



Avaya Solution & Interoperability Test Lab

Application Notes for TetraVX 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 TetraVX Customer Experience Platform (ICX) Contact Center to interoperate with Avaya Aura[®] Communication Manager and Avaya Aura[®] Application Enablement Services.

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 TetraVX Customer Experience Platform (ICX) Contact Center to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services.

In the compliance testing, ICX 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 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 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.

Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

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

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

For the testing associated with these Application Notes, the interface between Avaya systems and ICX utilized enabled capabilities of secure TSAPI and DMCC links.

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.
- 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: +18774963698
- Email: getservice@netrixllc.com

3. Reference Configuration

Figure 1 illustrates a sample configuration consisting of Avaya Aura® components and ICX.

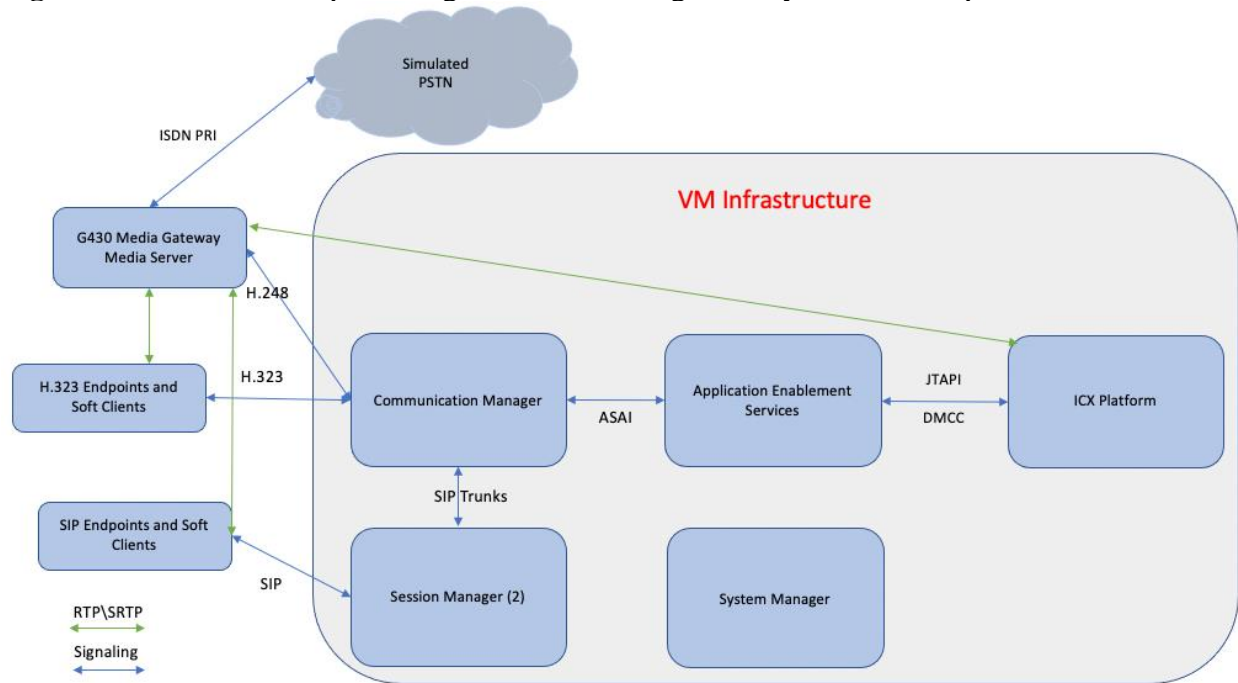


Figure 1: Test Configuration of ICX with Avaya Aura®

4. Equipment and Software Validated

The following equipment and software were used for the test configuration.

Equipment	Release/Version
Avaya Aura® Communication Manager	8.1.2.0.0.890.26095 (FP2)
Avaya Aura® Session Manager	8.1.2.1.812101
Avaya Aura® System Manager	8.1.2.0.0611588 (FP2)
Avaya Aura® Application Enablement Services	8.1.2.1.1.6-0
ICX on CentOS 6.x <ul style="list-style-type: none">• Interaction Manager	15.3

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 System Capacity (License)

The license file installed on the system controls these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative.

Use the **display system-parameters customer-options** command to determine these values. On **Page 4**, verify that the **Computer Telephony Adjunct Links** feature is enabled.

```
display system-parameters customer-options                                Page 4 of 12
                                OPTIONAL FEATURES

Abbreviated Dialing Enhanced List? y      Audible Message Waiting? y
Access Security Gateway (ASG)? y          Authorization Codes? y
Analog Trunk Incoming Call ID? y          CAS Branch? n
A/D Grp/Sys List Dialing Start at 01? y   CAS Main? n
Answer Supervision by Call Classifier? y   Change COR by FAC? n
ARS? y      Computer Telephony Adjunct Links? y
ARS/AAR Partitioning? y      Cvg Of Calls Redirected Off-net? y
ARS/AAR Dialing without FAC? y      DCS (Basic)? y
ASAI Link Core Capabilities? y      DCS Call Coverage? y
ASAI Link Plus Capabilities? y      DCS with Rerouting? y
Async. Transfer Mode (ATM) PNC? n      Digital Loss Plan Modification? y
Async. Transfer Mode (ATM) Trunking? n      DS1 MSP? y
ATM WAN Spare Processor? n            DS1 Echo Cancellation? y
ATMS? y
Attendant Vectoring? Y

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

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 link number and extension may vary. Enter “ADJ-IP” in the **Type** field, and a descriptive name in the **Name** field. Remaining entries are default.

