



**Application Notes for InGenius Connector Enterprise 4.0  
with Avaya Aura® Communication Manager 7.0 and Avaya  
Aura® Application Enablement Services 7.0 using  
Salesforce.com – Issue 1.0**

**Abstract**

These Application Notes describe the configuration steps required for InGenius Connector Enterprise 4.0 to interoperate with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0 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) 4.0 to interoperate with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0 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 used a web browser to connect to the ICE server and to the InGenius Connector Enterprise Open CTI running on the Salesforce.com cloud.

## 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 desktops and/or telephones. The click-to-dial calls were initiated by clicking on the contact phone number displayed on the agent desktops.

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 reason codes and pending aux work.
- 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:

- By design, the agent desktop does not support initiation of unattended conference.
- 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 transfer and conference of outbound calls, the transfer-to and conference-to agents 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.

## 2.3. Support

Technical support on ICE can be obtained through the following:

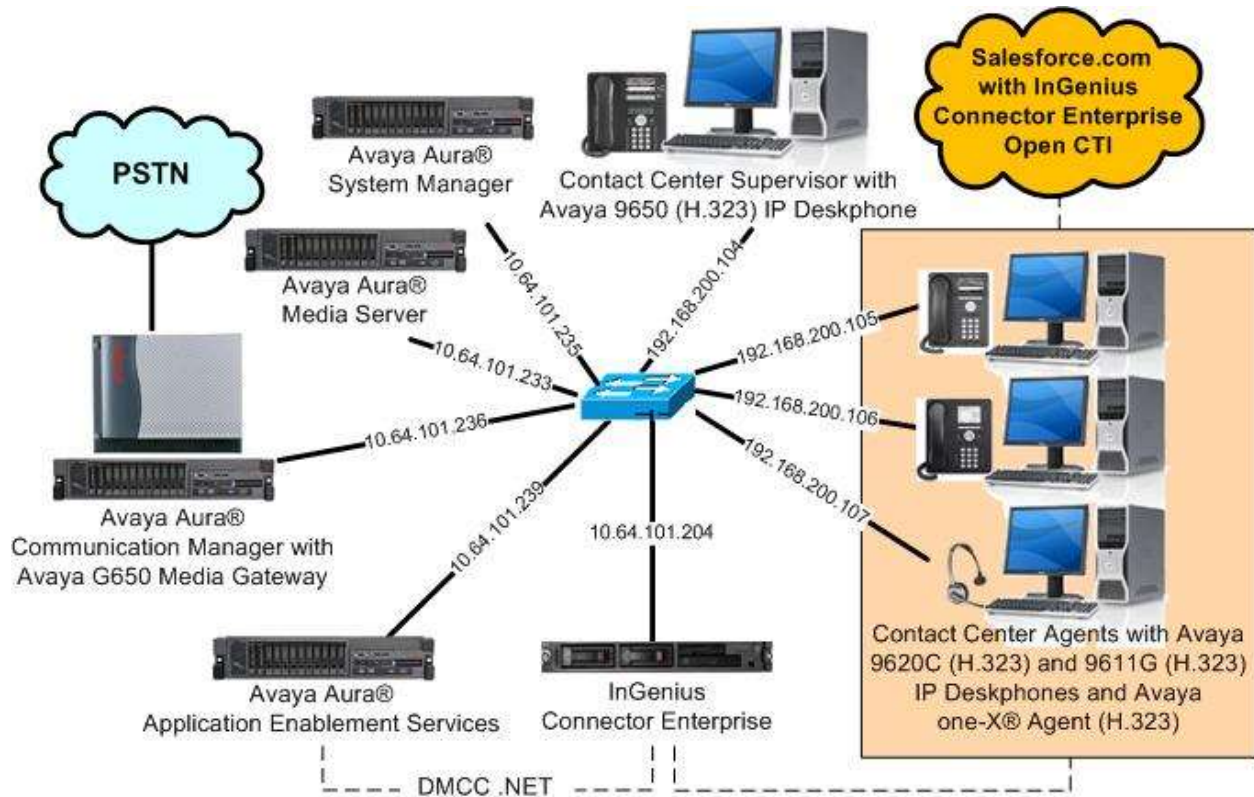
- **Phone:** (613) 591-9002
- **Email:** [icesupport@ingenius.com](mailto:icesupport@ingenius.com)
- **Web :** <http://ingenius.com/resources/support/>

### 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 in Virtual Environment	7.0 SP1 (7.0.0.1.0.441.22477)
Avaya G650 Media Gateway	NA
Avaya Aura® Media Server in Virtual Environment	7.7.0.236
Avaya Aura® Application Enablement Services in Virtual Environment	7.0 Patch 1 (7.0.0.0.1.13)
Avaya one-X® Agent	2.5.8 (2.5.58020.0)
Avaya 9611G IP Deskphone (H.323)	6.6029
Avaya 9620C & 9650 IP Deskphones (H.323)	3.250A
InGenius Connector Enterprise on Windows Server 2012 <ul style="list-style-type: none"><li>• Avaya DMCC XML</li><li>• Configuration Tool</li></ul>	4.0.1000.10784 R2 Standard 6.2 4.0.1000.10784
InGenius Connector Enterprise Open CTI on Salesforce.com	1.19 Winter 2016

## 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 4**. If this option is not set to “y”, then contact the Avaya sales team or business partner for a proper license file.

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

Abbreviated Dialing Enhanced List? y                               Audible Message Waiting? y
Access Security Gateway (ASG)? n                                   Authorization Codes? y
Analog Trunk Incoming Call ID? y                                  CAS Branch? n
A/D Grp/Sys List Dialing Start at 01? y                           CAS Main? n
Answer Supervision by Call Classifier? y                           Change COR by FAC? n
ARS? y Computer Telephony Adjunct Links? y
ARS/AAR Partitioning? y                                           Cvg Of Calls Redirected Off-net? y
ARS/AAR Dialing without FAC? 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 1                                                       Page 1 of 3
                                CTI LINK

CTI Link: 1
Extension: 60111
Type: ADJ-IP
Name: AES CTI Link
                                COR: 1
```

### 5.3. Administer System Parameters Features

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

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

SYSTEM PRINTER PARAMETERS
  Endpoint:                               Lines Per Page: 60

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

Navigate to **Page 13**, and enable **Send UCID to ASAI**. This parameter allows for the universal call ID to be sent to 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
  Prefer H.323 Over SIP For Dual-Reg Station 3PCC Make Call? 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 Finished Shift
Reason Code 2: Coffee               /n
Reason Code 3:                        /n
Reason Code 4:                        /n
Reason Code 5:                        /n
Reason Code 6:                        /n
Reason Code 7:                        /n
Reason Code 8:                        /n
Reason Code 9:                        /n

Default Reason Code:
```



## 6. Configure Avaya Aura® Application Enablement Services

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

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer InGenius user
- Disable security database
- Administer ports
- Restart services

### 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 reads "Application Enablement Services Management Console". Below this is a red horizontal bar. The main content area features a login form with the heading "Please login here:". The form contains two input fields: "Username" and "Password". Below these fields are two buttons: "Login" and "Reset". At the bottom of the page, there is a red horizontal bar and a copyright notice: "Copyright © 2009-2015 Avaya Inc. All Rights Reserved."

