



Application Notes for Configuring Autonomy Qfiniti to Interoperate with Avaya Aura[®] Communication Manager and Avaya Aura[®] 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[®] Communication Manager and Avaya Aura[®] 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[®] Communication Manager and Avaya Aura[®] 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[®] Communication Manager and Avaya Aura[®] 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

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.

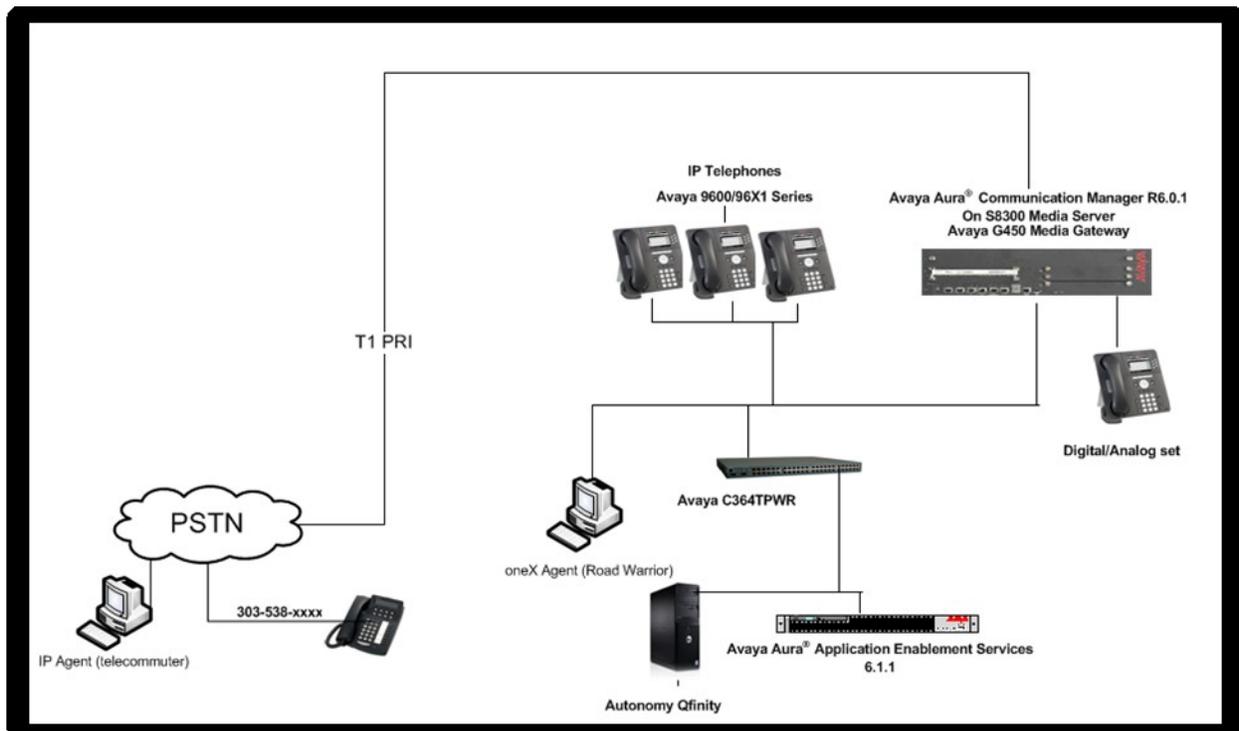


Figure 1 – Autonomy Qfiniti Compliance Test Configuration

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 [®] Communication Manager R6.0.1 SP5 |
| Dell R610 Server | Avaya Aura [®] Application Enablement Services R6.1.1 on Avaya System Platform |
| Avaya Phones 9600 Series IP Phones 96x1 Series IP Phones Avaya oneX [®] 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 data-bbox="298 281 1422 531">Verify Feature and License for the integration Applications that use Application Enablement Services TSAPI must have Computer Telephony Adjunct Links 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> <pre data-bbox="298 569 1435 1056"> display system-parameters customer-options Page 3 of 11 OPTIONAL FEATURES Abbreviated Dialing Enhanced List? y Audible Message Waiting? y Access Security Gateway (ASG)? n Authorization Codes? y Analog Trunk Incoming Call ID? y CAS Branch? n A/D Grp/Sys List Dialing Start at 01? y CAS Main? n Answer Supervision by Call Classifier? y Change COR by FAC? n ARS? y Computer Telephony Adjunct Links? y ARS/AAR Partitioning? y Cvg Of Calls Redirected Off-net? y ARS/AAR Dialing without FAC? n DCS (Basic)? y ASAI Link Core Capabilities? n DCS Call Coverage? y ASAI Link Plus Capabilities? n DCS with Rerouting? y Async. Transfer Mode (ATM) PNC? n Digital Loss Plan Modification? y Async. Transfer Mode (ATM) Trunking? n DS1 MSP? y ATM WAN Spare Processor? n ATMS? y DS1 Echo Cancellation? y Attendant Vectoring? y </pre> <p data-bbox="298 1100 1435 1171">Each port or virtual extension the recorder will use to Service Observe agent phones will require an IP_API_A license if not licensed on Application Enablement Services.</p> <pre data-bbox="298 1211 1435 1346"> display system-parameters customer-options Page 9 of 10 MAXIMUM IP REGISTRATIONS BY PRODUCT ID Product ID Rel. Limit Used IP_API_A : 100 0 </pre> |

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

| Step | Description |
|------|---|
| 3. | <p data-bbox="300 231 1429 336">Administer Ethernet Interface for Application Enablement Services Enter the change node-names ip command. The Application Enablement Services and procr node-names need to be defined here.</p> <pre data-bbox="300 378 1429 567"> 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 data-bbox="300 609 1429 714">On most R6 Communication Manager servers, the Processor Ethernet Interface will already be administered in the ip-interface list. The display ip-interface procr command will display the parameters of the Processor Ethernet Interface.</p> <pre data-bbox="300 756 1429 1134"> 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 data-bbox="300 1176 1429 1512"> 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>Administer Ethernet Interface for Application Enablement Services (Continued) Add an entry for Application Enablement Services as described below:</p> <ul style="list-style-type: none"> • Enter the change ip-services command. • In the Service Type field, type AESVCS. • In the Enabled field, type y. • In the Local Node field, type the Node name procr for the Processor Ethernet Interface. • In the Local Port field, use the default of 8765. • Note that in installations using CLAN connectivity, each CLAN interface would require similar configuration. | | | | | | | | | | | | | | | | | | | | | |
| | <pre>change ip-services Page 1 of 4</pre> <table border="1"> <thead> <tr> <th colspan="7">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> <th></th> </tr> </thead> <tbody> <tr> <td>AESVCS</td> <td>y</td> <td>procr</td> <td>8765</td> <td></td> <td></td> <td></td> </tr> </tbody> </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"> • In the AE Services Server field, type the Node name for the Application Enablement Services server. • In the Password field, type the same password to be administered on the Application Enablement Services server. • In the Enabled field, type y. | | | | | | | | | | | | | | | | | | | | | |
| | <pre>change ip-services Page 4 of 4</pre> <table border="1"> <thead> <tr> <th colspan="5">AE Services Administration</th> </tr> <tr> <th>Server ID</th> <th>AE Services Server</th> <th>Password</th> <th>Enabled</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td>1:</td> <td>aesserver2</td> <td>*</td> <td>y</td> <td>in use</td> </tr> </tbody> </table> | AE Services Administration | | | | | Server ID | AE Services Server | Password | Enabled | Status | 1: | aesserver2 | * | y | in use | | | | | | |
| AE Services Administration | | | | | | | | | | | | | | | | | | | | | | |
| Server ID | AE Services Server | Password | Enabled | Status | | | | | | | | | | | | | | | | | | |
| 1: | aesserver2 | * | y | in use | | | | | | | | | | | | | | | | | | |
| | <p>Note that the name and password entered for the AE Services Server and Password fields must match the name and password on the Application Enablement Services server.</p> | | | | | | | | | | | | | | | | | | | | | |

