



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

---

# **Application Notes for InGenius Connector Enterprise 2.20 with Avaya Aura® Communication Manager 6.3 and Avaya Aura® Application Enablement Services 6.3 using Salesforce.com – Issue 1.0**

## **Abstract**

These Application Notes describe the configuration steps required for InGenius Connector Enterprise 2.20 to interoperate with Avaya Aura® Communication Manager 6.3 and Avaya Aura® Application Enablement Services 6.3 using Salesforce.com. InGenius Connector Enterprise is a CRM-VoIP integration tool that sits between the customer's phone system and a CRM application.

In the compliance testing, InGenius Connector Enterprise used the Device, Media, and Call Control interface from Avaya Aura® Application Enablement Services to monitor contact center agents on Avaya Aura® Communication Manager, to provide screen pop, call control, and click-to-dial features from the agent desktops connected to Salesforce.com.

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 InGenius Connector Enterprise (ICE) 2.20 to interoperate with Avaya Aura® Communication Manager 6.3 and Avaya Aura® Application Enablement Services 6.3 using Salesforce.com. InGenius Connector Enterprise is a CRM-VoIP integration tool that sits between the customer's phone system and a CRM application.

In the compliance testing, ICE used the Device, Media, and Call Control (DMCC) XML interface from Avaya Aura® Application Enablement Services to monitor contact center agents on Avaya Aura® Communication Manager, to provide screen pop, call control, and click-to-dial features from the agent desktops. The agent desktops were connected to the cloud-based CRM provider Salesforce.com via an Internet browser.

## 2. General Test Approach and Test Results

The feature test cases were performed manually. Upon an agent log in, the application used DMCC to query device information and agent state, logged the agent into Communication Manager if needed, and requested device monitoring.

For the manual part of the testing, incoming ACD calls were placed with available agents that have web browser connections to Salesforce.com. All necessary call actions were initiated from the agent desktop and/or telephone. The click-to-dial calls were initiated by clicking on the contact phone number displayed on the agent desktop.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to the ICE 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 ICE:

- Use of DMCC logical device services to set agent states, including log in, log out, and work mode changes with support for pending modes and reason codes.
- Use of DMCC snapshot services to obtain information on agent stations and existing calls.
- Use of DMCC monitoring services to monitor agent stations and existing calls.
- Use of DMCC call control services to support call control and click-to-dial features.
- 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, send DTMF, click-to-dial from contact phone number, pending aux work, and reason codes.

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

## 2.2. Test Results

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

- 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.
- For blind transfer of outbound calls using the single step transfer service, the transfer-to agent may not receive a screen pop of the contact record associated with the called party on the PSTN. The screen pop is dependent on the PSTN service provider sending the connected number. For the same reason, the conference-to agent may not receive a screen pop for a conferenced outbound call.
- Depending on the agent desktop machine and internet bandwidth, call control actions may not always be accepted on the initial click. The acceptance can be improved by hovering over the call control icon to stop the icon animation prior to actual clicking, or by disabling icon animation via settings.

## 2.3. Support

Technical support on ICE can be obtained through the following:

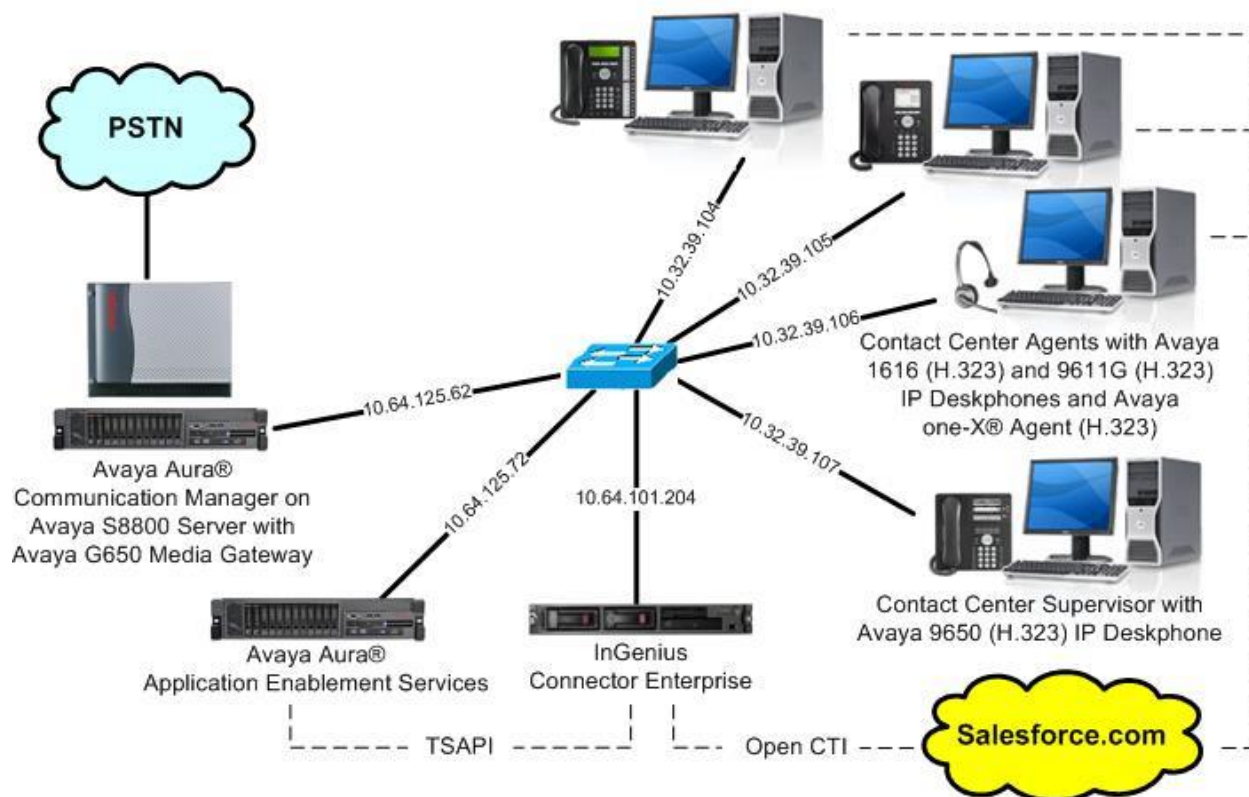
- **Phone:** (613) 591-9002
- **Email:** [icesupport@ingenius.com](mailto:icesupport@ingenius.com)
- **Web :** <http://ingenius.com/resources/support/>

