



Avaya Solution & Interoperability Test Lab

Application Notes for MiaRec with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for MiaRec to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. MiaRec is a call recording solution.

In the compliance testing, MiaRec used the Telephony Services Application Programming Interface from Avaya Aura® Application Enablement Services to monitor skill groups and agent stations on Avaya Aura® Communication Manager, and used the Multiple Registration feature via the Avaya Aura® Application Enablement Services Device, Media, and Call Control interface to capture the media associated with the monitored stations for call recording.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration steps required for MiaRec to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. MiaRec is a call recording solution.

In the compliance testing, MiaRec used the Telephony Services Application Programming Interface (TSAPI) from Application Enablement Services to monitor skill groups and agent stations on Communication Manager, and used the Multiple Registration feature via the Application Enablement Services Device, Media, and Call Control (DMCC) XML interface to capture the media associated with the monitored stations for call recording.

The TSAPI interface was used by MiaRec to monitor skill groups and agent stations on Communication Manager. The DMCC interface was used by MiaRec to register a virtual IP softphones against each monitored agent station to pick up the media for call recording.

When there was an active call at a monitored agent station, MiaRec was informed of the call via event reports from the TSAPI interface, and starts the call recording by using the media from the associated virtual IP softphone. The event reports were also used to determine when to stop the call recordings.

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of MiaRec, the application automatically performed device queries and requested monitoring of skill groups and agent stations using TSAPI, and registered the virtual IP softphones using DMCC.

For the manual part of the testing, each call was handled manually on the agent telephone with generation of unique audio content for recordings. Necessary user actions such as hold and resume were performed from the agent telephones to test various call scenarios.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to MiaRec.

The verification of tests included use of MiaRec logs for proper message exchanges, and use of MiaRec web interface for proper logging and playback of calls.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Application Enablement Services and MiaRec included encrypted signaling and authentication for DMCC, and did not include encryption for TSAPI and DMCC RTP, as requested by MiaRec.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on MiaRec:

- Handling of TSAPI messages in areas of event notification and value queries.
- Use of DMCC registration services to register and un-register virtual IP softphones.
- Use of DMCC Multiple Registration feature to obtain the media from the virtual IP softphones.
- Proper recording, logging, and playback of calls for scenarios involving inbound, outbound, internal, external, ACD, non-ACD, hold, resume, G.711, G.729, forwarding, long duration, multiple calls, multiple agents, conference, and transfer.

The serviceability testing focused on verifying the ability of MiaRec to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to MiaRec.

2.2. Test Results

All test cases were executed. The following were the observations on MiaRec from the compliance testing.

- By design, multiple call legs associated with each transfer and conference scenario are grouped together into an Interaction by MiaRec.
- For an Interaction, the order of recording entries presented under the ALL CALLS IN THIS INTERACTION sub-section may not correspond to the order presented in the CALL[x] tabs. The recommendation is to select the recording entry under the ALL CALLS IN THIS INTERACTION sub-section, to link to the associated entry details in the proper CALL[x] tab.
- For conference scenarios, the parties reported in the TO parameter included “Conf x”, where “x” is the universal call ID associated with the conference.

2.3. Support

Technical support on MiaRec can be obtained through the following:

- **Phone:** +1 (408) 580-0150
- **Email:** support@miarec.com
- **Web:** <https://www.miarec.com/support>

3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**. The detailed administration of basic connectivity between Communication Manager and Application Enablement Services, and of contact center devices are not the focus of these Application Notes and will not be described.

In the compliance testing, MiaRec monitored the skill groups and agent stations shown in the table below.

Device Type	Extension
VDN	60001, 60002
Skill Group	61001, 61002
Supervisor	65000
Agent Station	65001 (H.323), 66002 (SIP)
Agent ID	65881, 65882

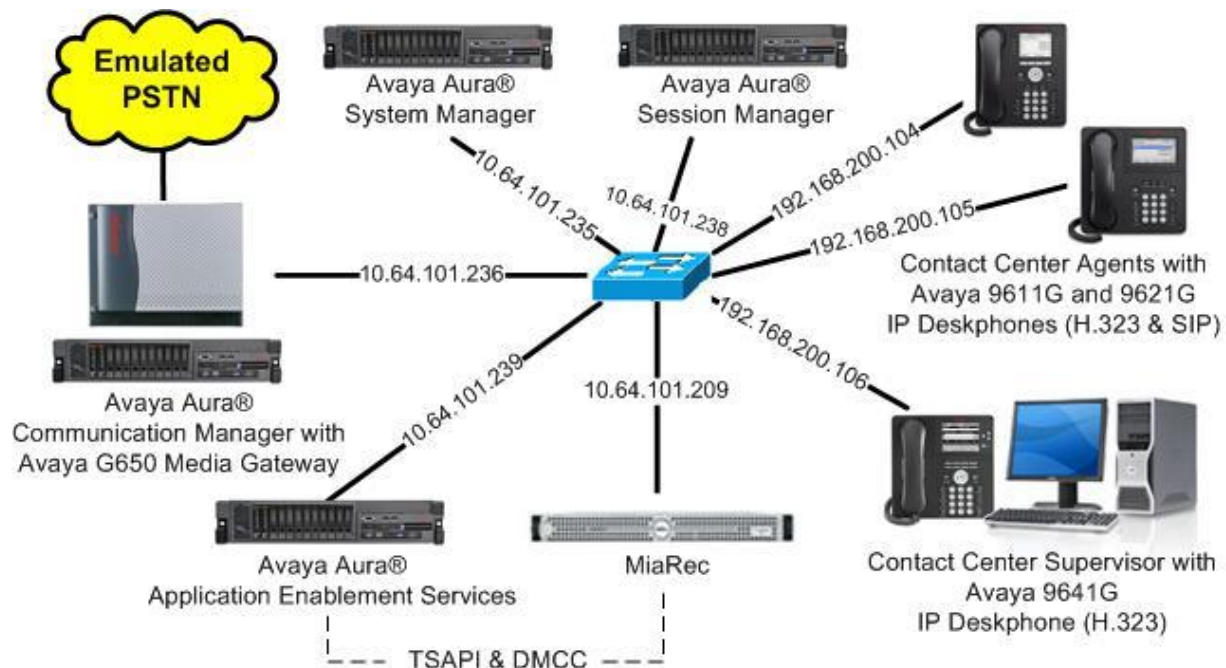


Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager in Virtual Environment	7.1.1 (7.1.1.0.0.532.23985)
Avaya G650 Media Gateway	NA
Avaya Aura® Media Server in Virtual Environment	7.8.0.333
Avaya Aura® Application Enablement Services in Virtual Environment	7.1.1 (7.1.1.0.0.5-0)
Avaya Aura® Session Manager in Virtual Environment	7.1.1 (7.1.1.0.711008)
Avaya Aura® System Manager in Virtual Environment	7.1 .1 (7.1.1.0.046931)
Avaya 9611G & 9641G IP Deskphone (H.323)	6.6506
Avaya 9621G IP Deskphone (SIP)	7.1.0.1.1
MiaRec on Windows Server 2012 R2 <ul style="list-style-type: none">Recorder (MiaRec.exe)Web PortalAvaya TSAPI Windows Client (csta32.dll)Avaya DMCC XML	6.0.1.21 Standard 6.0.0.44 6.0.0.387 7.0.0.138 7.0.0.38

5. Configure Avaya Aura® Communication Manager

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

- Verify license
- Administer CTI link
- Administer IP codec set
- Administer system parameters features
- Administer class of restriction
- Administer agent stations

5.1. Verify License

Log in to the System Access Terminal to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the “display system-parameters customer-options” command to verify that the **Computer Telephony Adjunct Links** customer option is set to “y” on **Page 4**. If this option is not set to “y”, then contact the Avaya sales team or business partner for a proper license file.

display system-parameters customer-options	Page 4 of 12
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? y	DCS Call Coverage? y
ASAI Link Plus Capabilities? y	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

Navigate to **Page 7**, and verify that the **Service Observing (Basic)** customer option is set to “y”. This customer option is needed as part for the registration method used by MiaRec.

display system-parameters customer-options	Page 7 of 12
CALL CENTER OPTIONAL FEATURES	
Call Center Release: 7.0	
ACD? y	Reason Codes? y
BCMS (Basic)? y	Service Level Maximizer? n
BCMS/VuStats Service Level? y	Service Observing (Basic)? y
BSR Local Treatment for IP & ISDN? y	Service Observing (Remote/By FAC)? y
Business Advocate? n	Service Observing (VDNs)? y
Call Work Codes? y	Timed ACW? y
DTMF Feedback Signals For VRU? y	Vectoring (Basic)? y
Dynamic Advocate? n	Vectoring (Prompting)? y

5.2. Administer CTI Link

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

add cti-link 1		Page 1 of 3
CTI LINK		
CTI Link: 1		
Extension: 60111		
Type: ADJ-IP		
COR: 1		
Name: AES CTI Link		

5.3. Administer IP Codec Set

Use the “change ip-codec-set n” command, where “n” is an existing codec set number used for integration with MiaRec.

