



# **Application Notes for Configuring Aura Alliance Client for Skype for Business 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 Skype for Business application to interoperate with Avaya Engagement Call Control Snap-in installed on Avaya Breeze™.

In the compliance testing, Aura Alliance Client for Skype for Business 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 Skype for Business application to interoperate with Avaya Engagement Call Control Snap-in installed on Avaya Breeze™.

In the compliance testing, the Aura Alliance Client for Skype for Business is a 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 was installed on 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.

## 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 Skype for Business:

- 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 Skype for Business 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 with the following observation.

- For an outbound call via PRI T1 trunk from the agent's deskphone to an external number, the Engagement Call Control snap-in does not get an **EstablishedEvent** from the AES when the external user answers the call. As a result, it was not able to pass this event to Aura Alliance Client for Skype for Business which led to the application not being able to control and monitor the call properly. This issue is being investigated by the Avaya development team.

## 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:

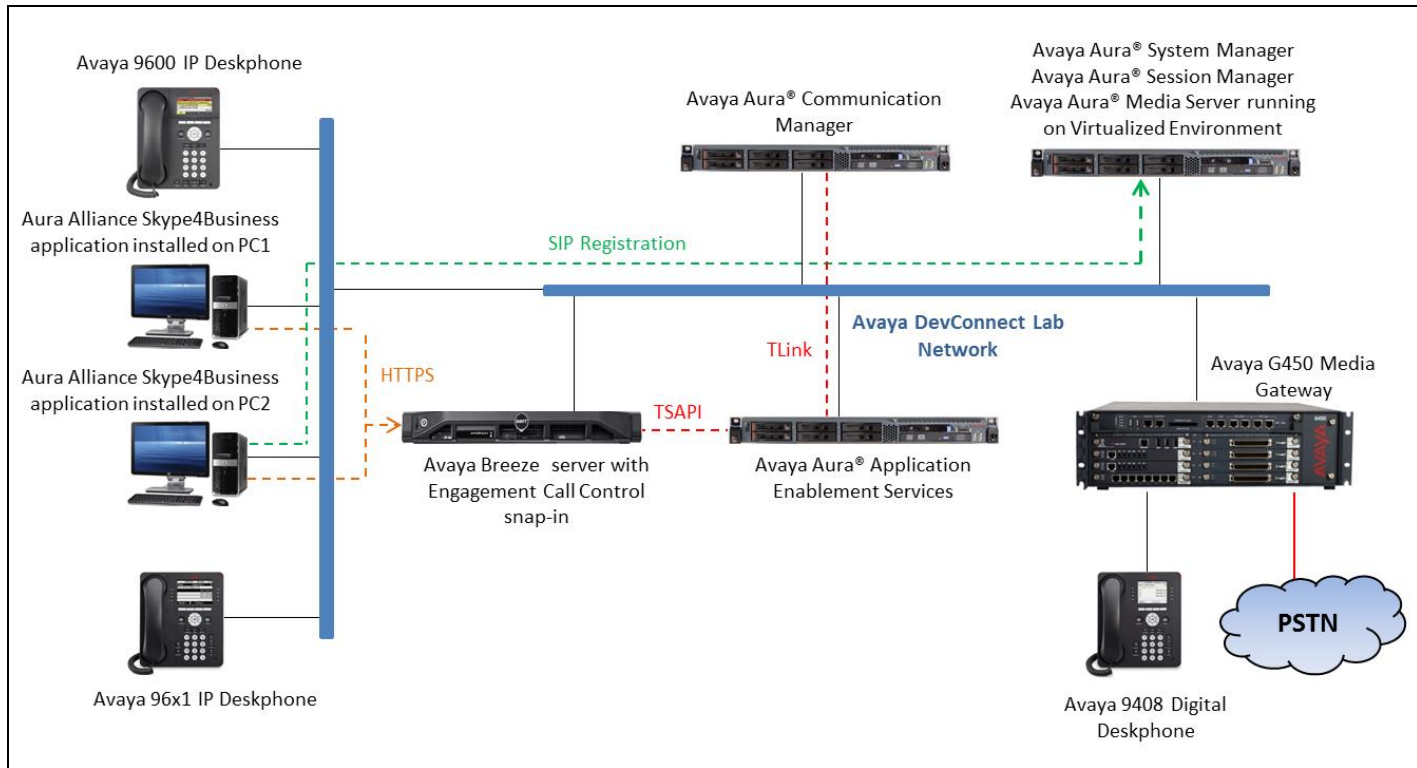
### **Aura Alliance Limited**

Tel: +44 (0)20 3127 7761

<http://www.auraalliance.com/global-support/>

### 3. Reference Configuration

**Figure 1** illustrates a sample configuration consisting of System Manager, Session Manager, Communication Manager, and Avaya Media Server running on Virtualized Environment. The Avaya G450 Media Gateway registers to Communication Manager and has PRI/T1 trunk to PSTN. The Aura Alliance Client for Skype for Business is running on a Windows 10 PC.



