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
- 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.

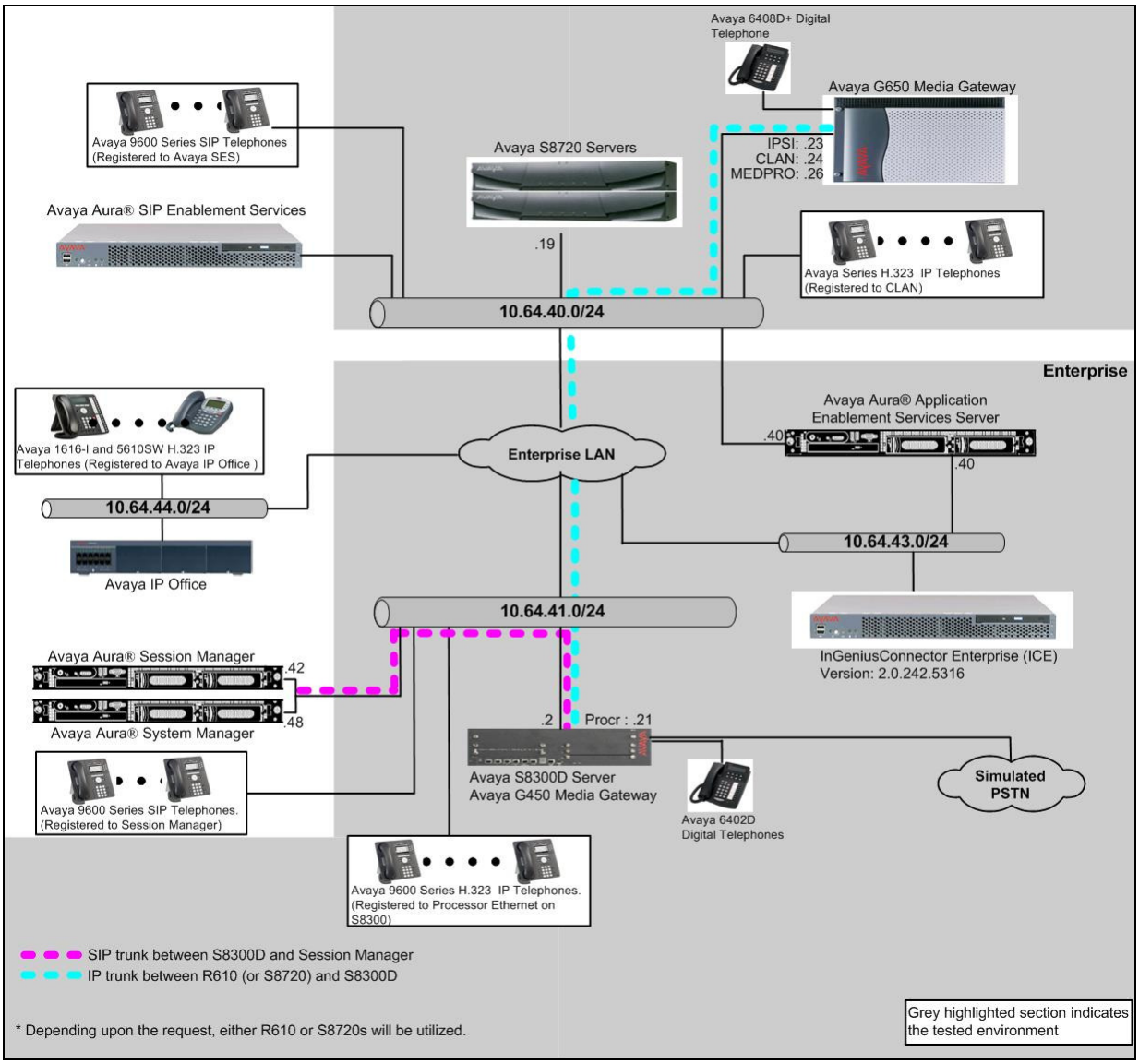


Figure 1: InGenius Connector Enterprise Test Configuration.

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 (*used for inter-switch test scenarios*)		Avaya Aura® Communication Manager 5.2.1 (R015x.02.1.016.4)
Avaya 9600 Series IP Telephones		
	9620 (H.323) 9630 (H.323) 9650 (H.323)	3.1 3.1 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                                            Page   1 of   4

                                   IP SERVICES
 Service      Enabled     Local        Local       Remote      Remote
  Type                    Node         Port        Node        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
                                          Time of Day Lock Table:
              Loss Group: 19         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              Media Complex Ext:
   Survivable Trunk Dest? y                           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

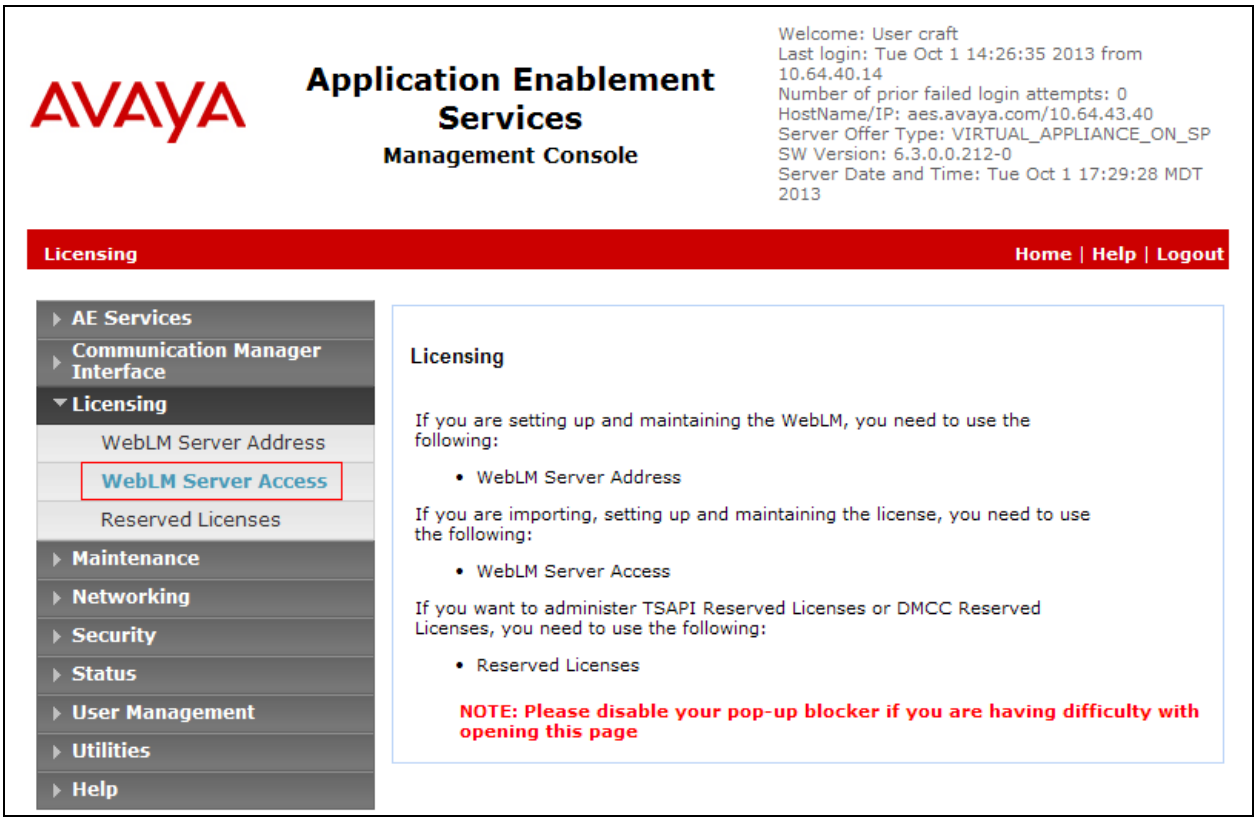
The Application Enablement Services server enables Computer Telephony Interface (CTI) applications to control and monitor telephony resources on Communication Manager.

