



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

---

# **Application Notes for Enghouse Interactive Communications Center 10.1 with Avaya Aura® Communication Manager 8.0 FP1 using Avaya Aura® Application Enablement Services 8.0 – Issue 1.0**

## **Abstract**

These Application Notes describe the configuration steps required for Enghouse Interactive Communications Center 10.1 to interoperate with Avaya Aura® Communication Manager 8.0 FP1 using Avaya Aura® Application Enablement Services 8.0. 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) 10.1 to interoperate with Avaya Aura® Communication Manager 8.0 FP1 using Avaya Aura® Application Enablement Services 8.0. 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.

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](http://www.enghouseinteractive.com)

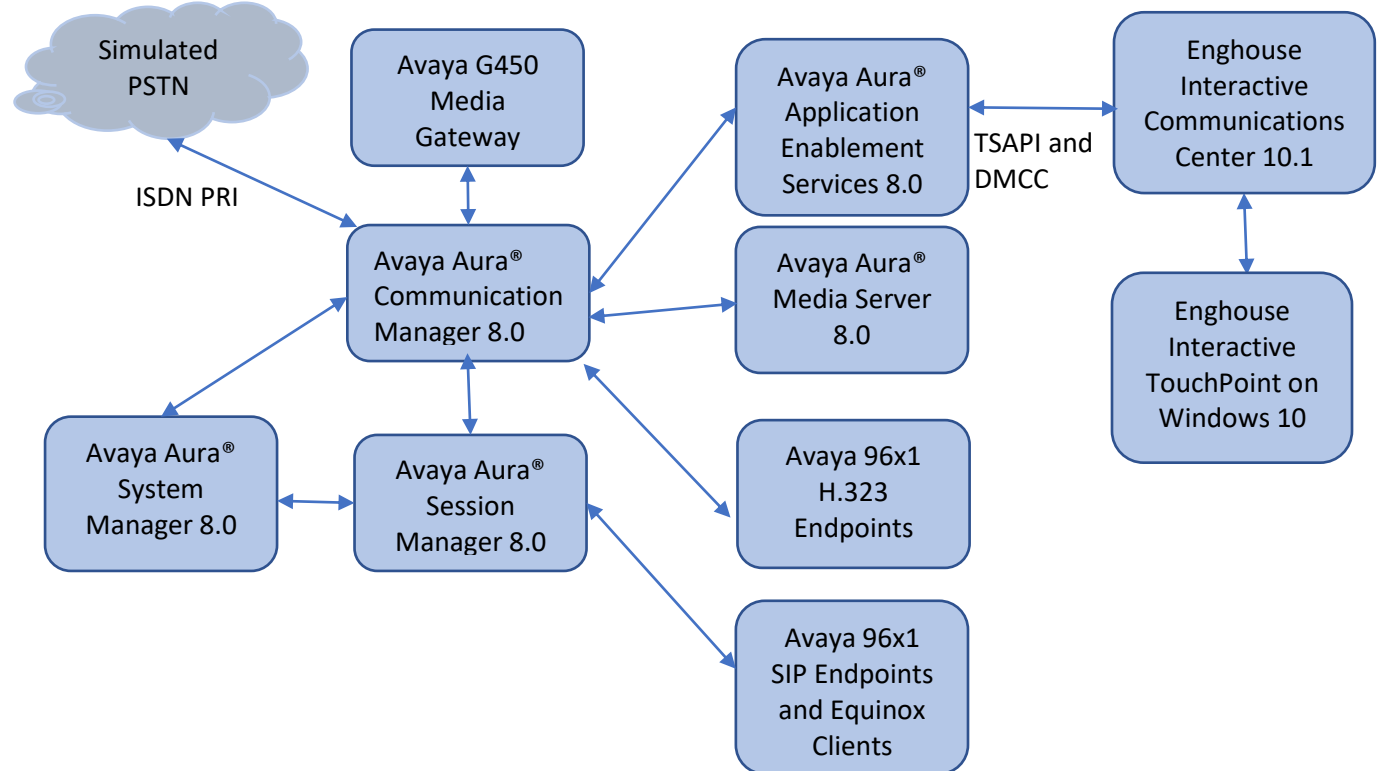
**Email:** [usa.support@enghouse.com](mailto:usa.support@enghouse.com)

### 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	70010, 70011
Supervisor & failure covering station	7000



**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	8.0.1.0.0 (8.0 FP1)
Avaya G450 Media Gateway	40.10.1
Avaya Aura® Media Server in Virtual Environment	8.0 SP2
Avaya Aura® Application Enablement Services in Virtual Environment	8.0.1
Avaya 9608G & 9641G IP Deskphone (H.323)	6.8
Enghouse Interactive Communications Center on Windows Server 2012 R2 Avaya TSAPI Windows Client (csta32.dll) Avaya DMCC XML	10.1.0.11994 Standard 8.0.0.38 8.0.0.0.419
Enghouse Interactive TouchPoint on Windows 10 Pro	10.1.0.11994

## 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
    Async. Transfer Mode (ATM) PNC? n
    Async. Transfer Mode (ATM) Trunking? n       Digital Loss Plan Modification? y
      ATM WAN Spare Processor? n           DS1 MSP? y
      ATMS? y          DS1 Echo Cancellation? y
      Attendant Vectoring? y

(NOTE: You must logoff & login to effect the permission changes.)
```

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	<b>Vectoring (Basic)?</b>	<b>y</b>
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		
<b>Extension: 79999</b>		
<b>Type: ADJ-IP</b>		
COR: 1		
<b>Name: aes8</b>		



### 5.3.Administer Vectors and VDNs

Administer a set of vectors and VDNs per EICC installation document [5]. 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
87001	71	Ring treatment
87002	72	Music treatment
87003	73	Busy treatment
87004	74	Failure coverage
87005	75	Voicemail routing
87006	70	General routing for the Sales application
87007	70	General routing for the Support application
87008	78	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 5.3**. 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 [5].

```
change vector 74                                     Page 1 of 6
                                                    CALL VECTOR
Number: 74                                           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 87000      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 87004                                     Page 1 of 3
                                                    VECTOR DIRECTORY NUMBER
Extension: 87004
Name*: SC Fail
Destination: Vector Number      74
```

### 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 [5].

```
change vector 70                                     Page 1 of 6
                                                    CALL VECTOR

  Number: 70                      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 87004          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 87006                                     Page 1 of 2
                                                    VECTOR DIRECTORY NUMBER

  Extension: 87006
  Name: EICC Sales
  Destination: Vector Number          70
```

```
add vdn 87007                                     Page 1 of 2
                                                    VECTOR DIRECTORY NUMBER

