



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

---

# **Application Notes for InteractCRM ThinConnect 7.1 with Avaya Aura® Communication Manager 6.3 and Avaya Aura® Application Enablement Services 6.3 – Issue 1.0**

## **Abstract**

These Application Notes describe the configuration steps required for InteractCRM ThinConnect 7.1 to interoperate with Avaya Aura® Communication Manager 6.3 and Avaya Aura® Application Enablement Services 6.3. InteractCRM ThinConnect is a desktop CTI solution.

In the compliance testing, InteractCRM ThinConnect 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 InteractCRM ThinConnect 7.1 to interoperate with Avaya Aura® Communication Manager 6.3 and Avaya Aura® Application Enablement Services 6.3. InteractCRM ThinConnect is a desktop CTI solution.

In the compliance testing, InteractCRM ThinConnect 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 the 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 with available agents. Manual call controls from the agent desktop were exercised to verify proper call handling such as transfer and conference.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to the ThinConnect server and to the agent desktop.

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 ThinConnect:

- 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 ThinConnect to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to ThinConnect.

## 2.2. Test Results

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

- 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 when only two parties remained on 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 with an agent during a brief 30 seconds of disruption to the desktop LAN connection, the active call can be dropped by the application as part of the agent re-login process.
- 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 ThinConnect can be obtained through the following:

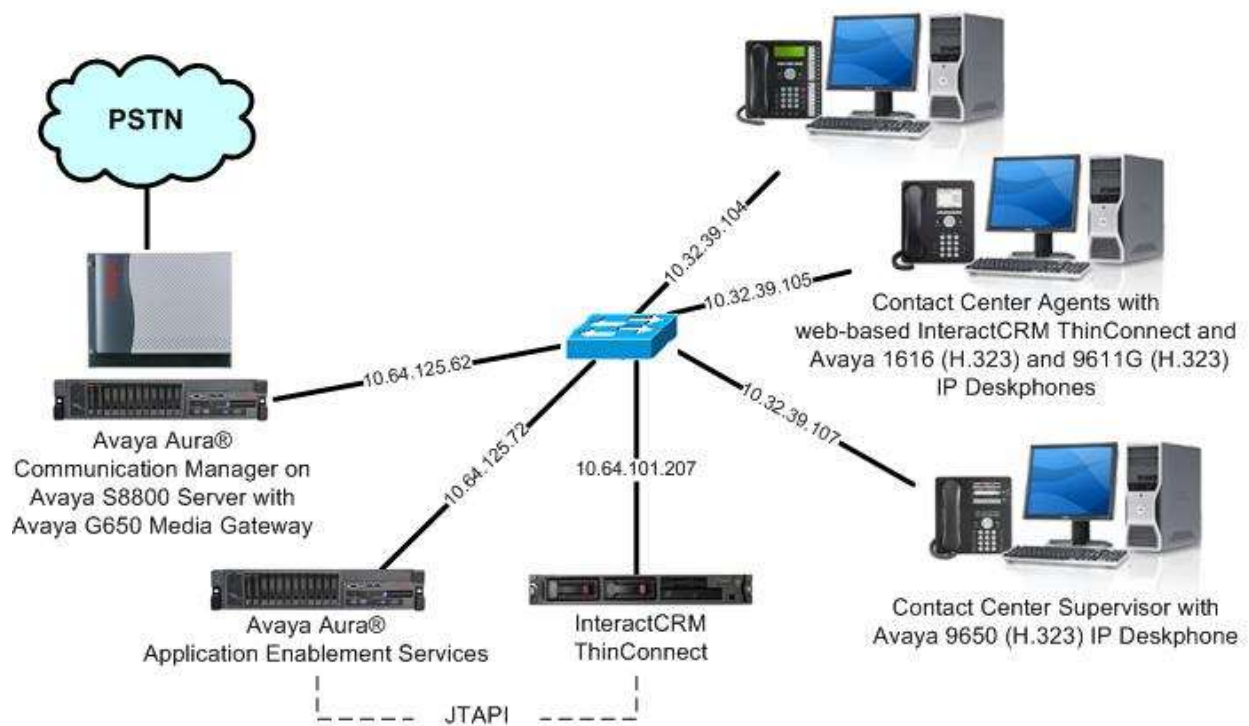
- **Phone:** (510) 795-7645
- **Email:** [usa@interactcrm.com](mailto:usa@interactcrm.com)

### 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, and of contact center devices are not the focus of these Application Notes and will not be described.

In the compliance testing, ThinConnect monitored the agent stations shown in the table below.

Device Type	Extension
VDNs	60001, 60002
Skill Groups	65081, 65082
Supervisor	65000
Agent Stations	65001, 65002
Agent IDs	65881, 65882
Agent Passwords	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 on Avaya S8800 Server with Avaya G650 Media Gateway	6.3.9 (R016x.03.0.124.0-21971)
Avaya Aura® Application Enablement Services	6.3.3 SP1 (6.3.3.1.10-0)
Avaya 1616 IP Deskphone (H.323)	1.350B
Avaya 9611G IP Deskphone (H.323)	6.4014
Avaya 9650 IP Deskphone (H.323)	3.230A
InteractCRM ThinConnect on Windows Server 2008 <ul style="list-style-type: none"><li>Interaction Manager</li><li>Avaya JTAPI Client</li></ul>	7.1 R2 Enterprise 6.3.0.3 (Build 40) 6.3.0.12

