



## Avaya Solution & Interoperability Test Lab

---

# Application Notes for Edigin SVRX with Avaya Aura<sup>®</sup> Communication Manager and Avaya Aura<sup>®</sup> Application Enablement Services - Issue 1.0

### Abstract

These Application Notes describe a compliance-tested configuration comprised of Avaya Aura<sup>®</sup> Communication Manager, Avaya Aura<sup>®</sup> Application Enablement Services, Avaya IP and Digital Telephones, and the Edigin SVRX application.

The Edigin SVRX recording and quality monitoring system allows customers to efficiently increase agent productivity by monitoring real-time agent activity, evaluating customer interactions, and training.

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<sup>®</sup> Communication Manager, Avaya Aura<sup>®</sup> Application Enablement Services, Avaya IP and Digital Telephones, and Edigin SVRX.

The SVRX recording and quality monitoring system allows customers to efficiently increase agent productivity by monitoring real-time agent activity, evaluating customer interactions, and training. Edigin SVRX delivers the entire user, manager, and administrator toolbox in a single intuitive interface that is browser based.

This interface includes access to:

- Voice recordings
- Screen recordings
- Agent performance dashboards
- Agent evaluation, training and testing
- Report builder
- Administrator tools

All of these areas are privilege based and password protected. During the compliance test, Voice recordings were tested and verified.

## 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 Edigin SVRX, Application Enablement Services, and Communication Manager.

## 1.2. Support

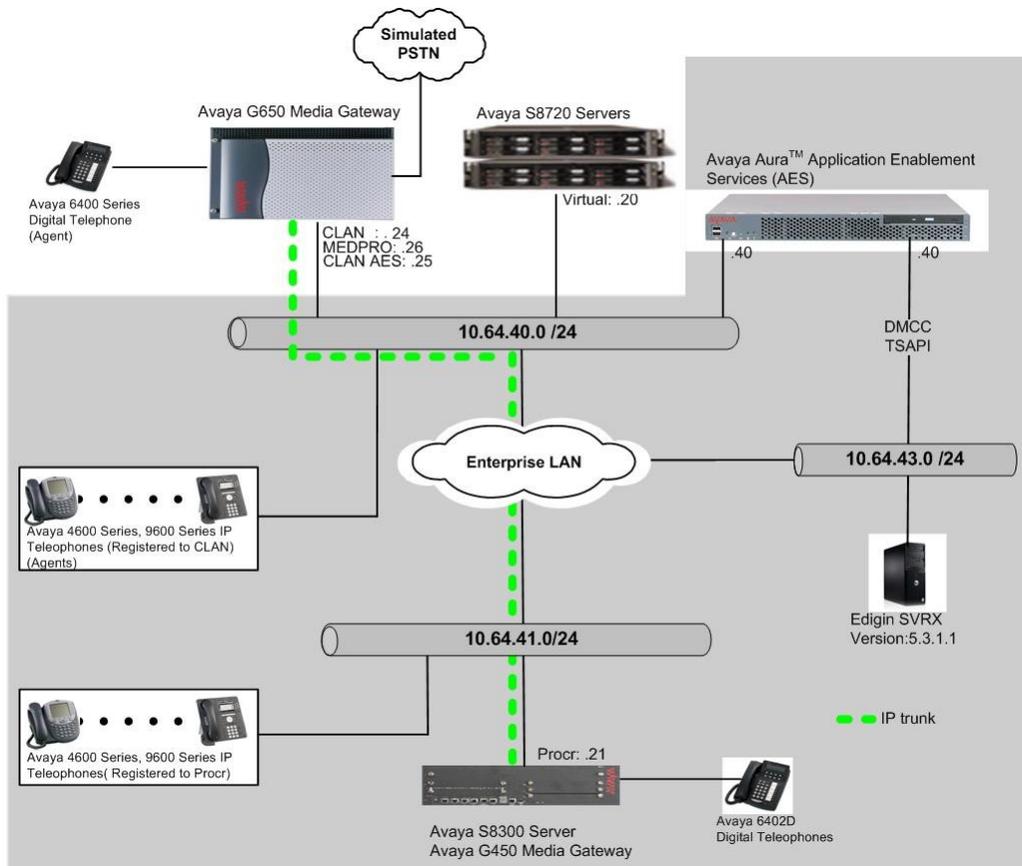
Technical support for the Edigin SVRX solution can be obtained by contacting Edigin:

- URL – <http://www.edigin.com/support>
- Phone – (877) 237-5151 Option 3

# 2. Reference Configuration

**Figure 1** illustrates the configuration used in these Application Notes. The sample configuration shows an enterprise with an Avaya Aura<sup>®</sup> Application Enablement Services server and Avaya S8300D Server with an Avaya G450 Media Gateway. Edigin SVRX was located in 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. Avaya S8720 Servers with an Avaya G650 Media Gateway were 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].



