



**Application Notes for Enghouse Interactive
Communications Center 10.0 with Avaya Aura®
Communication Manager 7.1 using Avaya Aura®
Application Enablement Services 7.1 – Issue 1.0**

Abstract

These Application Notes describe the configuration steps required for Enghouse Interactive Communications Center 10.0 to interoperate with Avaya Aura® Communication Manager 7.1 using Avaya Aura® Application Enablement Services 7.1. 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) 10.0 to interoperate with Avaya Aura® Communication Manager 7.1 using Avaya Aura® Application Enablement Services 7.1. 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.

In the compliance testing, agents and supervisors were configured as station users on Communication Manager, and have desktop computers running the Enghouse Interactive TouchPoint client application. The ACD functionality such as log in/out, work modes, queuing, and announcements were provided by EICC.

The TSAPI interface was used by EICC to monitor agent and supervisor station extensions, provide screen pops and call control from agent desktops, route incoming calls using adjunct routing capability, and support enable/disable of call forwarding and message waiting lamp using set value capability. In addition, TSAPI single step conference was used to support the supervisor monitor feature, which can be activated from the supervisor desktop running the TouchPoint application.

The DMCC interface was used by EICC to support voicemail, announcement, and basic call recording features via virtual IP softphones. The virtual IP softphones were registered by EICC with Communication Manager. Voicemail and announcement calls were redirected to available virtual IP softphones to terminate to EICC, and recording was accomplished by intruding a virtual IP softphone via TSAPI single step conference onto the active call to pick up 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 the TouchPoint client application 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 and clients.

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.

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

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

For the testing associated with these Application Notes, the interface between Application Enablement Services and EICC did not include use of any specific encryption features as requested by Enghouse Interactive.

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 lamp.
- Use of TSAPI call control service to support manual call control actions initiated from TouchPoint, call control for virtual IP softphones, and adding virtual IP softphones 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, message waiting lamp, 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 configuration used for the compliance testing is shown in **Figure 1**. 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 devices used in the compliance testing are shown in the table below. In the compliance testing, the agent and supervisor station extensions were monitored by EICC.

Device Type	Device Number/Extension
Agent stations	65001, 65002
Supervisor & failure covering station	65000

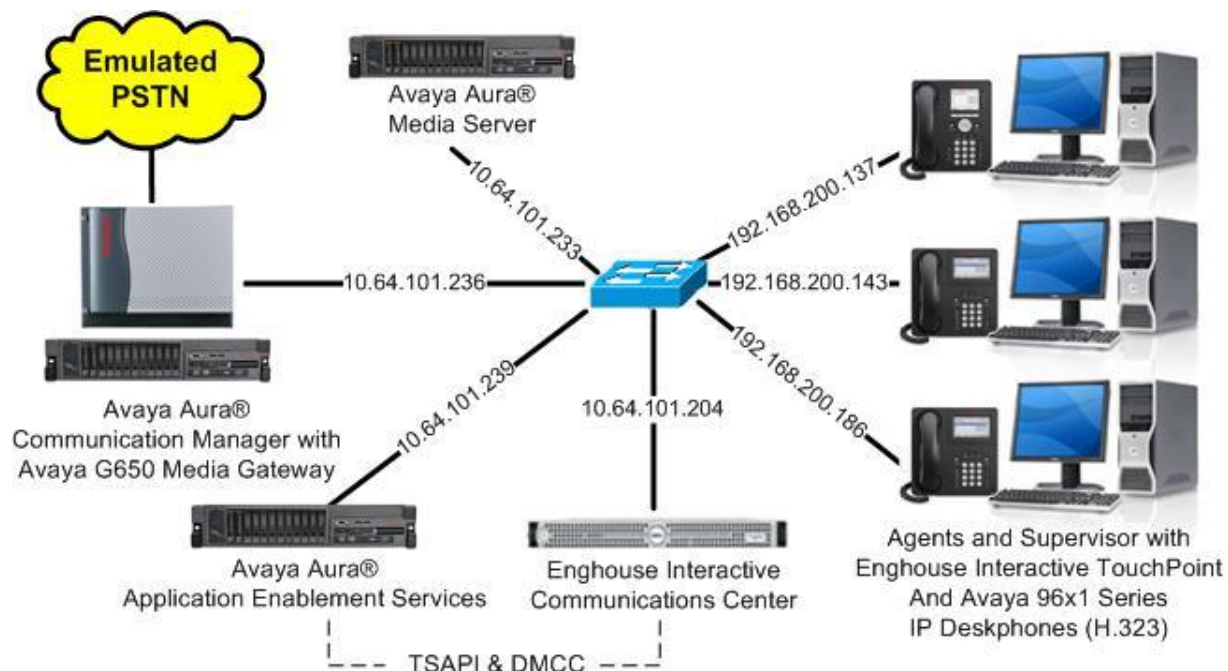


Figure 1: Compliance Testing Configuration

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	7.1.1 (7.1.1.0.0.532.23985)
Avaya G650 Media Gateway	NA
Avaya Aura® Media Server in Virtual Environment	7.8.0.333
Avaya Aura® Application Enablement Services in Virtual Environment	7.1.1 (7.1.1.0.0.5-0)
Avaya 9608G & 9641G IP Deskphone (H.323)	6.6506
Enghouse Interactive Communications Center on Windows Server 2012 R2 <ul style="list-style-type: none">• Avaya TSAPI Windows Client (csta32.dll)• Avaya DMCC XML	10.0.0.14152 Standard 7.1.1.36 4.2
Enghouse Interactive TouchPoint on Windows 10 Pro	10.0.0.14152

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 12
OPTIONAL FEATURES		
Abbreviated Dialing Enhanced List? y	Audible Message Waiting? y	
Access Security Gateway (ASG)? n	Authorization Codes? y	
Analog Trunk Incoming Call ID? y	CAS Branch? n	
A/D Grp/Sys List Dialing Start at 01? y	CAS Main? n	
Answer Supervision by Call Classifier? y	Change COR by FAC? n	
ARS? y	Computer Telephony Adjunct Links? y	
ARS/AAR Partitioning? y	Cvg Of Calls Redirected Off-net? y	
ARS/AAR Dialing without FAC? 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 12
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	
Name: AES CTI Link	COR: 1

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	CALL VECTOR	Page 1 of 6
Number: 700		
Name: EICC User Q		
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	2 secs hearing silence	Holidays? y
03 route-to	number 67704	
04 stop	with cov y if unconditionally	
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	VECTOR DIRECTORY NUMBER	Page 1 of 2
Extension: 67706		
Name: EICC Sales		
Destination: Vector Number	700	

add vdn 67707	VECTOR DIRECTORY NUMBER	Page 1 of 2
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
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 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	CALL VECTOR	Page 1 of 6
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	VECTOR DIRECTORY NUMBER	Page 1 of 2
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
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 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				Page 1 of 6			
CALL VECTOR							
Number: 705				Name: SC Voicemail			
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	120 secs hearing ringback						
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		Page 1 of 2	
VECTOR DIRECTORY NUMBER			
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	CALL VECTOR	Page 1 of 6
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 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 Hold”
- Destination: “Vector Number”
- Vector Number: The “SC Hold” vector number from above.

add vdn 67708	VECTOR DIRECTORY NUMBER	Page 1 of 2
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/ TN Jack
65000	S00002	CM Supervisor			7	1	
	9641		no			1	1
65001	S00102	CM Station 1			7	1	1
	9611		no			1	1
65002	S00118	CM Station 2			7	1	
	9641		no			1	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: IP                           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/ Hunt-to	Port/ Type	Name/ Surv GK NN	Move	Room/ Data Ext	Cv1/ Cv2	COR/ COS	Cable/ TN Jack
67791	S00027 4624	EICC Virtual #1	no		1	1	
67792	S00030 4624	EICC Virtual #2	no		1	1	

