



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for EMERES Softphone Module and Avaya Aura® Application Enablement Services 7.0 – Issue 1.0**

### **Abstract**

These Application Notes describe the configuration steps required for EMERES Softphone module application to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services.

In the compliance testing, EMERES Softphone application is windows application which uses the Telephony Services Application Programming Interface (TSAPI) from Avaya Aura® Application Enablement Services to monitor contact center agents on Avaya Aura® Communication Manager. The application provides call control features such as make an outbound call to any internal or external destination, conference, transfer and change agent status such as login, logout, on lunch break or after work; these status changes are updated on the agent's deskphone.

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 EMERES Softphone with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0.

The EMERES Softphone solution is specifically designed for Public Safety applications where call handling efficiency, accuracy and speed are essential. It includes a Softphone server and Softphone clients. The Softphone client (3rd party call control only, no voice/RTP processing) integrates with Avaya Aura® Application Enablement Services (AES) using Telephony Services Application Programming Interface (TSAPI) interface.

# 2. General Test Approach and Test Results

The feature test cases were performed manually. Incoming calls were placed to the VDN with available agents; the EMERES Softphone was used to verify proper call handling such as answer, hold and retrieve, transfer and conference. The click-to-dial calls were initiated by clicking on the contact phone number displayed on the Softphone history tab. Manually logging in and out an ACD agent on the Softphone verified that status changes correctly on the agent's desktop. Other statuses such as on lunch, on break or after work were also verified.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to the EMERES server and restarting the AES server.

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 EMERES Softphone client:

- Use of TSAPI event to monitor agent station.
- Use of TSAPI call control service to launch outbound call.
- Proper handling of call scenarios involving inbound, outbound, internal, external, ACD, non-ACD, drop, hold/resume, multiple calls, conference, transfer, long duration, click-to-dial from history phone number, pending aux work, and reason codes.

The serviceability testing focused on verifying the ability of EMERES Softphone to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection from EMERES server and restarting the AES server.

## 2.2. Test Results

All test cases were executed and passed successfully with the following observation.

- Outbound call via PRI T1 trunk from the agent's deskphone to the external number, the EMERES Softphone does not get **EstablishedEvent** from AES when the external user answers the call therefore the Softphone was not able to control and monitor the call properly. This issue is being investigated by Avaya development team.

