



Avaya Solution & Interoperability Test Lab

Application Notes for InGenius Connector Enterprise 6.4 with Avaya Aura® Communication Manager 8.0 and Avaya Aura® Application Enablement Services 8.0 using Salesforce.com – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for InGenius Connector Enterprise 6.4 to interoperate with Avaya Aura® Communication Manager 8.0 and Avaya Aura® Application Enablement Services 8.0 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 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) 6.4 to interoperate with Avaya Aura® Communication Manager 8.0 and Avaya Aura® Application Enablement Services 8.0 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 Application Enablement Services to monitor agents on Communication Manager to provide screen pop, call control and click-to-dial features from the agent desktops. The agent desktop used 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 the ACD on 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.

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 Application Enablement Services and ICE did not include use of any specific encryption features as requested by InGenius.

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.
- When the single step transfer setting on ICE is enabled, blind transfer of calls involving SIP agents can fail with transfer-from agent left with two separate calls. This issue is under investigation by Avaya, and the workaround is to use the attended transfer procedure instead or to disable the single step transfer setting.
- When the single step transfer setting on ICE is disabled, the Transfer Call request as part of the blind transfer implementation can be sent prematurely by ICE, such that the transfer-from agent can be left with a held call and a consultative call. The workaround is for the transfer-from agent to press the “Complete transfer” icon on the desktop to manually complete the transfer. This issue is more prevalent for blind transfers involving SIP agents.
- In the outbound conference scenario, when the PSTN party drops from the conference first, the conference-from agent desktop continued to reflect conference instead of connection with the remaining conference-to agent. This behavior did not appear to have any other impact as a subsequent drop by either agent did clear the remaining call with proper reflection on both agent desktops.

2.3. Support

Technical support on ICE can be obtained through the following:

- **Phone:** +1 (613) 591-9002
- **Email:** icesupport@ingenius.com
- **Web :** <https://www.ingenius.com/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 call 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	61001, 61002
Supervisor	65000
Agent Stations	65001, 66006
Agent IDs	65881, 65882
Agent Passwords	65881, 65882

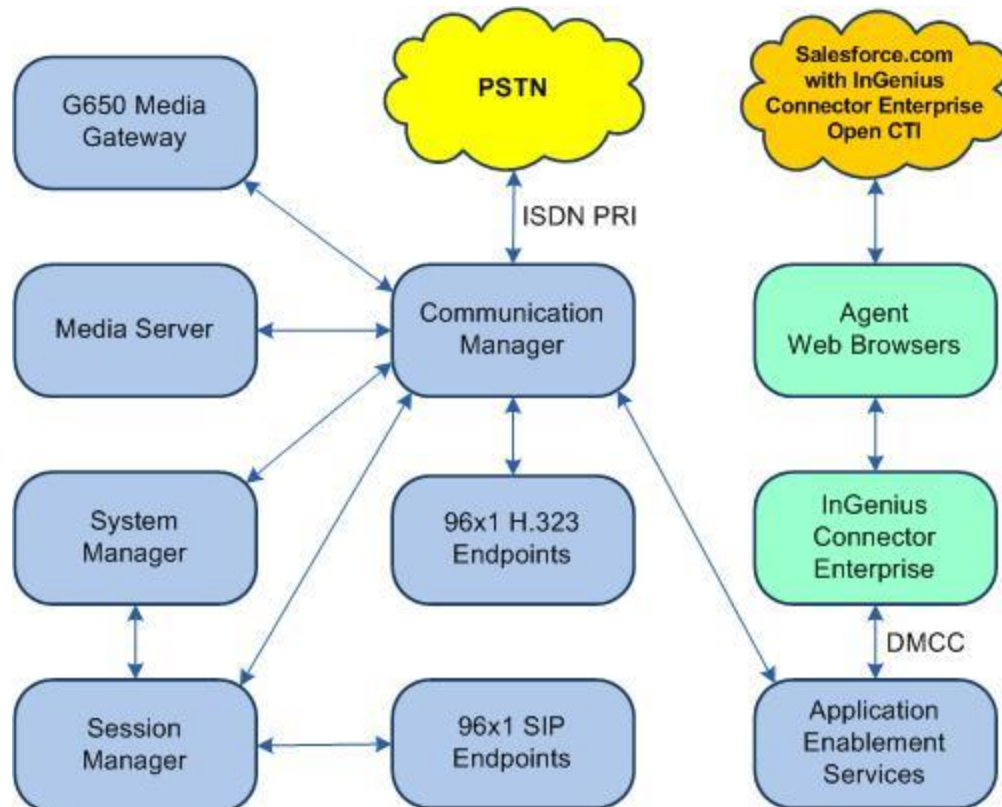


Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager in Virtual Environment	8.0.1 (8.0.1.0.0.822.25031)
Avaya G650 Media Gateway	NA
Avaya Aura® Media Server in Virtual Environment	8.0.0.150
Avaya Aura® Application Enablement Services in Virtual Environment	8.0 (8.0.0.0.0.6-0)
Avaya Aura® Session Manager in Virtual Environment	8.0 (8.0.0.0.80035)
Avaya Aura® System Manager in Virtual Environment	8.0 (8.0.0.0.098174)
Avaya 9611G & 9641G IP Deskphone (H.323)	6.6604
Avaya 9641G IP Deskphone (SIP)	7.1.3.0.11
InGenius Connector Enterprise on Windows Server 2016 <ul style="list-style-type: none">Avaya DMCC XMLInGenius Server Configuration	6.4.0.33866 Standard 6.1 6.4.0.33866
InGenius Connector Enterprise Open CTI on Salesforce.com	v43 Summer 19

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? 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
```

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
Unicode Name? n
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 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? 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 customers 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

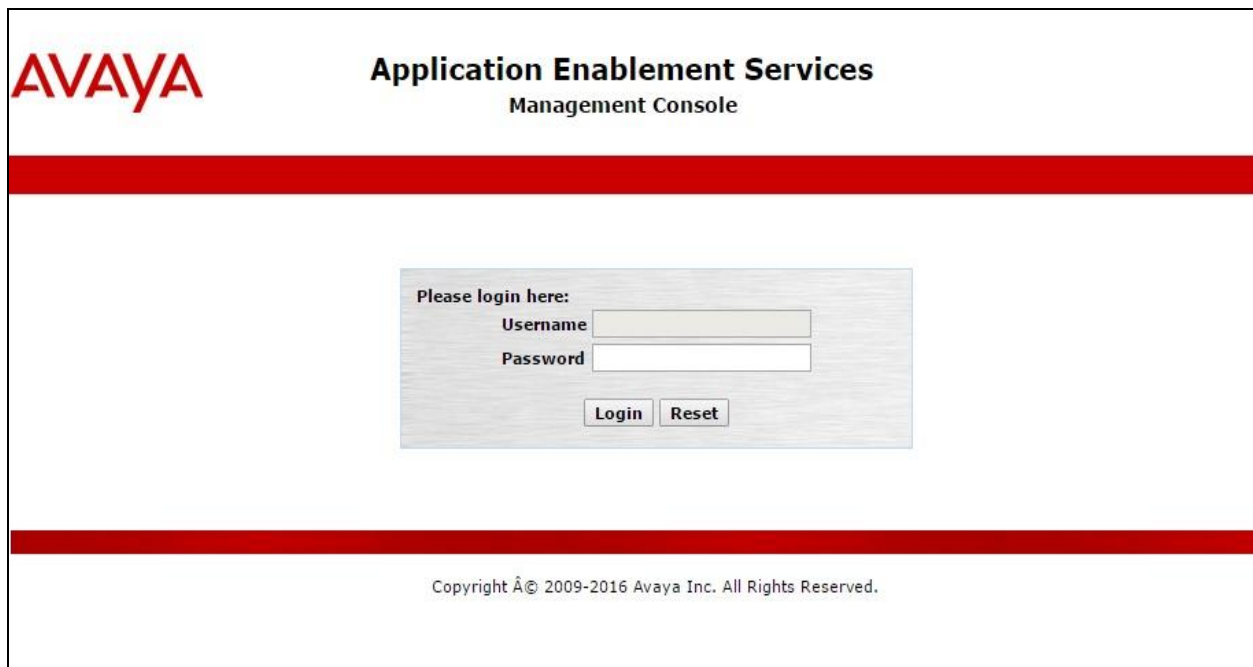
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer InGenius user
- Administer 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 "Application Enablement Services" is displayed in a large, bold font, with "Management Console" in a smaller font below it. A thick red horizontal bar spans the width of the page. Below this bar, centered, is a login box with a light gray background. Inside the box, the text "Please login here:" is at the top. Below it are two input fields: "Username" and "Password". At the bottom of the box are two buttons: "Login" and "Reset". Another thick red horizontal bar is located below the login box. At the very bottom of the page, centered, is the copyright notice: "Copyright © 2009-2016 Avaya Inc. All Rights Reserved."

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