6. Configure Avaya Aura® Application Enablement Services

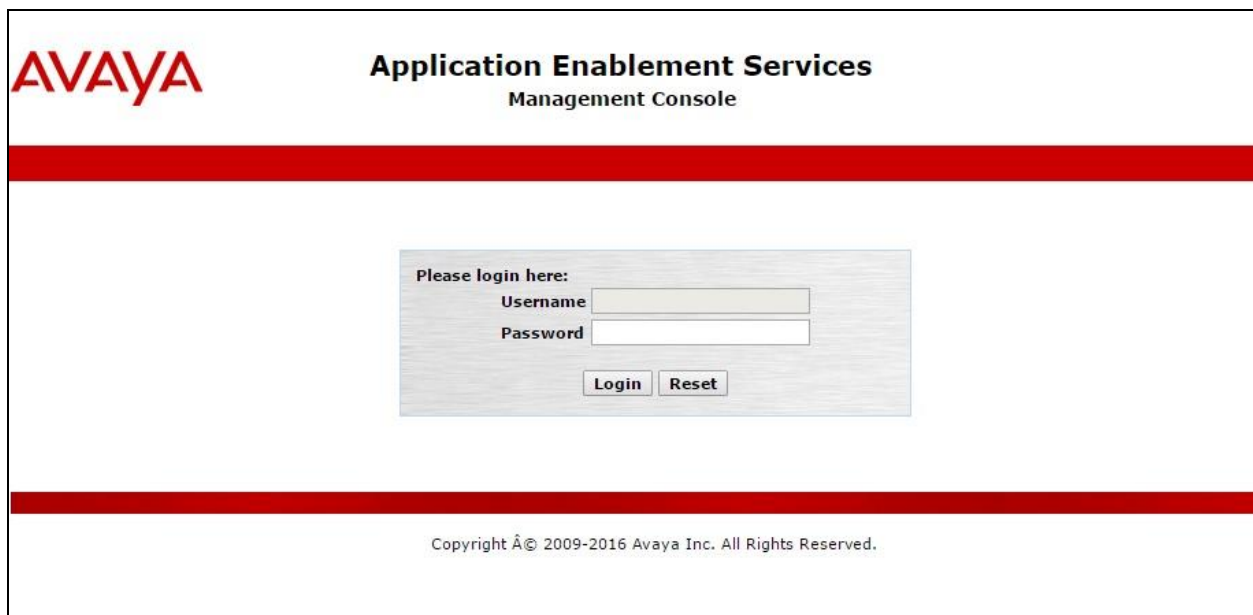
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- 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 shows the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title "Application Enablement Services Management Console". On the right, a welcome message for the user is displayed, including login details and system information. The left sidebar contains a navigation menu with options like AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area displays the "Welcome to OAM" message, explaining the purpose of the console and listing the administrative domains it manages: 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 managed by a single administrator or separate administrators.

Welcome: User
Last login: Tue Dec 5 10:38:11 2017 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: 7.1.1.0.0.5-0
Server Date and Time: Tue Dec 05 10:40:42 EST 2017
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 shows the Avaya Application Enablement Services Management Console with the "Licensing" section selected in the left sidebar. The main content area displays the "Licensing" page, which provides instructions on how to set up and maintain the WebLM, including the need to use the WebLM Server Address and the WebLM Server Access. It also mentions that if you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the Reserved Licenses option.

Welcome: User
Last login: Tue Dec 5 10:38:11 2017 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: 7.1.1.0.0.5-0
Server Date and Time: Tue Dec 05 10:40:42 EST 2017
HA Status: Not Configured

Licensing | 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

Select **Licensed products** → **APPL_ENAB** → **Application Enablement** in the left pane, to display the **Application Enablement (CTI)** screen in the right pane.

Verify that there are sufficient licenses for **TSAPI Simultaneous Users** and **Device Media and Call Control**, as shown below. 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**, which is needed for adjunct routing.

AVAYA
Aura® System Manager 7.1

Home Licenses

WebLM Home
Install license
Licensed products
APPL_ENAB
▼ Application_Enablement
View license capacity
View peak usage
CIE
► CIE
CMM
► Communication_Manager_Messaging
Configure Centralized Licensing
COMMUNICATION_MANAGER
► Call_Center
► Communication_Manager
Configure Centralized Licensing
MESSAGING
► Messaging
MSR
► Media_Server
SYSTEM_MANAGER

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

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

License installed on: September 13, 2017 1:10:08 PM +00:00

License File Host IDs: V7-2E-92-63-88-4C-01

Licensed Features

10 Items Show All ▼

Feature (License Keyword)	Expiration date	Licensed capacity
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	1000
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	1000
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	3
DLG VALUE_AES_DLG	permanent	16
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	1000
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	3

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 header includes the AVAYA logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The left navigation pane shows "AE Services" expanded, with "TSAPI" selected, and "TSAPI Links" highlighted. The main content area displays the "TSAPI Links" screen, which includes 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, specifically the "Add TSAPI Links" screen. The left navigation pane shows "AE Services" expanded, with "TSAPI" selected, and "TSAPI Links" highlighted. The main content area displays the "Add TSAPI Links" form, which includes fields for Link, Switch Connection, Switch CTI Link Number, ASAI Link Version, and Security. The values entered are: Link: 1, Switch Connection: cm7, Switch CTI Link Number: 1, ASAI Link Version: 7, and Security: Unencrypted. Below the form 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 the 'Switch Connections' table with one entry, 'cm7', which is selected. Below the table are buttons for 'Edit Connection', 'Edit PE/CLAN IPs', 'Edit H.323 Gatekeeper', 'Delete Connection', and 'Survivability Hierarchy'.

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> cm7	Yes	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. It features a text input field containing '10.64.101.236' and an 'Add Name or IP' button. Below the input field is a 'Name or IP Address' label and two buttons: 'Delete IP' and 'Back'.

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 Dec 5 10:38:11 2017 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: 7.1.1.0.0.5-0
Server Date and Time: Tue Dec 05 10:40:42 EST 2017
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 main navigation pane on the left lists various services, with "Security" expanded to show "Security Database" and "Control" selected. The right pane shows the "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" configuration page, which contains two unchecked checkboxes and an "Apply Changes" button.

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Tue Dec 5 10:38:11 2017 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: 7.1.1.0.0.5-0
Server Date and Time: Tue Dec 05 10:40:42 EST 2017
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](#)

6.8. 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 of which 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 retransmission count reduces wait time for TCP acknowledgments, and a warning states that the setting applies to all TCP and TLS sockets and should be used with caution.

Welcome: User
Last login: Tue Dec 5 10:38:11 2017 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: 7.1.1.0.0.5-0
Server Date and Time: Tue Dec 05 10:41:50 EST 2017
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 Dec 5 10:38:11 2017 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: 7.1.1.0.0.5-0
Server Date and Time: Tue Dec 05 10:40:42 EST 2017
HA Status: Not Configured

Maintenance | Service ControllerHome | 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](#)

StartStopRestart ServiceRestart AE ServerRestart LinuxRestart 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 and the text "Application Enablement Services Management Console". A welcome message for the user is shown in the top right corner, including login details and server information. The main navigation bar at the top contains links for "Security", "Security Database", and "Tlinks", along with "Home", "Help", and "Logout". The left sidebar lists various management categories, 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 Dec 5 10:38:11 2017 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: 7.1.1.0.0.5-0
Server Date and Time: Tue Dec 05 10:40:42 EST 2017
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 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 agent login class
- Administer agents and supervisors
- Administer mailboxes
- Administer lines