```
add cti-link 1                                     Page 1 of 3
CTI LINK
CTI Link: 1
Extension: 30099
Type: ADJ-IP
COR: 1
Name: AES8
Unicode Name? n
```

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: SILDenver
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: 1
```

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 UII During Conference/Transfer? n
    Call Classification After Answer Supervision? n
                        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 which will be used later to configure Contact Center. In the compliance testing, the one VDN shown below was used.

```
list vdn

                        VECTOR DIRECTORY NUMBERS

Name (22 characters)  Ext/Skills  VDN          Vec          Orig          Evnt
Ovr COR  TN PRT Num  Meas Annc  Noti
Adj

Voice           31500           n 1      1   V   6      none
1
```


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
```

REASON CODE NAMES		
	Aux Work/ Interruptible?	Logout
Reason Code 1:	Default	/n
Reason Code 2:	Break	/n
Reason Code 3:	Lunch	/n
Reason Code 4:	Training	/n
Reason Code 5:		/n
Reason Code 6:		/n
Reason Code 7:		/n
Reason Code 8:		/n
Reason Code 9:		/n

Default Reason Code: 1

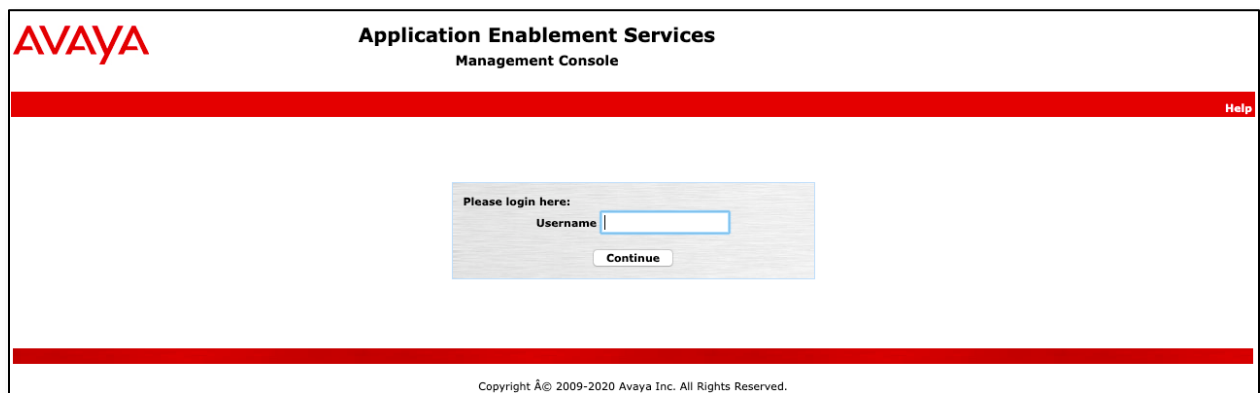
6. Configure Avaya Aura® Application Enablement Services

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

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer ICX user
- Administer security database
- Restart services
- Obtain Tlink name


6.1. Launch OAM Interface

Access the OAM web-based interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of the Application Enablement Services server. The **Please login here** screen is displayed. Log in using the appropriate credentials.



The screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. The title "Application Enablement Services Management Console" is centered at the top. 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:" and a "Username" label next to 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 text "Copyright © 2009-2020 Avaya Inc. All Rights Reserved." is displayed.

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



Application Enablement Services Management Console

Welcome: User cust
 Last login: Tue Mar 2 09:14:36 2021 from 192.168.4.131
 Number of prior failed login attempts: 0
 HostName/IP: sildvaes8.sildenver.org/10.64.115.28
 Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
 SW Version: 8.1.2.1.1.6-0
 Server Date and Time: Tue Mar 02 09:16:07 MST 2021
 HA Status: Not Configured

Home

Home | Help | Logout

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

Welcome to OAM

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


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

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

6.2. Verify License

System Manager was used as a central license server for the test environment. Log in using the appropriate credentials and navigate to display installed licenses. On System Manager, navigate to **Services → Licenses → Application_Enablement**.

Verify that there are sufficient licenses for **TSAPI Simultaneous Users** as shown above.


Aura® System Manager 8.1

Users Elements Services Widgets Shortcuts

admin

Home

Licenses

Licenses

- WebLM Home
- Install license
- Licensed products
- APPL_ENAB
- ▼ Application_Enablement
 - View license capacity
 - View peak usage
- COMMUNICATION_MANAGER
 - ▶ Call_Center
 - ▶ Communication_Manager
- Configure Centralized Licensing
- MSR
 - ▶ Media_Server
- SYSTEM_MANAGER
 - ▶ System_Manager
- SessionManager
 - ▶ SessionManager
- Utility_Services
