



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

---

# **Application Notes for InGenius Connector Enterprise with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services - Issue 1.0**

### **Abstract**

These Application Notes describe a compliance-tested configuration comprised of Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services, Avaya IP and Digital Telephones, and InGenius Connector Enterprise.

InGenius Connector Enterprise is a CRM-VoIP integration tool, which sits between the customer's phone system (e.g. Avaya) and contact management system (e.g. Salesforce), and allows the end user to perform call control and then log the call into the contact management system.

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 a compliance-tested configuration comprised of Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services, Avaya IP and Digital Telephones, and InGenius Connector Enterprise applications.

InGenius Connector Enterprise is an enterprise-level Computer-Telephony Integration (CTI) product designed to connect Avaya Aura Communication Manager with Salesforce.com or Microsoft Dynamics CRM. InGenius Connector Enterprise enables easier call control and ensures that telephony activity is accurately captured for detailed reporting in the CRM system. InGenius Connector Enterprise is a server-based CTI product that requires no desktop install. Once the server is configured, the end-user needs only to log into a connected CRM, and the ICE interface will be rendered in their web browser.

The Avaya Plugin for InGenius Connector Enterprise uses DMCC to communicate with the Avaya AES. InGenius Connector Enterprise requires both the DMCC service and the TSAPI service running in Application Enablement Services. InGenius Connector Enterprise utilizes the switch connection name to enable 3rd party call control.

## 2. General Test Approach and Test Results

The general approach was to exercise basic telephone and call operations on Avaya IP and Digital telephones using InGenius Connector Enterprise. The main objectives were to verify that:

- The user may successfully use InGenius Connector Enterprise to perform off-hook, on-hook, dial, answer, hold, retrieve, transfer, conference, and release operations on the physical telephone.
- The agent user may successfully use InGenius Connector Enterprise to log into and out of an ACD, and move between agent work modes.
- Manual operations performed on the physical telephone are correctly reflected in the InGenius Connector Enterprise.
- InGenius Connector Enterprise and manual telephone operations may be used interchangeably; for example, go off-hook using InGenius Connector Enterprise and manually dial digits.
- Display and call information on the physical telephone is accurately reflected in the InGenius Connector Enterprise.
- Call states are consistent between InGenius Connector Enterprise and the physical telephone.

For serviceability testing, failures such as cable pulls and resets were applied.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

## 2.1. Interoperability Compliance Testing

The interoperability compliance test included features and serviceability. The focus of the compliance test was primarily on verifying the interoperability between InGenius Connector Enterprise, Application Enablement Services, and Communication Manager.

## 2.2. Test Results

All test cases were executed and passed.

## 2.3. Support

Technical support for the InGenius Connector Enterprise solution can be obtained by contacting InGenius:

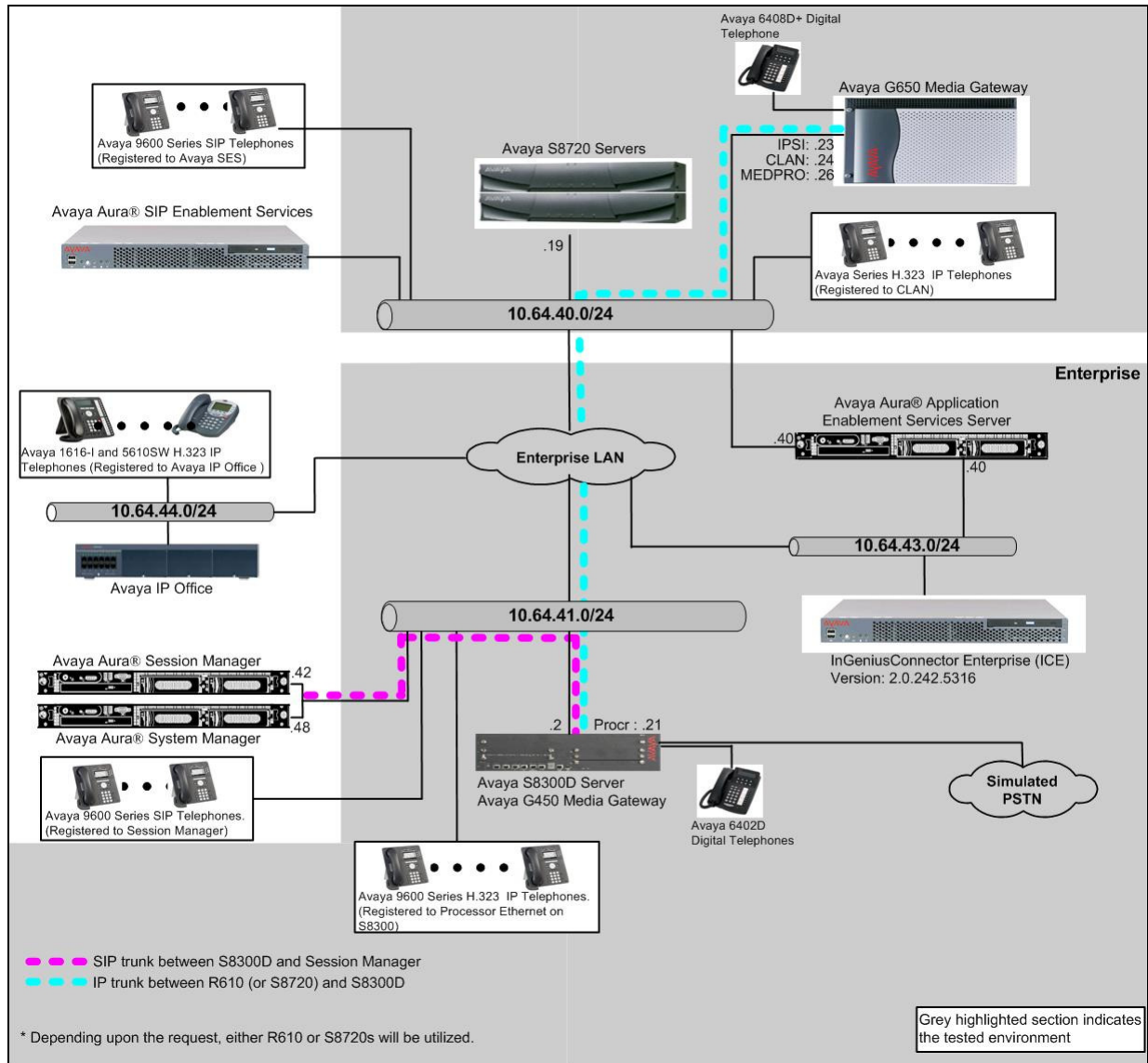
- URL – [icesupport@ingenius.com](mailto:icesupport@ingenius.com)
- Phone – (613) 591-9002 ext. 2400