**Figure 1: Test Configuration of Edigin SVRX with Avaya Aura<sup>®</sup> Application Enablement Services**

### 3. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya S8300 Server with Avaya G450 Media Gateway	Avaya Aura <sup>®</sup> Communication Manager 6.0 (R016x.00.0.345.0) with Patch 00.0345.0-18246
Avaya S8720 Servers with Avaya G650 Media Gateway	Avaya Aura <sup>®</sup> Communication Manager 5.2.1 (R015x.02.1.016.4) with the patch (02.1.016.4-17963)
Avaya Aura <sup>®</sup> Application Enablement Services Server	5.2.2 (r5-2-2-105-0)
Avaya 4625SW IP Telephone (H.323)	2.9
Avaya 9600 Series IP Telephones	
9620 (H.323)	3.1
9630 (H.323)	3.1
9650 (H.323)	3.1
9670 (H.323)	3.1
Avaya 6408D+ Digital Telephone	-
Edigin SVRX on Windows XP Pro with SP3	5.3.1.1

## 4. Configure Avaya Aura® 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
- IP Network Region

### 4.1. Configure IP Services

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

```
change node-names ip                                     Page 1 of 2
```

IP NODE NAMES	
Name	IP Address
CLAN	10.64.40.24
SES	10.64.40.41
SM-1	10.64.40.42
default	0.0.0.0
procr	10.64.41.21
procr6	::

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

```
change ip-services                                     Page 1 of 4
```

IP SERVICES					
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port
AESVCS	y	procr	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          xxxxxxxxxxxx  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 5
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
01: 124
02: 125
33:

```

## 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.

```
add hunt-group 83                                     Page 1 of 4
                                                    HUNT GROUP

Group Number: 83                                     ACD? y
Group Name: hunt-4-Edigin                            Queue? y
Group Extension: 72083                               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 83                                     Page 2 of 4
                                                    HUNT GROUP

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

Controlling Adjunct: none

Timed ACW Interval (sec):
Multiple Call Handling: none
```

## 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 72093                               Page 1 of 2
                AGENT LOGINID

Login ID: 72093                                         AAS? n
Name: Agent-3                                           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. 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 72093                               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: 83  1      16:
2:      17:
3:      18:
4:      19:
5:      20:
```

## 4.6. Configure Vector

Enter the **add vector q** command, where **q** is an unused vector number. Enter a descriptive name, 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. The following screen shows the configuration used during the compliance test.

```
add vector 83                                     Page 1 of 6
                                           CALL VECTOR

Number: 83                                     Name: Edigin
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 83      pri m
03 stop
04
```

## 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 72071 corresponds to VDN-Edigin, which in turn will invoke the actions specified in vector 83.

```
add vdn 72071                                     Page 1 of 3
                                           VECTOR DIRECTORY NUMBER

Extension: 72071
Name*: VDN-Edigin
Destination: Vector Number      83
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*:
```

## 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 SVRX application.

```

add station 72001                                     Page 1 of 5
                                                    STATION
Extension: 72001                                     Lock Messages? n          BCC: 0
Type: 9620                                           Security Code: *          TN: 1
Port: IP                                             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
                                                    Customizable Labels? y
  
```

On **Page 4** of the station form, under **ABBREVIATED DIALING → List2: group**, 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:

- auto-in
- 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(On Page 5), respectively. For Dial Code (DC), refer to **Section 4.3**.
- release (On Page 5)

```

add station 72001                                     Page 4 of 5
                                                    STATION
SITE DATA
Room:                                               Headset? n
Jack:                                              Speaker? n
Cable:                                             Mounting: d
Floor:                                             Cord Length: 0
Building:                                          Set Color:
ABBREVIATED DIALING
List1: personal 1                                  List2: group 1           List3:
BUTTON ASSIGNMENTS
1: call-appr                                       4: auto-in              Grp:
2: call-appr                                       5: aux-work            RC:   Grp:
3: call-appr                                       6: abrv-dial          List: 2 DC: 01
  
```

```

add station 72001                                     Page 5 of 5
                                                    STATION

BUTTON ASSIGNMENTS

7: abrv-dial List: 2 DC: 02                          10:
8: after-call                                     Grp:          11:
9: release                                         12:

```

Repeat the instructions provided in this section for each physical station that is to be monitored by Edigin SVRX.

