



**Application Notes for Interactrm Customer Experience Platform (ICX) Contact Center with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services – Issue 1.0**

**Abstract**

These Application Notes describe the configuration steps required for Interactrm Customer Experience Platform (ICX) Contact Center to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. ICX Contact Center is a desktop CTI application.

In the compliance testing, ICX Contact Center used the Java Telephony Application Programming Interface from Avaya Aura® Application Enablement Services to monitor contact center agents on Avaya Aura® Communication Manager, to provide screen pop and call control from the web-based agent desktops.

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 Interactrm Customer Experience Platform (ICX) Contact Center to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. Contact Center is a desktop CTI application, and an optional component of ICX.

In the compliance testing, Contact Center used the Java Telephony Application Programming Interface (JTAPI) from Avaya Aura® Application Enablement Services to monitor contact center agents on Avaya Aura® Communication Manager, to provide screen pop and call control from web-based agent desktops.

JTAPI is a client-side interface to the Telephony Services Application Programmer Interface (TSAPI) on Avaya Aura® Application Enablement Services. As such, these Application Notes will describe the required configurations for creation and connectivity to the TSAPI service.

# 2. General Test Approach and Test Results

The feature test cases were performed manually. Incoming calls were placed to the VDNs on Communication Manager with available agents. Manual call controls from the agent desktops with web-based connection to Contact Center were exercised to verify proper call handling such as transfer and conference.

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

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

## 2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on Contact Center:

- Handling of JTAPI/TSAPI messages in the areas of event notifications, value queries, and set agent states.
- Use of JTAPI/TSAPI call control services to support call control actions such as answer and transfer from the agent desktops.
- Proper handling of call scenarios involving inbound, outbound, internal, external, ACD, non-ACD, screen pop, drop, hold/resume, multiple calls, multiple agents, conference, transfer, long duration, pending work mode, and reason codes.

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

## 2.2. Test Results

All test cases were executed, and the following were observations on Contact Center:

- In general, mixed use of agent desktop and telephone to perform call control actions are supported. For the transfer and conference features, however, all actions need to start and complete from the same source.
- The application does not support TSAPI user credentials that contained the special character semicolon.
- In the conference scenario, after one of the other parties drop from the conference, the conference-from agent desktop will continue to show the Outgoing Conference dialog box until the end of the call.
- Toggling between two calls is not supported by the desktop by design, and the workaround is to use the telephone instead.
- When an active call stayed up at an agent during a brief disruption to the server or desktop LAN connection, the desktop browser window will disappear upon recovery, and the agent needs to log back into Contact Center after manually dropping the active call.
- Upon terminating a personal or internal call, the Wrap Up tab automatic comes to the foreground as in the case with ACD calls.

## 2.3. Support

Technical support on Contact Center can be obtained through the following:

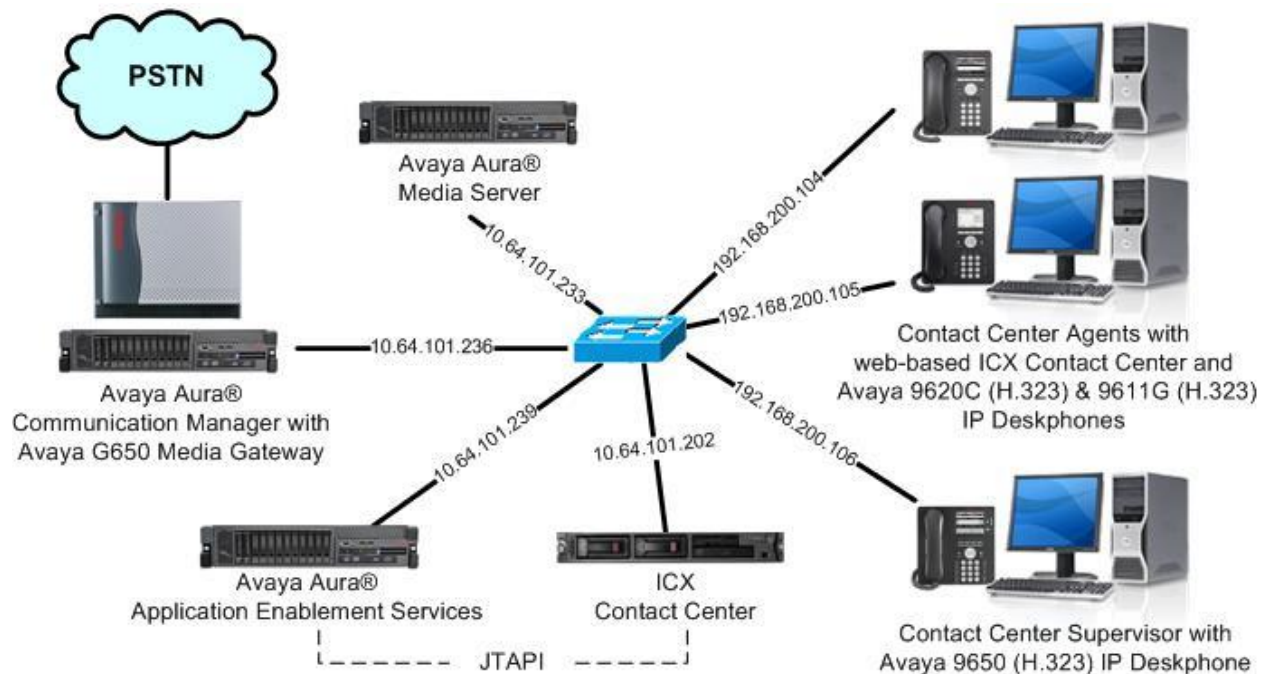
- **Phone:** (510) 795-7645
- **Email:** [usa@interactcrm.com](mailto:usa@interactcrm.com)

### 3. Reference Configuration

Contact Center can be configured on a single server or with components distributed across multiple servers. The compliance test configuration used a single server configuration, as shown in **Figure 1**.

The detailed administration of basic connectivity between Communication Manager and Application Enablement Services, and of contact center devices are not the focus of these Application Notes and will not be described. The contact center devices used in the compliance testing are shown in the table below.