## 3. Reference Configuration

**Figure 1** illustrates the configuration used in these Application Notes. The sample configuration shows an enterprise with an Application Enablement Services server and an Avaya S8300D Server running Communication Manager software with an Avaya G450 Media Gateway. InGenius Connector Enterprise was located in a different VLAN. Endpoints include Avaya 9600 Series H.323 IP Telephones and an Avaya 6408D Digital Telephone.

Avaya S8720 Servers with an Avaya G650 Media Gateway was included in the test to provide an inter-switch scenario.

**Note:** Basic administration of Application Enablement Services server is assumed. For details, see [2] in **Section 10**. The document is available at <http://support.avaya.com>.



**Figure 1: InGenius Connector Enterprise Test Configuration.**

## 4. Equipment and Software Validated

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

Equipment		Software/Firmware
Avaya S8300D Server with Avaya G450 Media Gateway		Avaya Aura® Communication Manager 6.3(R016x.03.0.124.0) w/ patch 03.0.124.0-20553
Avaya Aura® Application Enablement Services Server		6.3.0.0.212.0
Avaya S8720 Servers with Avaya G650 Media Gateway ( <i>used for inter-switch test scenarios</i> )		Avaya Aura® Communication Manager 5.2.1 (R015x.02.1.016.4)
Avaya 9600 Series IP Telephones		
	9620 (H.323)	3.1
	9630 (H.323)	3.1
	9650 (H.323)	3.1
Avaya 6408D+ Digital Telephone		-
InGenius Connect Enterprise		2.0.242.5316

## 5. Configure Avaya Aura® Communication Manager

This section describes the procedures for configuring IP Services, Feature Access Codes, Abbreviated Dialing, and controlled telephones.

### 5.1. Configure IP Services

Enter the **change node-names ip** command. In the compliance-tested configuration, the procr IP address was used for registering H.323 endpoints, and for connectivity to Application Enablement Services.

change node-names ip		Page 1 of 1
IP NODE NAMES		
Name	IP Address	
aes	10.64.43.40	
procr	10.64.41.21	
procr6	::	

Enter the **change ip-services** command. On **Page 1**, configure the Service Type field to **AESVCS** and the Enabled field to **y**. The Local Node field should be pointed to the **procr** that was configured previously in the IP NODE NAMES form in this section. During the compliance test, the default port was used for the Local Port field.

change ip-services

Page1 of 4

IP SERVICES

Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port
AESVCS	y	procr	8765		
CDR1		procr	0	rdtt	9002

On **Page 4**, enter the hostname of the Application Enablement Services server for the AE Services Server field. The server name may be obtained by logging in to the Application Enablement Services server using ssh, and running the command **uname -a**. Enter an alphanumeric password for the Password field. Set the Enabled field to **y**. The same password will be configured on the Application Enablement Services server in **Section 6.2**.

change ip-services				Page 4 of 4
AE Services Administration				
Server ID	AE Services	Password	Enabled	Status
	Server			
1:	aes	*	y	idle
2:				

## 5.2. Configure Feature Access Codes (FAC)

Enter the **change feature-access-codes** command. On **Page 5** of the **feature-access-codes** form, configure and enable the following access codes:

- After Call Work Access Code
- Auto-In Access Code
- Aux Work Access Code
- Login Access Code
- Logout Access Code

```
change feature-access-codes                                     Page 5 of 11
                                         FEATURE ACCESS CODE (FAC)

                                         Call Center Features

AGENT WORK MODES
    After Call Work Access Code: 120
        Assist Access Code: 121
            Auto-In Access Code: 122
                Aux Work Access Code: 123
                    Login Access Code: 124
                        Logout Access Code: 125
                            Manual-in Access Code: 126

SERVICE OBSERVING
    Service Observing Listen Only Access Code: 127
    Service Observing Listen/Talk Access Code: 128
        Service Observing No Talk Access Code: 129
    Service Observing Next Call Listen Only Access Code:
```

## 5.3. Configure Abbreviated Dialing

Enter the **add abbreviated-dialing group g** command, where **g** is the number of an available abbreviated dialing group. In the **DIAL CODE** list, enter the Feature Access Codes for ACD Login and Logout from **Section 5.2**.

```
add abbreviated-dialing group 1                               Page 1 of 1
                                         ABBREVIATED DIALING LIST

Group List: 1          Group Name: Call Center
Size (multiple of 5): 5  Program Ext:          Privileged? n
DIAL CODE
    11: 124
    12: 125
    13:
```

## 5.4. Configure Controlled Telephones

Enter the **change station r** command, where **r** is the extension of a registered, physical Avaya IP or Digital telephone. On **Page 1** of the **station** form, enter a phone Type, descriptive name, Security Code and set the IP SoftPhone field to **y** to allow the physical station to be controlled by a softphone such as the InGenius Connector Enterprise application.

```
change station 72001                                     Page 1 of 5

                                STATION

Extension: 72001                                           Lock Messages? n           BCC: 0
Type: 9620                                                 Security Code: *           TN: 1
Port: S00122                                              Coverage Path 1: 94        COR: 1
Name: H323-1                                              Coverage Path 2:           COS: 1
                                                           Hunt-to Station:          Tests? y

STATION OPTIONS

Loss Group: 19                                           Time of Day Lock Table:
                                                           Personalized Ringing Pattern: 1
                                                           Message Lamp Ext: 72001
Speakerphone: 2-way                                       Mute Button Enabled? n
Display Language: english
Survivable GK Node Name:
Survivable COR: internal
Survivable Trunk Dest? y
Media Complex Ext:
IP SoftPhone? y
IP Video Softphone? n
Short/Prefixed Registration Allowed: default
```

On **Page 4** of the station form, for **ABBREVIATED DIALING List 2**, enter the abbreviated dialing group configured in **Section 5.2**. On **Pages 4** and **5** of the station forms, configure the following **BUTTON ASSIGNMENTS** in addition to the call-appr (call appearance) buttons:

- auto-in (on Page 4)
- aux-work (on Page 4)
- abrv-dial – configure two of these buttons, one for Login and one for Logout, along with the Dial Codes from Abbreviated Dialing List 2 for ACD Login and Logout, respectively (on Page 4 and 5)
- after-call (On Page 5)

```
change station 72001                                     Page 4 of 5

                                STATION

SITE DATA
Room:                                                     Headset? n
Jack:                                                     Speaker? n
Cable:                                                    Mounting: d
Floor:                                                    Cord Length: 0
Building:                                                 Set Color:

ABBREVIATED DIALING
List1: personal 1      List2: group      1      List3:

BUTTON ASSIGNMENTS
1: call-appr          4: auto-in      Grp:
2: call-appr          5: aux-work      RC:      Grp:
3: call-appr          6: abrv-dial   List: 2 DC: 01 HL? n
```



change station 72001				Page 5 of 5	
				STATION	
BUTTON ASSIGNMENTS					
7:	abrv-dial List: 2 DC: 02 HL? n			10:	
8:	after-call		Grp:		11:
9:					12:

Repeat the instructions provided in this section for each physical station that is to be controlled / monitored by an InGenius Connector Enterprise.

## 6. Configure Avaya Aura® Application Enablement Services

The Application Enablement Services server enables Computer Telephony Interface (CTI) applications to control and monitor telephony resources on Communication Manager.

This section assumes that installation and basic administration of the Application Enablement Services server has been performed. The steps in this section describe the configuration of a Switch Connection, a CTI user, and a DMCC port.


### 6.1. Device and Media Call Control API Station Licenses

InGenius Connector Enterprise instances appear as “virtual” stations/softphones to Communication Manager. Each of these virtual stations, hereafter called Device and Media Call Control API station, requires a license. Note that this is separate and independent of Avaya IP Softphone licenses, which are required for Avaya IP Softphones but not required for Device and Media Call Control API stations. To check and verify that there are sufficient DMCC licenses, log in to <https://<IP address of the Application Enablement Services server>/index.jsp>, and enter appropriate login credentials to access the Application Enablement Services Management Console page.

Select the **Licensing** → **WebLM Server Access** link from the left pane of the window.

The screenshot displays the Avaya Application Enablement Services Management Console. At the top left is the Avaya logo. The main title is "Application Enablement Services Management Console". On the right, a welcome message for user 'craft' is shown, including login details and system version. A red navigation bar at the top contains "Licensing" and "Home | Help | Logout". A left sidebar lists various menu items: "AE Services", "Communication Manager Interface", "Licensing" (expanded), "WebLM Server Address", "WebLM Server Access" (highlighted with a red box), "Reserved Licenses", "Maintenance", "Networking", "Security", "Status", "User Management", "Utilities", and "Help". The main content area is titled "Licensing" and contains instructions for setting up and maintaining the WebLM, listing "WebLM Server Address" and "WebLM Server Access" as required items. A note at the bottom of the main content area states: "NOTE: Please disable your pop-up blocker if you are having difficulty with opening this page".