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.

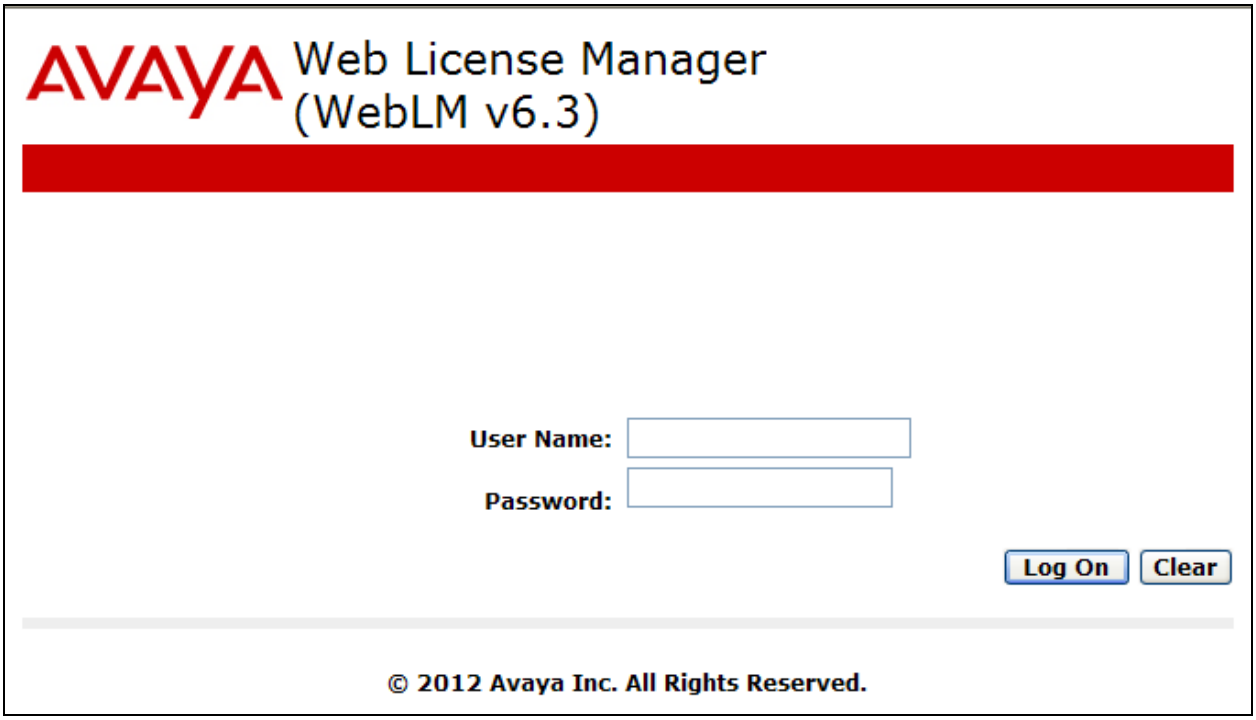
6.1. Device and Media Call Control API Station Licenses

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.



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



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

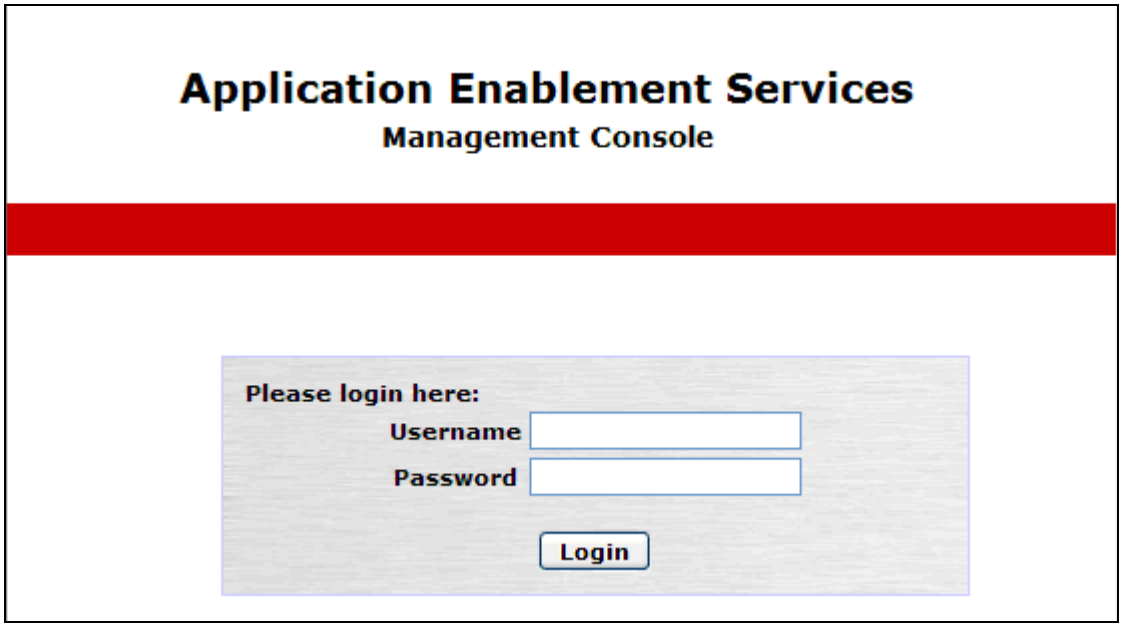
Feature (Keyword)	Expiration date	Licensed	Acquired
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	permanent	16	0
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	permanent	1000	0
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	permanent	3	0
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	permanent	16	0
Product Notes (VALUE_NOTES)	permanent	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiSmallServer MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_8832_vm;CtiMediumServer LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;unknown;CtiLargeServer TrustedApplications: IPS_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XM_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; PC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; OSPC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; VP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AEC_UNIFIED_CC_DESKTOP,,; CCE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T1_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T2_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; AVAYAVERINT_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted;	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

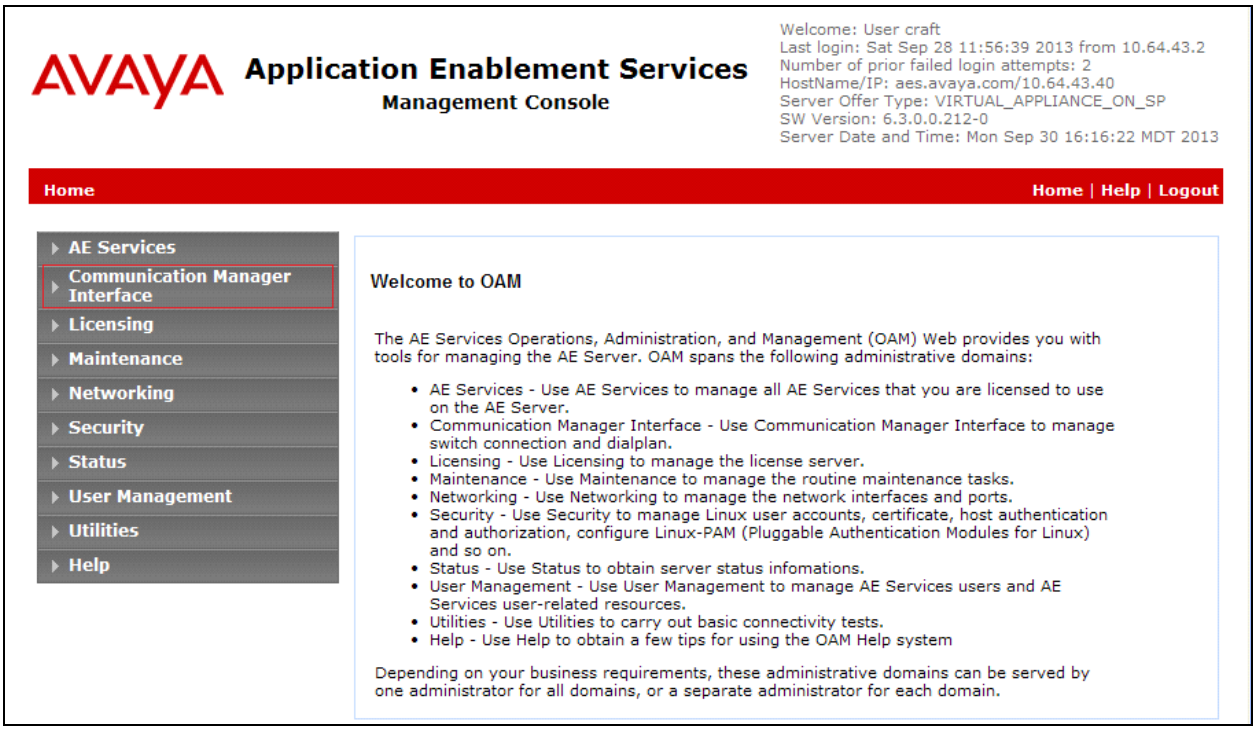
Feature	Acquired by	Count
VALUE_AES_TSAPI_USERS	TSAPI (aes)	2
VALUE_AES_DLG	DLG (aes)	1