For customer network that use encrypted media, make certain that “none” is included for **Media Encryption**, and that **Encrypted SRTP** is set to “best-effort”, these settings are needed for support of non-encrypted media from the virtual IP softphones used by MiaRec.

In the compliance testing, this IP codec set was assigned to the agent stations.

change ip-codec-set 1		Page 1 of 2
IP Codec Set		
Codec Set: 1		
Audio	Silence	Frames
Codec	Suppression	Per Pkt
1: G.711MU	n	2
2: G.729		20
3:		
4:		
5:		
6:		
7:		
Media Encryption		Encrypted SRTP: best-effort
1: 1-srtp-aescm128-hmac80		
2: aes		
3: none		
4:		
5:		

5.4. Administer System Parameters Features

Use the “change system-parameters features” command to enable **Create Universal Call ID (UCID)**, which is located on **Page 5**. For **UCID Network Node ID**, enter an available node ID.

```
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
    EC500 Routing in Survivable Mode: dpt-then-ec500
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: 27
```

Navigate to **Page 13**, and enable **Send UCID to ASAI**. This parameter allows for the universal call ID to be sent to MiaRec.

```
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

    Agent/Caller Disconnect Tones? n
    Interruptible Aux Notification Timer (sec): 3
    Zip Tone Burst for Callmaster Endpoints: double

ASAI
    Copy ASAI UI During Conference/Transfer? y
    Call Classification After Answer Supervision? y
                               Send UCID to ASAI? y
    For ASAI Send DTMF Tone to Call Originator? y
    Send Connect Event to ASAI For Announcement Answer? n
    Prefer H.323 Over SIP For Dual-Reg Station 3PCC Make Call? n
```

5.5. Administer Class of Restriction

Enter the “change cor n” command, where “n” is the class of restriction (COR) number used for integration with MiaRec. Set the **Can Be Service Observed** and **Can Be A Service Observer** fields to “y”, as shown below. For the compliance testing, this COR was assigned to the agent stations.

These settings are needed for the registration method used by MiaRec.

change cor 2		Page 1 of 23	
CLASS OF RESTRICTION			
COR Number: 2			
COR Description:			
FRL: 0		APLT? y	
Can Be Service Observed? y		Calling Party Restriction: none	
Can Be A Service Observer? y		Called Party Restriction: none	
Time of Day Chart: 1		Forced Entry of Account Codes? n	
Priority Queuing? n		Direct Agent Calling? n	
Restriction Override: none		Facility Access Trunk Test? n	
Restricted Call List? n		Can Change Coverage? n	

5.6. Administer Agent Stations

Use the “change station n” command, where “n” is the first H.323 agent station extension from **Section 3**. For **COR**, enter the COR number from **Section 5.5**.

Repeat this section to administer all H.323 agent stations from **Section 3**. In the compliance testing, one agent station was administered.

change station 65001		Page 1 of 5	
STATION			
Extension: 65001		Lock Messages? n	BCC: 0
Type: 9611		Security Code: *	TN: 1
Port: S00102		Coverage Path 1: 1	COR: 2
Name: CM7 Station 1		Coverage Path 2:	COS: 1
		Hunt-to Station:	Tests? y

6. Configure Avaya Aura® Application Enablement Services

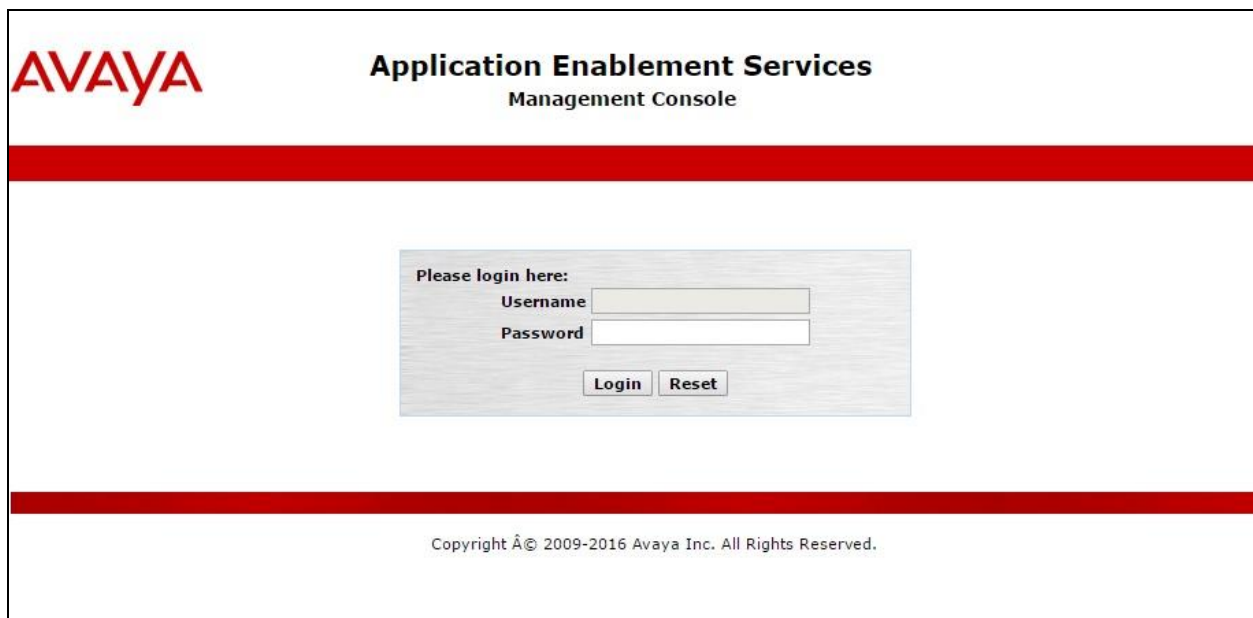
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer H.323 gatekeeper
- Administer security database
- Administer ports
- Restart services
- Administer MiaRec user
- Obtain Tlink name

6.1. Launch OAM Interface

Access the OAM web-based interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of the Application Enablement Services server.

The **Please login here** screen is displayed. Log in using the appropriate credentials.



The screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" is displayed in a large, bold font, with "Management Console" in a smaller font below it. A thick red horizontal bar spans the width of the page. Below this bar is a light gray rectangular box containing the login form. The form has the heading "Please login here:" followed by two input fields: "Username" and "Password". Below these fields are two buttons: "Login" and "Reset". Another thick red horizontal bar is located below the login box. At the bottom of the page, centered, is the copyright notice: "Copyright © 2009-2016 Avaya Inc. All Rights Reserved."

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

The screenshot shows the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title "Application Enablement Services Management Console". On the right, a welcome message for the user is displayed, including login details and system status. The left sidebar contains a navigation menu with options like AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area displays the "Welcome to OAM" message, explaining the purpose of the console and listing the administrative domains it manages: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. It also notes that these domains can be managed by a single administrator or separate administrators.

Welcome: User
Last login: Tue Nov 14 09:35:29 2017 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Tue Nov 14 10:01:03 EST 2017
HA Status: Not Configured

Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
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.
- High Availability - Use High Availability to manage AE Services HA.
- 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 all domains, or a separate administrator for each domain.