| Step | Description |
|------|--|
| 4. | <p data-bbox="298 235 1078 266">Administer Computer Telephony Integration (CTI) Link</p> <p data-bbox="298 270 1425 336">Enter the add cti-link <link number> command, where <link number> is an available CTI link number.</p> <ul data-bbox="347 346 1416 493" style="list-style-type: none"> <li data-bbox="347 346 1416 411">• In the Extension field, type <station extension>, where <station extension> is a valid station extension. <li data-bbox="347 422 802 453">• In the Type field, type ADJ-IP. <li data-bbox="347 464 945 493">• In the Name field, type a descriptive name. <pre data-bbox="298 525 1435 714"> add cti-link 1 Page 1 of 3 CTI LINK CTI Link: 1 Extension: 6201 Type: ADJ-IP COR: 1 Name: AES-10.64.10.21 </pre> <pre data-bbox="298 745 1435 934"> 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 data-bbox="298 966 1435 1113"> add cti-link 1 Page 3 of 3 CTI LINK Bridged Appearance Origination Restriction? n SAC/CF Override: n </pre> |

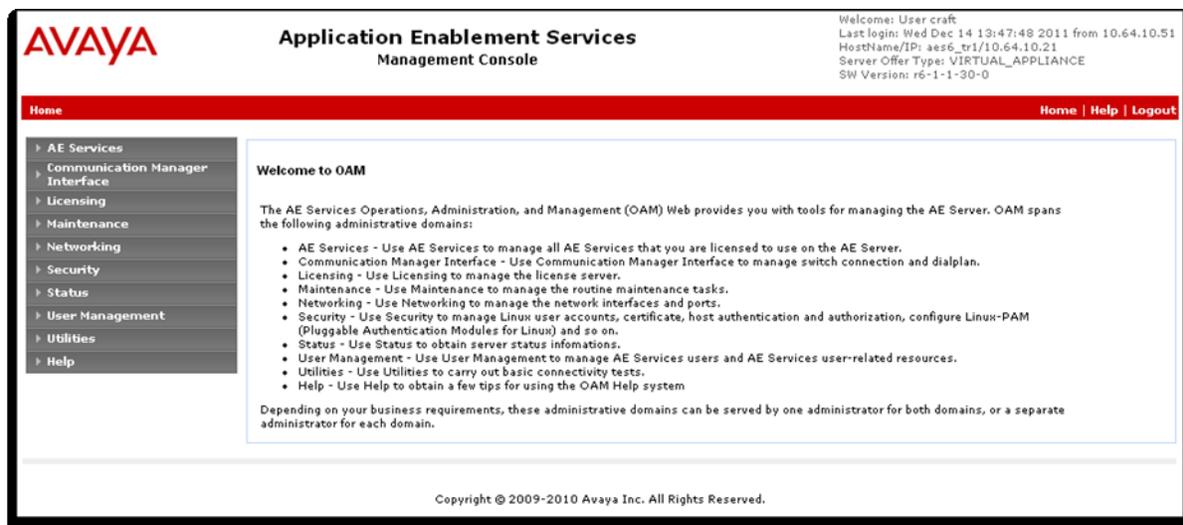
| Step | Description |
|------|--|
| 5. | <p data-bbox="298 237 1424 411">Add Qfiniti Virtual Extensions Use the add station x command to display a new station screen. Station Type 4612 and Security Code 123456 were used for each recording port. Use a Name such as DMCC Port x to differentiate the ports from other stations in the system. IP Softphone must be set to y for the recorder to be able to register via DMCC.</p> <pre data-bbox="298 443 1424 989"> 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 Loss Group: 19 Time of Day Lock Table: Personalized Ringing Pattern: 1 Message Lamp Ext: 6410 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 </pre> <p data-bbox="298 1056 1424 1161">On page 4, enter <i>serv-observ</i> on Button Assignment 6. 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 data-bbox="298 1192 1424 1787"> 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.



AVAYA Application Enablement Services Management Console

Welcome: User craft
Last login: Wed Dec 14 13:47:48 2011 from 10.64.10.51
HostName/IP: aes6_01/10.64.10.21
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-1-1-30-0

Home | Help | Logout

Home

AE Services
Communication Manager Interface
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Help

