



Avaya Solution & Interoperability Test Lab

Application Notes for InGenius Connector Enterprise 6.0 with Avaya Aura® Communication Manager 7.1 and Avaya Aura® Application Enablement Services 7.1 using Salesforce.com – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for InGenius Connector Enterprise 6.0 to interoperate with Avaya Aura® Communication Manager 7.1 and Avaya Aura® Application Enablement Services 7.1 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) 6.0 to interoperate with Avaya Aura® Communication Manager 7.1 and Avaya Aura® Application Enablement Services 7.1 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.

2.3. Support

Technical support on ICE can be obtained through the following:

- **Phone:** +1 (613) 591-9002
- **Email:** 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 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, 66002
Agent IDs	65881, 65882
Agent Passwords	65881, 65882

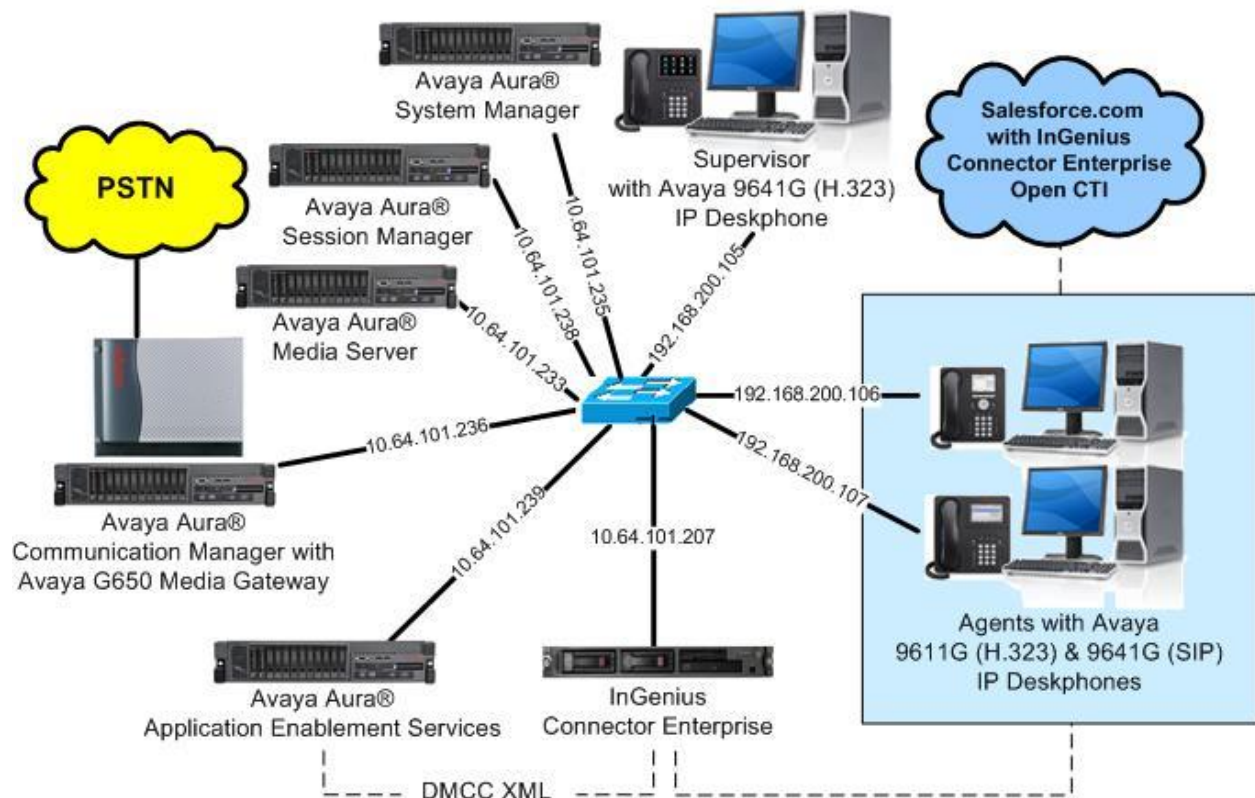


Figure 1: Compliance Testing Configuration

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	7.1.2 (7.1.2.0.0.532.24184)
Avaya G650 Media Gateway	NA
Avaya Aura® Media Server in Virtual Environment	7.8.0.333
Avaya Aura® Application Enablement Services in Virtual Environment	7.1.2 (7.1.2.0.0.3-0)
Avaya Aura® Session Manager in Virtual Environment	7.1.2 (7.1.2.0.712004)
Avaya Aura® System Manager in Virtual Environment	7.1.2 (7.1.2.0.057353)
Avaya 9611G & 9641G IP Deskphone (H.323)	6.6604
Avaya 9641G IP Deskphone (SIP)	7.1.1.0.9
InGenius Connector Enterprise on Windows Server 2012 <ul style="list-style-type: none">Avaya DMCC XMLInGenius Server Configuration	6.0.4.25288 R2 Standard 6.1 6.0.4.25288
InGenius Connector Enterprise Open CTI on Salesforce.com	v42 Spring 18

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	
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		
COR: 1		
Name: AES CTI Link		

5.3. Administer System Parameters Features

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

```
change system-parameters features                                     Page 5 of 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

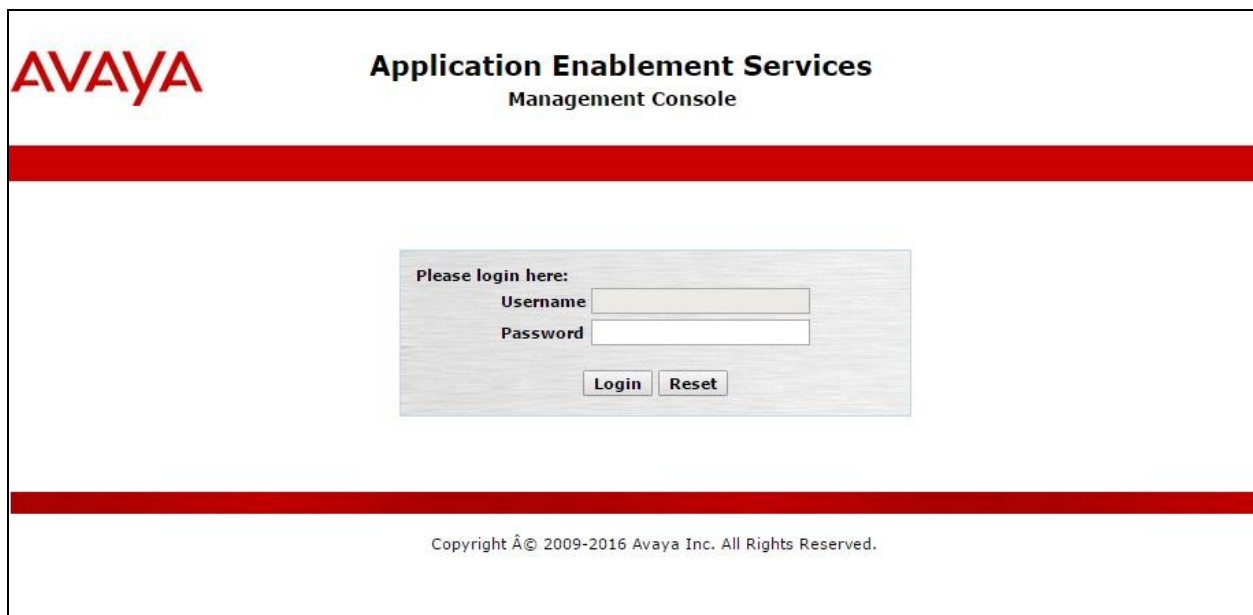
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- 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 separates the header from the main content area. In the center of the page is a light gray rectangular box containing the login form. The form has the text "Please login here:" followed by two input fields: "Username" and "Password". Below these fields are two buttons: "Login" and "Reset". Another thick red horizontal bar is located below the login box. At the 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: Mon Apr 16 09:15:27 2018 from 192.168.200.50", "Number of prior failed login attempts: 0", "HostName/IP: aes7/10.64.101.239", "Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE", "SW Version: 7.1.2.0.0.3-0", "Server Date and Time: Mon Apr 16 09:15:59 EDT 2018", 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 explaining the OAM Web's purpose. It lists several administrative domains and their corresponding tools: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. A note at the bottom states that these domains can be managed by a single administrator or separate administrators.

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Mon Apr 16 09:15:27 2018 from 192.168.200.50
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.2.0.0.3-0