  Extension: 87007
  Name: EICC Support
  Destination: Vector Number          70
```

### 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 [5].

change vector 71		Page 1 of 6	
CALL VECTOR			
<b>Number: 71</b>		<b>Name: SC Ring</b>	
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		
02 wait-time	60 secs hearing ringback		
03 route-to	number 87004 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 87001		Page 1 of 2	
VECTOR DIRECTORY NUMBER			
Extension: 87001			
<b>Name: SC Ring</b>			
<b>Destination: Vector Number</b>		<b>71</b>	

### 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 [5].

change vector 72			Page 1 of 6		
CALL VECTOR					
Number: 72		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 87004 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 87002		Page 1 of 2	
VECTOR DIRECTORY NUMBER			
Extension: 87002			
Name: SC Music			
Destination: Vector Number		72	

### 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 [5].

change vector 73	Page 1 of 6
CALL VECTOR	
<b>Number: 73</b>	
<b>Name: SC Busy</b>	
Multimedia? n	Attendant Vectoring? n
Basic? y	Meet-me Conf? n
Prompting? y	Lock? n
Variables? y	EAS? y
	G3V4 Enhanced? y
	ANI/II-Digits? y
	ASAI Routing? y
	LAI? y
	G3V4 Adv Route? y
	CINFO? y
	BSR? y
	Holidays? 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 87003	Page 1 of 2
VECTOR DIRECTORY NUMBER	
Extension: 87003	
<b>Name: SC Busy</b>	
<b>Destination: Vector Number</b>	<b>73</b>

### 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 [5].

change vector 75		Page 1 of 6	
CALL VECTOR			
<b>Number: 75</b>		<b>Name: SC Voicemail</b>	
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
			Holidays? 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 87005		Page 1 of 2	
VECTOR DIRECTORY NUMBER			
Extension: 87005			
<b>Name: SC Voicemail</b>			
<b>Destination: Vector Number</b>		<b>75</b>	

### 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 [5].

change vector 78		Page 1 of 6
CALL VECTOR		
<b>Number: 78</b>	<b>Name: SC Hold</b>	
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 87004 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 87008		Page 1 of 2
VECTOR DIRECTORY NUMBER		
Extension: 87008		
<b>Name: SC Hold</b>		
<b>Destination: Vector Number</b>	<b>78</b>	



## 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 “v87005” to designate as the first coverage point, where “87005” is the voicemail VDN extension from **Section 5.3.6**.

add coverage path 5		Page 1 of 1	
COVERAGE PATH			
Coverage Path Number: 5			
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			
<b>Point1: v87005</b>	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 70010		Page 1 of 5
STATION		
Extension: 70010	Lock Messages? n	BCC: 0
Type: 9641	Security Code: *	TN: 1
Port: S00102	<b>Coverage Path 1: 5</b>	COR: 1
Name: Agent 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? 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 70010 count 2									
STATIONS									
Ext/ Hunt-to	Port/ Type	Name/ Surv GK NN	Move	Room/ Data Ext	Cv1/ Cv2	COR/ COS	Cable/ TN	Jack	
70010	S00033 9641	Agent Station 1	no		7	1	1		
70011	S00036 9641	Agent Station 2	no		7	1	1		

list station 70000 count 1									
STATIONS									
Ext/ Hunt-to	Port/ Type	Name/ Surv GK NN	Move	Room/ Data Ext	Cv1/ Cv2	COR/ COS	Cable/ TN	Jack	
70000	S00029 9641	Supervisor	no		7	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 70016		Page 1 of 6
STATION		
Extension: 70016	Lock Messages? n	BCC: 0
<b>Type: 4624</b>	<b>Security Code: 6789</b>	TN: 1
Port: IP	Coverage Path 1:	COR: 1
<b>Name: EICC Virtual #1</b>	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	<b>IP SoftPhone? y</b>	
	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, 4 virtual IP softphones were administered as shown below.

list station 70016 count 4									
STATIONS									
Ext/ Hunt-to	Port/ Type	Name/ Surv GK NN	Move	Room/ Data	Ext	Cv1/ Cv2	COR/ COS	Cable/ TN	Jack
70016	S00061	EICC Virtual #1					1		
	4624		no				1	1	
70017	S00062	EICC Virtual #2					1		
	4624		no				1	1	
70018	S00063	EICC Virtual #3					1		
	4624		no				1	1	
70019	S00064	EICC Virtual #4					1		
	4624		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.



