



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Fortek VISION with Avaya Aura® Application Enablement Services 4.2.2 and Avaya Aura® Communication Manager 5.2.1 - Issue 1.0**

### **Abstract**

These Application Notes describe the configuration steps required to integrate Fortek VISION with Avaya Aura® Application Enablement Services 4.2.2 and Avaya Aura® Communication Manager 5.2.1. Fortek VISION integrates with the Avaya solution by using the Telephony Services Application Programming Interface (TSAPI) provided by Application Enablement Services to exercise third party call control.

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 the steps required to connect Fortek VISION to an Avaya VoIP (Voice over IP) enterprise solution consisting of Avaya Aura® Application Enablement Services (AES) and Avaya Aura® Communication Manager. Fortek VISION is a Computer Telephony Integration (CTI) platform that provides call control and monitoring functionality to end users via the Telephony Services API (TSAPI) interface on the Application Enablement Services. Fortek VISION utilizes a client/server model. The server component of the software will connect to the TSAPI Service on the Application Enablement Services. The client component of the software will communicate to the VISION server.

## 2. General Test Approach and Test Results

The compliance testing focused on the ability of Fortek VISION to successfully handle incoming calls and provide screen pop information to the VISION operator. All feature functionality test cases were performed manually to verify proper operation. The general test approach entailed:

- Establishing sessions from Fortek VISION to Application Enablement Services.
- Verify VISION operators were able to monitor call queues and that the information presented corresponded with Communication Manager.
- Verify Screen pop functionality including the presentation of Calling line ID.
- Verify call handling using basic telephony operations such as answer, hold/retrieve, transfer, consult, conference, and disconnect.
- Verify ability to transmit DTMF tones as entered from the VISION Control Room Client application.

The serviceability testing focused on verifying the ability of Fortek VISION to recover from adverse conditions, such as busying out the CTI link and disconnecting the Ethernet cable for the CTI link.

### 2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. The feature testing focused on verifying the ability of Fortek VISION to handle calls correctly, including:

- Basic telephony function such as call answer, call disconnect
- Verify ability to use features such as call hold, transfer and conference
- Verify ability to handle ACD call types correctly
- Verify ability to monitor ACD queues and calls
- Verify Screen pop functionality
- Verify ability to transmit DTMF tones requested from the VISION application

The serviceability testing focused on verifying the ability of Fortek VISION to recover from adverse conditions, such as busying out the CTI link and disconnecting the Ethernet cable for the CTI link.

## 2.2. Test Results

All feature and serviceability tests passed. Fortek VISION successfully interoperated with Communication manager and Application Enablement Services, handling incoming calls as required. For serviceability testing, Fortek VISION was able to resume call handling after restoration of connectivity to the Application Enablement Services server, from network disconnect/re-connect, and Fortek VISION resets with the following exception:

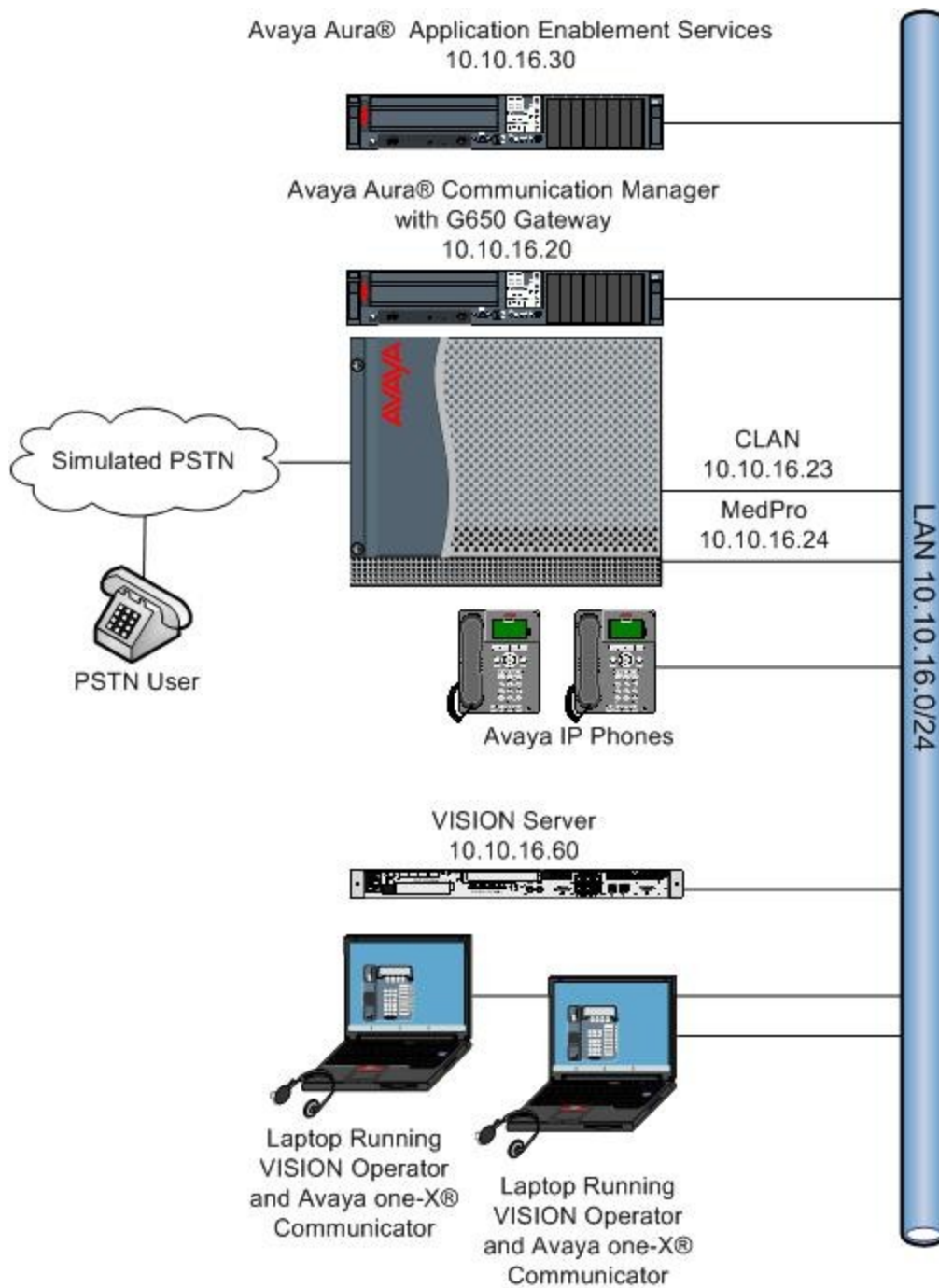
- It was observed that when the link between Application Enablement Services and Communication Manager goes offline the Fortek VISION system ends the monitoring of the Communication Manager devices. The TSAPI link remains active between Application Enablement Services and Fortek VISION. VISION was not receiving notification that the link is down and as a result the Fortek VISION server services must be restarted to re-enable the monitoring of the Communication Manager devices.