## 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 3**. 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	3 of	11
OPTIONAL FEATURES				
Abbreviated Dialing Enhanced List?	y	Audible Message Waiting?	y	
Access Security Gateway (ASG)?	n	Authorization Codes?	y	
Analog Trunk Incoming Call ID?	y	CAS Branch?	n	
A/D Grp/Sys List Dialing Start at 01?	y	CAS Main?	n	
Answer Supervision by Call Classifier?	y	Change COR by FAC?	n	
ARS?	y	<b>Computer Telephony Adjunct Links?</b>	<b>y</b>	
ARS/AAR Partitioning?	y	Cvg Of Calls Redirected Off-net?	y	
ARS/AAR Dialing without FAC?	n	DCS (Basic)?	y	
ASAI Link Core Capabilities?	n	DCS Call Coverage?	y	
ASAI Link Plus Capabilities?	n	DCS with Rerouting?	y	

### 5.2. Administer CTI Link

Add a CTI link using the “add cti-link n” command, where “n” is an available CTI link number. Enter an available extension number in the **Extension** field. Note that the CTI link number and extension number may vary. Enter “ADJ-IP” in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

add cti-link 2		Page	1 of	3
CTI LINK				
CTI Link:	2			
<b>Extension:</b>	60100			
<b>Type:</b>	ADJ-IP			
		COR:	1	
<b>Name:</b>	AES CTI Link			

### 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 20
      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 ThinConnect.

```
change system-parameters features                                     Page 13 of 20
      FEATURE-RELATED SYSTEM PARAMETERS

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

      Reporting for PC Non-Predictive Calls? n

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

ASAI
      Copy ASAI UII During Conference/Transfer? y
      Call Classification After Answer Supervision? y
      Send UCID to ASAI? y
      For ASAI Send DTMF Tone to Call Originator? y
      Send Connect Event to ASAI For Announcement Answer? n
```



## 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 ThinConnect. In the compliance testing, the two VDNs shown below were used.

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

## 5.5. Obtain Reason Codes

For contact centers that use reason codes, enter the “change reason-code-names” command to display the configured reason codes. Make a note of the **Aux Work** reason codes, which will be used later to configure ThinConnect.

Note that ThinConnect makes use of a default reason code and a system reason code for use with aux work upon login. In the compliance testing, separate reason codes were created for these two purposes, as shown below.

change reason-code-names

Page 1 of 1

REASON CODE NAMES

Aux Work/  
Interruptible?

Logout

Reason Code 1: **Tea Break** /n

Reason Code 2: **Lunch Brea** /n

Reason Code 3: **Restroom** /n

Reason Code 4: **Outbound** /n

Reason Code 5: **Aux on Login** /n

Reason Code 6: /n

Reason Code 7: /n

Reason Code 8: /n

Reason Code 9: /n

Default Reason Code: 0

## 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
- Disable security database
- Restart service
- Obtain Tlink name
- Administer InteractCRM user

### 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" and "Management Console" is displayed. A red horizontal bar spans the width of the page, with a "Help" link on the right. In the center, there is a login box with the text "Please login here:" followed by a "Username" label and a text input field. Below the input field is a "Continue" button. At the bottom of the page, a red horizontal bar is present, and below it, the copyright notice "Copyright © 2009-2014 Avaya Inc. All Rights Reserved." is displayed.

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, the title "Application Enablement Services Management Console", and a welcome message for the user. 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 shows the "Welcome to OAM" screen, which provides an overview of the OAM web 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 served by one administrator for all domains or a separate administrator for each domain.

**AVAYA** Application Enablement Services Management Console

Welcome: User  
Last login: Tue Jan 27 06:48:26 2015 from 10.32.39.20  
Number of prior failed login attempts: 0  
HostName/IP: aes\_125\_72/10.64.125.72  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
SW Version: 6.3.3.1.10-0  
Server Date and Time: Tue Jan 27 06:49:44 MST 2015  
HA Status: Not Configured

Home | Help | Logout

Home

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

**Welcome to OAM**

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

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

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

## 6.2. Verify License

Select **Licensing** → **WebLM Server Access** in the left pane, to display the **Web License Manager** pop-up screen (not shown), and log in using the appropriate credentials.

The screenshot displays the Avaya Application Enablement Services Management Console with the "Licensing" section selected in the left sidebar. The main content area shows the "Licensing" screen, which provides instructions on how to set up and maintain the WebLM, import, set up, and maintain the license, and administer TSAPI Reserved Licenses or DMCC Reserved Licenses. It lists the following steps: WebLM Server Address, WebLM Server Access, and Reserved Licenses.

**AVAYA** Application Enablement Services Management Console

Welcome: User  
Last login: Tue Jan 27 06:48:26 2015 from 10.32.39.20  
Number of prior failed login attempts: 0  
HostName/IP: aes\_125\_72/10.64.125.72  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
SW Version: 6.3.3.1.10-0  
Server Date and Time: Tue Jan 27 06:49:44 MST 2015  
HA Status: Not Configured

Home | Help | Logout

Licensing

AE Services  
Communication Manager Interface  
Licensing  
Maintenance  
Networking  
Security

**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

The **Web License Manager** screen below is displayed. 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 is sufficient license for **TSAPI Simultaneous Users**, as shown below.