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

The screenshot shows the Avaya Application Enablement Services Management Console. The top left features the Avaya logo and the title 'Application Enablement Services Management Console'. The top right displays system information: 'Welcome: User', 'Last login: Tue Nov 17 15:23:19 2015 from 192.168.200', 'Number of prior failed login attempts: 0', 'HostName/IP: aes7/10.64.101.239', 'Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE', 'SW Version: 7.0.0.0.1.13', 'Server Date and Time: Tue Nov 17 16:13:36 EST 2015', and 'HA Status: Not Configured'. A red navigation bar contains 'Home | Help | Logout'. On the left, a sidebar menu lists: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area is titled 'Welcome to OAM' and contains the following text: 'The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:'. A bulleted list follows: '• 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 infomations.', '• 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'. Below the list, it 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 applicable WebLM server log in screen (not shown). Log in using the appropriate credentials, and navigate to display installed licenses (not shown).

The screenshot shows the Avaya Application Enablement Services Management Console with the 'Licensing' page selected. The top left features the Avaya logo and the title 'Application Enablement Services Management Console'. The top right displays system information: 'Welcome: User', 'Last login: Tue Nov 17 15:23:19 2015 from 192.168.200.20', 'Number of prior failed login attempts: 0', 'HostName/IP: aes7/10.64.101.239', 'Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE', 'SW Version: 7.0.0.0.1.13', 'Server Date and Time: Tue Nov 17 16:13:36 EST 2015', and 'HA Status: Not Configured'. A red navigation bar contains 'Home | Help | Logout'. On the left, a sidebar menu lists: AE Services, Communication Manager Interface, High Availability, Licensing (expanded), Maintenance, and Networking. Under 'Licensing', the sub-items are: 'WebLM Server Address', 'WebLM Server Access' (highlighted), and 'Reserved Licenses'. The main content area is titled 'Licensing' and contains the following text: 'If you are setting up and maintaining the WebLM, you need to use the following:'. A bulleted list follows: '• WebLM Server Address'. Below that, it says: 'If you are importing, setting up and maintaining the license, you need to use the following:'. A bulleted list follows: '• WebLM Server Access'. Finally, it says: 'If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:'. A bulleted list follows: '• Reserved Licenses'.

Select **Licensed products** → **APPL\_ENAB** → **Application\_Enablement** in the left pane, to display the **Application Enablement (CTI)** screen in the right pane.

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

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

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

License installed on: October 12, 2015 2:21:49 PM +05:00

License File Host IDs: V1-19-37-90-8F-BF

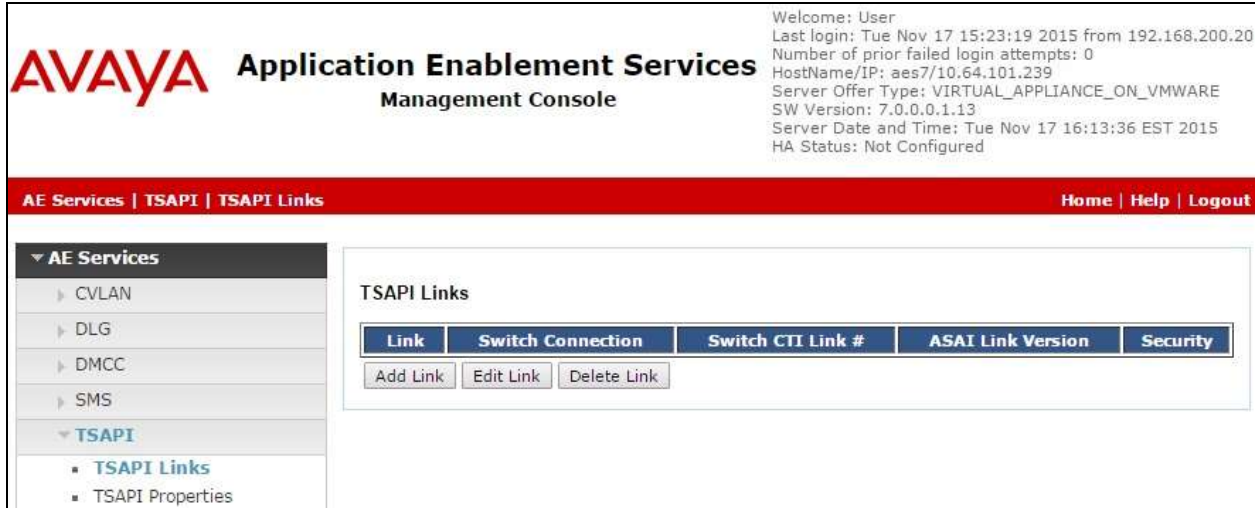
**Licensed Features**

10 Items Show All

Feature (License Keyword)	Expiration date	Licensed capacity
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	1000
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	3
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	16
Product Notes VALUE_NOTES	permanent	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;Cti5 MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_2 LargeServerTypes: isp2100;ibmx305;d1380g3;d1385g1;d1385g2;u TrustedApplications: 1PS_001, BasicUnrestrict DMCUnrestricted; 1XP_001, BasicUnrestrict DMCUnrestricted; 1XM_001, BasicUnrestrict DMCUnrestricted; PC_001, BasicUnrestrict DMCUnrestricted; CTE_001, BasicUnrestrict DMCUnrestricted; OSPC_001, BasicUnrestrict DMCUnrestricted; VP_001, BasicUnrestrict DMCUnrestricted; SAMETIME_001, VALUE_AES CCE_001, BasicUnrestricted, AdvancedUnrestr CSI_T1_001, BasicUnrestricted, AdvancedUnr CSI_T2_001, BasicUnrestricted, AdvancedUnr AVAYAVERINT_001, BasicUnrestricted, Advan DMCUnrestricted; CCT_ELITE_CALL_CTRL_001 AdvancedUnrestricted, DMCUnrestricted, Agen BasicUnrestricted, AdvancedUnrestricted, DMC AgentEvents; UNIFIED_DESKTOP_001, BasicU AdvancedUnrestricted, DMCUnrestricted, Agen BasicUnrestricted, AdvancedUnrestricted, DMC
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	3
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	1000
DLG VALUE_AES_DLG	permanent	16
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	1000
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	3

