

MiaRec

Avaya Aura-Integration-Guide

MiaRec, Inc.

Copyright © 2024 MiaRec, Inc.

Table of contents

1. Avaya Aura Recording Integration Guide	3
2. Avaya TSAPI DMCC Recording	4
2.1 1. Introduction	4
2.2 2. Configure Avaya Communication Manager	5
2.3 3. Configure Avaya Application Enablement Services	8
2.4 4. Configure MiaRec Call Recording System	19
2.5 5. Verification and Troubleshooting	24
2.6 6. Additional references	34
3. Avaya TSAPI Passive Recording	35
3.1 1. Introduction	35
3.2 2. Network Configuration	36
3.3 3. Configure Avaya Communication Manager	38
3.4 4. Configure Avaya Application Enablement Services	42
3.5 5. Configure MiaRec Call Recording System	49
3.6 6. Verification	53
3.7 7. Additional references	60

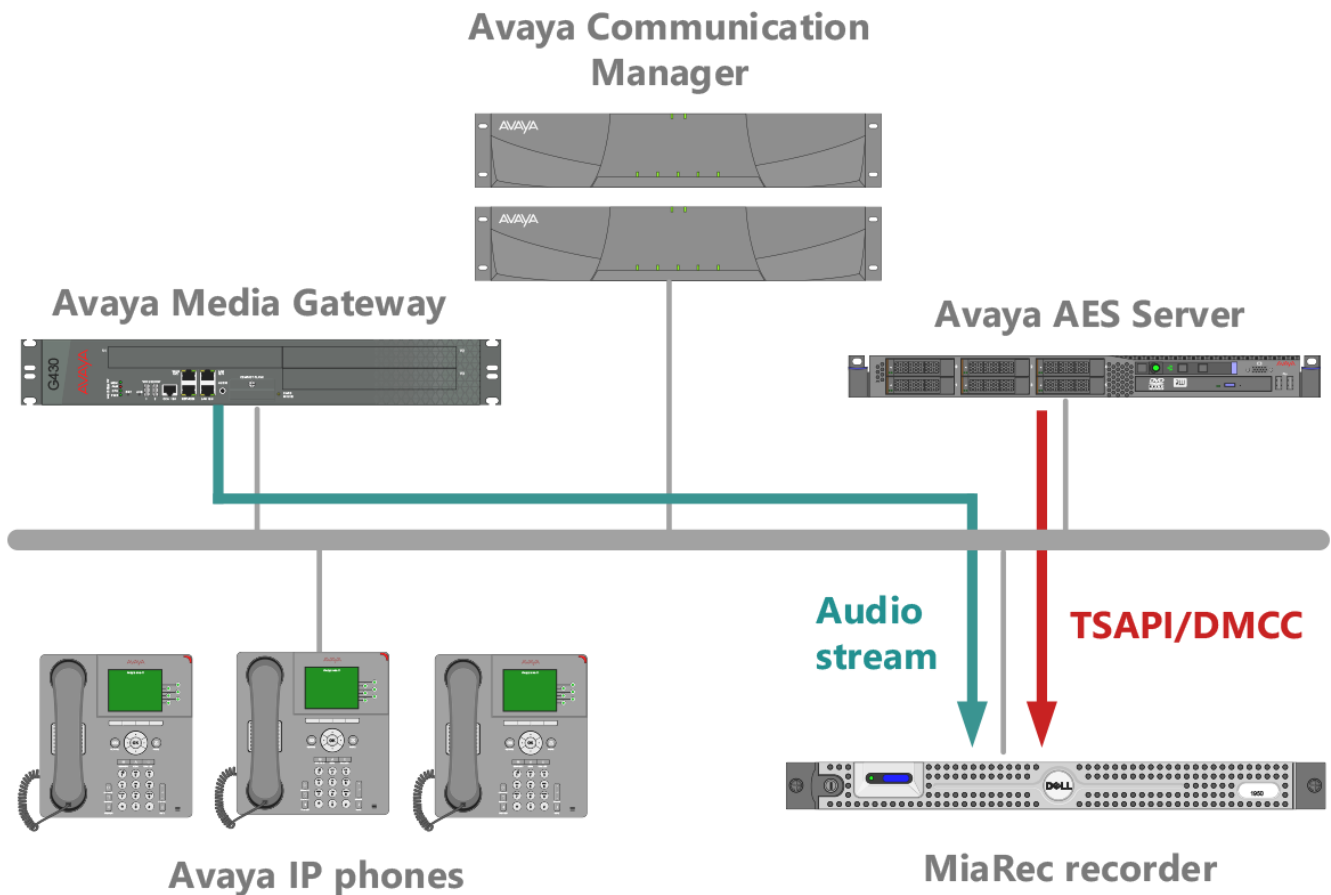
1. Avaya Aura Recording Integration Guide

This guide describes how to configure the MiaRec Call Recording System with the Avaya Application Enablement Services and Avaya Communication Manager to record incoming and outgoing phone calls using TSAPI and DMCC services.

2. Avaya TSAPI DMCC Recording

2.1 1. Introduction

MiaRec uses TSAPI interface from Avaya Aura Application Enablement Services (AES) to monitor skill groups and agent stations on Avaya Aura Communication Manager, and Device, Media, and Call Control (DMCC) interfaces to capture media associated with the monitored agents for call recording with the Multiple Registration method.



Requirements:

- Avaya Communication Manager v6.3.2 or higher.
- Avaya Application Enablement Services (AES) Server v6.3.1 or higher.
- TSAPI Basic License per each recorded extension and each monitored ACD Split / Hunt Groupz.
- DMCC Basic License for each recorded extension.

2.2 2. Configure Avaya Communication Manager

2.2.1 Overview

This section presents configuration steps for the Avaya Communication Manager. It is assumed that an appropriate license file and authentication file have been installed on the server, and that login and password credentials are available.

The configuration and verification operations illustrated in this section were all performed using the Communication Manager System Administration Terminal (SAT).

The procedures include the following areas:

- Verify license
- Verify the status CTI link for TSAPI service
- Administer system parameters features
- Administer agent stations

2.2.2 2.1 Verify license

Log into the System Access Terminal (SAT) to verify that the Communication Manager license has proper permissions for the features required for call recording. 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 Avaya sales team of 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)? y          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
ATMS? y      DS1 Echo Cancellation? y
Attendant Vectoring? y
```

2.2.3 2.2 Verify the status of CTI link for TSAPI service

Log into the System Access Terminal (SAT) to enter the "**status aesvcs cti-link**" command. The link status should show **no** for maintenance busy (**Mnt Busy**), the **Service State** should indicate **established** and **Version** should be **6** or higher.

```
status aesvcs cti-link

AE SERVICES CTI LINK STATUS

CTI  Version  Mnt  AE Services  Service  Msgs  Msgs
Link  Link      Busy Server      State   Sent  Rcvd
1     7        no  aes          established  15    15
```

If the CTI link is not established, then follow the instructions in the **Administering Communication Manager for AE Services** chapter in the **Application Enablement Services Administration and Maintenance Guide** document available at <http://support.avaya.com>.

2.2.4 2.3 Administer agent stations

Use the "**change station xxxxx**" command, where xxxxx is the phone's extension, and change **IP SoftPhone** to "**y**", to allow a virtual IP softphone (DMCC) to be registered against the station. The MiaRec application will use the Multiple Registration feature of Communication Manager to register the DMCC-based recording device against the station.

```
change station 3001                                     Page 1 of 5

                                STATION

Extension: 3001          Lock Messages? n          BCC: 0
Type: 9608              Security Code: *          TN: 1
Port: S00003           Coverage Path 1:          COR: 1
Name: User Two         Coverage Path 2:          COS: 1
                        Hunt-to Station:          Tests? y

STATION OPTIONS

                                Time of Day Lock Table:
Loss Group: 19          Personalized Ringing Pattern: 1
                        Message Lamp Ext: 3001
Speakerphone: 2-way    Mute Button Enabled? y
Display Language: english      Button Modules: 0
Survivable GK Node Name:
Survivable COR: internal      Media Complex Ext:
Survivable Trunk Dest? y      IP SoftPhone? y

                                IP Video Softphone? n
                                Short/Prefixed Registration Allowed: default

                                Customizable Labels? y
```

2.2.5 2.4 Administer System Parameters Features

Enter the "**change system-parameters features**" command. Navigate to **Page 5**, and verify that **Create Universal Call ID (UCID)** has value "**y**". If not, then set it to "**y**" and set **UCID Network Node ID** to an unassigned node ID.

```
change system-parameters features                       Page 5 of 17

                                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:

SEND ALL CALLS OPTIONS
Send All Calls Applies to: station    Auto Inspect on Send All Calls? n

UNIVERSAL CALL ID
Create Universal Call ID (UCID)? y    UCID Network Node ID: 9999
Copy UCID for Station Conference/Transfer? n
```

Navigate to **Page 13**, and set **Send UCID to ASAI** to "**y**". This parameter allows for the universal call ID to be sent to MiaRec call recording application.

```
change system-parameters features                       Page 13 of 17

                                FEATURE-RELATED SYSTEM PARAMETERS

CALL CENTER MISCELLANEOUS
                                Clear Callr-info: next-call
Allow Ringer-off with Auto-Answer? n

Reporting for PC Non-Predictive Calls? n

ASAI
Copy ASAI UUI During Conference/Transfer? n
Call Classification After Answer Supervision? n
Send UCID to ASAI? y
```

2.2.6 2.5 Configure Service Observe

For the purposes of Multi Registration, a service observer must be enabled for the COR to which the Target Stations will be assigned. Using the command "**change cor 1**" set both **Can be Service Observed?** and **Can be a Service Observer?** to "**y**".

