



Avaya Solution & Interoperability Test Lab

Application Notes for Calabrio Monitoring and Recording Services with Avaya Aura™ Communication Manager and Avaya Aura™ 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™ Communication Manager and Avaya Aura™ Application Enablement Services. Calabrio Monitoring and Recording Services uses real-time CTI data and RTP streams from Communication Manager to capture and 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 is a contact center and knowledge worker oriented recording solution. Using DMCC Multiple Registrations, and JTAPI, the recorder is able to register with Avaya Aura™ Communication Manager as an additional media endpoint for call activity occurring on the target agent and knowledge worker phones, with JTAPI providing call tagging data. These calls are recorded and stored with identifying information for cataloging and retrieval.

The interoperability of Monitoring and Recording Services with Avaya Aura™ Communication Manager is accomplished through Avaya Aura™ Application Enablement Services. These Application Notes describe the compliance test configuration used to test Calabrio Monitoring and Recording Services, with Avaya Aura™ Communication Manager running on an Avaya S8300D Server and an Avaya G450 Media Gateway.

Before Monitoring and Recording Services can start recording, it registers with Avaya Aura™ Application Enablement Services, performs an SMS service query to obtain a list of all of the Agents and Stations configured in Avaya Aura™ Communication Manager, and 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 that they work at. Dynamic assignment is not supported for any of the communication platforms supported by Monitoring and Recording Services. Future revisions of the application are expected to support dynamic assignment for free seating environments.

When the services are started on the Monitoring and Recording Services server, stations that are administered to be recorded are registered with Avaya Aura™ Communication Manager as a Dependent registration using the DMCC service on Avaya Aura™ Application Enablement Services. Once DMCC registration is successfully completed, Avaya Aura™ Communication Manager will send audio for all calls that originate or terminate on the registered stations to both the phone, and the recorder.

To ensure call records stored in the database are as rich as possible, the application uses the TSAPI/JTAPI capabilities of Avaya Aura™ 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.

1.1. Interoperability Compliance Testing

Compliance testing focused on the following areas, covered in the DevConnect Test Plan for Communication Manager and Application Enablement Services and Monitoring and Recording Services:

Phase 1 Installation & Configuration

Phase 2 Calabrio/Avaya Feature Functionality Verification

Phase 3 Failover and Serviceability Tests

Installation and configuration testing focused on the setup of all components and the ability to interoperate. The functionality testing focused on verifying Monitoring and Recording Services ability to detect, record, and search calls, while recording and storing recordings appropriately with basic telephony features. Serviceability testing focused on verifying the ability of Monitoring and Recording Services to recover from adverse conditions.

1.2. Support

Technical support on Calabrio Monitoring and Recording Services can be obtained through the following:

- **Phone:** +1 (763) 592-4680 or +1 (800) 303-1248
- **Web:** www.calabrio.com/support
- **Email:** calabriosupport@calabrio.com

2. Reference Configuration

Calabrio Monitoring and Recording Services can be configured on a single Windows Server, or distributed across multiple servers for larger scale deployments. The compliance test configuration used a single server configuration.

The detailed administration of basic connectivity between Avaya Aura™ Communication Manager, Avaya Aura™ Application Enablement Services, and of contact center devices, are not the focus of these Application Notes and will not be fully described.

In the compliance testing, the Monitoring and Recording Services solution was configured to monitor three physical station extensions “6001 - 6003” on Avaya Aura™ Communication Manager as well as two IP Agent stations “6004 – 6005” with one configured in Telecommuter mode, the other in Road Warrior mode. As DMCC Multiple Registrations functionality does not support Extension to Cellular (EC500) functionality, this scenario was not tested.

The interoperability of Monitoring and Recording Services with Avaya Aura™ Communication Manager is accomplished through Avaya Aura™ Application Enablement Services. The compliance test configuration used to test Monitoring and Recording Services included the Avaya S8300D Server, the Avaya G450 Media Gateway, Avaya Aura™ Application Enablement Services, Windows 2008 Server, soft clients, and telephones. **Figure 1** provides a high level topology.

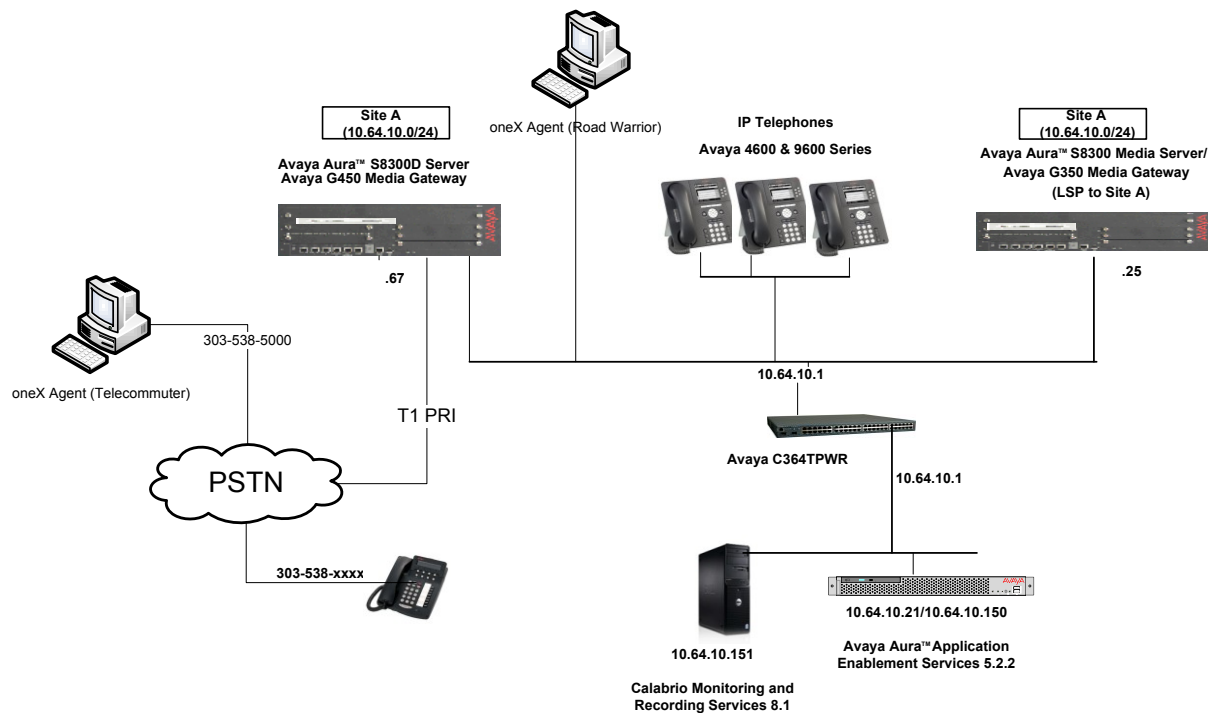


Figure 1: Calabrio Monitoring and Recording Services Compliance Test Sample Configuration

3. Equipment and Software Validated

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

Hardware/Software Component	Version/Description
Avaya S8300 Server and G450 Media Gateway	Avaya Aura™ Communication Manager 6.0 (R016x.00.0.345.0) with Cold Patch 18444
Avaya Aura™ Application Enablement Services	Release 5.2.2.105.0
Avaya 9600 and 2400 Series IP Telephones, and IP Agent	9620, 9630, 9640 (H.323), 2421 (H.323),
Avaya one-X™ Agent, Avaya IP Agent	R2, R7.0
Calabrio Monitoring and Recording Services on Windows 2008 Server, MS SQL 2008	8.1

4. Configure Avaya Aura™ Communication Manager

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

This section provides the procedures for configuring Avaya Aura™ Communication Manager. The procedures fall into the following areas:

- Verify Feature and License are adequate for the integration
- Administer Processor Ethernet Interface for Avaya Aura™ Application Enablement Services connectivity
- Administer Avaya Aura™ Communication Manager System Features
- Administer Computer Telephony Integration (CTI) Link
- Add SMS User Account
- Confirm Station Administration

The detailed administration of contact 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.

4.1. Verify Feature and License are adequate 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. TSAPI entitlements must be activated in both licenses. If this option is not set to “y”, contact the Avaya sales team or business partner for a proper license file.

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		
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		

Unlike many DMCC recording solutions, the Calabrio Monitoring and Recording Services solution does not require additional stations to be configured, nor will it consume IP_API_A registration licenses due to only being supported on Communications Manager R5 or later and Application Enablement Services R5.1 or later and the fact that it uses the DMCC Multiple Registrations method.