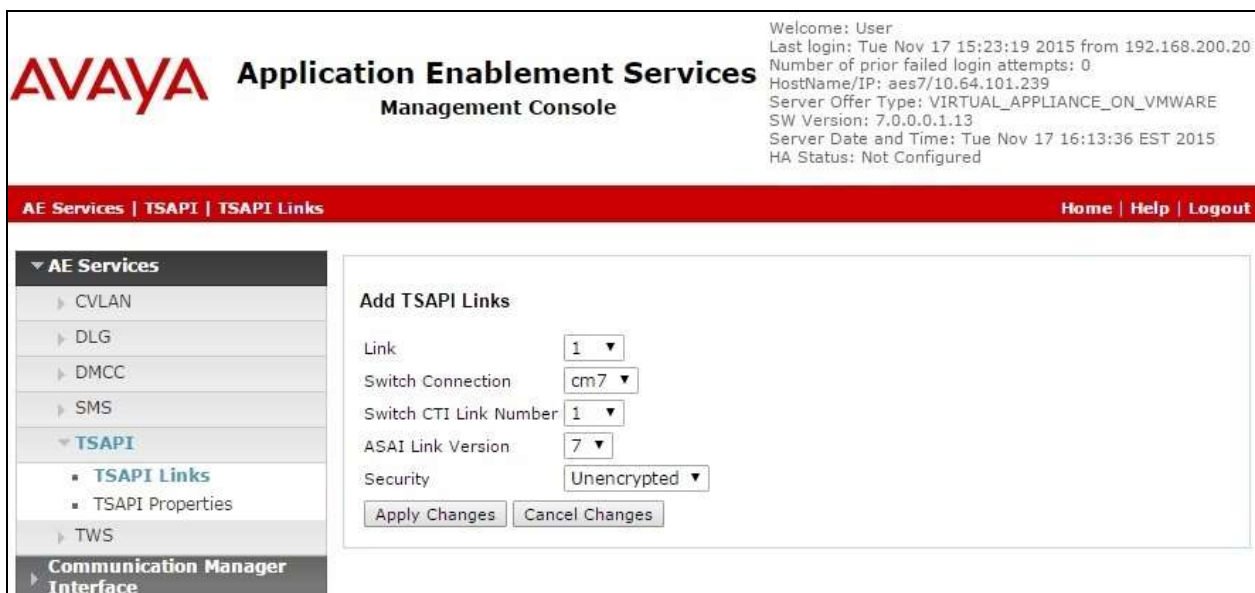
### 6.3. Administer TSAPI Link

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



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

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



## 6.4. 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.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the text 'Application Enablement Services Management Console'. A welcome message in the top right corner provides system information: 'Welcome: User', 'Last login: Tue Nov 17 15:23:19 2015 from 192.168.200.20', 'Number of prior failed login attempts: 0', 'HostName/IP: aes7/10.64.101.239', 'Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE', 'SW Version: 7.0.0.0.1.13', 'Server Date and Time: Tue Nov 17 16:13:36 EST 2015', and 'HA Status: Not Configured'. A red navigation bar contains 'User Management | User Admin | Add User' and 'Home | Help | Logout'. The left sidebar shows a tree view with 'User Management' expanded to 'User Admin' and 'Add User' selected. The main content area is titled 'Add User' and contains a form with the following fields: '\* User Id' (text input: ingenius), '\* Common Name' (text input: ingenius), '\* Surname' (text input: ingenius), '\* User Password' (password input: masked with dots), '\* Confirm Password' (password input: masked with dots), 'Admin Note' (text area), 'Avaya Role' (dropdown menu: None), 'Business Category' (text input), 'Car License' (text input), 'CM Home' (text input), 'Css Home' (text input), 'CT User' (dropdown menu: Yes), 'Department Number' (text input), 'Display Name' (text input), 'Employee Number' (text input), 'Employee Type' (text input), 'Enterprise Handle' (text input), and 'Given Name' (text input). A note above the form states 'Fields marked with \* : can not be empty.'

## 6.5. 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.

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

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the text "Application Enablement Services Management Console". On the right side of the header, there is a user information block: "Welcome: User", "Last login: Tue Nov 17 15:23:19 2015 from 192.168.200.20", "Number of prior failed login attempts: 0", "HostName/IP: aes7/10.64.101.239", "Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE", "SW Version: 7.0.0.0.1.13", "Server Date and Time: Tue Nov 17 16:13:36 EST 2015", and "HA Status: Not Configured".

The main content area is divided into a left navigation pane and a right main pane. The left pane shows a tree view of services, with "Security Database" expanded to show "Control" selected. The right pane displays the "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" configuration page. This page contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services". Below these checkboxes is an "Apply Changes" button.

## 6.6. 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.

The screenshot displays the Avaya Application Enablement Services Management Console. The top right corner shows a welcome message for the user, including login details and system information. The main interface is divided into a left navigation pane and a right content area. The left pane shows a tree view with 'Networking' expanded to 'Ports'. The right pane displays the 'Ports' configuration page, which is organized into three sections: CVLAN Ports, TSAPI Ports, and DMCC Server Ports. Each section contains various port settings and radio buttons for enabling or disabling them.

**CVLAN Ports**

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

**DLG Port**

TCP Port	5678	

**TSAPI Ports**

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

**DMCC Server Ports**

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

## 6.7. Restart Services

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

Welcome: User  
Last login: Tue Nov 17 10:29:16 2015 from 192.168.200.20  
Number of prior failed login attempts: 0  
HostName/IP: aes7/10.64.101.239  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 7.0.0.0.1.13  
Server Date and Time: Tue Nov 17 10:43:33 EST 2015  
HA Status: Not Configured

Maintenance | Service Controller Home | Help | Logout

**AVAYA** Application Enablement Services Management Console

Navigation menu:  
▶ AE Services  
▶ Communication Manager Interface  
▶ High Availability  
▶ Licensing  
▼ Maintenance  
    Date Time/NTP Server  
    ▶ Security Database  
    **Service Controller**  
    ▶ Server Data  
▶ Networking  
▶ Security  
▶ Status

**Service Controller**

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

For status on actual services, please use [Status and Control](#)

Start Stop Restart Service Restart AE Server Restart Linux Restart Web Server



## 7. Configure InGenius Connector Enterprise

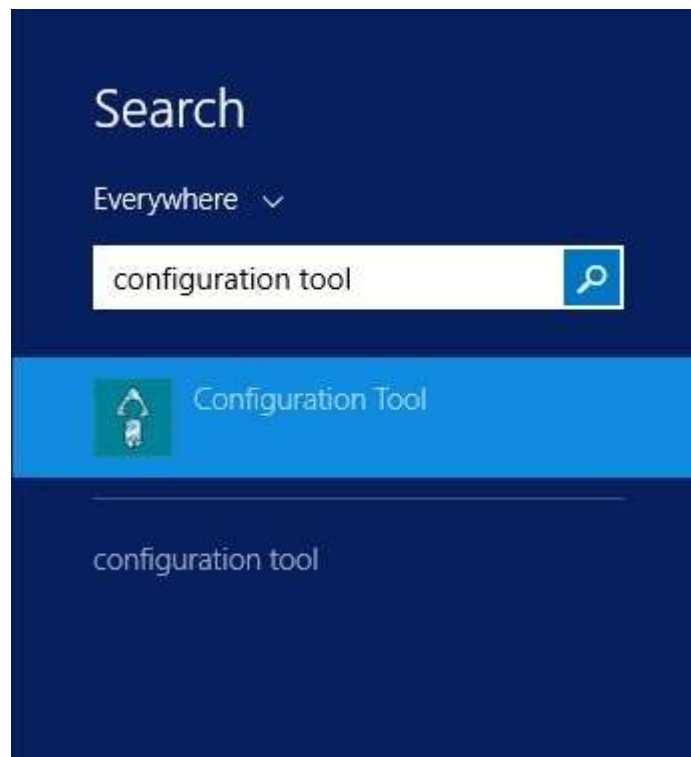
This section provides the procedures for configuring ICE. The procedures include the following areas:

- Launch configuration tool
- Administer dialing and number formatting
- Administer telephony
- Start service