Device Type	Extension
VDN	60001, 60002
Skill Group	61001, 61002
Supervisor	65000
Agent Station	65001, 66002
Agent ID	65881, 65882
Agent Password	65881, 65882



**Figure 1: Compliance Testing Configuration**

## 4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya Aura® Communication Manager in Virtual Environment	7.0.1 (7.0.1.0.0.441.23012)
Avaya G650 Media Gateway	NA
Avaya Aura® Media Server in Virtual Environment	7.7.0.334
Avaya Aura® Application Enablement Services in Virtual Environment	7.0.1 (7.0.1.0.1.15)
Avaya 9620C & 9650 IP Deskphones (H.323)	3.260A
Avaya 9611G IP Deskphone (H.323)	6.6115
ICX on Windows Server 2012 R2 Standard <ul style="list-style-type: none"><li>Interaction Manager</li><li>Avaya JTAPI Windows Client (ecsjtapia.jar)</li></ul>	3.0.16 (Build 118) NA 6.3.0.3 (Build 46) 6.2.9200

## 5. Configure Avaya Aura® Communication Manager

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

- Verify license
- Administer CTI link
- Administer system parameters features
- Obtain VDN names
- Obtain reason codes

### 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	<b>Computer Telephony Adjunct Links?</b>	<b>y</b>		
ARS/AAR Partitioning?	y	Cvg Of Calls Redirected Off-net?	y		
ARS/AAR Dialing without FAC?	n	DCS (Basic)?	y		
ASAI Link Core Capabilities?	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				

### 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: 60111</b>					
<b>Type: ADJ-IP</b>					
<b>Name: AES CTI Link</b>					
COR: 1					

### 5.3. Administer System Parameters Features

Use the “change system-parameters features” command to enable **Create Universal Call ID (UCID)**, which is located on **Page 5**. For **UCID Network Node ID**, enter an available node ID.

```
change system-parameters features                                     Page 5 of 19
                           FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS
  Endpoint:                  Lines Per Page: 60

SYSTEM-WIDE PARAMETERS
  Switch Name:
  Emergency Extension Forwarding (min): 10
  Enable Inter-Gateway Alternate Routing? n
  Enable Dial Plan Transparency in Survivable Mode? n
  COR to Use for DPT: station
  EC500 Routing in Survivable Mode: dpt-then-ec500
MALICIOUS CALL TRACE PARAMETERS
  Apply MCT Warning Tone? n    MCT Voice Recorder Trunk Group:
  Delay Sending RElease (seconds): 0
SEND ALL CALLS OPTIONS
  Send All Calls Applies to: station    Auto Inspect on Send All Calls? n
  Preserve previous AUX Work button states after deactivation? n
UNIVERSAL CALL ID
  Create Universal Call ID (UCID)? y    UCID Network Node ID: 27
```

Navigate to **Page 13**, and enable **Send UCID to ASAI**. This parameter allows for the universal call ID to be sent to Contact Center.

```
change system-parameters features                                     Page 13 of 19
                           FEATURE-RELATED SYSTEM PARAMETERS

CALL CENTER MISCELLANEOUS
  Callr-info Display Timer (sec): 10
  Clear Callr-info: next-call
  Allow Ringer-off with Auto-Answer? n

  Reporting for PC Non-Predictive Calls? n

  Agent/Caller Disconnect Tones? n
  Interruptible Aux Notification Timer (sec): 3
  Zip Tone Burst for Callmaster Endpoints: double

ASAI
  Copy ASAI UI During Conference/Transfer? y
  Call Classification After Answer Supervision? y
  Send UCID to ASAI? y
  For ASAI Send DTMF Tone to Call Originator? y
  Send Connect Event to ASAI For Announcement Answer? n
  Prefer H.323 Over SIP For Dual-Reg Station 3PCC Make Call? n
```



## 5.4. Obtain VDN Names

Use the “list vdn” command to display a list of pre-configured VDNs. Make a note of the **Name** for each VDNs from **Section 3**, which will be used later to configure Contact Center. In the compliance testing, the two VDNs shown below were used.

list vdn								Page	1
VECTOR DIRECTORY NUMBERS									
Name (22 characters)	Ext/Skills	VDN Ovr	COR	TN	Vec PRT	Num	Meas	Orig Annc	Evt Noti Adj
<b>ICX Sales</b>	<b>60001</b>	n	1	1	V	1	none		
<b>ICX Support</b>	<b>60002</b>	n	1	1	V	2	none		

## 5.5. Obtain Reason Codes

For contact centers that use reason codes for aux work, enter the “display reason-code-names” command to display the configured reason codes. Make a note of the reason codes for aux work, which will be used later to configure Contact Center.

display reason-code-names

Page 1 of 1

REASON CODE NAMES

Aux Work/  
Interruptible?

Logout

Reason Code 1: **Meeting**

/n

Reason Code 2: **Lunch**

/n

Reason Code 3:

/n

Reason Code 4:

/n

Reason Code 5:

/n

Reason Code 6:

/n

Reason Code 7:

/n

Reason Code 8:

/n

Reason Code 9:

/n

Default Reason Code:

## 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 ICX user
- Administer security database
- Restart TSAPI service
- 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. In the center, there is a light gray rectangular box containing the login form. The form has the text "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 at the bottom of the page, above the footer text.

AVAYA

**Application Enablement Services**  
Management Console

Please login here:

Username

Password

Login Reset

Copyright © 2009-2016 Avaya Inc. All Rights Reserved.

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

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title "Application Enablement Services Management Console". On the right, a welcome message for the user is shown, including login details and system status. 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, titled "Welcome to OAM", provides an overview of the OAM web interface and lists administrative domains: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. It also mentions that these domains can be managed by a single administrator or separate administrators.

Welcome: User  
Last login: Thu Jun 2 08:41:17 2016 from 192.168.200.20  
Number of prior failed login attempts: 0  
HostName/IP: aes7/10.64.101.239  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 7.0.1.0.1.15-0  
Server Date and Time: Thu Jun 02 09:03:12 EDT 2016  
HA Status: Not Configured

Home | Help | Logout

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

### Welcome to OAM

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

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

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

## 6.2. Verify License

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

The screenshot displays the Avaya Application Enablement Services Management Console with the "Licensing" section selected in the left sidebar. The main content area, titled "Licensing", provides instructions on how to set up and maintain the WebLM, including the need to use the following: WebLM Server Address, WebLM Server Access, and Reserved Licenses. It also mentions that if you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following: Reserved Licenses.

Welcome: User  
Last login: Thu Jun 2 08:41:17 2016 from 192.168.200.20  
Number of prior failed login attempts: 0  
HostName/IP: aes7/10.64.101.239  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 7.0.1.0.1.15-0  
Server Date and Time: Thu Jun 02 09:03:12 EDT 2016  
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**, as shown below.