## 2.3. Support

For technical support of Fortek products please check the support link at the following web address: <http://www.fortek.co.uk>.

### 3. Reference Configuration

The test configuration in **Figure 1** was used to test the interoperability of Fortek VISION with Communication Manager and Application Enablement Services. Fortek VISION connects over the LAN to the TSAPI Service on Application Enablement Services. Fortek VISION uses the TSAPI Service to exercise 3<sup>rd</sup> party call control over the Avaya one-X Communicator endpoints utilized by the VISION operators. Communication Manager will service connections to Avaya 9600 Series IP telephones, Avaya 2400 Series Digital telephones and the Avaya one-X Communicator soft phone used with the VISION Operators. Calls were made to and from the simulated PSTN connection.



**Figure 1: Network Topology Used for Testing**

## 4. Equipment and Software Validated

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

Equipment	Software
Avaya S8730 Server	Avaya Aura® Communication Manager 5.2.1 Service Pack 4.01
Avaya G650 Media Gateway CLAN -TN799DP MEDPRO- TN2302AP	HW 01 FW 038 HW 08 FW 057
Avaya S8510 Server	Avaya Aura® Application Enablement Services 4.2.2
Avaya 9600 Series IP Telephones	H.323 Firmware 3.1.1
Avaya one-X® Communicator	Avaya one-X® Communicator 5.2.0.23 (H.323)
Fortek VISION	3.22.15
Fortek Telephony Server	2.1
Fortek Telephony Management Client	1.14

## 5. Configure Avaya Aura® Communication Manager

These Application Notes assume that Communication Manager is installed and operational. This section describes the steps for configuring the Communication Manager ACD routing and connectivity to AES. The configuration steps described are also applicable to other Linux-based Avaya Servers and Media Gateways running Communication Manager.

### 5.1. Confirm Necessary Features

The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity. Log into the Communication Manager SAT interface and use the **display system-parameters customer-options** command to determine these values. On **Page 3** verify the fields **ARS** and **Computer Telephony Adjunct Links** are set to **y**.

<b>display system-parameters customer-options</b>	<b>Page 3 of 11</b>
OPTIONAL FEATURES	
Abbreviated Dialing Enhanced List? n	Audible Message Waiting? n
Access Security Gateway (ASG)? n	Authorization Codes? y
Analog Trunk Incoming Call ID? n	CAS Branch? n
A/D Grp/Sys List Dialing Start at 01? n	CAS Main? n
Answer Supervision by Call Classifier? n	Change COR by FAC? n
ARS? y	Computer Telephony Adjunct Links? y
ARS/AAR Partitioning? y	Cvg Of Calls Redirected Off-net? n

On **Page 6** confirm that the call centre features highlighted below are activated.

```

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

Call Center Release: 5.0

ACD? y
BCMS (Basic)? y
BCMS/VuStats Service Level? n
BSR Local Treatment for IP & ISDN? n
Business Advocate? n
Call Work Codes? n
DTMF Feedback Signals For VRU? n
Dynamic Advocate? n
Expert Agent Selection (EAS)? y
EAS-PHD? n
Forced ACD Calls? n
Least Occupied Agent? n
Lookahead Interflow (LAI)? n
Multiple Call Handling (On Request)? n
Multiple Call Handling (Forced)? n
PASTE (Display PBX Data on Phone)? n

Reason Codes? n
Service Level Maximizer? n
Service Observing (Basic)? y
Service Observing (Remote/By FAC)? n
Service Observing (VDNs)? n
Timed ACW? n
Vectoring (Basic)? y
Vectoring (Prompting)? y
Vectoring (G3V4 Enhanced)? y
Vectoring (3.0 Enhanced)? y
Vectoring (ANI/II-Digits Routing)? n
Vectoring (G3V4 Advanced Routing)? y
Vectoring (CINFO)? n
Vectoring (Best Service Routing)? n
Vectoring (Holidays)? n
Vectoring (Variables)? y

```

On **Page 9** confirm **Adjunct Routing**, is set to **y**.

```

display system-parameters customer-options                                     Page 9 of 11
ASAI ENHANCED FEATURES

Adjunct Routing? y
CTI Stations? y
Increased Adjunct Route Capacity? n
Phantom Calls? y

```

## 5.2. Define Feature Access Codes (FAC)

A FAC (feature access code) should be defined for each feature that will be used. Use **change feature-access-codes** to define the required access codes. On **Page 1** define a **Auto Route Selection (ARS) - Access Code**. This is required by Fortek VISION when placing external calls.

```

change feature-access-codes                                                  Page 1 of 8
FEATURE ACCESS CODE (FAC)
Abbreviated Dialing List1 Access Code:
Abbreviated Dialing List2 Access Code:
Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
Announcement Access Code: *56
Answer Back Access Code: *59
Attendant Access Code:
Auto Alternate Routing (AAR) Access Code:
Auto Route Selection (ARS) - Access Code 1: 9
Access Code 2:
Automatic Callback Activation: Deactivation:
Call Forwarding Activation Busy/DA: All: Deactivation:

```

### 5.3. Configure Node-Names IP

Use the **change node-names ip** command. Add an entry in the node-names form for the CLAN, AES server and the default gateway used for the IP network the CLAN will be connected to. A **Name** and **IP Address** should be added for each. The values used during the interoperability test are highlighted below.

```
change node-names ip                                     Page 1 of 2
                                                    IP NODE NAMES
      Name                IP Address
CLAN1                  10.10.16.23
CLAN2                    10.10.16.27
Gateway                10.10.16.1
MedPro1                  10.10.16.24
SM100                    10.10.16.11
default                  0.0.0.0
devconaes              10.10.16.30
procr                    10.10.16.20
sesactive                10.10.16.5
( 16 of 16 administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

### 5.4. Configure CLAN for AES Connectivity

Add the C-LAN to the system configuration using the **add ip-interface n** command, where **n** is the CLAN board location. Enter the CLAN node name assigned in Section 5.3 to the **Node Name** field. Enter values for the **Subnet Mask** and **Gateway Node Name** fields. In this case, **/24** and **Gateway** are used to correspond to the network configuration in these Application Notes. Set the **Enable Interface** field to **y**, and use a separate **Network Region** for the CLAN dedicated for AES connectivity. Default values may be used in the remaining fields.

