Avaya Solution & Interoperability Test Lab

Application Notes for Novo Technologies NovoLog with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using Multi Registration for Recordings – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Novo NovoLog to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using Multi Registration for Recordings.

The NovoLog is a software-only solution for voice call recording that offers various recording, playback and archiving features and options. During the compliance test, the Multi Registration recording method was utilized.

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.

©2012 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe the configuration steps required for Novo Technologies NovoLog to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using Multi Registration for Recordings.

Novo Technologies NovoLog allows organizations to record and to manage their call recordings in a secure manner. From this suite of applications, the NovoLog IP Recorder is the component responsible for recording calls on VoIP call processing system.

For its integration with Communication Manager, the NovoLog IP Recorder makes use of the DMCC API to register, through Application Enablement Services, with a set of phone extensions to be recorded. Once the registration process has been completed, the NovoLog IP Recorder is notified of any phone activity on those registered extensions which triggers the recording. Since NovoLog uses DMCC Call Control method, the Telephony Services API (TSAPI) of Application Enablement Services is utilized to receive call related events. After a call is terminated, the voice files created during this specific call are encoded (they can also be encrypted if required), the related information is saved into the database and the call is now ready for playback.

For playback purposes, it is possible to retrieve and review call information at any time or from any location. It not only allows its user to search and filter the recordings using many criteria, but it also allows the easy creation of custom playlists and the export of recording files.

2. General Test Approach and Test Results

All test cases were performed manually. The general approach was to place various types of calls to and from stations, and agents. These trunk calls were then monitored and recorded using the NovoLog IP Recorder. The recordings were verified for each call. For feature testing, the types of calls included inbound and outbound trunk calls, transferred calls, bridged calls, and conferenced calls. For serviceability testing, failures such as cable pulls, busyouts/releases of the trunk group, and resets were applied.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. The feature testing evaluated the ability of the NovoLog to monitor and record calls placed to and from stations and agents. The serviceability testing introduced failure scenarios to see if the NovoLog could resume recording after failure recovery.

2.2. Test Results

The test objectives were verified. For serviceability testing, the NovoLog operated properly after recovering from failures such as cable disconnects, and resets of the NovoLog, Application Enablement Services and Communication Manager.

©2012 Avaya Inc. All Rights Reserved.

2.3. Support

Technical support on the NovoLog can be obtained through the following:

- **Phone:** (888) 657- 6686
- **Web:** support@novo.ca

3. Reference Configuration

Figure 1 illustrates the configuration used in these Application Notes.

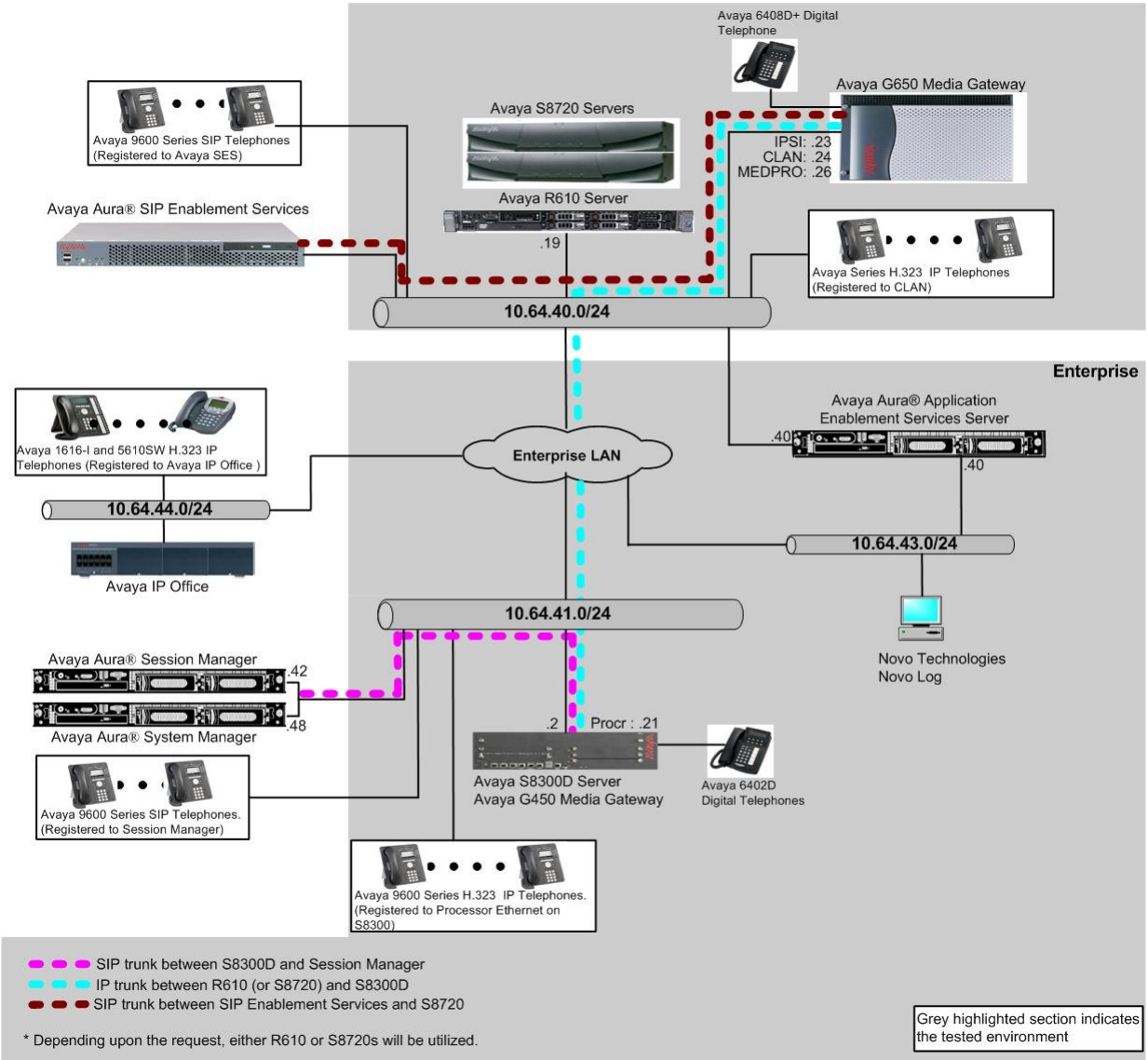


Figure 1: Novo Technologies NovoLog with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services

©2012 Avaya Inc. All Rights Reserved.

4. Equipment and Software Validated

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

Equipment		Software/Firmware
Avaya S8300D Server with Avaya G450 Media Gateway		Avaya Aura® Communication Manager 6.0.1(R016x.00.1.510.1) w/ patch 00.1.510.1-19303
Avaya Aura® Application Enablement Services Server		6.1 (R6-1-0-20-0)
Avaya S8720 Servers with Avaya G650 Media Gateway		Avaya Aura® Communication Manager 5.2.1 (R015x.02.1.016.4)
Avaya 9600 Series IP Telephones		
	9620 (H.323) 9630 (H.323) 9621G (H.323)	3.1 3.1 6.02
Avaya 9600 Series SIP Telephones ***Note: not used as recording stations***		
	9630 (SIP) 9640 (SIP) 9650 (SIP)	2.6.4 2.6.4 2.6.4
Avaya 6400 Series Digital Telephones		N/A
Avaya ERS 5520-48T-PWR switch		6.2
Extreme Networks Summit 48		4.1.21
Novo Technologies NovoLog		6.2

©2012 Avaya Inc. All Rights Reserved.

5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring hunt/skill group, vectors, Vector Directory Numbers (VDN), agents, agent login/logout feature access codes, recorded stations, IP codec, IP network regions, and Computer Telephony Interface (CTI) link in Communication Manager to integrate with the NovoLog. All the configuration changes in Communication Manager are performed through the System Access Terminal (SAT) interface. The highlights in the following screens indicate the values used during the compliance test.

For the compliance testing, the following contact center devices were used.