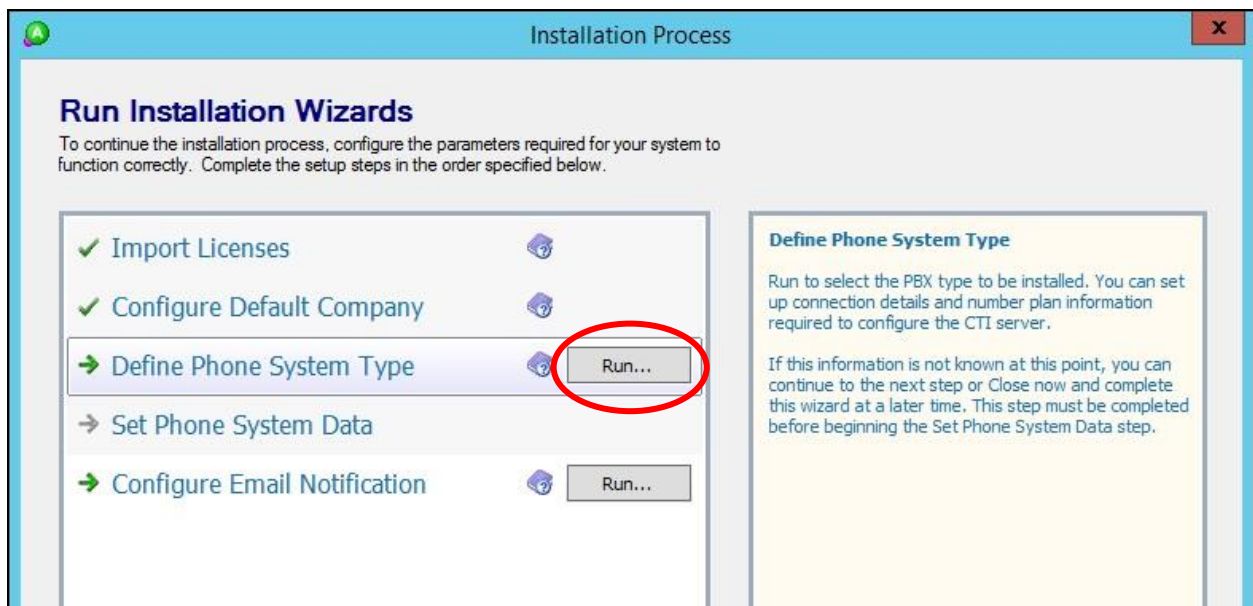
The configuration of EICC is typically performed by Enghouse Interactive installation technicians or third party resellers. The procedural steps are presented in these Application Notes for informational purposes.

Prior to configuration, the relevant Avaya TSAPI client is assumed to be installed on the EICC server, and that the TSAPI client has been configured with the IP address of the Application Enablement Services server as part of installation.

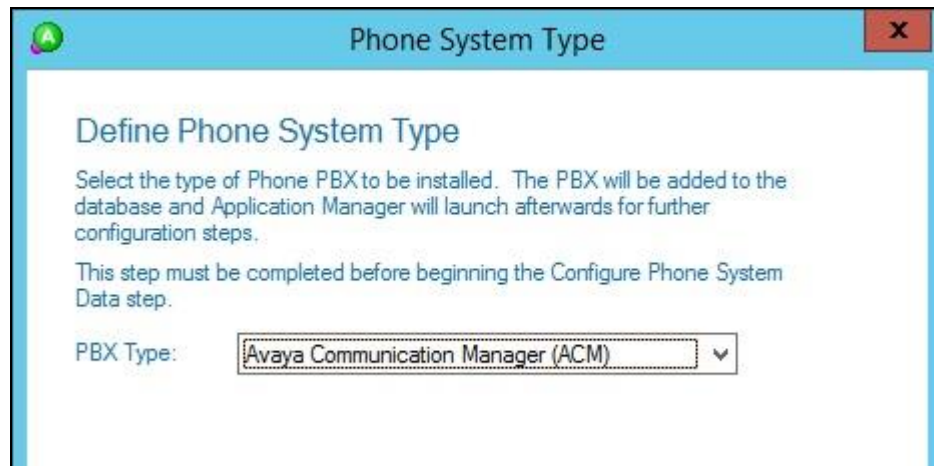
7.1. Administer Phone System Type

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**.

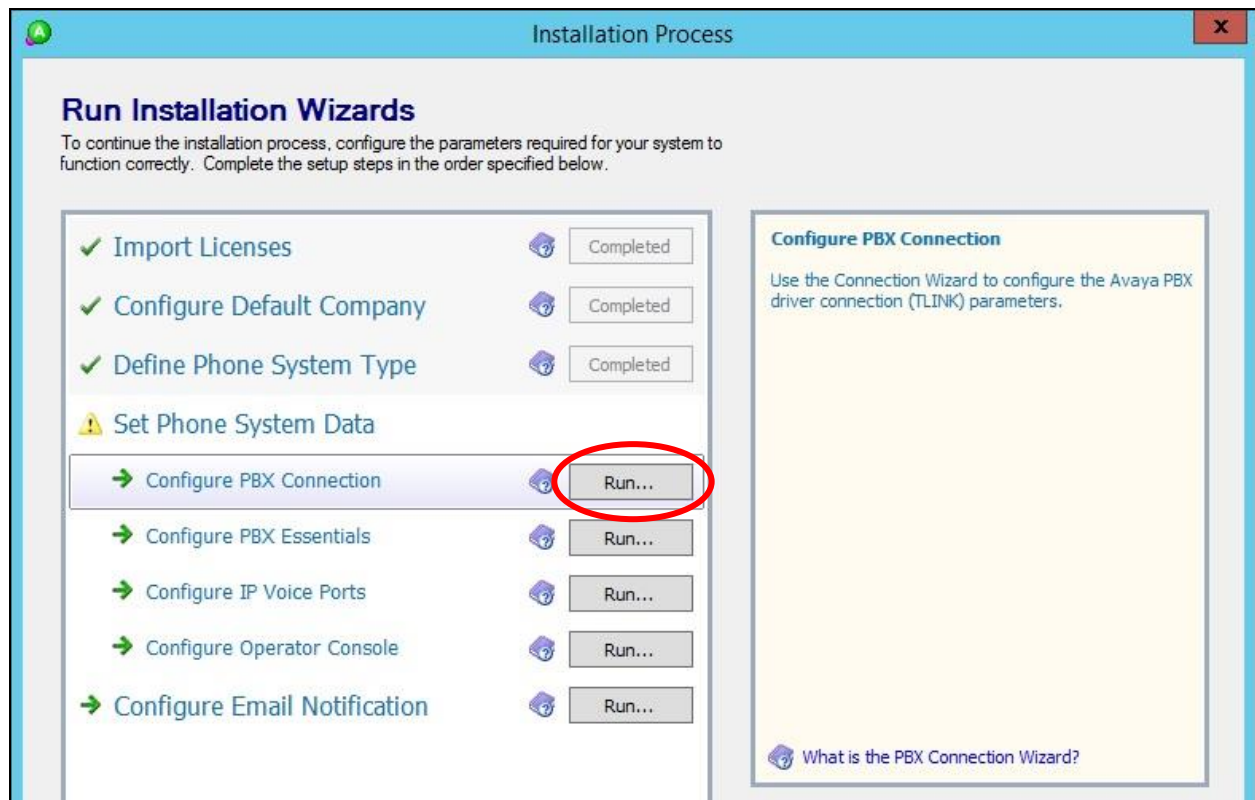


The **Phone System Type** screen is displayed. For **PBX Type**, select “Avaya Communication Manager (ACM)”.

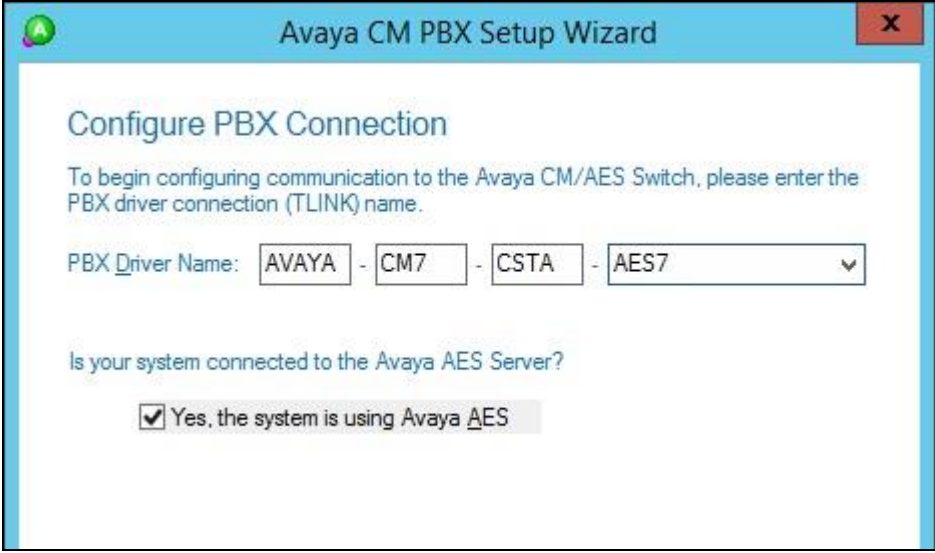


7.2. Administer Phone System Data

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 6.10** as shown below. Retain the default value in the remaining field.



