Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Aura Alliance Client for Notes/Sametime Deskphone Mode with Avaya Engagement Call Control Snap-in installed on Avaya Breeze™ – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Aura Alliance Client for Notes/Sametime application to interoperate with Avaya Engagement Call Control Snap-in installed on Avaya Breeze.

In the compliance testing, Aura Alliance Client for Notes/Sametime application used HTTPS protocol to connect to Avaya Engagement Call Control service to get events and monitor a deskphone on Avaya Aura® Communication Manager.

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 at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration steps required for Aura Alliance Client for Notes/Sametime application to interoperate with Avaya Engagement Call Control (ECC) Snap-in installed on Avaya Breeze. Engagement Call Control uses Application Enablement Services Device, Media and Call Control (DMCC) APIs and exposes a subset of the call control features as Representational State Transfer (REST) API and also publishes call events over HTTP.

In the compliance testing, Aura Alliance Client for Notes/Sametime is windows-based application that received call events from Engagement Call Control service to monitor and control a deskphone on Avaya Aura® Communication Manager.

2. General Test Approach and Test Results

The feature test cases were performed manually.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to the workstation which Aura Alliance Client application installed on it and restarting the Engagement Call Control service.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Avaya systems and the Aura Alliance Client for Notes/Sametime utilized enabled capabilities of Transport Layer Security (TLS) and HTTPS as requested by Aura Alliance

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. The feature testing focused on verifying the following on Aura Alliance Client for Notes/Sametime: Monitor and receive call events such as answer incoming call, place outgoing call, put call on hold...etc.

The serviceability testing focused on verifying the ability of Aura Alliance Client for Notes/Sametime to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection from the workstation and restarting the AES server.

2.2. Test Results

All test cases were executed and passed successfully.

2.3. Support

Support from Avaya is available by visiting the website http://support.avaya.com and a list of product documentation can be found in **Section 9** of these Application Notes. Technical support for the Aura Alliance Client product can be obtained as follows:

Aura Alliance Limited
Tel: +44 (0)20 3127 7761
http://www.auraalliance.com/global-support/

3. Reference Configuration

Figure 1 illustrates a sample configuration consisting of Avaya Aura® System Manager, Avaya Aura® Session Manager, Avaya Aura® Communication Manager, and Avaya Aura® Media Server running on Virtualized Environment. The Avaya G450 Media Gateway registers to Communication Manager and has PRI/T1 trunk to simulated PSTN. The Aura Alliance Client for Notes/Sametime was running on a Windows 10. Avaya Engagement Call Control snap-in installed on top of Avaya Breeze which has a TSAPI connection to Avaya Aura® Application Enablement Services server.

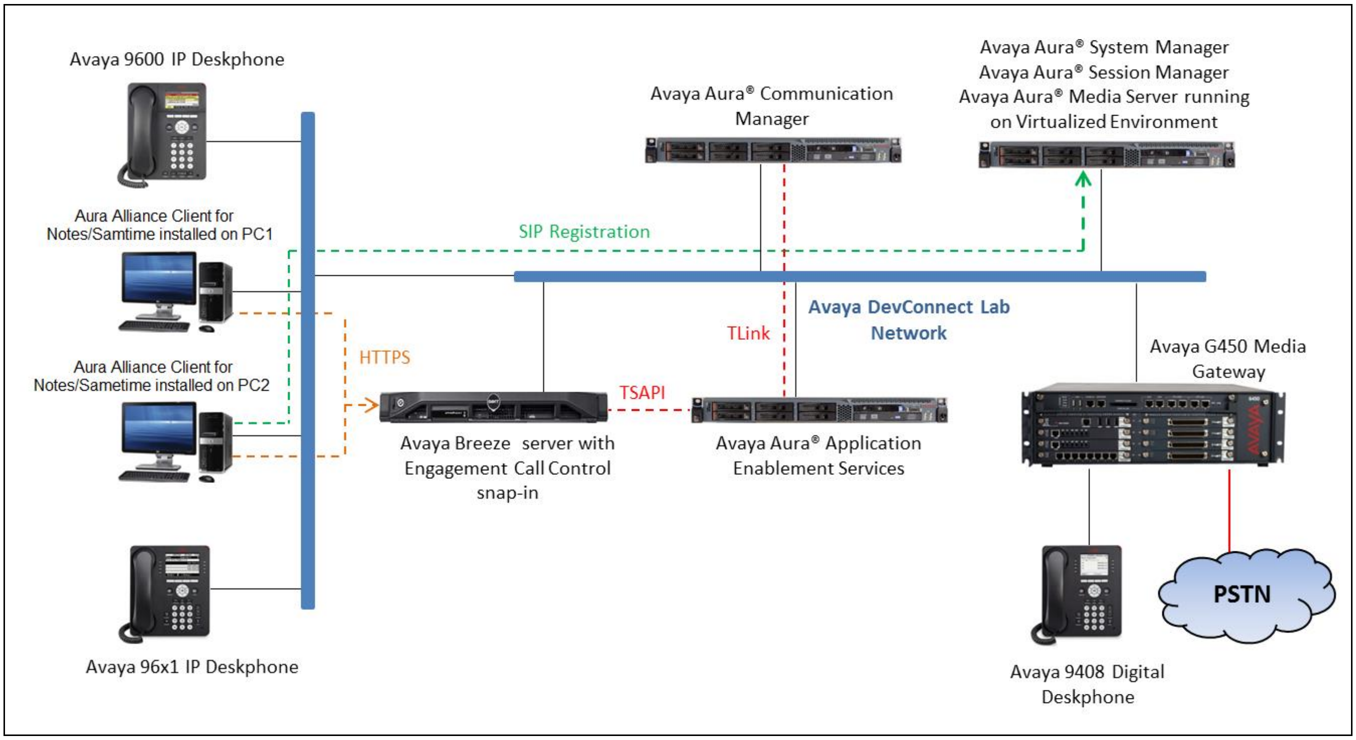

Avaya 9600 IP Deskphone
Aura Alliance Client for Notes/Samtime installed on PC1
Aura Alliance Client for Notes/Samtime installed on PC2
Avaya 96x1 IP Deskphone
Avaya Aura® Communication Manager
Avaya Aura® System Manager
Avaya Aura® Session Manager
Avaya Aura® Media Server running on Virtualized Environment
SIP Registration
HTTPS
TLink
TSAPI
Avaya DevConnect Lab Network
Avaya Breeze server with Engagement Call Control snap-in
Avaya Aura® Application Enablement Services
Avaya G450 Media Gateway
PSTN
Avaya 9408 Digital Deskphone

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 running in Virtual Environment	R017x.01.0.532. 7.1.1 FP1
Avaya G450 Media Gateway	38.20.0
Avaya Aura® Media Server running in Virtual Environment	7.8.0.333
Avaya Aura® Application Enablement Services in Virtual Environment	7.1.1.0.0.5-0
Avaya Aura® System Manager running on Virtualized Environment	7.1.1 FP1
Avaya Aura® Session Manager running on Virtualized Environment	7.1.1.0.711008
Avaya Breeze™	3.3.1.1
Avaya Engagement Call Control	3.3.0.0
Avaya 9611G IP Deskphone (SIP)	Avaya one-X® Deskphone Release 7.1.1
Avaya 9641GS IP Deskphone (H.323)	Avaya one-X® Deskphone Release 6.65
Aura Alliance Client running on IBM Notes IBM Notes	10.1.11 9.0 FP9

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 AE Services

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 4**. If this option is not set to "y", then contact the Avaya sales team or business partner for a proper license file.

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

    Abbreviated Dialing Enhanced List? y          Audible Message Waiting? y
        Access Security Gateway (ASG)? n              Authorization Codes? y
        Analog Trunk Incoming Call ID? y                       CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? y                         CAS Main? n
Answer Supervision by Call Classifier? y                Change COR by FAC? n
                                  ARS? y  Computer Telephony Adjunct Links? y
                 ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? n                      DCS (Basic)? y
          ASAI Link Core Capabilities? n                DCS Call Coverage? y
          ASAI Link Plus Capabilities? n               DCS with Rerouting? 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: 3332
     Type: ADJ-IP
                                                                    COR: 1
     Name: AES70
```

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  19
                        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: 01
     Copy UCID for Station Conference/Transfer? y
```

Navigate to **Page 13**, and enable **Send UCID to ASAI**. This parameter allows for the universal call ID to be sent to ASAI and it will be used by Engagement Call Control application.

```
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
  Prefer H.323 Over SIP For Dual-Reg Station 3PCC Make Call? n
```

5.4. Administer AE Services

To administer the transport link to AES, use the command “change ip-services”. On Page 1, add an entry with the following values. **Service Type** should be selected as **AESVCS**, enter “y” in **Enabled**, “procr” in the **Local Node** and “8765” in the **Local Port**.

```
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.**The password entered for **Password** field must match the password on the AES server in the Switch Connection in **Section 6.3**. The **AE Services Server** should match with the host name of the AES server. To obtain the host name of AES server, use the command “**uname –n**” in the Linux command prompt.

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

   Server ID    AE Services       Password          Enabled    Status
                   Server
      1:      aes70            *                      y        in use
```