**AVAYA**  
 Aura® System Manager 7.0

Last Logged on at: June 2, 2016 9:09 AM  
 GO... Log off

Home
 Licenses

WebLM Home  
 Install license  
 Licensed products  
 APPL\_ENAB  
 Application Enablement  
   View license capacity  
   View peak usage  
 COMMUNICATION\_MANAGER  
   Communication\_Manager  
   Call\_Center  
   Configure Centralized Licensing  
 MSR  
   Media\_Server  
 SessionManager  
   SessionManager  
 Uninstall license  
 Server properties  
 Shortcuts  
 Help for Installed Product

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

You are here: Licensed Products > Application\_Enablement > View License Capacity  
  
 License installed on: October 12, 2015 3:21:49 PM -04:00  
  

**License File Host IDs:**
V1-19-37-80-8F-BF

**Licensed Features**

10 Items
 Show All

Feature (License Keyword)	Expiration date	Licensed capacity
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	1000
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	3
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	16
Product Notes VALUE_NOTES	permanent	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiS MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_ LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;u TrustedApplications: IPS_001, BasicUnrestrict DMCUnrestricted; IXP_001, BasicUnrestricted, DMCUnrestricted; IXM_001, BasicUnrestricted, DMCUnrestricted; PC_001, BasicUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted, DMCUnrestricted; OSCP_001, BasicUnrestricted, DMCUnrestricted; VP_001, BasicUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AEC CCE_001, BasicUnrestricted, AdvancedUnrestrict CSI_T1_001, BasicUnrestricted, AdvancedUnr CSI_T2_001, BasicUnrestricted, AdvancedUnr AVAYAVERINT_001, BasicUnrestricted, Advan DMCUnrestricted; CCT_ELITE_CALL_CTRL_001 AdvancedUnrestricted, DMCUnrestricted, Ager BasicUnrestricted, AdvancedUnrestricted, DMC AgentEvents; UNIFIED_DESKTOP_001, BasicU AdvancedUnrestricted, DMCUnrestricted, Ager BasicUnrestricted, AdvancedUnrestricted, DMC
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	3
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	1000
DLG VALUE_AES_DLG	permanent	16
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	1000
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	3

### 6.3. Administer TSAPI Link

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

The screenshot shows the Avaya Application Enablement Services Management Console. The top right corner displays user information: Welcome: User, Last login: Thu Jun 2 08:41:17 2016 from 192.168.200.20, Number of prior failed login attempts: 0, HostName/IP: aes7/10.64.101.239, Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE, SW Version: 7.0.1.0.1.15-0, Server Date and Time: Thu Jun 02 09:03:12 EDT 2016, HA Status: Not Configured. The left navigation pane shows 'AE Services' expanded, with 'TSAPI' selected, and 'TSAPI Links' highlighted. The main content area is titled 'TSAPI Links' and contains a table with columns: Link, Switch Connection, Switch CTI Link #, ASAI Link Version, and Security. Below the table are buttons for 'Add Link', 'Edit Link', and 'Delete Link'.

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

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

The screenshot shows the 'Add TSAPI Links' screen in the Avaya Application Enablement Services Management Console. The left navigation pane is the same as the previous screenshot, with 'Communication Manager Interface' now visible below 'TSAPI Links'. The main content area is titled 'Add TSAPI Links' and contains form fields for: Link (dropdown with value 1), Switch Connection (dropdown with value cm7), Switch CTI Link Number (dropdown with value 1), ASAI Link Version (dropdown with value 7), and Security (dropdown with value Unencrypted). At the bottom are buttons for 'Apply Changes' and 'Cancel Changes'.



## 6.4. Administer ICX 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: Thu Jun 2 08:41:17 2016 from 192.168.200.20  
Number of prior failed login attempts: 0  
HostName/IP: aes7/10.64.101.239  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 7.0.1.0.1.15-0  
Server Date and Time: Thu Jun 02 09:31:00 EDT 2016  
HA Status: Not Configured

User Management | User Admin | Add User

Home | 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

Home Phone

## 6.5. 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. Make certain **Enable SDB for TSAPI Service, JTAPI and Telephony Web Services** is unchecked, as shown below.

In the event that the security database is used by the customer with parameter already enabled, then follow reference [2] to configure access privileges for the ICX user from **Section 6.4**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title "Application Enablement Services Management Console". A welcome message and system information are shown in the top right corner. The main navigation pane on the left lists various services, with "Security" expanded to show "Security Database" and "Control" selected. The main content area displays the "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" configuration page, which includes two unchecked checkboxes and an "Apply Changes" button.

Welcome: User  
Last login: Thu Jun 2 08:41:17 2016 from 192.168.200.20  
Number of prior failed login attempts: 0  
HostName/IP: aes7/10.64.101.239  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 7.0.1.0.1.15-0  
Server Date and Time: Thu Jun 02 09:03:12 EDT 2016  
HA Status: Not Configured

Security | Security Database | Control Home | Help | Logout

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

SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services

☐ Enable SDB for DMCC Service  
☐ Enable SDB for TSAPI Service, JTAPI and Telephony Web Services  
Apply Changes

## 6.6. Restart TSAPI Service

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

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title "Application Enablement Services Management Console". A welcome message in the top right corner states: "Welcome: User", "Last login: Thu Jun 2 08:41:17 2016 from 192.168.200.20", "Number of prior failed login attempts: 0", "HostName/IP: aes7/10.64.101.239", "Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE", "SW Version: 7.0.1.0.1.15-0", "Server Date and Time: Thu Jun 02 09:03:12 EDT 2016", and "HA Status: Not Configured".

The main interface features a left-hand navigation pane with the following menu items: "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance" (selected), "Date Time/NTP Server", "Security Database", "Service Controller" (highlighted), "Server Data", "Networking", "Security", and "Status".

The right-hand pane, titled "Service Controller", contains a table with two columns: "Service" and "Controller Status". The table lists several services, all of which are in a "Running" state. The "TSAPI Service" is checked with a checkbox.

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input type="checkbox"/> DMCC Service	Running
<input type="checkbox"/> CVLAN Service	Running
<input type="checkbox"/> DLG Service	Running
<input type="checkbox"/> Transport Layer Service	Running
<input checked="" type="checkbox"/> TSAPI Service	Running

Below the table, a note states: "For status on actual services, please use [Status and Control](#)". At the bottom of the pane, there is a row of buttons: "Start", "Stop", "Restart Service", "Restart AE Server", "Restart Linux", and "Restart Web Server".



## 6.7. 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 Contact Center.

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

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The main navigation bar shows "Security | Security Database | Tlinks" and links for "Home | Help | Logout". The left sidebar contains a tree view of the application's structure, with "Security" expanded to show "Security Database" and "Tlinks" selected. The main content area, titled "Tlinks", shows a single Tlink named "AVAYA#CM7#CSTA#AES7" with a "Delete Tlink" button.