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title "Application Enablement Services Management Console". On the right, a "Welcome" message provides user information: "Welcome: User", "Last login: Wed May 1 08:25:45 2019 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: 8.0.0.0.6-0", "Server Date and Time: Wed May 01 08:34:32 EDT 2019", and "HA Status: Not Configured". Below the header is a red navigation bar with "Home", "Help", and "Logout" links. The left 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 main content area 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 of domains and their functions: "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". A final paragraph 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 displays the Avaya Application Enablement Services Management Console with the "Licensing" section selected in the left sidebar. The top header and "Welcome" message are identical to the previous screenshot. The red navigation bar also remains the same. The left sidebar now highlights "Licensing" and includes sub-items: "WebLM Server Address", "WebLM Server Access", and "Reserved Licenses". The main content area is titled "Licensing" and contains three paragraphs of instructions: "If you are setting up and maintaining the WebLM, you need to use the following:" followed by a bulleted list with "WebLM Server Address"; "If you are importing, setting up and maintaining the license, you need to use the following:" followed by a bulleted list with "WebLM Server Access"; and "If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:" followed by a bulleted list with "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.

The screenshot shows the Avaya Aura System Manager 8.0 interface. The left pane displays a navigation tree with the following items: WebLM Home, Install license, Licensed products, APPL_ENAB, Application_Enablement (expanded), View by feature, View by local WebLM, Enterprise configuration, Local WebLM Configuration, Usages, Allocations, Periodic status, COMMUNICATION_MANAGER, Call_Center, Communication_Manager, MESSAGING, Messaging, and MSR. The right pane displays the 'Application Enablement (CTI) - Release: 8 - SID: 10503000 (Enterprise license file)' screen. It shows the breadcrumb 'You are here: Licensed Products > Application_Enablement > View by Feature' and the installation date 'License installed on: October 13, 2018 3:09:09 AM +00:00'. Below this, a text box displays 'License File Host IDs: V4-42-5D-06-BF-08-01'. A table lists the features and their license capacities:

Feature (License Keyword)	License Capacity
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	1000
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	16
Device Media and Call Control (VALUE_AES_DMCC_DMC)	1000
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	3
DLG (VALUE_AES_DLG)	16
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	1000
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	3
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	16

6.3. Administer TSAPI Link

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

The screenshot shows the AVAYA Application Enablement Services Management Console. The top header includes the AVAYA logo and the title "Application Enablement Services Management Console". On the right, a welcome message for the user is displayed, including login details and system status. The main navigation bar shows "AE Services | TSAPI | TSAPI Links" and "Home | Help | Logout". The left sidebar lists "AE Services" with sub-items: CVLAN, DLG, DMCC, SMS, TSAPI (expanded), TSAPI Links (selected), and TSAPI Properties. The main content area is titled "TSAPI Links" and contains a table with columns: Link, Switch Connection, Switch CTI Link #, ASAI Link Version, and Security. Below the table are buttons for "Add Link", "Edit Link", and "Delete Link".

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

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

The screenshot shows the AVAYA Application Enablement Services Management Console with the "Add TSAPI Links" screen. The top header and navigation bar are the same as the previous screenshot. The left sidebar shows "AE Services" with sub-items: CVLAN, DLG, DMCC, SMS, TSAPI (expanded), TSAPI Links (selected), TSAPI Properties, TWS, and Communication Manager Interface. The main content area is titled "Add TSAPI Links" and contains a form with the following fields: Link (dropdown menu showing "1"), Switch Connection (dropdown menu showing "cm7"), Switch CTI Link Number (dropdown menu showing "1"), ASAI Link Version (dropdown menu showing "9"), and Security (dropdown menu showing "Unencrypted"). Below the form are buttons for "Apply Changes" and "Cancel Changes".

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.

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Wed May 1 08:26:01 2019 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: 8.0.0.0.6-0
Server Date and Time: Wed May 01 09:20:48 EDT 2019
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

6.5. Administer Security Database

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

In the case 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 title "Application Enablement Services Management Console". A welcome message in the top right corner provides user information: "Welcome: User", "Last login: Wed May 1 08:25:45 2019 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: 8.0.0.0.6-0", "Server Date and Time: Wed May 01 08:34:32 EDT 2019", and "HA Status: Not Configured".