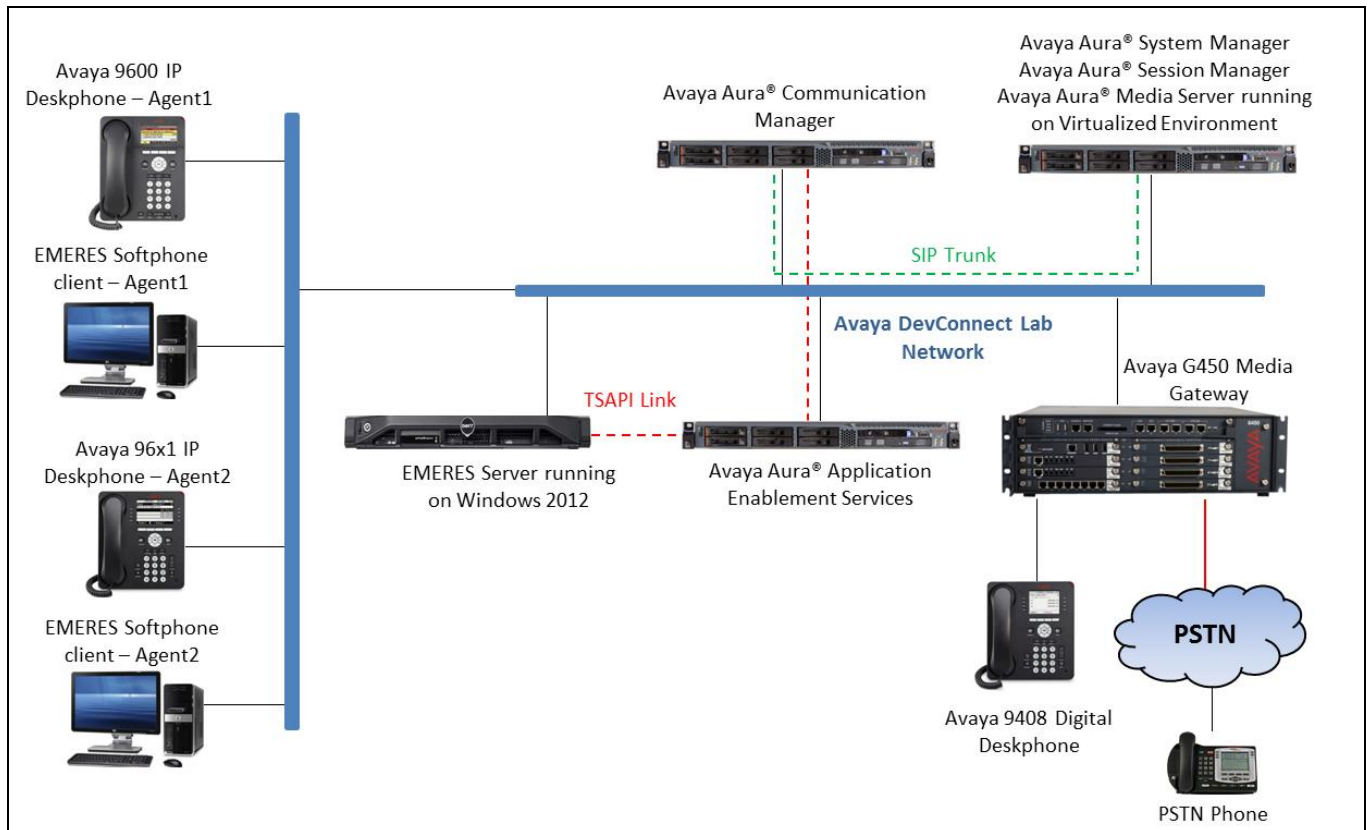
## 2.3. Support

For technical support on the EMERES Softphone Module, contact EMERES via email, or internet.

- **Web:** <http://www.emeres.com>

### 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 PSTN. The EMERES server running on Windows 2012 server and connected to Avaya Aura® Application Enablement Service using CTI user and TSAPI interface.



**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 Virtualized Environment	R017x.00.0.441.0 7.0.1.1.0-FP1SP1
Avaya G450 Media Gateway	37.19.0
Avaya Aura® Media Server running in Virtualized Environment	7.7.539
Avaya Aura® Application Enablement Services in Virtualized Environment	7.0.1.0.3.15
Avaya Aura® System Manager running on Virtualized Environment	7.0.1.1
Avaya Aura® Session Manager running on Virtualized Environment	7.0.1.1
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
Avaya 9640G IP Deskphone (H323)	Avaya one-X® Deskphone Release 3.25
EMERES Softphone Server running in Windows 2012 Server	9.5
EMERES Softphone client running in Windows 7 SP1	9.5

## 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 IP Node Names
- Administer AE Services
- Administer Hunt Group
- Administer VDN
- Administer Agent Login ID

### 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 a 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	<b>Computer Telephony Adjunct Links?</b>	<b>y</b>	
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				
<b>Extension: 3332</b>				
<b>Type: ADJ-IP</b>				
COR: 1				
<b>Name: AES70</b>				

### 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 EMERES 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 IP Node Names

Use the **change node-names ip** command to administer a Name and IP Address for AES. In the configuration used for compliance testing, the **procr** and **aes70** nodes were utilized to administer a CTI link between Communication Manager and AES

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
AMS1	10.33.1.30	
CMS18	10.33.1.20	
<b>aes70</b>	<b>10.33.1.4</b>	
default	0.0.0.0	
interopASM	10.33.1.12	
lsp	10.33.1.17	
<b>procr</b>	<b>10.33.1.6</b>	
procr6	::	

## 5.5. Administer AE Services

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

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

Go to **Page 4**, enter the following values. **AE Services Server** should be the AES IP node name that is configured in Section 5.3 above, enter a password in the Password field and select “y” in the **Enabled** field.

**Note:** 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 Server	Password	Enabled	Status
1:	<b>aes70</b>	<b>*</b>	<b>y</b>	in use



## 5.6. Administer Hunt Group Skillset

This section provides the hunt group configuration for the call center agents.

Agents will log into hunt group skillset 1 as configured below. Provide a descriptive name and set the **Group Extension** field to a valid extension. Enable the **ACD**, **Queue**, and **Vector** options. This hunt group will be specified in the **Agent LoginIDs** configured in **Section 5.8**

add hunt-group 1	HUNT GROUP	Page 1 of 4
Group Number: 1	ACD? y	
Group Name: Skill-1	Queue? y	
<b>Group Extension: 3320</b>	Vector? y	
Group Type: ucd-mia		
TN: 1		
COR: 1	MM Early Answer? n	
Security Code:	Local Agent Preference? n	
ISDN/SIP Caller Display:		
Queue Limit: unlimited		
Calls Warning Threshold:	Port:	
Time Warning Threshold:	Port:	