```
change cor 1                                     Page 1 of 23
CLASS OF RESTRICTION
COR Number: 1
COR Description:
FRL: 0                                           APLT? y
Can Be Service Observed? y                     Calling Party Restriction: outward
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
Access to MCT? y                               Fully Restricted Service? n
Group II Category For MFC: 7                   Hear VDN of Origin Annc.? n
Send ANI for MFE? n                           Add/Remove Agent Skills? n
MF ANI Prefix:                               Automatic Charge Display? n
Hear System Music on Hold? y PASTE (Display PBX Data on Phone)? n
Can Be Picked Up By Directed Call Pickup? n
Can Use Directed Call Pickup? n
Group Controlled Restriction: inactive
```

2.3 3. Configure Avaya Application Enablement Services

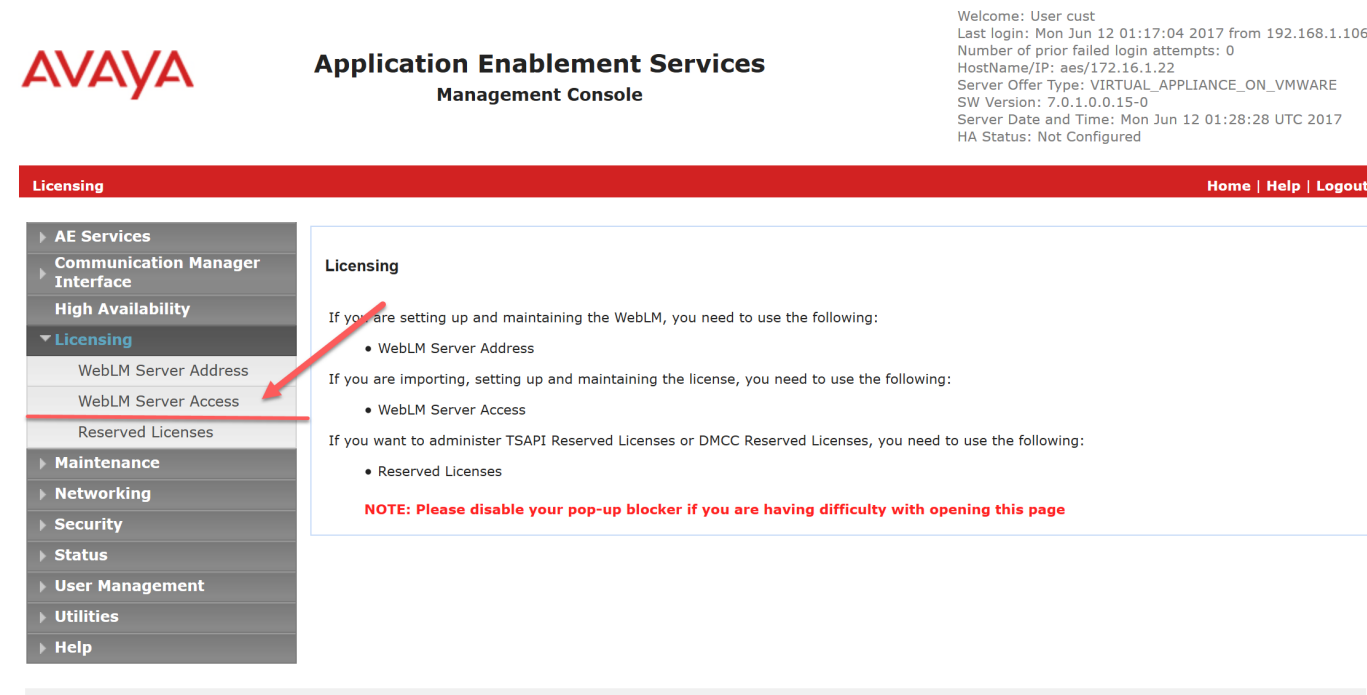
This section provides the procedures for configuring Avaya Application Enablement Services. The procedures include the following areas:

- Verify TSAPI and DMCC services licensing
- Administer TSAPI link
- Obtain Tlink name
- Administer CTI user for MiaRec

2.3.1 3.1. Verify TSAPI and DMCC services licensing

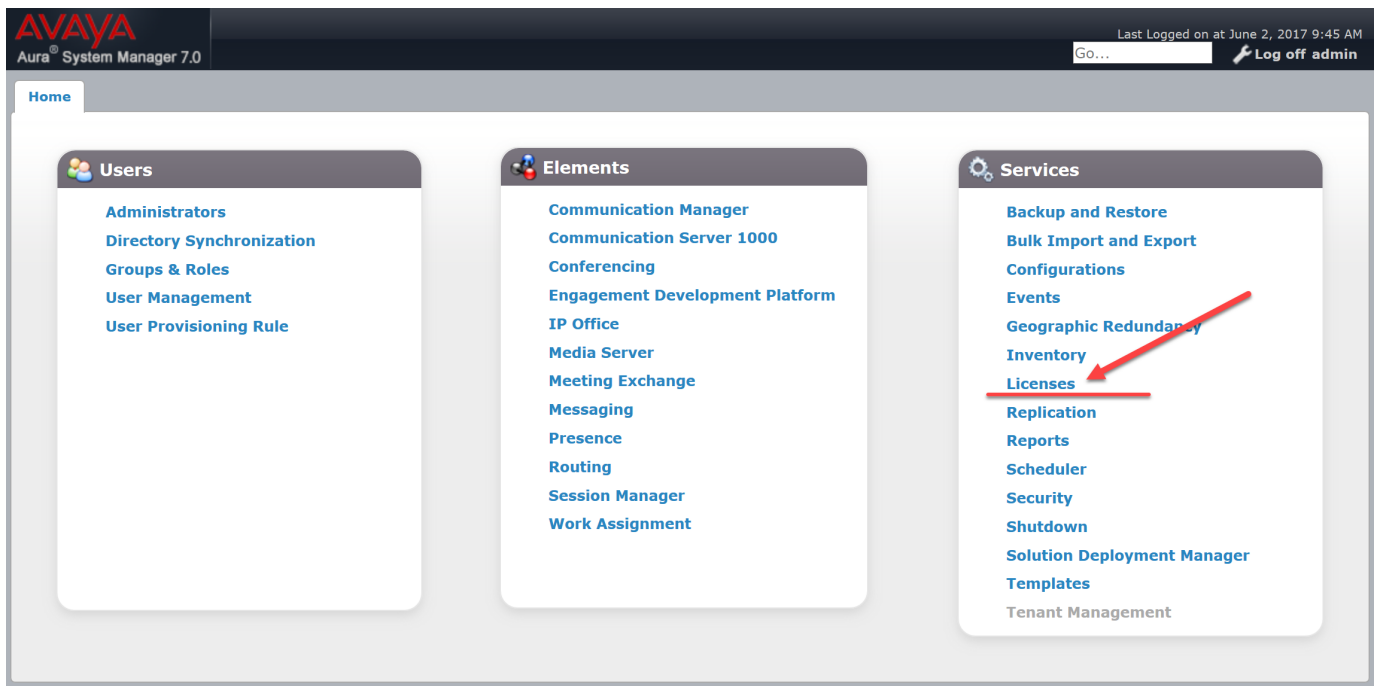
Prior to any administration, verify that the TSAPI and DMCC services have been licensed properly. Open the AES OAM web interface by browsing to "https://ip-address-or-dns", where "ip-address-or-dns" is the IP address or DNS alias of the Application Enablement Services server, and log in using the appropriate credentials (not shown).

Select **Licensing -> WebLM Server Access** in the left pane, to display the **Web License Manager** pop-up screen (not shown), and log in using the appropriate credentials.



Copyright Â© 2009-2016 Avaya Inc. All Rights Reserved.

If the licenses are managed centrally on the System Manager, then select **Services -> Licenses** in the System Manager home screen. Otherwise, the **Web License Manager** screen is shown immediately.



In the **Web License Manager** screen, select **Application_Enablement** under **Licenses Products** to display license capacity and current usage.

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 media recording.

MiaRec requires TSAPI Basic license for each monitored IP Phone, softphone and ACD Split (Hunt Group) and DMCC Basic license for each recorded IP phone and softphone.

If the TSAPI or DMCC service is not licensed, contact the Avaya sales team or business partner for a proper license file.

WebLM Home
Install license
Licensed products
APPL_ENAB
▶ Application_Enablement
CE
▶ COLLABORATION_ENVIRONMENT
CMM
▶ Communication_Manager_Messaging
Configure Centralized Licensing
COMMUNICATION_MANAGER
▶ Communication_Manager
▶ Call_Center
Configure Centralized Licensing
MSR
▶ Media_Server
PRESENCE_SERVICES
▶ Presence_Services
SessionManager
▶ SessionManager
Uninstall license
Server properties

Shortcuts
Help for Installed Product

Application Enablement (CTI) - Release: 7 - SID: 10503000 (Enterprise license file)

You are here: Licensed Products > Application_Enablement > View by Feature

License installed on: June 2, 2017 9:47:35 AM -07:00

License File Host IDs: V6-2A-4F-7A-D9-0C

Feature (License Keyword)	License Capacity	Currently available
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	16	16
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	1000	1000
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	3	3
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	16	16
Product Notes (VALUE_NOTES)	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiSmallServer MediumServerTypes: ibmx306;ibmx306m; dell1950;xen;hs20;hs20_8832_vm;CtiMediumServer LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;unknown;CtiLargeServer TrustedApplications: IPS_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XM_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; PC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; OSPC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; VP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AES_UNIFIED_CC_DESKTOP,; CCE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T1_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T2_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; AVAYAVERTINT_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CCT_ELITE_CALL_CTRL_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents; ANAV_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents; UNIFIED_DESKTOP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents; AACC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents; CE_AGENT_STATES_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents; TP_CLIENT_001, BasicUnrestricted, , , AgentEvents; EXT_CLIENT_001, , , AgentEvents; EXT_CLIENT_002, , , AgentEvents; EXT_CLIENT_003, , , AgentEvents; EXT_CLIENT_004, , , AgentEvents; EXT_CLIENT_005, , , AgentEvents; AAWFO_SELECT_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted;	Not counted
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	3	3
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	1000	994
DLG (VALUE_AES_DLG)	16	16
Device Media and Call Control (VALUE_AES_DMCC_DMC)	1000	998
AES ADVANCED MEDIUM SWITCH (VALUE_AES_AEC_MEDIUM_ADVANCED)	3	3

2.3.2 3.2. Administer TSAPI link

To administer a TSAPI link, select **AE Services -> TSAPI -> TSAPI Links** from the left pan of the **Management Console**. The **TSAPI Links** screen is displayed, as shown below. If the TSAPI Link is not configured yet, then click **Add Link** to create one.



Application Enablement Services Management Console

Welcome: User cust
Last login: Mon Jun 12 01:17:04 2017 from 192.168.1.106
Number of prior failed login attempts: 0
HostName/IP: aes/172.16.1.22
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.0.15-0
Server Date and Time: Mon Jun 12 01:32:42 UTC 2017
HA Status: Not Configured

AE Services | TSAPI | TSAPI Links

Home | Help | Logout

- ▼ AE Services
 - ▶ CVLAN
 - ▶ DLG
 - ▶ DMCC
 - ▶ SMS
 - ▼ TSAPI
 - TSAPI Links
 - TSAPI Properties
 - ▶ TWS

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
<input checked="" type="radio"/> 1	cm2	1	7	Unencrypted

[Add Link](#) [Edit Link](#) [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 "cm2" is selected. For **Switch CTI Link Number**, select the CTI Link number from **Section 2.2**. Make sure that **ASAI Link Version** is 6 or higher. Retain the default values in the remaining fields.



