



**Application Notes for Enghouse Interactive
Communications Center 2016R2 with Avaya Aura®
Communication Manager 7.0 using Avaya Aura®
Application Enablement Services 7.0 – Issue 1.0**

Abstract

These Application Notes describe the configuration steps required for Enghouse Interactive Communications Center 2016R2 to interoperate with Avaya Aura® Communication Manager 7.0 using Avaya Aura® Application Enablement Services 7.0. Enghouse Interactive Communications Center is a multi-channel and multi-contact solution that can handle voice, fax, web, and email contacts.

The compliance testing focused on the voice integration with Avaya Aura® Communication Manager via the Avaya Aura® Application Enablement Services Telephony Services Application Programming Interface and Device, Media, and Call Control interface.

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 Enghouse Interactive Communications Center (EICC) 2016R2 to interoperate with Avaya Aura® Communication Manager 7.0 using Avaya Aura® Application Enablement Services 7.0. EICC is a multi-channel and multi-contact solution that can handle voice, fax, web, and email contacts.

The compliance testing focused on the voice integration with Communication Manager via the Application Enablement Services Telephony Services Application Programming Interface (TSAPI) and Device, Media, and Call Control (DMCC) interface.

The agents and supervisors are configured as station users on Communication Manager, and have desktop computers running the Enghouse Interactive Desktop application. The ACD functionality such as queuing, work modes, and announcements are provided by EICC.

The TSAPI interface is used by EICC to monitor the agent and supervisor station extensions, provide screen pops and call control for agent desktops, route incoming calls using adjunct routing capability, and support enable/disable of call forwarding and message waiting lamps using set value capability.

The DMCC interface is used by EICC to support voicemail, announcement, and basic call recording features. Voicemail and announcement calls were redirected to an available virtual IP softphone to terminate to EICC, and recording was accomplished by intruding a virtual IP softphone via TSAPI single step conference onto an active call to pick up the media for recording.

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the EICC application, the application automatically used TSAPI to query device name, requested device monitoring, and registered for VDN routing. The application also automatically used DMCC to register the virtual IP softphones.

For the manual part of the testing, incoming calls were made to the general routing VDNs. The EICC server used query results and event reports to track agent states, and specified calls to be routed to available agents or to call treatment VDNs. Manual call controls from both the agent telephones and the agent desktop computers were exercised to verify call control features such as answering and transferring of calls.

Voicemail was tested by not answering call at the agent, and have the call covered to EICC with proper leaving of voice message and activation of agent message waiting lamp. Manual call was then made from the agent to the voicemail VDN to retrieve voice message and verify proper deactivation of message waiting lamp.

The serviceability test cases were performed manually by disconnecting and reconnecting the Ethernet connection to the EICC server.

The verification of tests included human checking of proper states at the telephones, and of capturing and analyzing the TSAPI and DMCC message traces from the EICC 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 EICC:

- Use of TSAPI query service to query device names.
- Use of TSAPI event report service to monitor agents, supervisor, and virtual IP softphones.
- Use of TSAPI routing service to route incoming calls.
- Use of TSAPI set value service to activate/deactivate call forwarding and message waiting indicator.
- Use of TSAPI call control service to support manual call control actions initiated from the agent desktop, to handle inbound voicemail calls to the virtual IP softphones, and to add virtual IP softphone to existing calls for media capture.
- Use of DMCC registration service to register and un-register the virtual IP softphones.
- Proper handling of call scenarios involving screen pop, inbound, outbound, ACD, non-ACD, drop, hold/reconnect, voicemail, blind/attended transfer, attended conference, call forwarding, supervisor monitor, multiple agents, multiple calls, queuing, send DTMF, long duration, and recording of basic calls.

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

2.2. Test Results

All test cases were executed. The following were observations on EICC from the compliance testing.

- EICC created one DMCC version per virtual IP softphone by design.
- For the attended conference scenario, after the PSTN drops, one of the remaining agent's Phone Calls section reflected his/her name instead of name of the other agent.

2.3. Support

Technical support on EICC can be obtained through the following:

- **Phone:** (800) 513-2810
- **Web:** www.enghouseinteractive.com
- **Email:** usa.support@enghouse.com

3. Reference Configuration

The detailed administration of basic connectivity between Communication Manager and Application Enablement Services is not the focus of these Application Notes and will not be described.

The contact center devices used in the compliance testing are shown in the table below. In the compliance testing, EICC monitored two agents and one supervisor station extensions shown below.

Device Type	Device Number/Extension
VDNs	67701-67708
Vectors	700-705, 708
Agent stations	65001, 66002
Supervisor & Failure covering station	65000

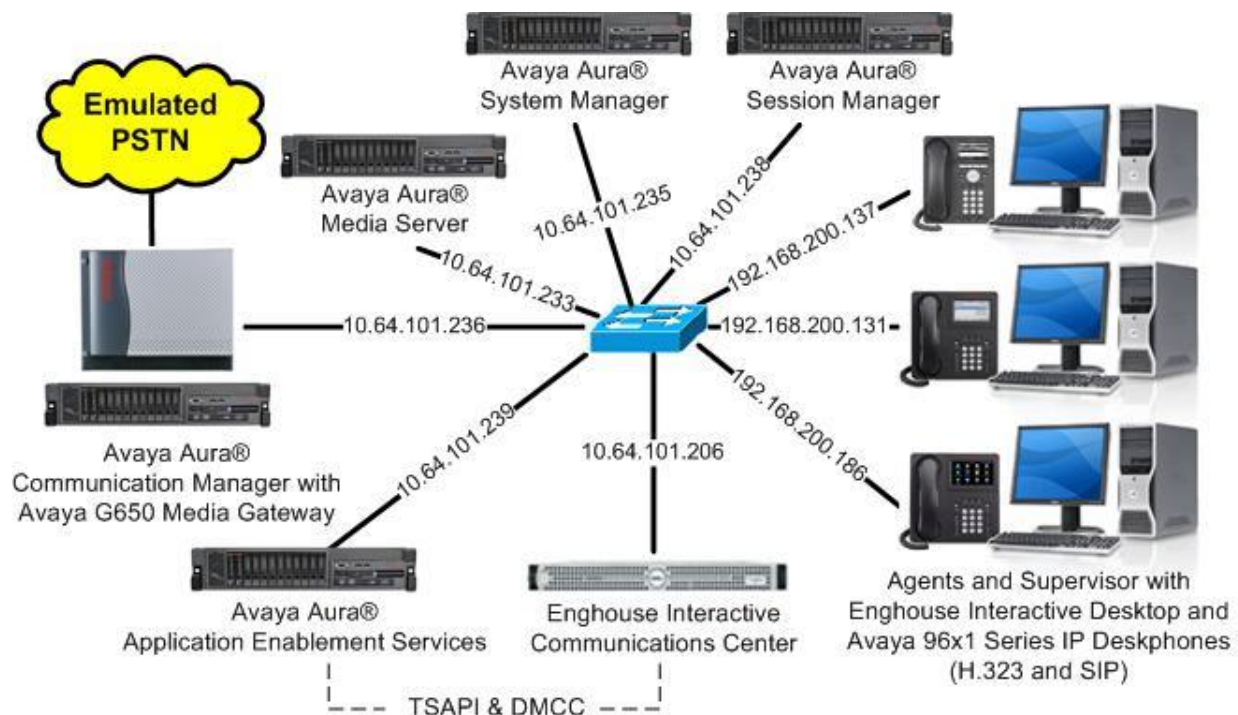


Figure 1: Compliance Testing Configuration

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 in Virtual Environment	7.0.1.1 (7.0.1.1.0.441.23169)
Avaya G650 Media Gateway	NA
Avaya Aura® Media Server in Virtual Environment	7.7.0.334
Avaya Aura® Application Enablement Services in Virtual Environment	7.0.1 (7.0.1.0.2.15-0)
Avaya Aura® Session Manager in Virtual Environment	7.0 .1.1 (7.0.1.1.701114)
Avaya Aura® System Manager in Virtual Environment	7.0 .1.1 (7.0.1.1.065378)
Avaya 9611G & 9641G IP Deskphone (H.323)	6.6302
Avaya 9621G IP Deskphone (SIP)	7.0.1.2.9
Enghouse Interactive Communications Center on Windows Server 2012 R2 <ul style="list-style-type: none">Avaya TSAPI Windows Client (csta32.dll)Avaya DMCC XML	2016R2 (9.1.0.4500 CU) Standard 6.3.3.103 6.2
Enghouse Interactive Desktop on Windows 10 Pro	2016R2 (9.1.0.4500 CU)

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 vectors and VDNs
- Administer voicemail coverage path
- Administer agents and supervisors
- Administer virtual IP softphones

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 11
OPTIONAL FEATURES		
Abbreviated Dialing Enhanced List? y	Audible Message Waiting? y	
Access Security Gateway (ASG)? n	Authorization Codes? y	
Analog Trunk Incoming Call ID? y	CAS Branch? n	
A/D Grp/Sys List Dialing Start at 01? y	CAS Main? n	
Answer Supervision by Call Classifier? y	Change COR by FAC? n	
ARS? y	Computer Telephony Adjunct Links? y	
ARS/AAR Partitioning? y	Cvg Of Calls Redirected Off-net? y	
ARS/AAR Dialing without FAC? y	DCS (Basic)? y	
ASAI Link Core Capabilities? y	DCS Call Coverage? y	
ASAI Link Plus Capabilities? y	DCS with Rerouting? y	

Navigate to **Page 7**, and verify that the **Vectoring (Basic)** customer option is set to “y”.

display system-parameters customer-options		Page 7 of 11
CALL CENTER OPTIONAL FEATURES		
Call Center Release: 7.0		
ACD? y	Reason Codes? y	
BCMS (Basic)? y	Service Level Maximizer? n	
BCMS/VuStats Service Level? y	Service Observing (Basic)? y	
BSR Local Treatment for IP & ISDN? y	Service Observing (Remote/By FAC)? y	
Business Advocate? n	Service Observing (VDNs)? y	
Call Work Codes? y	Timed ACW? y	
DTMF Feedback Signals For VRU? y	Vectoring (Basic)? y	
Dynamic Advocate? n	Vectoring (Prompting)? y	
Expert Agent Selection (EAS)? y	Vectoring (G3V4 Enhanced)? y	
EAS-PHD? y	Vectoring (3.0 Enhanced)? 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: 60111		
Type: ADJ-IP		
COR: 1		
Name: AES CTI Link		

5.3. Administer Vectors and VDNs

Administer a set of vectors and VDNs per EICC installation document [3]. These vectors and VDNs provide general routing and different call treatments to incoming calls. The vectors and VDNs that were used for the compliance testing are shown below.

VDN	Vector	Purpose
67701	701	Ring treatment
67702	702	Music treatment
67703	703	Busy treatment
67704	704	Failure coverage
67705	705	Voicemail routing
67706	700	General routing for the Sales application
67707	700	General routing for the Support application
67708	708	Hold treatment

5.3.1. Failure Coverage

Modify a vector using the “change vector n” command, where “n” is an available vector number. This vector will provide failure coverage and routing to the CTI link defined in **Section 5.2**. Note that the vector **Number** and **route-to number** may vary, and that the **route-to number** is used as the covering point in case of failure from the adjunct routing step.

In the compliance testing, the supervisor extension from **Section 3** was used as the covering point. As shown below, use “SC Fail” as the vector **Name**, with the wait treatment and remaining vector steps as specified in the EICC installation document [3].

```
change vector 704                                     Page 1 of 6
                                                    CALL VECTOR
Number: 704      Name: SC Fail
Multimedia? n    Attendant Vectoring? n    Meet-me Conf? n    Lock? n
Basic? y          EAS? y    G3V4 Enhanced? y    ANI/II-Digits? y    ASAI Routing? y
Prompting? y      LAI? y    G3V4 Adv Route? y    CINFO? y    BSR? y    Holidays? y
Variables? y      3.0 Enhanced? y
01 adjunct      routing link 1
02 wait-time    5 secs hearing silence
03 route-to     number 65000      with cov n if unconditionally
04 stop
05
```

Add a VDN using the “add vdn n” command, where “n” is an available extension. Associate this VDN with the newly added vector from above.

- **Name:** “SC Fail”
- **Destination:** “Vector Number”
- **Vector Number:** The “SC Fail” vector number from above.

```
add vdn 67704                                     Page 1 of 3
                                                    VECTOR DIRECTORY NUMBER
Extension: 67704
Name*: SC Fail
Destination: Vector Number      704
```

5.3.2. General Routing

Modify a vector using the “change vector n” command, where “n” is an available vector number. This vector will provide general routing to the CTI link defined in **Section 5.2**. Note that the vector **Number** and **route-to number** may vary, and that the **route-to number** is used as the covering point in case of failure from the adjunct routing step, and set to the failure coverage VDN from **Section 5.3.1**.