4.2. Administer Processor Ethernet Interface for Application Enablement Services Connectivity

Enter the **change node-names ip** command. The Application Enablement Services and **procr** node-names need to be defined here. The actual IP address may vary.

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	::	

On most R6 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.

display ip-interface procr		Page 1 of 2
IP INTERFACES		
Type: PROCR	Target socket load: 4800	
Enable Interface? y	Allow H.323 Endpoints? y	
Network Region: 1	Allow H.248 Gateways? y	
	Gatekeeper Priority: 5	
IPV4 PARAMETERS		
Node Name: procr	IP Address: 10.64.10.67	
Subnet Mask: /24		

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		

Add an entry for Application Enablement Services as described below:

- 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 [Reference 2].

change ip-services					Page	1 of	4
IP SERVICES							
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port		
AESVCS	y	procr	8765				
CDR1		procr	0	MTS	9000		
CDR2		procr	0	RDTT	9001		

On Page 4 of the IP Services form, enter the following values:

- In the **AE Services Server** field, type the name obtained from 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.

change ip-services				Page 4 of 4
AE Services Administration				
Server ID	AE Services Server	Password	Enabled	Status
1:	aesserver2	*	y	in use

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. The administered name for the Application Enablement Services server is created as part of the Application Enablement Services installation, and can be obtained from the Application Enablement Services server by typing **uname -n** at the Linux command prompt.

4.3. Administer Communication Manager System Features

Enter the **change system-parameters features** command and ensure that **Create Universal Call ID (UCID)** is enabled system wide on page 5, and that **Send UCID to ASAI** is set to “y” on page 13. Monitoring and Recording Services relies on UCID to track complex calls (Transfers and Conferences).

```
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
```

```
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
```


4.4. Administer Computer Telephony Integration (CTI) Link

This section provides the steps required for configuring a CTI Link.

Enter the **add cti-link <link number>** command, where **<link number>** is an available CTI link number.

- In the **Extension** field, type **<station extension>**, where **<station extension>** is a valid station extension.
- In the **Type** field, type **ADJ-IP**.
- In the **Name** field, type a descriptive name.

```
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
```

```
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
```

```
add cti-link 1                                     Page 3 of 3
                                         CTI LINK
Bridged Appearance Origination Restriction? n
                                         SAC/CF Override: n
```

4.5. Add SMS User Account

Monitoring and Recording Services uses the Application Enablement Services SMS interface to query for administered Stations and Agents for use in administering the application.

A privileged user was used in this test, however, a local administrator would likely 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, **User Profile 31** was created as shown below:

add user-profile 31			Page 1 of 41		
USER PROFILE 31					
User Profile Name: Calabrio SMS					
This Profile is Disabled? n			Shell Access? y		
Facility Test Call Notification? n			Acknowledgement Required? n		
Grant Un-owned Permissions? n			Extended Profile? n		
Name Cat Enbl			Name Cat Enbl		
Adjuncts A n			Routing and Dial Plan J n		
Call Center B y			Security K n		
Features C n			Servers L n		
Hardware D n			Stations M y		
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		

Read only access to Agents and Stations is required. Enter '**r-**' permissions for the **B** and **M** Categories on the **Set Permissions for Category:** entry on the **change user-profile xx** form (two separate transactions).

change user-profile 31			Page 3 of 41		
USER PROFILE 31					
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 --					
agent B r-					
agent-loginID B r-					
alarms H --					
alias station M r-					
alphanumeric-dial-table J --					
alternate-frl C --					
amw all G --					
amw asai G --					
amw audix G --					
amw pms G --					
analog-testcall board G --					

Then, create a user account on the **System Management Interface** web page and assign the user account to the user-profile created above.

Administrator Accounts -- Change Login

This page allows you to edit an administrator login.

[Click to Change](#)

Login name	<input type="text" value="calabrio"/>
<input type="checkbox"/> Primary group	<input type="text" value="users"/>
<input checked="" type="checkbox"/> Additional groups (profile)	<input type="text" value="prof31"/>
<input type="checkbox"/> Linux shell (/sbin/nologin for no shell)	<input type="text" value="/opt/ecs/bin/autosat"/>
Home directory	<input type="text" value="/var/home/calabrio"/>
<input type="checkbox"/> Lock this account	<input type="checkbox"/>
<input type="checkbox"/> Date after which account is disabled-blank to ignore (YYYY-MM-DD)	<input type="text"/>
<input checked="" type="checkbox"/> Select type of authentication	<div><input checked="" type="radio"/> Password <input type="radio"/> ASG: enter key <input type="radio"/> ASG: Auto-generate key</div>
Enter password or key	<input type="password" value="....."/>
Re-enter password or key	<input type="password" value="....."/>
Force password/key change on next login	<div><input type="radio"/> Yes <input checked="" type="radio"/> No</div> <p>The user will not be forced to change the password on next login. To enable this behavior, enter a new password and select the <i>Yes</i> option.</p>

4.6. Confirm Station Administration

All stations that will be recorded must be IP Softphone enabled, and the application needs to know the **security code** in order to successfully register, shown below.

change station 6004		Page 1 of 4
STATION		
Extension: 6004	Lock Messages? n	BCC: 0
Type: 4620	Security Code: 123456	TN: 1
Port: S00147	Coverage Path 1:	COR: 1
Name: IP Agent #1	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
	Time of Day Lock Table:	
Loss Group: 19	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 6004	
Speakerphone: 1-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	

5. Configure Avaya Aura™ Application Enablement Services

Avaya Aura™ Application Enablement Services enables applications to monitor and control telephony resources on Avaya Aura™ Communication Manager. The Avaya Aura™ Application Enablement Services server receives requests from applications and forwards them to Avaya Aura™ Communication Manager. Conversely, the Avaya Aura™ Application Enablement Services server receives responses and events from Avaya Aura™ Communication Manager and forwards them to the appropriate applications.

This section assumes that the installation and basic administration of the Avaya Aura™ Application Enablement Services server has already been performed. For more information on administering Avaya Aura™ Application Enablement Services, refer to the Avaya product documentation, Reference [2].

This section provides the procedures for configuring Avaya Aura™ Application Enablement Services. The procedures fall into the following areas:

- Confirm Network Configuration
- Configure Avaya Aura™ Communication Manager Switch Connections
- Verify TSAPI and DMCC Licensing
- Add TSAPI Links

- Add CTI User
- Enable Unrestricted Access to the Security Database
- Note the T-Link Name

Access the web-based administration interface using **https://<ip-address>** in a browser where **<ip-address>** is the client interface address of the Avaya Aura™ Application Enablement server. Click on the **Continue to Login** link. Login using appropriate credentials.

The screenshot shows the Avaya Application Enablement Services Management Console login page. At the top left is the Avaya logo. To its right is the title "Application Enablement Services" with the subtitle "Management Console" below it. A red horizontal bar spans the width of the page, with a "Help" link on the right. In the center, there is a login box with the text "Please login here:". Inside the box, there are two input fields: "Username" with the value "craft" and "Password" with masked characters "*****". Below these fields is a "Login" button. At the bottom of the page, a red horizontal bar is followed by the copyright notice "© 2009 Avaya, Inc. All Rights Reserved."

The **Welcome to OAM** screen is displayed next.

AVAYA**Application Enablement Services**
Management Console

Welcome: User craft
Last login: Mon Oct 11 09:42:32 2010 from 10.64.10.51
HostName/IP: aesserver2/10.64.10.21
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

HomeHome | Help | Logout

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

Welcome to OAM

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

- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- Licensing - Use Licensing to manage the license server.
- Maintenance - Use Maintenance to manage the routine maintenance tasks.
- Networking - Use Networking to manage the network interfaces and ports.
- Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.
- Status - Use Status to obtain server status informations.
- 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.

© 2009 Avaya, Inc. All Rights Reserved.

5.1. Confirm Network Configuration

Select **Networking > Network Configure** and note the client interface IP Address (**eth3** in this example) which will be used later in the application configuration. Application Enablement Services can be configured to use one or multiple NIC interfaces. It is preferable for security and performance reasons to use multiple interfaces and to have these on separate networks. The Communication Manager interface should always be bound to **eth0**.