6.2. Configure Switch Connection

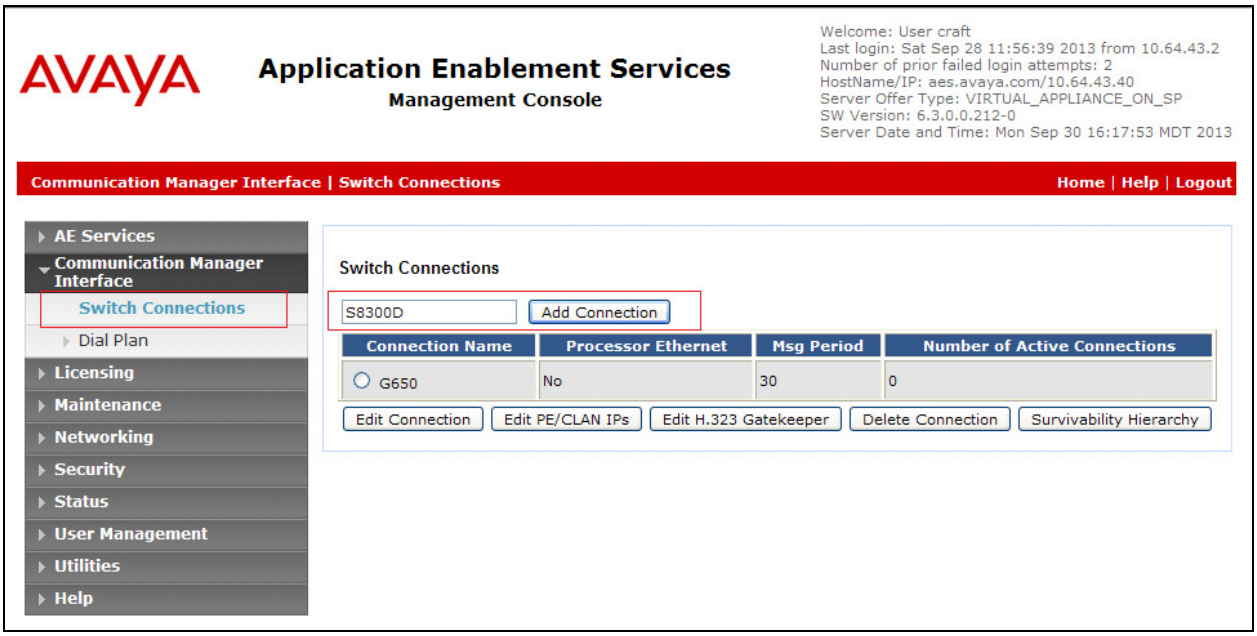
Launch a web browser, enter https://<IP address of the Application Enablement Services server> in the address field, and log in with the appropriate credentials for accessing the Application Enablement Services Management Console pages.



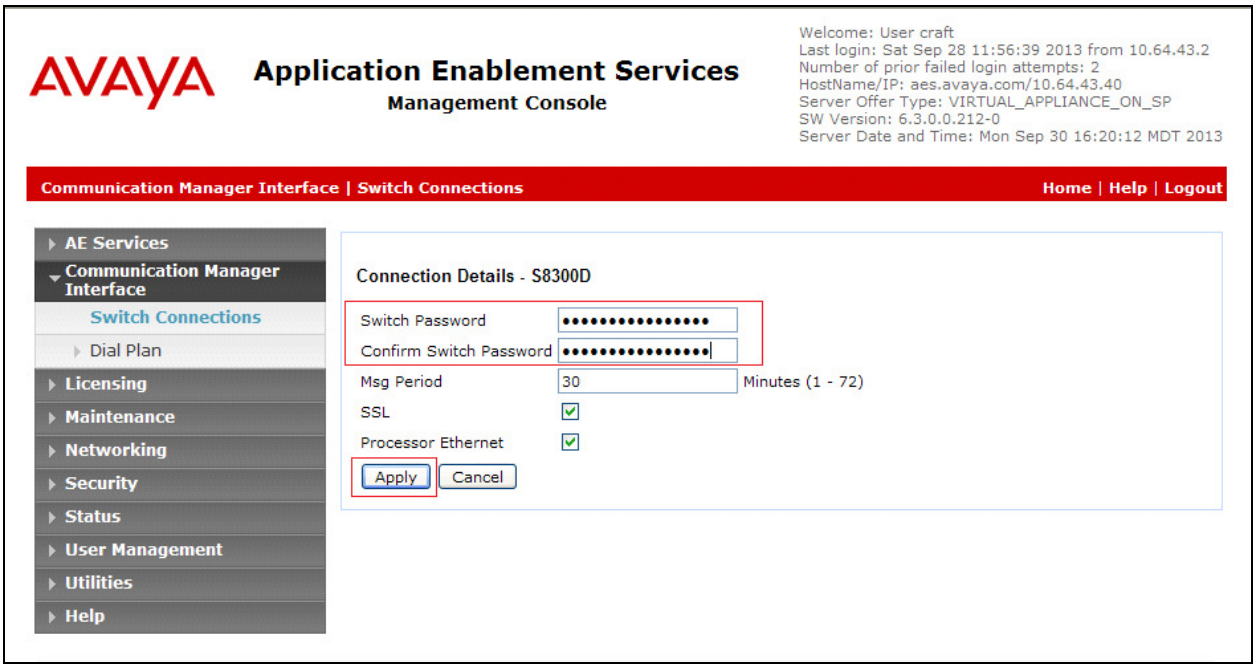
Click on **Communication Manager Interface → Switch Connections** in the left pane to invoke the Switch Connections page.