Application Enablement Services Management Console

Welcome: User cust
Last login: Mon Jun 12 01:17:04 2017 from 192.168.1.106
Number of prior failed login attempts: 0
HostName/IP: aes/172.16.1.22
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.0.15-0
Server Date and Time: Mon Jun 12 01:34:52 UTC 2017
HA Status: Not Configured

AE Services | TSAPI | TSAPI Links

Home | Help | Logout

- ▼ AE Services
 - ▶ CVLAN
 - ▶ DLG
 - ▶ DMCC
 - ▶ SMS
 - ▼ TSAPI
 - TSAPI Links
 - TSAPI Properties
 - ▶ TWS
 - ▶ Communication Manager Interface

Add TSAPI Links

Link

Switch Connection

Switch CTI Link Number

ASAI Link Version

Security

[Apply Changes](#) [Cancel Changes](#)

2.3.3 3.3. Verify Switch Connection PE/CLAN IPs

Select **Communications 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 "cm2", and click the **Edit PE/CLAN IPs** button for the corresponding connection.

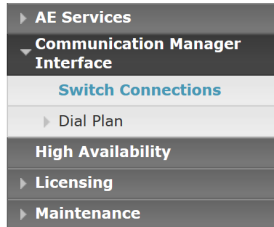


Application Enablement Services Management Console

Welcome: User cust
Last login: Mon Jun 12 02:23:01 2017 from 192.168.1.106
Number of prior failed login attempts: 0
HostName/IP: aes/172.16.1.22
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.0.15-0
Server Date and Time: Mon Jun 12 20:40:32 UTC 2017
HA Status: Not Configured

Communication Manager Interface | Switch Connections

[Home](#) | [Help](#) | [Logout](#)



Switch Connections

[Add Connection](#)

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> cm2	Yes	30	1

[Edit Connection](#)
[Edit PE/CLAN IPs](#)
[Edit H.323 Gatekeeper](#)
[Delete Connection](#)
[Survivability Hierarchy](#)

In the **Edit Processor Ethernet IP** screen, verify that ip-address is configured for Communication Manager and Status is shown "In Use". If the ip-address is not configured, then use **Add/Edit Name or IP** button to configure it.

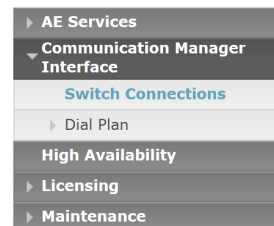


Application Enablement Services Management Console

Welcome: User cust
Last login: Mon Jun 12 02:23:01 2017 from 192.168.1.106
Number of prior failed login attempts: 0
HostName/IP: aes/172.16.1.22
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.0.15-0
Server Date and Time: Mon Jun 12 20:42:08 UTC 2017
HA Status: Not Configured

Communication Manager Interface | Switch Connections

[Home](#) | [Help](#) | [Logout](#)



Edit Processor Ethernet IP - cm2

172.16.1.21 [Add/Edit Name or IP](#)

Name or IP Address	Status
172.16.1.21	In Use

[Back](#)

Navigate back to the **Switch Connections** screen and verify that the **Number of Active Connections** is valid.

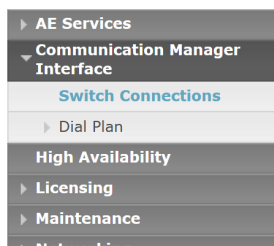


Application Enablement Services Management Console

Welcome: User cust
Last login: Mon Jun 12 20:40:14 2017 from 192.168.1.106
Number of prior failed login attempts: 0
HostName/IP: aes/172.16.1.22
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.0.15-0
Server Date and Time: Mon Jun 12 20:53:57 UTC 2017
HA Status: Not Configured

Communication Manager Interface | Switch Connections

[Home](#) | [Help](#) | [Logout](#)



Switch Connections

[Add Connection](#)

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> cm2	Yes	30	1

[Edit Connection](#)
[Edit PE/CLAN IPs](#)
[Edit H.323 Gatekeeper](#)
[Delete Connection](#)
[Survivability Hierarchy](#)

2.3.4 3.4. Verify Switch Connection H.323 Gatekeeper

Select **Communications 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 "cm2", and click **Edit H.323 Gatekeeper** button for the corresponding connection.



Application Enablement Services Management Console

Welcome: User cust
Last login: Mon Jun 12 02:23:01 2017 from 192.168.1.106
Number of prior failed login attempts: 0
HostName/IP: aes/172.16.1.22
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.0.15-0
Server Date and Time: Mon Jun 12 20:40:32 UTC 2017
HA Status: Not Configured

Communication Manager Interface | Switch Connections

Home | Help | Logout

- ▶ AE Services
- ▼ Communication Manager Interface
 - Switch Connections
 - ▶ Dial Plan
- High Availability
- ▶ Licensing
- ▶ Maintenance

Switch Connections

Add Connection

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> cm2	Yes	30	1

In the **Edit H.323 Gatekeeper** screen, verify that ip-address is configured for Communication Manager. If the ip-address is not configured yet, then use **Add Name or IP** button to configure it.



Application Enablement Services Management Console

Welcome: User cust
Last login: Mon Jun 12 02:23:01 2017 from 192.168.1.106
Number of prior failed login attempts: 0
HostName/IP: aes/172.16.1.22
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.0.15-0
Server Date and Time: Mon Jun 12 20:43:05 UTC 2017
HA Status: Not Configured

Communication Manager Interface | Switch Connections

Home | Help | Logout

- ▶ AE Services
- ▼ Communication Manager Interface
 - Switch Connections
 - ▶ Dial Plan
- High Availability
- ▶ Licensing

Edit H.323 Gatekeeper - cm2

Add Name or IP

Name or IP Address

☒ 172.16.1.21

Info

Usually, it is recommended to click **Edit Connection** button and uncheck **Secure H323 Connection** option. Otherwise, the DMCC RegisterTerminal request may fail with "unspecified" error.

2.3.5 3.5. Obtain Tlink name

Select **Security -> Security Database -> Tlinks** from the left pane. The **Tlinks** screen shows a listing of the Tlink names. Locate the Tlink Name associated with the switch connection to Avaya Communication Manager. 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 the MiaRec server.

In this case, the associated Tlink name is "AVAYA#CM2#CSTA#AES". Note the use of the switch connection "CM2" from **Section 3.2** as part of the Tlink name.

If Tlink doesn't exist, then follow instructions in **AE Services Administration** in document **Application Enablement Services Administration and Maintenance Guide** available at <http://support.avaya.com>



Application Enablement Services Management Console

Welcome: User cust
Last login: Mon Jun 12 01:28:24 2017 from 192.168.1.106
Number of prior failed login attempts: 0
HostName/IP: aes/172.16.1.22
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.0.15-0
Server Date and Time: Mon Jun 12 02:49:03 UTC 2017
HA Status: Not Configured

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

Tlinks

Tlink Name

☒ AVAYA#CM2#CSTA#AES[Delete Tlink](#)

2.3.6 3.6. Administer CTI user for MiaRec

