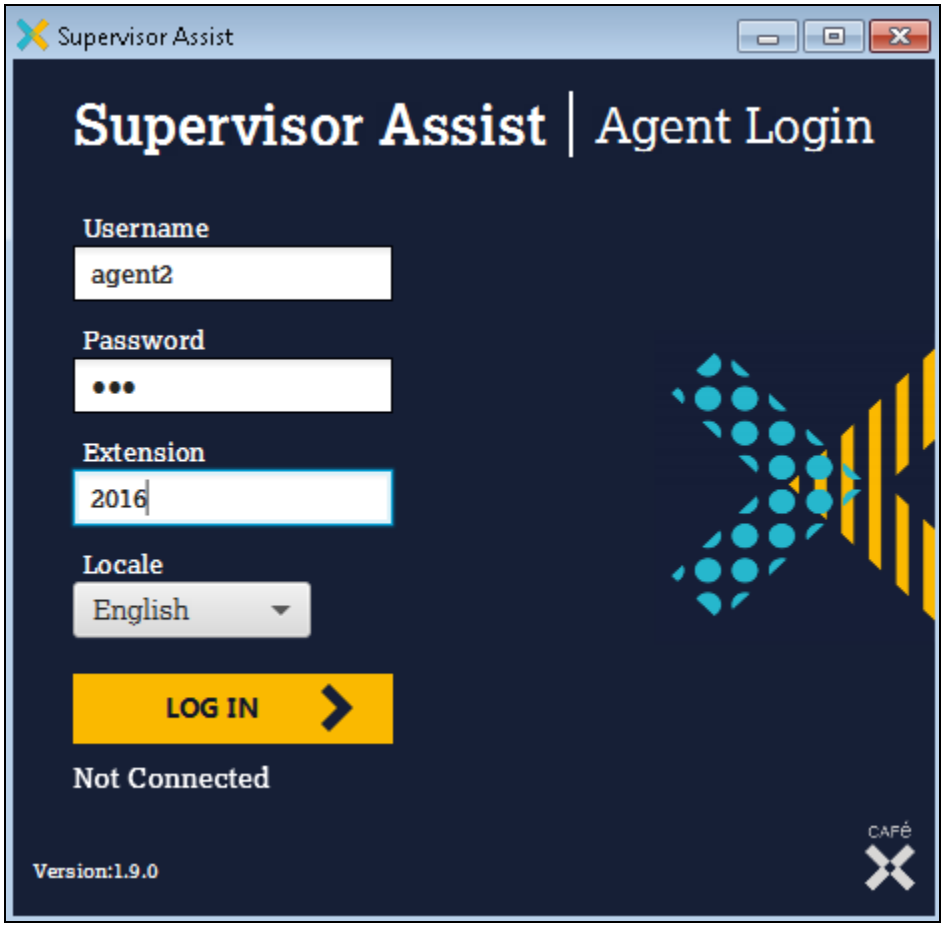
The correct configuration of the solution can be verified as follows.