 - ▶ Utility_Services
- Uninstall license
- Server properties
- Metering Collector Configuration
- Shortcuts

Application Enablement (CTI) - Release: 8 - SID: 10503000
Standard License file

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

License installed on: October 7, 2019 1:11:22 PM -07:00

License File Host IDs: VF-79-65-86-DB-65-01

Licensed Features

Feature (License Keyword)	Expiration date	Licensed capacity
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	1000
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	1000
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	3
DLG VALUE_AES_DLG	permanent	16
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	1000
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	3
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	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**, note that an existing TSAPI Link was used for testing, details are displayed using the **Edit Link** button.

Welcome: User cust
Last login: Tue Mar 2 09:14:36 2021 from 192.168.4.131
Number of prior failed login attempts: 0
HostName/IP: sildvaes8.sildenver.org/10.64.115.28
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.2.1.1.6-0
Server Date and Time: Tue Mar 02 09:26:06 MST 2021
HA Status: Not Configured

AVAYA Application Enablement Services Management Console

AE Services | TSAPI | TSAPI Links Home | Help | Logout

▼ AE Services

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

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
1	SILDVCM8	1	9	Both

Add Link Edit Link Delete Link

The **Add (or Edit) 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 “**SILDVCM8**” is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields.

Welcome: User cust
Last login: Tue Mar 2 09:14:36 2021 from 192.168.4.131
Number of prior failed login attempts: 0
HostName/IP: sildvaes8.sildenver.org/10.64.115.28
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.2.1.1.6-0
Server Date and Time: Tue Mar 02 09:29:08 MST 2021
HA Status: Not Configured

AVAYA Application Enablement Services Management Console

AE Services | TSAPI | TSAPI Links Home | Help | Logout

▼ AE Services

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

TSAPI Links

Edit TSAPI Links

Link 1

Switch Connection SILDVCM8

Switch CTI Link Number 1

ASAI Link Version 9

Security Both

Apply Changes Cancel Changes Advanced Settings

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. Following is the account after creation”:

Edit User

* User Id	<input type="text" value="tetravx"/>
* Common Name	<input type="text" value="VX"/>
* Surname	<input type="text" value="Tetra"/>
User Password	<input type="password"/>
Confirm Password	<input type="password"/>
Admin Note	<input type="text"/>
Avaya Role	<input type="text" value="None"/>
Business Category	<input type="text"/>
Car License	<input type="text"/>
CM Home	<input type="text"/>
Css Home	<input type="text"/>
CT User	<input type="text" value="Yes"/>

6.5. Administer Security Database

Select **Security** → **Security Database** → **Control** from the left pane, to display the **Enable SDB Control for DMCC Service** and **Enable SDB for TSAPI Service, JTAPI and Telephony Web Services** screen in the right pane. Make certain both parameters are unchecked, as shown below.

The screenshot shows the Avaya Application Enablement Services Management Console. The top navigation bar includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for "User cust" with login details. The left sidebar contains a tree view with "Security" expanded, showing "Security Database" and "Control". The main content area is titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" and contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services". An "Apply Changes" button is at the bottom.

