



## **Application Notes for Configuring Autonomy Qfiniti to Interoperate with Avaya Aura<sup>®</sup> Communication Manager and Avaya Aura<sup>®</sup> Application Enablement Services using Service Observation Mode – Issue 1.0**

### **Abstract**

These Application Notes describe a compliance-tested configuration consisting of the Autonomy Qfiniti, Avaya Aura<sup>®</sup> Communication Manager and Avaya Aura<sup>®</sup> Application Enablement Services.

Autonomy Qfiniti is a call recording solution which uses the Device, Media, and Call Control (DMCC) and TSAPI services on Application Enablement Services to record calls for Quality Monitoring and Compliance purposes.

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 consisting of the Autonomy Qfiniti, Avaya Aura<sup>®</sup> Communication Manager and Avaya Aura<sup>®</sup> Application Enablement Services.

Autonomy Qfiniti is a call recording solution which uses the Device, Media, and Call Control (DMCC) services on Application Enablement Services. All calls are recorded for Compliance recording requirements. When Quality Monitoring is required, calls matching pre-defined Quality criteria are retained, and calls that do not match the criteria are purged from the system.

In the Service Observation recording mode, Qfiniti registers recorder ports as virtual extensions on Communication Manager using the DMCC service, and initiates a Service Observation on agent stations to obtain audio from calls which subsequently route to the configured endpoints. The Service Observation is kept in effect at all times when the application is running. TSAPI monitors established through Application Enablement Services on ACD hunt groups and agent stations deliver context to tag the recordings for later analysis.

Note that Qfiniti is also capable of recording using a Streaming Media approach registering recorder ports as additional endpoints on existing agent IP or Digital stations. This Multiple Registering recording mode was tested in parallel and is described in a separate application notes document titled *Application Notes for Configuring Autonomy Qfiniti to Interoperate with Avaya Aura<sup>®</sup> Communication Manager and Avaya Aura<sup>®</sup> Application Enablement Services using Multiple Registration Mode*.

## 2. General Test Approach and Test Results

The compliance test focused on the ability for calls to be recorded. Calls were manually placed from the public switched telephone network (PSTN) directly to and from recorded devices, and to ACD queues.

### 2.1. Interoperability Compliance Testing

The compliance test validated the ability of Qfiniti to successfully record calls routed to and from Analog, Digital, IP and SIP endpoints including Call Center agents. Additional tests included the ability to record calls to and from phones with bridged appearances of other phones, and to record calls to phones with Extension to Cellular features enabled.

Additionally, testing confirmed the ability for Qfiniti to recover from common outages such as network outages and server reboots.

### 2.2. Test Results

The objectives described in **Section 2.1** were verified, a few observations are outlined below.

- When calls were handled by cell phone via EC500, calls successfully recorded when answered on either the desk or cell phone. Calls could continue to be recorded when extended from the desk to cell phone as well. However, due to a limitation in Communication Manager, calls answered on the cell and picked up on the desk did not continue recording. A fix is expected in the next releases of Communication Manager and Application Enablement Services.
- When Bridged Appearance calls occurred, inbound calls would not successfully record without the SA7900 Special Application feature enabled on Communication Manager. Enabling this feature however resulted in failure to record outbound calls. This was not an issue when the Media Streaming solution was used as described in the alternate configuration Application Notes referenced in **Section 1**.
- When Bridged Appearances were configured, Service Observation was possible when Automatic Exclusions were enabled in the Class of Service for the stations only if the **Service Observing Allowed with Exclusion** feature was enabled in the system-parameters features on Communication Manager.

### 2.3. Support

Information, documentation and technical support for Autonomy products can be obtained at:

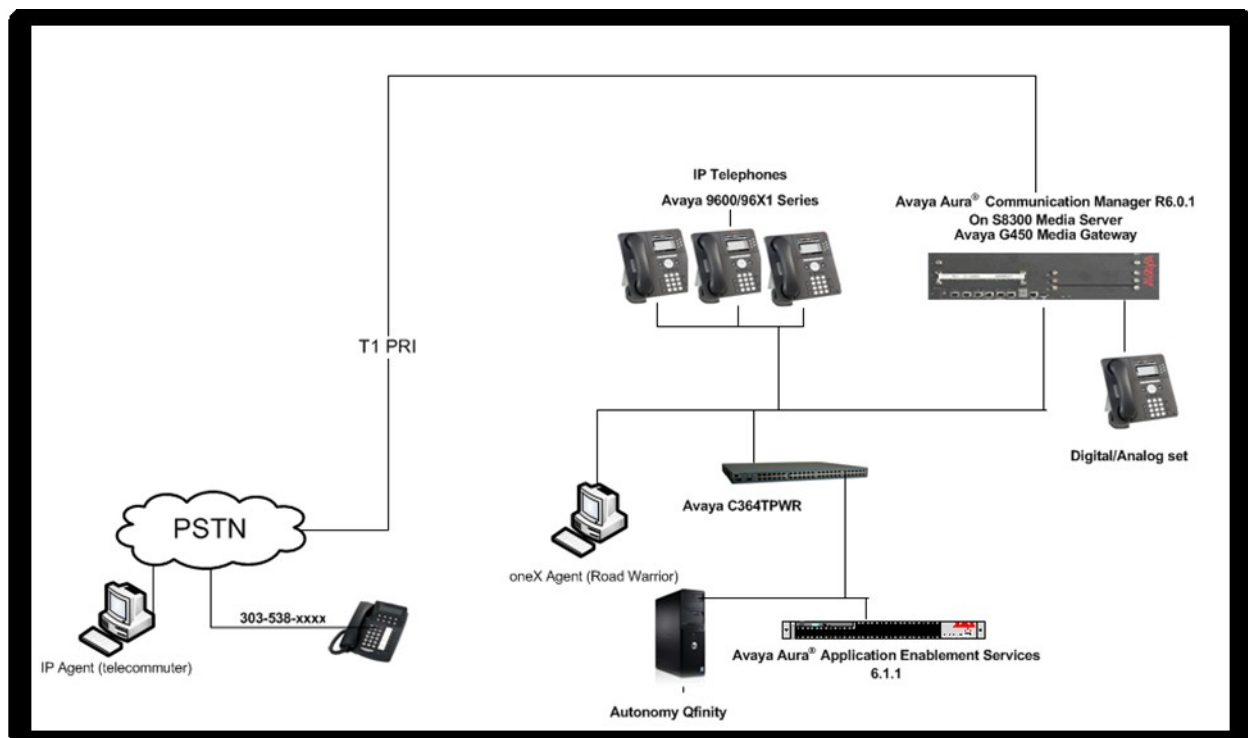
- Phone: 1 (415) 243 9955
- Web: <http://www.autonomy.com>
- Email: [autonomy@autonomy.com](mailto:autonomy@autonomy.com)

### 3. Reference Configuration

**Figure 1** illustrates the compliance test configuration consisting of:

- Avaya Aura® Communication Manager R6.0.1
- Avaya Aura® Application Enablement Services R6.1.1
- Various IP, SIP and Digital endpoints
- IP Agent and Avaya one-X® Agent softphones
- Autonomy Qfiniti server

Calls routed to and from Communication Manager used PRI trunks to connect to the PSTN. Calls to SIP endpoints used Avaya Aura® Session Manager (not shown in the diagram). The Session Manager configuration was in place to support SIP endpoints and did not require any configuration to accommodate this solution. Therefore, details of this part of the configuration will not be covered in these Application Notes.



**Figure 1 – Autonomy Qfiniti Compliance Test Configuration**

## 4. Equipment and Software Validated

The following equipment and software/firmware versions were used in the reference configuration described above:

Equipment	Version
Avaya S8300 Server with G450 Media Gateway	Avaya Aura <sup>®</sup> Communication Manager R6.0.1 SP5
Dell R610 Server	Avaya Aura <sup>®</sup> Application Enablement Services R6.1.1 on Avaya System Platform
Avaya Phones 9600 Series IP Phones 96x1 Series IP Phones Avaya oneX <sup>®</sup> Agent Avaya IP Agent	H.323 ver 3.11/SIP ver 2.6.4 H.323 ver 3.11/SIP ver 2.6.4 R2.5 R7.0
Windows 2003 Server	Autonomy Qfiniti R3.5 SP2 U2

## **5. Configure Avaya Aura® Communication Manager**

All the configuration changes in this section for Communication Manager are performed through the System Access Terminal (SAT) interface. For more details on configuring Communication Manager, refer to the Avaya product documentation, Reference [1].