Server Date and Time: Mon Apr 16 09:15:59 EDT 2018
HA Status: Not Configured

Home | Help | Logout

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

Welcome to OAM

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

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

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

6.2. Verify License

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. The top header and "Welcome" message are identical to the previous screenshot. The red navigation bar now shows "Licensing" as the active section. The left sidebar menu is updated: "Licensing" is highlighted with a blue arrow, and its sub-items, "WebLM Server Address", "WebLM Server Access", and "Reserved Licenses", are visible below it. The main content area is titled "Licensing" and provides instructions for setting up and maintaining the WebLM. It lists three categories of actions: "If you are setting up and maintaining the WebLM, you need to use the following:" (WebLM Server Address), "If you are importing, setting up and maintaining the license, you need to use the following:" (WebLM Server Access), and "If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:" (Reserved Licenses).

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Mon Apr 16 09:15:27 2018 from 192.168.200.50
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.2.0.0.3-0
Server Date and Time: Mon Apr 16 09:17:41 EDT 2018
HA Status: Not Configured

Licensing | Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
WebLM Server Address
WebLM Server Access
Reserved Licenses
Maintenance
Networking

Licensing

If you are setting up and maintaining the WebLM, you need to use the following:

- WebLM Server Address

If you are importing, setting up and maintaining the license, you need to use the following:

- WebLM Server Access

If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:

- Reserved Licenses

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.

AVAYA
Aura® System Manager 7.1

Last Logged on at: GO...

Home Licenses

WebLM Home
Install license
Licensed products
APPL_ENAB
▼ Application_Enablement
View license capacity
View peak usage
CIE
► CIE
CMM
► Communication_Manager_Messaging
Configure Centralized Licensing
COMMUNICATION_MANAGER
► Call_Center
► Communication_Manager
Configure Centralized Licensing
MESSAGING
► Messaging
MSR
► Media_Server
SYSTEM_MANAGER
► System_Manager

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

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

License installed on: February 23, 2018 7:13:58 PM +00:00

License File Host IDs: V8-7A-42-06-D9-59-01

Licensed Features

10 Items Show All ▼

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

6.3. Administer TSAPI Link

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

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

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
------	-------------------	-------------------	-------------------	----------

Buttons: Add Link, Edit Link, 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, specifically the "Add TSAPI Links" screen. The left sidebar shows the navigation tree with "AE Services" expanded, and "TSAPI" selected. The main content area displays the "Add TSAPI Links" form, which includes fields for Link, Switch Connection, Switch CTI Link Number, ASAI Link Version, and Security. Below the fields are buttons for "Apply Changes" and "Cancel Changes".