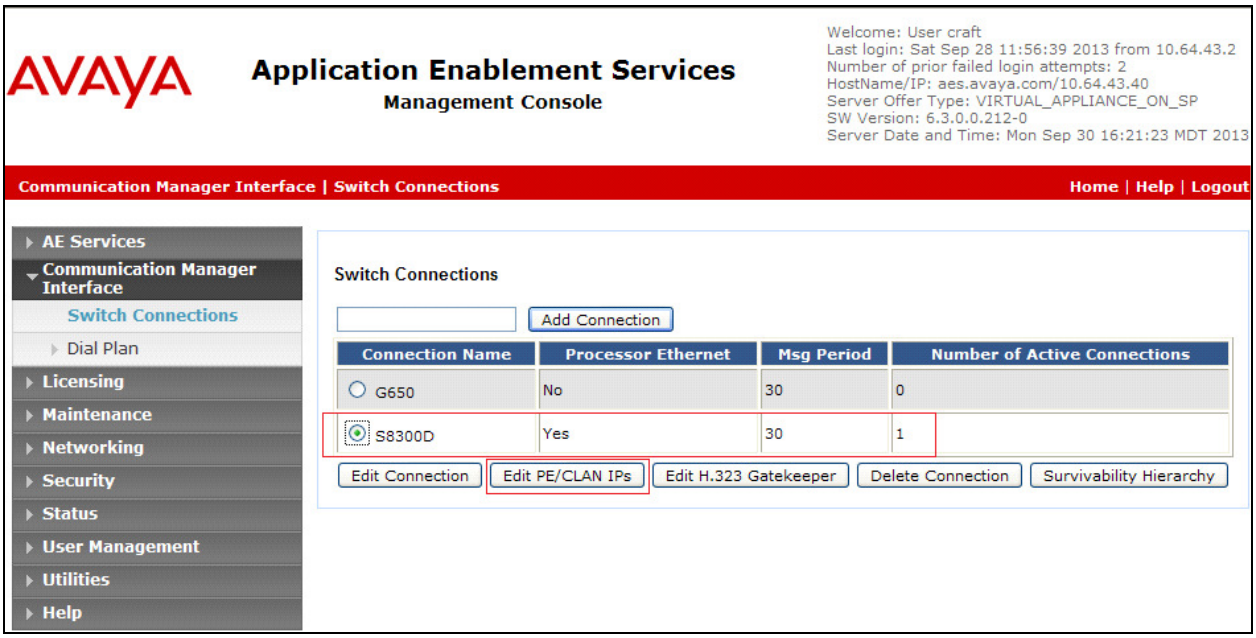
A Switch Connection defines a connection between the Application Enablement Services server and Communication Manager. Enter a descriptive name for the switch connection and click on **Add Connection**.



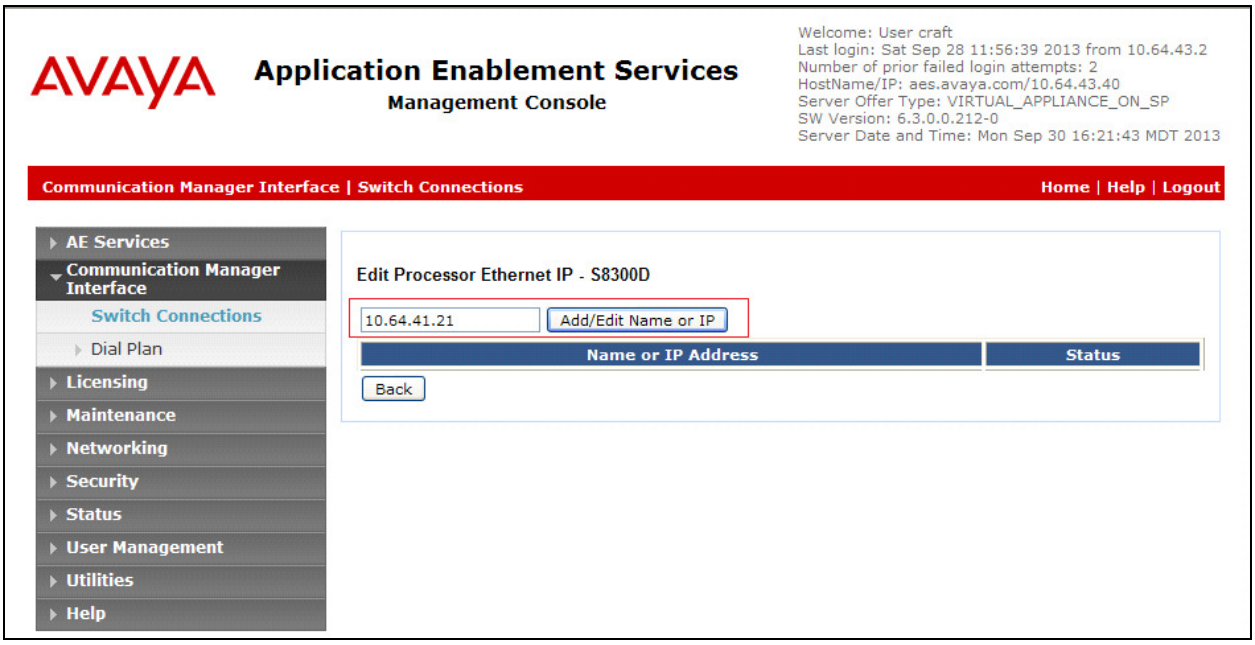
The next window that appears prompts for the Switch Password. Enter the same password that was administered in Communication Manager in **Section 5.1**. Click on **Apply**.



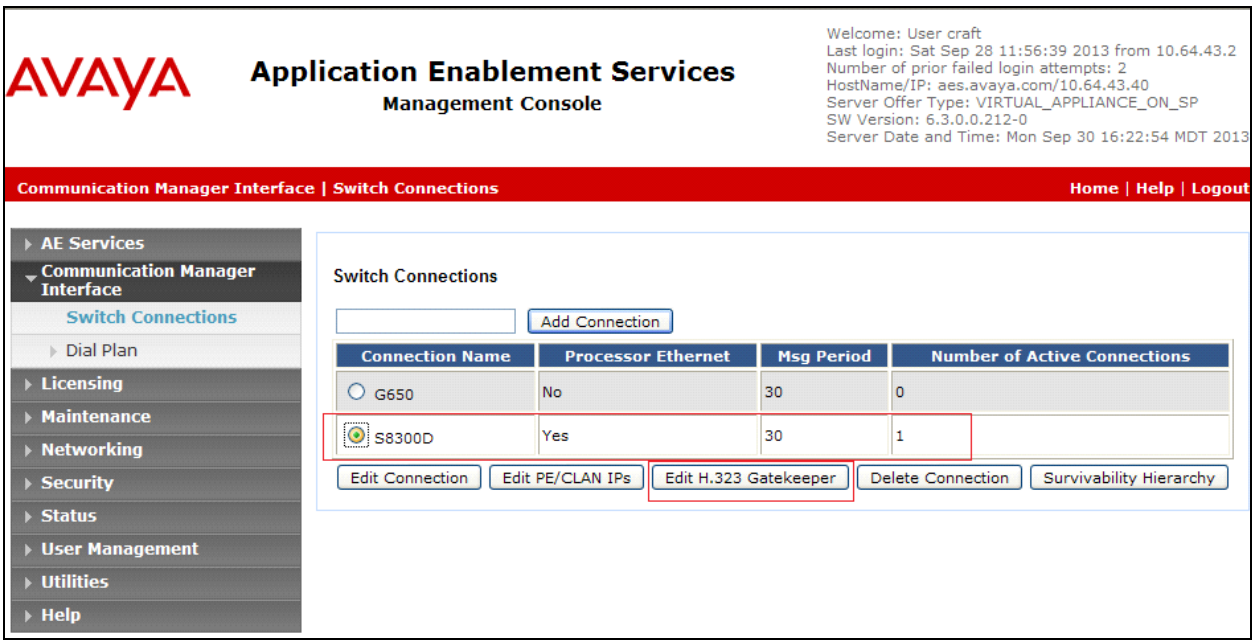
After returning to the Switch Connections page, select the radio button corresponding to the switch connection added previously, and click on the **Edit PE/CLAN IPs** button.