Welcome: User  
Last login: Thu Jun 2 08:41:17 2016 from 192.168.200.20  
Number of prior failed login attempts: 0  
HostName/IP: aes7/10.64.101.239  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 7.0.1.0.1.15-0  
Server Date and Time: Thu Jun 02 09:03:12 EDT 2016  
HA Status: Not Configured

Security | Security Database | Tlinks Home | Help | Logout

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

Tlinks  
Tlink Name  
AVAYA#CM7#CSTA#AES7  
Delete Tlink

## 7. Configure ICX Contact Center

This section provides the procedures for configuring Contact Center. The procedures include the following areas:

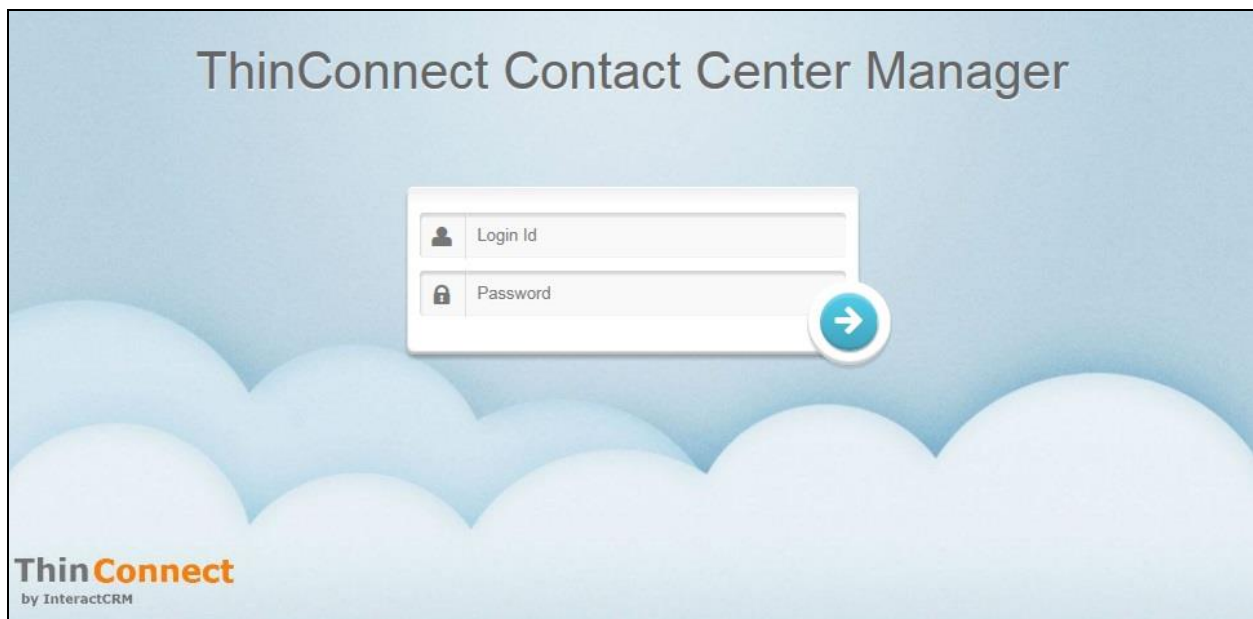
- Launch web interface
- Administer server
- Administer agents
- Administer queues
- Administer aux codes

The configuration of Contact Center is performed by Interactcrm implementation specialists. The procedural steps are presented in these Application Notes for informational purposes.

### 7.1. Launch Web Interface

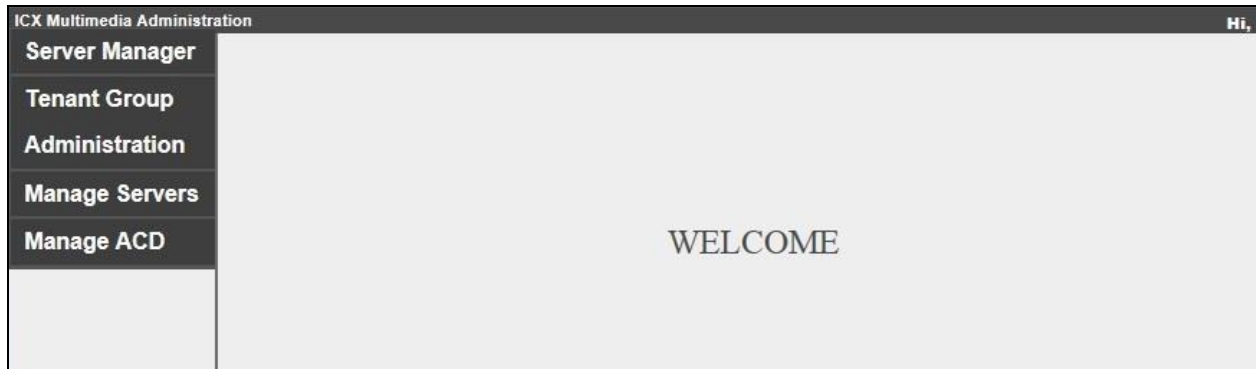
Launch the web interface by using the URL “http://ip-address:15050/ContactCenterManager” in an Internet Explorer browser window, where “ip-address” is the IP address of the ICX server running the Contact Center Manager component.

The **ThinConnect Contact Center Manager** screen below is displayed. Log in using the appropriate credentials.

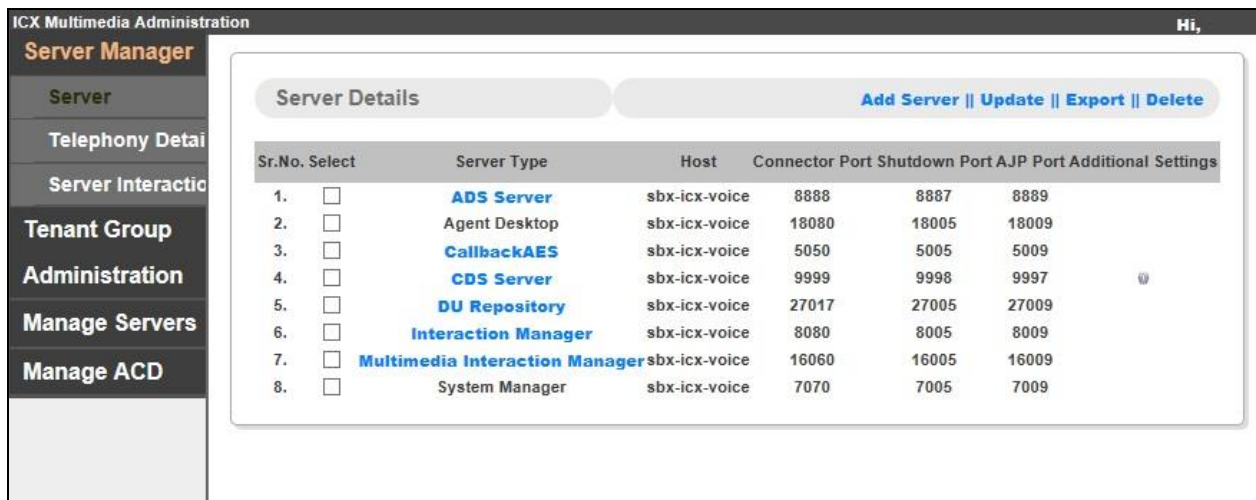


## 7.2. Administer Server

The **WELCOME** screen below is displayed



Select **Server Manager** → **Server** from the left pane, to display the **Server Details** screen.  
Click on the **Interaction Manager** entry.