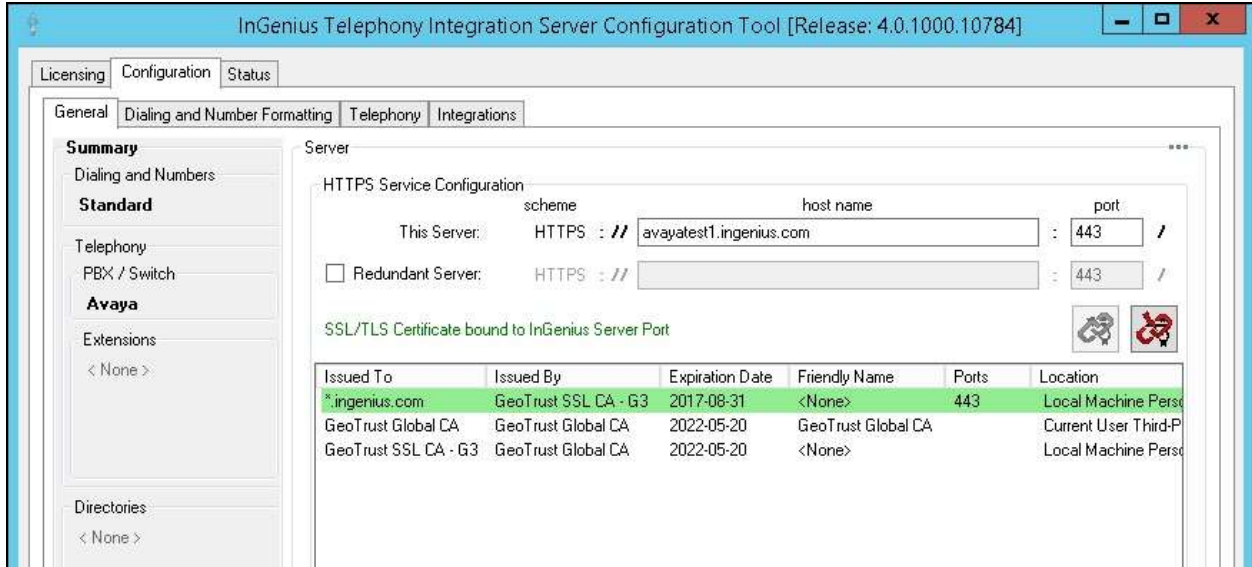
This section assumes the Connector Enterprise package has been imported and published, with the appropriate Security Role created, and users created and assigned to the Security Role. Refer to reference [3] for more details.

### 7.1. Launch Configuration Tool

From the ICE server, enter “configuration tool” anywhere on the desktop to locate the **Configuration Tool** application. Click on the pertinent entry from the result to launch the application.

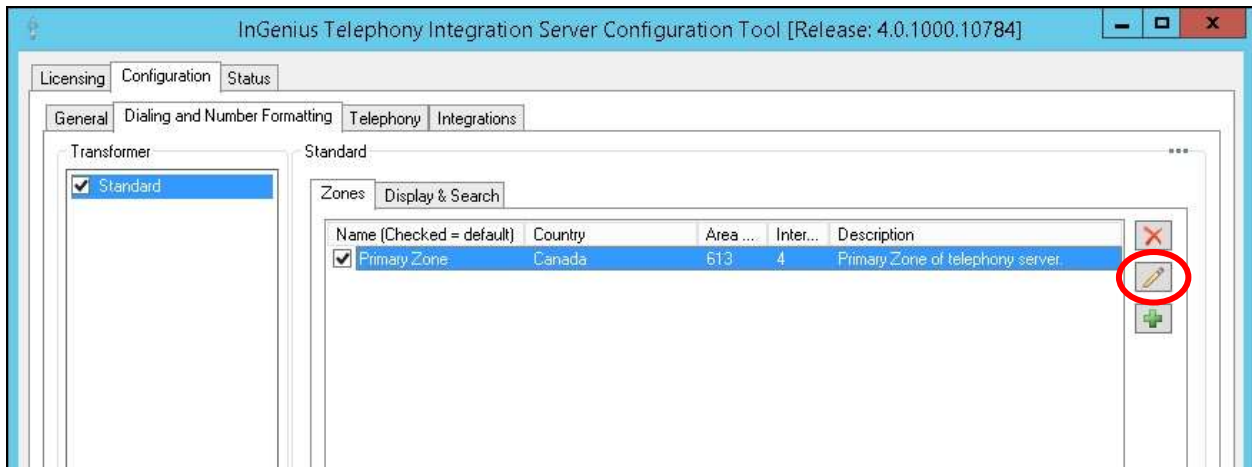


The **InGenius Telephony Integration Server Configuration Tool** screen is displayed.



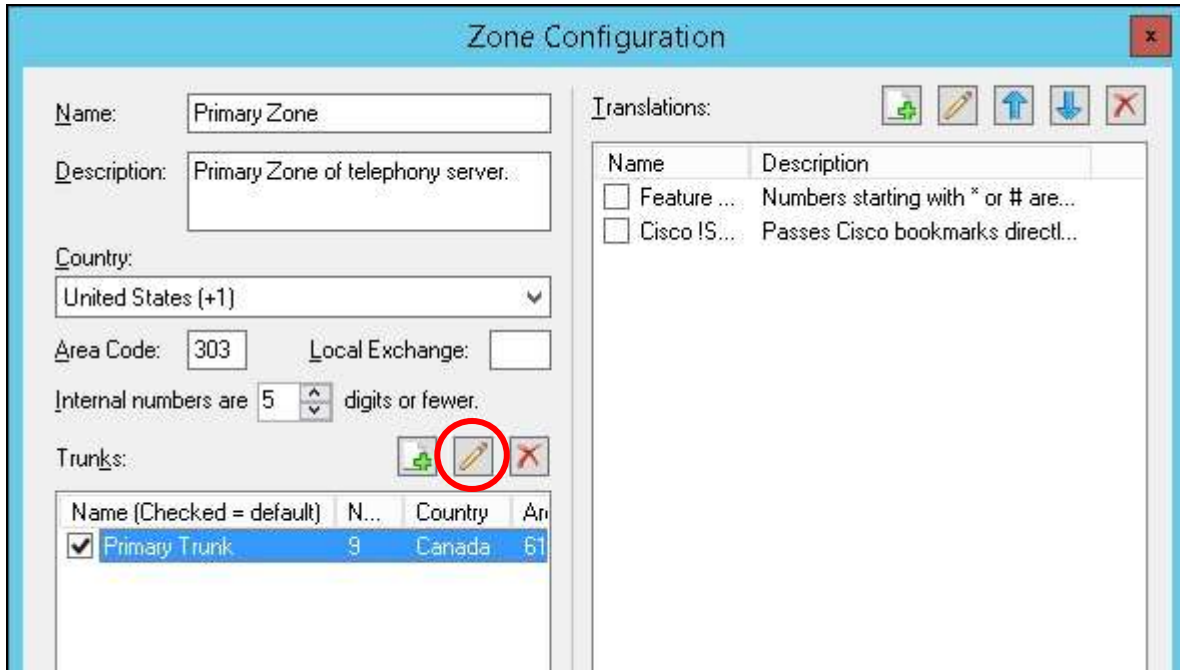
## 7.2. Administer Dialing and Number Formatting

Select **Configuration** → **Dialing and Number Formatting** from the top menu, followed by the **Zones** tab in the right pane. 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**, select and enter 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.