Enter a descriptive name for the vector **Name** field, and configure the remaining vector steps as specified in [3].

change vector 700	Page 1 of 6
CALL VECTOR	
Number: 700 Name: EICC User Q	
Multimedia? n	Attendant Vectoring? n Meet-me Conf? n Lock? n
Basic? y	EAS? y G3V4 Enhanced? y ANI/II-Digits? y ASAI Routing? y
Prompting? y	LAI? y G3V4 Adv Route? y CINFO? y BSR? y Holidays? y
Variables? y	3.0 Enhanced? y
01 adjunct	routing link 1
02 wait-time	2 secs hearing silence
03 route-to	number 67704 with cov y if unconditionally
04 stop	
05	

For each incoming call application, add a VDN using the “add vdn n” command, where “n” is an available extension. Associate this VDN with the newly added vector from above. For the compliance testing, two VDNs were added, as shown below.

- **Name:** A descriptive name.
- **Destination:** “Vector Number”
- **Vector Number:** The “EICC User Q” vector number from above.

add vdn 67706	Page 1 of 2
VECTOR DIRECTORY NUMBER	
Extension: 67706	
Name: EICC Sales	
Destination: Vector Number	700

add vdn 67707	Page 1 of 2
VECTOR DIRECTORY NUMBER	
Extension: 67707	
Name: EICC Support	
Destination: Vector Number	700

5.3.3. Ring Treatment

Modify a vector using the “change vector n” command, where “n” is an available vector number. This vector will provide ring treatment and routing to the CTI link defined in **Section 5.2**. Note that the vector **Number** and **route-to number** may vary, and that the **route-to number** is used as the covering point in case of failure from the adjunct routing step, and set to the failure coverage VDN from **Section 5.3.1**.

Enter a descriptive name for the vector **Name** field, and configure the remaining vector steps as specified in [3].

change vector 701	Page 1 of 6
CALL VECTOR	
Number: 701 Name: SC Ring	
Multimedia? n	Attendant Vectoring? n Meet-me Conf? n Lock? n
Basic? y	EAS? y G3V4 Enhanced? y ANI/II-Digits? y ASAI Routing? y
Prompting? y	LAI? y G3V4 Adv Route? y CINFO? y BSR? y Holidays? y
Variables? y	3.0 Enhanced? y
01 adjunct	routing link 1
02 wait-time	60 secs hearing ringback
03 route-to	number 67704 with cov n if unconditionally
04 stop	
05	

Add a VDN using the “add vdn n” command, where “n” is an available extension. Associate this VDN with the newly added vector from above.

- **Name:** “SC Ring”
- **Destination:** “Vector Number”
- **Vector Number:** The “SC Ring” vector number from above.

add vdn 67701	Page 1 of 2
VECTOR DIRECTORY NUMBER	
Extension: 67701	
Name: SC Ring	
Destination: Vector Number	701

5.3.4. Music Treatment

Modify a vector using the “change vector n” command, where “n” is an available vector number. This vector will provide music treatment and routing to the CTI link defined in **Section 5.2**.

Note that the vector **Number** and **route-to number** may vary, and that the **route-to number** is used as the covering point in case of failure from the adjunct routing step, and set to the failure coverage VDN from **Section 5.3.1**.

Enter a descriptive name for the vector **Name** field, and configure the remaining vector steps as specified in [3].

change vector 702	Page 1 of 6
CALL VECTOR	
Number: 702 Name: SC Music	
Multimedia? n	Attendant Vectoring? n Meet-me Conf? n Lock? n
Basic? y	EAS? y G3V4 Enhanced? y ANI/II-Digits? y ASAI Routing? y
Prompting? y	LAI? y G3V4 Adv Route? y CINFO? y BSR? y Holidays? y
Variables? y	3.0 Enhanced? y
01 adjunct	routing link 1
02 wait-time	60 secs hearing music
03 route-to	number 67704 with cov n if unconditionally
04 stop	
05	

Add a VDN using the “add vdn n” command, where “n” is an available extension. Associate this VDN with the newly added vector from above.

- **Name:** “SC Music”
- **Destination:** “Vector Number”
- **Vector Number:** The “SC Music” vector number from above.

add vdn 67702	Page 1 of 2
VECTOR DIRECTORY NUMBER	
Extension: 67702	
Name: SC Music	
Destination: Vector Number	702

5.3.5. Busy Treatment

Modify a vector using the “change vector n” command, where “n” is an available vector number. This vector will provide busy treatment and routing to the CTI link defined in **Section 5.2**. Note that the vector **Number** may vary.

Enter a descriptive name for the vector **Name** field, and configure the remaining vector steps as specified in [3].

change vector 703	Page 1 of 6
CALL VECTOR	
Number: 703 Name: SC Busy	
Multimedia? n	Attendant Vectoring? n Meet-me Conf? n Lock? n
Basic? y	EAS? y G3V4 Enhanced? y ANI/II-Digits? y ASAI Routing? y
Prompting? y	LAI? y G3V4 Adv Route? y CINFO? y BSR? y Holidays? y
Variables? y	3.0 Enhanced? y
01 adjunct	routing link 1
02 busy	
03	

Add a VDN using the “add vdn n” command, where “n” is an available extension. Associate this VDN with the newly added vector from above.

- **Name:** “SC Busy”
- **Destination:** “Vector Number”
- **Vector Number:** The “SC Busy” vector number from above.

add vdn 67703	Page 1 of 2
VECTOR DIRECTORY NUMBER	
Extension: 67703	
Name: SC Busy	
Destination: Vector Number	703

5.3.6. Voicemail Routing

Modify a vector using the “change vector n” command, where “n” is an available vector number. This vector will provide voicemail routing to the CTI link defined in **Section 5.2**. Note that the vector **Number** may vary.

Enter a descriptive name for the vector **Name** field, and configure the remaining vector steps as specified in [3].

change vector 705	CALL VECTOR	Page 1 of 6
Number: 705	Name: SC Voicemail	
Multimedia? n	Attendant Vectoring? n	Meet-me Conf? n
Basic? y	EAS? y	G3V4 Enhanced? y
Prompting? y	LAI? y	G3V4 Adv Route? y
Variables? y	3.0 Enhanced? y	CINFO? y
01 adjunct	routing link 1	BSR? y
02 wait-time	120 secs hearing ringback	Holidays? y
03 stop		
04		

Add a VDN using the “add vdn n” command, where “n” is an available extension. Associate this VDN with the newly added vector from above.

- **Name:** “SC Voicemail”
- **Destination:** “Vector Number”
- **Vector Number:** The “SC Voicemail” vector number from above.

add vdn 67705	VECTOR DIRECTORY NUMBER	Page 1 of 2
	Extension: 67705	
	Name: SC Voicemail	
	Destination: Vector Number	705

5.3.7. Hold Treatment

Modify a vector using the “change vector n” command, where “n” is an available vector number. This vector will provide hold treatment and routing to the CTI link defined in **Section 5.2**. Note that the vector **Number** and **route-to number** may vary, and that the **route-to number** is used as the covering point in case of failure from the adjunct routing step, and set to the failure coverage VDN from **Section 5.3.1**.

Enter a descriptive name for the vector **Name** field, and configure the remaining vector steps as specified in [3].

change vector 708		Page 1 of 6	
CALL VECTOR			
Number: 708		Name: SC Hold	
Multimedia? n	Attendant Vectoring? n	Meet-me Conf? n	Lock? n
Basic? y	EAS? y	G3V4 Enhanced? y	ANI/II-Digits? y
Prompting? y	LAI? y	G3V4 Adv Route? y	ASAI Routing? y
Variables? y	3.0 Enhanced? y	CINFO? y	BSR? y
01 adjunct	routing link 1	Holidays? y	
02 wait-time	60 secs hearing music		
03 route-to	number 67704	with cov n if unconditionally	
04 stop			
05			

Add a VDN using the “add vdn n” command, where “n” is an available extension. Associate this VDN with the newly added vector from above.

- Name: “SC Hold”
- Destination: “Vector Number”
- Vector Number: The “SC Hold” vector number from above.

add vdn 49108		Page 1 of 2	
VECTOR DIRECTORY NUMBER			
Extension: 67708			
Name: SC Hold			
Destination: Vector Number		708	

5.4. Administer Voicemail Coverage Path

Add a coverage path using the “add coverage path n” command, where “n” is an available coverage path number.

For the **Point1** field, enter “v67705” to designate as the first coverage point, where “67705” is the voicemail VDN extension from **Section 5.3.6**.

add coverage path 7		Page 1 of 1	
COVERAGE PATH			
Coverage Path Number: 7			
Cvg Enabled for VDN Route-To Party? n		Hunt after Coverage? n	
Next Path Number:		Linkage	
COVERAGE CRITERIA			
Station/Group Status	Inside Call	Outside Call	
Active?	n	n	
Busy?	y	y	
Don't Answer?	y	y	Number of Rings: 2
All?	n	n	
DND/SAC/Goto Cover?	y	y	
Holiday Coverage?	n	n	
COVERAGE POINTS			
Terminate to Coverage Pts. with Bridged Appearances? n			
Point1: v67705	Rng:	Point2:	
Point3:		Point4:	
Point5:		Point6:	

5.5. Administer Agents and Supervisors

Use the “change station n” command, where “n” is first existing agent station extension from **Section 3**. In the **Coverage Path 1** field, enter the voicemail coverage path number from **Section 5.4**.

```
change station 65001
```

Page 1 of 5

STATION		
Extension: 65001	Lock Messages? n	BCC: 0
Type: 9611	Security Code: *	TN: 1
Port: S00102	Coverage Path 1: 7	COR: 1
Name: CM7 Station 1	Coverage Path 2:	COS: 1
	Hunt-to Station:	Tests? y

STATION OPTIONS

Location: 1	Time of Day Lock Table:
Loss Group: 19	Personalized Ringing Pattern: 1
	Message Lamp Ext: 65001
Speakerphone: 2-way	Mute Button Enabled? y
Display Language: english	Button Modules: 0
Survivable GK Node Name:	
Survivable COR: internal	Media Complex Ext:
Survivable Trunk Dest? y	IP SoftPhone? n
	IP Video Softphone? n
	Short/Prefixed Registration Allowed: default

Repeat this section for all agents and supervisors. In the compliance testing, two agents and one supervisor were configured as shown below.

```
list station 65000 count 3
```

STATIONS							
Ext/ Hunt-to	Port/ Type	Name/ Surv GK NN	Move	Room/ Data Ext	Cv1/ Cv2	COR/ COS	Cable/ Jack
65000	S00036	CM7 Supervisor			7	1	
	9641		no			1	
65001	S00102	CM7 Station 1			7	1	
	9611		no			1	
66002	S00004	Avaya, SIP 2			7	1	
	9621SIPCC		no			1	

5.6. Administer Virtual IP Softphones

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

- **Type:** “4624”
- **Name:** A descriptive name.
- **Security Code:** A desired value.
- **IP SoftPhone:** “y”

```

add station 67791
                                     Page 1 of 6
                                     STATION
Extension: 67791                    Lock Messages? n                    BCC: 0
  Type: 4624                        Security Code: 123456                TN: 1
  Port: S00129                     Coverage Path 1:                COR: 1
  Name: EICC Virtual #1             Coverage Path 2:                COS: 1
                                     Hunt-to Station:                Tests? y

STATION OPTIONS
      Location:                    Time of Day Lock Table:
      Loss Group: 19               Personalized Ringing Pattern: 1
                                   Message Lamp Ext: 67791
      Speakerphone: 2-way          Mute Button Enabled? y
      Display Language: english
      Survivable GK Node Name:
      Survivable COR: internal      Media Complex Ext:
      Survivable Trunk Dest? y      IP SoftPhone? y

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

Repeat this section to administer the desired number of virtual IP softphones using sequential extension numbers and same security code value. In the compliance testing, two virtual IP softphones were administered as shown below.