```
add ip-interface 01a02                                   Page 1 of 3
                                                    IP INTERFACES
      Type: C-LAN
      Slot: 01A02      Target socket load and Warning level: 400
      Code/Suffix: TN799 D      Receive Buffer TCP Window Size: 8320
Enable Interface? y          Allow H.323 Endpoints? y
      VLAN: n              Allow H.248 Gateways? y
      Network Region: 1      Gatekeeper Priority: 5

                                                    IPV4 PARAMETERS
      Node Name: CLAN1
      Subnet Mask: /24
      Gateway Node Name: Gateway

      Ethernet Link: 1
      Network uses 1's for Broadcast Addresses? y
```



## 5.5. Configure Transport Link for Application Enablement Services Connectivity

To administer the transport link to AES use the **change ip-services** command. On **Page 1** add an entry with the following values:

- **Service Type:** should be set to **AESVCS**
- **Enabled:** set to **y**
- **Local Node:** set to the node name assigned for the CLAN in **Section 5.3**
- **Local Port** Retain the default value of **8765**

change ip-services					Page	1 of	4
IP SERVICES							
Service	Enabled	Local	Local	Remote	Remote		
Type		Node	Port	Node	Port		
AESVCS	y	CLAN1	8765				

Go to **Page 4** of the ip-services form, and enter the following values:

- **AE Services Server:** Name obtained from the AES server, in this case **devconaes**
- **Password:** Enter a password to be administered on the AES server
- **Enabled:** Set to **y**

**Note:** The name and password entered for the **AE Services Server** and **Password** fields must match the name and password on the AES server in **Section 6.2**. The administered name for the AES server is created as part of the AES installation, and can be obtained from the AES server by typing **uname -n** at the Linux command prompt.

change ip-services				Page 4 of 4
AE Services Administration				
Server ID	AE Services Server	Password	Enabled	Status
1:	devconaes	gatekeeper123	y	in use
2:				

## 5.6. Configure CTI Link for TSAPI Service

Add a CTI link using the **add cti-link n** command. Enter an available extension number in the **Extension** field. Enter **ADJ-IP** in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

```
add cti-link 1                                     Page 1 of 3
CTI LINK
CTI Link: 1
Extension: 3700
Type: ADJ-IP
Name: AESCTILink1                                COR: 1
```

## 5.7. Configure Fortek VISION Stations

For these application notes Fortek VISION will use Avaya one-X Communicator to provide voice to the Fortek VISION operator. Avaya one-X Communicator will register to the Communication Manager with station details configured in this section. Use the command **add station n**. In the station form, set the **Type** to **4621**, provide a descriptive **Name** and specify a **Security Code** used to login as the station, Set the **IP Softphone** fields to **y**.

```
add station 6635                                     Page 1 of 5
STATION
Extension: 6635                                     Lock Messages? n      BCC: 0
Type: 4621                                           Security Code: 6635   TN: 1
Port:                                                Coverage Path 1:      COR: 1
Name: Fortek Op1                                     Coverage Path 2:      COS: 1
Hunt-to Station:
STATION OPTIONS
Loss Group: 19                                     Time of Day Lock Table:
Speakerphone: 2-way                               Personalized Ringing Pattern: 1
Display Language: english                         Message Lamp Ext: 6635
Survivable GK Node Name:                          Mute Button Enabled? y
Survivable COR: internal                           Expansion Module? n
Survivable Trunk Dest? y                           Media Complex Ext:
IP SoftPhone? y
IP Video Softphone? n
Customizable Labels? y
```

On **Page 3** ensure that two call appearances (**call-appr**) and a **release** button are configured under **BUTTON ASSIGNMENTS**.

add station 6635		Page 3 of 5
STATION		
SITE DATA		
Room:		Headset? n
Jack:		Speaker? n
Cable:		Mounting: d
Floor:		Cord Length: 0
Building:		Set Color:
ABBREVIATED DIALING		
List1:	List2:	List3:
<b>BUTTON ASSIGNMENTS</b>		
1: call-appr	5:	
2: call-appr	6:	
3:	7:	
4: release	8:	

## 5.8. Configure Fortek VISION Call Queues

For the example configuration a number of VDNs and vectors were set to provide call routing. Three call queues and one Call hold queue were configured. The configuration for the Call queue VDNs and vectors are identical so only the configuration of the first call queue and call hold queue are discussed. Further call queues may be configured by repeating the following steps.

### 5.8.1. Configure Call Queues

Use the command **change vector n** and assign a descriptive **Name** to the Call Vector. Fortek VISION is responsible for routing each received call, as such the call vector is configured with a number of adjunct routing steps to hand the routing decision to Fortek VISION. The adjunct routing link defined in **Section 5.6** is used. If a call is not routed after the first adjunct routing step the vector will wait 10 seconds before attempting another adjunct route, if after the third attempt the call is not routed by Fortek VISION then the call will default to an emergency fall back location, in this example extension **6620** is used.

change vector 10		Page 1 of 6
CALL VECTOR		
Number: 10	Name: Fortek Q1	
Multimedia? n	Attendant Vectoring? n	
Basic? y	EAS? y	
Prompting? n	LAI? n	
Variables? y	3.0 Enhanced? y	
01 adjunct	routing link 1	
02 wait-time	10 secs hearing ringback	
03 adjunct	routing link 1	
04 wait-time	10 secs hearing ringback	
05 adjunct	routing link 1	
06 wait-time	10 secs hearing ringback	
07 route-to	number 6620 with cov n if unconditionally	
08 stop		

Each call vector must have an associated VDN (Vector Directory Number). Fortek VISION will use the VDN extension to monitor call queues. Use the command **add vdn n** and assign a descriptive **Name** to the VDN. For the **Destination: Vector Number** field enter the vector number configured in the previous step. Set **Allow VDN Override** to **y**.