Provide appropriate login credentials to access the Web License Manager page.



The image shows the login page for the Avaya Web License Manager (WebLM v6.3). At the top left is the Avaya logo in red, followed by the text "Web License Manager (WebLM v6.3)". Below this is a thick red horizontal bar. The main area of the page is white and contains a login form. The form has two labels: "User Name:" and "Password:", each followed by a text input field. To the right of the input fields are two buttons: "Log On" and "Clear". At the bottom of the page, there is a thin gray horizontal bar and a copyright notice: "© 2012 Avaya Inc. All Rights Reserved."

**AVAYA** Web License Manager  
(WebLM v6.3)

User Name:

Password:

© 2012 Avaya Inc. All Rights Reserved.

On the Install License page, select **License Products** → **APPL\_ENAB** → **Application\_Enablement** link from the left pane of the window. Verify that there are sufficient DMCC licenses.

AVAYA

Web License Manager (WebLM v6.3)

[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

WebLM Home

Install license

Licensed products

APPL\_ENAB

Application\_Enablement

View license capacity

View peak usage

Uninstall license

Server properties

Manage users

Shortcuts

Help for Installed Product

Application Enablement (CTI) - Release: 6 - SID: 10503000 (Standard License file)

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

License installed on: June 2, 2011 9:55:08 AM - 06:00

License File Host IDs: 00-16-3E-43-49-72

Licensed Features

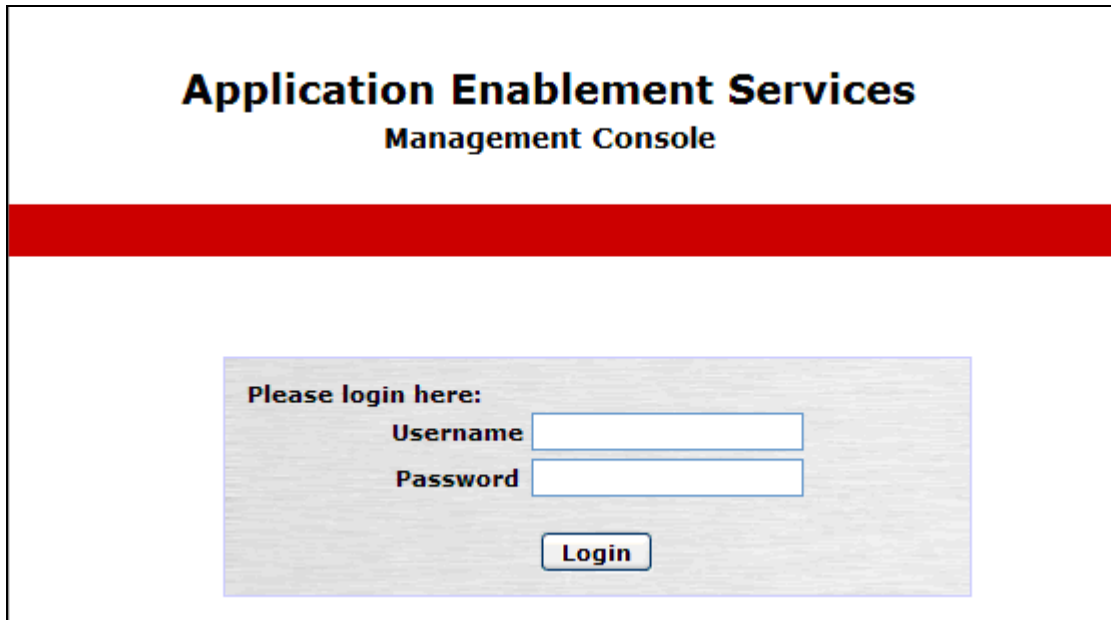
Feature (Keyword)	Expiration date	Licensed	Acquired
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	permanent	16	0
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	permanent	1000	0
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	permanent	3	0
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	permanent	16	0
Product Notes (VALUE_NOTES)	permanent	<div> <div>SmallServerTypes:</div> <div>s8300c;s8300d;ico;premio;bn8400;laptop;CtiSmallServer</div> <div>MediumServerTypes:</div> <div>ibmx306;ibmx306m;dell1950;xen;hs20;hs20_8832_vm;CtiMediumServer</div> <div>LargeServerTypes:</div> <div>isp2100;ibmx305;d380g3;d385g1;d385g2;unknown;CtiLargeServer</div> <div>TrustedApplications:</div> <div>IPS_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, 1XP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, 1XM_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, PC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, CTE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, OSPC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, VP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, SAMETDME_001, VALUE_AES_UNIFIED_CC_DESKTOP, CCE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, CSLT1_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, CSLT2_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AVAYAVERINT_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted;</div> </div>	Not counted
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	permanent	3	0
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	permanent	1000	2
DLG (VALUE_AES_DLG)	permanent	16	1
Device Media and Call Control (VALUE_AES_DMCC_DMC)	permanent	1000	0
AES ADVANCED MEDIUM SWITCH (VALUE_AES_AEC_MEDIUM_ADVANCED)	permanent	3	0

Acquired licenses

Feature	Acquired by	Count
VALUE_AES_TSAPI_USERS	TSAPI (aes)	2
VALUE_AES_DLG	DLG (aes)	1

## 6.2. Configure Switch Connection

Launch a web browser, enter <https://<IP address of the Application Enablement Services server>> in the address field, and log in with the appropriate credentials for accessing the Application Enablement Services Management Console pages.



