Avaya Solution & Interoperability Test Lab

Application Notes for CTI Group SmartRecord 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 CTI Group SmartRecord application.

CTI Group SmartRecord, a hosted call recording system, is a carrier-class call recording system designed specifically for telecommunications companies and service providers that provide hosted IP telephony services to their end user customers.

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 CTI Group SmartRecord.

CTI Group SmartRecord, a hosted call recording system, is a carrier-class call recording system designed specifically for telecommunications companies and service providers that provide hosted IP telephony services to their end user customers.

The SmartRecord system has the following basic components (additional components may be optionally provided based on customer specific needs):

- **Web Portal –** This is an ASP .NET Framework website, hosted within Microsoft Windows Internet Information Systems (IIS 7.0) available over the HTTP Protocol (optionally HTTP/S). This portal is built on the .NET Framework distributed with Windows Server 2008. This portal also houses SmartRecord APIs, web services for archival services, and web services for other end-user desktop utilities. On the preferred hardware platforms, the SmartRecord system can handle up to 200 web transactions per second.

- **FTP Server –** This is a custom FTP server developed by CTI Group. This FTP server provides passive FTP support for downloading recorded calls.

- **Database Services** – CTI Group SmartRecord leverages the Microsoft SQL Server 2008 database platform [Express, Workgroup, Standard, or Enterprise editions with SQL Server Advanced Services (Full-Text Search Capabilities)]. This underlying database platform houses the SmartRecord database, which contains the tenancy structure, call records, and user customizations. The actual audio files associated with the recordings are not housed within this database. Licensing for the SmartRecord system is ultimately tied to the created and deployed database housed within SQL Server 2008.

- **Queue Service Bus** – CTI Group SmartRecord has a service queue for incoming call events, alerts, and other event driven infrastructure. This queue service is built on the Microsoft Message Queuing Platform available as a part of Windows Server 2008.

- **Utilities and Scheduled Tasks –** A number of automated functions run on the platform to sweep calls, perform database optimizations, and further drive automated efficiency into the SmartRecord platform. These scheduled tasks are executed as Windows scheduled tasks.

- **Recorder –** CTI Group SmartRecord records phone conversations when a phone number or extension belonging to a SmartRecord Group is marked as a recordable number. This application can run on either the Windows Server 2008 operating system or RedHat Enterprise Linux 5 operating system.

- **Media Server –** For most implementations, this is the most fundamental scalability unit of the SmartRecord platform. The Media Server performs the actual recording of audio conversations presented to it in the form of real-time protocol (digital audio over RTP). It natively supports the G.711 u-Law and a-Law, and G.729 CODECs. This media server is written in the Java programming language and depends on JRE 1.5 Update 10 and runs on the Windows Server 2008 platform or RedHat Enterprise Linux 5.

- **Temporary Storage –** The CTI Group solution initially writes encoded audio from the Media Server to a temporary storage facility. The spindle speed of this temporary storage is exceedingly important. Ideally, CTI Group prefers if temporary storage is on disk spindles with rotational speeds exceeding 10,000 revolutions per minute (RPM).

- **Permanent Storage** – The CTI Group solution natively supports any networked (SAN/NAS) storage platform accessible from the Windows Server 2008 operating system. Preferably this storage is Windows Hardware Quality Lab (WHQL) certified. The CTI Group solution also has native support for the Windows Distributed File System (DFS) and RedHat Global File System (GFS).

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 CTI Group SmartRecord, Application Enablement Services, and Communication Manager.

1.2. Support

Technical support for the CTI Group SmartRecord solution can be obtained by contacting CTI Group:

- URL – http://www.ctigroup.com/index.php?section=616
- Phone – (866) 845-2991

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 an Avaya G650 Media Gateway. CTI Group SmartRecord was located remotely, and connected to Application Enablement Services via a firewall through internet. 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 reference **[2]**.

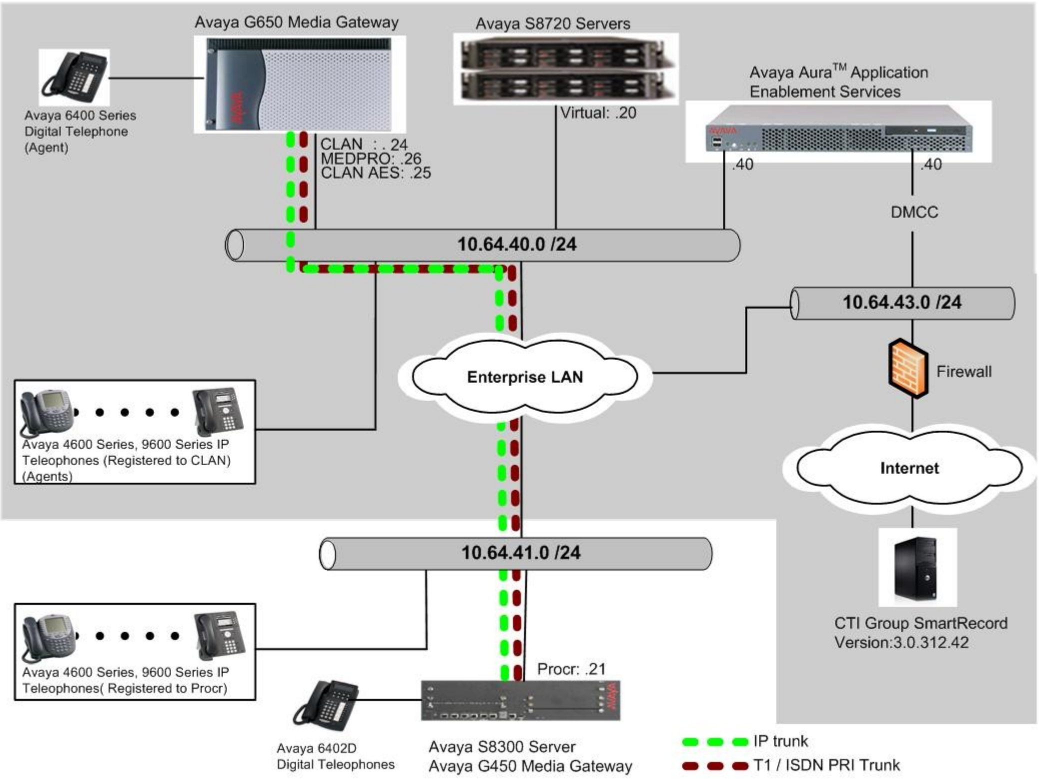

Avaya G650 Media Gateway
Avaya S8720 Servers
Avaya Aura™ Application Enablement Services
Avaya 6400 Series Digital Telephone (Agent)
CLAN : . 24
MEDPRO: .26
CLAN AES: .25
Virtual: .20
.40
.40
DMCC
10.64.40.0 /24
10.64.43.0 /24
Enterprise LAN
Firewall
Internet
Avaya 4600 Series, 9600 Series IP Teleophones (Registered to CLAN) (Agents)
10.64.41.0 /24
Avaya 4600 Series, 9600 Series IP Teleophones(Registered to Procr)
Procr: .21
CTI Group SmartRecord Version:3.0.312.42
Avaya 6402D Digital Telephones
Avaya S8300 Server
Avaya G450 Media Gateway
IP trunk
T1 / ISDN PRI Trunk

Figure 1: CTI Group SmartRecord 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 with Avaya G650 Media Gateway	Avaya Aura™ Communication Manager 5.2.1 (R015x.02.1.016.4) with the patch (02.1.016.4-17963)
Avaya Aura™ Application Enablement Services Server	5.2.2 (r5-2-2-105-0)
Avaya S8300 Server with Avaya G450 Media Gateway	Avaya Aura™ Communication Manager 5.2.1 (R015x.02.1.016.4) with the patch (02.1.016.4-17963)
Avaya 4625SW IP Telephone (H.323)	2.9
Avaya 9600 Series IP Telephones	
9620 (H.323) 9630 (H.323) 9650 (H.323) 9670 (H.323)	3.1 3.1 3.1 3.1
Avaya 6408D+ Digital Telephone	-
CTI Group SmartRecord on Windows 2008 Server R1	3.0.312.42

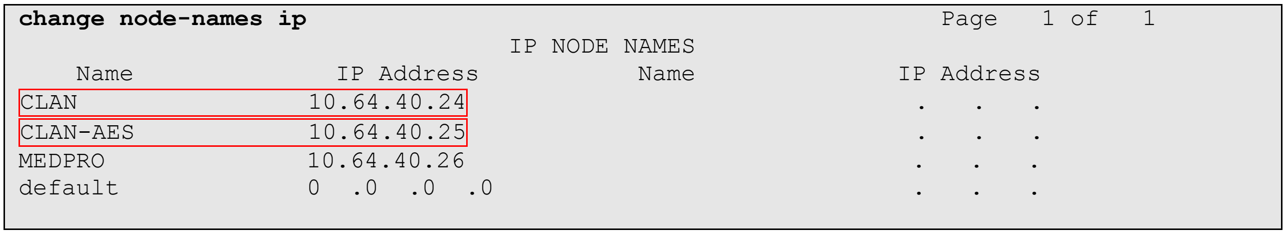
4. Configure Avaya Aura^{TM} Communication Manager

This section describes the procedure for setting up the following topics:

- IP Services
- Feature Access Codes
- Abbreviated Dialing
- Hunt Group
- Agent ID
- Vector
- VDN
- Monitored/recorded Telephones
- Recording Telephones.

