Avaya Solution & Interoperability Test Lab

Application Notes for TantaComm Capture with Avaya Aura® Communication Manager 6.3 and Avaya Aura® Application Enablement Services 6.3 using Single Step Conference – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for TantaComm Capture to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services 6.3 using Single Step Conference. TantaComm Capture is a call recording solution.

In the compliance testing, TantaComm Capture used the Telephony Services Application Programming Interface and Device, Media, and Call Control XML interface from Avaya Aura® Application Enablement Services to monitor skill groups and agent stations on Avaya Aura® Communication Manager, and to capture the media associated with the monitored agents for call recordings.

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 TantaComm Capture to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services 6.3 using Single Step Conference. TantaComm Capture is a call recording solution.

In the compliance testing, TantaComm Capture used the Telephony Services Application Programming Interface (TSAPI) and Device, Media, and Call Control (DMCC) XML interface from Avaya Aura® Application Enablement Services to monitor skill groups and agent stations on Avaya Aura® Communication Manager, and to capture the media associated with the monitored agents for call recordings.

The TSAPI interface is used by TantaComm Capture to monitor skill groups and agent stations on Avaya Aura® Communication Manager. The DMCC interface is used by TantaComm Capture to register virtual IP softphones, and for adding virtual IP softphones to active calls using the Single Step Conference feature.

When there is an active call at the monitored agent, TantaComm Capture is informed of the call via event reports from the TSAPI interface. TantaComm Capture starts the call recording by using the Single Step Conference feature from the DMCC interface to add a virtual IP softphone to the active call to obtain the media. The event reports are also used to determine when to stop the call recordings.

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the Capture application, the application automatically requests monitoring of skill groups and agent stations using TSAPI, and registers the virtual IP softphones using DMCC.

For the manual part of the testing, each call was handled manually on the agent station with generation of unique audio content for the recordings. Necessary user actions such as hold and resume were performed from the agent telephones to test the different call scenarios.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to Capture.

The verification of tests included use of Capture logs for proper message exchanges, and use of Capture web interface for proper logging and playback of calls.

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

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on Capture:

- Handling of TSAPI messages in areas of event notification.
- Use of DMCC registration services to register and un-register the virtual IP softphones.
- Use of DMCC call control services to activate Single Step Conference for the virtual IP softphones to obtain media for call recordings.
- Proper recording, logging, and playback of calls for scenarios involving inbound, outbound, internal, external, ACD, non-ACD, hold, resume, multiple calls, multiple agents, conference, and transfer.

The serviceability testing focused on verifying the ability of Capture to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to Capture.

2.2. Test Results

All test cases were executed, and the following were observations on Capture:

- Capture version 14.0.0 displayed as 1.0.0 due to build problem. This will be addressed in build 14.0.1.
- For the attended transfer scenario involving agent transferring of call to non-monitored supervisor, the recording entry may not show up until the next call takes place in the system and with call duration reflecting the extra wait period. Nevertheless, the actual call is recorded properly up to the point of transfer as expected.
- For internal calls between two local users, by design the application produced one recording entry against the destination user when the destination user is monitored. As such, an internal call from a monitored agent to a non-monitored destination such as a supervisor was therefore not recorded. Similarly, for the attended conference scenario involving agent conferencing a non-monitored supervisor, the private conversation between the agent and the non-monitored supervisor was not recorded.

2.3. Support

Technical support on Capture can be obtained through the following:

- **Phone:** (800) 444-8522, option 2
- **Email:** support@tantacomm.com

3. Reference Configuration

Capture can be configured on a single server or with components distributed across multiple servers. The compliance test used a single server configuration.

The detailed administration of basic connectivity between Communication Manager, Application Enablement Services, System Manager, Session Manager, and of contact center devices are not the focus of these Application Notes and will not be described.

In the compliance testing, Capture monitored the skill groups and agent stations shown in the table below.

Device Type	Extension
VDN	49001, 49002
Skill Group	48101, 48102
Supervisor	45000
Agent Station	45001, 46002
Agent ID	45881, 45882

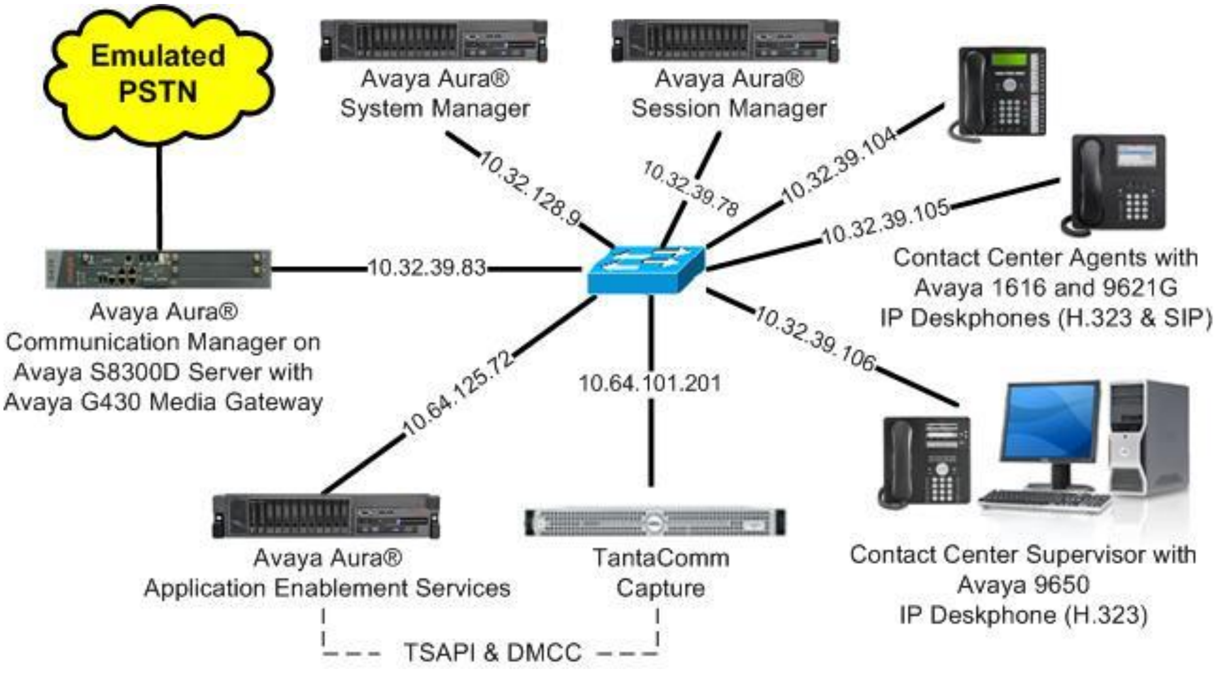

Emulated PSTN
Avaya Aura® System Manager
Avaya Aura® Session Manager
10.32.128.9
10.32.39.78
10.32.39.104
10.32.39.105
Contact Center Agents with Avaya 1616 and 9621G IP Deskphones (H.323 & SIP)
10.32.39.83
Avaya Aura® Communication Manager on Avaya S8300D Server with Avaya G430 Media Gateway
10.32.39.106
10.64.125.72
10.64.101.201
Avaya Aura® Application Enablement Services
TantaComm Capture
Contact Center Supervisor with Avaya 9650 IP Deskphone (H.323)
TSAPI & DMCC

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® Communication Manager on Avaya S8300D Server with Avaya G430 Media Gateway	6.3.5 (R016x.03.0.124.0-21460) 6.3.5 (35.8.0)
Avaya Aura® Application Enablement Services	6.3.1 (6.3.1.0.19-0)
Avaya Aura® Session Manager	6.3.7
Avaya Aura® System Manager	6.3.5
Avaya 1616 IP Deskphone (H.323)	1.350B
Avaya 9621G IP Deskphone (SIP)	6.3.1.22
Avaya 9650 IP Deskphone (H.323)	3.220A
TantaComm Capture on Windows Server 2008 • TStsapi.exe • ars_dmcc.exe • Avaya TSAPI Windows Client (csta32.dll) • Avaya DMCC XML SDK	14.0.0 R2 Standard 14.2.0.0 14.2.2.0 6.1.1.469 6.1.0.501

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 system parameters features
- Administer virtual IP softphones
- Administer IP codec set

5.1. Verify License

Log in to 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 3**. 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   3 of  11
                                OPTIONAL FEATURES

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

5.2. 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: 40001
     Type: ADJ-IP
                                                                     COR: 1
     Name: AES CTI Link
```

5.3. Administer System Parameters Features

Use the “change system-parameters features” command to enable **Create Universal Call ID (UCID)**, which is located on **Page 5**. For **UCID Network Node ID**, enter an available node ID.

```
change system-parameters features                              Page   5 of  20
                        FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS
  Endpoint:               Lines Per Page: 60

SYSTEM-WIDE PARAMETERS
                                     Switch Name:
            Emergency Extension Forwarding (min): 10
          Enable Inter-Gateway Alternate Routing? n
Enable Dial Plan Transparency in Survivable Mode? n
                              COR to Use for DPT: station
                EC500 Routing in Survivable Mode: dpt-then-ec500
MALICIOUS CALL TRACE PARAMETERS
               Apply MCT Warning Tone? n   MCT Voice Recorder Trunk Group:
      Delay Sending RELease (seconds): 0
SEND ALL CALLS OPTIONS
     Send All Calls Applies to: station    Auto Inspect on Send All Calls? n
              Preserve previous AUX Work button states after deactivation? n
UNIVERSAL CALL ID
     Create Universal Call ID (UCID)? y    UCID Network Node ID: 1
```

Navigate to **Page 13**, and enable **Send UCID to ASAI**. This parameter allows for the universal call ID to be sent to Capture.

```
change system-parameters features                              Page  13 of  20
                        FEATURE-RELATED SYSTEM PARAMETERS
 CALL CENTER MISCELLANEOUS
           Callr-info Display Timer (sec): 10
                         Clear Callr-info: next-call
        Allow Ringer-off with Auto-Answer? n

    Reporting for PC Non-Predictive Calls? n

            Agent/Caller Disconnect Tones? n
          Interruptible Aux Notification Timer (sec): 3
             Zip Tone Burst for Callmaster Endpoints: double

  ASAI
            Copy ASAI UUI During Conference/Transfer? y
        Call Classification After Answer Supervision? y
                                   Send UCID to ASAI? y
          For ASAI Send DTMF Tone to Call Originator? y
  Send Connect Event to ASAI For Announcement Answer? n
```

5.4. Administer Virtual IP Softphones

Add a virtual IP softphone using the “add station n” command, where “n” is an available extension number. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Extension:** The available extension number.
- **Type:** “4624”
- **Name:** A descriptive name.
- **Security Code:** A desired code.
- **IP SoftPhone:** “y”

```
add station 45991                                               Page   1 of   5
                                     STATION

Extension: 45991                         Lock Messages? n               BCC: 0
     Type: 4624                          Security Code: 123456           TN: 1
     Port: IP                          Coverage Path 1:                 COR: 1
     Name: TantaComm Virtual #1        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: 45991
            Speakerphone: 2-way               Mute Button Enabled? y
        Display Language: english                Expansion Module? n
 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
```

Repeat this section to administer the desired number of virtual IP softphones. In the compliance testing, two virtual IP softphones were administered as shown below, to allow for simultaneous recording of two monitored agents in **Section 3**.

```
list station 45991 count 2

                                  STATIONS

Ext/          Port/   Name/                       Room/       Cv1/ COR/   Cable/
 Hunt-to       Type      Surv GK NN        Move    Data Ext    Cv2  COS TN Jack

45991         S00051  TantaComm Virtual #1                         1
               4624                        no                      1   1
45992         S00054  TantaComm Virtual #2                         1
               4624                        no                      1   1
```

5.5. Administer IP Codec Set

Use the “change ip-codec-set n” command, where “n” is an existing codec set number used for integration with Capture. For **Audio Codec**, make sure “G.729A” is included, as this is the only codec type supported by Capture. In the compliance testing, this IP codec set was assigned to the agents and to the virtual IP softphones.