### 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, ICE 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, 65003
Agent IDs	65881, 65882, 65883
Agent Passwords	65881, 65882, 65883



**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	6.3.6 (R016x.03.0.124.0-21591)
Avaya Aura® Application Enablement Services	6.3.3 SP1 (6.3.3.1.10-0)
Avaya one-X® Agent	2.5.5 (2.5.50022.0)
Avaya 1616 IP Deskphone (H.323)	1.350B
Avaya 9611G IP Deskphone (H.323)	6.4.0.14
Avaya 9650 IP Deskphone (H.323)	3.230A
InGenius Connector Enterprise on Windows Server 2008 <ul style="list-style-type: none"><li>• Avaya DMCC XML</li><li>• Configuration Tool</li><li>• Connector Enterprise Open CTI</li></ul>	2.20 R2 Enterprise SP 1 6.1 2.20.230.8421 1.17
Salesforce.com	Winter 2015

## 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 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 ICE.

```
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 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 reason codes, which will be used later to configure ICE.

```
change reason-code-names                                     Page 1 of 1

                                REASON CODE NAMES

                                Aux Work/      Logout
                                Interruptible?

Reason Code 1: Lunch           /n End Session
Reason Code 2: Break          /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
- Disable security database
- Restart service
- Administer InGenius user
- Administer ports

### 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 shows the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a user status box on the right. The status box displays: "Welcome: User", "Last login: Tue Oct 28 10:55:57 2014 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 Oct 28 11:42:34 MDT 2014", and "HA Status: Not Configured". Below the header is a red navigation bar with "Home" on the left and "Home | Help | Logout" on the right. The main content area is divided into a left sidebar and a central pane. The sidebar contains a list of menu items: "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking", "Security", "Status", "User Management", "Utilities", and "Help". The central pane is titled "Welcome to OAM" and contains a paragraph: "The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:". This is followed by a bulleted list: "• 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.", and "• Help - Use Help to obtain a few tips for using the OAM Help system". At the bottom of the central pane, a note states: "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 shows the Avaya Application Enablement Services Management Console with the "Licensing" menu item selected in the left sidebar. The sidebar menu items are: "AE Services", "Communication Manager Interface", "Licensing" (highlighted), "WebLM Server Address", "WebLM Server Access" (highlighted), "Reserved Licenses", "Maintenance", "Networking", and "Security". The central pane is titled "Licensing" and contains three sections of instructions: "If you are setting up and maintaining the WebLM, you need to use the following:" followed by "• WebLM Server Address", "If you are importing, setting up and maintaining the license, you need to use the following:" followed by "• WebLM Server Access", and "If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:" followed by "• Reserved Licenses". The top header and status box are identical to the previous screenshot. The red navigation bar shows "Licensing" on the left and "Home | Help | Logout" on the right.

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 are sufficient licenses for **TSAPI Simultaneous Users**, as shown below. Note that the TSAPI license is used for device monitoring and call control via DMCC, and that no specific DMCC license is required for integration with ICE.


**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-ED-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;CtiS MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_ LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;u TrustedApplications: IPS_001, BasicUnrestrict DMCUnrestricted; 1XP_001, BasicUnrestricted DMCUnrestricted; 1XM_001, BasicUnrestricted DMCUnrestricted; PC_001, BasicUnrestricted DMCUnrestricted; CIE_001, BasicUnrestricted DMCUnrestricted; OSPC_001, BasicUnrestrict 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, BasicUnrestrict 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 right corner displays user information: "Welcome: User", "Last login: Tue Oct 28 10:55:57 2014 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 Oct 28 11:42:34 MDT 2014", and "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 "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 AVAYA Application Enablement Services Management Console with the "Add TSAPI Links" screen. The left navigation pane shows "AE Services" expanded, with "TSAPI" selected, and "TSAPI Links" highlighted. The main content area is titled "Add TSAPI Links" and contains form fields for "Link", "Switch Connection", "Switch CTI Link Number", "ASAI Link Version", and "Security". The "Link" field has a value of "1", "Switch Connection" has "S8800", "Switch CTI Link Number" has "2", "ASAI Link Version" has "6", and "Security" has "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 Oct 28 10:55:57 2014 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 Oct 28 11:42:34 MDT 2014  
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 Oct 28 10:55:57 2014 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 Oct 28 11:42:34 MDT 2014  
HA Status: Not Configured

Maintenance | Service ControllerHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▼ Maintenance

▶ Date Time/NTP Server

▶ Security Database

▶ Service Controller

▶ Server Data

▶ Networking

▶ Security

▶ Status

▶ User Management

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. Administer InGenius 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 Oct 28 10:55:57 2014 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 Oct 28 11:42:34 MDT 2014  
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



## 6.7. Administer Ports

Select **Networking** → **Ports** from the left pane, to display the **Ports** screen in the right pane.

In the **DMCC Server Ports** section, select the radio button for **Encrypted Port** under the **Enabled** column, as shown below. Retain the default values in the remaining fields.