**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 on Virtual Environment	R017x.00.0.441.0 7.0.1.1.0-FP1SP3
Avaya G450 Media Gateway	37.39.0
Avaya Aura® Media Server running on Virtual Environment	7.7.539
Avaya Aura® Application Enablement Services on Virtual Environment	7.0.1.0.3.15
Avaya Aura® System Manager running on Virtualized Environment	7.0.1.2
Avaya Aura® Session Manager running on Virtualized Environment	7.0.1.2
Avaya Breeze™ running on Virtualized Environment	3.2.0
• Engagement Call Control Snap-in	3.2.0.1.320119
Avaya 9611G IP Deskphone (SIP)	Avaya one-X® Deskphone Release 7.0.1.2
Avaya 9641G IP Deskphone (H.323)	Avaya one-X® Deskphone Release 6.6.4
Aura Alliance Client for Skype for Business	3.2.51.1

## 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 appropriate 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 an appropriate 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 the 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 UII 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**” under **Enabled**, “**procr**” for the **Local Node** and “**8765**” as the **Local Port**.

change ip-services						Page 1 of 4
IP SERVICES						
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port	
<b>AESVCS</b>	<b>y</b>	<b>procr</b>	<b>8765</b>			

Go to **Page 4**. The password entered for the **Password** field must match the password on the AES server in the Switch Connection as specified 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 Server	Password	Enabled	Status		
1:	<b>aes70</b>	<b>*</b>	<b>y</b>	in use		



## 6. Configure Avaya Aura® Application Enablement Services

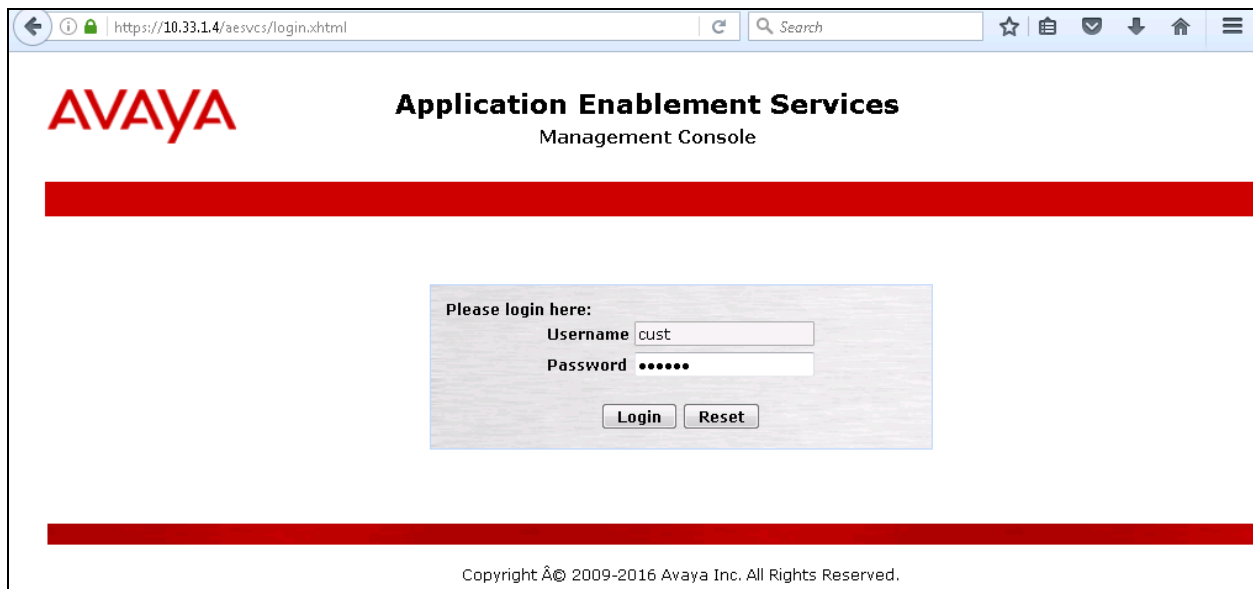
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer Switch Connection
- Administer TSAPI Link
- Administer CTI User
- Configure 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.