The screenshot shows the 'Avaya CM PBX Setup Wizard' window with the title 'Configure PBX Connection'. Below the title, a message states: 'To begin configuring communication to the Avaya CM/AES Switch, please enter the PBX driver connection (TLINK) name.' There is a dropdown menu for 'PBX_Driver Name' with the value 'AVAYA - CM7 - CSTA - AES7' selected. Below this, a question asks 'Is your system connected to the Avaya AES Server?' with a checked checkbox and the text 'Yes, the system is using Avaya AES'.

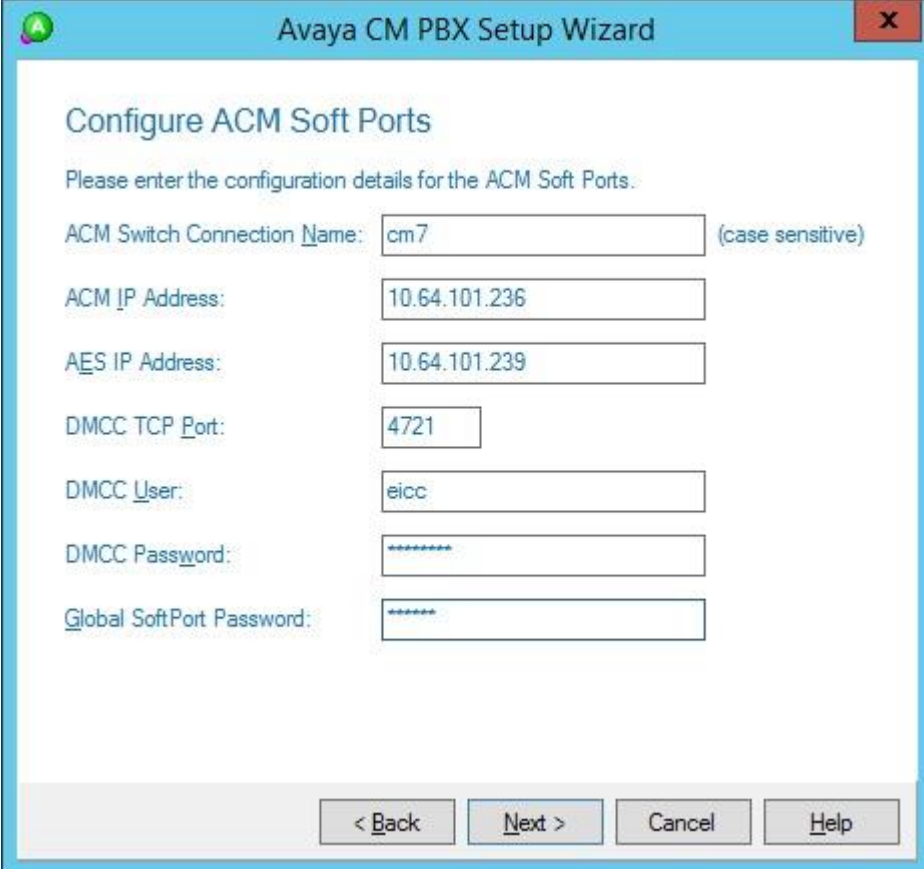
The **Avaya CM PBX Setup Wizard → Configure Avaya CTI User** screen is displayed next. Enter the EICC user credentials from **Section 6.5**.



The screenshot shows the 'Avaya CM PBX Setup Wizard' window with the title 'Configure Avaya CTI User'. Below the title, a message states: 'Please enter the User Name and Password of the CTI User used to access the Avaya CM/AES driver.' There are two input fields: 'User Name' with the value 'eicc' and 'Password' with a masked value '*****'.

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**.

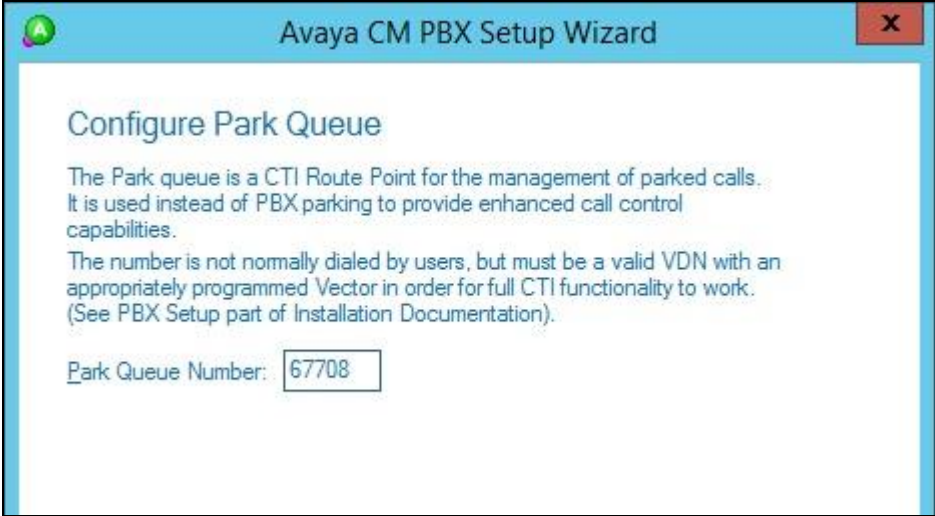


The screenshot shows a window titled "Avaya CM PBX Setup Wizard" with a close button (X) in the top right corner. The main heading is "Configure ACM Soft Ports". Below it, a message says "Please enter the configuration details for the ACM Soft Ports." The form contains the following fields:

- ACM Switch Connection Name: cm7 (case sensitive)
- ACM IP Address: 10.64.101.236
- AES IP Address: 10.64.101.239
- DMCC TCP Port: 4721
- DMCC User: eicc
- DMCC Password: (masked with asterisks)
- Global SoftPort Password: (masked with asterisks)

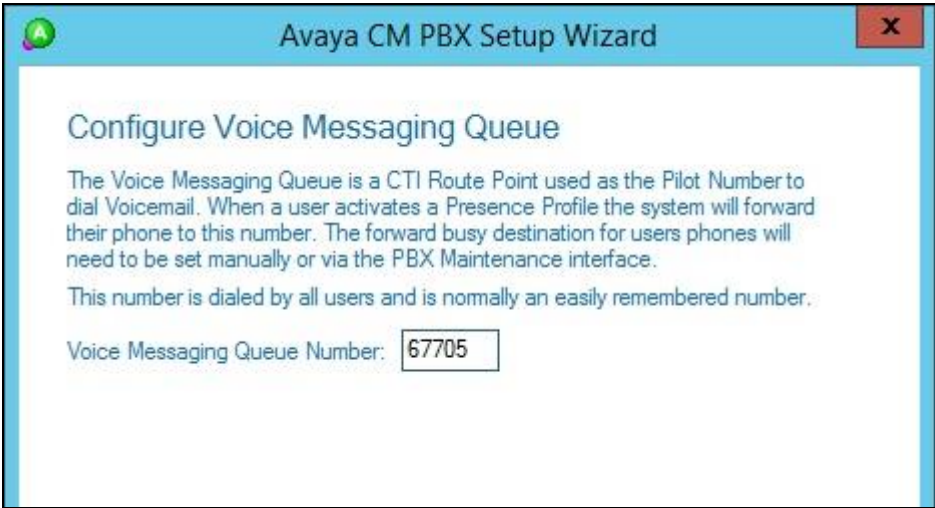
At the bottom, there are four buttons: "< Back", "Next >", "Cancel", and "Help".