On Page 2 of the Hunt Group form, enable the **Skill** option and **Both** in the **Measured** field.

add hunt-group 1	HUNT GROUP	Page 2 of 4
Skill? y	Expected Call Handling Time (sec): 180	
AAS? n		
<b>Measured: Both</b>		
Supervisor Extension:		
Controlling Adjunct: none		
Multiple Call Handling: none		
Timed ACW Interval (sec):	After Xfer or Held Call Drops? n	

## 5.7. Administer VDN

Use the “**add vdn <ext>**” command to add a VDN number. In the **Destination** field, enter **Vector Number** and enter a vector number as shown in the screen below.

```
add vdn 3340                                     Page 1 of 3
                                         VECTOR DIRECTORY NUMBER

      Extension: 3340
      Name*: Contact Center 1
      Destination: Vector Number           1
      Attendant Vectoring? n
      Meet-me Conferencing? n
      Allow VDN Override? n
      COR: 1
      TN*: 1
      Measured: both      Report Adjunct Calls as
ACD*? n
      Acceptable Service Level (sec): 20
      VDN of Origin Annc. Extension*:
      1st Skill*:
      2nd Skill*:
      3rd Skill*:
```

## 5.8. Administer Agent Login ID

To add an **Agent LoginID**, use the command “**add agent-loginID <agent ID>**” for each agent. In the compliance test, three agent login IDs 1000, 1001, and 1002 were created.

```
add agent-loginID 1000                           Page 1 of 2
                                         AGENT LOGINID

      Login ID: 1000                                AAS? n
      Name: Agent 1000                              AUDIX? n
      TN: 1
      COR: 1
      Coverage Path:                                LWC Reception: spe
      Security Code: 1234                          LWC Log External Calls? n
      Attribute:                                    AUDIX Name for Messaging:

      LoginID for ISDN/SIP Display? n
      Password:
      Password (enter again):
      Auto Answer: station
      MIA Across Skills: system
AUX Agent Considered Idle (MIA)? system  ACW Agent Considered Idle: system
      Aux Work Reason Code Type: system
      Logout Reason Code Type: system
      Maximum time agent in ACW before logout (sec): system
      Forced Agent Logout Time:
WARNING: Agent must log in again before changes take effect
```

On Page 2 of the **Agent LoginID** form, set the skill number (**SN**) to hunt group 1, which is the hunt group (skill) that the agents will log into.

add agent-loginID 1000			Page 2 of 2		
AGENT LOGINID					
Direct Agent Skill:			Service Objective? n		
Call Handling Preference: skill-level			Local Call Preference? n		
SN	RL	SL	SN	RL	SL
1: 1		1	16:		
2:			17:		
3:			18:		
4:			19:		
5:			20:		
6:					
7:					
8:					
9:					
10:					
11:					
12:					
13:					
14:					
15:					

## 5.9. Administer Station

To add a station, use the command “**add station <station extension>**” where the <station extension> is an available station in the system. On **Page 1**, enter an IP phone model in the **Type** field, a passcode in the **Security Code** field.

add station 3301			Page 1 of 6		
STATION					
Extension: 3301		Lock Messages? n		BCC: 0	
<b>Type: 9641</b>		<b>Security Code: *</b>		TN: 1	
Port: S00011		Coverage Path 1: 1		COR: 1	
Name: H323 3301		Coverage Path 2:		COS: 1	
		Hunt-to Station:		Tests? y	
STATION OPTIONS					
Loss Group: 19		Time of Day Lock Table:			
		Personalized Ringing Pattern: 1			
		Message Lamp Ext: 3301			
Speakerphone: 2-way		Mute Button Enabled? y			
Display Language: english		Button Modules: 1			
Survivable GK Node Name: lsp		Media Complex Ext:			
Survivable COR: internal		IP SoftPhone? y			
Survivable Trunk Dest? y					
		IP Video Softphone? n			
		Short/Prefixed Registration Allowed: default			
		Customizable Labels? y			

On **Page 4**, enter buttons for agent's deskphone such as **aux-work**, **auto-in**, **after-call**, **manual-in**, and **release**.

add station 3301		Page 4 of 6	
STATION			
SITE DATA			
Room:		Headset?	n
Jack:		Speaker?	n
Cable:		Mounting:	d
Floor:		Cord Length:	0
Building:		Set Color:	
ABBREVIATED DIALING			
List1:	List2:	List3:	
BUTTON ASSIGNMENTS			
1: call-appr	5: auto-in	Grp:	
2: call-appr	6: after-call	Grp:	
3: call-appr	7: manual-in	Grp:	
4: aux-work	8: release		
RC:	Grp:		
voice-mail 3333			

