



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

---

# **Application Notes for Calabrio Monitoring and Recording Services with Avaya Aura<sup>®</sup> Communication Manager and Avaya Aura<sup>®</sup> Application Enablement Services – Issue 1.0**

## **Abstract**

These Application Notes describe the configuration steps required for the Calabrio Monitoring and Recording Services solution to interoperate with Avaya Aura<sup>®</sup> Communication Manager and Avaya Aura<sup>®</sup> Application Enablement Services.

Calabrio Monitoring and Recording Services (MARS) uses the Avaya Aura<sup>®</sup> Application Enablement Services TSAPI and Device, Media and Call Control (DMCC) services to capture real-time CTI data and RTP streams from Avaya Aura<sup>®</sup> Communication Manager to produce recordings of phone activity for agents and knowledge workers.

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

Calabrio Monitoring and Recording Services (MARS) is a contact center and knowledge worker oriented recording solution. Using the Avaya Aura® Application Enablement Services System Management Services (SMS), Device, Media and Call Control (DMCC) Multiple Registrations or Single Step Conference capabilities, and JTAPI, the recorder is able to register with Avaya Aura® Communication Manager as an IP softphone and use various methods to capture audio from targeted agent's phone, with JTAPI providing call tagging data.

Before MARS can start recording, it registers with Application Enablement Services, performs an SMS service query to obtain a list of all of the Agents and Stations configured in Communication Manager. The administrator then associates this data with devices to be recorded by the application. The application uses a static assignment of Call Center agents, and Knowledge Workers, to the station to which they work. Dynamic assignment is not supported for any of the communication platforms supported by MARS.

When the services are started, the MARS server registers with Communication Manager as a Dependent registration using the DMCC service on stations that are administered with Softphone enabled in Communication Manager and administered to be recorded in MARS. Once DMCC registration is successfully completed, Communication Manager will send audio for all calls that originate or terminate on the registered stations to both the phone, and the recorder.

For stations that do not have Softphone enabled, including all station types such as SIP, IP, Digital or analog, MARS uses dedicated, virtual stations in Communication Manager to add to calls using the Single Step Conference TSAPI method.

To ensure call records stored in the database are as rich as possible, the application uses the TSAPI/JTAPI capabilities of Application Enablement Services to monitor the station activity. This occurs following successful DMCC registrations. If DMCC registration fails, the JTAPI associations are not requested by the application.

## 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 MARS 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 MARS 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.

- For endpoints recorded using the Multiple Registration method, calls handled by cell phone via EC500 could not be recorded when answered on the cell phone. This is a limitation of this recording method and is not supported by Avaya. Endpoints requiring this capability must be configured for the Single Step Conferencing method. Using this alternate approach, calls were successfully recorded on the cell phone mapped to the desk phone.
- For some transfer and conferencing tests, though all call legs were recorded, information for originating calling party (calling party number) was not preserved.
- When the MARS server loses network connectivity for over 200 seconds, the CTI link is not re-established. However, restarting the CTI service on the MARS server restores the communication.

### 2.3. Support

Technical support on Calabrio MARS can be obtained through the following:

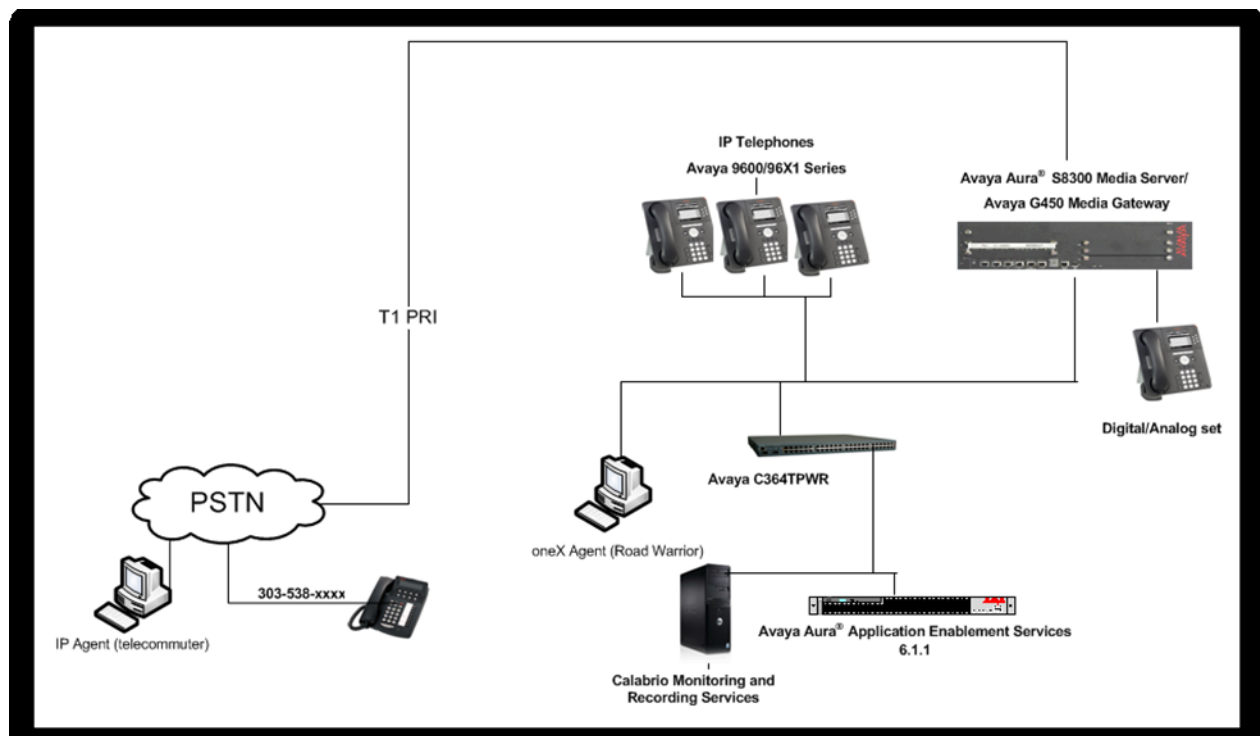
- Phone: +1 (763) 592-4680 or +1 (800) 303-1248
- Web: <http://calabrio.com/about-calabrio/services/>
- Email: [calabriosupport@calabrio.com](mailto:calabriosupport@calabrio.com)

### 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
- Calabrio MARS 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 – Calabrio MARS Compliance Test Configuration**

## 4. Equipment and Software Validated

The following equipment and version were used in the reference configuration described above:

Equipment	Version
Avaya Aura <sup>®</sup> Communication Manager running on S8300 Server	R6.0.1 SP 00.1.510.1-19528
Avaya Aura <sup>®</sup> Application Enablement Services running on Dell R610 Server	R6.1.1
Avaya Phones: <ul style="list-style-type: none"><li>• 9600 Series IP Phones</li><li>• 96x1 Series IP Phones</li><li>• Avaya oneX<sup>®</sup> Agent</li><li>• Avaya IP Agent</li></ul>	H.323 ver 3.11/SIP ver 2.6.4 H.323 ver 3.11/SIP ver 2.6.4 R2.5 R7.0
Calabrio MARS running on Windows 2008 Server, MS SQL 2008	R8.8.1.57

## **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 fall into the following areas:

- Verify Feature and License for the integration
- Administer Communication Manager System Features
- Administer Ethernet Interface for Application Enablement Services
- Administer Computer Telephony Integration (CTI) Link
- Add SMS User Account
- Verify Agent 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>Enter the <b>display system-parameters customer-options</b> command and ensure that <b>Computer Telephony Adjunct Links</b> is set to <b>y</b>. Applications that use Application Enablement Services TSAPI must have <b>Computer Telephony Adjunct Links</b> enabled on Communication Manager. This Communication Manager feature entitlement is provided with each TSAPI license. TSAPI entitlements must be activated in both the Communication Manager and Application Enablement Services licenses. If this option is not set to <b>y</b>, contact the Avaya sales team or business partner for a proper license file.</p> <pre> display system-parameters customer-options 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 Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? y ATM WAN Spare Processor? n              DS1 MSP? y ATMS? y      DS1 Echo Cancellation? y Attendant Vectoring? y </pre> <p>Each recording 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> <pre> display system-parameters customer-options MAXIMUM IP REGISTRATIONS BY PRODUCT ID  Product ID  Rel. Limit      Used IP_API_A    : 100          0 </pre>