The screenshot shows a web browser window with the URL `https://10.33.1.4/aesvcs/login.xhtml`. The page features the Avaya logo on the left and the title "Application Enablement Services Management Console" in the center. A prominent red horizontal bar is positioned below the title. In the center of the page, there is a login form with the heading "Please login here:". The form contains two input fields: "Username" with the value "cust" and "Password" with masked characters "\*\*\*\*\*". Below the password field are two buttons: "Login" and "Reset". At the bottom of the page, a red horizontal bar is present, and the footer text reads "Copyright © 2009-2016 Avaya Inc. All Rights Reserved."

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

The screenshot shows the Avaya Application Enablement Services Management Console. The top left features the Avaya logo. The main header reads "Application Enablement Services Management Console". In the top right corner, there is a welcome message: "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", and "HA Status: Not Configured". Below the header is a navigation bar with "Home" on the left and "Home | Help | Logout" on the right. A left-hand navigation menu lists various categories: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area is titled "Welcome to OAM" and contains the following text: "The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:" followed by a bulleted list: "• 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". Below the list, it states: "Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain." At the bottom of the page, there is a copyright notice: "Copyright © 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 login screen (not shown). Log in using the appropriate credentials and navigate to display installed licenses (not shown).

The screenshot shows the Avaya Application Enablement Services Management Console with the "Licensing" section selected. The top left features the Avaya logo. The main header reads "Application Enablement Services Management Console". In the top right corner, there is a welcome message: "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", and "HA Status: Not Configured". Below the header is a navigation bar with "Licensing" on the left and "Home | Help | Logout" on the right. The left-hand navigation menu is expanded to show "Licensing" with sub-items: "WebLM Server Address", "WebLM Server Access", and "Reserved Licenses". The main content area is titled "Licensing" and contains the following text: "If you are setting up and maintaining the WebLM, you need to use the following:" followed by a bulleted list: "• WebLM Server Address". Below that, it says: "If you are importing, setting up and maintaining the license, you need to use the following:" followed by a bulleted list: "• WebLM Server Access". Then it says: "If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:" followed by a bulleted list: "• Reserved Licenses". At the bottom of the main content area, there is a red note: "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**

10 Items Show All


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;CtiS MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20 LargeServerTypes: isp2100;ibmx305;d1380g3;d1385g1;d1385g2;u TrustedApplications: IPS_001, BasicUnrestrict DMCUnrestricted; 1XP_001, BasicUnrestricted DMCUnrestricted; 1XM_001, BasicUnrestricted DMCUnrestricted; PC_001, BasicUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted, DMCUnrestricted; OSPC_001, BasicUnrestrict DMCUnrestricted; VP_001, BasicUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AE CCE_001, BasicUnrestricted, AdvancedUnrestr CSI_T1_001, BasicUnrestricted, AdvancedUnre CSI_T2_001, BasicUnrestricted, AdvancedUnre 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 select the **Processor Ethernet** checkbox if the Processor Ethernet is used in Communication Manager. Click **Apply** button to save the configuration.

The screenshot displays the Avaya Application Enablement Services Management Console. The top left features the Avaya logo and the title 'Application Enablement Services Management Console'. The top right shows a welcome message for user 'cust' and system information including the last login time (Fri Nov 25 10:50:11 2016), number of failed login attempts (0), host name/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), and HA status (Not Configured). A red navigation bar at the top contains 'Communication Manager Interface | Switch Connections' and 'Home | Help | Logout'. On the left is a sidebar menu with options: AE Services, Communication Manager Interface (expanded), Switch Connections (selected), Dial Plan, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area is titled 'Connection Details - interopCM' and contains the following configuration fields: 'Switch Password' and 'Confirm Switch Password' (both masked with dots), 'Msg Period' (30) with a unit of 'Minutes (1 - 72)', 'Provide AE Services certificate to switch' (checkbox), 'Secure H323 Connection' (checkbox), and 'Processor Ethernet' (checkbox checked). 'Apply' and 'Cancel' buttons are at the bottom.

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



## Application Enablement Services

Management Console

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

Communication Manager Interface | Switch Connections
Home | Help | Logout

▶ AE Services
▼ Communication Manager Interface
Switch Connections
▶ Dial Plan
▶ High Availability
▶ Licensing
▶ Maintenance
▶ Networking
▶ Security
▶ Status
▶ User Management
▶ Utilities
▶ Help

### Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input type="radio"/> CLAN1	No	30	1
<input checked="" type="radio"/> interopCM	Yes	30	1
<input type="radio"/> server1	Yes	30	0