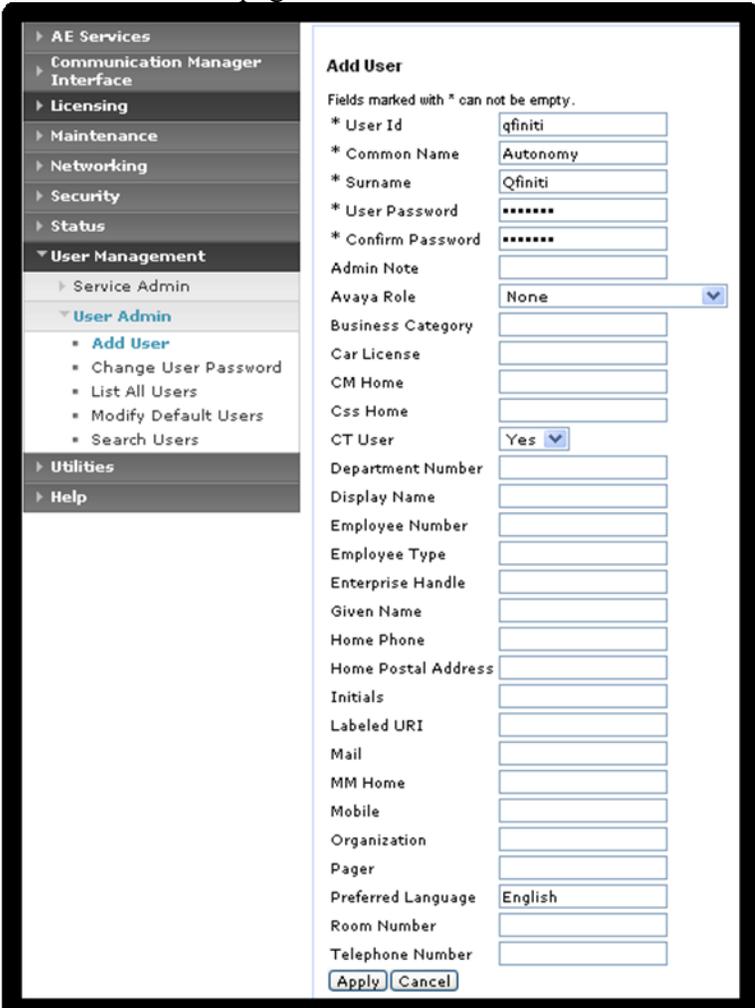
Welcome to OAM

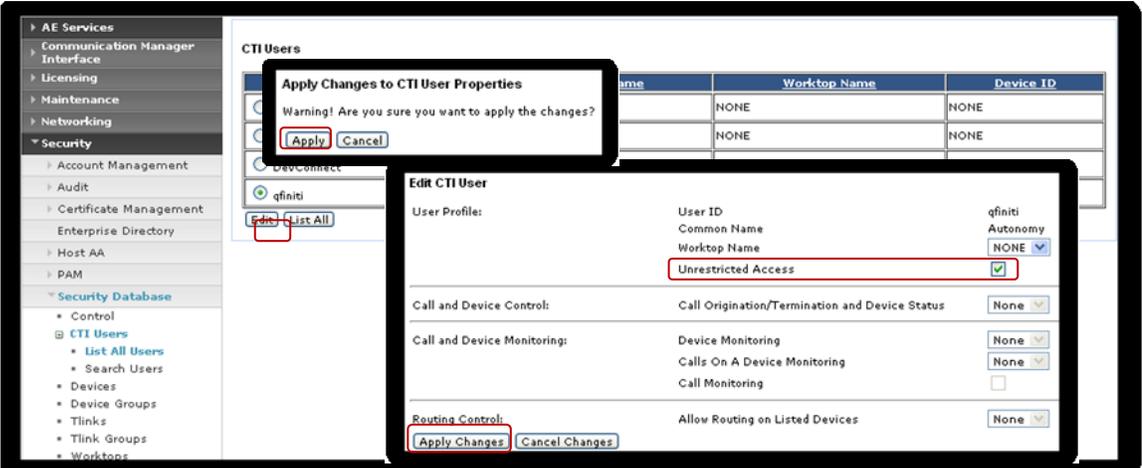
The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

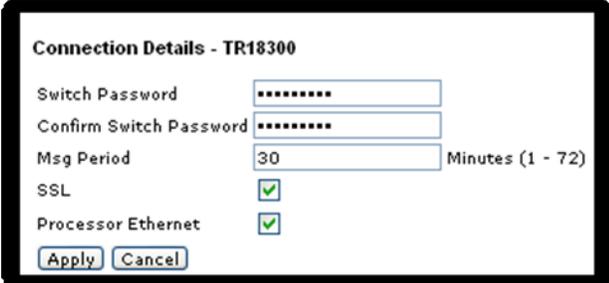
- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- Licensing - Use Licensing to manage the license server.
- Maintenance - Use Maintenance 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.

Copyright © 2009-2010 Avaya Inc. All Rights Reserved.

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

| Step | Description |
|------|---|
| 2. | <p>Enable Unrestricted Access</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 Security > CTI Users > List All Users and select the qfiniti user and click Edit.</p> <p>On the Edit CTI User panel, check the Unrestricted Access box and click the Apply Changes button.</p> <p>Click Apply when asked to confirm the change on the Apply Changes to CTI User Properties dialog.</p> <p>Note, this step requires entry on multiple panels. Each panel was superimposed below to consolidate the task.</p>  <p>The screenshot shows three overlapping panels from the Avaya AEM console. The background panel is the 'CTI Users' page, showing a table with columns 'Name', 'Worktop Name', and 'Device ID'. The 'qfiniti' user is selected, and the 'List All' button is highlighted with a red box. Overlaid on top is the 'Edit CTI User' form for the 'qfiniti' user. The 'Unrestricted Access' checkbox is checked and highlighted with a red box. The 'Apply Changes' button at the bottom is also highlighted with a red box. A third panel, 'Apply Changes to CTI User Properties', is overlaid on top of the 'Edit CTI User' form, displaying a warning message: 'Warning! Are you sure you want to apply the changes?' with 'Apply' and 'Cancel' buttons. The 'Apply' button is highlighted with a red box.</p> |

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

| Step | Description |
|------|-------------|
|------|-------------|

4.

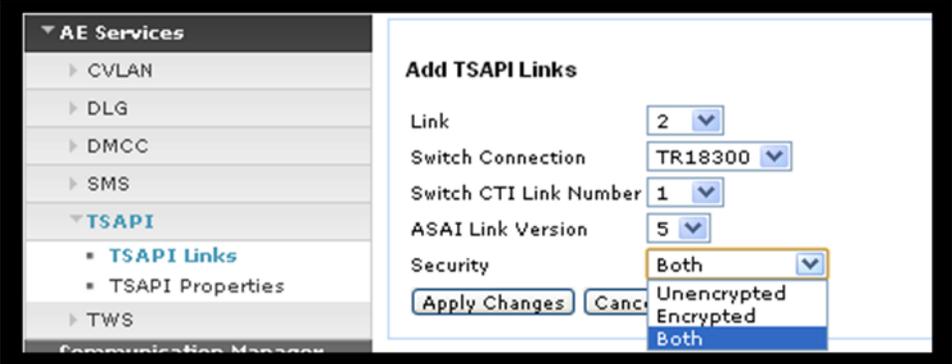
Add TSAPI Links

Navigate to the **AE Services -> TSAPI -> TSAPI Links** page to add the TSAPI CTI Link. Click **Add Link**.

Select a Switch Connection using the drop down menu. Select the **Switch CTI Link Number** using the drop down menu. The **Switch CTI link Number** must match the number configured in the **cti-link** form in **Section 5, Step 4**.

If the application will use Encrypted Links, select **Encrypted** in the **Security** selection box.