### **5.1. Configure Communication Manager Details**

This section provides the procedures for configuring Communication Manager. The procedures include the following areas:

- Verify Feature and License for the integration
- Configure system-wide features
- Administer Ethernet Interface for Avaya Aura® Application Enablement Services
- Administer Computer Telephony Integration (CTI) Link
- Add Qfiniti Virtual Extensions

The detailed administration of call center entities, such as VDN, Skill, Split, Logical Agents and Station Extensions are assumed to be in place and are not covered in these Application Notes.

Step	Description
1.	<p><b>Verify Feature and License for the integration</b></p> <p>Applications that use Application Enablement Services TSAPI must have <b>Computer Telephony Adjunct Links</b> enabled on Communication Manager. This feature entitlement is provided with each TSAPI license purchased for Application Enablement Services. TSAPI entitlements must be activated in both the Application Enablement Services and Communication Manager licenses. If this option is not set to “y”, contact the Avaya sales team or business partner for a proper license file.</p>
	<div><div>display system-parameters customer-options</div><div>Page3 of 11</div><div>OPTIONAL FEATURES</div><div><div><div>Abbreviated Dialing Enhanced List? y</div><div>Access Security Gateway (ASG)? n</div><div>Analog Trunk Incoming Call ID? y</div><div>A/D Grp/Sys List Dialing Start at 01? y</div><div>Answer Supervision by Call Classifier? y</div><div>ARS? y</div><div>ARS/AAR Partitioning? y</div><div>ARS/AAR Dialing without FAC? n</div><div>ASAI Link Core Capabilities? n</div><div>ASAI Link Plus Capabilities? n</div><div>Async. Transfer Mode (ATM) PNC? n</div><div>Async. Transfer Mode (ATM) Trunking? n</div><div>ATM WAN Spare Processor? n</div><div>ATMS? y</div><div>Attendant Vectoring? y</div></div><div><div>Audible Message Waiting? y</div><div>Authorization Codes? y</div><div>CAS Branch? n</div><div>CAS Main? n</div><div>Change COR by FAC? n</div><div><b>Computer Telephony Adjunct Links? y</b></div><div>Cvg Of Calls Redirected Off-net? y</div><div>DCS (Basic)? y</div><div>DCS Call Coverage? y</div><div>DCS with Rerouting? y</div><div>Digital Loss Plan Modification? y</div><div>DS1 MSP? y</div><div>DS1 Echo Cancellation? y</div></div></div></div>
	<p>Each port or virtual extension the recorder will use to Service Observe agent phones will require an <b>IP_API_A</b> license if not licensed on Application Enablement Services.</p>
	<div><div>display system-parameters customer-options</div><div>Page9 of 10</div><div>MAXIMUM IP REGISTRATIONS BY PRODUCT ID</div><div><div><div>Product ID</div><div>Rel. Limit</div><div>Used</div></div><div><div><b>IP_API_A</b></div><div><b>: 100</b></div><div><b>0</b></div></div></div></div>

Step	Description
2.	<p><b>Configure system-wide features</b></p> <p>Service Observation solutions may require settings for certain situations. Use the <b>change system-parameters features</b> command to make these changes.</p> <p>When recording warning tones are required, enable the <b>Service Observing: Warning Tone</b> setting.</p> <p>If bridged calling is used with Exclusions, enable the <b>Service Observing Allowed with Exclusion</b> setting to enable the recorder ports to join calls with exclusions.</p> <p>If more than one Service Observation is required on the same call, such as for redundant servers or to allow supervisors to live monitor recorded calls, enable the <b>Allow Two Observers in Same Call</b> setting.</p>
	<div> <div>change system-parameters features</div> <div> <div>FEATURE-RELATED SYSTEM PARAMETERS</div> <div>CALL CENTER SYSTEM PARAMETERS</div> <div>EAS</div> <div> <div>Expert Agent Selection (EAS) Enabled? y</div> <div>Minimum Agent-LoginID Password Length: 4</div> <div>Direct Agent Announcement Extension: Delay:</div> <div>Message Waiting Lamp Indicates Status For: station</div> </div> <div>VECTURING</div> <div> <div>Converse First Data Delay: 0 Second Data Delay: 2</div> <div>Converse Signaling Tone (msec): 100 Pause (msec): 70</div> <div>Prompting Timeout (secs): 10</div> <div>Interflow-qpos EWT Threshold: 2</div> <div>Reverse Star/Pound Digit For Collect Step? n</div> <div>Available Agent Adjustments for BSR? n</div> <div>BSR Tie Strategy: 1st-found</div> <div>Store VDN Name in Station's Local Call Log? n</div> </div> <div>SERVICE OBSERVING</div> <div> <div>Service Observing: Warning Tone? y or Conference Tone? n</div> <div>Service Observing Allowed with Exclusion? y</div> <div>Allow Two Observers in Same Call? y</div> </div> </div> </div> <div>Page 11 of 19</div>



Step	Description
3.	<p><b>Administer Ethernet Interface for Application Enablement Services</b> Enter the <b>change node-names ip</b> command. The Application Enablement Services and <b>procr</b> node-names need to be defined here.</p> <pre> change node-names ip                                     Page 1 of 2                                  IP NODE NAMES       Name                IP Address aesserver2             10.64.10.21 default                0.0.0.0 procr                  10.64.10.67 procr6                 :: </pre> <p>On most R6 Communication Manager servers, the Processor Ethernet Interface will already be administered in the ip-interface list. The <b>display ip-interface procr</b> command will display the parameters of the Processor Ethernet Interface.</p> <pre> display ip-interface procr                               Page 1 of 2                                  IP INTERFACES                                  Type: PROCR                                  Target socket load: 4800  Enable Interface? y                                Allow H.323 Endpoints? y                                 Allow H.248 Gateways? y Network Region: 1                                Gatekeeper Priority: 5                                  IPV4 PARAMETERS Node Name: procr                                IP Address: 10.64.10.67 Subnet Mask: /24 </pre> <pre> display ip-interface procr                               Page 2 of 2                                  IP INTERFACES  Speed: 100Mbps Duplex: Full                                  IPV6 PARAMETERS Node Name: procr6 IP Address: ::  Subnet Mask: /64 Enable Interface? n </pre>

Step	Description																		
	<p><b>Administer Ethernet Interface for Application Enablement Services (Continued)</b> Add an entry for Application Enablement Services as described below:</p> <ul style="list-style-type: none"><li>• Enter the <b>change ip-services</b> command.</li><li>• In the <b>Service Type</b> field, type <b>AESVCS</b>.</li><li>• In the <b>Enabled</b> field, type <b>y</b>.</li><li>• In the <b>Local Node</b> field, type the Node name <b>procr</b> for the Processor Ethernet Interface.</li><li>• In the <b>Local Port</b> field, use the default of <b>8765</b>.</li><li>• Note that in installations using CLAN connectivity, each CLAN interface would require similar configuration.</li></ul>																		
	<div><div>change ip-services</div><div>Page1 of4</div></div> <table><tr><th colspan="6">IP SERVICES</th></tr><tr><th>Service Type</th><th>Enabled</th><th>Local Node</th><th>Local Port</th><th>Remote Node</th><th>Remote Port</th></tr><tr><td>AESVCS</td><td>y</td><td>procr</td><td>8765</td><td></td><td></td></tr></table>	IP SERVICES						Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port	AESVCS	y	procr	8765		
IP SERVICES																			
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port														
AESVCS	y	procr	8765																
	<p>On Page 4 of the IP Services form, enter the following values:</p> <ul style="list-style-type: none"><li>• In the <b>AE Services Server</b> field, type the Node name for the Application Enablement Services server.</li><li>• In the <b>Password</b> field, type the same password to be administered on the Application Enablement Services server.</li><li>• In the <b>Enabled</b> field, type <b>y</b>.</li></ul>																		
	<div><div>change ip-services</div><div>Page4 of4</div></div> <div>AE Services Administration</div> <table><tr><th>Server ID</th><th>AE Services Server</th><th>Password</th><th>Enabled</th><th>Status</th></tr><tr><td>1:</td><td>aesserver2</td><td>*</td><td>y</td><td>in use</td></tr></table>	Server ID	AE Services Server	Password	Enabled	Status	1:	aesserver2	*	y	in use								
Server ID	AE Services Server	Password	Enabled	Status															
1:	aesserver2	*	y	in use															
	<p>Note that the name and password entered for the <b>AE Services Server</b> and <b>Password</b> fields must match the name and password on the Application Enablement Services server.</p>																		