Device Type	Device Number/Extension
VDN	72074
Vector	74
Skill group	74
Logical agent IDs	72091, 72092, 72093, 72094, 72095
Recorded stations (IP Telephones)	IP Telephones: 72001, 72002, 72003 DCP Telephone: 72008 IP Agents: 72007

5.1. Hunt/Skill Groups, Agent Logins, and Call Vectoring

Enter the **display system-parameters customer-options** command. On **Page 6**, verify that the ACD and Vectoring (Basic) fields are set to **y**. If not, contact an authorized Avaya account representative to obtain these licenses.

```
display system-parameters customer-options                          Page   6 of  11
                          CALL CENTER OPTIONAL FEATURES

                           Call Center Release: 6.0

                                 ACD? y                          Reason Codes? y
                       BCMS (Basic)? y                Service Level Maximizer? n
          BCMS/VuStats Service Level? y              Service Observing (Basic)? y
  BSR Local Treatment for IP & ISDN? y     Service Observing (Remote/By FAC)? y
                  Business Advocate? n               Service Observing (VDNs)? y
                    Call Work Codes? y                               Timed ACW? y
      DTMF Feedback Signals For VRU? y                      Vectoring (Basic)? y
                   Dynamic Advocate? n                 Vectoring (Prompting)? y
       Expert Agent Selection (EAS)? y              Vectoring (G3V4 Enhanced)? y
                            EAS-PHD? y               Vectoring (3.0 Enhanced)? y
                  Forced ACD Calls? n     Vectoring (ANI/II-Digits Routing)? y
               Least Occupied Agent? y     Vectoring (G3V4 Advanced Routing)? y
          Lookahead Interflow (LAI)? y                     Vectoring (CINFO)? y
Multiple Call Handling (On Request)? y      Vectoring (Best Service Routing)? y
    Multiple Call Handling (Forced)? y                  Vectoring (Holidays)? y
  PASTE (Display PBX Data on Phone)? y                 Vectoring (Variables)? y
        (NOTE: You must logoff & login to effect the permission changes.)
```


©2012 Avaya Inc. All Rights Reserved.

Enter the **add hunt-group n** command, where **n** is an unused hunt group number. On **Page 1** of the hunt-group form, assign a descriptive **Group Name** and **Group Extension** valid in the provisioned dial plan. Set the **ACD**, **Queue**, and **Vector** fields to **y**. When ACD is enabled, hunt group members serve as ACD agents and must log in to receive ACD split/skill calls. When Queue is enabled, calls to the hunt group will be served by a queue. When Vector is enabled, the hunt group will be vector controlled.

```
add hunt-group 74                                                Page   1 of   4
                                   HUNT GROUP

            Group Number: 74                                  ACD? y
              Group Name: hunt-4-Novo                       Queue? y
         Group Extension: 72084                            Vector? y
              Group Type: ucd-mia
                      TN: 1
                     COR: 1                       MM Early Answer? n
           Security Code:                  Local Agent Preference? n
 ISDN/SIP Caller Display:

             Queue Limit: unlimited
 Calls Warning Threshold:      Port:
  Time Warning Threshold:      Port:
```

On **Page 2**, set the **Skill** field to **y**, which means that agent membership in the hunt group is based on skills, rather than pre-programmed assignment to the hunt group.

```
add hunt-group 74                                                Page   2 of   4
                                   HUNT GROUP

                     Skill? y      Expected Call Handling Time (sec): 180
                       AAS? n
                  Measured: none
     Supervisor Extension:


      Controlling Adjunct: none




   Multiple Call Handling: none


 Timed ACW Interval (sec):          After Xfer or Held Call Drops? n
```


©2012 Avaya Inc. All Rights Reserved.

Enter the **add agent-loginID p** command, where **p** is a valid extension in the provisioned dial plan. On **Page 1** of the agent-loginID form, enter a descriptive **Name** and **Password**.

```
add agent-loginID 72091                                          Page   1 of   2
                                  AGENT LOGINID

                Login ID: 72091                                    AAS? n
                    Name: Agent-1                                AUDIX? n
                      TN: 1                              LWC Reception: spe
                     COR: 1                     LWC Log External Calls? n
           Coverage Path:                     AUDIX Name for Messaging:
           Security Code:
                                        LoginID for ISDN/SIP Display? n
                                                            Password:
                                                  Password (enter again):
                                                        Auto Answer: station
                                                 MIA Across Skills: system
                                            ACW Agent Considered Idle: system
                                            Aux Work Reason Code Type: system
                                              Logout Reason Code Type: system
                       Maximum time agent in ACW before logout (sec): system
                                             Forced Agent Logout Time:   :

     WARNING:  Agent must log in again before changes take effect
```

On **Page 2**, set the **Skill Number** (SN) to the hunt group number previously created in this section. The **Skill Level** (SL) may be set according to customer requirements.

Repeat this step as necessary to configure additional agent extensions.

```
add agent-loginID 72091                                          Page   2 of   2
                                  AGENT LOGINID
      Direct Agent Skill:                                Service Objective? n
Call Handling Preference: skill-level                Local Call Preference? n

    SN   RL SL          SN   RL SL
 1: 74      1        16:
 2:                  17:
 3:                  18:
 4:                  19:
```

Enter the **change vector q** command, where **q** is an unused vector number. Enter a descriptive Name, and program the vector to deliver calls to the hunt/skill group number. Agents that are logged into the hunt/skill group will be able to answer calls queued to the hunt/skill group.

```
change vector 74                                                 Page   1 of   6
                                   CALL VECTOR

    Number: 74                Name: Vector-Novo
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n           Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 wait-time    2   secs hearing ringback
02 queue-to     skill 74   pri m
03
```


©2012 Avaya Inc. All Rights Reserved.

Enter the **add vdn r** command, where **r** is an extension valid in the provisioned dial plan. Specify a descriptive Name for the VDN and specify the vector configured in the previous step as the Vector Number. In the example below, incoming calls to extension 72074 will be routed to VDN 72074, which in turn will invoke the actions specified in vector 74.

```
add vdn 72074                                                    Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 72074
                                 Name*: VDN-Novo
                           Destination: Vector Number        74
                   Attendant Vectoring? n
                  Meet-me Conferencing? n
                    Allow VDN Override? n
                                   COR: 1
                                   TN*: 1
                              Measured: none

        VDN of Origin Annc. Extension*:
                            1st Skill*:
                            2nd Skill*:
                            3rd Skill*:
```

Enter the **change feature-access-codes** command. Define the **Auto-In Access Code**, **Login Access Code**, **Logout Access Code**, and **Aux Work Access Code**.

```
change feature-access-codes                                      Page   5 of  10
                                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:
```


©2012 Avaya Inc. All Rights Reserved.

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**, created previously, for ACD Login and Logout.

```
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
     01: 124
     02: 125
     03:
     04:
     05:
```

5.2. Recorded Stations

The stations that were recorded during the compliance testing include an Avaya Digital Telephone, Avaya IP Telephones (Avaya 9600 and 96x1 Series), and an Avaya one-X Agent. The extensions used were in the ranges 72001-72009.

Enter the **add station s** command, where **s** is an extension valid in the provisioned dial plan. On **Page 1** of the STATION form, set the **Type** field to an IP telephone set type and enter a descriptive name, specify the **Security Code**, and set the **IP SoftPhone** field to **y**.

Repeat this step as necessary, with the same Security Code, to configure additional recorded stations.

```
add station 72001                                                  Page   1 of   5
                                     STATION

Extension: 72001                        Lock Messages? n               BCC: 0
     Type: 9620                         Security Code: *                TN: 1
     Port: S00002                     Coverage Path 1:                 COR: 1
     Name: S8300-IP-1                 Coverage Path 2:                 COS: 1
                                      Hunt-to Station:
STATION OPTIONS
               Location:                  Time of Day Lock Table:
              Loss Group: 19         Personalized Ringing Pattern: 1
                                                Message Lamp Ext: 72001
            Speakerphone: 2-way               Mute Button Enabled? y
        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
```


©2012 Avaya Inc. All Rights Reserved.

5.3. Audio Codec Configuration

Enter the **change ip-codec-set t** command, where **t** is a number between 1 and 7, inclusive.

Note: Novo Technologies NovoLog supports G.711MU and G.711A. During the compliance test, G.711MU was utilized. The codec has to match between Communication Manager and Novo NovoLog (recording codec).

```
change ip-codec-set 1                                          Page   1 of   2

                           IP Codec Set

    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU           n          2        20
 2:
```

5.4. IP Network Regions

During compliance testing, a C-LAN board dedicated for H.323 endpoint registration was assigned to IP network region 1. Set the **Codec Set** field to **1**. The Avaya IP Telephones and Avaya IP Agent, as well as Avaya AES DMCC stations used by the NovoLog, registered with the C-LAN board (CLAN) and were thus also assigned to IP network region 1. One consequence of assigning the aforementioned Avaya IP Telephones, Avaya IP Agent, Avaya AES DMCC stations, and MedPro boards to a common IP network region is that the RTP traffic between them is governed by the same codec set.

```
change ip-network-region 1                                     Page   1 of  20
                              IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain: avaya.com
    Name:
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                     IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                     RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```


©2012 Avaya Inc. All Rights Reserved.

5.5. Configure TSAPI CTI Link

Enter the **add cti-link m** command, where **m** is a number between 1 and 64, inclusive. Enter a valid Extension under the provisioned dial plan. Set the **Type** field to **ADJ-IP** and assign a descriptive Name to the CTI link. Default values may be used in the remaining fields.