```

add vdn 1010                                     Page 1 of 3
                                         VECTOR DIRECTORY NUMBER

      Extension: 1010
      Name*: Fortek Q1
      Destination: Vector Number      10
Attendant Vectoring? n
Meet-me Conferencing? n
  Allow VDN Override? y
      COR: 1
      TN*: 1
      Measured: none
  
```

Repeat these steps for each call queue required.

### 5.8.2. Configure Call Hold Queue

Fortek VISION uses a VDN and Vector as a holding location for parked calls. This allows other operators the ability to pick up a call that has been parked. Use the command **change vector n** and assign a descriptive **Name** to the Vector. As with the call queue VDN Fortek VISION is responsible for routing each call received by the vector, this vector attempts an adjunct route every 30 seconds until the call is routed or the caller disconnects. Unlike the call queue vector there is no fallback location.

```

change vector 13                                Page 1 of 6
                                         CALL VECTOR

      Number: 13      Name: Fortek Hold
Multimedia? n      Attendant Vectoring? n      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? y      3.0 Enhanced? y
01 wait-time      1      secs hearing silence
02 adjunct      routing link 1
03 wait-time      30      secs hearing silence
04 adjunct      routing link 1
05 goto step      3      if unconditionally
06 stop
07
  
```

To assign a Call hold VDN use the command **add vdn n** and assign a descriptive **Name** to the VDN. For the **Destination: Vector Number** field enter the vector number configured in the previous step. Leave the **Allow VDN Override** field with the default value of **n**.

```
add vdn 1013                                     Page 1 of 3
                                         VECTOR DIRECTORY NUMBER

      Extension: 1013
      Name*: Fortek Hold VDN
      Destination: Vector Number      13
Attendant Vectoring? n
Meet-me Conferencing? n
  Allow VDN Override? n
      COR: 1
      TN*: 1
      Measured: none
```

Use the command **list vdn** to display all configured VDNs.