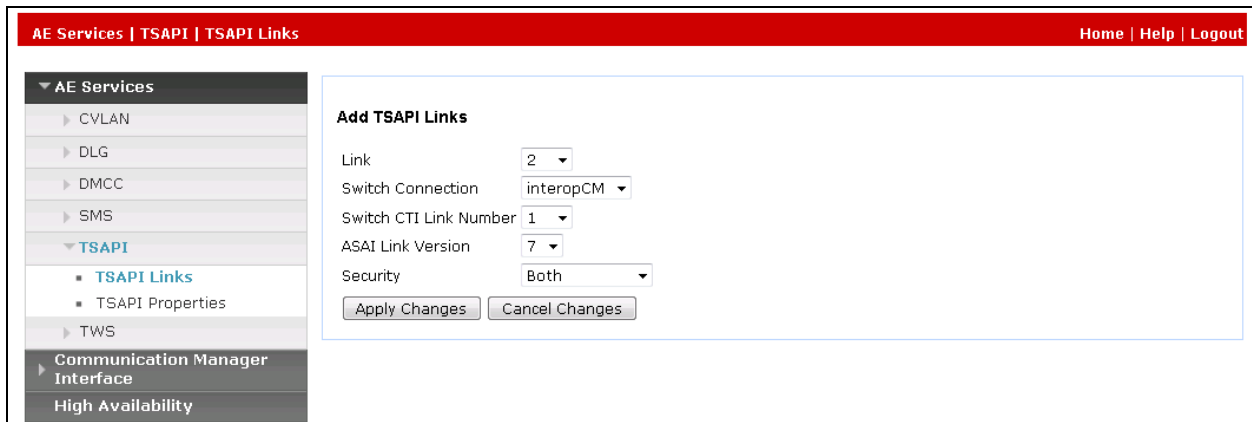
Enter the IP address of the Processor Ethernet of Communication Manager in the box and click the **Add/Edit Name of IP** button to add the IP.

Select **Edit H.323 Gatekeeper** button to add an IP address of the gatekeeper, the Gatekeeper IP address in this case is also the Processor Ethernet.

## 6.4. Administer TSAPI Link

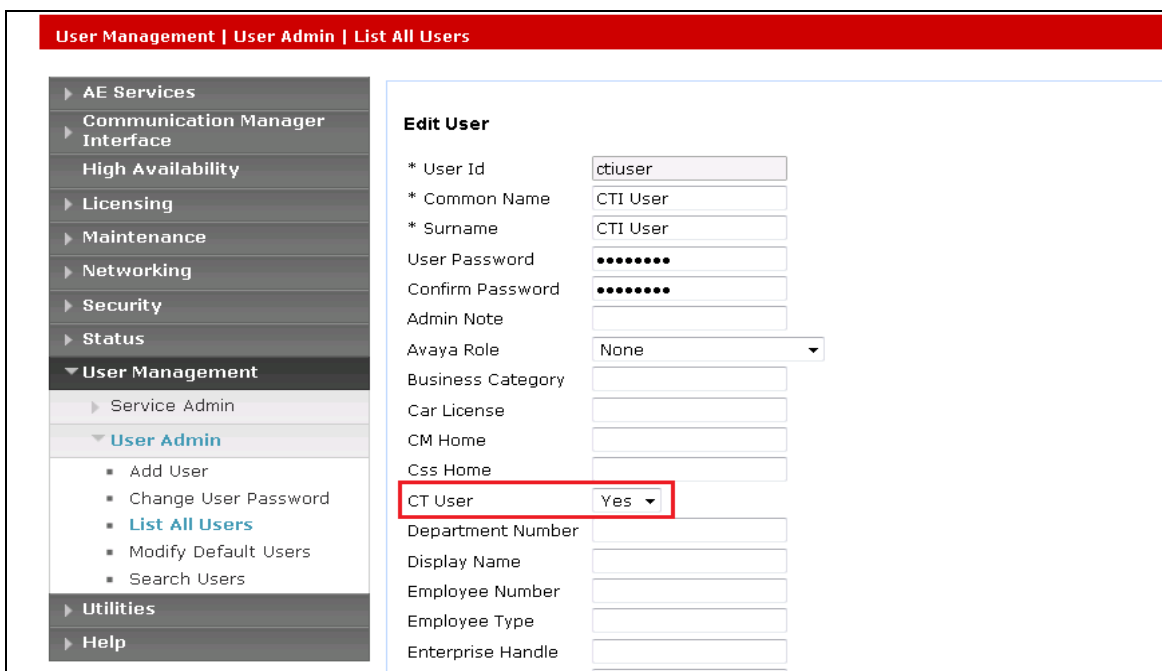
Select **AE Services** → **TSAPI** → **TSAPI Links** from the left pane of the **Management Console** to administer a TSAPI link. The **TSAPI Links** screen is displayed, as shown below. Click **Add Link**.

