Avaya Solution & Interoperability Test Lab

Application Notes for VirtualLogger Call Recording Engine with Avaya Aura^{TM} Communication Manager and Avaya Aura^{TM} Application Enablement Services - Issue 1.0

Abstract

These Application Notes describe a compliance-tested configuration comprised of Avaya Aura^{TM} Communication Manager, Avaya Aura^{TM} Application Enablement Services, Avaya IP and Digital Telephones, and the VirtualLogger Call Recording Engine desktop application.

VirtualLogger Call Recording Engine is a trunk tap recording solution, and utilizes the TSAPI for phone events.

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^{TM} Communication Manager, Avaya Aura^{TM} Application Enablement Services, Avaya IP and Digital Telephones, and VirtualLogger Call Recording Engine.

VirtualLogger Call Recording Engine (CRE) is a software recording solution that monitors trunks for voice traffic. Each T1/ISDN-PRI trunk needs to have a tap point installed between the Central Office (CO) and a PBX using an RJ45 T-splitter adaptor or by installing a dual RJ45 jack. A T1 cross-over network cable will be connected to the tap point on one end, and the other end connected to the Ai-Logix DP series card (DP6409). During the compliance test, Avaya S8720 Servers with Avaya G650 Media Gateway simulated the CO, and Avaya S8300 Server with Avaya G450 Media Gateway simulated the PBX. The VirtualLogger CRE monitors and records CO side stations.

The compliance testing will focus on the integration between VirtualLogger Call Recording Engine service, Communication Manager, Application Enablement Services, and Avaya IP and digital telephones. VirtualLogger provided the Call Recording Engine application with a special configuration file designed to fully test the Call Recording Engine functionality. Telephone operations such as off-hook, on-hook, dialing, answering, hold, transfer, conference, etc. will be performed from the physical telephones. In addition, telephone displays and call states on the physical telephones and in Call Recording Engine will be verified for consistency.

1.1. Interoperability Compliance Testing

The interoperability compliance test included features and serviceability. The focus of the compliance testing was primarily on verifying the interoperability between VirtualLogger Call Recording Engine, Application Enablement Services, and Communication Manager.

1.2. Support

Technical support for the VirtualLogger Call Recording Engine solution can be obtained by contacting VirtualLogger:

- URL – helpdesk@virtuallogger.com
- Phone – 866-864-5376

2. 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 Avaya S8720 Media Servers with a G650 Media Gateway. The Call Recording Engine was located on a different VLAN. Endpoints include Avaya 9600 Series H.323 IP Telephones, an Avaya 4625 H.323 IP Telephone, and an Avaya 6408D Digital Telephone. An Avaya S8300 Server with an Avaya G450 Media Gateway was included in the test to provide an inter-switch scenario.

Note: Basic administration of the Application Enablement Services server is assumed. For details, see [2].

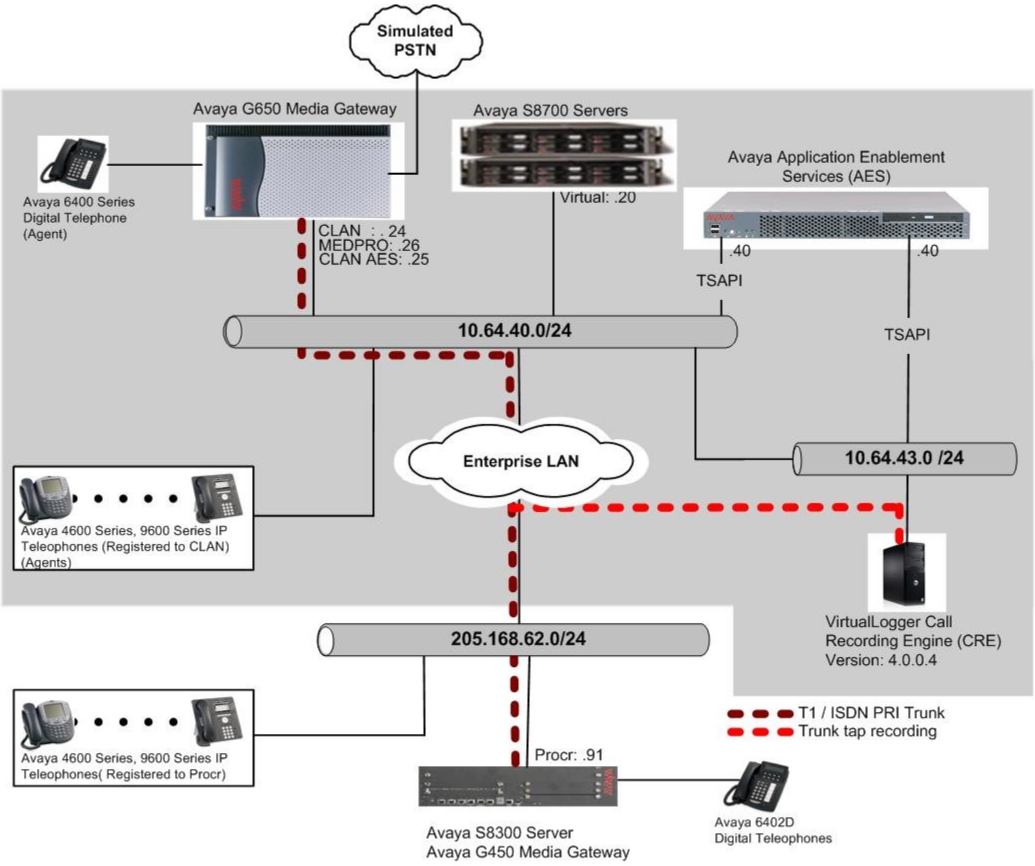

Simulated PSTN
Avaya G650 Media Gateway
Avaya S8700 Servers
Avaya Application Enablement Services (AES)
Avaya 6400 Series Digital Telephone (Agent)
Virtual: .20
CLAN : . 24
MEDPRO: .26
CLAN AES: .25
.40
.40
TSAPI
TSAPI
10.64.40.0/24
Enterprise LAN
10.64.43.0 /24
Avaya 4600 Series, 9600 Series IP Teleophones (Registered to CLAN) (Agents)
VirtualLogger Call Recording Engine (CRE) Version: 4.0.0.4
205.168.62.0/24
T1 / ISDN PRI Trunk
Trunk tap recording
Avaya 4600 Series, 9600 Series IP Teleophones(Registered to Procr)
Procr: .91
Avaya S8300 Server
Avaya G450 Media Gateway
Avaya 6402D Digital Teleophones

Figure 1: VirtualLogger Call Recording Engine Test Configuration

3. Equipment and Software Validated

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

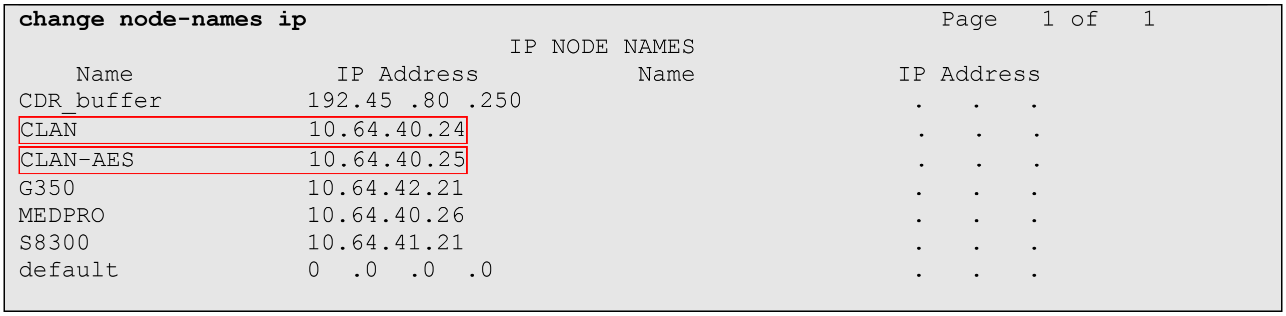
Equipment	Software/Firmware
Avaya S8720 Servers	Avaya Aura™ Communication Manager 5.2.1 (R015x.02.1.016.4)
Avaya G650 Media Gateway	
TN2312BP IP Server Interface TN799DP C-LAN Interface TN2302AP IP Media Processor	HW12 FW22 HW1 FW16 HW11 FW107
Avaya S8300 Server with Avaya G450 Media Gateway	Avaya Aura™ Communication Manager 5.2.1 (R015x.02.1.016.4)
Avaya Aura™ Application Enablement Services Server	5.2 (r5-2-0-98-0)
Avaya 4625SW IP Telephone	2.5
Avaya 9600 Series IP Telephones	
9620 (H.323) 9630 (H.323) 9650 (H.323)	3.1 3.1 3.1
Avaya 6424D+ Digital Telephone	-
VirtualLogger Call Recording Engine	4.0.0.4

4. Configure Aura^{TM} Avaya Communication Manager

This section describes the procedure for setting up a Feature Access Codes. Abbreviated dialing, and controlled telephones.

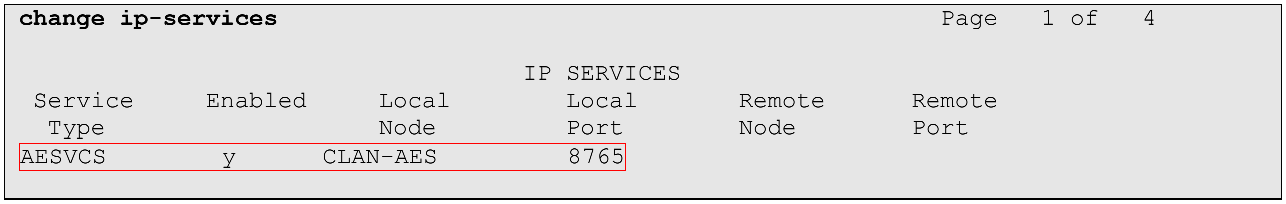
4.1. Configure IP Services

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



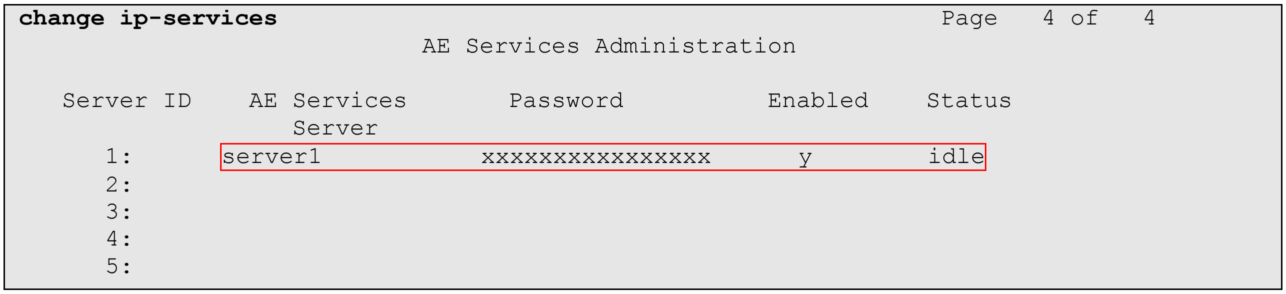
```
change node-names ip                                          Page   1 of   1
                                  IP NODE NAMES
    Name                 IP Address              Name                 IP Address
CDR_buffer           192.45 .80 .250                                 .   .   .
CLAN                 10.64.40.24                                     .   .   .
CLAN-AES             10.64.40.25                                     .   .   .
G350                 10.64.42.21                                     .   .   .
MEDPRO               10.64.40.26                                     .   .   .
S8300                10.64.41.21                                     .   .   .
default              0   .0   .0   .0                                .   .   .
```