```
add cti-link 4                                                  Page   1 of   3
                                 CTI LINK
 CTI Link: 4
Extension: 72000
     Type: ADJ-IP
                                                                   COR: 1
     Name: TSAPI
```

Enter the **change node-names ip** command. In the compliance-tested configuration, the procr IP address was utilized for registering H.323 endpoints (Avaya IP Telephones, Avaya IP Agents, and Avaya AES DMCC stations) and also was used for connectivity to the Application Enablement Services server.

```
change node-names ip                                            Page   1 of   2
                                IP NODE NAMES
    Name              IP Address
CLAN                10.64.40.24
IPOffice            10.64.44.21
SES                 10.64.40.41
SM-1                10.64.40.42
SM-2                10.64.21.31
aes                 10.64.43.40
default             0.0.0.0
msgserver-ip        10.64.41.21
pcr                 204.27.235.31
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 **procr** that was configured previously in the node-name ip form. During the compliance test, the default port was utilized 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       pcr             5852
CDR2                   procr           0       rdtt-1          9004
```


©2012 Avaya Inc. All Rights Reserved.

On **Page 4**, enter the hostname of the AES server for the AE Services Server field. The server name may be obtained by logging in to the AES server using ssh, and run **uname –a**. Enter an alphanumeric password for the Password field. Set the Enabled field to **y**. The same password will be configured on the AES server in **Section 6.1**.

```
change ip-services                                              Page   4 of   4
                            AE Services Administration