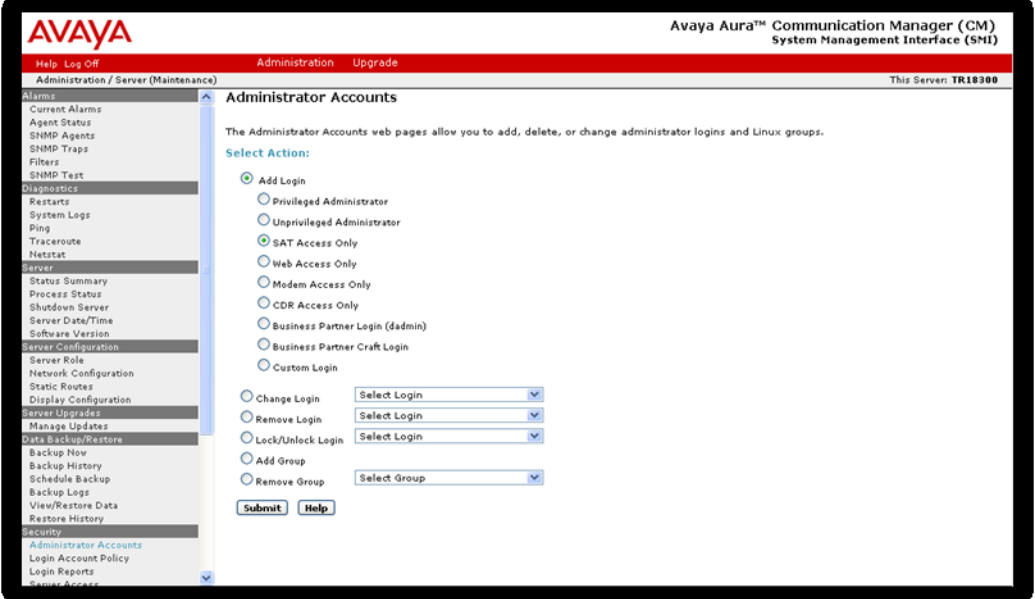
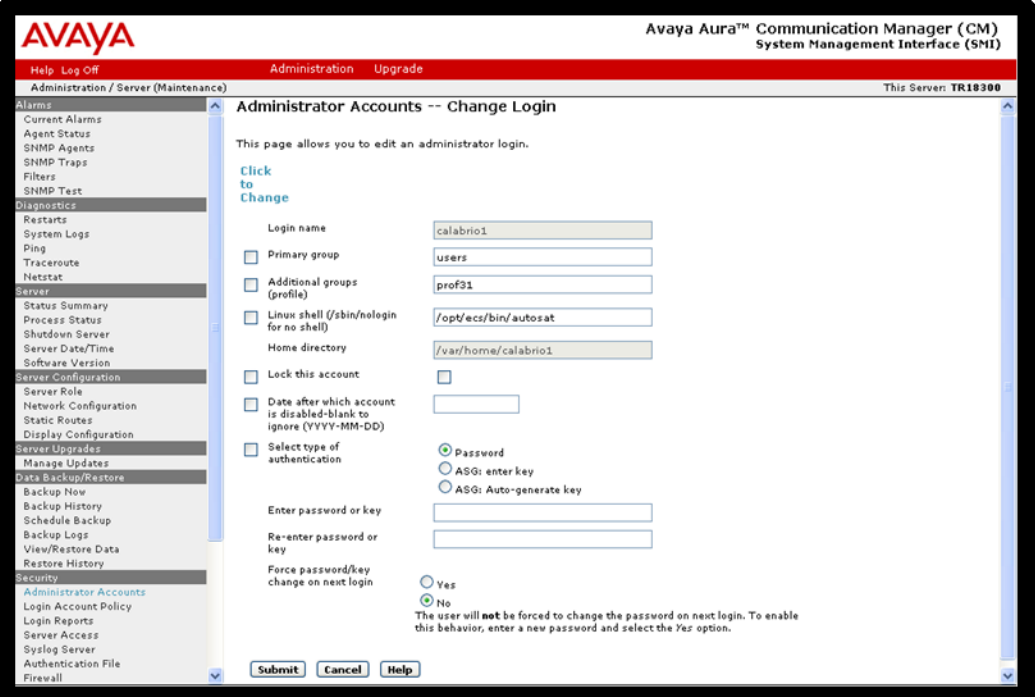
Step	Description
2.	<p><b>Administer Communication Manager System Features</b>  Enter the <b>change system-parameters features</b> command and ensure that <b>Create Universal Call ID (UCID)</b> is enabled system wide on page 5 and define a relevant <b>UCID Network Node ID</b> (1 was used in the test) and that <b>Send UCID to ASAI</b> is set to <b>y</b> on page 13. MARS relies on UCID to track complex calls (Transfers and Conferences).</p> <pre> change system-parameters features                                     Page  5 of 19                                 FEATURE-RELATED SYSTEM PARAMETERS  SYSTEM PRINTER PARAMETERS   Endpoint:                               Lines Per Page: 60  SYSTEM-WIDE PARAMETERS                                 Switch Name:                                 Emergency Extension Forwarding (min): 10                                 Enable Inter-Gateway Alternate Routing? n                                 Enable Dial Plan Transparency in Survivable Mode? n                                 COR to Use for DPT: station  MALICIOUS CALL TRACE PARAMETERS                                 Apply MCT Warning Tone? n    MCT Voice Recorder Trunk Group:                                 Delay Sending RElease (seconds): 0  SEND ALL CALLS OPTIONS   Send All Calls Applies to: station    Auto Inspect on Send All Calls? n   Preserve previous AUX Work button states after deactivation? n  UNIVERSAL CALL ID   Create Universal Call ID (UCID)? y    UCID Network Node ID: 1 </pre> <pre> change system-parameters features                                     Page 13 of 19                                 FEATURE-RELATED SYSTEM PARAMETERS  CALL CENTER MISCELLANEOUS   Callr-info Display Timer (sec): 10   Clear Callr-info: next-call   Allow Ringer-off with Auto-Answer? n    Reporting for PC Non-Predictive Calls? n    Interruptible Aux Notification Timer (sec): 3  ASAI   Copy ASAI UUI During Conference/Transfer? n   Call Classification After Answer Supervision? n   Send UCID to ASAI? y   For ASAI Send DTMF Tone to Call Originator? y </pre>



Step	Description
3.	<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.
	<pre>change node-names ip</pre> <div>Page 1 of 2</div> <pre> 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 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</pre> <div>Page 1 of 2</div> <pre> 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</pre> <div>Page 2 of 2</div> <pre> 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>Page 1 of 4</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></div>	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 name obtained from 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 in <b>Section 6.1, Step 1</b>.</li><li>• In the <b>Enabled</b> field, type <b>y</b>.</li></ul>																		
	<div><div>change ip-services</div><div>Page 4 of 4</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></td></tr></table></div>	Server ID	AE Services Server	Password	Enabled	Status	1:	aesserver2	*	y									
Server ID	AE Services Server	Password	Enabled	Status															
1:	aesserver2	*	y																
	<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>																		
4.	<p><b>Administer Computer Telephony Integration (CTI) Link</b> Enter the <b>add cti-link &lt;link number&gt;</b> command, where <b>&lt;link number&gt;</b> is an available CTI link number.</p> <ul style="list-style-type: none"><li>• In the <b>Extension</b> field, type <b>&lt;station extension&gt;</b>, where <b>&lt;station extension&gt;</b> 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>																		
	<div><div>add cti-link 1</div><div>Page 1 of 3</div><div>CTI LINK</div><div>CTI Link: 1 Extension: 6201 Type: ADJ-IP Name: AES-10.64.10.21</div><div>COR: 1</div></div>																		