**Trunk**

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:

Translations to dialable:

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

Auto configure local dialing

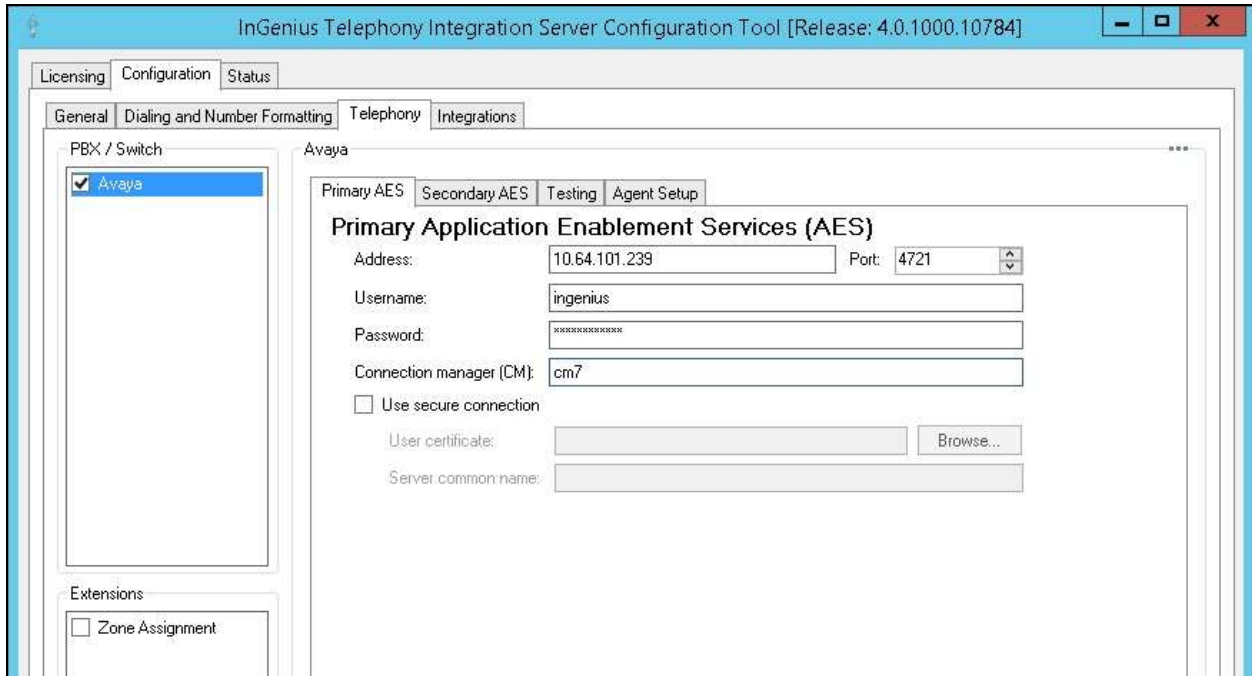
OK Cancel

### 7.3. Administer Telephony

The **InGenius Telephony Integration Server Configuration Tool** screen is displayed again. Select **Configuration** → **Telephony** from the top menu, followed by the **Primary AES** tab in the right pane to display the screen below.

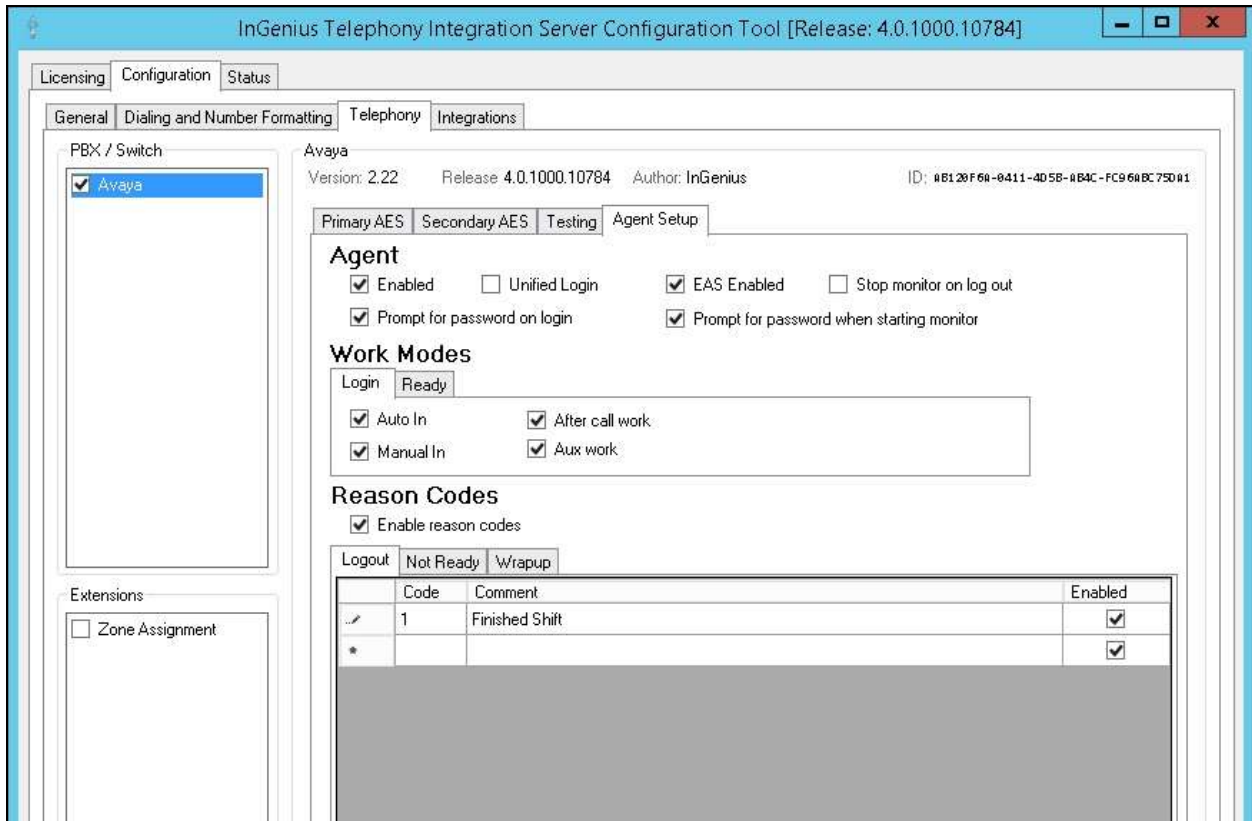
Enter the following values for the specified fields, and retain the default values in the remaining fields.

- **Address:** The IP address of Application Enablement Services.
- **Username:** The InGenius user credentials from **Section 6.4**.
- **Password:** The InGenius user credentials from **Section 6.4**.
- **Connection manager:** The relevant switch connection name from **Section 6.3**.