#### 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**. Repeat the instructions provided in this section for each virtual station that will be used for a Single Step Conference.

```

add station 72501                                     Page 1 of 5
                                                    STATION

Extension: 72501                                     Lock Messages? n          BCC: 0
Type: 9630                                           Security Code: *          TN: 1
Port: S00078                                         Coverage Path 1:          COR: 1
Name: DMCC-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: 72501
Speakerphone: 2-way                                 Mute Button Enabled? y
Display Language: english                           Button Modules: 0
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

                                                    Customizable Labels? y

```

## 4.10. Configure IP Network Region

Enter the **change ip-network-map** command, and put the IP address of Application Enablement Services (or a subnet) into a Network Region. During the compliance test, the IP-Network-Region 1 is utilized.

```
change ip-network-map                                     Page 1 of 63
                                                    IP ADDRESS MAPPING

IP Address                                               Subnet Network      Emergency
Bits      Region VLAN Location Ext
-----
FROM: 10.64.40.0                                       /24      1      n
TO: 10.64.40.255
FROM: /                                                n
TO:
```

Enter the **change ip-network-region** command. On Page 3, set the Near End Establishes TCP Signaling Socket field under the TCP SIGNALING LINK ESTABLISHMENT FOR AVAYA H.323 ENDPOINTS section to **n**.

```
change ip-network-region 1                             Page 3 of 20
                                                    IP NETWORK REGION

INTER-GATEWAY ALTERNATE ROUTING / DIAL PLAN TRANSPARENCY
Incoming LDN Extension:
Conversion To Full Public Number - Delete:      Insert:
Maximum Number of Trunks to Use for IGAR:
Dial Plan Transparency in Survivable Mode? n

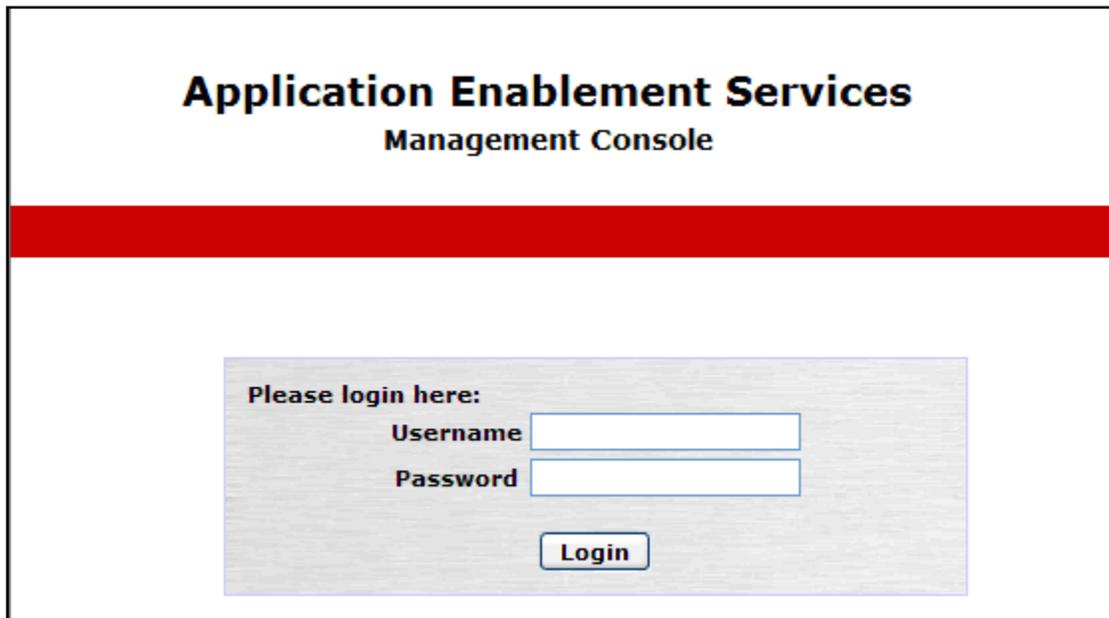
BACKUP SERVERS (IN PRIORITY ORDER)      H.323 SECURITY PROFILES
1                                         1 challenge
2                                         2
3                                         3
4                                         4
5
6                                         Allow SIP URI Conversion? y

TCP SIGNALING LINK ESTABLISHMENT FOR AVAYA H.323 ENDPOINTS
Near End Establishes TCP Signaling Socket? n
Near End TCP Port Min: 61440
Near End TCP Port Max: 61444
```

## 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.



The screenshot shows the login interface for the Avaya Application Enablement Services Management Console. At the top, the title "Application Enablement Services Management Console" is displayed in bold black text. Below the title is a thick red horizontal bar. Underneath the bar is a light gray rectangular box containing the login form. The form starts with the text "Please login here:" followed by two input fields: "Username" and "Password". Below these fields is a "Login" button.

## 5.1. Configure Switch Connection

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

The screenshot shows the Avaya Application Enablement Services Management Console. The header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for user "craft" with login details. A navigation bar contains "Home", "Help", and "Logout". A left sidebar lists menu items: AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area is titled "Welcome to OAM" and provides an overview of the OAM web interface, listing administrative domains and their functions. A note at the bottom states that administrative domains can be served by one administrator for both domains or a separate administrator for each domain.