Step	Description
4.	<p><b>Administer Computer Telephony Integration (CTI) Link</b>  Enter the <b>add cti-link</b> &lt;link number&gt; command, where &lt;link number&gt; is an available CTI link number.</p> <ul style="list-style-type: none"> <li>In the <b>Extension</b> field, type &lt;station extension&gt;, where &lt;station extension&gt; is a valid station extension.</li> <li>In the <b>Type</b> field, type <b>ADJ-IP</b>.</li> <li>In the <b>Name</b> field, type a descriptive name.</li> </ul>
	<pre> add cti-link 1                                     Page 1 of 3                                      CTI LINK CTI Link: 1 Extension: 6201 Type: ADJ-IP Name: AES-10.64.10.21                                COR: 1 </pre>
	<pre> add cti-link 1                                     Page 2 of 3                                      CTI LINK FEATURE OPTIONS Event Minimization? n      Special Character for Restricted Number? n IC Adjunct Routing? n      Send Disconnect Event for Bridged Appearance? n                                      Two-Digit Aux Work Reason Codes? n                                      Block CMS Move Agent Events? n </pre>
	<pre> add cti-link 1                                     Page 3 of 3                                      CTI LINK Bridged Appearance Origination Restriction? n SAC/CF Override: n </pre>

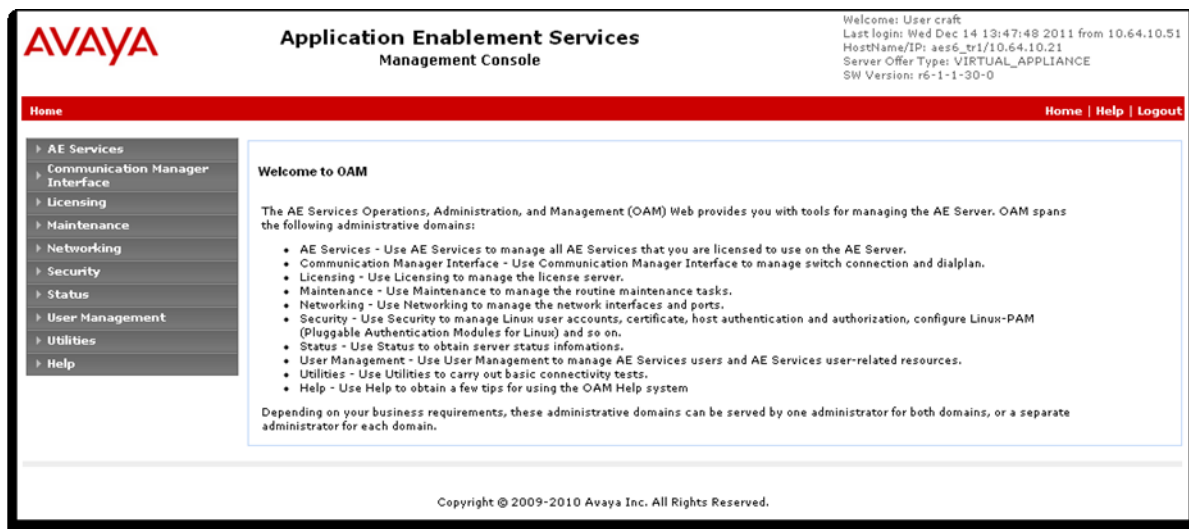
Step	Description
5.	<p><b>Add Qfiniti Virtual Extensions</b>            Use the <b>add station x</b> command to display a new station screen. Station <b>Type 4612</b> and <b>Security Code 123456</b> were used for each recording port. Use a <b>Name</b> such as <b>DMCC Port x</b> to differentiate the ports from other stations in the system. <b>IP Softphone</b> must be set to <b>y</b> for the recorder to be able to register via DMCC.</p> <pre> add station 6410                                      Page 1 of 5                                       STATION  Extension: 6410                      Lock Messages? n                BCC: 0   Type: 4612                        Security Code: 123456            TN: 1   Port: S00008                      Coverage Path 1:              COR: 1   Name: DMCC Port 1                 Coverage Path 2:              COS: 1                                      Hunt-to Station:  STATION OPTIONS                                  Time of Day Lock Table:                                 Personalized Ringing Pattern: 1                                 Message Lamp Ext: 6410                                 Mute Button Enabled? y                                 Speakerphone: 2-way                                 Display Language: english Survivable GK Node Name:                                 Survivable COR: internal Survivable Trunk Dest? y          Media Complex Ext:                                      IP SoftPhone? y                                       IP Video Softphone? n                                      Short/Prefixed Registration Allowed: default           </pre> <p>On page 4, enter <b>serv-observ</b> on <b>Button Assignment 6</b>. The application will use DMCC commands to push this specific button on each recording port in order to initiate Service Observation on the target devices.</p> <pre> add station 6410                                      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:                           List2:                           List3:  BUTTON ASSIGNMENTS   1: call-appr                      7:   2: call-appr                      8:   3: call-appr                      9:   4:                               10:   5:                               11:   6: serv-observ                   12:           </pre>

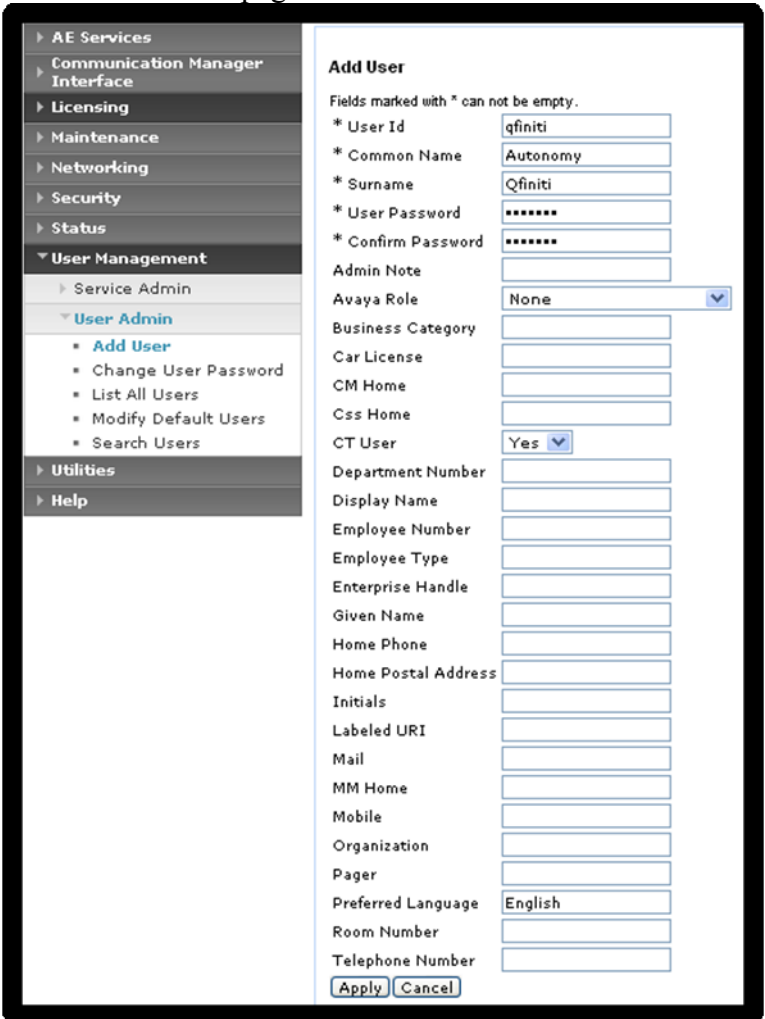
## 6. Configure Avaya Aura® Application Enablement Services

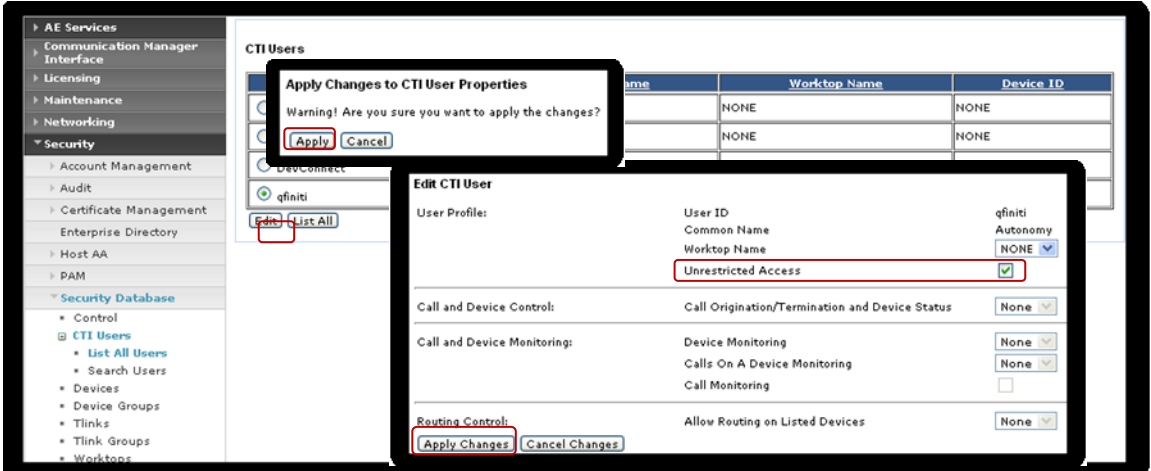
Configuration of Avaya Aura® Application Enablement Services required a user account be configured for Qfiniti. Additional information is provided to illustrate how the connectivity with Avaya Aura® Communication Manager was previously configured.