6.2. Verify License

Select **Licensing** → **WebLM Server Access** in the left pane, to display the applicable WebLM server log in screen (not shown). Log in using the appropriate credentials, and navigate to display installed licenses (not shown).

The screenshot shows the Avaya Application Enablement Services Management Console with the "Licensing" section selected in the left sidebar. The main content area displays the "Licensing" page, which provides instructions on how to set up and maintain the WebLM, import and set up the license, and administer TSAPI Reserved Licenses or DMCC Reserved Licenses. The left sidebar shows the navigation menu with "Licensing" selected, and sub-options like WebLM Server Address, WebLM Server Access, and Reserved Licenses. The top header and welcome message are the same as in the previous screenshot.

Welcome: User
Last login: Tue Nov 14 09:35:29 2017 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Tue Nov 14 10:01:03 EST 2017
HA Status: Not Configured

Licensing | Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
WebLM Server Address
WebLM Server Access
Reserved Licenses
Maintenance
Networking

Licensing

If you are setting up and maintaining the WebLM, you need to use the following:

- WebLM Server Address

If you are importing, setting up and maintaining the license, you need to use the following:

- WebLM Server Access

If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:

- Reserved Licenses

Select **Licensed products** → **APPL_ENAB** → **Application Enablement** in the left pane, to display the **Application Enablement (CTI)** screen in the right pane.

Verify that there are sufficient licenses for **TSAPI Simultaneous Users** and **Device Media and Call Control**, as shown below. Note that the TSAPI license is used for device monitoring, and the DMCC license is used for the virtual IP softphones.

AVAYA
Aura® System Manager 7.1

Home Licenses

WebLM Home
Install license
Licensed products
APPL_ENAB
▼ Application Enablement
View license capacity
View peak usage
CIE
► CIE
CMM
► Communication_Manager_Messaging
Configure Centralized Licensing
COMMUNICATION_MANAGER
► Call_Center
► Communication_Manager
Configure Centralized Licensing
MESSAGING
► Messaging
MSR
► Media_Server
SYSTEM_MANAGER

Application Enablement (CTI) - Release: 7 - SID: 10503000

You are here: Licensed Products > Application_Enablement > View License Capacity

License installed on: September 13, 2017 1:10:08 PM +00:00

License File Host IDs: V7-2E-92-63-88-4C-01

Licensed Features

10 Items Show All

Feature (License Keyword)	Expiration date	Licensed capacity
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	1000
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	1000
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	3
DLG VALUE_AES_DLG	permanent	16
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	1000
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	3

6.3. Administer TSAPI Link

Select **AE Services** → **TSAPI** → **TSAPI Links** from the left pane of the **Management Console**, to administer a TSAPI link. The **TSAPI Links** screen is displayed, as shown below. Click **Add Link**.

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 the user. The left sidebar shows a navigation tree with "AE Services" expanded, and "TSAPI" selected. Under "TSAPI", "TSAPI Links" is highlighted. The main content area displays the "TSAPI Links" screen, which includes a table with columns: Link, Switch Connection, Switch CTI Link #, ASAI Link Version, and Security. Below the table are buttons for "Add Link", "Edit Link", and "Delete Link".

The **Add TSAPI Links** screen is displayed next.

The **Link** field is only local to the Application Enablement Services server, and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection "cm7" is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields.

The screenshot shows the AVAYA Application Enablement Services Management Console with the "Add TSAPI Links" screen displayed. The left sidebar shows the navigation tree with "AE Services" expanded, "TSAPI" selected, and "TSAPI Links" highlighted. The main content area displays the "Add TSAPI Links" form, which includes fields for Link, Switch Connection, Switch CTI Link Number, ASAI Link Version, and Security. The Link field is set to 1, Switch Connection is set to cm7, Switch CTI Link Number is set to 1, ASAI Link Version is set to 7, and Security is set to Unencrypted. Below the form are buttons for "Apply Changes" and "Cancel Changes".

6.4. Administer H.323 Gatekeeper

Select **Communication Manager Interface** → **Switch Connections** from the left pane. The **Switch Connections** screen shows a listing of the existing switch connections.

Locate the connection name associated with the relevant Communication Manager, in this case “cm7”, and select the corresponding radio button. Click **Edit H.323 Gatekeeper**.

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane has 'Communication Manager Interface' expanded, with 'Switch Connections' selected. The main area displays the 'Switch Connections' table with one entry, 'cm7', which is selected with a radio button. Below the table are buttons for 'Edit Connection', 'Edit PE/CLAN IPs', 'Edit H.323 Gatekeeper', 'Delete Connection', and 'Survivability Hierarchy'. The top right corner shows user login information.

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> cm7	Yes	30	1

The **Edit H.323 Gatekeeper** screen is displayed next. Enter the IP address of a C-LAN circuit pack or the Processor C-LAN on Communication Manager to use as the H.323 gatekeeper, in this case “10.64.101.236” as shown below. Click **Add Name or IP**.

The screenshot shows the 'Edit H.323 Gatekeeper - cm7' screen. The left navigation pane is the same as the previous screenshot. The main area has a text input field containing '10.64.101.236' and an 'Add Name or IP' button. Below the input field are 'Delete IP' and 'Back' buttons. The top right corner shows the same user login information.

6.5. Administer Security Database

Select **Security** → **Security Database** → **Control** from the left pane, to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane.

Check both parameters, as shown below.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title "Application Enablement Services Management Console". A welcome message for the user is shown in the top right corner, including login details and system information. Below the header, a red navigation bar contains the breadcrumb "Security | Security Database | Control" and links for "Home | Help | Logout". The left sidebar lists various management categories, with "Security" expanded to show "Security Database" and "Control" selected. The main content area, titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services", contains two checked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services". An "Apply Changes" button is located below these options.

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Tue Nov 14 09:35:29 2017 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Tue Nov 14 10:08:28 EST 2017
HA Status: Not Configured

Security | Security Database | Control [Home](#) | [Help](#) | [Logout](#)

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
 Account Management
 Audit
 Certificate Management
 Enterprise Directory
 Host AA
 PAM
 Security Database
 Control

SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services

☒ Enable SDB for DMCC Service
☒ Enable SDB for TSAPI Service, JTAPI and Telephony Web Services
[Apply Changes](#)

6.7. Restart Services

Select **Maintenance** → **Service Controller** from the left pane, to display the **Service Controller** screen in the right pane. Check **DMCC Service** and **TSAPI Service**, and click **Restart Service**.

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Nov 14 09:35:29 2017 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Tue Nov 14 10:01:03 EST 2017
HA Status: Not Configured

Maintenance | Service ControllerHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▼ Maintenance

▶ Date Time/NTP Server

▶ Security Database

▶ Service Controller

▶ Server Data

▶ Networking

▶ Security

▶ Status

Service Controller

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input checked="" type="checkbox"/> DMCC Service	Running
<input type="checkbox"/> CVLAN Service	Running
<input type="checkbox"/> DLG Service	Running
<input type="checkbox"/> Transport Layer Service	Running
<input checked="" type="checkbox"/> TSAPI Service	Running

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

StartStopRestart ServiceRestart AE ServerRestart LinuxRestart Web Server

6.8. Administer MiaRec User

Select **User Management** → **User Admin** → **Add User** from the left pane, to display the **Add User** screen in the right pane.

Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password**, and **Confirm Password**. For **CT User**, select “Yes” from the drop-down list. Retain the default value in the remaining fields.

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Nov 14 09:35:29 2017 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Tue Nov 14 10:04:10 EST 2017
HA Status: Not Configured

User Management | User Admin | Add UserHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▼ User Management

▶ Service Admin

▼ User Admin

■ Add User

■ Change User Password

■ List All Users

■ Modify Default Users

■ Search Users

▶ Utilities

▶ Help

Add User

Fields marked with * can not be empty.