Form fields:

- Link: 1
- Switch Connection: cm7
- Switch CTI Link Number: 1
- ASAI Link Version: 8
- Security: Unencrypted

Buttons: Apply Changes, 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: Mon Apr 16 09:15:27 2018 from 192.168.200.50
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.2.0.0.3-0
Server Date and Time: Mon Apr 16 09:22:27 EDT 2018
HA Status: Not Configured

User Management | User Admin | Add UserHome | 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 Idingenius

* Common Nameingenius

* Surnameingenius

* User Password*****

* Confirm Password*****

Admin Note

Avaya RoleNone ▼

Business Category

Car License

CM Home

Css Home

CT UserYes ▼

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 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 title "Application Enablement Services Management Console". A welcome message and system information are shown in the top right corner. The main navigation pane on the left lists various services, with "Security" expanded to show "Security Database" and "Control" selected. The main content area displays the "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" configuration page, which contains two unchecked checkboxes and an "Apply Changes" button.

Welcome: User
Last login: Mon Apr 16 09:15:27 2018 from 192.168.200.50
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.2.0.0.3-0
Server Date and Time: Mon Apr 16 09:23:07 EDT 2018
HA Status: Not Configured

AVAYA Application Enablement Services
Management Console

Security | Security Database | Control Home | Help | Logout

▸ AE Services
▸ Communication Manager Interface
▸ High Availability
▸ Licensing
▸ Maintenance
▸ Networking
▼ Security
▸ Account Management
▸ Audit
▸ Certificate Management
▸ Enterprise Directory
▸ Host AA
▸ PAM
▼ Security Database
▪ Control

SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services

☐ Enable SDB for DMCC Service
☐ Enable SDB for TSAPI Service, JTAPI and Telephony Web Services
Apply Changes

6.6. 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: Mon Apr 16 09:15:27 2018 from 192.168.200.50
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.2.0.0.3-0
Server Date and Time: Mon Apr 16 09:23:34 EDT 2018
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 Port9998

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

H.323 Ports

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: Mon Apr 16 09:15:27 2018 from 192.168.200.50
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.2.0.0.3-0
Server Date and Time: Mon Apr 16 09:23:59 EDT 2018
HA Status: Not Configured

Maintenance | Service ControllerHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▼ Maintenance

Date Time/NTP Server

▶ Security Database

Service Controller

▶ Server Data

▶ Networking

▶ Security

▶ Status

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.

Recommended access to System Manager is via FQDN.
[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

User ID:

Password:

[Change Password](#)

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 **User Management** screen below. Select the entry associated with the first SIP agent station from **Section 3**, in this case “66002”, and click **Edit**.

AVAYA
Aura® System Manager 7.1

Last Logged on at: Go...

Home / Users / User Management / Manage Users

Search

User Management

Users

More Actions

3 Items All

	Last Name	First Name	Display Name	Login Name	SIP Handle	Last Login
<input checked="" type="checkbox"/>	Avaya	SIP 2	Avaya, SIP 2	66002@dr220.com	66002	

The **User Profile Edit** screen is displayed. Select the **Communication Profile** tab to display the screen below.

Navigate to the **CM Endpoint Profile** sub-section, and click **Endpoint Editor**.

AVAYA
Aura® System Manager 7.1

Last Logged on at: [] Go...

Home / Users / User Management / Manage Users

User Profile Edit: 66002@dr220.com [Commit & Continue]

Communication Profile

Communication Profile Password: [] [Edit]

[New] [Delete] [Done] [Cancel]

Name

☒ Primary

Select : None

* Name: [Primary]

Default : ☒

Communication Address

[New] [Edit] [Delete]

Type	Handle	Domain
<input type="checkbox"/> Avaya SIP	66002	dr220.com

Select : All, None

☒ **Session Manager Profile**

☒ **CM Endpoint Profile**

* System: [DR220-CM7-ES]

* Profile Type: [Endpoint]

Use Existing Endpoints: ☐

* Extension: [66002] [Endpoint Editor]

Display Extension Ranges: []

Template: [Select/Reset]

The **Edit Endpoint** screen is displayed next. For **Type of 3PCC Enabled**, select “Avaya” from the drop-down list as shown below. Retain the default values in the remaining fields.

AVAYA
Aura® System Manager 7.1

Last Logged on at: [] Go...