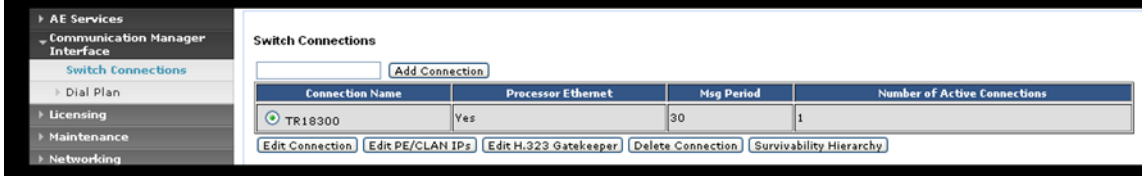
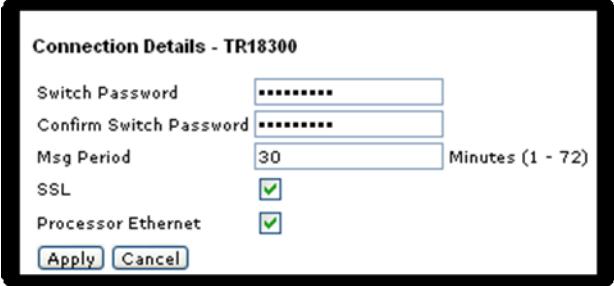

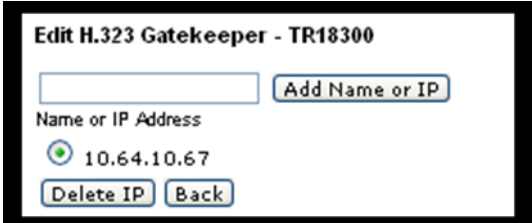
### 6.1. Configure Application Enablement Services Details

All administration is performed by web browser. Initially, users land on the Welcome to OAM page shown below. Note that all navigation is performed by clicking links in the Navigation Panel on the left side of the screen. Context panels will then appear on the right side of the screen.

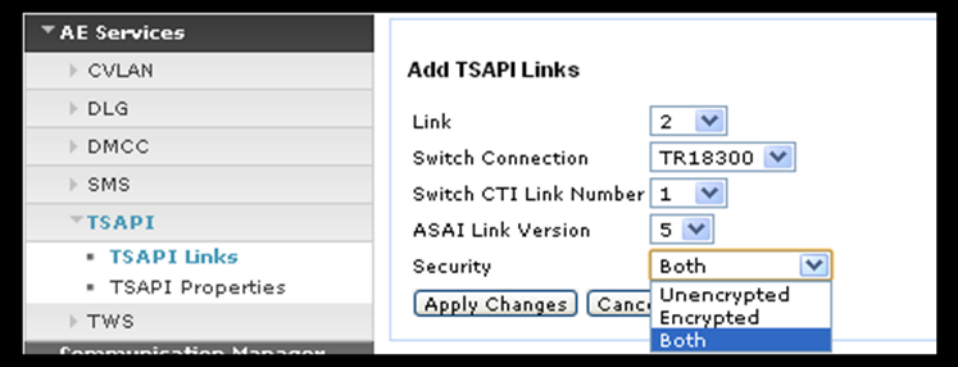
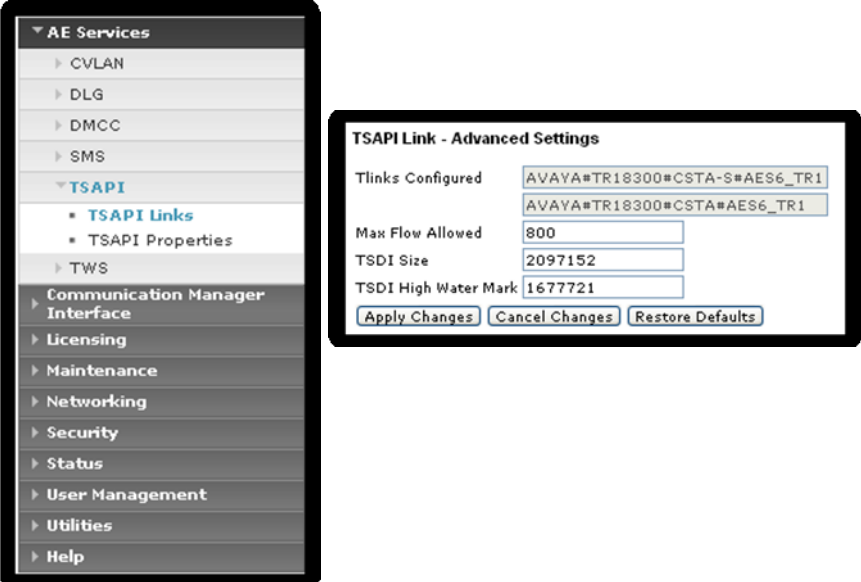


Step	Description
1.	<p><b>Configure Qfiniti user</b></p> <p>In the Navigation Panel, select <b>User Management &gt; User Admin &gt; Add User</b>. The <b>Add User</b> panel will display as shown below. Enter an appropriate <b>User Id</b>, <b>Common Name</b>, <b>Surname</b>, and <b>User Password</b>. Select <b>Yes</b> from the <b>CT User</b> dropdown list.</p> <p>Click <b>Apply</b> at the bottom of the pages to save the entries.</p> 

Step	Description
2.	<p><b>Enable Unrestricted Access</b></p> <p>If the Security Database (SDB) is enabled on Application Enablement Services, set the Qfiniti user account to Unrestricted Access to enable any device (station, ACD extension, DMCC port) to be used implicitly. This step avoids the need to duplicate administration.</p> <p>Navigate to <b>Security &gt; CTI Users &gt; List All Users</b> and select the <b>qfiniti</b> user and click <b>Edit</b>.</p> <p>On the <b>Edit CTI User</b> panel, check the <b>Unrestricted Access</b> box and click the <b>Apply Changes</b> button.</p> <p>Click <b>Apply</b> when asked to confirm the change on the <b>Apply Changes to CTI User Properties</b> dialog.</p> <p>Note, this step requires entry on multiple panels. Each panel was superimposed below to consolidate the task.</p> 

Step	Description
3.	<p data-bbox="298 233 1433 373"><b>Configure Communication Manager Switch Connections</b> To add links to the Communication Manager, navigate to the <b>Communication Manager Interface &gt; Switch Connections</b> page and enter a name for the new switch connection. This was previously configured as <b>TR18300</b> for this test environment:</p>  <p data-bbox="298 569 1433 709">Use the <b>Edit Connection</b> button shown above to configure the <b>Switch Password</b>. This must match the password configured in <b>Section 5, Step 3</b> above. Enter the <b>Switch Password</b> and check the <b>Processor Ethernet</b> box if using the <b>procr</b> interface, as shown below.</p>  <p data-bbox="298 1037 1433 1108">Use the <b>Edit PE/CLAN IPs</b> button (shown in this section's first screen shot above) to configure the <b>procr</b> or <b>CLAN IP Address(es)</b> for TSAPI message traffic.</p>  <p data-bbox="298 1331 1433 1402">Use the <b>Edit H.323 Gatekeeper</b> button (shown in this section's first screen shot above) to configure the <b>procr</b> or <b>CLAN IP Address(es)</b> for DMCC registrations.</p> 



Step	Description
<p><b>4.</b></p>	<p><b>Add TSAPI Links</b>            Navigate to the <b>AE Services -&gt; TSAPI -&gt; TSAPI Links</b> page to add the TSAPI CTI Link. Click <b>Add Link</b>.</p> <p>Select a Switch Connection using the drop down menu. Select the <b>Switch CTI Link Number</b> using the drop down menu. The <b>Switch CTI link Number</b> must match the number configured in the <b>cti-link</b> form in <b>Section 5, Step 4</b>.</p> <p>If the application will use Encrypted Links, select <b>Encrypted</b> in the <b>Security</b> selection box.</p> <p>Click <b>Apply Changes</b>.</p> 
<p><b>5.</b></p>	<p><b>Note the TLink Information</b>            Navigate to <b>AE Services &gt; TSAPI &gt; TSAPI Links</b> and note the <b>TLinks Configured</b>. This information will be used in <b>Section 7, Step 4</b>.</p> 