Step	Description
5.	<p><b>Add SMS User Account</b></p> <p>MARS uses the Application Enablement Services SMS interface to query for administered Stations and Agents for use in administering the application.</p> <p>A privileged user was used in this test; however, a local administrator would want to restrict the user account. This involves creating a user profile at the SAT, and then creating and assigning that user to the profile in the web admin pages. To illustrate, the add <b>user profile 31</b> command was used to create the profile used in the test as shown below. The <b>Call Center B</b> and <b>Stations M</b> categories were set to <b>y</b>.</p> <pre> add user-profile 31 USER PROFILE 31 Page 1 of 41  User Profile Name: Calabrio SMS  This Profile is Disabled? n Facility Test Call Notification? n Grant Un-owned Permissions? n Shell Access? y Acknowledgement Required? n Extended Profile? n  Name      Cat  Enbl      Name      Cat  Enbl Adjuncts  A    n      Routing and Dial Plan J    n <b>Call Center B</b>  <b>y</b>      Security K    n Features  C    n      Servers L    n Hardware  D    n      <b>Stations M</b>  <b>y</b> Hospitality E    n      System Parameters N    n IP        F    n      Translations O    n Maintenance G    n      Trunking P    n Measurements and Performance H    n      Usage Q    n Remote Access I    n      User Access R    n </pre> <p>Read only access to Agents and Stations is required. Enter <b>r-</b> permissions for the <b>B</b> and <b>M</b> Categories on the <b>Set Permissions for Category:</b> entry on the <b>change user-profile xx</b> form. This requires two separate transactions, so repeat for each category.</p> <pre> change user-profile 31 USER PROFILE 31 Page 3 of 41  Set Permissions For Category: M To: r- Set All Permissions To: '-'=no access 'r'=list,display,status 'w'=add,change,remove+r 'm'=maintenance Name      Cat  Perm aesvcs link A    -- aesvcs-server A    -- <b>agent B</b>      <b>r-</b> <b>agent-loginID B</b> <b>r-</b> alarms H    -- <b>alias station M</b> <b>r-</b> alphanumeric-dial-table J    -- alternate-frl C    -- amw all G    -- amw asai G    -- amw audix G    -- amw pms G    -- analog-testcall board G    -- </pre>

Step	Description
	<p><b>Add SMS User Account (Continued)</b></p> <p>Create a user account on the Communication Manager <b>System Management Interface</b> web page by navigating to the <b>Administer Accounts</b> page and selecting the radio button <b>Add Login</b>. For the Compliance Test, an account with <b>SAT Access Only</b> was used. Click <b>Submit</b> to continue the process.</p>  <p>The account used for testing was previously created. The <b>Change Login</b> screen below shows the entries used when the account was created. The account was assigned to <b>Profile 31</b> defined in <b>Step 5</b> above, and a <b>Password</b> was created.</p> 

Step	Description
6.	<p><b>Verify Agent Extensions</b></p> <p>All stations that will be recorded must have <b>IP Softphone</b> enabled, and the application needs to know the <b>security code</b> in order to successfully register. For stations that are unable to support Softphone, or which the administrator prefers to record using Single Step Conference, leave the <b>IP Softphone</b> setting disabled. Use the <b>display station n</b> command to verify information, or <b>change station n</b> to make changes if necessary.</p> <pre> display station 6001                                 Page 1 of 5                                 STATION  Extension: 6001                Lock Messages? n                BCC: 0     Type: 9630                  Security Code: 123456                TN: 1     Port: S00008                Coverage Path 1:                COR: 1     Name: Agent X                Coverage Path 2:                COS: 1                                 Hunt-to Station:  STATION OPTIONS                                 Time of Day Lock Table:                                 Loss Group: 19                Personalized Ringing Pattern: 1                                 Speakerphone: 2-way                Message Lamp Ext: 6410                                 Display Language: english                Mute Button Enabled? y 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>

## 6. Configure Avaya Aura® Application Enablement Services

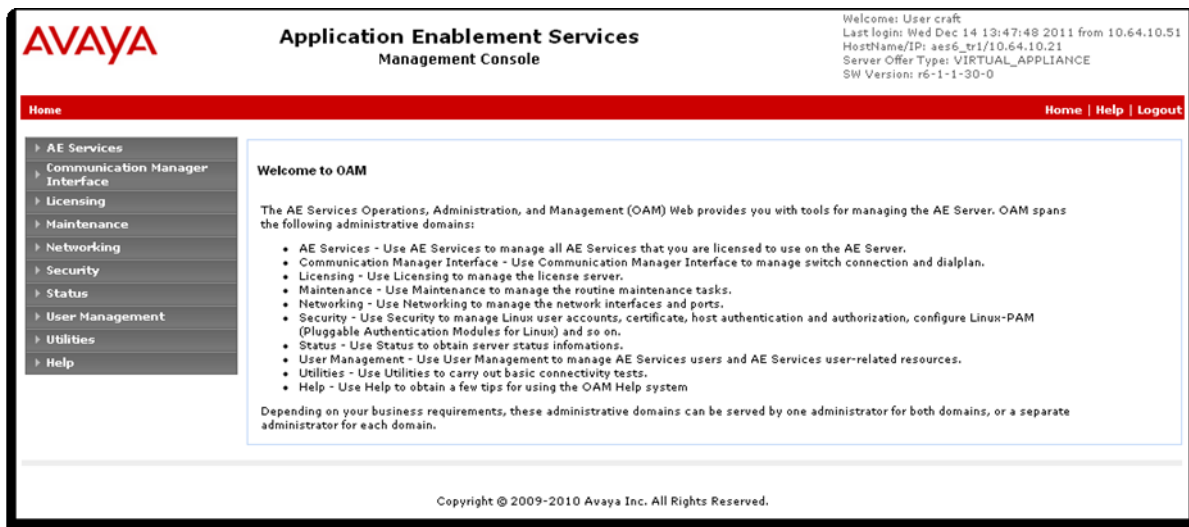
Configuration of Avaya Aura® Application Enablement Services required a user account be configured for MARS. Additional information is provided to illustrate how the connectivity with Avaya Aura® Communication Manager was previously configured.

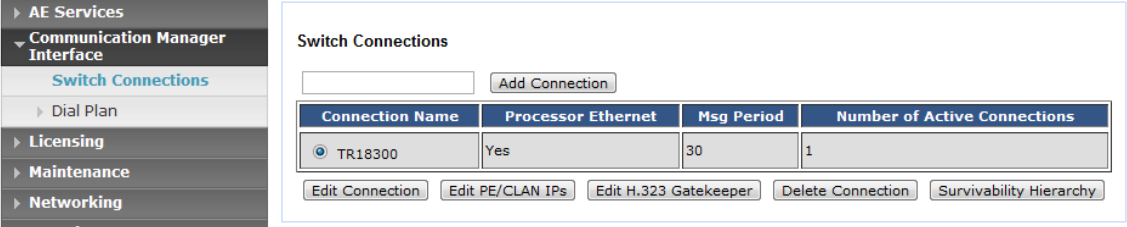
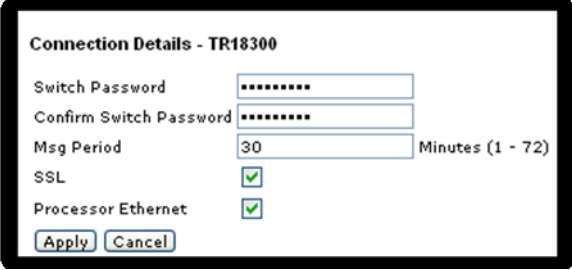

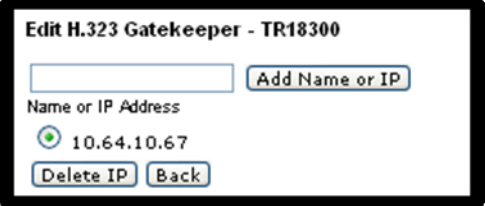
### 6.1. Configure Application Enablement Services Details

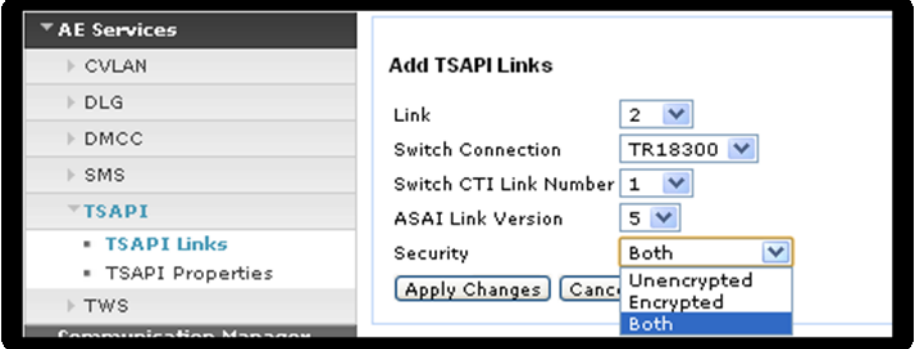
All administration is performed by web browser. Initially, users land on the Welcome to OAM page shown below. Note that all navigation is performed by clicking links in the Navigation Panel on the left side of the screen, context panels will then appear on the right side of the screen.