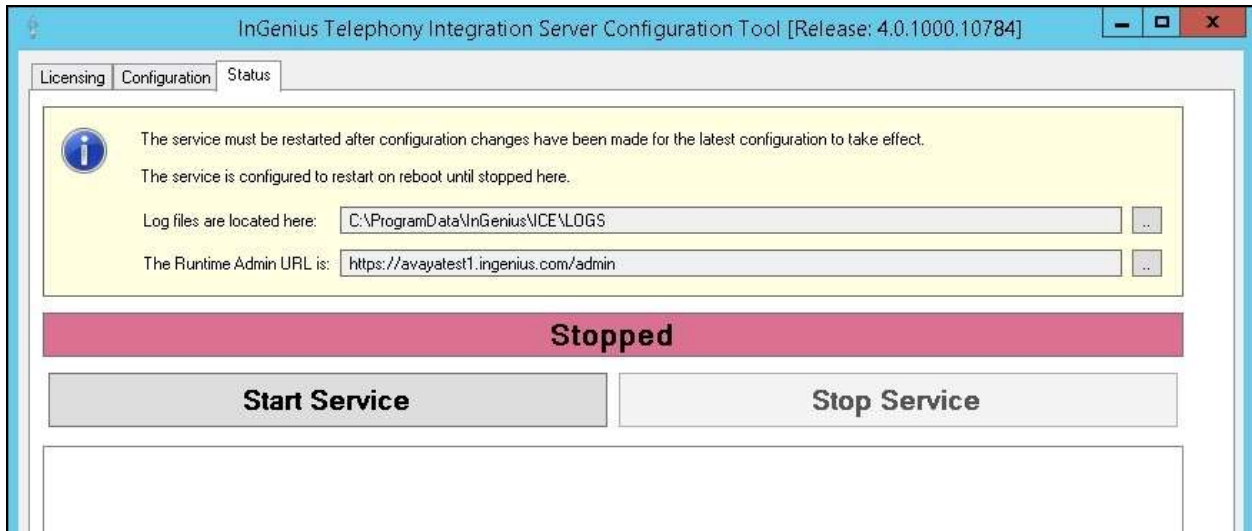
Select the **Agent Setup** tab in the right pane to display the screen below. Follow reference [4] to update parameters in the **Agent** and **Work Modes** sub-sections to the proper settings. The screenshot below shows the values used in the compliance testing.

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**. In the compliance testing, one reason code was created under the **Logout** tab as shown below, and two reason codes were created under the **Not Ready** tab (not shown).

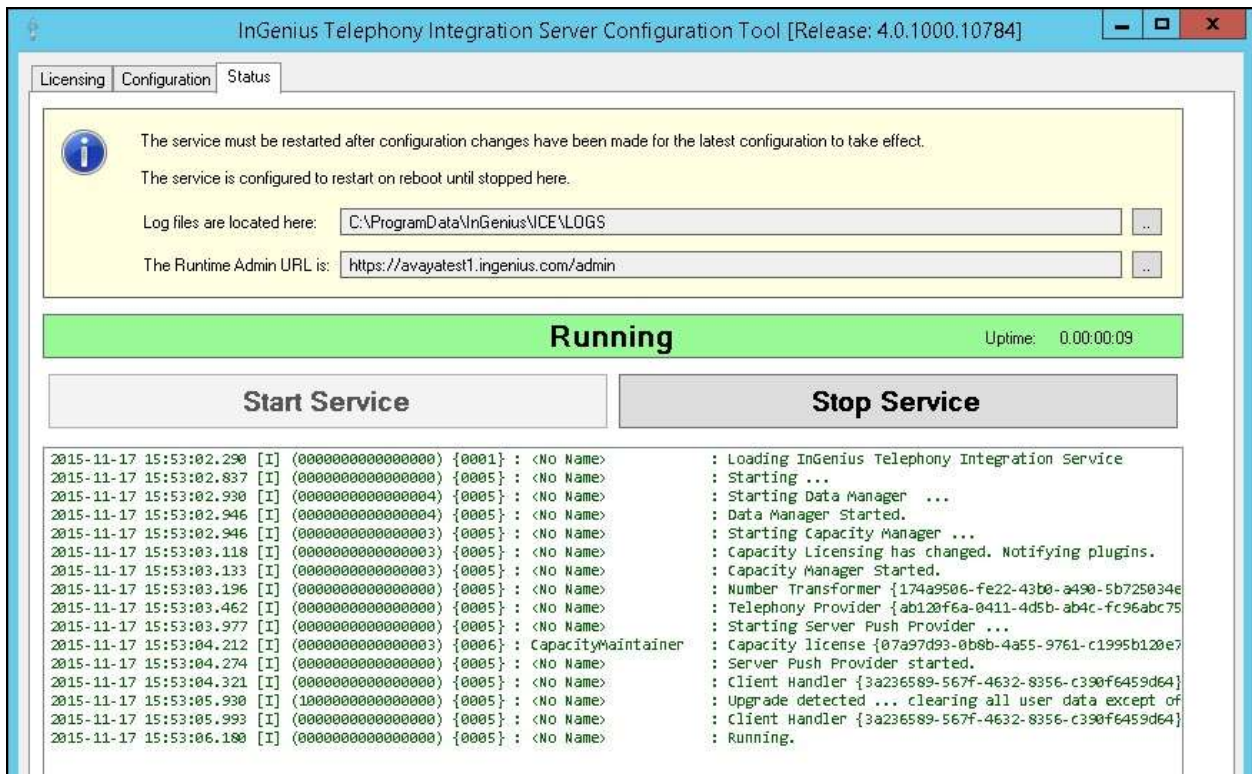


## 7.4. Start Service

Select **Status** from the top menu to display the screen below, and click **Start Service**.



The screen is updated, as shown below.



## 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	7	no	aes7	established	2063	1924

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

On Application Enablement Services, verify the status of the DMCC service 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 6.4**.



### Application Enablement Services Management Console

Welcome: User  
 Last login: Thu Nov 19 10:35:13 2015 from 192.168.200.20  
 Number of prior failed login attempts: 0  
 HostName/IP: aes7/10.64.101.239  
 Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
 SW Version: 7.0.0.0.1.13  
 Server Date and Time: Thu Nov 19 13:20:39 EST 2015  
 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**
    - Switch Conn Summary

#### DMCC Service Summary - Session Summary

Please do not use back button

Enable page refresh every  seconds

Session Summary [Device Summary](#)  
 Generated on Thu Nov 19 13:20:39 EST 2015

Service Uptime: 2 days, 2 hours 36 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 21

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
A9E2F12A4FEFF30C0 8DD93037DD6FB5B-21	ingenius	InGenius Avaya Plugin	10.64.101.204	XML Unencrypted	0

Item 1-1 of 1  
 Go

TLT; Reviewed:  
SPOC 1/12/2016

Solution & Interoperability Test Lab Application Notes  
©2016 Avaya Inc. All Rights Reserved.

24 of 31  
ICE-SF-AES7



Verify the status of the TSAPI service 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**, 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”.

AVAYA Application Enablement Services Management Console

Welcome: User  
 Last login: Thu Nov 19 10:35:13 2015 from 192.168.200.20  
 Number of prior failed login attempts: 0  
 HostName/IP: aes7/10.64.101.239  
 Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
 SW Version: 7.0.0.1.13  
 Server Date and Time: Thu Nov 19 13:28:02 EST 2015  
 HA Status: Not Configured