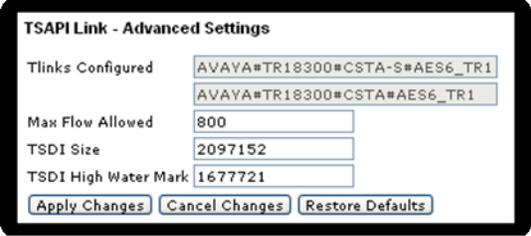
Click **Apply Changes**.

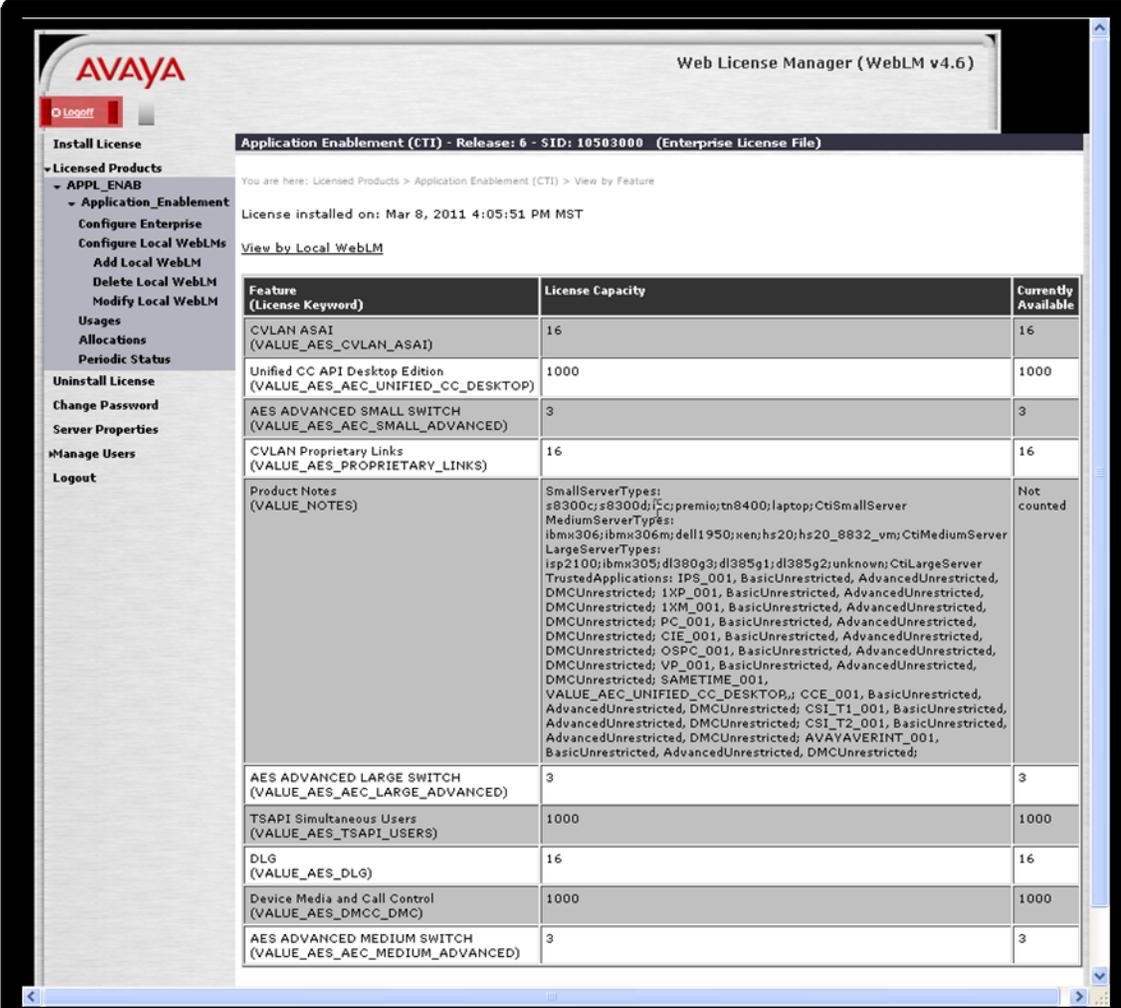


5.

Note the TLink Information

Navigate to **AE Services > TSAPI > TSAPI Links** and note the **TLinks Configured**. This information will be used in **Section 7, Step 4**.