The procedures fall into the following areas:

- Configure Communication Manager Switch Connections
- Add TSAPI Links
- Configure Calabrio User
- Enable Unrestricted Access
- Note the TLink Information
- Confirm TSAPI and DMCC Licenses

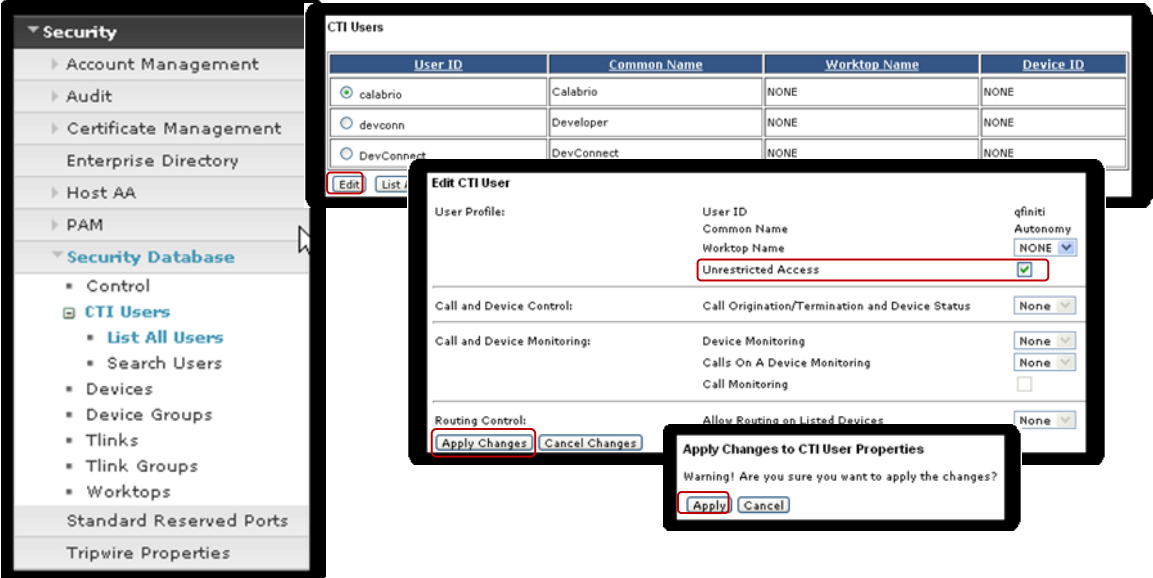


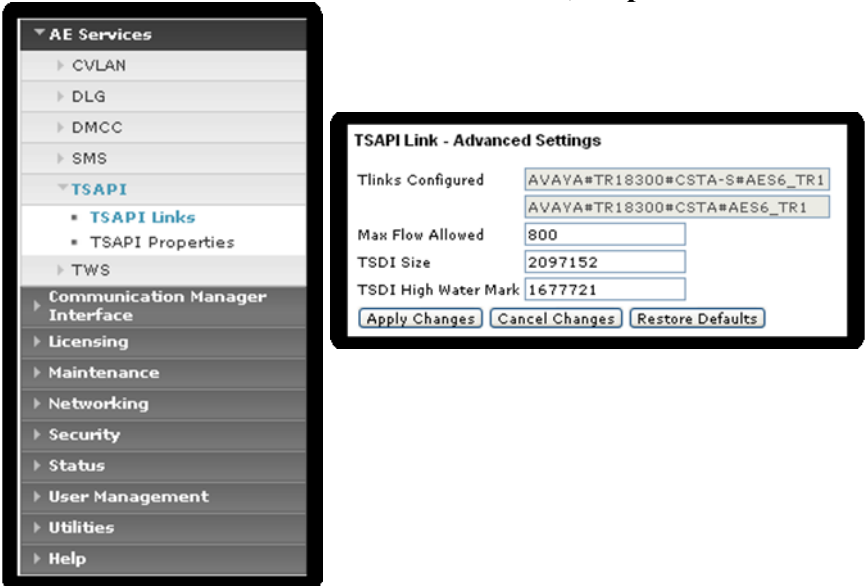
Step	Description
1.	<p><b>Configure Communication Manager Switch Connections</b></p> <p>To add links to the Communication Manager, navigate to the <b>Communication Manager Interface → Switch Connections</b> page and enter a name for the new switch connection and click the <b>Add Connection</b> button. This was previously configured as <b>TR18300</b> for this test environment:</p>  <p>Use the <b>Edit Connection</b> button shown above to configure the connection. Enter the <b>Switch Password</b> and check the <b>Processor Ethernet</b> box if using the <b>procr</b> interface, as shown below. This must match the password configured in <b>Section 5.1, Step 3</b> above.</p>  <p>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>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
2.	<p><b>Add TSAPI Links</b></p> <p>Navigate to the <b>AE Services</b> → <b>TSAPI</b> → <b>TSAPI Links</b> page to add the TSAPI CTI Link. Click <b>Add Link</b> (not shown).</p> <p>Select a <b>Switch Connection</b> 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 5.1, 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> 



Step	Description
<b>3.</b>	<p><b>Configure Calabrio user</b></p> <p>In the Navigation Panel, select <b>User Management</b> → <b>User Admin</b> → <b>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>, <b>User Password</b>, and <b>Confirm 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> <div data-bbox="276 651 1084 1449"> </div>

Step	Description
4.	<p><b>Enable Unrestricted Access</b></p> <p>If the Security Database (SDB) is enabled on Application Enablement Services, set the calabrio 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 → Security Database → CTI Users → List All Users</b> and select the <b>calabrio</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
5.	<p><b>Note the TLink Information</b> Navigate to <b>AE Services → TSAPI → TSAPI Links</b> and note the <b>TLinks Configured</b>. This information will be used in <b>Section 7.1, Step 2</b>.</p>  <p>The screenshot displays the Avaya Management System interface. On the left is a navigation menu with the following items: AE Services (expanded), CVLAN, DLG, DMCC, SMS, TSAPI (expanded), TSAPI Links (selected), TSAPI Properties, TWS, Communication Manager Interface, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. On the right is the 'TSAPI Link - Advanced Settings' configuration page. It contains the following fields: 'Tlinks Configured' with two text boxes containing 'AVAYA#TR18300#CSTA-S#AES6_TR1', 'Max Flow Allowed' with a text box containing '800', 'TSDI Size' with a text box containing '2097152', and 'TSDI High Water Mark' with a text box containing '1677721'. At the bottom of the configuration page are three buttons: 'Apply Changes', 'Cancel Changes', and 'Restore Defaults'.</p>

Step	Description
6.	<p><b>Confirm TSAPI and DMCC Licenses</b></p> <p>Calabrio MARS uses a DMCC (VALUE_AES_DMCC_DMC) license for each recording port. Additionally, a TSAPI Basic (VALUE_AES_TSAPI_USERS) 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. If the licensed quantities are not sufficient for the implementation, contact the Avaya sales team or business partner for a proper license file.</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 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;s8300d;isc;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 Calabrio MARS