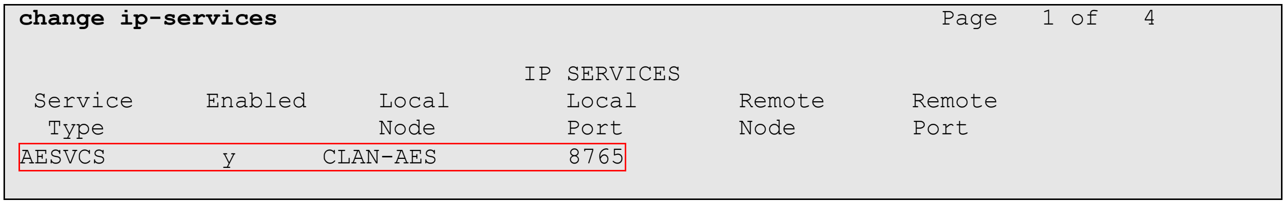
4.1. Configure IP Services

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.



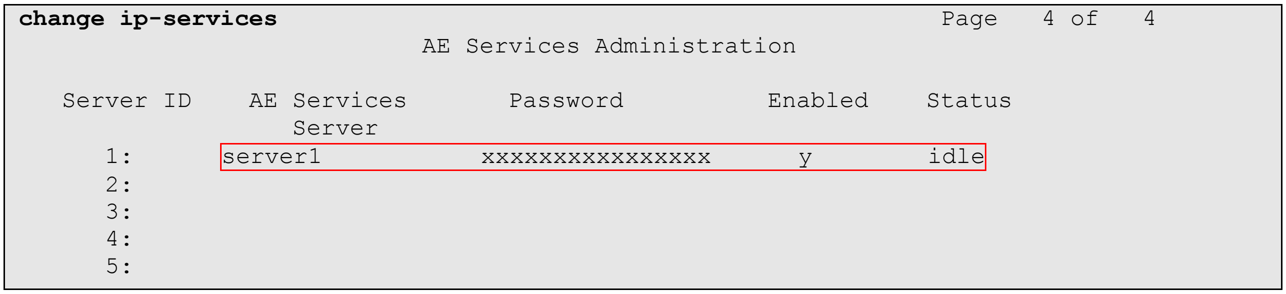
```
change node-names ip                                          Page   1 of   1
                                  IP NODE NAMES
    Name              IP Address          Name               IP Address
CLAN                10.64.40.24                                .   .   .
CLAN-AES            10.64.40.25                                .   .   .
MEDPRO              10.64.40.26                                .   .   .
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 5.1**.

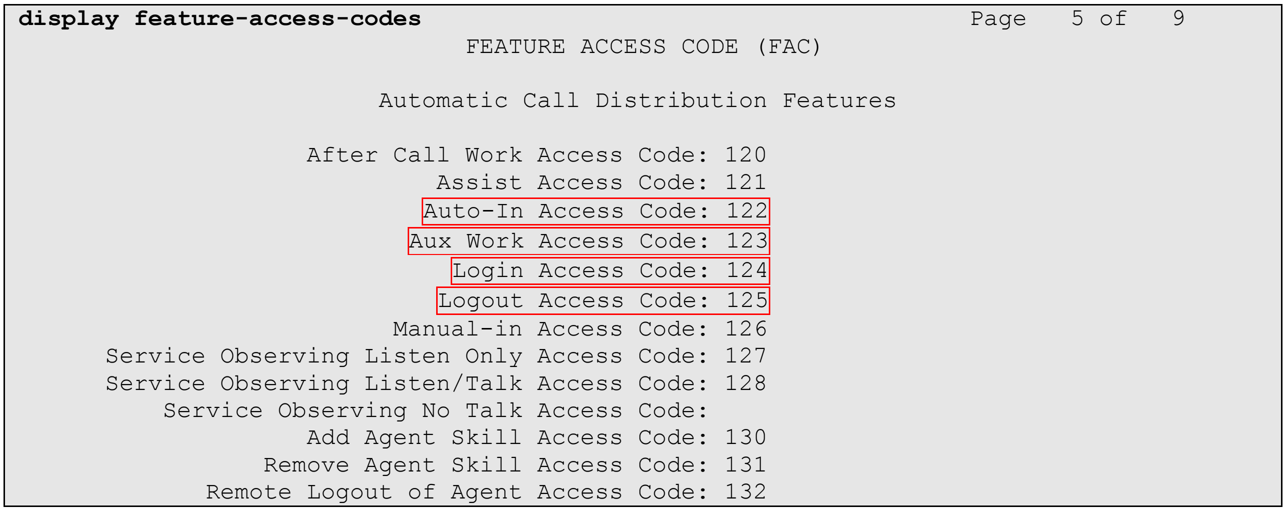


```
change ip-services                                          Page   4 of   4
                            AE Services Administration

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

4.2. Configure 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:

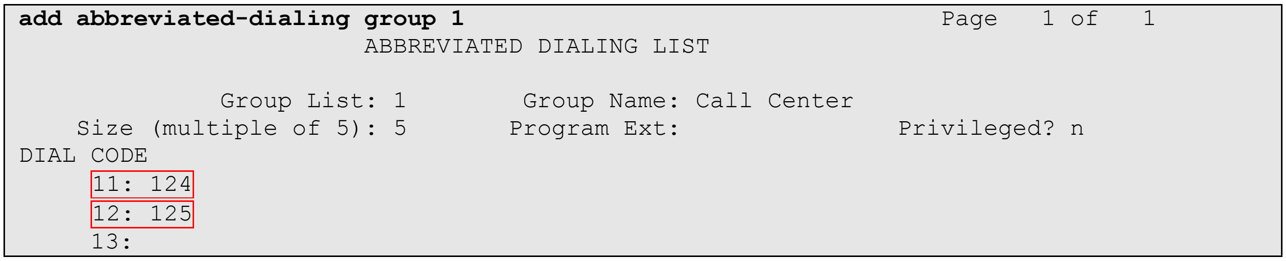
- Auto-In Access Code
- Aux Work Access Code
- Login Access Code
- Logout Access Code



```
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
```

4.3. 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 4.2**

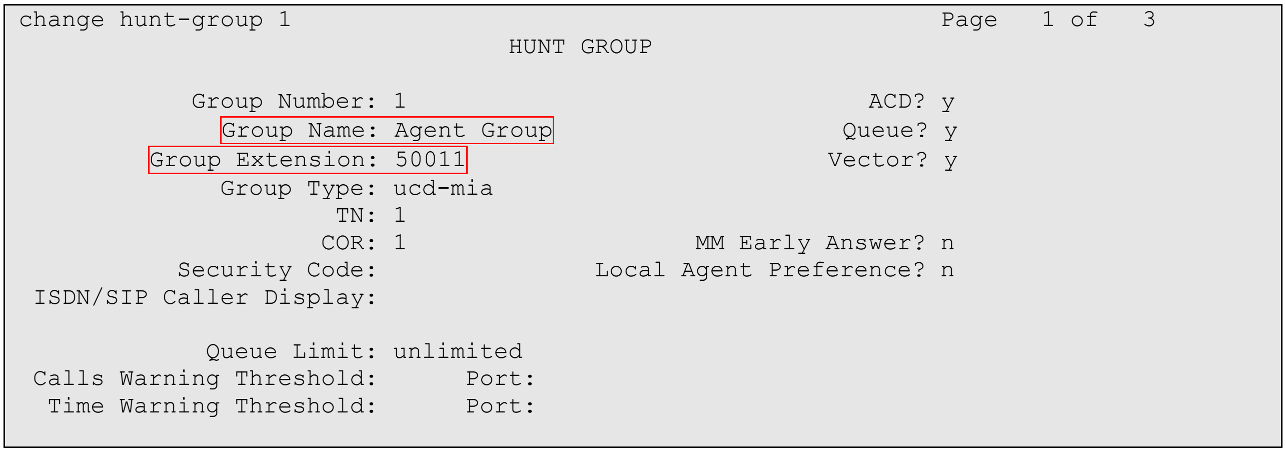


```
add abbreviated-dialing group 1                             Page   1 of   1
                        ABBREVIATED DIALING LIST

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

4.4. Configure Hunt Group

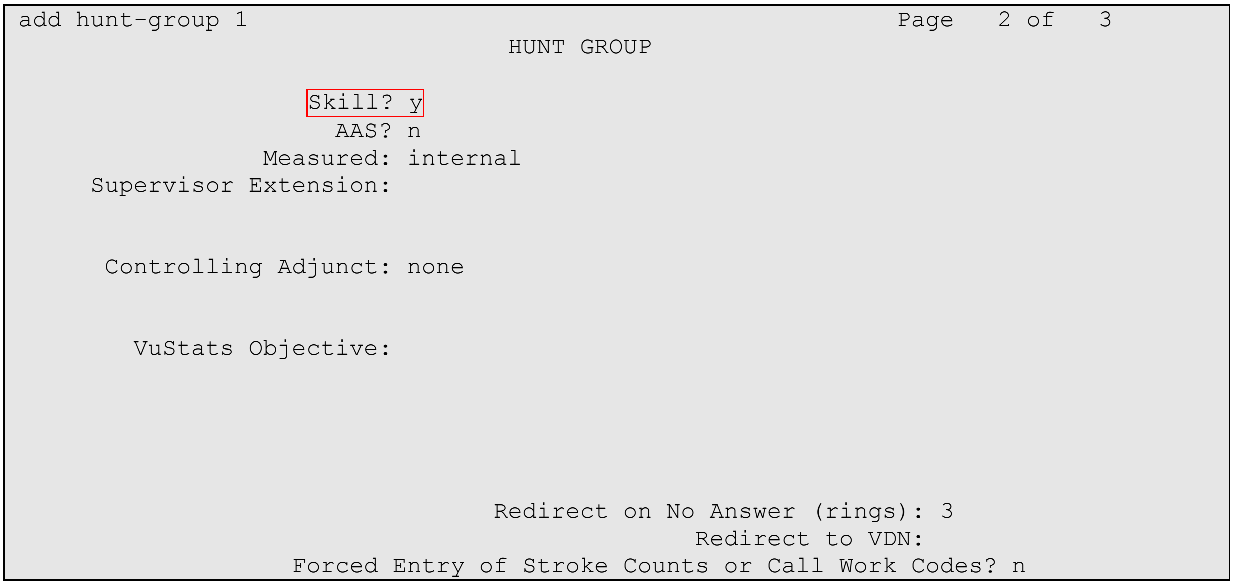
Enter the **add hunt-group n** command; where **n** is an unused hunt group number. On **Page 1**, assign a descriptive Group Name and Group Extension valid in the provisioned dial plan.

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: 50011                           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:
```