**AVAYA**

**Application Enablement Services**  
Management Console

Welcome: User  
Last login: Tue Oct 28 10:55:57 2014 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 Oct 28 11:42:34 MDT 2014  
HA Status: Not Configured

Networking | Ports

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▼ Networking

▶ AE Service IP (Local IP)

▶ Network Configure

▶ Ports

▶ TCP Settings

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Ports

CVLAN Ports

Unencrypted TCP Port9999Enabled Disabled

Encrypted TCP Port9998Enabled Disabled

DLG PortTCP Port5678

TSAPI Ports

TSAPI Service Port450Enabled Disabled

Local TLINK Ports

TCP Port Min1024

TCP Port Max1039

Unencrypted TLINK Ports

TCP Port Min1050

TCP Port Max1065

Encrypted TLINK Ports

TCP Port Min1066

TCP Port Max1081

DMCC Server Ports

Unencrypted Port4721Enabled Disabled

Encrypted Port4722Enabled Disabled

TR/87 Port4723Enabled Disabled

## 7. Configure InGenius Connector Enterprise

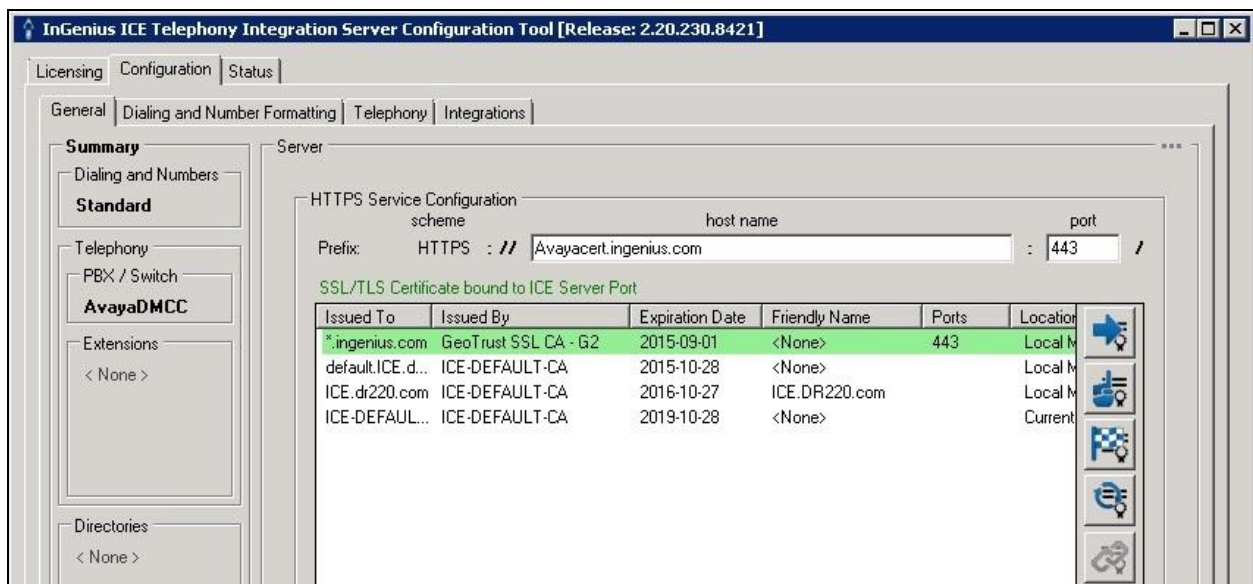
This section provides the procedures for configuring ICE. The procedures include the following areas:

- Launch configuration tool
- Administer dialing and number formatting
- Administer telephony
- Start service
- Obtain CTI adapter URL

This section assumes the Connector Enterprise Open CTI package has been installed, with Call Centre created, and users created and assigned to the Call Centre. Refer to reference [3] for more details.

### 7.1. Launch Configuration Tool

From the ICE server, select **Start → All Programs → InGenius → InGenius Connector Enterprise → Configuration Tool** to display the **InGenius ICE Telephony Integration Server Configuration Tool** screen below.



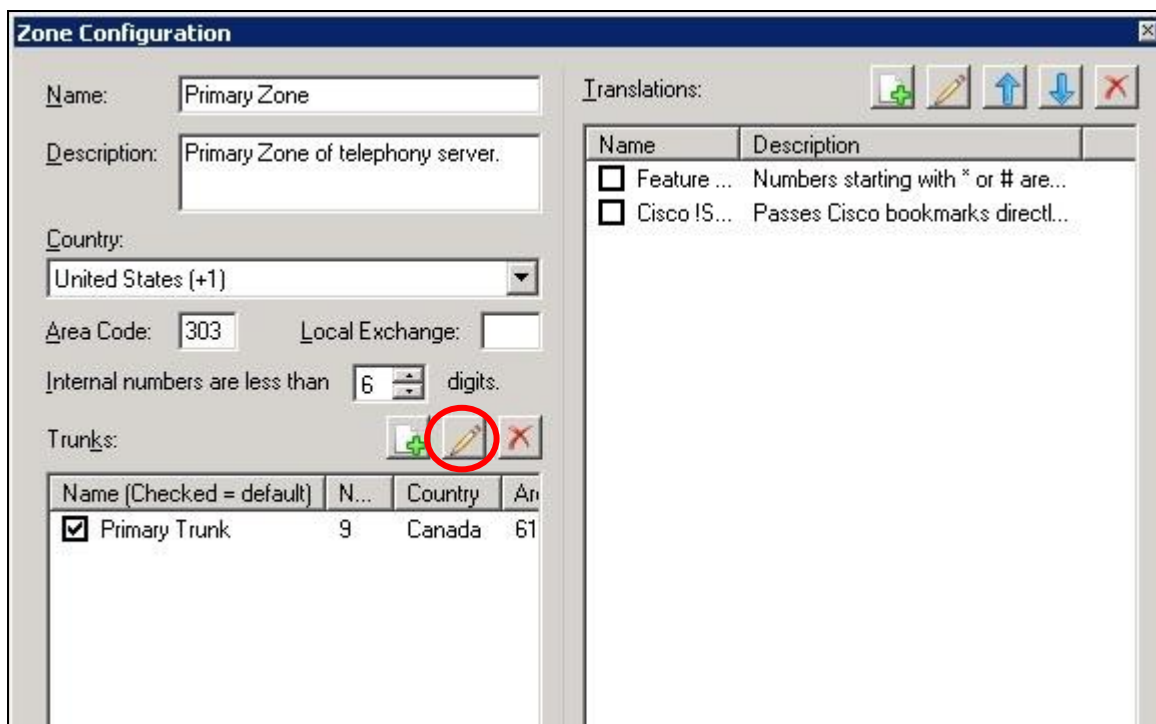
## 7.2. Administer Dialing and Number Formatting

Select **Configuration → Dialing and Number Formatting** from the top menu, followed by the **Zones** tab. Select the default entry, and click the **Edit translation** icon shown below.