## 6. Configure Avaya Aura® Application Enablement Services

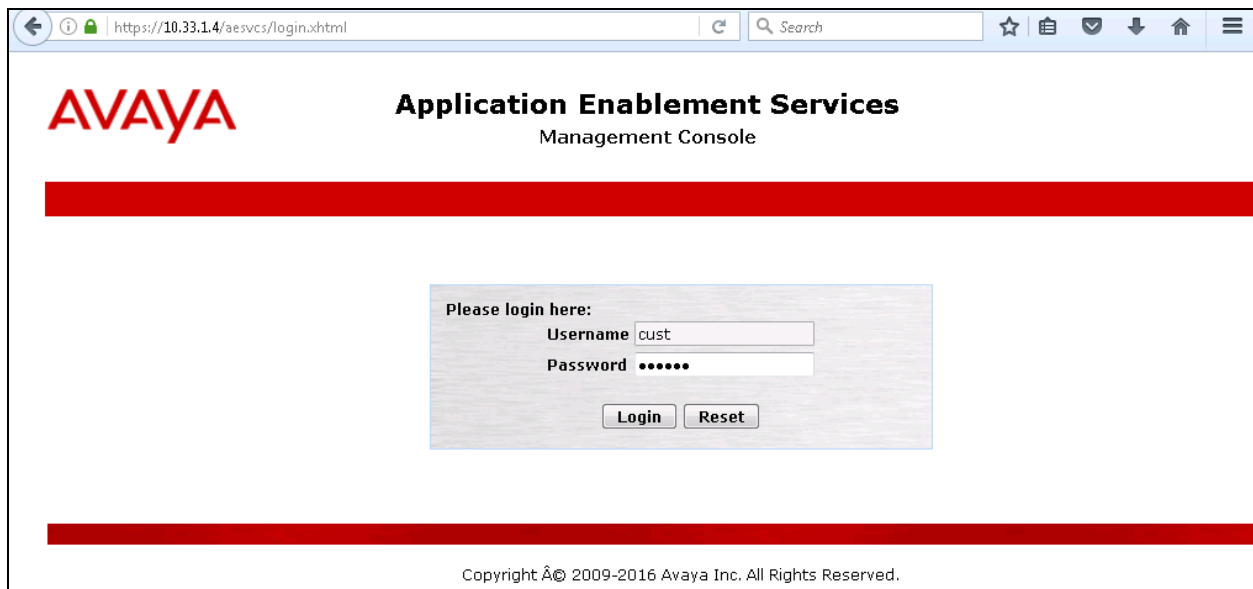
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- 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.



The screenshot shows a web browser window with the URL `https://10.33.1.4/aesvcs/login.xhtml`. The page features the Avaya logo and the title "Application Enablement Services Management Console". A red horizontal bar is positioned above a central login box. The login box contains the text "Please login here:" followed by "Username" and "Password" labels. The username field is populated with "cust" and the password field is masked with seven dots. Below the fields are "Login" and "Reset" buttons. Another red horizontal bar is located at the bottom of the page, above the copyright notice: "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 header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for user "cust" with login details. A red navigation bar contains "Home", "Help", and "Logout". On the left, a sidebar lists menu items: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area displays "Welcome to OAM" with a description of the OAM web interface and a list of administrative domains and their functions. A copyright notice is at the bottom.

**AVAYA** Application Enablement Services Management Console

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

Home | Help | Logout

Home

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

**Welcome to OAM**

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

- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- High Availability - Use High Availability to manage AE Services HA.
- Licensing - Use Licensing to manage the license server.
- Maintenance - Use Maintenance to manage the routine maintenance tasks.
- Networking - Use Networking to manage the network interfaces and ports.
- Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.
- Status - Use Status to obtain server status informations.
- User Management - Use User Management to manage AE Services users and AE Services user-related resources.
- Utilities - Use Utilities to carry out basic connectivity tests.
- Help - Use Help to obtain a few tips for using the OAM Help system

Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain.

Copyright © 2009-2016 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).

The screenshot shows the Avaya Application Enablement Services Management Console with the "Licensing" menu item selected in the sidebar. The main content area displays "Licensing" with instructions on how to set up and maintain the WebLM, including a list of required information: WebLM Server Address, WebLM Server Access, and Reserved Licenses. A note at the bottom advises disabling pop-up blockers. The top header and navigation bar are identical to the previous screenshot.

**AVAYA** Application Enablement Services Management Console

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

Home | Help | Logout

Licensing

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▼ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

WebLM Server Address

[WebLM Server Access](#)

Reserved Licenses

**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**

Verify that there are sufficient licenses for **TSAPI Simultaneous Users**, as shown below.