```

list station 67791 count 2
                                     STATIONS
Ext/      Port/   Name/      Room/      Cv1/  COR/  Cable/
 Hunt-to   Type     Surv GK NN  Data Ext   Cv2   COS   Jack
-----
67791      S00129  EICC Virtual #1      no      1
         4624
67792      S00132  EICC Virtual #2      no      1
         4624
  
```

6. Configure Avaya Aura® Application Enablement Services

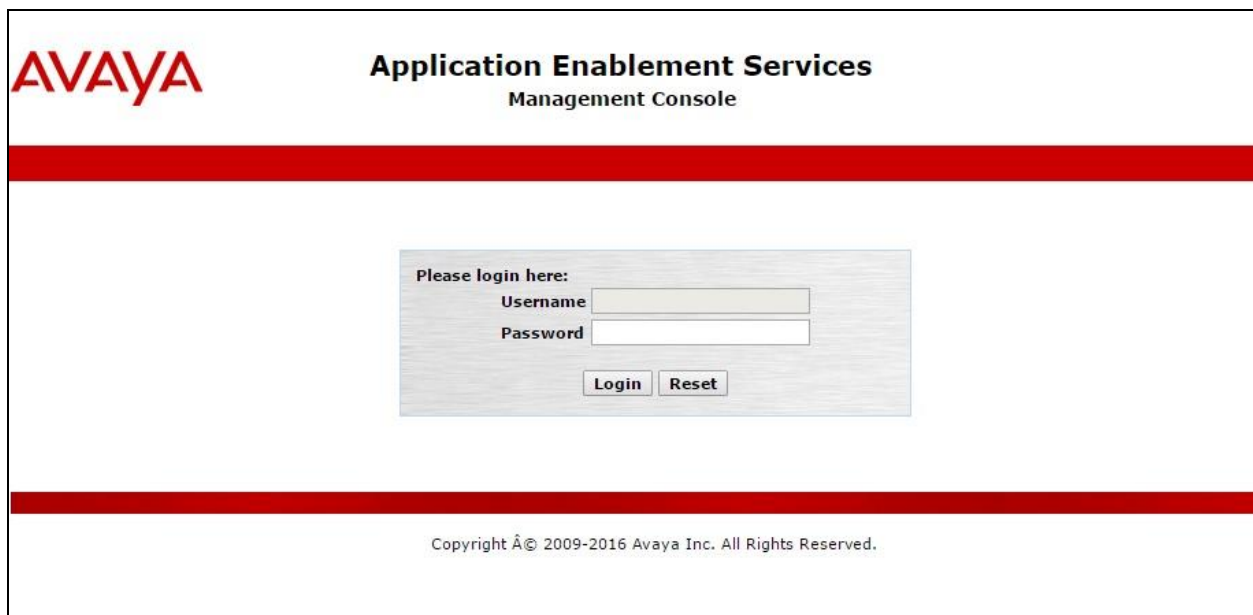
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer H.323 gatekeeper
- Administer EICC user
- Administer security database
- Administer ports
- Administer TCP settings
- Restart services
- Obtain Tlink name

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 the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" is displayed in a large, bold font, with "Management Console" in a smaller font below it. A thick red horizontal bar spans the width of the page. Below this bar is a light gray rectangular box containing the login form. The form has the heading "Please login here:" followed by two input fields: "Username" and "Password". Below these fields are two buttons: "Login" and "Reset". Another thick red horizontal bar is located below the login box. At the bottom of the page, centered, is the copyright notice: "Copyright © 2009-2016 Avaya Inc. All Rights Reserved."

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

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title "Application Enablement Services Management Console". A welcome message in the top right corner provides user information: "Welcome: User", "Last login: Tue Sep 20 13:56:14 2016 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: 7.0.1.0.2.15-0", "Server Date and Time: Tue Sep 20 14:07:06 EDT 2016", and "HA Status: Not Configured". A red navigation bar at the top contains "Home", "Help", and "Logout" links. On the left, a sidebar menu lists various services: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area, titled "Welcome to OAM", explains that the OAM Web provides tools for managing the AE Server and lists administrative domains: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. It also notes that these domains can be served by one administrator for all or separate administrators for each.

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Tue Sep 20 13:56:14 2016 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: 7.0.1.0.2.15-0
Server Date and Time: Tue Sep 20 14:07:06 EDT 2016
HA Status: Not Configured

Home | Help | Logout

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.

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 displays the Avaya Application Enablement Services Management Console with the "Licensing" section selected in the sidebar. The top header and welcome message are identical to the previous screenshot. The red navigation bar now highlights "Licensing". The sidebar menu shows "Licensing" expanded, with sub-items: "WebLM Server Address", "WebLM Server Access", and "Reserved Licenses". The main content area, titled "Licensing", provides instructions for setting up and maintaining the WebLM, including the need to use the following: WebLM Server Address, WebLM Server Access, and Reserved Licenses. It also mentions that if you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following: Reserved Licenses.

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Tue Sep 20 13:56:14 2016 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: 7.0.1.0.2.15-0
Server Date and Time: Tue Sep 20 14:07:06 EDT 2016
HA Status: Not Configured

Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
WebLM Server Address
WebLM Server Access
Reserved Licenses
Maintenance
Networking

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

Verify that there are sufficient licenses for **TSAPI Simultaneous Users** and **Device Media and Call Control**, as shown below. The TSAPI license is used for device monitoring and the DMCC license is used for the virtual IP softphones. Also verify that there is an applicable advanced switch license, in this case **AES ADVANCED LARGE SWITCH**.

TLT; Reviewed: Solution & Interoperability Test Lab Application Notes 21 of 51
SPOC 11/3/2016 ©2016 Avaya Inc. All Rights Reserved. EICC-AES7

6.3. 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 screenshot shows the AVAYA Application Enablement Services Management Console. The top right corner displays user information: "Welcome: User", "Last login: Tue Sep 20 13:56:14 2016 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: 7.0.1.0.2.15-0", "Server Date and Time: Tue Sep 20 14:07:06 EDT 2016", and "HA Status: Not Configured". The left navigation pane shows "AE Services" expanded, with "TSAPI" selected, and "TSAPI Links" highlighted. The main content area is titled "TSAPI Links" and contains a table with columns: "Link", "Switch Connection", "Switch CTI Link #", "ASAI Link Version", and "Security". Below the table are buttons for "Add Link", "Edit Link", and "Delete Link".

The **Add TSAPI Links** screen is displayed next.

The **Link** field is only local to the Application Enablement Services server, and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection "cm7" is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields.

The screenshot shows the AVAYA Application Enablement Services Management Console with the "Add TSAPI Links" screen. The left navigation pane shows "AE Services" expanded, with "TSAPI" selected, and "TSAPI Links" highlighted. The main content area is titled "Add TSAPI Links" and contains form fields for "Link", "Switch Connection", "Switch CTI Link Number", "ASAI Link Version", and "Security". The "Link" field has a dropdown menu with "1" selected. The "Switch Connection" field has a dropdown menu with "cm7" selected. The "Switch CTI Link Number" field has a dropdown menu with "1" selected. The "ASAI Link Version" field has a dropdown menu with "7" selected. The "Security" field has a dropdown menu with "Unencrypted" selected. Below the form fields are buttons for "Apply Changes" and "Cancel Changes".

6.4. Administer H.323 Gatekeeper

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

Locate the connection name associated with the relevant Communication Manager, in this case “cm7”, and select the corresponding radio button. Click **Edit H.323 Gatekeeper**.