### Application Enablement Services Management Console

Please login here:

Username

Copyright © 2009-2018 Avaya Inc. All Rights Reserved.

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



### Application Enablement Services Management Console

Welcome: User cust  
Last login: Tue Mar 26 15:40:17 2019 from 10.128.224.59  
Number of prior failed login attempts: 0  
HostName/IP: aes8.hcm.com/fe80::250:56ff:feb7:8ca7%eth2  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.0.1.0.0.5-0  
Server Date and Time: Tue Mar 26 15:47:40 ICT 2019  
HA Status: Not Configured

[Home](#)

[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.

Copyright © 2009-2018 Avaya Inc. All Rights Reserved.

## 6.2. Verify License

Select **Licensing** → **WebLM Server Access** in the left pane, to display the applicable WebLM server log in screen (not shown). Log in using the appropriate credentials, and navigate to display installed licenses (not shown).

The screenshot displays the Avaya Application Enablement Services Management Console. At the top left is the Avaya logo. To its right, the text reads "Application Enablement Services Management Console". In the top right corner, a welcome message is shown: "Welcome: User cust", followed by login details: "Last login: Tue Mar 26 15:40:17 2019 from 10.128.224.59", "Number of prior failed login attempts: 0", "HostName/IP: aes8.hcm.com/fe80::250:56ff:feb7:8ca7%eth2", "Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE", "SW Version: 8.0.1.0.0.5-0", "Server Date and Time: Tue Mar 26 15:49:11 ICT 2019", and "HA Status: Not Configured". Below this is a red navigation bar with "Licensing" on the left and "Home | Help | Logout" on the right. On the left side of the console, there is a vertical menu with options: "AE Services", "Communication Manager Interface", "High Availability", "Licensing" (which is expanded), "WebLM Server Address", "WebLM Server Access" (highlighted in blue), "Reserved Licenses", and "Maintenance". The main content area on the right is titled "Licensing" and contains three sections of instructions: "If you are setting up and maintaining the WebLM, you need to use the following:" with a bullet point for "WebLM Server Address"; "If you are importing, setting up and maintaining the license, you need to use the following:" with a bullet point for "WebLM Server Access"; and "If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:" with a bullet point for "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 8.0

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾ Search 🔍 🔔 ☰ | admin

Home | **Licenses**

**Licenses** ▴

- Licensed products
  - APPL\_ENAB
    - ▼ Application\_Enablement
      - View license capacity
      - View peak usage
    - CE
      - COLLABORATION\_ENVIRONMENT
    - COLLABORATION\_DESIGNER
      - Collaboration\_Designer
    - MESSAGING
      - Messaging
    - MSR
      - Media\_Server
    - SYSTEM\_MANAGER
      - System\_Manager
    - SessionManager
      - SessionManager
    - Uninstall license
    - Server properties
  - Shortcuts
  - Help for Licensed products

You are here: Licensed Products > Application\_Enablement > View License Capacity

License installed on: December 28, 2018 11:22:53 AM +07:00

**License File Host IDs:** V0-55-3B-33-B4-26-01

**Licensed Features**

13 Items 🔍 Show All ▾

Feature (License Keyword)	Expiration date	Licensed capacity
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	1000
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	1000
AES HA LARGE VALUE_AES_HA_LARGE	permanent	1000
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	1000
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	1000
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	1000
AES HA MEDIUM VALUE_AES_HA_MEDIUM	permanent	1000
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	1000
DLG VALUE_AES_DLG	permanent	1000
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	1000
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	1000

## 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**.



**Application Enablement Services**  
Management Console

Welcome: User cust  