   Server ID    AE Services       Password          Enabled    Status
                   Server
      1:       aes                [redacted]          y        idle
      2:
      3:
      4:
      5:
      6:
```


©2012 Avaya Inc. All Rights Reserved.

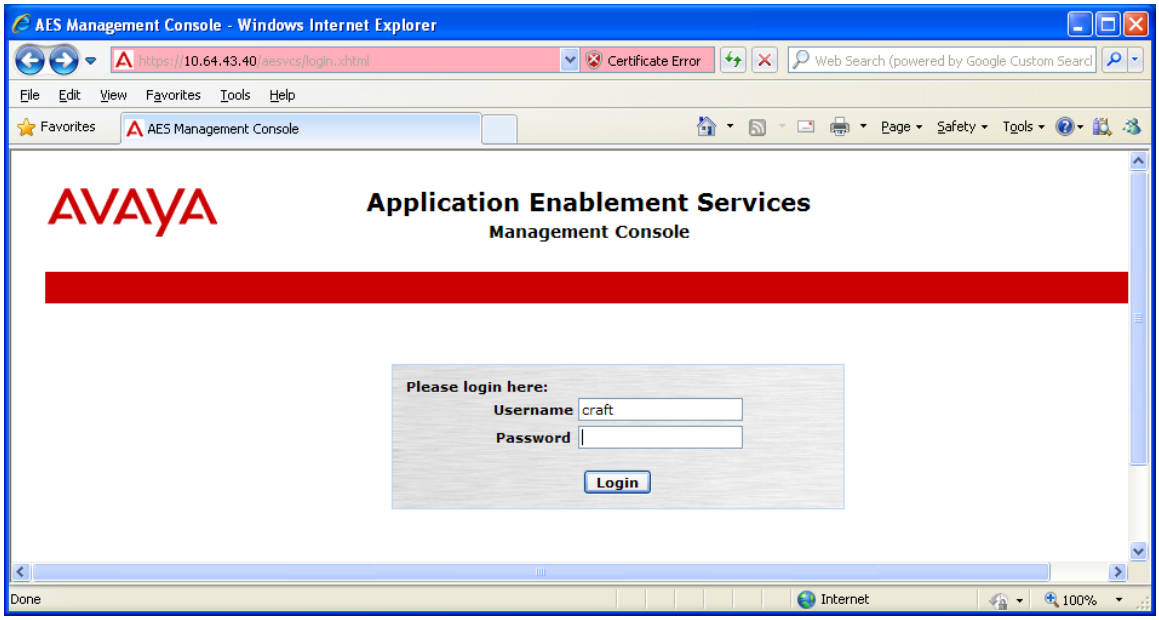
6. Configure Avaya Aura® Application Enablement Services

Application Enablement Services enable Computer Telephony Interface (CTI) applications to control and monitor telephony resources on Communication Manager. Application Enablement Services receive requests from CTI applications, and forwards them to Communication Manager. Conversely, Application Enablement Services receive responses and events from Communication Manager and forwards them to the appropriate CTI applications.

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, creating a CTI link for TSAPI, and a CTI user.

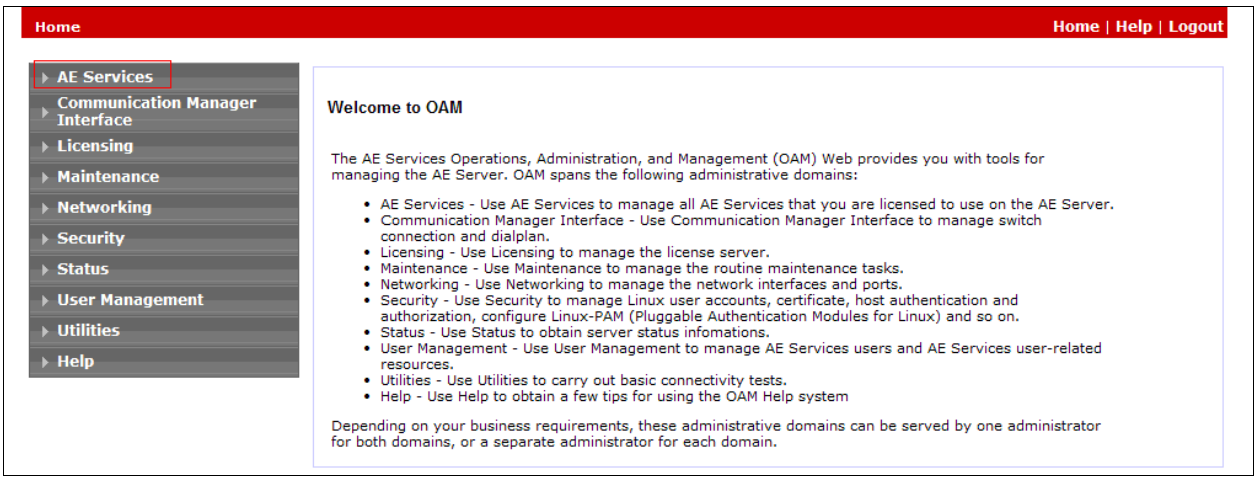
6.1. Configure Switch Connection

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

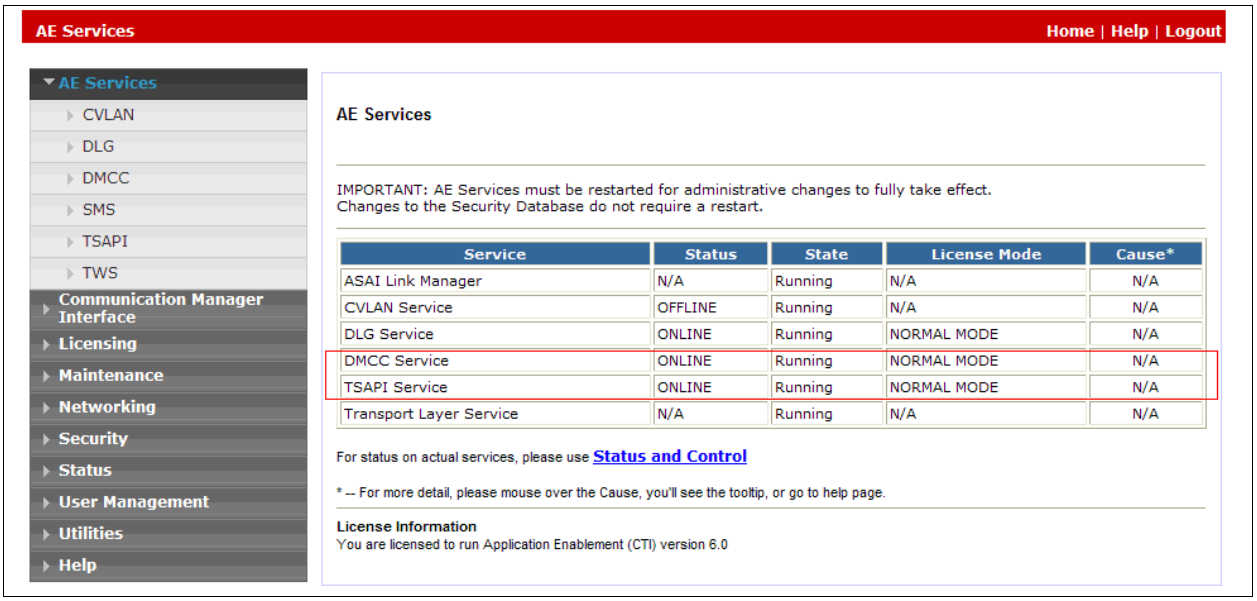


©2012 Avaya Inc. All Rights Reserved.

The Welcome to OAM screen is displayed next. Select **AE Services** from the left pane.

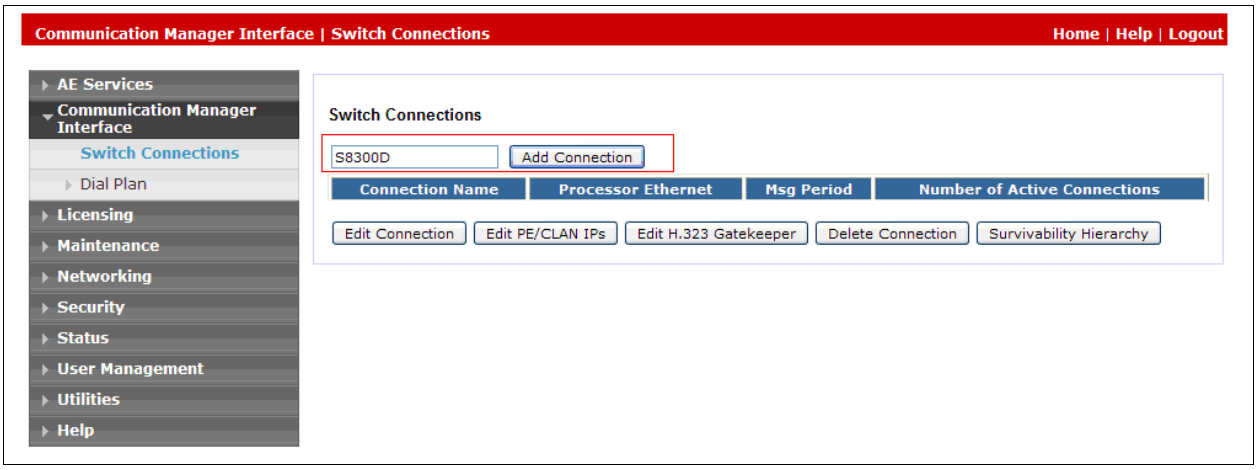


Verify that AES is licensed for the DMCC and TSAPI service, as shown in the screen below.

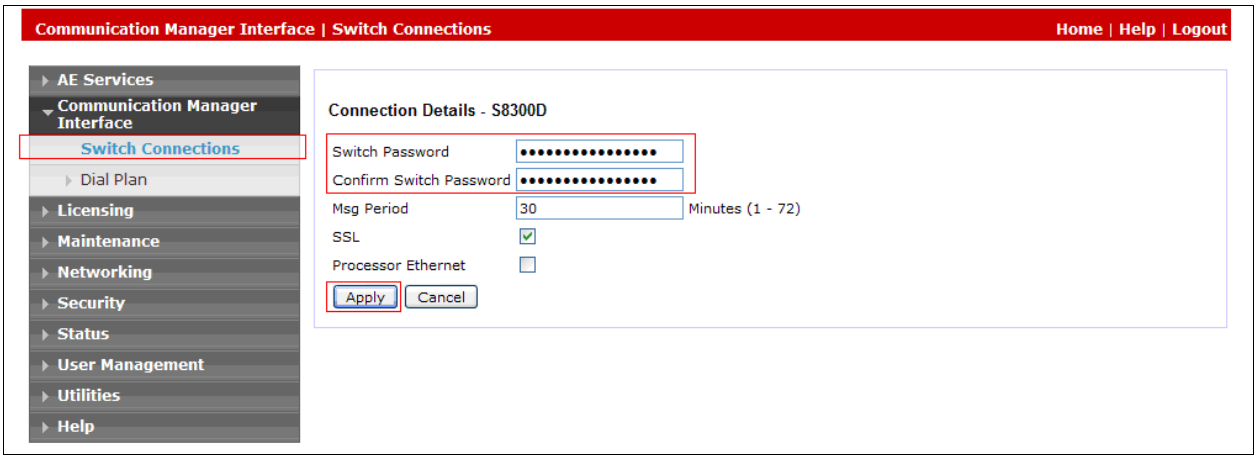


©2012 Avaya Inc. All Rights Reserved.

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**.

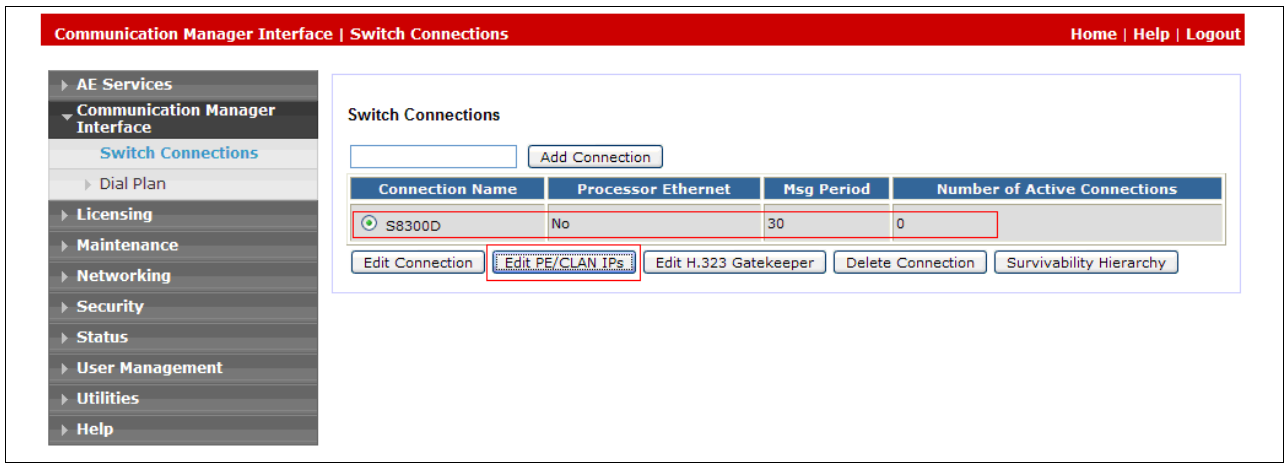