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane has 'Communication Manager Interface' expanded, with 'Switch Connections' selected. The main area displays a table of switch connections. The table has four columns: 'Connection Name', 'Processor Ethernet', 'Msg Period', and 'Number of Active Connections'. There is one entry with 'cm7' as the connection name, 'No' for processor ethernet, '30' for msg period, and '1' for the number of active connections. Below the table are buttons for 'Edit Connection', 'Edit PE/CLAN IPs', 'Edit H.323 Gatekeeper', 'Delete Connection', and 'Survivability Hierarchy'. The top right of the console shows user information: 'Welcome: User', 'Last login: Tue Sep 20 13:56:14 2016 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: 7.0.1.0.2.15-0', 'Server Date and Time: Tue Sep 20 14:07:06 EDT 2016', and 'HA Status: Not Configured'.

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> cm7	No	30	1

The **Edit H.323 Gatekeeper** screen is displayed next. Enter the IP address of a C-LAN circuit pack or the Processor C-LAN on Communication Manager to use as the H.323 gatekeeper, in this case “10.64.101.236” as shown below. Click **Add Name or IP**.

The screenshot shows the 'Edit H.323 Gatekeeper - cm7' screen. The left navigation pane is the same as the previous screenshot. The main area has a text input field containing '10.64.101.236' and an 'Add Name or IP' button. Below the input field are labels 'Name or IP Address', 'Delete IP', and 'Back'. The top right of the console shows user information: 'Welcome: User', 'Last login: Tue Sep 13 09:45:41 2016 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: 7.0.1.0.2.15-0', 'Server Date and Time: Tue Sep 13 09:48:55 EDT 2016', and 'HA Status: Not Configured'.

6.5. Administer EICC 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.

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Sep 20 14:28:42 2016 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: 7.0.1.0.2.15-0
Server Date and Time: Tue Sep 20 17:12:17 EDT 2016
HA Status: Not Configured

User Management | User Admin | Add UserHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▼ User Management

▶ Service Admin

▼ User Admin

■ Add User

■ Change User Password

■ List All Users

■ Modify Default Users

■ Search Users

▶ Utilities

▶ Help

Add User

Fields marked with * can not be empty.

* User Id

* Common Name

* Surname

* User Password

* Confirm Password

Admin Note

Avaya Role

Business Category

Car License

CM Home

Css Home

CT User

Department Number

Display Name

Employee Number

Employee Type

Enterprise Handle

Given Name

6.6. Administer 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.

In the event that the security database is used by the customer with parameters already enabled, then follow reference [2] to configure access privileges for the EICC user from **Section 6.5**.

The screenshot displays 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 the user. The left navigation pane shows a tree structure with "Security" expanded, leading to "Security Database" and then "Control". 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". An "Apply Changes" button is located below these options.

Welcome: User
Last login: Tue Sep 20 13:56:14 2016 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: 7.0.1.0.2.15-0
Server Date and Time: Tue Sep 20 14:07:06 EDT 2016
HA Status: Not Configured

Security | Security Database | Control

Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
Account Management
Audit
Certificate Management
Enterprise Directory
Host AA
PAM
Security Database
Control

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

6.7. Administer Ports

Select **Networking** → **Ports** from the left pane, to display the **Ports** screen in the right pane.

In the **DMCC Server Ports** section, select the radio button for **Unencrypted Port** under the **Enabled** column, as shown below. Retain the default values in the remaining fields.

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Sep 20 13:56:14 2016 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: 7.0.1.0.2.15-0
Server Date and Time: Tue Sep 20 14:07:06 EDT 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 Settings

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Ports

CVLAN Ports

Unencrypted TCP Port9999

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

Encrypted Port4722

TR/87 Port4723

6.8. Administer TCP Settings

Select **Networking** → **TCP/TLS Settings** from the left pane, to display the **TCP / TLS Settings** screen in the right pane. For **TCP Retransmission Count**, select **TSAPI Routing Application Configuration (6)**, as shown below.

The screenshot displays 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 the user. The left navigation pane shows a tree structure with "Networking" expanded, and "TCP/TLS Settings" selected. The main content area shows the "TCP / TLS Settings" configuration page. It includes sections for "TLSv1 Protocol Configuration" with checkboxes for TLSv1.0, TLSv1.1, and TLSv1.2 (the last is checked), and "TCP Retransmission Count" with radio buttons for "Standard Configuration (15)" and "TSAPI Routing Application Configuration (6)" (the latter is selected). Below these are buttons for "Apply Changes", "Restore Defaults", and "Cancel Changes". A note explains that a smaller TCP Retransmission Count reduces the time the server waits for a TCP acknowledgement. A warning states that the setting applies to all TCP and TLS sockets and should be used with caution.

Welcome: User
Last login: Tue Sep 20 13:56:14 2016 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: 7.0.1.0.2.15-0
Server Date and Time: Tue Sep 20 14:07:51 EDT 2016
HA Status: Not Configured

Networking | TCP / TLS Settings 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

TCP / TLS Settings

TLSv1 Protocol Configuration

- ☐ Support TLSv1.0 Protocol
- ☐ Support TLSv1.1 Protocol
- ☒ Support TLSv1.2 Protocol

TCP Retransmission Count

- ☐ Standard Configuration (15)
- ☒ TSAPI Routing Application Configuration (6)

Apply Changes Restore Defaults Cancel Changes

Note: A smaller TCP Retransmission Count reduces the amount of time that the AE Services server waits for a TCP acknowledgement before closing the socket. Select the Standard Configuration setting unless this AE Services server is used by TSAPI routing applications.