6. Configure Avaya Aura® Application Enablement Services

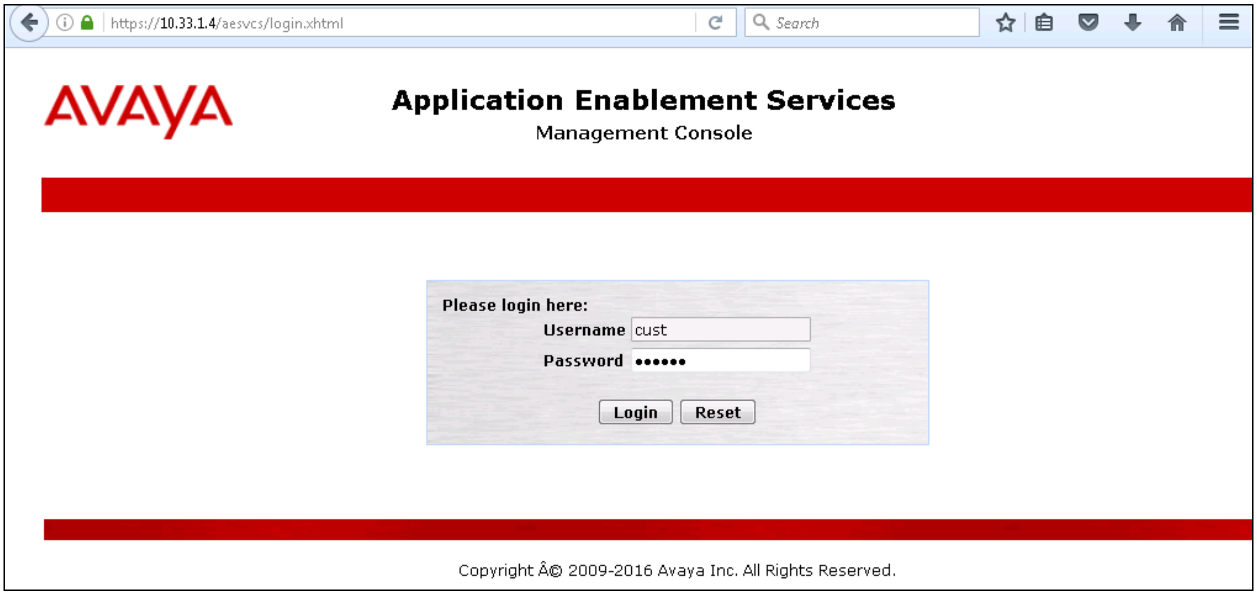
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer Switch Connection
- Administer TSAPI link
- Administer CTI user
- Administer Security Database
- Administer ports
- Restart services

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.

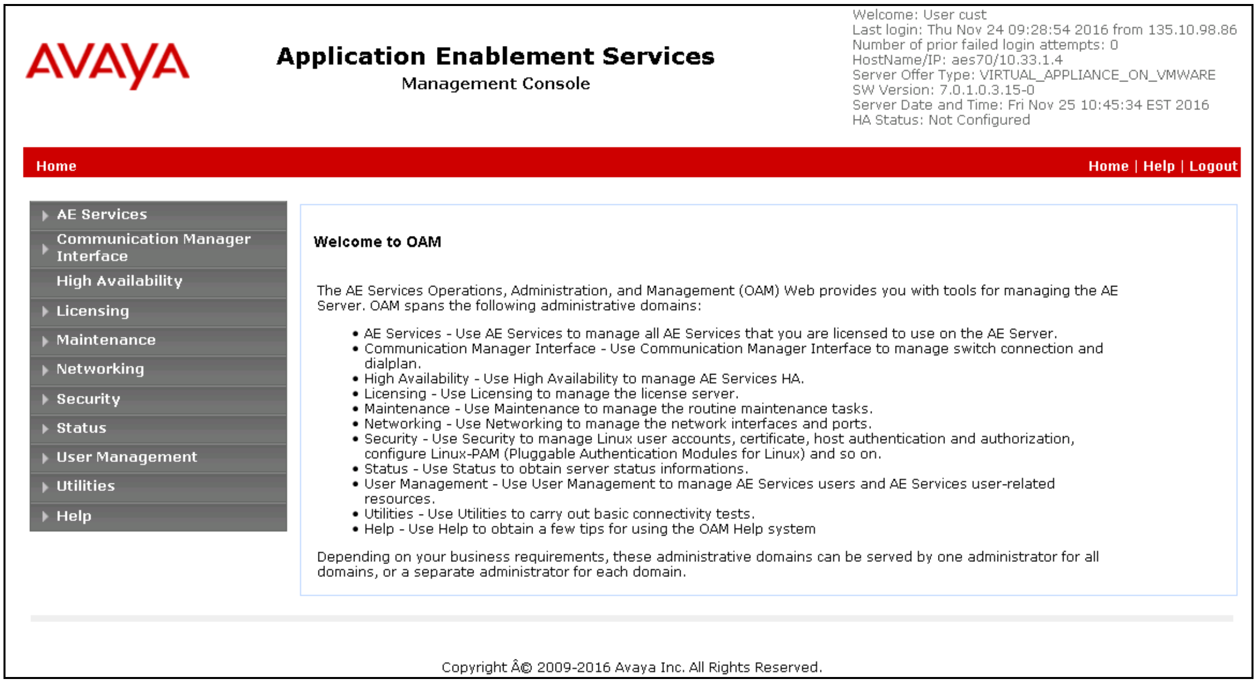


https://10.33.1.4/aesvcs/login.xhtml

Application Enablement Services
Management Console

Please login here:
Username cust
Password ••••••

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



Welcome: User cust
Last login: Thu Nov 24 09:28:54 2016 from 135.10.98.86
Number of prior failed login attempts: 0
HostName/IP: aes70/10.33.1.4
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.3.15-0
Server Date and Time: Fri Nov 25 10:45:34 EST 2016
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:

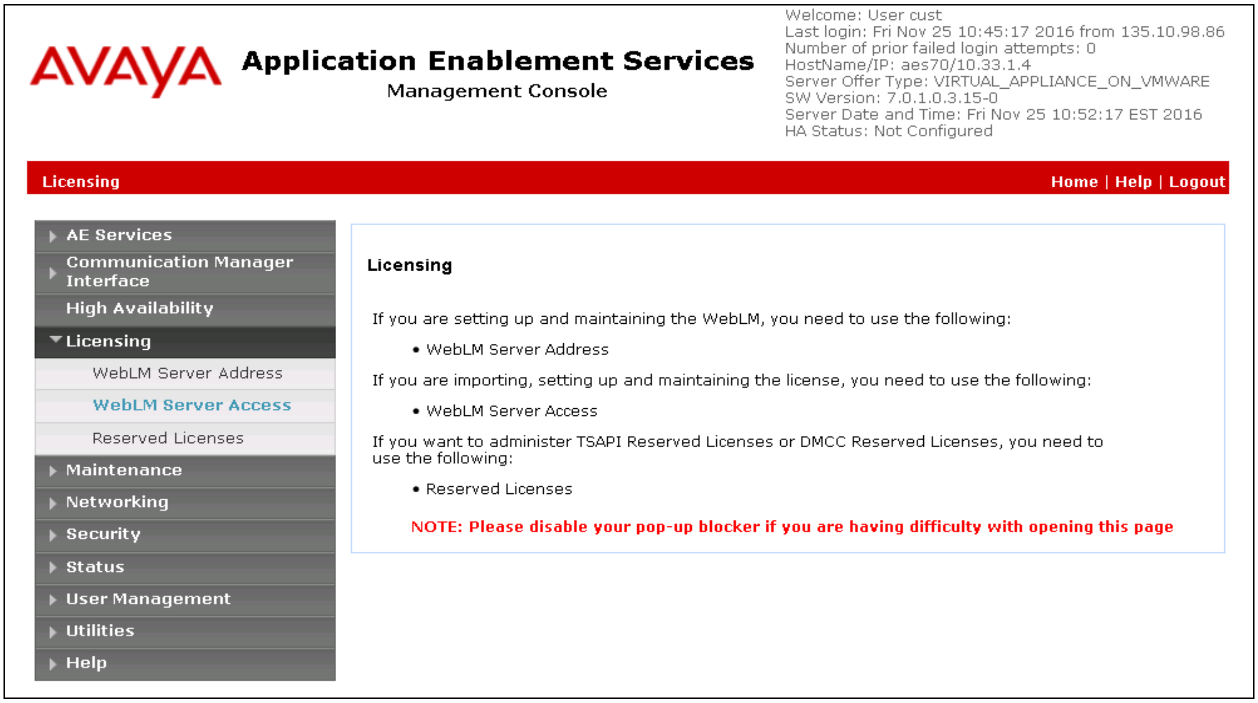
- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- High Availability - Use High Availability to manage AE Services HA.
- Licensing - 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 Â© 2009-2016 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: Fri Nov 25 10:45:17 2016 from 135.10.98.86
Number of prior failed login attempts: 0
HostName/IP: aes70/10.33.1.4
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.3.15-0
Server Date and Time: Fri Nov 25 10:52:17 EST 2016
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