AVAYA**Application Enablement Services**
Management Console

Welcome: User craft
Last login: Thu Sep 30 09:59:37 2010 from 10.64.10.51
HostName/IP: aesserver2/10.64.10.21
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

Networking | Network ConfigureHome | Help | Logout

- AE Services
- Communication Manager Interface
- Licensing
- Maintenance
- Networking
 - AE Service IP (Local IP)
 - Network Configure
 - Ports
- Security
- Status
- User Management
- Utilities
- Help

Network Configure

Hostname: aesserver2
DNS Domain: avaya.com
Primary DNS Server: 205.171.3.65
Secondary DNS Server: 205.171.2.65
Default Gateway: 10.64.10.1

Interface	Auto_Neg/Speed/Duplex	Physical IP Address	Netmask	Enable	Connectivity
eth0	on / 100 / full	10.64.10.21	255.255.255.0	<input checked="" type="checkbox"/>	switch, media
eth1	on / unknown / unknown	192.11.13.6	255.255.255.252	<input checked="" type="checkbox"/>	N/A
eth2	N/A			<input type="checkbox"/>	N/A
eth3	on / 100 / full	10.64.10.150	255.255.255.0	<input checked="" type="checkbox"/>	client
eth4	N/A			<input type="checkbox"/>	N/A

Apply Changes Cancel Changes

5.2. 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 **S8300DCM6** for this test environment:

The screenshot shows the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for "User craft" with login details. The main navigation bar shows "Communication Manager Interface | Switch Connections" and links for "Home | Help | Logout". A left sidebar lists various services, with "Communication Manager Interface" expanded to show "Switch Connections". The main content area, titled "Switch Connections", contains an "Add Connection" button and a table with the following data:

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
S8300DCM6	Yes	30	1
S8300mobile	No	30	0
devcon31	No	30	0

Below the table are buttons for "Edit Connection", "Edit PE/CLAN IPs", "Edit H.323 Gatekeeper", and "Delete Connection". The footer indicates "© 2009 Avaya, Inc. All Rights Reserved."

Use the **Edit Connection** button shown above to configure the **Switch Password**. This must match the password configured in section 4.2 above. Enter the **Switch Password** and check the **Processor Ethernet** box if using the **procr** interface, as shown below.

The screenshot shows the "Connection Details - S8300DCM6" configuration page. It includes fields for "Switch Password" and "Confirm Switch Password", a "Msg Period" of 30 minutes, and checkboxes for "SSL" and "Processor Ethernet", both of which are checked. "Apply" and "Cancel" buttons are at the bottom. The header and sidebar are consistent with the previous screenshot.

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.

The screenshot shows the Avaya Application Enablement Services Management Console. The left sidebar contains a navigation menu with options: AE Services, Communication Manager Interface (selected), Switch Connections (selected), Dial Plan, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area is titled 'Edit Processor Ethernet IP - S8300DCM6'. It features a text input field containing '10.64.10.67' and an 'Add/Edit Name or IP' button. Below this is a table with two columns: 'Name or IP Address' and 'Status'. The table contains one entry: '10.64.10.67' with a status of 'In Use'. A 'Back' button is located at the bottom of the table.

Welcome: User craft
Last login: Mon Sep 27 15:59:11 2010 from 10.64.10.51
HostName/IP: aesserver2/10.64.10.150
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services
Communication Manager Interface
Switch Connections
Dial Plan
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Help

Edit Processor Ethernet IP - S8300DCM6

10.64.10.67 Add/Edit Name or IP

Name or IP Address	Status
10.64.10.67	In Use

Back

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.

The screenshot shows the Avaya Application Enablement Services Management Console. The left sidebar contains a navigation menu with options: AE Services, Communication Manager Interface (selected), Switch Connections (selected), Dial Plan, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area is titled 'Edit H.323 Gatekeeper - S8300DCM6'. It features a text input field containing '10.64.10.67' and an 'Add Name or IP' button. Below this is a section labeled 'Name or IP Address' with a green checkmark icon next to '10.64.10.67'. A 'Delete IP' button is located at the bottom of this section.

Welcome: User craft
Last login: Mon Sep 27 15:59:11 2010 from 10.64.10.51
HostName/IP: aesserver2/10.64.10.150
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services
Communication Manager Interface
Switch Connections
Dial Plan
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Help

Edit H.323 Gatekeeper - S8300DCM6

Add Name or IP

Name or IP Address

10.64.10.67

Delete IP

5.3. Verify TSAPI and DMCC Licensing

The Calabrio Monitoring and Recording Services application will consume a **TSAPI** and **DMCC_DMC** license for each station that is to be monitored and recorded. If the number of licenses are not adequate for the integration, contact Avaya sales or an authorized reseller.

Navigate to **Licensing > WebLM Server Access** and login using appropriate credentials. Select **Application_Enablement** under **Licensed Products > APPL_ENAB** to display entitlements and acquired licenses.

Note that integrations with older releases of Communication Manager will also consume an **IP_API_A** license in Communication Manager. With Communication Manager R5 and Application Enablement Services 4.1 and later, **IP_API_A** will only be consumed if adequate **DMCC DMC** licenses are not available on Application Enablement Services.

AVAYA

Web License Manager (WebLM v4.6)

Logout

Install License

Licensed Products

Application_Enablement

Uninstall License

Change Password

Server Properties

Manage Users

Logout

Application Enablement (CTI) - Release: S-ID: 10503000 (Standard License File)

You are here: Licensed products > Application Enablement (CTI)

License installed on: Jul 8, 2010 2:19:07 PM MDT

[View Peak Usage](#)

Licensed Features

Feature (Maxused)	Expiration Date	Licensed	Acquired
Unified CC API Desktop Edition (VALUE_ABE_ARC_UNIFIED_CC_DESKTOP)	permanent	10000	0
Device Media and Call Control (VALUE_ABE_DHCC_OAC)	permanent	10000	5
DUS (VALUE_ABE_DUS)	permanent	1	0
CYLAN ASAI (VALUE_ABE_CYLAN_ASAI)	permanent	1	0
AES ADVANCED SMALL SWITCH (VALUE_ABE_AES_SMALL_ADVANCED)	permanent	5	0
CYLAN Proprietary Link (VALUE_ABE_PROPRIETARY_LINKS)	permanent	5	0
AES ADVANCED LARGE SWITCH (VALUE_ABE_AES_LARGE_ADVANCED)	permanent	5	0
TSAPI Simultaneous Users (VALUE_ABE_TSAPI_USERS)	permanent	10000	5
AES ADVANCED MEDIUM SWITCH (VALUE_ABE_AES_MEDIUM_ADVANCED)	permanent	5	0
Product Notes (VALUE_NOTES)	permanent	SmallServers: ASB00-ASB00-cc-premco-trn400-aptop MacMiniServers: cmv105, cmv105-der1590, xen1x20, h20_8832_yrn LargeServers: lp1210, yrn125, d389g, d389g2, unknown TrunkApplications: IPF_001, BasicUnrestricted, AdvancedUnrestricted, DHCUnrestricted, VIF_001, BasicUnrestricted, AdvancedUnrestricted, DHCUnrestricted, VIF_001, BasicUnrestricted, AdvancedUnrestricted, DHCUnrestricted, PC_001, BasicUnrestricted, L3gateUnrestricted, DHCUnrestricted, CIL_001, BasicUnrestricted, AdvancedUnrestricted, DHCUnrestricted, CSPC_001, BasicUnrestricted, AdvancedUnrestricted, DHCUnrestricted, VIF_001, BasicUnrestricted, AdvancedUnrestricted, DHCUnrestricted; SAFEHOME_001 VALUE_ABE_UNIFIED_CC_DESKTOP, COE_001, BasicUnrestricted, AdvancedUnrestricted, DHCUnrestricted, CIL_001, BasicUnrestricted, AdvancedUnrestricted, DHCUnrestricted; CIL_001, BasicUnrestricted, AdvancedUnrestricted, DHCUnrestricted; AIVA-VENIT_001, BasicUnrestricted, AdvancedUnrestricted, DHCUnrestricted;	not counted

Acquired Licenses

Feature	Acquired by	Count
(VALUE_ABE_DHCC_OAC)	DHCC (asservr2)	5
(VALUE_ABE_TSAPI_USERS)	TSAPI (asservr2)	5

The screenshot below gives a closer look at these license counts.

Feature (Keyword)	Expiration Date	Licensed	Acquired
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	permanent	10000	0
Device Media and Call Control (VALUE_AES_DMCC_DMC)	permanent	10000	5
DLG (VALUE_AES_DLG)	permanent	1	0
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	permanent	1	0
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	permanent	8	0
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	permanent	8	0
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	permanent	8	0
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	permanent	10000	5
AES ADVANCED MEDIUM SWITCH (VALUE_AES_AEC_MEDIUM_ADVANCED)	permanent	8	0

5.4. 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 CTI link number must match the number configured in the **cti-link** form in **Section 4.4**. Click **Apply Changes**.