**Web License Manager (WebLM v6.3)**
Help About Change Password

WebLM Home  
Install license  
Licensed products  
APPL\_ENAB  
▼ Application\_Enablement  
View license capacity  
View peak usage  
Uninstall license  
Server properties  
Manage users  
Shortcuts  
Help for Installed Product

**Application Enablement (CTI) - Release: 6 - SID: 10503000**
**Standard License file**

You are here: Licensed Products > Application\_Enablement > View License Capacity  
License installed on: May 11, 2012 7:07:47 PM -04:00  
License File Host IDs: 00-16-3E-48-E0-82  
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	10000
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	16
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	16
Product Notes VALUE_NOTES	permanent	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;Cti5 MediumServerTypes: ibmx306;ibmx306m;del11950;xen;hs20;hs20_2 LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;un TrustedApplications: IPS_001, BasicUnrestricted DMCUnrestricted; IXF_001, BasicUnrestricted DMCUnrestricted; IXN_001, BasicUnrestricted DMCUnrestricted; PC_001, BasicUnrestricted DMCUnrestricted; CIE_001, BasicUnrestricted DMCUnrestricted; OSFC_001, BasicUnrestricted DMCUnrestricted; VP_001, BasicUnrestricted DMCUnrestricted; SAMETIME_001 VALUE_AES_UNIFIED_CC_DESKTOP,, CCE, AdvancedUnrestricted, DMCUnrestricted; CSI AdvancedUnrestricted, DMCUnrestricted; CSI AdvancedUnrestricted, DMCUnrestricted; AVA BasicUnrestricted, AdvancedUnrestricted, DMC CCT_ELITE_CALL_CTRL_001, BasicUnrestricted DMCUnrestricted, AgentEvents;
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	16
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	10000
DLG VALUE_AES_DLG	permanent	16
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	10000
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	16

### 6.3. Administer TSAPI Link

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

The screenshot shows the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The left navigation pane shows "AE Services" expanded, with "TSAPI" selected, and "TSAPI Links" highlighted. The main content area displays the "TSAPI Links" screen, which includes a table with columns: Link, Switch Connection, Switch CTI Link #, ASAI Link Version, and Security. Below the table are buttons for "Add Link", "Edit Link", and "Delete Link".

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

The **Link** field is only local to the Application Enablement Services server, and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection "S8800" 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. The main content area displays the "Add TSAPI Links" form, which includes fields for Link, Switch Connection, Switch CTI Link Number, ASAI Link Version, and Security. The values entered are: Link: 1, Switch Connection: S8800, Switch CTI Link Number: 2, ASAI Link Version: 6, and Security: Unencrypted. Below the fields are buttons for "Apply Changes" and "Cancel Changes".

## 6.4. Disable Security Database

Select **Security** → **Security Database** → **Control** from the left pane, to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane. Uncheck both fields below.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The left navigation pane shows a tree structure with "Security" expanded, and "Control" selected under "Security Database". The main content area is titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" and contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services". An "Apply Changes" button is located below the checkboxes.

Welcome: User  
Last login: Tue Jan 27 06:48:26 2015 from 10.32.39.20  
Number of prior failed login attempts: 0  
HostName/IP: aes\_125\_72/10.64.125.72  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
SW Version: 6.3.3.1.10-0  
Server Date and Time: Tue Jan 27 06:49:44 MST 2015  
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



## 6.5. Restart 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**.



**Application Enablement Services**  
Management Console

Welcome: User  
Last login: Tue Jan 27 06:48:26 2015 from 10.32.39.20  
Number of prior failed login attempts: 0  
HostName/IP: aes\_125\_72/10.64.125.72  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
SW Version: 6.3.3.1-10-0  
Server Date and Time: Tue Jan 27 06:49:44 MST 2015  
HA Status: Not Configured

Maintenance | Service Controller

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▼ Maintenance

▶ Date Time/NTP Server

▶ Security Database

▶ Service Controller

▶ Server Data

▶ Networking

▶ Security

▶ Status

▶ User Management

Service Controller

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

## 6.6. 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 ThinConnect.

In this case, the associated Tlink name is “AVAYA#S8800#CSTA#AES\_125\_72”. Note the use of the switch connection “S8800” 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 pane on the left lists various services, with "Security" expanded to show "Security Database" and "Tlinks" selected. The main content area shows the "Tlinks" page with a list of Tlink names. Two Tlink names are listed: "AVAYA#S8300D#CSTA#AES\_125\_72" and "AVAYA#S8800#CSTA#AES\_125\_72". The second Tlink name is selected, and a "Delete Tlink" button is visible below it.

AVAYA Application Enablement Services Management Console

Welcome: User  
Last login: Tue Jan 27 06:48:26 2015 from 10.32.39.20  
Number of prior failed login attempts: 0  
HostName/IP: aes\_125\_72/10.64.125.72  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
SW Version: 6.3.3.1.10-0  
Server Date and Time: Tue Jan 27 06:49:44 MST 2015  
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#S8300D#CSTA#AES\_125\_72  
☒ AVAYA#S8800#CSTA#AES\_125\_72


Delete Tlink



## 6.7. Administer InteractCRM 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  
Last login: Tue Jan 27 06:48:26 2015 from 10.32.39.20  
Number of prior failed login attempts: 0  
HostName/IP: aes\_125\_72/10.64.125.72  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
SW Version: 6.3.3.1.10-0  
Server Date and Time: Tue Jan 27 06:49:44 MST 2015  
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