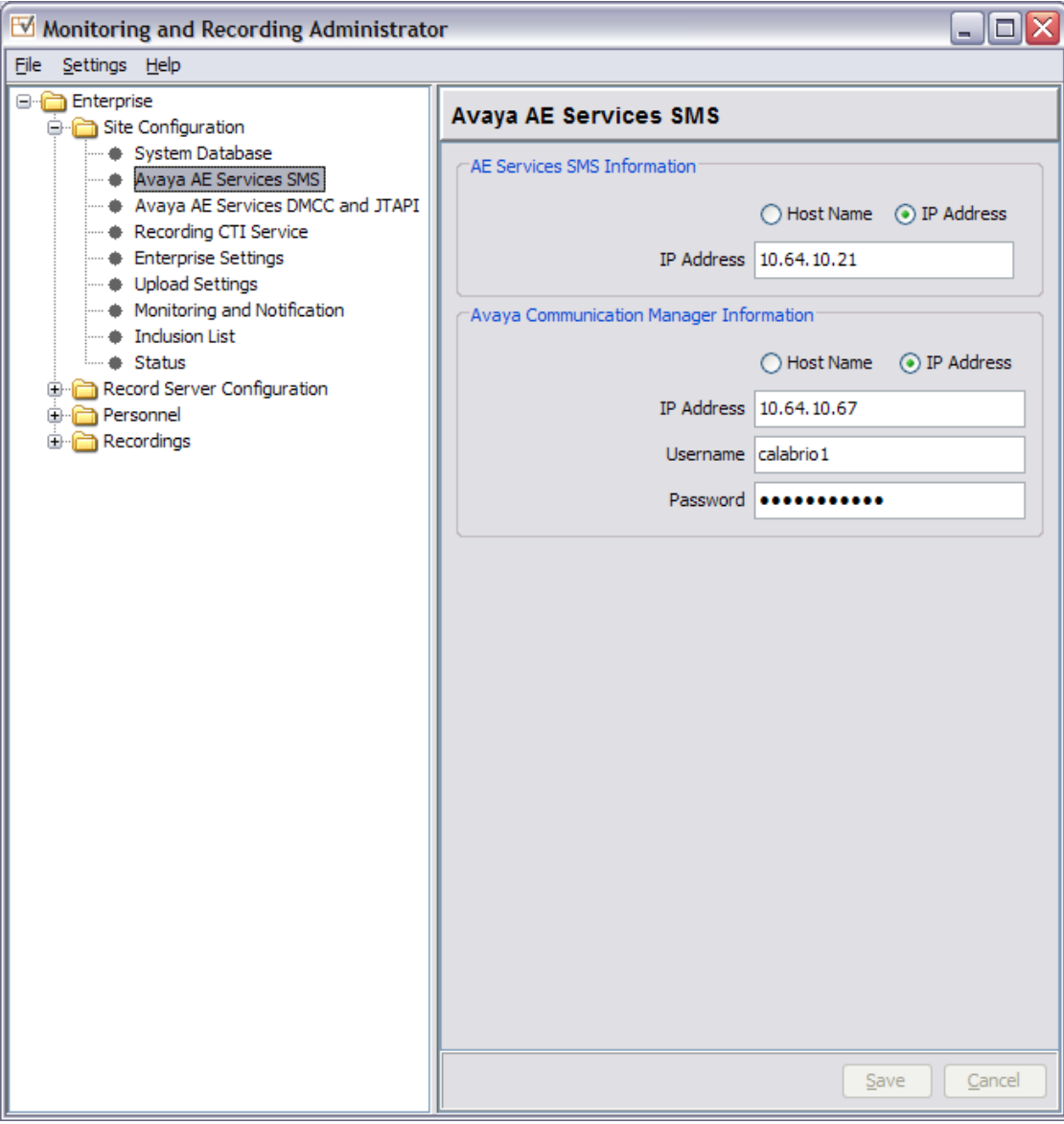
The initial configuration of the MARS server is typically performed by Calabrio technicians or authorized installers. These Application Notes will only cover the steps necessary to configure the MARS solution to interoperate with Avaya Aura<sup>®</sup> Communication Manager and Avaya Aura<sup>®</sup> Application Enablement Services.

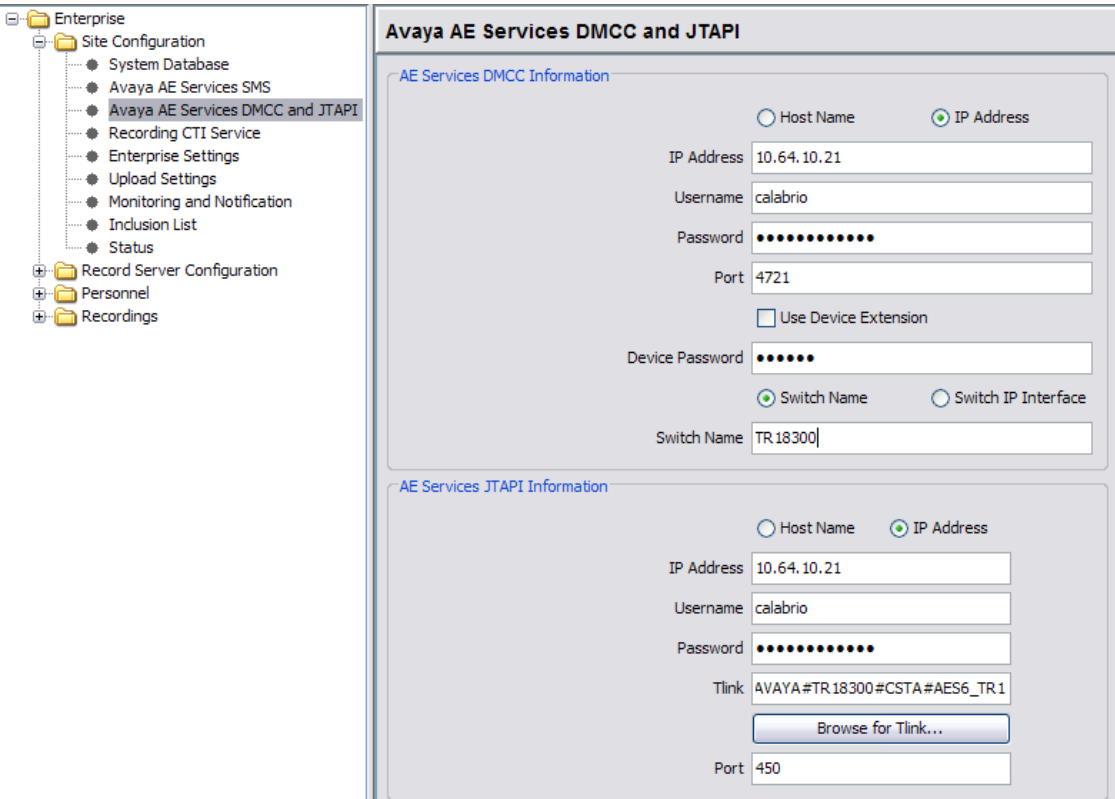
### 7.1. MARS Configuration Details

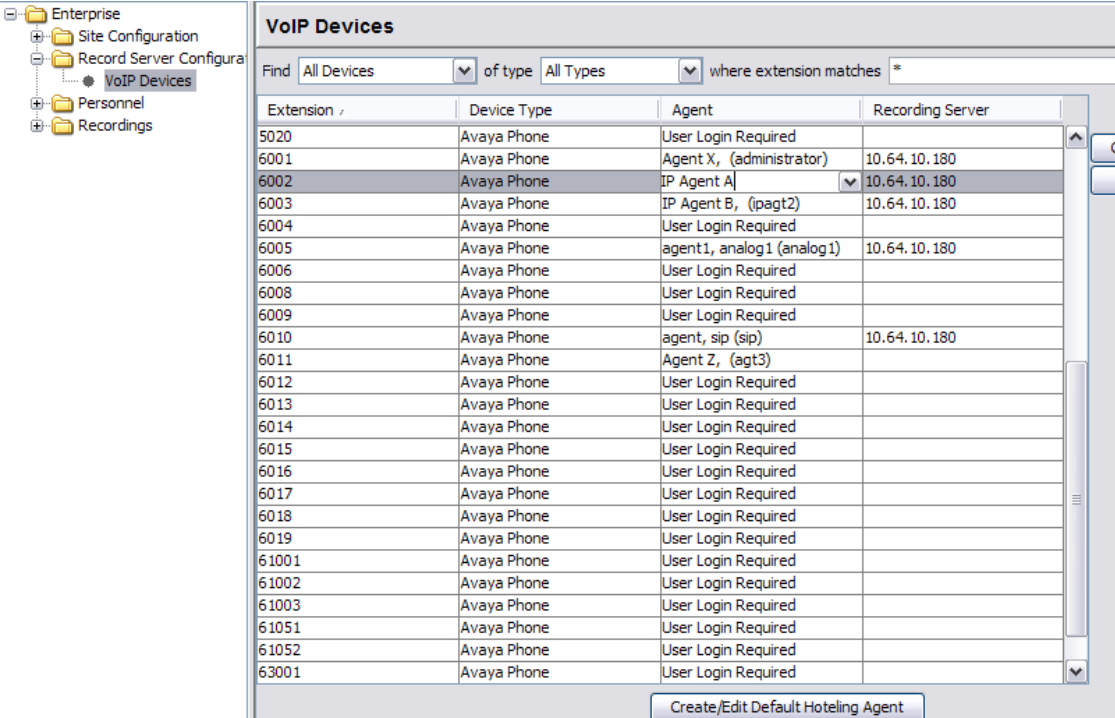
On the Calabrio MARS server, launch the Monitoring and Recording Administrator application from the Windows Programs menu and log in with the appropriate credentials.