Status | Status and Control | TSAPI Service Summary Home | Help | Logout

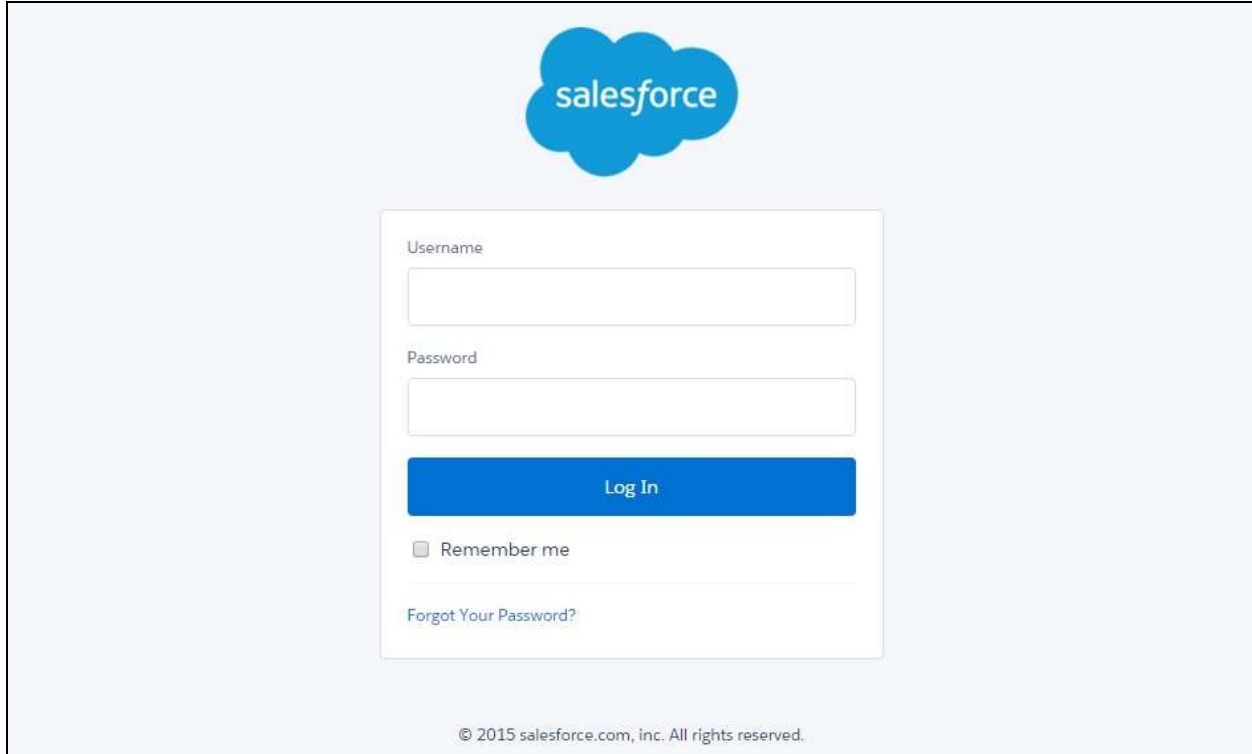
Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input checked="" type="radio"/>	1	cm7	1	Talking	Wed Nov 18 09:08:44 2015	Online	17	3	2014	2160	30

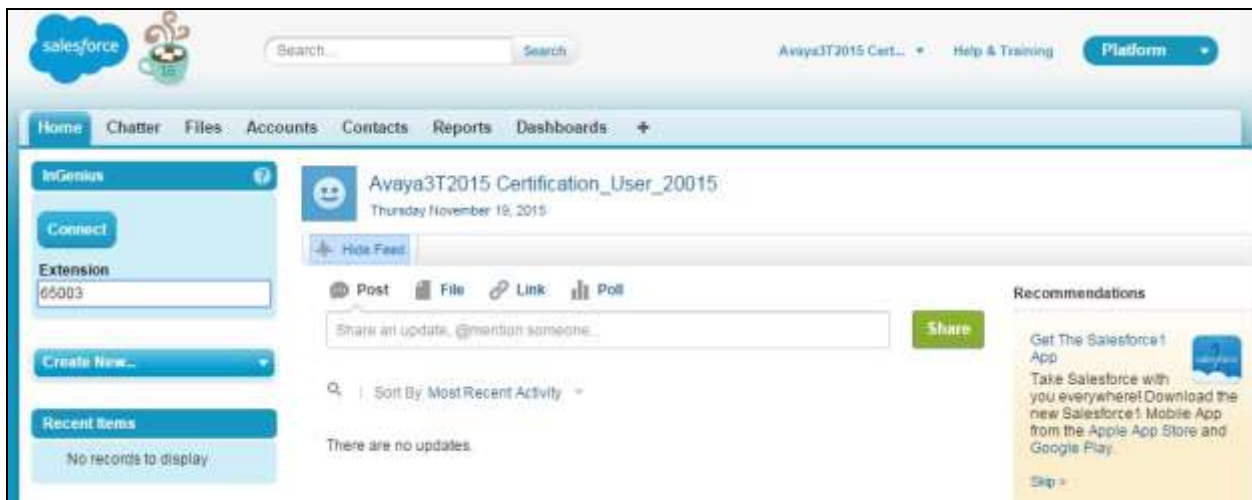
For service-wide information, choose one of the following:

### 8.3. Verify InGenius Connector Enterprise

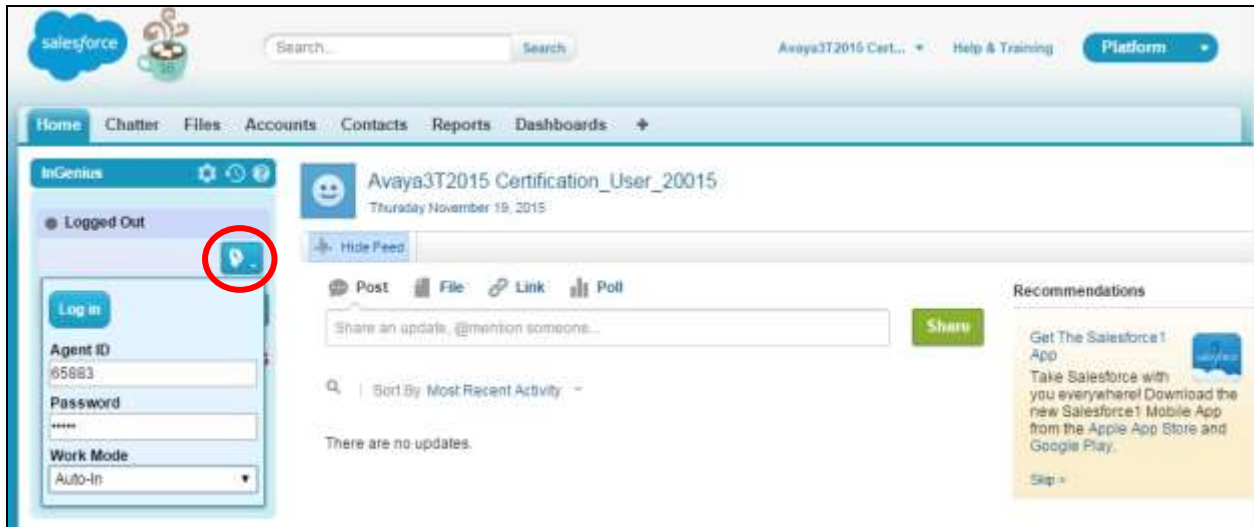
From an agent PC, launch an Internet browser window and enter the URL provided by the end customer for Salesforce.com. Log in with the relevant user credentials provided by InGenius.