The **Add TSAPI Links** screen is displayed on 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 the step above, is 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.



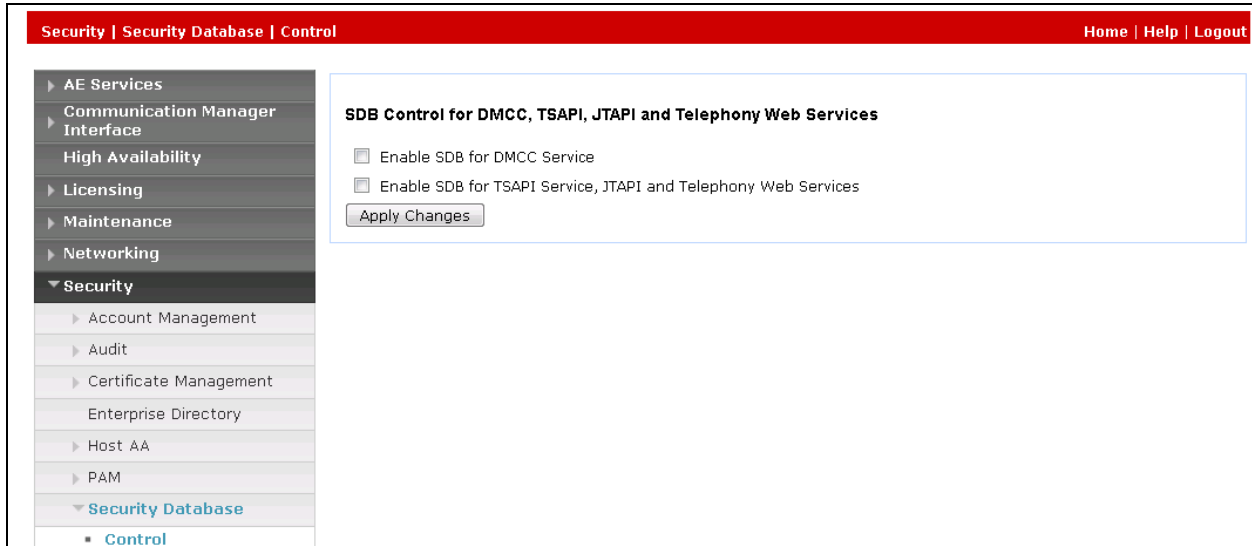
## 6.5. Administer CTI User

Select **User Management** → **User Admin** → **Add User** from the left pane, to display the **Add User** screen in the right pane (the below screen displays the **Edit User** screen for an existing user). Enter the 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.



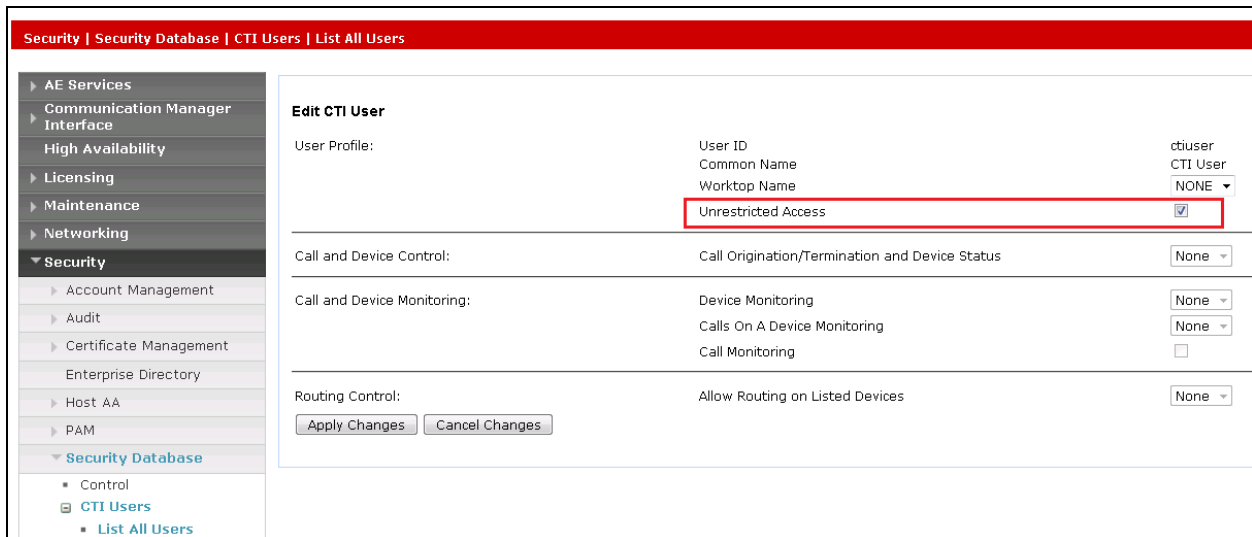
## 6.6. Configure Security Database

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.