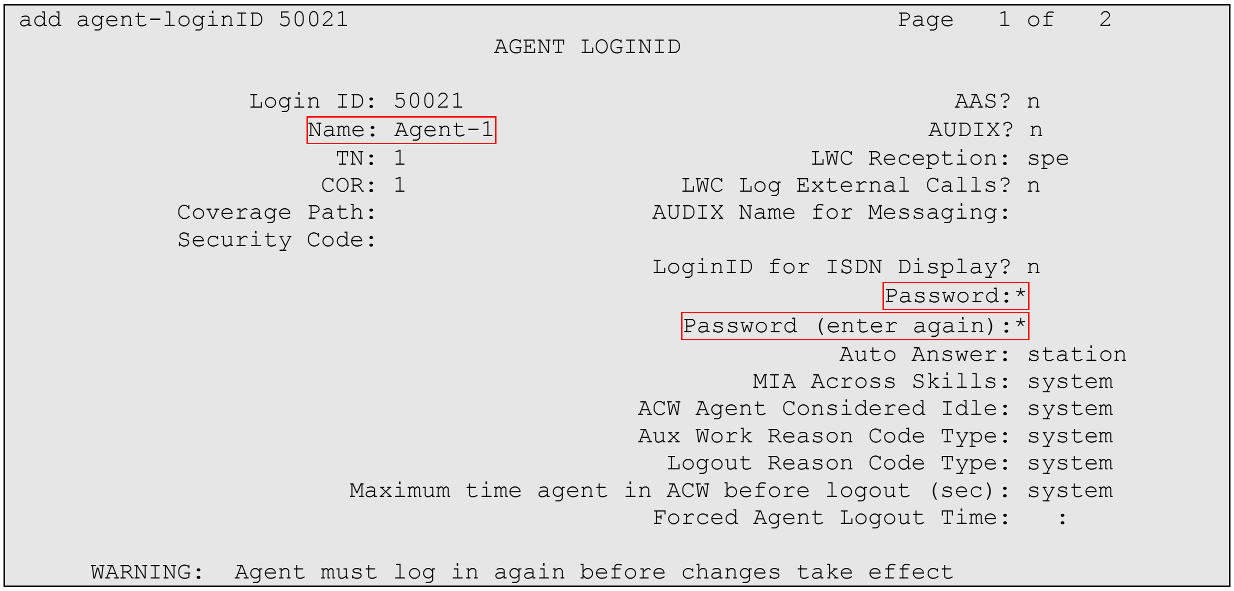
On **Page 2**, set the Skill field to **y**, this means that agent membership in the hunt group is based on skills, rather than a pre-programmed assignment to the hunt group.



```
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
```

4.5. Configure Agent ID

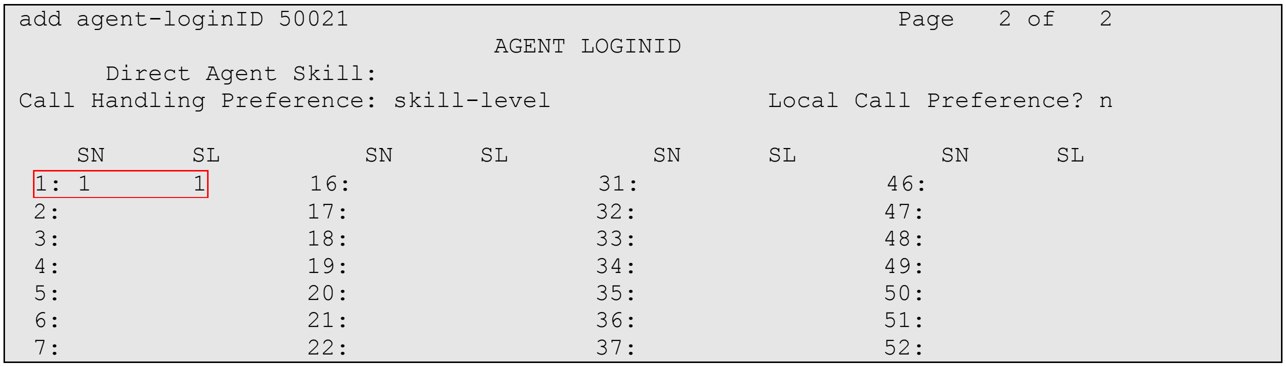
Enter the **add agent-loginID p** command, where **p** is a valid extension in the provisioned dial plan. On **Page 1**, enter a descriptive name, and password.



```
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.

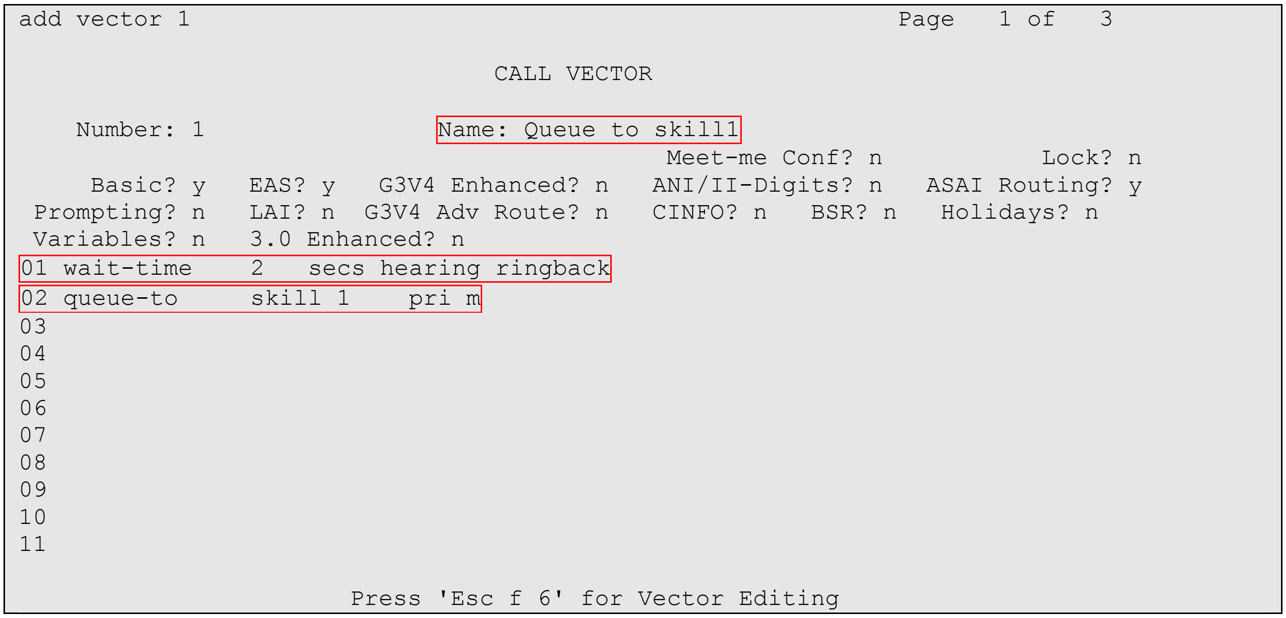
Repeat steps in this section as necessary to configure additional agent extensions.



```
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:
```

4.6. Configure Vector

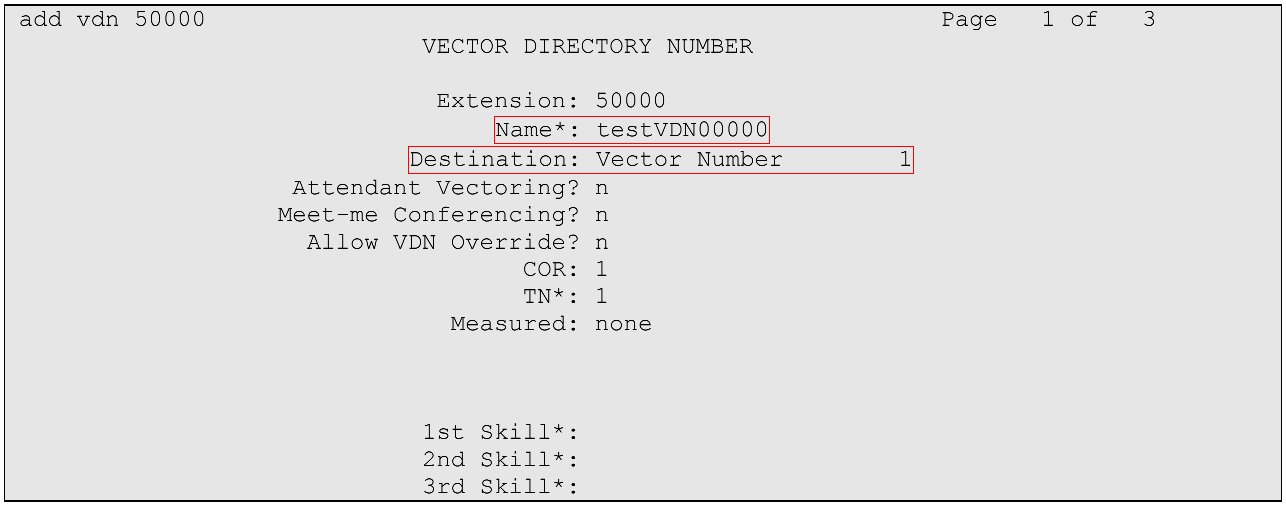
Enter the **add vector q** command, where **q** is an unused vector number. Enter a descriptive name, and administer the vector to deliver calls to the hunt/skill group number. Agents that are logged into the hunt/skill group will be able to answer calls queued to the hunt/skill group.