The main navigation bar is red and contains the breadcrumb "Security | Security Database | Control" and links for "Home | Help | Logout". The left sidebar is a dark grey menu with the following items: "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking", "Security" (expanded), "Account Management", "Audit", "Certificate Management", "Enterprise Directory", "Host AA", "PAM", "Security Database" (expanded), and "Control" (selected).

The main content area is titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services". It 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 **Unencrypted 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: Wed May 1 08:25:45 2019 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: 8.0.0.0.0.6-0
Server Date and Time: Wed May 01 08:34:32 EDT 2019
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/TLS Settings

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Ports

CVLAN Ports

Unencrypted TCP Port9999

Encrypted TCP Port9999

DLG PortTCP Port5678

TSAPI Ports

TSAPI Service Port450

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 Port4721

Encrypted Port4722

TR/87 Port4723

Enabled Disabled

☒ ☐

☒ ☐

☐ ☒

☒ ☐

☐ ☒

☐ ☒

☐ ☒

☐ ☒

☐ ☒

☐ ☒

☐ ☒

☐ ☒

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**.

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Wed May 1 08:25:45 2019 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: 8.0.0.0.6-0
Server Date and Time: Wed May 01 08:34:32 EDT 2019
HA Status: Not Configured

Maintenance | Service Controller

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▼ Maintenance

▶ Date Time/NTP Server

▶ Security Database

▶ Service Controller

▶ Server Data

▶ Networking

▶ Security

▶ Status

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](#)

StartStopRestart ServiceRestart AE ServerRestart LinuxRestart Web Server

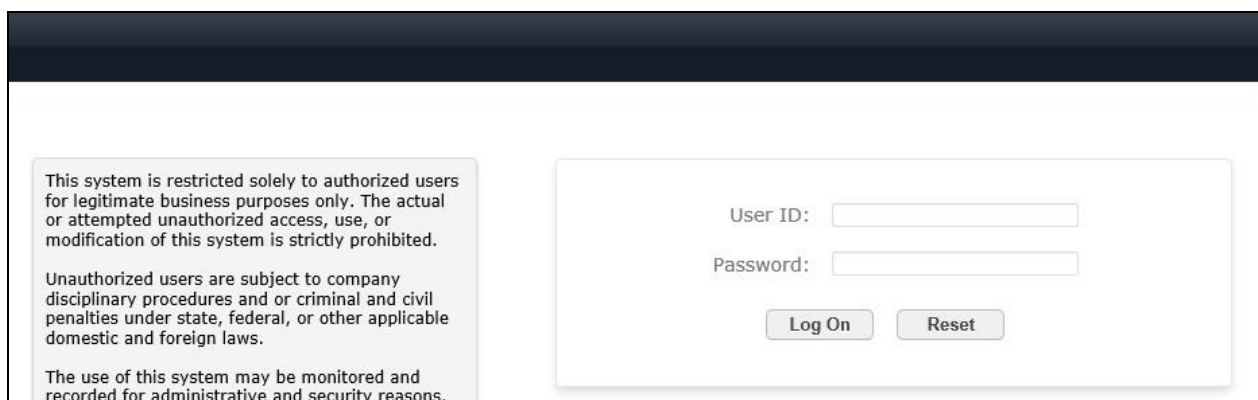
7. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager, which is performed via the web interface of System Manager. The procedures include the following areas:

- Launch System Manager
- Administer users

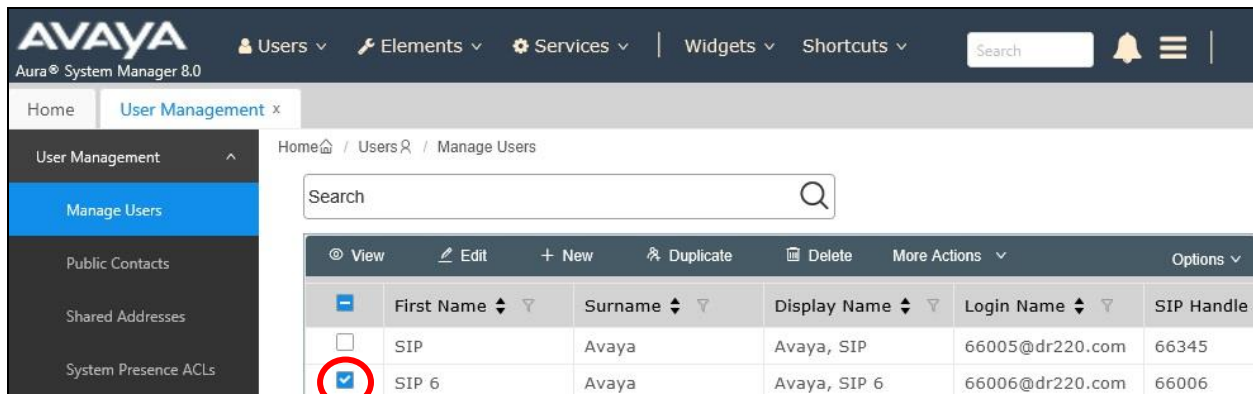
7.1. Launch System Manager

Access the System Manager web interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of System Manager. Log in using the appropriate credentials.



7.2. Administer Users

In the subsequent screen (not shown), select **Users → User Management**. Select **User Management → Manage Users** from the left pane to display the screen below. Select the entry associated with the first SIP agent station from **Section 3**, in this case “66006”, and click **Edit**.



	First Name	Surname	Display Name	Login Name	SIP Handle
<input type="checkbox"/>	SIP	Avaya	Avaya, SIP	66005@dr220.com	66345
<input checked="" type="checkbox"/>	SIP 6	Avaya	Avaya, SIP 6	66006@dr220.com	66006

The **User Profile | Edit** screen is displayed. Select the **Communication Profile** tab, followed by **CM Endpoint Profile** to display the screen below.

Click on the **Editor** icon shown below.