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**.



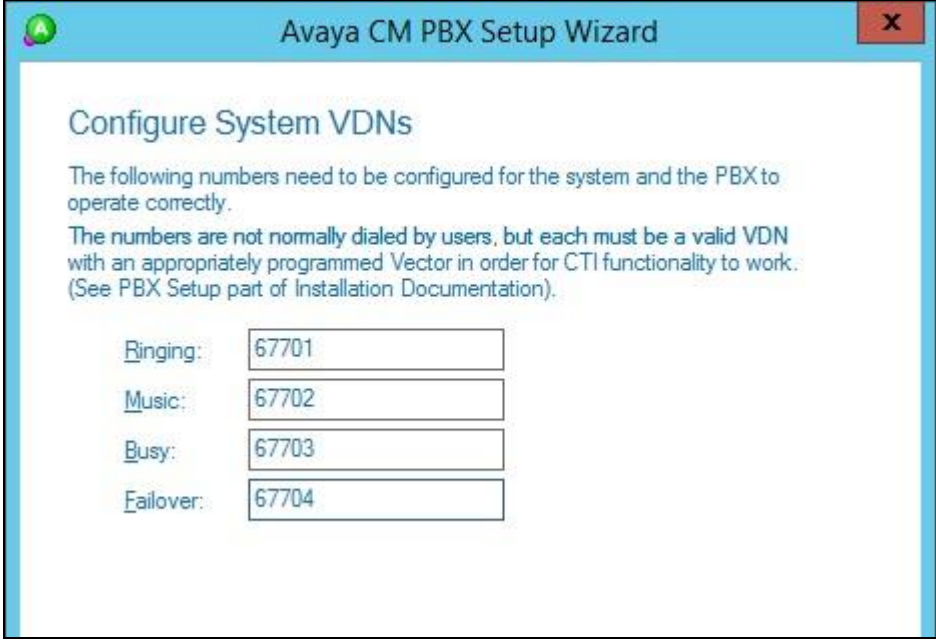
The screenshot shows a window titled "Avaya CM PBX Setup Wizard" with a close button (X) in the top right corner. The main content area is titled "Configure Park Queue". Below the title, there is explanatory text: "The Park queue is a CTI Route Point for the management of parked calls. It is used instead 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 the 'Avaya CM PBX Setup Wizard' window with the title 'Configure System VDNs'. It contains instructional text and four input fields for VDN numbers.

Configure System VDNs

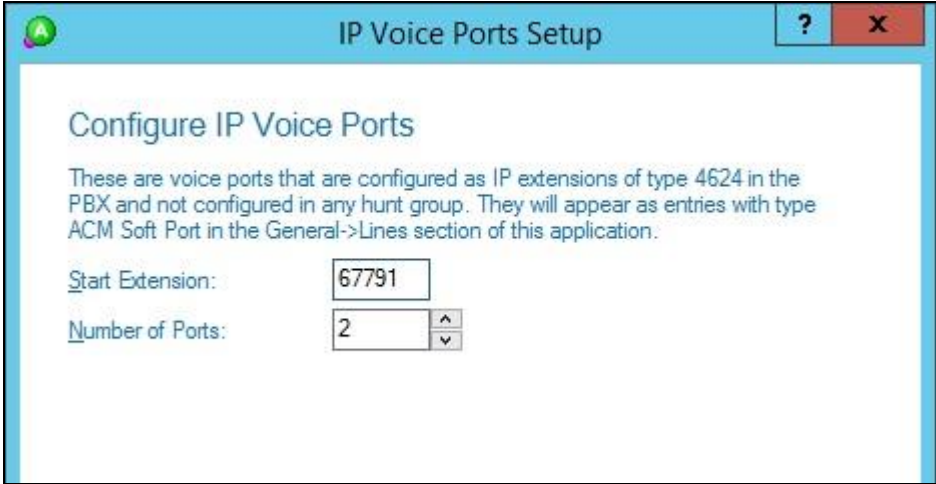
The following numbers need to be configured for the system and the PBX to operate correctly.

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).

Ring:	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**, select the total number of virtual IP softphones from **Section 5.6**, in this case “2”.

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



The screenshot shows the 'IP Voice Ports Setup' window with the title 'Configure IP Voice Ports'. It contains instructional text and two input fields for IP voice port configuration.

Configure IP Voice Ports

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.

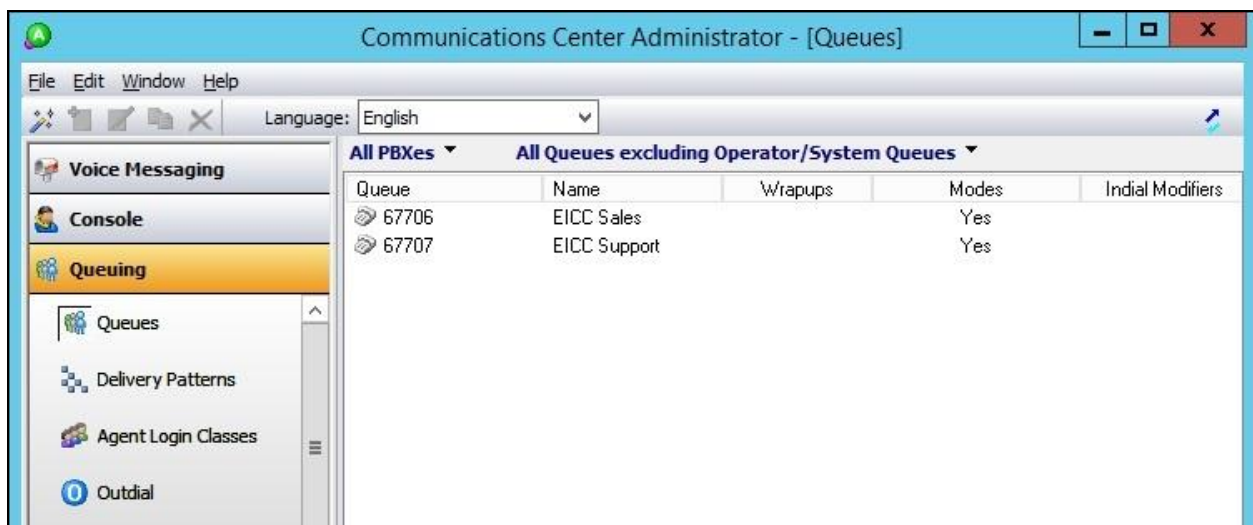
Start Extension:	67791
Number of Ports:	2

7.3. 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.

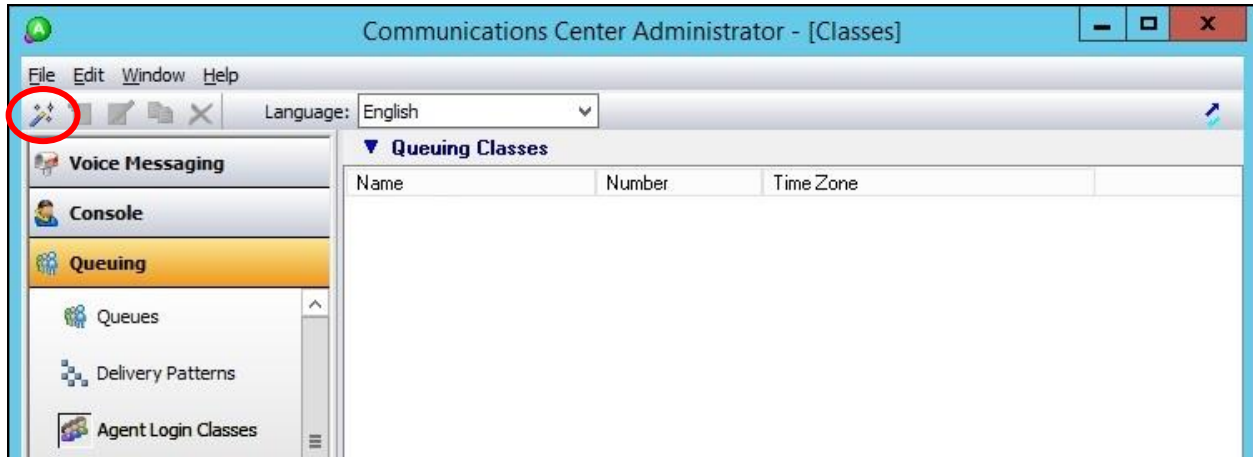


Follow the **Adding a New Queue Wizard** in the subsequent screens (not shown) to configure a new queue for each general routing VDN in **Section 5.3.2**. In the compliance testing, two queues were created as shown below.