```
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
```

4.7. Configure VDN

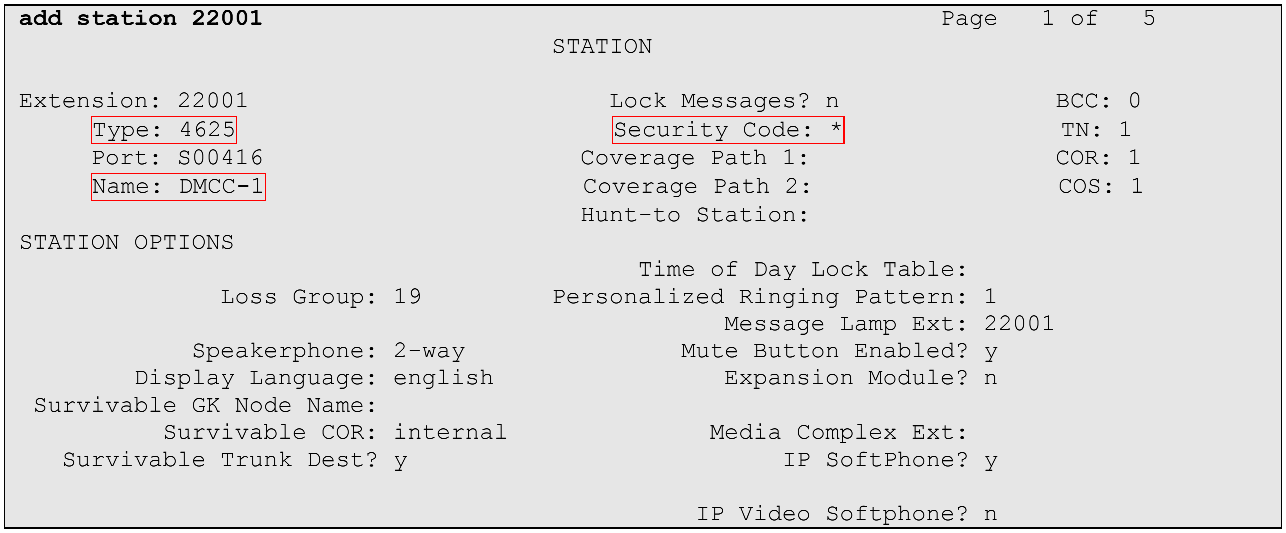
Enter the **add vdn r** command, where **r** is an extension valid in the provisioned dial plan. Specify a descriptive name for the VDN and the Vector Number configured in the previous step. In the example below, incoming calls to extension 50000 corresponds to testVDN00000, which in turn will invoke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

4.8. Configure Monitored / Recorded Telephones

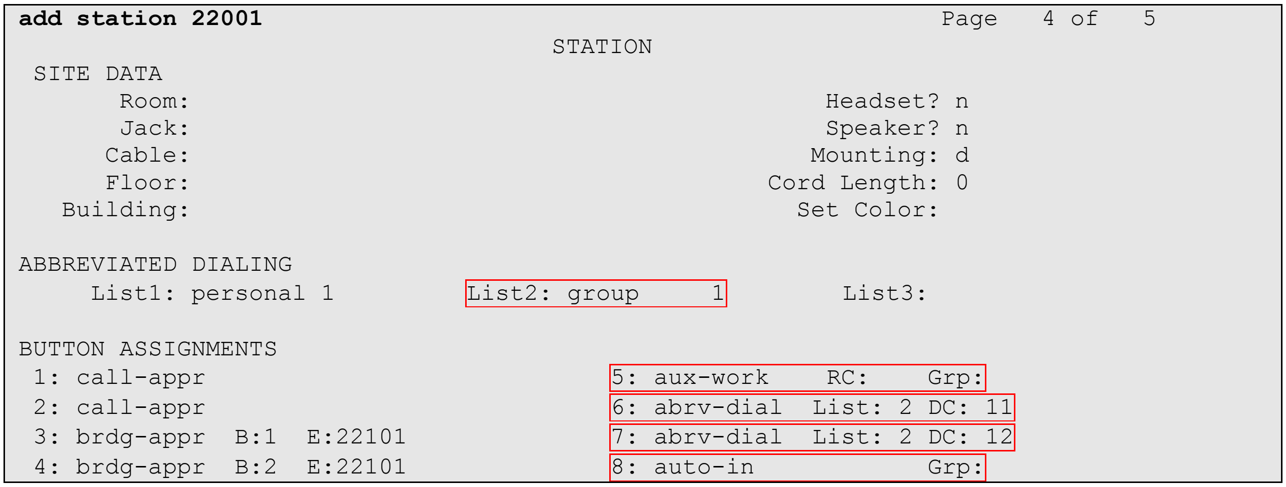
Enter the **add station r** command, where **r** is the extension of a registered, physical Avaya IP or Digital telephone. On **Page 1** of the STATION form, enter a phone Type, descriptive name, Security Code to allow the physical station to be monitored / recorded by the SmartRecord application. During the compliance test, stations 22001-22009 were utilized.



```
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 4.3**. 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 **List** for ACD Login and Logout, respectively.
- auto-in (On Page 5)

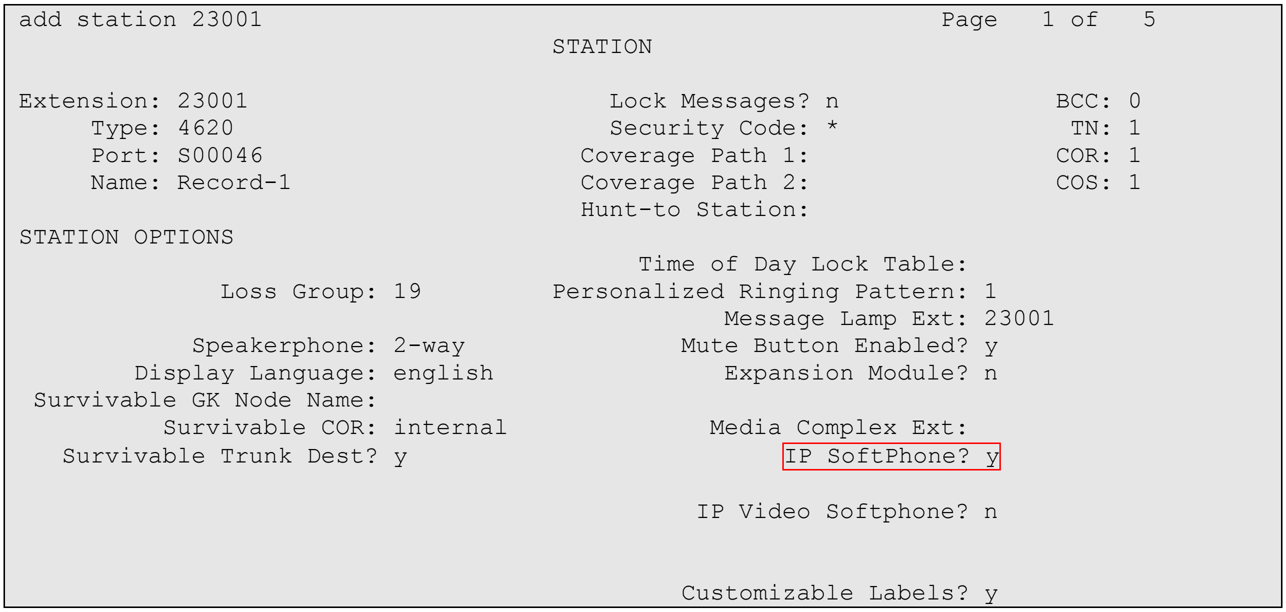


```
add station 22001                                               Page   4 of    5
                                     STATION
 SITE DATA
      Room:                                                Headset? n
      Jack:                                                Speaker? n
     Cable:                                               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: auto-in            Grp:
```

Repeat the instructions provided in this section for each physical station that is to be monitored by a CTI Group SmartRecord.

4.9. Configure DMCC Recording Telephones for Single Step Conference

Enter the **add station r** command, where **r** is the extension valid in the provisioned dial plan. On **Page 1** of the STATION form, set the IP SoftPhone field to **y**. During the compliance test, stations 23001-23023 were utilized as recording stations.