Step	Description
6.	<p><b>Confirm TSAPI and DMCC Licenses</b></p> <p>Qfiniti uses a <b>DMCC_DMC</b> license for each recording port. Additionally, a <b>TSAPI Basic</b> license is used for each agent station, and each skill group being monitored. If DMCC_DMC is licensed on Application Enablement Services, then an IP_API_A is generally not required on Communication Manager R5 and later. Please consult product offer documentation for more details.</p>

AVAYA

Web License Manager (WebLM v4.6)

Logout

Install License

Licensed Products

- APPL\_ENAB
  - Application Enablement
    - Configure Enterprise
    - Configure Local WebLMs
      - Add Local WebLM
      - Delete Local WebLM
      - Modify Local WebLM

Usages

- Allocations
- Periodic Status

Uninstall License

Change Password

Server Properties

Manage Users

Logout

Application Enablement (CTI) - Release: 6 - SID: 10503000 (Enterprise License File)

You are here: Licensed Products > Application Enablement (CTI) > View by Feature

License installed on: Mar 8, 2011 4:05:51 PM MST

[View by Local WebLM](#)

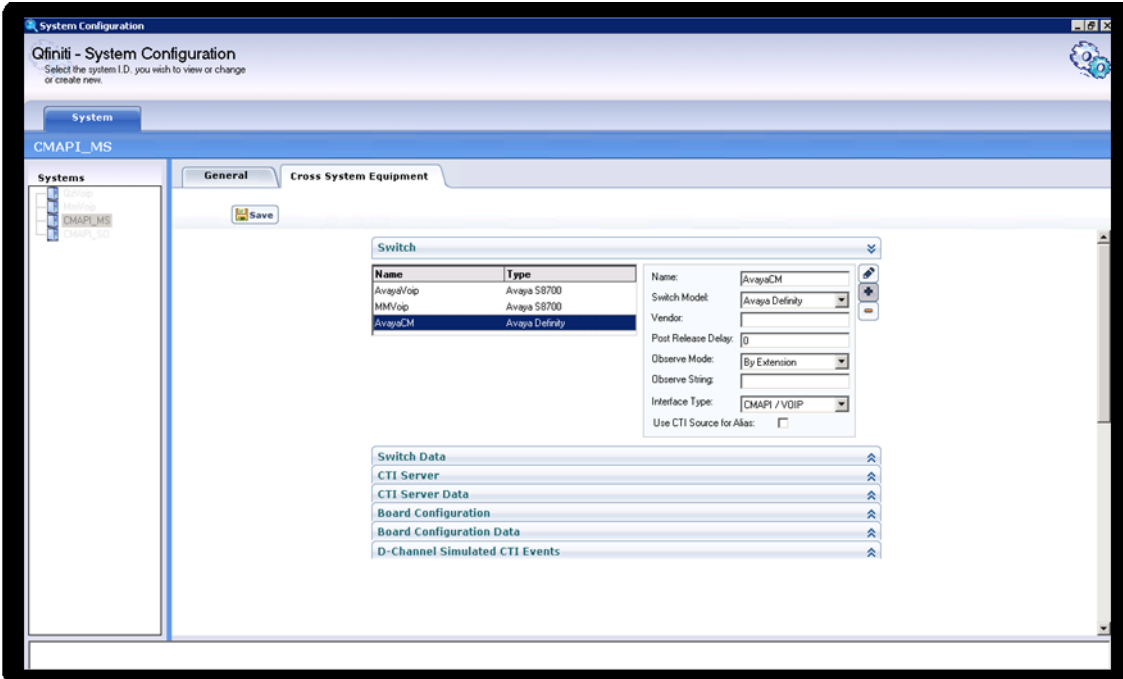
Feature (License Keyword)	License Capacity	Currently Available
CVLAN ASAT (VALUE_AES_CVLAN_ASAT)	16	16
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	1000	1000
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	3	3
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	16	16
Product Notes (VALUE_NOTES)	SmallServerTypes: s8300c;s8300d;f;c;premio;tn8400;laptop;CtiSmallServer MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_8832_vm;CtiMediumServer LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;unknown;CtiLargeServer TrustedApplications: IPS_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XM_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; PC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; OSPC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; VP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AES_UNIFIED_CC_DESKTOP, CCE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T1_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T2_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; AVAYAVERINT_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted;	Not counted
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	3	3
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	1000	1000
DLG (VALUE_AES_DLG)	16	16
Device Media and Call Control (VALUE_AES_DMCC_DMC)	1000	1000
AES ADVANCED MEDIUM SWITCH (VALUE_AES_AEC_MEDIUM_ADVANCED)	3	3

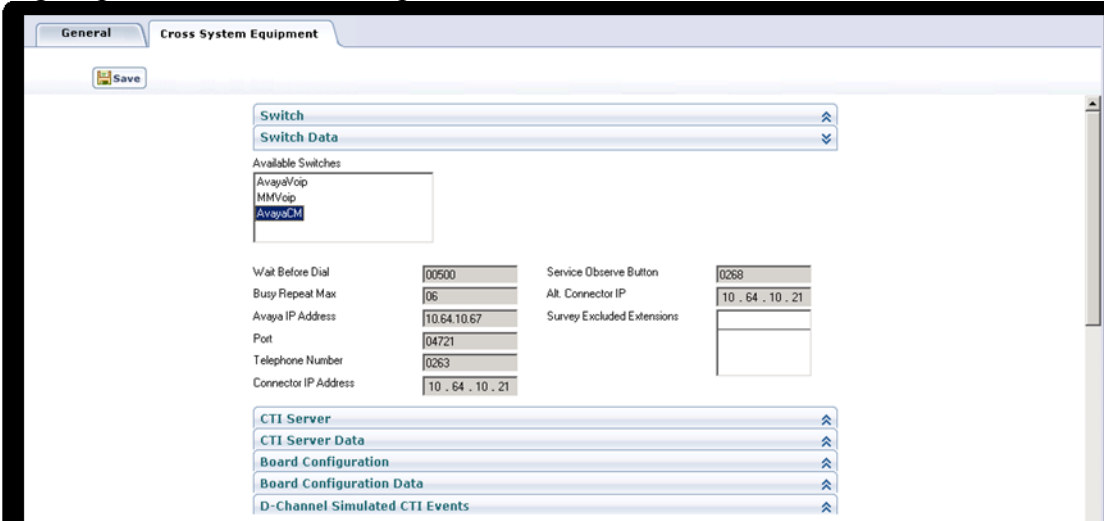
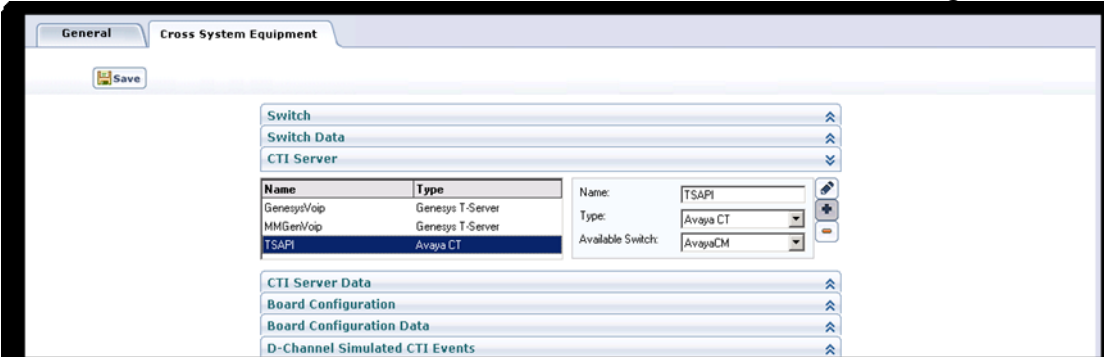
## 7. Configure Autonomy Qfiniti