The **Zone Configuration** screen is displayed next. For **Country**, **Area Code**, and **Internal numbers are less than**, select the values to match the network configuration. Retain the default values in the remaining fields.

Select the default entry in the **Trunks** sub-section, and click on the **Edit Trunk** icon shown below.



The **Trunk** screen is displayed. Follow reference [4] to update trunk parameter values to match the network configuration. The screenshot below shows the values used in the compliance testing.

The screenshot shows a 'Trunk' configuration window with the following fields and options:

- Name:** Primary Trunk
- Description:** Primary trunk of telephony server.
- Prefix:** 9
- Country:** United States (+1)
- Area Code:** 303
- Local Exchange:**
- Allowed calls:**
  - ☒ Local
  - ☒ Dial area code for local calls
  - ☒ Long Distance
  - ☒ International
- Long distance carrier code:**
- International carrier code:**
- Test dialing:**
  - Enter number to dial:**
  - Expanded to:**
  - Dialable:**

On the right side, there is a 'Translations to dialable:' section with a table:

Name	Description
<input type="checkbox"/> Argentina ...	International call from North A...

At the bottom right, there are buttons for 'Auto configure local dialing', 'OK', and 'Cancel'.

### 7.3. Administer Telephony

The **InGenius ICE Telephony Integration Server Configuration Tool** screen is displayed again. Select **Configuration → Telephony** from the top menu, followed by the **Connection Info** tab to display the screen below.

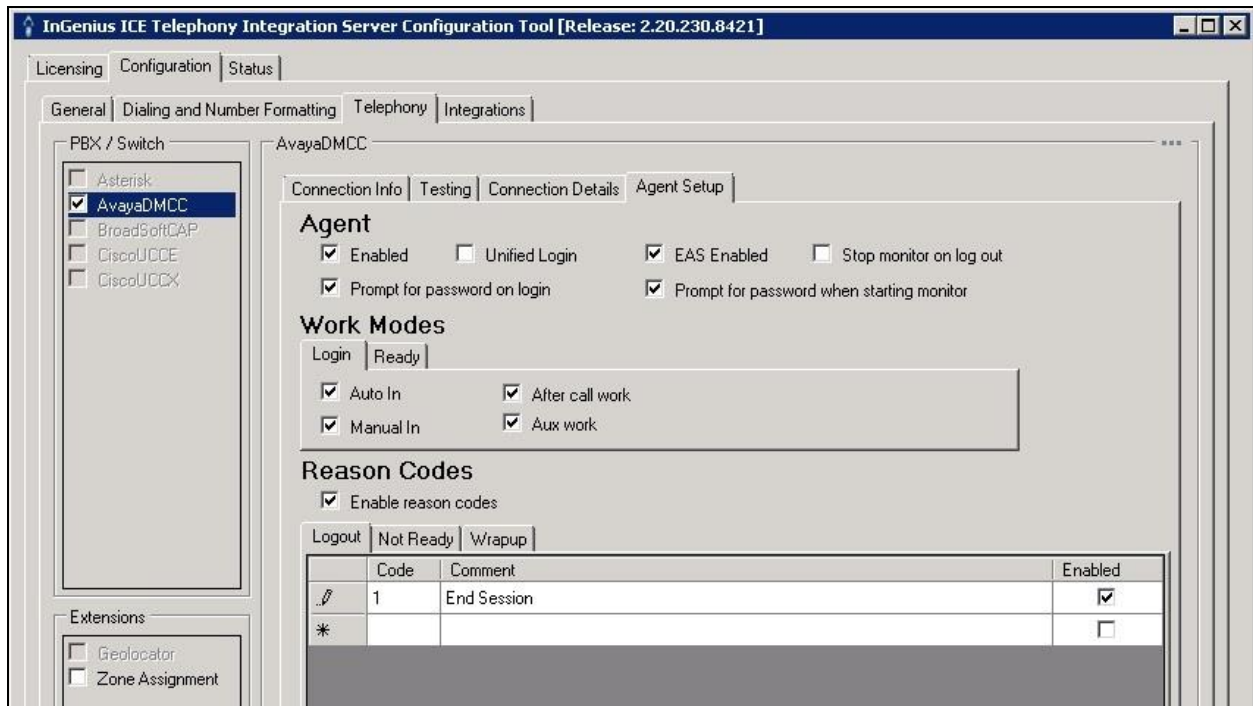
Enter the following values for the specified fields, and retain the default values in the remaining fields.

- **Address:** The IP address of Application Enablement Services.
- **Username:** The InGenius user credentials from **Section 6.6**.
- **Password:** The InGenius user credentials from **Section 6.6**.
- **Server name:** The relevant switch connection name from **Section 6.3**.