Select **User Management -> 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**. Retain the default value of **"None"** for **Avaya Role**, and select **"Yes"** from the **CT User** drop-down list. Click on **Apply** at the bottom of the screen (not shown below). Make a note of the User Id and Password, to be used later for configuring the MiaRec server.



Application Enablement Services Management Console

Welcome: User cust
Last login: Mon Jun 12 01:28:24 2017 from 192.168.1.106
Number of prior failed login attempts: 0
HostName/IP: aes/172.16.1.22
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.0.15-0
Server Date and Time: Mon Jun 12 02:40:09 UTC 2017
HA Status: Not Configured

User Management | User Admin | Add User

Home | 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 Id	miarec
* Common Name	miarec
* Surname	miarec
* 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	

Next, you need to change the security level for the CTI User as it needs to have unrestricted access privileges.

Select **Administration -> Security Database -> CTI Users -> List All Users** from the left pane. Choose the previously created CTI user, and click **Edit**.



Application Enablement Services Management Console

Welcome: User cust
Last login: Mon Jun 12 01:28:24 2017 from 192.168.1.106
Number of prior failed login attempts: 0
HostName/IP: aes/172.16.1.22
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.0.15-0
Server Date and Time: Mon Jun 12 02:44:07 UTC 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**
 - Control
 - CTI Users**
 - List All Users**
 - Search Users
 - Devices

CTI Users

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

Edit List All

The **Edit CTI User** screen appears. Tick the **Unrestricted Access** box and **Apply Changes** at the bottom of the screen.



Application Enablement Services Management Console

Welcome: User cust
Last login: Mon Jun 12 01:28:24 2017 from 192.168.1.106
Number of prior failed login attempts: 0
HostName/IP: aes/172.16.1.22
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.0.15-0
Server Date and Time: Mon Jun 12 02:45:12 UTC 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**
 - Control
 - ▣ **CTI Users**
 - [List All Users](#)
 - Search Users
 - Devices

Edit CTI User

User Profile:	User ID	miarec
	Common Name	miarec
	Worktop Name	NONE ▾
	Unrestricted Access	<input checked="" type="checkbox"/>
Call and Device Control:	Call Origination/Termination and Device Status	Any ▾
Call and Device Monitoring:	Device Monitoring	Any ▾
	Calls On A Device Monitoring	Any ▾
	Call Monitoring	<input checked="" type="checkbox"/>
Routing Control:	Allow Routing on Listed Devices	None ▾
<input type="button" value="Apply Changes"/> <input type="button" value="Cancel Changes"/>		

2.3.7 3.7. Configure DMCC port

On the AES Management Console navigate to **Networking -> Ports** to set the DMCC server port. Enable either **Unencrypted Port** or "Encrypted Port**" or both as shown in the screen below. Note the port values to use in the following steps for MiaRec server configuration. Click **Apply Changes** button (not shown) at the bottom of the screen to complete the process.



Application Enablement Services Management Console

Welcome: User cust
Last login: Mon Jun 12 01:28:24 2017 from 192.168.1.106
Number of prior failed login attempts: 0
HostName/IP: aes/172.16.1.22
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.0.15-0
Server Date and Time: Mon Jun 12 02:46:46 UTC 2017
HA Status: Not Configured

Networking | Ports

Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ Licensing
- ▶ Maintenance
- ▼ Networking
 - AE Service IP (Local IP)
 - Network Configure
 - Ports**
 - TCP/TLS Settings
- ▶ Security
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

Ports

CVLAN Ports			Enabled Disabled
Unencrypted TCP Port	9999	<input checked="" type="radio"/>	<input type="radio"/>
Encrypted TCP Port	<input type="text" value="9998"/>	<input checked="" type="radio"/>	<input type="radio"/>
<hr/>			
DLG Port	TCP Port	5678	
<hr/>			
TSAPI Ports			Enabled Disabled
TSAPI Service Port	450	<input checked="" type="radio"/>	<input type="radio"/>
Local TLINK Ports			
TCP Port Min	1024		
TCP Port Max	1039		
Unencrypted TLINK Ports			
TCP Port Min	<input type="text" value="1050"/>		
TCP Port Max	<input type="text" value="1065"/>		
Encrypted TLINK Ports			
TCP Port Min	<input type="text" value="1066"/>		
TCP Port Max	<input type="text" value="1081"/>		
<hr/>			
DMCC Server Ports			Enabled Disabled
Unencrypted Port	<input type="text" value="4721"/>	<input checked="" type="radio"/>	<input type="radio"/>
Encrypted Port	<input type="text" value="4722"/>	<input checked="" type="radio"/>	<input type="radio"/>
TR/87 Port	<input type="text" value="4723"/>	<input type="radio"/>	<input checked="" type="radio"/>
<hr/>			
H.323 Ports			
TCP Port Min	<input type="text" value="20000"/>		
TCP Port Max	<input type="text" value="29999"/>		
Local UDP Port Min	<input type="text" value="20000"/>		
Local UDP Port Max	<input type="text" value="29999"/>		
<hr/>			
Server Media			Enabled Disabled
			<input checked="" type="radio"/> <input type="radio"/>
RTP Local UDP Port Min*	<input type="text" value="30000"/>		
RTP Local UDP Port Max*	<input type="text" value="49999"/>		

2.3.8 3.8. Enable Security Database

Select **Security -> Security Database -> Control** from the left pane, to display the **SDB Control for DMCC and TSAPI** screen in the right pane. Check **Enable SDB for DMCC Service** and **Enable SDB TSAPI Service, JTAPI and Telephony Service**, and click **Apply Changes**.

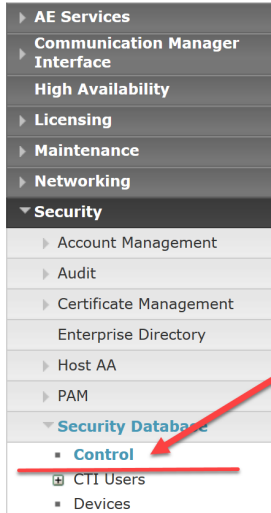


Application Enablement Services Management Console

Welcome: User cust
Last login: Mon Jun 12 01:28:24 2017 from 192.168.1.106
Number of prior failed login attempts: 0
HostName/IP: aes/172.16.1.22
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.0.15-0
Server Date and Time: Mon Jun 12 02:29:53 UTC 2017
HA Status: Not Configured

Security | Security Database | Control

Home | Help | Logout



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

MiaRec application uses a password-less authentication when registering devices against AES.

To permit a password-less authentication, the following requirements must be satisfied:

- The SDB on the AE Services server is enabled (see this Step)
- The CTI user has **Unrestricted Access** in the SDB (see the Step 3.6)
- The extension's class of restriction (COR) on the Communication manager has (see the Step 2.5):