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

The screenshot shows the Avaya Application Enablement Services Management Console. The top navigation bar includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message: "Welcome: User craft. Last login: Mon Sep 27 15:59:11 2010 from 10.64.10.51. HostName/IP: aesserver2/10.64.10.150. Server Offer Type: TURNKEY. SW Version: r5-2-2-105-0". The main navigation menu on the left lists "AE Services", "CVLAN", "DLG", "DMCC", "SMS", "TSAPI", "Communication Manager Interface", "Licensing", "Maintenance", "Networking", "Security", "Status", "User Management", "Utilities", and "Help". The "TSAPI" section is expanded, showing "TSAPI Links" and "TSAPI Properties". The "TSAPI Links" page is displayed, featuring a form titled "Edit TSAPI Links". The form contains the following fields: "Link" (value: 3), "Switch Connection" (dropdown menu showing "S8300DCM6"), "Switch CTI Link Number" (dropdown menu showing "1"), "ASAI Link Version" (dropdown menu showing "4"), and "Security" (dropdown menu showing "Unencrypted"). At the bottom of the form are two buttons: "Apply Changes" and "Cancel Changes".

5.5. Add a CTI User

Monitoring and Recording Services requires a CTI user account to access Application Enablement Services. Select **User Management -> User Admin -> Add User** from the left pane.

In the **Add User** screen, enter the following values:

- In the **User Id** field, type a meaningful user id.
- In the **Common Name** field, type a descriptive name.
- In the **Surname** field, type a descriptive surname.
- In the **User Password** field, type a password for the user.
- In the **Confirm Password** field, re-enter the same password for the user.
- In the **Avaya Role** field, retain the default of **None**.
- In the **CT User** field, select **Yes** from the dropdown menu.
- Click **Apply** at the bottom of the screen (not shown here).

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title 'Application Enablement Services Management Console', and a welcome message for 'User craft' with login details. A red navigation bar contains links for 'User Management | User Admin | Add User', 'Home | Help | Logout'. A left sidebar lists various system components, with 'User Management' expanded to show 'User Admin' and 'Add User' selected. The main content area is the 'Add User' form, which includes a list of fields with asterisks indicating required information. The 'CT User' dropdown is set to 'Yes'.

AVAYA Application Enablement Services Management Console

Welcome: User craft
Last login: Wed Oct 13 10:22:51 2010 from 10.64.10.51
HostName/IP: aesserver2/10.64.10.21
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

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

Add User

Fields marked with * can not be empty.

* User Id: calabrio

* Common Name: Calabrio

* Surname:

* User Password:

* Confirm Password:

Admin Note:

Avaya Role: None

Business Category:

Car License:

CM Home:

Css Home:

CT User: Yes

Department Number:

Display Name:

Employee Number:

Employee Type:

Enterprise Handle:

Given Name:

Home Phone:

Home Postal Address:

Initials:

Labeled URI:

Mail:

MM Home:

Mobile:

Organization:

Pager:

Preferred Language: English

5.6. Enable Unrestricted Access to the Security Database

The Calabrio user account will require unrestricted SDB access in order to be able to access any of the Devices (stations) administered to be recorded in the application.

To change the security level for the CT User Select **Security -> Security Database -> CTI Users -> List All Users** from the left pane. Choose the CTI user, and click **Edit** (not shown below).

On the **Edit CTI User** page, check the **Unrestricted Access** option and click on **Apply Changes**.

Edit CTI User

User Profile:

User ID	Calabrio
Common Name	Calabrio
Worktop Name	NONE
Unrestricted Access	<input checked="" type="checkbox"/>

Call Origination and Termination / Device Status

None

Call and Device Monitoring:

Device	None
Call / Device	None
Call	<input type="checkbox"/>

Routing Control:

Allow Routing on Listed Devices

None

5.7. Note the T-Link Name

This information will be used to confirm the application configuration below.

Select **Status > Status and Control > TSAPI Service Summary** from the left pane and select **Edit T-Links** (not shown below). Once at the **Edit T-Links** screen, this screen shows a select box of the Tlink names. A new Tlink name is automatically generated by the Application Enablement Services server upon creation of a new switch connection. Locate and select the Tlink name associated with the relevant switch connection which would use the name of the switch connection as part of the Tlink name (not shown below). This screen will also provide information on the status of the TLink as shown below:

AVAYA

Application Enablement Services
Management Console

Welcome: User craft
Last login: Mon Oct 11 16:12:49 2010 from 10.64.10.51
HostName/IP: aesserver2/10.64.10.21
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

Status | Status and Control | TSAPI Service SummaryHome | Help | Logout

AE Services

Communication Manager Interface

Licensing

Maintenance

Networking

Security

Status

Alarm Viewer

Logs

Status and Control

CVLAN Service Summary

DLG Services Summary

DMCC Service Summary

Switch Conn Summary

TSAPI Service Summary

User Management

Utilities

Help

Tlink Status

☐ Enable page refresh every 60 seconds

Tlink AVAYA#S8300DCM6#CSTA#AESSERVER2

SubmitTSDI Info

AVAYA#DEVCON31#CSTA#AESSERVER2

General Info

RegisteredYES

Number of Open Streams0

Tlink Version5.2.1 Build 483

Supported ProtocolsTS1-2

SecurityCSTA

Flow Control - TSDI Buffer

Max Flow Allowed800

Max Flow Reached0Reset Max Flow Reached

Invoke IDs

In Use0

Max Used0Reset Max IDs

Outstanding Connections

Current0

Max Used0Reset Max Connections

Back

© 2009 Avaya, Inc. All Rights Reserved.

6. Configure the Monitoring and Recording Services server

This section provides the procedures for configuring the Monitoring and Recording Services server. The procedures include the following areas:

- Configuration of the Avaya Aura[™] Application Enablement Interfaces
- Configuration of Devices and Agents
- Launch Calabrio User Interface
- View Recorded Calls

The initial configuration of the Monitoring and Recording Services server is typically performed by Calabrio technicians or authorized installers. The procedural steps are presented in these Application Notes for informational purposes.

6.1. Configuration of the Application Enablement Interfaces

Before Monitoring and Recording Services can be configured for target devices, the interface must be defined. This is done via the **Monitoring and Recording Administrator** application which is installed on a workstation in the customer environment.

In CLAN configurations, using the **Host Name** of the switch connection defined in 5.2 in the **Communication Manager Information** entry will be preferred; this will allow Application Enablement Services and Communication Manager to pool resources on behalf of the application.

The screenshot shows the 'Monitoring and Recording Administrator' application window. The left sidebar contains a tree view with the following structure:

- Enterprise
 - Site Configuration
 - Monitoring and Recording Database
 - Avaya AE Services**
 - Monitoring and Recording CTI Service
 - Enterprise Settings
 - Upload Settings
 - Monitoring and Notification
 - Inclusion List
 - Status
 - Record Server Configuration
 - VoIP Devices
 - Personnel
 - User Administration
 - Team Administration
 - Group Administration
 - Recordings
 - Quality Management
 - Workflows
 - qualityWf
 - Evaluation Forms
 - Templates
 - Forms
 - Archive
 - Workflows
 - arwf
 - Metadata
 - Export

The main content area is titled 'Avaya AE Services' and contains four configuration sections:

- AE Services JTAPI Information:**
 - Host Name: ☐ IP Address: ☒
 - IP Address: 10.64.10.150
 - Username: calabrio
 - Password: *****
 - Tlink: AVAYA#58300DCM6#CSTA#AESSEVER2
 - Browse for Tlink... button
 - Port: 450
- AE Services DMCC Information:**
 - Host Name: ☐ IP Address: ☒
 - IP Address: 10.64.10.150
 - Username: calabrio
 - Password: *****
 - Port: 4721
 - ☐ Use Device Extension
 - Device Password: *****
- AE Services SMS Information:**
 - Host Name: ☐ IP Address: ☒
 - IP Address: 10.64.10.150
 - Username: interop@10.64.10.67
 - Password: *****
- Communication Manager Information:**
 - Host Name: ☐ IP Address: ☒
 - IP Address: 10.64.10.67