KP; Reviewed:  
SPOC 2/8/2017

### 6.3. Administer Switch Connection

Select **Communication Manager Interface** → **Switch Connection** 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 5.5** in the **Switch Password** and **Confirm Switch Password** and check on **Processor Ethernet** field if the Processor Ethernet is used in Communication Manager. Click **Apply** button to save the configuration.

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane is expanded to 'Communication Manager Interface' > 'Switch Connections'. The main content area displays the 'Connection Details - interopCM' configuration page. The page includes fields for 'Switch Password', 'Confirm Switch Password', 'Msg Period' (set to 30 minutes), 'Provide AE Services certificate to switch' (unchecked), 'Secure H323 Connection' (unchecked), and 'Processor Ethernet' (checked). 'Apply' and 'Cancel' buttons are at the bottom.

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

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

**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: ☒  
Apply Cancel

Select the **interopCM** switch connection has been added above and selects **Edit PE/CLAN IPs** to add IP address of switch connection.

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane is expanded to 'Communication Manager Interface' > 'Switch Connections'. The main content area displays the 'Switch Connections' table. The table has columns: 'Connection Name', 'Processor Ethernet', 'Msg Period', and 'Number of Active Connections'. The 'interopCM' connection is selected and highlighted with a red box. Below the table, the 'Edit PE/CLAN IPs' button is also highlighted with a red box.

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**

Add Connection

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

Edit Connection Edit PE/CLAN IPs Edit H.323 Gatekeeper Delete Connection Survivability Hierarchy



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

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services  
Communication Manager Interface  
Switch Connections  
Dial Plan  
High Availability  
Licensing  
Maintenance  
Networking  
Security

**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 to add an IP address of gate keeper, the Gatekeeper IP address in this case is also the Processor Ethernet.

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services  
Communication Manager Interface  
Switch Connections  
Dial Plan  
High Availability  
Licensing  
Maintenance

**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**.

**AVAYA** Application Enablement Services Management Console

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

AE Services | TSAPI | TSAPI Links Home | Help | Logout

AE Services  
CVLAN  
DLG  
DMCC  
SMS  
TSAPI  
TSAPI Links  
TSAPI Properties

**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 is added in the step above. 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 link. Retain the default values in the remaining fields.

The screenshot shows the 'Add TSAPI Links' configuration page. The left sidebar has a tree view with 'TSAPI Links' selected. The main content area has the following fields:

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

At the bottom of the form are two buttons: 'Apply Changes' and '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.

The screenshot shows the 'Edit User' configuration page. The left sidebar has a tree view with 'User Admin' selected, and 'Add User' is highlighted. The main content area has the following fields:

- \* User Id: ctiuser
- \* Common Name: CTI User
- \* Surname: CTI User
- User Password: [masked]
- Confirm Password: [masked]
- Admin Note: [empty]
- Avaya Role: None
- Business Category: [empty]
- Car License: [empty]
- CM Home: [empty]
- Csx Home: [empty]
- CT User: Yes
- Department Number: [empty]
- Display Name: [empty]
- Employee Number: [empty]
- Employee Type: [empty]
- Enterprise Handle: [empty]

The 'CT User' field is highlighted with a red box.

## 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 a web interface with a red header bar containing "Security | Security Database | Control" and "Home | Help | Logout". On the left is a navigation tree with categories: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, and Security. The Security category is expanded, showing sub-items: Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, Security Database, and Control. The Security Database item is selected, and the Control sub-item is active. The main content area is titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" and contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services". Below these is an "Apply Changes" button.

Select **Security → Security Database → CTI Users → List All Users** and select the “test” CTI user which is 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.

The screenshot shows a web interface with a red header bar containing "Security | Security Database | CTI Users | List All Users". On the left is a navigation tree with categories: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, and Security. The Security category is expanded, showing sub-items: Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, Security Database, and CTI Users. The CTI Users item is selected, and the List All Users sub-item is active. The main content area is titled "Edit CTI User" and contains a form for editing a CTI user. The form has a "User Profile:" section with fields for "User ID", "Common Name", and "Worktop Name". The "Unrestricted Access" checkbox is checked and highlighted with a red box. Below this are sections for "Call and Device Control:", "Call and Device Monitoring:", and "Routing Control:". The "Call and Device Control:" section has a dropdown for "Call Origination/Termination and Device Status" set to "None". The "Call and Device Monitoring:" section has dropdowns for "Device Monitoring" (set to "None"), "Calls On A Device Monitoring" (set to "None"), and "Call Monitoring" (unchecked). The "Routing Control:" section has a dropdown for "Allow Routing on Listed Devices" set to "None". At the bottom are "Apply Changes" and "Cancel Changes" buttons.