The **Edit Server** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

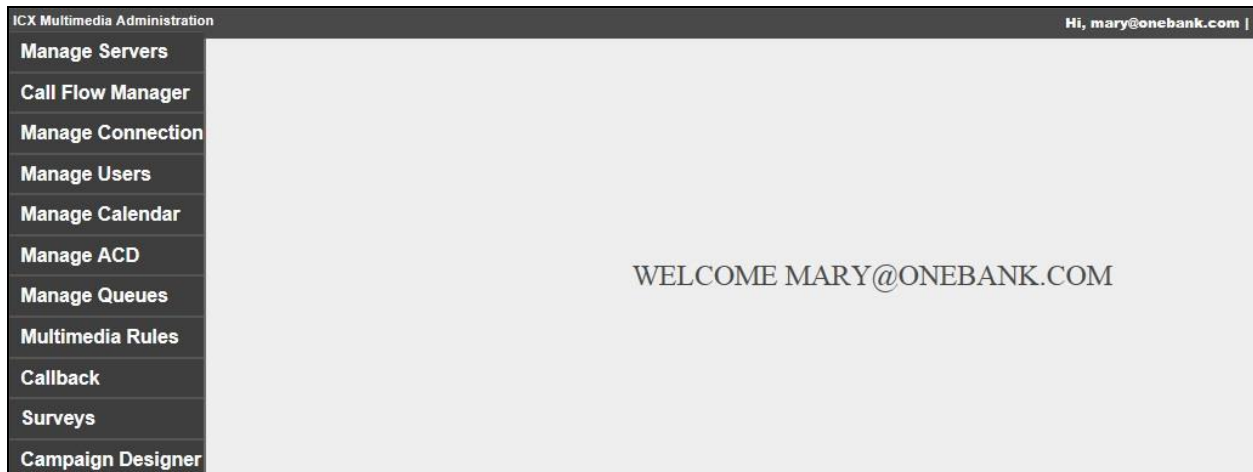
- **AES Host Name:** IP address of Application Enablement Services.
- **AES User Name:** The ICX user credentials from **Section 6.4**.
- **AES Password:** The ICX user credentials from **Section 6.4**.
- **TS Link String:** The Tlink name from **Section 6.7**.

ICX Multimedia Administration		Hi,
<b>Server Manager</b>		
Server	<b>Edit Server</b>	
Telephony Details		
Server Interaction		
Tenant Group		
Administration		
Manage Servers		
Manage ACD		
	SDK Path *	MIS
	AES Host Name *	10.64.101.239
	AES Port *	450
	AES User Name *	ICXicx123#
	AES Password *	ICXicx123#
	TS Link String *	AVAYA#CM7#CSTA#AES7
	Debug Level *	4
	Trace File Location *	L:\Interaction Manager\VIMTrac
	Heart Beat Interval in Telephony for AES *	40
	Max QM communicator thread count *	10
	Max QM communicator worker count *	10
	QM communicator sleep time *	10
	Is CDS Server Enabled *	1
	Enable Outbound Dialer *	0
	Outbound Dialer URL *	http://localhost
	Max Idle Timeout for web socket *	28800000
	Session Restore Timeout for web socket *	180000
	Thread Time interval for web socket *	5000
	Protocol *	http
	Is Voice Only Deployment *	1
	Enable Password Encryption *	0
	Agent Job Status Check Interval(Min) *	5
	Initial Batch Size *	75
	Next Batch Size *	25
	Normal Ceiling *	150
	Max Ceiling *	200
	<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

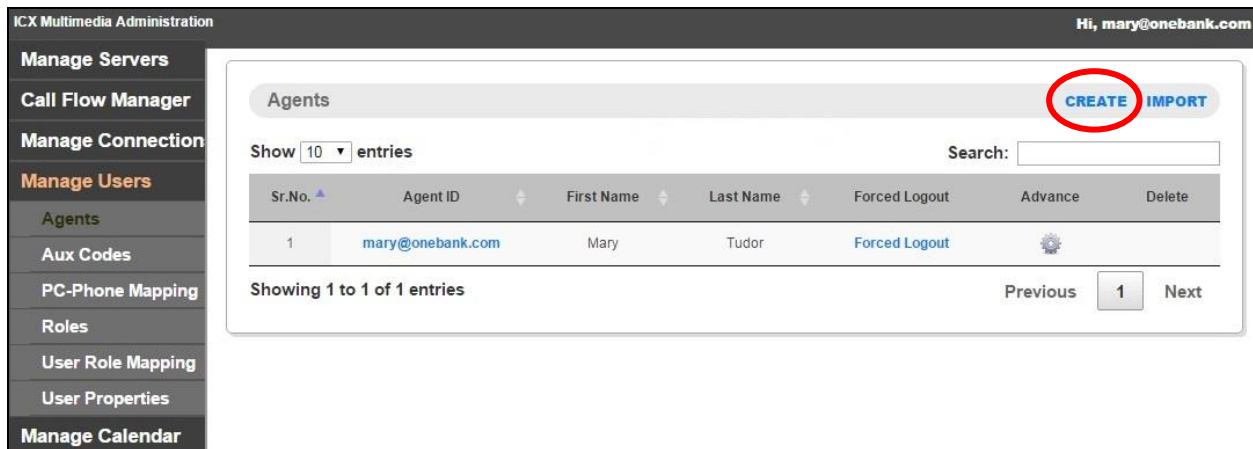
### 7.3. Administer Agents

Follow reference [3] to create a tenant group and an administrative user for the tenant group.

Use the procedures in **Section 7.1** to launch the web interface, and log in using an administrative account, in this case [mary@onebank.com](mailto:mary@onebank.com).



Select **Manage Users** → **Agents** from the left pane, to display the **Agents** screen. Click on **CREATE**.



The **Add Agent** screen is displayed. Enter desired values for **Login ID**, **First Name**, **Last Name**, **Preferred Name**, **Password**, and **Confirm Password**.

For **Role**, select **AGENT**. For **Channels**, check **Voice-Avaya**.

For **PBX ID**, **PBX Password**, and **Confirm PBX Password**, enter the first agent ID and agent password from **Section 3**. For **Hunt Group**, enter the first skill group extension that the agent belongs to from **Section 3**.

Retain the default values for the remaining fields.