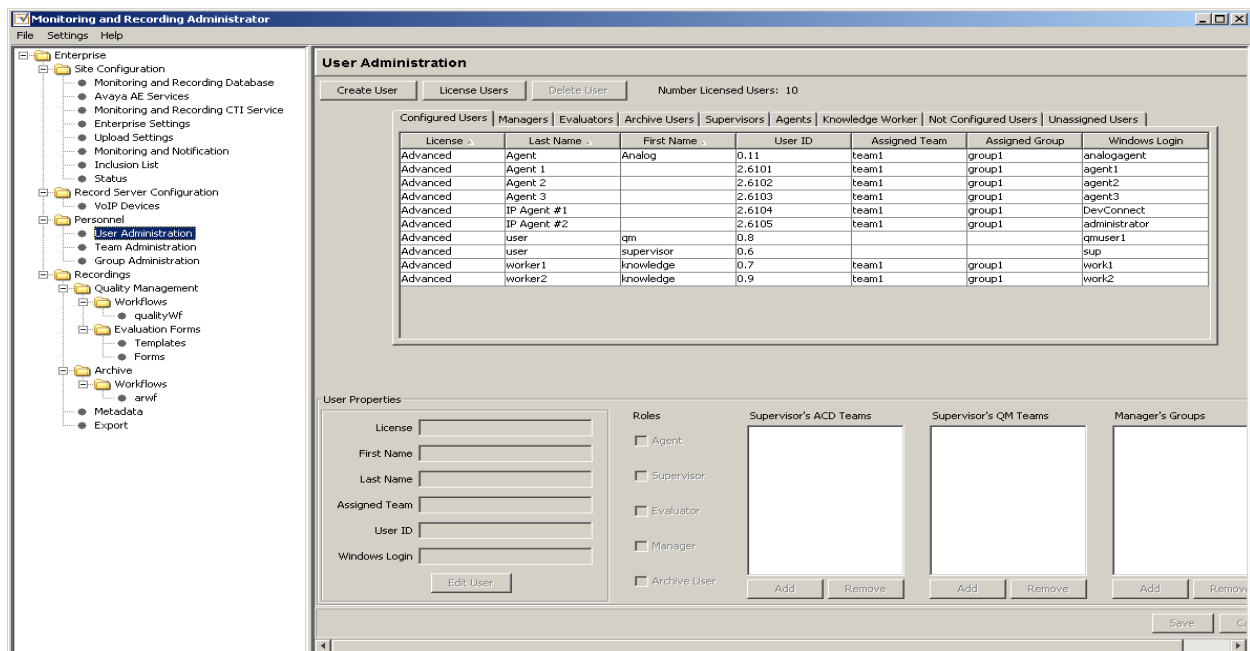
At the bottom right of the window are 'Save' and 'Cancel' buttons.

6.2. Configuration of Devices and Agents

When the SMS query completes, the devices to be recorded are configured by assigning a recording server to each device on the **VoIP Devices** page, and then assigning an Agent or Knowledge Worker to that device on the **User Administration** page. The configuration of these objects is illustrated below and covered in greater detail in the Installation Guide [Reference 3].

The screenshot displays the 'Monitoring and Recording Administrator' application window. The left sidebar shows a tree view with 'Enterprise' > 'Record Server Configuration' > 'VoIP Devices' selected. The main area is titled 'VoIP Devices' and contains a table with columns: Extension, Device Type, Agent, and Recording Server. A search bar at the top allows filtering by 'Find All Devices', 'of type All Types', and 'where extension matches *'. A 'Bulk Configuration' panel on the right includes a 'Configure Recording Server' button. The table lists devices 6001 through 6043, all of type 'Avaya Phone'. Devices 6001-6006 are assigned agents and recording servers. Devices 6007-6043 are currently unassigned. A dropdown menu is open for device 6007, showing a list of available agents: Agent 1, (agent1); Agent 2, (agent2); Agent 3, (agent3); Agent, Analog (analogagent); IP Agent #1, (DevConnect); IP Agent #2, (administrator); and user, supervisor (sup).

Extension	Device Type	Agent	Recording Server
6001	Avaya Phone	Agent 1, (agent1)	10.64.10.151
6002	Avaya Phone	worker2, knowledge (work2)	10.64.10.151
6003	Avaya Phone	Agent 3, (agent3)	10.64.10.151
6004	Avaya Phone	IP Agent #1, (DevConnect)	10.64.10.151
6005	Avaya Phone	IP Agent #2, (administrator)	10.64.10.151
6006	Avaya Phone	Agent, Analog (analogagent)	10.64.10.151
6007	Avaya Phone		
6008	Avaya Phone		
6020	Avaya Phone	Agent 1, (agent1)	
6021	Avaya Phone	Agent 2, (agent2)	
6022	Avaya Phone	Agent 3, (agent3)	
6023	Avaya Phone	Agent, Analog (analogagent)	
6024	Avaya Phone	IP Agent #1, (DevConnect)	
6025	Avaya Phone	IP Agent #2, (administrator)	
6026	Avaya Phone	user, supervisor (sup)	
6027	Avaya Phone		
6028	Avaya Phone		
6029	Avaya Phone		
6030	Avaya Phone		
6031	Avaya Phone		
6032	Avaya Phone		
6033	Avaya Phone		
6034	Avaya Phone		
6035	Avaya Phone		
6036	Avaya Phone		
6037	Avaya Phone		
6038	Avaya Phone		
6039	Avaya Phone		
6040	Avaya Phone		
6041	Avaya Phone		
6042	Avaya Phone		
6043	Avaya Phone		

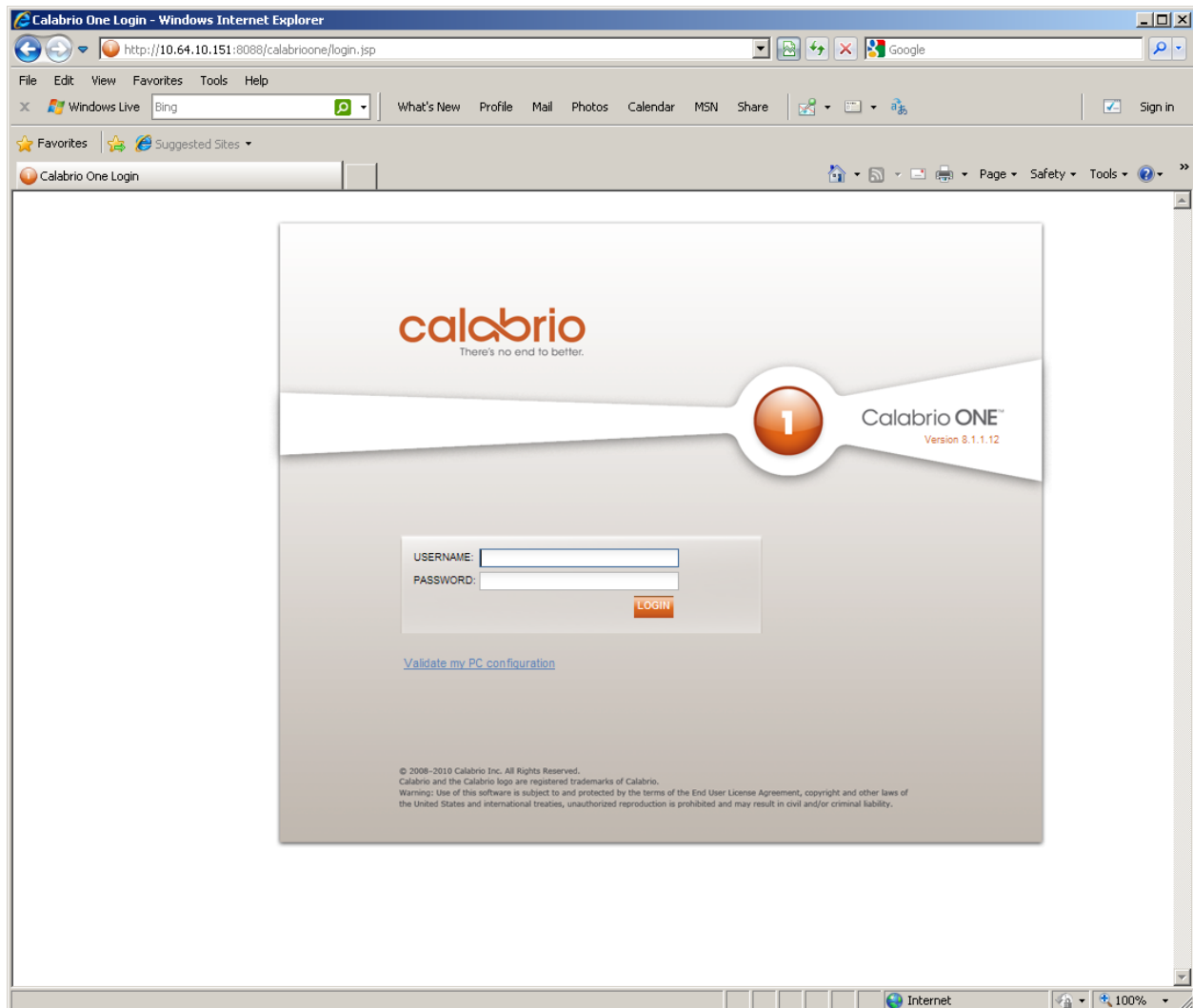


When the Monitoring and Recording services are started, the server establishes a Dependent Registration on each of the assigned devices, then initiates a TSAPI monitor on the station using the JTAPI service on Application Enablement Services. Once this is completed, the application is ready to record.