Home / Users / User Management / Manage Users

Edit Endpoint

System DR220-CM7-ES **Extension** 66002
Template Select **Set Type** 9641SIPCC
Port S00004 **Security Code** []
Name Avaya, SIP 2

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	
* Class of Restriction (COR)	1	* Class Of Service (COS)	1				
* Emergency Location Ext	66002	* Message Lamp Ext.	66002				
* Tenant Number	1	Type of 3PCC Enabled Avaya ▼					
* SIP Trunk	Qaar	Coverage Path 2					
Coverage Path 1	1	Localized Display Name		Avaya, SIP 2			
Lock Message	<input type="checkbox"/>	Enable Reachability for Station Domain Control		system ▼			
Multibyte Language	Not Applicable ▼						

*Required

8. Configure InGenius Connector Enterprise

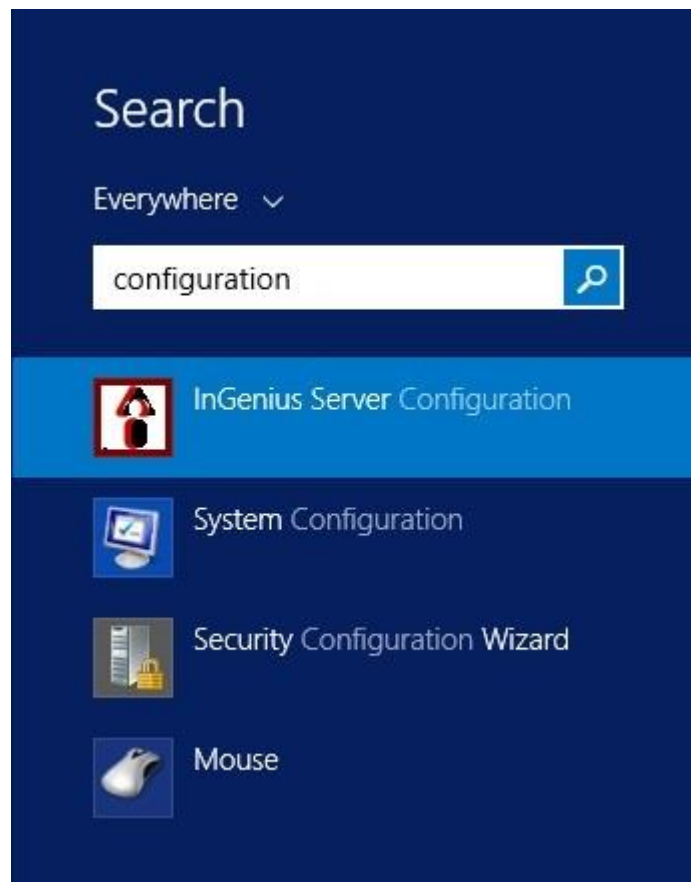
This section provides the procedures for configuring ICE. The procedures include the following areas:

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

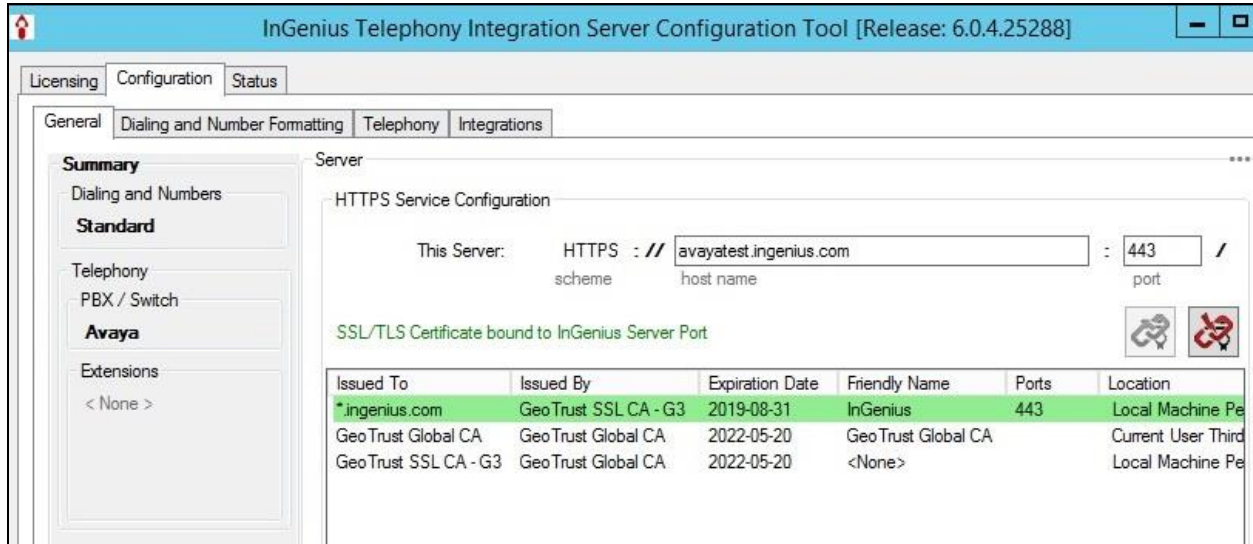
This section assumes the Connector Enterprise package has been imported and published, with the appropriate Security Role created, and users created and assigned to the Security Role. Refer to reference [4] for more details.

8.1. Launch InGenius Server Configuration

From the ICE server system tray, select the Windows icon (not shown) and enter “configuration” anywhere on the desktop to locate the **InGenius Server Configuration** application. Click on the pertinent entry from the result to launch the application.

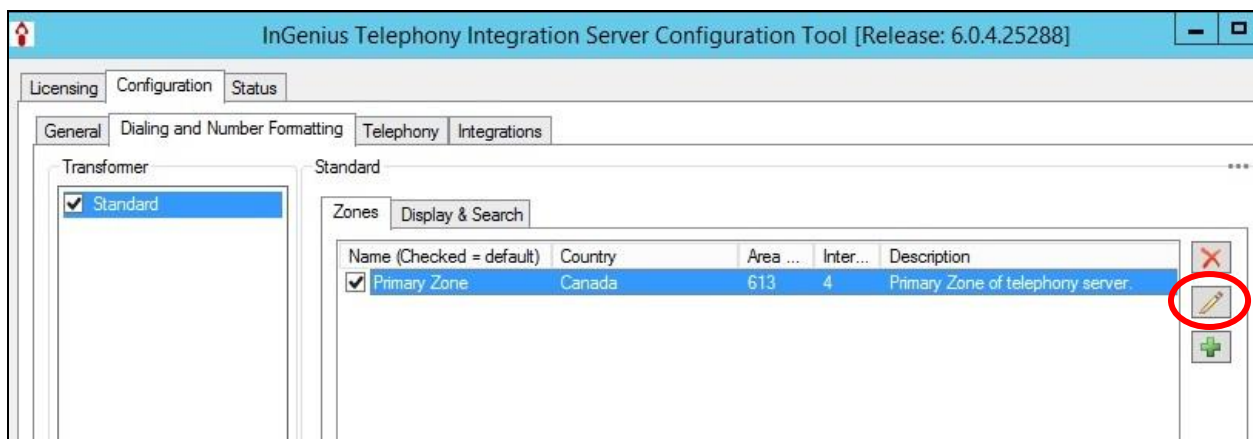


The **InGenius Telephony Integration Server Configuration Tool** screen is displayed.



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.