The screenshot shows the 'Add Agent' form within the ICX Multimedia Administration interface. The left sidebar contains a navigation menu with options like 'Manage Servers', 'Call Flow Manager', 'Manage Connection', 'Manage Users' (highlighted), 'Agents', 'Aux Codes', 'PC-Phone Mapping', 'Roles', 'User Role Mapping', 'User Properties', 'Manage Calendar', 'Manage ACD', 'Manage Queues', 'Multimedia Rules', 'Callback', 'Surveys', 'Campaign Designer', 'Report Access', 'Tenant Administration', and 'Manage License'. The main content area is titled 'Add Agent' and contains the following fields and controls:

- Login ID \***: agent1@onebank.com
- First Name \***: AgentOne
- Last Name \***: ICX
- Preferred Name \***: AgentOne
- Password \***: [masked]
- Confirm Password \***: [masked]
- Supervisor**: ☐
- Role**: AGENT (dropdown)
- Channels**:
  - ☐ Email : 0
  - ☒ Voice-Avaya : 1
- Mode**: ☐ acd ☒ eas
- PBX ID \***: 65881
- PBX Password**: [masked]
- Confirm PBX Password**: [masked]
- Station ID**: [empty]
- Hunt Group \***: 61001
- Campaign Mode \***: INBOUND (dropdown)
- Chat**: ☐ : 0
- Twitter**: ☐ : 0
- SMS**: ☐ : 0
- Fax**: ☐ : 0
- Voice-Native**: ☐ : 0
- Task Ceiling**: [empty]
- SME**: ☐
- Blending**: ☐ : Open Blending (dropdown)

At the bottom of the form are 'Save' and 'Cancel' buttons.

Repeat this section to add an agent for every agent in **Section 3**. In the compliance testing, two agents were created, as shown below.

ICX Multimedia Administration Hi, mary@onebank.com

**Manage Servers**  
**Call Flow Manager**  
**Manage Connection**  
**Manage Users**  
 Agents  
 Aux Codes  
 PC-Phone Mapping  
 Roles  
 User Role Mapping  
 User Properties  
 Manage Calendar  
 Manage ACD

**Agents** CREATE IMPORT

Show 10 entries Search:

Sr.No. ▲	Agent ID	First Name	Last Name	Forced Logout	Advance	Delete
1	agent1@onebank.com	AgentOne	ICX	Forced Logout		Delete
2	agent2@onebank.com	AgentTwo	ICX	Forced Logout		Delete
3	mary@onebank.com	Mary	Tudor	Forced Logout		

Showing 1 to 3 of 3 entries Previous 1 Next

## 7.4. Administer Queues

Select **Manage Queues** → **Configure Queues** from the left pane, to display the **Queues** screen. Click on **CREATE**.

ICX Multimedia Administration Hi, mary@onebank.com

**Manage Servers**  
**Call Flow Manager**  
**Manage Connection**  
**Manage Users**  
**Manage Calendar**  
**Manage ACD**  
**Manage Queues**  
 Interaction Outcome  
 Configure Queues

**Queues** CREATE

Sr.No.	Name	ID	Media	Tenant	Addressable	Threshold	Delete
--------	------	----	-------	--------	-------------	-----------	--------



The **Add Queue** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Media Type:** “Voice-Avaya”
- **Tenant:** Select the applicable tenant, in this case “One Bank”.
- **ID:** The first VDN extension from **Section 3**.
- **Name:** The corresponding VDN name from **Section 5.4**.
- **Monitor Context Data:** Check this field.
- **Display In Directory:** Check this field.
- **Queue Group:** “DefaultVoiceQueueGroup”

ICX Multimedia Administration Hi, mary@onebank.com

**Manage Servers**  
**Call Flow Manager**  
**Manage Connection**  
**Manage Users**  
**Manage Calendar**  
**Manage ACD**  
**Manage Queues**  
 Interaction Outcom  
 Configure Queues  
 Agent Queue Mappi  
 Manage Queue Gro  
 SLA Profile  
 Top X Queues  
 Multimedia Rules  
 Callback  
 Surveys

**Add Queue**

Media Type \* Voice-Avaya ▼

=====

Tenant \* One Bank ▼

ID \* 60001

Name \* ICX Sales

Monitor Context Data : ☒

Display In Directory : ☒

Queue Group \* DefaultVoiceQueueGroup ▼

WrapUp Category 1 : --Select-- ▼

WrapUp Category 2 : --Select-- ▼

WrapUp Category 3 : --Select-- ▼

WrapUp Category 4 : --Select-- ▼

WrapUp Category 5 : --Select-- ▼

Priority Group \* No Priority Profiling ▼

Enable Blending : ☐

Add Cancel

Repeat this section to add a queue for each VDN in **Section 3**. In the compliance testing, two queues were created, as shown below.

ICX Multimedia Administration Hi, mary@onebank.com

**Manage Servers**  
**Call Flow Manager**  
**Manage Connection**  
**Manage Users**  
**Manage Calendar**  
**Manage ACD**  
**Manage Queues**  
 Interaction Outcom  
 Configure Queues

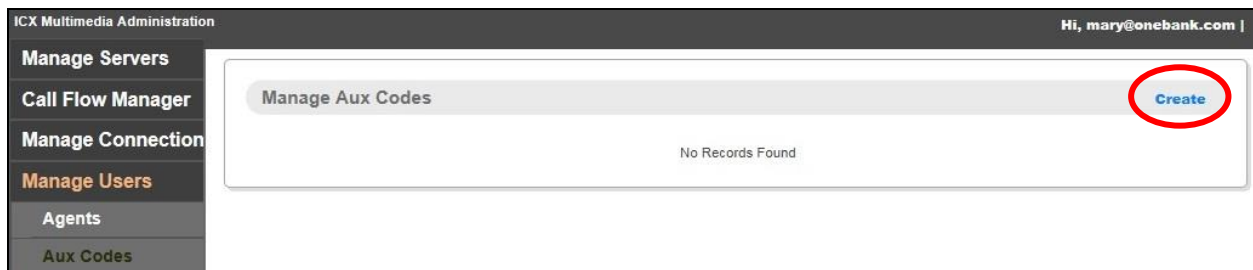
**Queues** CREATE

Sr.No.	Name	ID	Media	Tenant	Addressable	Threshold	Delete
1	ICX Sales	60001	Voice-Avaya	One Bank	YES		Delete
2	ICX Support	60002	Voice-Avaya	One Bank	YES		Delete



## 7.5. Administer Aux Codes

Select **Manage Users** → **Aux Codes** from the left pane, to display the **Manage Aux Codes** screen. Click on **Create**.