8.1. Verify CaféX Supervisor Assist

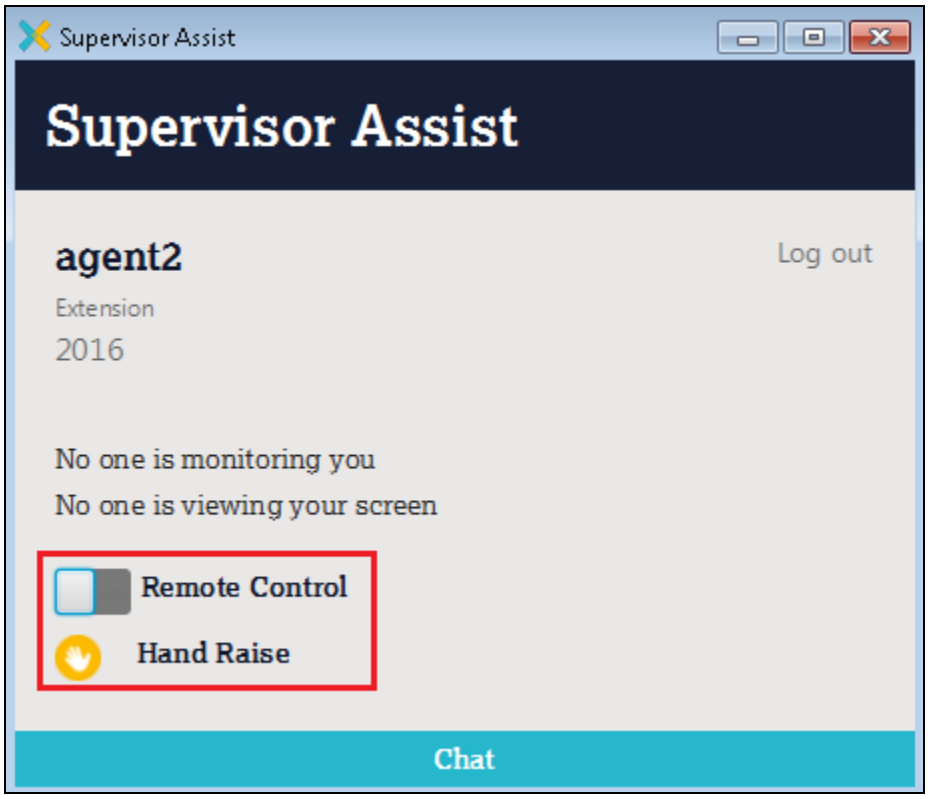
Each new agent must browse to the Supervisor Assist server and enter their agent username and password. Once logged in Launch Agent is clicked on which initiates a download of a Java Applet (not shown) that allows the launch of the **Supervisor Assist** for **Agent Login**.

8.1.1. Launch Supervisor Assist for Agent Login.

Launch the Java Applet that was downloaded from Supervisor Assist. This program is shown below where **agent2** is logging in. These credentials will be the result of the agents previously provisioned (outside the scope of this document – see official Café X documentation).