The screenshot shows the Avaya Aura System Manager 8.0 interface. The top navigation bar includes the Avaya logo, "Aura® System Manager 8.0", and tabs for Users, Elements, Services, Widgets, and Shortcuts. A search bar and notification bell are also present. The left sidebar shows the "User Management" menu with options like "Manage Users", "Public Contacts", "Shared Addresses", "System Presence ACLs", and "Communication Profile...". The main content area is titled "User Profile | Edit | 66006@dr220.com" and features tabs for Identity, Communication Profile, Membership, and Contacts. The "Communication Profile" tab is active, showing fields for "System" (DR-CM), "Profile Type" (Endpoint), "Extension" (66006), "Set Type" (9641SIPCC), "Port" (S00018), "Preferred Handle" (Select), and "Sip Trunk" (aar). The "CM Endpoint Profile" is highlighted in the left sidebar. The "Extension" field has an Editor icon circled in red.

In the popped-up screen, locate the **Type of 3PCC Enabled** parameter, and select “Avaya” from the drop-down list as shown below. Retain the existing values in the remaining fields.

The screenshot shows the Avaya Aura System Manager 8.0 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.0', and links for Users, Elements, Services, Widgets, and Shortcuts. A search bar and a notification bell are also present. The left sidebar shows the 'User Management' menu with options like 'Manage Users', 'Public Contacts', 'Shared Addresses', 'System Presence ACLs', and 'Communication Profile...'. The main content area is titled 'User Profile | Edit | 66006@dr220.com' and features tabs for Identity, Communication Profile, Membership, and Contacts. The 'Communication Profile' tab is active, showing various configuration options. The 'General Options (G)' tab is selected, displaying fields for Class of Restriction (COR), Emergency Location Ext, Tenant Number, SIP Trunk, Coverage Path 1, Lock Message, and Multibyte Language. The 'Class Of Service (COS)' and 'Message Lamp Ext.' fields are also visible. The 'Type of 3PCC Enabled' dropdown is highlighted with a red box and set to 'Avaya'. Other fields include 'Coverage Path 2', 'Localized Display Name' (Avaya, SIP 6), and 'Enable Reachability for Station Domain Control' (system). The 'SIP URI' field is empty. The 'Primary Session Manager' section shows 'IPv4: 10.64.101.238' and 'IPv6:'. The 'Secondary Session Manager' section is also visible.

General Options (G)	Feature Options (F)	Site Data (S)	Abbreviated Call Dialing (A)
Enhanced Call Fwd (E)	Button Assignment (B)	Profile Settings (P)	Group Membership (M)
* Class of Restriction (COR)	1	* Class Of Service (COS)	1
* Emergency Location Ext	66006	* Message Lamp Ext.	66006
* Tenant Number	1		
* SIP Trunk	Qaar	Type of 3PCC Enabled	Avaya
Coverage Path 1		Coverage Path 2	
Lock Message	<input type="checkbox"/>	Localized Display Name	Avaya, SIP 6
Multibyte Language	Not Applicable	Enable Reachability for Station Domain Control	system
SIP URI			
Primary Session Manager			
IPv4:	10.64.101.238	IPv6:	
Secondary Session Manager			

8. Configure InGenius Connector Enterprise

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

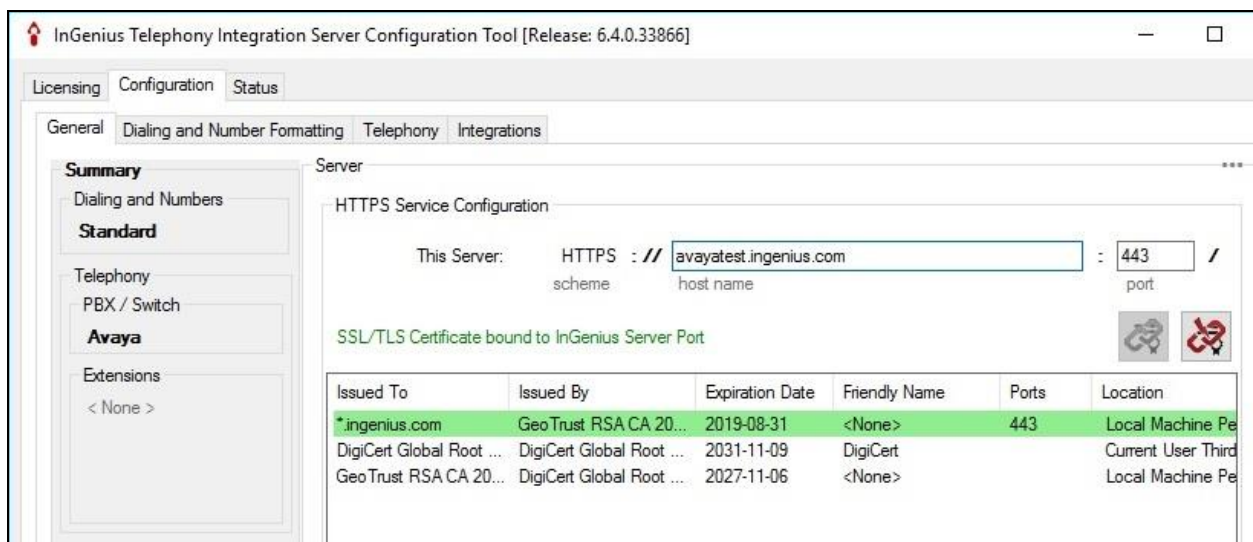
- Launch InGenius Server Configuration
- Administer dialing and number formatting
- Administer telephony
- Start service

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 [4] for more details.

8.1. Launch InGenius Server Configuration

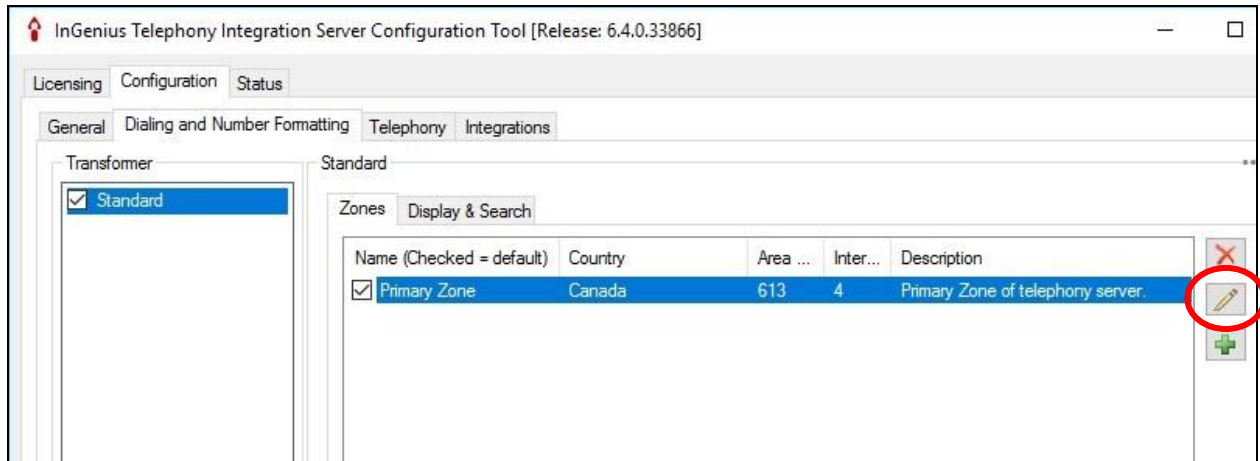
From the ICE server, navigate to **Start → InGenius → InGenius Server Configuration** to launch the application if necessary. Note that the application is automatically launched at the conclusion of the ICE installation.