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 **CLAN-AES** board 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      CLAN-AES          8765
```

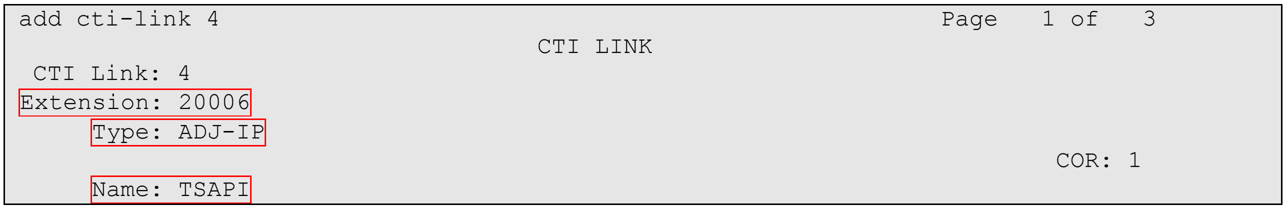
On **Page 4**, enter the hostname of the Application Enablement Services server for the AE Services Server field. The server name may be obtained by logging in to the Application Enablement Services server using ssh, and running the command **uname –a**. Enter an alphanumeric password for the Password field. Set the Enabled field to **y**. The same password will be configured on the Application Enablement Services server in **Section 5.2**.



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

   Server ID     AE Services        Password          Enabled     Status
                    Server
       1:       server1          xxxxxxxxxxxxxxxx       y          idle
       2:
       3:
       4:
       5:
```

4.2. Configure CTI link

Enter the **add cti-link g** command, where **g** is the number between 1 and 64, inclusive. Enter a valid Extension under the provisioned dial plan in Communication Manager, set the Type field to **ADJ-IP**, and assign a descriptive Name to the CTI link.

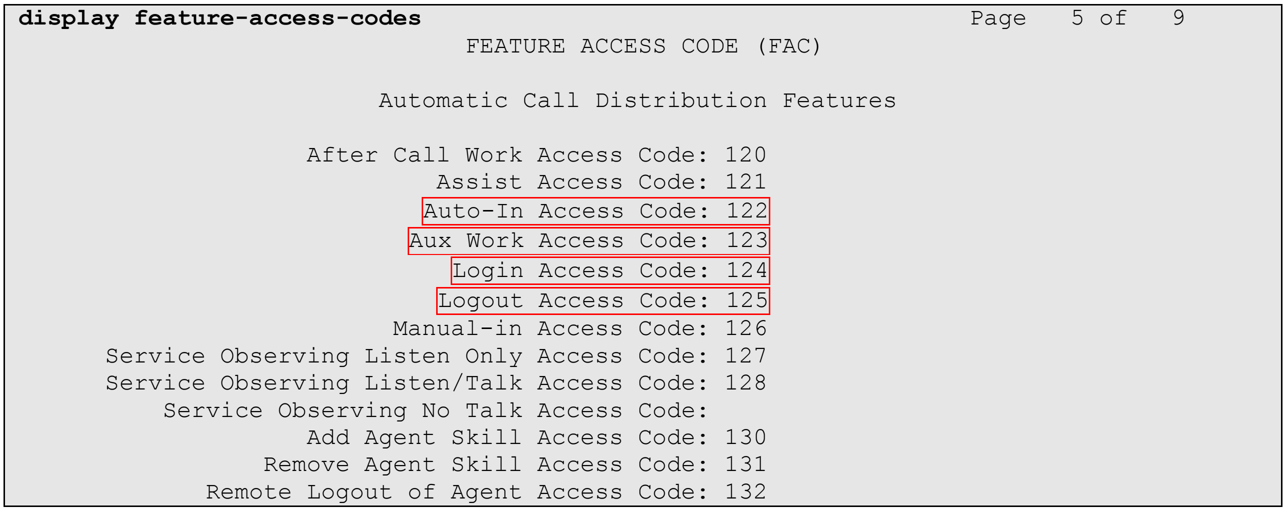


```
add cti-link 4                                                  Page   1 of   3
                                    CTI LINK
 CTI Link: 4
Extension: 20006
     Type: ADJ-IP
                                                                        COR: 1
     Name: TSAPI
```

4.3. Configure Feature Access Codes (FAC)

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

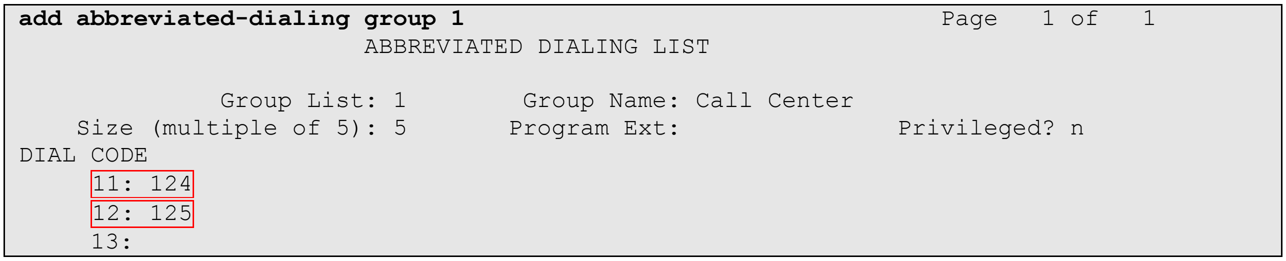
- Auto-In Access Code
- Aux Work Access Code
- Login Access Code
- Logout Access Code



```
display feature-access-codes                                      Page   5 of   9
                               FEATURE ACCESS CODE (FAC)

                         Automatic Call Distribution Features

                    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 Listen Only Access Code: 127
      Service Observing Listen/Talk Access Code: 128
          Service Observing No Talk Access Code:
                    Add Agent Skill Access Code: 130
                 Remove Agent Skill Access Code: 131
             Remote Logout of Agent Access Code: 132
```

4.4. 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 4.3**

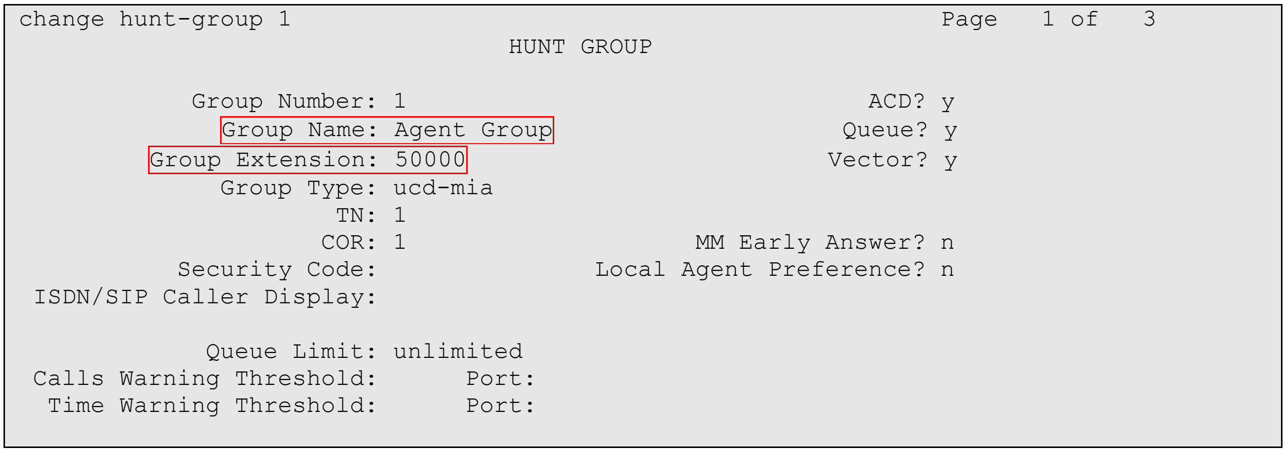


```
add abbreviated-dialing group 1                                 Page   1 of   1
                        ABBREVIATED DIALING LIST

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

4.5. Configure Hunt Group

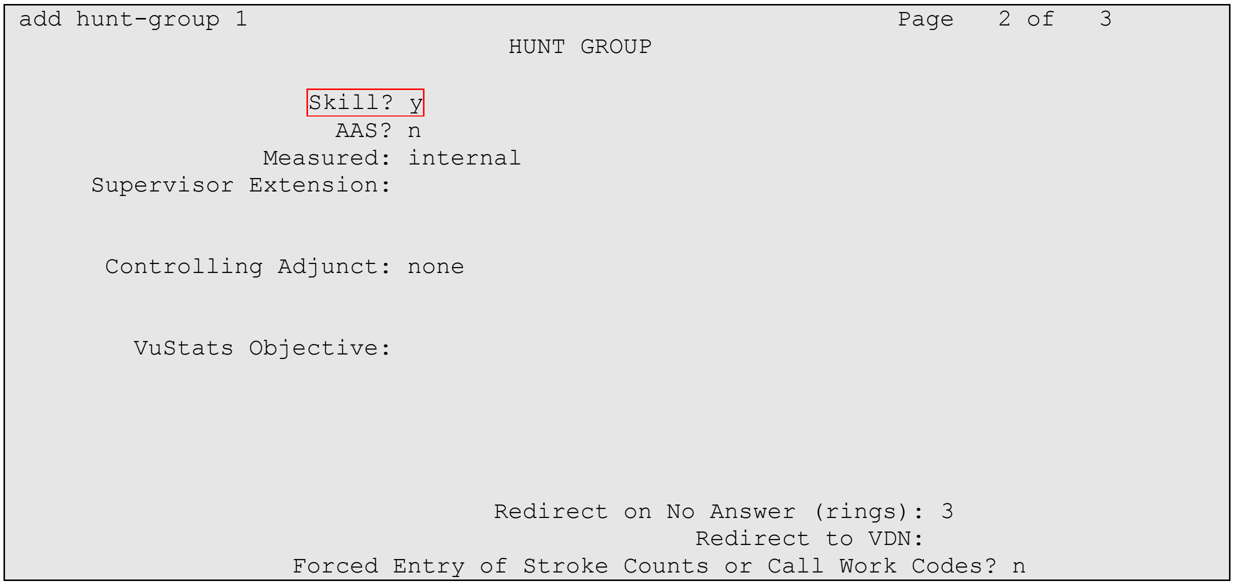
Enter the **add hunt-group n** command, where **n** is an unused hunt group number. On **Page 1**, assign a descriptive Group Name and Group Extension valid in the provisioned dial plan.

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.



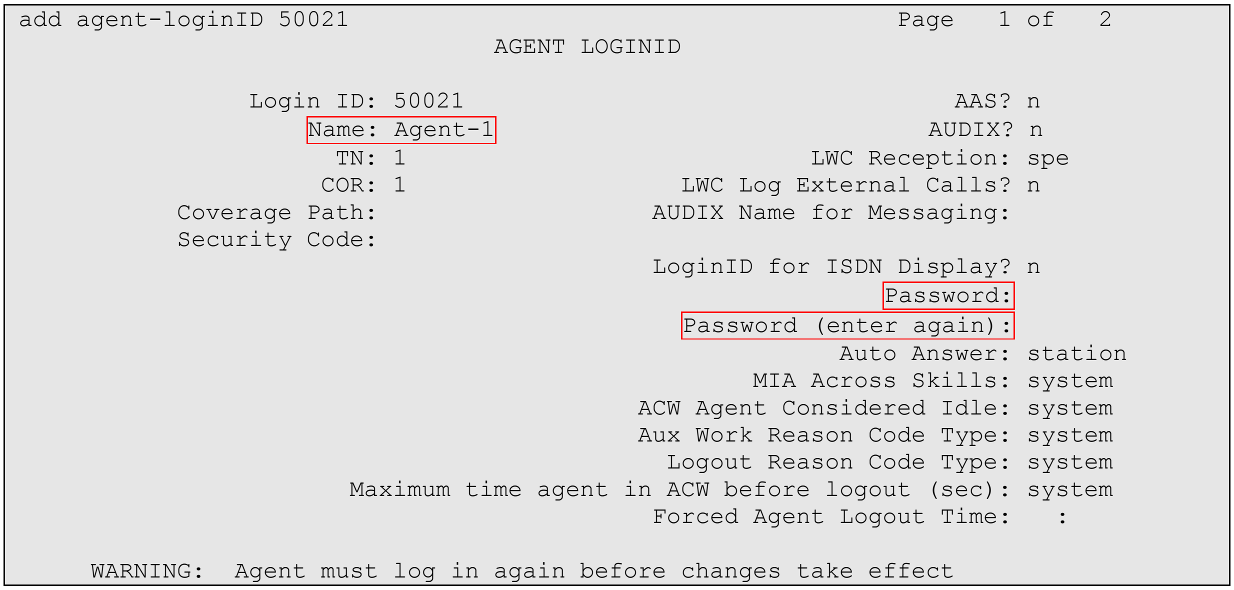
```
change hunt-group 1                                             Page   1 of   3
                                  HUNT GROUP