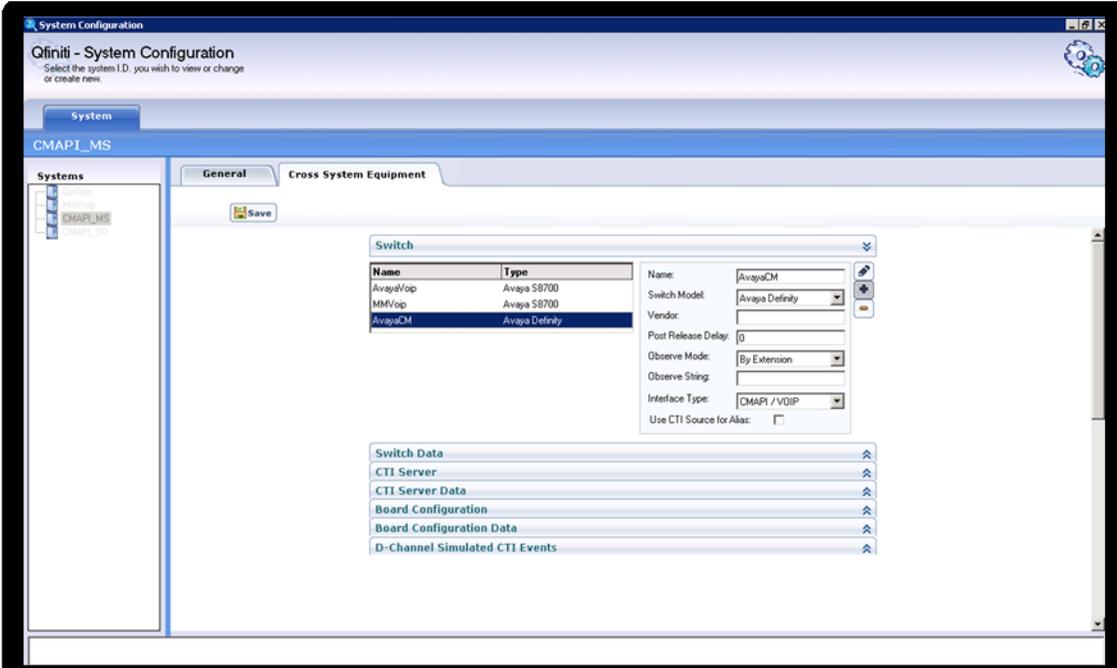
| Step | Description | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---------------------------|------------------|---------------------|-----------------------------------|----|----|---|------|------|--|---|---|---|----|----|-----------------------------|---|-------------|--|---|---|--|------|------|---------------------|----|----|--|------|------|--|---|---|
| 6. | <p>Confirm TSAPI and DMCC Licenses</p> <p>Qfiniti uses a DMCC_DMC license for each recording port. Additionally, a TSAPI Basic 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>  <table border="1" data-bbox="544 724 1380 1417"> <thead> <tr> <th>Feature (License Keyword)</th> <th>License Capacity</th> <th>Currently Available</th> </tr> </thead> <tbody> <tr> <td>CVLAN ASAI (VALUE_AES_CVLAN_ASAI)</td> <td>16</td> <td>16</td> </tr> <tr> <td>Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)</td> <td>1000</td> <td>1000</td> </tr> <tr> <td>AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)</td> <td>3</td> <td>3</td> </tr> <tr> <td>CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)</td> <td>16</td> <td>16</td> </tr> <tr> <td>Product Notes (VALUE_NOTES)</td> <td>SmallServerTypes: s8300c;s9300d;ic;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; SARETIME_001, VALUE_AES_UNIFIED_CC_DESKTOP, CCE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T1_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T2_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; AVAYAVERTINT_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted;</td> <td>Not counted</td> </tr> <tr> <td>AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)</td> <td>3</td> <td>3</td> </tr> <tr> <td>TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)</td> <td>1000</td> <td>1000</td> </tr> <tr> <td>DLG (VALUE_AES_DLG)</td> <td>16</td> <td>16</td> </tr> <tr> <td>Device Media and Call Control (VALUE_AES_DMCC_DMC)</td> <td>1000</td> <td>1000</td> </tr> <tr> <td>AES ADVANCED MEDIUM SWITCH (VALUE_AES_AEC_MEDIUM_ADVANCED)</td> <td>3</td> <td>3</td> </tr> </tbody> </table> | Feature (License Keyword) | License Capacity | Currently Available | CVLAN ASAI (VALUE_AES_CVLAN_ASAI) | 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;s9300d;ic;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; SARETIME_001, VALUE_AES_UNIFIED_CC_DESKTOP, CCE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T1_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T2_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; AVAYAVERTINT_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 |
| Feature (License Keyword) | License Capacity | Currently Available | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| CVLAN ASAI (VALUE_AES_CVLAN_ASAI) | 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;s9300d;ic;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; SARETIME_001, VALUE_AES_UNIFIED_CC_DESKTOP, CCE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T1_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T2_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; AVAYAVERTINT_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[®] Communication Manager and Avaya Aura[®] Application Enablement Services.

7.1. Qfiniti Configuration Details

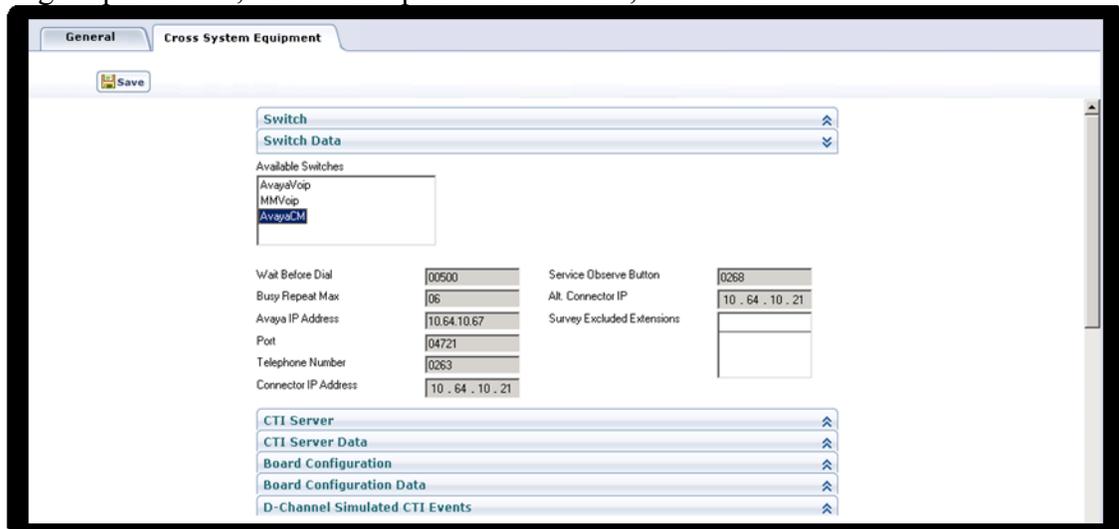
On the etalk Qfiniti server, launch the Qfiniti System Configuration application from the Windows Programs menu and log in with the appropriate credentials.

| Step | Description |
|------|--|
| 1. | <p>Create a Switch Definition</p> <p>In the System folder, select the Cross System Equipment tab. In the Switch section, click on the New Switch icon (pen pointing southwest). Assign descriptive strings for Name and Vendor, and set Switch Model to <i>Avaya Definity</i>, Observe Mode to <i>By Extension</i>, and Interface Type to <i>CMAPI / VoIP</i>. Click on the + icon to temporarily save these entries.</p>  |

| Step | Description |
|------|-------------|
|------|-------------|

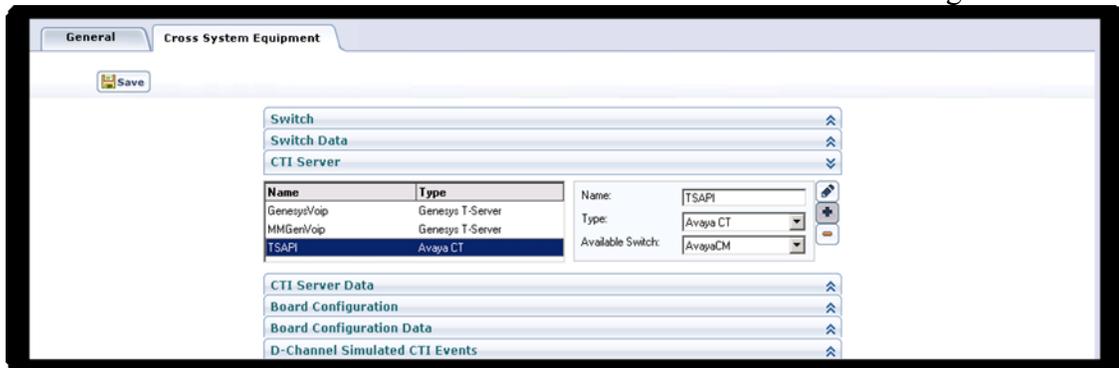
| | |
|-----------|-------------------------------------|
| 2. | <p>Configure Switch Data</p> |
|-----------|-------------------------------------|