**AVAYA 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 | 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**.

The screenshot shows the Avaya Application Enablement Services Management Console, specifically the "Switch Connections" page. The header and navigation bar are similar to the previous screenshot. The left sidebar has "Communication Manager Interface" expanded to show "Switch Connections". The main content area is titled "Switch Connections" and features a text input field containing "S8300G450" and an "Add Connection" button. Below this is a table with columns: Connection Name, Processor Ethernet, Msg Period, and Number of Active Connections. The table contains one entry: S8720G650, No, 30, 0. Below the table are buttons for "Edit Connection", "Edit PE/CLAN IPs", "Edit H.323 Gatekeeper", and "Delete Connection".

**AVAYA Application Enablement Services Management Console**

Welcome: User craft  
Last login: Wed Nov 3 14:01:28 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

S8300G450

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

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**.

**AVAYA Application Enablement Services Management Console**

Welcome: User craft  
 Last login: Wed Nov 3 14:01:28 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 - S8300G450**

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

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

**AVAYA Application Enablement Services Management Console**

Welcome: User craft  
 Last login: Wed Nov 3 14:01:28 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**

[Add Connection]

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> S8300G450	Yes	30	0
<input type="radio"/> S8720G650	No	30	0

Edit Connection Edit PE/CLAN IPs Edit H.323 Gatekeeper Delete Connection

Enter the procr 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: Wed Nov 3 14:01:28 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

Edit Processor Ethernet IP - S8300G450

Name or IP Address	Status

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

**AVAYA Application Enablement Services Management Console**

Welcome: User craft  
Last login: Wed Nov 3 14:01:28 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

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> S8300G450	Yes	30	0
<input type="radio"/> S8720G650	No	30	0

On the **Edit H.323 Gatekeeper – S8300G450** page, enter the procr IP address which will be used for the DMCC service. Click on **Add Name or IP**.

The screenshot displays the Avaya Application Enablement Services Management Console. At the top left is the Avaya logo and the text "Application Enablement Services Management Console". At the top right, there is a welcome message: "Welcome: User craft", "Last login: Wed Nov 3 14:01:28 2010 from 10.64.43.10", "HostName/IP: server1/10.64.40.40", "Server Offer Type: TURNKEY", and "SW Version: r5-2-2-105-0". Below this is a red navigation bar with "Communication Manager Interface | Switch Connections" on the left and "Home | Help | Logout" on the right. A left-hand navigation menu lists various services: AE Services, Communication Manager Interface (expanded), Switch Connections (highlighted), Dial Plan, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area is titled "Edit H.323 Gatekeeper - S8300G450" and contains a form with a text input field containing "10.64.41.21", an "Add Name or IP" button, a "Name or IP Address" label, and a "Delete IP" button.

## 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 SVRX 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.

**AVAYA** Application Enablement Services  
Management Console

Welcome: User craft  
Last login: Wed Nov 3 14:01:28 2010 from 10.64.43.10  
HostName/IP: server1/10.64.40.40  
Server Offer Type: TURNKEY  
SW Version: r5-2-2-105-0

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

Navigation Menu:  
▶ AE Services  
▶ Communication Manager Interface  
▶ Licensing  
▶ Maintenance  
▶ Networking  
▶ Security  
▶ Status  
▼ User Management  
    ▶ Service Admin  
    ▼ User Admin  
        ▪ Add User  
        ▪ Change User Password  
        ▪ List All Users  
        ▪ Modify Default Users  
        ▪ Search Users  
▶ Utilities  
▶ Help

**Add User**

Fields marked with \* can not be empty.

* User Id	<input type="text" value="edigin"/>
* Common Name	<input type="text" value="edigin"/>
* Surname	<input type="text" value="edigin"/>
* User Password	<input type="password" value="....."/>
* Confirm Password	<input type="password" value="....."/>
Admin Note	<input type="text"/>
Avaya Role	<input type="text" value="None"/>
Business Category	<input type="text"/>
Car License	<input type="text"/>
CM Home	<input type="text"/>
Css Home	<input type="text"/>
CT User	<input type="text" value="Yes"/>
Department Number	<input type="text"/>
Display Name	<input type="text"/>
Employee Number	<input type="text"/>

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.

## Application Enablement Services

### Management Console

Welcome: User craft  
 Last login: Wed Nov 3 14:01:28 2010 from 10.64.43.10  
 HostName/IP: server1/10.64.40.40  
 Server Offer Type: TURNKEY  
 SW Version: r5-2-2-105-0

Security | Security Database | CTI Users | List All Users
Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▼ Security
  - ▶ Account Management
  - ▶ Audit
  - ▶ Certificate Management
  - Enterprise Directory
  - ▶ Host AA
  - ▶ PAM
  - ▼ Security Database
    - Control
    - ▣ CTI Users
      - List All Users
      - Search Users

#### CTI Users

User ID	Common Name	Worktop Name	Device ID
<input checked="" type="radio"/> edigin	edigin	NONE	NONE
<input type="radio"/> test	test	NONE	NONE

CRK; Reviewed:  
SPOC 1/25/2011

Solution & Interoperability Test Lab Application Notes  
©2011 Avaya Inc. All Rights Reserved.