The steps include:

- Configuration of the Application Enablement Interfaces – SMS
- Configuration of the Application Enablement Interfaces
- Configuration of Devices
- Configuration of Agents
- Configuration of Recording Schedules (Workflows)

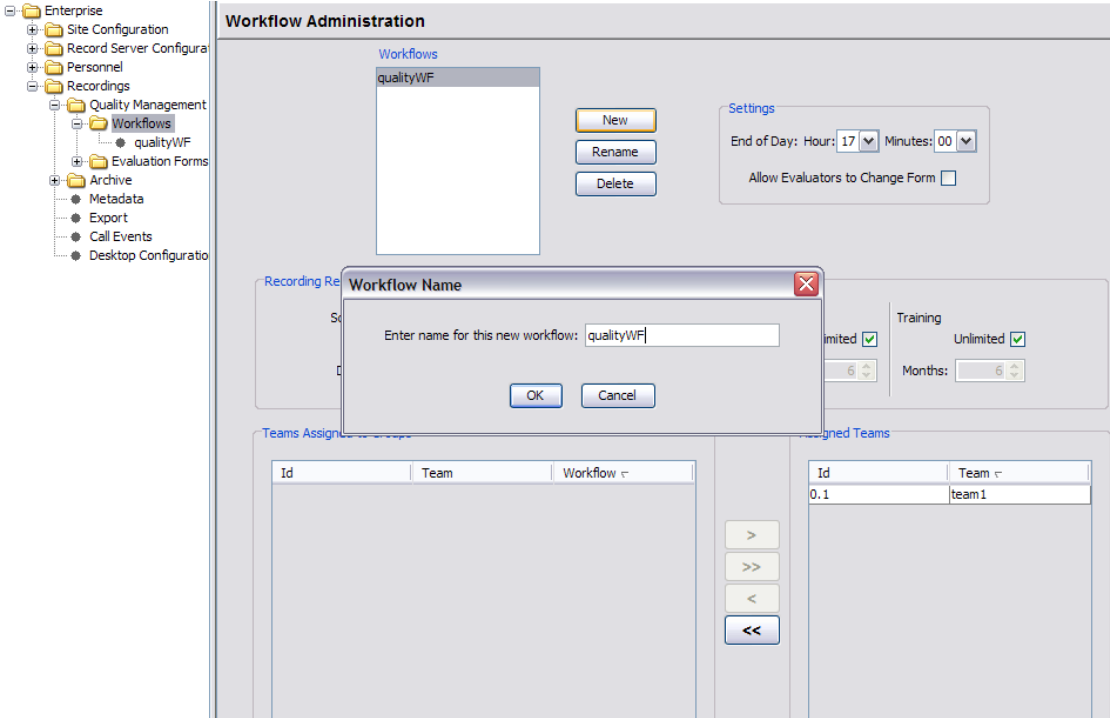
Step	Description
<p>1.</p>	<p><b>Configuration of the Application Enablement Interfaces – SMS</b></p> <p>Under the <b>Site Configuration</b>, select the <b>Avaya AE Services SMS</b> object in the navigation panel.</p> <p>Provide the <b>IP Address</b> or <b>Host Name</b> of the <b>Application Enablement Services</b> server in the <b>AE Services SMS Information</b> section. In the <b>Avaya Communication Manager Information</b> section, provide the <b>IP Address</b> of Communication Manager procr as well as the <b>Username</b> and <b>Password</b> configured in <b>Section 5.1, Step 5</b> above.</p> 

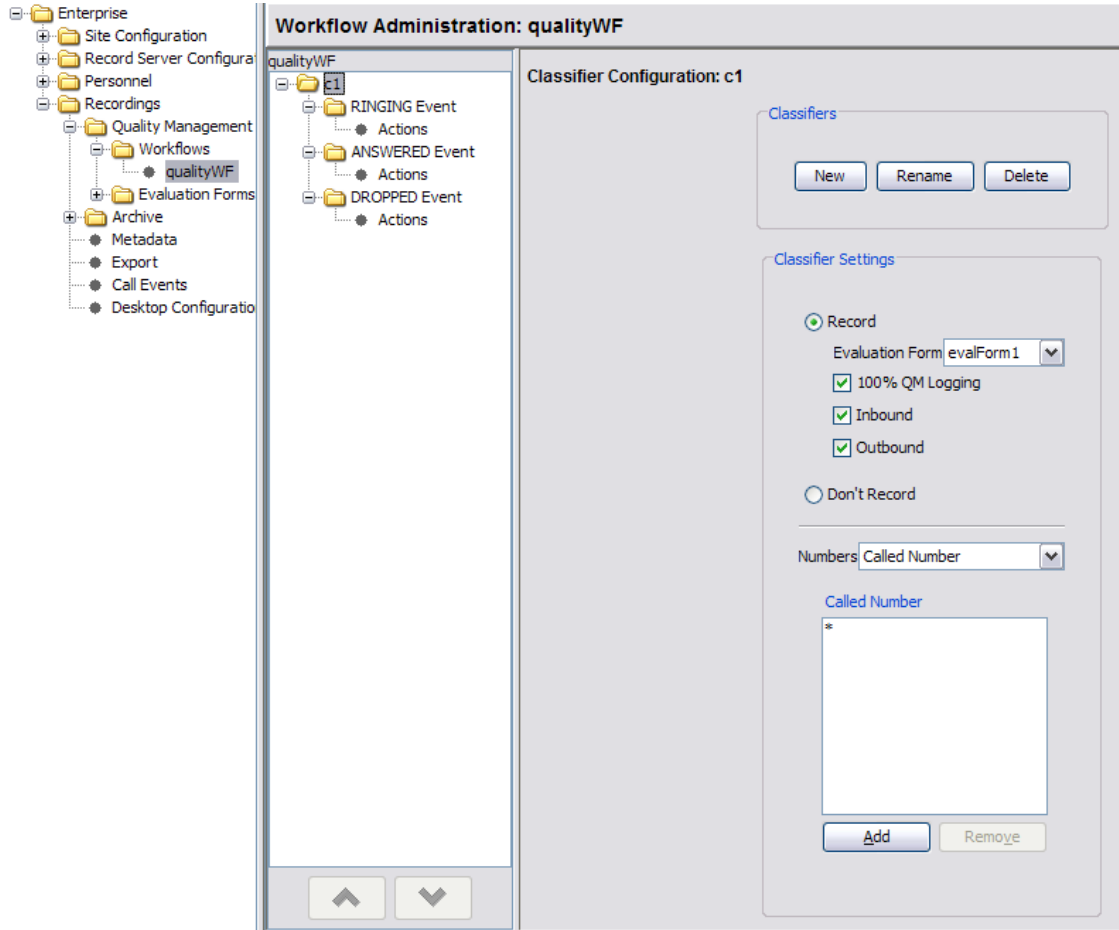
Step	Description
2.	<p><b>Configuration of the Application Enablement Interfaces</b></p> <p>Select the <b>Avaya AE Services DMCC and JTAPI</b> object in the navigation panel. In the <b>AE Services DMCC Information</b> section, provide:</p> <ul style="list-style-type: none"> <li>• <b>Host Name</b> or <b>IP Address</b> of the <b>Application Enablement Services</b> server</li> <li>• <b>Username</b> and <b>Password</b> (from <b>Section 6.1, Step 3</b>)</li> <li>• Enter <b>Port 4721</b> (the default DMCC listen port).</li> <li>• <b>Device Password</b> for the stations. Note that all station passwords must be the same for this solution; however, check with Calabrio for alternatives if necessary.</li> <li>• <b>Switch Name</b> or <b>Switch IP Interface</b>. This entry must match the configuration in <b>Section 6.1, Step 1</b>. Switch Name (TR18300) is preferred when multiple IP Interfaces are used for H.323 Gatekeepers as it allows Application Enablement to manage registrations in a pool.</li> </ul> <p>In the <b>AE Services JTAPI Information</b> section, provide:</p> <ul style="list-style-type: none"> <li>• <b>Host Name</b> or <b>IP Address</b> of the procr or CLAN used for the AE Services Switch Link configured in <b>Section 6.1, Step 1</b>. Repeat the <b>Username</b> and <b>Password</b>.</li> <li>• Enter or browse for the <b>Tlink</b> information as configured in <b>Section 6.1, Step 5</b>.</li> <li>• Use the default <b>Port 450</b> which is the TSAPI service listening port on Application Enablement Services. Click <b>Save</b> to complete this step.</li> </ul> 