## 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.

**AVAYA**

**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 11:58:36 EST 2016  
HA Status: Not Configured

Networking | Ports

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▼ Networking

AE Service IP (Local IP)

Network Configure

Ports

TCP/TLS Settings

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

**Ports**

CVLAN Ports

Unencrypted TCP Port9999

Enabled Disabled

Encrypted TCP Port9998

DLG PortTCP Port5678

TSAPI Ports

TSAPI Service Port450

Local TLINK Ports

TCP Port Min1024

TCP Port Max1039

Unencrypted TLINK Ports

TCP Port Min1050

TCP Port Max1065

Encrypted TLINK Ports

TCP Port Min1066

TCP Port Max1081

DMCC Server Ports

Unencrypted Port4721

Enabled Disabled

Encrypted Port4722

TR/87 Port4723

## 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

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▼ Maintenance

Date Time/NTP Server

▶ Security Database

Service Controller

▶ Server Data

▶ Networking

▶ Security

**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](#)

Start

Stop

Restart Service

Restart AE Server

Restart Linux

Restart Web Server

KP; Reviewed:  
SPOC 2/8/2017

Solution & Interoperability Test Lab Application Notes  
©2017 Avaya Inc. All Rights Reserved.

20 of 29  
EMERES-AES7

## 7. Configure EMERES System

This section provides steps to configure EMERES Softphone Module application. During the compliance test, the installation and configuration of EMERES system was performed by EMERES engineer. This section describes the initial and basic configuration of EMERES application.

The configuration in the EMERES Softphone must be done in 2 steps at two in order for the soft phone to work. First part must be done in the ini file called **AvayaAES.ini** and the second part in the database using the application **DispatchNowTelephonyConfigurator.exe**.

### 7.1. Configuration of ini file AvayaAES.ini

All the part in bold should be set, the rest should remain intact

```
[AES]
Extension=3301
AcdGroupExtension=3320
AcdGroupName=Skill-2

StartAutoKeepAlive=true

#Session duration - the maximum time that the AE Services server will wait for a
#timer reset, before moving the session to the inactive state. This timer is reset
#when the server receives a ResetApplicationSessionTimer message from
#the application.
SessionDuration=180

#Session cleanup time – the amount of time that the AE Services server waits,
#after the connection to the client has been lost. Once this time has expired, the
#session, and any devices, monitors and device registrations associated with the
#session, are cleaned up. This timer defaults to 0 for backwards compatibility
#purposes, but it is recommended that it be set to a higher value, such as 60.
SessionCleanupDelay=60

# If not passed from the application use the Agent and AgentPassword from ini file
Agent=1000
AgentPassword=1234
AgentStatePollingTO=2000
ReportDivertedAsReleased=true

#Parameters that should be in global config
AesSocketPort=4721
AesIpAddr=10.33.1.4
SwitchIpInterface=10.33.1.6
```

```

SecureSocket=false
SwitchName=interopCM
DmccLogin=ctiuser
DmccPassword=CTIuser123#
SessionName=EmeresSession
ProtocoleVersion=http://www.ecma-international.org/standards/ecma-323/csta/ed3/priv7
AllowCertificateNameMismatch=true

# Soft phone parameters
UseAsSoftPhone=false
ForceLogin=false
MediaInfoDepMode=Independent
MediaMode=None
#Extension means extension password only used when registering terminal
Password=1234

[Audiolog]
SimulPlayback=true
ServerName=192.168.1.25
UserId=Admin
Password=Admin
SharedDirectory=al_record
RemoteDirectory=d:\record











[DEBUG]
AvayaAES_AgentStateMonitor=false
AvayaAES_XMLDisplay=false