The screenshot shows the 'SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services' configuration page. The left navigation pane is expanded to 'Security Database' > 'Control'. The main content area contains two checkboxes: 'Enable SDB for DMCC Service' and 'Enable SDB for TSAPI Service, JTAPI and Telephony Web Services', both of which are unchecked. An 'Apply Changes' button is located below the checkboxes.

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



The screenshot shows the 'Edit CTI User' configuration page for the user 'ctiuser'. The left navigation pane is expanded to 'Security Database' > 'CTI Users' > 'List All Users'. The main content area displays the user profile and various control settings. The 'Unrestricted Access' checkbox is checked and highlighted with a red box. The 'Apply Changes' button is visible at the bottom left.

Edit CTI User		
User Profile:	User ID	ctiuser
	Common Name	CTI User
	Worktop Name	NONE
	Unrestricted Access	<input checked="" type="checkbox"/>
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	<input type="checkbox"/>
Routing Control:	Allow Routing on Listed Devices	None



## 6.7. Administer Ports

Select **Networking** → **Ports** from the left pane, to display the **Ports** screen in the right pane. In the **TSAPI Ports** section select the **Enabled** radio button for **TSAPI Service Port 450** and in the **DMCC Server Ports** section select the **Enabled** radio button for **Unencrypted Port 4721** 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

**AVAYA Application Enablement Services Management Console**

Networking | Ports Home | Help | Logout

**Ports**

CVLAN Ports Enabled Disabled

Unencrypted TCP Port	9999	<input checked="" type="radio"/>	<input type="radio"/>
Encrypted TCP Port	9998	<input type="radio"/>	<input checked="" type="radio"/>

---

DLG Port TCP Port 5678

---

TSAPI Ports Enabled Disabled

TSAPI Service Port	450	<input checked="" type="radio"/>	<input type="radio"/>
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	<input checked="" type="radio"/>	<input type="radio"/>
Encrypted Port	4722	<input type="radio"/>	<input checked="" type="radio"/>
TR/87 Port	4723	<input type="radio"/>	<input checked="" type="radio"/>

## 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 Server**.

Maintenance | Service Controller Home | Help | Logout

**Service Controller**

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input type="checkbox"/> DMCC Service	Running
<input type="checkbox"/> CVLAN Service	Running
<input type="checkbox"/> DLG Service	Running
<input type="checkbox"/> Transport Layer Service	Running
<input type="checkbox"/> 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. The procedure for how to install and configure the Avaya Engagement Call Control snap-in on Avaya Breeze is referenced in **Section 11[2]**.

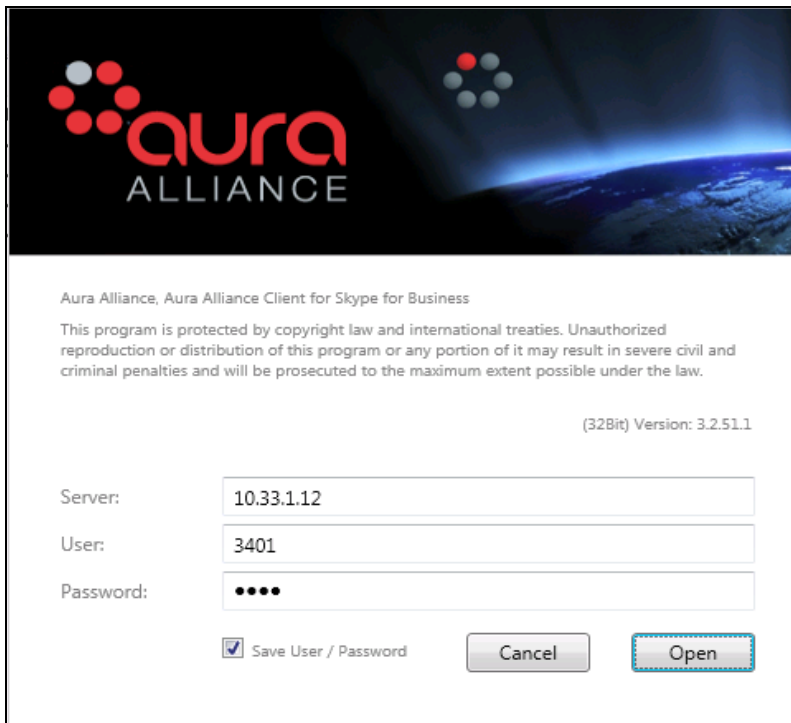
## 8. Configure Aura Alliance Client for Skype for Business

This section provides steps to configure the Aura Alliance Client application. During the 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 Aura Alliance Client for Skype for Business application is installed, run the application from the Start menu. Enter the signalling IP address of Session Manager in the **Server** field, the SIP user extension in the **User** field and the password if the SIP user extension in the **Password** field.