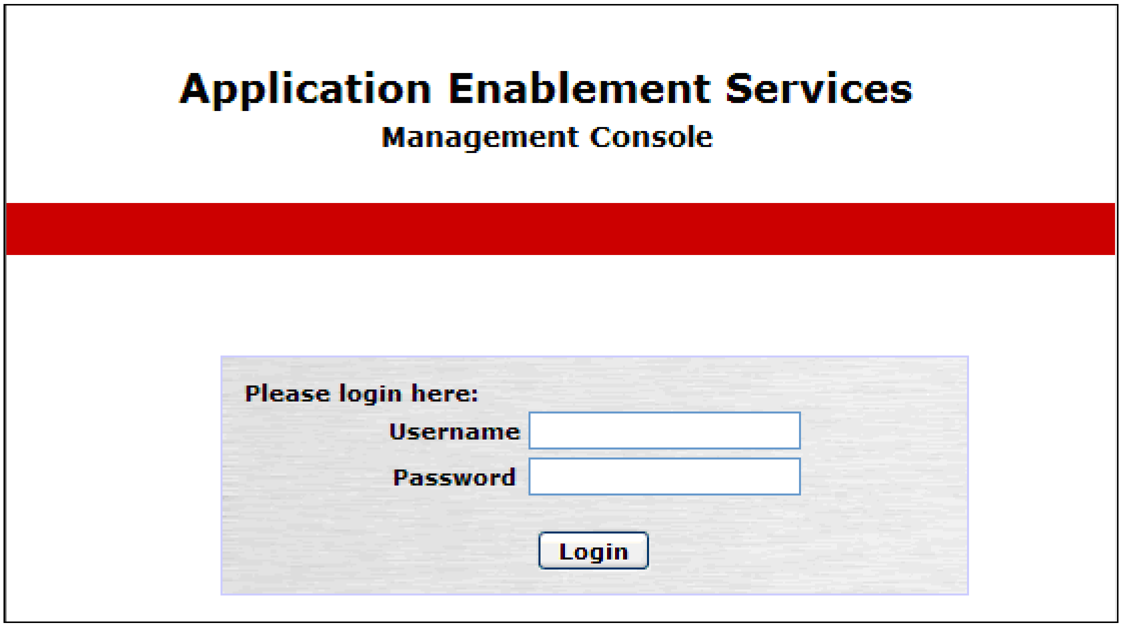


```
add station 23001                                               Page   1 of   5
                                     STATION

Extension: 23001                         Lock Messages? n               BCC: 0
     Type: 4620                          Security Code: *                TN: 1
     Port: S00046                      Coverage Path 1:                 COR: 1
     Name: Record-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: 23001
            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


                                              Customizable Labels? y
```

5. Configure Avaya Application Enablement Services

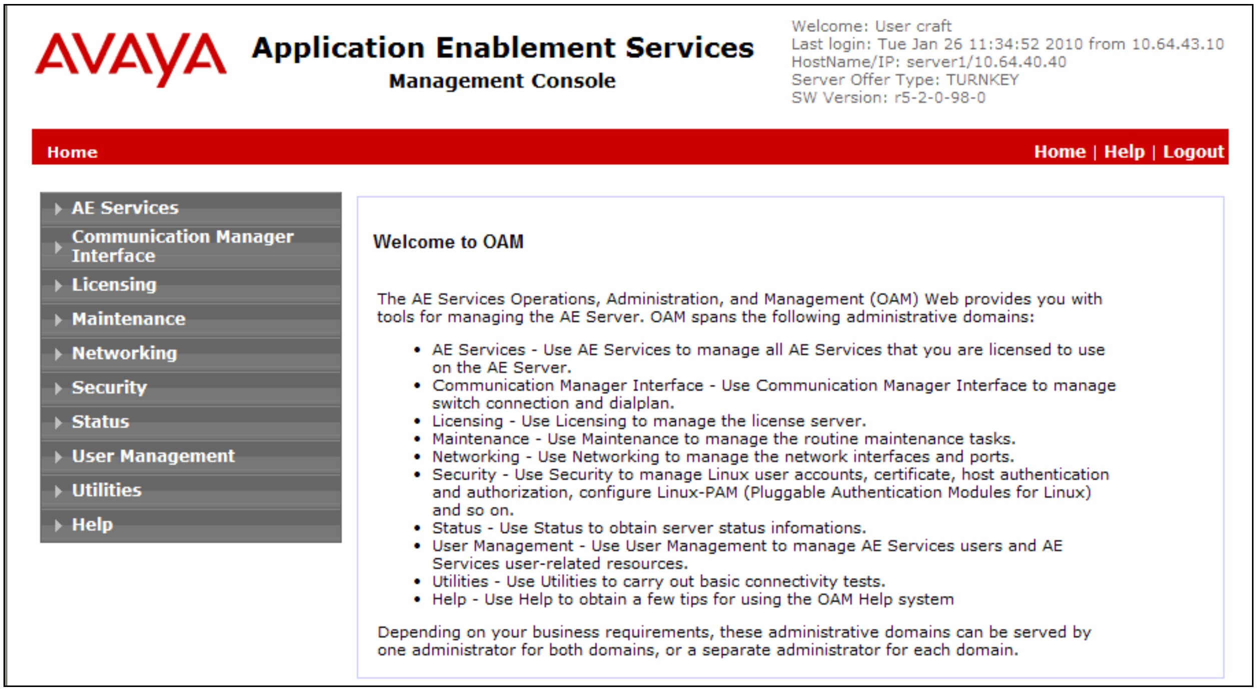
This section assumes that the license is installed, and installation and basic administration of the Avaya Application Enablement Services server has been performed. The steps in this section describe the configuration of a Switch Connection, a CTI user.

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 page.



5.1. Configure Switch Connection

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



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

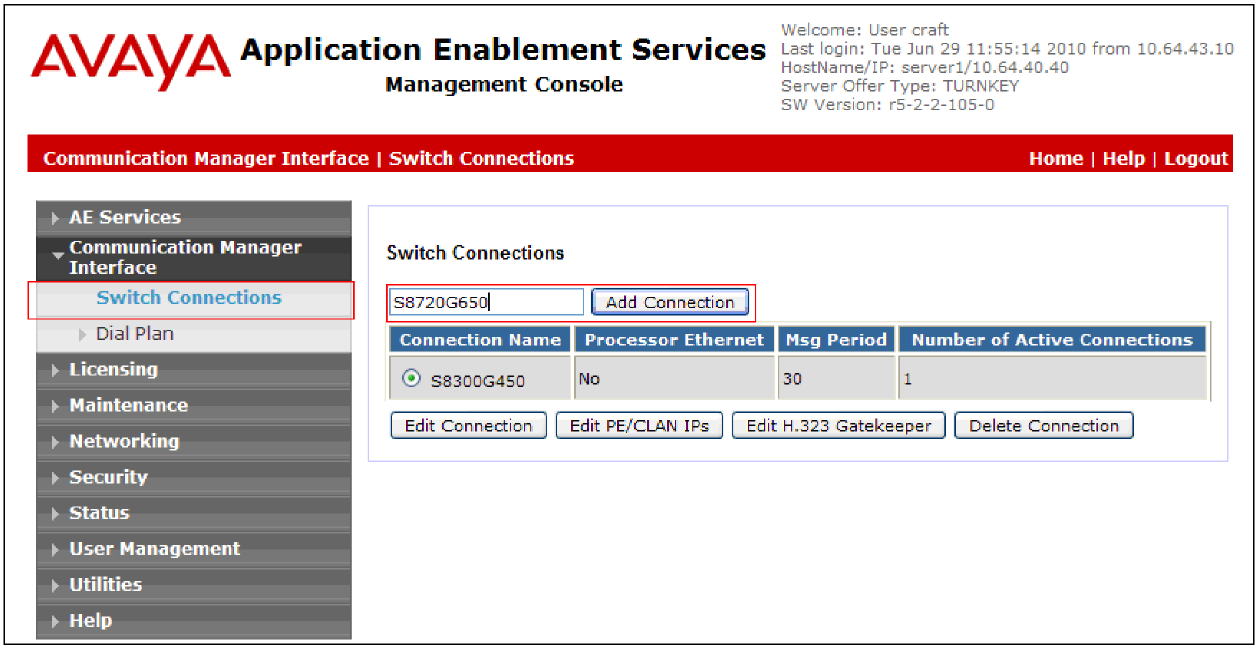
Welcome to OAM

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**.



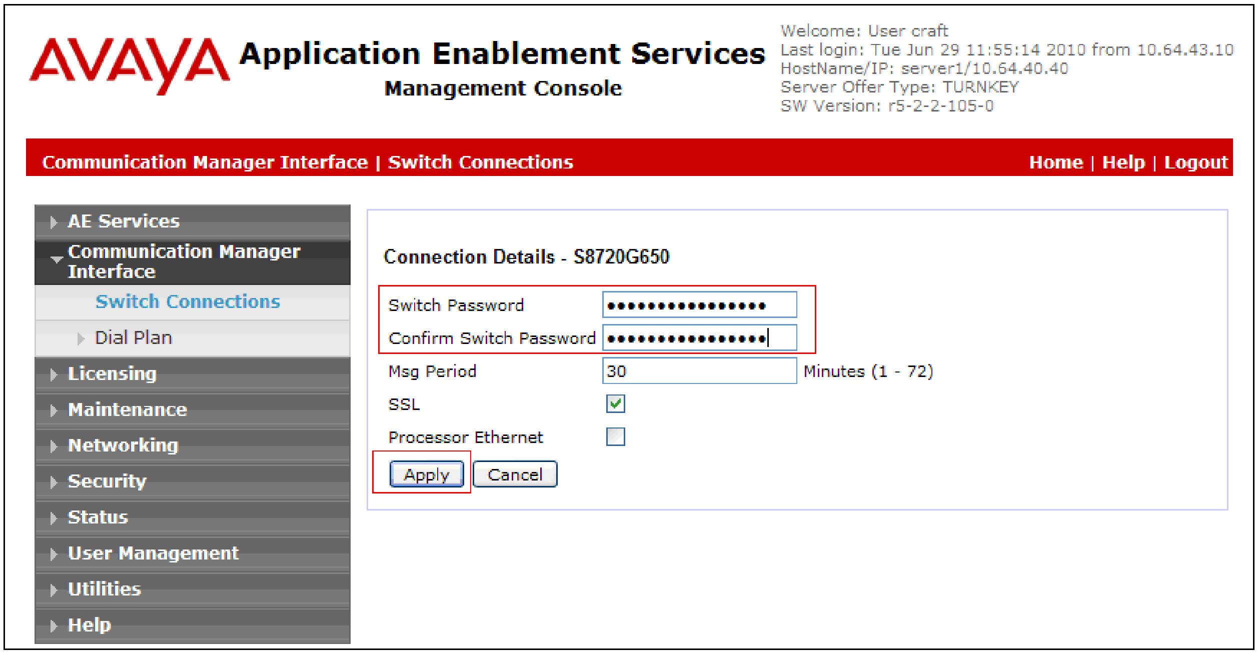
Application Enablement Services
Management Console
Welcome: User craft
Last login: Tue Jun 29 11:55:14 2010 from 10.64.43.10
HostName/IP: server1/10.64.40.40
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0
Communication Manager Interface | Switch Connections
Home | Help | Logout
AE Services
Communication Manager Interface
Switch Connections
Dial Plan
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Help

Switch Connections

S8720G650 Add Connection

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**.