Zone Configuration

Name: Primary Zone

Description: Primary Zone of telephony server.

Country: United States (+1)

Area Code: 303 Local Exchange:

Internal numbers are 5 digits or fewer.

Trunks:

Name (Checked = default)	N...	Country	Ar
<input checked="" type="checkbox"/> Primary Trunk	9	Canada	61

Translations:

Name	Description
<input type="checkbox"/> Feature ...	Numbers starting with * or # are...
<input type="checkbox"/> Cisco !S...	Passes Cisco bookmarks directl...

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.

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...
<input type="checkbox"/> Mexican ...	International calls to Mexican ...

Auto configure local dialing

OK Cancel

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:** The relevant switch connection name from **Section 6.3**.

InGenius Telephony Integration Server Configuration Tool [Release: 6.0.4.25288]

Licensing Configuration Status

General Dialing and Number Formatting **Telephony** Integrations

PBX / Switch

☒ Avaya

Avaya

Primary AES Secondary AES Testing Agent Setup

Primary Application Enablement Services (AES)

Address: 10.64.101.239 Port: 4721

Username: ingenius

Password: *****

Connection manager (CM): cm7

☐ Use secure connection

Server common name:

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: 6.0.4.25288]

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

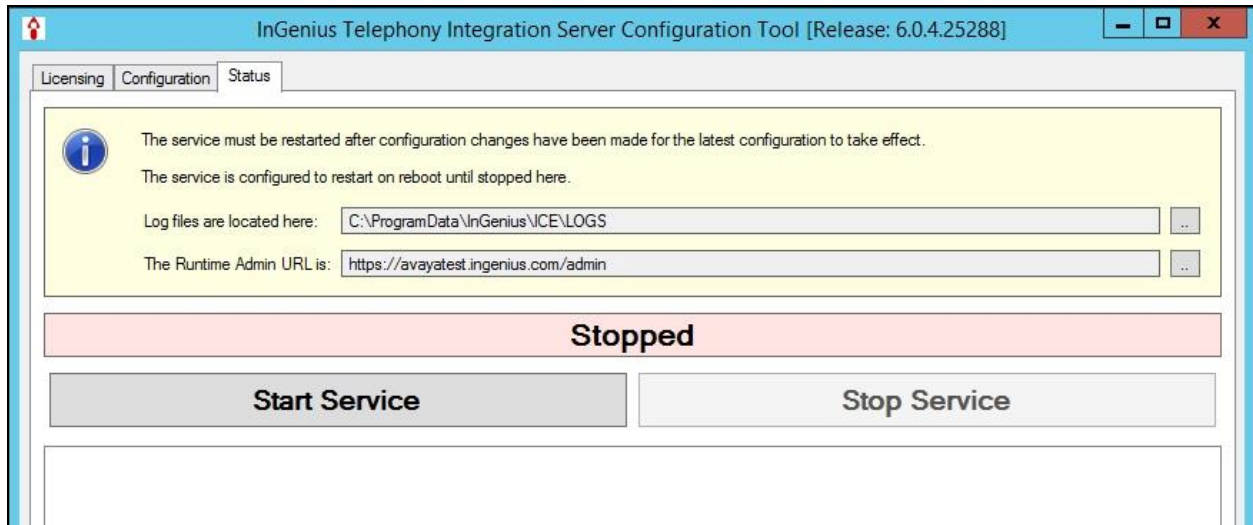
Code	Comment	Enabled
1	Lunch	<input checked="" type="checkbox"/>
2	Coffee	<input checked="" type="checkbox"/>
*		<input checked="" type="checkbox"/>

Extensions

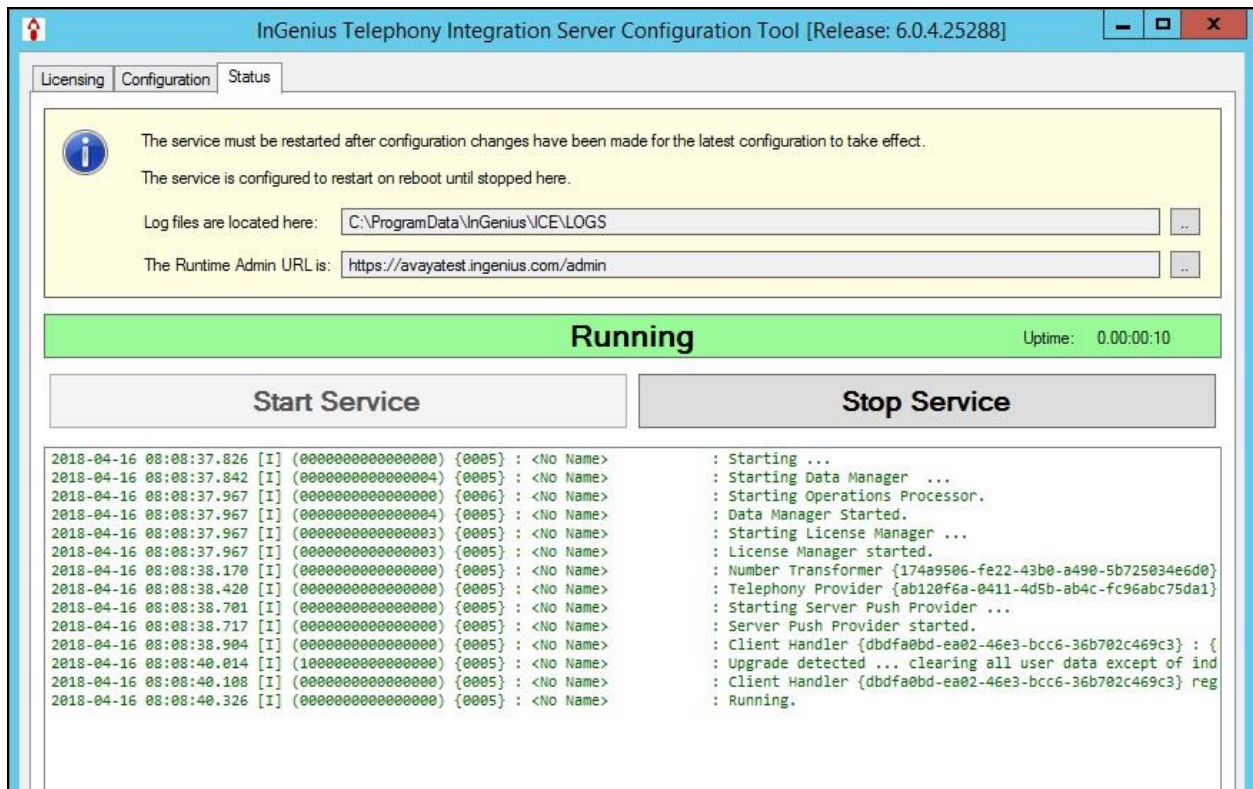
☐ Zone Assignment

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	8	no	aes7	established	425	419

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: Mon Apr 16 10:46:55 2018 from 192.168.200.50
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.2.0.0.3-0
Server Date and Time: Mon Apr 16 11:30:38 EDT 2018
HA Status: Not Configured

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

AE Services

Communication Manager Interface

High Availability

Licensing

Maintenance

Networking

Security

Status

Alarm Viewer

Log Manager

Logs

Status and Control

CVLAN Service Summary

DLG Services Summary

DMCC Service Summary

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)

Generated on Mon Apr 16 11:30:28 EDT 2018

Service Uptime: 55 days, 19 hours 29 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 4

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"/>	023FA07C8CA08AC67 3FCEF11A264263C-5	ingenius	InGenius Avaya Plugin	10.64.101.204	XML Unencrypted	0