            Group Number: 1                                ACD? y
              Group Name: Agent Group                    Queue? y
         Group Extension: 50000                         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**, this means that agent membership in the hunt group is based on skills, rather than a pre-programmed assignment to the hunt group.



```
add hunt-group 1                                             Page   2 of   3
                                  HUNT GROUP

                    Skill? y
                      AAS? n
                 Measured: internal
     Supervisor Extension:


      Controlling Adjunct: none


        VuStats Objective:





                                 Redirect on No Answer (rings): 3
                                               Redirect to VDN:
                   Forced Entry of Stroke Counts or Call Work Codes? n
```

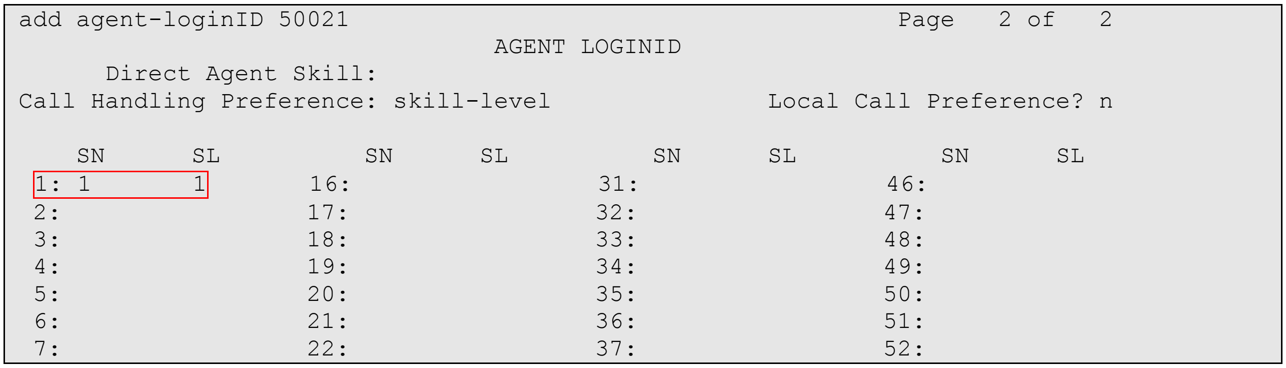
Enter the **add agent-loginID p** command, where **p** is a valid extension in the provisioned dial plan. On **Page 1**, enter a descriptive name, and password.



```
add agent-loginID 50021                                      Page   1 of   2
                                 AGENT LOGINID

                Login ID: 50021                                  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 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
```

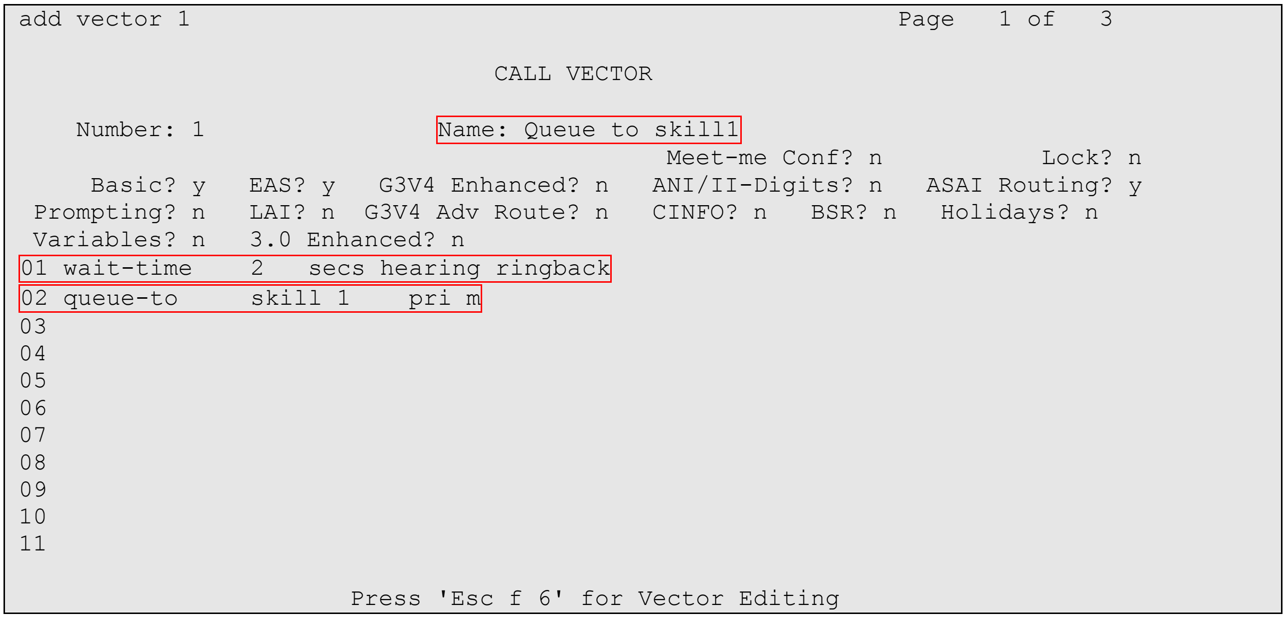
On **Page 2**, set the Skill Number (SN) to the hunt group number previously created. The Skill Level (SL) may be set according to customer requirements.

Repeat this step as necessary to configure additional agent extensions.



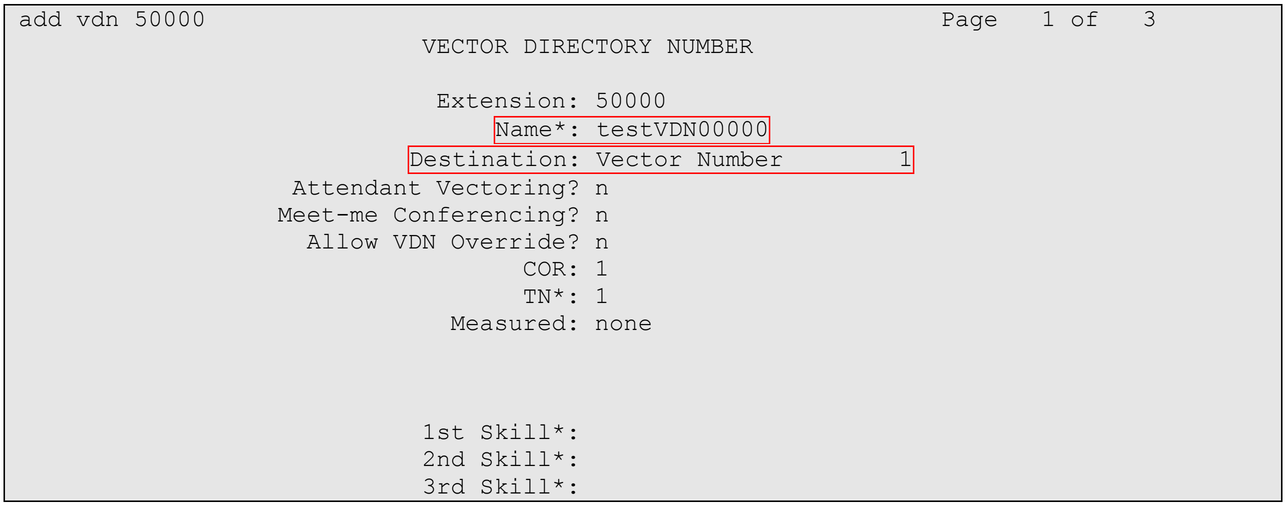
```
add agent-loginID 50021                                       Page   2 of   2
                                 AGENT LOGINID
      Direct Agent Skill:
Call Handling Preference: skill-level              Local Call Preference? n

    SN       SL          SN       SL          SN       SL          SN       SL
 1: 1        1       16:                  31:                  46:
 2:                  17:                  32:                  47:
 3:                  18:                  33:                  48:
 4:                  19:                  34:                  49:
 5:                  20:                  35:                  50:
 6:                  21:                  36:                  51:
 7:                  22:                  37:                  52:
```

Enter the **add vector q** command, where **q** is an unused vector number. Enter a descriptive name, and administer 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.



```
add vector 1                                                  Page   1 of   3

                                 CALL VECTOR

    Number: 1                Name: Queue to skill1
                                              Meet-me Conf? n           Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? n   ANI/II-Digits? n   ASAI Routing? y
 Prompting? n   LAI? n  G3V4 Adv Route? n   CINFO? n    BSR? n    Holidays? n
 Variables? n   3.0 Enhanced? n
01 wait-time     2   secs hearing ringback
02 queue-to      skill 1    pri m
03
04
05
06
07
08
09
10
11
                       Press 'Esc f 6' for Vector Editing
```