* User Idmiarec

* Common Namemiarec

* Surnamemiarec

* User Password*****

* Confirm Password*****

Admin Note

Avaya RoleNone ▼

Business Category

Car License

CM Home

Css Home

CT UserYes ▼

Department Number

Display Name

Employee Number

Employee Type

Enterprise Handle

Given Name

Select **Security** → **Security Database** → **CTI Users** → **List All Users** from the left pane (not shown), to display the **CTI Users** screen in the right pane. Select the new MiaRec user, in this case “miarec”, and click **Edit**.

Application Enablement Services
Management Console

Welcome: User
Last login: Tue Nov 14 09:35:29 2017 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Tue Nov 14 10:05:53 EST 2017
HA Status: Not Configured

Security | Security Database | CTI Users | List All Users
Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
▼ Security
Account Management
Audit

CTI Users

User ID	Common Name	Worktop Name	Device ID
<input type="radio"/> aesp5	aesp5	NONE	NONE
<input type="radio"/> aesp5h	aesp5h	NONE	NONE
<input checked="" type="radio"/> miarec	miarec	NONE	NONE

Edit
List All

The **Edit CTI User** screen is displayed next. Check **Unrestricted Access**, which is required in order for MiaRec to register virtual IP softphones against agent station extensions without use of passwords.

Application Enablement Services
Management Console

Welcome: User
Last login: Tue Nov 14 09:35:29 2017 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Tue Nov 14 10:05:53 EST 2017
HA Status: Not Configured

Security | Security Database | CTI Users | List All Users
Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
▼ Security
Account Management
Audit
Certificate Management
Enterprise Directory
Host AA
PAM
▼ Security Database

Edit CTI User

User Profile:

User ID
Common Name
Worktop Name
Unrestricted Access

miarec
miarec
NONE ▼
☒

Call and Device Control:

Call Origination/Termination and Device Status

None ▼

Call and Device Monitoring:

Device Monitoring
Calls On A Device Monitoring
Call Monitoring

None ▼
None ▼
☐

Routing Control:

Allow Routing on Listed Devices

None ▼

Apply Changes
Cancel Changes

6.9. Obtain Tlink Name

Select **Security** → **Security Database** → **Tlinks** from the left pane. The **Tlinks** screen shows a listing of the Tlink names. A new Tlink name is automatically generated for the TSAPI service. Locate the Tlink name associated with the relevant switch connection, which would use the name of the switch connection as part of the Tlink name. Make a note of the associated Tlink name, to be used later for configuring MiaRec.

In this case, the associated Tlink name is “AVAYA#CM7#CSTA#AES7”. Note the use of the switch connection “CM7” from **Section 6.3** as part of the Tlink name.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the text "Application Enablement Services Management Console". A welcome message in the top right corner reads: "Welcome: User", "Last login: Tue Nov 14 09:35:29 2017 from 192.168.200.20", "Number of prior failed login attempts: 0", "HostName/IP: aes7/10.64.101.239", "Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE", "SW Version: 7.1.1.0.0.5-0", "Server Date and Time: Tue Nov 14 10:01:03 EST 2017", and "HA Status: Not Configured".

The main navigation bar shows "Security | Security Database | Tlinks" and "Home | Help | Logout". The left sidebar contains a tree view with the following items: "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking", "Security" (expanded), "Account Management", "Audit", "Certificate Management", "Enterprise Directory", "Host AA", "PAM", "Security Database" (expanded), "Control", "CTI Users", "Devices", "Device Groups", and "Tlinks" (selected).

The main content area is titled "Tlinks" and displays a single Tlink entry with the name "AVAYA#CM7#CSTA#AES7". A "Delete Tlink" button is visible next to the entry.

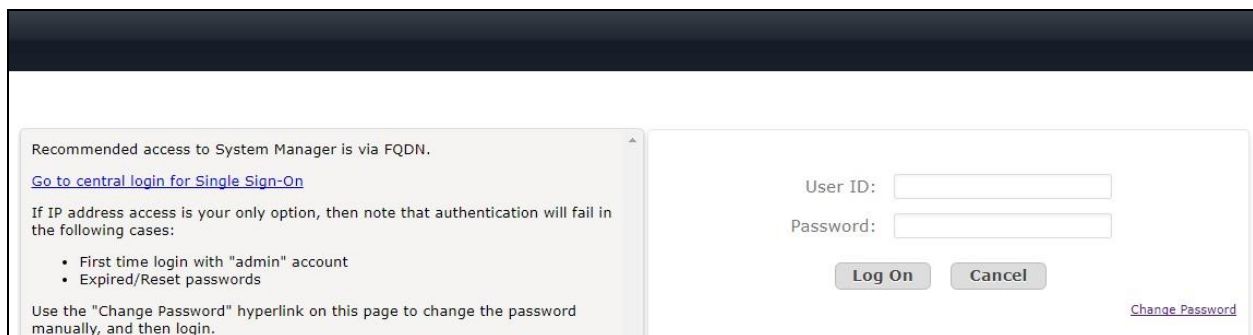
7. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager, which is performed via the web interface of System Manager. The procedures include the following areas:

- Launch System Manager
- Administer users

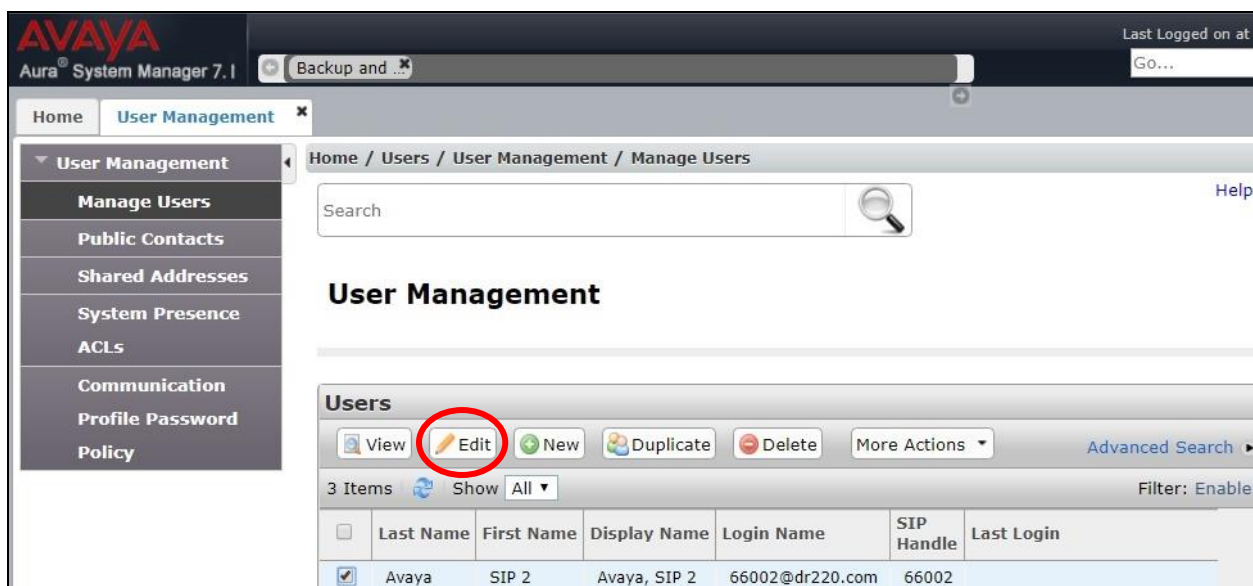
7.1. Launch System Manager

Access the System Manager web interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of System Manager. Log in using the appropriate credentials.



7.2. Administer Users

In the subsequent screen (not shown), select **Users** → **User Management**. Select **User Management** → **Manage Users** from the left pane to display the **User Management** screen below. Select the entry associated with the first SIP agent station from **Section 3**, in this case “66002”, and click **Edit**.



	Last Name	First Name	Display Name	Login Name	SIP Handle	Last Login
<input checked="" type="checkbox"/>	Avaya	SIP 2	Avaya, SIP 2	66002@dr220.com	66002	

The **User Profile Edit** screen is displayed. Select the **Communication Profile** tab to display the screen below.

Navigate to the **CM Endpoint Profile** sub-section, and click **Endpoint Editor**.