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



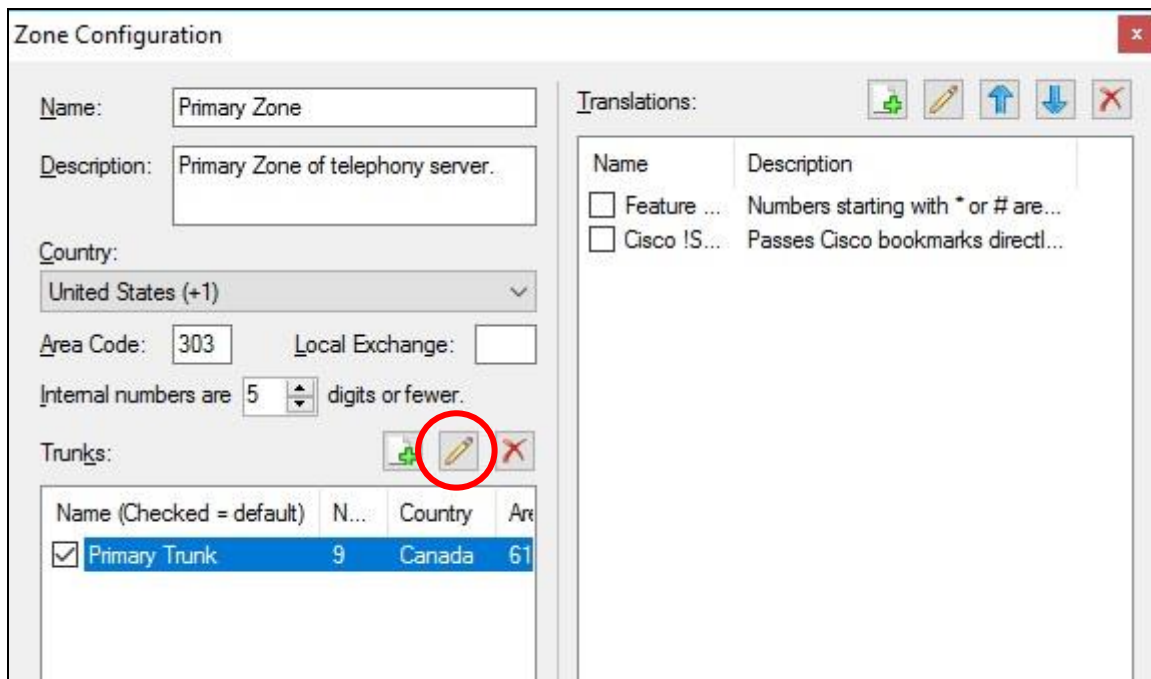
8.2. Administer Dialing and Number Formatting

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 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 [5] 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. On the left, there are fields for 'Name' (Primary Trunk), 'Description' (Primary trunk of telephony server.), 'Prefix' (9), 'Country' (United States (+1)), 'Area Code' (303), and 'Local Exchange'. Below these are checkboxes for 'Allowed calls': Local, Dial area code for local calls, Long Distance, and International, all of which are checked. Further down are fields for 'Long distance carrier code' and 'International carrier code'. At the bottom left is a 'Test dialing' section with fields for 'Enter number to dial', 'Expanded to', and 'Dialable'. On the right, there is a 'Translations to dialable' section with a table containing two entries: 'Argentina ...' and 'Mexican ...'. At the bottom right, there is an 'Auto configure local dialing' button and 'OK' and 'Cancel' buttons.

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

8.3. 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 (CM):** The relevant switch connection name from **Section 6.3**.

The screenshot displays the 'InGenius Telephony Integration Server Configuration Tool' window. The 'Configuration' tab is active, and the 'Telephony' sub-tab is selected. On the left, under 'PBX / Switch', 'Avaya' is checked. The main area shows the 'Primary AES' configuration for 'Avaya'. The 'Primary AES' tab is selected, showing fields for 'Address' (10.64.101.239), 'Port' (4721), 'Username' (ingenius), 'Password' (masked with asterisks), 'Connection manager (CM)' (cm7), and an unchecked 'Use secure connection' checkbox. A 'Server common name' field is also present but empty.

Select the **Agent Setup** tab in the right pane to display the screen below. Follow reference [5] 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 customers that use reason codes, check **Enable reason codes** in the **Reason Codes** sub-section and follow reference [5] to create reason code entries to match **Section 5.4**. In the compliance testing, one reason code was created under the **Logout** tab.

InGenius Telephony Integration Server Configuration Tool [Release: 6.4.0.33866]

Licensing Configuration Status

General Dialing and Number Formatting Telephony Integrations

PBX / Switch

Avaya

Primary AES Secondary AES Testing Agent Setup

Agent

☒ Enabled ☐ Unified Login ☒ EAS Enabled ☒ Stop monitor on log out

☒ Prompt for password on login ☒ Prompt for password when starting monitor

Work Modes

Login Ready

☒ Auto In ☒ After call work

☒ Manual In ☒ Aux work

Reason Codes

☒ Enable reason codes

Logout Not Ready Wrap-up

	Code	Comment	Enabled
	1	Finished Shift	<input checked="" type="checkbox"/>
*			<input checked="" type="checkbox"/>

Extensions

☐ Zone Assignment

Two reason codes were created under the **Not Ready** tab.