The screenshot displays the login interface for the Application Enablement Services Management Console. At the top, the title "Application Enablement Services" is centered in a large, bold, black font, with "Management Console" centered below it in a slightly smaller, bold, black font. A thick red horizontal bar separates the header from the main content area. In the center of the page, there is a light gray rectangular box with a thin blue border. Inside this box, the text "Please login here:" is positioned at the top left. Below this text, the labels "Username" and "Password" are aligned to the left of two white input fields. At the bottom center of the gray box is a blue "Login" button with white text.

Click on **Communication Manager Interface → Switch Connections** in the left pane to invoke the Switch Connections page.

**AVAYA** Application Enablement Services Management Console

Welcome: User craft  
 Last login: Sat Sep 28 11:56:39 2013 from 10.64.43.2  
 Number of prior failed login attempts: 2  
 HostName/IP: aes.avaya.com/10.64.43.40  
 Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
 SW Version: 6.3.0.0.212-0  
 Server Date and Time: Mon Sep 30 16:16:22 MDT 2013

Home | Help | Logout

Home

- AE Services
- Communication Manager Interface**
- 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.
- 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.

A Switch Connection defines a connection between the Application Enablement Services server and Communication Manager. Enter a descriptive name for the switch connection and click on **Add Connection**.

**AVAYA** Application Enablement Services Management Console

Welcome: User craft  
 Last login: Sat Sep 28 11:56:39 2013 from 10.64.43.2  
 Number of prior failed login attempts: 2  
 HostName/IP: aes.avaya.com/10.64.43.40  
 Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
 SW Version: 6.3.0.0.212-0  
 Server Date and Time: Mon Sep 30 16:17:53 MDT 2013

Communication Manager Interface | Switch Connections | Home | Help | Logout

- AE Services
- Communication Manager Interface
  - Switch Connections**
  - Dial Plan
- Licensing
- Maintenance
- Networking
- Security
- Status
- User Management
- Utilities
- Help

**Switch Connections**

S8300D

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input type="radio"/> G650	No	30	0

The next window that appears prompts for the Switch Password. Enter the same password that was administered in Communication Manager in **Section 5.1**. Click on **Apply**.

**AVAYA Application Enablement Services Management Console**

Welcome: User craft  
 Last login: Sat Sep 28 11:56:39 2013 from 10.64.43.2  
 Number of prior failed login attempts: 2  
 HostName/IP: aes.avaya.com/10.64.43.40  
 Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
 SW Version: 6.3.0.0.212-0  
 Server Date and Time: Mon Sep 30 16:20:12 MDT 2013

Communication Manager Interface | Switch Connections Home | Help | Logout

**Connection Details - S8300D**

Switch Password: [password field]  
 Confirm Switch Password: [password field]  
 Msg Period: 30 Minutes (1 - 72)  
 SSL: ☒  
 Processor Ethernet: ☒  
 [Apply] [Cancel]

After returning to the Switch Connections page, select the radio button corresponding to the switch connection added previously, and click on the **Edit PE/CLAN IPs** button.

**AVAYA Application Enablement Services Management Console**

Welcome: User craft  
 Last login: Sat Sep 28 11:56:39 2013 from 10.64.43.2  
 Number of prior failed login attempts: 2  
 HostName/IP: aes.avaya.com/10.64.43.40  
 Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
 SW Version: 6.3.0.0.212-0  
 Server Date and Time: Mon Sep 30 16:21:23 MDT 2013

Communication Manager Interface | Switch Connections Home | Help | Logout


**Switch Connections**

[Add Connection]

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input type="radio"/> G650	No	30	0
<input checked="" type="radio"/> S8300D	Yes	30	1

[Edit Connection] [Edit PE/CLAN IPs] [Edit H.323 Gatekeeper] [Delete Connection] [Survivability Hierarchy]

On the **Edit Processor Ethernet IP – S8300D** page, enter the procr IP address which will be used for the DMCC service. Click on **Add/Edit Name or IP**.



**Application Enablement Services**  
Management Console

Welcome: User craft  
Last login: Sat Sep 28 11:56:39 2013 from 10.64.43.2  
Number of prior failed login attempts: 2  
HostName/IP: aes.avaya.com/10.64.43.40  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
SW Version: 6.3.0.0.212-0  
Server Date and Time: Mon Sep 30 16:21:43 MDT 2013


Communication Manager Interface | Switch Connections
Home | Help | Logout

AE Services
Communication Manager Interface
Switch Connections
Dial Plan
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Help

Edit Processor Ethernet IP - S8300D

Name or IP Address	Status
<input type="button" value="Back"/>	

After returning to the Switch Connections page, select the radio button corresponding to the switch connection added previously, and click on the **Edit H.323 Gatekeeper** button for DMCC call control and monitor.