19 of 29  
Edigin\_SVRX-AES

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.

The screenshot shows the Avaya Application Enablement Services Management Console interface. The top navigation bar includes 'Security | Security Database | CTI Users | List All Users' and 'Home | Help | Logout'. The left sidebar lists various services, with 'Security Database' expanded to show 'CTI Users' and 'List All Users'. The main content area is titled 'Edit CTI User' and contains the following fields:

User Profile:	User ID	edigin
	Common Name	edigin
	Worktop Name	NONE
	Unrestricted Access	<input checked="" type="checkbox"/>
Call Origination and Termination / Device Status		None
Call and Device Monitoring:	Device	None
	Call / Device	None
	Call	<input type="checkbox"/>
Routing Control:	Allow Routing on Listed Devices	None

At the bottom of the form, there are two buttons: 'Apply Changes' (highlighted with a red box) and 'Cancel Changes'.

## 6. Configure Edigin SVRX

Edigin installs, configures, and customizes the SVRX application for their end customers. For installing Edigin SVRX and configuring Edigin SVRX to interface with Application Enablement Services, see Appendix A.

## 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 the Edigin SVRX, 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, Edigin SVRX was able to record the recorded/monitored stations after restarts of the Edigin SVRX. In addition, after Edigin 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, Edigin SVRX 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/ Link	AE Services Server	Remote IP	Remote Port	Local Node	Msgs Sent	Msgs Rcvd
01/01	server1	10.64.43.40	36538	procr	17	18

### 8.2. From Application Enablement Services

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

The screenshot shows the Avaya Application Enablement Services Management Console. The top navigation bar includes 'AE Services', 'Home', 'Help', and 'Logout'. The left sidebar lists various service categories, with 'AE Services' expanded to show 'CVLAN', 'DLG', 'DMCC', 'SMS', and 'TSAPI'. The main content area displays the 'AE Services' status, including an important note: 'IMPORTANT: AE Services must be restarted for administrative changes to fully take effect. Changes to the Security Database do not require a restart.' Below this is a table of service statuses:

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 Edigin SVRX application. Edigin SVRX 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

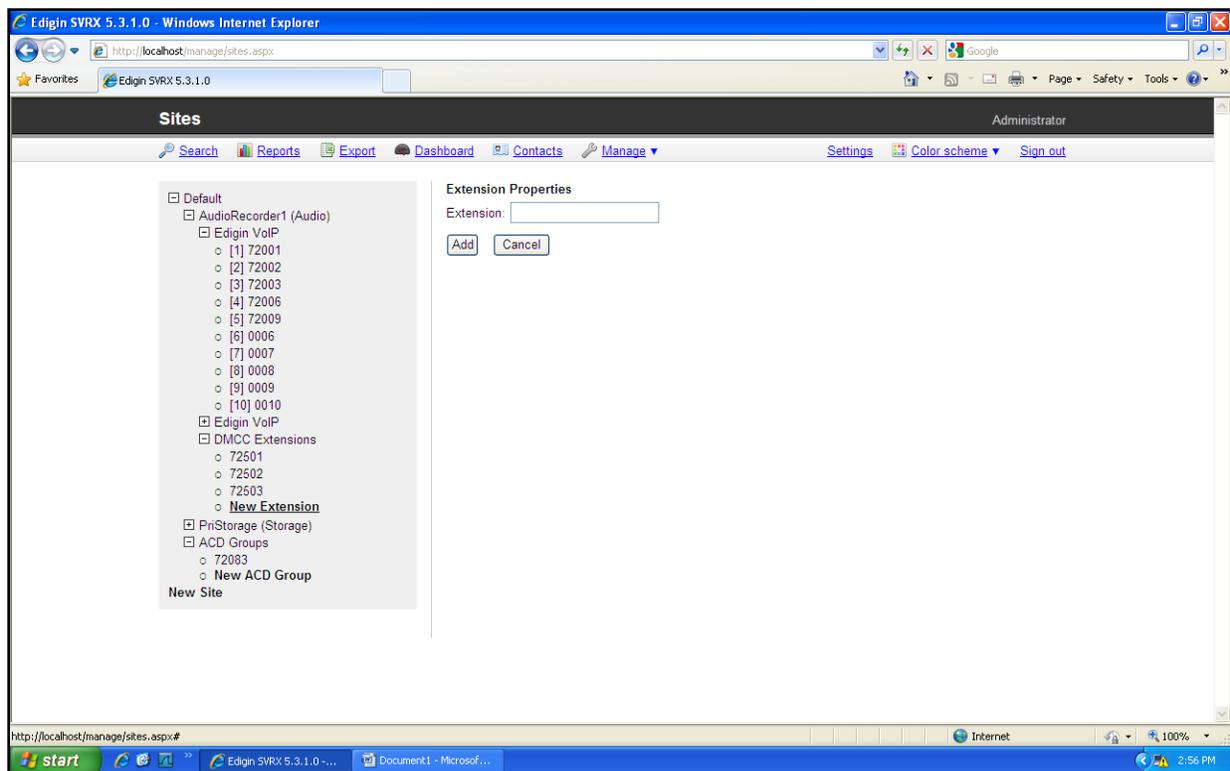
## Appendix A

**Note:** This section describes the configuration steps for Edigin SVRX. The following configuration steps have been provided by an Edigin engineer.