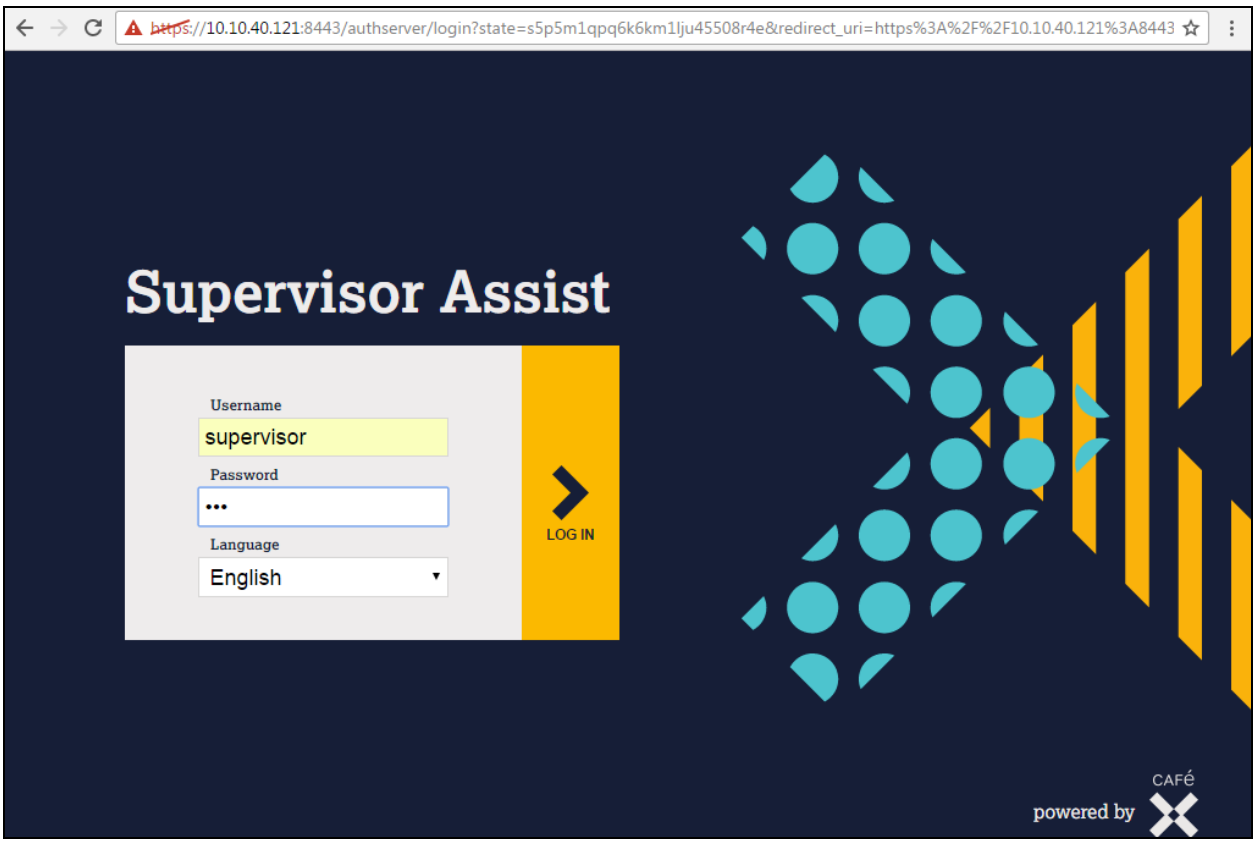


Once logged in the agent can request assistance by selecting **Remote Control** or **Hand Raise** as shown below.