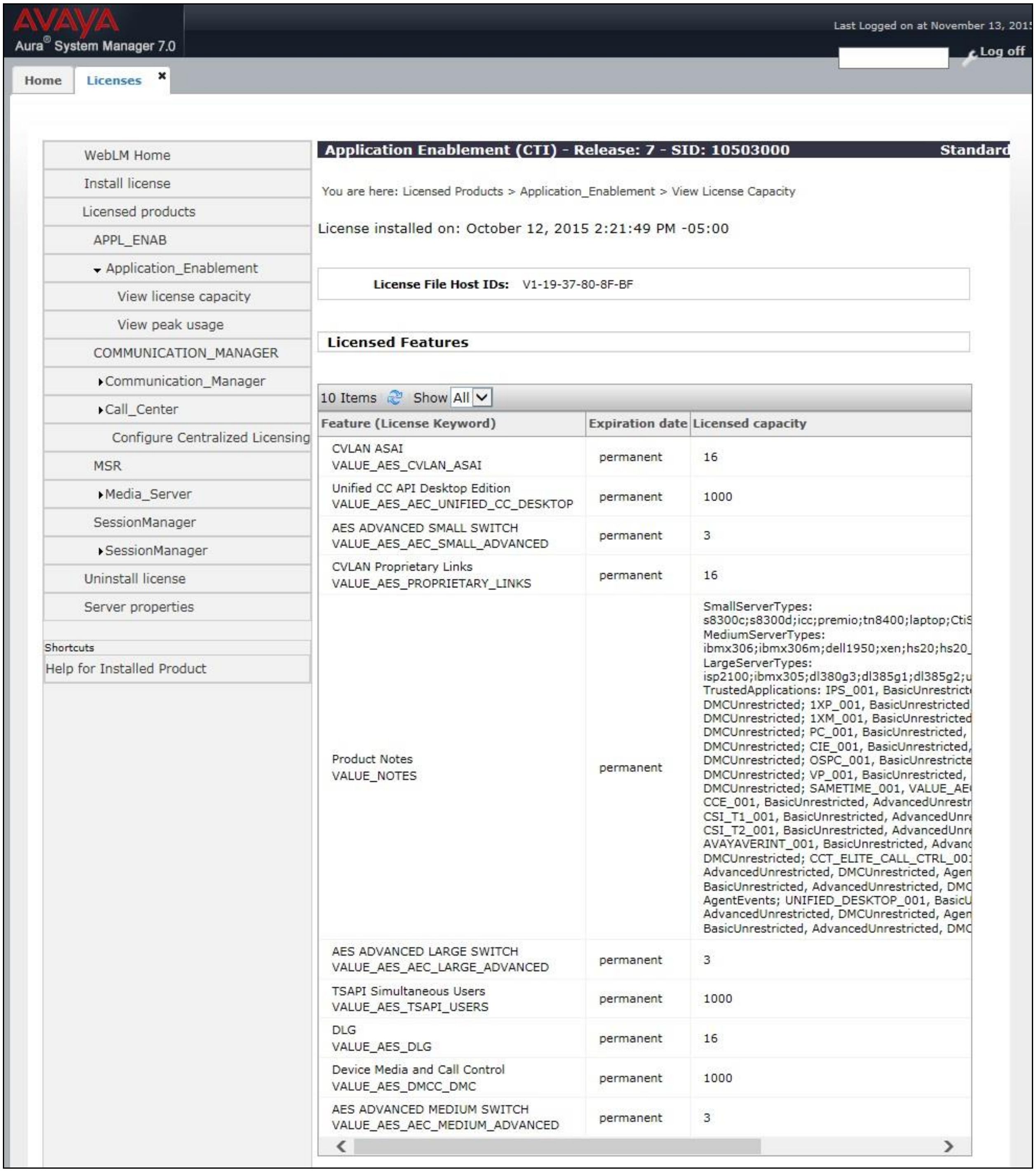
If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:

- Reserved Licenses

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

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**, as shown below.



Application Enablement (CTI) - Release: 7 - SID: 10503000 **Standard**

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

License installed on: October 12, 2015 2:21:49 PM -05:00

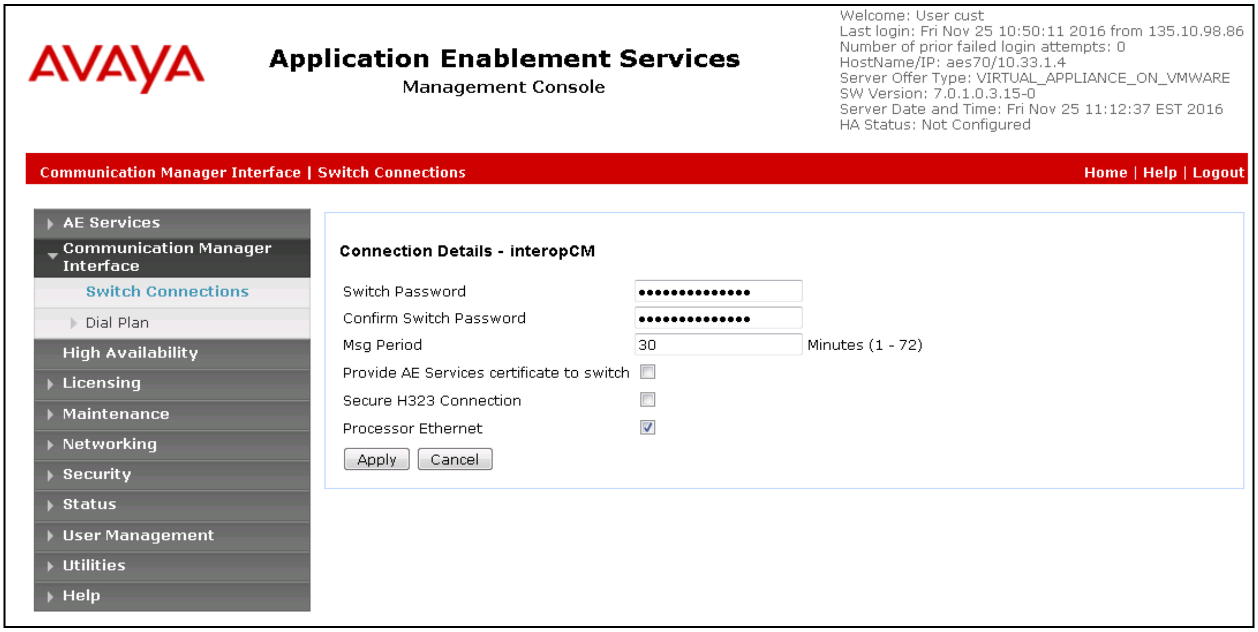
License File Host IDs: V1-19-37-80-8F-BF

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	1000
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	3
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;u TrustedApplications: IPS_001, BasicUnrestrict DMCUnrestricted; 1XP_001, BasicUnrestricted DMCUnrestricted; 1XM_001, BasicUnrestricted DMCUnrestricted; PC_001, BasicUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted, DMCUnrestricted; OSPC_001, BasicUnrestricte DMCUnrestricted; VP_001, BasicUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AE CCE_001, BasicUnrestricted, AdvancedUnrestr CSI_T1_001, BasicUnrestricted, AdvancedUnr CSI_T2_001, BasicUnrestricted, AdvancedUnr AVAYAVERINT_001, BasicUnrestricted, Advanc DMCUnrestricted; CCT_ELITE_CALL_CTRL_00 AdvancedUnrestricted, DMCUnrestricted, Agen BasicUnrestricted, AdvancedUnrestricted, DMC AgentEvents; UNIFIED_DESKTOP_001, BasicU AdvancedUnrestricted, DMCUnrestricted, Agen BasicUnrestricted, AdvancedUnrestricted, DMC
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	3
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	1000
DLG VALUE_AES_DLG	permanent	16
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	1000
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	3

6.3. Administer Switch Connection

Select **Communication Manager Interface → Switch Connections** from the left pane of the **Management Console**, enter a name in **Switch Connection** box and click **Add** button (not shown). Enter the password as configured in **Section 5.4** in the **Switch Password** and **Confirm Switch Password** fields and check on **Processor Ethernet** field if the Processor Ethernet is used in Communication Manager. Click **Apply** button to save the configuration.