Edigin installs, configures, and customizes the SVRX for the customer prior to shipment. Customer specific configuration for integration with Application Enablement Services is described below.

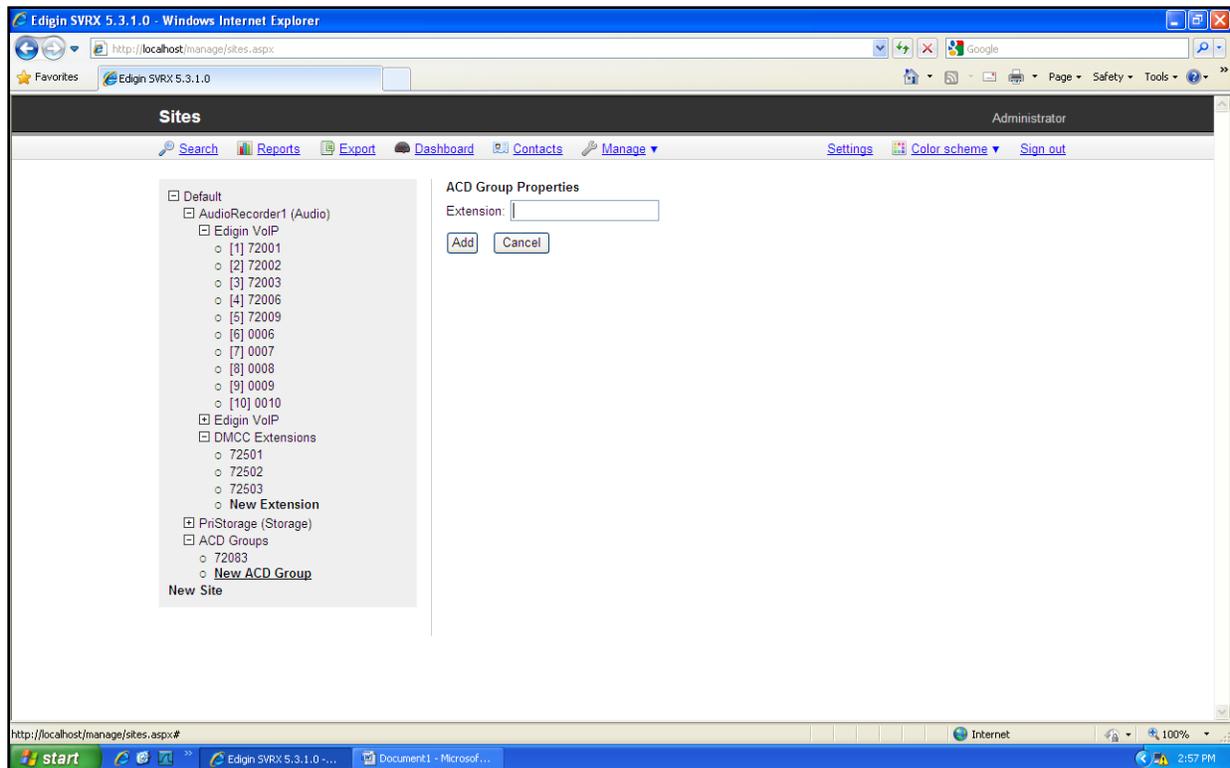
Add DMCC Recording Extensions:

1. Select Manage->Sites
2. Under the Site->AudioRecorder->DMCC Extensions, click New Extension
3. Type in the DMCC extension used for recording and click Add.
4. Repeat for each extension.