In the event that the security database is used by the customer with parameter enabled, then navigate to **Security** → **Security Database** → **CTI Users** → **List All Users** and select the user created in **Section 6.7** (not shown) and click the Edit button. On the Edit CTI User screen, check **Unrestricted Access** to grant access to any devices administered in the ICX application.

The screenshot shows the Avaya Application Enablement Services Management Console with the "Edit CTI User" page. The left sidebar shows "Security" expanded, with "Security Database" and "CTI Users" expanded, and "List All Users" selected. The main content area is titled "Edit CTI User" and shows a form for "User Profile" with fields for "User ID", "Common Name", "Worktop Name", and "Unrestricted Access" (checked). Below this are sections for "Call and Device Control", "Call and Device Monitoring", and "Routing Control", each with a "None" dropdown menu. "Apply Changes" and "Cancel Changes" buttons are at the bottom.

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 Callback.

In this case, the associated Tlink name is “AVAYA#SILDVCM8#CSTA-S#SILDVAES8”. Note the use of the switch connection from **Section 6.5** 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 user "cust" with login details. A red navigation bar contains "Security | Security Database | Tlinks" and links for "Home | Help | Logout". The left sidebar lists various services, with "Security" expanded to show "Security Database" and "Tlinks" selected. The main content area, titled "Tlinks", shows a list of Tlink names. The first entry is "AVAYA#SILDVCM8#CSTA#SILDVAES8" with a blue selection icon. The second entry, "AVAYA#SILDVCM8#CSTA-S#SILDVAES8", is highlighted in yellow and has a "Delete Tlink" button next to it.

6.8. Restart Services

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, the title "Application Enablement Services Management Console", and a welcome message for user "cust" with system details. A red navigation bar shows "Maintenance | Service Controller" and links for "Home | Help | Logout".

On the left, a sidebar menu lists various sections: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance (selected), Date Time/NTP Server, Security Database, Service Controller (highlighted), Server Data, Networking, and Security.

The main content area, titled "Service Controller", contains a table with two columns: "Service" and "Controller Status".

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input type="checkbox"/> DMCC Service	Running
<input type="checkbox"/> CVLAN Service	Stopped
<input type="checkbox"/> DLG Service	Stopped
<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, a row of buttons includes "Start", "Stop", "Restart Service" (which is highlighted), "Restart AE Server", "Restart Linux", and "Restart Web Server".

7. Configure ICX Contact Center

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

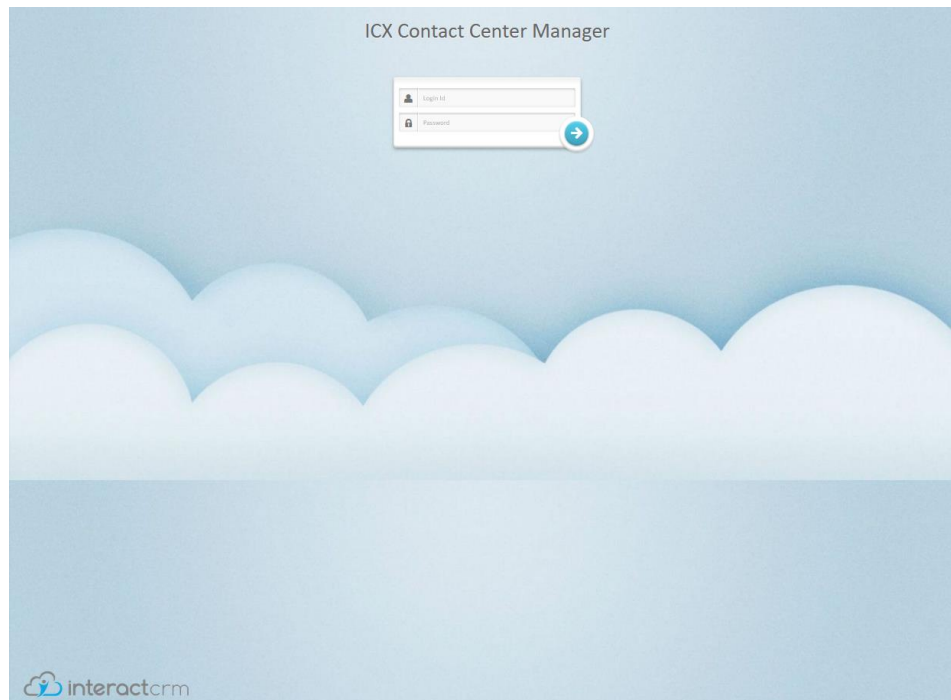
- Launch web interface
- Administer server
- Administer agents
- Administer queues
- Administer aux codes

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

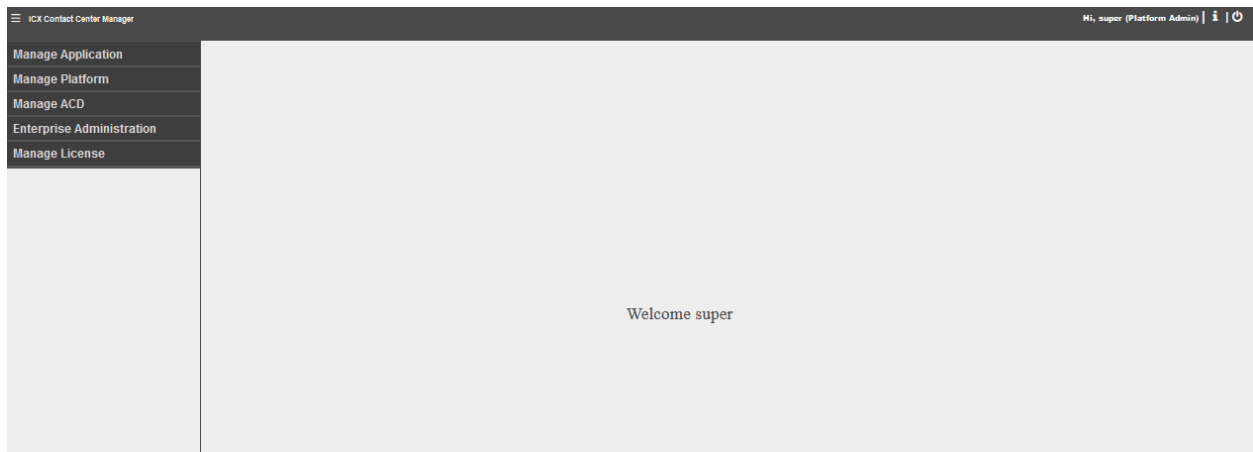
Launch the web interface by using the URL “https://ip-address:15050/ContactCenterManager” in an Internet Explorer browser window, where “ip-address” is the IP address of the ICX server running the Contact Center Manager component.

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