Last login: Mon Mar 25 17:38:53 2019 from 10.128.224.59  
Number of prior failed login attempts: 0  
HostName/IP: aes8.hcm.com/fe80::250:56ff:feb7:8ca7%eth2  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.0.1.0.0.5-0  
Server Date and Time: Mon Mar 25 17:49:07 ICT 2019  
HA Status: Not Configured

AE Services | TSAPI | TSAPI LinksHome | Help | Logout

▼ AE Services


- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▼ TSAPI
  - TSAPI Links
  - TSAPI Properties

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
<div>Add LinkEdit LinkDelete Link</div>				

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 “CM8” is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields.



**Application Enablement Services**  
Management Console

Welcome: User cust  
Last login: Mon Mar 25 17:38:53 2019 from 10.128.224.59  
Number of prior failed login attempts: 0  
HostName/IP: aes8.hcm.com/fe80::250:56ff:feb7:8ca7%eth2  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.0.1.0.0.5-0  
Server Date and Time: Mon Mar 25 17:58:54 ICT 2019  
HA Status: Not Configured

AE Services | TSAPI | TSAPI LinksHome | Help | Logout

▼ AE Services

- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▼ TSAPI
  - TSAPI Links
  - TSAPI Properties
- ▶ TWS

Add TSAPI Links

Link1  
Switch ConnectionCM8  
Switch CTI Link Number1  
ASAI Link Version9  
SecurityUnencrypted  

Apply ChangesCancel Changes



Communication Manager Interface | Switch Connections
 Home | Help | Logout

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

### Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
CM8	Yes	30	1

Communication Manager Interface | Switch Connections
 Home | Help | Logout

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

### Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
CM8	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 “10.30.5.93” as shown below. Click **Add Name or IP**.

Communication Manager Interface | Switch Connections
 Home | Help | Logout

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

### Edit H.323 Gatekeeper - CM8

Name or IP Address

## 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.



### Application Enablement Services Management Console

Welcome: User cust  
Last login: Mon Mar 25 17:38:53 2019 from 10.128.224.59  
Number of prior failed login attempts: 0  
HostName/IP: aes8.hcm.com/fe80::250:56ff:feb7:8ca7%eth2  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.0.1.0.0.5-0  
Server Date and Time: Mon Mar 25 18:10:58 ICT 2019  
HA Status: Not Configured

User Management | User Admin | Add User

[Home](#) | [Help](#) | [Logout](#)

<ul style="list-style-type: none"><li>▶ AE Services</li><li>▶ Communication Manager Interface</li><li>▶ High Availability</li><li>▶ Licensing</li><li>▶ Maintenance</li><li>▶ Networking</li><li>▶ Security</li><li>▶ Status</li><li>▼ User Management<ul style="list-style-type: none"><li>▶ Service Admin</li><li>▼ User Admin<ul style="list-style-type: none"><li>■ Add User</li><li>■ Change User Password</li><li>■ List All Users</li><li>■ Modify Default Users</li><li>■ Search Users</li></ul></li><li>▶ Utilities</li><li>▶ Help</li></ul></li></ul>	<h3>Add User</h3> <p>Fields marked with * can not be empty.</p> <p>* User Id <input type="text" value="eicc"/></p> <p>* Common Name <input type="text" value="eicc"/></p> <p>* Surname <input type="text" value="eicc"/></p> <p>* User Password <input type="password" value="....."/></p> <p>* Confirm Password <input type="password" value="....."/></p> <p>Admin Note <input type="text"/></p> <p>Avaya Role <input type="text" value="None"/></p> <p>Business Category <input type="text"/></p> <p>Car License <input type="text"/></p> <p>CM Home <input type="text"/></p> <p>Css Home <input type="text"/></p> <p>CT User <input type="text" value="Yes"/></p> <p>Department Number <input type="text"/></p> <p>Display Name <input type="text"/></p> <p>Employee Number <input type="text"/></p> <p>Employee Type <input type="text"/></p> <p>Enterprise Handle <input type="text"/></p> <p>Given Name <input type="text"/></p> <p>Home Phone <input type="text"/></p> <p>Home Postal Address <input type="text"/></p> <p>Initials <input type="text"/></p> <p>Labeled URI <input type="text"/></p> <p>Mail <input type="text"/></p> <p>MM Home <input type="text"/></p> <p>Mobile <input type="text"/></p>