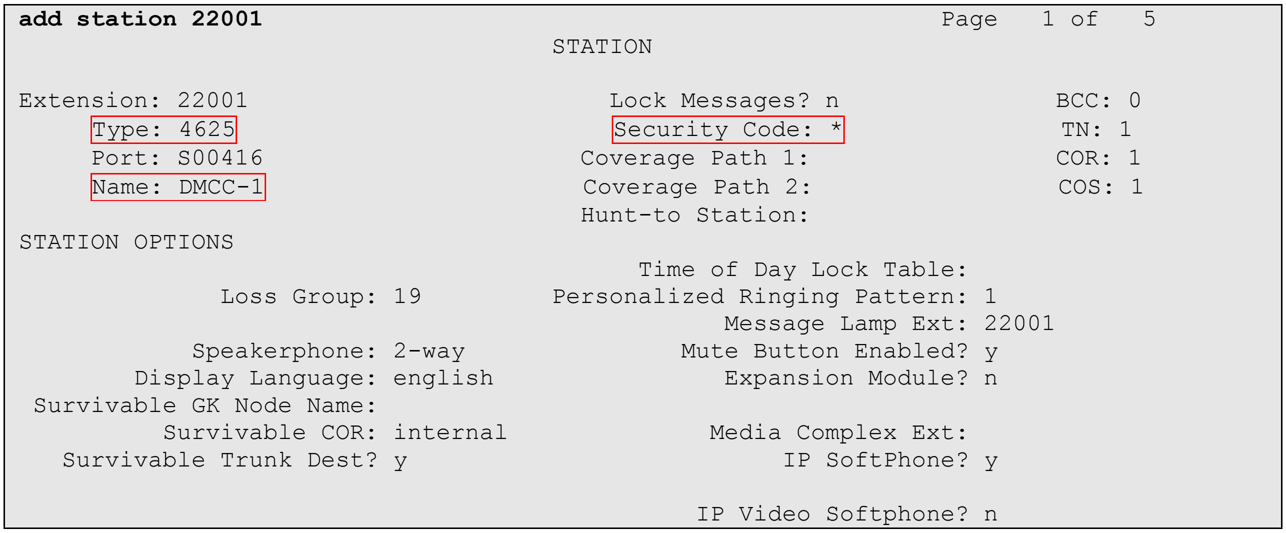
Enter the **add vdn r** command, where **r** is an extension valid in the provisioned dial plan. Specify a descriptive name for the VDN and the Vector Number configured in the previous step. In the example below, incoming calls to extension 50000 corresponds to testVDN00000, which in turn will invoke the actions specified in vector 1.



```
add vdn 50000                                                Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 50000
                                 Name*: testVDN00000
                           Destination: Vector Number        1
                  Attendant Vectoring? n
                 Meet-me Conferencing? n
                   Allow VDN Override? n
                                   COR: 1
                                   TN*: 1
                              Measured: none



                            1st Skill*:
                            2nd Skill*:
                            3rd Skill*:
```

4.6. Configure Monitored Telephones

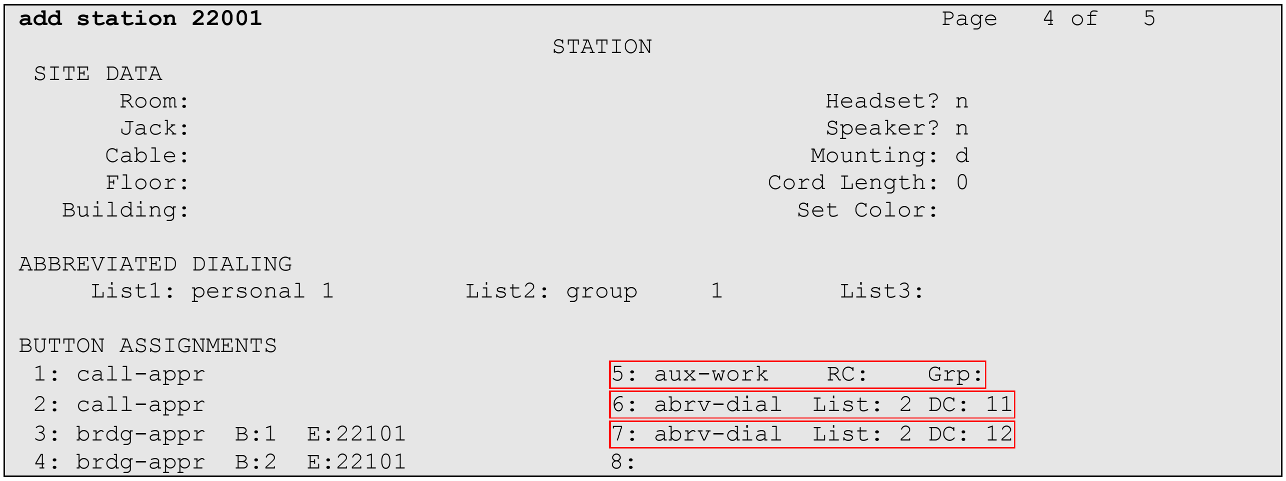
Enter the **change station r** command, where **r** is the extension of a registered, physical Avaya IP or Digital telephone. On **Page 1** of the **station** form, enter a phone Type, descriptive name, Security Code to allow the physical station to be monitored by the Call Recording Engine application.



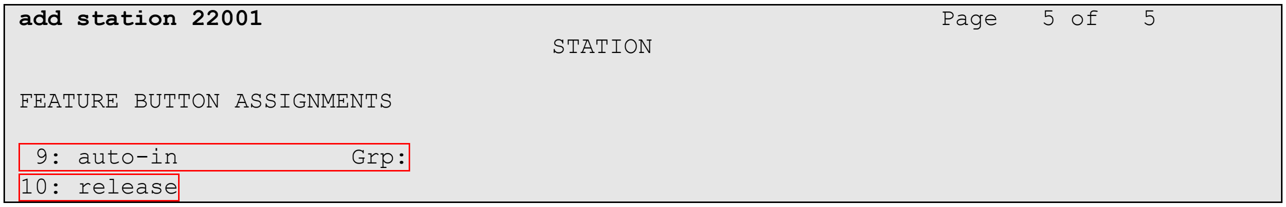
```
add station 22001                                            Page   1 of   5
                                     STATION

Extension: 22001                         Lock Messages? n              BCC: 0
     Type: 4625                          Security Code: *               TN: 1
     Port: S00416                      Coverage Path 1:                COR: 1
     Name: DMCC-1                      Coverage Path 2:                COS: 1
                                       Hunt-to Station:
STATION OPTIONS
                                           Time of Day Lock Table:
              Loss Group: 19         Personalized Ringing Pattern: 1
                                                Message Lamp Ext: 22001
            Speakerphone: 2-way                Mute Button Enabled? y
        Display Language: english                 Expansion Module? n
 Survivable GK Node Name:
          Survivable COR: internal               Media Complex Ext:
   Survivable Trunk Dest? y                           IP SoftPhone? y

                                                IP Video Softphone? n
```

On **Page 4** of the station form, for **ABBREVIATED DIALING List 1**, enter the abbreviated dialing group configured in **Section 4.4** On **Pages 4** and **5** of the station forms, configure the following BUTTON ASSIGNMENTS in addition to the call-appr (call appearance) buttons:

- aux-work
- abrv-dial – configure two of these buttons, one for Login and one for Logout, along with the Dial Codes from Abbreviated Dialing **List1** for ACD Login and Logout, respectively.
- auto-in (On Page 5)
- release (On Page 5)



```
add station 22001                                               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                            5: aux-work     RC:    Grp:
 2: call-appr                            6: abrv-dial  List: 2 DC: 11
 3: brdg-appr  B:1   E:22101             7: abrv-dial  List: 2 DC: 12
 4: brdg-appr  B:2   E:22101             8:
```



```
add station 22001                                               Page   5 of   5
                                     STATION

FEATURE BUTTON ASSIGNMENTS

 9: auto-in             Grp:
10: release
```

Repeat the instructions provided in this section for each physical station that is to be monitored by a VirtualLogger CRE.

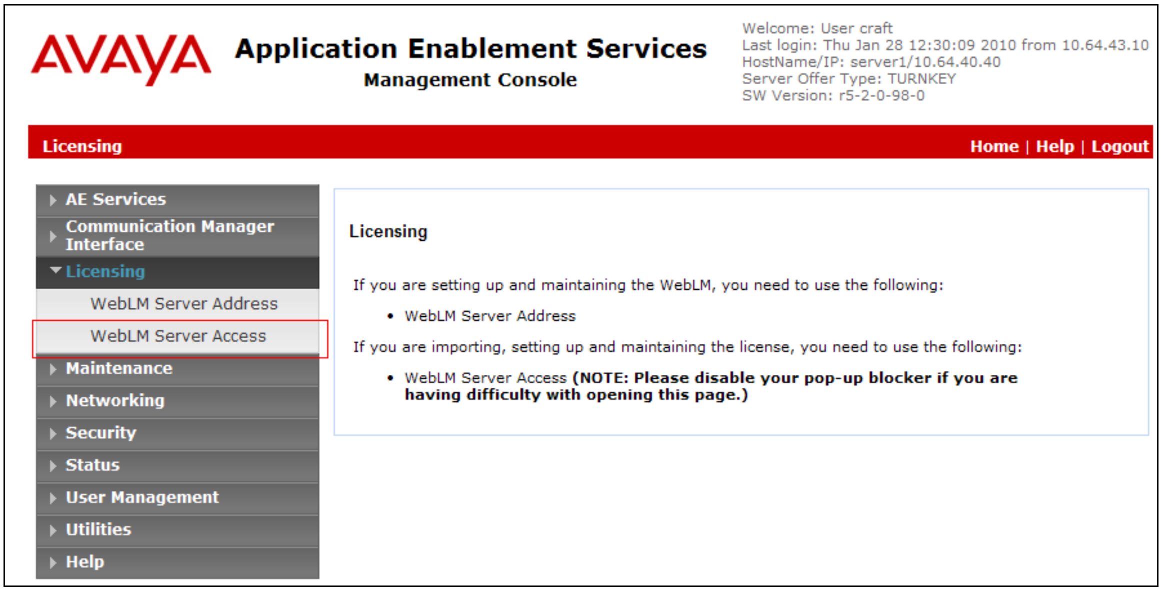
5. Configure Avaya Application Enablement Services

The Avaya Application Enablement Services server enables Computer Telephony Interface (CTI) applications to 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 and a CTI user.

5.1. TSAPI Licenses

To check and verify that there are sufficient TSAPI 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.