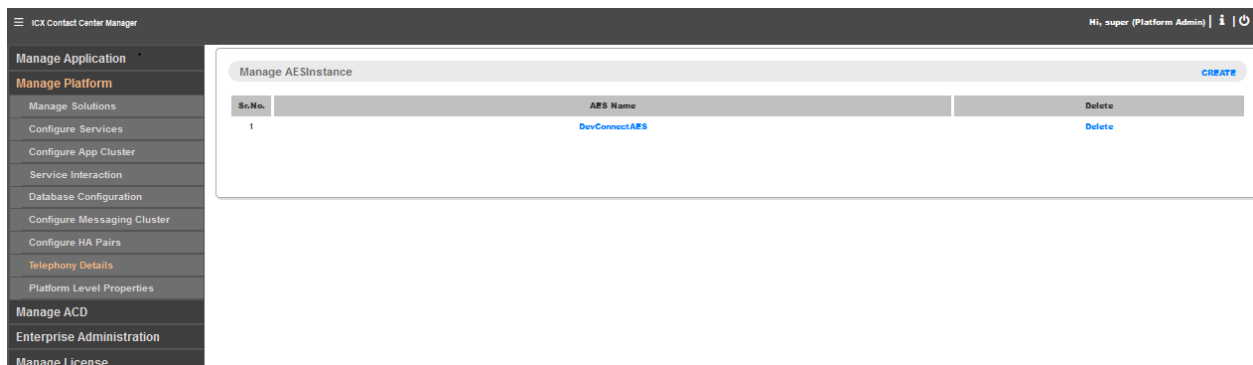


7.2. Administer Server

The **WELCOME** screen below is displayed



Select **Manage Platform**→ **Telephony Details** from the left pane, to display the **Manage AES Instance** screen. Click on the **AES** entry.



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

- **AES Server Address:** IP address of Application Enablement Services.
- **TSAPI Service Login ID:** The ICX user credentials from **Section 6.4**.
- **TSAPI Service Password:** The ICX user credentials from **Section 6.4**.
- **AES TLINK Identifier:** The Tlink name from **Section 6.7**.
- **TSAPI Port:** **450**
- **DMCC Port:** **4722**

The screenshot displays the 'Edit Telephony Details' configuration page in the ICX Contact Center Manager. The page is organized into three main sections: Telephony Details, TSAPI Service Details, and DMCC Service Details. The left sidebar provides navigation options, and the top right corner shows the user's name and role.

Telephony Details:

- *AES Server Instance Name : DevConnectAES
- Site : DMCC Primary Set 01 (dropdown)
- *AES Server Address : 10.64.115.28
- Status : ☒ Active ☐ Inactive

TSAPI Service Details:

- *AES TLINK Identifier : AVAYA#SILDVCM8#CSTA-
- *TSAPI Service Login ID : beta-vx
- *TSAPI Service Password : [masked]
- *Confirm Password : [masked]
- *TSAPI Port : 450
- Debug Level : 4 (Recommended) (dropdown)

DMCC Service Details:

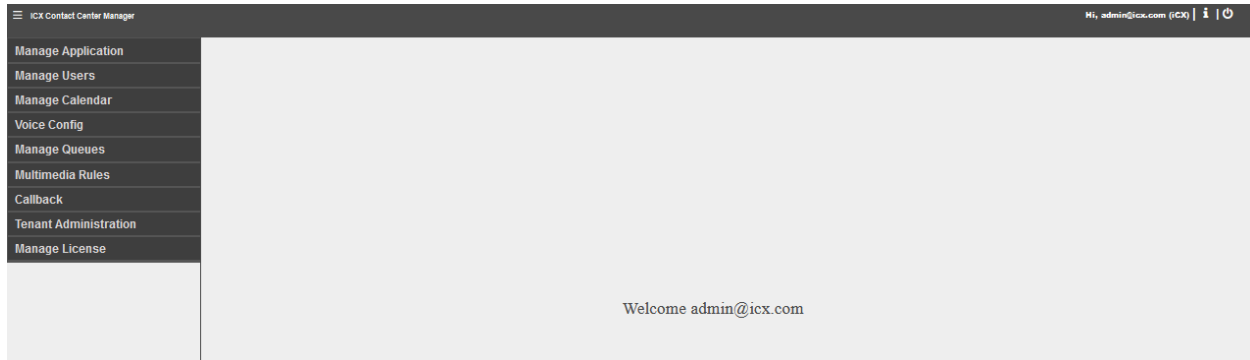
- *Switch Connection Name : SILDVCM8
- *Avaya Communication Manager IP : 10.64.115.25
- *AES CT User Name : beta-vx
- *AES CT User Password : [masked]
- *Confirm Password : [masked]
- *DMCC Port : 4722
- Audio Format (Codec) : G711U (dropdown)
- Encrypt Media Stream : ☐ AES ☒ None
- AES Secure : ☒ True ☐ False

Buttons at the bottom: Update, Cancel

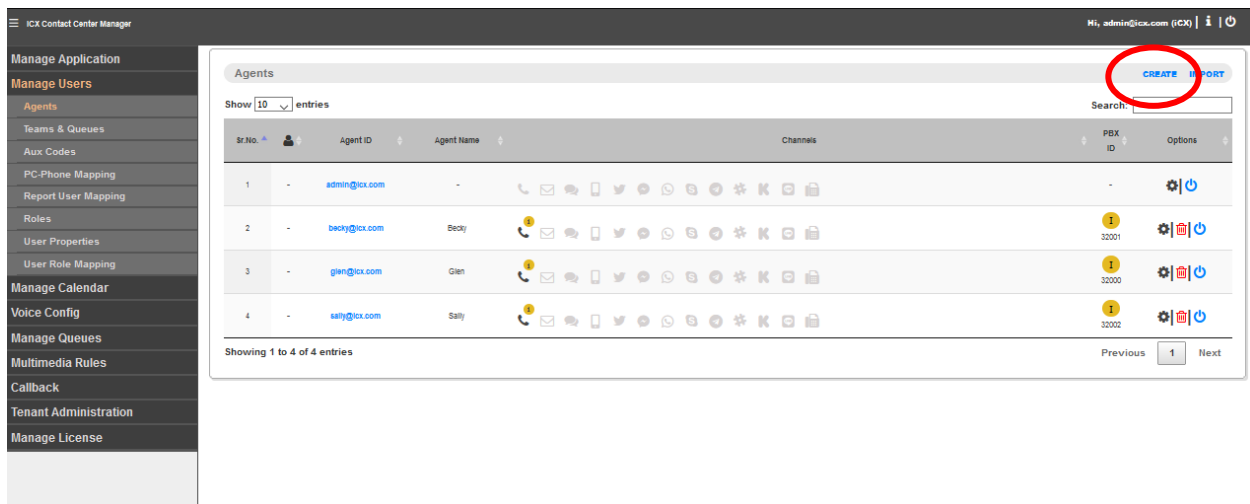
7.3. Administer Agents

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 **admin@icx.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 **Channel**, check **Phone (Avaya)**.

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

Retain the default values for the remaining fields.

Add Agent

Logon Information

Login ID: david@cx.com
Password: *****
Confirm Password: *****
Age: 25

Personal Information

First Name: David
Last Name: Smith
Preferred Name: David
Email ID: david@cx.com
Gender: Male

User Profile

Supervisor: OFF
BUE: OFF

Phone (Avaya) ☒

PBX ID: 32008
PBX Password: *****
Confirm PBX Password: *****
Hunt Group: 31000
Campaign Mode: Inbound Only

Multimedia

Email: 0
Chat: 0
Twitter: 0
SMS: 0
Fax: 0
Facebook: 0
Skype: 0
Telegram: 0
Slack: 0
Kik: 0
Line: 0
WhatsApp: 0

Additional configuration

Task Ceiling: 1
Blending: Open Blending
User Timezone: America/Chicago
Team: General
Site: DefaultSite
Group Ceiling: NA

Save Cancel

Repeat this section to add an agent for every agent. In the compliance testing, four agents were created, as shown below.

Agents

CREATE IMPORT

Show 10 entries Search:

Sr.No.	Agent ID	Agent Name	Channels	PBX ID	Options
1	admin@icx.com	-	[Icons]	-	[Settings, Status]
2	becky@icx.com	Becky	[Icons]	32001	[Settings, Deletion, Status]
3	david@icx.com	David	[Icons]	32005	[Settings, Deletion, Status]
4	glen@icx.com	Glen	[Icons]	32000	[Settings, Deletion, Status]
5	sally@icx.com	Sally	[Icons]	32002	[Settings, Deletion, Status]

Showing 1 to 5 of 5 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**.

Queues

CREATE

Display 50 records Search:

Sr.No.	Name	ID	Media	Entry Point	Addressable	Threshold	Action
1	Marketing Queue	31506 (Incoming VDN)	Phone (Avaya)	DefaultTenant	NO	---	[Edit, Deletion]