---	---

## 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 [4] to configure access privileges for the EICC user from **Section 6.5**.



### Application Enablement Services Management Console

Welcome: User cust  
Last login: Mon Mar 25 17:43:45 2019 from 10.128.224.59  
Number of prior failed login attempts: 0  
HostName/IP: aes8.hcm.com/fe80::250:56ff:feb7:8ca7%eth2  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.0.1.0.0.5-0  
Server Date and Time: Mon Mar 25 18:29:44 ICT 2019  
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 cust  
Last login: Mon Mar 25 17:43:45 2019 from 10.128.224.59  
Number of prior failed login attempts: 0  
HostName/IP: aes8.hcm.com/fe80::250:56ff:feb7:8ca7%eth2 :  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.0.1.0.0.5-0  
Server Date and Time: Mon Mar 25 18:32:41 ICT 2019  
HA Status: Not Configured

Networking | Ports

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▼ Networking

▶ AE Service IP (Local IP)

▶ Network Configure

▶ Ports

▶ TCP/TLS Settings

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

**Ports**

CVLAN Ports

			Enabled	Disabled
Unencrypted TCP Port	9999		<input checked="" type="radio"/>	<input type="radio"/>
Encrypted TCP Port	<input type="text" value="9998"/>		<input type="radio"/>	<input checked="" type="radio"/>

DLG Port

	TCP Port	
	5678	

TSAPI Ports

			Enabled	Disabled
TSAPI Service Port	450		<input checked="" type="radio"/>	<input type="radio"/>
Local TLINK Ports				
TCP Port Min	1024			
TCP Port Max	1039			
Unencrypted TLINK Ports				
TCP Port Min	<input type="text" value="1050"/>			
TCP Port Max	<input type="text" value="1065"/>			
Encrypted TLINK Ports				
TCP Port Min	<input type="text" value="1066"/>			
TCP Port Max	<input type="text" value="1081"/>			

DMCC Server Ports

			Enabled	Disabled
Unencrypted Port	<input type="text" value="4721"/>		<input checked="" type="radio"/>	<input type="radio"/>
Encrypted Port	<input type="text" value="4722"/>		<input type="radio"/>	<input checked="" type="radio"/>
TR/87 Port	<input type="text" value="4723"/>		<input checked="" type="radio"/>	<input type="radio"/>

H.323 Ports

TCP Port Min	<input type="text" value="20000"/>
TCP Port Max	<input type="text" value="29999"/>
Local UDP Port Min	<input type="text" value="20000"/>
Local UDP Port Max	<input type="text" value="29999"/>


NAQ; Reviewed  
SPOC 4/24/2019

Solution & Interoperability Test Lab Application Notes  
©2019 Avaya Inc. All Rights Reserved.

28 of 54  
EICC-AES8

## 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.

**Application Enablement Services**  
Management Console

Welcome: User cust  
Last login: Mon Mar 25 17:43:45 2019 from 10.128.224.59  
Number of prior failed login attempts: 0  
HostName/IP: aes8.hcm.com/fe80::250:56ff:feb7:8ca7%eth2  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.0.1.0.0.5-0  
Server Date and Time: Mon Mar 25 18:34:19 ICT 2019  
HA Status: Not Configured

Networking | TCP / TLS SettingsHome | 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**.



**Application Enablement Services**  
Management Console

Welcome: User cust  
Last login: Tue Mar 26 14:26:05 2019 from 10.128.224.59  
Number of prior failed login attempts: 0  
HostName/IP: aes8.hcm.com/fe80::250:56ff:feb7:8ca7%eth2 :  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.0.1.0.0.5-0  
Server Date and Time: Tue Mar 26 14:47:14 ICT 2019  
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

▶ User Management

▶ Utilities

▶ Help

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#CM8#CSTA#AES8”. Note the use of the switch connection “CM8 from **Section 6.3** as part of the Tlink name.

**Application Enablement Services**  
Management Console

Welcome: User cust  
Last login: Tue Mar 26 14:26:05 2019 from 10.128.224.59  
Number of prior failed login attempts: 0  
HostName/IP: aes8.hcm.com/fe80::250:56ff:feb7:8ca7%eth2  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.0.1.0.0.5-0  