AVAYA
Aura® System Manager 7.1

Last Logged on at
Go...

Home / Users / User Management / Manage Users

User Profile Edit: 66002@dr220.com

Commit & Continue

Communication Profile

Communication Profile Password: [Edit](#)

[New](#) [Delete](#) [Done](#) [Cancel](#)

Name

☒ Primary

Select : None

* Name:

Default : ☒

Communication Address

[New](#) [Edit](#) [Delete](#)

Type	Handle	Domain
<input type="checkbox"/> Avaya SIP	66002	dr220.com

Select : All, None

☒ **Session Manager Profile**

☒ **CM Endpoint Profile**

* System:

* Profile Type:

Use Existing Endpoints: ☐

* Extension: [Display Extension Ranges](#) **Endpoint Editor**

Template:

Set Type:

The **Edit Endpoint** screen is displayed next. For **Type of 3PCC Enabled**, select “Avaya” from the drop-down list as shown below. Retain the default values in the remaining fields.

AVAYA
Aura® System Manager 7.1

Last Logged on at
Go...

Home User Management

Home / Users / User Management / Manage Users

Edit Endpoint

System DR220-CM7-ES **Extension** 66002
Template Select **Set Type** 9621SIPCC
Port S00004 **Security Code**
Name Avaya, SIP 2

General Options (G) **Feature Options (F)** **Site Data (S)** **Abbreviated Call Dialing (A)**

Enhanced Call Fwd (E) **Button Assignment (B)** **Profile Settings (P)** **Group Membership**

*** Class of Restriction (COR)** 1 *** Class Of Service (COS)** 1
*** Emergency Location Ext** 66002 *** Message Lamp Ext.** 66002
*** Tenant Number** 1 **Type of 3PCC Enabled** Avaya
*** SIP Trunk** aar **Coverage Path 2**
Coverage Path 1 1 **Localized Display Name** Avaya, SIP 2
Lock Message ☐ **Enable Reachability for Station Domain Control** system
Multibyte Language Not Applicable

***Required**

Select the **Feature Options** tab in the right pane. Check **IP Softphone** as shown below, and retain the default values in the remaining fields.

Repeat this section to administer all SIP agent stations from **Section 3**. In the compliance testing, one agent station was administered.

The screenshot displays the Avaya Aura System Manager 7.1 web interface. The top navigation bar includes the Avaya logo, the text 'Aura System Manager 7.1', a 'Backup and ...' button, and a 'Last Logged' status. The main navigation pane on the left shows a tree structure with 'User Management' expanded, containing sub-items like 'Manage Users', 'Public Contacts', 'Shared Addresses', 'System Presence', 'ACLs', 'Communication', 'Profile Password', and 'Policy'. The breadcrumb trail indicates the path: 'Home / Users / User Management / Manage Users'. The main content area is titled 'Edit Endpoint' and contains a form for configuring an endpoint. The form is divided into several sections: 'General Options (G)' (marked with a red star), 'Feature Options (F)', 'Site Data (S)', and 'Abbreviated Call Dialing (A)'. The 'Feature Options (F)' tab is currently selected. Within this tab, there are sub-sections for 'Enhanced Call Fwd (E)', 'Button Assignment (B)', 'Profile Settings (P)', and 'Group Membership'. The 'Profile Settings (P)' sub-section is active, showing various configuration options. The 'Active Station Ringing' is set to 'single'. The 'MWI Served User Type' is set to 'None'. The 'Per Station CPN - Send Calling Number' is set to 'None'. The 'IP Phone Group ID' is empty. The 'Remote Soft Phone Emergency Calls' is set to 'as-on-local'. The 'LWC Reception' is set to 'spe'. The 'AUDIX Name' is set to 'None'. The 'Short/Prefixed Registration Allowed' is set to 'default'. The 'Voice Mail Number' is empty. The 'Auto Answer' is set to 'none'. The 'Coverage After Forwarding' is set to a dropdown menu. The 'Display Language' is set to 'english'. The 'Hunt-to Station' is empty. The 'Loss Group' is set to '19'. The 'Survivable COR' is set to 'internal'. The 'Time of Day Lock Table' is set to 'None'. The 'Music Source' is empty. The 'Features' section at the bottom contains a list of checkboxes. The 'IP SoftPhone' checkbox is checked and highlighted with a red box. Other checked features include 'Coverage Message Retrieval', 'Survivable Trunk Dest', 'Restrict Last Appearance', 'Direct IP-IP Audio Connections', 'H.320 Conversion', and 'IP Video Softphone'. Other unchecked features include 'Always Use', 'IP Audio Hairpinning', 'Bridged Call Alerting', 'Bridged Idle Line Preference', 'Data Restriction', 'Bridged Appearance Origination Restriction', 'Idle Appearance Preference', 'LWC Activation', 'CDR Privacy', and 'Per Button Ring Control'.

System	Extension
DR220-CM7-ES	66002

Template	Set Type
Select	9621SIPCC

Port	Security Code
S00004	

Name
Avaya, SIP 2

General Options (G) *	Feature Options (F)	Site Data (S)	Abbreviated Call Dialing (A)
Enhanced Call Fwd (E)	Button Assignment (B)	Profile Settings (P)	Group Membership

Active Station Ringing	Auto Answer
single	none

MWI Served User Type	Coverage After Forwarding
None	

Per Station CPN - Send Calling Number	Display Language
None	english

IP Phone Group ID	Hunt-to Station

Remote Soft Phone Emergency Calls	Loss Group
as-on-local	19

LWC Reception	Survivable COR
spe	internal

AUDIX Name	Time of Day Lock Table
None	None

Short/Prefixed Registration Allowed	Music Source
default	

Features	
<input type="checkbox"/> Always Use	<input type="checkbox"/> Idle Appearance Preference
<input type="checkbox"/> IP Audio Hairpinning	<input checked="" type="checkbox"/> IP SoftPhone
<input type="checkbox"/> Bridged Call Alerting	<input checked="" type="checkbox"/> LWC Activation
<input type="checkbox"/> Bridged Idle Line Preference	<input type="checkbox"/> CDR Privacy
<input checked="" type="checkbox"/> Coverage Message Retrieval	<input checked="" type="checkbox"/> Direct IP-IP Audio Connections
<input type="checkbox"/> Data Restriction	<input type="checkbox"/> H.320 Conversion
<input checked="" type="checkbox"/> Survivable Trunk Dest	<input type="checkbox"/> IP Video Softphone
<input type="checkbox"/> Bridged Appearance Origination Restriction	<input type="checkbox"/> Per Button Ring Control
<input checked="" type="checkbox"/> Restrict Last Appearance	