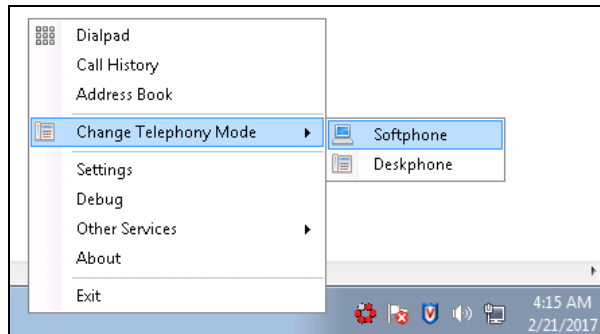
Note 1: Aura Alliance Client for Skype for Business has two modes: Softphone and Deskphone, the client requires the signalling IP address of Session Manager, a SIP user and its password to log in to the Softphone mode first then the user can switch to Deskphone mode.

Note 2: In order for the Aura Alliance Client for Skype for Business to control a SIP deskphone, ensure that the SIP deskphone has **Type of 3PCC Enabled** set to **Avaya** and uses the TLS protocol to register to Session Manager.

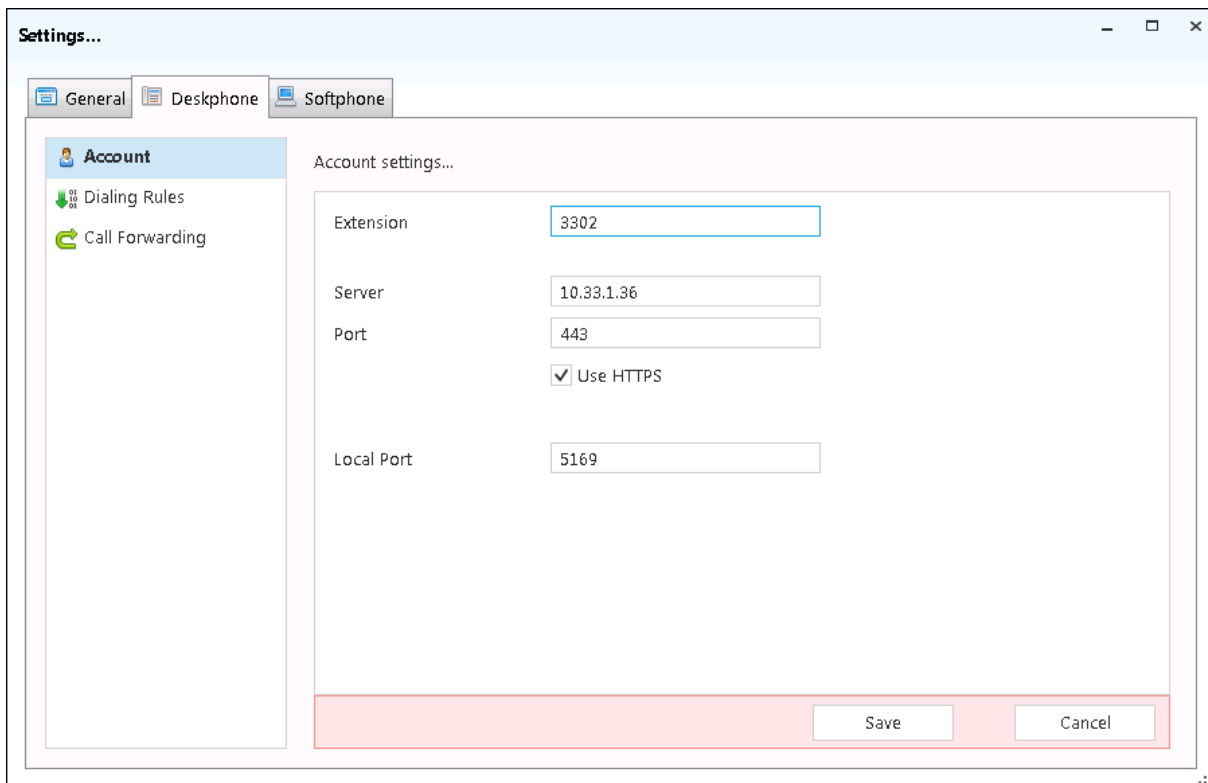


The screenshot shows the configuration dialog for the Aura Alliance Client. The title bar reads "Aura Alliance, Aura Alliance Client for Skype for Business". Below the title bar is a copyright notice: "This program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program or any portion of it may result in severe civil and criminal penalties and will be prosecuted to the maximum extent possible under the law." The version number is "(32Bit) Version: 3.2.51.1". The dialog contains three input fields: "Server" with the value "10.33.1.12", "User" with the value "3401", and "Password" with four dots. At the bottom, there is a checked checkbox for "Save User / Password", a "Cancel" button, and an "Open" button.