7.4. Administer Agent Login Class

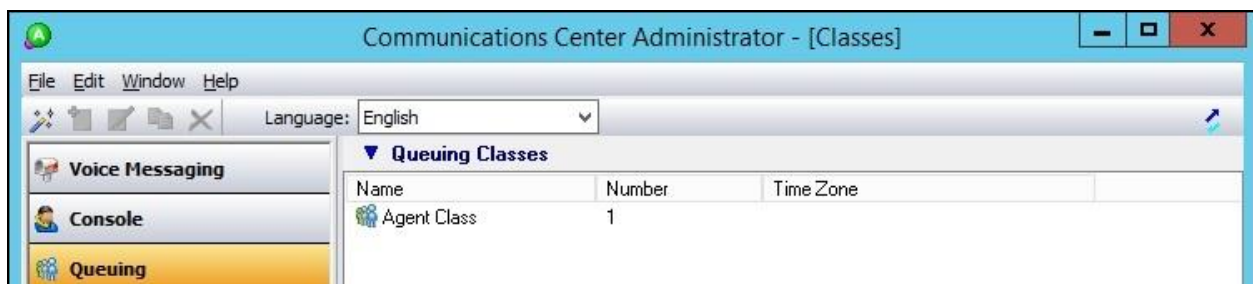
Select **Queuing** → **Agent login Classes** from the left pane, followed by the **Add Wizard** icon located at the upper left corner of the screen.



Follow the **Adding New Agent Login Class Wizard** in the subsequent screens to configure a new agent login class. In the **Select the Queues** screen, select the queues created from **Section 7.3**, as shown below.



In the compliance testing, one agent login class was created.



7.5. 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 to configure a corresponding entry for each agent and supervisor in **Section 3**. In the **Select Agent Login Class** screen, select the agent login class created from **Section 7.4**, as shown below.

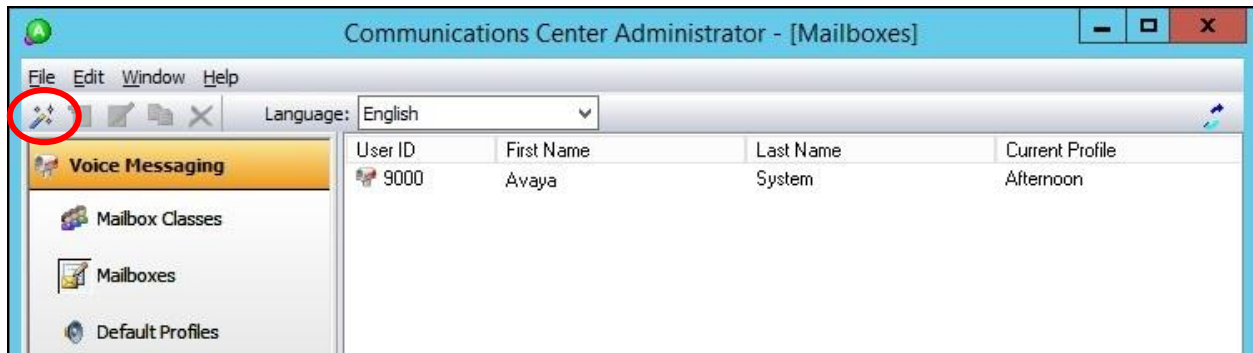


In the compliance testing, two agents and one supervisor were created.

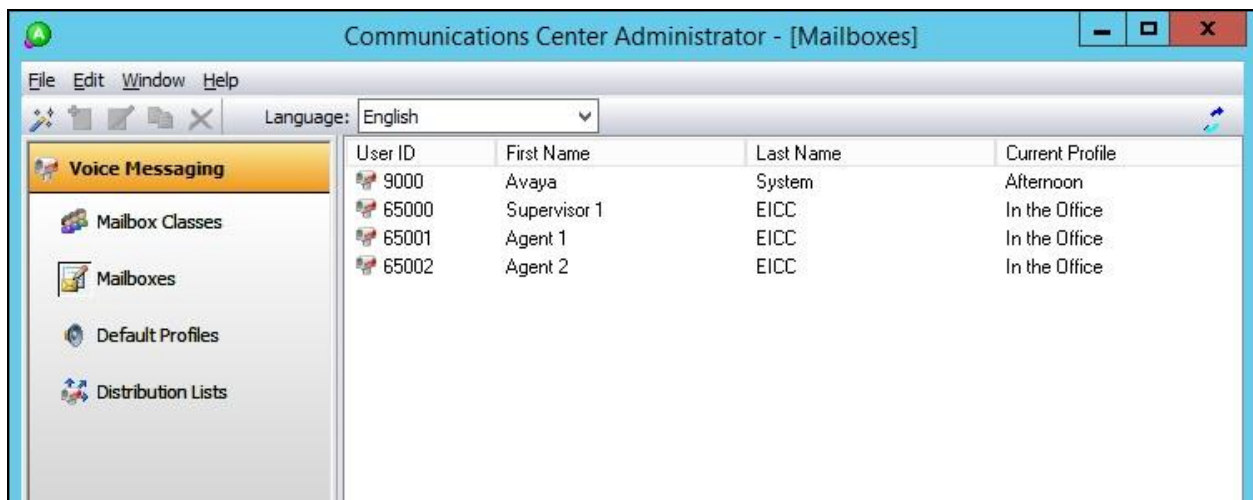


7.6. Administer Mailboxes

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 7.5**. In the compliance testing, three mailboxes were created.