8. Configure MiaRec

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

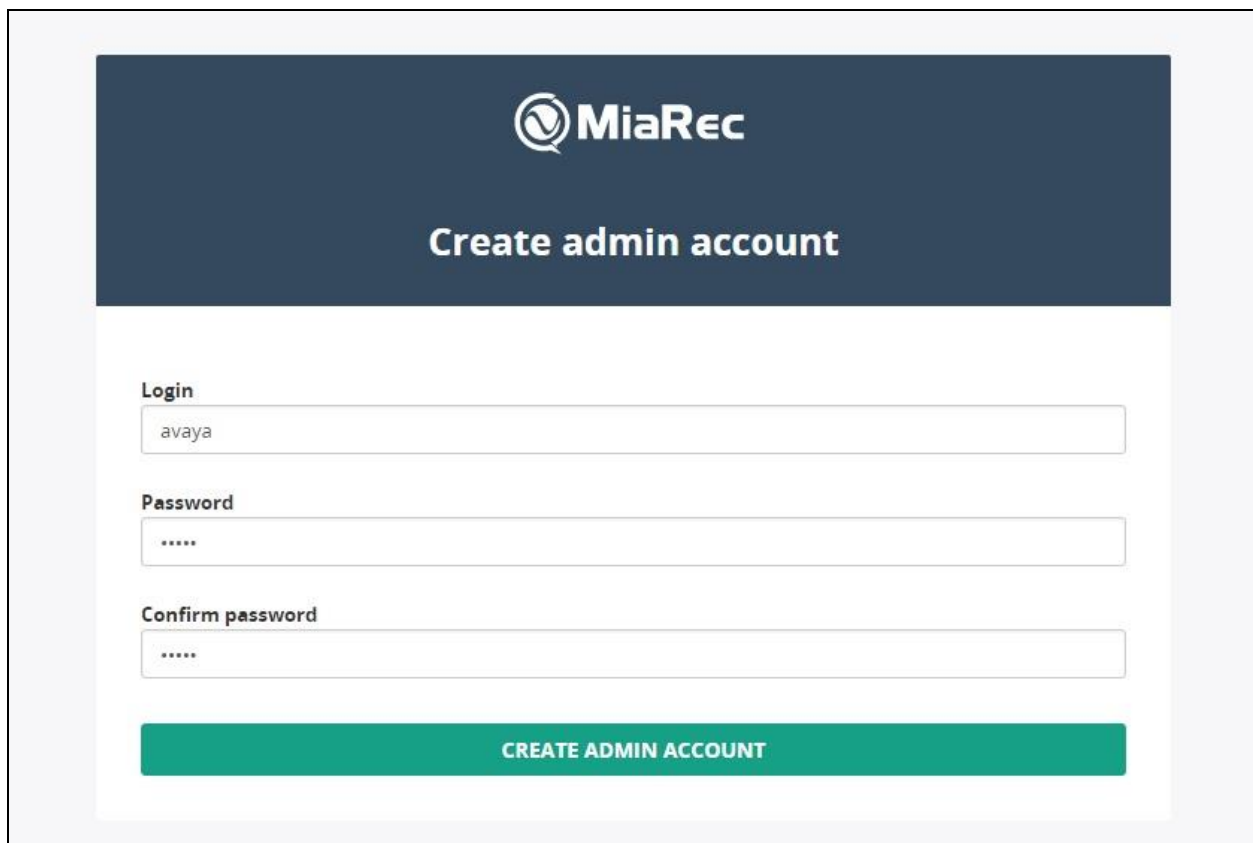
- Launch web interface
- Administer DMCC
- Administer TSAPI

Prior to configuration, the relevant Avaya TSAPI client is assumed to be installed on the MiaRec server, and that the TSAPI client has been configured with the IP address of the Application Enablement Services server as part of installation.

8.1. Launch Web Interface

Access the MiaRec web-based interface by using the URL “http://ip-address” in an Internet browser window, where “ip-address” is the IP address of the MiaRec server.

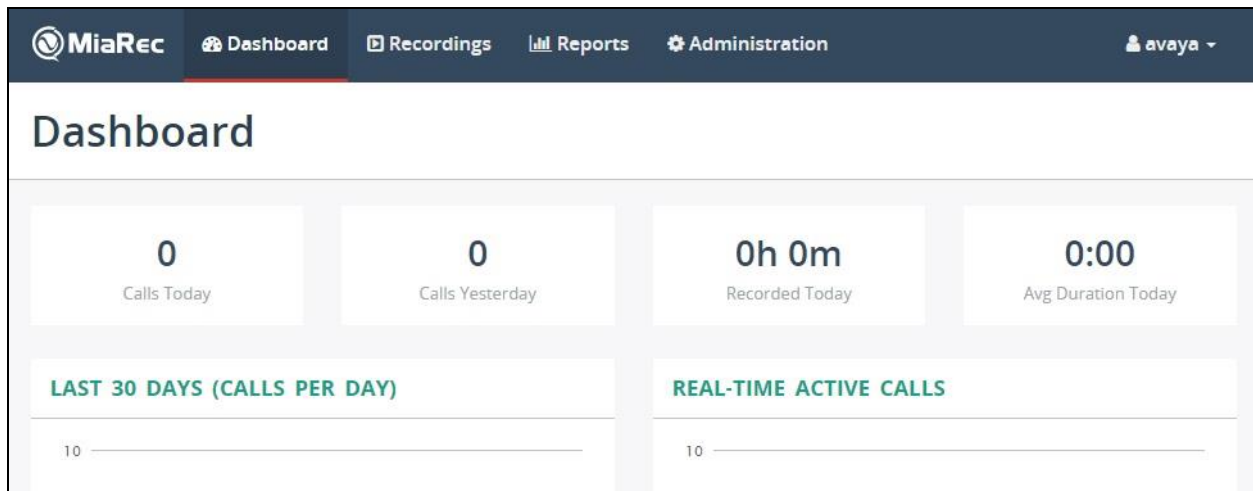
The **Create admin account** screen is displayed upon initial access. Enter desired credentials for the administrative account.



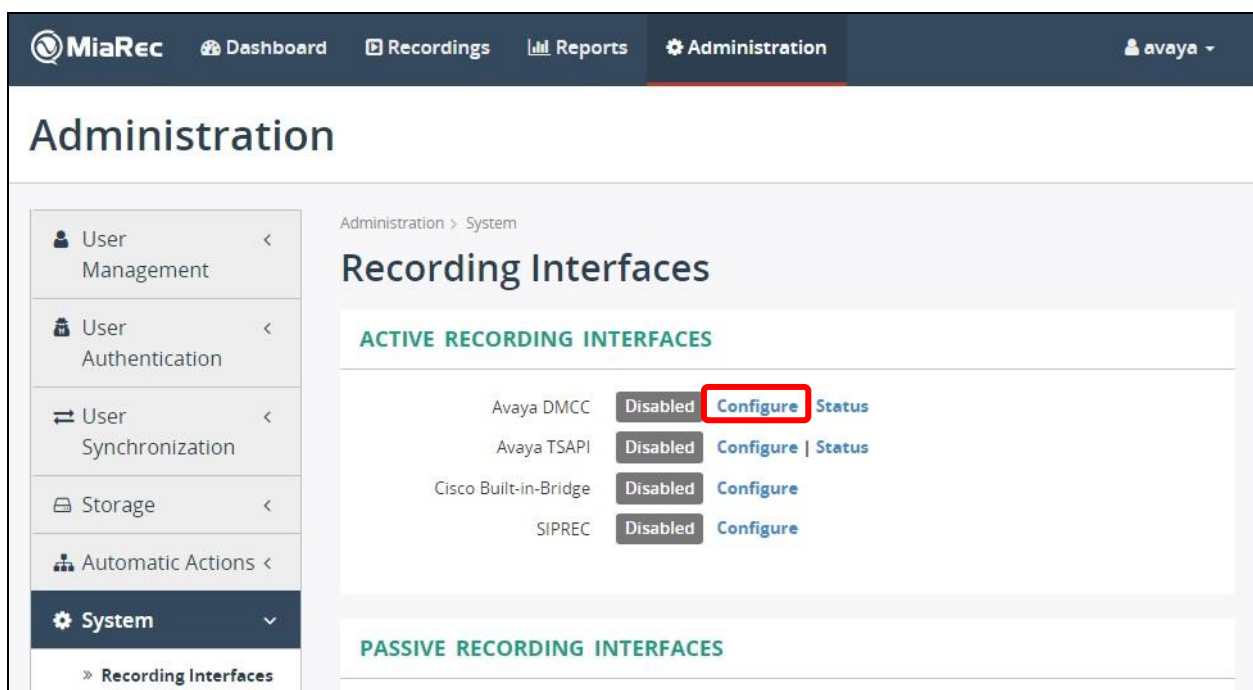
The screenshot displays the MiaRec web interface for creating an admin account. At the top, the MiaRec logo is centered above the title "Create admin account". Below the title, there are three input fields: "Login" with the text "avaya", "Password" with masked characters "*****", and "Confirm password" also with masked characters "*****". A green button labeled "CREATE ADMIN ACCOUNT" is positioned at the bottom of the form.

8.2. Administer DMCC

The **Dashboard** screen is displayed next. Select **Administration** from the top menu.



The **Administration** screen is displayed. Select **System** → **Recording Interfaces** from the left pane, to display **Recording Interfaces** in the right pane. Next to **Avaya DMCC**, select **Configure**, as shown below.