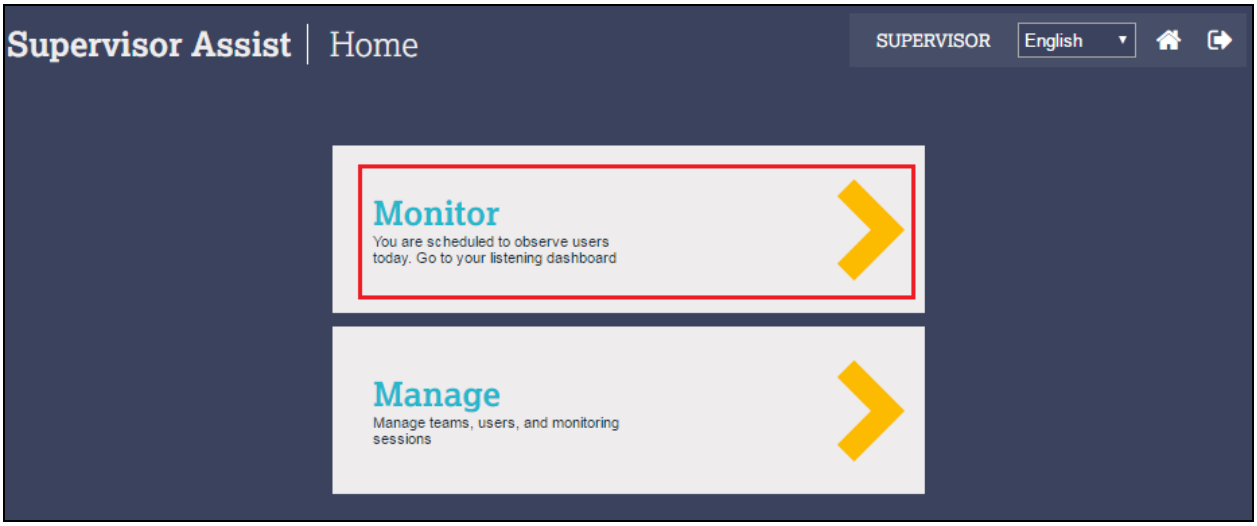


8.1.2. Launch Supervisor Assist for Supervisor Login

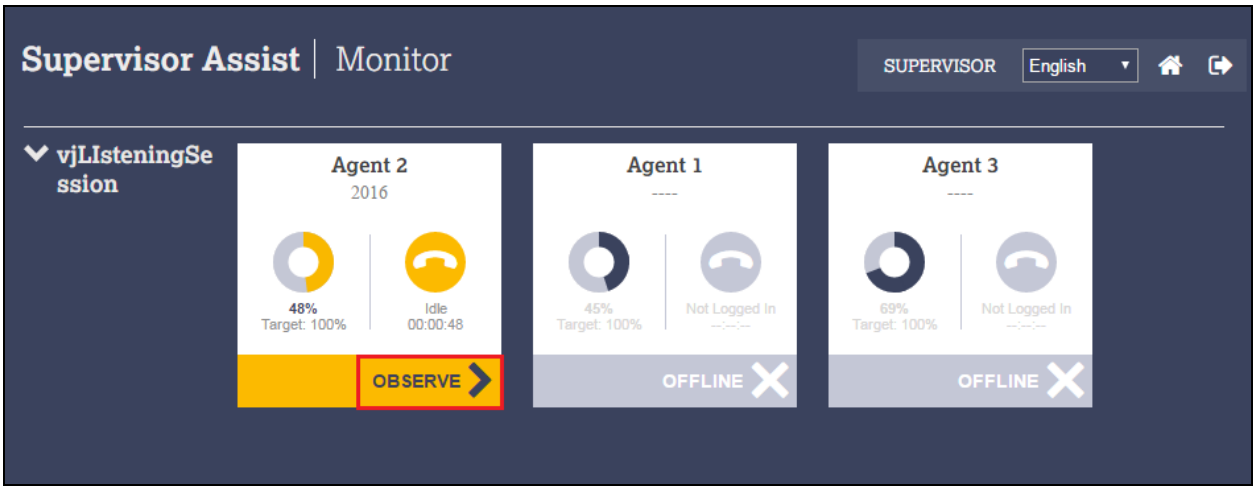
As per **Section 7**, open a Chrome browser to the Supervisor Assist server and enter the appropriate credentials. These supervisor credentials will be the result of previously adding a supervisor (outside the scope of this document – see Café X documentation).



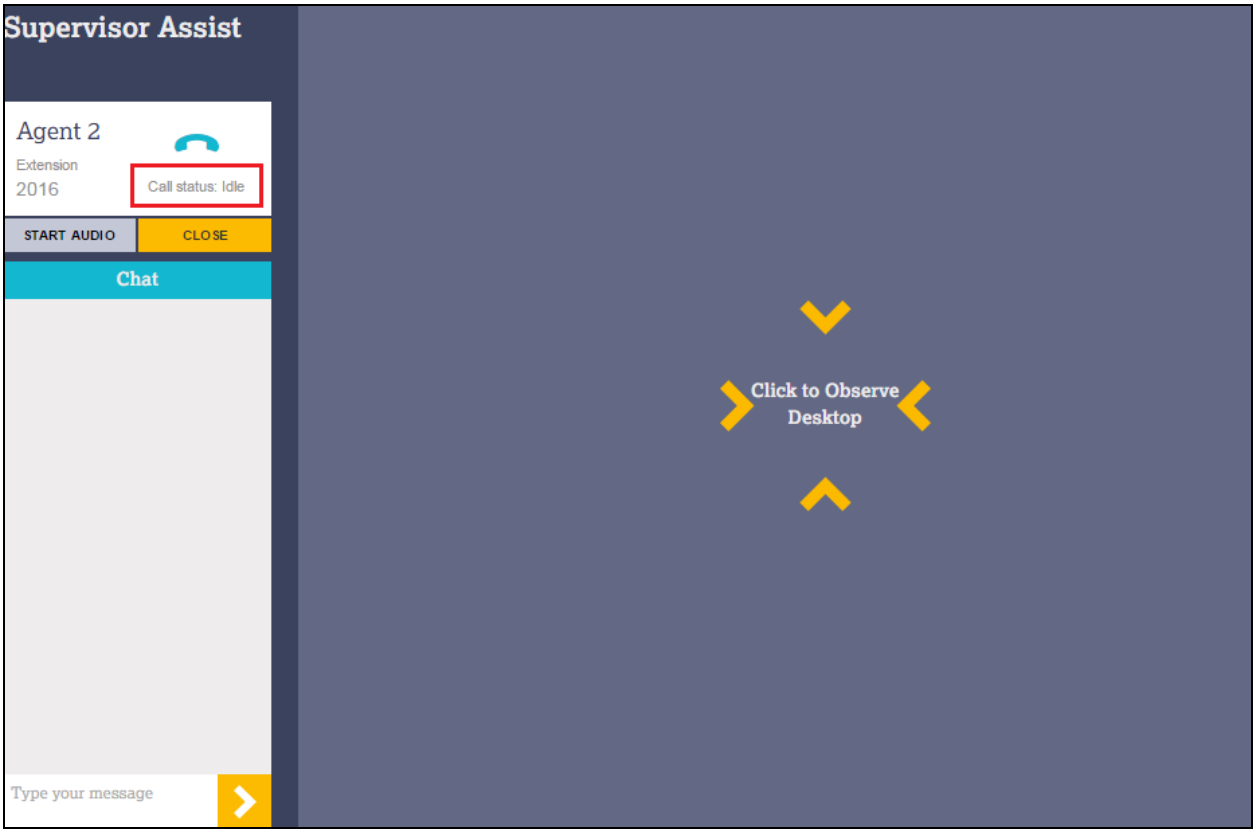
Click on **Monitor**.