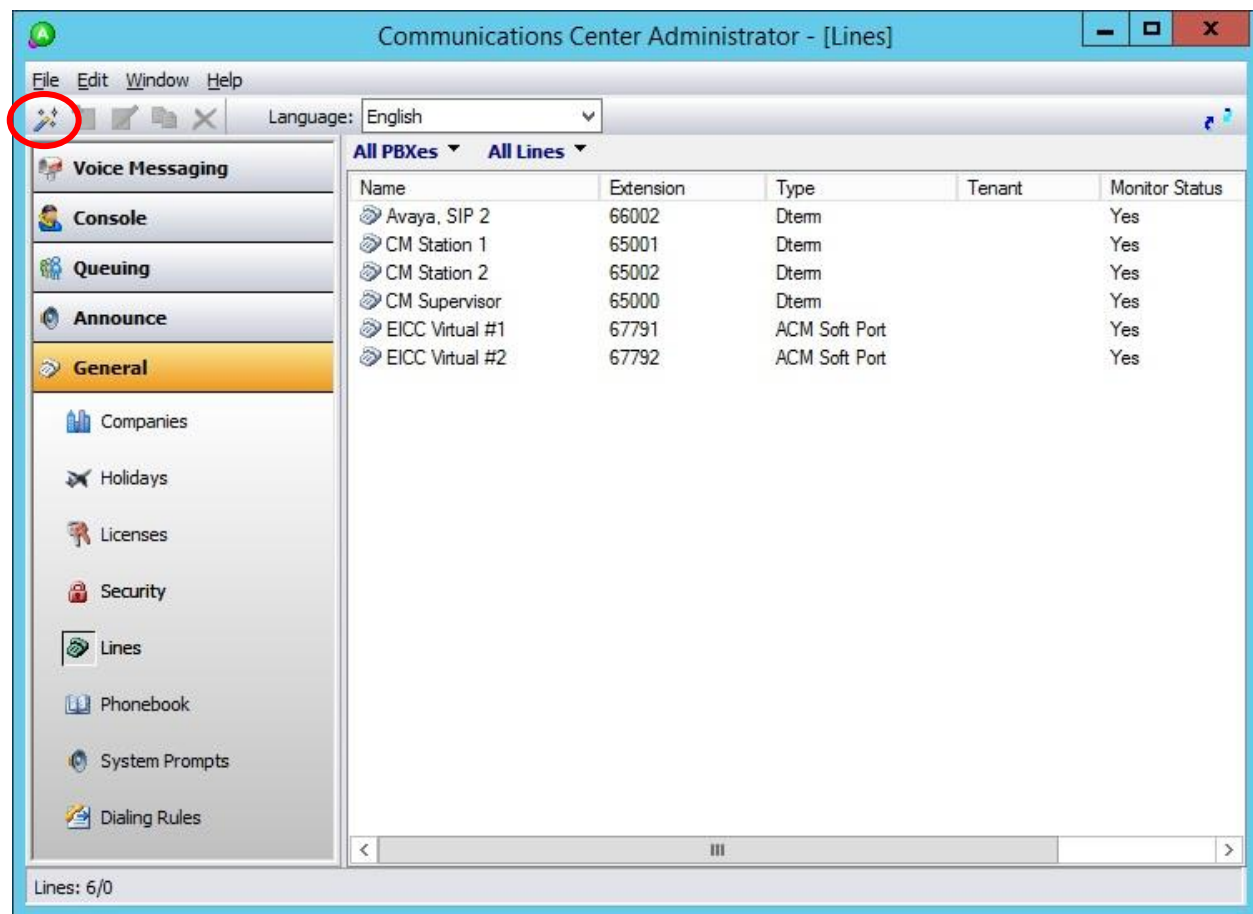


7.7. Administer Lines

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 7.5**.

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.



8. Verification Steps

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

8.1. 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	26	14

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	6.6506		10.64.101.236	
65001	9611	IP_Phone	tls	192.168.200.137	
	1	6.6506		10.64.101.236	
65002	9641	IP_Phone	tls	192.168.200.143	
	1	6.6506		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	

8.2. 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**, in this case “5”.

AVAYA

Application Enablement Services
Management Console

Welcome: User
Last login: Wed Dec 6 09:06:06 2017 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: 7.1.1.0.0.5-0
Server Date and Time: Wed Dec 06 09:07:14 EST 2017
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	Wed Nov 15 12:40:09 2017	Online	17	5	15	24	30


OnlineOffline

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

TSAPI Service StatusTLink StatusUser Status

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: Wed Dec 6 09:06:06 2017 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: 7.1.1.0.0.5-0
 Server Date and Time: Wed Dec 06 09:07:29 EST 2017
 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 Wed Dec 06 09:07:29 EST 2017

Service Uptime: 0 days, 22 hours 24 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"/>	AF6718A046E4D6330 1A258C47B5C36D8-1	eicc		10.64.101.204	XML Unencrypted	1
<input type="checkbox"/>	503CD624B49387980 F1AB35336AD7491-0	eicc		10.64.101.204	XML Unencrypted	1

Terminate Sessions
Show Terminated Sessions

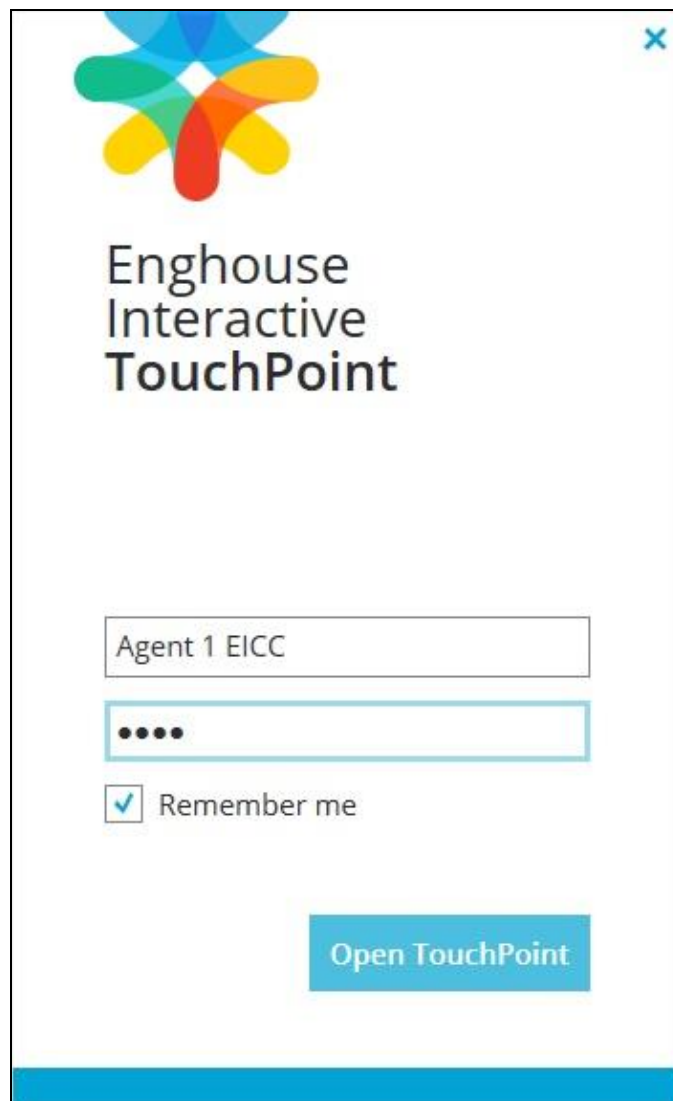
Item 1-2 of 2
1 Go

8.3. Verify Enghouse Interactive Communications Center

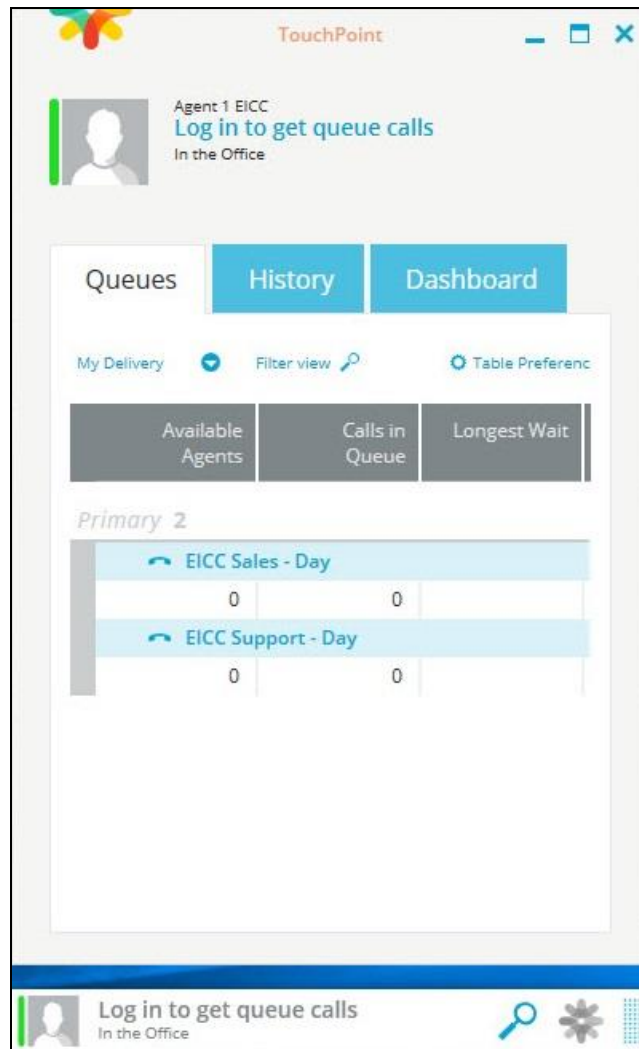
From the agent desktop, double-click on the **TouchPoint** shortcut icon shown below, which was created as part of TouchPoint installation.