 - **Can Be Service Observed** set to y
 - **Can Be a Service Observer** set to y

2.3.9 3.9. Restart TSAPI and DMCC 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**.

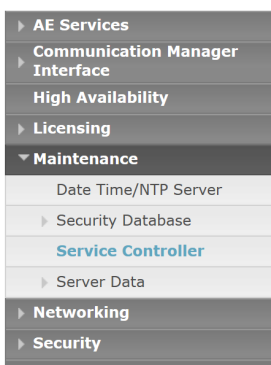


Application Enablement Services Management Console

Welcome: User cust
Last login: Mon Jun 12 01:28:24 2017 from 192.168.1.106
Number of prior failed login attempts: 0
HostName/IP: aes/172.16.1.22
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.0.15-0
Server Date and Time: Mon Jun 12 02:33:05 UTC 2017
HA Status: Not Configured

Maintenance | Service Controller

Home | Help | Logout



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](#)

Start Stop **Restart Service** Restart AE Server Restart Linux Restart Web Server

2.4 4. Configure MiaRec Call Recording System

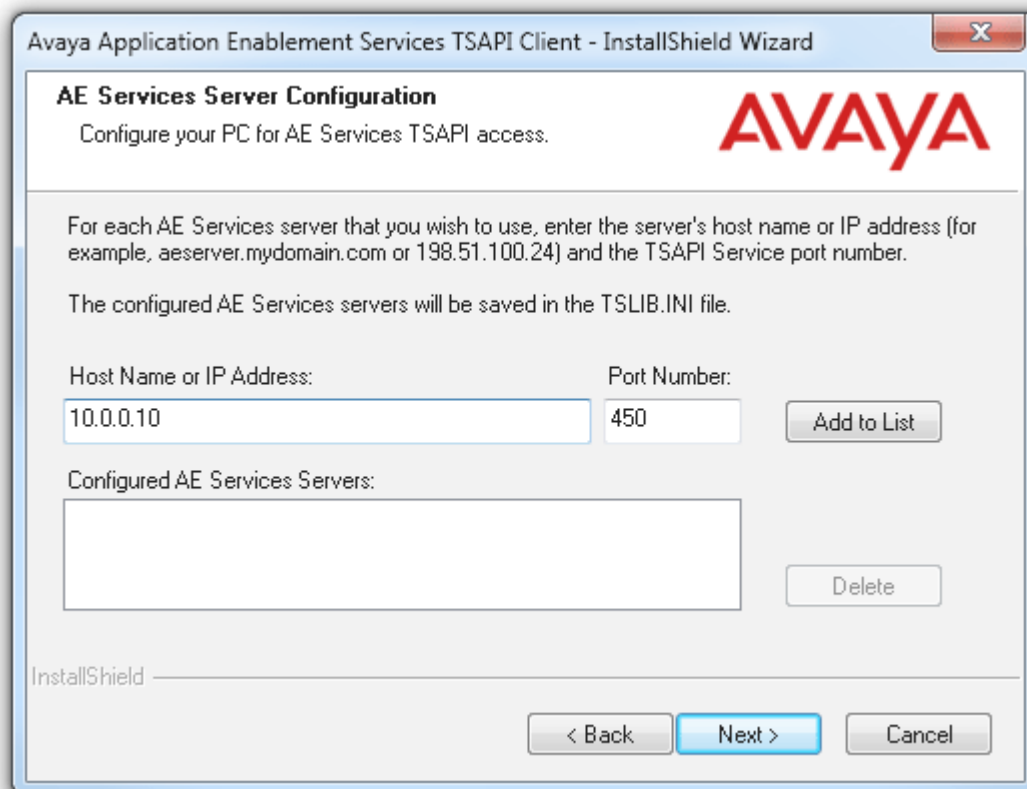
This section presents configuration steps for MiaRec call recording system. It is assumed that MiaRec is already installed on the server. The procedures include the following areas:

- Install AES TSAPI Client
- Administer MiaRec TSAPI link to AES
- Administer MiaRec DMCC link to AES

2.4.1 4.1. Install AES TSAPI Client

Download Application Enablement Services TSAPI Client from <http://support.avaya.com>

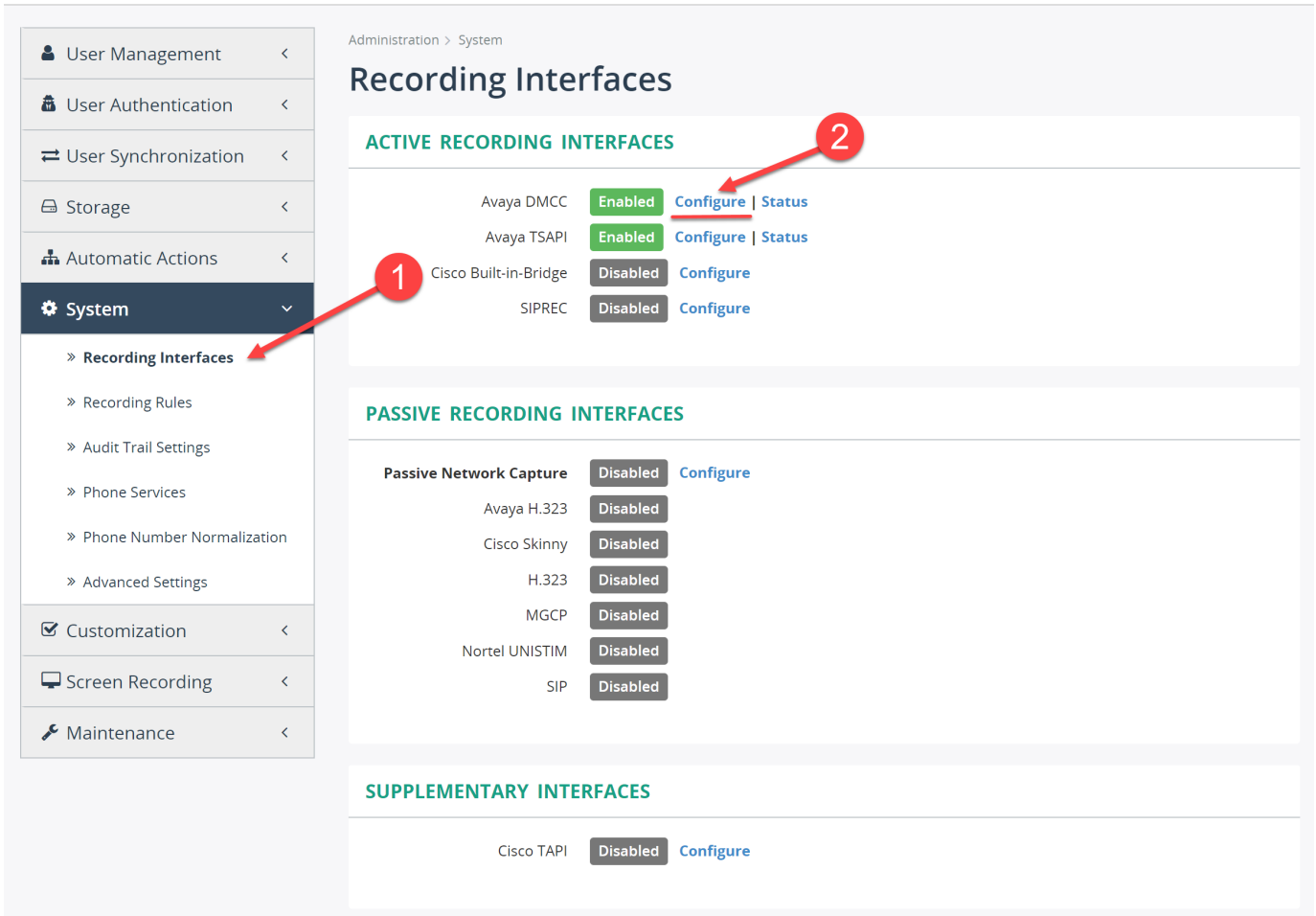
Install it on MiaRec server. During installation enter the IP address of the Avaya AES server in the **Host Name or IP Address** field, retaining the default port of 450 (see below screenshot). Click on **Add to List** and then **Next** to finish installation.



2.4.2 4.2. Administer MiaRec DMCC settings

Navigate in the MiaRec web interface to **Administration -> System -> Recording Interfaces** and click the **Configure** link for **Avaya DMCC** interface.

Administration



Administration > System

Recording Interfaces

ACTIVE RECORDING INTERFACES

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

PASSIVE RECORDING INTERFACES

Passive Network Capture	Status	Action
Avaya H.323	Disabled	Configure
Cisco Skinny	Disabled	
H.323	Disabled	
MGCP	Disabled	
Nortel UNISTIM	Disabled	
SIP	Disabled	

SUPPLEMENTARY INTERFACES

Cisco TAPI	Disabled	Configure
------------	----------	---------------------------

In the **Configure Recording Interface (Avaya DMCC)** screen, configure the following settings:

- Option **Enable** should be checked.
- Option **AES server** should point to HOST:PORT of AES server, where the **HOST** is an ip-address or DNS name of the Application Enablement Services server and the **PORT** is DMCC port obtained in the **Section 3.7. Configure DMCC port**.
- Option **Use SSL** should be checked when Encrypted DMCC port is used for connection to AES server.
- Option **DMCC login** and "DMCC password*" should be set to the credentials of CTI user created in **Section 3.6. Administer CTI user for MiaRec**.
- Option **SwitchName** should be set the hostname of Communication Manager used to register DMCC virtual softphone against to.
- Retain default settings for other values.

Administration > System > Recording Interfaces

Configure Recording Interface

Enable *

☒ Enable Avaya DMCC recording

AES server

172.16.1.22:4721

Address of AES server. Format: host:port

Use SSL

☐ Use SSL

Use TLS/SSL connection to AES server

DMCC login

miarec

DMCC password

.....

SwitchName

cm2

Hostname of Avaya CM server. Either SwitchName or SwithIPInterface or both should be configured

SwitchIPInterface

0.0.0.0

IP address of Avaya CM server. Either SwitchName or SwithIPInterface or both should be configured. Recommended value: 0.0.0.0 (the ip-address will be resolved automatically from SwitchName)

Begin RTP port range

32000

Begin UDP port range for RTP media

End RTP port range

33999

End UDP port range for RTP media

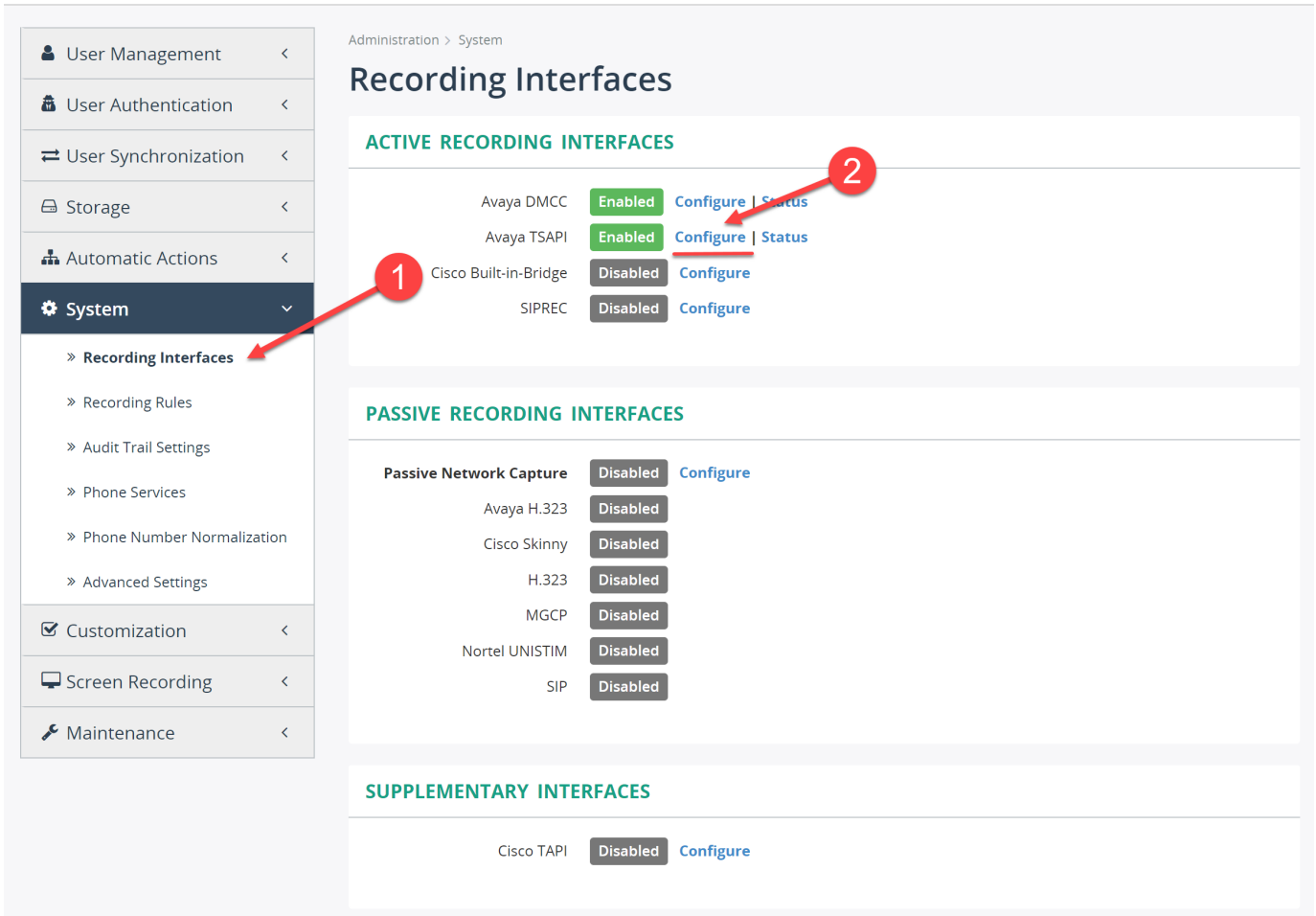
Public Ip-address

Public IP-address if the recorder is behind NAT. Otherwise leave empty

2.4.3 4.3. Administer MiaRec TSAPI settings

Navigate in the MiaRec web interface to **Administration -> System -> Recording Interfaces** and click **Configure** link for **Avaya TSAPI** interface.

Administration



Administration > System

Recording Interfaces

ACTIVE RECORDING INTERFACES

Interface	Status	Actions
Avaya DMCC	Enabled	Configure Status
Avaya TSAPI	Enabled	Configure Status
Cisco Built-in-Bridge	Disabled	Configure
SIPREC	Disabled	Configure

PASSIVE RECORDING INTERFACES

Interface	Status	Actions
Passive Network Capture	Disabled	Configure
Avaya H.323	Disabled	
Cisco Skinny	Disabled	
H.323	Disabled	
MGCP	Disabled	
Nortel UNISTIM	Disabled	
SIP	Disabled	

SUPPLEMENTARY INTERFACES

Interface	Status	Actions
Cisco TAPI	Disabled	Configure

In the **Configure Recording Interface (Avaya TSAPI)** screen, configure the following settings:

- Option **Enable** should be checked.
- Option **TSAPI Link** should point to the obtained TLink in the **Section 3.5. Obtain Tlink name**.
- Option **TSAPI login** and "TSAPI password**" should be set to the credentials of CTI user created in **Section 3.6. Administer CTI user for MiaRec**.
- Option **Media Source** should be set to **DMCC**.
- Option **Monitored phones** should list all recorded extensions, comma-separated. A range of extensions is supported, like 3000-3100, 5001, 5002.
- Option **Monitored ACD Splits** should list all ACDs, which the recorded users may login to. MiaRec monitors ACDs for login/logout events. A range value is supported, like 4900-49100, 55000, 56000.
- Option **Ignore dialing phase** could be enabled to avoid recording of initial dialing phase of the outgoing call scenario.
- Retain default settings for other values.

Configure Recording Interface

Enable * ☒ Enable Avaya TSAPI recording

TSAPI Link

TSAPI link, like AVAYA#SWITCH1#CSTA#SERVERNAME1

TSAPI login

TSAPI account name

TSAPI password

TSAPI account password

Media Source ☐ Passive - port mirroring
☒ DMCC

Monitored phones

A range of monitored phones (comma-separated). Example: 3000-3100,5001,5002

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.

2.5 5. Verification and Troubleshooting

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

2.5.1 5.1. Verify Avaya Communication Manager

On Avaya Communication Manager, verify the status of the administered CTI links by using 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	aes-server1	established	15	15

The "**status aesvcs interface**" command should indicate the interface is **listening**.