Warning: This setting applies to all TCP and TLS sockets on the AE Services Server and so it should be used with caution.

6.9. Restart Services

Select **Maintenance** → **Service Controller** from the left pane, to display the **Service Controller** screen in the right pane. Check **DMCC Service** and **TSAPI Service**, and click **Restart Service**.

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Sep 20 13:56:14 2016 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: 7.0.1.0.2.15-0
Server Date and Time: Tue Sep 20 14:07:06 EDT 2016
HA Status: Not Configured

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

▶ Status

Service Controller

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input checked="" 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 checked="" 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

6.10. Obtain Tlink Name

Select **Security** → **Security Database** → **Tlinks** from the left pane. The **Tlinks** screen shows a listing of the Tlink names. A new Tlink name is automatically generated for the TSAPI service. Locate the Tlink name associated with the relevant switch connection, which would use the name of the switch connection as part of the Tlink name. Make a note of the associated Tlink name, to be used later for configuring EICC.

In this case, the associated Tlink name is “AVAYA#CM7#CSTA#AES7”. Note the use of the switch connection “CM7” from **Section 6.3** as part of the Tlink name.

The screenshot displays 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 the user. The main navigation bar shows "Security | Security Database | Tlinks" and links for "Home | Help | Logout". The left sidebar contains a tree view of the application's structure, with "Security" expanded to show "Security Database" and "Tlinks" selected. The main content area, titled "Tlinks", shows a single Tlink named "AVAYA#CM7#CSTA#AES7" with a "Delete Tlink" button.

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Tue Sep 20 13:56:14 2016 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: 7.0.1.0.2.15-0
Server Date and Time: Tue Sep 20 14:07:06 EDT 2016
HA Status: Not Configured

Security | Security Database | Tlinks Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
Account Management
Audit
Certificate Management
Enterprise Directory
Host AA
PAM
Security Database
Control
CTI Users
Devices
Device Groups
Tlinks

Tlinks

Tlink Name
AVAYA#CM7#CSTA#AES7
Delete Tlink

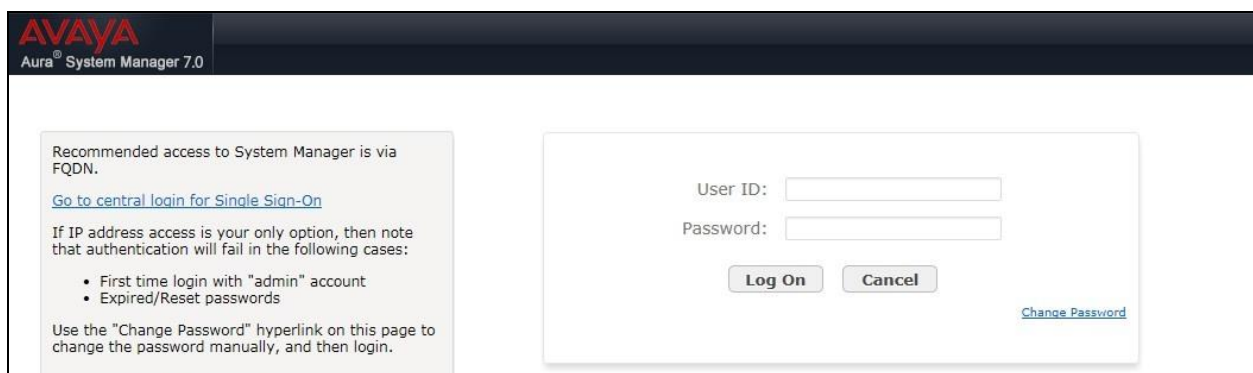
7. Configure Avaya Aura® Session Manager

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

- Launch System Manager
- Administer users

7.1. Launch System Manager

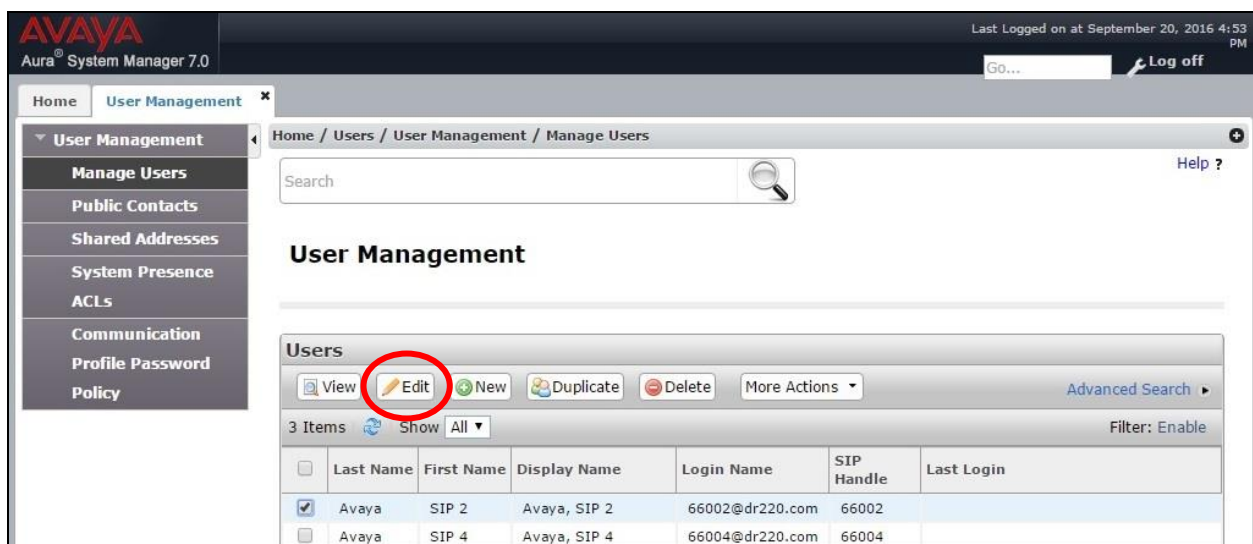
Access the System Manager web interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of System Manager. Log in using the appropriate credentials.



The screenshot shows the Avaya Aura System Manager 7.0 login page. On the left, there is a text box with instructions: "Recommended access to System Manager is via FQDN. Go to central login for Single Sign-On. If IP address access is your only option, then note that authentication will fail in the following cases: • First time login with 'admin' account • Expired/Reset passwords. Use the 'Change Password' hyperlink on this page to change the password manually, and then login." On the right, there is a login form with fields for "User ID:" and "Password:", a "Log On" button, a "Cancel" button, and a "Change Password" hyperlink.

7.2. Administer Users

In the subsequent screen (not shown), select **Users** → **User Management**. Select **User Management** → **Manage Users** from the left pane to display the **User Management** screen below. Select the entry associated with the first SIP agent station from **Section 3**, in this case “66002”, and click **Edit**.



The screenshot shows the Avaya Aura System Manager 7.0 User Management screen. The left navigation pane has "User Management" selected, with "Manage Users" highlighted. The main content area shows the "User Management" title and a search bar. Below the title, there is a "Users" section with a table of users. The "Edit" button in the "Users" section is circled in red. The table has columns: Last Name, First Name, Display Name, Login Name, SIP Handle, and Last Login. There are 3 items shown, with the first item selected.

	Last Name	First Name	Display Name	Login Name	SIP Handle	Last Login
<input checked="" type="checkbox"/>	Avaya	SIP 2	Avaya, SIP 2	66002@dr220.com	66002	
<input type="checkbox"/>	Avaya	SIP 4	Avaya, SIP 4	66004@dr220.com	66004	

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

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

AVAYA
Aura® System Manager 7.0

Last Logged on at September 20, 2016 4:53 PM
Go... Log off

Home User Management x

Home / Users / User Management / Manage Users

Help ?

User Profile Edit: 66002@dr220.com Commit & Conf

Identity * Communication Profile Membership Contacts

Communication Profile

Communication Profile Password: Edit

New Delete Done Cancel

Name

Primary

Select : None

* Name: Primary

Default : ☒

Communication Address

New Edit Delete

Type	Handle	Domain
<input type="checkbox"/> Avaya SIP	66002	dr220.com

Select : All, None

☒ **Session Manager Profile**

☒ **CM Endpoint Profile**

* System DR220-CM7-ES

* Profile Type Endpoint

Use Existing Endpoints ☐

* Extension 66002 **Endpoint Editor**

Template Select/Reset

Set Type 9621SIPCC

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

Repeat this section for all SIP agent users.

The screenshot shows the Avaya Aura System Manager 7.0 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 7.0', and a 'Log off' button. The main navigation pane on the left lists 'User Management' and its sub-items: 'Manage Users', 'Public Contacts', 'Shared Addresses', 'System Presence', 'ACLs', 'Communication', 'Profile Password', and 'Policy'. The breadcrumb trail indicates the path: 'Home / Users / User Management / Manage Users'. The 'Edit Endpoint' screen is displayed, featuring a 'Done' and 'Cancel' button at the top right. Below the breadcrumb, there is a 'Save As Template' link. The main form area contains several fields: 'System' (DR220-CM7-ES), 'Extension' (66002), 'Template' (Select), 'Set Type' (9621SIPCC), 'Port' (S00004), and 'Security Code'. The 'Name' field is set to 'Avaya, SIP 2'. Below these fields is a tabbed interface with four tabs: 'General Options (G) *', 'Feature Options (F)', 'Site Data (S)', and 'Abbreviated Call Dialing (A)'. The 'General Options (G) *' tab is active, showing various configuration options. The 'Type of 3PCC Enabled' dropdown is highlighted with a red circle. Other options include 'Class of Restriction (COR)', 'Emergency Location Ext.', 'Tenant Number', 'SIP Trunk', 'Coverage Path 1', 'Lock Message', 'Multibyte Language', 'Class Of Service (COS)', 'Message Lamp Ext.', 'Coverage Path 2', 'Localized Display Name', and 'Enable Reachability for Station Domain Control'. The 'Done' and 'Cancel' buttons are at the bottom right.