**Application Enablement Services**  
Management Console

Welcome: User craft  
Last login: Sat Sep 28 11:56:39 2013 from 10.64.43.2  
Number of prior failed login attempts: 2  
HostName/IP: aes.avaya.com/10.64.43.40  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
SW Version: 6.3.0.0.212-0  
Server Date and Time: Mon Sep 30 16:22:54 MDT 2013

Communication Manager Interface | Switch Connections
Home | Help | Logout

AE Services
Communication Manager Interface
Switch Connections
Dial Plan
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Help

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input type="radio"/> G650	No	30	0
<input checked="" type="radio"/> S8300D	Yes	30	1

On the **Edit H.323 Gatekeeper – S8300D** page, enter the procr IP address which will be used for the DMCC service. Click on **Add Name or IP**.





## Application Enablement Services Management Console

Welcome: User craft  
Last login: Sat Sep 28 11:56:39 2013 from 10.64.43.2  
Number of prior failed login attempts: 2  
HostName/IP: aes.avaya.com/10.64.43.40  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
SW Version: 6.3.0.0.212-0  
Server Date and Time: Mon Sep 30 16:23:17 MDT 2013

Communication Manager Interface | Switch Connections

[Home](#) | [Help](#) | [Logout](#)

- ▶ AE Services
- ▼ Communication Manager Interface
  - Switch Connections
  - ▶ Dial Plan
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

### Edit H.323 Gatekeeper - S8300D

Name or IP Address

### 6.3. Configure the CTI Users

Navigate to **User Management → User Admin → Add User** link from the left pane of the window. On the Add User page, provide the following information:

- User Id
- Common Name
- Surname
- User Password
- Confirm Password

The above information (User ID and User Password) must match with the information configured in the InGenius Connector Enterprise Configuration Tool page in **Section 7**.

Select **Yes** using the drop down menu on the CT User field. This enables the user as a CTI user. Default values may be used in the remaining fields. Click the **Apply** button (not shown) at the bottom of the screen to complete the process.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title 'Application Enablement Services Management Console', and a welcome message for 'User craft' with login details. A red navigation bar contains links for 'User Management | User Admin | Add User' and 'Home | Help | Logout'. The left sidebar shows a tree view with 'User Management' expanded and 'Add User' selected. The main content area is the 'Add User' form, which includes fields for User Id, Common Name, Surname, User Password, and Confirm Password (all marked with an asterisk). Below these are fields for Admin Note, Avaya Role (set to None), Business Category, Car License, CM Home, and Cms Home. The 'CT User' field is a dropdown menu set to 'Yes'. At the bottom are fields for Department Number, Display Name, and Employee Number.

Welcome: User craft  
Last login: Sat Sep 28 11:56:39 2013 from 10.64.43.2  
Number of prior failed login attempts: 2  
HostName/IP: aes.avaya.com/10.64.43.40  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
SW Version: 6.3.0.0.212-0  
Server Date and Time: Mon Sep 30 16:27:11 MDT 2013

**AVAYA** Application Enablement Services  
Management Console

User Management | User Admin | Add User Home | Help | Logout

AE Services  
Communication Manager Interface  
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 ICE\_CT  
\* Common Name ICE\_CT  
\* Surname ICE\_CT  
\* User Password .....  
\* Confirm Password .....  
Admin Note  
Avaya Role None  
Business Category  
Car License  
CM Home  
Cms Home  
CT User Yes  
Department Number  
Display Name  
Employee Number

Once the user is created, navigate to the **Security** → **Security Database** → **CTI Users** → **List All Users** link from the left pane of the window. Select the User ID created previously, and click the **Edit** button to set the permission of the user.

**AVAYA**

**Application Enablement Services**  
Management Console

Welcome: User craft  
Last login: Sat Sep 28 11:56:39 2013 from 10.64.43.2  
Number of prior failed login attempts: 2  
HostName/IP: aes.avaya.com/10.64.43.40  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
SW Version: 6.3.0.0.212-0  
Server Date and Time: Mon Sep 30 16:28:04 MDT 2013

Security | Security Database | CTI Users | List All Users

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▶ Networking

▼ Security

▶ Account Management

▶ Audit

▶ Certificate Management

Enterprise Directory

▶ Host AA

▶ PAM

▼ Security Database

▪ Control

▣ CTI Users

▪ List All Users

▪ Search Users

CTI Users

User ID	Common Name	Worktop Name	Device ID
ICE_CT	ICE_CT	NONE	NONE

Edit

List All

Provide the user with unrestricted access privileges by checking the **Unrestricted Access** button. Click on the **Apply Changes** button.