## 7. Configure InteractCRM ThinConnect

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

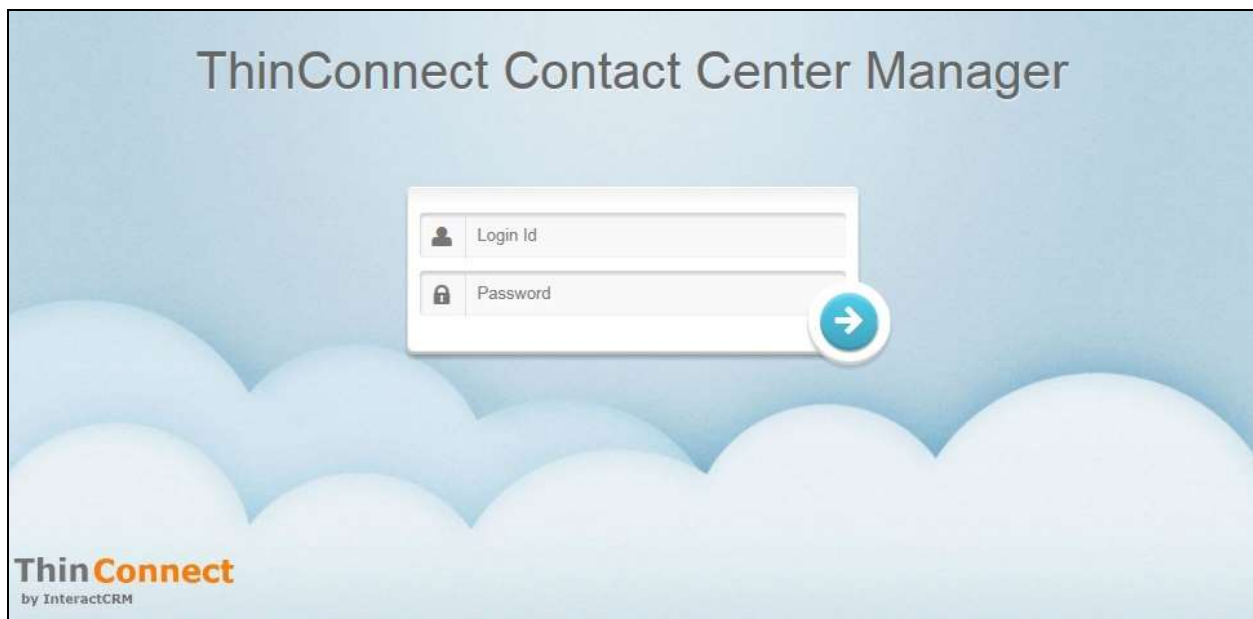
- Launch web interface
- Administer server
- Administer agents
- Administer queues
- Administer aux codes

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

### 7.1. Launch Web Interface

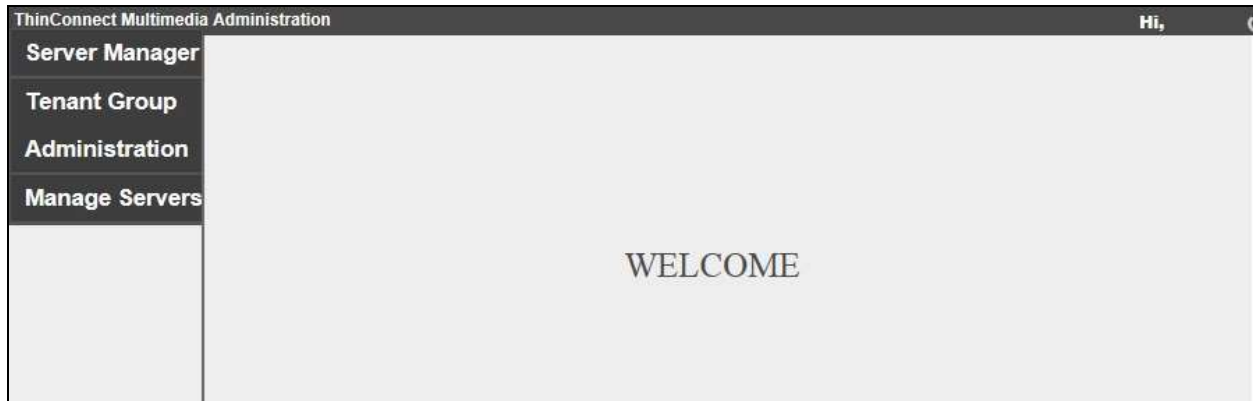
Launch the web interface by using the URL “http://ip-address:15050/ContactCenterManager” in an Internet Explorer browser window, where “ip-address” is the IP address of the ThinConnect server.