```
change ip-codec-set 1                                           Page   1 of   2

                          IP Codec Set

    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU           n         2        20
 2: G.729A            n         2        20
 3:
```

6. Configure Avaya Aura® Application Enablement Services

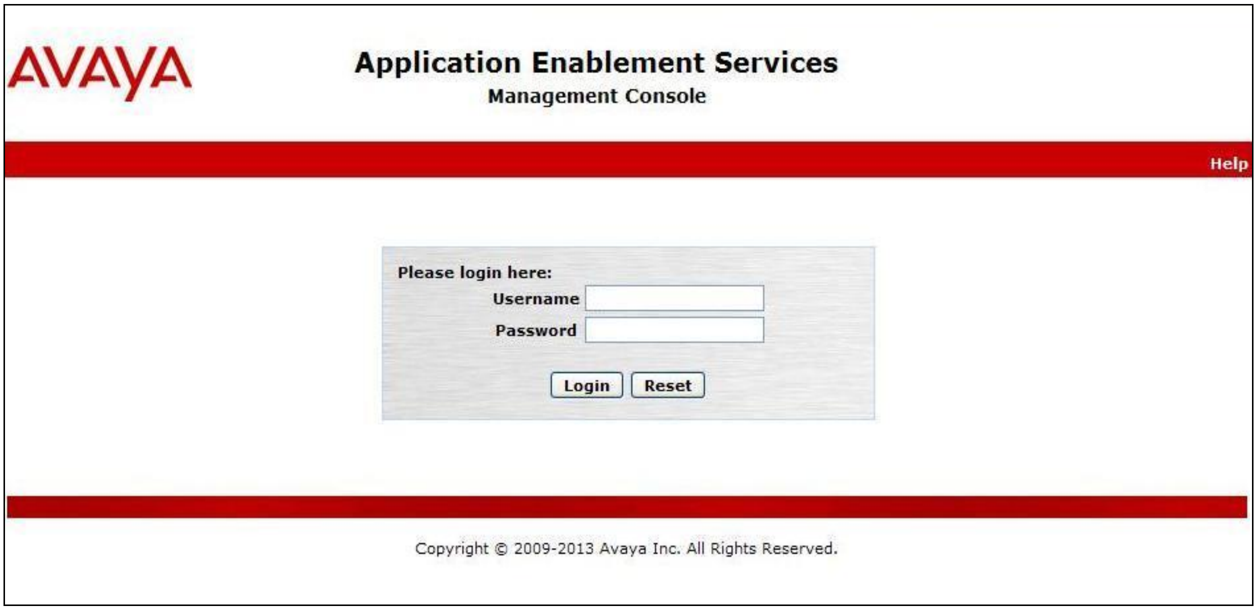
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer H.323 gatekeeper
- Disable security database
- Restart services
- Obtain Tlink name
- Administer TantaComm user
- Enable ports

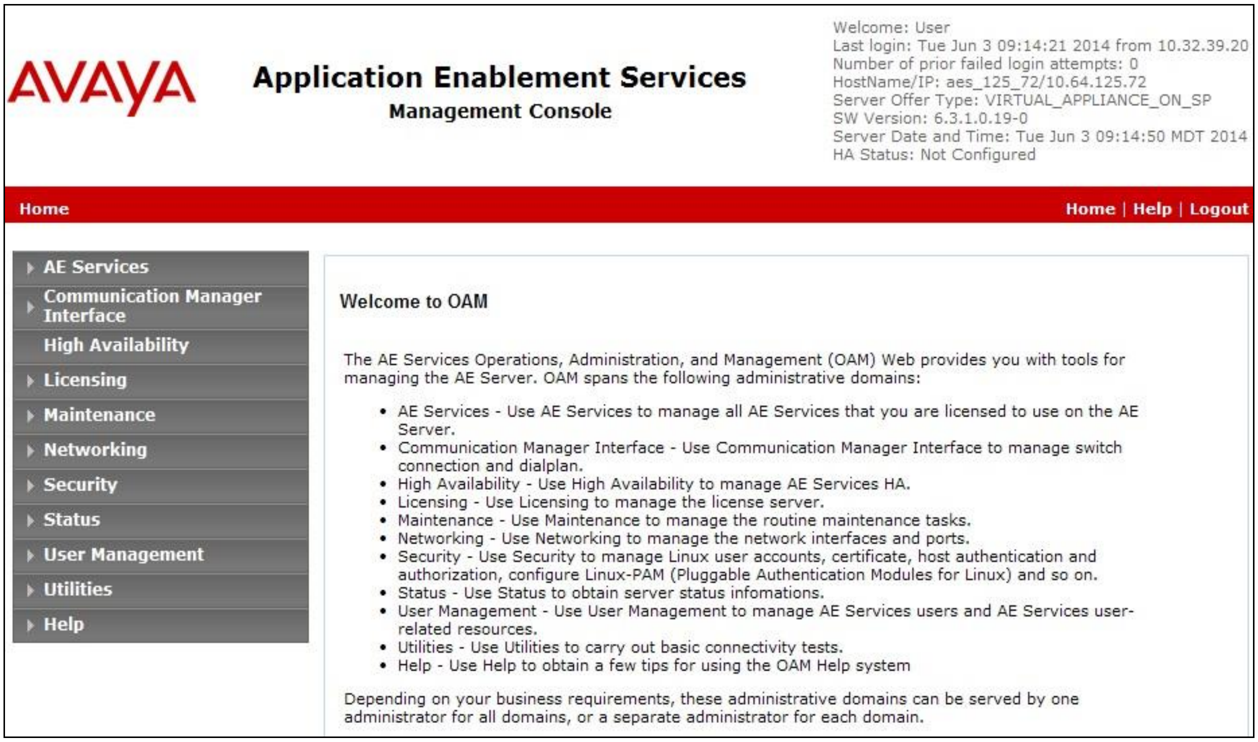
6.1. Launch OAM Interface

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.


AVAYA
Application Enablement Services
Management Console
Help
Please login here:
Username
Password
Login
Reset
Copyright © 2009-2013 Avaya Inc. All Rights Reserved.

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



Welcome: User
Last login: Tue Jun 3 09:14:21 2014 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.1.0.19-0
Server Date and Time: Tue Jun 3 09:14:50 MDT 2014
HA Status: Not Configured

Welcome to OAM

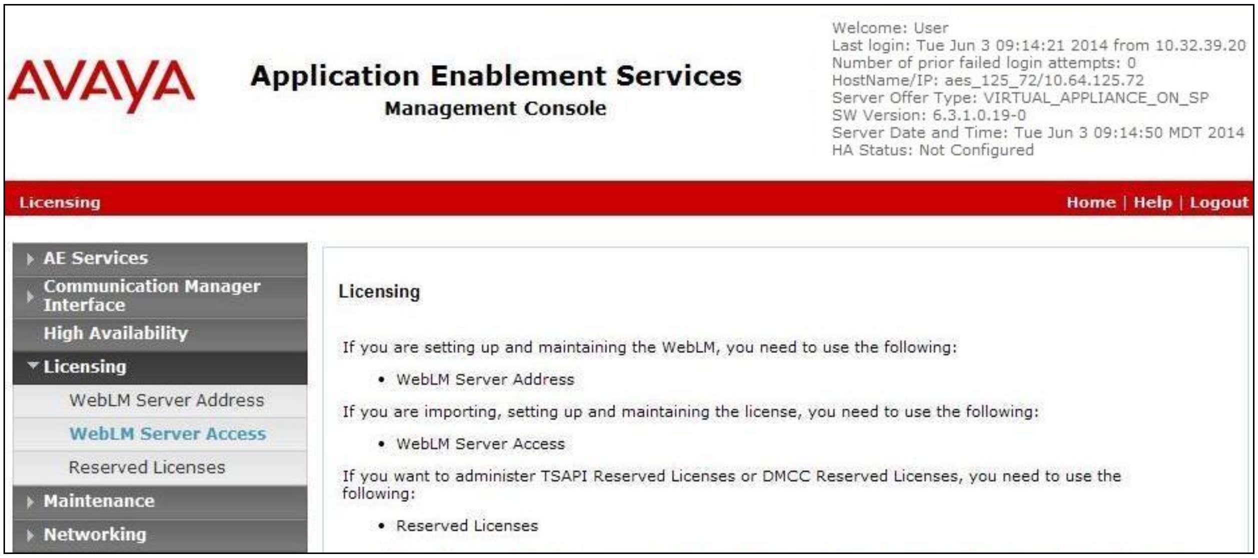
The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

- 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 infomations.
- 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.

6.2. Verify License

Select **Licensing → WebLM Server Access** in the left pane, to display the **Web License Manager** pop-up screen (not shown), and log in using the appropriate credentials.



Welcome: User
Last login: Tue Jun 3 09:14:21 2014 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.1.0.19-0
Server Date and Time: Tue Jun 3 09:14:50 MDT 2014
HA Status: Not Configured

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:

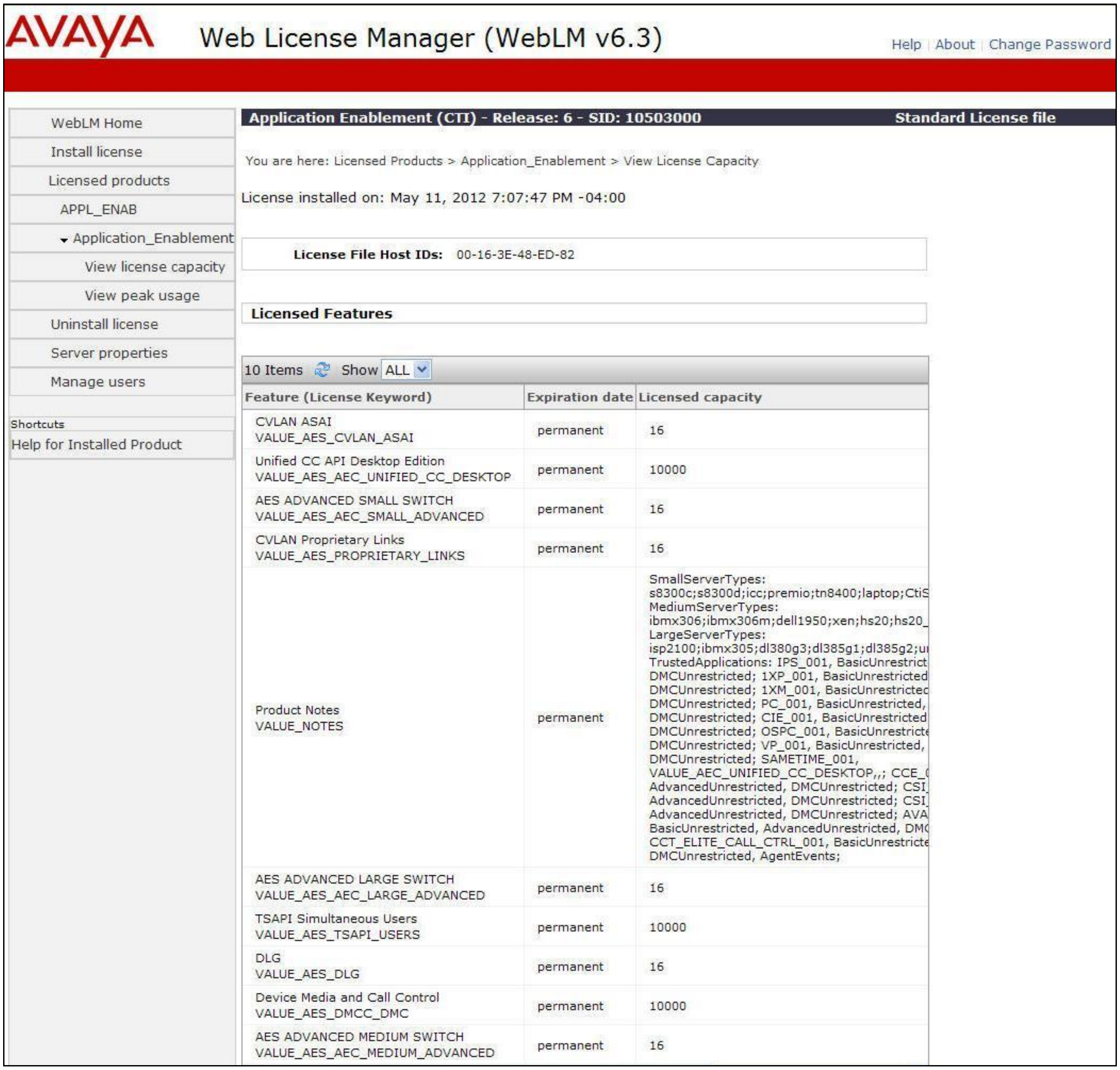
- WebLM Server Access

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

- Reserved Licenses

The **Web License Manager** screen below is displayed. Select **Licensed products → APPL_ENAB → Application_Enablement** in the left pane, to display the **Application Enablement (CTI)** screen in the right pane.

Verify that there are sufficient licenses for **TSAPI Simultaneous Users** and **Device Media and Call Control**, as shown below. Note that the TSAPI license is used for device monitoring, and the DMCC license is used for the virtual IP softphones.



Application Enablement (CTI) - Release: 6 - SID: 10503000 **Standard License file**

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

License installed on: May 11, 2012 7:07:47 PM -04:00

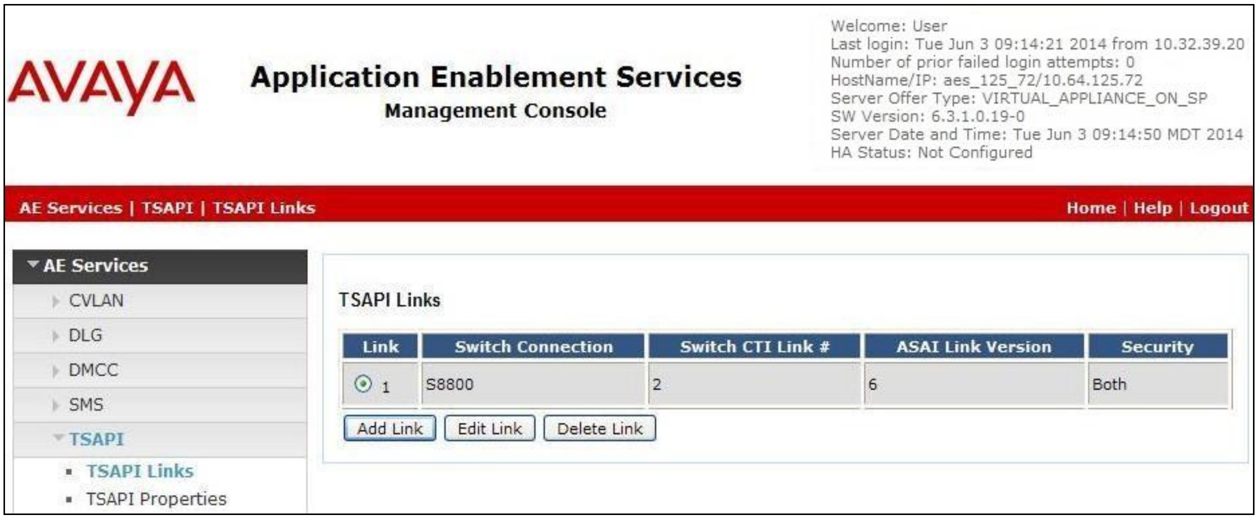
License File Host IDs: 00-16-3E-48-ED-82

Licensed Features

Feature (License Keyword)	Expiration date	Licensed capacity
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	10000
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	16
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	16