Licensing

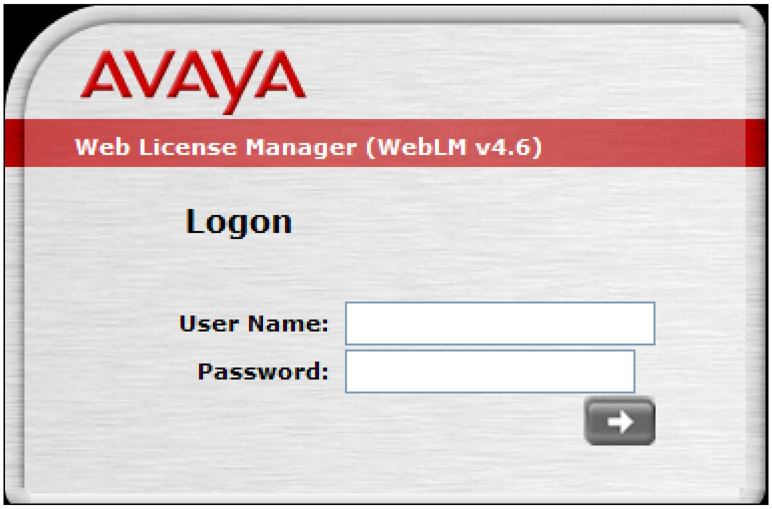
If you are setting up and maintaining the WebLM, you need to use the following:

- WebLM Server Address

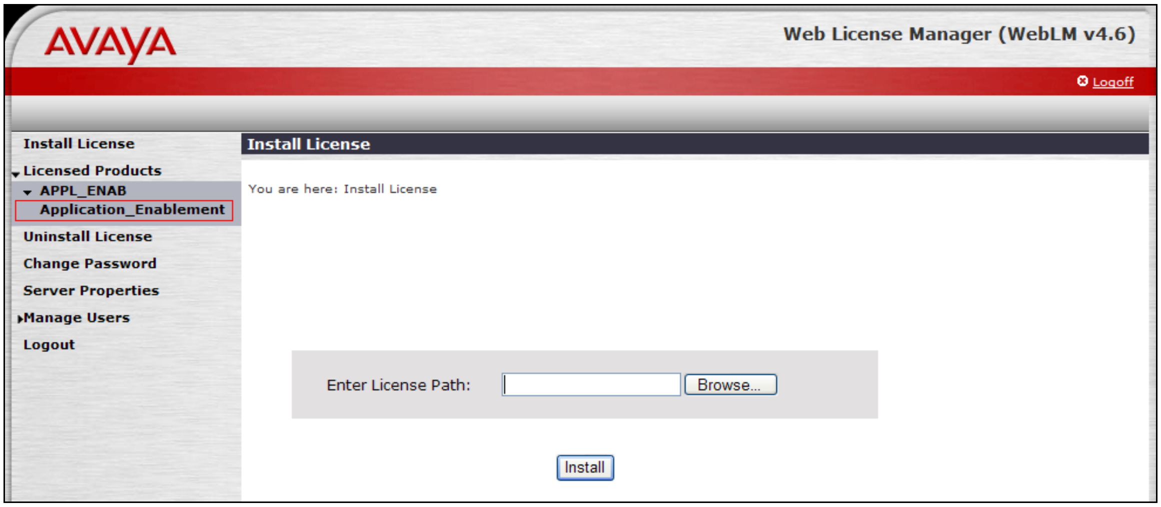
If you are importing, setting up and maintaining the license, you need to use the following:

- WebLM Server Access **(NOTE: Please disable your pop-up blocker if you are having difficulty with opening this page.)**

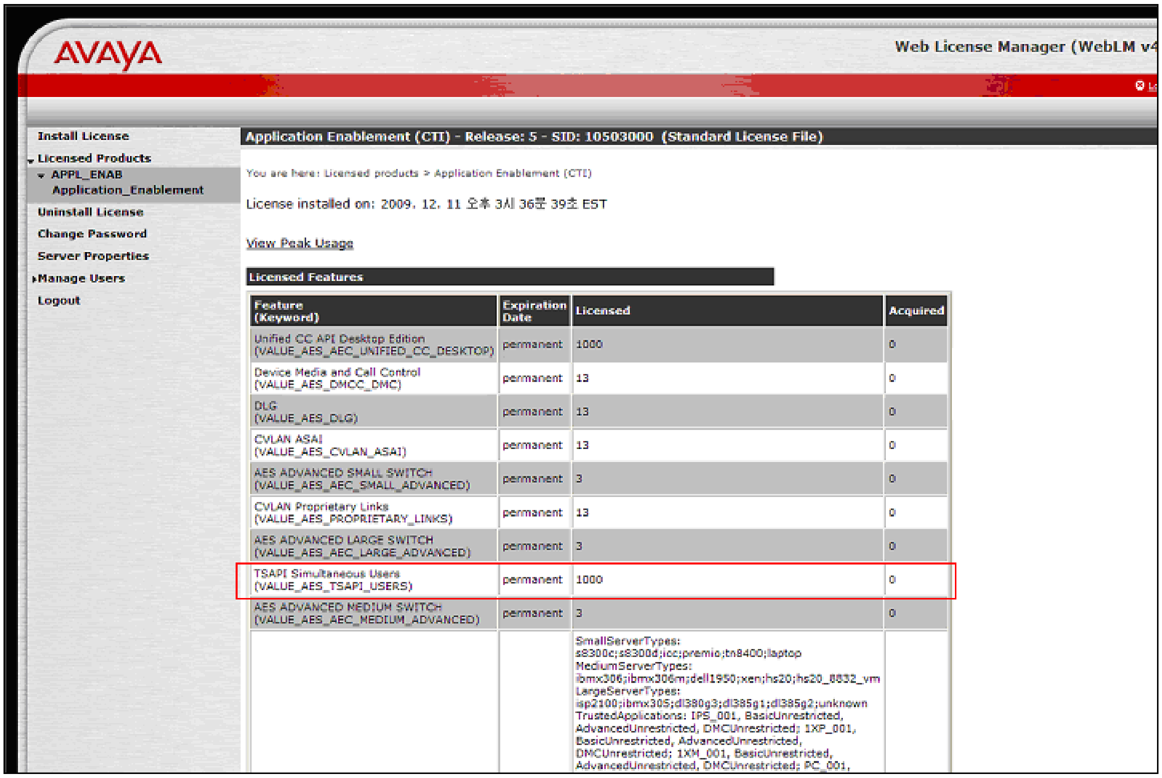
Provide appropriate login credentials to access the Web License Manager page.



On the Install License page, select **License Products** ➔ **Application_Enablement** link from the left pane of the window.



On the Licensed Features page, verify that there are sufficient TSAPI licenses.



Application Enablement (CTI) - Release: 5 - SID: 10503000 (Standard License File)

You are here: Licensed products > Application Enablement (CTI)

License installed on: 2009. 12. 11 오후 3시 36분 39초 EST

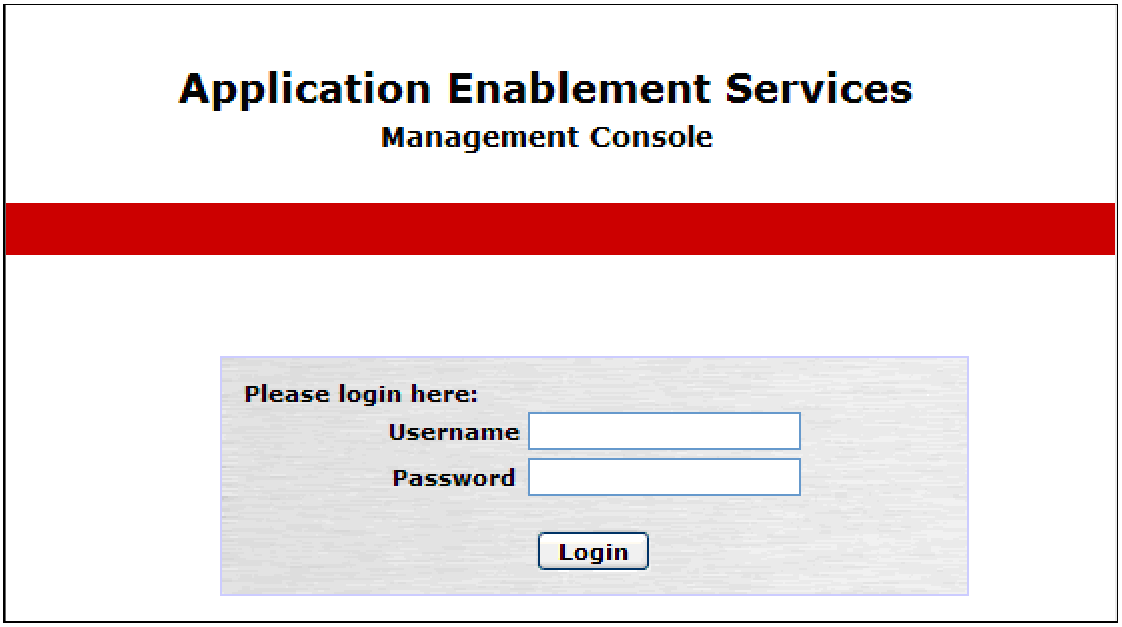
View Peak Usage

Licensed Features

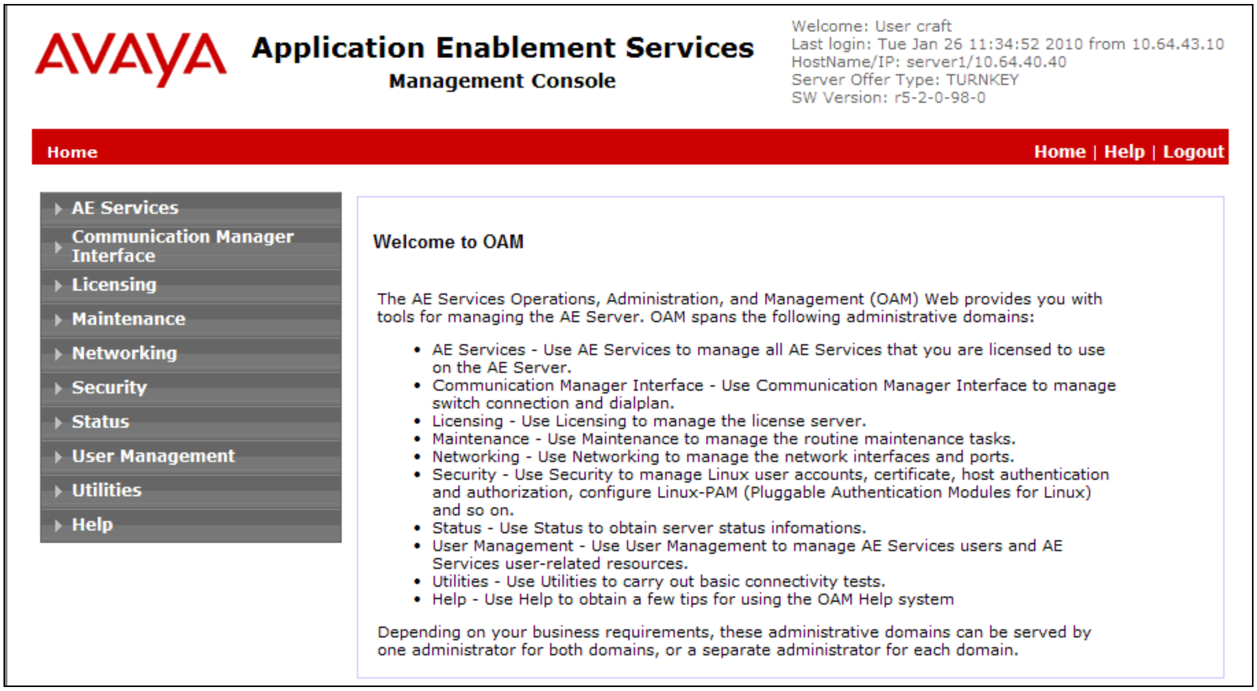
Feature (Keyword)	Expiration Date	Licensed	Acquired
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	permanent	1000	0
Device Media and Call Control (VALUE_AES_DMCC_DMC)	permanent	13	0
DLG (VALUE_AES_DLG)	permanent	13	0
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	permanent	13	0
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	permanent	3	0
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	permanent	13	0
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	permanent	3	0
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	permanent	1000	0
AES ADVANCED MEDIUM SWITCH (VALUE_AES_AEC_MEDIUM_ADVANCED)	permanent	3	0
		SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_8832_vm LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;unknown TrustedApplications: IPS_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XM_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; PC_001,	

5.2. 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 Connection** in the left pane to invoke the Switch Connections page.