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

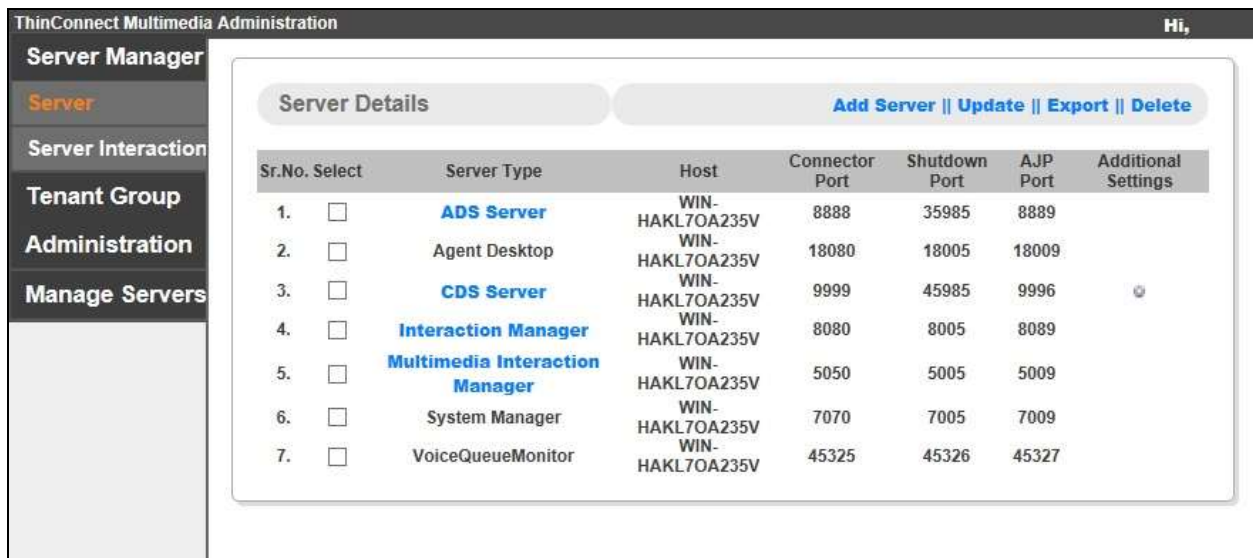


## 7.2. Administer Server

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.



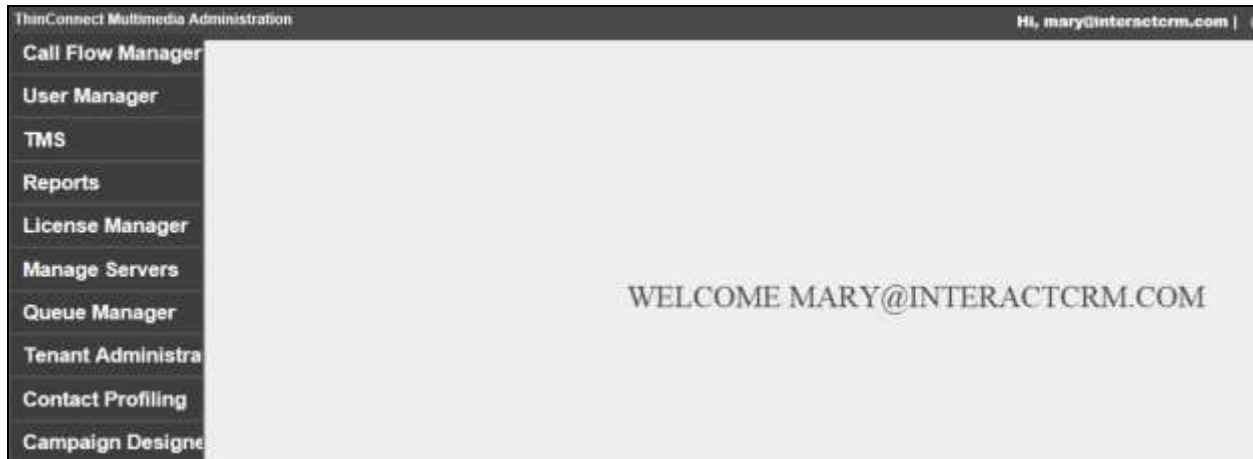
The **Edit Server** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **AES Host Name:** IP address of Application Enablement Services.
- **AES User Name:** The InteractCRM user credentials from **Section 6.7**.
- **AES Password:** The InteractCRM user credentials from **Section 6.7**.
- **TS Link String:** The Tlink name from **Section 6.6**.

ThinConnect Multimedia Administration		Hi,
<b>Server Manager</b>		
<b>Server</b>		
Server Interaction		
Tenant Group		
Administration		
Manage Servers		
<b>Edit Server</b>		
SDK Path *	MIS	
AES Host Name *	10.64.125.72	
AES Port *	450	
AES User Name *	interactcrm	
AES Password *	InteractCRM123;	
TS Link String *	AVAYA#S8800#CSTA#AES_12	
Debug Level *	4	
Trace File Location *	C:/Users/Administrator/Docum	
Heart Beat Interval in Telephony for AES *	40	
Max QM communicator thread count *	10	
Max QM communicator worker count *	5	
QM communicator sleep time *	30	
Is CDS Server Enabled *	1	
Enable Outbound Dialer *	0	
Outbound Dialer URL *	http://localhost	
Is Voice Only Deployment *	1	
Enable Password Encryption *	0	
Agent Job Status Check Interval(Min) *	5	
		<b>Save</b> <b>Cancel</b>

### 7.3. Administer Agents

Follow [3] to create a tenant group and an admin user for the tenant group. Use the procedures in **Section 7.1** to launch the web interface, and log in using the admin user account, in this case [mary@interactcrm.com](mailto:mary@interactcrm.com).



Select **User Manager** → **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**.

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**.

ThinConnect Multimedia Administration Hi, mary@interactcrm.com

**Add Agent**

Login ID \* agent1@interactcrm.co

First Name \* AgentOne

Last Name \* InteractCRM

Preferred Name \* AgentOne

Password \* .....

Confirm Password \* .....

Supervisor : ☐

Role : AGENT

Channels :

☐ Email : 0/5

☒ Voice :

Mode : ☐ acd ☒ eas

PBX ID \* 65881

PBX Password : .....

Confirm PBX Password : .....