Product Notes VALUE_NOTES	permanent	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;Cti MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_ LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2; TrustedApplications: IPS_001, BasicUnrestrict DMCUnrestricted; 1XP_001, BasicUnrestricted DMCUnrestricted; 1XM_001, BasicUnrestricte DMCUnrestricted; PC_001, BasicUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted DMCUnrestricted; OSPC_001, BasicUnrestrict DMCUnrestricted; VP_001, BasicUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AEC_UNIFIED_CC_DESKTOP,,; CCE_ AdvancedUnrestricted, DMCUnrestricted; CSI AdvancedUnrestricted, DMCUnrestricted; CSI AdvancedUnrestricted, DMCUnrestricted; AVA BasicUnrestricted, AdvancedUnrestricted, DM CCT_ELITE_CALL_CTRL_001, BasicUnrestrict DMCUnrestricted, AgentEvents;
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	16
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	10000
DLG VALUE_AES_DLG	permanent	16
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	10000
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	16

6.3. Administer TSAPI Link

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



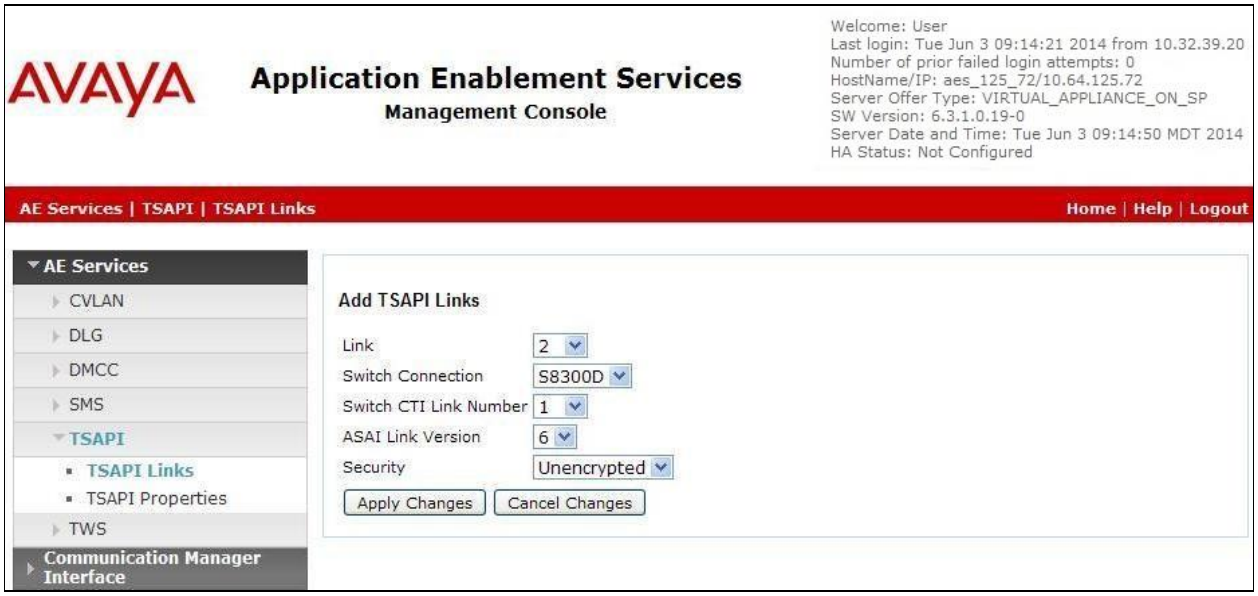
Welcome: User
Last login: Tue Jun 3 09:14:21 2014 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.1.0.19-0
Server Date and Time: Tue Jun 3 09:14:50 MDT 2014
HA Status: Not Configured

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
● 1	S8800	2	6	Both

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 "S8300D" is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields.



Welcome: User
Last login: Tue Jun 3 09:14:21 2014 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.1.0.19-0
Server Date and Time: Tue Jun 3 09:14:50 MDT 2014
HA Status: Not Configured

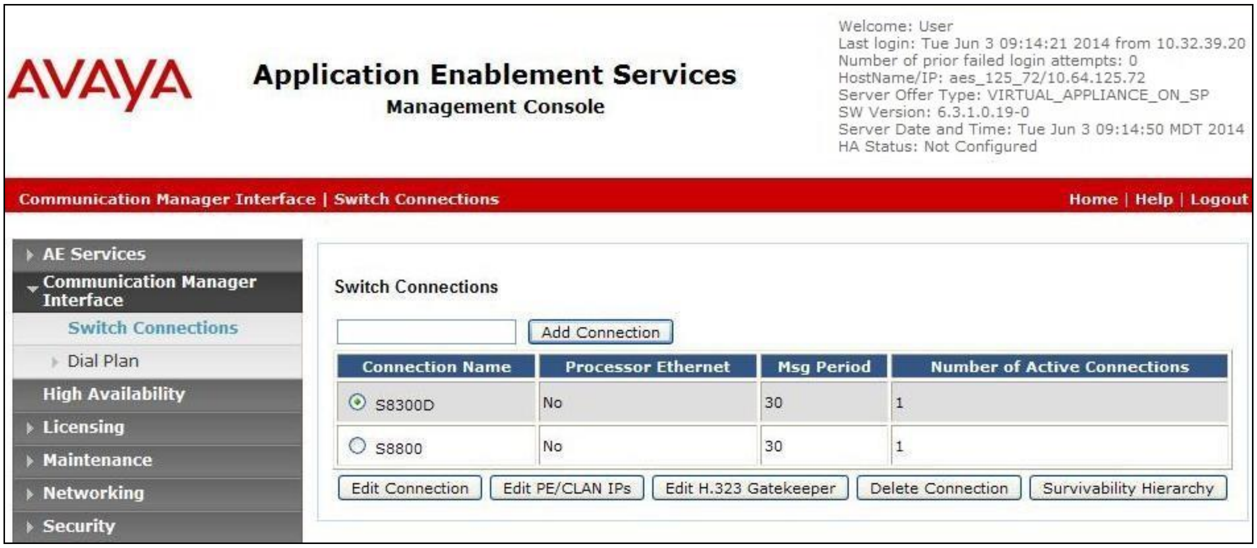
Add TSAPI Links

Link: 2
Switch Connection: S8300D
Switch CTI Link Number: 1
ASAI Link Version: 6
Security: Unencrypted

6.4. Administer H.323 Gatekeeper

Select **Communication Manager Interface → Switch Connections** from the left pane. The **Switch Connections** screen shows a listing of the existing switch connections.

Locate the connection name associated with the relevant Communication Manager, in this case "S8300D", and select the corresponding radio button. Click **Edit H.323 Gatekeeper**.

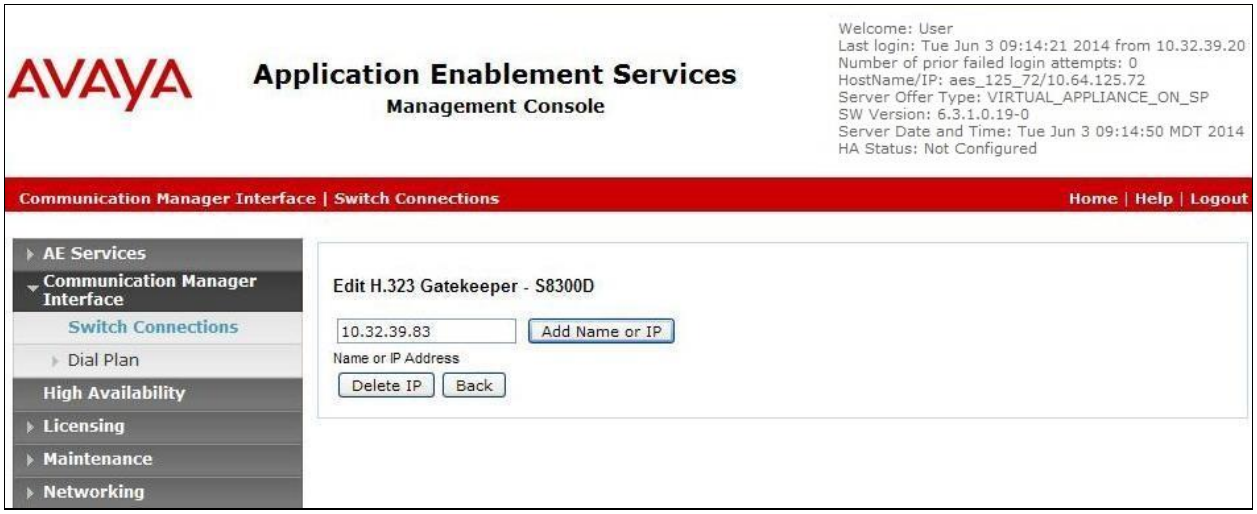


Welcome: User
Last login: Tue Jun 3 09:14:21 2014 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.1.0.19-0
Server Date and Time: Tue Jun 3 09:14:50 MDT 2014
HA Status: Not Configured

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
● S8300D	No	30	1
○ S8800	No	30	1

The **Edit H.323 Gatekeeper** screen is displayed. Enter the IP address of a C-LAN circuit pack or the Processor C-LAN on Communication Manager to use as the H.323 gatekeeper, in this case "10.32.39.83" as shown below. Click **Add Name or IP**.



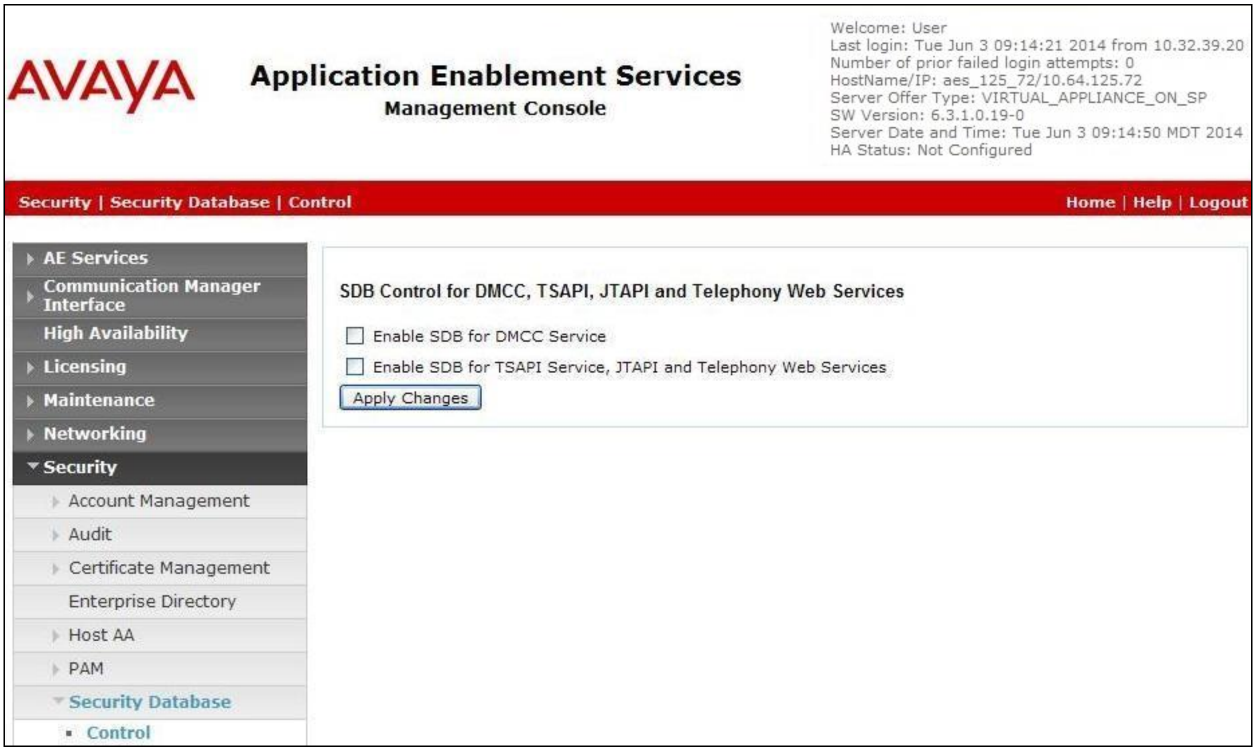
Welcome: User
Last login: Tue Jun 3 09:14:21 2014 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.1.0.19-0
Server Date and Time: Tue Jun 3 09:14:50 MDT 2014
HA Status: Not Configured

Edit H.323 Gatekeeper - S8300D

Name or IP Address: 10.32.39.83

6.5. Disable 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.



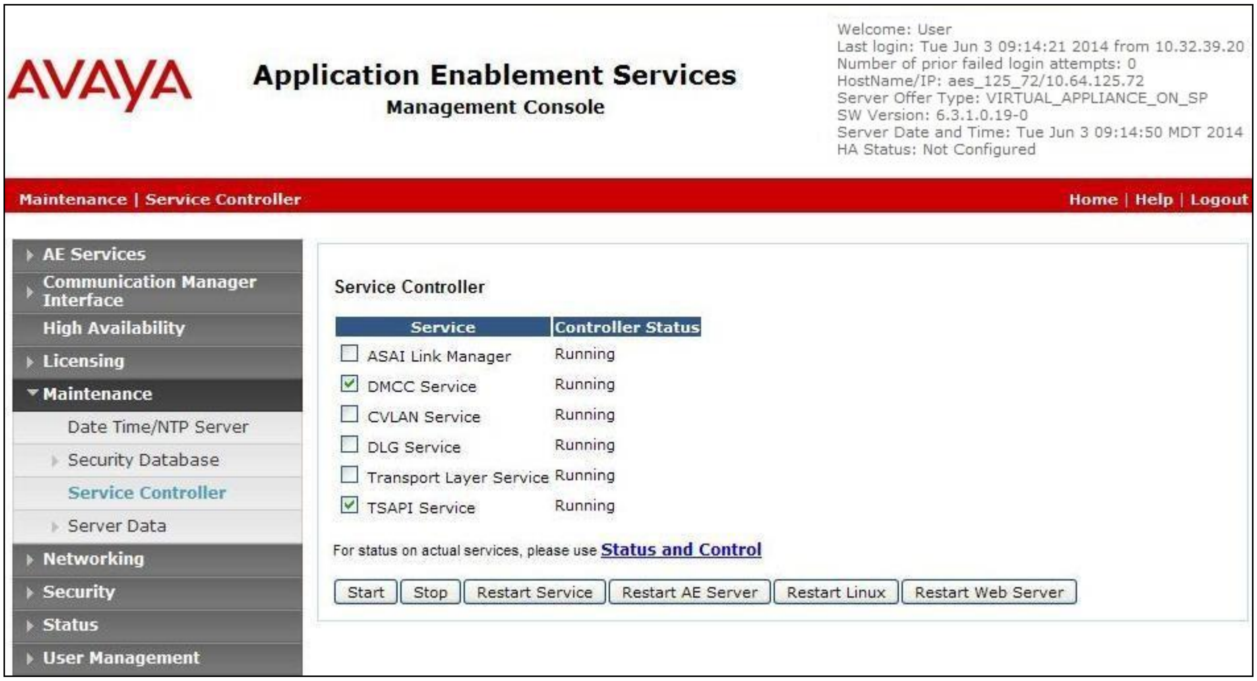
Welcome: User
Last login: Tue Jun 3 09:14:21 2014 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.1.0.19-0