```

## 7.2. Configuration in the database

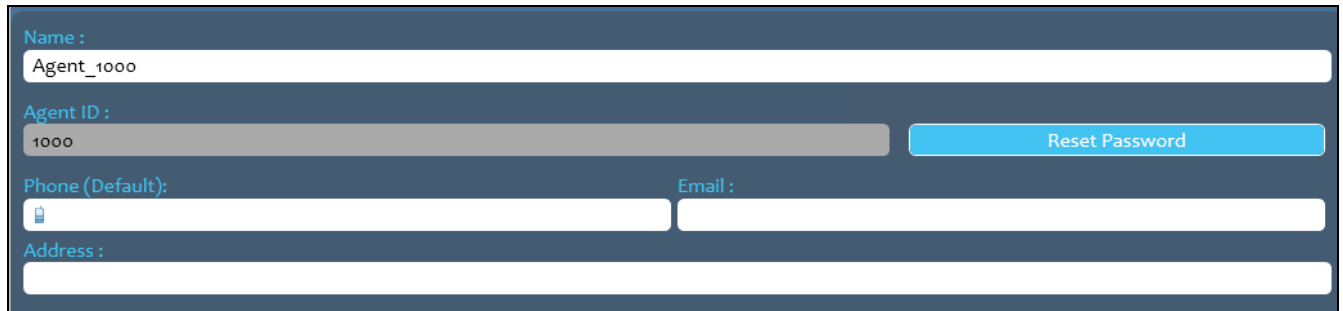
- Line configuration

In the compliance test there were 3 extensions 3301, 3302 and 3402 and 2 hunt group skillsets 3320 and 3321 were configured but only one can be used in a telephony session which was the hunt group number 3320.

Name	Line Group	Line Type	Queue Buttons		
3301	3301	Internal	Interno		
3302	3302	Internal	Interno		
3320	3320	911	911		
3321	3321	911	911		
3402	3402	Internal	Interno		

- Agent configuration (AGENTS section)

**Agent ID** is the login name and **Name** is the text that will appear at the top of the soft phone. Password is tiburon123 for all agents. The rest of the values are set at default.



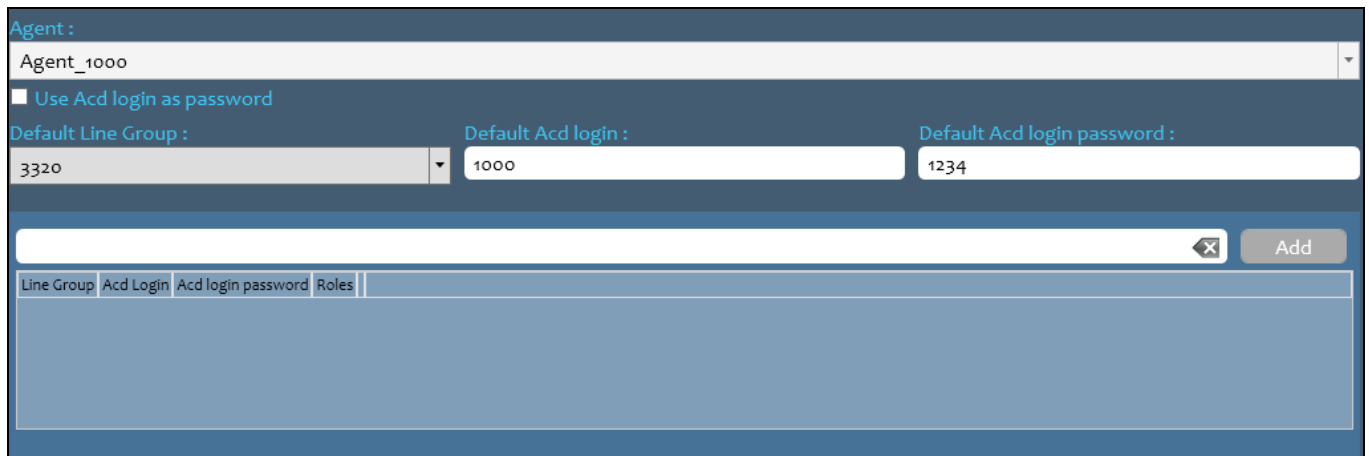
Name :  
Agent\_1000

Agent ID :  
1000 Reset Password

Phone (Default): Email :

Address :

- In ACD LOGINS section: select the agent name as configured in the step above from the combo box and the select the hunt group skillset number **3320** that the agent will be logged into from the Default Line Group section. Then enter the agent's password that will be used to log into the hunt group queue 3320 in the **Default Acd login password** field.