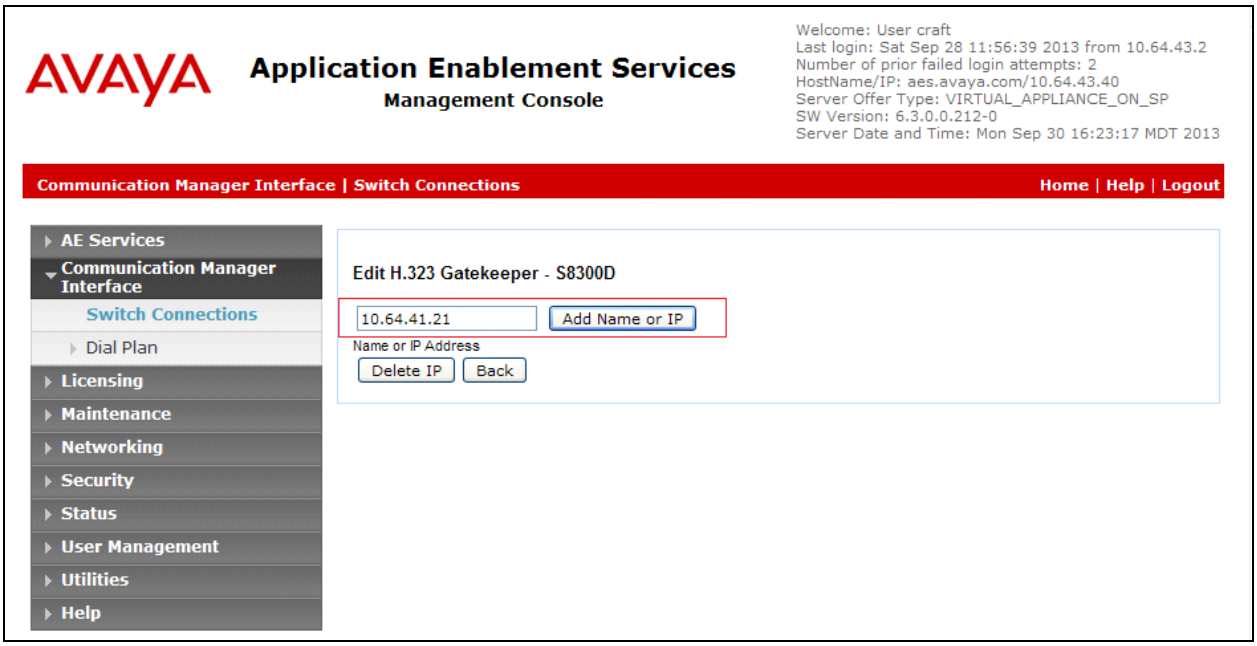
On the **Edit Processor Ethernet IP – S8300D** page, enter the procr IP address which will be used for the DMCC service. Click on **Add/Edit Name or IP**.



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.



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**.



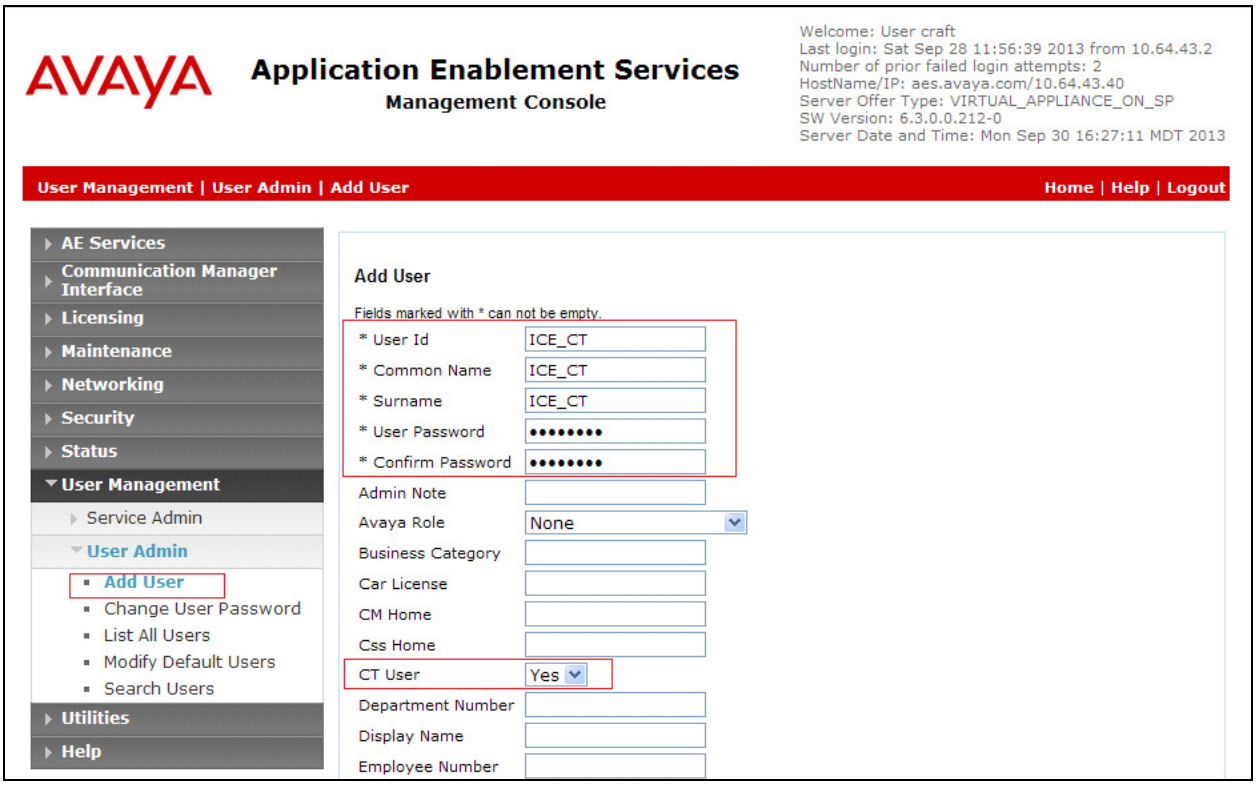
6.3. Configure the CTI Users

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:

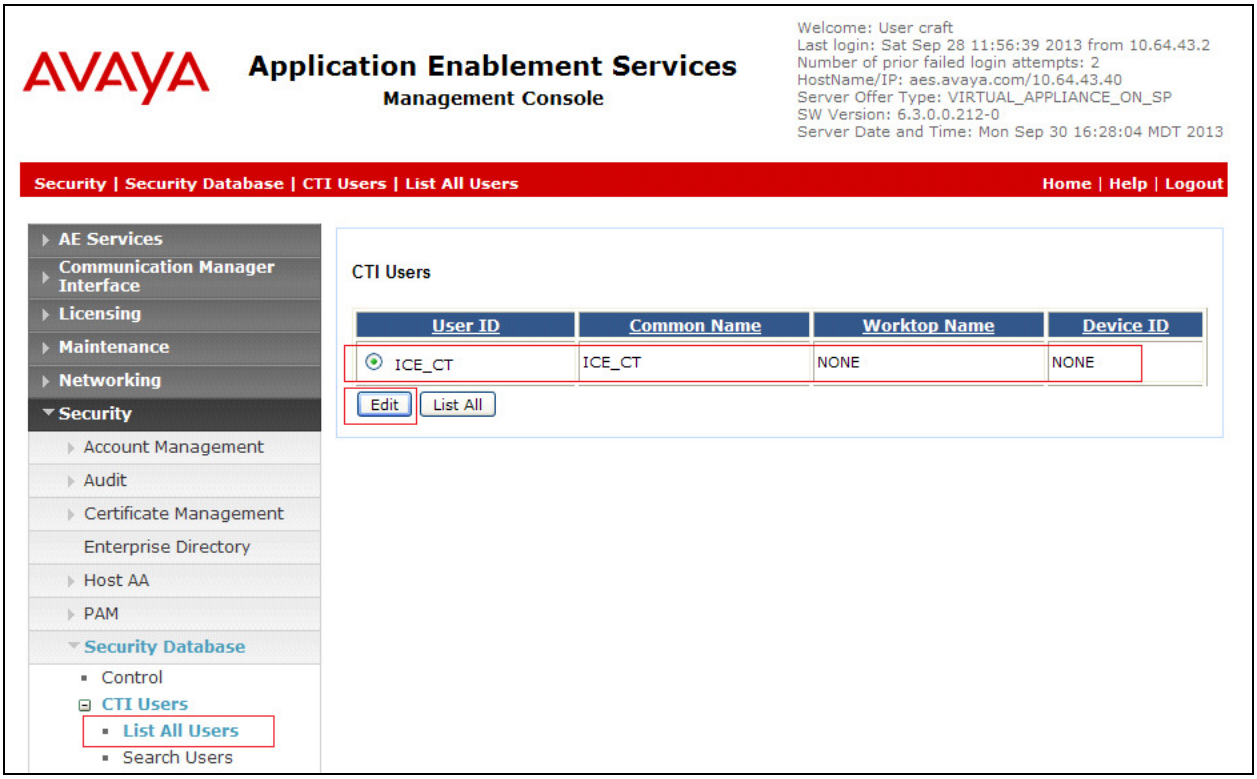
- User Id
- Common Name
- Surname
- User Password
- Confirm Password