Reason Codes

☒ Enable reason codes

Logout Not Ready Wrap-up

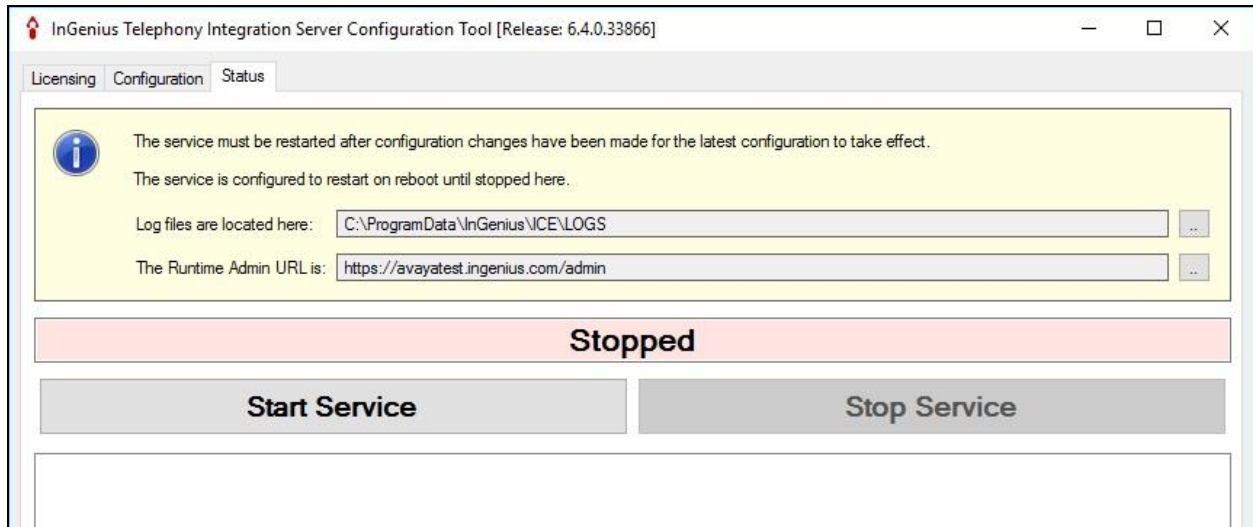
	Code	Comment	Enabled
	1	Lunch	<input checked="" type="checkbox"/>
	2	Coffee	<input checked="" type="checkbox"/>
*			<input checked="" type="checkbox"/>

Extensions

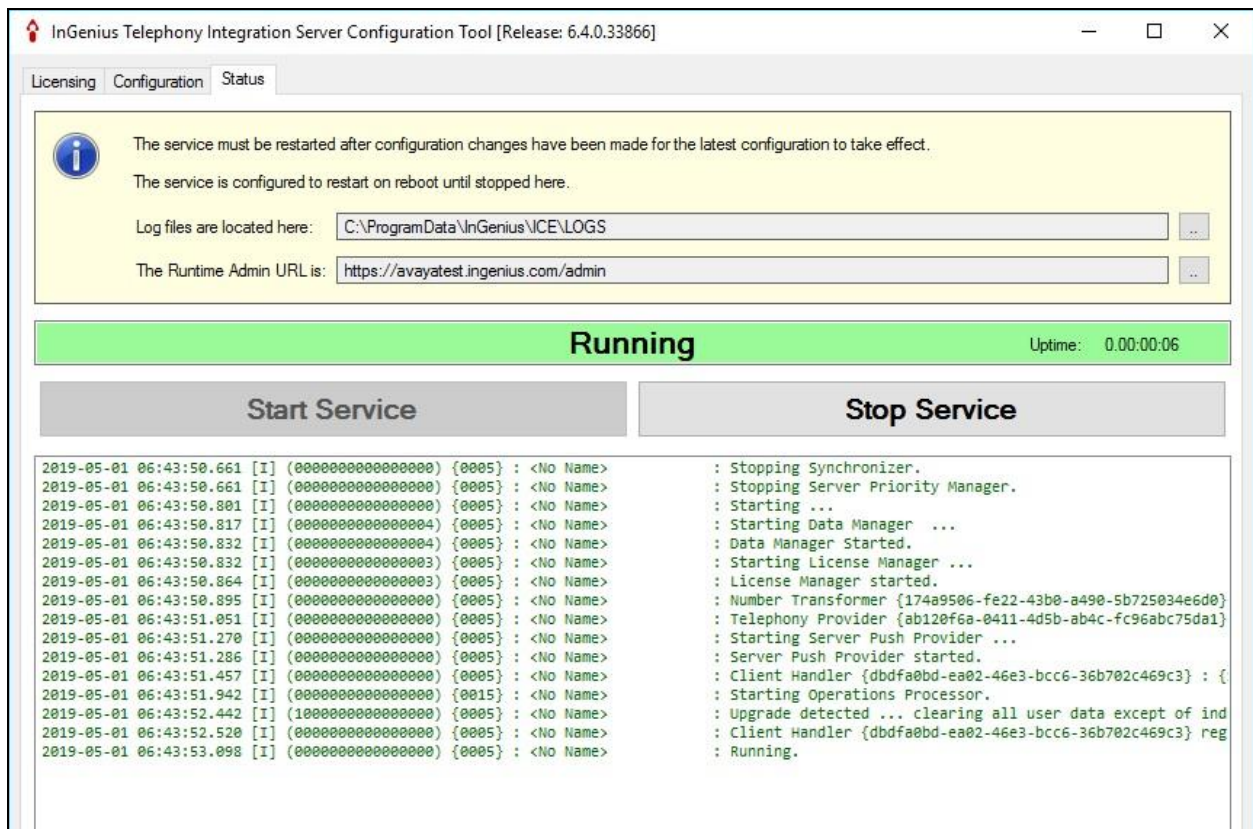
☐ Zone Assignment

8.4. Start Service

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



The screen is updated, as shown below.



9. Verification Steps

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

9.1. 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	9	no	aes7	established	1087	1069

9.2. 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**.

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Wed May 1 09:18:00 2019 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: 8.0.0.0.6-0
Server Date and Time: Wed May 01 10:14:10 EDT 2019
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

▶ Logs

▶ Log Manager

▼ 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 Wed May 01 10:14:00 EDT 2019

Service Uptime: 27 days, 19 hours 59 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 2

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"/>	5F8FE37B5E2E22734 0B4E784E3FF8D7-1	ingenius	InGenius Avaya Plugin	10.64.101.205	XML Unencrypted	0

Terminate Sessions Show Terminated Sessions

Item 1-1 of 1
1 Go

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 connected to the agent stations on Communication Manager, in this case “2”.