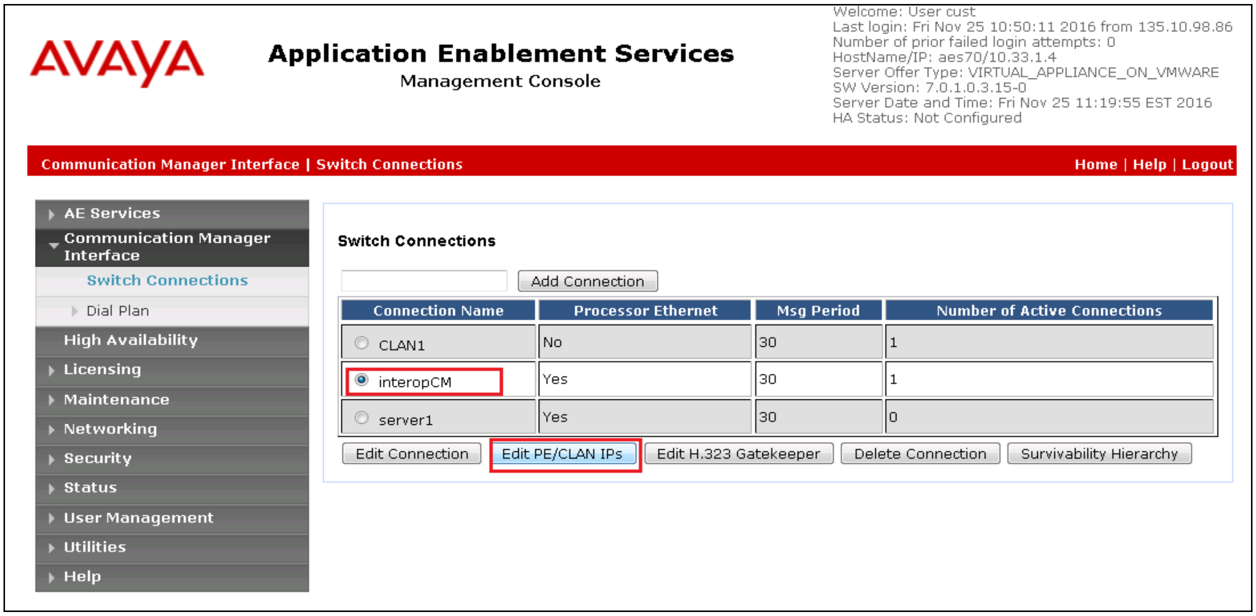


Welcome: User cust
Last login: Fri Nov 25 10:50:11 2016 from 135.10.98.86
Number of prior failed login attempts: 0
HostName/IP: aes70/10.33.1.4
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.3.15-0
Server Date and Time: Fri Nov 25 11:12:37 EST 2016
HA Status: Not Configured

Connection Details - interopCM

Switch Password	••••••••••••••
Confirm Switch Password	••••••••••••••
Msg Period	30 Minutes (1 - 72)
Provide AE Services certificate to switch	□
Secure H323 Connection	□
Processor Ethernet	☑

Select the **interopCM** switch connection that has been added above, and select **Edit PE/CLAN IPs** to add the IP address for the switch connection.

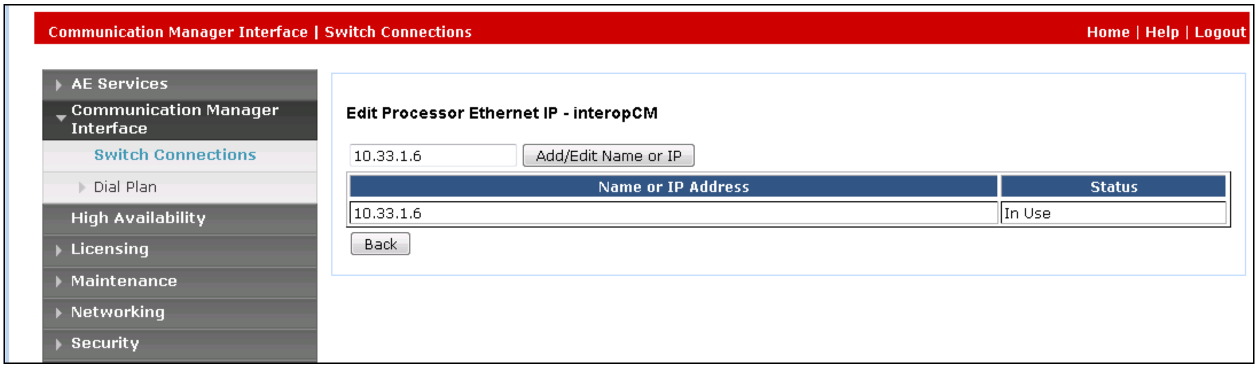


Welcome: User cust
Last login: Fri Nov 25 10:50:11 2016 from 135.10.98.86
Number of prior failed login attempts: 0
HostName/IP: aes70/10.33.1.4
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.3.15-0
Server Date and Time: Fri Nov 25 11:19:55 EST 2016
HA Status: Not Configured

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
○ CLAN1	No	30	1
● interopCM	Yes	30	1
○ server1	Yes	30	0

Enter the IP address of the Processor Ethernet of Communication Manager in the box and click the **Add/Edit Name of IP** button to add the IP.

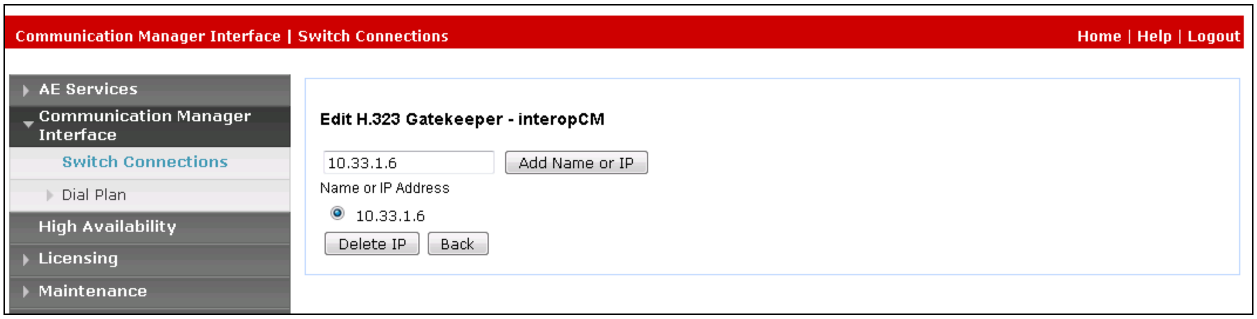


Edit Processor Ethernet IP - interopCM

10.33.1.6

Name or IP Address	Status
10.33.1.6	In Use

Select **Edit H.323 Gatekeeper** button from the Switch Connection page to add an IP address of gate keeper, the Gatekeeper IP address in this case is also the Processor Ethernet.



Edit H.323 Gatekeeper - interopCM

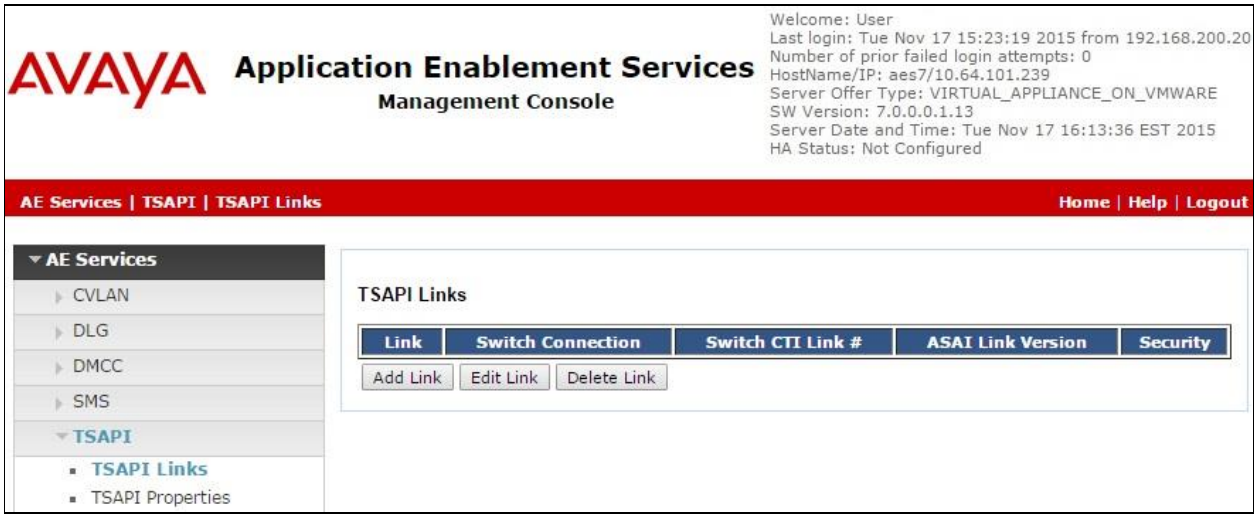
10.33.1.6

Name or IP Address

● 10.33.1.6

6.4. 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**.