Previous 1 Next

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:** “Phone (Avaya)”
- **Entry Point:** Select the applicable tenant, in this case “Default Tenant”.
- **ID:** The Agent VDN extension.
- **Name:** The corresponding VDN name from **Section 5.4**.
- **Queue Group:** “DefaultVoiceQueueGroup”

ICX Contact Center Manager

Hi, admin@icx.com (iCX) | i | ⚙

Add Queue

Media Type * Phone (Avaya) ▾

Entry Point * DefaultTenant ▾

ID * 31500 Enter Hunt group Extension here

Name * Sales Queue

Queue Type * Agent VDN ▾

Queue Group * DefaultVoiceQueueGroup ▾

Timed ACW in Secs :

WrapUp Category 1 : --Select-- ▾

WrapUp Category 2 : --Select-- ▾

WrapUp Category 3 : --Select-- ▾

WrapUp Category 4 : --Select-- ▾

WrapUp Category 5 : --Select-- ▾

Enable Blending : ☐

Add Cancel

Repeat this section to add a queue for each VDN. In the compliance testing, below queues were created.

ICX Contact Center Manager

Hi, admin@icx.com (iCX) | i | ⚙

Queues CREATE

Display 50 ▾ records Search:

Sr.No. ▲	Name	ID	Media	Entry Point	Addressable	Threshold	Action
1	Marketing Queue	31506 (Incoming VDN)	Phone (Avaya)	DefaultTenant	NO	---	
2	Sales Queue	31500 (Agent VDN)	Phone (Avaya)	DefaultTenant	NO		
3	Sales Skill	31000 - 1	Phone (Avaya)	DefaultTenant	NO		
4	Support Queue	31505 (Transfer VDN)	Phone (Avaya)	DefaultTenant	YES	---	

Showing 1 to 4 of 4 entries Previous 1 Next

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 Contact Center Manager

Hi, admin@icx.com (iCX) | i | ⚙

Manage Application

Manage Users

Agents

Teams & Queues

Aux Codes

PC-Phone Mapping

Report User Mapping

Roles

User Properties

User Role Mapping

Manage Calendar

Voice Config

Manage Queues

Multimedia Rules

Callback

Tenant Administration

Manage License

Manage Aux Codes

Display 50 records Search:

Sr.No.	Aux Code Name	AUX Code on PBX	System AUX Type	Is Payable Aux	Action
1	Aux On Login	1	Yes	1	
2	Blend Aux	55	Yes	0	
3	iCX Outbound	11	Yes	0	
4	Meeting	23	No	1	
5	Mentoring	7	No	0	
6	RONA	5	Yes	0	

Showing 1 to 6 of 6 entries Previous 1 Next

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**.
- **Aux Code on PBX:** The first aux work reason code number in **Section 5.5**.

ICX Contact Center Manager

Hi, admin@icx.com (iCX) | i | ⚙

Manage Application

Manage Users

Agents

Teams & Queues

Aux Codes

PC-Phone Mapping

Report User Mapping

Roles

User Properties

User Role Mapping

Manage Calendar

Add AuxCode

AUX Code Name : Lunch Break

AUX Code on PBX : 5



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**! Error! Reference source not found.. In the compliance testing, 7 aux codes were created, as shown on next page.

ICX Contact Center Manager

Hi, admin@icx.com (iCX) |  

Manage Application

Manage Users

Agents

Teams & Queues

Aux Codes

PC-Phone Mapping

Report User Mapping

Roles

User Properties

User Role Mapping

Manage Calendar

Voice Config

Manage Queues

Multimedia Rules

Callback

Tenant Administration








Manage License

Manage Aux Codes

Create

Display 50 records

Search:

Sr.No. ▲	Aux Code Name	AUX Code on PBX	System AUX Type	Is Payable Aux	Action
1	Aux On Login	1	Yes	1	
2	Blend Aux	55	Yes	0	
3	iCX Outbound	11	Yes	0	
4	Lunch Break	3	No	0	
5	Meeting	23	No	1	
6	Mentoring	7	No	0	
7	RONA	5	Yes	0	

Showing 1 to 7 of 7 entries

Previous

1

Next

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 Error! Reference source not found.**, 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	9	no	sildvaes8	established	15	15

Verify the registration status of Agents by using the “list agent-login-ID” command. Verify that all Agent extensions are displayed.