Application Enablement Services
Management Console
Welcome: User craft
Last login: Tue Jan 26 11:34:52 2010 from 10.64.43.10
HostName/IP: server1/10.64.40.40
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0
Home
Home | Help | Logout
AE Services
Communication Manager Interface
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Help

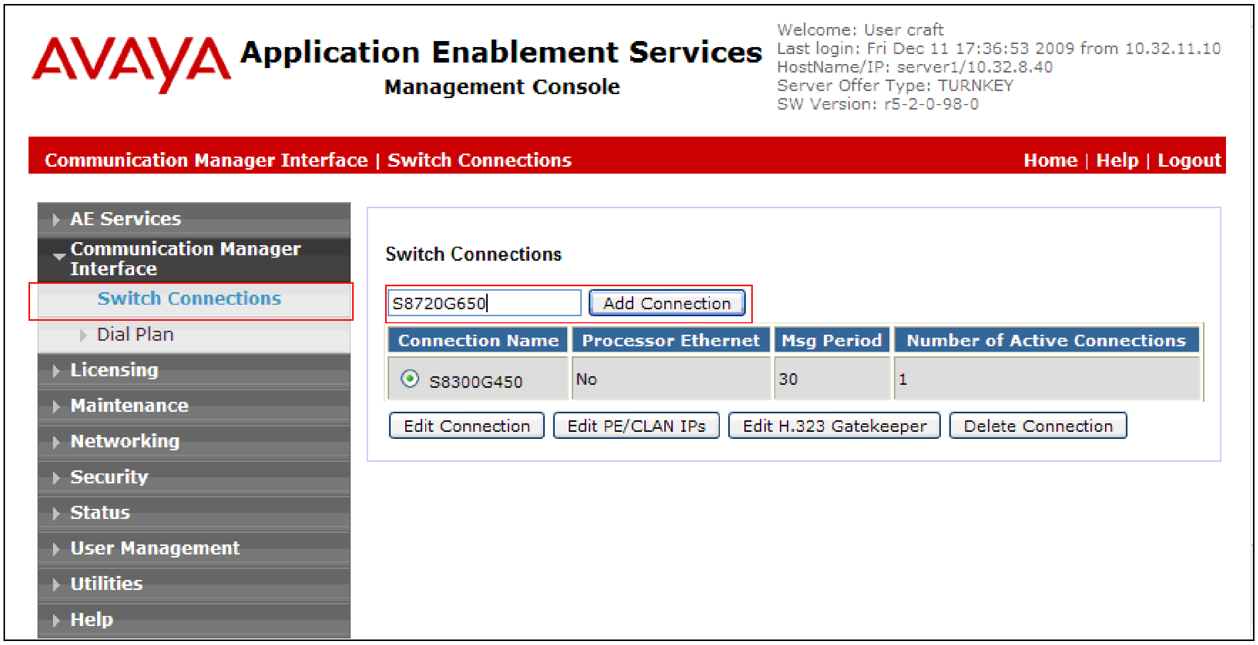
Welcome to OAM

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 infomations.
- 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 both 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**.



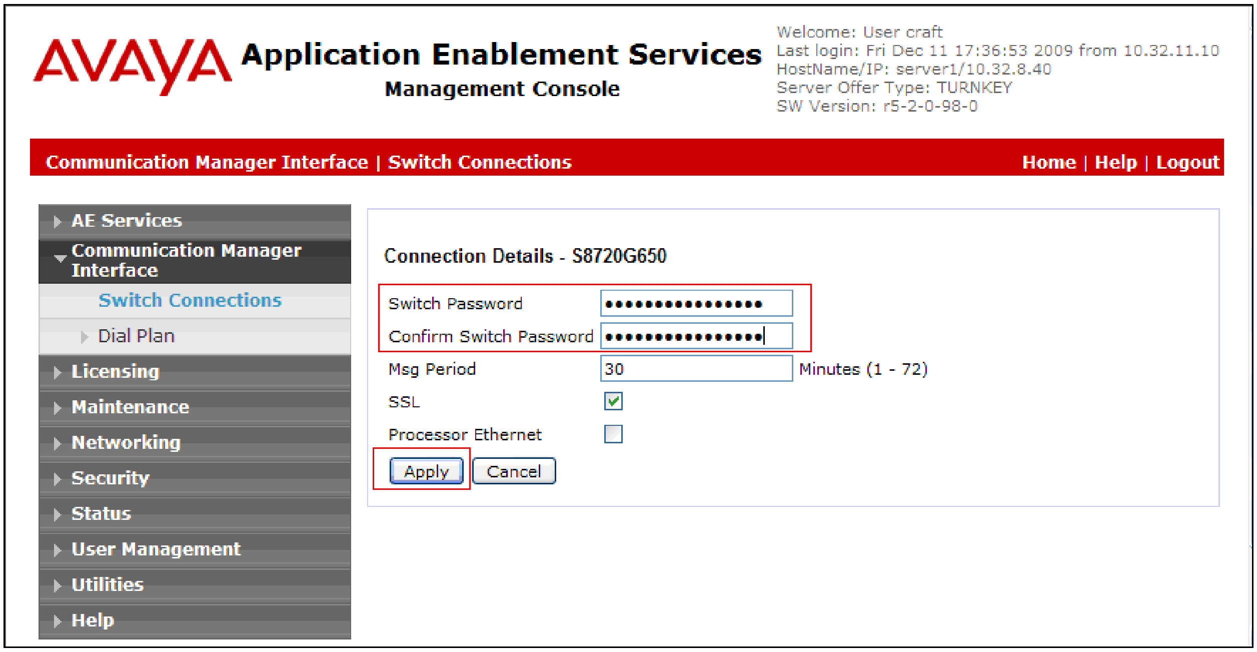
Welcome: User craft
Last login: Fri Dec 11 17:36:53 2009 from 10.32.11.10
HostName/IP: server1/10.32.8.40
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

Switch Connections

S8720G650

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
● S8300G450	No	30	1

The next window that appears prompts for the Switch Connection password. Enter the same password that was administered in Avaya Communication Manager in **Section 4.1**. Click on **Apply**.



Welcome: User craft
Last login: Fri Dec 11 17:36:53 2009 from 10.32.11.10
HostName/IP: server1/10.32.8.40
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

Connection Details - S8720G650

Switch Password	••••••••••••••••
Confirm Switch Password	••••••••••••••••
Msg Period	30 Minutes (1 - 72)
SSL	☑
Processor Ethernet	□

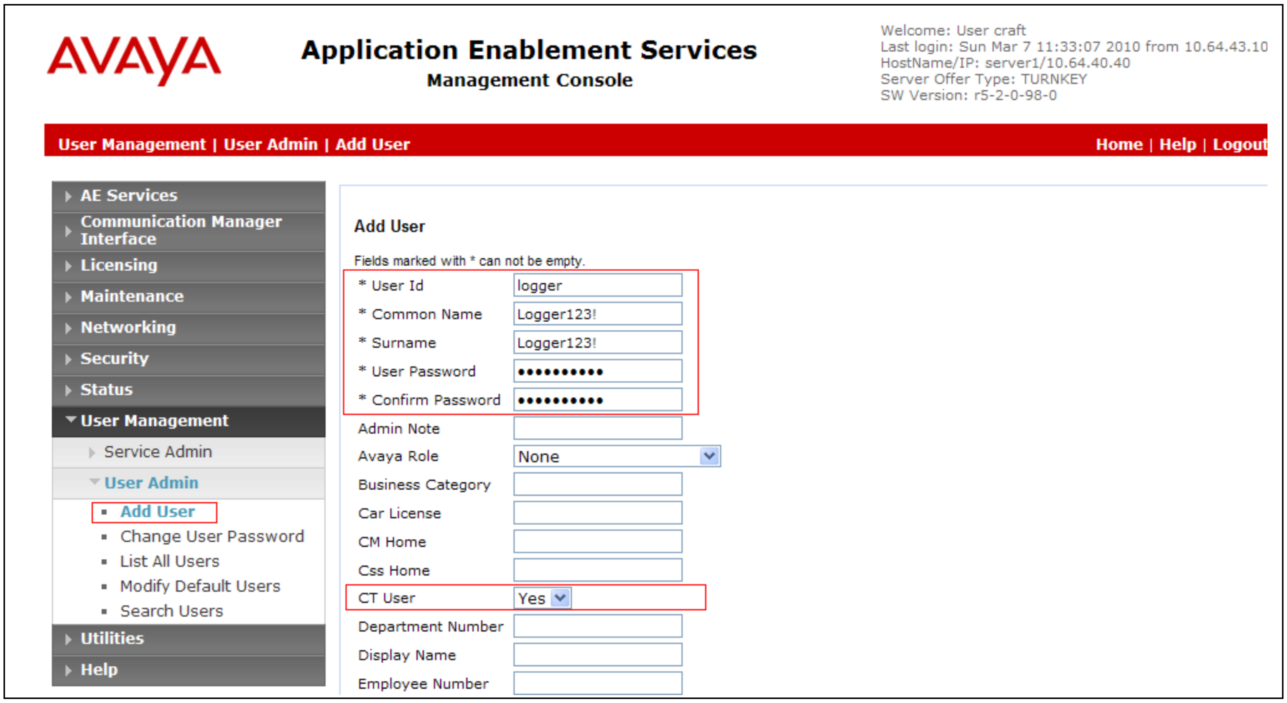
5.3. Configure the CTI Users

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 Call Recording Engine Configuration page in **Section 6**.

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.