```
list vdn
                                         VECTOR DIRECTORY NUMBERS
```

Name (22 characters)	Ext/Skills	VDN Ovr	COR	TN	PRT	Vec Num	Meas	Orig Annc	Evnt Noti Adj
Fortek Q1	1010	y	1	1	V	10	none		
Fortek Q2	1011	y	1	1	V	11	none		
Fortek Q3	1012	y	1	1	V	12	none		
Fortek Hold VDN	1013	n	1	1	V	13	none		

## 6. Configure Avaya Aura® Application Enablement Services

This section covers the administration of Application Enablement Services (AES). AES is configured via an Internet browser using the Administration web interface. It is assumed that AES software and the license file have already been installed.

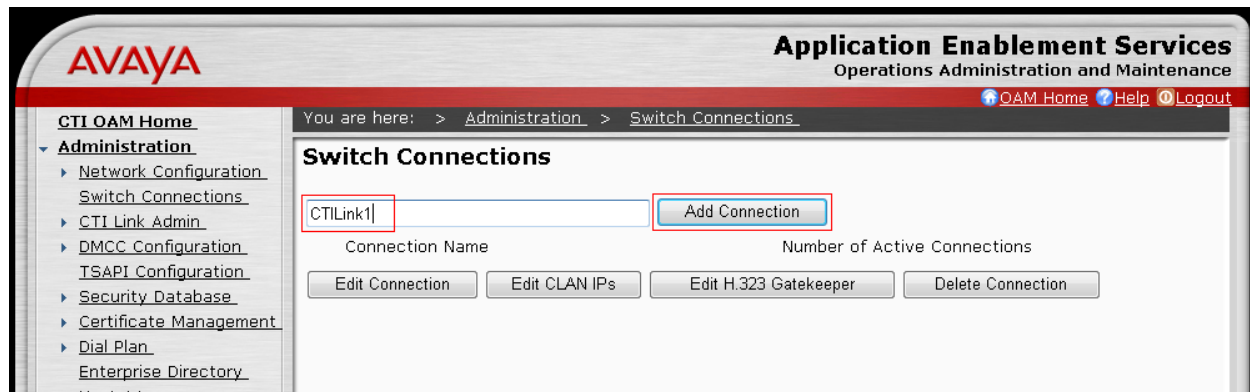
### 6.1. Logging in to Avaya Aura® Application Enablement Services

To access the administration web interface, enter **https://<ip-addr>/MVAP** as the URL in an Internet browser, where <ip-addr> is the IP address of AES. The login screen is displayed, log in with the appropriate credentials and then select the **Login** button.



## 6.2. Add Switch Connection

From the left pane of the Administration web interface, navigate to **Administration** → **Switch Connections**. Enter a name for the switch connection to be added and select the **Add Connection** button.



In the resulting screen enter and confirm the **Switch Password**. This must match the password configured in **Section 5.5**. When finished select the **Apply** button.

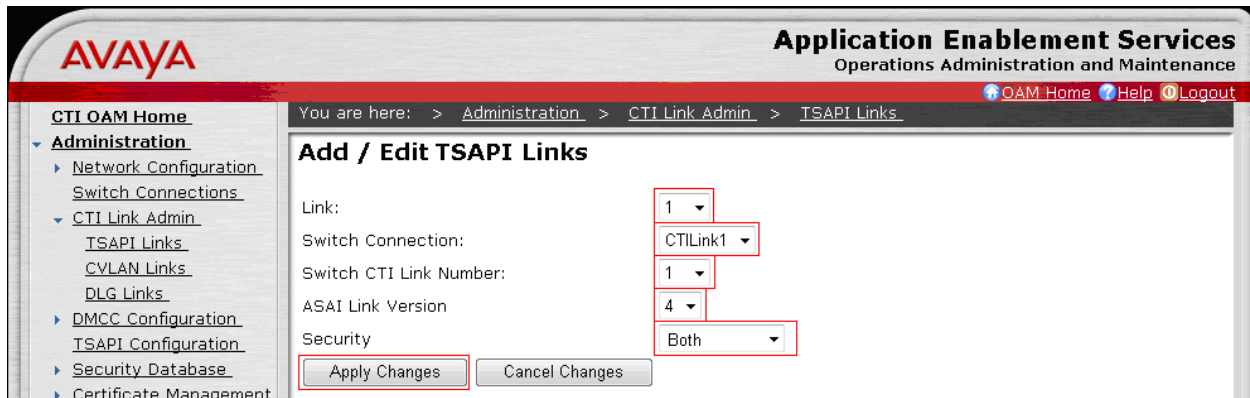


Back in the **Switch Connections** screen select the radio button for the recently added switch connection and select the **Edit CLAN IPs** button (not shown). In the resulting screen enter the IP address of the CLAN that will be used for the AES connection and select the **Add Name or IP** button.

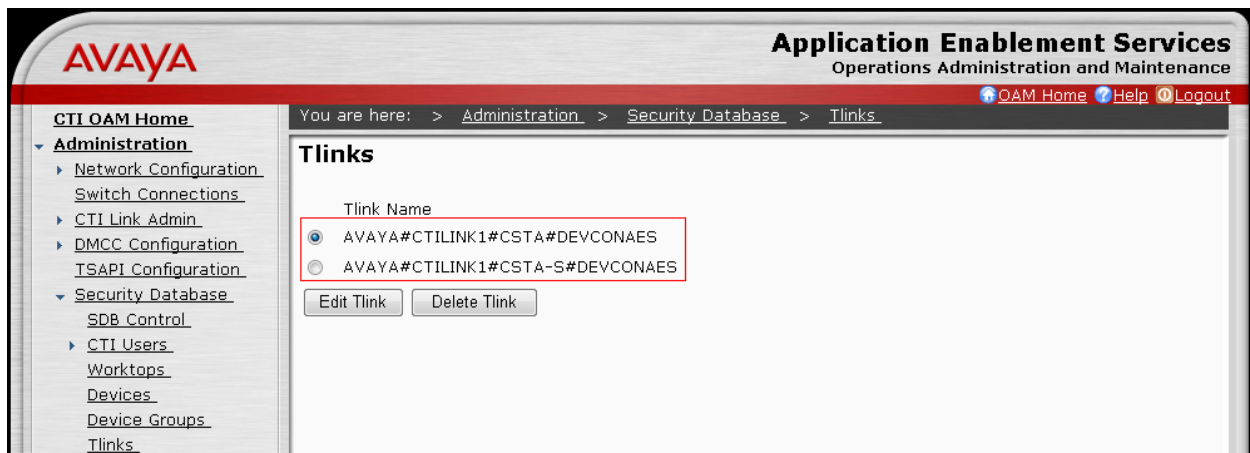


### 6.3. Add TSAPI Link

From the left pane of the Administration web interface, navigate to **Administration → CTI Link Admin → TSAPI Links**. For **Link** select the next available link number using the drop down menu. For the **Switch Connection** field select the switch connection defined in **Section 6.2**. The **Switch CTI Link Number** must match the CTI link configured number in **Section 5.6**. Ensure that the **ASAI Link Version** field is set to **4**. Set the **Security** field to **Both** to create a secure and a non-secure TSAPI link. When all the values have been set, select the **Apply Changes** button.



Once the TSAPI link has been added navigate to **Administration → Security Database → Tlinks** to view the **Tlink Name**. The secure connection is the second link in the screen below and is denoted by the characters **CSTA-S** in the **Tlink Name**.






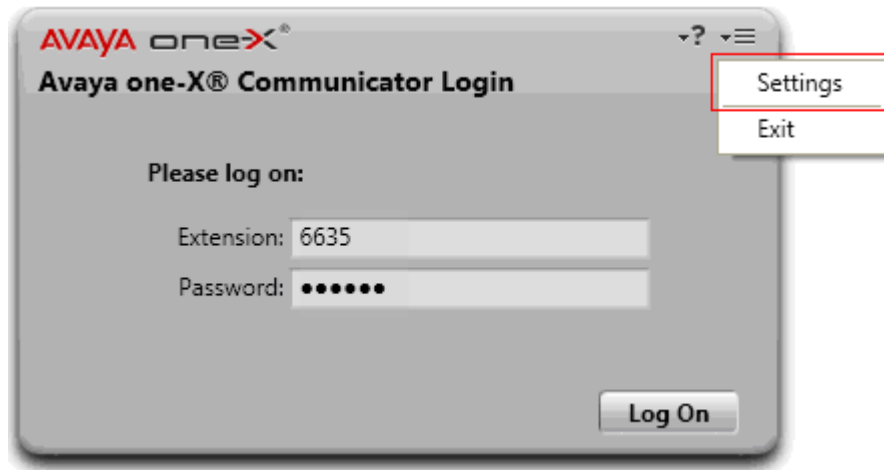
## 6.4. Add TSAPI User

From the left pane of the Administration web interface, navigate to **User Management** → **Add User**. From the **Add User** screen enter values for all of the compulsory fields marked with \*. The **User ID** and **User Password** are used in the configuration of Fortek Vision. In addition to the compulsory fields the **CT User** field should be set to **Yes**. When complete select the **Apply** button (not shown).

The screenshot displays the Avaya Application Enablement Services (AES) Administration and Monitoring (AAM) web interface. The top header features the Avaya logo and the text 'Application Enablement Services Operations Administration and Monitoring'. A breadcrumb trail indicates the current location: 'You are here: > User Management > Add User'. The left sidebar contains a navigation menu with 'User Management Home' and a list of links: 'List All Users', 'Add User', 'Search Users', 'Modify Default User', 'Change User Password', 'Service Management', and 'Help'. The main