Recording can be initiated by configuring rules. Typically, every call is recorded, but not all recordings will be tagged for Quality purposes. Quality tagging enables the administrator to define rules such as time of day, call direction, called numbers (VDNs) and other criteria to assist in screening recordings for characteristics that are of interest to the user.

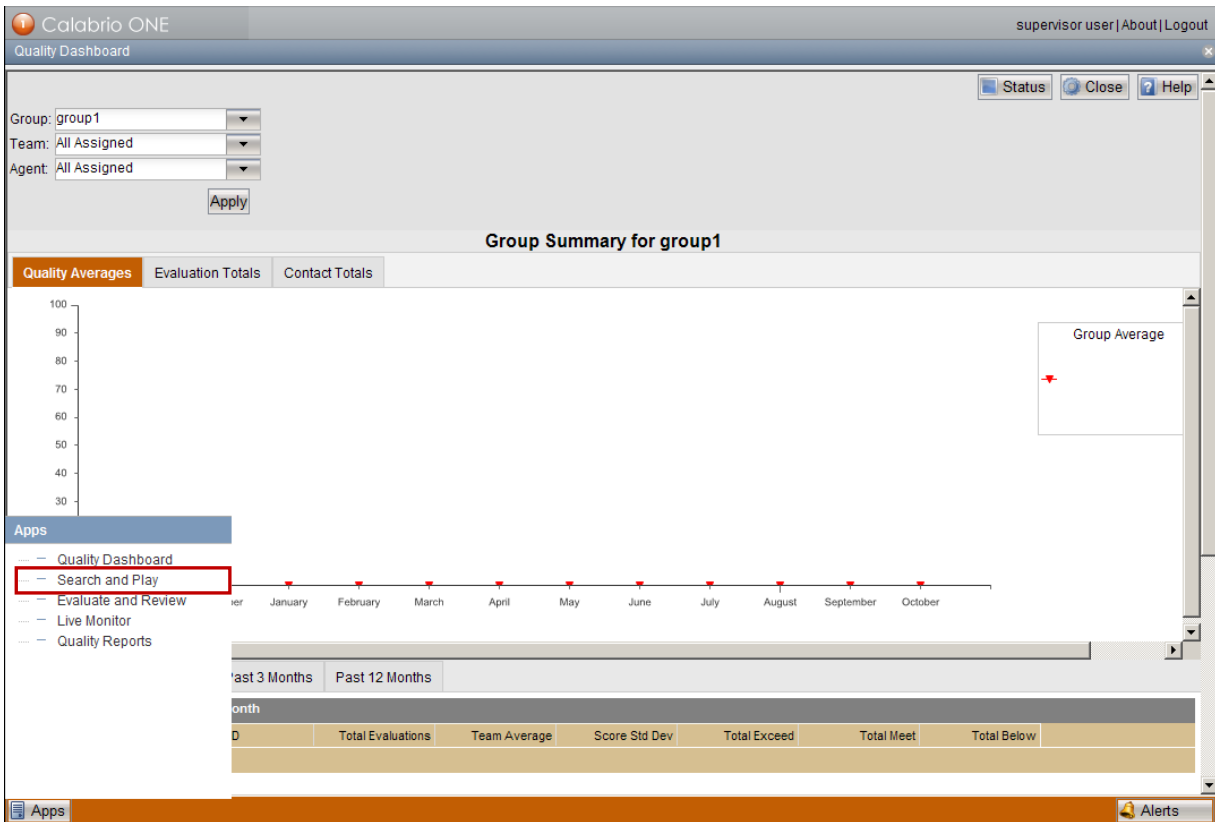
6.3. Launch Calabrio User Interface

Access the web-based user interface using the URL **http://<ip-address>:8088/calabrioone** in a browser window, where **<ip-address>** is the address of the Monitoring and Recording Services server. The **Log In** screen is displayed as shown below. Log in using the appropriate credentials.



6.4. Viewing Recorded Calls

Once logged in, a user may launch the **Search and Play** interface and define search criteria for recorded calls.



User Filters
 First Name:
 Last Name:
 Group:
 Team:

Recording Filters
 Metadata Field:
 Metadata Value:
 Phone #:
 Start Date:
 End Date:
 Contact ID:
☐ Tagged

	First Name	Last Name	Group Name	Team Name	Calling Number	Called Number	Date	Time	Time Zone	% Score	Reason
	knowledge	worker2	group1	team1	6001	6002	9/30/10	10:37 AM	America/Denver		Logging
	knowledge	Agent 1	group1	team1	6001	6002	9/30/10	10:37 AM	America/Denver		Logging
	knowledge	Agent 1	group1	team1	6001	6002	9/30/10	10:20 AM	America/Denver		Logging
	knowledge	worker2	group1	team1	3035381753	6500	9/29/10	11:24 AM	America/Denver		Logging
	knowledge	worker2	group1	team1	3035381753	6500	9/29/10	11:19 AM	America/Denver		Logging
	knowledge	worker2	group1	team1	3035381753	6500	9/29/10	11:15 AM	America/Denver		Logging
	knowledge	worker2	group1	team1	3035381753	6500	9/29/10	11:14 AM	America/Denver		Logging
	knowledge	worker2	group1	team1	6003	6002	9/29/10	10:59 AM	America/Denver		Logging
	knowledge	Agent 3	group1	team1	6003	6002	9/29/10	10:58 AM	America/Denver		Logging
	knowledge	worker2	group1	team1	6003	6002	9/29/10	10:43 AM	America/Denver		Logging
	knowledge	Agent 3	group1	team1	6003	6002	9/29/10	10:43 AM	America/Denver		Logging
	knowledge	worker2	group1	team1	6003	6002	9/29/10	10:27 AM	America/Denver		Logging
	knowledge	Agent 3	group1	team1	6003	6002	9/29/10	10:27 AM	America/Denver		Logging
	knowledge	Agent 1	group1	team1	6003	6002	9/28/10	4:49 PM	America/Denver		Logging
	knowledge	worker2	group1	team1	6003	6002	9/28/10	4:49 PM	America/Denver		Logging

Selecting the icon in front of the item of interest will launch a playback window as demonstrated below. For Audio only recordings, it will look like this:

Calabrio ONE

supervisor user | About | Logout

Search and Play

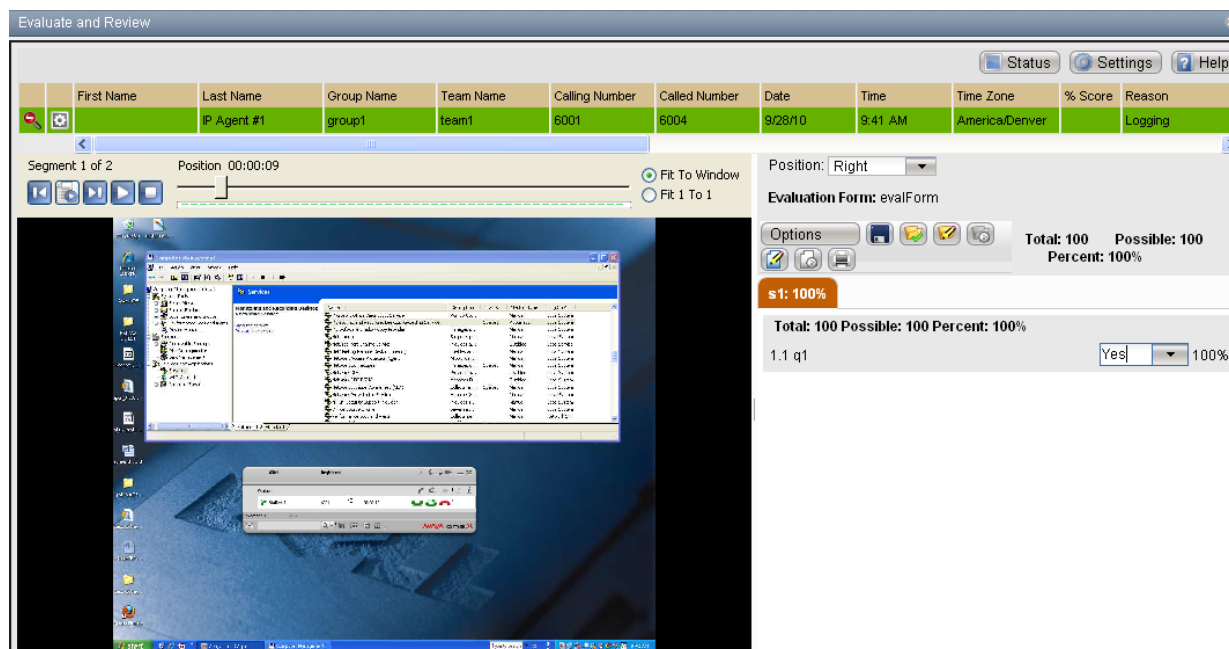
	First Name	Last Name	Group Name	Team Name	Calling Number	Called Number	Date	Time	Time Zone	% Score	Reason
	knowledge	worker2	group1	team1	6001	6002	9/30/10	10:37 AM	America/Denver		Logging