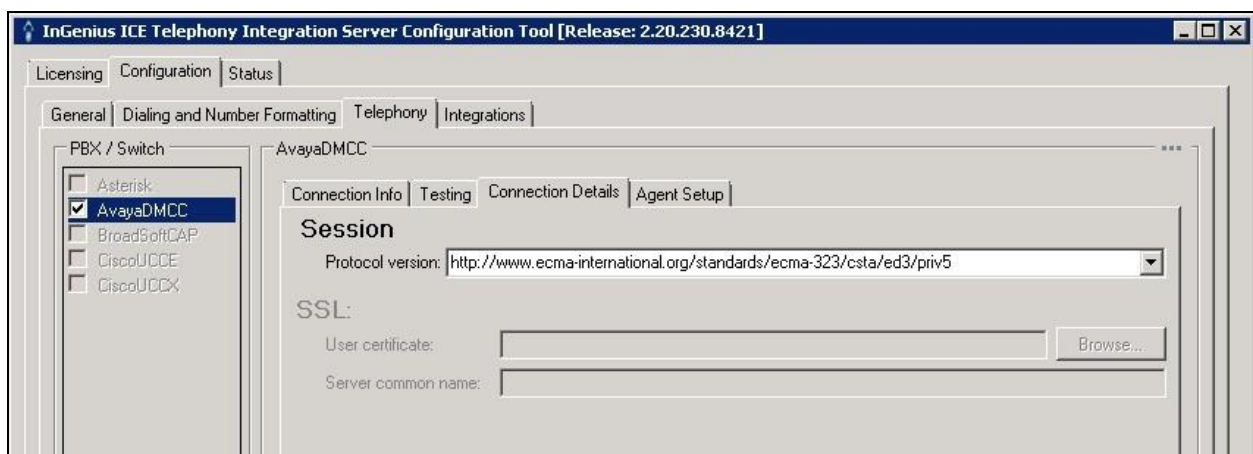
The screenshot shows the 'InGenius ICE Telephony Integration Server Configuration Tool' window. The 'Configuration' tab is selected, and the 'Telephony' sub-tab is active. On the left, under 'PBX / Switch', 'AvayaDMCC' is selected. Under 'Extensions', 'Geolocator' and 'Zone Assignment' are unchecked. The main area shows 'AvayaDMCC' configuration. The 'Connection Info' sub-tab is active. Under 'Application Enablement Services (AES)', the 'Address' is '10.64.125.72', 'Port' is '4721', 'Username' is 'ingenius', and 'Password' is masked. There is an unchecked checkbox for 'Use secondary server if primary fails to connect' with its own fields. There is also an unchecked checkbox for 'Use secure connection'. Under 'Connection Manager (CM)', the 'Server name' is 'S8800'.

Select the **Agent Setup** tab to display the screen below. Follow reference [4] to update parameters in the **Agent** and **Work Modes** sub-sections to the proper settings. The screenshot below shows the values used in the compliance testing.

For contact centers that use reason codes, check **Enable reason codes** in the **Reason Codes** sub-section, and follow reference [4] to create reason code entries to match **Section 5.4**.

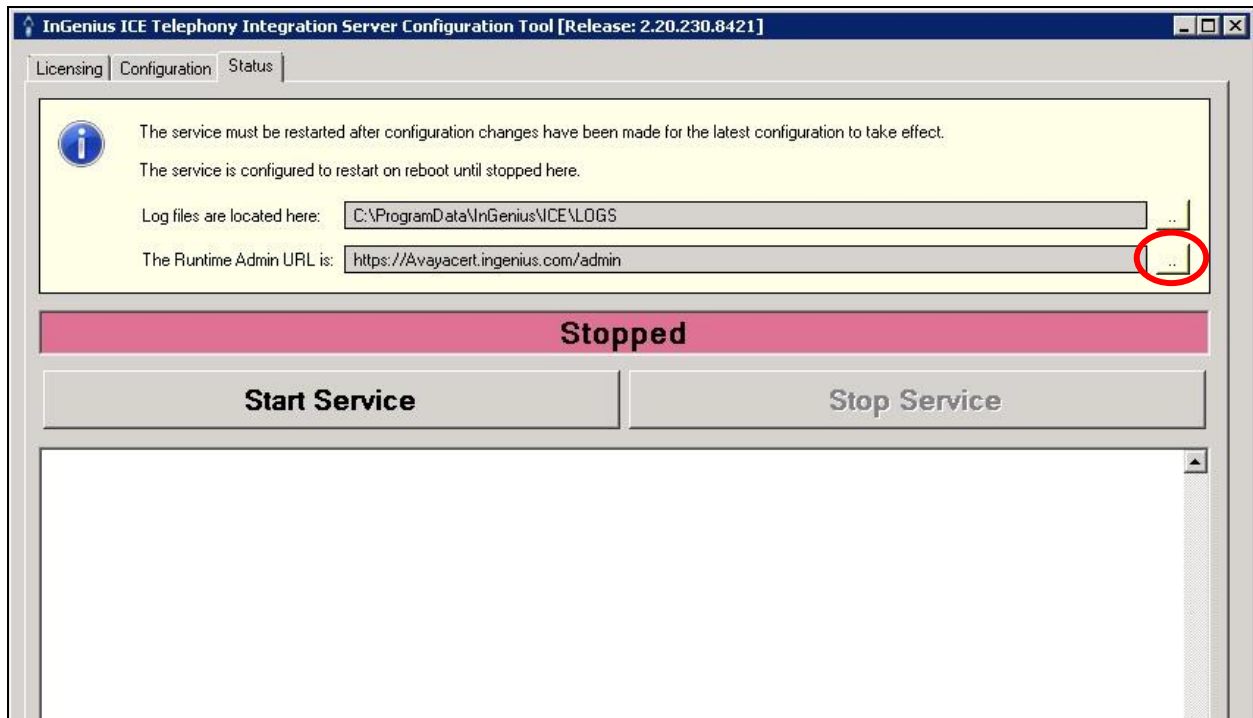


Select the **Connection Details** tab to display the screen below. For **Protocol version**, retain the default value shown below.