General Options (G) *		Feature Options (F)		Site Data (S)		Abbreviated Call Dialing (A)	
Enhanced Call Fwd (E)		Button Assignment (B)		Profile Settings (P)		Group Membership (M)	
* Class of Restriction (COR)	1	* Class Of Service (COS)	1				
* Emergency Location Ext	66002	* Message Lamp Ext.	66002				
* Tenant Number	1	* Type of 3PCC Enabled	Avaya				
* SIP Trunk	Qaar	Coverage Path 2					
Coverage Path 1	1	Localized Display Name	Avaya, SIP 2				
Lock Message	<input type="checkbox"/>	Enable Reachability for Station Domain Control	system				
Multibyte Language	Not Applicable						

8. Configure Enghouse Interactive Communications Center

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

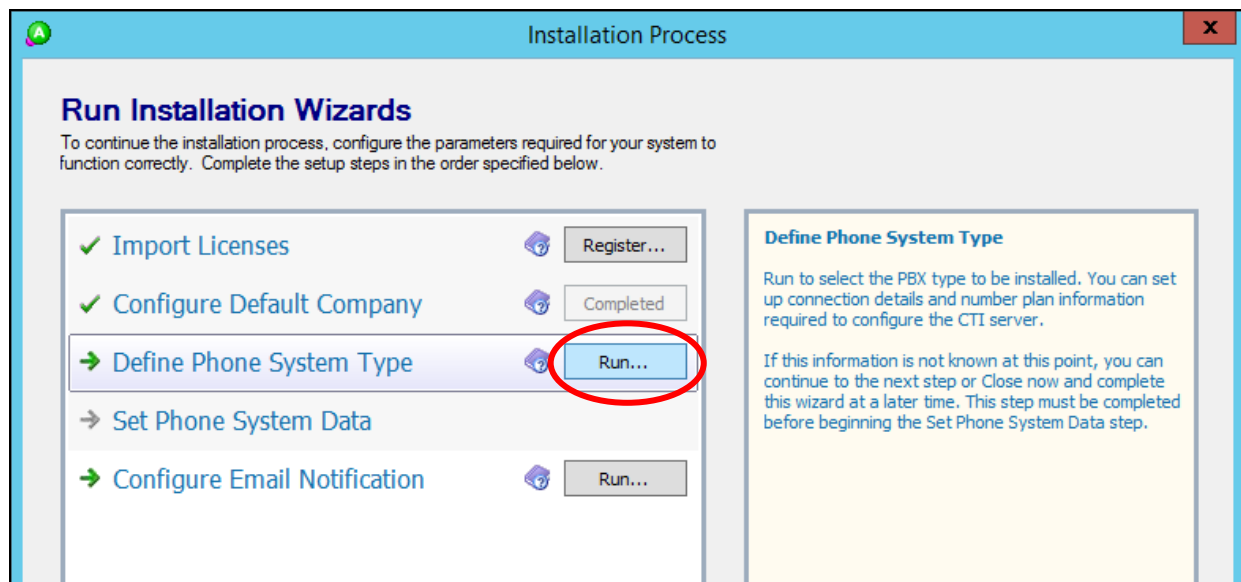
- Administer phone system type
- Administer phone system data
- Administer queues
- Administer agents and supervisors
- Administer mailboxes
- Administer lines

The configuration of EICC is typically performed by Enghouse Interactive installation technicians or third party resellers. The procedural steps are presented in these Application Notes for informational purposes.

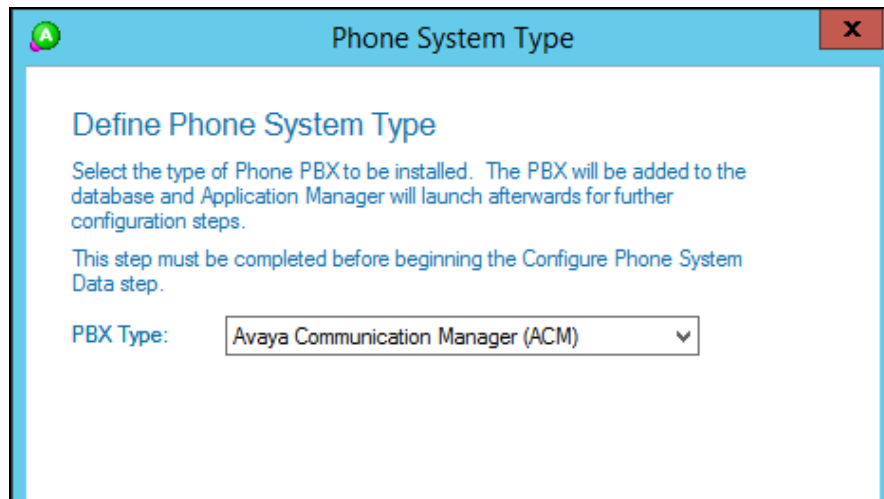
8.1. Administer Phone System Type

At the conclusion of installation, the **Installation Process** screen will be displayed by the Installation Wizard. Follow [3] to import licenses and configure the default company.

The **Installation Process** screen shown below is displayed next. Click the **Run** icon associated with **Define Phone System Type**.

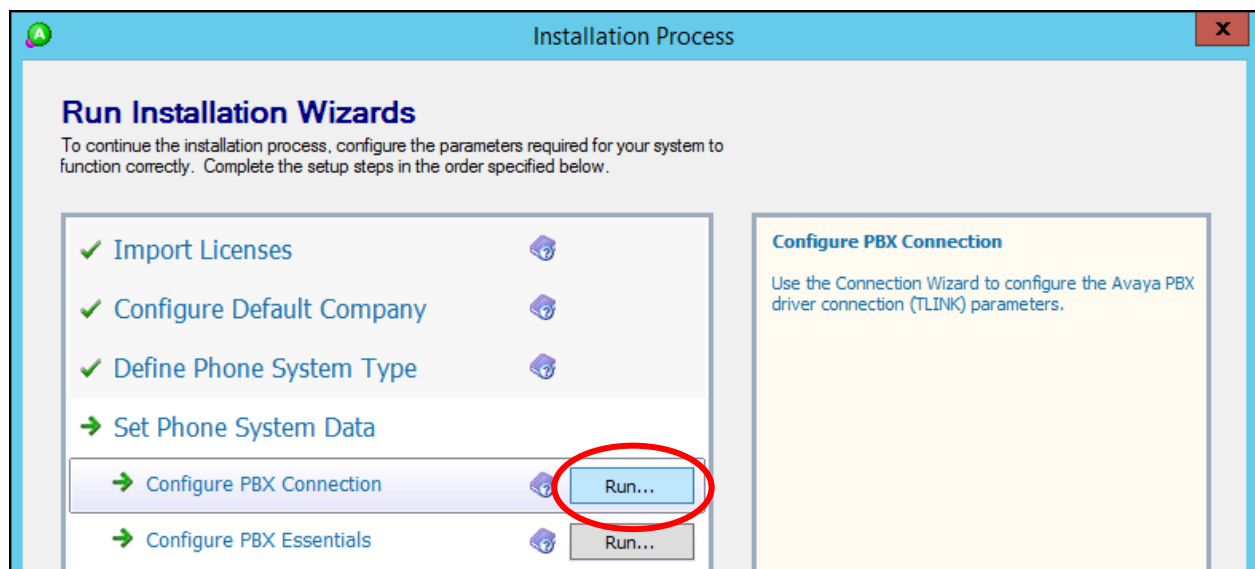


The **Phone System Type** screen is displayed. For **PBX Type**, select “Avaya Communication Manager (ACM)”.

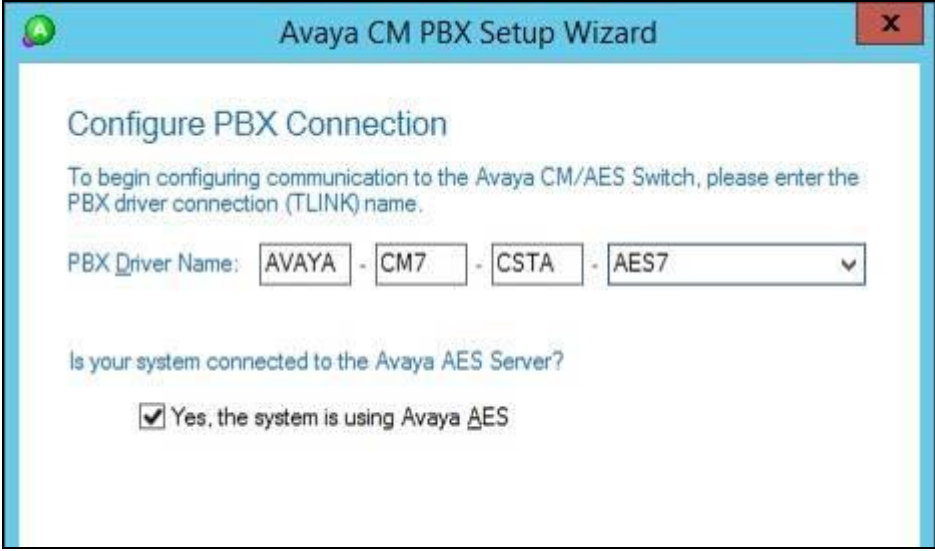


8.2. Administer Phone System Data

The **Installation Process** screen shown below is displayed next. Click the **Run** icon associated with **Set Phone System Data** → **Configure PBX Connection**.



The **Avaya CM PBX Setup Wizard → Configure PBX Connection** screen is displayed. For **PBX Driver Name**, enter the Tlink name from **Section 6.3**, as shown below. Retain the default value in the remaining field.



The screenshot shows the 'Avaya CM PBX Setup Wizard' window with the 'Configure PBX Connection' title. The instructions state: 'To begin configuring communication to the Avaya CM/AES Switch, please enter the PBX driver connection (TLINK) name.' The 'PBX Driver Name' field is a multi-part dropdown menu showing 'AVAYA - CM7 - CSTA - AES7'. Below this, the question 'Is your system connected to the Avaya AES Server?' is followed by a checked checkbox and the text 'Yes, the system is using Avaya AES'.

The **Avaya CM PBX Setup Wizard → Configure Avaya CTI User** screen is displayed next. Enter the EICC user credentials from **Section 6.5**.



The screenshot shows the 'Avaya CM PBX Setup Wizard' window with the 'Configure Avaya CTI User' title. The instructions state: 'Please enter the User Name and Password of the CTI User used to access the Avaya CM/AES driver.' The 'User Name' field contains 'eicc' and the 'Password' field contains a series of asterisks.

The **Avaya CM PBX Setup Wizard → Configure ACM Soft Ports** screen is displayed. Enter the following values for the specified fields.

- **ACM Switch Connection Name:** The relevant switch connection name from **Section 6.3**.
- **ACM IP Address:** IP address of H.323 gatekeeper from **Section 6.4**.
- **AES IP Address:** IP address of Application Enablement Services server.
- **DMCC TCP Port:** “4721”
- **DMCC User:** The EICC user credentials from **Section 6.5**.
- **DMCC Password:** The EICC user credentials from **Section 6.5**.
- **Global SoftPort Password:** The security code value from **Section 5.6**.

Avaya CM PBX Setup Wizard

Configure ACM Soft Ports

Please enter the configuration details for the ACM Soft Ports.

ACM Switch Connection Name: (case sensitive)

ACM IP Address:

AES IP Address:

DMCC TCP Port:

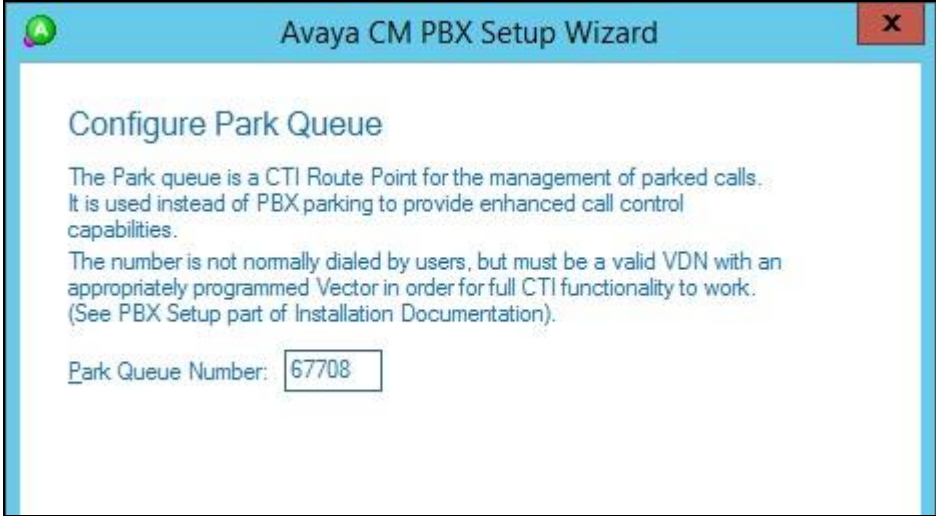
DMCC User:

DMCC Password:

Global SoftPort Password:

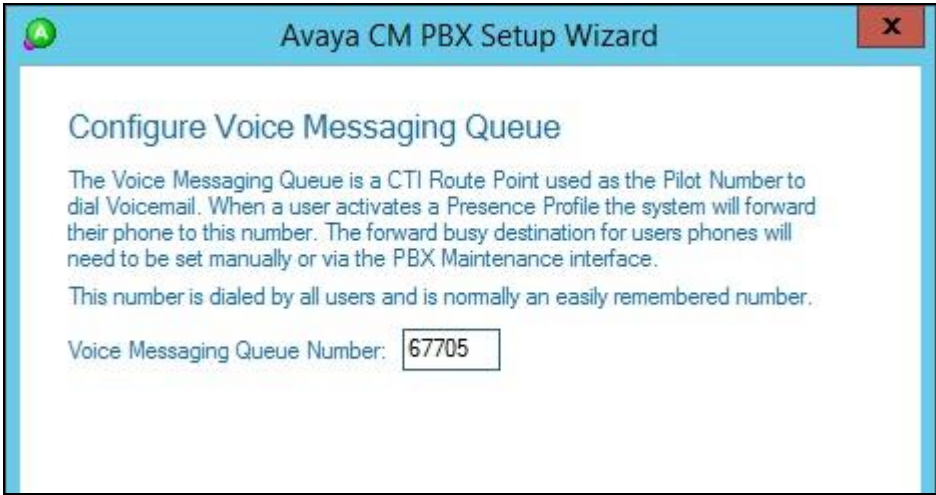
< Back Next > Cancel Help

Continue with the Installation Wizard until the **Avaya CM PBX Setup Wizard → Configure Park Queue** screen is displayed. For **Park Queue Number**, enter the extension of the hold VDN from **Section 5.3.7**.



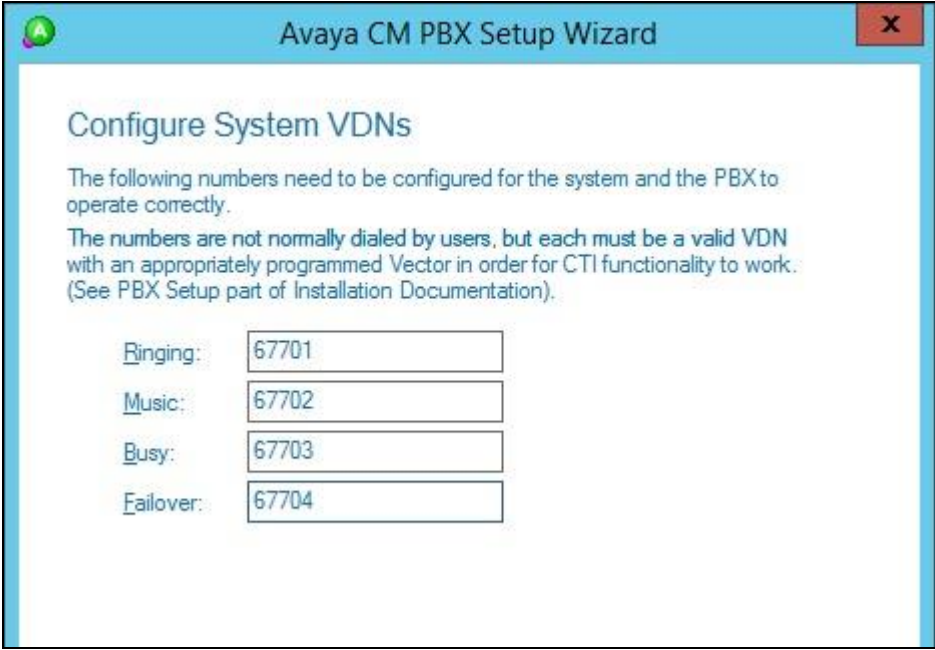
The screenshot shows a window titled "Avaya CM PBX Setup Wizard" with a close button (X) in the top right corner. The main content area is titled "Configure Park Queue". Below the title, there is explanatory text: "The Park queue is a CTI Route Point for the management of parked calls. It is used instead of PBX parking to provide enhanced call control capabilities." and "The number is not normally dialed by users, but must be a valid VDN with an appropriately programmed Vector in order for full CTI functionality to work. (See PBX Setup part of Installation Documentation)". At the bottom, there is a label "Park Queue Number:" followed by a text input field containing the value "67708".

The **Avaya CM PBX Setup Wizard → Configure Voice Messaging Queue** screen is displayed next. For **Voice Messaging Queue Number**, enter the extension of the voicemail VDN from **Section 5.3.6**.



The screenshot shows a window titled "Avaya CM PBX Setup Wizard" with a close button (X) in the top right corner. The main content area is titled "Configure Voice Messaging Queue". Below the title, there is explanatory text: "The Voice Messaging Queue is a CTI Route Point used as the Pilot Number to dial Voicemail. When a user activates a Presence Profile the system will forward their phone to this number. The forward busy destination for users phones will need to be set manually or via the PBX Maintenance interface." and "This number is dialed by all users and is normally an easily remembered number.". At the bottom, there is a label "Voice Messaging Queue Number:" followed by a text input field containing the value "67705".