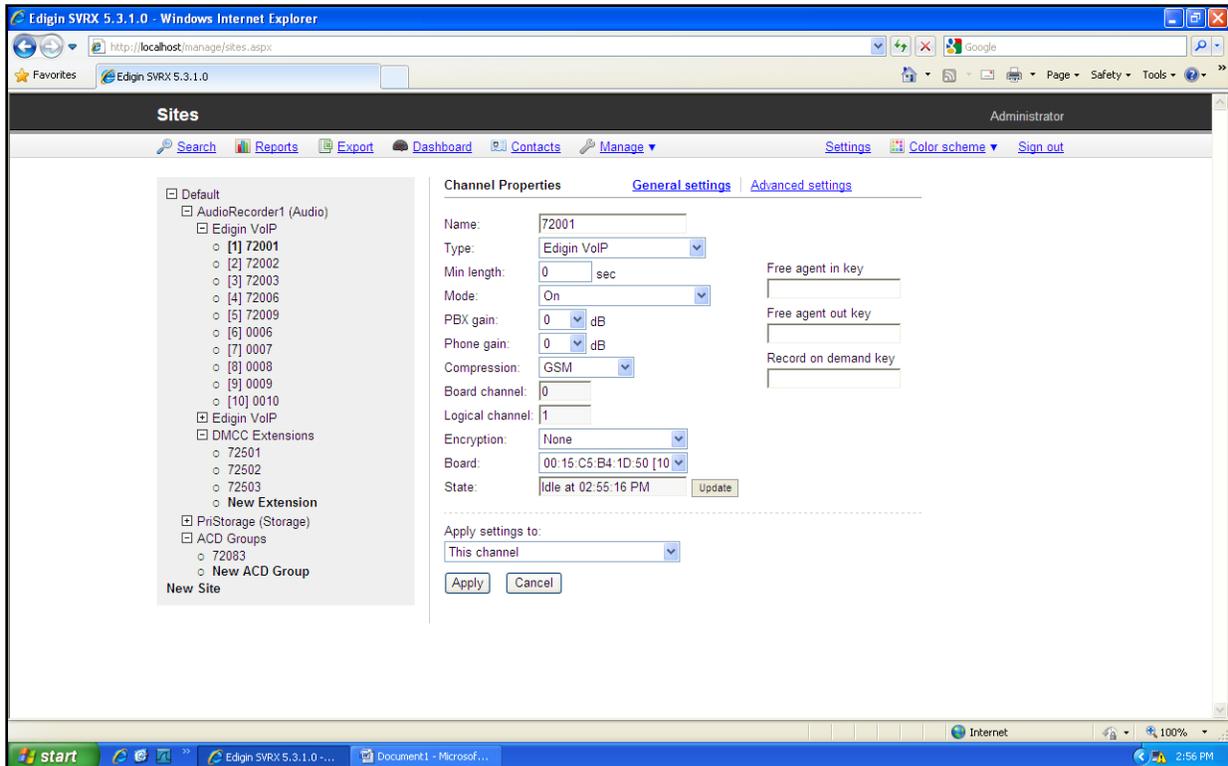
## Add Avaya Hunt Group Extensions

1. Select Manage->Sites
2. Under the Site->ACD Groups, click New ACD Group
3. Type in the Avaya Hunt Group extension and click Add.
4. Repeat for each hunt group.