Server Date and Time: Tue Mar 26 15:26:16 ICT 2019  
HA Status: Not Configured

Security | Security Database | TlinksHome | 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#CM8#CSTA#AES8

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

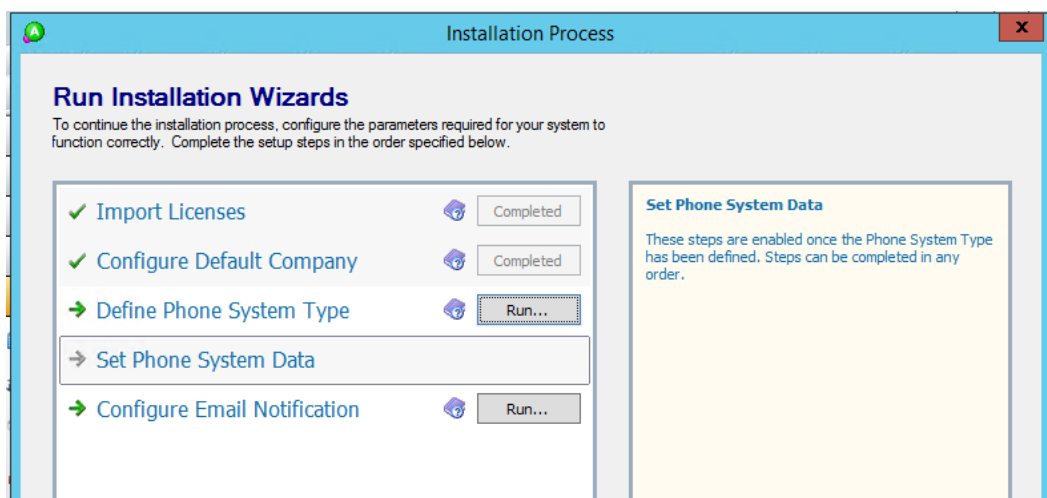
The configuration of EICC is typically performed by Enghouse Interactive installation technicians or third-party resellers. The procedural steps are presented in these Application Notes for informational purposes.

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

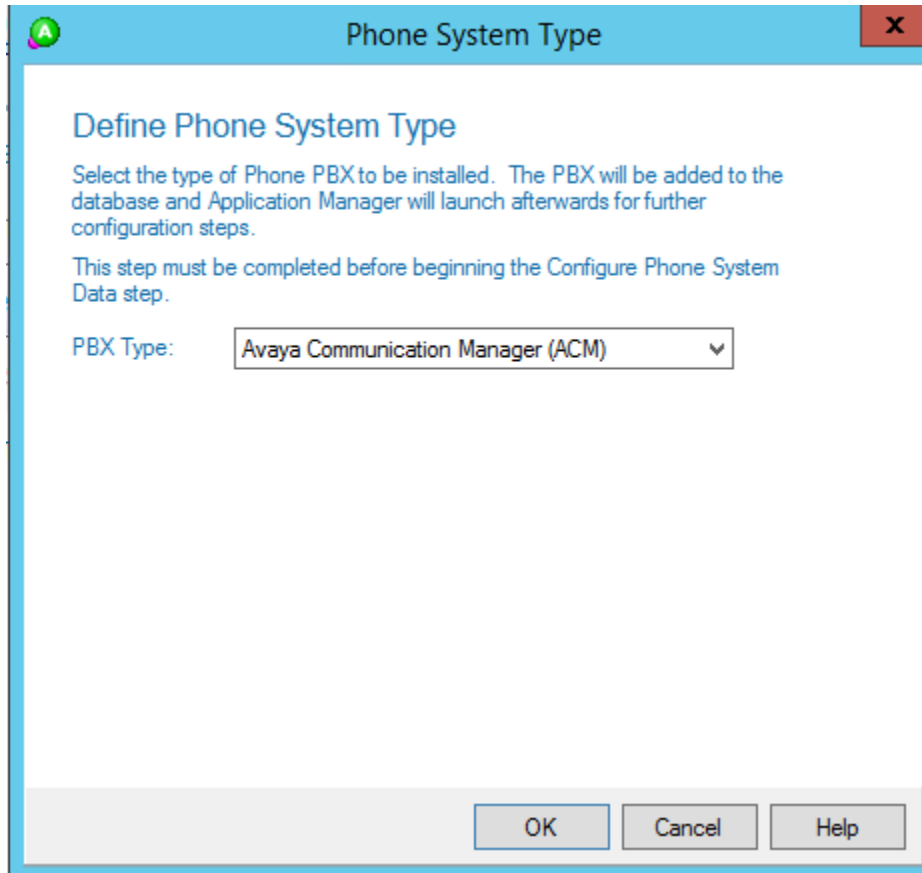
At the conclusion of installation, the **Installation Process** screen will be displayed by the Installation Wizard. Follow [5] to import licenses and configure the default company.

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)”.

A screenshot of a Windows-style dialog box titled "Phone System Type". The dialog has a blue header bar with a green "A" icon on the left and a red "X" close button on the right. The main content area is white and contains the following text: "Define Phone System Type" in blue, followed by "Select the type of Phone PBX to be installed. The PBX will be added to the database and Application Manager will launch afterwards for further configuration steps." and "This step must be completed before beginning the Configure Phone System Data step." Below this is a label "PBX Type:" followed by a dropdown menu showing "Avaya Communication Manager (ACM)" with a downward arrow. At the bottom right, there are three buttons: "OK", "Cancel", and "Help".

**Phone System Type**

**Define Phone System Type**

Select the type of Phone PBX to be installed. The PBX will be added to the database and Application Manager will launch afterwards for further configuration steps.

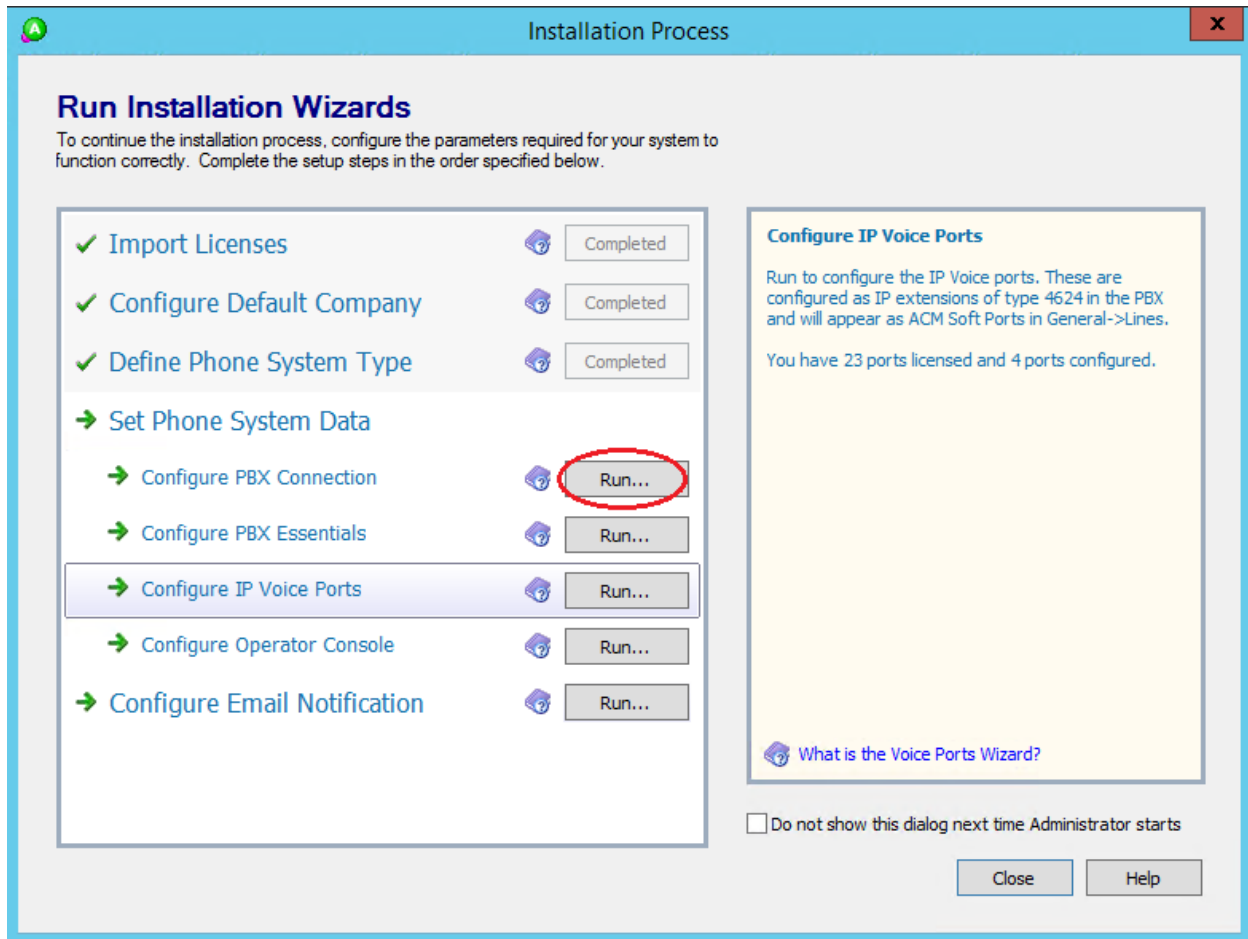
This step must be completed before beginning the Configure Phone System Data step.

PBX Type:

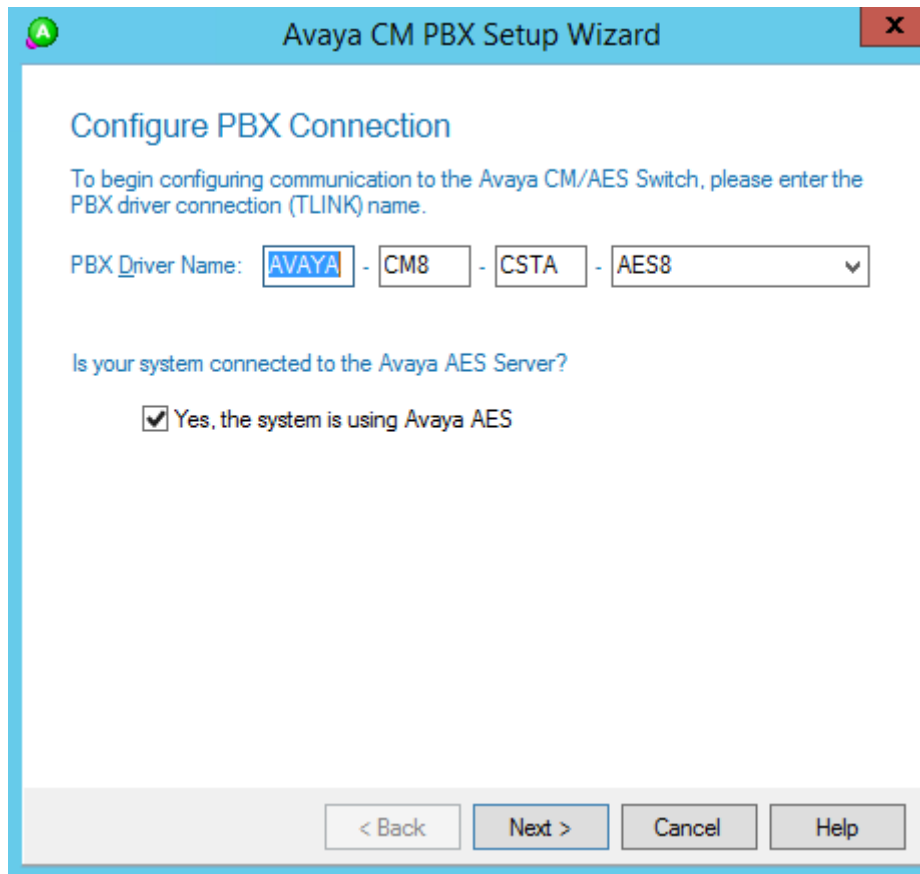
OK Cancel Help

## 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**

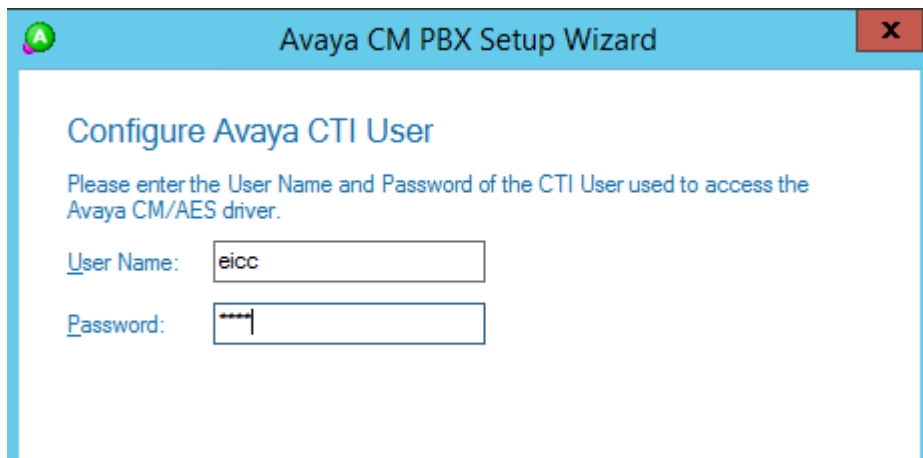


The **Avaya CM PBX Setup Wizard → Configure PBX Connection** screen is displayed. For **PBX Driver Name**, enter the Tlink name from **Section 6.10** as shown below. Retain the default value in the remaining field.



The screenshot shows the 'Configure PBX Connection' window of the Avaya CM PBX Setup Wizard. The title bar is blue with a green 'A' icon and a red 'X' button. The main area has a light blue header 'Configure PBX Connection' and a blue instruction: 'To begin configuring communication to the Avaya CM/AES Switch, please enter the PBX driver connection (TLINK) name.' Below this is a 'PBX Driver Name' field with four dropdown menus: 'AVAYA', 'CM8', 'CSTA', and 'AES8'. A checkbox labeled 'Yes, the system is using Avaya AES' is checked. At the bottom are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

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 'Configure Avaya CTI User' window of the Avaya CM PBX Setup Wizard. The title bar is blue with a green 'A' icon and a red 'X' button. The main area has a light blue header 'Configure Avaya CTI User' and a blue instruction: 'Please enter the User Name and Password of the CTI User used to access the Avaya CM/AES driver.' Below this are two input fields: 'User Name' with the text 'eicc' and 'Password' with four asterisks '\*\*\*\*'.

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

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

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:

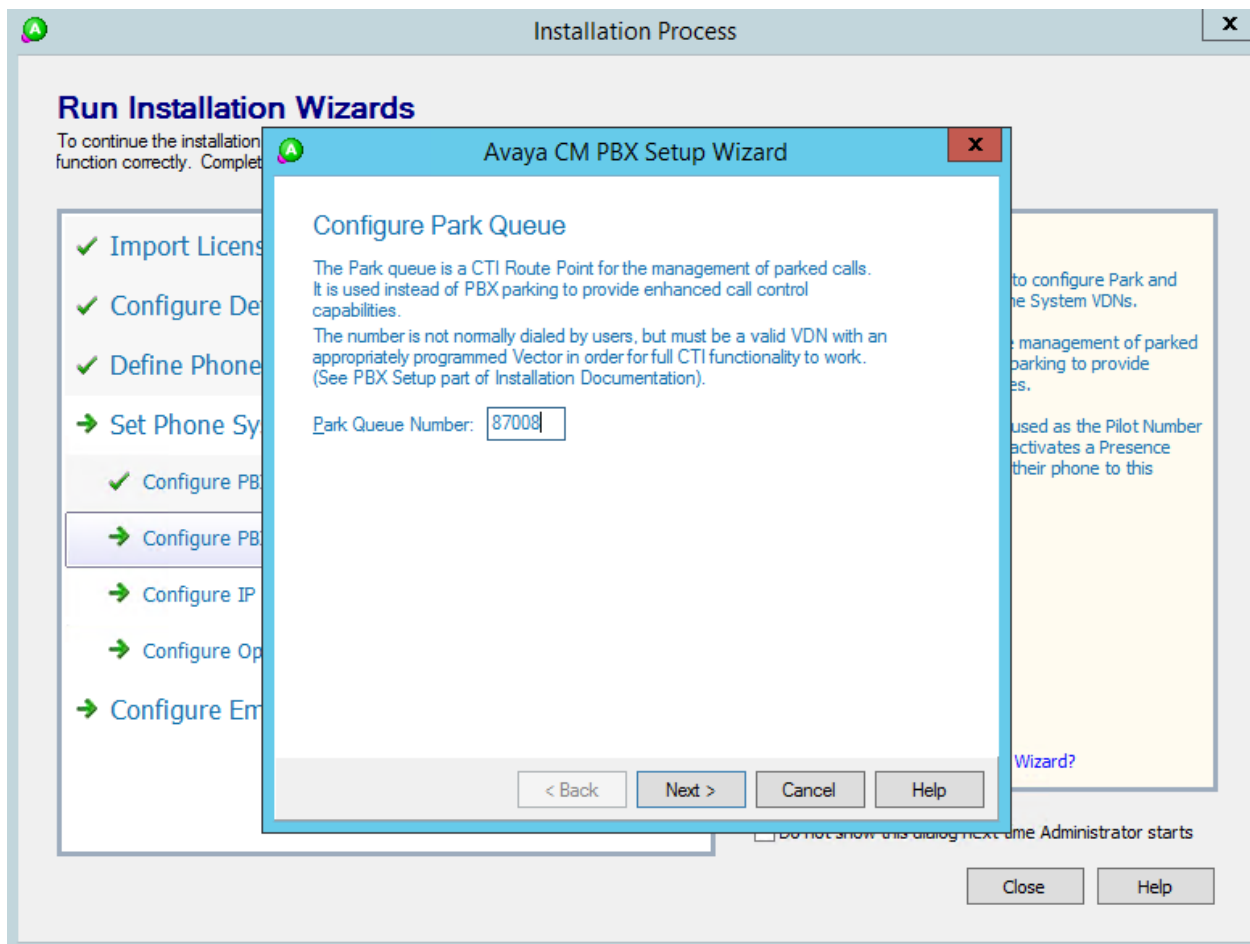
DMCC User:

DMCC Password:

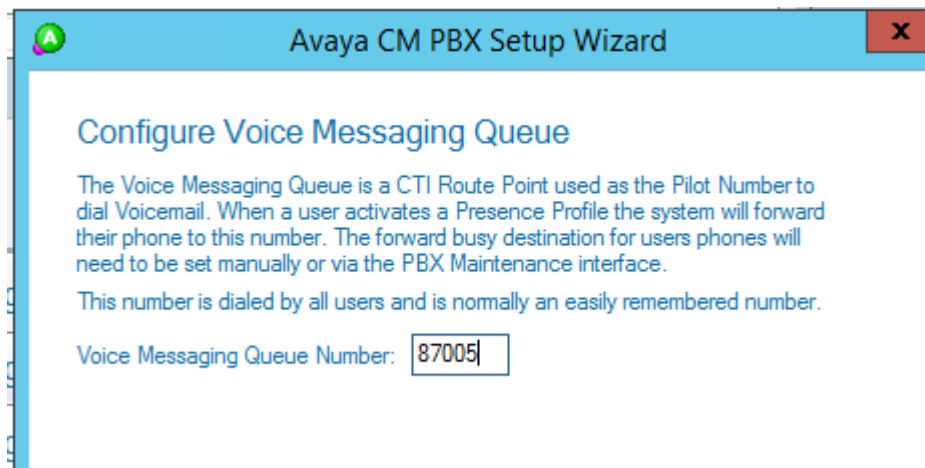
Global SoftPort Password:

< 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**.

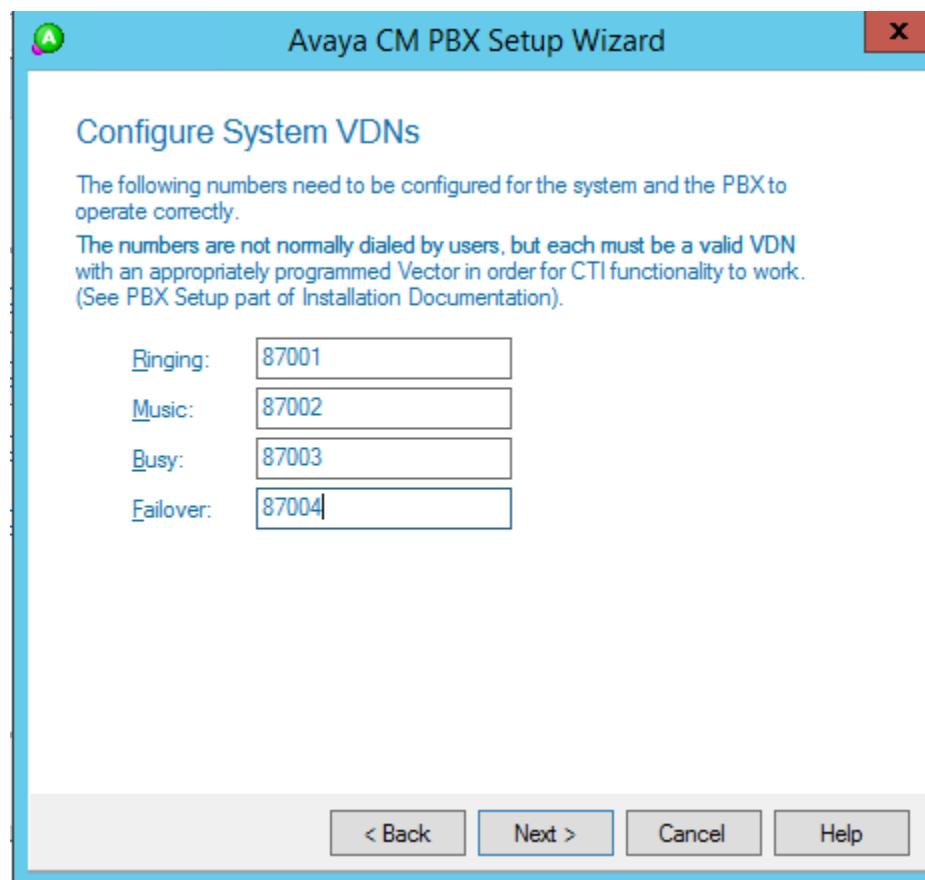


The **Avaya CM PBX Setup Wizard → Configure Voice Messaging Queue** screen is displayed next. For **Voice Messaging Queue Number**, enter the extension of the voicemail VDN from **Section 5.3.6**.