**AVAYA** **Application Enablement Services**  
Management Console

Welcome: User craft  
Last login: Sat Sep 28 11:56:39 2013 from 10.64.43.2  
Number of prior failed login attempts: 2  
HostName/IP: aes.avaya.com/10.64.43.40  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
SW Version: 6.3.0.0.212-0  
Server Date and Time: Mon Sep 30 16:28:29 MDT 2013

Security | Security Database | CTI Users | List All Users

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▶ Networking

▼ Security

▶ Account Management

▶ Audit

▶ Certificate Management

Enterprise Directory

▶ Host AA

▶ PAM

▼ Security Database

▪ Control

▣ CTI Users

▪ List All Users

▪ Search Users

Edit CTI User

User Profile:

User IDICE\_CT

Common NameICE\_CT

Worktop NameNONE ▾

Unrestricted Access☒

Call and Device Control:

Call Origination/Termination and Device StatusNone ▾

Call and Device Monitoring:

Device MonitoringNone ▾

Calls On A Device MonitoringNone ▾

Call Monitoring☐

Routing Control:


Allow Routing on Listed DevicesNone ▾

Apply Changes

Cancel Changes

## 6.4. Configure the DMCC Port

Navigate to the **Networking → Ports** link, from the left pane of the window, to set the DMCC server port. During the compliance test, the default port values were utilized. The following screen displays the default port values. Since the unencrypted port was utilized during the compliance test, set the Unencrypted Port field to **Enabled**. Default values may be used in the remaining fields. Click the **Apply Changes** button (not shown) at the bottom of the screen to complete the process.

**Application Enablement Services**  
Management Console

Welcome: User craft  
Last login: Sat Sep 28 11:56:39 2013 from 10.64.43.2  
Number of prior failed login attempts: 2  
HostName/IP: aes.avaya.com/10.64.43.40  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
SW Version: 6.3.0.0.212-0  
Server Date and Time: Mon Sep 30 16:33:45 MDT 2013

Networking | PortsHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▼ Networking

AE Service IP (Local IP)

Network Configure

Ports

TCP Settings

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Ports

CVLAN Ports

Unencrypted TCP Port9999Enabled Disabled

Encrypted TCP Port9998Enabled Disabled

DLG PortTCP Port5678

TSAPI Ports

TSAPI Service Port450Enabled Disabled

Local TLINK Ports

TCP Port Min1024

TCP Port Max1039

Unencrypted TLINK Ports

TCP Port Min1050

TCP Port Max1065

Encrypted TLINK Ports

TCP Port Min1066

TCP Port Max1081

DMCC Server Ports

Unencrypted Port4721Enabled Disabled

Encrypted Port4722Enabled Disabled

TR/87 Port4723Enabled Disabled

## 6.5. Configure Tlinks

Navigate to the **Security** → **Security Database** → **Tlinks** link, from the left pane of the window, to verify the Tlink that will be utilized during the compliance test.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for user "craft" with login details. A red navigation bar contains links for "Security", "Security Database", and "Tlinks", along with "Home", "Help", and "Logout". The left sidebar shows a tree view of the application's structure, with "Tlinks" highlighted under the "Security Database" section. The main content area, titled "Tlinks", shows a "Tlink Name" field with two radio button options: "AVAYA#S8300D#CSTA#AES" (selected) and "AVAYA#S8300D#CSTA-S#AES". A "Delete Tlink" button is also present.

Welcome: User craft  
Last login: Sat Sep 28 11:56:39 2013 from 10.64.43.2  
Number of prior failed login attempts: 2  
HostName/IP: aes.avaya.com/10.64.43.40  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
SW Version: 6.3.0.0.212-0  
Server Date and Time: Mon Sep 30 16:34:30 MDT 2013

Security | Security Database | Tlinks Home | Help | Logout

AE Services  
Communication Manager Interface  
Licensing  
Maintenance  
Networking  
▼ Security  
    Account Management  
    Audit  
    Certificate Management  
    Enterprise Directory  
    Host AA  
    PAM  
    ▼ Security Database  
        Control  
        CTI Users  
        Devices  
        Device Groups  
        Tlinks  
        Tlink Groups  
        Worktops

Tlinks


Tlink Name

☒ AVAYA#S8300D#CSTA#AES  
☐ AVAYA#S8300D#CSTA-S#AES

Delete Tlink

Navigate to **Maintenance** → **Service Controller**, and verify below services are running:

- DMCC Service
- TSAPI

**Application Enablement Services**  
Management Console

Welcome: User craft  
Last login: Sat Sep 28 11:56:39 2013 from 10.64.43.2  
Number of prior failed login attempts: 2  
HostName/IP: aes.avaya.com/10.64.43.40  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_SP  
SW Version: 6.3.0.0.212-0  
Server Date and Time: Mon Sep 30 16:34:59 MDT 2013

Maintenance | Service ControllerHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ Licensing

▼ Maintenance

▶ Date Time/NTP Server

▶ Security Database

▶ Service Controller

▶ Server Data

▶ Networking

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Service Controller

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

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

Start

Stop

Restart Service

Restart AE Server

Restart Linux

Restart Web Server

## 7. Configure InGenius Connector Enterprise

An InGenius Implementation Coordinator walks the end customer (generally the customer's IT Administrator or Avaya Administrator) through the various steps to install, configure, and customize the ICE server software.