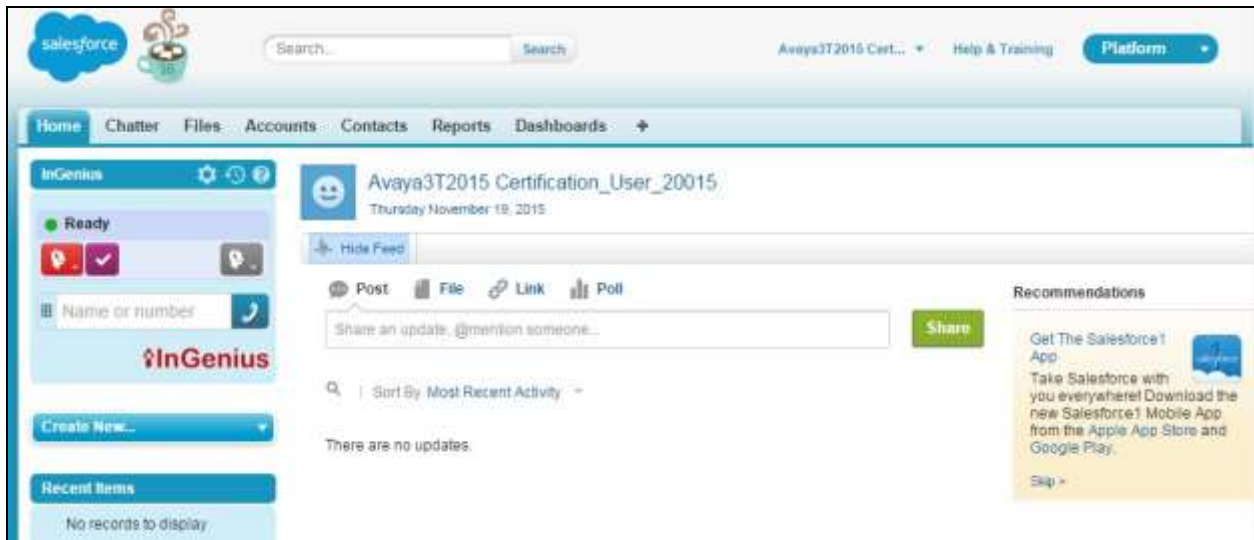
The screen below is displayed next. In the left pane, enter the relevant agent station extension from **Section 3**, and click **Connect**.



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**.



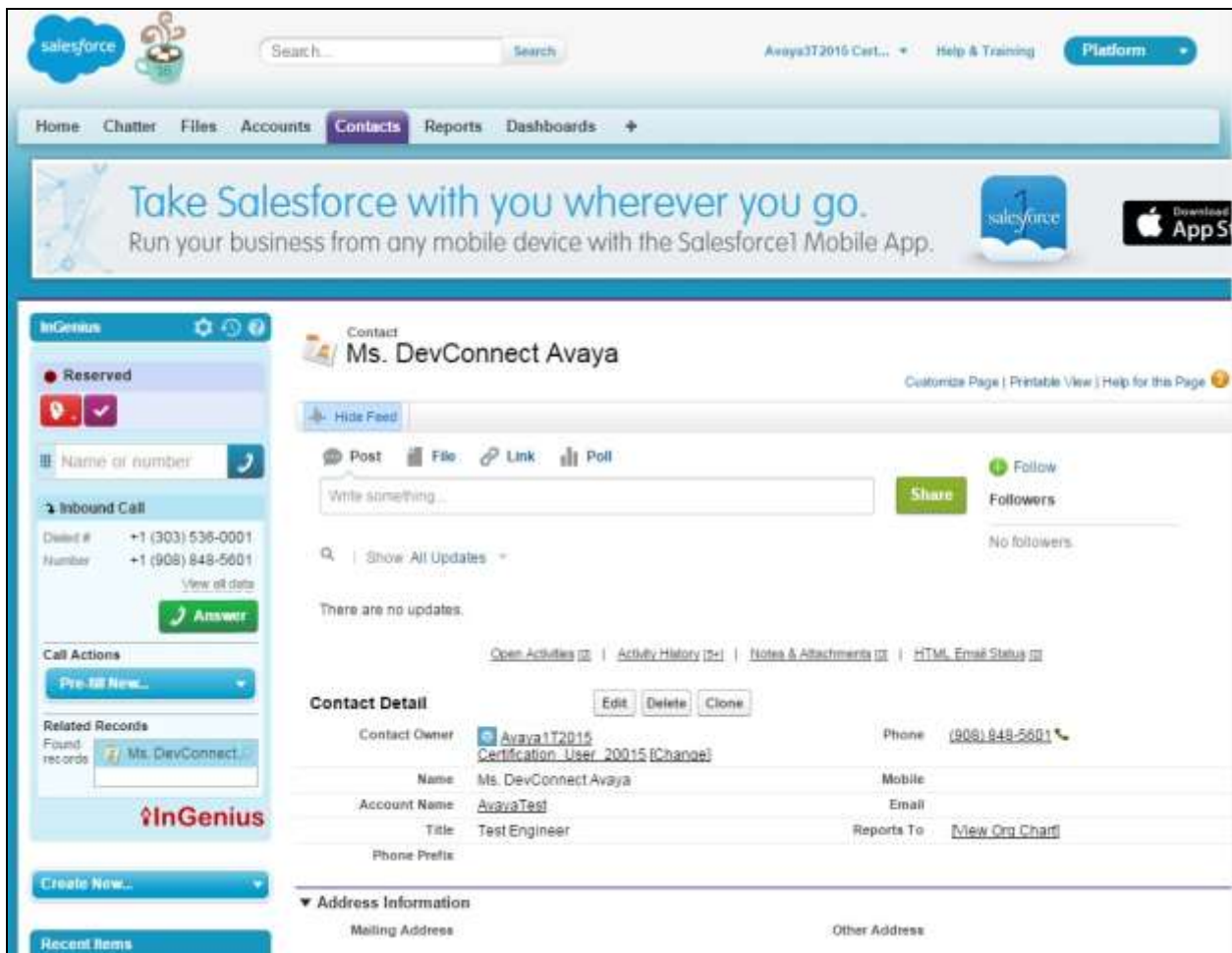
Verify that the left pane is updated, and showing the agent in the **Ready** state.



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.



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 InGenius interface. On the left, the 'InGenius' sidebar shows a 'Talking' status with a red microphone icon and a 'Connected' status with a green checkmark and a timer of 07:59:37. Below this, a call log entry is visible for 'Ms. DevConnect...' with a subject 'Call 10/11/2015 9:28 PM' and a number '+1 (908) 848-5601'. The main content area shows the contact record for 'Ms. DevConnect Avaya'. The 'Contact Detail' section includes the following information:

Contact Owner	Avaya1T2015 Certification User 20015 (Change)	Phone	(908) 848-5601
Name	Ms. DevConnect Avaya	Mobile	
Account Name	AvayaTest	Email	
Title	Test Engineer	Reports To	View Org Chart
Phone Prefix			

Below the contact details, there are sections for 'Address Information' (Mailing Address, Other Address) and 'Additional Information'. The top navigation bar includes 'Home', 'Chatter', 'Files', 'Accounts', 'Contacts', 'Reports', and 'Dashboards'. The top right corner shows 'Avaya3T2015 Cert...', 'Help & Training', and 'Platform'.

## 9. Conclusion

These Application Notes describe the configuration steps required for InGenius Connector Enterprise 4.0 to successfully interoperate with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0 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*, Release 7.0, Issue 1, August 2015, available at <http://support.avaya.com>.
2. *Administering and Maintaining Aura® Application Enablement Services*, Release 7.0, Issue 1, August 2015, available at <http://support.avaya.com>.
1. *InGenius Connector Enterprise for Salesforce Server Installation Guide for IT Administrator*, Version 2.23.301, available at <http://go.ingenius.com/iceavayasalesforceinstallguide>.
2. *InGenius Connector Enterprise for Salesforce and Avaya Aura Communications Manager User Guide*, Version 2.23.301, available at <http://go.ingenius.com/iceavayasalesforceuserguide>.

---

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

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

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