The **Configure Recording Interface** screen below is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Enable:** Check this field.
- **AES server:** IP address of Application Enablement Services followed by the encrypted DMCC port from **Section 6.6**.
- **Use SSL:** Check this field.
- **DMCC login:** The MiaRec user credentials from **Section 6.8**.
- **DMCC password:** The MiaRec user credentials from **Section 6.8**.
- **SwitchName:** The switch connection name from **Section 6.3**.
- **Dependency Mode:** Select **INDEPENDENT (SIP stations)** when SIP stations are used.

The screenshot displays the MiaRec Administration interface. The top navigation bar includes links for Dashboard, Recordings, Reports, and Administration. The left sidebar shows a tree view of system settings, with 'System' expanded to show 'Recording Interfaces'. The main content area is titled 'Configure Recording Interface' and contains the following configuration fields:

- Enable:** A checkbox labeled 'Enable Avaya DMCC recording' which is checked.
- AES server:** A text input field containing '10.64.101.239:4722'. Below the field is a hint: 'Address of AES server. Format: host:port'.
- Use SSL:** A checkbox labeled 'Use SSL' which is checked. Below the field is a hint: 'Use TLS/SSL connection to AES server'.
- DMCC login:** A text input field containing 'miarec'.
- DMCC password:** A password input field with masked characters '.....'.
- SwitchName:** A text input field containing 'cm7'. Below the field is a hint: 'Hostname of Avaya CM server. Either SwitchName or SwitchIPInterface or both should be configured'.
- SwitchIPInterface:** A text input field containing '0.0.0.0'. Below the field is a hint: 'IP address of Avaya CM server. Either SwitchName or SwitchIPInterface or both should be configured. Recommended value: 0.0.0.0 (the ip-address will be resolved automatically from SwitchName)'.
- Dependency Mode:** Two radio button options: 'DEPENDENT (H.323 stations)' (unselected) and 'INDEPENDENT (SIP stations)' (selected). Below these is a hint: 'Dependency Mode for Multiple Registration'.

8.3. Administer TSAPI

The **Administration** screen is displayed again, showing **Enabled** status for **Avaya DMCC**.

Next to **Avaya TSAPI**, select **Configure**, as shown below.

The screenshot shows the MiaRec Administration interface. The top navigation bar includes links for Dashboard, Recordings, Reports, and Administration (which is currently selected). The user profile 'avaya' is visible in the top right. The main heading is 'Administration'. On the left, a sidebar menu lists various system management options, with 'System' expanded to show 'Recording Interfaces'. The main content area is titled 'Recording Interfaces' and shows a table of active recording interfaces. The table lists four interfaces: Avaya DMCC (Enabled), Avaya TSAPI (Disabled), Cisco Built-in-Bridge (Disabled), and SIPREC (Disabled). The 'Configure' button for Avaya TSAPI is highlighted with a red box. Below the active interfaces, there is a section for 'PASSIVE RECORDING INTERFACES'.

ACTIVE RECORDING INTERFACES		
Avaya DMCC	Enabled	Configure Status
Avaya TSAPI	Disabled	Configure Status
Cisco Built-in-Bridge	Disabled	Configure
SIPREC	Disabled	Configure

PASSIVE RECORDING INTERFACES

The **Configure Recording Interface** screen below is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Enable:** Check this field.
- **TSAPI Link:** The Tlink name from **Section 6.9**.
- **TSAPI login:** The MiaRec user credentials from **Section 6.8**.
- **TSAPI password:** The MiaRec user credentials from **Section 6.8**.
- **Monitored phones:** The agent station extensions from **Section 3**.
- **Monitored ACD Splits:** The skill group extensions from **Section 3**.

The screenshot displays the MiaRec Administration interface. The top navigation bar includes links for Dashboard, Recordings, Reports, and Administration. The left sidebar shows the 'System' menu expanded, with 'Recording Interfaces' selected. The main content area is titled 'Configure Recording Interface' and contains the following fields:

- Enable:** A checkbox labeled 'Enable Avaya TSAPI recording' which is checked.
- TSAPI Link:** A text input field containing 'AVAYA#CM7#CSTA#AES7'. Below the field is a hint: 'TSAPI link, like AVAYA#SWITCH1#CSTA#SERVERNAME1'.
- TSAPI login:** A text input field containing 'miarec'. Below the field is a hint: 'TSAPI account name'.
- TSAPI password:** A password input field showing masked characters '*****'. Below the field is a hint: 'TSAPI account password'.
- Media Source:** Two radio button options: 'Passive - port mirroring' (unselected) and 'DMCC' (selected).
- Monitored phones:** A text input field containing '65001,66002'. Below the field is a hint: 'A range of monitored phones (comma-separated). Example: 3000-3100,5001,5002'.
- Monitored ACD Splits:** A text input field containing '61001-61002'.

Scroll down the screen as necessary. For **Ignore dialing phase**, configure as desired. In the compliance testing, this field was checked to only enable recording for answered calls.

For the **No-Audio Normal Timeout**, configure this parameter as desired. In the compliance testing, the parameter was configured for waiting 240 seconds, before force complete on recording for calls that were disrupted as part of serviceability scenarios.

Integration	
<input checked="" type="checkbox"/> Customization <	
<input type="checkbox"/> Screen Recording <	
<input type="checkbox"/> Maintenance <	

Monitored ACD Splits

A range of monitored ACD Splits (comma-separated). Monitoring of ACD Splits is necessary for correct processing of Agent Login/Logout events. Example: 49000-49100,55000,56000

Ignore dialing phase ☒ Ignore audio during dialing phase

If set to 'yes', then recording will begin from the moment when call is actually answered and dial-tone will not be recorded into audio file.

No-Audio Begin Timeout seconds

This timeout specifies how long to wait for the first RTP media packet before give up

No-Audio Normal Timeout seconds

In case of RTP transmission stopping, this timeout specifies how long to wait for RTP restoration before forcibly completing call recording

No-Audio Hold Timeout seconds

In case of RTP transmission stopping due to call hold, this timeout specifies how long to wait for call resume before forcibly completing call recording

9. Verification Steps

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

9.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify status of the administered CTI link by using the “status aesvcs cti-link” command. Verify that the **Service State** is “established” for the CTI link number administered in **Section 5.2**, as shown below.

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	7	no	aes7	established	72	63

Verify registration status of the virtual IP softphones by using the “list registered-ip-stations” command. Verify that all monitored phones from **Section 8.3** are displayed along with the IP address of the Application Enablement Services server, as shown below.

```
list registered-ip-stations
```

REGISTERED IP STATIONS					
Station Ext or Orig Port	Set Type/ Net Rgn	Prod ID/ Release	Station IP Address/ Gatekeeper IP Address	Skt	IP Address
65000	9641	IP_Phone	192.168.200.106	tls	
	1	6.6506	10.64.101.236		
65001	9611	IP_Phone	192.168.200.104	tls	
	1	6.6506	10.64.101.236		
65001	9611	IP_API_A	10.64.101.239	tcp	
	1	3.2040	10.64.101.236		
66002	9621SIPCC	IP_API_A	10.64.101.239	tcp	
	1	3.2040	10.64.101.236		

9.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify status of the TSAPI link by selecting **Status** → **Status and Control** → **TSAPI Service Summary** from the left pane. The **TSAPI Link Details** screen is displayed.

Verify the **Status** is “Talking” for the TSAPI link administered in **Section 6.3**, and that the **Associations** column reflects the total number of monitored skill groups and agent stations from **Section 3**, in this case “4”, as shown below.

AVAYA Application Enablement Services
Management Console

Welcome: User
Last login: Mon Nov 27 12:41:40 2017 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Mon Nov 27 14:26:53 EST 2017
HA Status: Not Configured

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

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

▶ Log Manager

▶ Logs

▼ Status and Control

■ CVLAN Service Summary

■ DLG Services Summary

■ DMCC Service Summary

■ Switch Conn Summary

■ TSAPI Service Summary

TSAPI Link Details


☐ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input checked="" type="radio"/>	1	cm7	1	Talking	Wed Nov 15 12:40:09 2017	Online	17	4	63	72	30

For service-wide information, choose one of the following:

Verify status of the DMCC link by selecting **Status → Status and Control → DMCC Service Summary** from the left pane. The **DMCC Service Summary – Session Summary** screen is displayed.