The Aura Alliance Client for Skype for Business application appears in the system tray, right click on the application and select the **Deskphone** mode.



Navigate to **Settings** from the context menu above and select the **Deskphone** tab. In the **Account settings** window enter an extension of a deskphone that the application wants to monitor and control, e.g. “3302”. Enter the IP address of Engagement Call Control service in the **Server** field and keep the other fields at default. Click **Save** button to save changes.



## 9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Aura Alliance Client for Skype for Business 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 Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs 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 being used by 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 Wed Feb 22 12:16:15 EST 2017

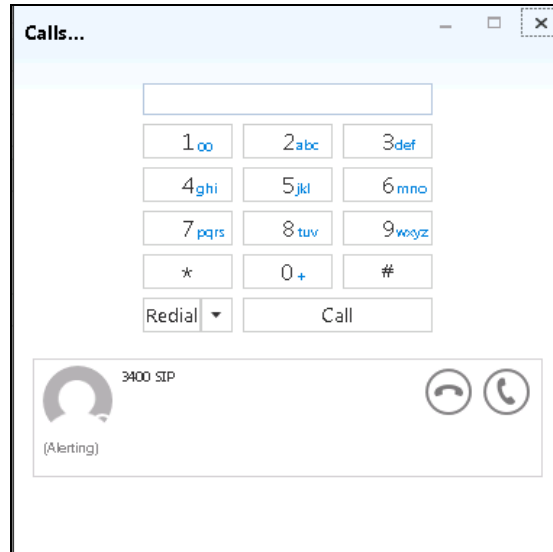
Service Uptime: 12 days, 1 hours 3 minutes  
 Number of Active Sessions: 1  
 Number of Sessions Created Since Service Boot: 2  
 Number of Existing Devices: 3  
 Number of Devices Created Since Service Boot: 3

<input type="checkbox"/>	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	7932F35168B2E87FC E5CD4C1E17C84A5-1	ctiuser	Khepri Call Server Connector	10.33.1.36	XML Encrypted	3

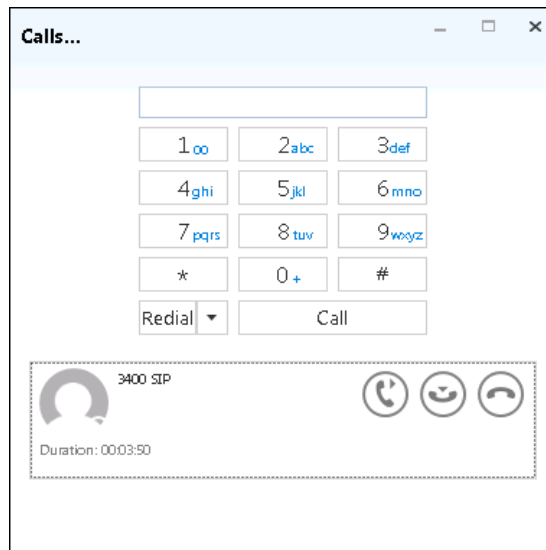
Item 1-1 of 1  
 Go

### 9.3. Verify Aura Alliance Client Skype for Business

Place a call to the extension of the deskphone that the Aura Alliance Client Skype for Business application monitors, e.g. 3302. The **Calls** window of the Skype for Business application will popup to alert an incoming call. Answer the incoming call on the deskphone by selecting the **Answer** button on the **Calls** window.



Verify call states on the deskphone and the **Calls** window of Skype for Business application are synchronized.



## 10. Conclusion

These Application Notes describe the configuration steps required for Aura Alliance Client Skype for Business to successfully interoperate with Avaya Breeze™ via Engagement Call Control service. All feature and serviceability test cases were completed successfully 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 7.0.3, Document 03-300509, Issue 10, June 2016.
- [2] Avaya Engagement Call Control Snap-in Reference.
- [3] Administering Avaya Breeze™, Release 3.2, Issue1, October 2016
- [4] Avaya Aura® Application Enablement Services Administration and Maintenance Guide, Release 7.0, Document 02-300357, Jan 2016.

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

---

**©2017 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at [devconnect@avaya.com](mailto:devconnect@avaya.com).