Application Enablement Services

Management Console

Welcome: User

Last login: Wed May 1 10:13:43 2019 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: 8.0.0.0.0.6-0

Server Date and Time: Wed May 01 10:26:45 EDT 2019

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

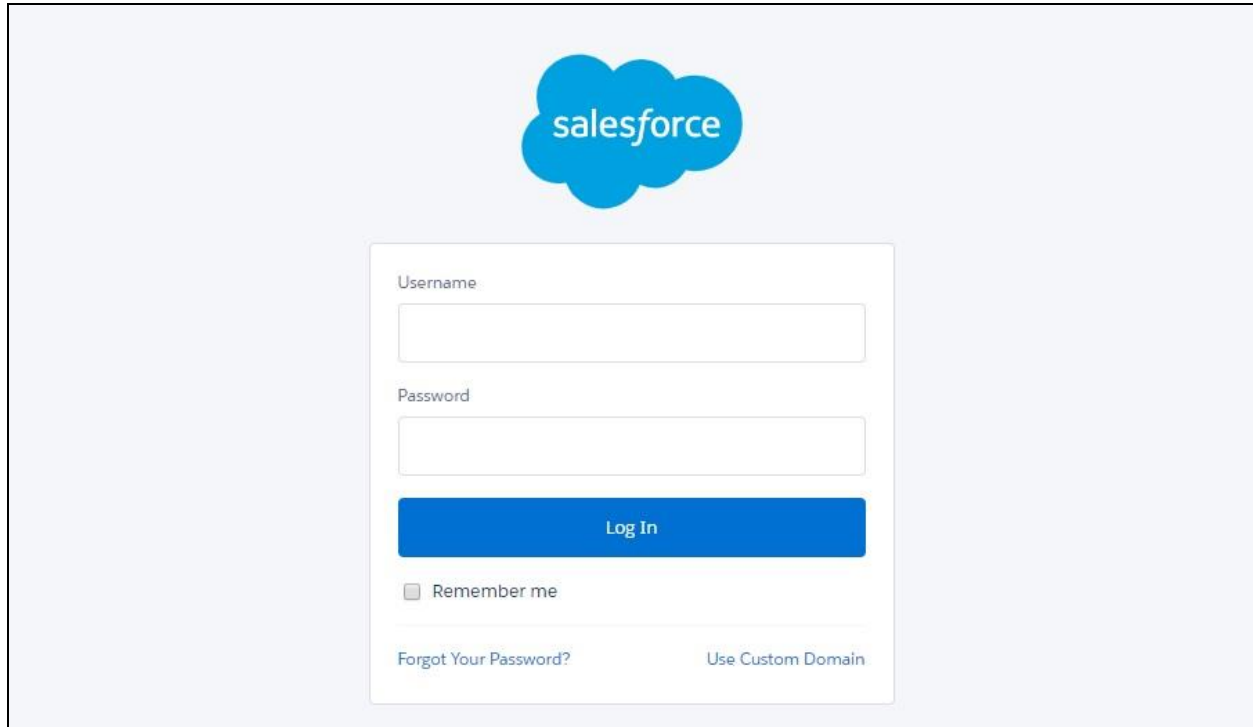
	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input checked="" type="radio"/>	1	cm7	1	Talking	Wed Apr 3 14:14:08 2019	Online	18	2	1108	1126	30

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

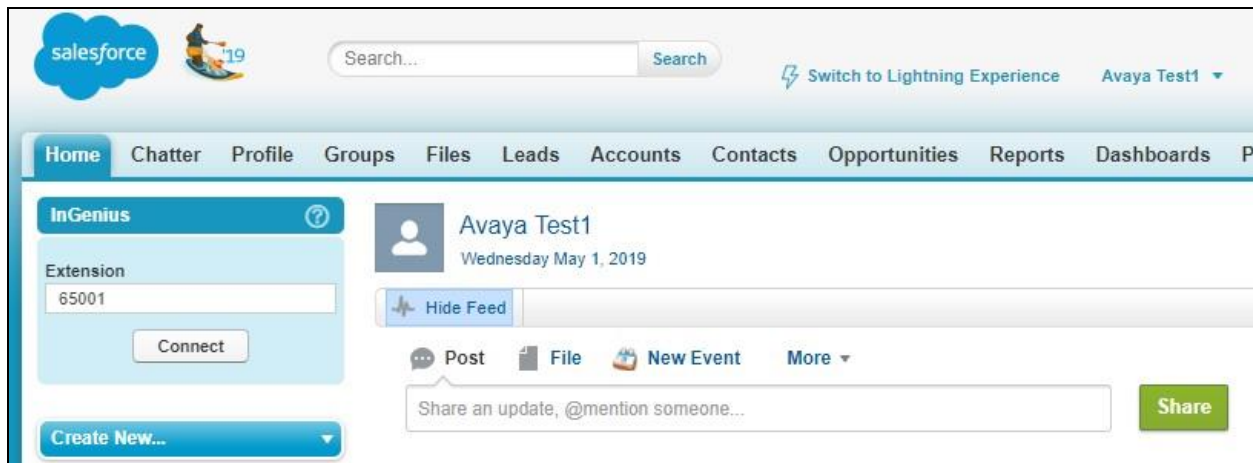
TSAPI Service Status
TLink Status
User Status

9.3. Verify InGenius Connector Enterprise

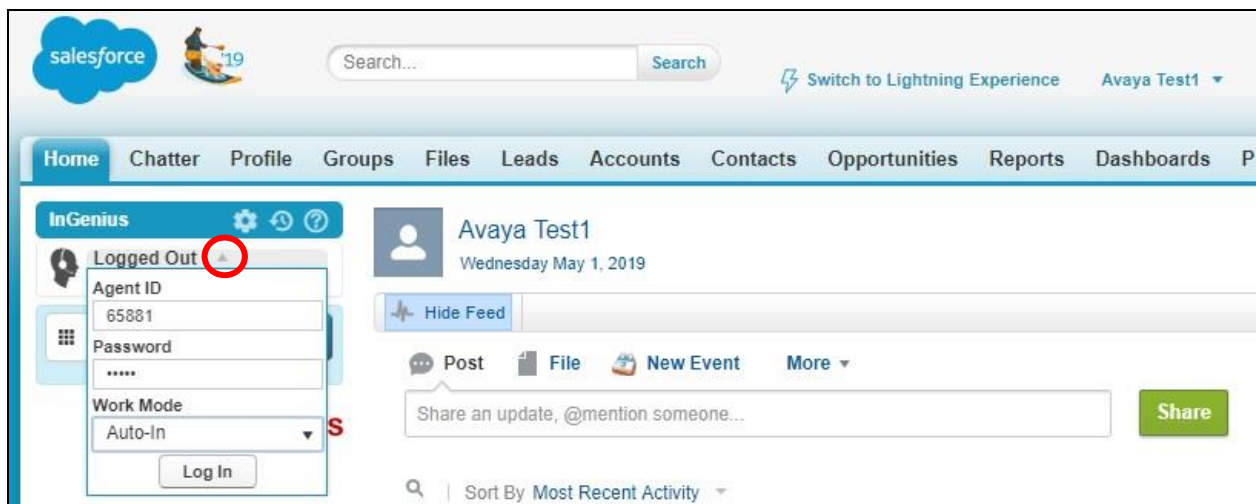
From an agent PC, launch an Internet browser window and enter the URL provided by the end customer for Salesforce.com. Log in with the relevant user credentials provided by InGenius.