Server Date and Time: Tue Jun 3 09:14:50 MDT 2014
HA Status: Not Configured

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

☐ Enable SDB for DMCC Service
☐ Enable SDB for TSAPI Service, JTAPI and Telephony Web Services

6.6. 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 click **Restart Service**.



Welcome: User
Last login: Tue Jun 3 09:14:21 2014 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.1.0.19-0
Server Date and Time: Tue Jun 3 09:14:50 MDT 2014
HA Status: Not Configured

Service Controller

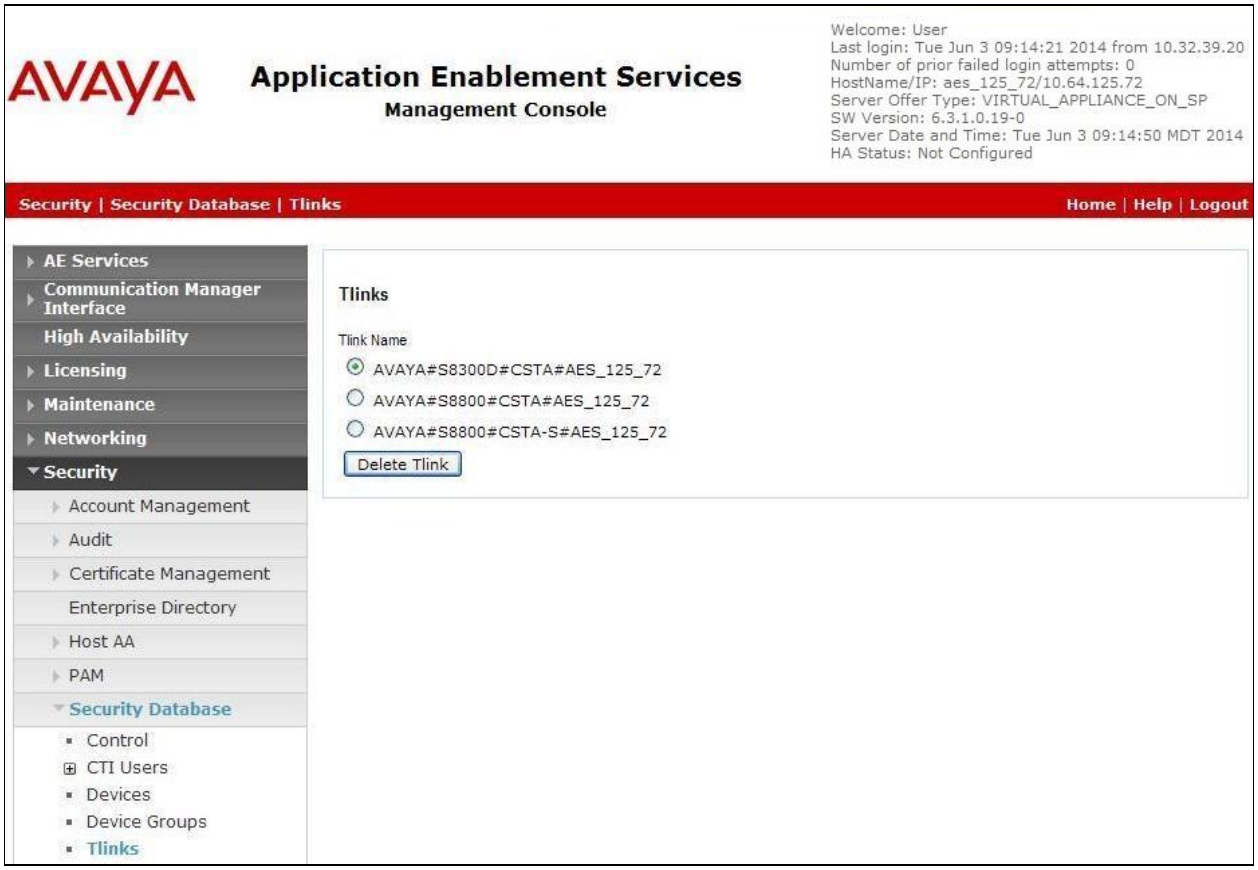
Service	Controller Status
☐ ASAI Link Manager	Running
☑ DMCC Service	Running
☐ CVLAN Service	Running
☐ DLG Service	Running
☐ Transport Layer Service	Running
☑ TSAPI Service	Running

For status on actual services, please use **Status and Control**

6.7. 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 Capture.

In this case, the associated Tlink name is "AVAYA#**S8300D**#CSTA#AES_125_72". Note the use of the switch connection "S8300D" from **Section 6.3** as part of the Tlink name.



Welcome: User
Last login: Tue Jun 3 09:14:21 2014 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.1.0.19-0
Server Date and Time: Tue Jun 3 09:14:50 MDT 2014
HA Status: Not Configured

Tlinks

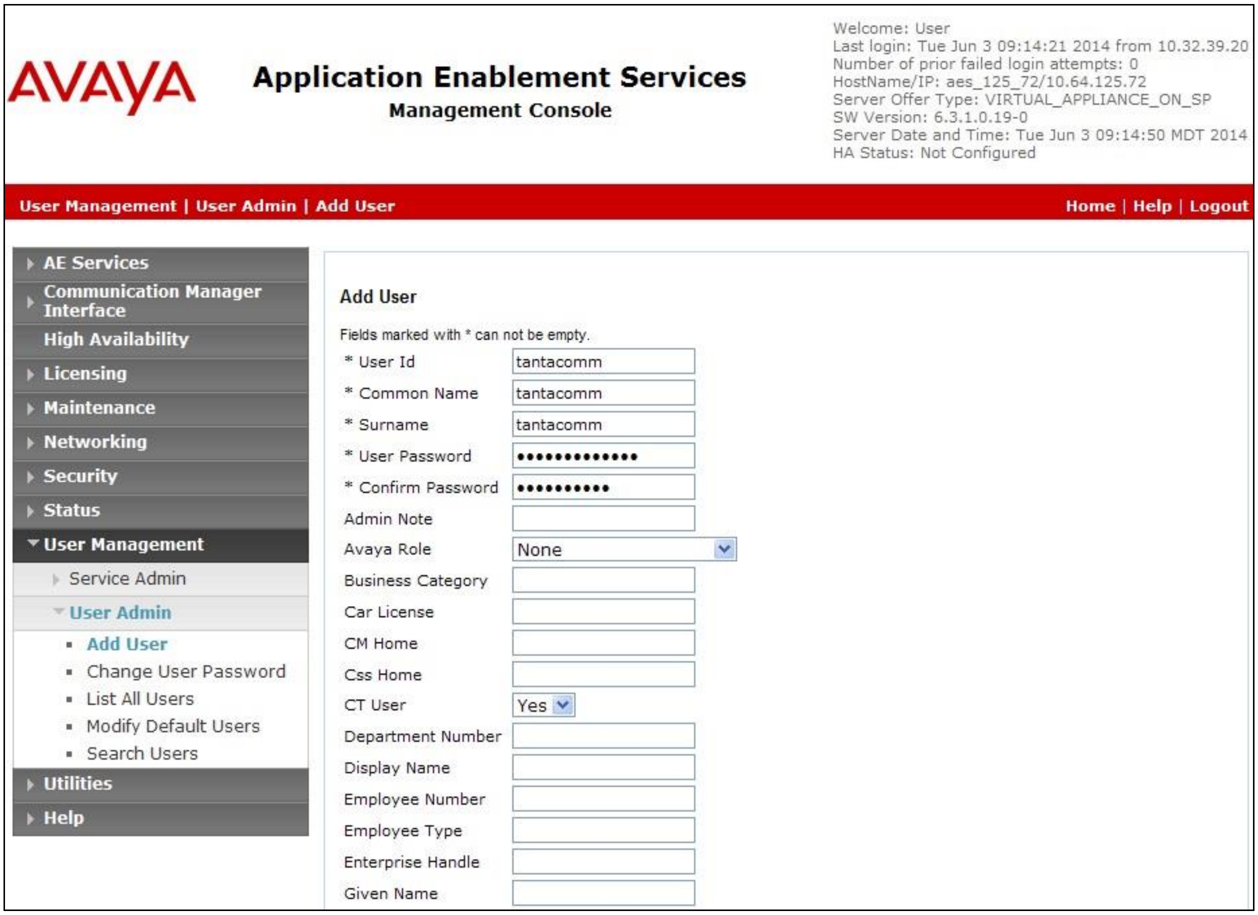
Tlink Name

● AVAYA#S8300D#CSTA#AES_125_72
○ AVAYA#S8800#CSTA#AES_125_72
○ AVAYA#S8800#CSTA-S#AES_125_72

6.8. Administer TantaComm 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.



Welcome: User
Last login: Tue Jun 3 09:14:21 2014 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.1.0.19-0
Server Date and Time: Tue Jun 3 09:14:50 MDT 2014
HA Status: Not Configured

Add User

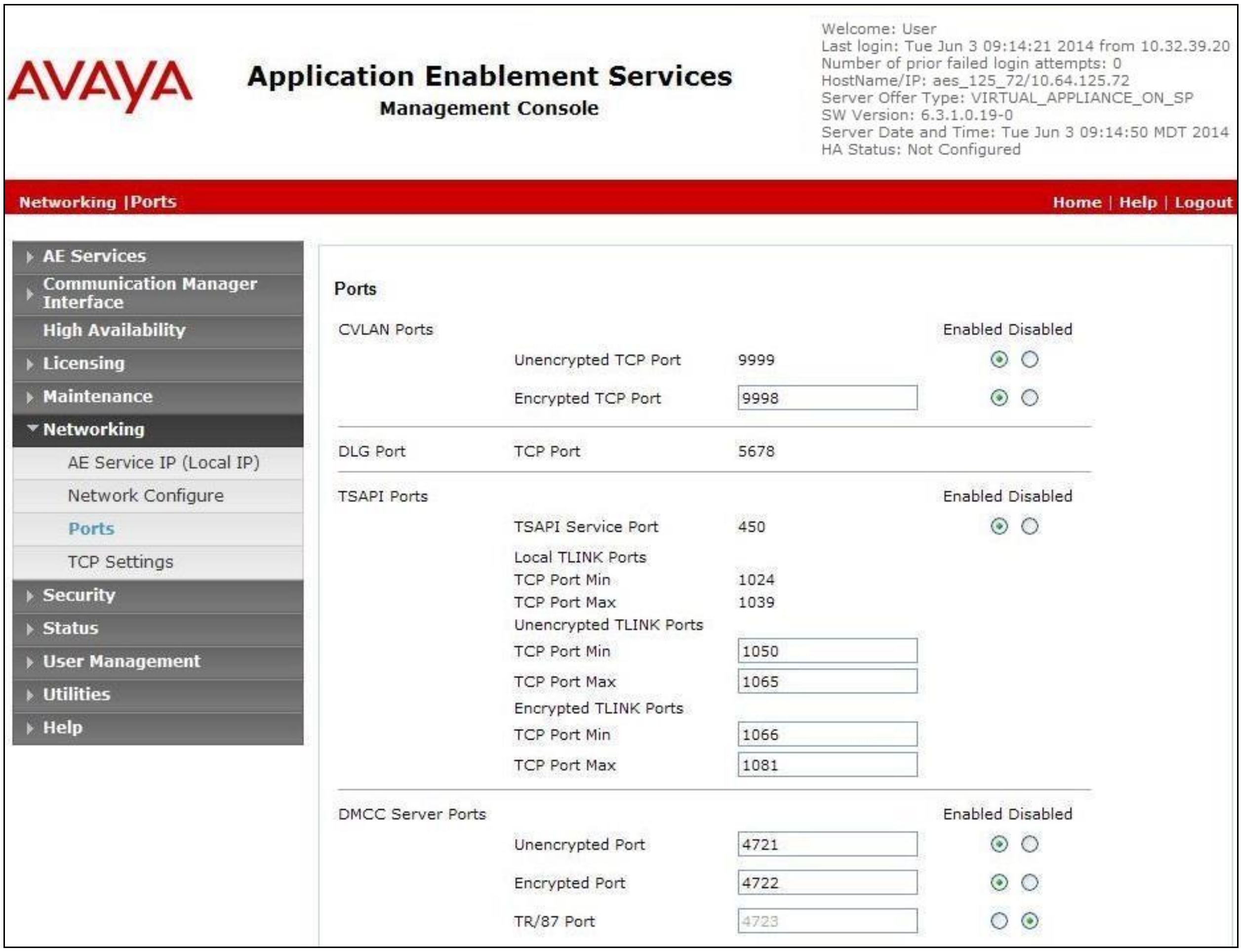
Fields marked with * can not be empty.

* User Id	tantacomm
* Common Name	tantacomm
* Surname	tantacomm
* 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	
Given Name	

6.9. Enable 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
Last login: Tue Jun 3 09:14:21 2014 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.1.0.19-0
Server Date and Time: Tue Jun 3 09:14:50 MDT 2014
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	○	●

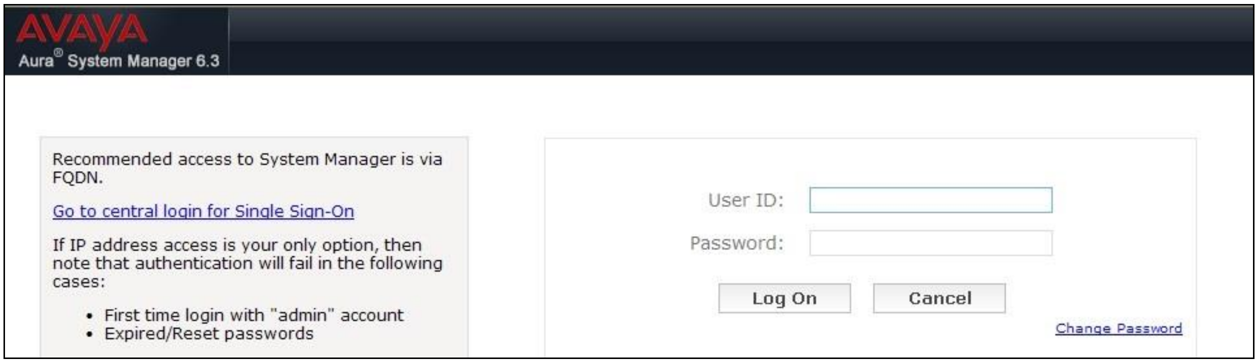
7. Configure Avaya Aura® Session Manager

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

- Launch System Manager
- Administer users

7.1. Launch System Manager

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



Recommended access to System Manager is via FQDN.

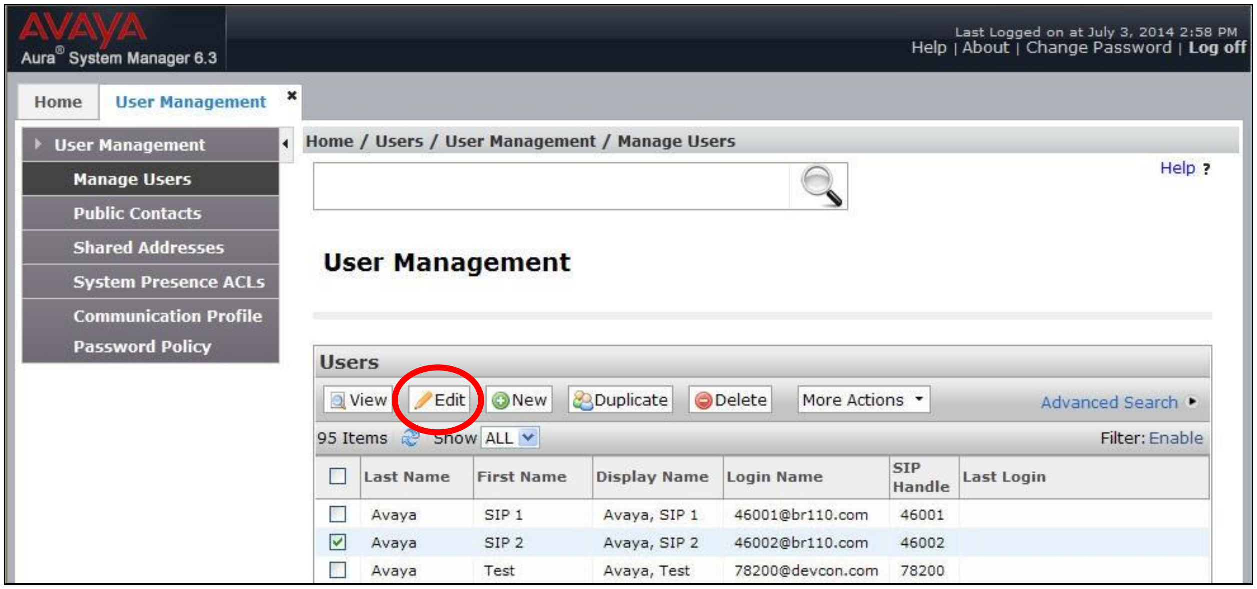
Go to central login for Single Sign-On

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

7.2. Administer Users

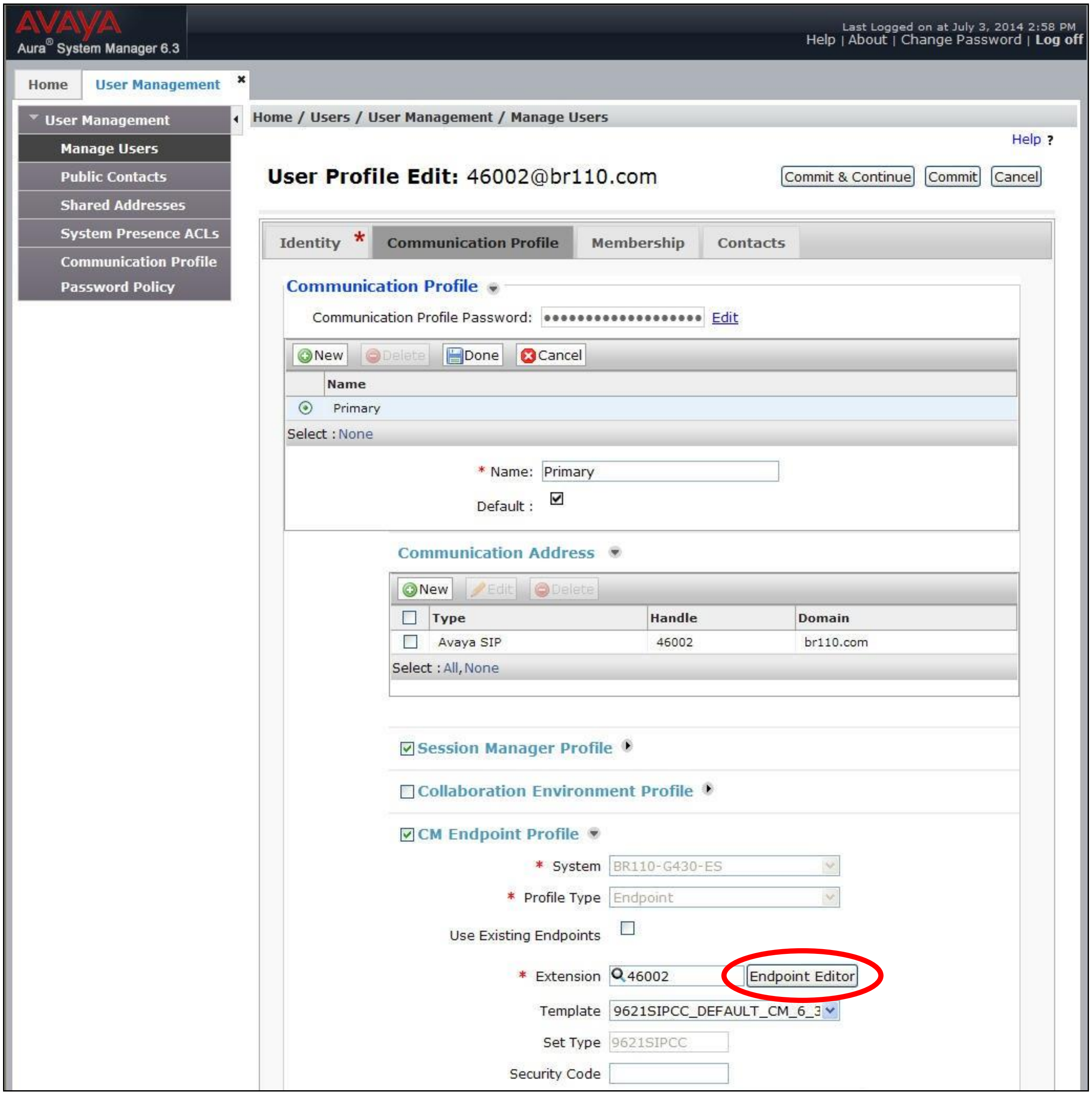
In the subsequent screen (not shown), select **Users → User Management → Manage Users** to display the **User Management** screen below. Select the entry associated with the first SIP agent station from **Section 3**, in this case “46002”, and click **Edit**.



☐	Last Name	First Name	Display Name	Login Name	SIP Handle	Last Login
☐	Avaya	SIP 1	Avaya, SIP 1	46001@br110.com	46001	
☑	Avaya	SIP 2	Avaya, SIP 2	46002@br110.com	46002	
☐	Avaya	Test	Avaya, Test	78200@devcon.com	78200	