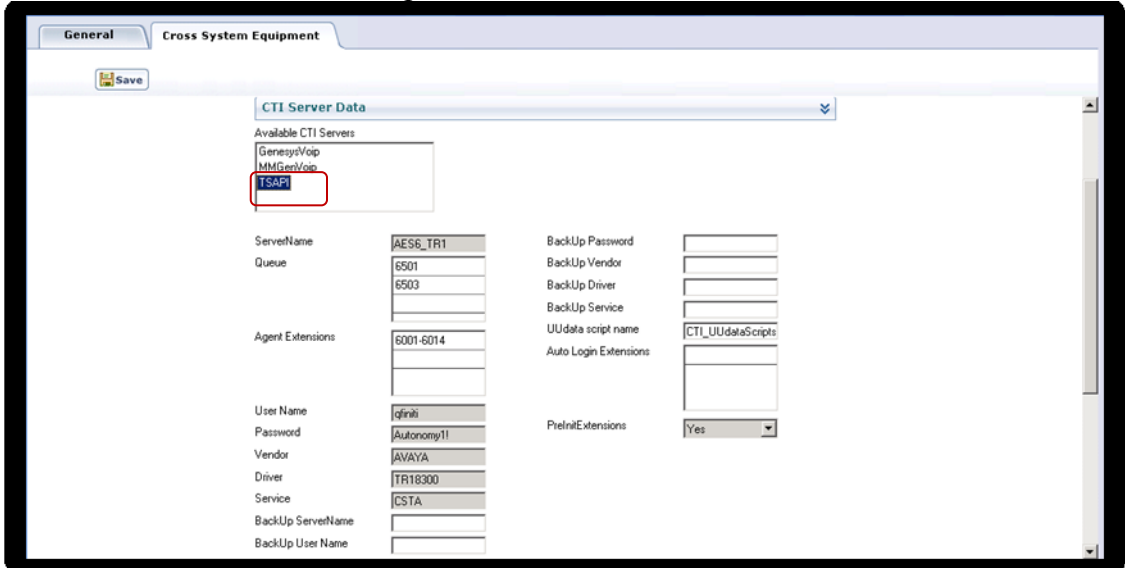
The Qfiniti solution is typically installed by Autonomy engineers or their partners. These Application Notes will only cover the steps necessary to configure the Qfiniti solution to interoperate with Avaya Aura<sup>®</sup> Communication Manager and Avaya Aura<sup>®</sup> Application Enablement Services.

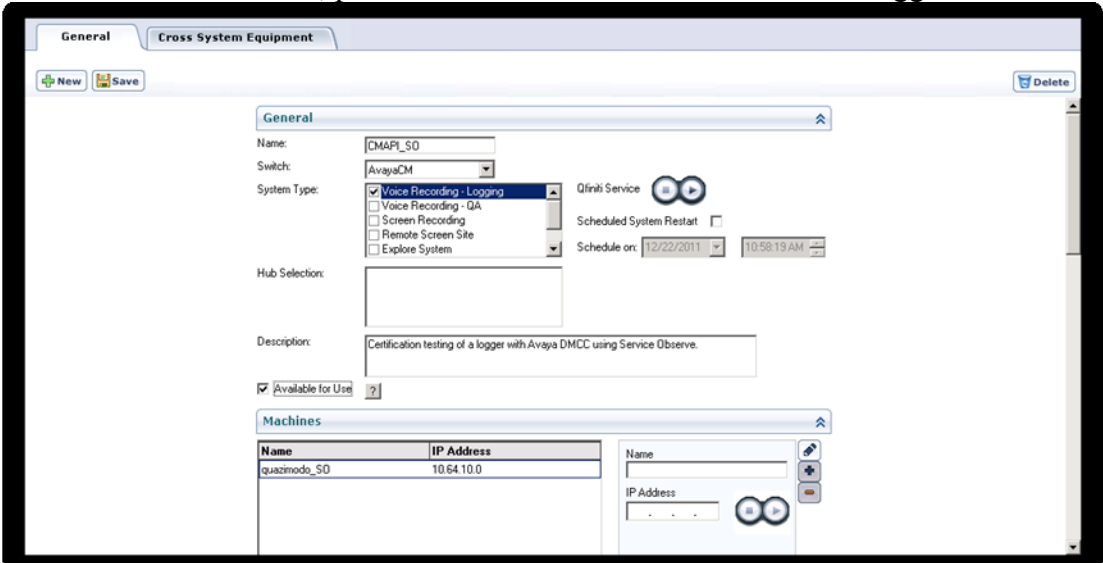
### 7.1. Qfiniti Configuration Details

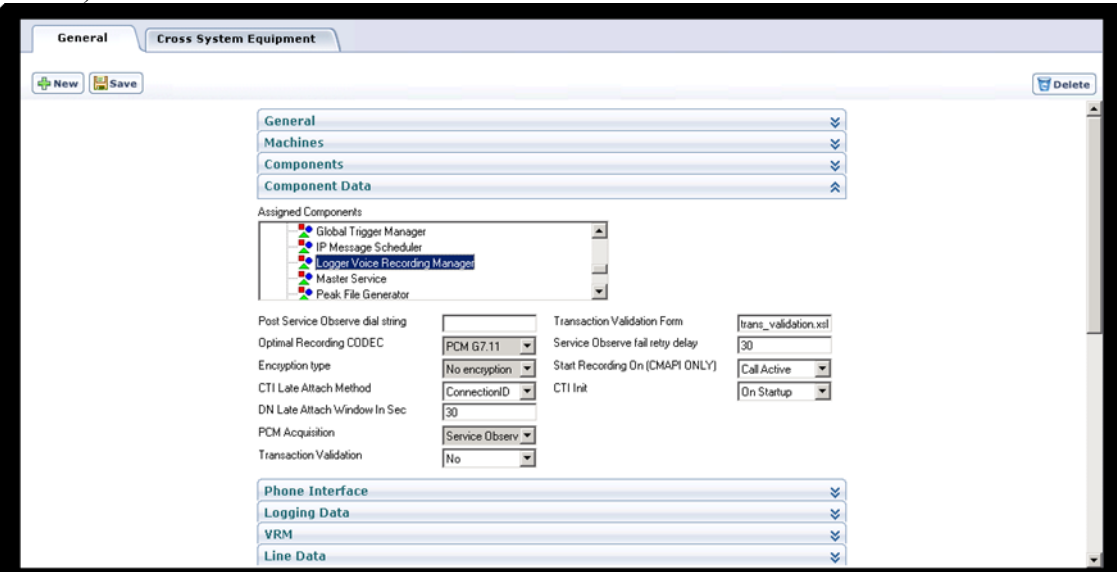
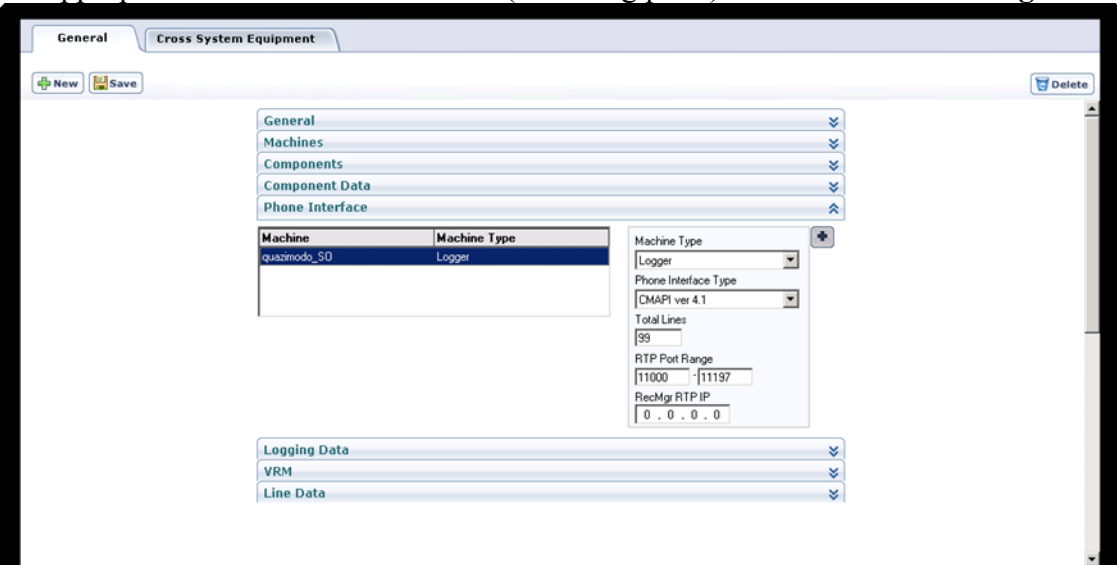
On the etalk Qfiniti server, launch the Qfiniti System Configuration application from the Windows Programs menu and log in with the appropriate credentials.