Segment 2 of 2 Position 00:00:00

Apps

Alerts

If the contact included screen recordings, it will appear like this:



7. General Test Approach and Test Results

All feature functionality test cases were performed manually to verify proper operation. The following scenarios were tested using the test configuration diagram shown in **Figure 1**.

The installation test cases were covered with the setup of Avaya Aura™ Communication Manager, Avaya Aura™ Application Enablement Services, and Calabrio Monitoring and Recording Services. The clean removal of the application was also covered in this section.

The functionality test cases were performed manually. Various calls were placed including incoming and outgoing PSTN calls to the monitored VDN, incoming and outgoing calls to and between the agents, and both telephones and soft clients. Calls were made with monitored and non-monitored agents, per test case specification.

The serviceability test cases were performed manually by disconnecting and reconnecting the Ethernet cable to the Monitoring and Recording Services server at different intervals, powering down Avaya Aura™ Communication Manager, powering down the Avaya Aura™ Application Enablement Services server, and also by stopping the CTI service on Avaya Aura™ Application Enablement Services.

The verification of tests included manually listening to recordings from the web, checking the timestamps and data of the recordings, and performing searches. All test cases passed. No errors were detected.

8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Aura™ Communication Manager, Avaya Aura™ Application Enablement Services, and Calabrio Monitoring and Recording Services.

Check the service state of your Avaya Aura™ Communication Manager CTI links by entering the **status aesvcs cti-link** command. The link status should show **no** for maintenance busy (**Mnt Busy**) and the **Service State** should indicate **established**.

status aesvcs cti-link						
AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	4	no	aesserver2	established	15	15
Command successfully completed						
Command:						

The **status aesvcs interface** command should indicate the interface is listening, even before Avaya Aura™ Application Enablement Services is configured.

AE SERVICES INTERFACE STATUS			
Local Node	Enabled?	Number of Connections	Status
procr	yes	1	listening
Command successfully completed			
Command:			

The **status aesvcs link** command will indicate the number of messages sent from, and received at the CLAN interface (or procr), to and from Avaya Aura™ Application Enablement Services, including maintenance traffic.

status aesvcs link						
AE SERVICES LINK STATUS						
Srvr/ Link	AE Services Server	Remote IP	Remote Port	Local Node	Msgs Sent	Msgs Rcvd
01/01	aesserver2	10.64.10.21	59815	procr	620	606
Command successfully completed						
Command:						

Once the Monitoring and Recording Services server is running, the **list registered-ip-stations** command will show both active phone registrations, and an entry for each station to be recorded that is associated with the Avaya Aura™ Application Enablement Services client link IP Address (10.64.10.150).

list registered-ip-stations					Page 1
REGISTERED IP STATIONS					
Station Ext or Orig Port	Set Type/ Net Rgn	Prod ID/ Release	TCP Skt Gatekeeper	Station IP Address/ IP Address	
6001	9640	IP_Phone	y	10.64.10.44	
	1	3.110b		10.64.10.67	
6002	9620	IP_Phone	y	10.64.10.41	
	1	3.110b		10.64.10.67	
6002	9620	IP_API_A	y	10.64.10.150	
	1	3.2040		10.64.10.67	
6003	9630	IP_Phone	y	10.64.10.43	
	1	3.110b		10.64.10.67	
6003	9630	IP_API_A	y	10.64.10.150	
	1	3.2040		10.64.10.67	
6004	4620	IP_Agent	y	10.64.10.50	
	1	9.0		10.64.10.67	
6004	4620	IP_API_A	y	10.64.10.150	
	1	3.2040		10.64.10.67	
press CANCEL to quit -- press NEXT PAGE to continue					
ESC-x=Cancel Esc-e=Submit Esc-p=Prev Pg Esc-n=Next Pg Esc-h=Help Esc-r=Refresh					

In addition, each station to be recorded will show an ASAI monitor association by using the **list monitored-station** command.

list monitored-station				
MONITORED STATION				
Station Ext	Association 1		Association 2	
	CTI Link	CRV	CTI Link	CRV
6002	1	32		
6003	1	12		
6004	1	63		
6005	1	41		
Command successfully completed				
Command:				

Navigate to **AE Services** on the Avaya Aura™ Application Enablement Services server to verify that services are **ONLINE** and **NORMAL MODE** for the TSAPI and DMCC Services, as shown in the screen below.

Application Enablement Services
Management Console

Welcome: User craft
Last login: Mon Sep 27 15:59:11 2010 from 10.64.10.51
HostName/IP: aesserver2/10.64.10.150
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

AE Services
Home | Help | Logout

AE Services

CVLAN
DLG
DMCC
SMS
TSAPI
Communication Manager Interface
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Help

AE Services

IMPORTANT: AE Services must be restarted for administrative changes to fully take effect. Changes to the Security Database do not require a restart.

Service	Status	State	License Mode	Cause*
ASAI Link Manager	N/A	Running	N/A	N/A
CVLAN Service	OFFLINE	Running	N/A	N/A
DLG Service	OFFLINE	Running	N/A	N/A
DMCC Service	ONLINE	Running	NORMAL MODE	N/A
TSAPI Service	ONLINE	Running	NORMAL MODE	N/A
Transport Layer Service	N/A	Running	N/A	N/A

For status on actual services, please use [Status and Control](#)

* -- For more detail, please mouse over the Cause, you'll see the tooltip, or go to help page.

License Information

You are licensed to run Application Enablement (CTI) version 5.0

Once the application has successfully started, the **DMCC Service Summary** will show all of the stations to be recorded as **REGISTERED** devices.

Application Enablement Services
Management Console

Welcome: User craft
Last login: Mon Sep 27 16:32:55 2010 from 10.64.10.51
HostName/IP: aesserver2/10.64.10.150
Server Offer Type: TURNKEY
SW Version: r5-2-2-105-0

Status | Status and Control | DMCC Service Summary
Home | Help | Logout

AE Services
Communication Manager Interface
Licensing
Maintenance
Networking
Security
Status
Alarm Viewer
Logs
Status and Control
CVLAN Service Summary
DLG Services Summary
DMCC Service Summary
Switch Conn Summary
TSAPI Service Summary
User Management
Utilities
Help