The next window that appears prompts for the Switch Password. Enter the same password that was administered on Communication Manager in **Section 5.5**. Default values may be used in the remaining fields. Click on **Apply**.

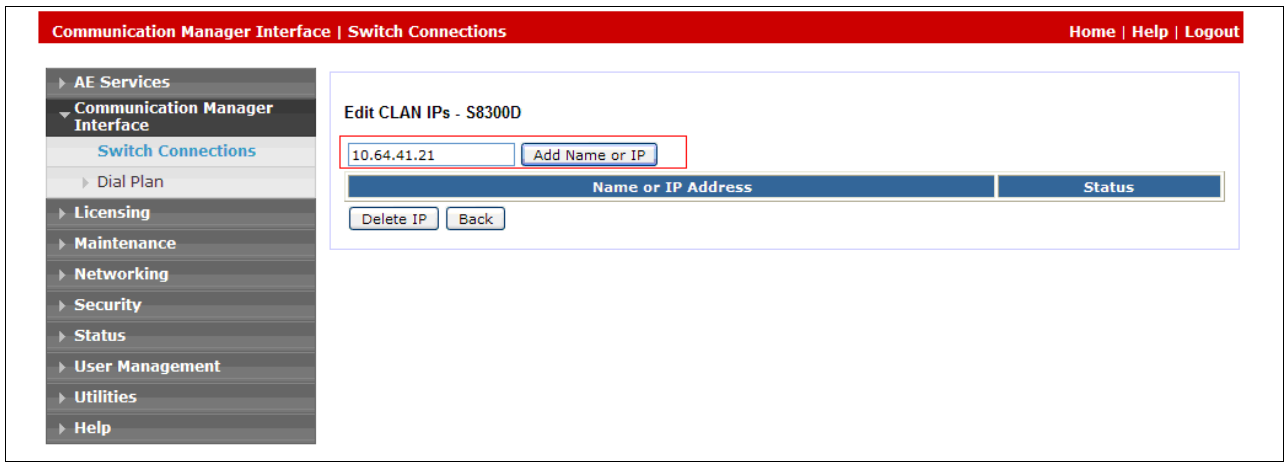


©2012 Avaya Inc. All Rights Reserved.

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

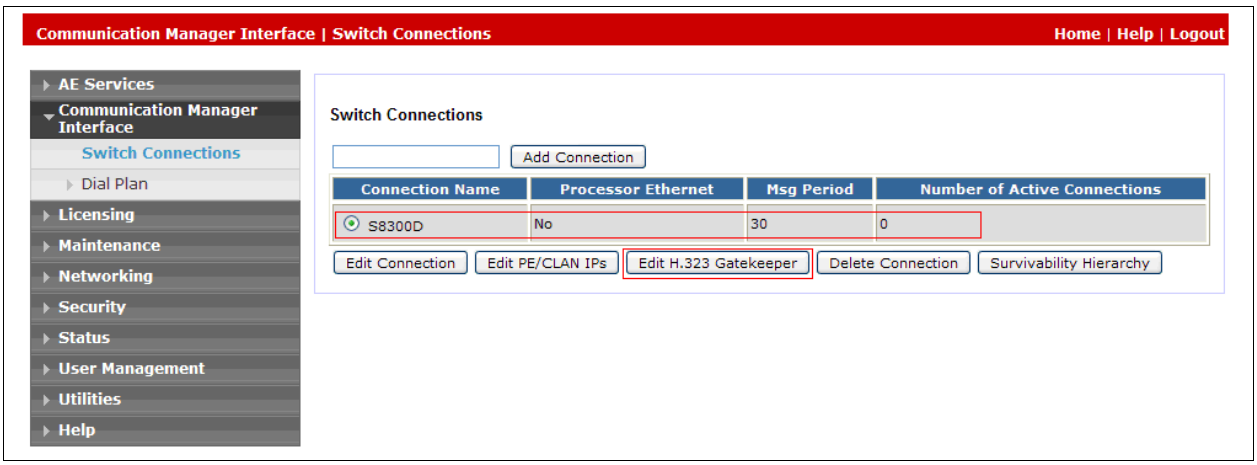


Enter the IP address of Procr used for Application Enablement Services connectivity from **Section 5.6**, and click on **Add Name or IP**.

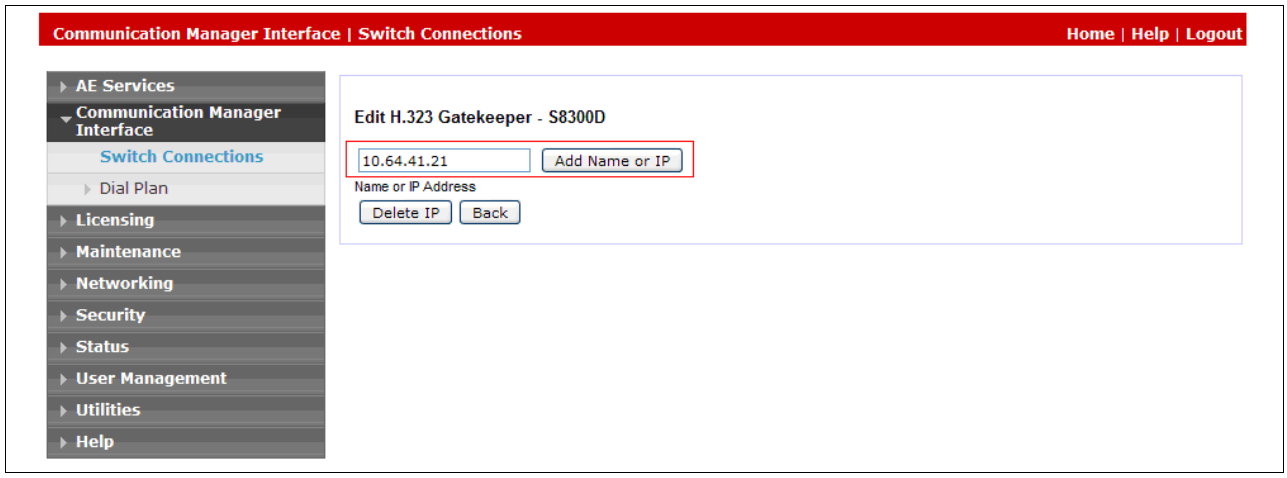


©2012 Avaya Inc. All Rights Reserved.

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



Enter the IP address of Procr used for Application Enablement Services connectivity from **Section 5.5**, and click on **Add Name or IP**.

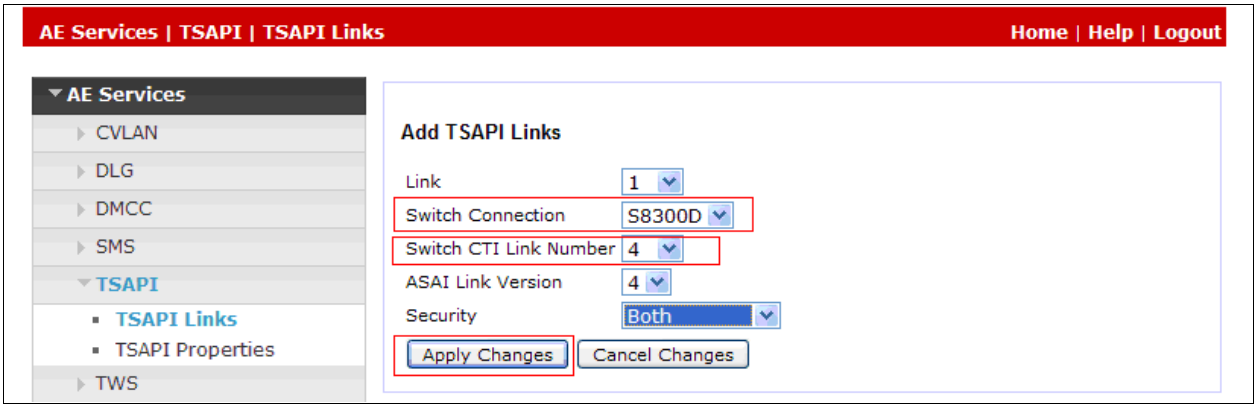


©2012 Avaya Inc. All Rights Reserved.

6.2. Configure TSAPI CTI Link

Navigate to **AE Services → TSAPI → TSAPI Links** to configure the TSAPI CTI link. Click the **Add Link** button to start configuring the TSAPI link.

Select the switch connection using the drop-down menu. Select the switch connection configured in **Section 6.1**. Select the **Switch CTI Link Number** using the drop-down menu. The CTI link number should match with the number configured in the cti-link form in **Section 5.5**. Click **Apply Changes**.



©2012 Avaya Inc. All Rights Reserved.

The following screen shows the TSAPI CTI link configuration.