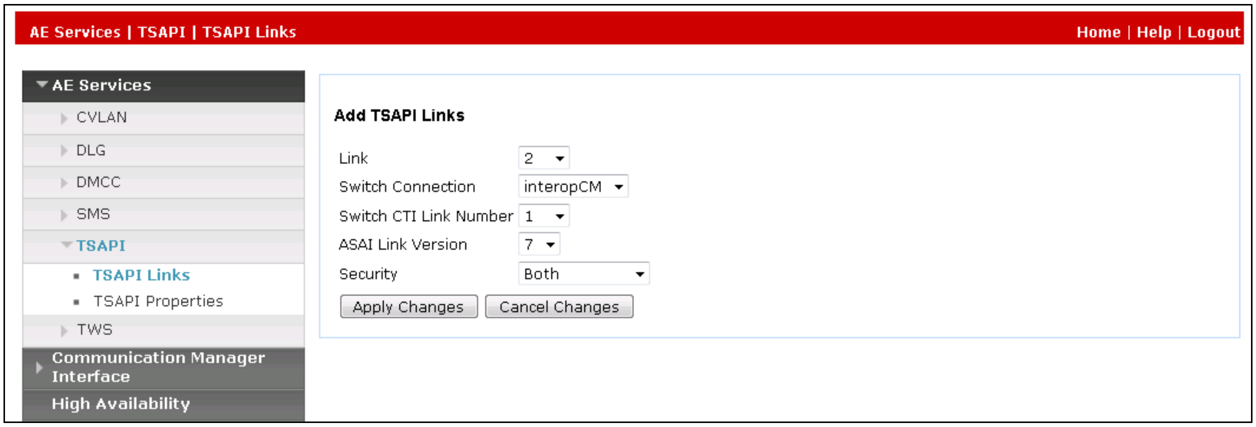


Welcome: User
Last login: Tue Nov 17 15:23:19 2015 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.0.0.1.13
Server Date and Time: Tue Nov 17 16:13:36 EST 2015
HA Status: Not Configured

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security

The **Add TSAPI Links** screen is displayed in the right side. 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 "**interopCM**" ,which was added in Section 6.3 above, was selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Select **Both** in the **Security** dropdown menu to support both unencrypted and encrypted TSAPI links. Retain the default values in the remaining fields.



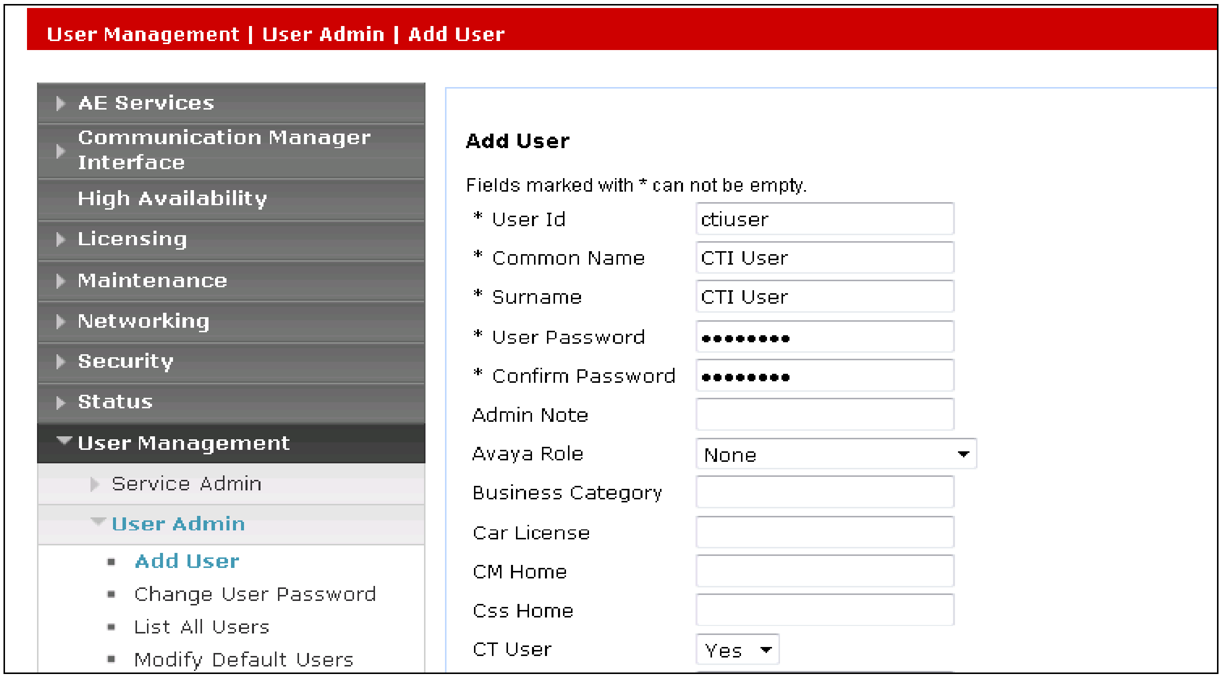
Add TSAPI Links

Link	2
Switch Connection	interopCM
Switch CTI Link Number	1
ASAI Link Version	7
Security	Both

Apply Changes | Cancel Changes

6.5. Administer CTI 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.



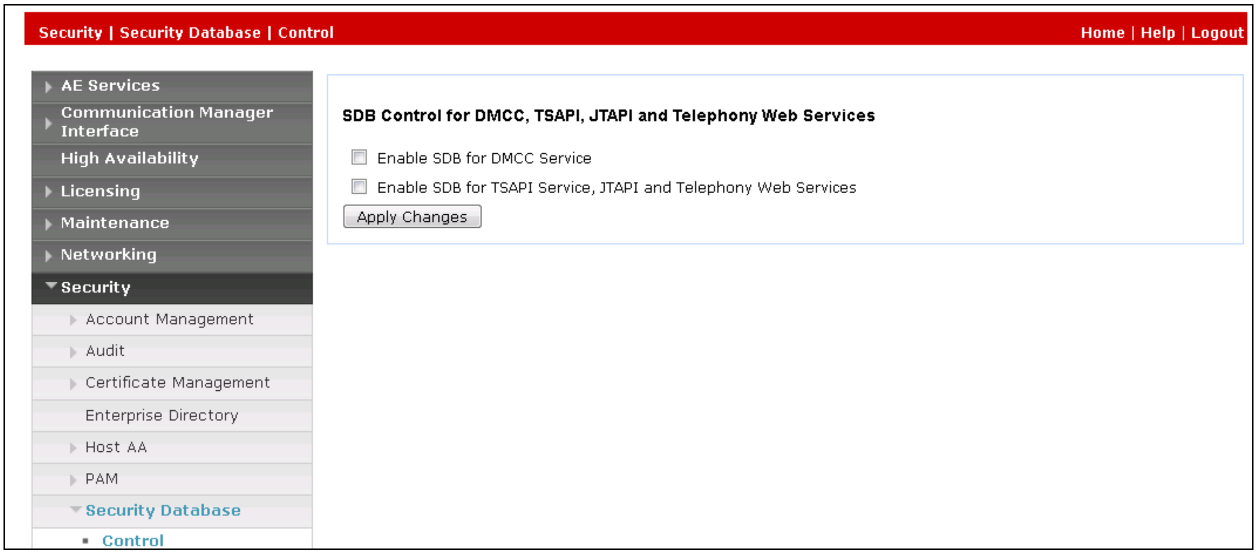
Add User

Fields marked with * can not be empty.