The screenshot shows a window titled "Avaya CM PBX Setup Wizard" with a close button (X) in the top right corner. The main heading is "Configure Voice Messaging Queue". Below the heading, 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. This number is dialed by all users and is normally an easily remembered number." Below this text, there is a label "Voice Messaging Queue Number:" followed by a text input field containing the value "87005".

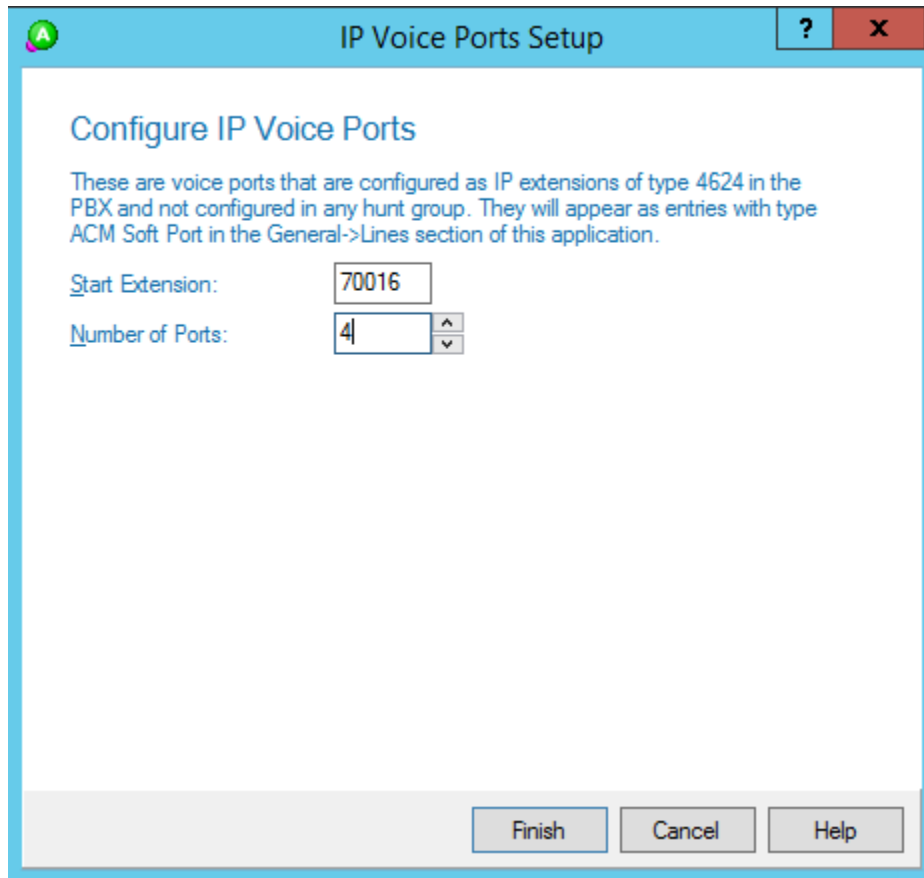
The **Avaya CM PBX Setup Wizard → Configure System VDNs** screen is displayed next. Enter the ring, music, busy, and failure VDNs from **Section 5.3** respectively, as shown below.



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, there are four labels with corresponding text input fields: "Ringing:" with value "87001", "Music:" with value "87002", "Busy:" with value "87003", and "Failover:" with value "87004". At the bottom of the window, there are four buttons: "< Back", "Next >", "Cancel", and "Help".

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 “4”.

Follow [5] to complete the Installation Wizard and subsequent CTI server setup via Application Manager.



**IP Voice Ports Setup**

### 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:

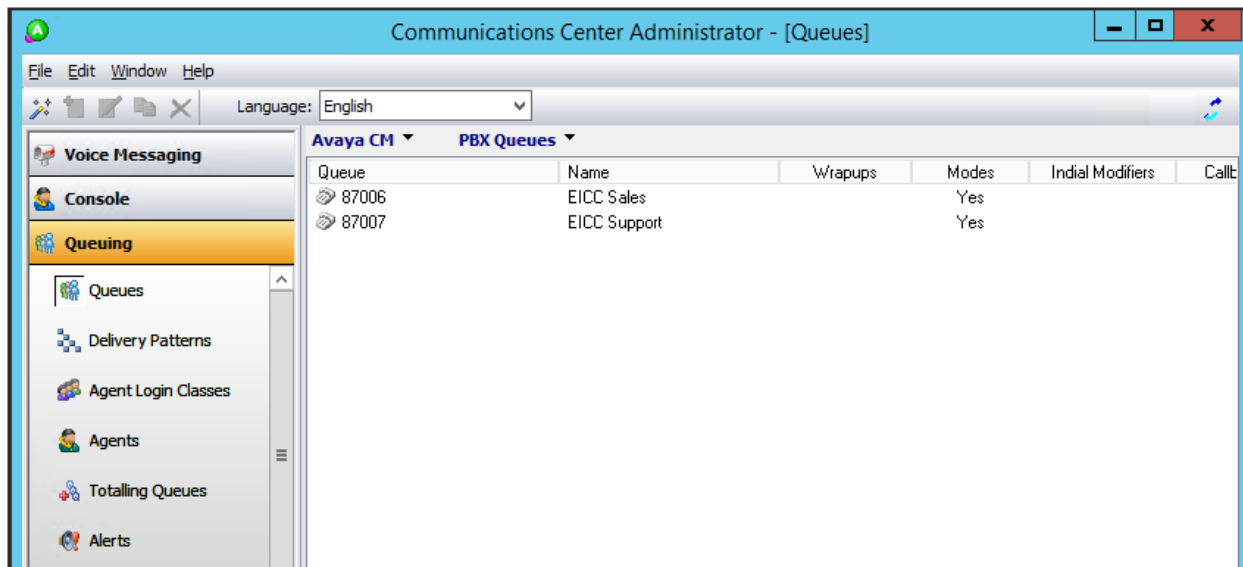
Number of Ports:  ^ v

### 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.



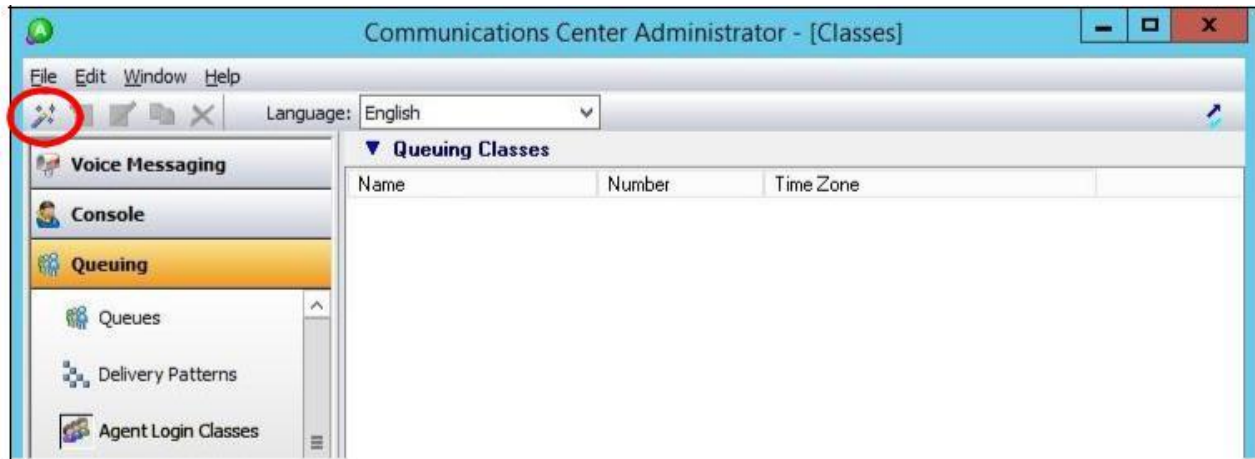
Follow the **Adding a New Queue Wizard** in the subsequent screens (not shown) to configure a new queue for each general routing VDN in **Section 5.3.2**. In the compliance testing, two queues were created as shown below.



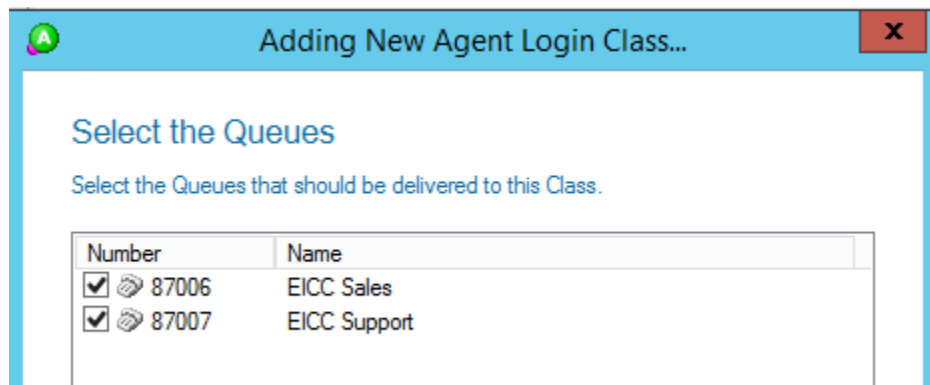


## 7.4.Administer Agent Login Class

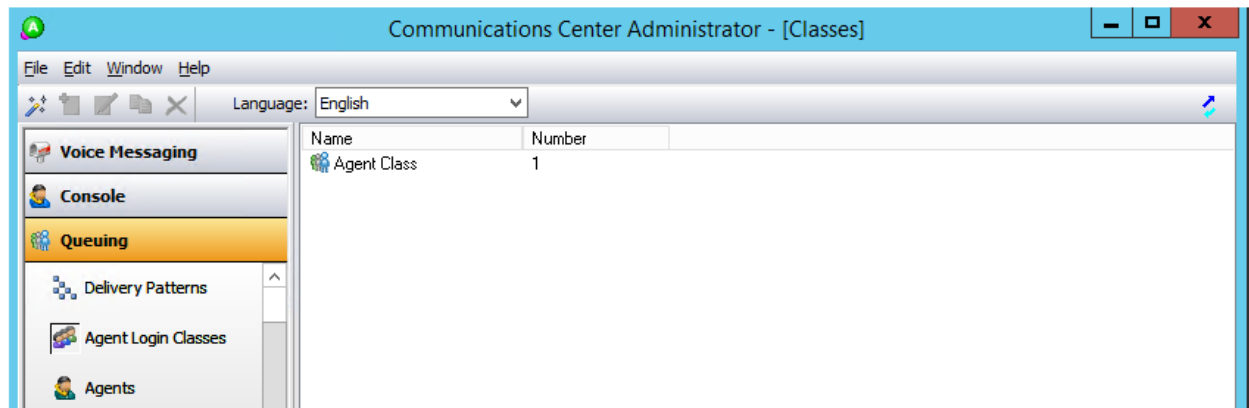
Select **Queuing** → **Agent login Classes** from the left pane, followed by the **Add Wizard** icon located at the upper left corner of the screen.



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

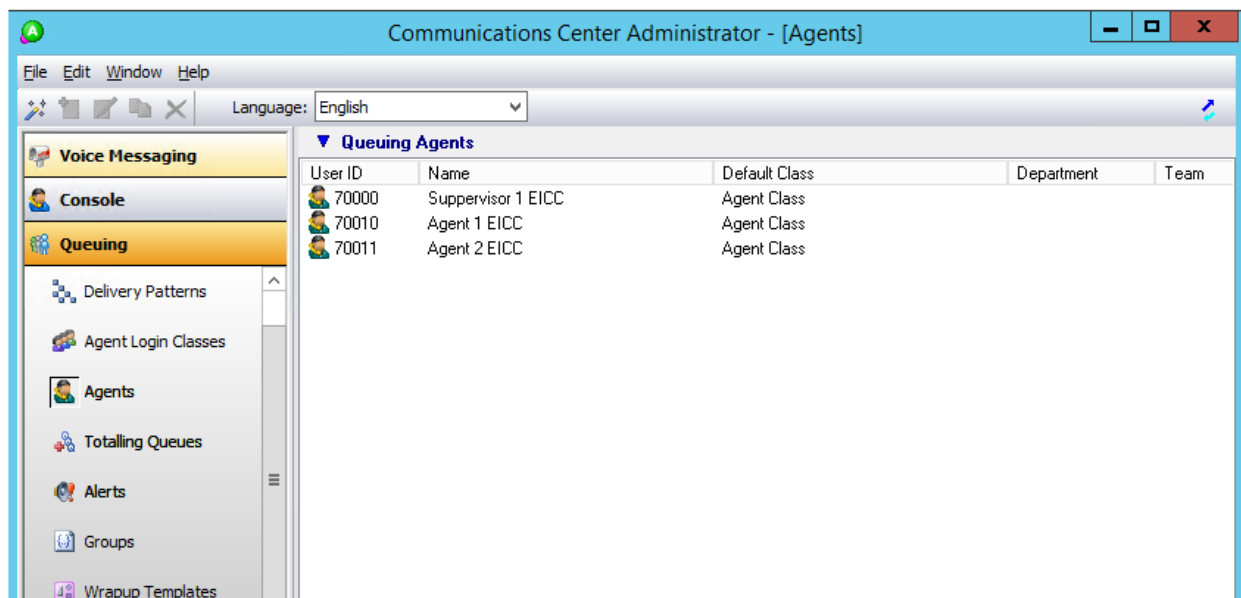
Select **Queuing** → **Agents** from the left pane, followed by the **Add Wizard** icon located at the upper left corner of the screen.



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.

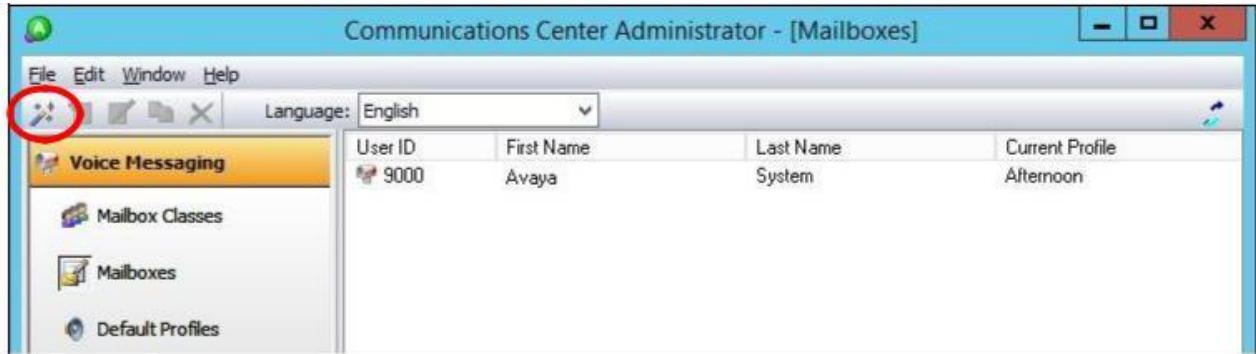


In the compliance testing, two agents and one supervisor were created.

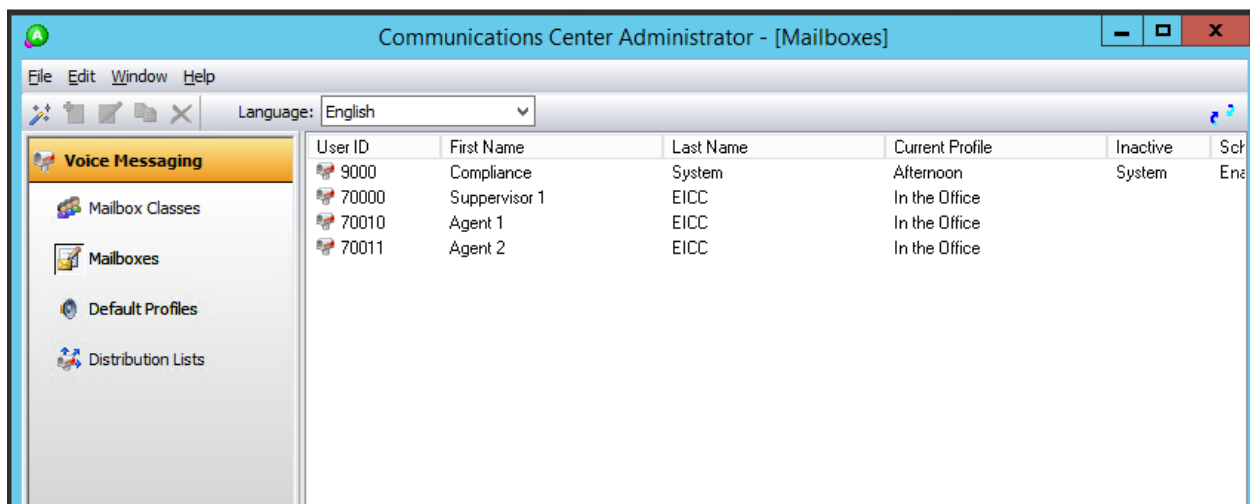


## 7.6.Administer Mailboxes

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.

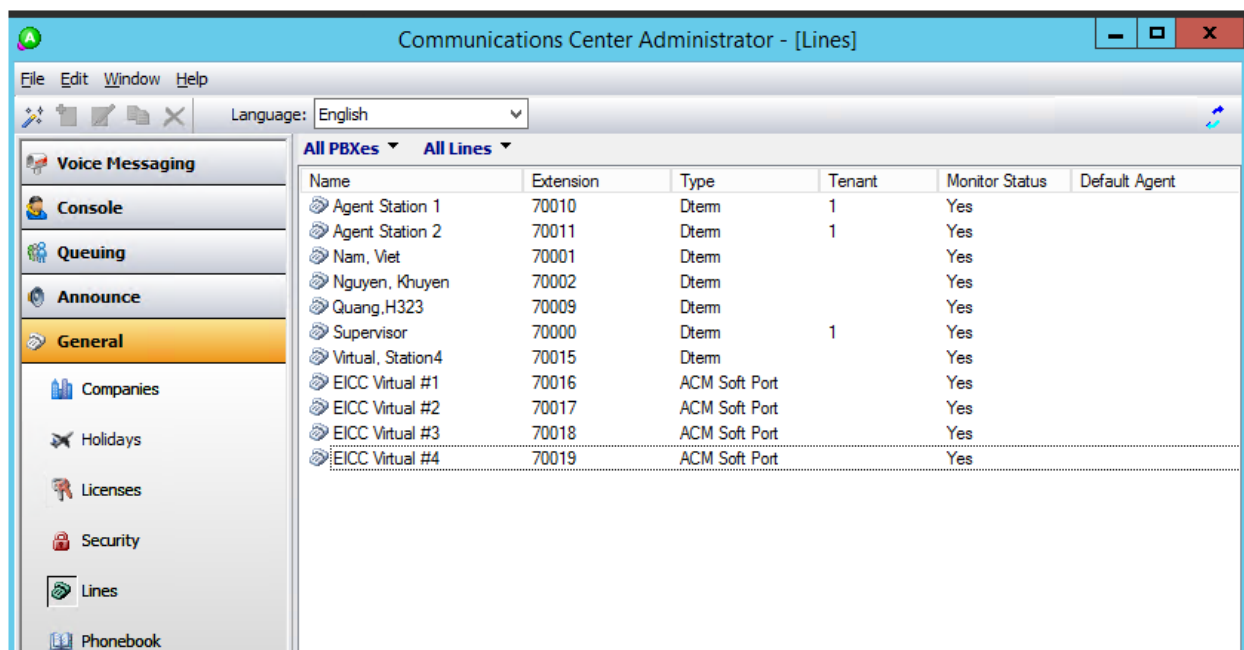


## 7.7.Administer Lines

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.



Name	Extension	Type	Tenant	Monitor Status	Default Agent
Agent Station 1	70010	Dterm	1	Yes	
Agent Station 2	70011	Dterm	1	Yes	
Nam, Viet	70001	Dterm		Yes	
Nguyen, Khuyen	70002	Dterm		Yes	
Quang, H323	70009	Dterm		Yes	
Supervisor	70000	Dterm	1	Yes	
Virtual, Station4	70015	Dterm		Yes	
EICC Virtual #1	70016	ACM Soft Port		Yes	
EICC Virtual #2	70017	ACM Soft Port		Yes	
EICC Virtual #3	70018	ACM Soft Port		Yes	
EICC Virtual #4	70019	ACM Soft Port		Yes	

## 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
<b>1</b>	<b>9</b>	<b>no</b>	<b>aes8</b>	<b>established</b>	<b>14</b>	<b>14</b>

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 Socket	Set Type/ Net Rgn	Prod ID/ Release	Station IP Address/ Gatekeeper IP Address
70000	9641	IP_Phone	10.128.224.59
tls	1	6.8002	10.30.5.93
70009	9620	IP_Phone	10.102.4.14
tcp	1	3.280A	10.30.5.93
70010	9641	IP_Phone	10.102.4.70
tls	1	6.8002	10.30.5.93
70011	9641	IP_Phone	10.102.4.71
tls	1	6.8002	10.30.5.93
<b>70016</b>	<b>4624</b>	<b>IP_API_A</b>	<b>10.30.5.95</b>
tcp	<b>1</b>	<b>3.2040</b>	<b>10.30.5.93</b>
<b>70017</b>	<b>4624</b>	<b>IP_API_A</b>	<b>10.30.5.95</b>
tcp	<b>1</b>	<b>3.2040</b>	<b>10.30.5.93</b>

## 8.1. 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 “7”.



**Application Enablement Services**  
Management Console

Welcome: User cust  
Last login: Tue Mar 26 15:40:17 2019 from 10.128.224.59  
Number of prior failed login attempts: 0  
HostName/IP: aes8.hcm.com/fe80::250:56ff:feb7:8ca7%eth2  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.0.1.0.0.5-0  
Server Date and Time: Tue Mar 26 15:49:11 ICT 2019  
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

▶ Logs

▶ Log Manager

▼ Status and Control

▶ CVLAN Service Summary