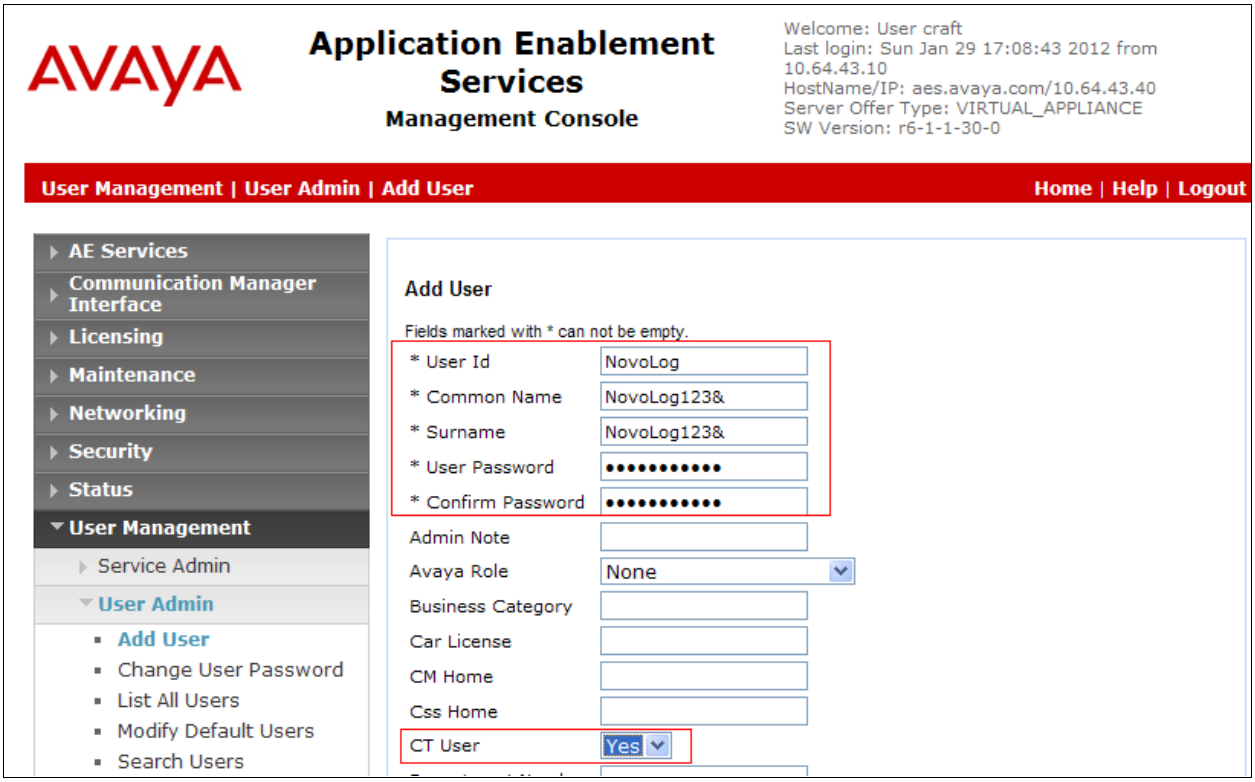
©2012 Avaya Inc. All Rights Reserved.

6.3. Configure CTI User

Navigate to **User Management → Add User**. On the Add User page, provide the following information:

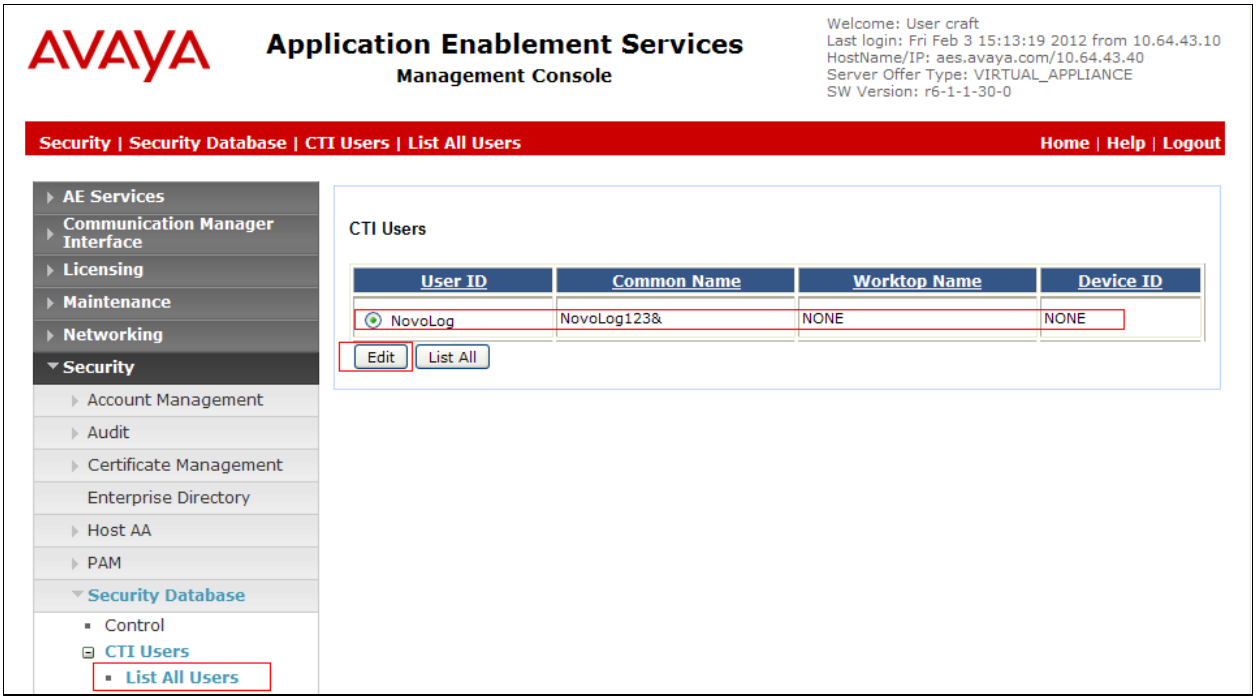
- **User Id**
- **Common Name**
- **Surname**
- **User Password**
- **Confirm Password**

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

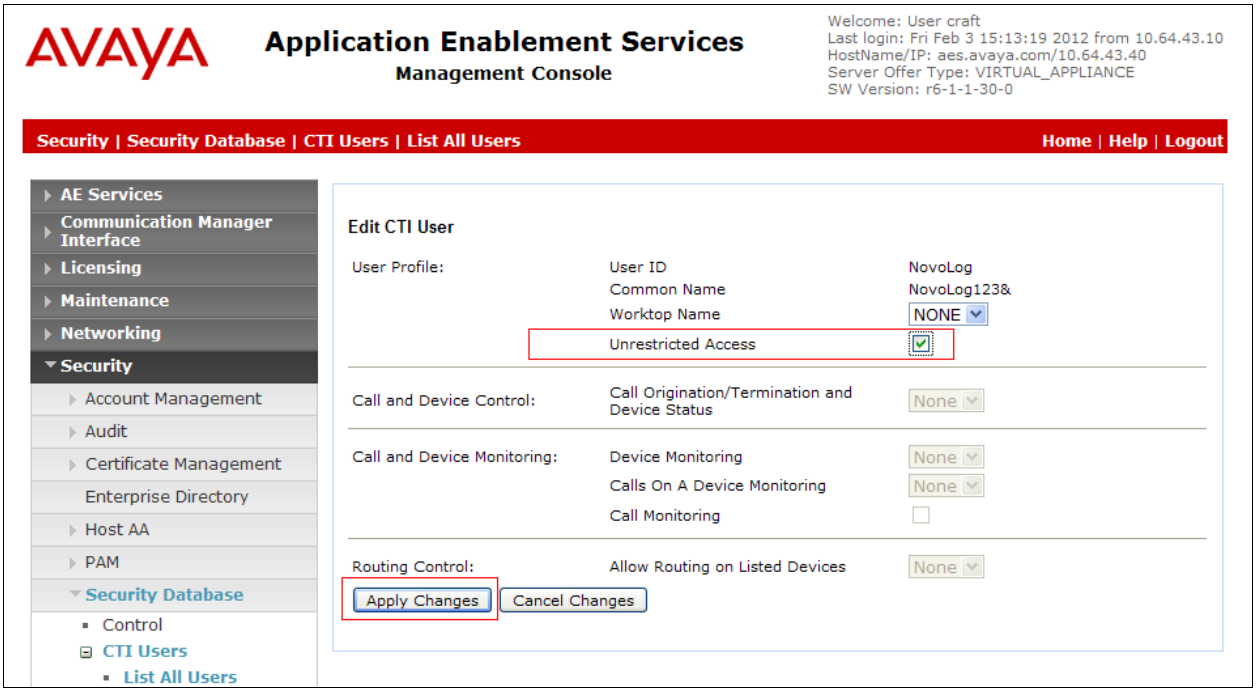


©2012 Avaya Inc. All Rights Reserved.

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

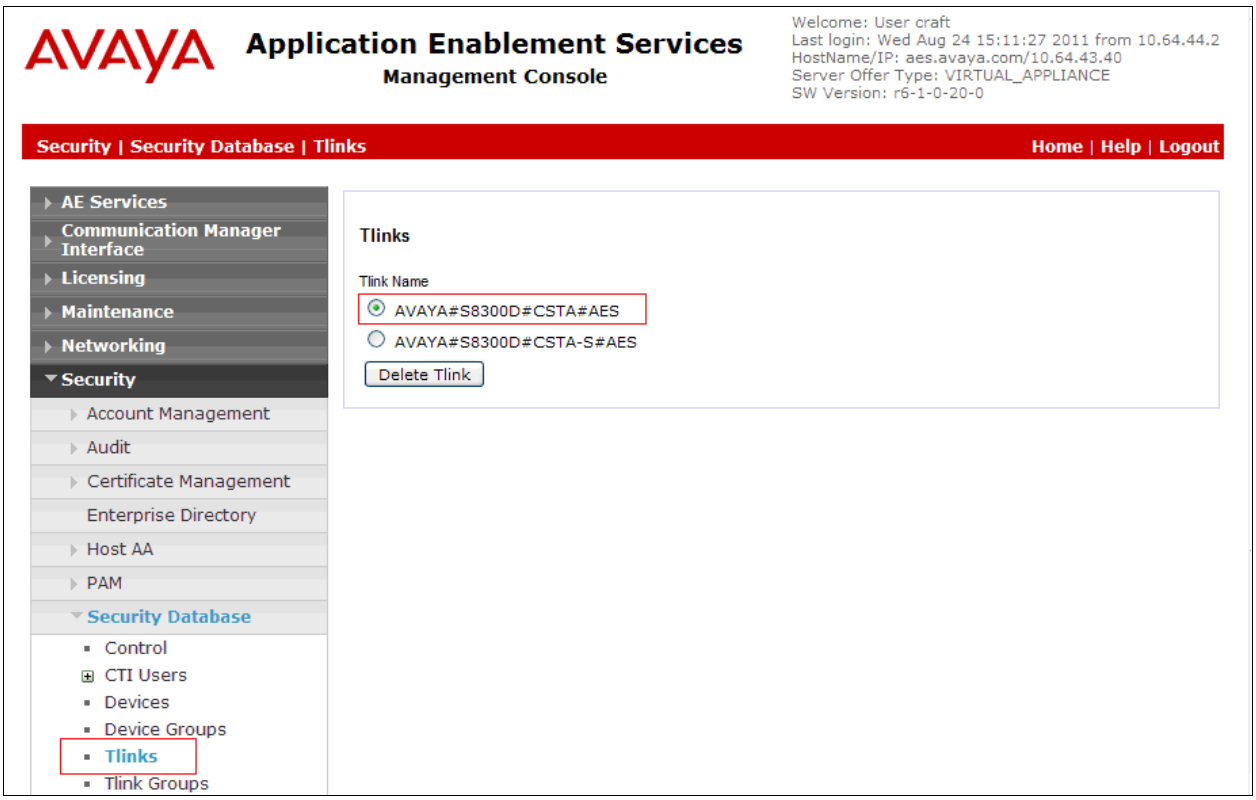


Provide the user with unrestricted access privileges by checking the Unrestricted Access check box. Click the **Apply Changes** button.



©2012 Avaya Inc. All Rights Reserved.

Navigate to the **Security → Security Database → Tlinks** page and verify the Tlink name. The following screen shows the Tlink used during the compliance test.



©2012 Avaya Inc. All Rights Reserved.

7. Configure Novo Technologies NovoLog

Novo Technologies installs, configures, and customizes the NovoLog solution for their end customers. This section briefly describes the configuration of the NovoLog Recorder.

7.1. Configure NovoLog Recorder

Configuring the NovoLog Recorder can be performed through the **NovoLogIpRecorder.ini** file. The NovoLogIpRecorder.ini file is located in the **<Installation Drive> → NovoLogNt → Config** directory. The following shows the contents of the NovoLogIpRecorder.ini file.