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**.

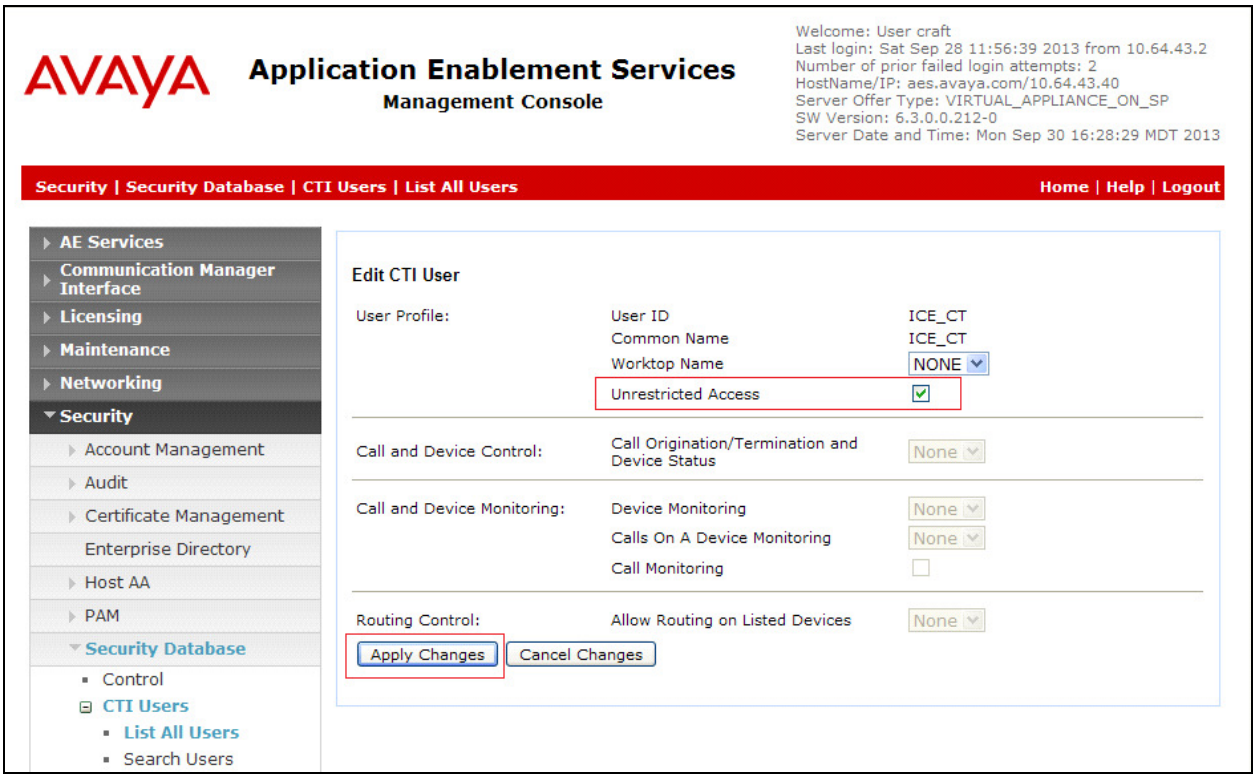
Select **Yes** using the drop down menu on the CT User field. This enables the user as a CTI user. Default values may be used in the remaining fields. Click the **Apply** button (not shown) at the bottom of the screen to complete the process.



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.