* User Id	ctiuser
* Common Name	CTI User
* Surname	CTI User
* User Password	••••••••
* Confirm Password	••••••••
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes

6.6. Configure 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.



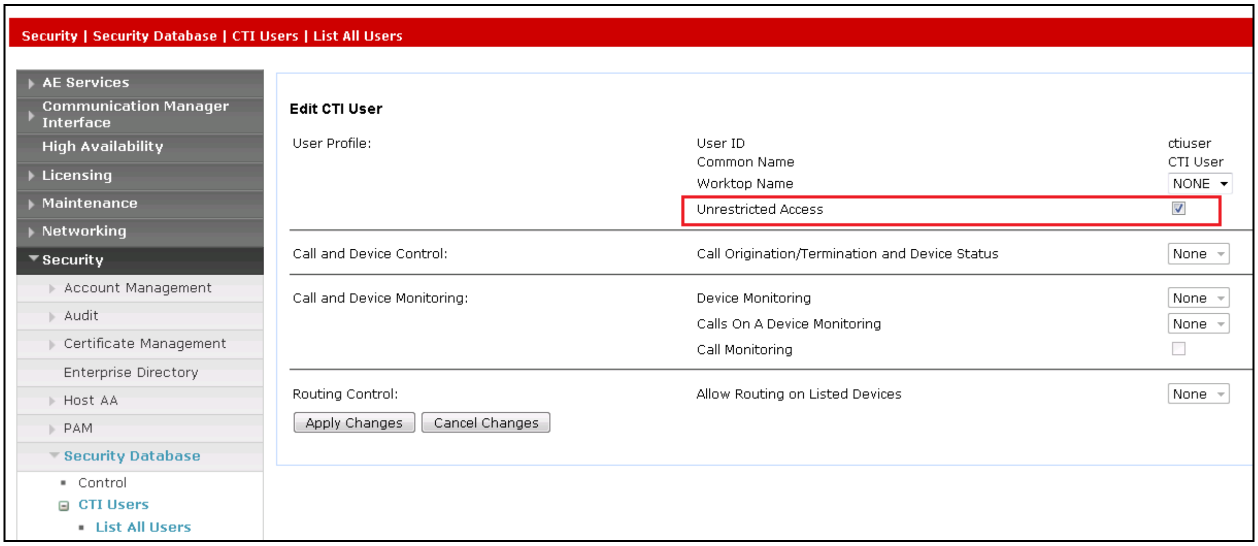
SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services

□ Enable SDB for DMCC Service

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

Apply Changes

Select **Security → Security Database → CTI Users → List All Users** and select the CTI user which was created in **Section 6.5** and select **Edit** button (not shown). In the **Edit CTI User**, select the check box **Unrestricted Access** and click **Apply Changes** to save the configuration.



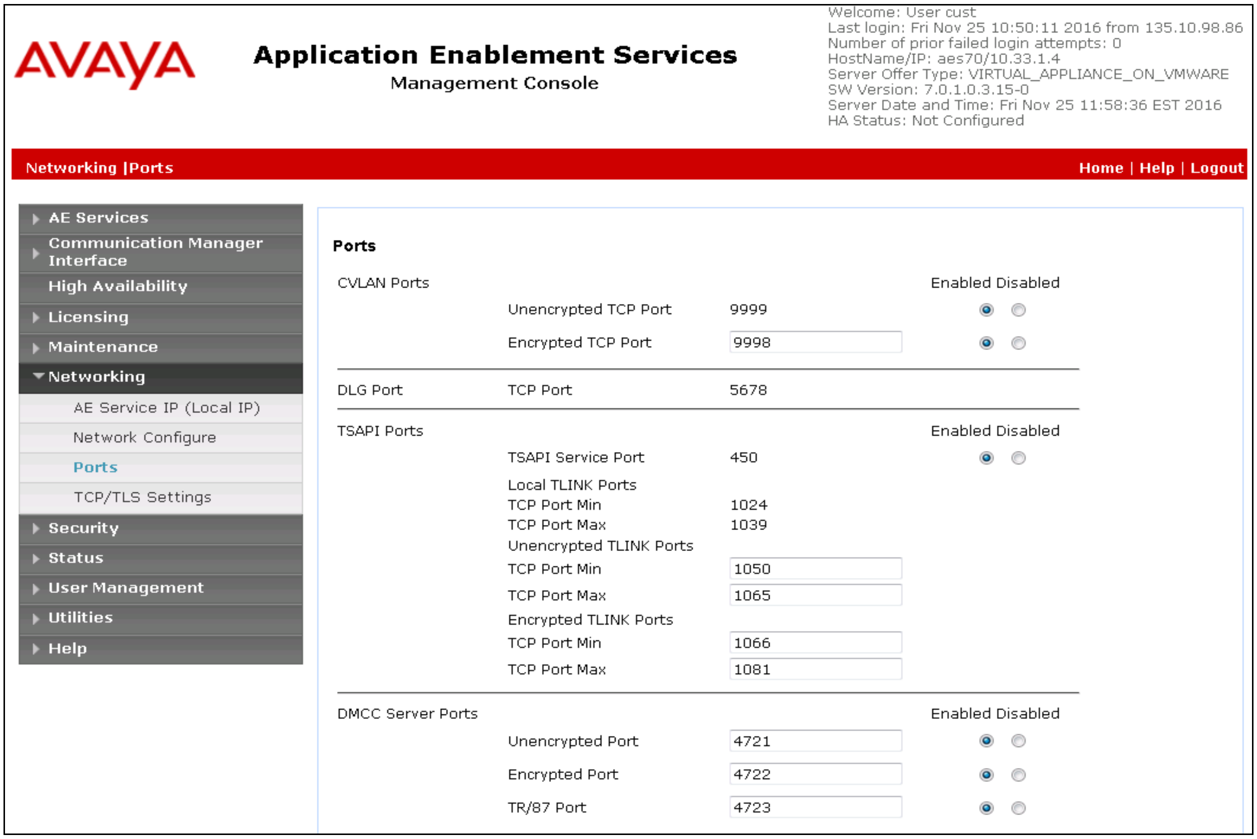
Edit CTI User

User Profile:	User ID	ctiuser
	Common Name	CTI User
	Worktop Name	NONE
	Unrestricted Access	☑
Call and Device Control:	Call Origination/Termination and Device Status	None
Call and Device Monitoring:	Device Monitoring	None
	Calls On A Device Monitoring	None
	Call Monitoring	□
Routing Control:	Allow Routing on Listed Devices	None

Apply Changes   Cancel Changes

6.7. Administer Ports

Select **Networking → Ports** from the left pane, to display the **Ports** screen in the right pane. In **TSAPI Ports** section, select the radio button for **TSAPI Service Port 450** and in the **DMCC Server Ports** section, select the radio button for **Unencrypted Port 4721** under the **Enabled** column, as shown below. Retain the default values in the remaining fields.



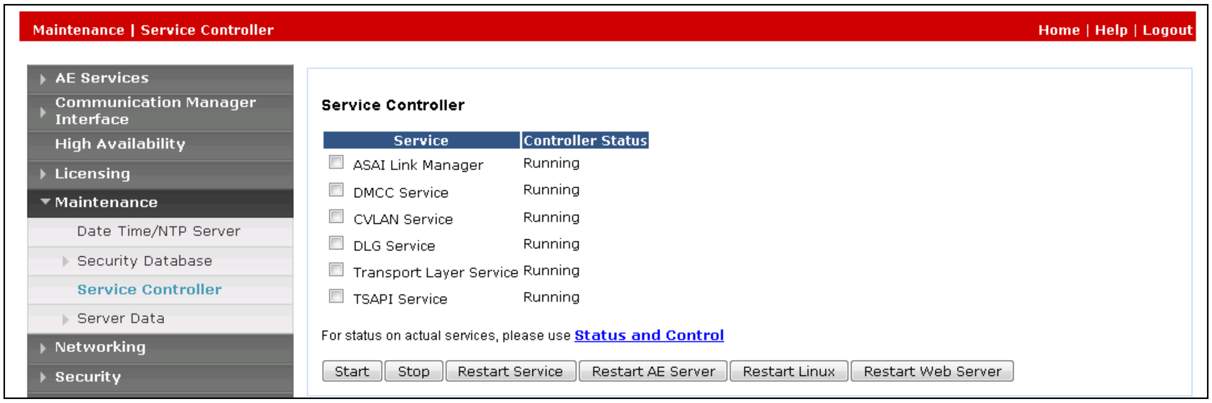
Welcome: User cust
Last login: Fri Nov 25 10:50:11 2016 from 135.10.98.86
Number of prior failed login attempts: 0
HostName/IP: aes70/10.33.1.4
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.3.15-0
Server Date and Time: Fri Nov 25 11:58:36 EST 2016
HA Status: Not Configured

Ports

			Enabled	Disabled
CVLAN Ports			Enabled	Disabled
	Unencrypted TCP Port	9999	●	○
	Encrypted TCP Port	9998	●	○
DLG Port	TCP Port	5678		
TSAPI Ports			Enabled	Disabled
	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			Enabled	Disabled
	Unencrypted Port	4721	●	○
	Encrypted Port	4722	●	○
	TR/87 Port	4723	●	○

6.8. Restart Services

Select **Maintenance → Service Controller** from the left pane, to display the **Service Controller** screen in the right pane. Click **Restart AE Service**.