InGenius Connector Enterprise integrates Application Enablement Services, to control and monitor the phone states. In these Application Notes, only the interface between InGenius Connector Enterprise and Application Enablement Services will be discussed.

Navigate to **Start → Configuration Tool**, and the InGenius ICE Telephony Server Configuration Toll screen is displayed. Select **Configuration → Telephony**.

The screenshot displays the 'InGenius ICE Telephony Integration Server Configuration Tool [Release: 2.0.242.5316]'. The interface includes a sidebar with tabs: 'General', 'Dialing and Number Formatting', 'Telephony' (highlighted), and 'Integrations'. Under 'Telephony', there are sub-sections: 'Summary' (Dialing and Numbers: Standard), 'PBX / Switch' (AvayaDMCC), 'Extensions' (< None >), 'Directories' (< None >), and 'Integrations' (Salesforce). The main configuration area is titled 'Server' and contains two sections: 'HTTP Service Configuration' and 'Run-Time Administration Access'. In the 'HTTP Service Configuration' section, the 'HTTP Prefix' is set with 'scheme' as 'HTTP', 'host name' as 'localhost', and 'port' as '8888'. The 'Run-Time Administration Access' section shows 'Active Directory Group Name' as 'ICERuntimeAdmins' and an unchecked checkbox for 'Require Role Membership For Local Connections'. At the bottom of the configuration area are buttons for 'Advanced...', 'Reset To Defaults', and 'Undo'. The bottom status bar shows 'There are no unsaved changes.' with 'Cancel' and 'Save' buttons.



In the AvayaDMCC screen, select the **Connection Info** tab. Provide the following information:

- **Address** – Enter the IP address of the Application Enablement Services server.
- **Port** – Enter the DMCC port (4721) configured in **Section 6.4**.
- **Username** – Enter the user name created for InGenius Connector Enterprise in **Section 6.3**.
- **Password** – Enter the password created for InGenius Connector Enterprise in **Section 6.3**.
- **Server name** – Enter the Switch Connection Name configured in **Section 6.2**.

The screenshot displays the 'InGenius ICE Telephony Integration Server Configuration Tool [Release: 2.0.242.5316]' window. The 'Configuration' tab is active, and the 'AvayaDMCC' sub-tab is selected. The 'Connection Info' sub-tab is also selected, showing the 'Application Enablement Services (AES)' configuration. The fields are filled with the following values: Address: 10.64.43.40, Port: 4721, Username: ICE\_CT, Password: (masked), and Connection Manager (CM) Server name: S8300D. The 'Testing' section shows 'Connected' and 'Disconnected' status options, with a 'Test' button. The 'PBX / Switch' section on the left has 'AvayaDMCC' checked. The 'Extensions' section has 'Geolocator' and 'Zone Assignment' unchecked. The 'Advanced...' button is visible at the bottom left. The bottom right shows 'Reset To Defaults' and 'Undo' buttons. A status bar at the very bottom indicates 'There are no unsaved changes.' with 'Cancel' and 'Save' buttons.

InGenius ICE Telephony Integration Server Configuration Tool [Release: 2.0.242.5316]

Configuration | Status

General | Dialing and Number Formatting | Telephony | Integrations

PBX / Switch

- ☒ AvayaDMCC
- ☐ CiscoCTI

AvayaDMCC

Connection Info | Connection Details | Agent Setup

**Application Enablement Services (AES)**

Address: 10.64.43.40

Port: 4721 ☐ Use secure connection

Username: ICE\_CT

Password: \*\*\*\*\*

**Connection Manager (CM)**

Server name: S8300D

**Testing**

Connected

Disconnected

Test

Advanced...

Reset To Defaults Undo

There are no unsaved changes. Cancel Save

## 8. Verification Steps

The following steps may be used to verify the configuration:

- From the InGenius Connector Enterprise server, ping IP interfaces, in particular the Application Enablement Services server, and verify connectivity.
- For the physical IP telephones, verify that the physical telephones are registered by using the **list registered-ip-stations** command on the SAT. For the physical Digital telephones, verify that the telephones are attached to the correct ports.
- Go off-hook and on-hook on the controlled telephones manually and using InGenius Connector Enterprise to verify consistency.
- Place and answer calls from the controlled telephones manually and using InGenius Connector Enterprise to verify consistency.

## 9. Conclusion

These Application Notes described a compliance-tested configuration comprised of Communication Manager, Application Enablement Services, Avaya IP and Digital Telephones, and the InGenius Connector Enterprise application. InGenius Connector Enterprise allows a user to operate a physical telephone and view call and telephone display information through a graphical user interface (GUI). During compliance testing, calls were successfully placed to and from Avaya IP and Digital Telephones that were controlled and monitored by the InGenius Connector Enterprise application.

## 10. Additional References

Product documentation for Avaya products may be found at <http://support.avaya.com>.

[1] *Administering Avaya Aura® Communication Manager*, Document 03-300509, Release 6.3, May 2013, available at <http://support.avaya.com>.

[2] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 6.3, Issue 1, March 2013

Product information for InGenius products may be found at <http://wp.ingeniussoftware.com/ice-for-salesforce/>

---

**©2013 Avaya Inc. All Rights Reserved.**

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

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