content area is titled 'Add User' and includes a note: 'Fields marked with \* can not be empty.' The form contains the following fields: '\* User Id' (text input with 'Fortek'), '\* Common Name' (text input with 'Fortek'), '\* Surname' (text input with 'Fortek'), '\* User Password' (password input with masked characters), '\* Confirm Password' (password input with masked characters), 'Admin Note' (text input), 'Avaya Role' (dropdown menu with 'None' selected), 'Business Category' (text input), 'Car License' (text input), 'CM Home' (text input), 'Css Home' (text input), 'CT User' (dropdown menu with 'Yes' selected), and 'Department Number' (text input). Red rectangular boxes highlight the compulsory fields marked with an asterisk.

## 7. Configure Avaya one-X® Communicator

These Application Notes assume that Avaya one-X Communicator is already installed. This section focuses only on the configuration needed to login Avaya one-X communicator. After starting Avaya one-X Communicator, select  → **Settings** from the menu as shown below.



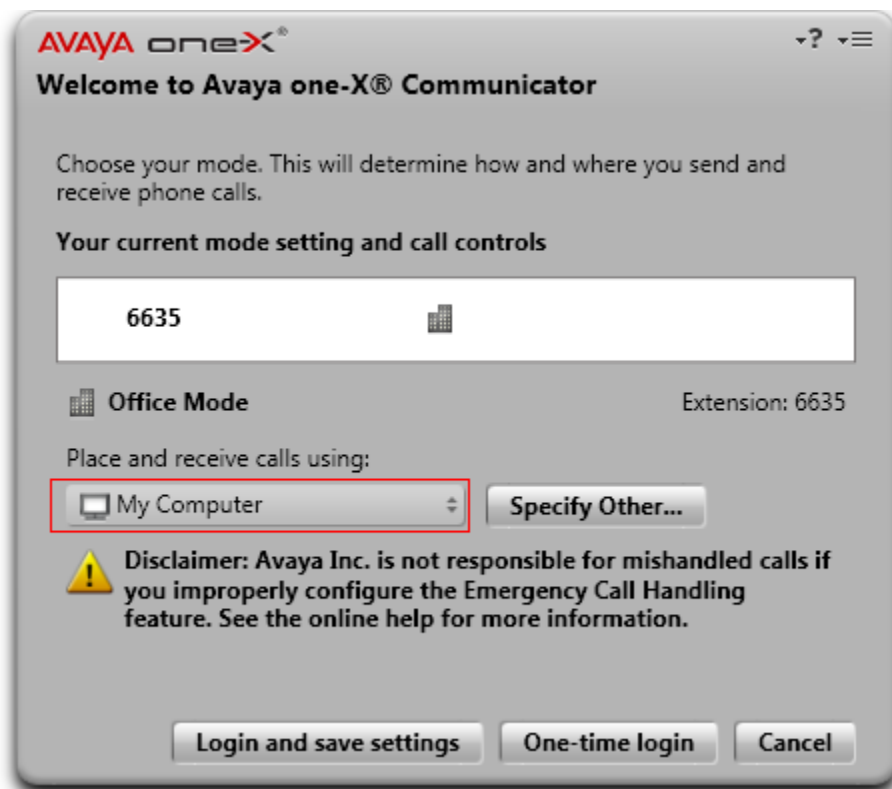
In the resulting screen select **Phone** from the left panel. In the **Server** field enter the IP address of the CLAN that Avaya one-X Communicator will register to. For **Extension** and **Password** fields enter the extension number and password set up in **Section 5.7**. Click **OK**.

The screenshot shows a 'General Settings' dialog box with a 'Phone' tab selected in the left sidebar. The main area is titled 'Phone' and contains three input fields: 'Server' with the value '10.10.16.23', 'Extension' with the value '6635', and 'Password' with masked characters '•••••'. These three fields are enclosed in a red rectangular box. Below these fields is a section titled 'Alternate Server Addresses' with a large empty text area and two buttons, 'Add' and 'Remove', positioned below the text area. At the bottom of the dialog box are three buttons: 'Discover', 'OK', and 'Cancel'.

Click the **Log On** button on the Avaya one-X Communicator login screen.



As the VISION operators will use USB headsets, select **My Computer** for the **Place and receive calls using** field. Click **Login and save settings**.



## 8. Configure VISION

This section covers the installation and configuration steps to allow VISION to interoperate with the Avaya solution. For VISION to be able to work with the Avaya solution, some information is required at the time of install. This section describes the parts of the VISION installation that require Avaya solution information.

### 8.1. Edit AESConfiguration.xml File

For VISION to interoperate correctly with the Avaya solution it requires some information to be declared in the **AESConfiguration.xml** file used by the Fortek telephony server. The required information includes the AES connection information, all operator extensions and VDN numbers. To edit the xml file navigate to **C:\FortekTelephonyServer\Avaya\AES** and edit the **AESConfiguration.xml** file.

- For **ServerName** enter the Tlink name verified in **Section 6.3**
- For **UserName** and **Password** enter the CTI username and password configured in **Section 6.4**
- If fallback is to be used then a fall back extension should be specified as **DefaultFallbackExtension** this can be any valid extension on Communication Manager (e.g. station or VDN)
- Each extension number that will be used by a VISION agent needs to be defined as a **Device**, this includes the default fallback extension.
- **The VDN number for each Call queue is defined within the AESConfiguration file as a DeviceIdentifier, each call queue also has a QueueName this is displayed to the VISION agent and is used to identify the type of call.**