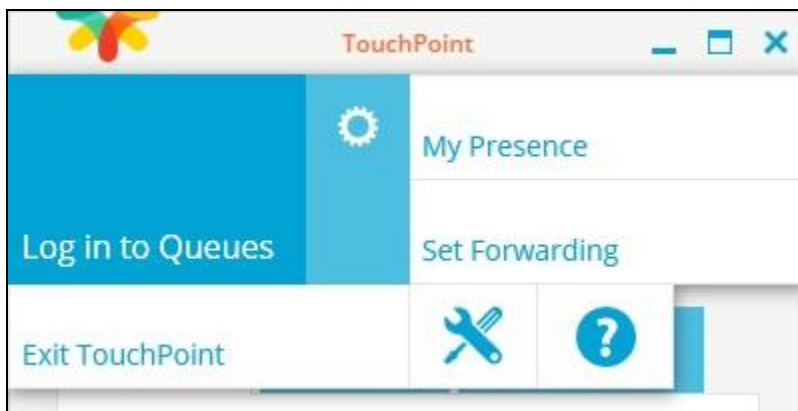
The **Enghouse Interactive TouchPoint** login screen below is displayed. Enter the login name associated with an agent from **Section 7.5**, and use the generic default PIN value from EICC. Retain the default value in the remaining field.

A screenshot of the Enghouse Interactive TouchPoint login screen. The screen has a white background with a blue border. At the top left is a large, colorful logo consisting of overlapping petals in blue, green, yellow, and red. To the right of the logo is a small blue 'X' icon. Below the logo, the text "Enghouse Interactive TouchPoint" is displayed in a large, black, sans-serif font. Underneath the text are two input fields. The first field contains the text "Agent 1 EICC". The second field contains four black dots, indicating a password field. Below the second field is a checkbox with a blue checkmark and the text "Remember me". At the bottom center of the screen is a blue button with the text "Open TouchPoint" in white. A solid blue horizontal bar is at the very bottom of the screen.

The main **TouchPoint** screen, also referred to as the Statistics Window is displayed, along with a Call Bar above the system tray, as shown below. From the Statistics Window, click on **Log in to get queue calls** toward the top of the screen.



In the updated Statistics Window shown below, select **Log in to Queues**.



Verify that both the Statistics Window and Call Bar are updated to reflect **Logged In**, as shown below.

TouchPoint

Agent 1 EICC
Logged In
Queues: 2 Phone
In the Office

Queues History Dashboard

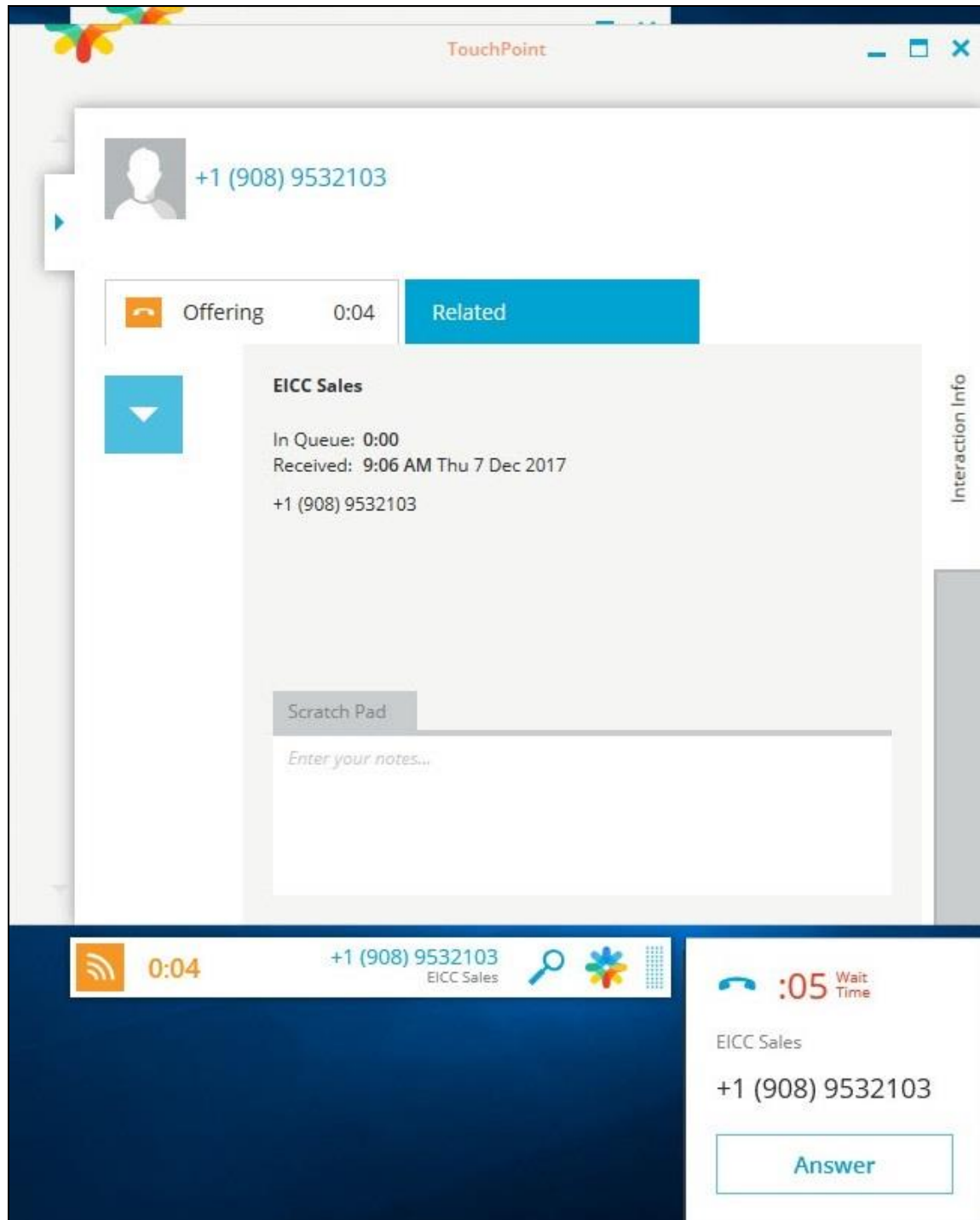
My Delivery Filter view Table Preference

Available Agents	Calls in Queue	Longest Wait
Primary 2		
EICC Sales - Day		
1	0	
EICC Support - Day		
1	0	

Logged In
In the Office

Make an incoming call from PSTN to a general routing VDN in **Section 5.3.2**. Verify that the agent desktop is populated with an **Interaction Info** screen with an **Offering** tab, along with a Pop-up Notification box, and that the Call Bar is updated to reflect the active call.

Click **Answer** in the Pop-up Notification box, and verify that the agent is connected to the PSTN caller with two-way talk paths.



9. Conclusion

These Application Notes describe the configuration steps required for Enghouse Interactive Communications Center 10.0 to successfully interoperate with Avaya Aura® Communication Manager 7.1 using Avaya Aura® Application Enablement Services 7.1. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

10. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Release 7.1.1, Issue 2, August 2017, available at <http://support.avaya.com>.
2. *Administering and Maintaining Aura® Application Enablement Services*, Release 7.1.1, Issue 3, September 2017, available at <http://support.avaya.com>.
3. *CC 10.0 First-time Installation and Server Setup – Avaya Communication Manager*, June 2017, available at <https://partnerportal.enghouseinteractive.com/Sys/Document/index>.
4. *CC 10.0 for PBX Programming Manual – Avaya Communication Manager*, June 2017, available at <https://partnerportal.enghouseinteractive.com/Sys/Document/index>.

©2018 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.