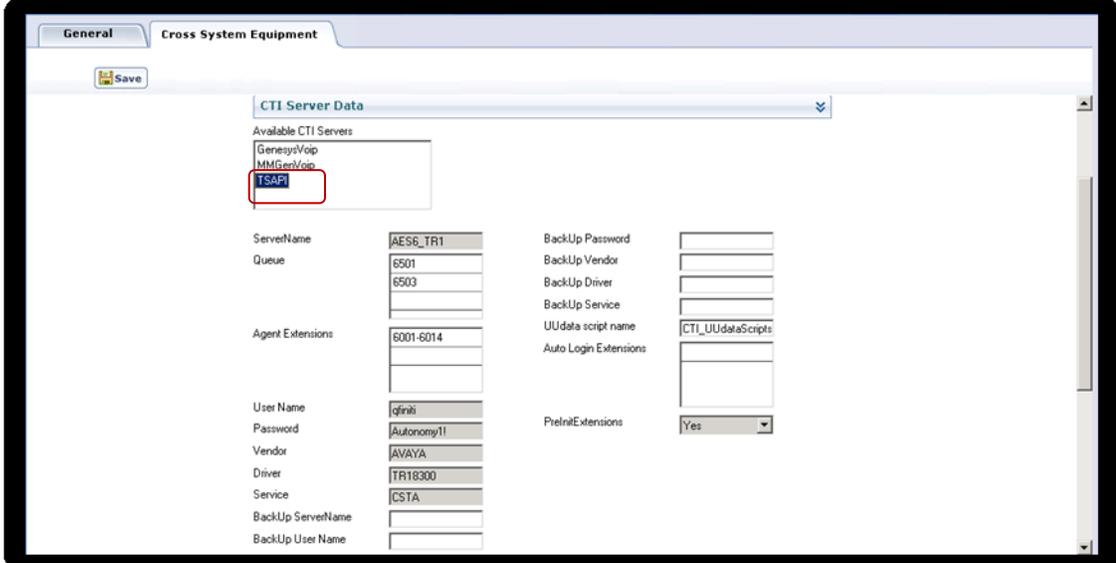
Scroll down to the **Switch Data** section and from the **Available Switches** list, select the switch configured in Step 1. Set **Avaya IP Address** to the IP address of the Procr or C-LAN used for AES Device and Media Control API station registration (see **Section 5 Step 3**), **Port** to **04721**, and **Connector IP Address** to the IP address of the Application Enablement Services server. For **Telephone Number**, enter **0263** (corresponding to the first call appearance button on IP and Digital phone sets). For **Service Observe Button**, enter a value in the range **0266** to **0286**, inclusive, corresponding to the Service Observe button administered on each Device and Media Control API station in **Section 5 Step 5**. 0266 corresponds to Button 4 on IP and Digital phone sets, 0267 corresponds to Button 5, and so on.

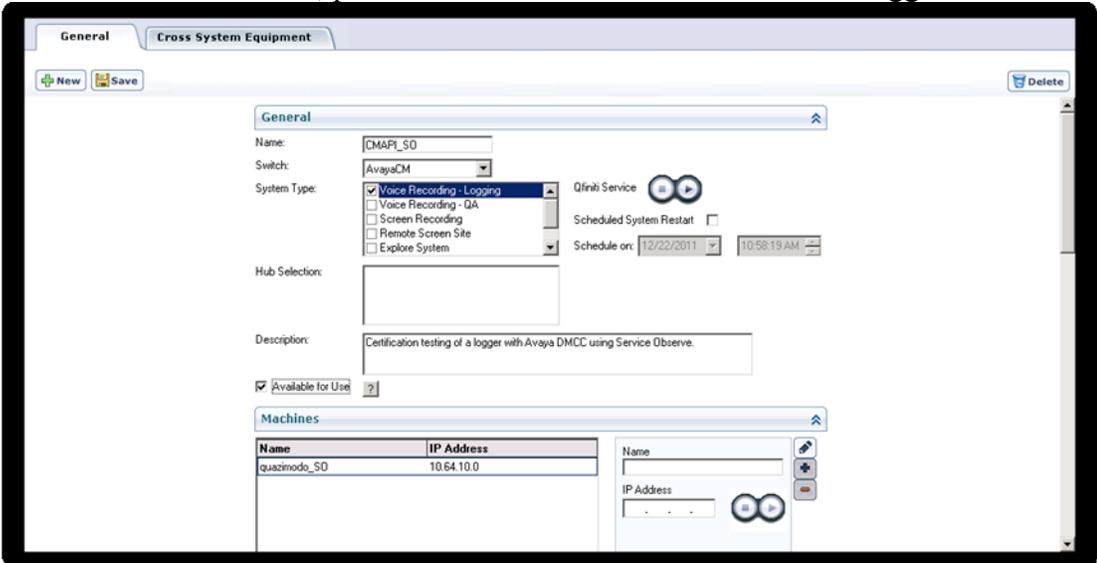


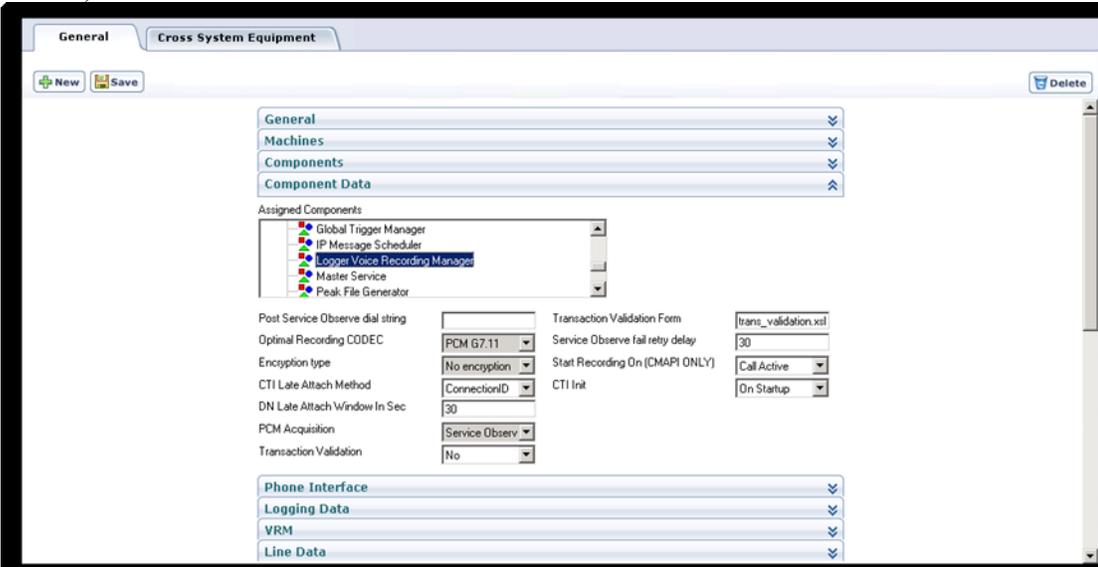
| | |
|-----------|---------------------------------|
| 3. | <p>Create CTI Server</p> |
|-----------|---------------------------------|