The **User Profile Edit** screen is displayed. Select the **Communication Profile** tab to display the screen below.

Navigate to the **CM Endpoint Profile** sub-section, and click **Endpoint Editor**.



User Profile Edit: 46002@br110.com

Communication Profile Password: ••••••••••••••••••• Edit

	Name
●	Primary

Select : None

* Name: Primary

Default : ☑

Communication Address

☐	Type	Handle	Domain
☐	Avaya SIP	46002	br110.com

Select : All, None

☑ Session Manager Profile

☐ Collaboration Environment Profile

☑ CM Endpoint Profile

* System BR110-G430-ES

* Profile Type Endpoint

Use Existing Endpoints ☐

* Extension 46002

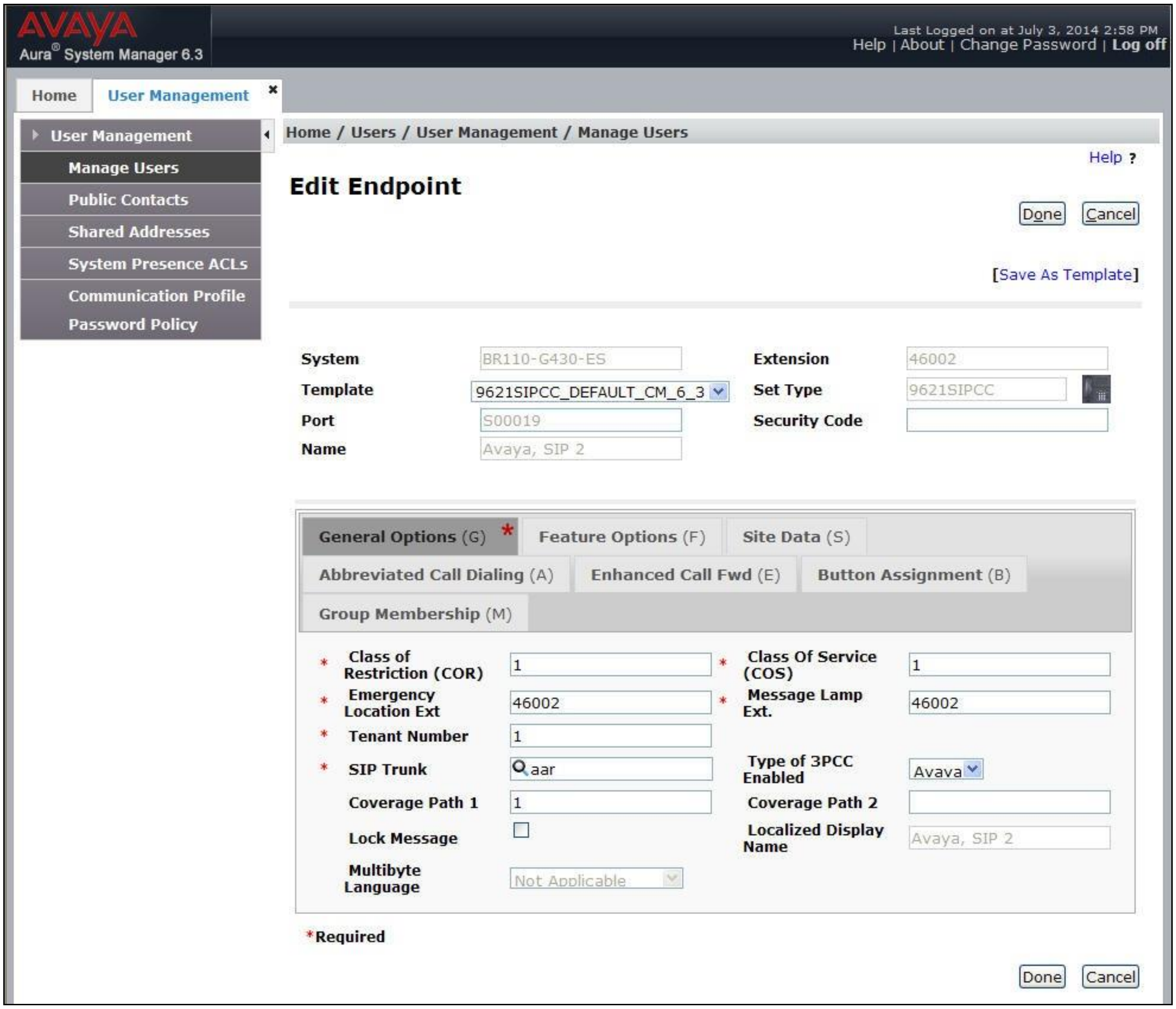
Template 9621SIPCC_DEFAULT_CM_6_3

Set Type 9621SIPCC

Security Code

The **Edit Endpoint** screen is displayed next. For **Type of 3PCC Enabled**, select “Avaya” from the drop-down list as shown below. Retain the default values in the remaining fields.

Repeat this section for all SIP agent users.



Edit Endpoint

System	BR110-G430-ES	Extension	46002
Template	9621SIPCC_DEFAULT_CM_6_3	Set Type	9621SIPCC
Port	S00019	Security Code	
Name	Avaya, SIP 2		

* Class of Restriction (COR)	1	* Class Of Service (COS)	1
* Emergency Location Ext	46002	* Message Lamp Ext.	46002
* Tenant Number	1		
* SIP Trunk	aar	Type of 3PCC Enabled	Avaya
Coverage Path 1	1	Coverage Path 2	
Lock Message	☐	Localized Display Name	Avaya, SIP 2
Multibyte Language	Not Applicable		

8. Configure TantaComm Capture

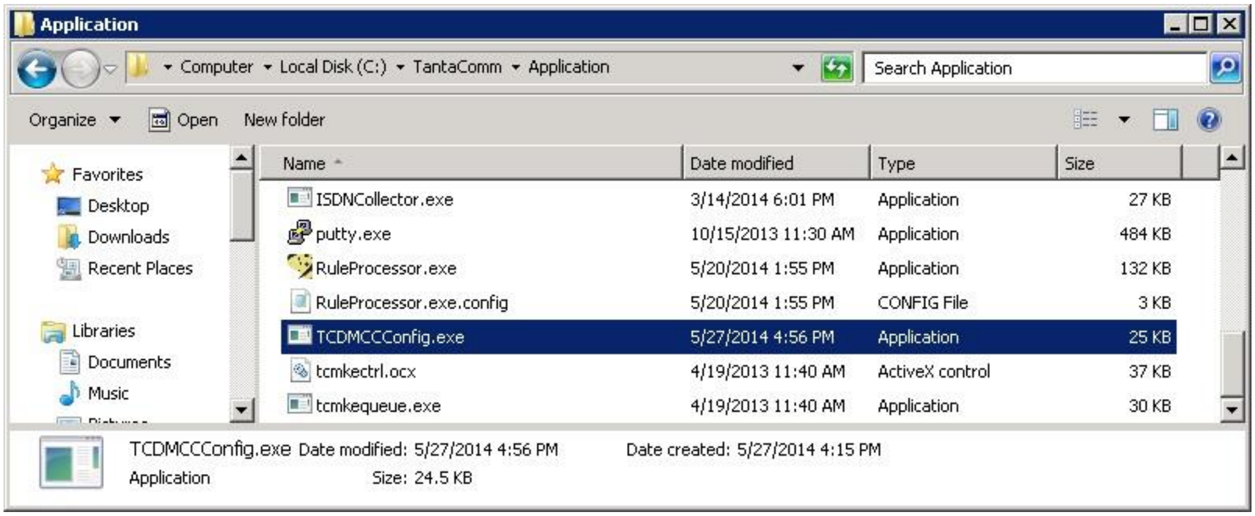
This section provides the procedures for configuring Capture. The procedures include the following areas:

- Administer TCDMCCConfig
- Restart services

The configuration of Capture is performed by the TantaComm technical services team. The procedural steps are presented in these Application Notes for informational purposes.

8.1. Administer TCDMCCConfig

From the Capture server, navigate to the **C:\TantaComm\Application** directory, and double click on the **TCDMCCConfig** application shown below.



Name	Date modified	Type	Size
ISDNCollector.exe	3/14/2014 6:01 PM	Application	27 KB
putty.exe	10/15/2013 11:30 AM	Application	484 KB
RuleProcessor.exe	5/20/2014 1:55 PM	Application	132 KB
RuleProcessor.exe.config	5/20/2014 1:55 PM	CONFIG File	3 KB
TCDMCCConfig.exe	5/27/2014 4:56 PM	Application	25 KB
tcmkectrl.ocx	4/19/2013 11:40 AM	ActiveX control	37 KB
tcmkequeue.exe	4/19/2013 11:40 AM	Application	30 KB

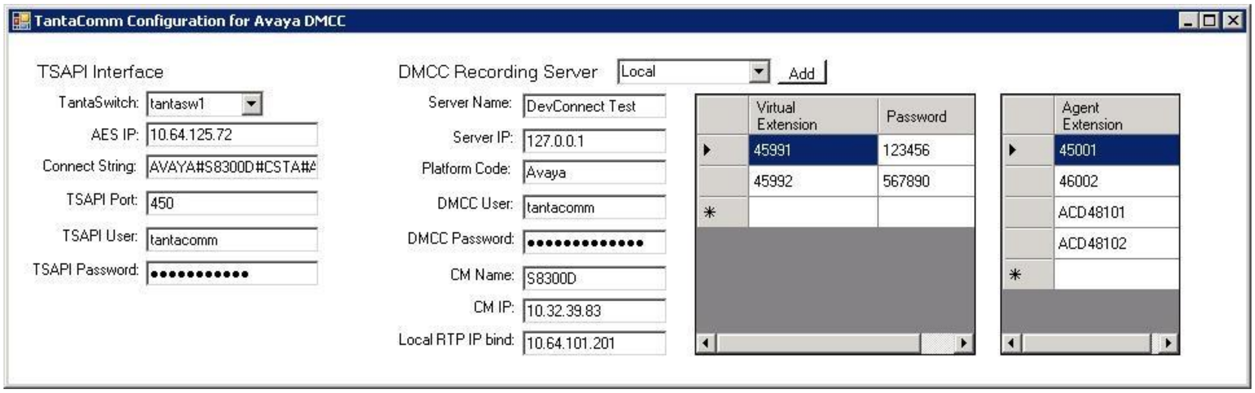
TCDMCCConfig.exe Date modified: 5/27/2014 4:56 PM Date created: 5/27/2014 4:15 PM
Application Size: 24.5 KB

The **TantaComm Configuration for Avaya DMCC** screen is displayed. Enter the following values for the specified fields.

- **TantaSwitch:** Select the applicable switch that was pre-configured.
- **AES IP:** Enter the IP address of Application Enablement Services.
- **Connection String:** The Tlink name from **Section 6.7**.
- **TSAPI Port:** "450"
- **TSAPI User:** The TantaComm user credentials from **Section 6.8**.
- **TSAPI Password:** The TantaComm user credentials from **Section 6.8**.
- **DMCC Recording Server:** "Local"
- **Server Name:** Enter a desired name.