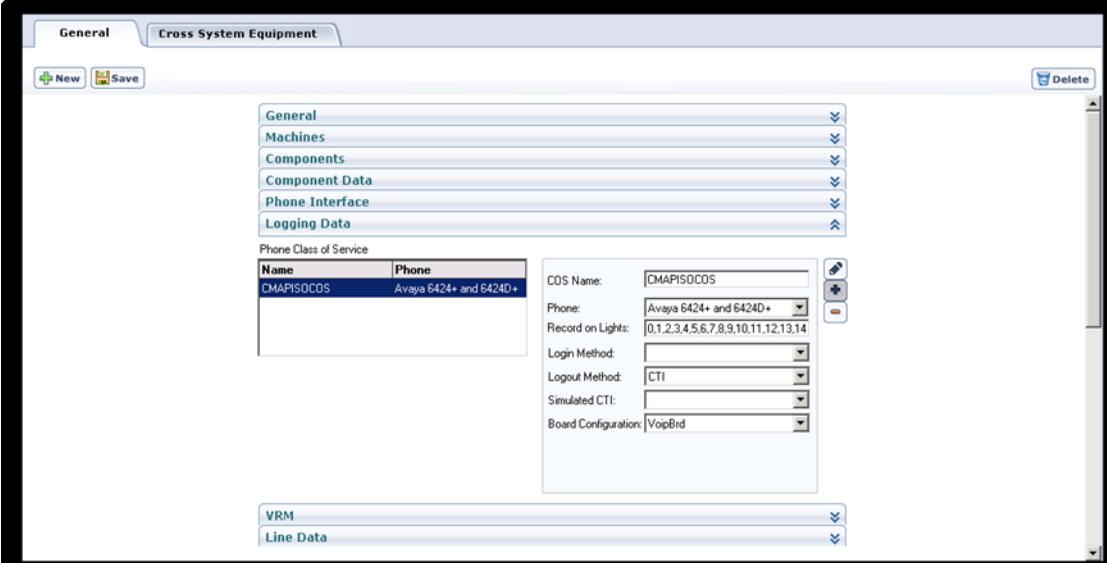
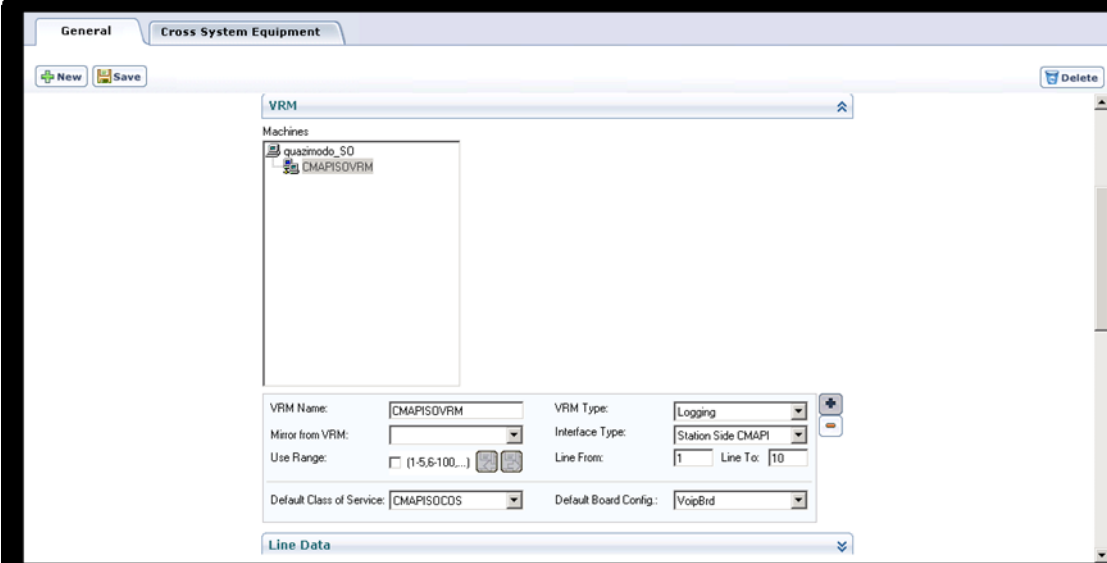
Step	Description
1.	<p><b>Create a Switch Definition</b></p> <p>In the <b>System</b> folder, select the <b>Cross System Equipment</b> tab. In the <b>Switch</b> section, click on the <b>New Switch</b> icon (pen pointing southwest). Assign descriptive strings for <b>Name</b> and <b>Vendor</b>, and set <b>Switch Model</b> to <i>Avaya Definity</i>, <b>Observe Mode</b> to <i>By Extension</i>, and <b>Interface Type</b> to <i>CMAPI / VoIP</i>. Click on the + icon to temporarily save these entries.</p>  <p>The screenshot shows the 'Qfiniti - System Configuration' window. The 'System' folder is selected in the left pane, and the 'Cross System Equipment' tab is active. The 'Switch' section is expanded, showing a table of existing switches and a form for adding a new one. The table lists three switches: 'Avaya/Vop' (Avaya S8700), 'MH/Vop' (Avaya S8700), and 'AvayaCM' (Avaya Definity). The form for the new switch has the following values: Name: 'AvayaCM', Switch Model: 'Avaya Definity', Vendor: (empty), Post Release Delay: '0', Observe Mode: 'By Extension', Observe String: (empty), Interface Type: 'CMAPI / VOIP', and 'Use CTI Source for Alias' is unchecked. Below the form are links for 'Switch Data', 'CTI Server', 'CTI Server Data', 'Board Configuration', 'Board Configuration Data', and 'D-Channel Simulated CTI Events'.</p>

Step	Description
2.	<p><b>Configure Switch Data</b></p> <p>Scroll down to the <b>Switch Data</b> section and from the <b>Available Switches</b> list, select the switch configured in Step 1. Set <b>Avaya IP Address</b> to the IP address of the Procr or C-LAN used for AES Device and Media Control API station registration (see <b>Section 5 Step 3</b>), <b>Port</b> to <b>04721</b>, and <b>Connector IP Address</b> to the IP address of the Application Enablement Services server. For <b>Telephone Number</b>, enter <b>0263</b> (corresponding to the first call appearance button on IP and Digital phone sets). For <b>Service Observe Button</b>, enter a value in the range <b>0266</b> to <b>0286</b>, inclusive, corresponding to the Service Observe button administered on each Device and Media Control API station in <b>Section 5 Step 5</b>. 0266 corresponds to Button 4 on IP and Digital phone sets, 0267 corresponds to Button 5, and so on.</p> 
3.	<p><b>Create CTI Server</b></p> <p>In the <b>CTI Server</b> section, click on the <b>New Switch</b> icon (pen pointing southwest). Assign descriptive strings for <b>Name</b>, and set <b>Type</b> to <b>Avaya CT</b>, and select <b>AvayaCM</b> from the <b>Available Switch</b> selection. Click on the + icon to save the changes.</p> 

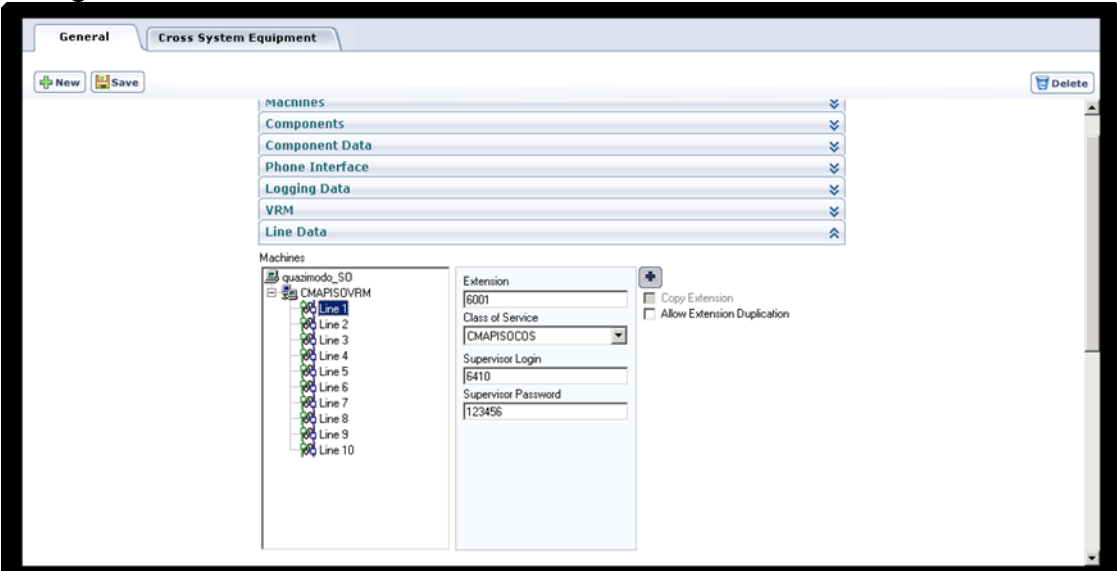
Step	Description
4.	<p data-bbox="280 233 657 268"><b>Configure CTI Server Data</b></p> <p data-bbox="280 306 1390 485">Scroll down to the <b>CTI Server Data</b> section and from the <b>Available CTI Servers</b> list, select the CTI server configured in <b>Step 3</b>. Enter the <b>User Name</b> and <b>Password</b> of the user account created in <b>Section 6.1 Step 1</b>. For <b>Queue</b>, enter the hunt/skill groups that agents will log into. For <b>Agent Extensions</b>, enter the extensions of the physical stations that agents will use.</p> <p data-bbox="280 525 1380 663">For <b>ServerName</b>, <b>Vendor</b>, <b>Driver</b>, and <b>Service</b>, use the information contained in the Service ID (given in the format &lt;Vendor&gt;#&lt;Driver&gt;#&lt;Service&gt;#&lt;ServerName&gt;, see <b>Section 6.1 Step 5</b>) of the Application Enablement Services server. Set those fields as follows:</p> <ul data-bbox="280 672 1213 810" style="list-style-type: none"> <li>• <b>ServerName</b>: hostname of the Application Enablement Services server</li> <li>• <b>Vendor</b>: <i>AVAYA</i></li> <li>• <b>Driver</b>: the Advertised Switch Name of the CTI link</li> <li>• <b>Service</b>: <i>CSTA</i></li> </ul> <p data-bbox="280 852 873 888">Click on the Save icon at the top of the screen.</p> 