```
status aesvcs interface
```

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

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 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	aes-server1	10.0.0.25	43909	procr	224	209

Once the MiaRec call recording application is running, the "**list monitored-station**" command will show each station, which is monitored by MiaRec via TSAPI interface.

```
list monitored-station
```

MONITORED STATION								
Station Ext	Association 1 CTI Link	Association 1 CRV	Association 2 CTI Link	Association 2 CRV	Association 3 CTI Link	Association 3 CRV	Association 4 CTI Link	Association 4 CRV
32129	1	10						
32130	1	9						
32131	1	22						
32132	1	7						

2.5.2 5.2 Verify Avaya Application Enablement Services

On Application Enablement Services, verify the status of the switch connection by selecting **Status -> Status and Control -> Switch Conn Summary** from the left pane. Verify that the **Conn State** is "**Talking**" for the switch connection associated with Avaya Communication Manager, and that the **Associations** column reflects the total number of monitored skill groups and agent stations as configured previously.



Application Enablement Services Management Console

Welcome: User cust
Last login: Mon Jun 12 21:23:45 2017 from 192.168.1.106
Number of prior failed login attempts: 0
HostName/IP: aes/172.16.1.22
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.0.15-0
Server Date and Time: Mon Jun 12 22:22:49 UTC 2017
HA Status: Not Configured

Status | Status and Control | Switch Conn 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
- ▶ User Management

Switch Connections Summary

☐ Enable page refresh every 60 seconds

	Switch Conn	Conn State	Processor Ethernet	Since	Online/Offline	Active/Standby/ Admin'd TEP Conns	Num of TCI Conns	SSL	Msgs To Switch	Msgs From Switch	Msg Period
<input checked="" type="radio"/>	cm2	Talking	Yes	Tue Jun 6 14:51:55 2017	Online	1 / 0 / 1	2	Enabled	615	630	30

Online Offline Connection Details Per Service Connections Details

Verify the status of the TSAPI link by selecting **Status -> Status and Control -> TSAPI Service Summary** from the left pane. Verify the **Conn Status** is **Talking** as shown below.



Application Enablement Services Management Console

Welcome: User cust
Last login: Mon Jun 12 21:23:45 2017 from 192.168.1.106
Number of prior failed login attempts: 0
HostName/IP: aes/172.16.1.22
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.0.15-0
Server Date and Time: Mon Jun 12 22:24:06 UTC 2017
HA Status: Not Configured

Status | Status and Control | TSAPI 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**
- ▶ User Management

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	cm2	1	Talking	Tue Jun 6 14:51:55 2017	Online	17	6	15	15	30

Online Offline

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

TSAPI Service Status TLink Status User Status

Verify the status of the CTI User by selecting **Status -> Status and Control -> TSAPI Service Summary** from the left pane. Click the **User Status** button (not shown below). The **CTI User Status** screen is displayed. Verify that an open session exists for the CTI user created for MiaRec as shown below. This verification step assumes that MiaRec application is configured properly and running.



Application Enablement Services Management Console

Welcome: User cust
Last login: Mon Jun 12 21:23:45 2017 from 192.168.1.106
Number of prior failed login attempts: 0
HostName/IP: aes/172.16.1.22
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.0.15-0
Server Date and Time: Mon Jun 12 22:28:54 UTC 2017
HA Status: Not Configured

Status | Status and Control | TSAPI 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**

CTI User Status

☐ Enable page refresh every 60 seconds

CTI Users All Users Submit

Open Streams 3

Closed Streams 50

Open Streams

Name	Time Opened	Time Closed	Tlink Name
miarec	Mon 12 Jun 2017 09:41:57 PM UTC		AVAYA#CM2#CSTA#AES
DMCCCLCSUserDoNotModify	Tue 06 Jun 2017 02:51:44 PM UTC		AVAYA#CM2#CSTA#AES
DMCCCLCSUserDoNotModify	Tue 06 Jun 2017 02:51:44 PM UTC		AVAYA#CM2#CSTA#AES

Show Closed Streams Close All Opened Streams Back

Verify the 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 and that the **# of Associated Devices** column reflects the total number of configured DMCC devices.



Application Enablement Services Management Console

Welcome: User cust
Last login: Mon Jun 12 21:23:45 2017 from 192.168.1.106
Number of prior failed login attempts: 0
HostName/IP: aes/172.16.1.22
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.0.15-0
Server Date and Time: Mon Jun 12 22:25:28 UTC 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
 - ▶ User Management
 - ▶ Utilities

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)

Generated on Mon Jun 12 22:25:18 UTC 2017

Service Uptime: 6 days, 7 hours 33 minutes

Number of Active Sessions: 2

Number of Sessions Created Since Service Boot: 59

Number of Existing Devices: 2

Number of Devices Created Since Service Boot: 93

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	AF8ECA05829692F1E 2DA3CEC9B2BE058-63	miarec	MiaRec	192.168.1.106	XML Encrypted	2
<input type="checkbox"/>	8872309FAEFE5902C CF76FC6B4317AD9-14	miarec	testTool	192.168.1.106	XML Unencrypted	0

Terminate Sessions Show Terminated Sessions

Item 1-2 of 2
1 Go

Click **Device Summary** link in the **Status -> Status and Control -> DMCC Service Summary** screen to see the list of currently registered DMCC devices.



Application Enablement Services Management Console

Welcome: User cust
Last login: Mon Jun 12 21:23:45 2017 from 192.168.1.106
Number of prior failed login attempts: 0
HostName/IP: aes/172.16.1.22
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.0.15-0
Server Date and Time: Mon Jun 12 22:30:57 UTC 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
- ▶ User Management

DMCC Service Summary - Device Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

[Session Summary](#) Device Summary

Generated on Mon Jun 12 22:30:37 UTC 2017

Service Uptime: 6 days, 7 hours and 38 minutes

Number of Active Sessions: 2

Number of Sessions Created Since Service Boot: 59

Number of Existing Devices: 2

Number of Devices Created Since Service Boot: 93

	Device ID	Gatekeeper IP address	State	Associated Sessions
<input type="checkbox"/>	3000:cm2:0.0.0.0:0	172.16.1.21	REGISTERED	1
<input type="checkbox"/>	3001:cm2:0.0.0.0:0	172.16.1.21	REGISTERED	1

Terminate Devices

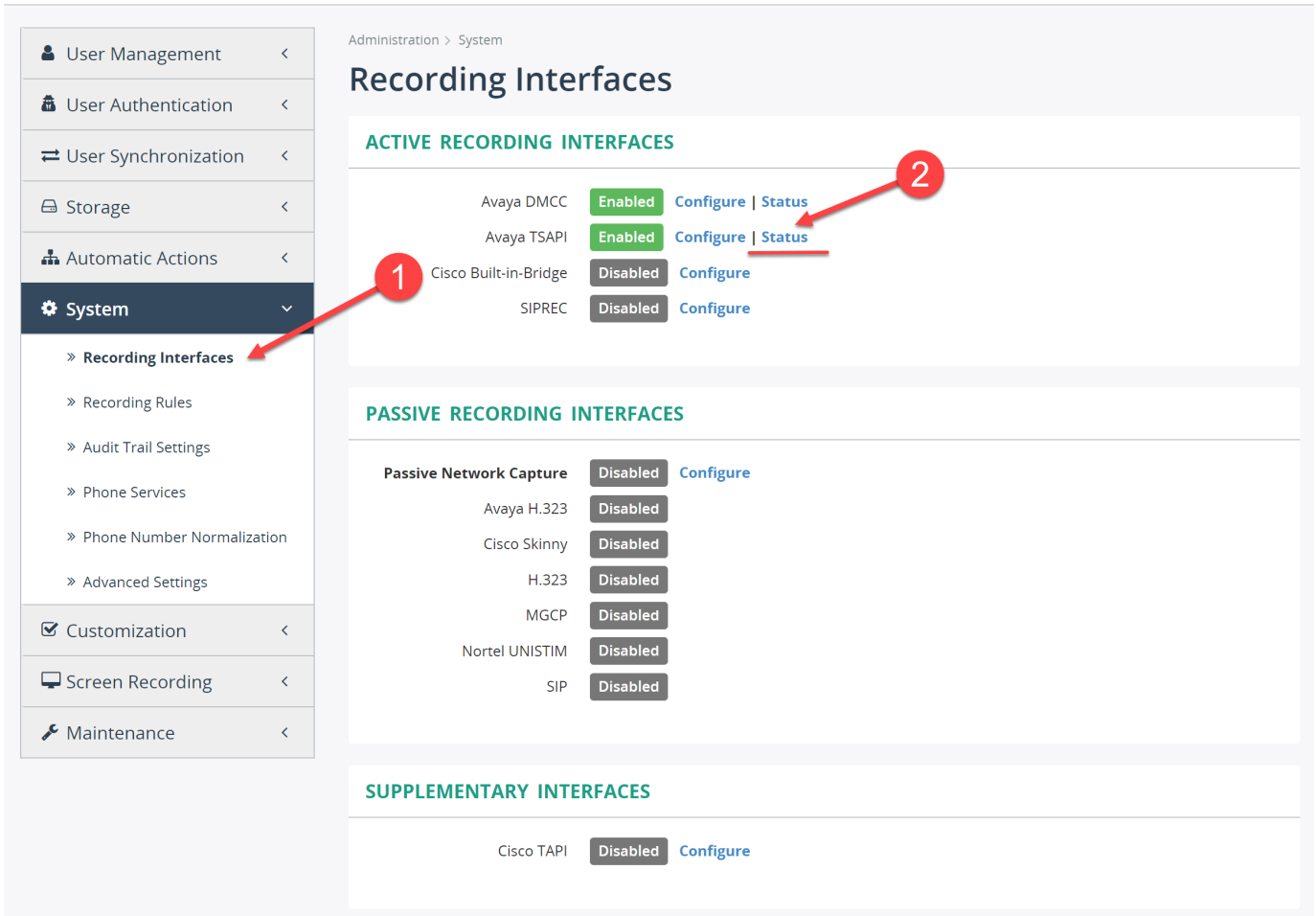
Item 1-2 of 2

1 Go

2.5.3 5.3. Verify TSAPI device monitoring status in MiaRec

Navigate in the MiaRec web interface to **Administration -> System -> Recording Interfaces** and click the **Status** link for **Avaya TSAPI** interface.

Administration



Administration > System

Recording Interfaces

ACTIVE RECORDING INTERFACES

Interface	Status	Actions
Avaya DMCC	Enabled	Configure Status
Avaya TSAPI	Enabled	Configure Status
Cisco Built-in-Bridge	Disabled	Configure
SIPREC	Disabled	Configure

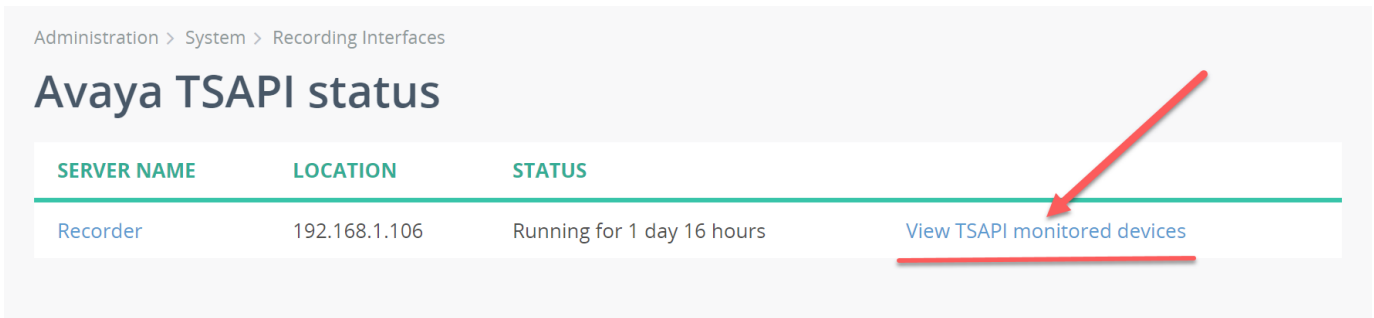
PASSIVE RECORDING INTERFACES

Interface	Status	Actions
Passive Network Capture	Disabled	Configure
Avaya H.323	Disabled	
Cisco Skinny	Disabled	
H.323	Disabled	
MGCP	Disabled	
Nortel UNISTIM	Disabled	
SIP	Disabled	

SUPPLEMENTARY INTERFACES

Interface	Status	Actions
Cisco TAPI	Disabled	Configure

In the **Avaya TSAPI status** screen, click the **View TSAPI monitored devices** link for the appropriate recorder instance (the screenshot below shows one instance).



Administration > System > Recording Interfaces

Avaya TSAPI status

SERVER NAME	LOCATION	STATUS	
Recorder	192.168.1.106	Running for 1 day 16 hours	View TSAPI monitored devices