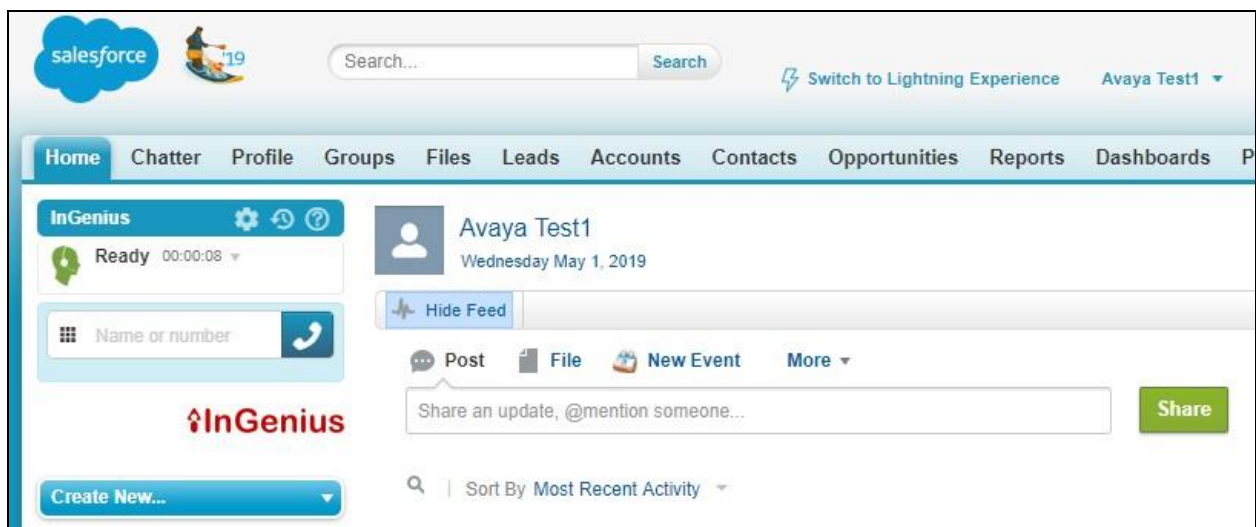
The screen below is displayed next. In the left pane, enter the relevant agent station extension from **Section 3**, and click **Connect**.



The left pane is updated, as shown below. Click on the **Logged Out** 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.

Note that in the case where there is more than one contact record matching to the PSTN caller number, then all records will be presented in the **Found 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 displays the Salesforce InGenius interface. The top navigation bar includes the Salesforce logo, a search bar, and links to 'Switch to Lightning Experience', 'Avaya Test1', and 'Setup'. The main navigation menu contains 'Home', 'Chatter', 'Profile', 'Groups', 'Files', 'Leads', 'Accounts', 'Contacts' (highlighted), 'Opportunities', 'Reports', 'Dashboards', and 'Products'.

The left sidebar features the 'InGenius' header with a 'Reserved' status and a timer. Below it is a search bar for 'Name or number'. The 'Inbound Call' section shows a 'Dialled #' of 60001 and a 'Number' of +1 (908) 953-2103, with a green 'Answer' button. The 'Found records' section lists 'Ms. DevConnect1 Avaya'.

The main content area displays the contact profile for 'Ms. DevConnect1 Avaya'. It includes a 'Show Feed' button and a 'Click to add topics' link. Below this is a 'Contact Detail' section with buttons for 'Edit', 'Delete', and 'Clone'. The details include: 'Contact Owner' (Avaya Test1 [Change]), 'Name' (Ms. DevConnect1 Avaya), 'Account Name' (AvayaTest), 'Title' (Test Engineer), 'Phone' ((908) 953-2103), 'Mobile', 'Email', and 'Reports To' ([View Org Chart]).

The 'Address Information' section shows the 'Mailing Address' as 350 Mount Kemble Avenue, Morristown NJ 07960, and a map view of the location. The 'Other Address' field is also present.

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

The screenshot displays the Salesforce interface for a contact record. The top navigation bar includes the Salesforce logo, a search bar, and links to 'Switch to Lightning Experience', 'Avaya Test1', and 'Setup'. The main navigation bar contains tabs for Home, Chatter, Profile, Groups, Files, Leads, Accounts, **Contacts**, Opportunities, Reports, Dashboards, and Products.

The left sidebar features the 'InGenius' section with a 'Talking' status and a timer of 00:00:18. Below this is a search bar for 'Name or number' and a 'Connected' call log showing a call to 'Dialled # 60001' with the number '+1 (908) 953-2103' on 01/05/2019 at 10:29 AM.

The main content area shows the contact record for 'Ms. DevConnect1 Avaya'. The 'Contact Detail' section includes fields for 'Contact Owner' (Avaya Test1), 'Name' (Ms. DevConnect1 Avaya), 'Account Name' (AvayaTest), and 'Title' (Test Engineer). The 'Address Information' section shows the 'Mailing Address' as '350 Mount Kemble Avenue, Morristown NJ 07960' and includes a map of the location.

10. Conclusion

These Application Notes describe the configuration steps required for InGenius Connector Enterprise 6.4 to successfully interoperate with Avaya Aura® Communication Manager 8.0 and Avaya Aura® Application Enablement Services 8.0 using Salesforce.com. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

11. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Release 8.0, Issue 2.1, November 2018, available at <http://support.avaya.com>.
2. *Administering Aura® Application Enablement Services*, Release 8.0, Issue 1, July 2018, available at <http://support.avaya.com>.
3. *Administering Avaya Aura® Session Manager*, Release 8.0, Issue 2, August 2018, available at <http://support.avaya.com>.
4. *InGenius Connector Enterprise for Salesforce Server Installation Guide for IT Administrator*, Version 6.4, available upon request to InGenius Support.
5. *InGenius Connector Enterprise for Salesforce and Avaya Aura Communications Manager User Guide*, Version 6.4, available upon request to InGenius Support.

©2019 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.