ICX Multimedia Administration | Hi, mary@onebank.com |

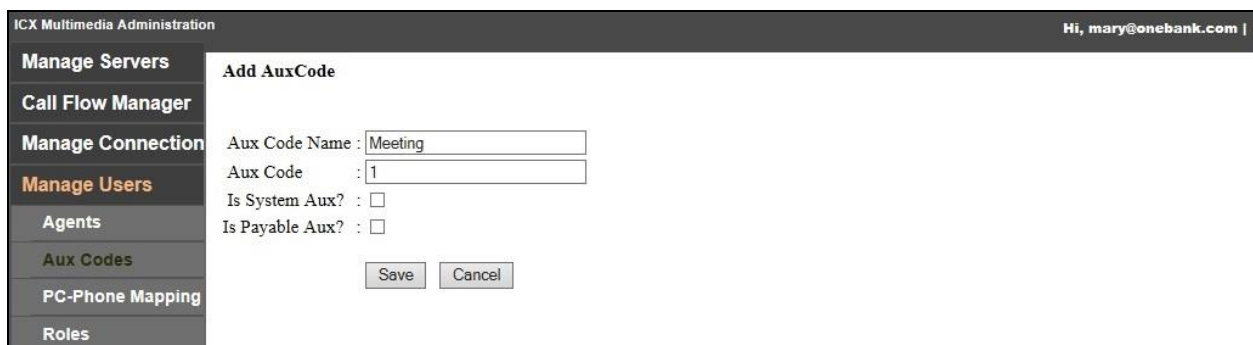
Manage Servers  
Call Flow Manager  
Manage Connection  
Manage Users  
Agents  
Aux Codes

Manage Aux Codes [Create](#)

No Records Found

The **Add AuxCode** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Aux Code Name:** The first aux work reason code name in **Section 5.5**.
- **Tenant:** The first aux work reason code number in **Section 5.5**.



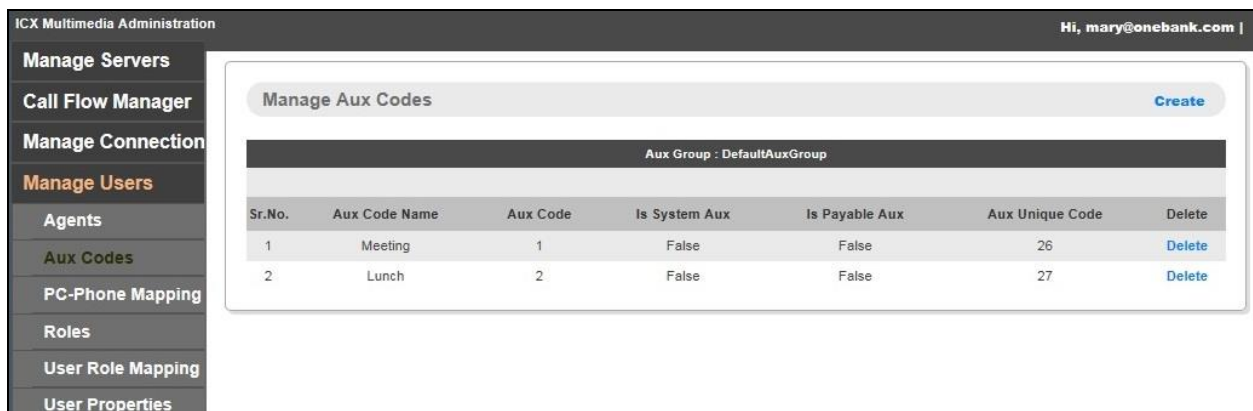
ICX Multimedia Administration | Hi, mary@onebank.com |

Manage Servers  
Call Flow Manager  
Manage Connection  
Manage Users  
Agents  
Aux Codes  
PC-Phone Mapping  
Roles

Add AuxCode

Aux Code Name : Meeting  
Aux Code : 1  
Is System Aux? : ☐  
Is Payable Aux? : ☐  
[Save](#) [Cancel](#)

Repeat this section to create an aux code for each aux work reason code in **Section 5.5**. In the compliance testing, two aux codes were created, as shown below. Note that the **Aux Unique Code** values were automatically generated by ICX.



ICX Multimedia Administration | Hi, mary@onebank.com |

Manage Servers  
Call Flow Manager  
Manage Connection  
Manage Users  
Agents  
Aux Codes  
PC-Phone Mapping  
Roles  
User Role Mapping  
User Properties

Manage Aux Codes [Create](#)

Aux Group : DefaultAuxGroup

Sr.No.	Aux Code Name	Aux Code	Is System Aux	Is Payable Aux	Aux Unique Code	Delete
1	Meeting	1	False	False	26	<a href="#">Delete</a>
2	Lunch	2	False	False	27	<a href="#">Delete</a>