The **Avaya CM PBX Setup Wizard → Configure System VDNs** screen is displayed next. Enter the ring, music, busy, and failure VDNs from **Section 5.3** respectively, as shown below.

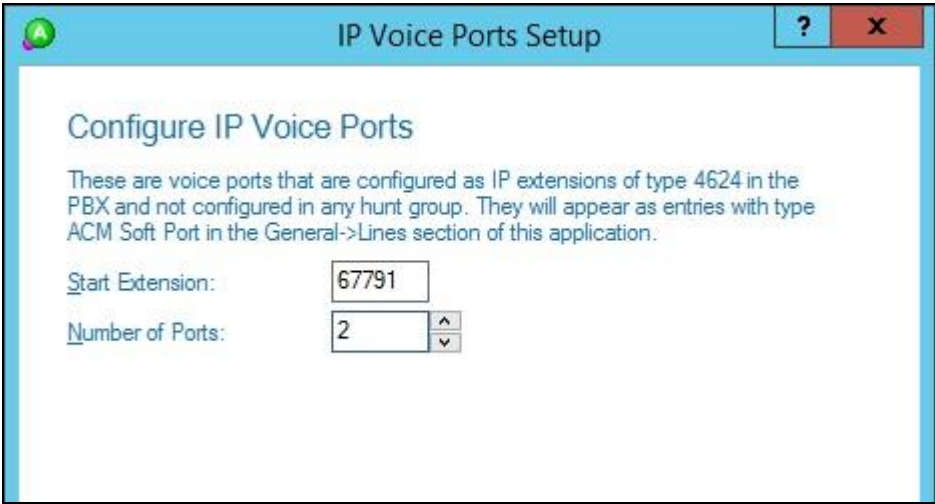


The screenshot shows a window titled "Avaya CM PBX Setup Wizard" with a close button (X) in the top right corner. The main heading is "Configure System VDNs". Below the heading, there is explanatory text: "The following numbers need to be configured for the system and the PBX to operate correctly. The numbers are not normally dialed by users, but each must be a valid VDN with an appropriately programmed Vector in order for CTI functionality to work. (See PBX Setup part of Installation Documentation)." Below this text are four input fields, each with a label and a value: "Ringing:" with "67701", "Music:" with "67702", "Busy:" with "67703", and "Failover:" with "67704".

Ringing:	67701
Music:	67702
Busy:	67703
Failover:	67704

Continue with the Installation Wizard until the **IP Voice Ports Setup → Configure IP Voice Ports** screen is displayed. For **Start Extension**, enter the first virtual IP softphone extension from **Section 5.6**. For **Number of Ports**, enter the total number of virtual IP softphones from **Section 5.6**.

Follow [3] to complete the Installation Wizard and subsequent CTI server setup via Application Manager.

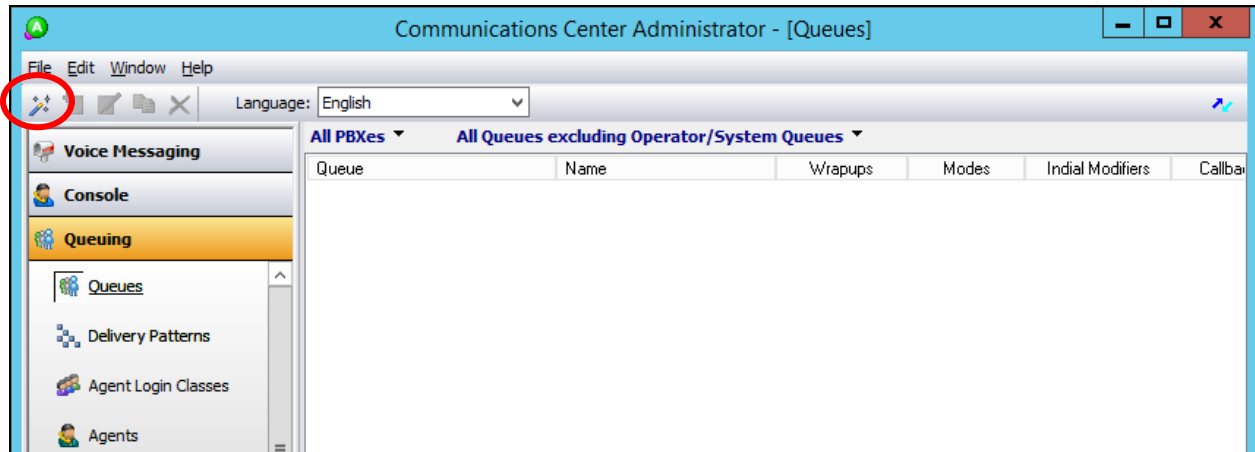


The screenshot shows a window titled "IP Voice Ports Setup" with a help button (?) and a close button (X) in the top right corner. The main heading is "Configure IP Voice Ports". Below the heading, there is explanatory text: "These are voice ports that are configured as IP extensions of type 4624 in the PBX and not configured in any hunt group. They will appear as entries with type ACM Soft Port in the General->Lines section of this application." Below this text are two input fields: "Start Extension:" with "67791" and "Number of Ports:" with "2" and up/down arrow buttons.

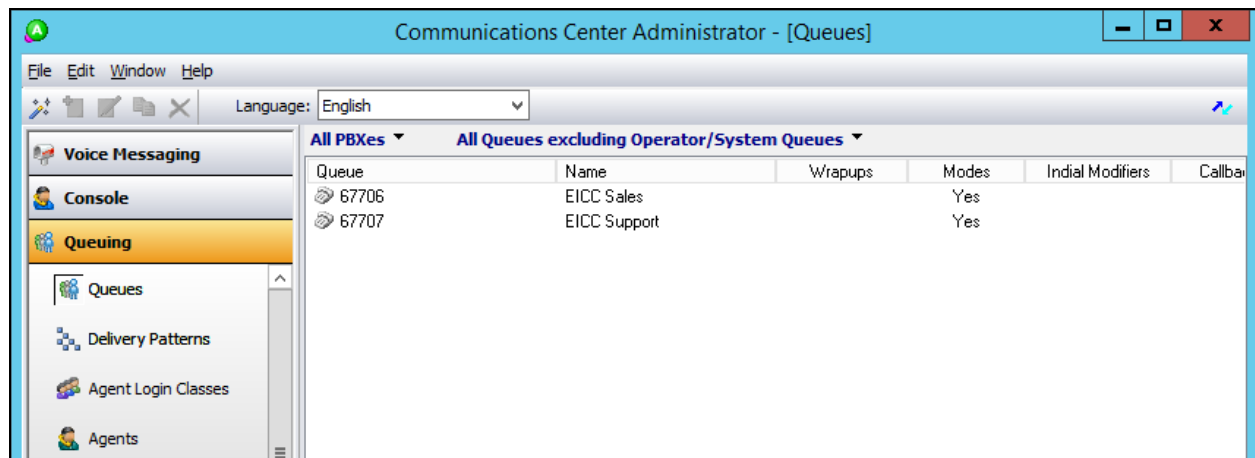
Start Extension:	67791
Number of Ports:	2

8.3. Administer Queues

The **Administrator** screen is displayed upon completion of the Installation Wizard and CTI server setup. Select **Queuing** → **Queues** from the left pane, followed by the **Add Wizard** icon located at the upper left of the screen.

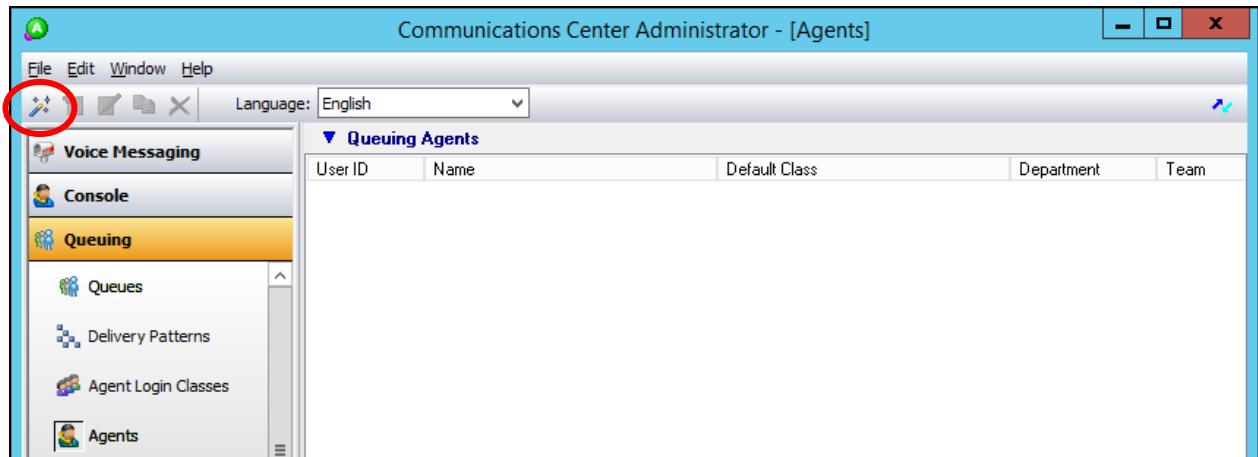


Follow the **Adding a New Queue Wizard** in the subsequent screens (not shown) to configure a new queue for each general routing VDN in **Section 5.3.2**. In the compliance testing, two queues were created as shown below.



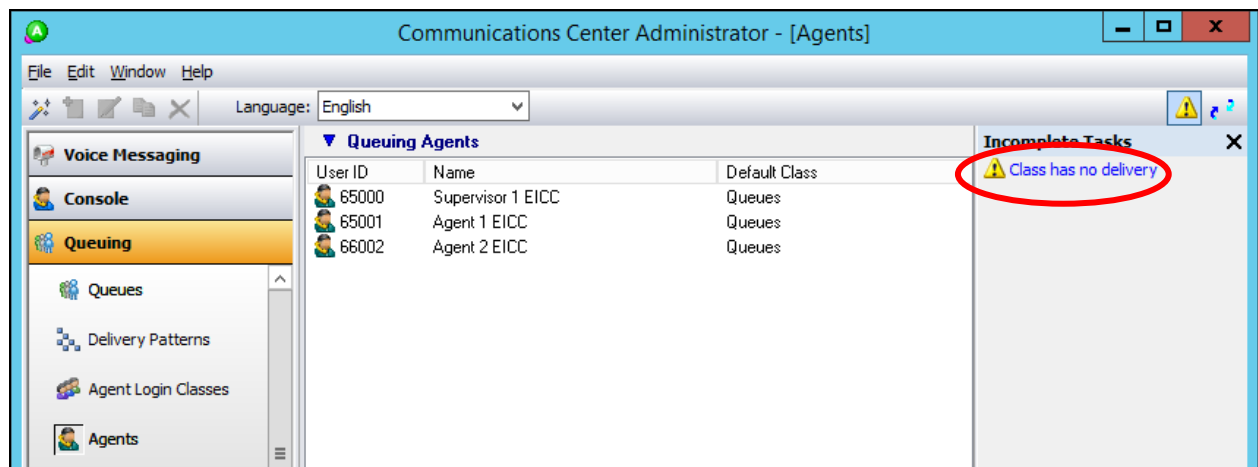
8.4. Administer Agents and Supervisors

Select **Queuing** → **Agents** from the left pane, followed by the **Add Wizard** icon located at the upper left corner of the screen.

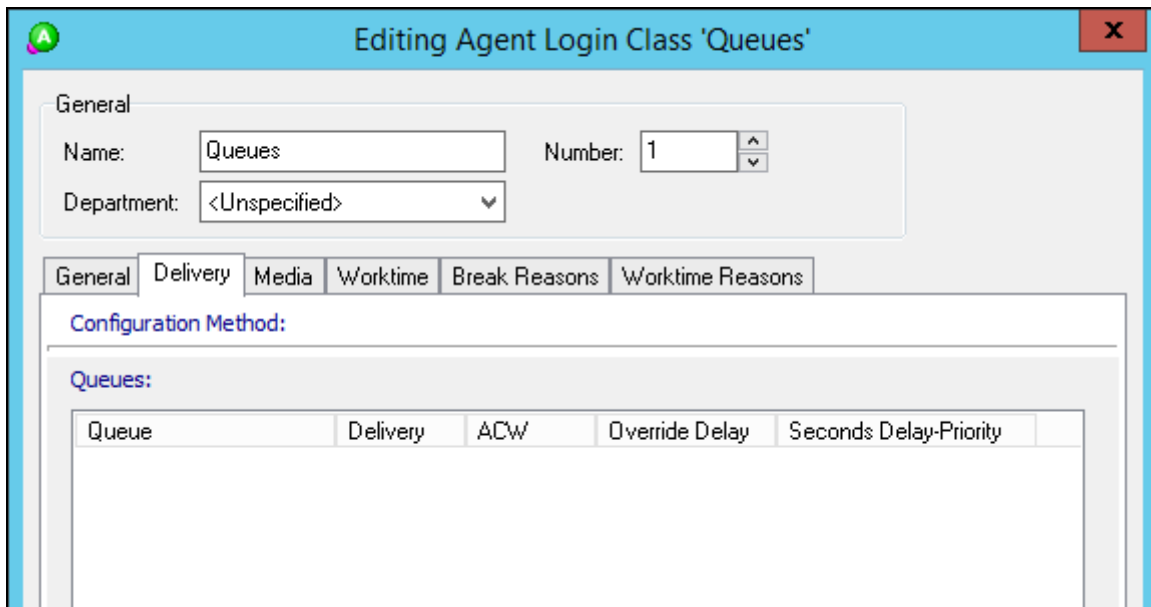


Follow the **Add Agent Wizard** in the subsequent screens (not shown) to configure a corresponding entry for each agent and supervisor in **Section 3**. In the compliance testing, two agents and one supervisor were created as shown below.

Double click on **Class has no delivery**.

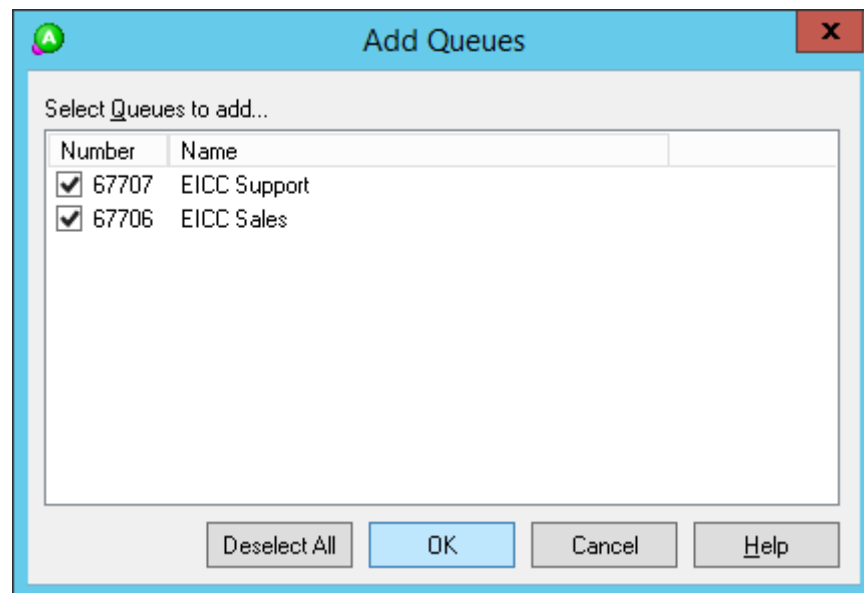


The **Editing Agent Login Class** screen is displayed. Select the **Delivery** tab, and click **Add** (not shown).



The dialog box is titled "Editing Agent Login Class 'Queues'". It has a "General" tab selected. The "General" section contains fields for "Name" (Queues), "Number" (1), and "Department" (<Unspecified>). Below this is a "Configuration Method:" section with a "Queues:" sub-section. The "Queues:" sub-section contains a table with columns: Queue, Delivery, ACW, Override Delay, and Seconds Delay-Priority. The table is currently empty.

The **Add Queues** screen is displayed next. Check the entries corresponding to the general routing VDNs from **Section 5.3.2**, to enable calls to these VDNs to be delivered.

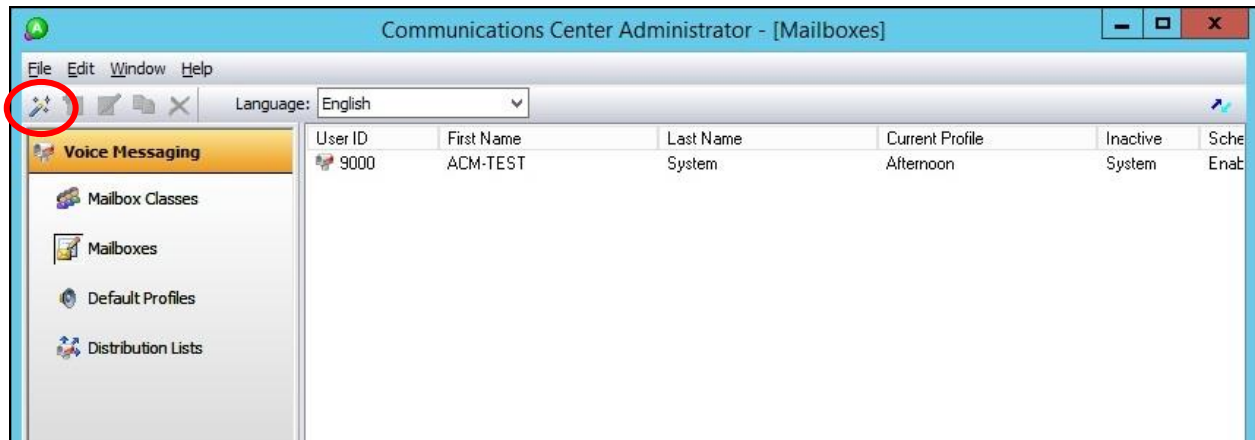


The dialog box is titled "Add Queues". It contains a section "Select Queues to add..." with a table listing available queues. The table has columns "Number" and "Name". Two entries are listed: "67707 EICC Support" and "67706 EICC Sales", both of which are checked. At the bottom of the dialog are buttons for "Deselect All", "OK", "Cancel", and "Help".

Number	Name
<input checked="" type="checkbox"/> 67707	EICC Support
<input checked="" type="checkbox"/> 67706	EICC Sales

8.5. Administer Mailboxes

Select **Voice Messaging** → **Mailboxes** from the left pane, followed by the **Add Wizard** icon located at the upper left corner of the screen.



Follow the **Add Mailboxes Wizard** in the subsequent screens (not shown) to configure a corresponding mailbox for each agent and supervisor from **Section 8.4**. The screen below shows the mailboxes that were created.

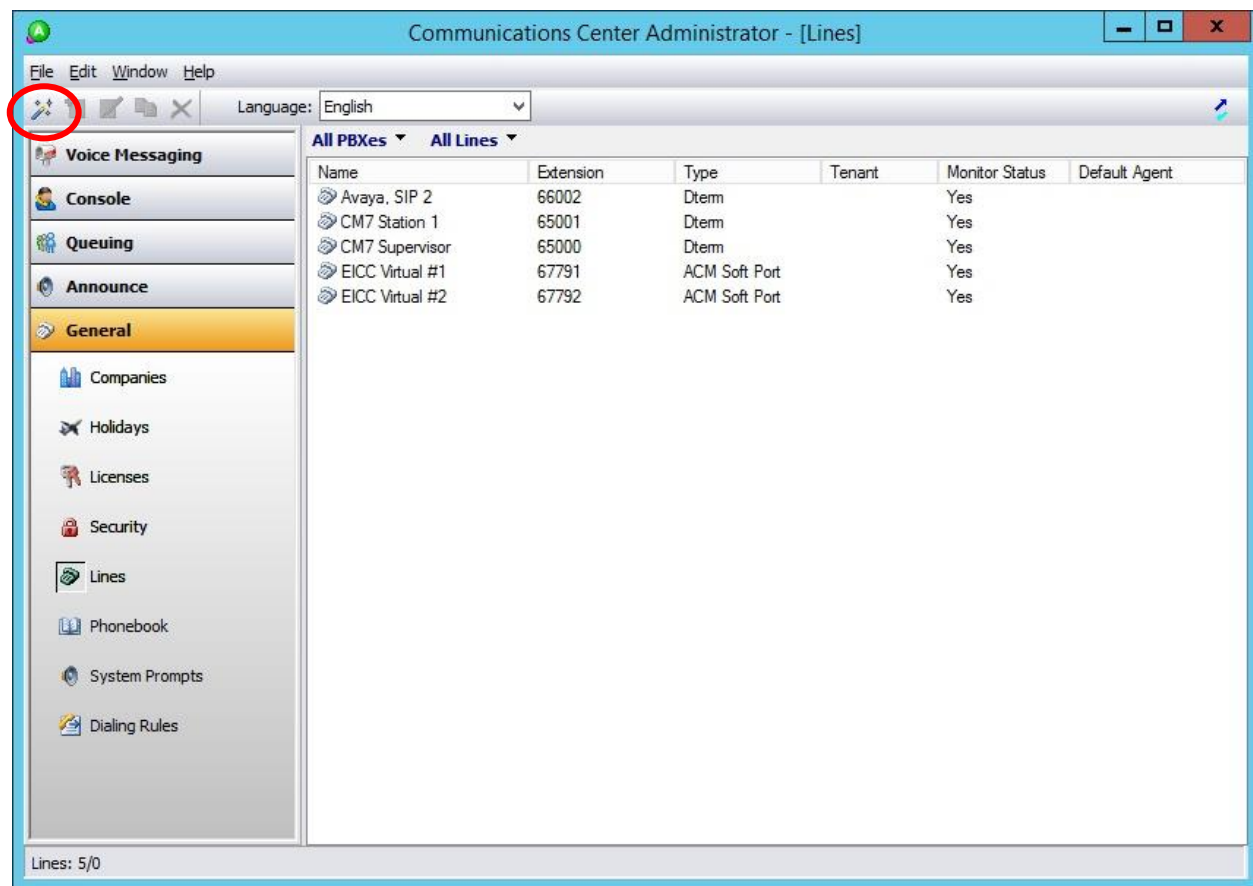


8.6. Administer Lines

Select **General** → **Lines** from the left pane, followed by the **Add Wizard** icon located at the upper left corner of the screen. Follow the **Adding Line Wizard** in the subsequent screens (not shown) to configure a corresponding line for each agent and supervisor from **Section 8.4**.

Note that the lines for virtual IP softphones were created automatically, and that lines for agents and supervisors can either be created manually using the wizard, or by having each agent and supervisor dial a monitored VDN for EICC to “learn” the extension and create the line automatically.

In the compliance testing, all lines were created automatically with agents and supervisor dialing the voicemail VDN for EICC to “learn” the extensions.



9. Verification Steps

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

9.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify 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	aes7	established	33	31

Verify the registration status of virtual IP softphones by using the “list registered-ip-stations” command. Verify that all virtual IP softphone from **Section 5.6** are displayed along with the IP address of the Application Enablement Services server, as shown below.