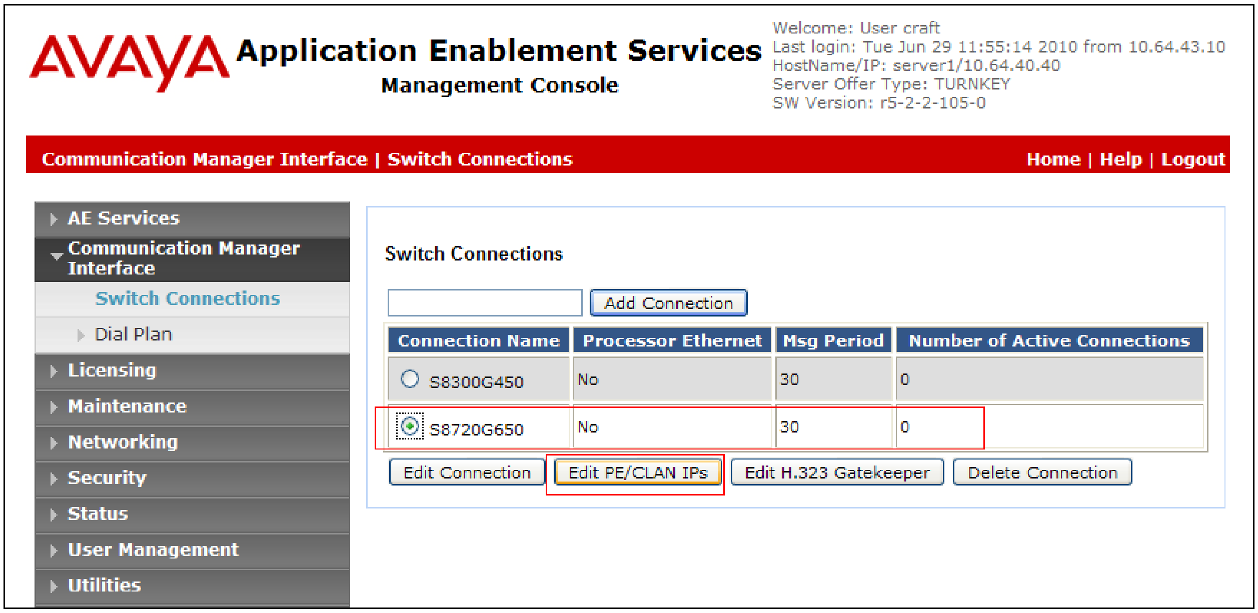


Application Enablement Services
Management Console
Welcome: User craft
Last login: Tue Jun 29 11:55:14 2010 from 10.64.43.10
HostName/IP: server1/10.64.40.40
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0
Communication Manager Interface | Switch Connections
Home | Help | Logout
AE Services
Communication Manager Interface
Switch Connections
Dial Plan
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Help

Connection Details - S8720G650

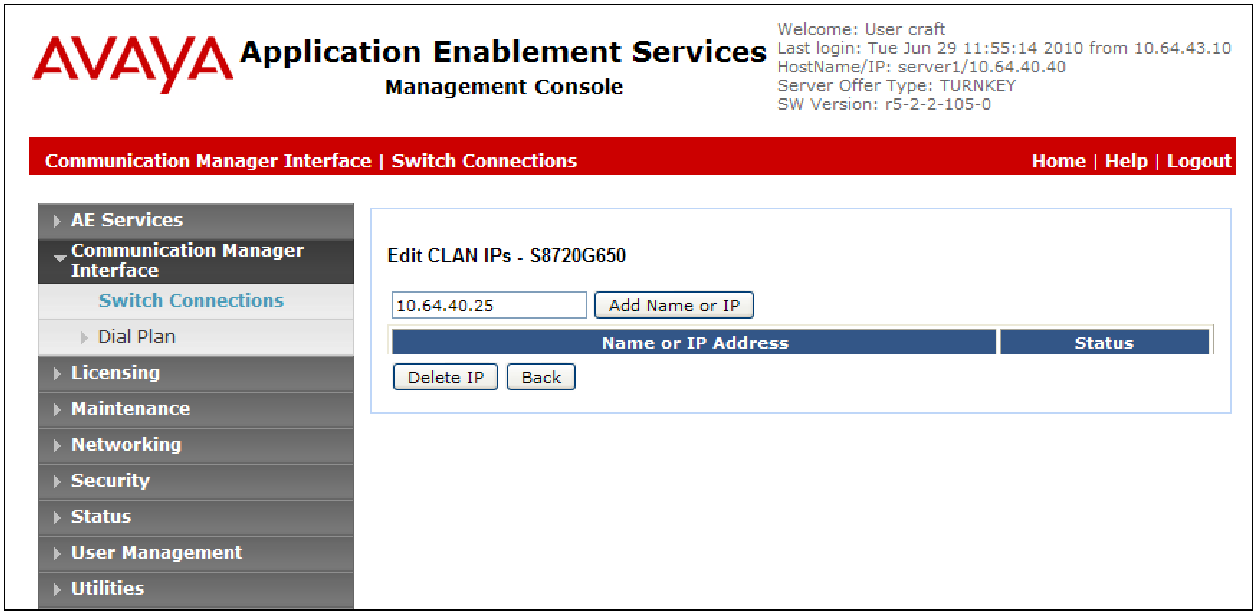
Switch Password	●●●●●●●●●●●●●●●●
Confirm Switch Password	●●●●●●●●●●●●●●●●
Msg Period	30 Minutes (1 - 72)
SSL	☑
Processor Ethernet	□

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**.



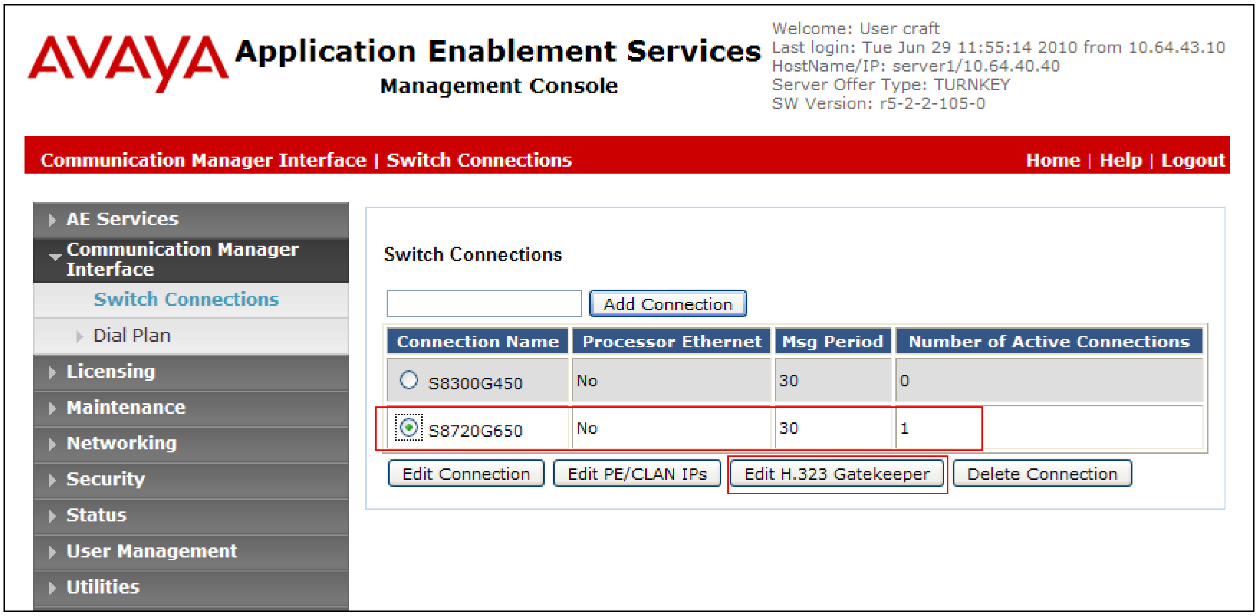
Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
○ S8300G450	No	30	0
● S8720G650	No	30	0

Enter the CLAN-AES IP address created in **Section 4.1**, and click on **Add Name or IP**.


AVAYA Application Enablement Services
Management Console
Welcome: User craft
Last login: Tue Jun 29 11:55:14 2010 from 10.64.43.10
HostName/IP: server1/10.64.40.40
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0
Communication Manager Interface | Switch Connections
Home | Help | Logout
AE Services
Communication Manager Interface
Switch Connections
Dial Plan
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Edit CLAN IPs - S8720G650
Add Name or IP
Name or IP Address
Status
Delete IP
Back

10.64.40.25

After the completion, navigate back to **Administration → Switch Connections** in the left pane to invoke the Switch Connections page. Click on **Edit H.323 Gatekeeper** for DMCC call control and monitor.