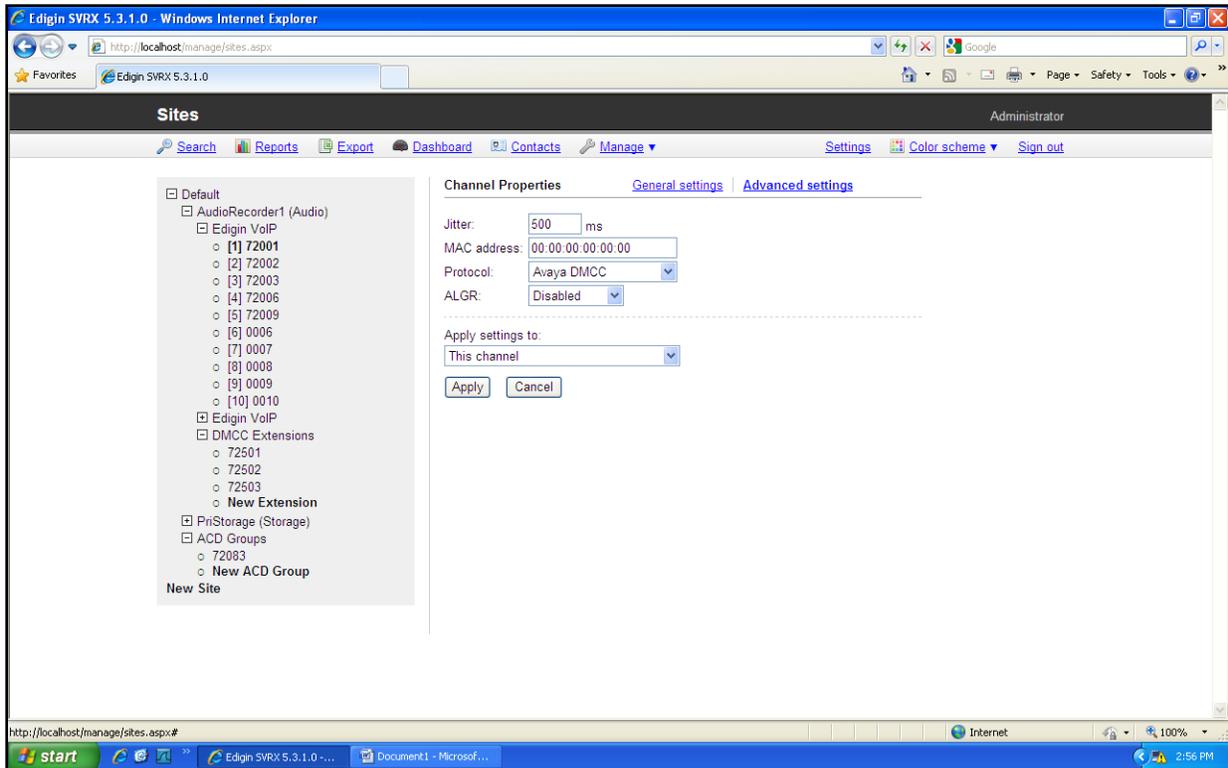
## Update Recorded Station Settings

1. Select Manage->Sites
2. Under the Site->AudioRecorder->Edigin VoIP, click on a channel.
3. Update the Name field to an extension that needs to be recorder and click Apply.
4. Repeat for each extension.



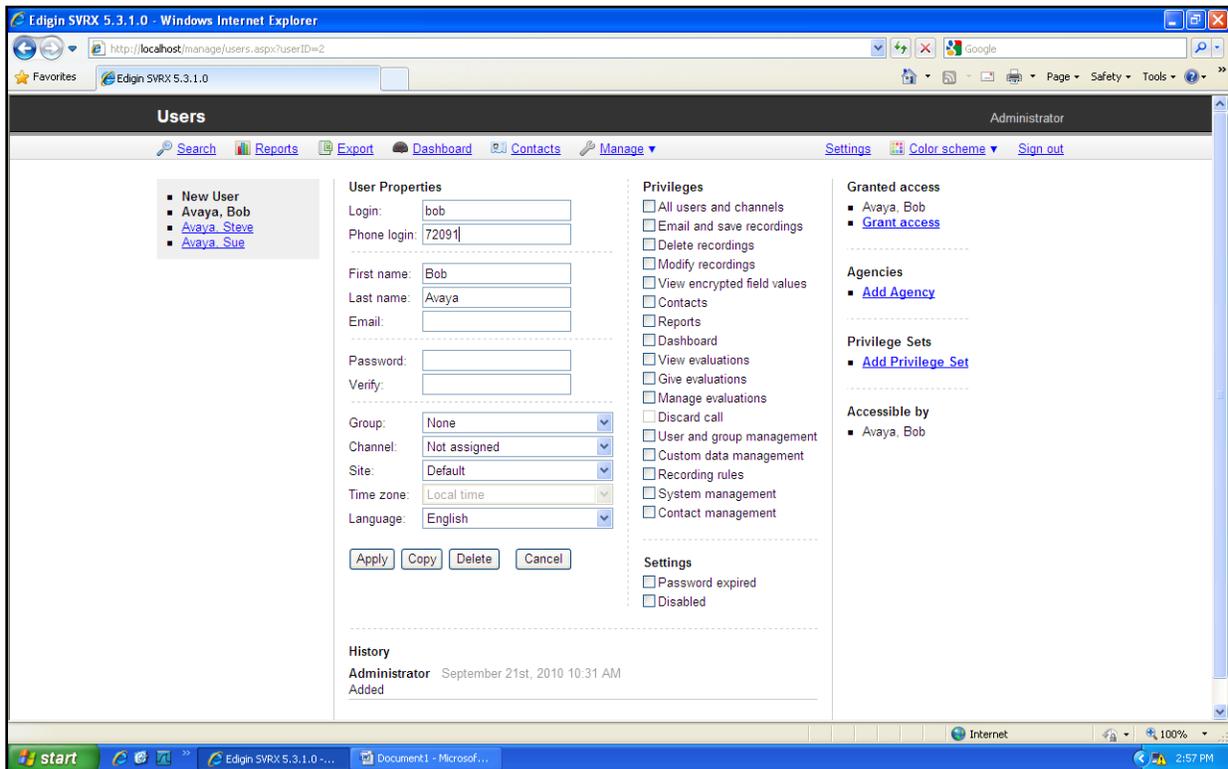
## Update Recorded Station Settings

1. Click on the Advanced settings link for the extension
2. Update the Protocol field to an Avaya DMCC and click Apply.
3. The other fields can be left to the default values shown.
4. Repeat for each extension.



## Create Agent User accounts

1. Select Manage->Users
2. Select New User
3. Set the Login to a unique Edigin login for this user.
4. Set the Phone login field to the Avaya agent login extension.
5. Set the First and Last name
6. Click Add.
7. Repeat for each agent.



## Set the AudioRecorder Application settings appropriately.

```
<add key="SignalingServerIP" value="10.64.120.12" />
<add key="ExtPassword" value="1234" />
<add key="CMHost" value="10.64.120.15" />
<add key="CMUser" value="aessim" />
<add key="CMPassword" value="AESsim123#" />
```

SignalingServerIP is the Communication manager IP.

ExtPassword is the phone password.

The rest of the parameters are AES login info.



---

**©2011 Avaya Inc. All Rights Reserved.**

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

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