```
<AESConfiguration>
  <ServerName>AVAYA#CTILINK1#CSTA#DEVCONAES</ServerName>
  <UserName>Fortek</UserName>
  <Password>Fortek123#</Password>
  <ReconnectionPeriod>5000</ReconnectionPeriod>
  <DllPath>.\Avaya\AES\Dependencies</DllPath>

  - --<text removed for brevity>---

  <FallbackOptions>
    <FallbackEnabled>>false</FallbackEnabled>
    <DefaultTimeBeforeFallback>300</DefaultTimeBeforeFallback>
    <DefaultFallbackExtension>6620</DefaultFallbackExtension>
  </FallbackOptions>
```

AESConfiguration file continued.

```
---<text removed for brevity>--

<DeviceDirectory>
  <TelephoneDirectoryEntry>
    <Device>6635</Device>
    <Location>CTILT001</Location>
  </TelephoneDirectoryEntry>
  <TelephoneDirectoryEntry>
    <Device>6636</Device>
    <Location>CTILT02</Location>
  </TelephoneDirectoryEntry>
  <TelephoneDirectoryEntry>
    <Device>6620</Device>    <!--Fallback-->
  </TelephoneDirectoryEntry>
</DeviceDirectory>

<!--Live Queues-->
<QueueInformation>
  <TSAPIQueueInfo SupportsCLI="true" NeedsRouting="true">
    <QueueName>Primary 999</QueueName>
    <DeviceIdentifier>1010</DeviceIdentifier>
  </TSAPIQueueInfo>
  <TSAPIQueueInfo SupportsCLI="true" NeedsRouting="true">
    <CLITestNumber>01384012830</CLITestNumber>
    <QueueName>Secondary 999</QueueName>
    <DeviceIdentifier>1011</DeviceIdentifier>
  </TSAPIQueueInfo>
  <TSAPIQueueInfo SupportsCLI="true" NeedsRouting="true">
    <QueueName>Agency</QueueName>
    <DeviceIdentifier>1012</DeviceIdentifier>
  </TSAPIQueueInfo>
  <TSAPIQueueInfo SupportsCLI="true" NeedsRouting="true">
    <QueueName>Hold</QueueName>
    <DeviceIdentifier>1013</DeviceIdentifier>
  </TSAPIQueueInfo>
</QueueInformation>

</AESConfiguration>
```

## 8.2. Edit TMC.ini File

On each VISION operator workstation the TMC.ini file must be configured. To edit the TMC.ini file navigate to **C:\Windows\System32\TMC.ini** and edit the **TMC.ini** file.

- Under the heading **[servers]** enter the ip address and port of the Fortek VISION server in the format of **IP=<ipaddress>:<port>**, for example, **IP=10.10.16.55:12000** is used
- Under the heading **[Softphone]** set **Softphone=AVAYA** and **KeepOpen=Yes**, this ensures that the VISION operator software will keep the Avaya one-X communicator soft client open while it is running, should Avaya one-X Communicator be closed down for some reason.
- Under the heading **[HeadsetMicrophoneMute]** set **Control=Mute** to allow VISION to mute Avaya one-X communicator via the VISION operator client

```
[Debug]
Trace=Yes
TraceLevel=511
TraceEICOMTMC=No
TraceFileTMC=C:\Vision3\Telephony\Logs\TMC.log
TraceFileVoiceRecorder=C:\Vision3\Telephony\Logs\VoiceRecorder.log

[servers]
IP=10.10.16.55:12000

[Softphone]
Softphone=AVAYA
KeepOpen=Yes

[Monitoring]
MonitorNetwork=False
MonitorPort=11003
MonitorServiceName=Fortek Call Monitor

[AudioControls]
Count=3
CONTROL1=Headset Volume
CONTROL2=Microphone Volume
CONTROL3=Speaker Volume

[Speaker Volume]
Device=Realtek HD Audio output
Line=Master Volume
Control=Master Volume