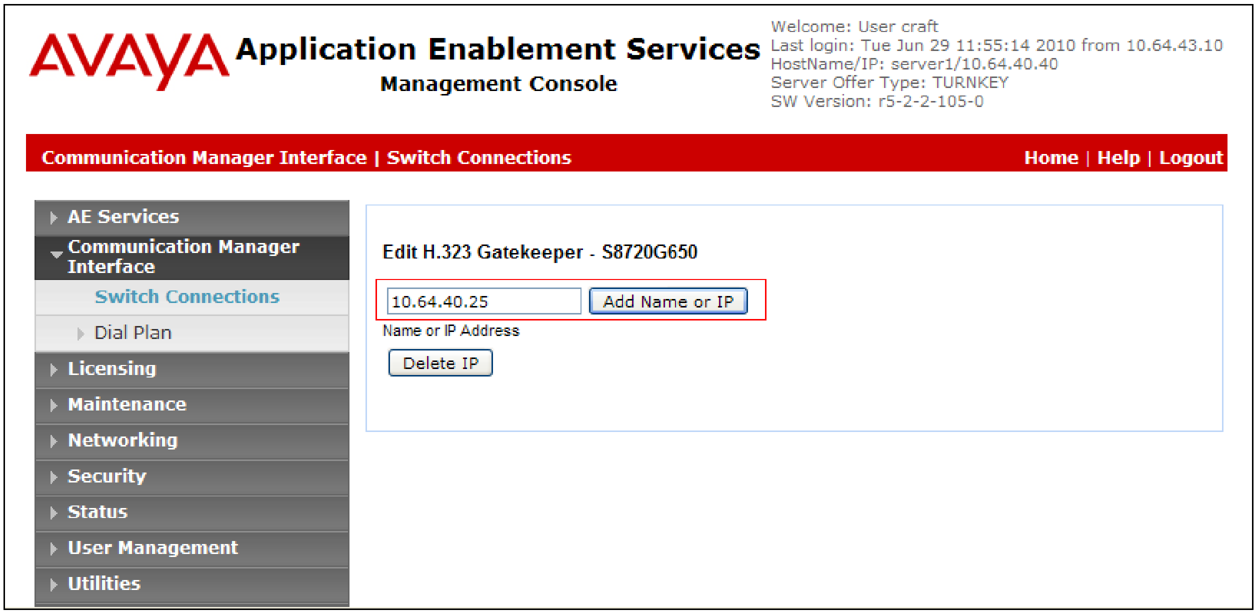


Welcome: User craft
Last login: Tue Jun 29 11:55:14 2010 from 10.64.43.10
HostName/IP: server1/10.64.40.40
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
○ S8300G450	No	30	0
● S8720G650	No	30	1

On the **Edit H.323 Gatekeeper – S8720G650** page, enter the CLAN-AES IP address which will be used for the DMCC service. Click on **Add Name or IP**.



Welcome: User craft
Last login: Tue Jun 29 11:55:14 2010 from 10.64.43.10
HostName/IP: server1/10.64.40.40
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

Edit H.323 Gatekeeper - S8720G650

Name or IP Address: 10.64.40.25

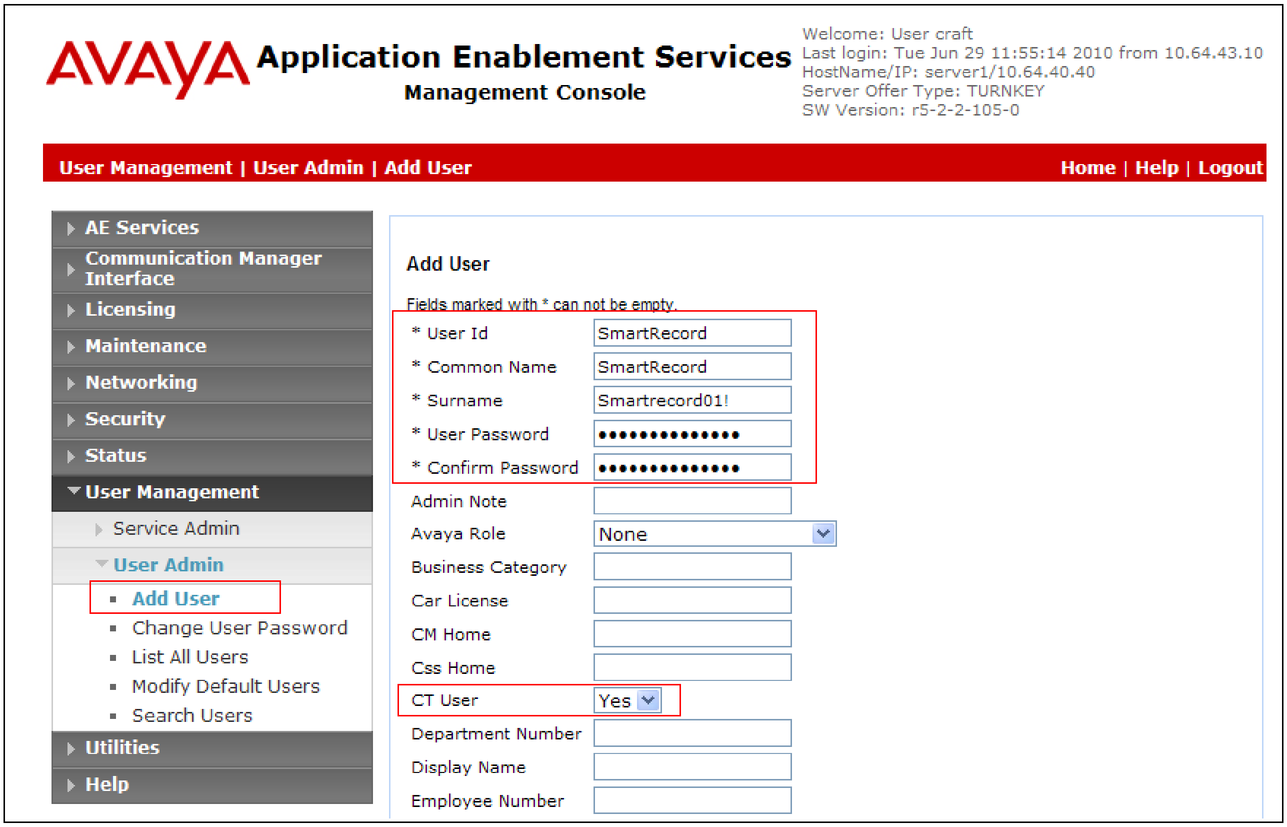
5.2. Configure the CTI Users

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 SmartRecord 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.



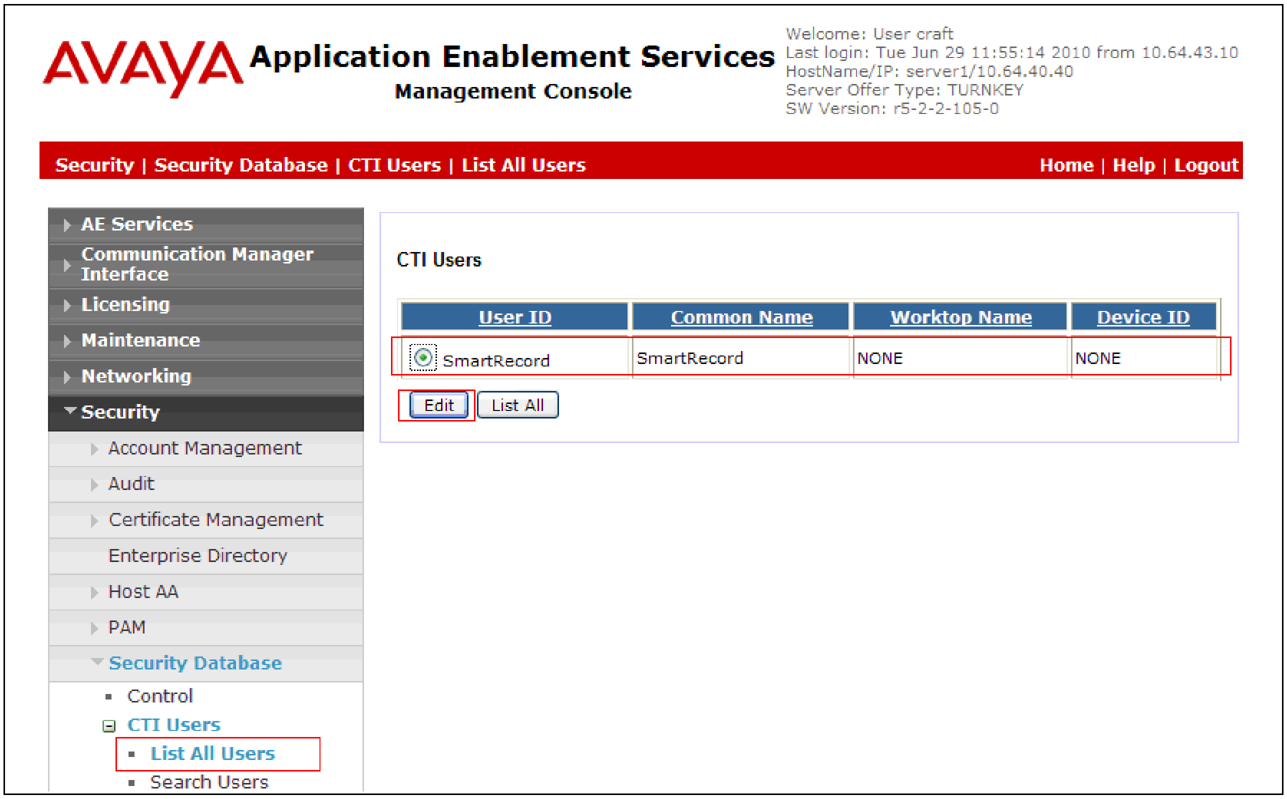
Welcome: User craft
Last login: Tue Jun 29 11:55:14 2010 from 10.64.43.10
HostName/IP: server1/10.64.40.40
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

Add User

Fields marked with * can not be empty.

* User Id	SmartRecord
* Common Name	SmartRecord
* Surname	Smartrecord01!
* 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.