```
list registered-ip-stations
```

REGISTERED IP STATIONS					
Station Ext or Orig Port	Set Type/ Net Rgn	Prod ID/ Release	Station IP Address/ Skt Gatekeeper IP Address		
65000	9641	IP_Phone	tls 192.168.200.186		
	1	6.6302	10.64.101.236		
65001	9611	IP_Phone	tls 192.168.200.137		
	1	6.6302	10.64.101.236		
67791	4624	IP_API_A	tcp 10.64.101.239		
	1	3.2040	10.64.101.236		
67792	4624	IP_API_A	tcp 10.64.101.239		
	1	3.2040	10.64.101.236		

9.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify the status of the TSAPI link by selecting **Status** → **Status and Control** → **TSAPI Service Summary** from the left pane. The **TSAPI Link Details** screen is displayed.

Verify the **Status** is “Talking” for the TSAPI link administered in **Section 6.3**, and that the **Associations** column reflects the total number of agents and supervisor from **Section 3** plus the number of virtual IP softphones from **Section 5.6**.

**Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Sep 20 17:08:26 2016 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: 7.0.1.0.2.15-0
Server Date and Time: Tue Sep 20 17:43:18 EDT 2016
HA Status: Not Configured

Status | Status and Control | TSAPI 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

TSAPI Link Details


☐ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input checked="" type="radio"/>	1	cm7	1	Talking	Tue Sep 20 13:52:01 2016	Online	17	5	31	33	30

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

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

Verify the **User** column shows action sessions with the EICC user name from **Section 6.5**, and that the total number of sessions reflects the number of virtual IP softphones from **Section 5.6**.



Application Enablement Services

Management Console

Welcome: User
 Last login: Tue Sep 20 17:08:26 2016 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: 7.0.1.0.2.15-0
 Server Date and Time: Tue Sep 20 17:43:29 EDT 2016
 HA Status: Not Configured

Status | Status and Control | DMCC Service Summary
Home | 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

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)
 Generated on Tue Sep 20 17:43:29 EDT 2016

Service Uptime: 0 days, 3 hours 50 minutes

Number of Active Sessions: 2

Number of Sessions Created Since Service Boot: 2

Number of Existing Devices: 2

Number of Devices Created Since Service Boot: 2

■	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	734B83593027C4A79 51E5F5A087C4104-0	eicc		10.64.101.206	XML Unencrypted	1
<input type="checkbox"/>	F88572255A6415B52 8BDFCFCE3EDA791-1	eicc		10.64.101.206	XML Unencrypted	1

Terminate Sessions
Show Terminated Sessions

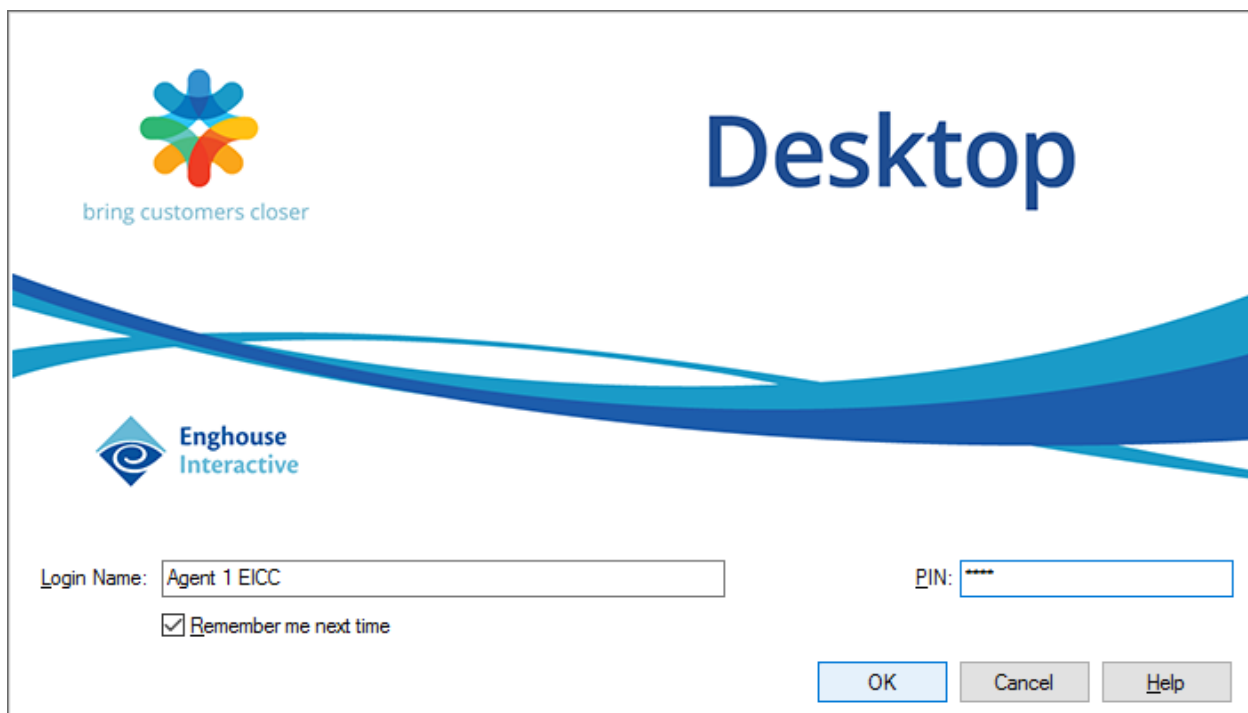
Item 1-2 of 2
1 Go

9.3. Verify Enghouse Interactive Communications Center

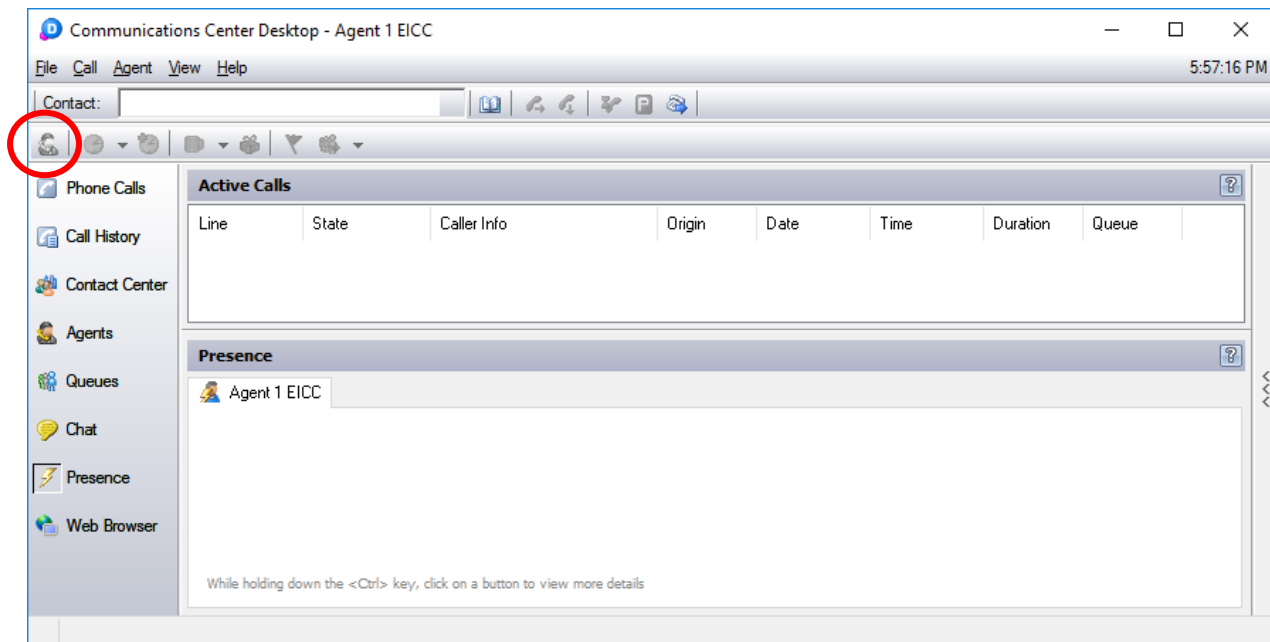
From the agent desktop, double-click on the **Desktop** shortcut icon shown below, which was created as part of Enghouse Interactive Desktop installation.



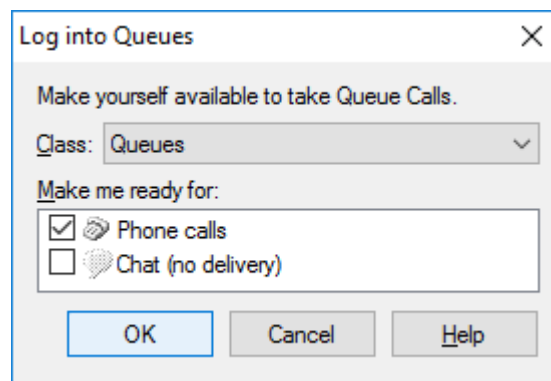
The **Desktop** login screen is displayed. Enter the login name associated with an agent from **Section 8.4**, and use the generic default PIN value from EICC. Retain the default value in the remaining field.

The login screen features the Enghouse Interactive logo (a colorful flower-like shape) and the tagline 'bring customers closer' on the left. The word 'Desktop' is displayed in large blue font on the right. Below the logo is the Enghouse Interactive logo and name. The login fields are: 'Login Name:' with a text box containing 'Agent 1 EICC', and 'PIN:' with a text box containing '****'. There is a checkbox labeled 'Remember me next time' which is checked. At the bottom right are three buttons: 'OK', 'Cancel', and 'Help'.

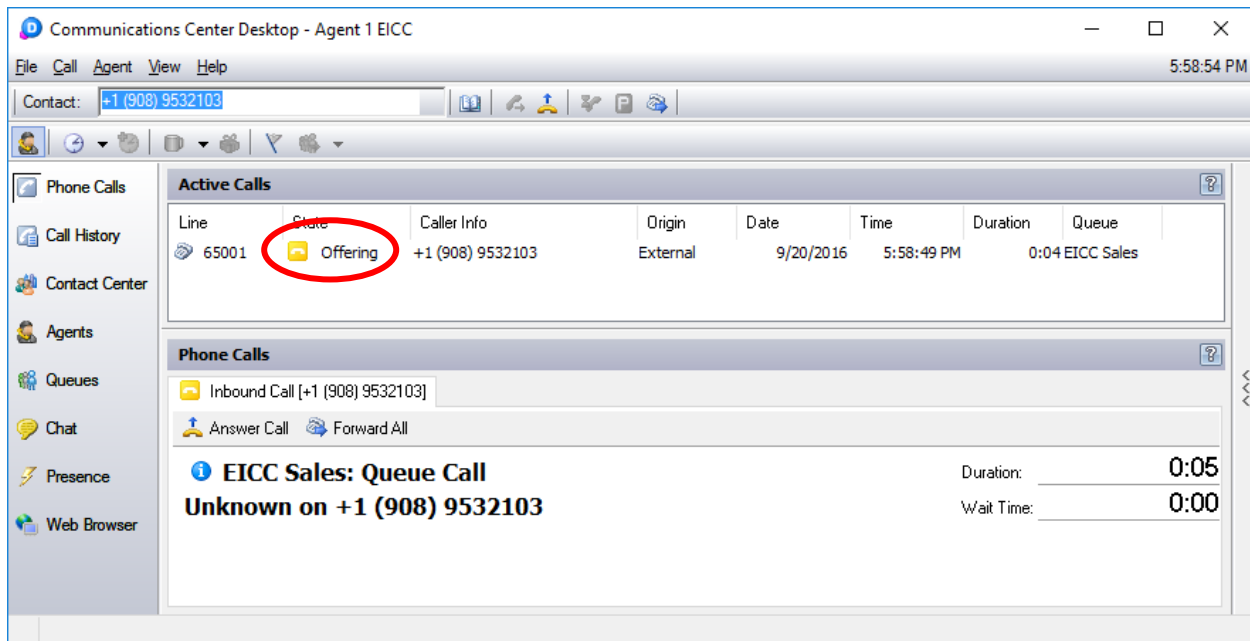
The **Communications Center Desktop** screen is displayed. Click on the **Log into Queues** icon shown below.



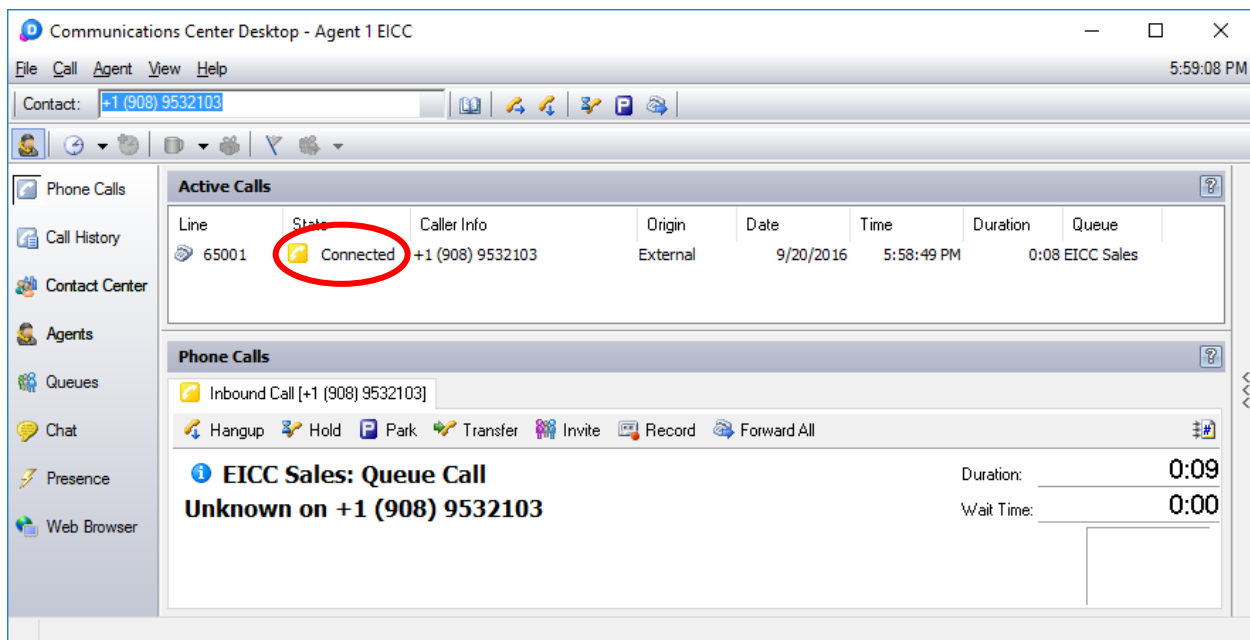
The **Log into Queues** dialog box is displayed next. Retain all default values.



Make an incoming call from PSTN to the EICC Sales group, with available agent “65001”. Verify that the agent desktop is populated with a voice call entry, and that the **State** is “Offering”, as shown below. Click **Answer Call**.



Verify that the agent is connected to the PSTN caller with two-way talk paths, and that the **State** is updated to “Connected”, as shown below.



10. Conclusion

These Application Notes describe the configuration steps required for Enghouse Interactive Communications Center 2016R2 to successfully interoperate with Avaya Aura® Communication Manager 7.0 using Avaya Aura® Application Enablement Services 7.0. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

11. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Release 7.0.1, Issue 2.1, August 2016, available at <http://support.avaya.com>.
2. *Administering and Maintaining Aura® Application Enablement Services*, Release 7.0.1, Issue 2, August 2016, available at <http://support.avaya.com>.
3. *CC 2016 R2 First-time Installation and Server Setup – Avaya Communication Manager*, 4 May 2016, available via Communication Manager training course provided by Enghouse Interactive.

©2016 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.