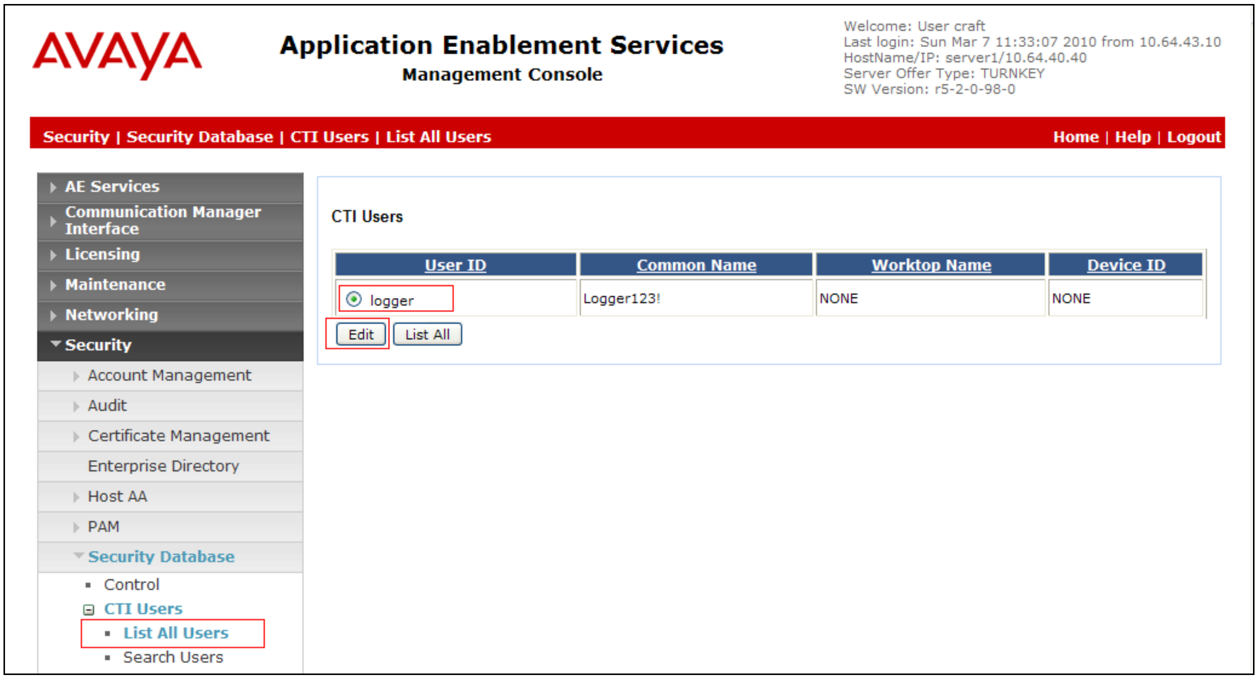
Welcome: User craft
Last login: Sun Mar 7 11:33:07 2010 from 10.64.43.10
HostName/IP: server1/10.64.40.40
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

Add User

Fields marked with * can not be empty.

* User Id	logger
* Common Name	Logger123!
* Surname	Logger123!
* User Password	••••••••••
* Confirm Password	••••••••••
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Css 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.



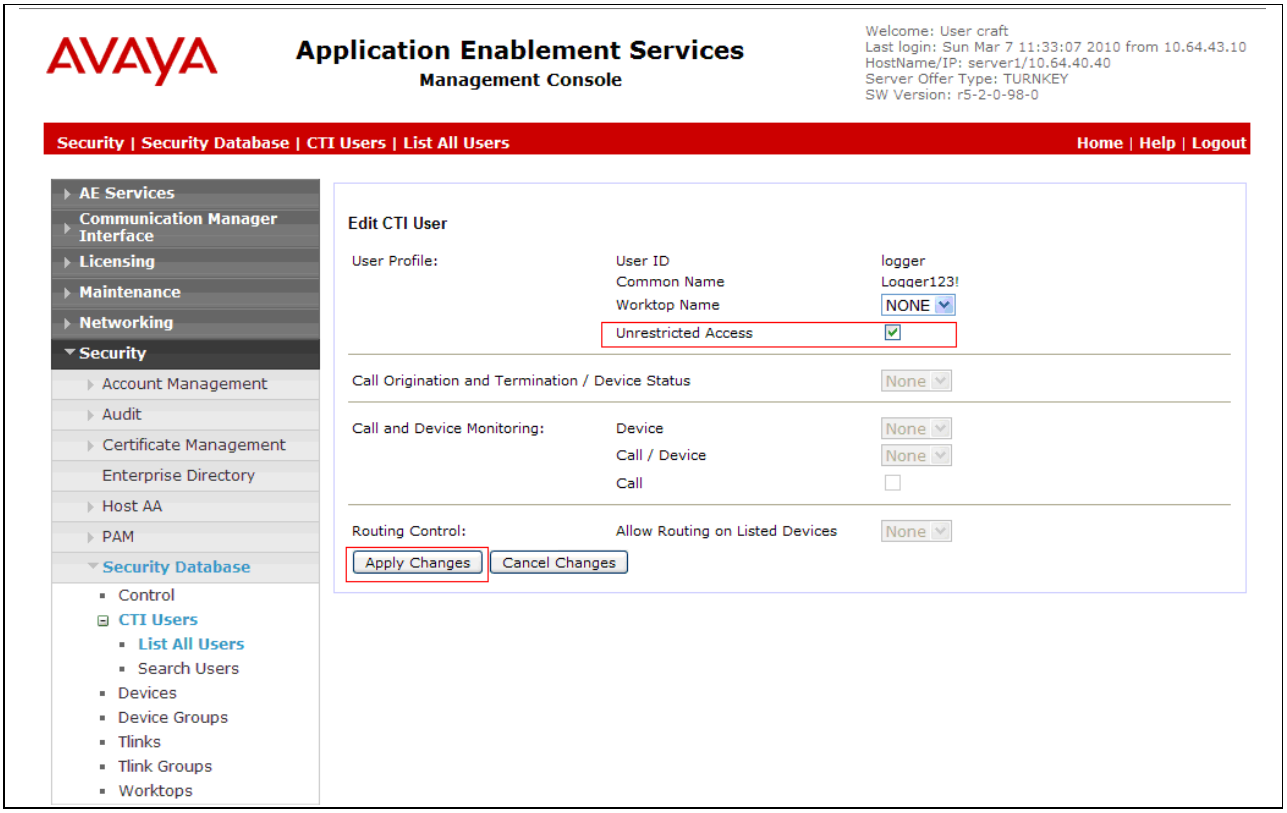
Welcome: User craft
Last login: Sun Mar 7 11:33:07 2010 from 10.64.43.10
HostName/IP: server1/10.64.40.40
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

CTI Users

User ID	Common Name	Worktop Name	Device ID
● logger	Logger123!	NONE	NONE

Edit   List All

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



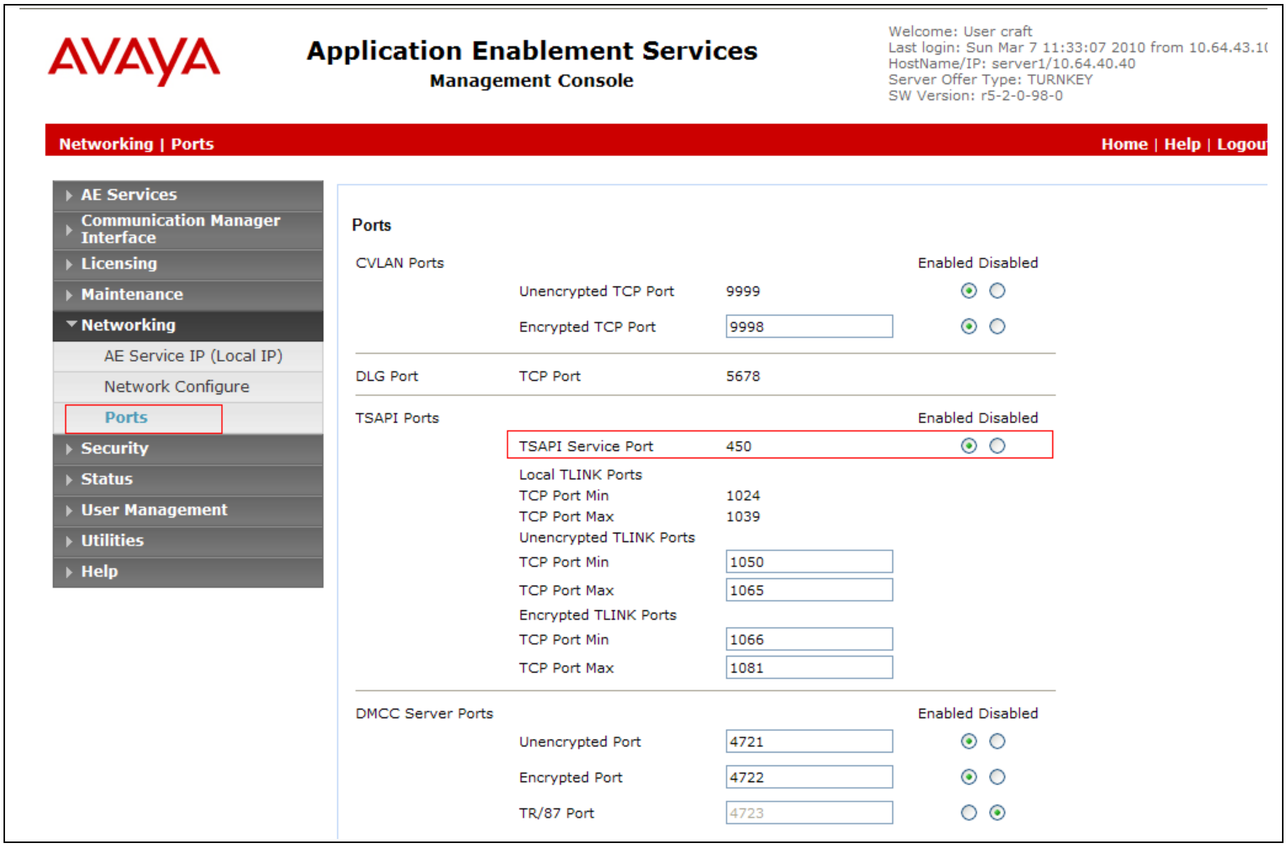
Welcome: User craft
Last login: Sun Mar 7 11:33:07 2010 from 10.64.43.10
HostName/IP: server1/10.64.40.40
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

Edit CTI User

User Profile:	User ID	logger
	Common Name	Logger123!
	Worktop Name	NONE
	Unrestricted Access	☑
Call Origination and Termination / Device Status		None
Call and Device Monitoring:	Device	None
	Call / Device	None
	Call	□
Routing Control:	Allow Routing on Listed Devices	None

5.4. Configure the CTI Port

Navigate to the **Networking → Ports** link, from the left pane of the window, to set the TSAPI port. Make sure the port is enabled. The following screen displays the default port values.