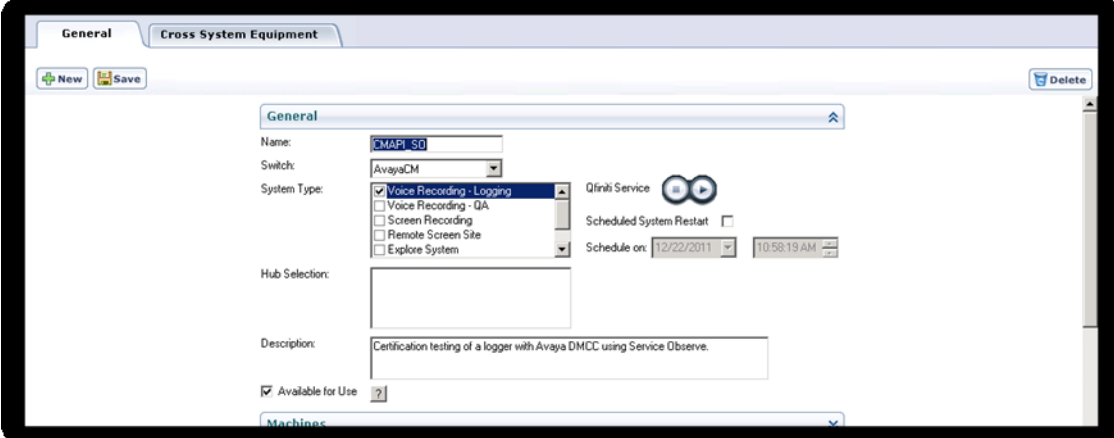
Step	Description
5.	<p><b>Create a Voice Logger</b></p> <p>Navigate to the <b>General</b> tab and click the <b>New</b> icon to create the Voice Logger. Provide a descriptive <b>Name</b>, select <b>AvayaCM</b> in the <b>Switch</b> selector (created in Step 1 above), and select <b>Voice Recording – Logging</b> for the <b>System Type</b>. Check <b>Available for Use</b> to make the logger active.</p> <p>In the <b>Machines</b> sections, provide a <b>Name</b> and <b>IP Address</b> for the Logger.</p> 
6.	<p>In the <b>Components</b> section, assign the desired Qfiniti components to the selected machine name. Note: This step is not shown in detail; it will be performed by Autonomy and is covered in product documentation. The minimum set of components required for use with Avaya DMCC is:</p> <ul style="list-style-type: none"> <li>• Agent Monitor</li> <li>• Alarm Manager Server</li> <li>• Archive Manager</li> <li>• Central Messaging Server</li> <li>• CTI Manager</li> <li>• Data Import Listener</li> <li>• Disk Monitor</li> <li>• Dispatcher</li> <li>• Global Trigger Manager</li> <li>• IP Message Scheduler</li> <li>• Logger Voice Recording Manager</li> <li>• Master Service</li> <li>• Peak File Generator</li> <li>• Plan Manager</li> <li>• Qfiniti File Server</li> <li>• Session Manager</li> </ul>

Step	Description
7.	<p>In the <b>Component Data</b> section, select <b>Logger Voice Recording Manager</b> in the <b>Assigned Components</b> list. Select the <b>Optimal Recording CODEC</b>, <b>Encryption type</b>, <b>PCM Acquisition</b> and <b>Start Recording On</b> as required. Note the <b>PCM Acquisition</b> setting defines that this logger will record using <i>Service Observation</i>. Click the <b>Save</b> button to save any changes made on this page. Configure other components as needed. In particular, Archive Manager and Qfiniti File Server must have an appropriate file path specified for archiving and recording respectively (not shown).</p> 
8.	<p>In the <b>Phone Interface</b> section, click + to add a new interface definition for the logger. Select <b>Logger</b> for the <b>Machine Type</b>, <b>CMAPI ver 4.1</b> for the <b>Phone Interface Type</b>, the appropriate number of <b>Total Lines</b> (recording ports) and an <b>RTP Port Range</b>.</p> 

Step	Description
9.	<p>In the <b>Logging Data</b> section, define a <b>Phone Class of Service</b> as shown below.</p> 
10.	<p>In the <b>VRM</b> section, create a new entry using the + sign and provide the following options. Select the <b>Default Class of Service</b> configured in Step 9 above.</p> 



Step	Description
11.	<p>In the <b>Line Data</b> section, add a recording line using the + button. Enter the <b>Extension</b> of the agent device to be recorded, select the <b>Class of Service</b> defined in Step 9, and enter a <b>Supervisor Login</b> and <b>Password</b> for one of the available Device and Media Control API stations that were configured in <b>Section 5.1 Step 5</b>. Repeat this for each recording line.</p> <p>When all lines are configured, scroll to the top of the page and click <b>Save</b> to save all settings.</p> 
12.	<p><b>Edit the TSAPI TSLIB.INI File</b></p> <p>Open the TSLIB.INI file located in the C:\WINDOWS folder. Add the following line in the <b>[Telephony Servers]</b> section of the file: &lt;AES Server Client Connectivity IP address&gt;=450. The line specifies the IP address and port that Qfiniti will use to connect to the TSAPI service on the AES server. For example, the following line was entered during compliance testing: <b>10.64.10.21=450</b></p>

Step	Description
13.	<p>Scroll up to the <b>General</b> section. Check the <b>Available for Use</b> checkbox and click on the <b>Start Service</b> icon.</p> 

## 8. Verification Steps

The following steps may be used to verify the configuration:

- Verify that Application Enablement Services is enabled and listening (use the **status aesvcs interface** command on the Communication Manager SAT).
- Verify communication between Communication Manager and the Application Enablement Services server (use the **status aesvcs link** command on the Communication Manager SAT, or navigate to **Status and Control > Switch Conn Summary** on the Application Enablement Services CTI OAM page and verify that the state of the Switch Connection is *talking*).
- Verify that the CTI link is established (use the **status aesvcs cti-link** command on the Communication Manager SAT).
- Verify that the Qfiniti recording ports are registered as “IP\_API\_A” stations in Communication Manager (use the **list registered-ip-stations** command on the Communication Manager SAT).
- Verify the Qfiniti has successfully monitored the agent stations using TSAPI (use the **list monitored-stations** command on the Communication Manager SAT).
- Verify that calls may be successfully completed to and from agents. Verify that the call recordings are accurate and complete.
- Log agents into a hunt/skill group and verify that calls may be successfully completed to and from the agents.

## 9. Conclusion

These Application Notes described the procedures for configuring Autonomy Qfiniti to monitor and record calls placed to and from agents and phones on Avaya Aura<sup>®</sup> Communication Manager. In the configuration described in these Application Notes, Qfiniti uses the Call Control Services and Device and Media Control Services of Avaya Aura<sup>®</sup> Application Enablement Services to perform recording. During compliance testing, Qfiniti successfully recorded calls placed to and from agents and stations, as well as calls placed to a VDN and then queued to an agent hunt/skill group.

## 10. Additional References

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

### Avaya

[1] *Administering Avaya Aura<sup>™</sup> Communication Manager*, Doc # 03-300509, Release 6.0, Issue 6.0, June 2010.

[2] *Avaya Aura<sup>®</sup> Application Enablement Services Administration and Maintenance Guide*, Release 6.1, Issue 2, February 2011.

### Autonomy

Product information for Autonomy products can be found at <http://www.autonomy.com>

---

**©2012 Avaya Inc. All Rights Reserved.**

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

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