Agent :  
Agent\_1000

☐ Use Acd login as password

Default Line Group : Default Acd login : Default Acd login password :

3320 1000 1234

Add

Line Group	Acd Login	Acd login password	Roles

## 8. Verification Steps

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

### 8.1. 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

### 8.2. 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 User **test** that was used by EMERES application.

Status | Status and Control | DMCC Service SummaryHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

▶ Alarm Viewer

▶ Log Manager

▶ Logs

▼ Status and Control

▶ CVLAN Service Summary

▶ DLG Services Summary

▶ DMCC Service Summary

▶ Switch Conn Summary

▶ TSAPI Service Summary

▶ User Management

▶ Utilities

▶ Help

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)

Generated on Tue Dec 06 11:32:31 EST 2016

Service Uptime: 5 days, 1 hours 35 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 16

Number of Existing Devices: 1

Number of Devices Created Since Service Boot: 10

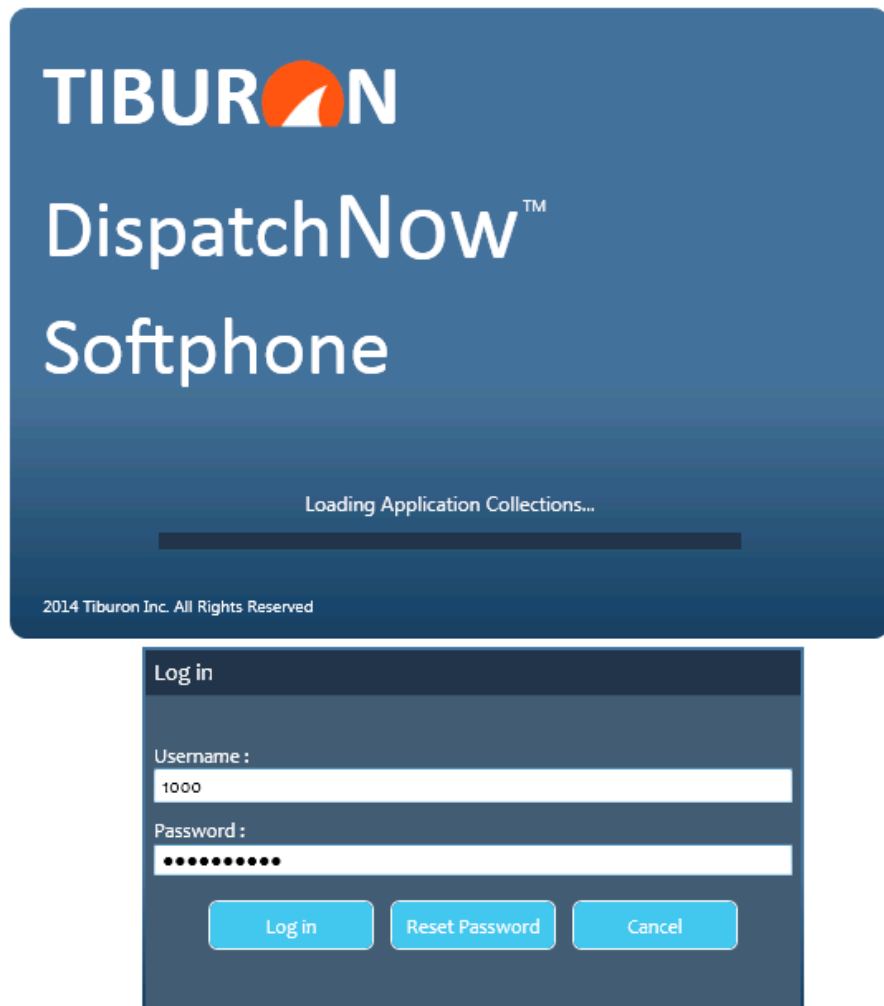
	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	62F9B127B3D4A6AC7 704950FC4903599-8	ctiuser	EmeresSession	10.10.97.30	XML Unencrypted	1

Item 1-1 of 1  
1 Go



### 8.3. Verify EMERES Softphone

Launch the EMERES Softphone client, enter a pre-defined username and its password in the **Username** and **Password** fields. Click **Login** button to log in the Softphone client.



When the Softphone client is logged in, select the **Log In** button to log in to the hunt group skill 3320 as configure in **Section 5.6** and select **Set Ready**, observe the states on the agent's deskphone are changed accordingly. The agent is now in Ready mode as indicated with the green circle next to agent's name Agent\_1000 shown in the picture below.



Place a ACD call to VDN number, the ACD call then is presented to the agent's deskphone, answer the ACD call by selecting the hunt group number button on the Softphone. The call is established on the agent's deskphone and the state is synchronized in the EMERES Softphone.



## 9. Conclusion

These Application Notes describe the configuration steps required for EMERES Softphone Module to successfully interoperate with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

## 10. 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] Administering Avaya Aura® Session Manager, Release 7.0, Issue 7, Jan 2016.
- [3] Administering Avaya Aura® Experience Portal, Release 7.0.1, April 2015.
- [4] Avaya Aura® Application Enablement Services Administration and Maintenance Guide, Release 7.0, Document 02-300357, Jan 2016.

Documentation related to EMERES may directly be obtained from EMERES

---

**©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).