- **Server IP:** "127.0.0.1"
- **Platform Code:** "Avaya"
- **DMCC User:** The TantaComm user credentials from **Section 6.8**.
- **DMCC Password:** The TantaComm user credentials from **Section 6.8**.
- **CM Name:** The switch connection name from **Section 6.3**.
- **CM IP:** The H.323 gatekeeper IP address from **Section 6.4**.
- **Local RTP IP bind:** The IP address of the Capture server.

In the **Virtual Extension** and **Password** columns, enter the extension and corresponding security code of each virtual IP softphone from **Section 5.4**.

In the **Agent Extension** column, enter the agent station and skill group extensions from **Section 3**. For skill group extensions, prepend "ACD" before the extension as shown below.



TantaSwitch: tantasw1
AES IP: 10.64.125.72
Connect String: AVAYA#S8300D#CSTA#A
TSAPI Port: 450
TSAPI User: tantacomm
TSAPI Password: ●●●●●●●●●●●●●

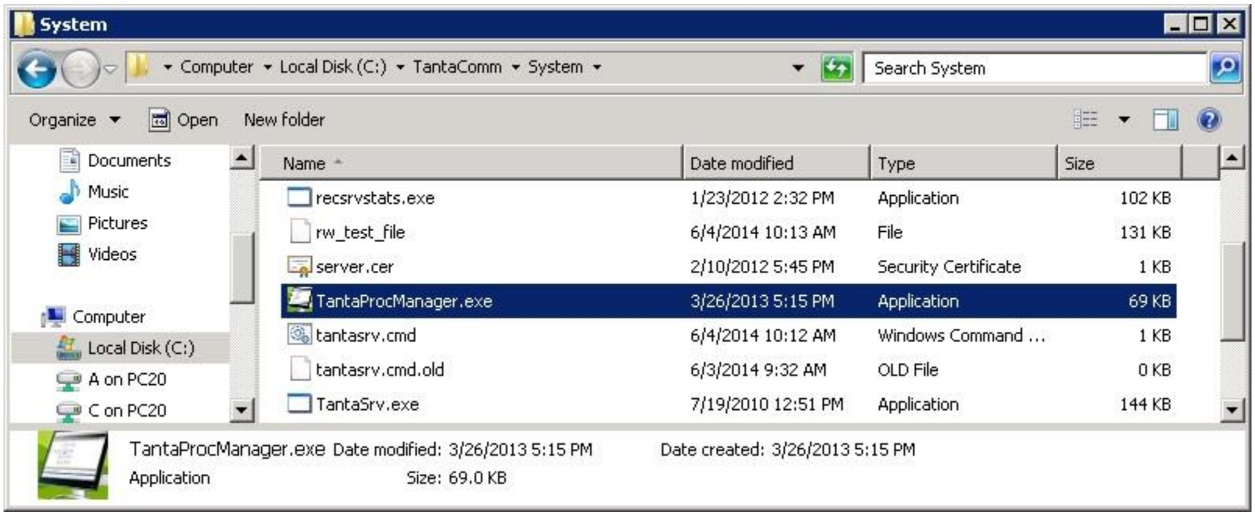
DMCC Recording Server: Local
Server Name: DevConnect Test
Server IP: 127.0.0.1
Platform Code: Avaya
DMCC User: tantacomm
DMCC Password: ●●●●●●●●●●●●●●
CM Name: S8300D
CM IP: 10.32.39.83
Local RTP IP bind: 10.64.101.201

	Virtual Extension	Password
▶	45991	123456
	45992	567890
*		

	Agent Extension
▶	45001
	46002
	ACD48101
	ACD48102
*	

8.2. Restart Services

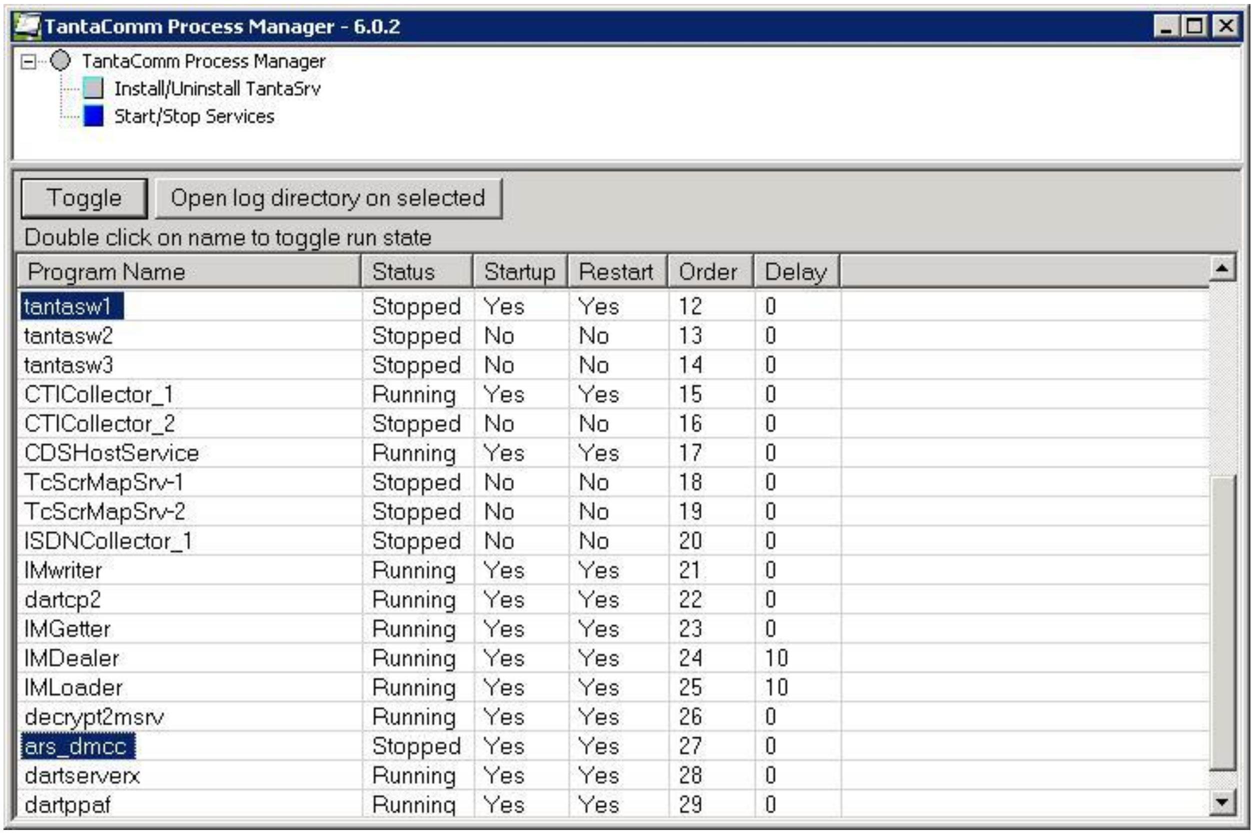
Navigate to C**:\TantaComm\System** directory, and double click on the **TantaProcManager** application shown below.



Name	Date modified	Type	Size
recsrvstats.exe	1/23/2012 2:32 PM	Application	102 KB
rw_test_file	6/4/2014 10:13 AM	File	131 KB
server.cer	2/10/2012 5:45 PM	Security Certificate	1 KB
TantaProcManager.exe	3/26/2013 5:15 PM	Application	69 KB
tantasrv.cmd	6/4/2014 10:12 AM	Windows Command ...	1 KB
tantasrv.cmd.old	6/3/2014 9:32 AM	OLD File	0 KB
TantaSrv.exe	7/19/2010 12:51 PM	Application	144 KB

TantaProcManager.exe Date modified: 3/26/2013 5:15 PM Date created: 3/26/2013 5:15 PM
Application Size: 69.0 KB

The **TantaComm Process Manager** screen is displayed. Scroll down as necessary to select and restart the **tantasw1** and **ars_dmcc**, as shown below.


TantaComm Process Manager - 6.0.2
TantaComm Process Manager
Install/Uninstall TantaSrv
Start/Stop Services
Toggle
Open log directory on selected

Double click on name to toggle run state

Program Name	Status	Startup	Restart	Order	Delay
tantasw1	Stopped	Yes	Yes	12	0
tantasw2	Stopped	No	No	13	0
tantasw3	Stopped	No	No	14	0
CTICollector_1	Running	Yes	Yes	15	0
CTICollector_2	Stopped	No	No	16	0
CDSHostService	Running	Yes	Yes	17	0
TcScrMapSrv-1	Stopped	No	No	18	0
TcScrMapSrv-2	Stopped	No	No	19	0
ISDNCollector_1	Stopped	No	No	20	0
IMwriter	Running	Yes	Yes	21	0
dartcp2	Running	Yes	Yes	22	0
IMGetter	Running	Yes	Yes	23	0
IMDealer	Running	Yes	Yes	24	10
IMLoader	Running	Yes	Yes	25	10
decrypt2msrv	Running	Yes	Yes	26	0
ars_dmcc	Stopped	Yes	Yes	27	0
dartserverx	Running	Yes	Yes	28	0
dartppaf	Running	Yes	Yes	29	0

9. Verification Steps

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

9.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify the 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     6        no    aes_125_72       established   57       57
```