## 7.4. Start Service

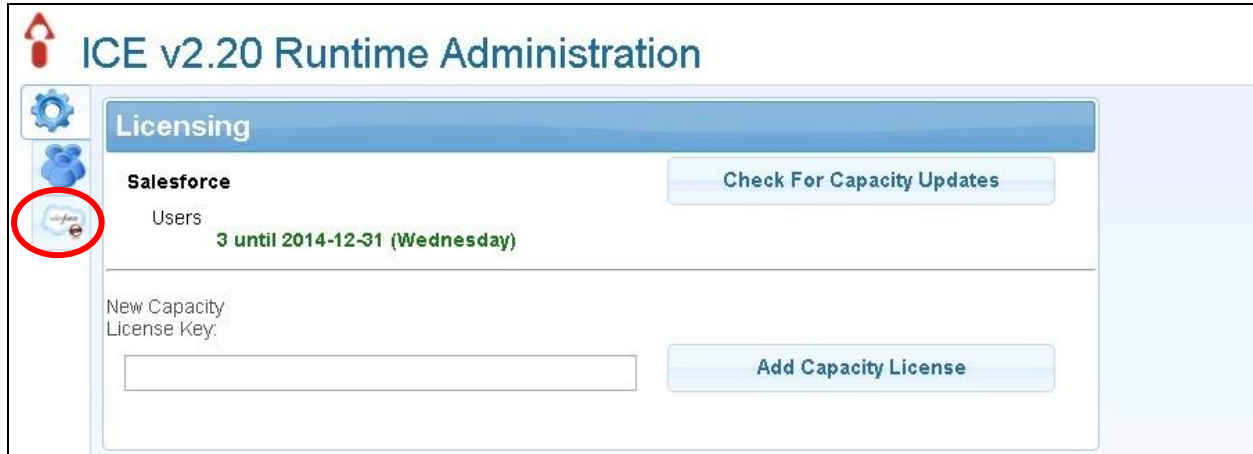
Select **Status** from the top menu to display the screen below, and click **Start Service**. After starting the service, click on the icon associated with the runtime URL shown below.





## 7.5. Obtain CTI Adapter URL

A browser is launched and displays the **ICE v2.20 Runtime Administration** screen. Click on the **Salesforce** icon from the left pane.



The screen is updated, showing a list of pre-configured profiles. Click on the **Edit** icon associated with the proper profile.





The screen is updated as shown below. Make a note of the **CTI Adapter URL**, which will be used by the agents with Salesforce.com.

The screenshot shows the 'ICE v2.20 Runtime Administration' web interface. The browser address bar displays 'https://ice.dr220.com/admin/default.html'. The page title is 'ICE v2.20 Runtime Administration' with a user 'admin' logged in. A navigation bar includes a 'Back to Call Center Profiles' button. The main heading is 'Edit call center profile: AvayaCert'. Below this is a tabbed interface with tabs numbered 1 through 9, and 'Save' and 'Next' buttons. Tab 1, 'General Info', is selected. On the left, a sidebar shows a tree view: 'Call Center' > 'ICE Call Center' > 'All Call Centers > ICE Call Center' > 'Call Center Detail' > 'General Information'. The 'General Information' section is expanded, showing 'Internal Name' as 'ICECALLCENTER' and 'Display Name' as 'ICE Call Center'. The 'CTI Adapter URL' is set to 'https://cs9.salesforce.com', which is circled in red. Other fields include 'Call center profile title (aka Display Name)' set to 'Avaya\_Cert' and a checkbox for 'Enable Console UI in Service Cloud Console'. A note at the bottom states: 'Any changes you make in the following sections will be applied to the UI as soon as you click Save.'

## 8. Verification Steps

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

### 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		no		down	0	0
2	6	no	aes_125_72	established	665	665

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

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

Verify the **User** column shows an active session with the InGenius user name from **Section 6.6**.

**Application Enablement Services  
Management Console**

Welcome: User  
Last login: Thu Oct 30 07:22:50 2014 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: Thu Oct 30 07:25:24 MDT 2014  
HA Status: Not Configured

Status | Status and Control | **DMCC Service Summary** | Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ **Status**

Alarm Viewer

Log Manager

▶ Logs

▼ **Status and Control**

■ CVLAN Service Summary

■ DLG Services Summary

■ **DMCC Service Summary**

**DMCC Service Summary - Session Summary**

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)  
Generated on Thu Oct 30 07:25:14 MDT 2014

Service Uptime: 2 days, 20 hours 58 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 14

Number of Existing Devices: 0

Number of Devices Created Since Service Boot: 0


	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	9AA4A23F352B078C1 44F7FE68C5FA1C0-14	ingenius	ICE Avaya Plugin	10.64.101.204	XML Unencrypted	0

Terminate Sessions | Show Terminated Sessions

Item 1-1 of 1  
1 Go

Verify the status of the TSAPI link by selecting **Status → Status and Control → TSAPI Service Summary** from the left pane. The **TSAPI Link Details** screen is displayed.

Verify the **Status** is “Talking” for the TSAPI link administered in **Section 6.3**, and that the **Associations** column reflects the number of agents from **Section 3** that are currently logged into ICE and therefore monitored, in this case “3”.



## Application Enablement Services

### Management Console

Welcome: User  
 Last login: Thu Oct 30 07:22:50 2014 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: Thu Oct 30 07:23:46 MDT 2014  
 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