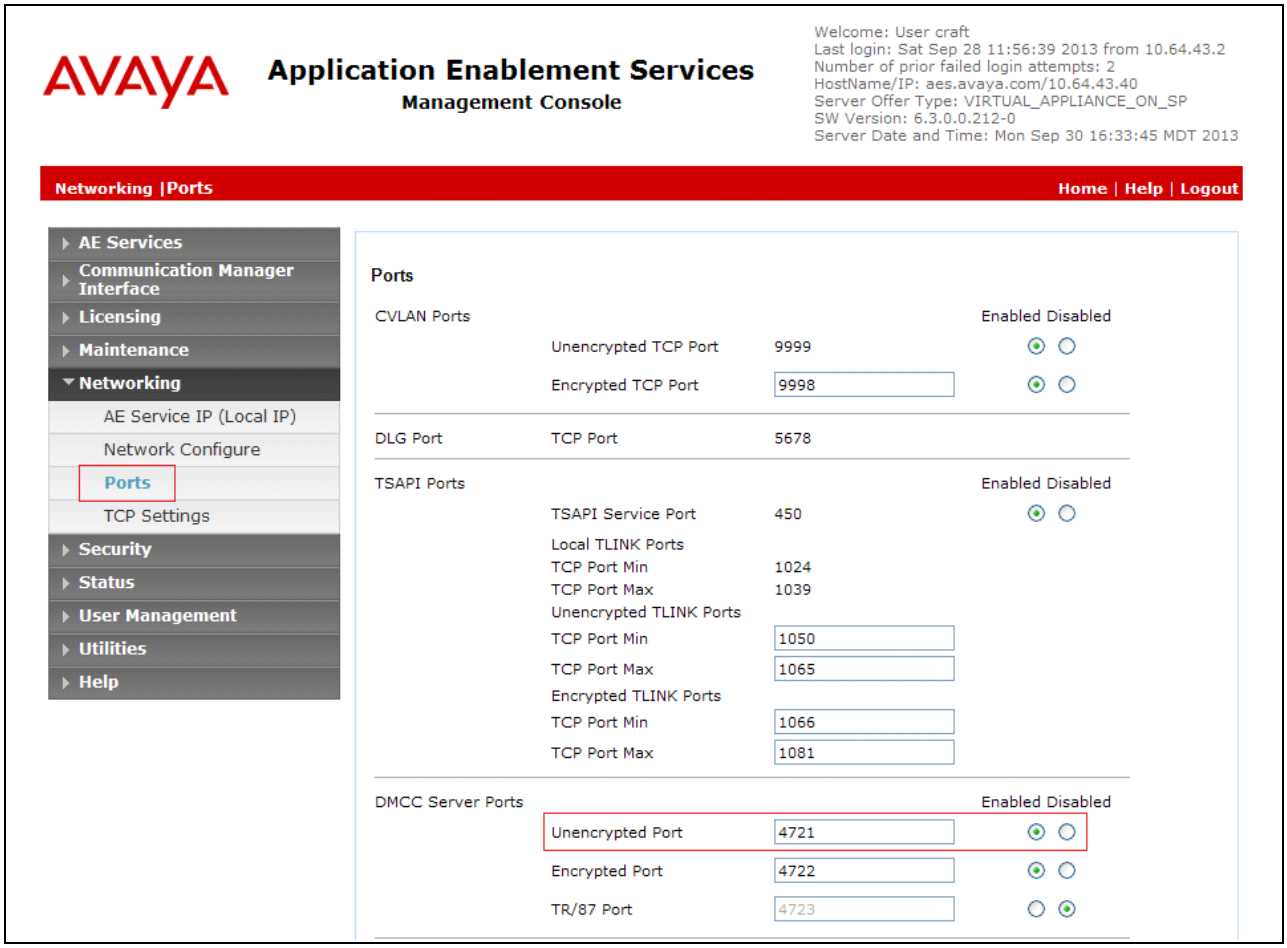


Provide the user with unrestricted access privileges by checking the **Unrestricted Access** button. Click on the **Apply Changes** button.



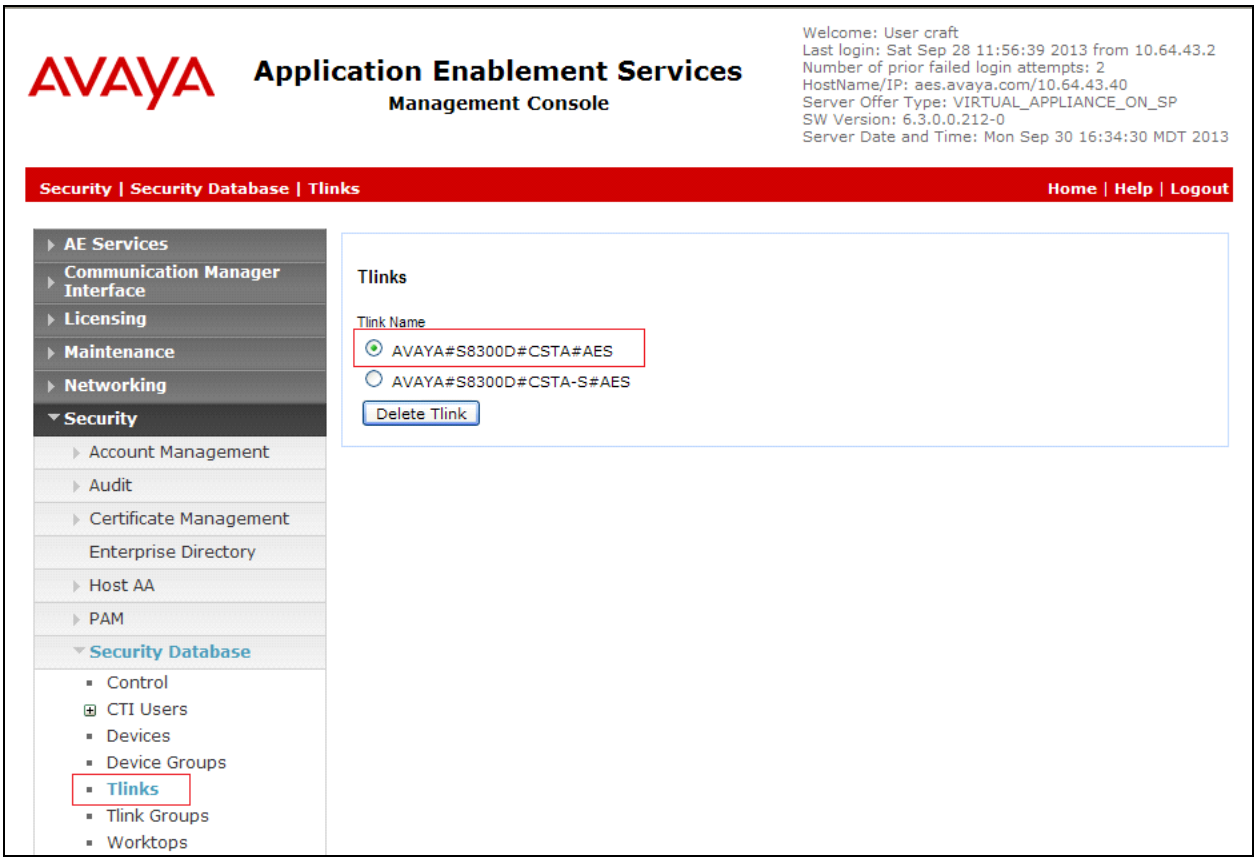
6.4. Configure the DMCC Port

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.



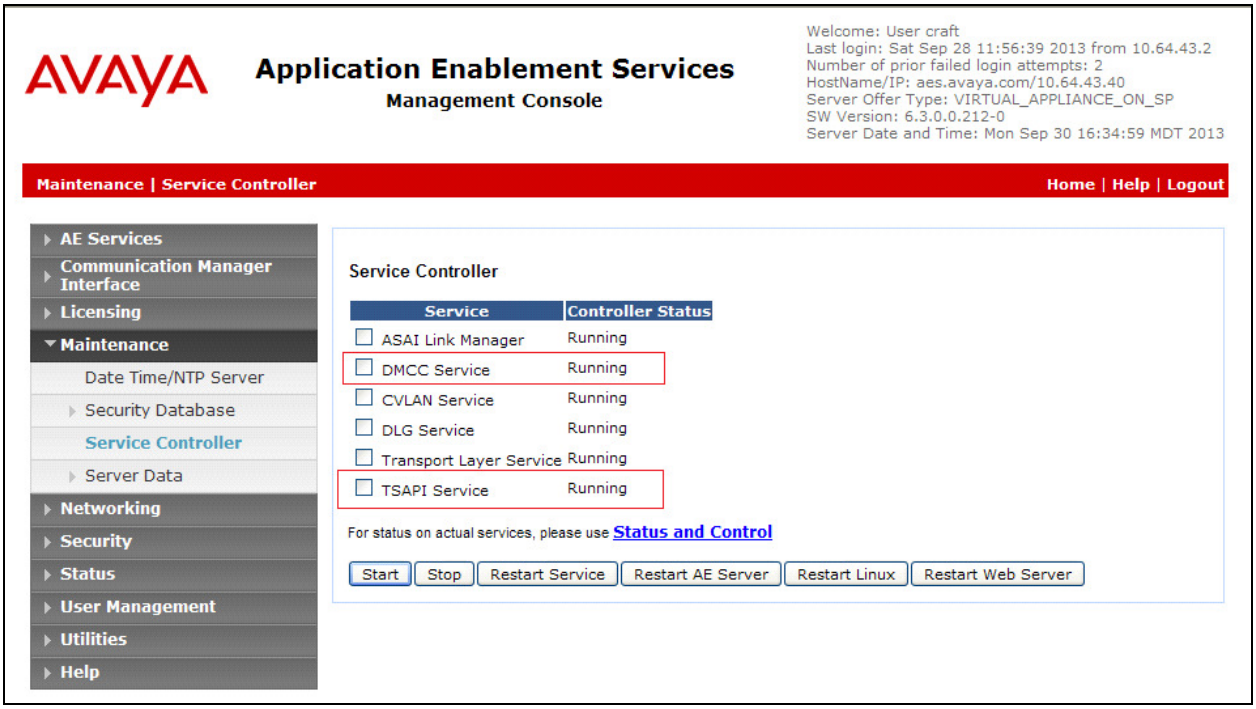
6.5. Configure Tlinks

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.