```
list agent-loginID
```

AGENT LOGINID								
Login ID	Name	Extension		Dir	Agt	AAS/AUD	COR	AgPr SO
	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv
32001	SIL Agent 2	30008			1		1	lv1
	1/01	/	/	/	/	/	/	/
32002	Agent 3	30007			1		1	lv1
	1/01	/	/	/	/	/	/	/

With an active call, use the status station command to verify the agent is in an ACD call.

```
status station 30007
```

ACD STATUS							Page 9 of 9
Grp/Mod	Grp/Mod	Grp/Mod	Grp/Mod	Grp/Mod	Grp/Mod	Grp/Mod	
1/AI	/	/	/	/	/	/	On ACD Call? yes
/	/	/	/	/	/	/	
/	/	/	/	/	/	/	Occupancy: 72.0

8.2. Verify Avaya Aura® Application Enablement Services

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

Verify that the **Status** is “Talking” for the TSAPI link administered in **Section 6.3**, as shown below.

AVAYA

Application Enablement Services
Management Console

Welcome: User cust
Last login: Thu Mar 4 08:31:40 2021 from 192.168.4.131
Number of prior failed login attempts: 0
HostName/IP: sildvae8.sildenver.org/10.64.115.28
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.2.1.1.6-0
Server Date and Time: Mon Mar 08 07:57:56 MST 2021
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

Logs

Log Manager

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
	1	SILDVCM8	1	Talking	Mon Feb 22 14:12:48 2021	Online	18	9	49	53	30