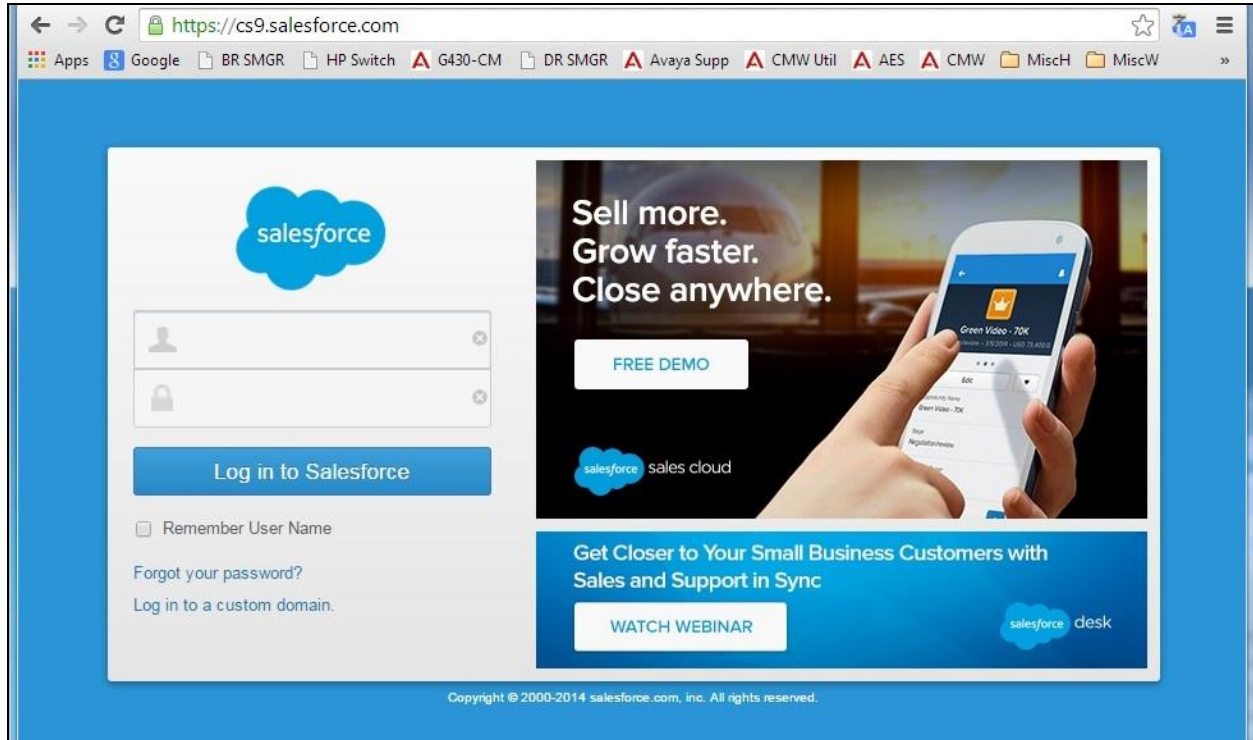
	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input checked="" type="radio"/>	1	S8800	2	Talking	Mon Oct 27 11:28:03 2014	Online	16	3	707	707	30
<input type="radio"/>	2	S8300D	1	Switch Down	Mon Oct 27 10:26:02 2014	Online	16	0	0	0	30

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

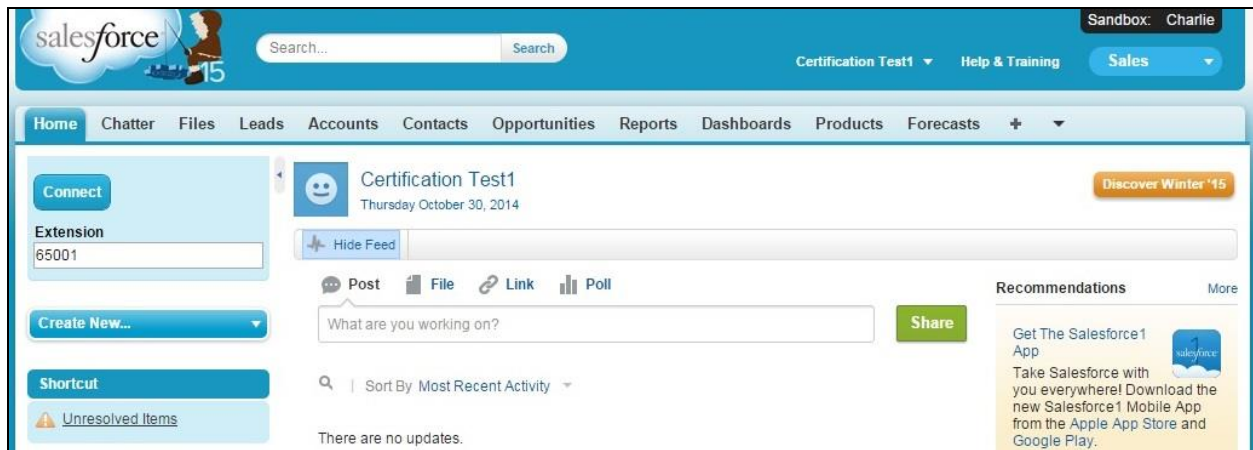
TSAPI Service Status
TLink Status
User Status

### 8.3. Verify InGenius Connector Enterprise

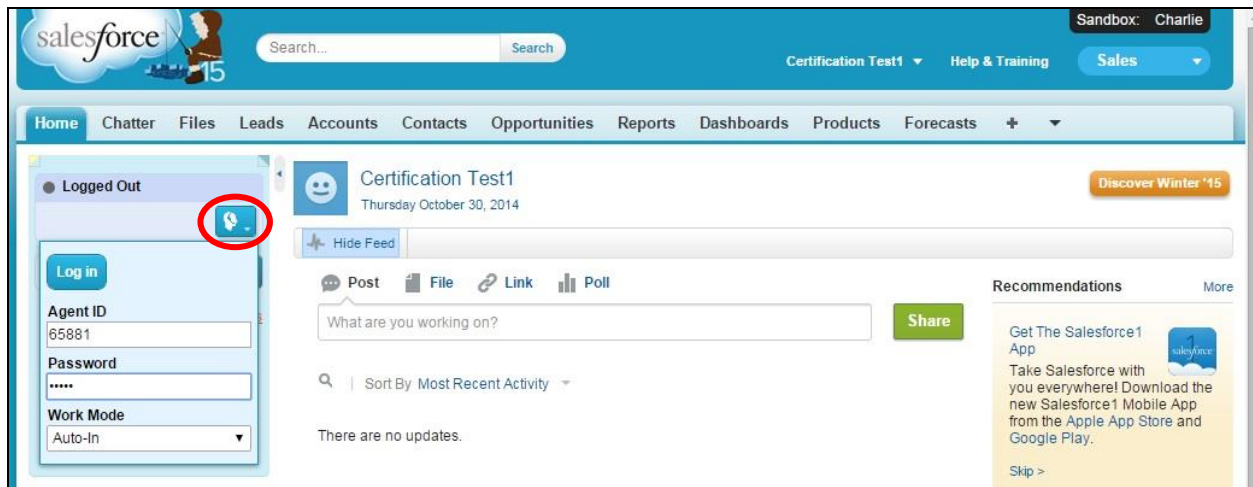
From the agent PC, launch an Internet browser window and enter the CTI adapter URL from **Section 7.5** for Salesforce.com. Log in with the relevant user credentials provided by InGenius.