## 8. Verification Steps

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

### 8.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify the status of the administered CTI link by using the “status aesvcs cti-link” command. Verify that the **Service State** is “established” for the CTI link number administered in **Section 5.2**, as shown below.


```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	7	no	aes7	established	6	8

### 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 (not shown below). 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 number of agents from **Section 3** that are currently logged into Contact Center and therefore monitored, in this case “2”.

**Application Enablement Services**  
Management Console

Welcome: User  
Last login: Thu Jun 2 09:47:41 2016 from 192.168.200.20  
Number of prior failed login attempts: 0  
HostName/IP: aes7/10.64.101.239  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 7.0.1.0.1.15-0  
Server Date and Time: Thu Jun 02 15:27:38 EDT 2016  
HA Status: Not Configured

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

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

▶ Log Manager

▶ Logs

▼ Status and Control

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	Thu Jun 2 15:24:02 2016	Online	17	2	14	10	30

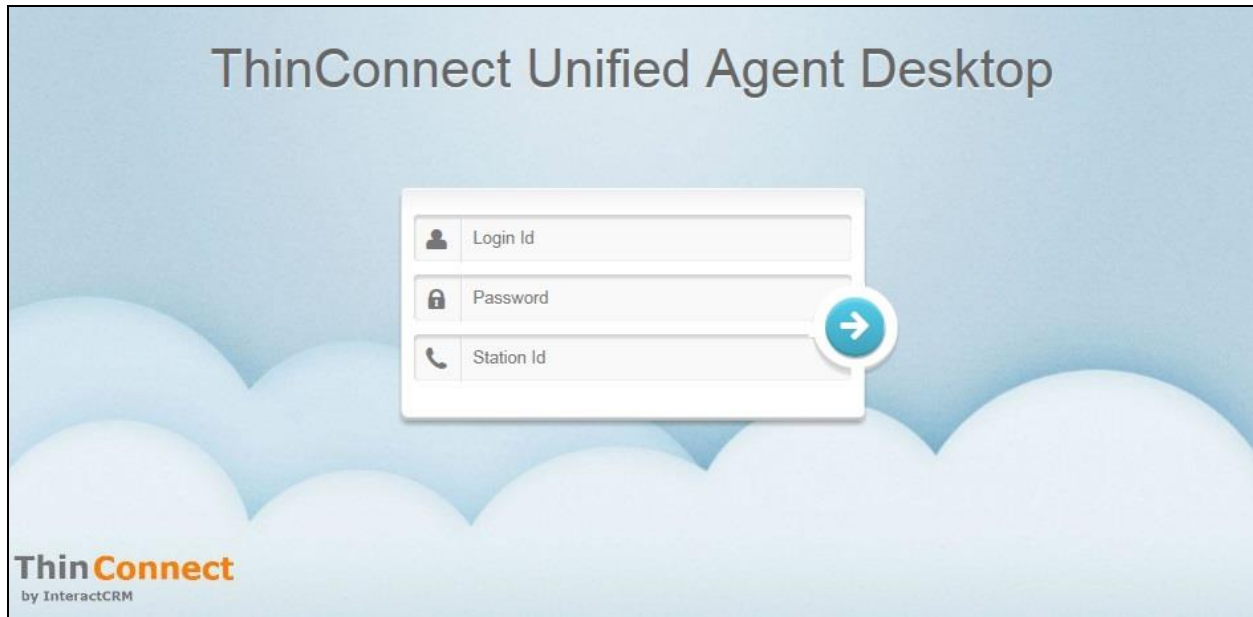
Online Offline

For service-wide information, choose one of the following:  
TSAPI Service Status TLink Status User Status

### 8.3. Verify ICX Contact Center

From the agent PC, launch the Internet Explorer browser and enter the URL “http://ip-address:18080/AgentDesktop/html/AgentDesktop.jsp”, where “ip-address” is the IP address of the ICX server running the Interaction Manager component.

The **ThinConnect Unified Agent Desktop** screen is displayed. For **Login Id** and **Password**, enter the relevant user credentials from **Section 7.3**. For **Station Id**, enter the applicable agent station extension from **Section 3**.

The image shows the ThinConnect Unified Agent Desktop login interface. It features a light blue background with a stylized cloud pattern at the bottom. In the center, there is a white login form with three input fields: 'Login Id' (with a person icon), 'Password' (with a lock icon), and 'Station Id' (with a phone icon). A blue circular button with a white right-pointing arrow is positioned to the right of the 'Station Id' field. The 'ThinConnect by InteractCRM' logo is located in the bottom left corner of the screen.

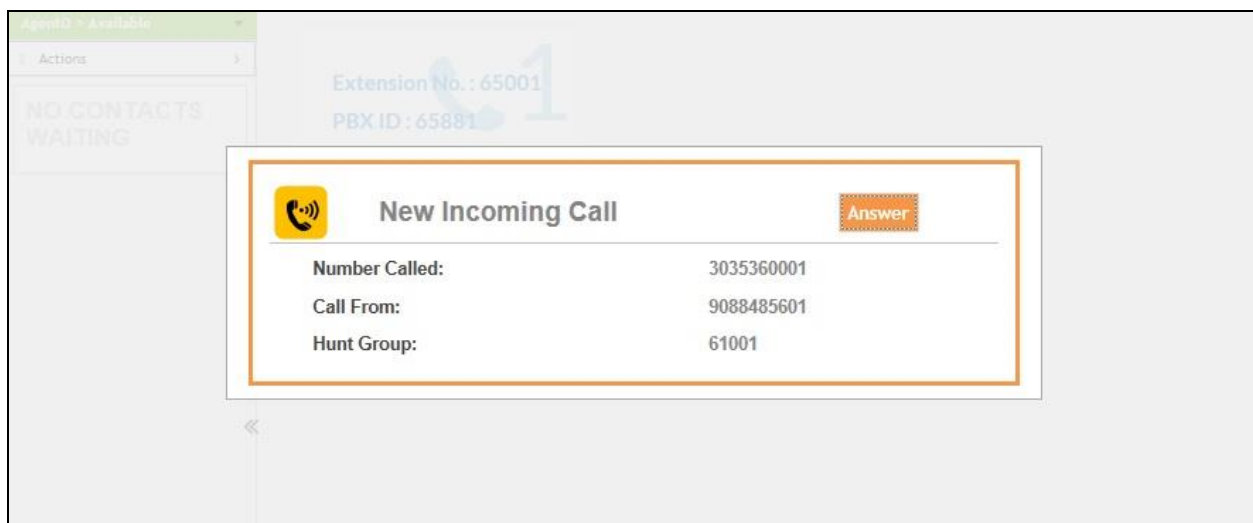
The screen below is displayed next. In the left pane, click on the **AgentO>Aux on Login** drop-down list and select **Become Available**.

The image displays the AgentO>Aux on Login screen. The left pane has a red header with the text 'AgentO>Aux on Login' and a dropdown menu. Below the header, there is a section titled 'Actions' with a right-pointing arrow. Underneath, a box contains the text 'NO CONTACTS WAITING'. The main area of the screen is light gray and displays 'Extension No.: 65001' and 'PBX ID: 65881' in blue text, accompanied by a large blue number '1' and a blue telephone handset icon.

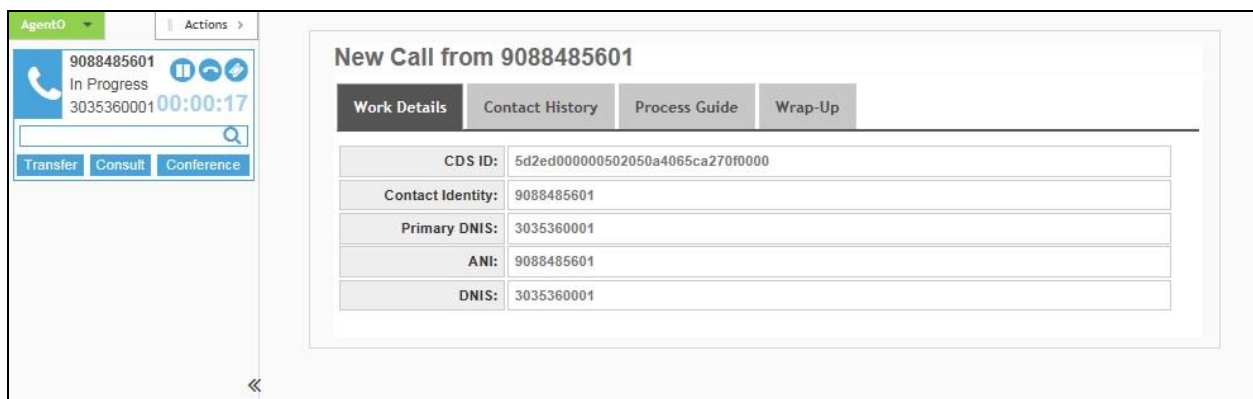
The left pane is updated, showing the agent in the **Available** mode, as shown below.



Make an incoming ACD call. Verify that the screen of the available agent is updated to reflect **New Incoming Call**, along with proper call information, as shown below. Click **Answer**.



Verify that the agent is connected to the PSTN caller with two-way talk paths, and that the screen is updated to reflect call **In Progress** in the left pane, as shown below.



## 9. Conclusion

These Application Notes describe the configuration steps required for ICX Contact Center to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. All feature and serviceability test cases were completed with an observation 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 7.0, Issue 1, August 2015, available at <http://support.avaya.com>.
2. *Administering and Maintaining Aura® Application Enablement Services*, Release 7.0, Issue 1, August 2015, available at <http://support.avaya.com>.
3. *Interactcrm Customer Experience Platform Voice Installation Manual*, ICX Version 3.0.16, available upon request to InteractcrmSupport.

---

**©2016 Avaya Inc. All Rights Reserved.**

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

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