Terminate Sessions Show Terminated Sessions

Item 1-1 of 1

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”.

AVAYA

Application Enablement Services
Management Console

Welcome: User
Last login: Mon Apr 16 10:46:55 2018 from 192.168.200.50
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.2.0.0.3-0
Server Date and Time: Mon Apr 16 11:31:52 EDT 2018
HA Status: Not Configured

Status | Status and Control | TSAPI Service SummaryHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

▶ Log Manager

▶ Logs

▼ Status and Control

■ CVLAN Service Summary

■ DLG Services Summary

■ DMCC Service Summary

■ Switch Conn Summary

■ TSAPI Service Summary

TSAPI Link Details

☐ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input checked="" type="radio"/>	1	cm7	1	Talking	Mon Feb 19 15:00:30 2018	Online	17	2	477	483	30

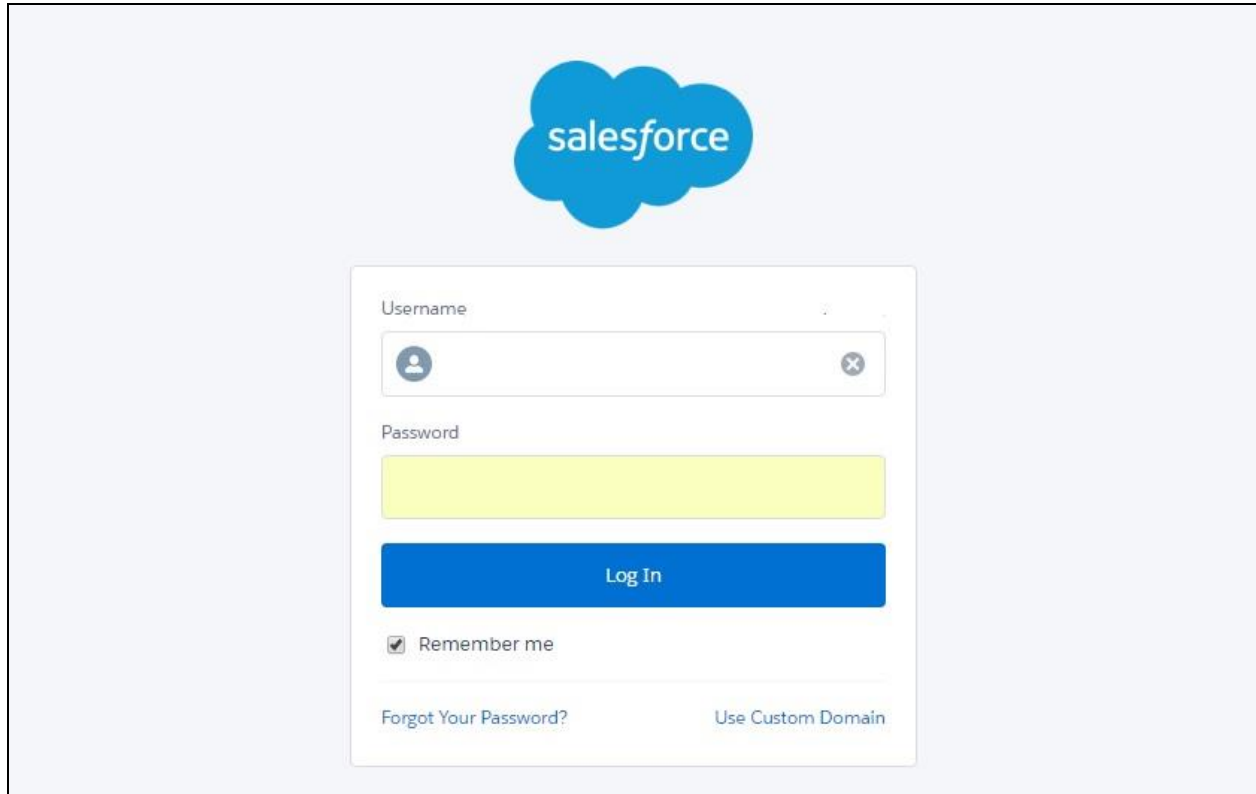
OnlineOffline

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

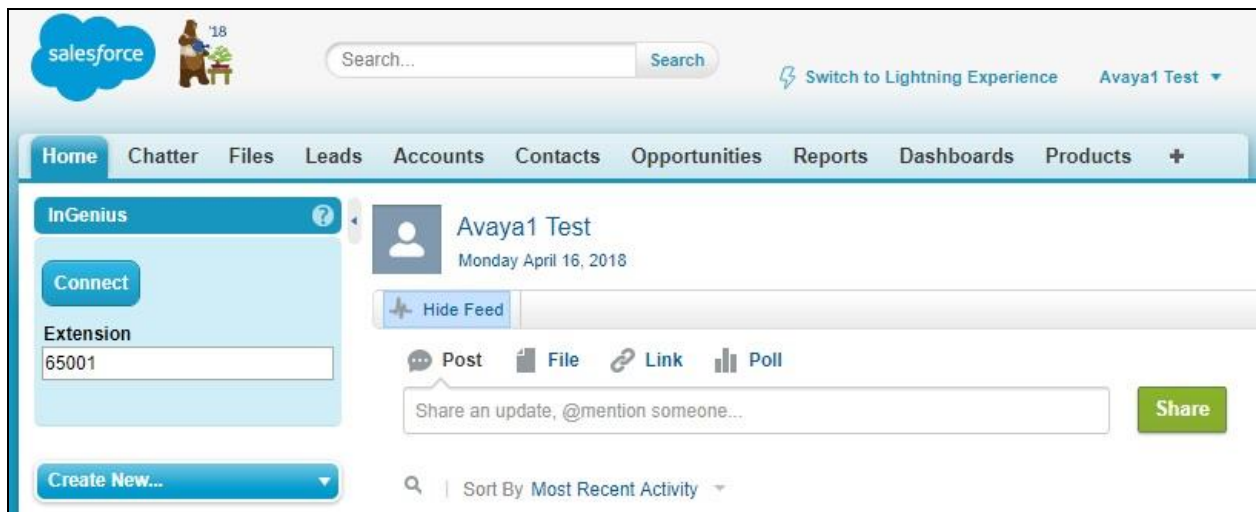
TSAPI Service StatusTLink StatusUser Status

9.3. Verify InGenius Connector Enterprise

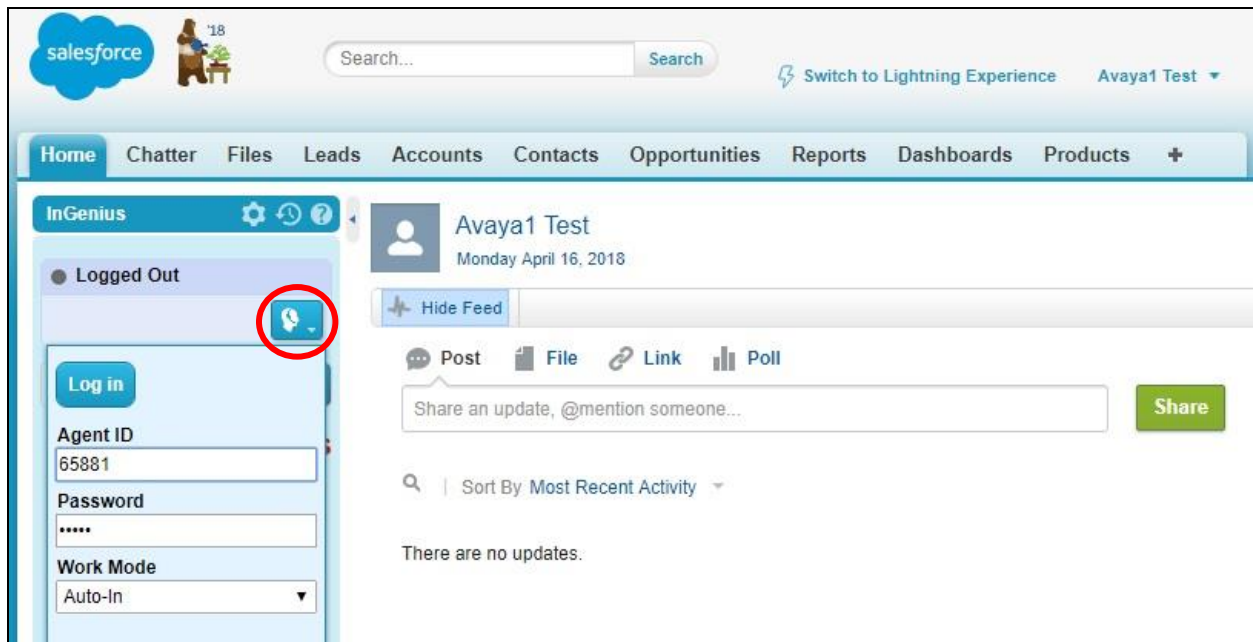
From an agent PC, launch an Internet browser window and enter the URL provided by the end customer for Salesforce.com. Log in with the relevant user credentials provided by InGenius.