Step	Description
3.	<p><b>Configuration of Devices</b></p> <p>When the SMS query completes, all devices from Communication Manager are listed in the VoIP Devices page Enterprise → Record Server Configuration → VoIP Devices.</p> <p>A device is assigned to be recorded by assigning a <b>Recording Server</b> to each device on the <b>VoIP Devices</b> page, and then assigning an <b>Agent</b> to that device using drop down lists in each column. Agents are configured on the <b>User Administration</b> page as described in the next step.</p> <p>Click <b>Save</b> to complete this step.</p> 



Step	Description																																																																						
4.	<h3>Configuration of Agents</h3> <p>Users are created and maintained on the <b>User Administration</b> page <b>Enterprise → Personnel → User Administration</b>. Users can be assigned to teams, and once created, can be statically assigned to a VoIP Device as demonstrated in <b>Step 3</b>. See product documentation for more details on this step.</p> <div><div><ul style="list-style-type: none"><li>Enterprise<ul style="list-style-type: none"><li>Site Configuration</li><li>Record Server Configuration</li><li>Personnel<ul style="list-style-type: none"><li>User Administration</li><li>Team Administration</li><li>Group Administration</li></ul></li><li>Recordings</li></ul></li></ul></div><div><div>User Administration</div><div><div>Create UserLicense UsersDelete User *Number Licensed Users: 8</div><div>Configured UsersManagersEvaluatorsArchive UsersSupervisorsAgentsKnowledge WorkerNot Configured UsersUnassigned Users</div><table><thead><tr><th>License</th><th>Last Name</th><th>First Name</th><th>User ID</th><th>Assigned Team</th><th>Assigned Group</th><th>Windows Login</th></tr></thead><tbody><tr><td>AQM</td><td>agent</td><td>sip</td><td>0.8</td><td>team1</td><td>group1</td><td>sip</td></tr><tr><td>AQM</td><td>agent1</td><td>analog1</td><td>0.7</td><td>team1</td><td>group1</td><td>analog1</td></tr><tr><td>AQM</td><td>Agent X</td><td></td><td>2.6301</td><td>team1</td><td>group1</td><td>administrator</td></tr><tr><td>AQM</td><td>Agent Y</td><td></td><td>2.6302</td><td>team1</td><td>group1</td><td>agt2</td></tr><tr><td>AQM</td><td>Agent Z</td><td></td><td>2.6303</td><td>team1</td><td>group1</td><td>agt3</td></tr><tr><td>AQM</td><td>IP Agent A</td><td></td><td>2.6304</td><td>team1</td><td>group1</td><td>devconnect</td></tr><tr><td>AQM</td><td>IP Agent B</td><td></td><td>2.6305</td><td>team1</td><td>group1</td><td>ipagt2</td></tr><tr><td>AQM</td><td>person</td><td>supervisor</td><td>0.6</td><td>team1</td><td>group1</td><td>supervisor</td></tr><tr><td>Unlicensed</td><td>Administrator</td><td></td><td>0.9</td><td></td><td></td><td>administrator</td></tr></tbody></table><div><div>User Properties</div><div><div><div>LicenseAQM</div><div>First Name</div><div>Last NameAgent X</div><div>Assigned Teamteam1</div><div>User ID2.6301</div><div>Windows Loginadministrator</div><div>Edit User</div></div><div><div>Roles</div><div><input checked="" type="checkbox"/> Agent * <input type="checkbox"/> Supervisor <input type="checkbox"/> Evaluator <input type="checkbox"/> Manager <input type="checkbox"/> Archive User</div></div><div><div>Supervisor's QM Teams</div><div></div><div>AddRemove</div></div><div><div>Manager's Groups</div><div></div><div>AddRemove</div></div></div></div></div></div></div>	License	Last Name	First Name	User ID	Assigned Team	Assigned Group	Windows Login	AQM	agent	sip	0.8	team1	group1	sip	AQM	agent1	analog1	0.7	team1	group1	analog1	AQM	Agent X		2.6301	team1	group1	administrator	AQM	Agent Y		2.6302	team1	group1	agt2	AQM	Agent Z		2.6303	team1	group1	agt3	AQM	IP Agent A		2.6304	team1	group1	devconnect	AQM	IP Agent B		2.6305	team1	group1	ipagt2	AQM	person	supervisor	0.6	team1	group1	supervisor	Unlicensed	Administrator		0.9			administrator
License	Last Name	First Name	User ID	Assigned Team	Assigned Group	Windows Login																																																																	
AQM	agent	sip	0.8	team1	group1	sip																																																																	
AQM	agent1	analog1	0.7	team1	group1	analog1																																																																	
AQM	Agent X		2.6301	team1	group1	administrator																																																																	
AQM	Agent Y		2.6302	team1	group1	agt2																																																																	
AQM	Agent Z		2.6303	team1	group1	agt3																																																																	
AQM	IP Agent A		2.6304	team1	group1	devconnect																																																																	
AQM	IP Agent B		2.6305	team1	group1	ipagt2																																																																	
AQM	person	supervisor	0.6	team1	group1	supervisor																																																																	
Unlicensed	Administrator		0.9			administrator																																																																	

Step	Description
5.	<p><b>Configuration of Recording Schedules (Workflows)</b></p> <p>For the Compliance Test, all calls were recorded, inbound and outbound using a Workflow to define the conditions.</p> <p>On the <b>Recordings → Quality Management → Workflows</b> page, click the <b>New</b> button to create a Workflow, enter a name for the new workflow, and click <b>OK</b>. To assign the workflow to a team, select a team from the <b>Teams Assigned to Groups</b> list on the left side of the bottom of the page, and click the &gt; button to move that group into the <b>Assigned Teams</b> for the workflow.</p> <p>Click on <b>Save</b> to complete this step.</p> 

Step	Description
6.	<p data-bbox="280 233 1153 268"><b>Configuration of Recording Schedules (Workflows) - Continued</b></p> <p data-bbox="280 304 1377 485">Click on the newly created Workflow to edit the details of the schedule. For the Compliance Test, 100% QM Logging was enabled for <b>Inbound</b> and <b>Outbound</b> calls. If an <b>Evaluation Form</b> is to be used by users reviewing the recordings for this workflow, then select a previously configured Evaluation Form. Configuration of Evaluation Forms is beyond the scope of these Application Notes.</p> 