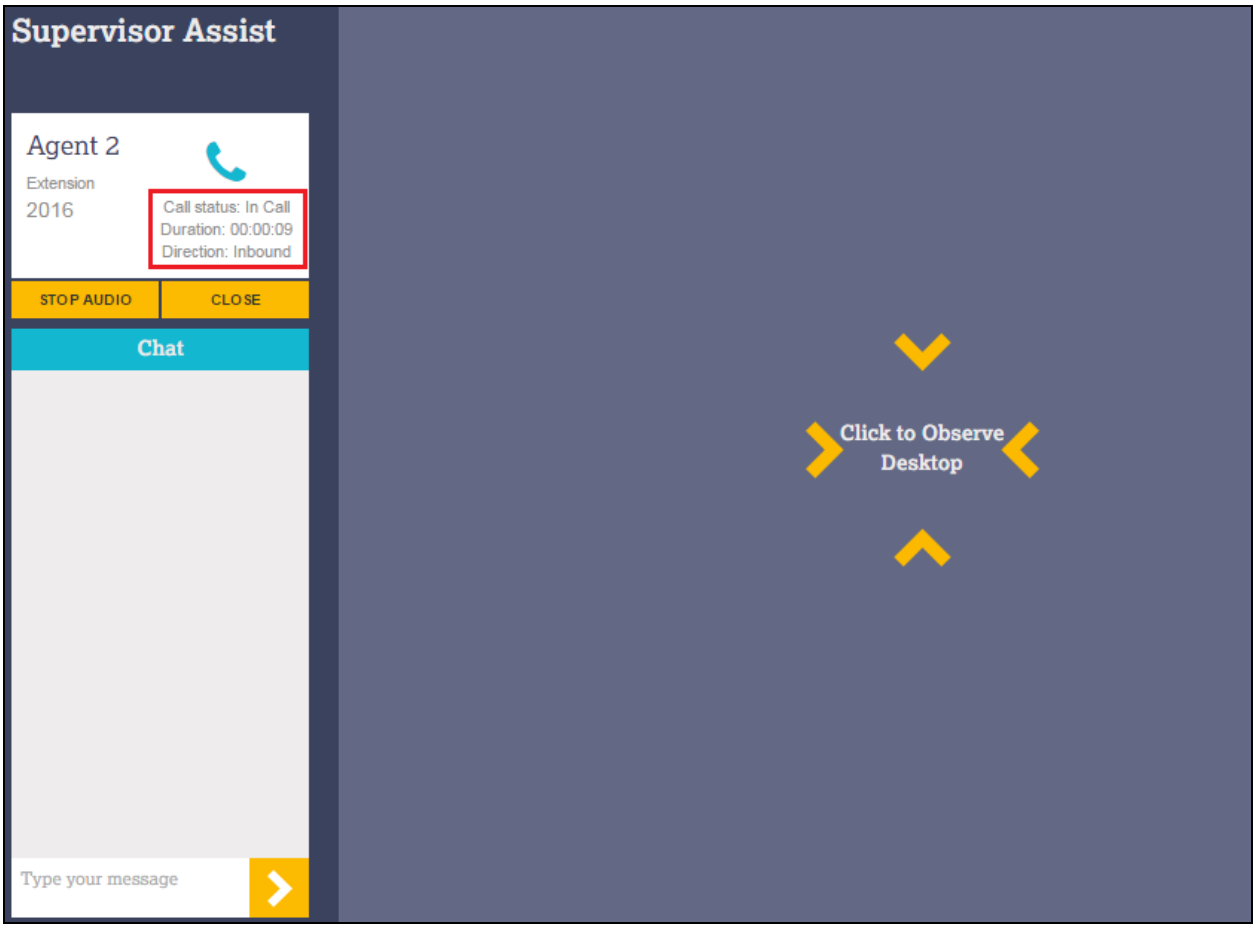
A list of agents that can be monitored is shown, **Agent 2** is currently the only agent logged in and therefore can only be monitored. To monitor **Agent 2** click on **OBSERVE** as shown below.