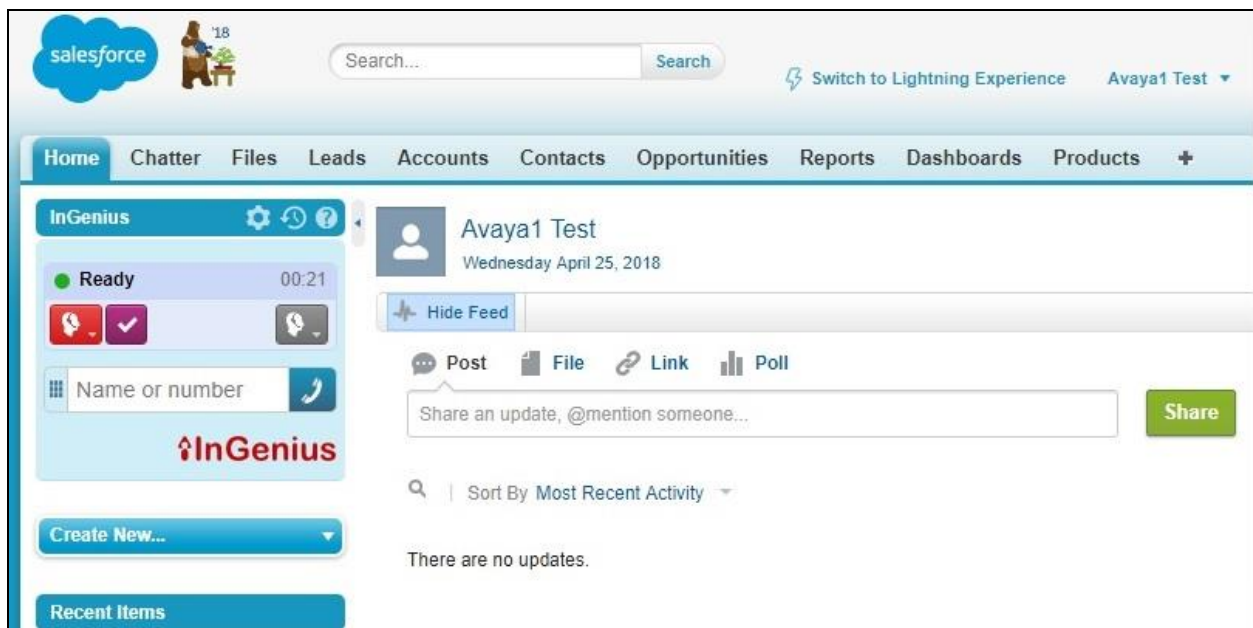
The screen below is displayed next. In the left pane, enter the relevant agent station extension from **Section 3**, and click **Connect**.



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



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



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

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

Click **Answer** in the left pane.

The screenshot displays the Salesforce InGenius interface. The top navigation bar includes the Salesforce logo, a search bar, and links to 'Switch to Lightning Experience', 'Avaya1 Test', and 'Help & Training'. The main navigation menu lists 'Home', 'Chatter', 'Files', 'Leads', 'Accounts', 'Contacts', 'Opportunities', 'Reports', 'Dashboards', and 'Products'. A banner below the navigation menu reads 'Take Salesforce with you wherever you go. Run your business from any mobile device with Salesforce for iOS and Android.' The left sidebar contains the 'InGenius' section with a 'Reserved' status, a 'Name or number' search bar, an 'Inbound Call' section showing a dialed number and a number, and a 'Call Actions' section with a 'New...' button. Below this is the 'Related Records' section showing a list of records, including 'Ms. DevConnect Avaya'. The main content area displays the contact record for 'Ms. DevConnect Avaya'. It includes a 'Hide Feed' button, a 'Post' section with a 'Write something...' text box and a 'Share' button, and a 'Followers' section showing 'No followers'. Below the feed is a 'Contact Detail' section with buttons for 'Edit', 'Delete', and 'Clone'. The contact details include 'Contact Owner' (Avaya1 Test), 'Phone' ((908) 953-2103), 'Name' (Ms. DevConnect Avaya), 'Account Name' (AvayaTest), 'Title' (Test Engineer), and 'Reports To' ([View Org Chart]). The 'Address Information' section shows the 'Mailing Address' as 350 Mount Kemble Ave, Morristown NJ 07960, and a map view of the location.

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 shows the Salesforce InGenius interface. The top navigation bar includes links for Home, Chatter, Files, Leads, Accounts, **Contacts**, Opportunities, Reports, Dashboards, and Products. A search bar and a 'Switch to Lightning Experience' button are also present. Below the navigation bar is a banner for 'Take Salesforce with you wherever you go.' The left sidebar, titled 'InGenius', displays call status updates: 'Talking' (00:36) and 'Connected' (00:22). The 'Connected' status shows the dialed number '+1 (303) 536-0001' and the number '+1 (908) 953-2103'. The main area shows the contact record for 'Ms. DevConnect Avaya'. The contact details include: Contact Owner 'Avaya1 Test', Name 'Ms. DevConnect Avaya', Account Name 'AvayaTest', Title 'Test Engineer', Phone '(908) 953-2103', and Mailing Address '350 Mount Kemble Ave, Morristown NJ 07960'. The interface also includes a 'Call Log' section and a 'Call Actions' dropdown menu.

10. Conclusion

These Application Notes describe the configuration steps required for InGenius Connector Enterprise 6.0 to successfully interoperate with Avaya Aura® Communication Manager 7.1 and Avaya Aura® Application Enablement Services 7.1 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 7.1.2, Issue 5, February 2018, available at <http://support.avaya.com>.
2. *Administering and Maintaining Aura® Application Enablement Services*, Release 7.1.2, Issue 4, December 2017, available at <http://support.avaya.com>.
3. *Administering Avaya Aura® Session Manager*, Release 7.1.2, Issue 4, March 2018, available at <http://support.avaya.com>.
4. *InGenius Connector Enterprise for Salesforce Server Installation Guide for IT Administrator*, Version 6.0, available upon request to InGenius Support.
5. *InGenius Connector Enterprise for Salesforce and Avaya Aura Communications Manager User Guide*, Version 6.0, available upon request to InGenius Support.

©2018 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.