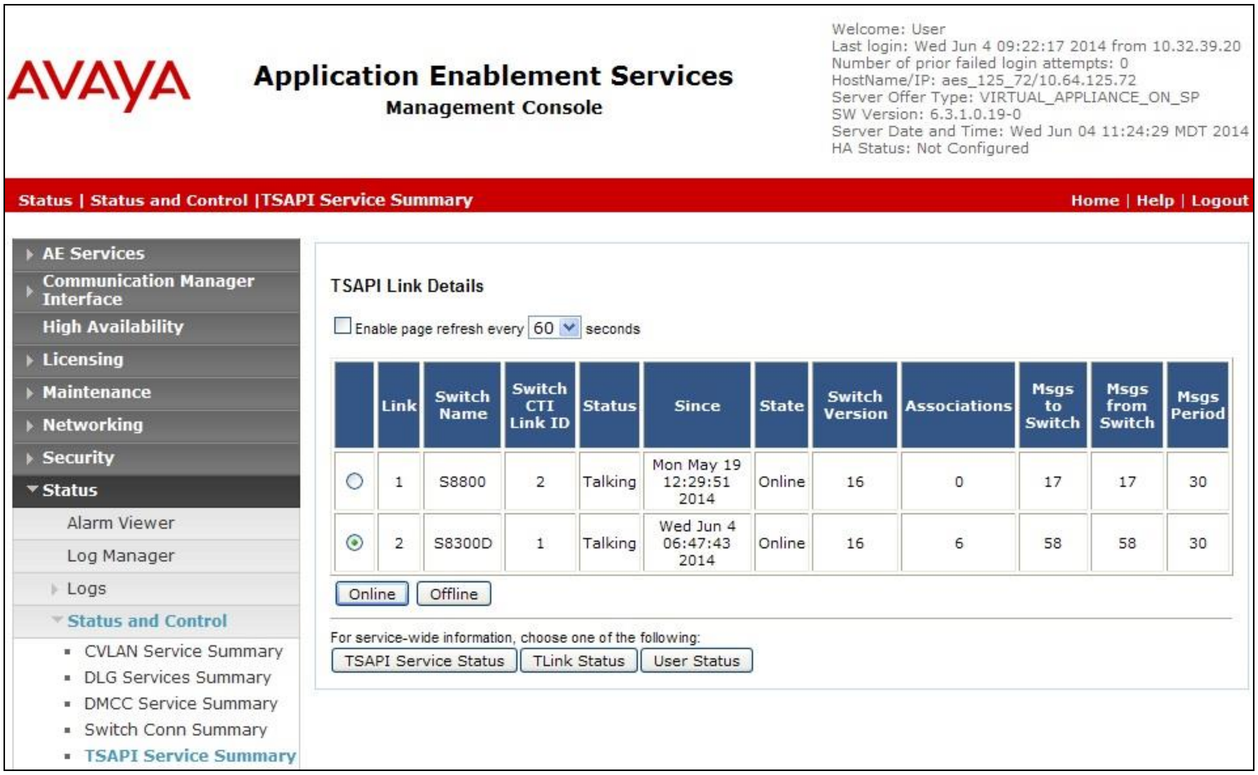
Verify the registration status of the virtual IP softphones by using the “list registered-ip-stations” command. Verify that all virtual IP softphone extensions from **Section 5.4** are displayed along with the IP address of the Application Enablement Services server, as shown below.

```
list registered-ip-stations

                            REGISTERED IP STATIONS

Station Ext    Set Type/ Prod ID/   TCP Station IP Address/
or Orig Port   Net Rgn   Release    Skt Gatekeeper IP Address
------------- --------- ---------- --- -------------------------------------
45000          9650      IP_Phone    y  10.32.39.106
               1         3.220A         10.32.39.83
45001          1616      IP_Phone    y  10.32.39.104
               1         1.350B         10.32.39.83
45991          4624      IP_API_A    y  10.64.125.72
               1         3.2040         10.32.39.83
45992          4624      IP_API_A    y  10.64.125.72
               1         3.2040         10.32.39.83
```