[Headset Volume]
Device=PLTDA60
Line=Speaker
Control=Volume

[Microphone Volume]
Device=PLTDA60
Line=Wave In
Control=Volume

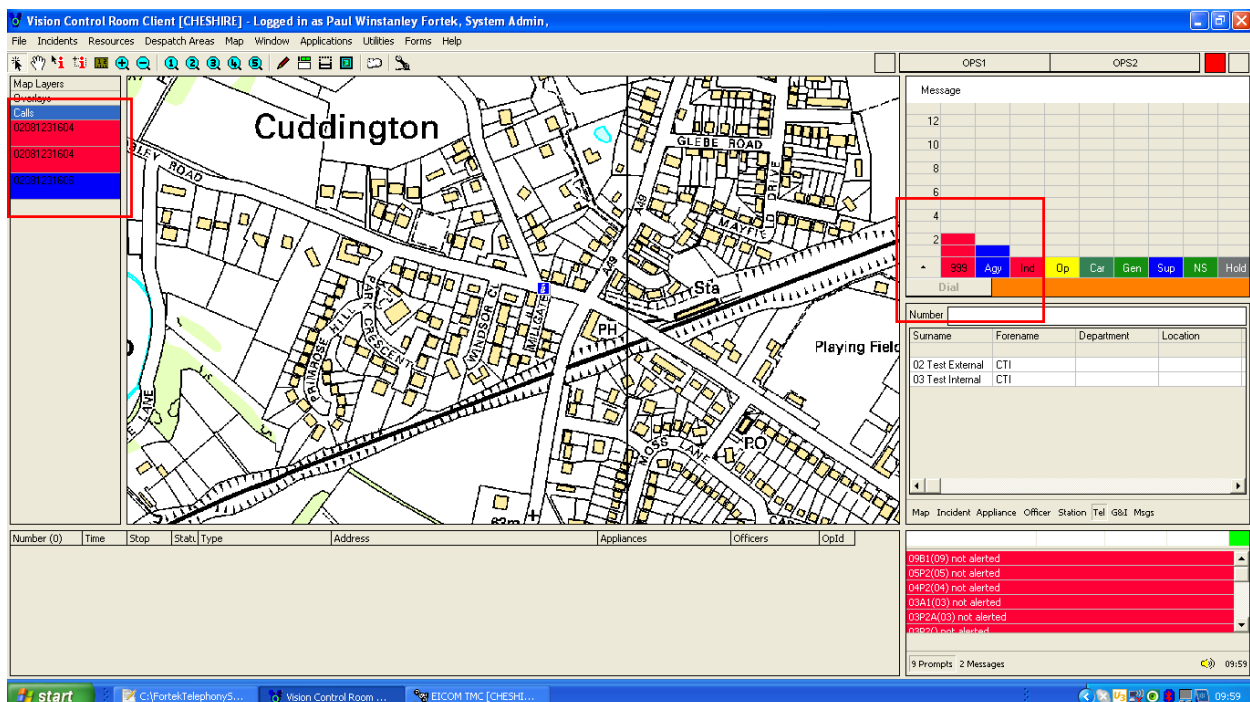
[HeadsetMicrophoneMute]
Device=PLTDA60
Line=Capture
Control=Mute
```

## 9. Log in to VISION Control Room Client as an Operator

From the VISION operator workstation double click the VISION desktop icon and in the resulting window enter appropriate login credentials and click **Log On**.

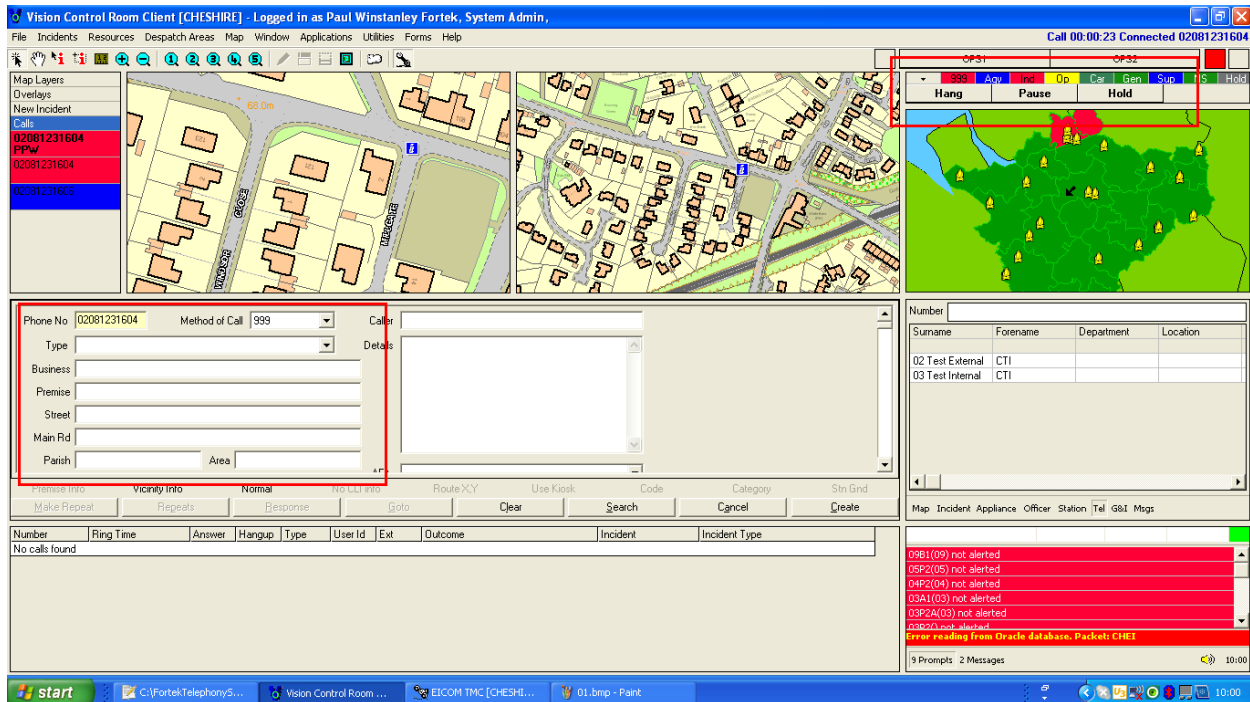


The following screen is then presented to the VISION Operator. Queued calls can be seen on the right hand side of the screen, each column represents a call queue. In the screen below two **999** calls and one **Agy** call can be seen in queue. The calling line ID for each call is displayed on the left hand side of the screen and is colour coded to match the call queue columns.





When an operator accepts a call the callers phone number and other available information is displayed and the telephony function buttons appear towards the top right of the screen.



## 10. Verification Steps

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

### 10.1. Verify Avaya Aura® Communication Manager

The following steps can ensure that the communication between Communication Manager and the Application Enablement Services server is functioning correctly. Check the TSAPI link status with Application Enablement Services by using the command **status aesvcs cti-link**. Verify the **Service State** of the TSAPI link is **established**.

<b>status aesvcs cti-link</b>						
AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	<b>Service State</b>	Msgs Sent	Msgs Rcvd
<b>1</b>	<b>4</b>	<b>no</b>	<b>devconnaes</b>	<b>established</b>	<b>14</b>	<b>14</b>

Use the command **status aesvcs interface** to verify that the **Local Node CLAN1 Status** is connected and **listening**.

<b>status aesvcs interface</b>			
AE SERVICES INTERFACE STATUS			
Local Node	Enabled?	Number of Connections	Status
<b>CLAN1</b>	<b>yes</b>	<b>1</b>	<b>listening</b>

Verify that there is a link with Application Enablement Services and that messages are being sent and received by using the command **status aesvcs link**.

<b>status aesvcs link</b>						
AE SERVICES LINK STATUS						
Srvr/ Link	AE Services Server	Remote IP	Remote Port	Local Node	Msgs Sent	Msgs Rcvd
<b>01/01</b>	<b>devconnaes</b>	<b>10.10.16.30</b>	<b>58744</b>	<b>CLAN1</b>	<b>626</b>	<b>611</b>

## 10.2. Verify Avaya Aura® Application Enablement Services

The following steps are carried out on Application Enablement Services to ensure that the communication link between Communication Manager and the Application Enablement Services server is functioning correctly.

### 10.2.1. Switch Connection

On the Application Enablement Services Management Console verify the status of the TSAPI link by selecting **Status and Control** → **Switch Conn Summary** to display the **TSAPI Link Details** screen. Verify the status of the TSAPI link by checking that the **Conn State** is **Talking** and the link is **Online**.

**AVAYA** Application Enablement Services  
Operations Administration and Maintenance

You are here: > [Status and Control](#) > [Switch Conn Summary](#)

### Switch Connections Summary

Switch Conn	Conn State	Since	Online/Offline	Active CLANs/ Admin'd CLANs	# of TCI Conns	Msgs To Switch	Msgs From Switch	Msg Period
CTILink1	Talking	2010-12-03 13:33:52.0	Online	1 / 1	2	17	17	30

## 10.3. Verify Fortek Vision

To verify Fortek VISION is communicating correctly with Application Enablement Services make a few calls to the Call queue VDNs and verify that the calls are visible to the VISION operators from the VISION Control Room Client.

## 11. Conclusion

These Application Notes describe the required configuration steps for Fortek VISION to successfully interoperate with Avaya Aura® Communication Manager 5.2.1 and Avaya Aura® Application Enablement Services 4.2.2. All feature functionality and serviceability test cases were completed successfully. Observations made during testing are noted in **Section 2.2**.

## 12. Additional References

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

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

1. *Administering Avaya Aura® Communication Manager, Document No. 03-300509, May 2009*
2. *Avaya Aura® Call Center 5.2 Call Vectoring and Expert Agent Selection (EAS) Reference, Document No. 07-600780, April 2009*
3. *Application Enablement Services Administration and Maintenance Guide Document No. 02-300357, May 2009*

Documentation for Fortek products may be requested from Fortek at <http://www.fortek.co.uk>.

---

**©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).