Verify the **User** column shows an active session with the MiaRec user name from **Section 6.8**, and that the **# of Associated Devices** column reflects the number of monitored phones from **Section 8.3**, in this case “2”, as shown below.



Application Enablement Services
 Management Console

Welcome: User
 Last login: Mon Nov 27 12:41:40 2017 from 192.168.200.20
 Number of prior failed login attempts: 0
 HostName/IP: aes7/10.64.101.239
 Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
 SW Version: 7.1.1.0.0.5-0
 Server Date and Time: Mon Nov 27 14:25:53 EST 2017
 HA Status: Not Configured

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

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▼ Status
 - Alarm Viewer
 - ▶ Log Manager
 - ▶ Logs
 - ▼ Status and Control
 - CVLAN Service Summary
 - DLG Services Summary
 - DMCC Service Summary
 - Switch Conn Summary
 - TSAPI Service Summary

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every seconds

Session Summary [Device Summary](#)
 Generated on Mon Nov 27 14:25:28 EST 2017

Service Uptime: 12 days, 1 hours 44 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 31

Number of Existing Devices: 2

Number of Devices Created Since Service Boot: 62

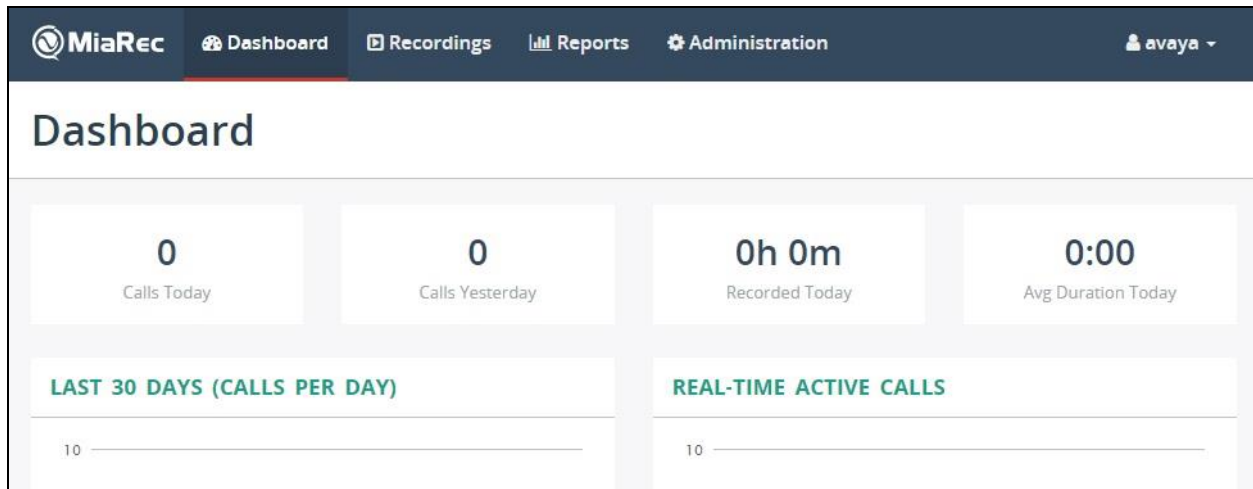
■	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	2D808591C7BA2C9CA F3E3E9B7AAD7E26-30	miarec	MiaRec	10.64.101.209	XML Encrypted	2

Item 1-1 of 1
 Go

9.3. Verify MiaRec

Log an agent into the skill groups to handle and complete an ACD call. Follow the procedures in **Section 8.1** to launch the MiaRec web interface, and log in with pertinent credentials.

The **Dashboard** screen is displayed. Select **Recordings** from the top menu.



The **Recordings** screen is displayed next. Verify that there is an entry reflecting the last call, with proper values in the relevant fields, as shown below.

The screenshot shows the MiaRec Recordings interface. It has the same top navigation bar as the dashboard. Below the navigation bar is a 'Recordings' header. A filter bar contains tabs: ALL CALLS, ACTIVE CALLS, MY CALLS, BY USER, NOT ASSIGNED TO USER, BY CATEGORY, and ADVANCED SEARCH. Below the tabs are search filters: 'Select a Date Range', 'Select a User or Group', and 'Search a Text'. Action buttons include 'No auto-refresh', 'Categories', 'Download', 'Delete', and 'More'. A pagination indicator shows '0-20 of 1'. Below these is a table with the following data:

	USER	DATE	TIME	DURATION	FROM	TO	CATEGORIES
<input type="checkbox"/>		Today	11:28 AM	1:26	9089532103	65001 (CM Station 1)	

Click on the entry to see additional information, and select **More details**, as shown below.

The screenshot displays the MiaRec web application interface. At the top, a dark blue navigation bar contains the MiaRec logo and links to Dashboard, Recordings (which is highlighted), Reports, and Administration. A user profile for 'avaya' is visible in the top right corner. Below the navigation bar, the 'Recordings' section is titled. A filter bar includes tabs for 'ALL CALLS', 'ACTIVE CALLS', 'MY CALLS', 'BY USER', 'NOT ASSIGNED TO USER', 'BY CATEGORY', and 'ADVANCED SEARCH'. Below these tabs are input fields for 'Select a Date Range', 'Select a User or Group', and 'Search a Text', along with a 'Search' button. A secondary bar contains controls for 'No auto-refresh', 'Categories', 'Download', 'Delete', and 'More', along with a pagination indicator '0-20 of 1'. The main content area features a table with columns: USER, DATE, TIME, DURATION, FROM, TO, and CATEGORIES. A single call entry is shown with the following details: From: 9089532103 (assign to user), To: 65001 CM Station 1 (assign to user), Date/Time: Today 11:28:21 AM, Duration: 1:26. Below the table, a detailed view of the call is shown, including a play button, a progress bar, and a 'Save audio file' button. A red box highlights the 'More details' button, which is next to an 'Evaluate' button. At the bottom, there is a 'Notes' section with an 'Add note' link.

USER	DATE	TIME	DURATION	FROM	TO	CATEGORIES
	Today	11:28 AM	1:26	9089532103	65001 (CM Station 1)	

From: 9089532103 (assign to user)
To: 65001 CM Station 1 (assign to user)
Date/Time: Today 11:28:21 AM
Duration: 1:26

00:00 00:00 Save audio file

More details Evaluate

Notes: Add note

The screen below is displayed next. Verify proper values in the relevant fields. Select **Play**, and verify that the call recording can be played back.

MiaRec Dashboard Recordings Reports Administration avaya

Call 9089532103 -> 65001

Mark as confidential Delete Call

MEDIA PLAYER

Switch to basic player

0 10 20 30 40 50 60 1:10 1:20

► Play Save audio file

INFO

Date: **Today**

Connect Time: **11:28:21 AM**

Disconnect Time: **11:29:47 AM**

Duration: **1:26**

Watermark: [View](#)

FROM

User: **Unknown User** (assign)

Phone Number: **9089532103**

Phone Name:

Phone Id:

Ip-address: **0.0.0.0 (0)**

Live monitor phone 9089532103

TO

User: **Unknown User** (assign)

Phone Number: **65001**

Orig Dialed Digits: **3035360001**

Phone Name: **CM Station 1**

Phone Id:

Ip-address: **0.0.0.0 (0)**

Live monitor phone 65001

AVAYA PBX INFO

Agent ID: **65881**

Agent Name: **CM Agent 1**

10. Conclusion

These Application Notes describe the configuration steps required for MiaRec to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

11. Additional References

This section references the product documentation relevant to these Application Notes.

1. *Administering Avaya Aura® Communication Manager*, Release 7.1.1, Issue 2, August 2017, available at <http://support.avaya.com>.
2. *Administering and Maintaining Aura® Application Enablement Services*, Release 7.1.1, Issue 3, September 2017, available at <http://support.avaya.com>.
3. *MiaRec Administration Guide*, available at <http://www.miarec.com/doc/administration-guide>.

©2018 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.