9.2. 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 monitored skill groups, agent stations, and virtual IP softphones from **Section 8.1**.



Welcome: User
Last login: Wed Jun 4 09:22:17 2014 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.1.0.19-0
Server Date and Time: Wed Jun 04 11:24:29 MDT 2014
HA Status: Not Configured

TSAPI Link Details

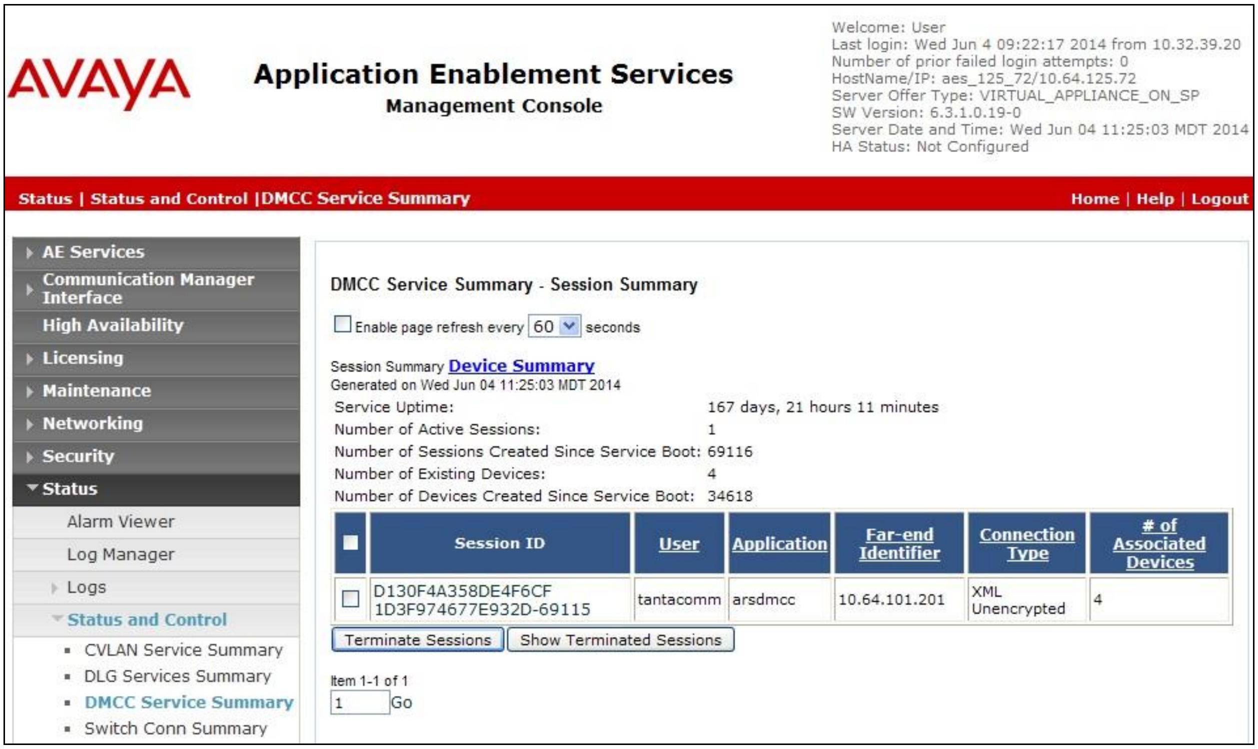
☐ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
○	1	S8800	2	Talking	Mon May 19 12:29:51 2014	Online	16	0	17	17	30
●	2	S8300D	1	Talking	Wed Jun 4 06:47:43 2014	Online	16	6	58	58	30

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

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 an active session with the TantaComm user name from **Section 6.8**, and that the **# of Associated Devices** column reflects the total number of virtual IP softphone and agent station extensions from **Section 8.1**.



Welcome: User
Last login: Wed Jun 4 09:22:17 2014 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.1.0.19-0
Server Date and Time: Wed Jun 04 11:25:03 MDT 2014
HA Status: Not Configured

DMCC Service Summary - Session Summary

☐ Enable page refresh every 60 seconds

Session Summary **Device Summary**
Generated on Wed Jun 04 11:25:03 MDT 2014

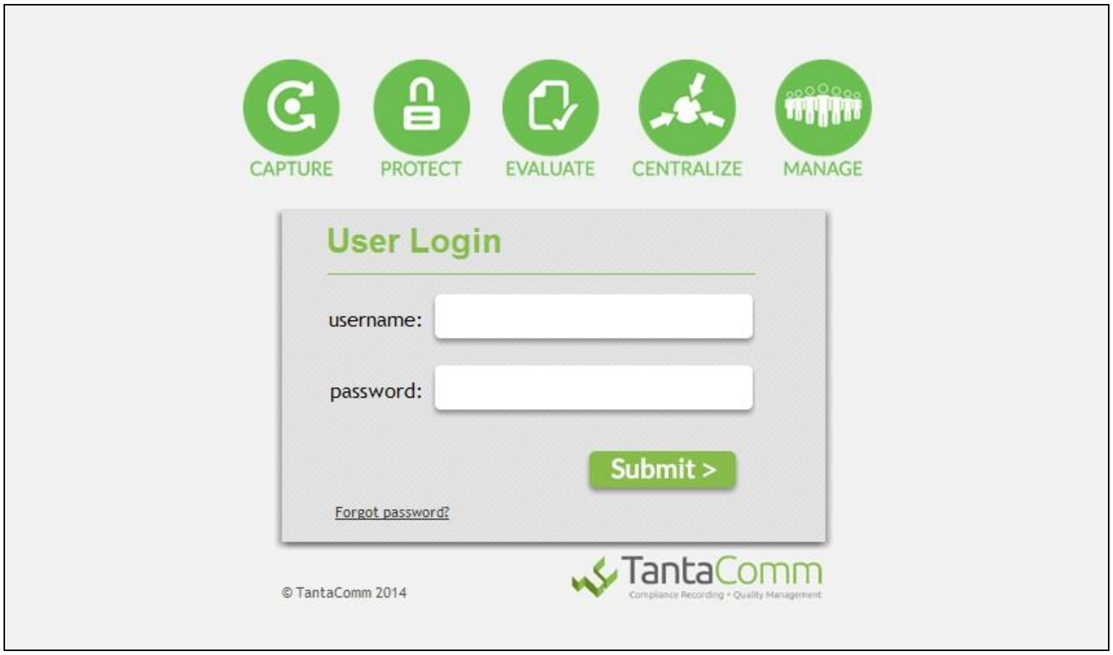
Service Uptime:	167 days, 21 hours 11 minutes
Number of Active Sessions:	1
Number of Sessions Created Since Service Boot:	69116
Number of Existing Devices:	4
Number of Devices Created Since Service Boot:	34618

☐	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
☐	D130F4A358DE4F6CF 1D3F974677E932D-69115	tantacomm	arsdmcc	10.64.101.201	XML Unencrypted	4

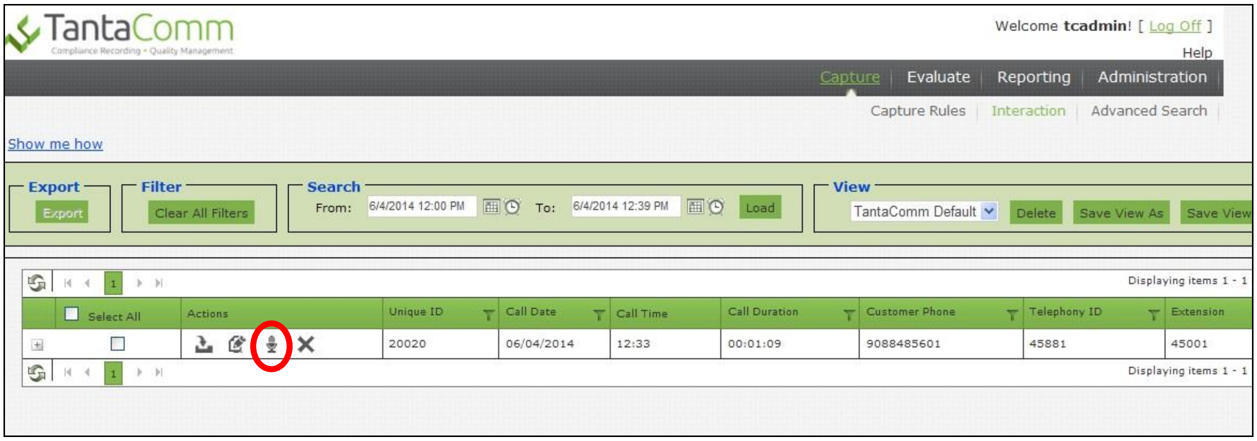
Item 1-1 of 1
1

9.3. Verify TantaComm Capture

Log an agent into the skill group to handle and complete an ACD call. Access the Capture web-based interface by using the URL “http://ip-address/capture” in an Internet browser window, where “ip-address” is the IP address of the Capture server. Log in using the appropriate credentials.



The **TantaComm** screen below is displayed. Set the applicable **Search** date and time range to display a list of recent recording entries. Verify that there is an entry reflecting the last call, with proper values in the relevant fields. Click on the associated **Play Audio** icon shown below.



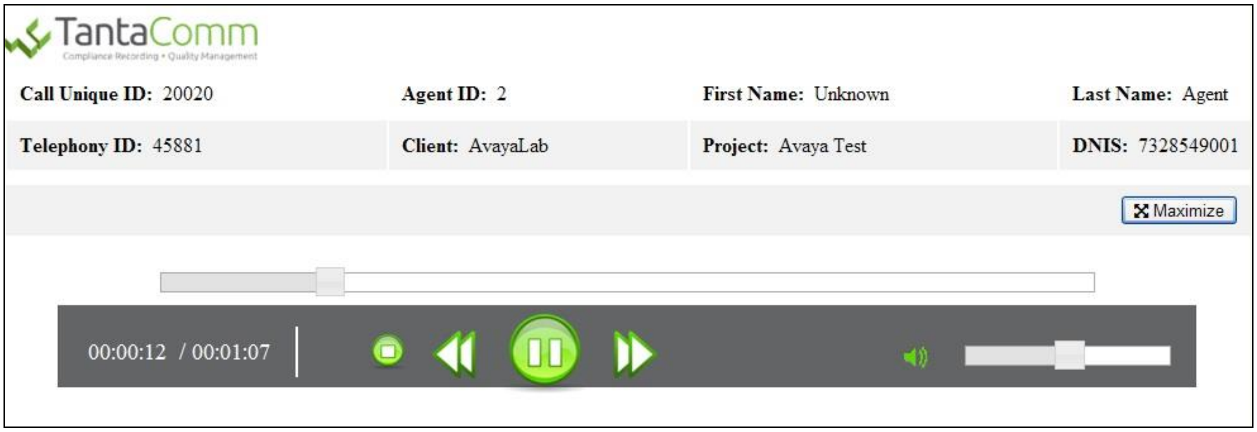
From: 6/4/2014 12:00 PM To: 6/4/2014 12:39 PM

View: TantaComm Default

	☐ Select All	Actions	Unique ID	Call Date	Call Time	Call Duration	Customer Phone	Telephony ID	Extension
+	☐		20020	06/04/2014	12:33	00:01:09	9088485601	45881	45001

Verify that a pop-up screen is displayed and that the call recording is played back.

Note that the **Project** and **Client** names shown below were all pre-configured parameters, and that the agent **First Name** and **Last Name** can be configured on the Capture server if desired for display purposes. The agent names shown below are the default values.



Call Unique ID: 20020	**Agent ID:** 2	**First Name:** Unknown	**Last Name:** Agent
Telephony ID: 45881	**Client:** AvayaLab	**Project:** Avaya Test	**DNIS:** 7328549001

10. Conclusion

These Application Notes describe the configuration steps required for TantaComm Capture to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services 6.3 using Single Step Conference. All feature and serviceability test cases were completed with an observation noted in **Section 2.2**.

11. Additional References

This section references the product documentation relevant to these Application Notes.

1. *Administering Avaya Aura® Communication Manager*, Document 03-300509, Issue 9, Release 6.3, October 2013, available at http://support.avaya.com.

2. *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 6.3, Issue 2, October 2013, available at http://support.avaya.com.

3. *CAPTURE VOIP Recording with DMCC*, 2013, available upon request to TantaComm support.

4. *TantaComm Capture Administration guides*, available upon request to TantaComm support.

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.