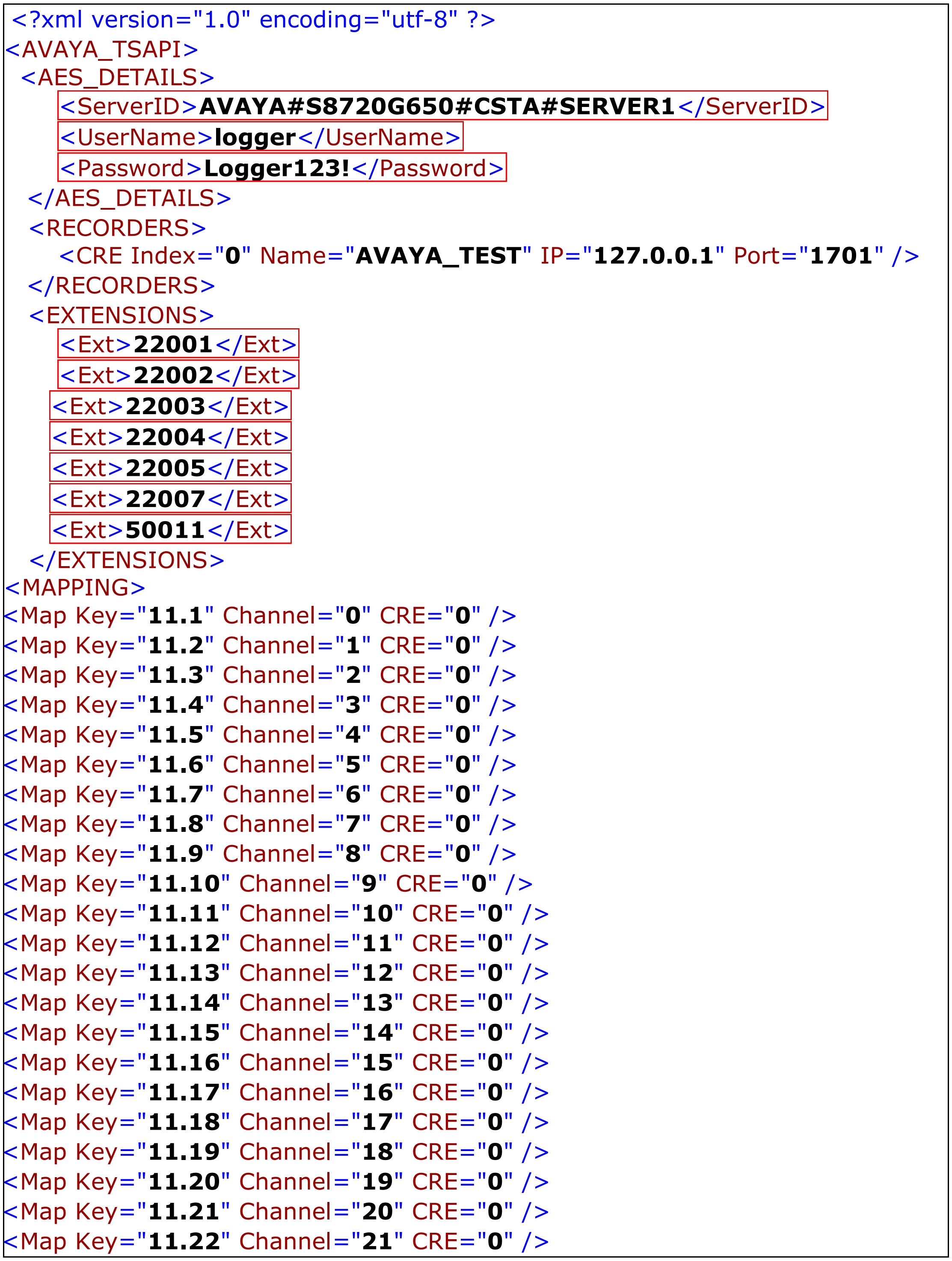
Welcome: User craft
Last login: Sun Mar 7 11:33:07 2010 from 10.64.43.1
HostName/IP: server1/10.64.40.40
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

Ports

			Enabled	Disabled
CVLAN Ports				
	Unencrypted TCP Port	9999	●	○
	Encrypted TCP Port	9998	●	○
DLG Port	TCP Port	5678		
TSAPI Ports				
	TSAPI Service Port	450	●	○
	Local TLINK Ports			
	TCP Port Min	1024		
	TCP Port Max	1039		
	Unencrypted TLINK Ports			
	TCP Port Min	1050		
	TCP Port Max	1065		
	Encrypted TLINK Ports			
	TCP Port Min	1066		
	TCP Port Max	1081		
DMCC Server Ports				
	Unencrypted Port	4721	●	○
	Encrypted Port	4722	●	○
	TR/87 Port	4723	○	●

6. Configure VirtualLogger Call Recording Engine

VirtualLogger, installs, configures, and customizes the Call Recording Engine application for their end customers. Include in this section is the CTI configuration file which interfaces with Application Enablement Services.



```xml
 <?xml version="1.0" encoding="utf-8" ?>
<AVAYA_TSAPI>
  <AES_DETAILS>
      <ServerID>AVAYA#S8720G650#CSTA#SERVER1</ServerID>
      <UserName>logger</UserName>
      <Password>Logger123!</Password>
   </AES_DETAILS>
   <RECORDERS>
      <CRE Index="0" Name="AVAYA_TEST" IP="127.0.0.1" Port="1701" />
   </RECORDERS>
   <EXTENSIONS>
      <Ext>22001</Ext>
      <Ext>22002</Ext>
     <Ext>22003</Ext>
     <Ext>22004</Ext>
     <Ext>22005</Ext>
     <Ext>22007</Ext>
     <Ext>50011</Ext>
   </EXTENSIONS>
<MAPPING>
<Map Key="11.1" Channel="0" CRE="0" />
<Map Key="11.2" Channel="1" CRE="0" />
<Map Key="11.3" Channel="2" CRE="0" />
<Map Key="11.4" Channel="3" CRE="0" />
<Map Key="11.5" Channel="4" CRE="0" />
<Map Key="11.6" Channel="5" CRE="0" />
<Map Key="11.7" Channel="6" CRE="0" />
<Map Key="11.8" Channel="7" CRE="0" />
<Map Key="11.9" Channel="8" CRE="0" />
<Map Key="11.10" Channel="9" CRE="0" />
<Map Key="11.11" Channel="10" CRE="0" />
<Map Key="11.12" Channel="11" CRE="0" />
<Map Key="11.13" Channel="12" CRE="0" />
<Map Key="11.14" Channel="13" CRE="0" />
<Map Key="11.15" Channel="14" CRE="0" />
<Map Key="11.16" Channel="15" CRE="0" />
<Map Key="11.17" Channel="16" CRE="0" />
<Map Key="11.18" Channel="17" CRE="0" />
<Map Key="11.19" Channel="18" CRE="0" />
<Map Key="11.20" Channel="19" CRE="0" />
<Map Key="11.21" Channel="20" CRE="0" />
<Map Key="11.22" Channel="21" CRE="0" />
```

```
<Map Key="11.23" Channel="22" CRE="0" />
<Map Key="11.24" Channel="23" CRE="0" />
 </MAPPING>
 </AVAYA_TSAPI>
```

7. 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 through a trunk. Those trunk calls were monitored using TSAPI, and calls were recorded using VirtualLogger CRE. During the test, recorded calls were verified. For feature testing, the types of calls included inbound and outbound trunk calls, transferred calls, bridged calls, and conferenced calls.

For serviceability testing, VirtualLogger CRE was able to record the monitored stations after restarts of the VirtualLogger CRE. In addition, after VirtualLogger lost network connectivity to the Application Enablement Services server, it was able to recover the existing session to the Application Enablement Services server when network connectivity was restored before the session expired. When CTI link between communication Manager and the Application Enablement Service server goes down and back up, the service has to be restarted from VirtualLogger CRE.

8. Verification Steps

8.1. From Communication Manager

The following steps may be used to verify the configuration:
Verify the status of the administered AES link by using the **status aesvcs link** command.

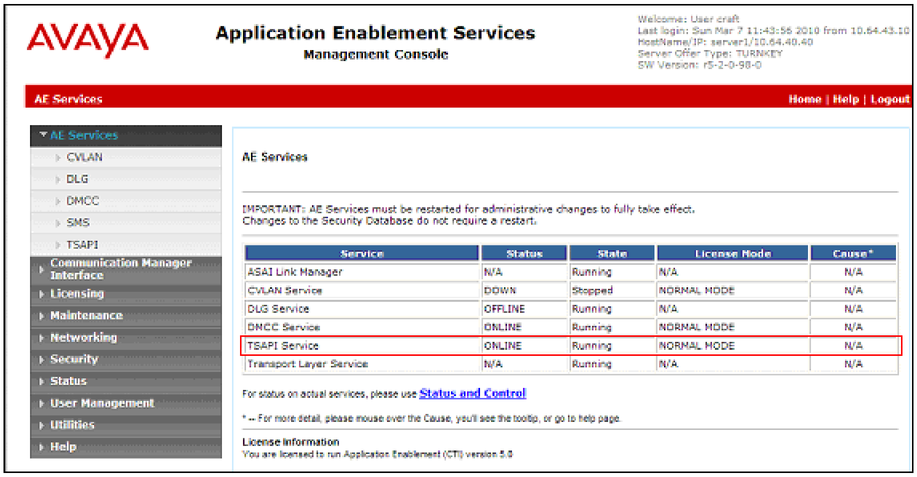
```
status aesvcs link

                            AE SERVICES LINK STATUS

Srvr/  AE Services     Remote IP         Remote  Local Node       Msgs     Msgs
Link   Server                            Port                     Sent     Rcvd

01/01  server1         10.64.43.40       36538   CLAN-AES         17       18
```

Verify the status of the administered TSAPI CTI link by using the **status aesvcs cti-link** command.

```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

CTI   Version  Mnt   AE Services      Service       Msgs     Msgs
Link           Busy  Server           State         Sent     Rcvd

4     4        no    server1          established   15       15
```

8.2. From Application Enablement Services

Verify the status of the TSAPI Services by selecting AE Services from the left pane.



Welcome: User craft
Last login: Sun Mar 7 11:43:56 2010 from 10.64.43.10
HostName/IP: server1/10.64.40.40
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

AE Services

IMPORTANT: AE Services must be restarted for administrative changes to fully take effect.
Changes to the Security Database do not require a restart.

Service	Status	State	License Mode	Cause*
ASAI Link Manager	N/A	Running	N/A	N/A
CVLAN Service	DOWN	Stopped	NORMAL MODE	N/A
DLG Service	OFFLINE	Running	N/A	N/A
DMCC Service	ONLINE	Running	NORMAL MODE	N/A
TSAPI Service	ONLINE	Running	NORMAL MODE	N/A
Transport Layer Service	N/A	Running	N/A	N/A

For status on actual services, please use Status and Control

* -- For more detail, please mouse over the Cause, you'll see the tooltip, or go to help page.

License Information
You are licensed to run Application Enablement (CTI) version 5.0

9. Conclusion

These Application Notes described a compliance-tested configuration comprised of Communication Manager, Application Enablement Services, Avaya IP and Digital Telephones, and the VirtualLogger Call Recording Engine application. VirtualLogger Call Recording Engine was able to record calls that came through the trunk, and collected call events from Application Enablement Services using TSAPI.

10. Additional References

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

[1] *Administering Avaya Aura™ Communication Manager*, Issue 5.0, May 2009, Document Number 03-300509

[2] *Avaya Aura™ Application Enablement Services Administration and Maintenance Guide*, Release 5.2, Issue 11, November 2009, Document Number 02-300357

Product information for VirtualLogger products may be found at http://www.virtualloggersoft.com/

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.