▶ DLG Services Summary

▶ DMCC Service Summary

▶ Switch Conn Summary

▶ TSAPI Service Summary

▶ User Management

▶ Utilities

▶ Help

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	CM8	1	Talking	Tue Mar 26 18:48:36 2019	Online	18	7	8	8	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 cust  
 Last login: Tue Mar 26 15:40:17 2019 from 10.128.224.59  
 Number of prior failed login attempts: 0  
 HostName/IP: aes8.hcm.com/fe80::250:56ff:feb7:8ca7%eth2  
 Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
 SW Version: 8.0.1.0.0.5-0  
 Server Date and Time: Tue Mar 26 15:49:11 ICT 2019  
 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

▶ Logs

▶ Log Manager

▼ Status and Control

■ CVLAN Service Summary

■ DLG Services Summary

■ **DMCC Service Summary**

■ Switch Conn Summary

■ TSAPI Service Summary

▶ User Management

▶ Utilities

▶ Help

### DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)  
 Generated on Wed Mar 27 18:17:21 ICT 2019  
 Service Uptime: 0 days, 1 hours 10 minutes  
 Number of Active Sessions: 4  
 Number of Sessions Created Since Service Boot: 57  
 Number of Existing Devices: 4  
 Number of Devices Created Since Service Boot: 50

☐	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
☐	3519F917F84279A05 52436AC901C61FB-53	CCT		10.128.224.162	XML Unencrypted	1
☐	2D2F40D90EEA23846 D51B57A58301891-56	CCT		10.128.224.162	XML Unencrypted	1
☐	C1636002424BB2414 8AA218F0D99A366-54	CCT		10.128.224.162	XML Unencrypted	1
☐	D3C4743D9B4B28F73 0C436753B6DAA8B-55	CCT		10.128.224.162	XML Unencrypted	1

Terminate Sessions
Show Terminated Sessions

Item 1-4 of 4  
1 Go

Copyright © 2009-2018 Avaya Inc. All Rights Reserved.



## 8.2. Verify Enghouse Interactive Communications Center

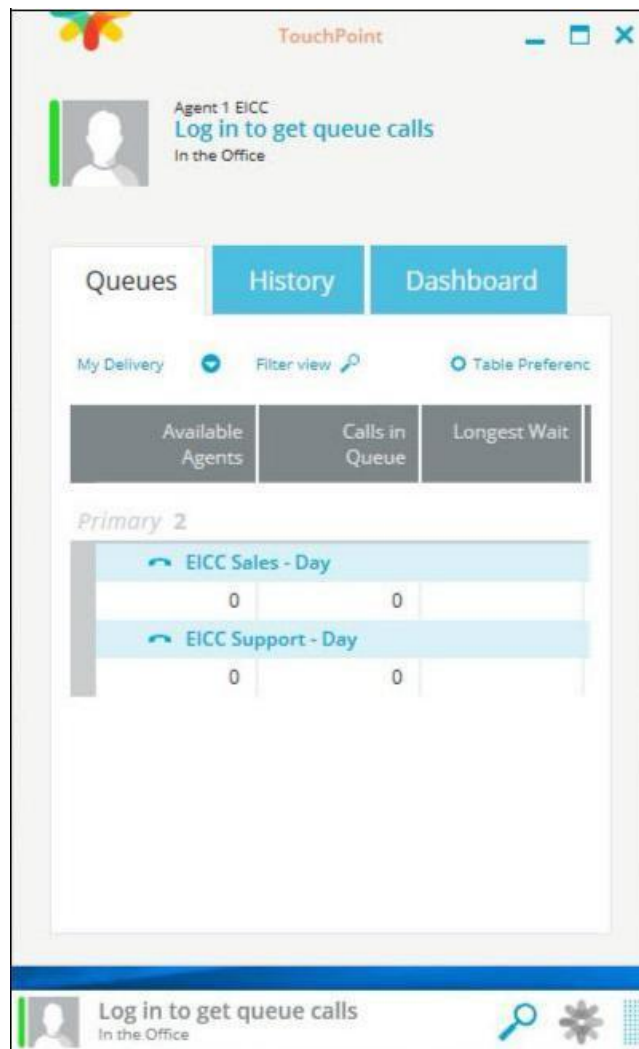
From the agent desktop, double-click on the **TouchPoint** shortcut icon shown below, which was created as part of TouchPoint installation.



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.

The login screen for Enghouse Interactive TouchPoint. It has a white background with a large, colorful flower logo at the top center. Below the logo, the text 'Enghouse Interactive TouchPoint' is displayed in a large, black, sans-serif font. There are two input fields: the first is labeled 'Agent 1 EICC' and contains the text 'Agent 1 EICC'; the second is a password field with four black dots. Below the password field is a checkbox labeled 'Remember me' which is checked. At the bottom center is a blue button with the text 'Open TouchPoint'. A small blue 'X' icon is in the top right corner of the window.

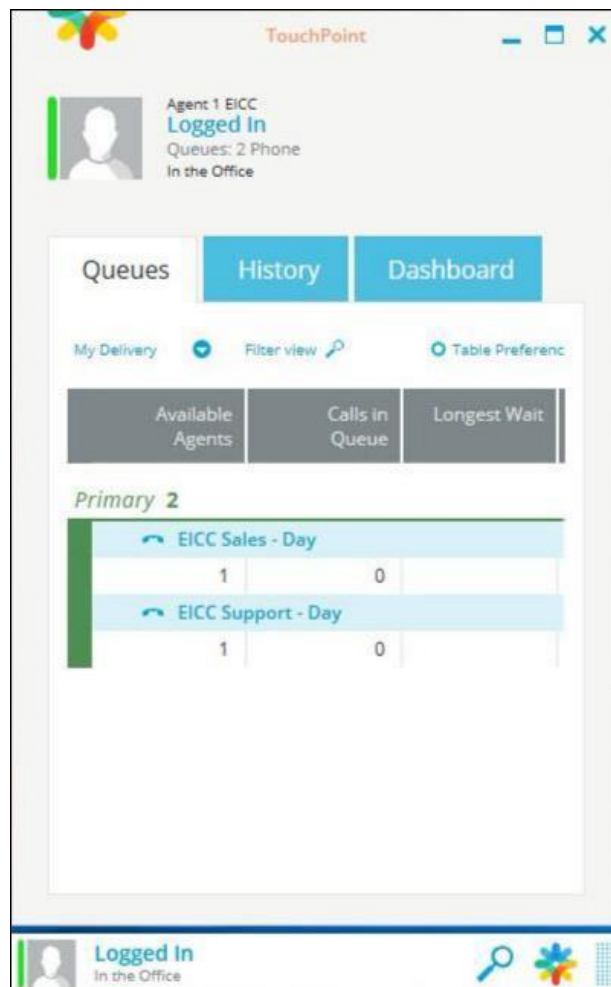
The main **TouchPoint** screen, also referred to as the Statistics Window is displayed, along with a Call Bar above the system tray, as shown below. From the Statistics Window, click on **Log in to get queue calls** toward the top of the screen.



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.



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 10.1 to successfully interoperate with Avaya Aura® Communication Manager 8.0 using Avaya Aura® Application Enablement Services 8.0. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

## 10. Additional References

This section references the Avaya and Enghouse Interactive product documentation that are relevant to these Application Notes.

Product documentation for Avaya products may be found at <http://support.avaya.com>.

1. *Administering Avaya Aura® Communication Manager, Release 8, Issue 2.0, Nov 2018*
2. *Administering Avaya Aura® Session Manager, Release 8, Issue 2, August 2018*
3. *Administering Avaya Aura® System Manager, Release 8, Issue 4, September 2018*
4. *Administering Avaya Aura® Application Enablement Services, Release 8.0.1, Issue 2, December 2018*

Product documentation for Enghouse Interactive Communication Center may be found at <http://www.enghouseinteractive.com>

5. *PBX Programming Manual - Avaya Communication Manager Installation Manual CC 10.1, August 2018*

---

**©2019 Avaya Inc. All Rights Reserved.**

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

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