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**

7. Configure Avaya Breeze and Engagement Call Control Service

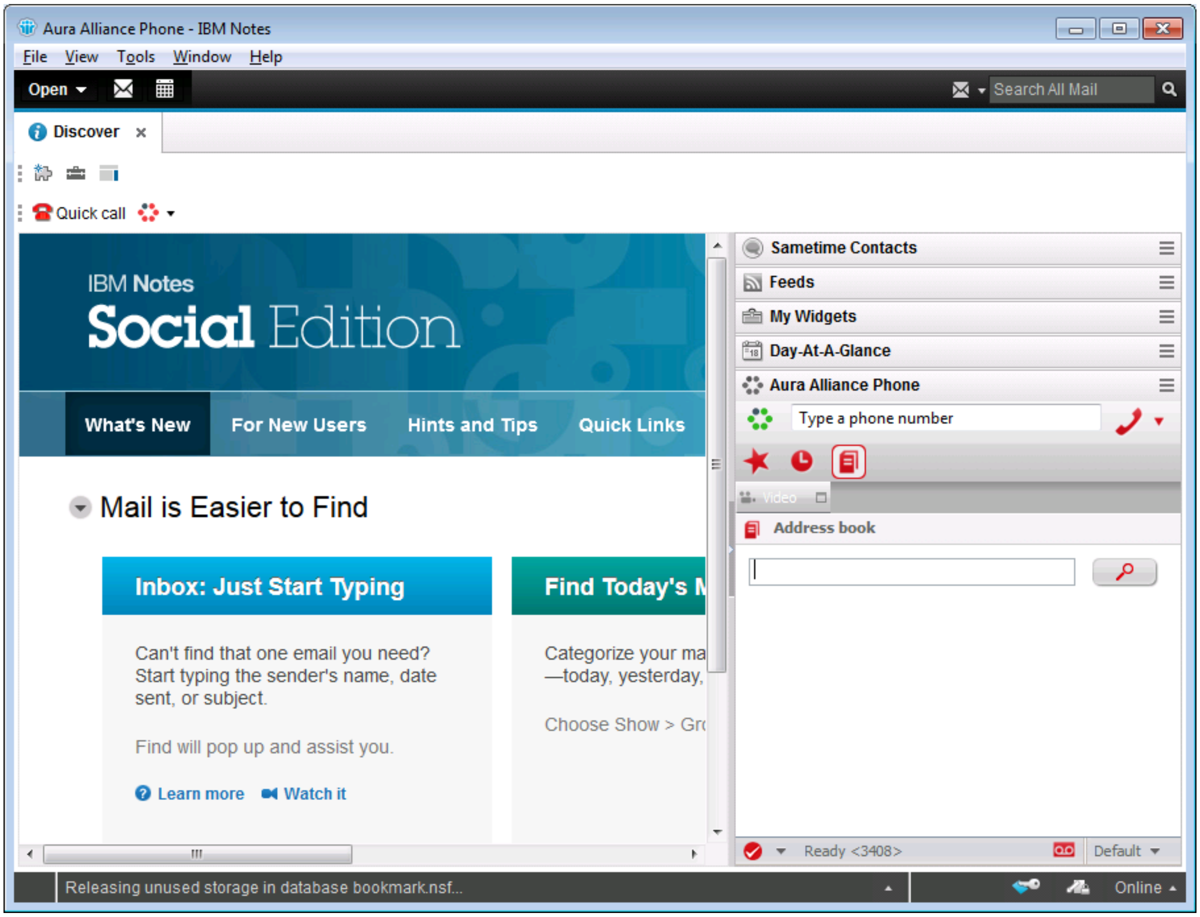
This document assumes Avaya Breeze™ and Engagement Call Control snap-in are already in place and configured. For procedure of how to install and configure Avaya Engagement Call Control snap-in on Avaya Breeze, please refer to **Section 11[2]**.

8. Configure Aura Alliance Client for Notes/Sametime

This section provides steps to configure the Aura Alliance Client application. During compliance test, the installation and configuration of Aura Alliance Client application was performed by an Aura Alliance engineer. This section describes the initial and basic configuration of the Aura Alliance Client application.

From the PC where IBM Notes application is installed, run the Aura Alliance Phone application from the Start menu. The Aura Alliance Phone – IBM Notes window is displayed as below.

Note: In order for Aura Alliance Client for Notes/Sametime to control a SIP deskphone, ensure that SIP deskphone has **Type of 3PCC Enabled** set to **Avaya** and use TLS protocol to register to Session Manager.



Can't find that one email you need? Start typing the sender's name, date sent, or subject.

Find will pop up and assist you.

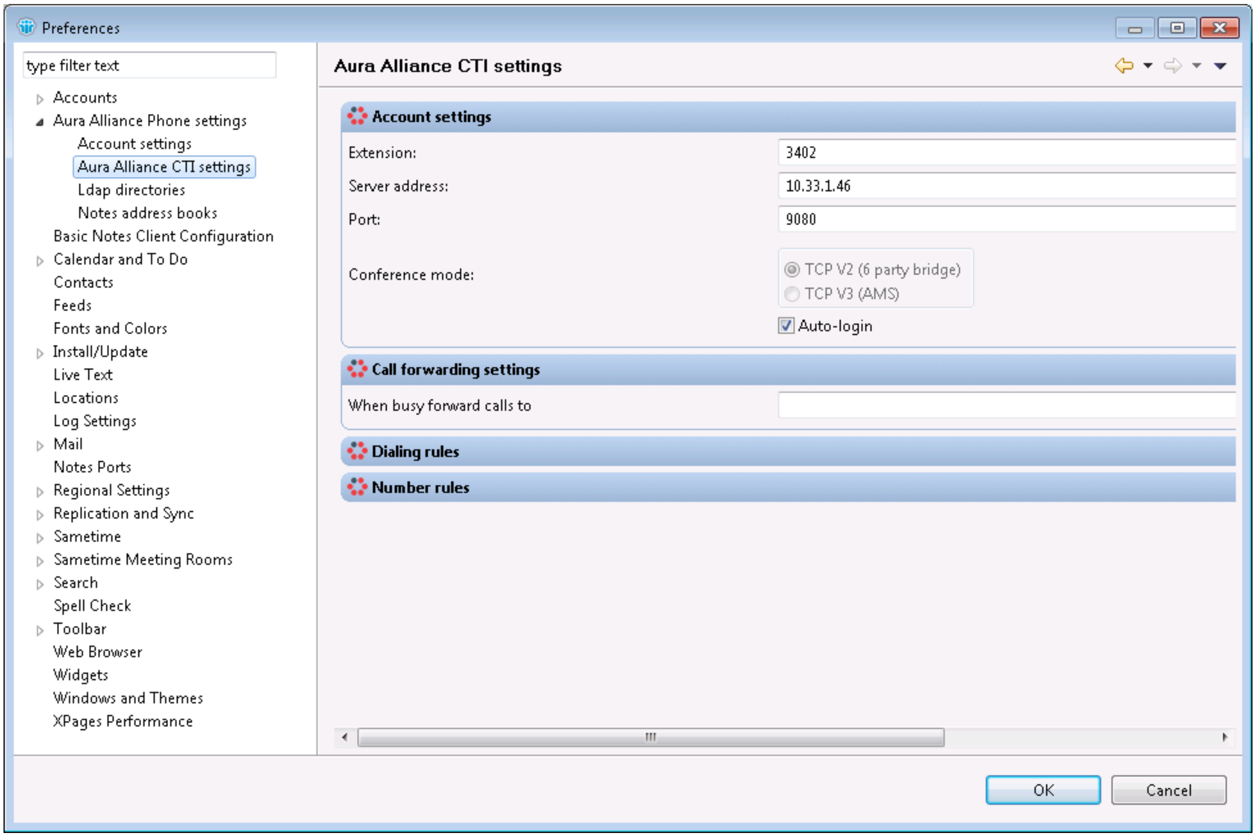
Categorize your ma —today, yesterday,

Choose Show > Gr

Releasing unused storage in database bookmark.nsf...

Navigate to menu **File → Preferences → Aura Alliance Phone settings → Aura Alliance CTI settings**. The **Aura Alliance CTI settings** window is displayed in the right side of **Preferences** Window. For Aura Alliance client to control a phone extension, enter the extension number 3402 of a deskphone in the **Extension** field, signalling IP address 10.33.1.46 of Engagement Call Control service in the **Server address** field and the port 9080 in the **Port** field. Keep other settings at default.

Click **OK** button to save the change on completion.



Extension: 3402

Server address: 10.33.1.46

Port: 9080

Conference mode: ● TCP V2 (6 party bridge) ○ TCP V3 (AMS)

☑ Auto-login

When busy forward calls to

9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Aura Alliance Client for Notes/Sametime and Avaya Engagement Call Control service on Avaya Breeze.