```
[Config]
;---PBX Integration Type ---
; 0 -> Undefined
; 1 -> AudioCodes Passive Recording
; 2 -> Avaya AE Services
; 3 -> Cisco Built-In Bridge
IntegrationType=2

; Number of second before a database connection retry.
TryConnectionDelay=300

;---COMPRESSION CODEC---
; 0  -> keep file format, no compression
; 1  -> PCM (no compression)
; 2  -> ADPCM
; 85 -> MP3
CompressionCodec=2
.
.
.
.
.
[RecordingDevices]
; Ip Address of the network card where the RTP
; communication is redirected.
RtpCaptureIpAddress=10.64.44.151 - IP address of the NovoLog Recording server

; Starting UDP port where the RTP communication is redirected.
; There will be two UDP Port per recording device,
; each incremented by two.
StartingUdpPort=5000
.
.
.
.
.
; IP Address of the Application Enablement server.
; Applies to the StartApplicationSession command.
AesIpAddress=10.64.43.40 - IP address of Application Enablement Services server
; AES connection port.
; Applies to the StartApplicationSession command.
; Typical value:
;   4721 for unsecure communications.
;   4722 for secure (encrypted) communications.
AesPort=4721 - Connection port for Application Enablement Services
; User name used to log to the AE server.
; Applies to the StartApplicationSession command.
AesUsername=NovoLog - User Name created in Application Enablement Services
```


©2012 Avaya Inc. All Rights Reserved.

```
; Password used to log to the AE server.
; Applies to the StartApplicationSession command.
AesPassword=NovoLog123& - Password created in Application Enablement Services
; Optionnal AE Services session name.
; Applies to the StartApplicationSession command.
SessionName=NovoLogIpRecorder
; The number of seconds the AE server will wait to cleanup the session if no 'keep
alive' message has been received.
; Applies to the StartApplicationSession command.
; The default value is 60.
SessionCleanupDelay=60
; The number of seconds that the session will last if no 'keep alive' messages are
received.
; Applies to the StartApplicationSession command.
; The default value is 180.
SessionDuration=180
.
.
.
.
.

[NV001] - This section ([NV001] - [NV009]) configures the recorded phones
Description=Physical Phone 72001
AgentId=72001
Extension1=72001
ScreenRecordingEnable=0
KeepTaggedRecordingsOnly=0
MaskDtmf=0
Password=1234 - Optional if the system is configured for password-less registration
DeviceInstance=1

[NV002]
Description=Physical Phone 72002
AgentId=72002
Extension1=72002
ScreenRecordingEnable=0
KeepTaggedRecordingsOnly=0
MaskDtmf=0
Password=1234
DeviceInstance=1

[NV003]
Description=Physical Phone 72003
AgentId=72003
Extension1=72003
ScreenRecordingEnable=0
KeepTaggedRecordingsOnly=0
MaskDtmf=0
Password=1234
DeviceInstance=1

[NV004]
Description=Physical Phone 72004
AgentId=72004
Extension1=72004
ScreenRecordingEnable=0
KeepTaggedRecordingsOnly=0
MaskDtmf=0
Password=1234
DeviceInstance=1
```

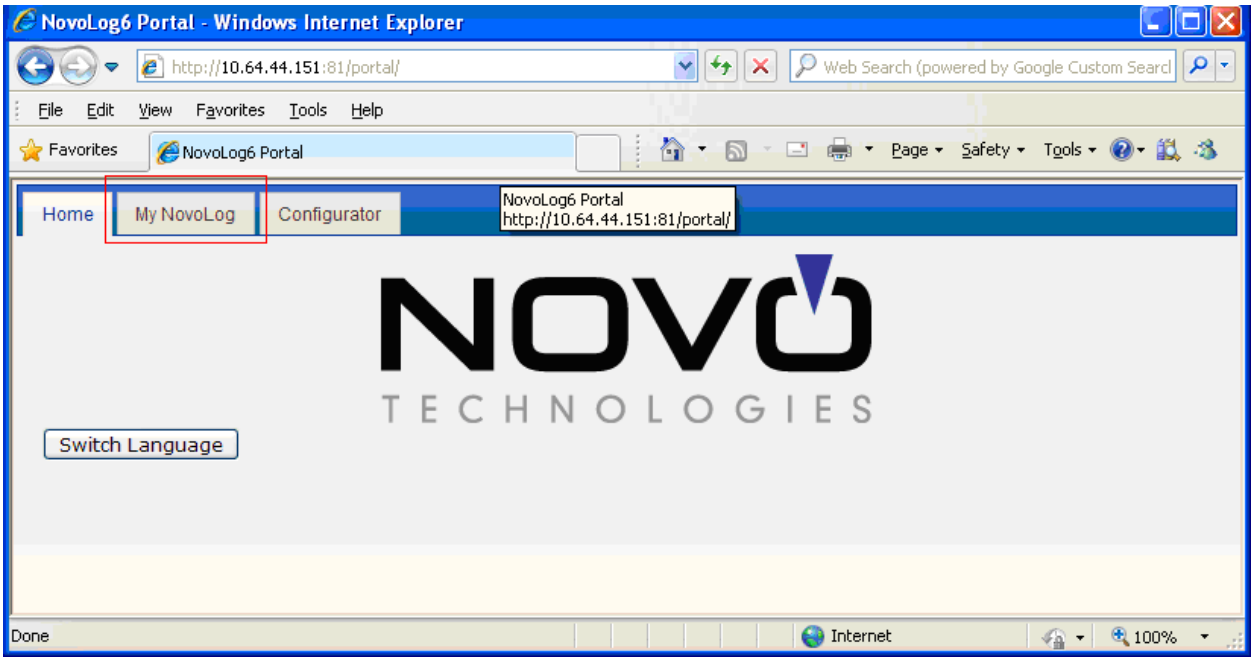

©2012 Avaya Inc. All Rights Reserved.