Station ID :

Hunt Group \* 65081

Campaign Mode \* INBOUND

☐ Chat : 0/5

☐ Twitter : 0/5

☐ SMS : 0/5

☐ Fax : 0/5

☐ SIPVoice : 0/5

Task Ceiling :

SME : ☐

☐ Blending : Open Blending

Save Cancel

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

ThinConnect Multimedia Administration Hi, mary@interactcrm.com

Call Flow Manager  
User Manager  
**Agents**  
Aux Codes  
Action Rights  
Roles  
User Role Mapping  
TMS

Agents CREATE IMPORT

Agent added successfully.

Sr.No.	Agent ID	First Name	Last Name	Forced Logout	Advance	Delete
1	agent1@interactcrm.com	AgentOne	InteractCRM	Forced Logout		Delete
2	agent2@interactcrm.com	AgentTwo	InteractCRM	Forced Logout		Delete
3	mary@interactcrm.com	Mary	InteractCRM	Forced Logout		

## 7.4. Administer Queues

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

ThinConnect Multimedia Administration Hi, mary@interactcrm.com

Call Flow Manager  
User Manager  
TMS  
Reports  
License Manager  
Manage Servers  
Queue Manager  
**Manage 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”
- **Tenant:** “Voice Tenant”
- **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”

ThinConnect Multimedia Administration

Hi, mary@interactcrm.com

**Add Queue**

Media Type \*

Tenant \*

ID \*

Name \*

Monitor Context Data : ☒

Display In Directory : ☒

Queue Group \*

WrapUp Category 1: :

WrapUp Category 2: :

WrapUp Category 3: :

WrapUp Category 4: :

WrapUp Category 5: :

Priority Group \*

Enable Blending : ☐

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

ThinConnect Multimedia Administration

Hi, mary@interactcrm.com

**Queues** [CREATE](#)

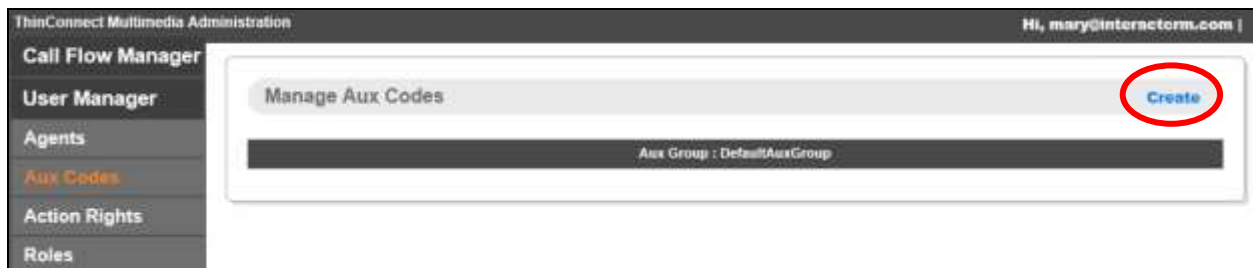
Queue added successfully

Sr.No.	Name	ID	Media	Tenant	Addressable	Threshold	Delete
1	<a href="#">InteractCRM Sales</a>	60001	Voice	VoiceTenant	YES		<a href="#">Delete</a>
2	<a href="#">InteractCRM Support</a>	60002	Voice	VoiceTenant	YES		<a href="#">Delete</a>



## 7.5. Administer Aux Codes

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

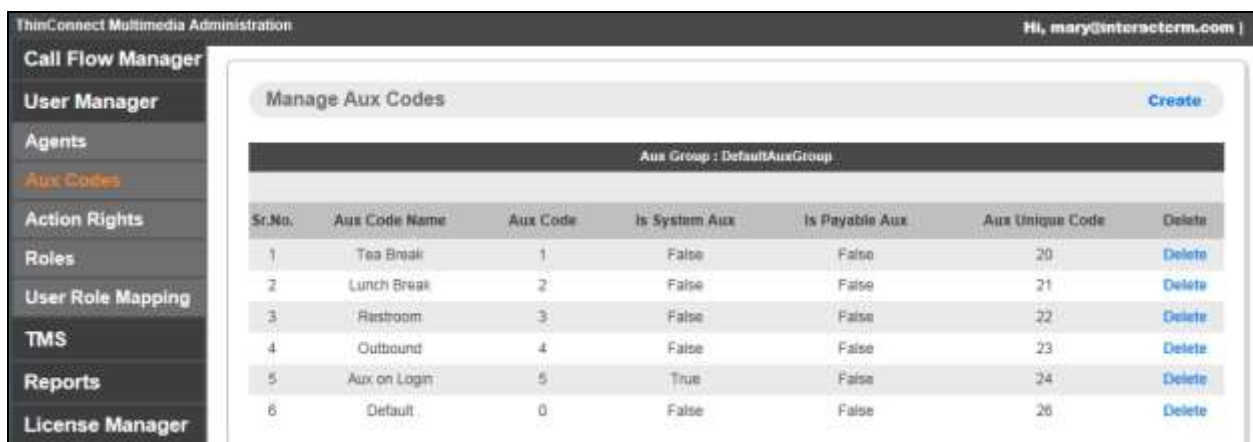


The **Add AuxCode** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

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



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



Sr.No.	Aux Code Name	Aux Code	Is System Aux	Is Payable Aux	Aux Unique Code	Delete
1	Tea Break	1	False	False	20	Delete
2	Lunch Break	2	False	False	21	Delete
3	Restroom	3	False	False	22	Delete
4	Outbound	4	False	False	23	Delete
5	Aux on Login	5	True	False	24	Delete
6	Default	0	False	False	26	Delete

## 8. Verification Steps

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

### 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
2	6	no	aes_125_72	established	92	80

### 8.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify 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 number of agents from **Section 3** that are currently logged into ThinConnect and therefore monitored, in this case “2”.