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

- DMCC Service
- TSAPI

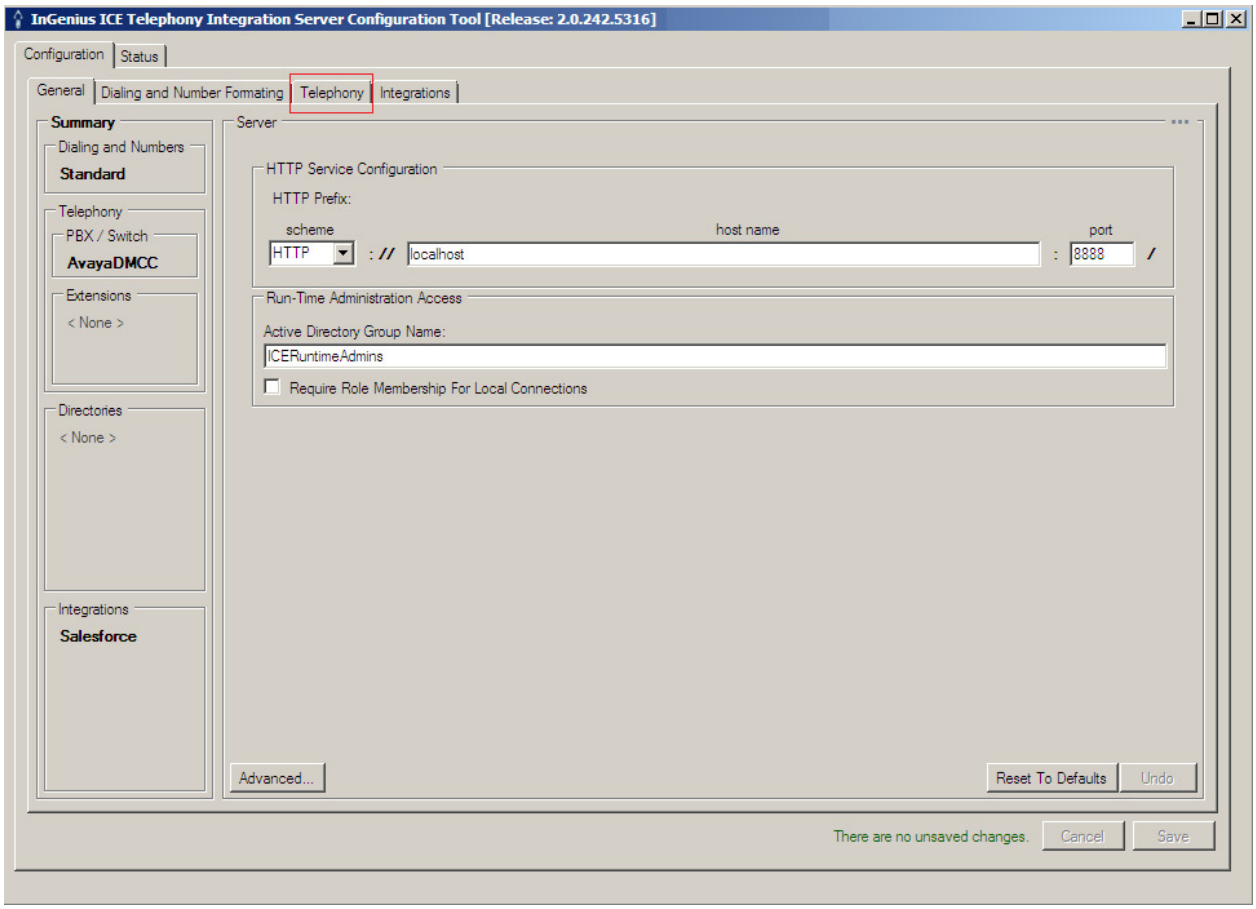


7. Configure InGenius Connector Enterprise

An InGenius Implemenation 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.

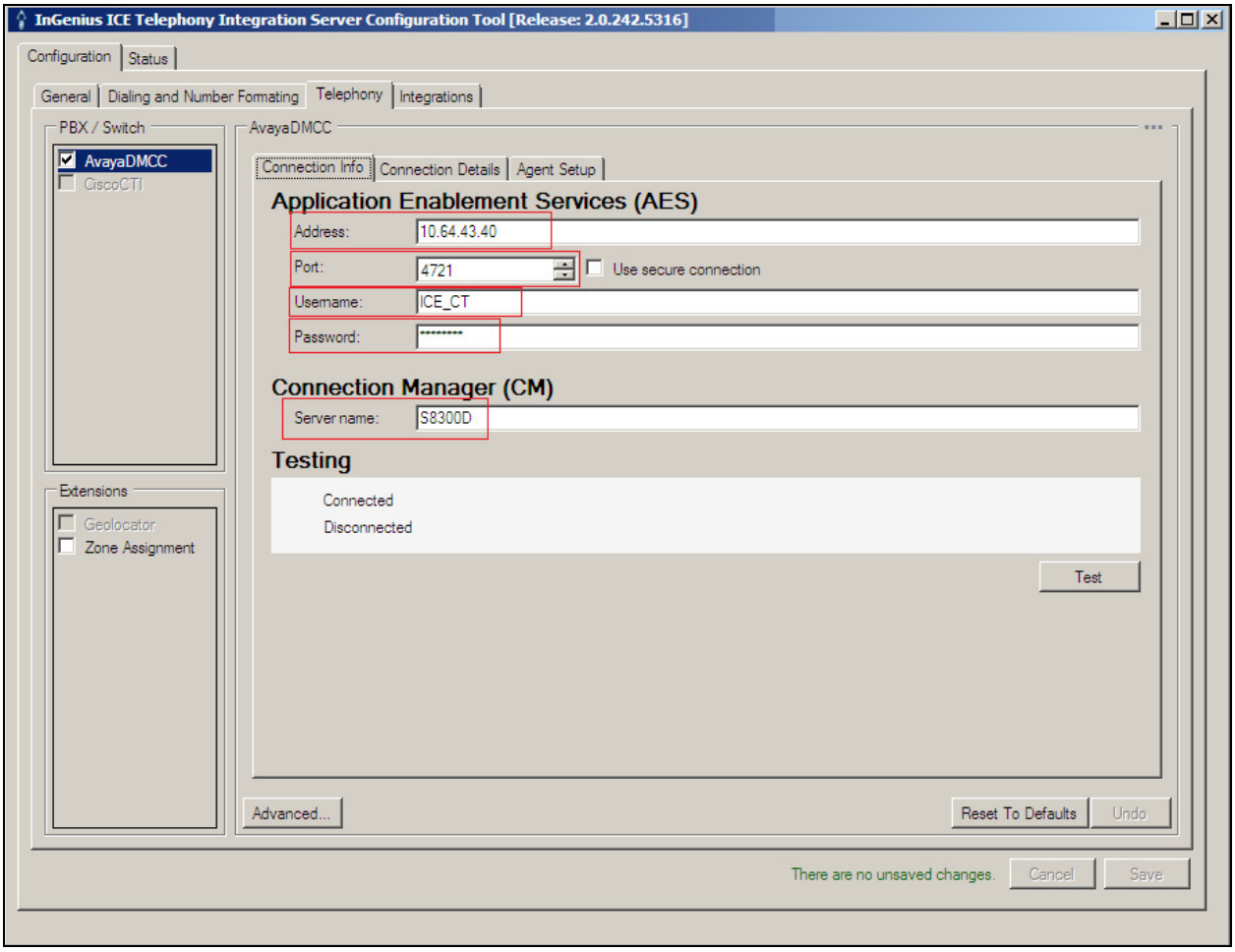
InGenius Connector Enterprise integrates Application Enablement Services, to control and monitor the phone states. In these Application Notes, only the interface between InGenius Connector Enterprise and Application Enablement Services will be discussed.

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



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**.



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/

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.