```
[NV005]
Description=Physical Phone 72005
AgentId=72005
Extension1=72005
ScreenRecordingEnable=0
KeepTaggedRecordingsOnly=0
MaskDtmf=0
Password=1234
DeviceInstance=1

[NV006]
Description=Physical Phone 72006
AgentId=72006
Extension1=72006
ScreenRecordingEnable=0
KeepTaggedRecordingsOnly=0
MaskDtmf=0
Password=1234
DeviceInstance=1

[NV007]
Description=Physical Phone 72007
AgentId=72007
Extension1=72007
ScreenRecordingEnable=0
KeepTaggedRecordingsOnly=0
MaskDtmf=0
Password=1234
DeviceInstance=1

[NV008]
Description=Physical Phone 72008
AgentId=72008
Extension1=72008
ScreenRecordingEnable=0
KeepTaggedRecordingsOnly=0
MaskDtmf=0
Password=1234
DeviceInstance=1

[NV009]
Description=Physical Phone 72009
AgentId=72009
Extension1=72009
ScreenRecordingEnable=0
KeepTaggedRecordingsOnly=0
MaskDtmf=0
Password=1234
DeviceInstance=1
.
.
Entries can be added if more phones are to be recorded
Entry numbers must be consecutive
```

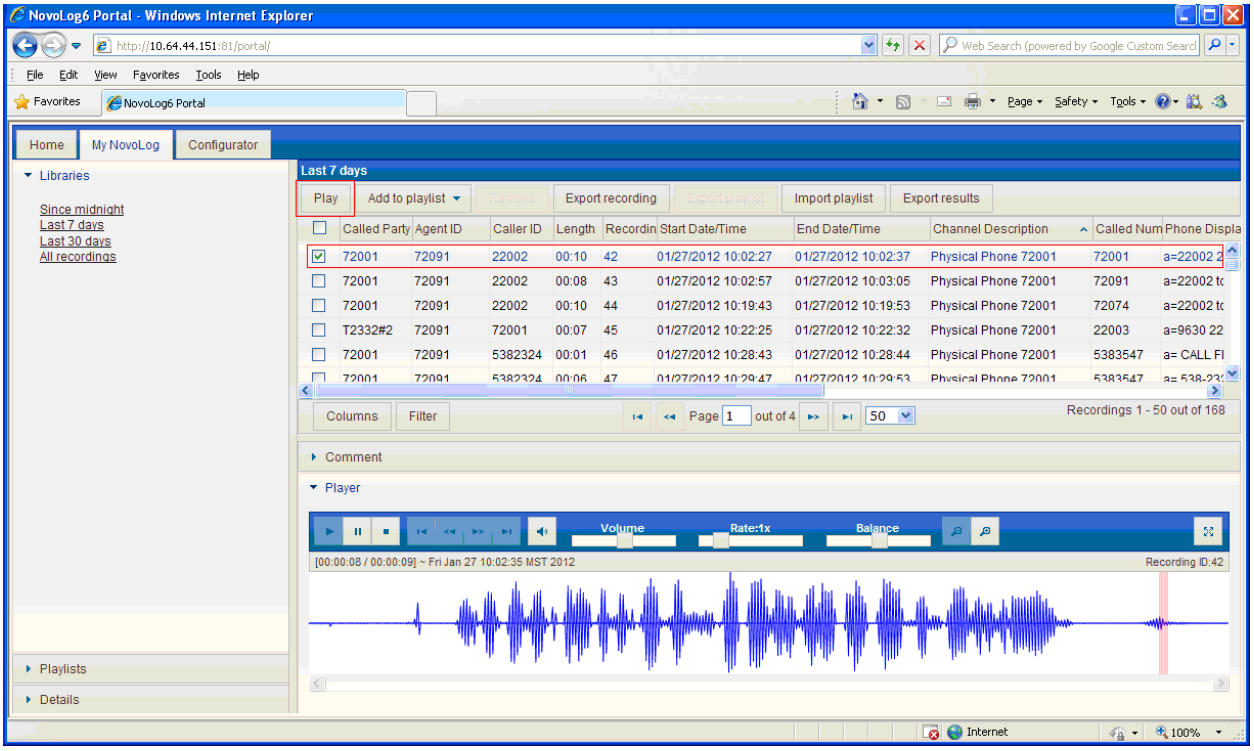

©2012 Avaya Inc. All Rights Reserved.

7.2. NovoLog Recording Playback

Launch a web browser, enter http://<IP Address of NovoLog Web Server>/portal in the URL for accessing the NovoLog home page. Select **My NovoLog** from the main menu.



On the My NovoLog page, provide credentials. Select call record(s), and click the **Play** button.



©2012 Avaya Inc. All Rights Reserved.

8. Verification Steps

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

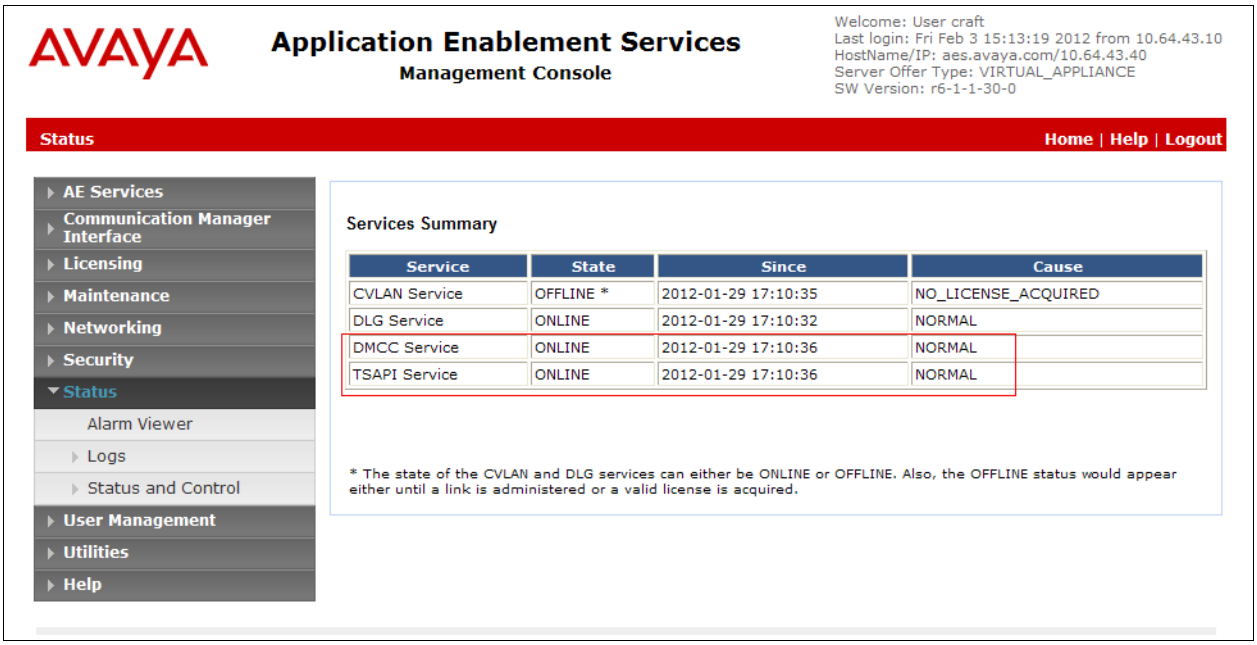
8.1. Verify Avaya Aura® Communication Manager

Using the command, run the **list registered-ip-stations** command and verify two extensions are registered. One with the physical extension IP address and another one with AES IP address.

```
list registered-ip-stations

                              REGISTERED IP STATIONS

Station Ext    Set Type/  Prod ID/    TCP Station IP Address/
or Orig Port   Net Rgn    Release     Skt Gatekeeper IP Address
-------------- --------- ---------- --- ----------------------------------------
72001          9620      IP_Phone     y  10.64.41.201
               1         3.101S          10.64.41.21
72001          9620      IP_API_A     y  10.64.43.40
               1         3.2040          10.64.41.21
72002          9630      IP Phone     y  10.64.40.105
               1         6.020S          10.64.41.21
72002          9630      IP_API_A     y  10.64.43.40
               1         3.2040          10.64.41.21
72003          9650      IP_Phone     y  10.64.41.203
               1         3.101S          10.64.41.21
72003          9650      IP_API_A     y  10.64.43.40
               1         3.2040          10.64.41.21
72008          6408D+    IP_API_A     y  10.64.43.40
               1         3.2040          10.64.41.21
```

8.2. Verify Avaya Aura® Application Enablement Services

From the Application Enablement Services Management Console web pages, verify the state of the DMCC and TSAPI Services are set to **NORMAL** by selecting **Status** from the left pane.



©2012 Avaya Inc. All Rights Reserved.

9. Conclusion

These Application Notes describe the configuration steps required for Novo Technologies NovoLog to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. All feature and serviceability test cases were completed.

10. Additional References

This section references the Avaya and Novo product documentation that is relevant to these Application Notes.

[1] *Administering Avaya Aura™ Communication Manager, Release 6.0, 03-300509, Issue 6.0, June 2010*, available at http://support.avaya.com
[2] Avaya Aura® Application Enablement Services Administration and Maintenance Guide, Release 6.1, Issue 2, February 2011, available at http://support.avaya.com.

[3] NovoLogIpRecorder – Avaya AES Integration – Configuration Guide, 1.0, October, 2011
[4] NovoLog Administrator's Guide, May 2011
[5] My NovoLog User's Guide, September 2011

©2012 Avaya Inc. All Rights Reserved.

©2012 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.