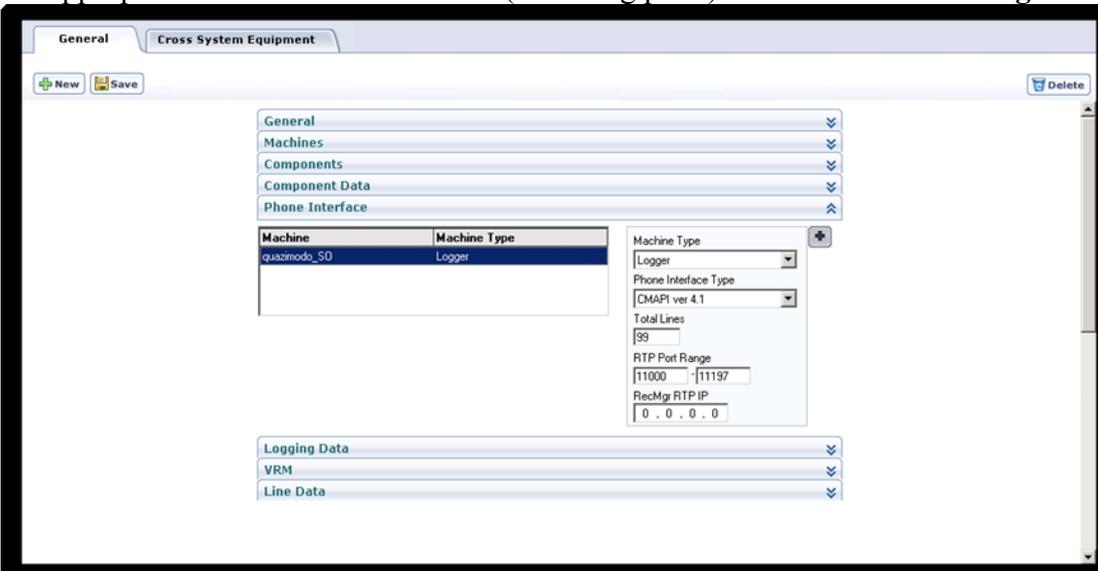
In the **CTI Server** section, click on the **New Switch** icon (pen pointing southwest). Assign descriptive strings for **Name**, and set **Type** to **Avaya CT**, and select **AvayaCM** from the **Available Switch** selection. Click on the + icon to save the changes.

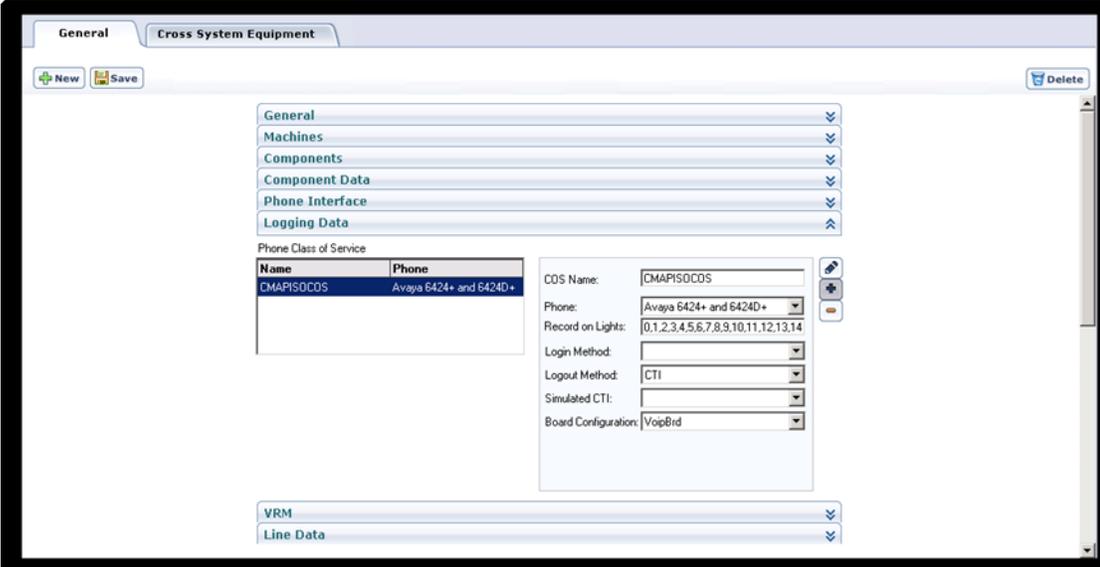
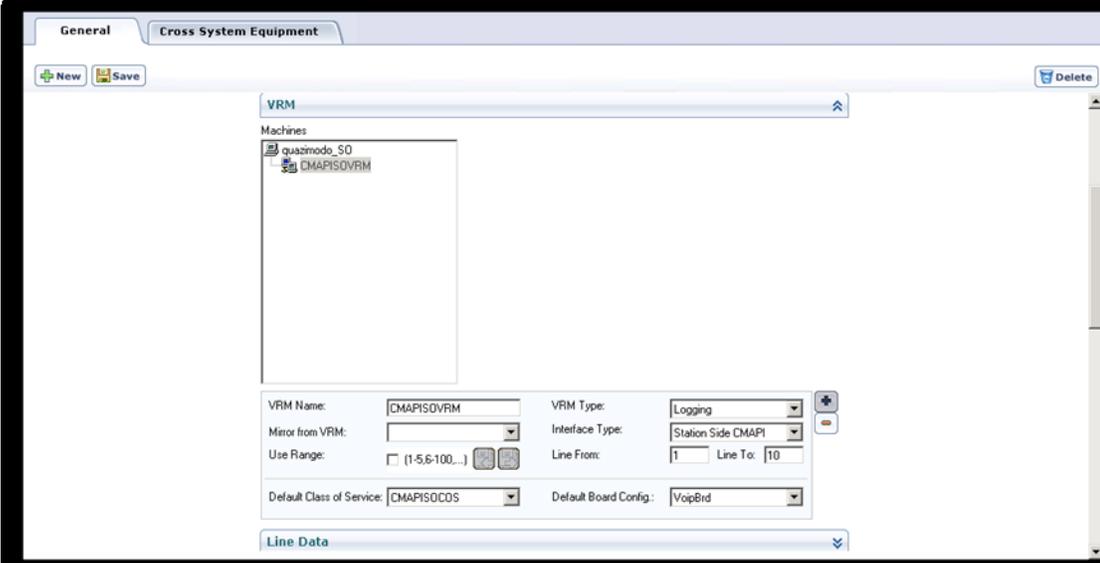