9.1. Verify Avaya Aura® Communication Manager

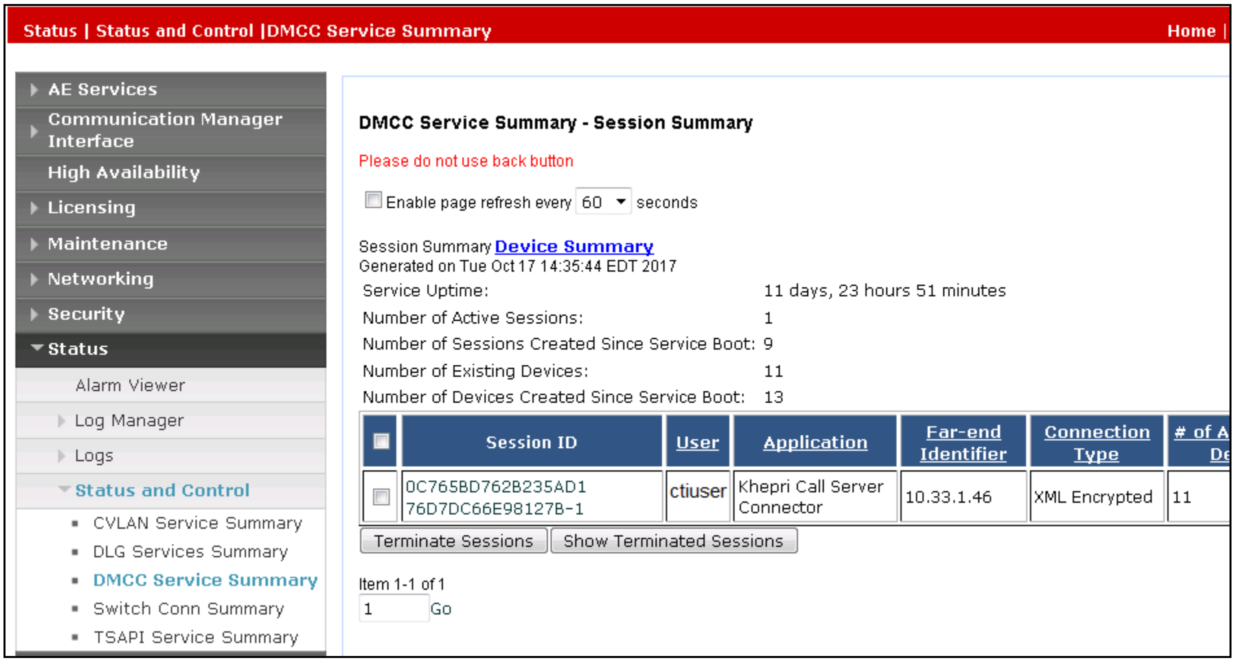
On Communication Manager, verify the status of the administered CTI link by using the "**status aesvcs cti-link**" command. Verify that the **Service State** is "established" for the CTI link number administered in **Section 5.2**, as shown below.

```
status aesvcs cti-link

                           AE SERVICES CTI LINK STATUS

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

1      7        no    aes70            established   15       15
```

9.2. Verify Avaya Aura® Application Enablement Services

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

Verify that the **Session ID** is associated with the CTI user "ctiuser" and the **Far-end Identifier** is associated with the Engagement Call Control service.



DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary Device Summary
Generated on Tue Oct 17 14:35:44 EDT 2017

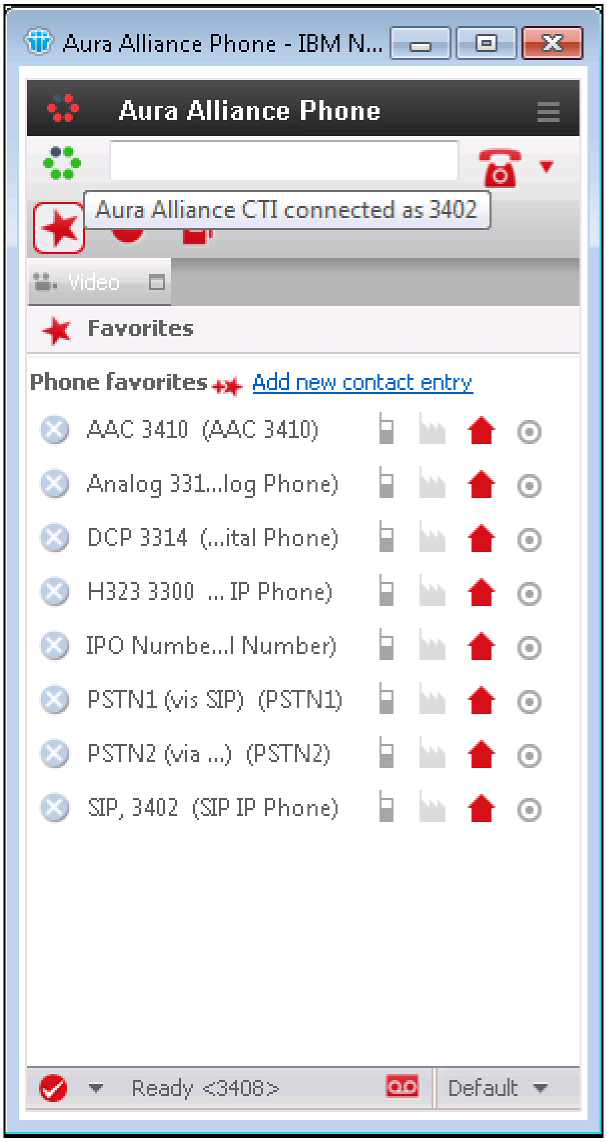
Service Uptime:	11 days, 23 hours 51 minutes
Number of Active Sessions:	1
Number of Sessions Created Since Service Boot:	9
Number of Existing Devices:	11
Number of Devices Created Since Service Boot:	13

☐	Session ID	User	Application	Far-end Identifier	Connection Type	# of A De
☐	0C765BD762B235AD1 76D7DC66E98127B-1	ctiuser	Khepri Call Server Connector	10.33.1.46	XML Encrypted	11

Item 1-1 of 1
1 Go

9.3. Verify Aura Alliance Client Notes/Sametime

Green circle icon next to the calling box indicates that Aura Alliance client successfully connects to Avaya Breeze to control a deskphone. Move the mouse over the green circle icon to get information of the deskphone extension that is being controlled by Aura Alliance client.



Aura Alliance Phone - IBM N...

Aura Alliance Phone

Aura Alliance CTI connected as 3402

Favorites

Phone favorites Add new contact entry

AAC 3410 (AAC 3410)

Analog 331...log Phone)

DCP 3314 (...ital Phone)

H323 3300 ... IP Phone)

IPO Numbe...l Number)

PSTN1 (vis SIP) (PSTN1)

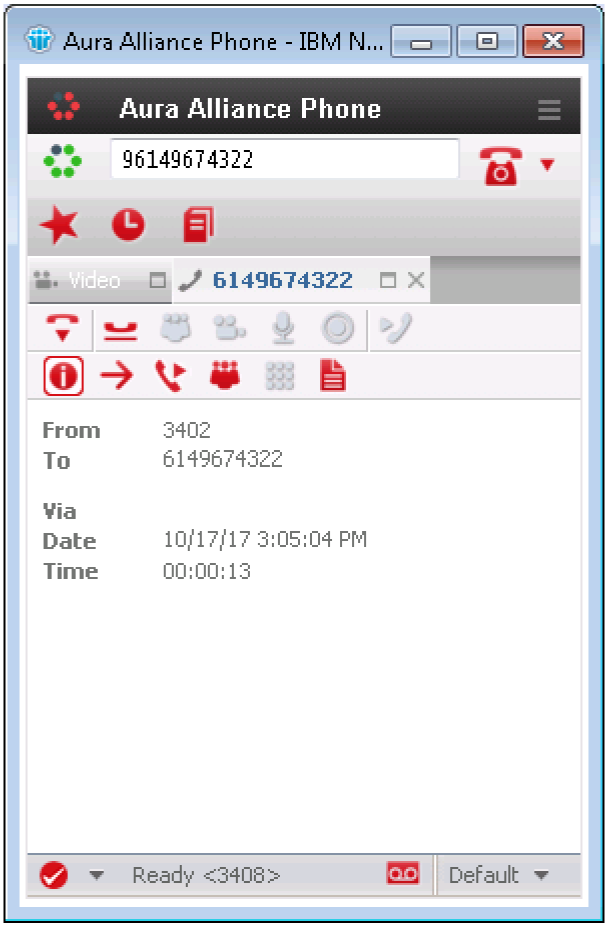
PSTN2 (via ...) (PSTN2)

SIP, 3402 (SIP IP Phone)

Ready <3408>

Default

Place an outbound call and verify call states on the deskphone and the call tab window of Aura Alliance client application. It should be synchronized. The screen below shows the call from the extension 3402 of deskphone to external number 6149674322.



From 3402
To 6149674322

Via
Date 10/17/17 3:05:04 PM
Time 00:00:13

10. Conclusion

These Application Notes describe the configuration steps required for Aura Alliance Client Notes/Sametime to successfully interoperate with Avaya Breeze™ via Engagement Call Control service. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

11. Additional References

This section references the product documentation that is relevant to these Application Notes. Documentation for Avaya products may be obtained via http://support.avaya.com

[1] Administering Avaya Aura® Communication Manager, Release 7.1, Document 03-300509, Issue 10, August 2017.

[2] Avaya Engagement Call Control Snap-in Reference.

[3] Administering Avaya Breeze™, Release 3.3, Issue1, June 2017

[4] Avaya Aura® Application Enablement Services Administration and Maintenance Guide, Release 7.1, Document 02-300357, August 2017.

Documentation related to Aura Alliance may directly be obtained from Aura Alliance.

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.