DMCC Service Summary - Device Summary

☐ Enable page refresh every 60 seconds

[Session Summary](#) Device Summary
Generated on Tue Sep 28 08:18:10 MDT 2010

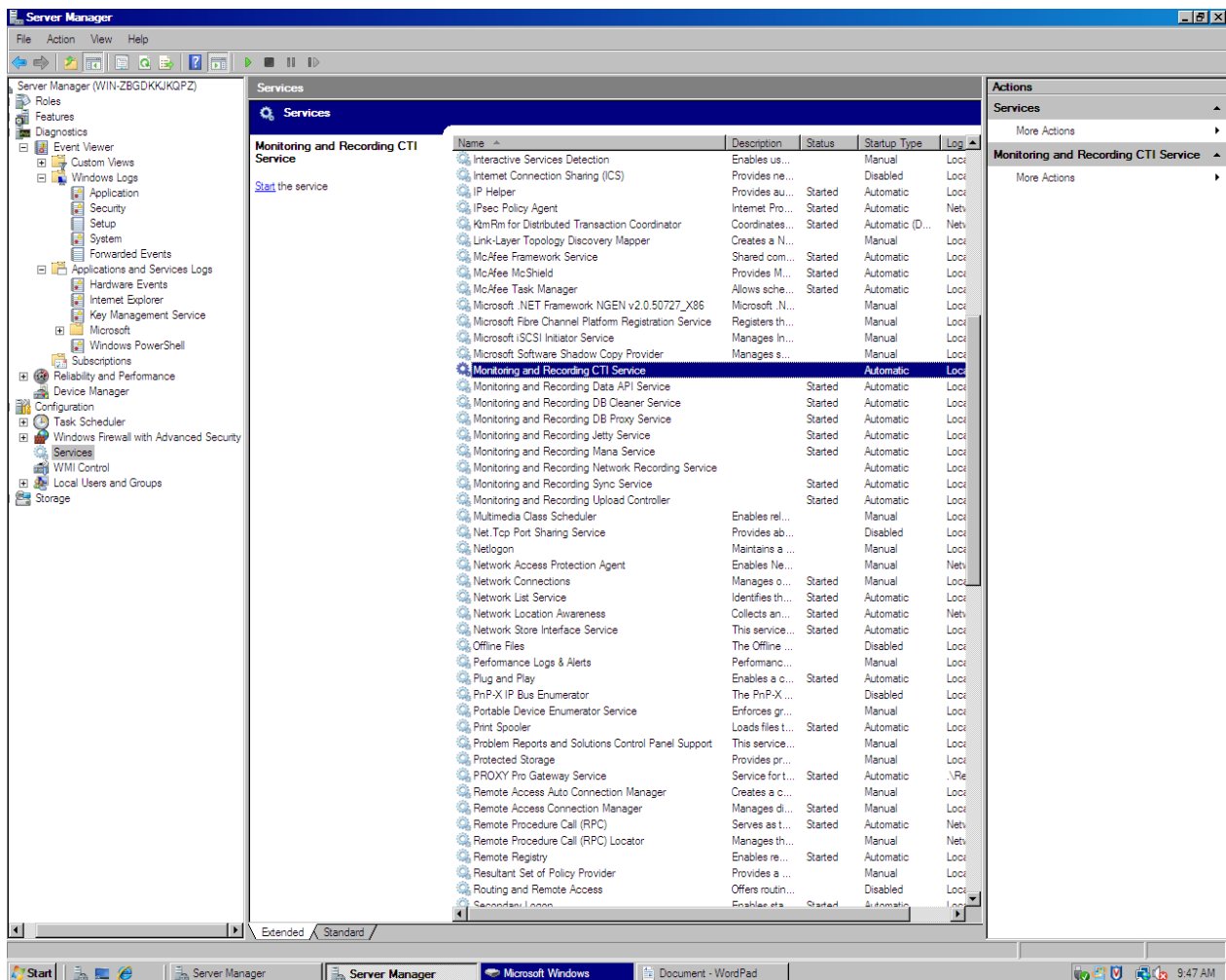
Service Uptime: 0 days, 0 hours and 1 minutes
Number of Active Sessions: 1
Number of Sessions Created Since Service Boot: 1
Number of Existing Devices: 5
Number of Devices Created Since Service Boot: 5

	Device ID	State	Associated Sessions
<input type="checkbox"/>	6001:S8300DCM6:10.64.10.67:0	REGISTERED	1
<input type="checkbox"/>	6002:S8300DCM6:10.64.10.67:0	REGISTERED	1
<input type="checkbox"/>	6003:S8300DCM6:10.64.10.67:0	REGISTERED	1
<input type="checkbox"/>	6004:S8300DCM6:10.64.10.67:0	REGISTERED	1
<input type="checkbox"/>	6005:S8300DCM6:10.64.10.67:0	REGISTERED	1

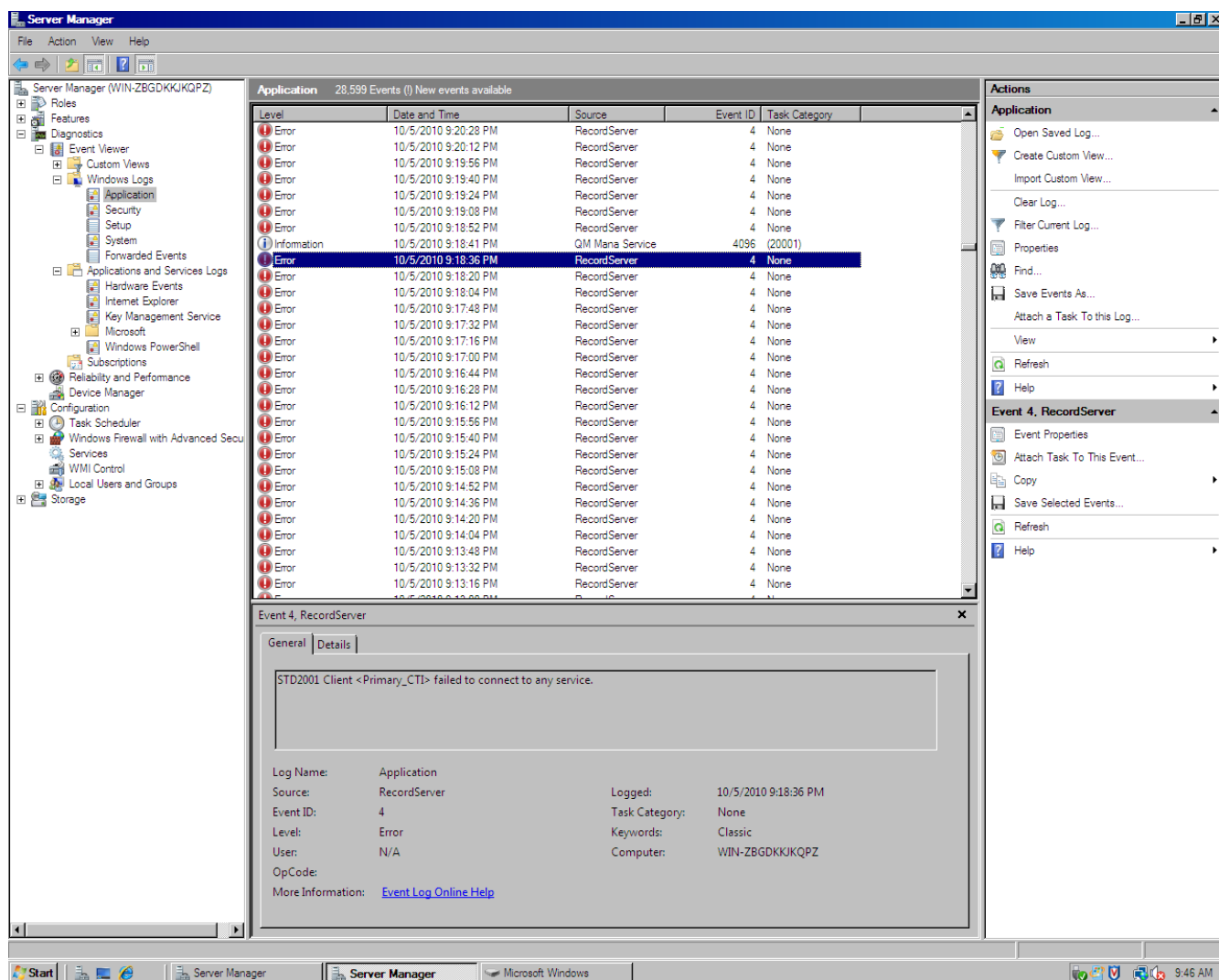
[Terminate Devices](#)

Item 1-5 of 5

To verify the setup from the Calabrio side, log in to the server and confirm the **Monitoring and Recording** services are **started** in the Windows **Services** manager page (NOTE: some services are not running in the screenshot below).



The Windows **Event Viewer** will list any status events of concern, and if configured, SNMP or email alarm notifications will be sent to alert the user of system alarms.



9. Conclusion

Calabrio Monitoring and Recording Services successfully captured and recorded phone activity for agents and knowledge workers. All test cases completed successfully.

10. Additional References

This section references the Avaya and Calabrio product documentation that are relevant to these Application Notes.

Avaya product documentation can be found at <http://support.avaya.com>:

[1] *Administering Avaya Aura™ Communication Manager*, Doc ID: 03-300509, Issue 6.0, Release 6.0, June 2010

[2] *Avaya MultiVantage Application Enablement Services Administration and Maintenance Guide*, Doc ID: 02-300357, Release 5.2, Issue 11, November 2009

[3] *Calabrio One Monitoring and Recording Services Installation Guide, Rev.8.1*

[4] *Calabrio One Monitoring and Recording Services Application User Guide, Rev. 8.0*

[5] *Calabrio One Monitoring and Recording Services Application Administrator User Guide, Rev. 8.1*

©2010 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.