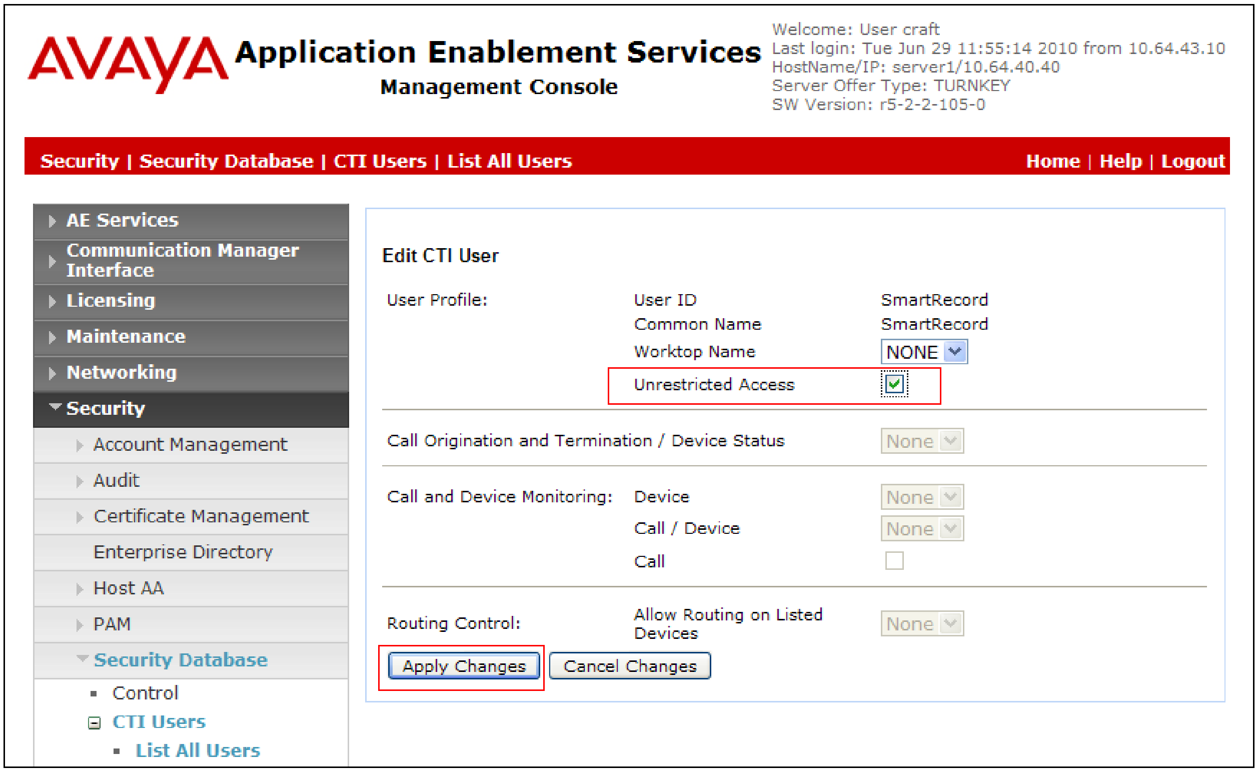


Welcome: User craft
Last login: Tue Jun 29 11:55:14 2010 from 10.64.43.10
HostName/IP: server1/10.64.40.40
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

CTI Users

User ID	Common Name	Worktop Name	Device ID
● SmartRecord	SmartRecord	NONE	NONE

Provide the user with unrestricted access privileges by putting a check in the box next to the Unrestricted Access field. Click the **Apply Changes** button.



Welcome: User craft
Last login: Tue Jun 29 11:55:14 2010 from 10.64.43.10
HostName/IP: server1/10.64.40.40
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

Edit CTI User

User Profile:	User ID	SmartRecord
	Common Name	SmartRecord
	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

6. Configure CTI Group SmartRecord

CTI Group installs, configures, and customizes the SmartRecord application for their end customers. Included in this section is an initial configuration file which interfaces with Application Enablement Services.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
- <SRIPConfigure xmlns="www.ctigroup.com">
    <minHangCallDurationInHour>6</minHangCallDurationInHour>
    <extensionUpdateIntervalInSeconds>60</extensionUpdateIntervalInSeconds>
  - <remotehost>
.*
  - <mediaserver>
      <ip>192.168.36.12</ip>
      <port>8087</port>
    </mediaserver>
- <!--
    Additional media servers can be added for load balancing
                  <mediaserver>
                          <ip>192.168.36.12</ip>
                          <port>8087</port>
                  </mediaserver>
  -->
</remotehost>
  - <Avaya>
<!--  only extensions of the provider or tenant with specified reocrding roup name
will be recorded. -->
<!-- multiple recording groups can be configured here, separated by comma, e.g.,
provider1,provider2, etc. -->
<recordinggroups>avaya</recordinggroups>
<media.port.start>2000</media.port.start>
<!-- AES and switch configurations   -->
<!--  if the secure is used, the related security data should be provided -->
<cmapi.server_ip>205.168.62.81</cmapi.server_ip>
<cmapi.server_port>4721</cmapi.server_port>
<cmapi.secure>false</cmapi.secure>
<cmapi.username>SmartRecord</cmapi.username>
<cmapi.password>Smartrecord01!</cmapi.password>
<switchip>10.64.40.25</switchip>
<switchname>S8720G650</switchname>
<cmapi.session_duration_timer>240</cmapi.session_duration_timer>
<cmapi.session_cleanup_delay>120</cmapi.session_cleanup_delay>
<!-- Specify a single or a range of recording stations(comma delimited) -->
<recordingstations>23001-23023</recordingstations>
<!--  Recording station password has to be the same for all stations -->
<recordingstationpassword>1234</recordingstationpassword>
<!-- codec set used by recording stations, in sequence and case sensative. If none is
set, avaya default will be  used -->
<recordingstationcodecset>g711U,g711A,g729,g729A</recordingstationcodecset>
</avaya>
- <webserviceclient>
    <dbserviceurl>http://localhost/SRWebService/DBService.asmx</dbserviceurl>
  </webserviceclient>
 </SRIPConfigure
```

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 or intra switch network. Those trunk calls were monitored by CTI Group SmartRecord, and calls were recorded using Single Step Conference. 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, CTI Group SmartRecord was able to record the recorded/monitored stations after restarts of the CTI Group SmartRecord. In addition, after CTI Group 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 the link between Communication Manager and the Application Enablement Service server went down and back up, CTI Group SmartRecord was able to resume recording.

8. Verification Steps

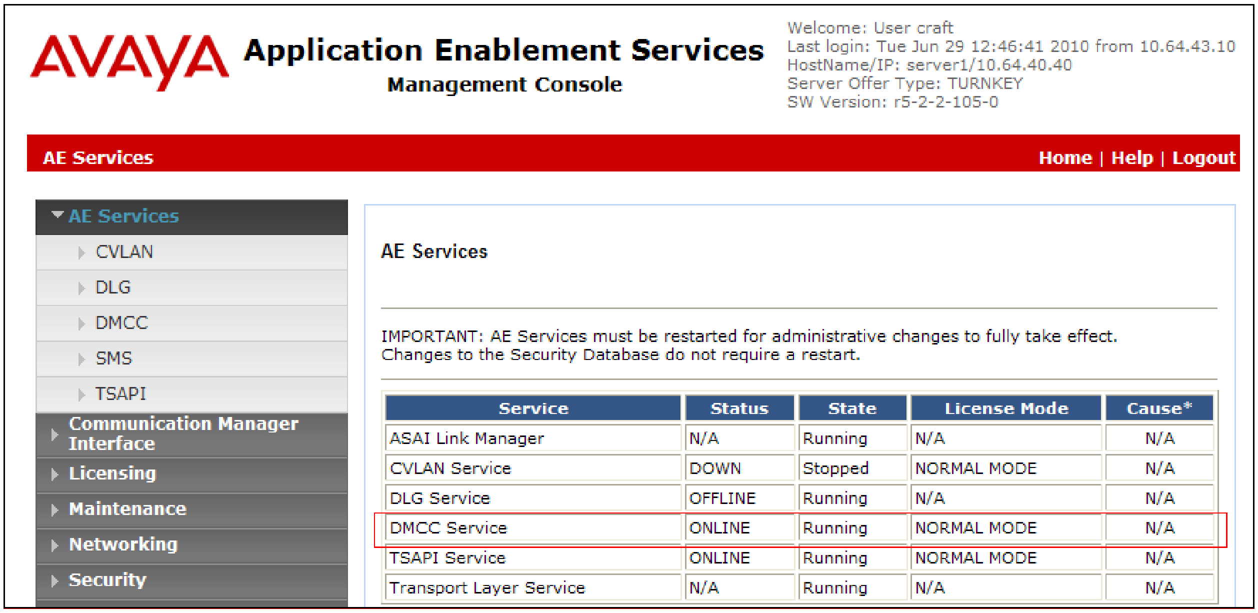
8.1. From Communication Manager

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
```

8.2. From Application Enablement Services

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



Welcome: User craft
Last login: Tue Jun 29 12:46:41 2010 from 10.64.43.10
HostName/IP: server1/10.64.40.40
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

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

9. Conclusion

These Application Notes described a compliance-tested configuration comprised of Communication Manager, Application Enablement Services, Avaya IP and Digital Telephones, and the CTI Group SmartRecord application. CTI Group SmartRecord was able to record calls that came through the trunk, and intra switch environment.

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 CTI Group products may be found at http://www.ctigroup.com/
[3] *CTI Group SmartRecord Installation and Configuration Guide,* May 2010
[4] *CTI Group SmartRecord Recommended Hardware and Software Guide,* April 2010
[5] *CTI Group SmartRecord End Users Interface Users Guide*, April 2010
[6] *CTI Group SmartRecord API Descriptions*, April 2010
[7] *CTI Group SmartRecord Administrative Interface User's Guide,* March 2010

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.