With the agent ready to take a call the status should show as **Idle** as shown below.

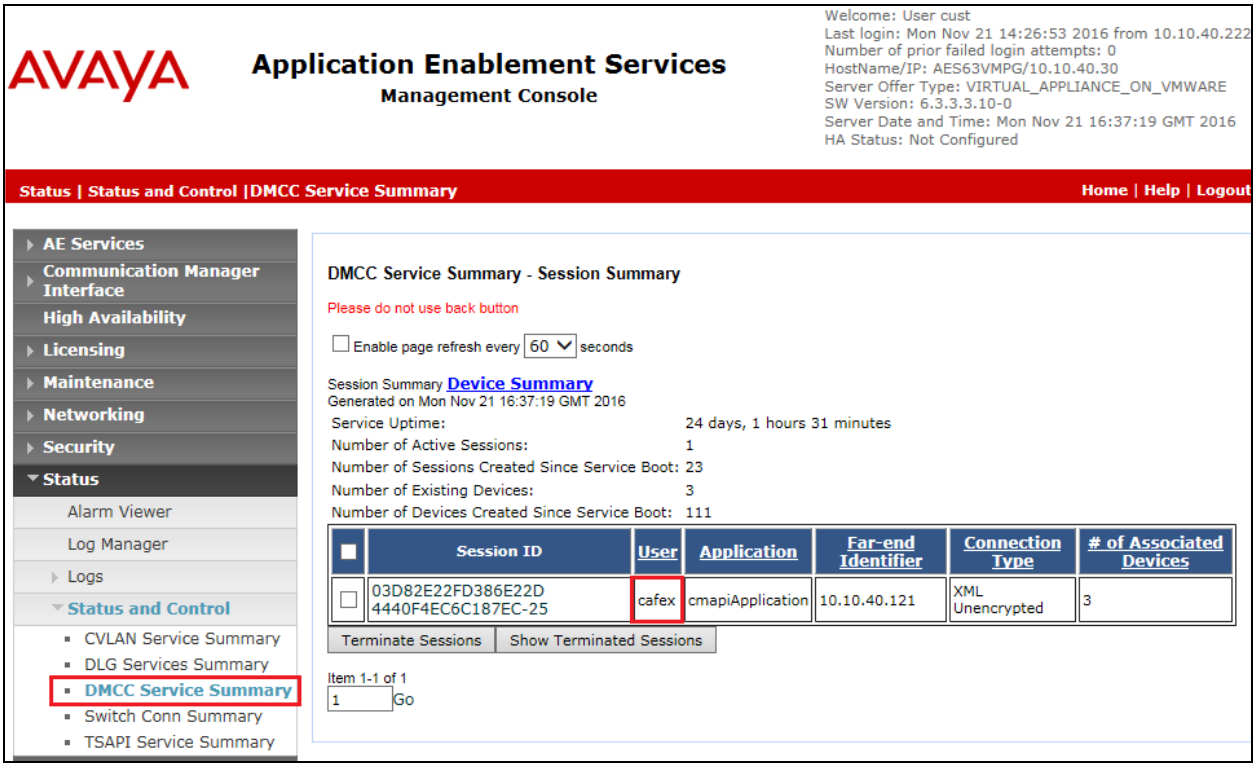


When the agent is on a call, then the **Call status** will show as **In Call** and the **Direction** will also be displayed as either **Inbound** or Outbound.



8.2. Verify DMCC Connection Status

Using the Application Enablement Services web interface, click **Status → Status and Control → DMCC Service Summary**. The **cafex** user created in **Section 6.5** should be visible as being connected as shown below.



9. Conclusion

These Application Notes describe the compliance testing of CaféX Supervisor Assist 1.9.0 with Avaya Aura® Communication Manager, and Avaya Aura® Application Enablement Services. All test cases were executed successfully with all issues and observations noted in **Section 2.2**.

10. Additional References

This section references the product documentations 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,* Document ID 03-300509

[2] *Avaya Aura® Communication Manager Feature Description and Implementation,* Document ID 555-245-205

[3] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide* Release 6.3

[4] *Avaya Aura® Session Manager Overview*, Doc *# 03603323Avaya Aura ® Contact Centre SIP Commissioning*, Doc # NN44400-511, Release 6.3

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.