## 8. Verification Steps

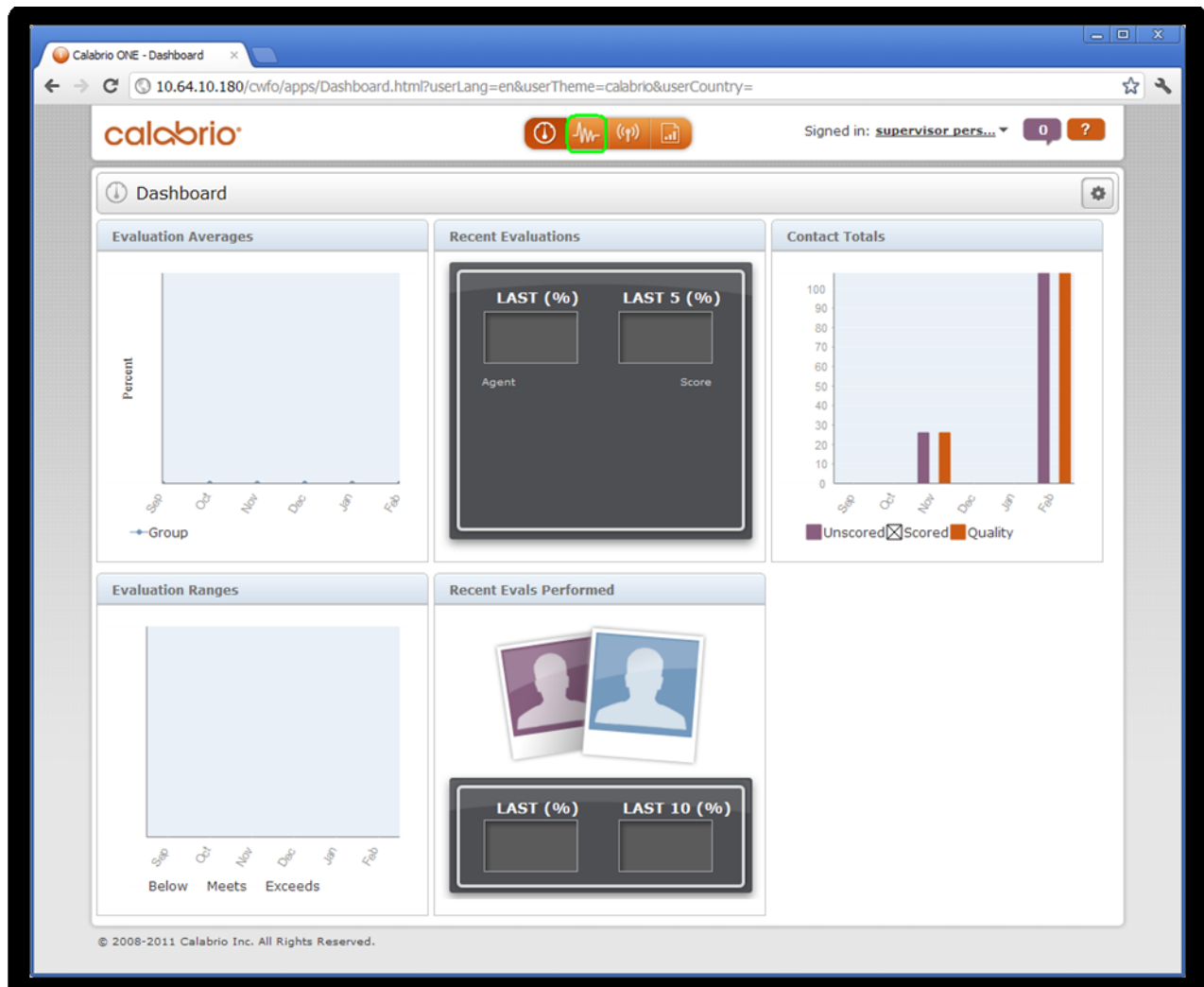
The following steps may be used to verify the configuration:

- 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 SAT, or navigate to **Status and Control → Switch Conn Summary** on the 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 SAT).
- Verify that the Calabrio recording ports are registered as **IP\_API\_A** stations in Communication Manager (use the **list registered-ip-stations** command on the SAT).
- Verify the Calabrio has successfully monitored the agent stations using TSAPI (use the **list monitored-stations** command on the 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.

Access the Calabrio web-based user interface using the URL **http://<ip-address>/cwfo** in a browser window, where **<ip-address>** is the address of the MARS server. The **Log In** screen is displayed as shown below. Use appropriate credentials to login.



Once logged in, launch the **Recording** interface from the Dashboard to reach the Search Recordings page.



On the **Recording** page, click **New or Refined Search**, create search criteria and click **Search** to find recordings.

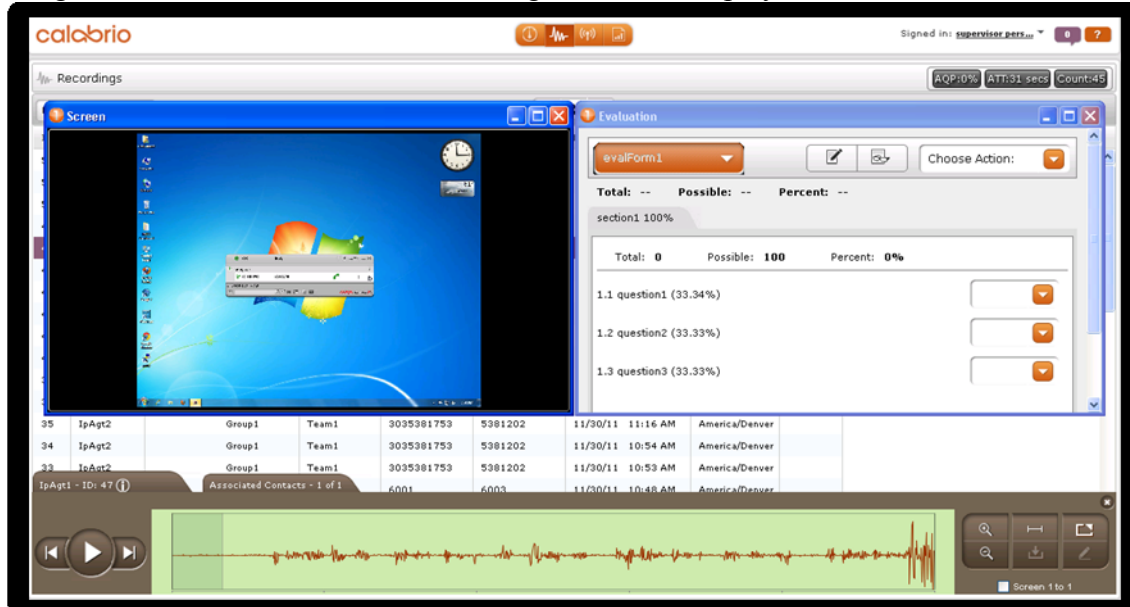
The screenshot shows the Calabrio ONE web application interface. The browser address bar indicates the URL: `10.64.10.180/cwfo/apps/Recordings.html?userLang=en&userTheme=calabrio&userCountry=`. The user is signed in as `supervisor pers...`. The search criteria section is highlighted with a green box and includes the following fields:

- Search Recordings** (with an `Expand Search` dropdown)
- Organization** (dropdown menu)
- Name** (text input)
- Phone Number** (text input)
- In the past we** (dropdown menu)
- Date Range** (dropdown menu)
- Specific Date** (text input)
- Time** (text input)
- All Evaluations** (dropdown menu)
- Search Scope** (dropdown menu)
- State** (text input)
- Search** (button)
- Cancel** (button)

Below the search criteria, the **Recordings** section is visible. It includes a **New or Refine Search** button and a table of recordings. The table has the following columns: **Contact**, **Last Name**, **Group Name**, **Team Name**, **Calling Number**, **Called Number**, **Date**, **Time**, **Time Zone**, **% Score**, and **Call Duration**. The table contains 15 rows of data, all showing recordings from 2/14/12 and 2/15/12.

Contact	Last Name	Group Name	Team Name	Calling Number	Called Number	Date	Time	Time Zone	% Score	Call Duration
298	Agent X	Group1	Team1	6001	6013	2/15/12	03:56 PM	America/Denver		00:00
281	Agent X	Group1	Team1	3035381753	5381202	2/14/12	02:37 PM	America/Denver		00:00
280	Agent X	Group1	Team1	3035381753	5381202	2/14/12	02:33 PM	America/Denver		00:00
279	Agent X	Group1	Team1	3035381753	5381202	2/14/12	02:26 PM	America/Denver		00:00
278	Agent X	Group1	Team1	3035381753	5381202	2/14/12	02:23 PM	America/Denver		00:00
277	Agent X	Group1	Team1	3035381753	5381202	2/14/12	02:21 PM	America/Denver		00:00
276	IP Agent B	Group1	Team1	6001	6514	2/14/12	02:10 PM	America/Denver		00:00
275	Agent X	Group1	Team1	6001	6514	2/14/12	02:09 PM	America/Denver		00:00
273	Agent X	Group1	Team1	3035381753	5381202	2/14/12	02:08 PM	America/Denver		00:00
272	Agent X	Group1	Team1	3035381753	5381202	2/14/12	02:04 PM	America/Denver		00:00
271	Agent X	Group1	Team1	6001	6304	2/14/12	01:55 PM	America/Denver		00:00
270	IP Agent A	Group1	Team1	6001	6304	2/14/12	01:55 PM	America/Denver		00:00
266	Agent X	Group1	Team1	3035381753	5381202	2/14/12	01:52 PM	America/Denver		00:00
265	Agent X	Group1	Team1	3035381753	5381202	2/14/12	01:47 PM	America/Denver		00:00

Selecting a call of interest and double clicking will launch a playback window as shown below.



## 9. Conclusion

These Application Notes described the procedures for configuring Calabrio MARS 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, Calabrio uses the Device and Media Control Services of Avaya Aura® Application Enablement Services to perform recording. During compliance testing, Calabrio successfully recorded calls placed to and from agents and station, 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.

### Calabrio

Product information for Calabrio products can be found at <http://calabrio.com/about-calabrio/services/>

---

**©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).