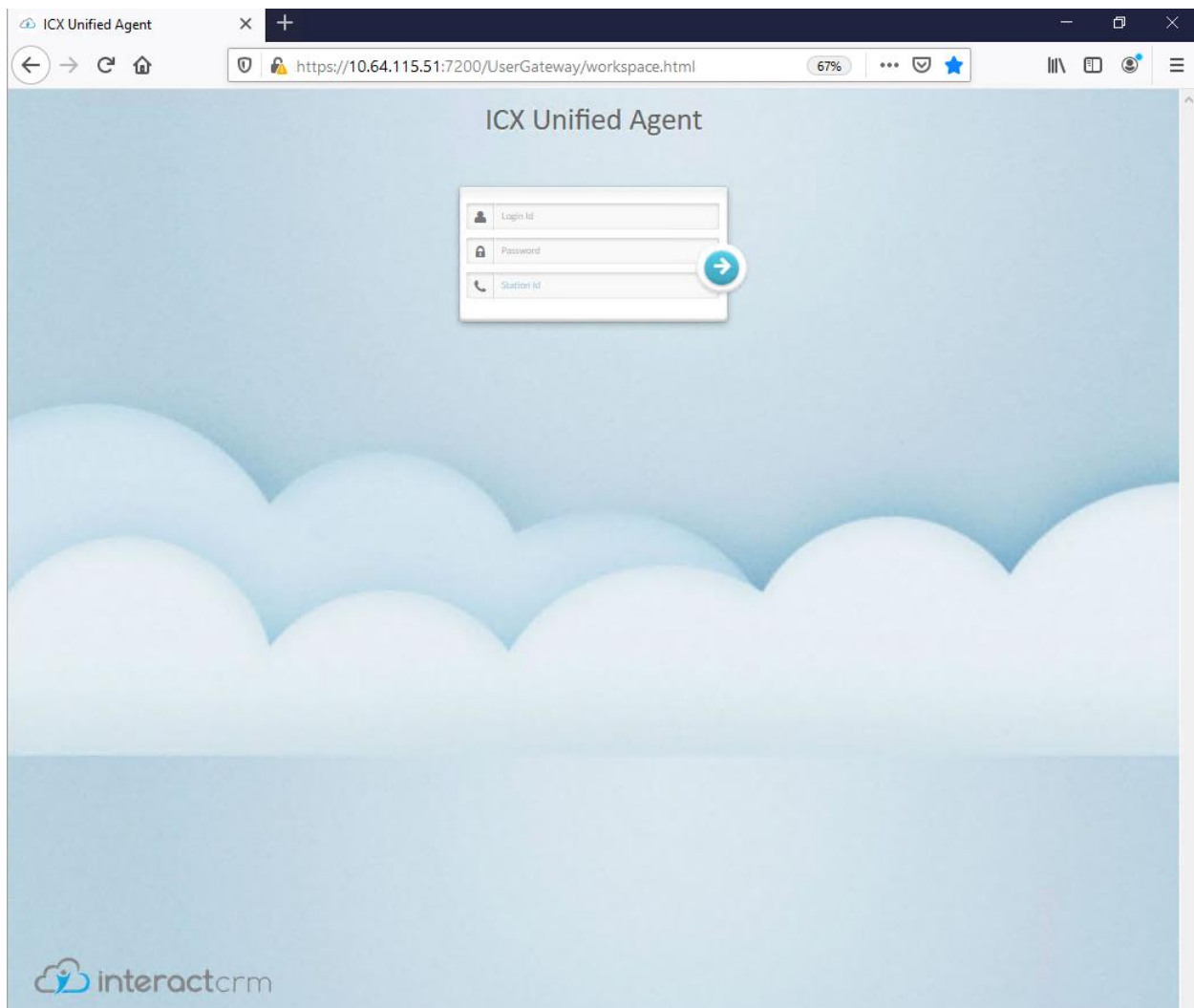
For service-wide information, choose one of the following:

8.3. Verify ICX

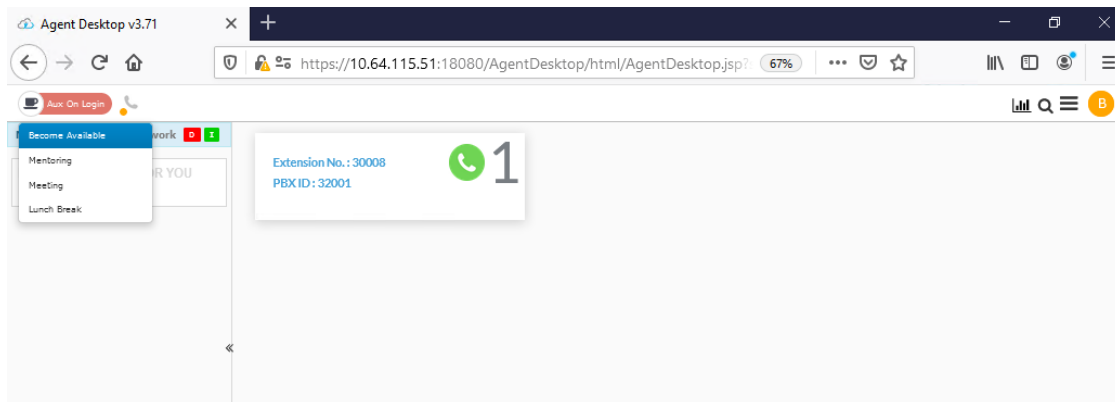
From the agent PC, launch the Firefox browser and enter the URL:
“https://IPAddr:7200/UserGateway/workspace.html”

where “IPADDR” is the IP address of the ICX server running the Interaction Manager component.

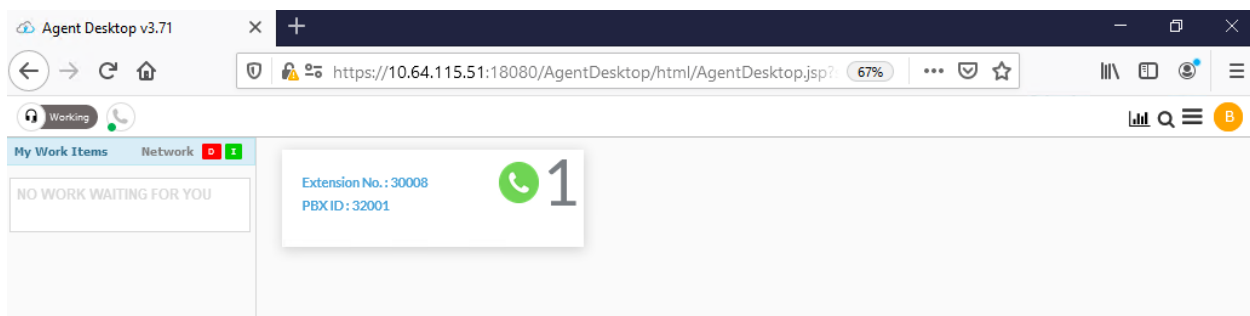
The **Unified Agent Desktop** screen is displayed. For **Login Id** and **Password**, enter the relevant user credentials from **Section 7.3**. For **Station Id**, enter the applicable agent station extension.



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

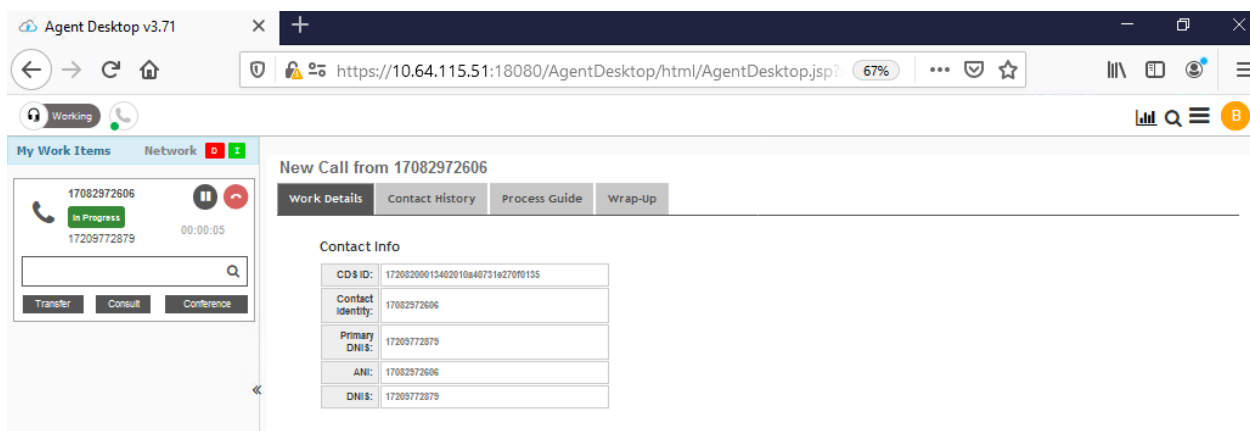


The left pane is updated, showing the agent in the **Working** mode, as shown below.



Make an incoming ACD call. Verify that the screen of the available agent is updated to reflect 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 8.1.X available at <http://support.avaya.com>.
2. *Administering and Maintaining Aura® Application Enablement Services*, Release 8.1.X, available at <http://support.avaya.com>.
3. *ICX Voice Install Guide 3.17.7*, available upon request to Interactcrm Support.

©2021 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.