Application Enablement Services  
Management Console

Welcome: User  
Last login: Wed Jan 28 09:06:41 2015 from 10.32.39.20  
Number of prior failed login attempts: 0  
HostName/IP: aes\_125\_72/10.64.125.72  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
SW Version: 6.3.3.1.10-0  
Server Date and Time: Wed Jan 28 11:08:56 MST 2015  
HA Status: Not Configured

Status | Status and Control | TSAPI Service Summary

Home | Help | Logout

AE Services

Communication Manager Interface

High Availability

Licensing

Maintenance

Networking

Security

Status

Alarm Viewer

Log Manager

Logs

Status and Control

CVLAN Service Summary

DLG Services Summary

DMCC Service Summary

Switch Conn Summary

TSAPI Service Summary

TSAPI Link Details

☐ Enable page refresh every 60 seconds

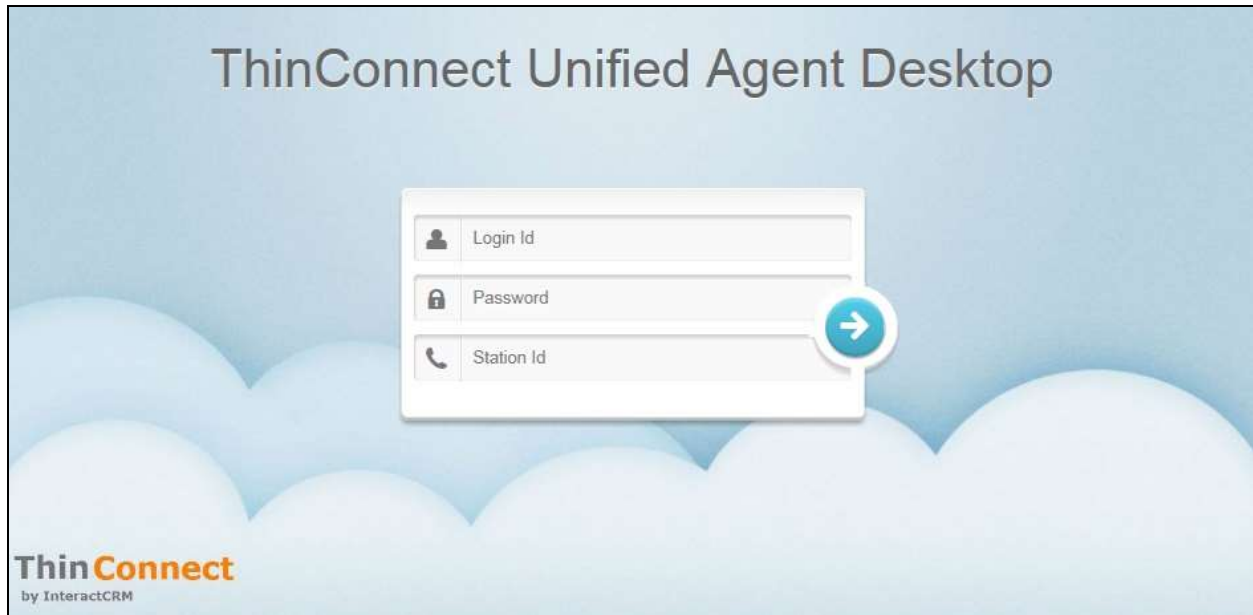
	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input checked="" type="radio"/>	1	S8800	2	Talking	Fri Jan 2 12:46:50 2015	Online	16	2	81	93	30
<input type="radio"/>	2	S8300D	1	Switch Down	Fri Jan 2 14:09:17 2015	Online	16	0	0	0	30

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

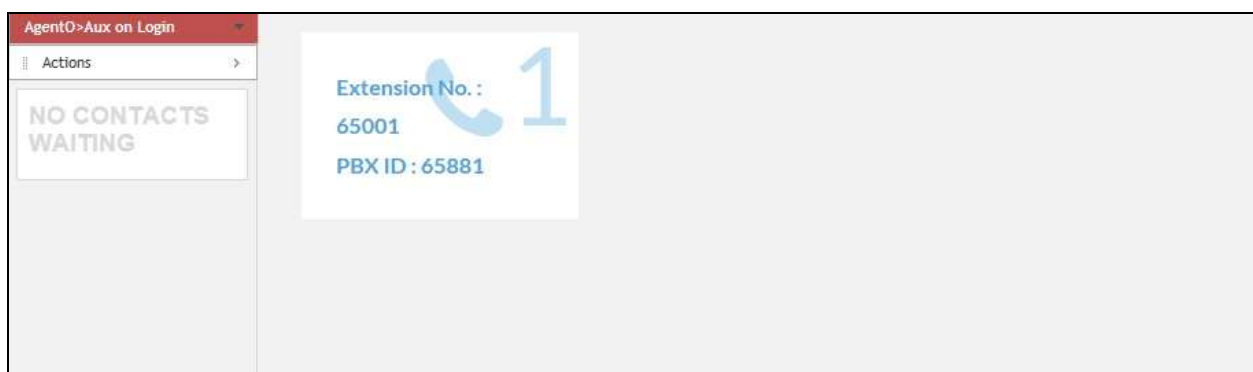
### 8.3. Verify InteractCRM ThinConnect

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

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 white login form in the center. The form has 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 text 'ThinConnect Unified Agent Desktop' is displayed at the top in a large, dark font. In the bottom left corner, the 'ThinConnect by InteractCRM' logo is visible.