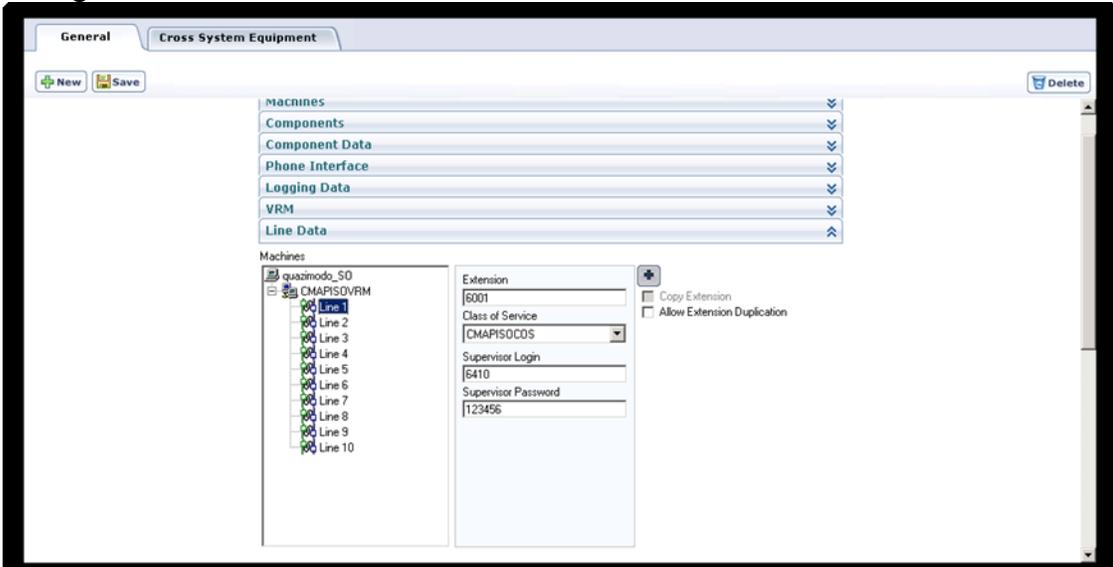
| Step | Description |
|------|--|
| 4. | <p data-bbox="280 233 657 268">Configure CTI Server Data</p> <p data-bbox="280 306 1386 485">Scroll down to the CTI Server Data section and from the Available CTI Servers list, select the CTI server configured in Step 3. Enter the User Name and Password of the user account created in Section 6.1 Step 1. For Queue, enter the hunt/skill groups that agents will log into. For Agent Extensions, enter the extensions of the physical stations that agents will use.</p> <p data-bbox="280 527 1386 663">For ServerName, Vendor, Driver, and Service, use the information contained in the Service ID (given in the format <Vendor>#<Driver>#<Service>#<ServerName>, see Section 6.1 Step 5) of the Application Enablement Services server. Set those fields as follows:</p> <ul data-bbox="280 674 1214 810" style="list-style-type: none"> • ServerName: hostname of the Application Enablement Services server • Vendor: <i>AVAYA</i> • Driver: the Advertised Switch Name of the CTI link • Service: <i>CSTA</i> <p data-bbox="280 852 873 888">Click on the Save icon at the top of the screen.</p>  |

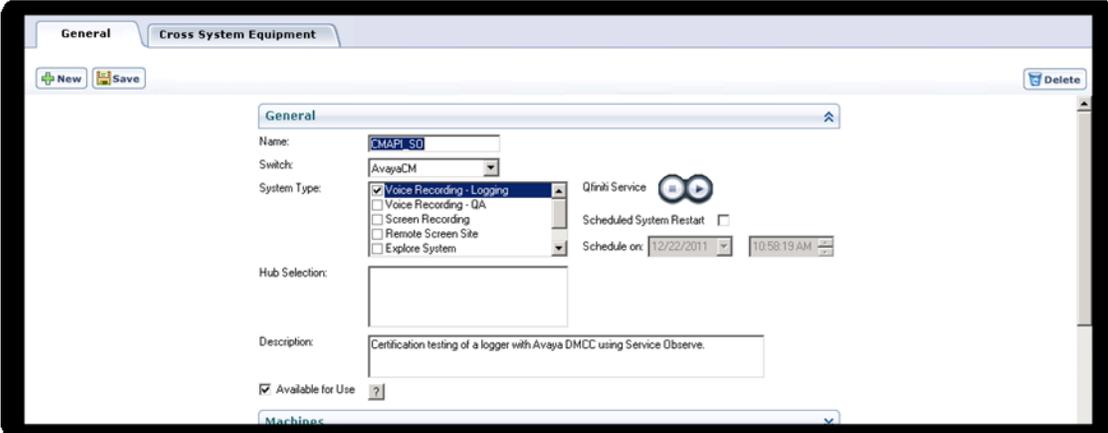
| Step | Description |
|-----------|--|
| <p>5.</p> | <p>Create a Voice Logger</p> <p>Navigate to the General tab and click the New icon to create the Voice Logger. Provide a descriptive Name, select AvayaCM in the Switch selector (created in Step 1 above), and select Voice Recording – Logging for the System Type. Check Available for Use to make the logger active.</p> <p>In the Machines sections, provide a Name and IP Address for the Logger.</p>  |
| <p>6.</p> | <p>In the Components 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"> • Agent Monitor • Alarm Manager Server • Archive Manager • Central Messaging Server • CTI Manager • Data Import Listener • Disk Monitor • Dispatcher • Global Trigger Manager • IP Message Scheduler • Logger Voice Recording Manager • Master Service • Peak File Generator • Plan Manager • Qfiniti File Server • Session Manager |

| Step | Description |
|------|---|
| 7. | <p>In the Component Data section, select Logger Voice Recording Manager in the Assigned Components list. Select the Optimal Recording CODEC, Encryption type, PCM Acquisition and Start Recording On as required. Note the PCM Acquisition setting defines that this logger will record using <i>Service Observation</i>. Click the Save 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 Phone Interface section, click + to add a new interface definition for the logger. Select Logger for the Machine Type, CMAPI ver 4.1 for the Phone Interface Type, the appropriate number of Total Lines (recording ports) and an RTP Port Range.</p>  |
|----|---|

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

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

| Step | Description |
|------|--|
| 13. | <p>Scroll up to the General section. Check the Available for Use checkbox and click on the Start Service 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[®] 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[®] 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[™] Communication Manager*, Doc # 03-300509, Release 6.0, Issue 6.0, June 2010.

[2] *Avaya Aura[®] 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.