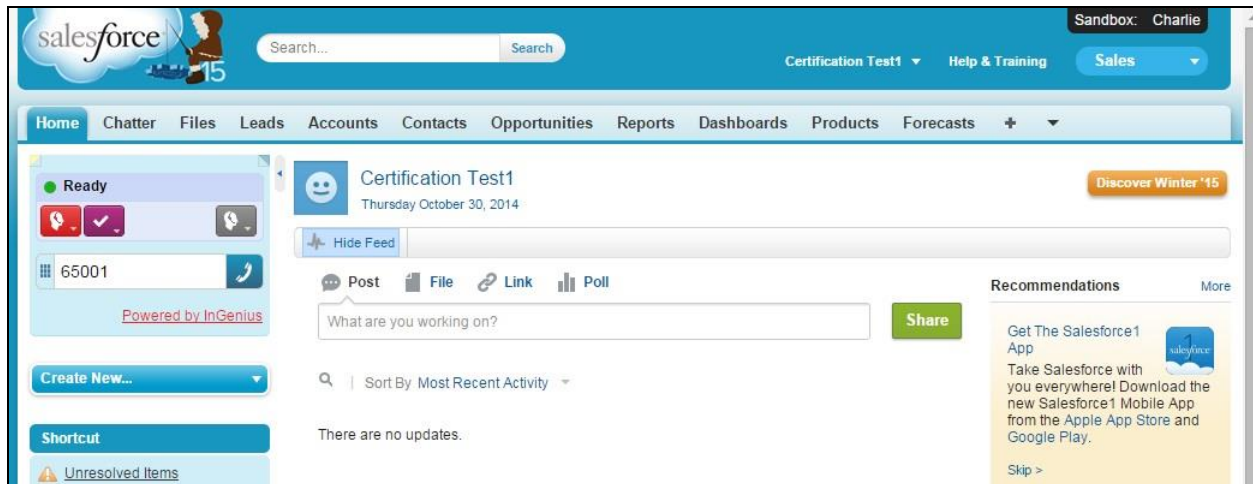
The screen below is displayed next. In the left pane, enter the relevant agent station extension from **Section 3**, and click **Connect**.



The left pane is updated, as shown below. Click on the **Log in** drop-down, to display additional parameters. For **Agent ID** and **Password**, enter the relevant credentials from **Section 3**. For **Work Mode**, select the desired work mode, in this case “Auto-In”. Click **Log in**.



Verify that the left pane is updated showing the agent in the **Ready** state.





Make an incoming ACD call. Verify that the left pane of the available agent is updated to reflect **Reserved** and **Inbound Call**, along with proper call information. Also verify that the right pane is populated with the uniquely matching contact record associated with the PSTN caller number, as shown below.

In the event that there is more than one contact record matching to the PSTN caller number, then all records will be presented in the **Related Records** sub-section in the left pane, and the agent will need to manually select the pertinent one to populate in the right pane.

Click **Answer** in the left pane.

The screenshot shows the Salesforce interface with the 'Contacts' tab selected. The left sidebar displays the 'Reserved' status and 'Inbound Call' details, including the dialed number +1 (303) 536-0001 and the number +1 (908) 848-5601. The 'Answer' button is visible. The main area shows the contact record for 'DevConnect Avaya'. The contact details table is as follows:

Contact Detail	
Contact Owner	Certification Test1 [Change]
Name	DevConnect Avaya
Account Name	Test Company
Title	
Skype	
Reports To	View Org Chart
Phone	(908) 848-5601
Mobile	
Email	
Phone System	
User's CRM	
Dealer	

Verify that the agent is connected to the PSTN caller with two-way talk paths, and that the left pane is updated to reflect **Talking** and **Connected**, as shown below.

The screenshot displays the Salesforce user interface. At the top, the Salesforce logo and navigation bar are visible. The main navigation menu includes Home, Chatter, Files, Leads, Accounts, **Contacts**, Opportunities, Reports, Dashboards, Products, and Forecasts. A banner below the navigation bar promotes the Salesforce Mobile App. On the left sidebar, the 'Talking' status is highlighted, and the 'Connected' status is also visible. The main content area shows the contact details for 'DevConnect Avaya'. The 'Call Log' section on the left indicates a call on 30/10/2014 at 9:29 AM with the number +1 (908) 848-5601. The 'Contact Detail' section on the right provides information about the contact, including the contact owner (Certification Test1), name (DevConnect Avaya), account name (Test Company), and phone number ((908) 848-5601).

## 9. Conclusion

These Application Notes describe the configuration steps required for InGenius Connector Enterprise 2.20 to successfully interoperate with Avaya Aura® Communication Manager 6.3 and Avaya Aura® Application Enablement Services 6.3 using Salesforce.com. 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. *InGenius Connector Enterprise for Salesforce Server Installation Guide for IT Administrator*, Revised June 2014, Version 2.20.234, available at <http://go.ingenius.com/iceavayasalesforceinstallguide>.
4. *InGenius Connector Enterprise for Salesforce and Avaya Aura Communications Manager User Guide*, Revised June 2014, Version 2.20.234, available at <http://go.ingenius.com/iceavayasalesforceuserguide>.



---

**©2014 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).