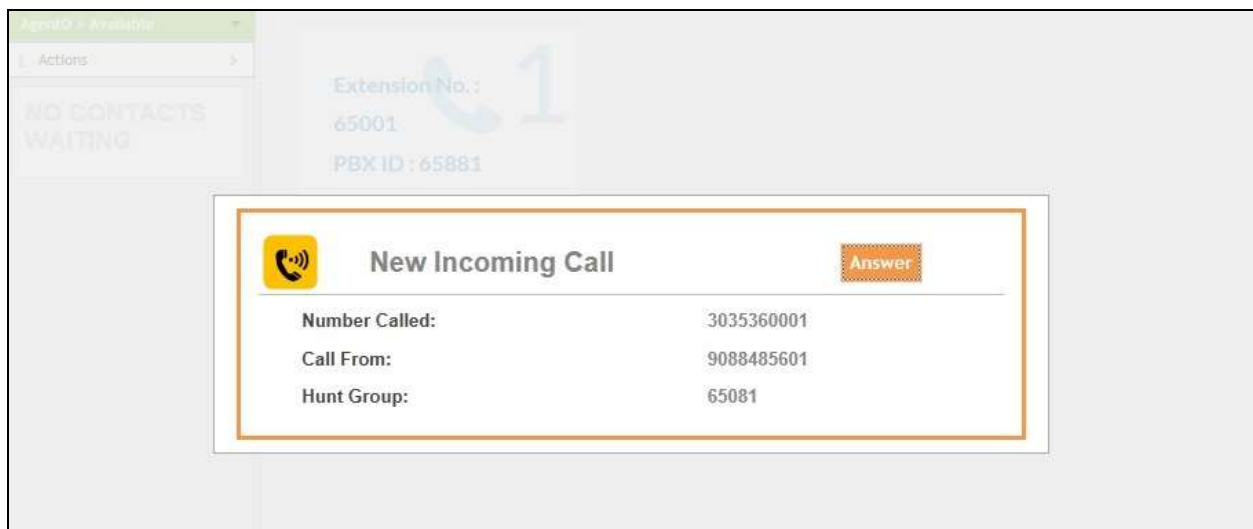
The screen below is displayed next. In the left pane, click on the **AgentO>Aux on Login** drop-down list and select **Become Available**.

The image displays the AgentO>Aux on Login screen. It is divided into two main sections. The left section, titled 'AgentO>Aux on Login', contains a 'NO CONTACTS WAITING' message. The right section displays the agent's status and contact information: 'Extension No. : 65001' and 'PBX ID : 65881'. A large blue number '1' is prominently displayed next to the extension number, and a blue phone icon is also visible.

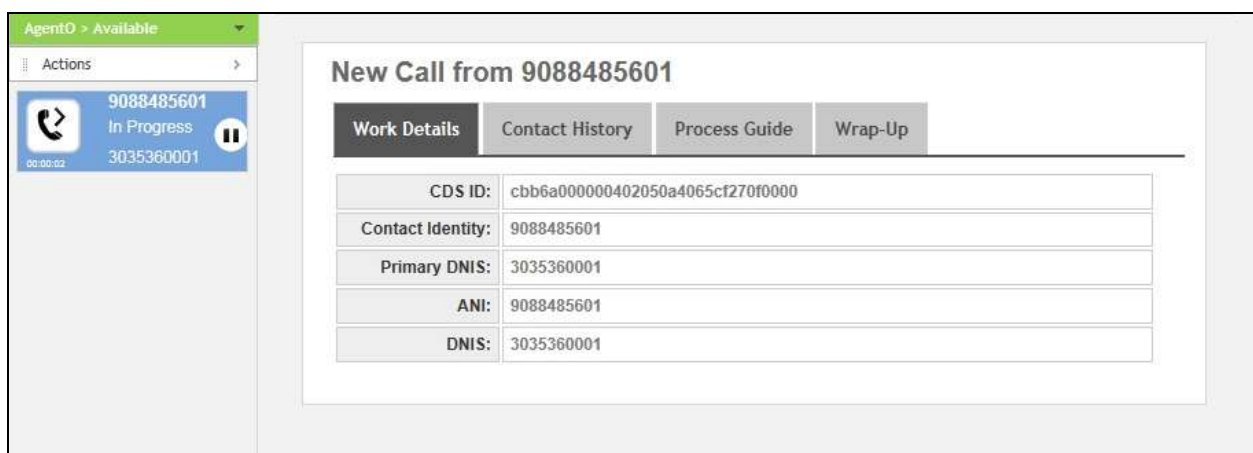
The left pane is updated, showing the agent in the **Available** mode.



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 InteractCRM ThinConnect 7.1 to successfully interoperate with Avaya Aura® Communication Manager 6.3 and Avaya Aura® Application Enablement Services 6.3. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

## 10. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Document 03-300509, Issue 10, Release 6.3, June 2014, available at <http://support.avaya.com>.
2. *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 6.3, 02-300357, June 2014, available at <http://support.avaya.com>.
3. *InteractCRM ThinConnect Installation Manual*, January 12, 2015, available upon request to InteractCRM Support.

---

**©2015 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).