In the **Avaya TSAPI monitored devices** screen, verify the status of the monitored devices. If any device shows a **failed** state, then click the extension link in that window to see the detailed error message.

Administration > System > Recording Interfaces > Avaya TSAPI status

Avaya TSAPI monitored devices

Recorder Name: **Recorder**Host IP: **192.168.1.106**Status: **Running for 1 day 17 hours**

Monitored Devices

Search



0-7 of 7



EXTENSION	DEVICE NAME	AGENT ID	AGENT NAME	MONITOR STATE	TSAPI IP	ACTIVE CALLS	TOTAL CALLS	LAST EVENT TIME
3001	User Two			active	192.168.1.104	1	4	1 minute 10 seconds ago
3000	Phone One			active	192.168.1.103	1	5	1 minute 10 seconds ago
49000				failed		0	0	5 seconds ago
3003	User 3003			active		0	0	5 seconds ago
3002	User 3			active		0	0	5 seconds ago

The error message describes the actual reasons of the failure. Read the message and apply appropriate corrections. For example, the message in the following screenshot says that device identifier (extension) is not valid. In this case, remove this extension from the **Monitored Phones** list in configuration.

Administration > System > Recording Interfaces > Avaya TSAPI status > Recorder DEV1

Avaya TSAPI monitored device

Extension: **49000**Media Source: **dmcc**

Device Name

Agent ID

Agent Name

Monitor State **failed**

H.323 IP

TSAPI IP

Active Calls **0**Total Calls **0**Last Event Time **1 minute 6 seconds ago**Monitor Start Time **1 minute 6 seconds ago**Error Code **12**

Error **INVALID_CSTA_DEVICE_IDENTIFIER (12) An invalid device identifier (extension) has been specified**

Recommendations **Check a list of monitored phones inside configuration file**

If the **Avaya TSAPI monitored devices** screen shows none of devices (neither successfully monitored nor failed), then probably the TSAPI link connection is not established to AES server. In this case, navigate to **Administration -> Maintenance -> System Log** and check any error messages. The screenshot below shows that the TSAPI login/password is invalid. Make the appropriate corrections to the configuration.

Wide view 

Administration

User Management <

User Authentication <

User Synchronization <

Storage <

Automatic Actions <

System <

Customization <

Screen Recording <

Maintenance

» System Log

» System Status

Administration > Maintenance

System Log

2017/06/11 - 2017/06/11

Select a Severity

Select a Type

Search

Delete

0-1 of 1

SEVERITY

DATE

SOURCE & TYPE

MESSAGE

Error

Today 4:55 PM

Recorder Protocol:Avaya::TSAPI

Failed to establish a connection to Avaya AES Server: TSERVER_BAD_PASSWORD_OR_LOGIN (25) The password, login, or both did not pass the TSAPI Service authentication checks. Check the TSAPI password and login settings inside configuration file

20 per page

0-1 of 1

2.5.4 5.4. Verify DMCC device registration status in MiaRec

Navigate in the MiaRec web interface to **Administration -> System -> Recording Interfaces** and click the **Status** link for the **Avaya DMCC** interface.

Administration

Administration > System

Recording Interfaces

ACTIVE RECORDING INTERFACES

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

PASSIVE RECORDING INTERFACES

Passive Network Capture	Disabled	Configure
Avaya H.323	Disabled	
Cisco Skinny	Disabled	
H.323	Disabled	
MGCP	Disabled	
Nortel UNISTIM	Disabled	
SIP	Disabled	

SUPPLEMENTARY INTERFACES

Cisco TAPI	Disabled	Configure
------------	----------	---------------------------

In the **Avaya DMCC status** screen, click the **View DNCC registered devices** link for the appropriate recorder instance (the screenshot below shows one instance).

Administration > System > Recording Interfaces

Avaya DMCC status

SERVER NAME	LOCATION	STATUS	
Recorder	192.168.1.106	Running for 1 day 16 hours	View DMCC registered devices

In the **Avaya DMCC devices** screen, verify status of the registered devices. If any device shows a **failed** state, then click the extension link in that window to see the detailed error message.

Administration > System > Recording Interfaces > Avaya DMCC status

Avaya DMCC devices

Recorder Name: Recorder

Host IP: 192.168.1.106

Status: Running for 1 day 16 hours

Registered Devices

Search by Extension

Search

0-2 of 2

EXTENSION

REGISTRATION STATE

ACTIVE CALLS

TOTAL CALLS

LAST EVENT TIME

3001

Registered

0

1

48 seconds ago

3000

Registered

0

1

48 seconds ago

100

per page

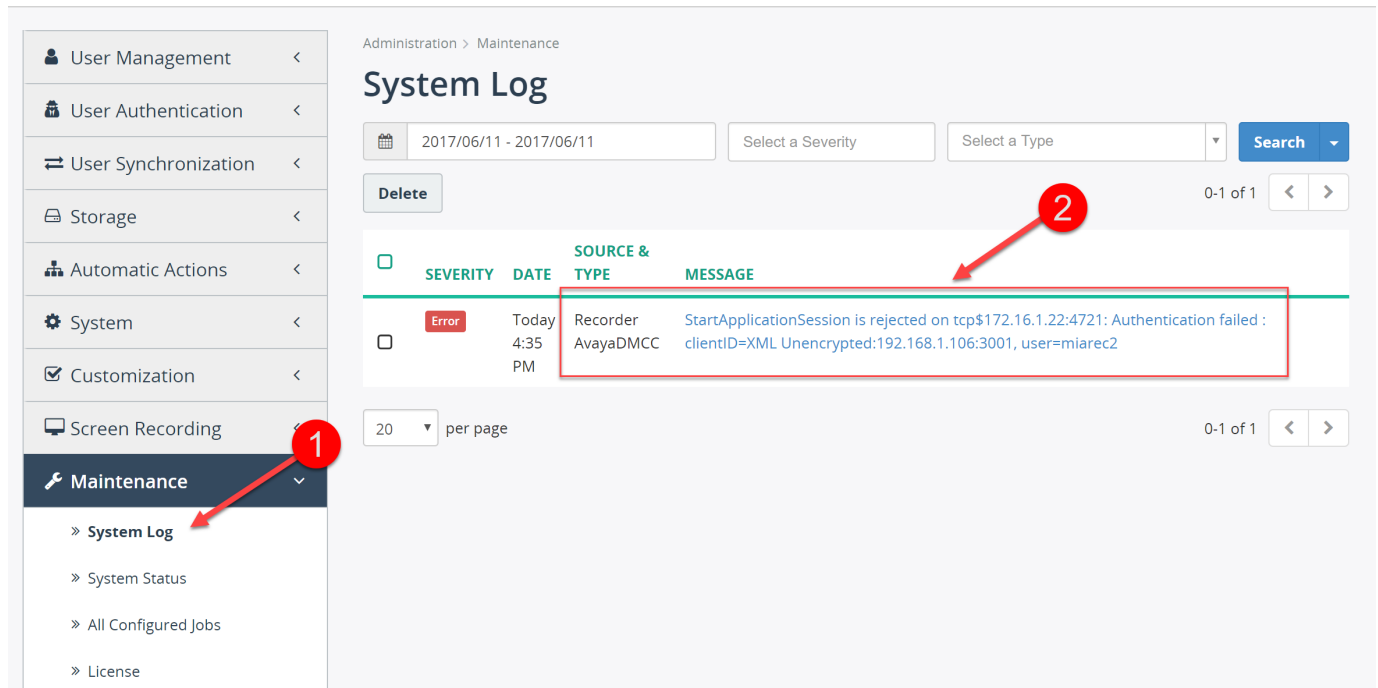
0-2 of 2

If the **Avaya DMCC registered devices** screen shows none of devices (neither successfully registered nor failed), then probably the DMCC connection is not established to the AES server. In this case, navigate to **Administration -> Maintenance -> System Log** and check any error messages. The screenshot below shows that the DMCC login/password is rejected. Make the appropriate corrections to the configuration.

- 32/60 -

Copyright © 2024 MiaRec, Inc.

Administration



Administration > Maintenance

System Log

2017/06/11 - 2017/06/11

0-1 of 1

<input type="checkbox"/>	SEVERITY	DATE	SOURCE & TYPE	MESSAGE
<input type="checkbox"/>	Error	Today 4:35 PM	Recorder AvayaDMCC	StartApplicationSession is rejected on tcp\$172.16.1.22:4721: Authentication failed : clientID=XML Unencrypted:192.168.1.106:3001, user=miarec2

20 per page 0-1 of 1

2.5.5 5.5. Check MiaRec trace log

MiaRec provides detailed logging for troubleshooting purposes. Navigate to **Administration -> Maintenance -> Troubleshooting** to enable log in MiaRec.

2.6 6. Additional references

- **Administering Avaya Communication Manager** (available at <http://support.avaya.com>)
- **Application Enablement Services Administration and Maintenance Guide** (available at <http://support.avaya.com>)
- **Application Enablement Services TSAPI, JTAPI and CVLAN Client and SDK Installation Guide** (available at <http://support.avaya.com>)

3. Avaya TSAPI Passive Recording

3.1 1. Introduction

This article describes how to configure the MiaRec Call Recording System with the Avaya Application Enablement Services and Avaya Communication Manager to record incoming and outgoing phone calls.

MiaRec uses port mirroring on a network switch to capture media associated with the recorded stations and TSAPI interface of Avaya Application Enablement Services (AES) to extract agent and call state information.

Requirements:

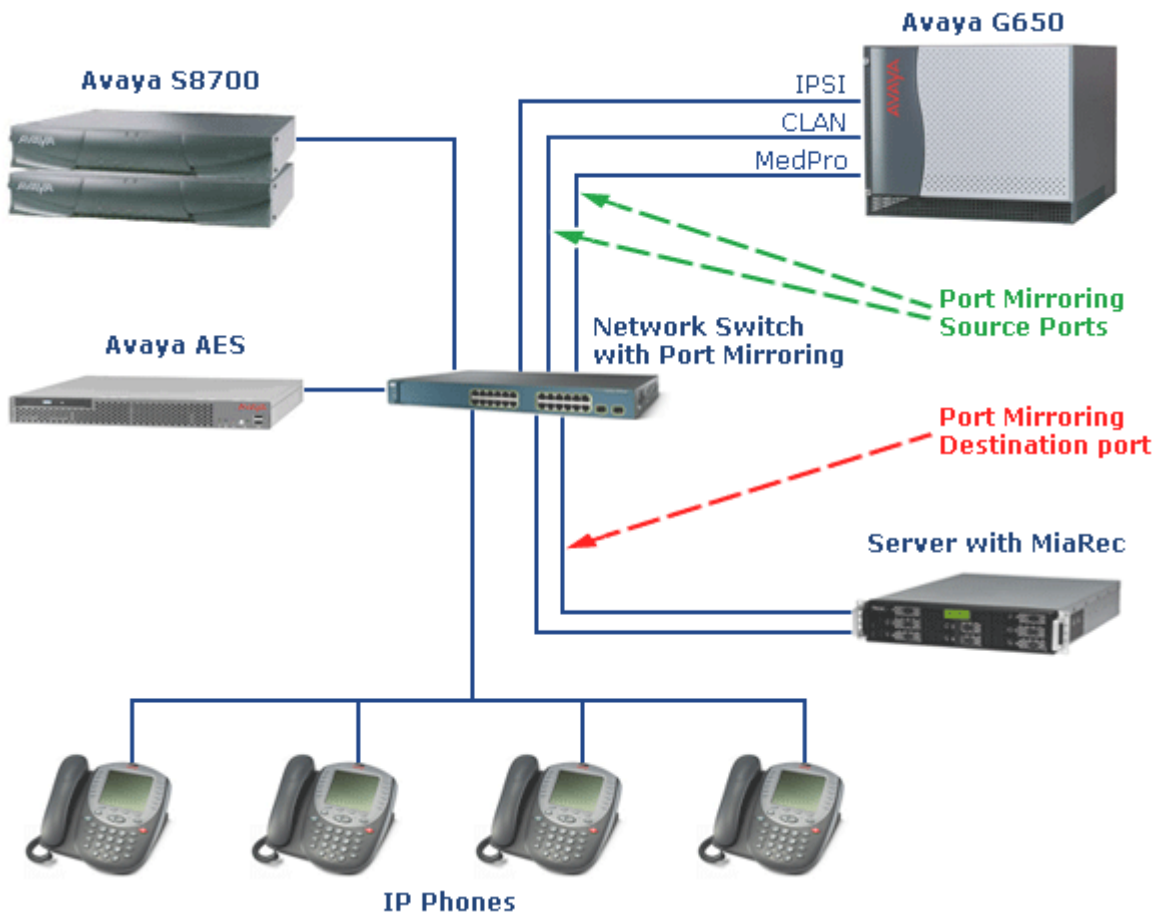
- Avaya Communication Manager v6.3.2 or higher
- Avaya Application Enablement Services (AES) Server v6.3.1 or higher
- TSAPI Basic License per each recorded extension and each monitored ACD Split / Hunt Group
- Network Switch with Port Mirroring support
- Server for MiaRec with two network adapters

3.2 2. Network Configuration

MiaRec uses a port mirroring function on a network switch to capture the voice packet related to the agents' IP phones and softphones. MiaRec server needs to have two Network Interface Cards (NICs), one of which is used for port mirroring (capturing voice) and another is used for regular network connection. The first NIC doesn't need to have TCP/IP stack enabled (see Network adapter configuration)

The port mirroring function has to be configured on a network switch in the following way:

- Ports of the C-LAN and MedPro cards should be configured as sources for port mirroring session
- MiaRec capturing port should be configured as a destination for port mirroring session



Below is an example of port mirroring configuration on **Extreme Networks Summit X250e-24p** network switch.

Assuming that:

- **C-LAN** card is connected to **Port 1** of the Summit X250e
- **MedPro** card is connected to **Port 2** of the Summit X250e
- **MiaRec** capturing NIC is connected to **Port 24** of the Summit X250e

In this case you need to execute following commands on the switch:

```
enable mirroring port 24
mirroring add port 1
mirroring add port 2
```

Save configuration into permanent memory (NVRAM), otherwise the port mirroring settings will be lost after the switch reboot:

save config

3.3 3. Configure Avaya Communication Manager

This section presents configuration steps for the Avaya Communication Manager. It is assumed that an appropriate license file and authentication file have been installed on the server, and that login and password credentials are available.

The configuration and verification operations illustrated in this section were all performed using the Communication Manager System Administration Terminal (SAT).

The procedures include the following areas:

- Verify the status CTI link for TSAPI service
- Disable RTP encryption
- Enable RTCP reporting
- Disable IP-IP Direct Audio (optional)
- Administer System Parameters Features

3.3.1 3.1. Verify the status of CTI link for TSAPI service

Log into the System Access Terminal (SAT) to enter the "**status aesvcs cti-link**" command. The link status should show **no** for maintenance busy (**Mnt Busy**), the **Service State** should indicate **established** and **Version** should be **6** or higher.

```
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	aes	established	15	15

If the CTI link is not established, then follow instructions in chapter **Administering Communication Manager for AE Services** in document **Application Enablement Services Administration and Maintenance Guide** available at <http://support.avaya.com>

3.3.2 3.2. Disable RTP encryption

Execute the "**list ip-codec-set**" command.

```
list ip-codec-set
```

IP CODEC SETS					
Codec Set	Codec 1	Codec 2	Codec 3	Codec 4	Codec 5
1	G.711MU				
2	G.711MU				
3	G.711MU				
4	G.711MU				
5	G.711MU				
6	G.711MU				
7	G.711MU				

For each of codec sets, execute the "**change ip-codec-set N**" command, where **N** is an index of set (from 1 to 7 in above example).

For example, to edit the first codec set, execute the "**change ip-codec-set 1**" command and make certain that **Media Encryption** list contains only a single value "none". If other values are presented there (for example, "aes"), then remove all other values except "none" as shown below:

```
change ip-codec-set 1
```

Page 1 of 2

IP Codec Set
Codec Set: 1

Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size(ms)
1: G.711MU	n	2	20
2:			
3:			
4:			
5:			
6:			
7:			

Media Encryption
1: none
2:
3:

Repeat this step for all the remaining codec sets.

3.3.3 3.3. Enable RTCP reporting

Enter the **"change ip-network-region N"** command, where **N** is an existing network region used for the agents' ip phones and softphones. Make certain that the **RTCP Reporting Enabled** field is set to **"y"**, as shown below. The RTCP packets are used by MiaRec to map IP addresses to agent extensions.

change ip-network-region 1	Page 1 of 19
IP NETWORK REGION	
Region: 1	
Location:	Authoritative Domain: voip.example.com
Name:	
MEDIA PARAMETERS	Intra-region IP-IP Direct Audio: yes
Codec Set: 1	Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048	IP Audio Hairpinning? y
UDP Port Max: 3029	
DIFFSERV/TOS PARAMETERS	RTCP Reporting Enabled? y
Call Control PHB Value: 34	RTCP MONITOR SERVER PARAMETERS
Audio PHB Value: 46	Use Default Server Parameters? y
Video PHB Value: 26	

3.3.4 3.4. Disable IP-IP Direct Audio (optional)

You can skip this step if recording of internal calls between IP phones is not needed.

Avaya Communication Manager supports "shuffling" of the media streams, which allows two IP phones to send media directly between each other bypassing the media gateway. "Shuffling" (IP-IP Direct Audio) should be disabled when internal calls between IP phones need to be recorded. IP-IP Direct Audio can be disabled either for individual IP phones or for a whole ip network region.

To disable IP-IP Direct Audio for individual IP phone, enter the **"change station xxxxx"**, where xxxxx is phone's extension and change **"Direct IP-IP Audio Connections"** to **"n"** on **Page 2**.

Parameter **"IP Audio Harpinning"** is recommended to set to **"y"**. In this case, MedPro board acts as a proxy without allocating of resources on TDM bus.

change station 51001	Page 2 of 5
STATION	
FEATURE OPTIONS	
LWC Reception: spe	Auto Select Any Idle Appearance? n
LWC Activation? y	Coverage Msg Retrieval? y
LWC Log External Calls? n	Auto Answer: none
CDR Privacy? n	Data Restriction? n
Redirect Notification? y	Idle Appearance Preference? n
Per Button Ring Control? n	Bridged Idle Line Preference? n
Bridged Call Alerting? n	Restrict Last Appearance? y
Active Station Ringing: single	
	EMU Login Allowed? n
H.320 Conversion? n	Per Station CPN - Send Calling Number?
Service Link Mode: as-needed	
Multimedia Mode: enhanced	
MWI Served User Type:	Display Client Redirection? n
AUDIX Name:	Select Last Used Appearance? n
IP Hoteling? n	Coverage After Forwarding? s
	Multimedia Early Answer? n
Remote Softphone Emergency Calls: as-on-local	Direct IP-IP Audio Connections? n
Emergency Location Ext: 51001	Always Use? n IP Audio Hairpinning? y

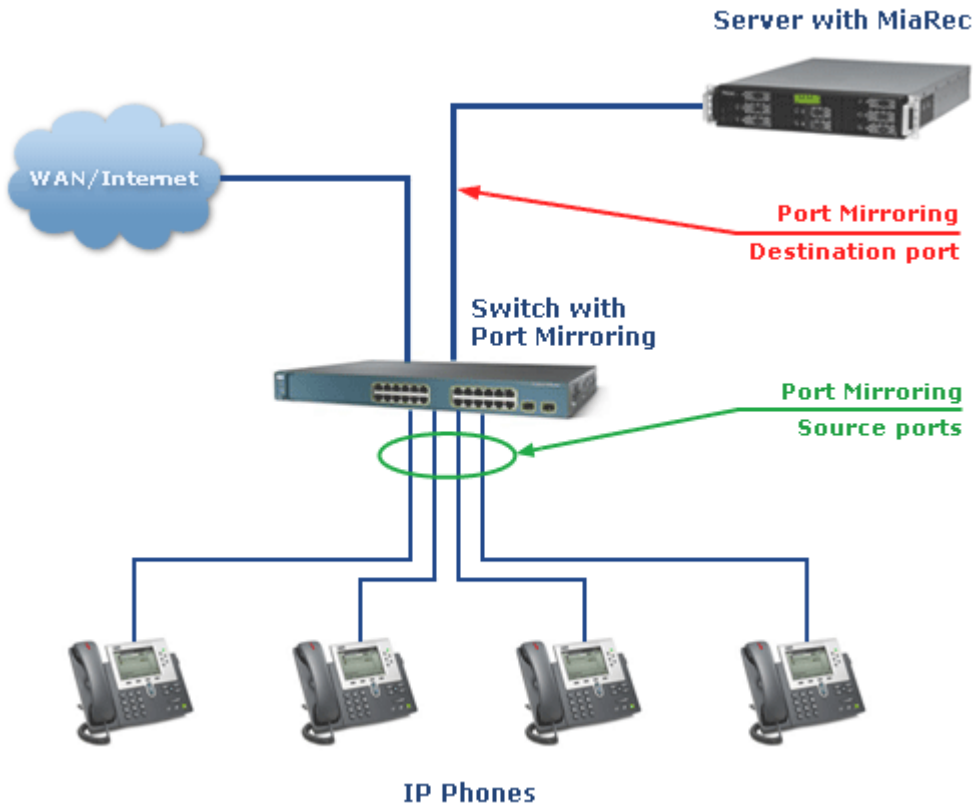
To disable IP-IP Direct Audio for all IP phones inside the IP network region, enter the **"change ip-network-region N"** command, where **N** is an existing network region used for the agents' ip phones and softphones and change **"Intra-region IP-IP Direct Audio"** and **"Inter-region IP-IP Direct Audio"** to **"no"**.

Parameter **"IP Audio Hairpinning"** is recommended to set to **"y"**.

```
change ip-network-region 1                               Page 1 of 19
                                     IP NETWORK REGION
Region: 1
Location:                               Authoritative Domain: voip.example.com
Name:
MEDIA PARAMETERS                               Intra-region IP-IP Direct Audio: no
  Codec Set: 1                               Inter-region IP-IP Direct Audio: no
  UDP Port Min: 2048                         IP Audio Hairpinning? y
  UDP Port Max: 3029
DIFFSERV/TOS PARAMETERS                       RTCP Reporting Enabled? y
  Call Control PHB Value: 34                 RTCP MONITOR SERVER PARAMETERS
  Audio PHB Value: 46                       Use Default Server Parameters? y
  Video PHB Value: 26
```

Alternatively, instead of changing "IP-IP Direct Audio" parameter, you can change port mirroring configuration and mirror each IP phone's port rather than CLAN and MedPro ports (see below network diagram).

Such configuration of port mirroring allows a recording of internal calls without changing of "IP-IP Direct Audio" parameter.



3.3.5 3.5. Administer System Parameters Features

Enter the **"change system-parameters features"** command. Navigate to **Page 5**, and verify that **Create Universal Call ID (UCID)** has value **"y"**. If not, then set it to **"y"** and set **UCID Network Node ID** to an unassigned node ID.

```
change system-parameters features                       Page 5 of 17
                                     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:

SEND ALL CALLS OPTIONS

Send All Calls Applies to: station

Auto Inspect on Send All Calls? n

UNIVERSAL CALL ID

Create Universal Call ID (UCID)? y

UCID Network Node ID: 9999

Copy UCID for Station Conference/Transfer? n

Navigate to **Page 13**, and set **Send UCID to ASAI** to **"y"**. This parameter allows for the universal call ID to be sent to MiaRec call recording application.

change system-parameters features

Page 13 of 17

FEATURE-RELATED SYSTEM PARAMETERS

CALL CENTER MISCELLANEOUS

Clear Callr-info: next-call

Allow Ringer-off with Auto-Answer? n

Reporting for PC Non-Predictive Calls? n

ASAI

Copy ASAI UUI During Conference/Transfer? n

Call Classification After Answer Supervision? n

Send UCID to ASAI? y

3.4 4. Configure Avaya Application Enablement Services

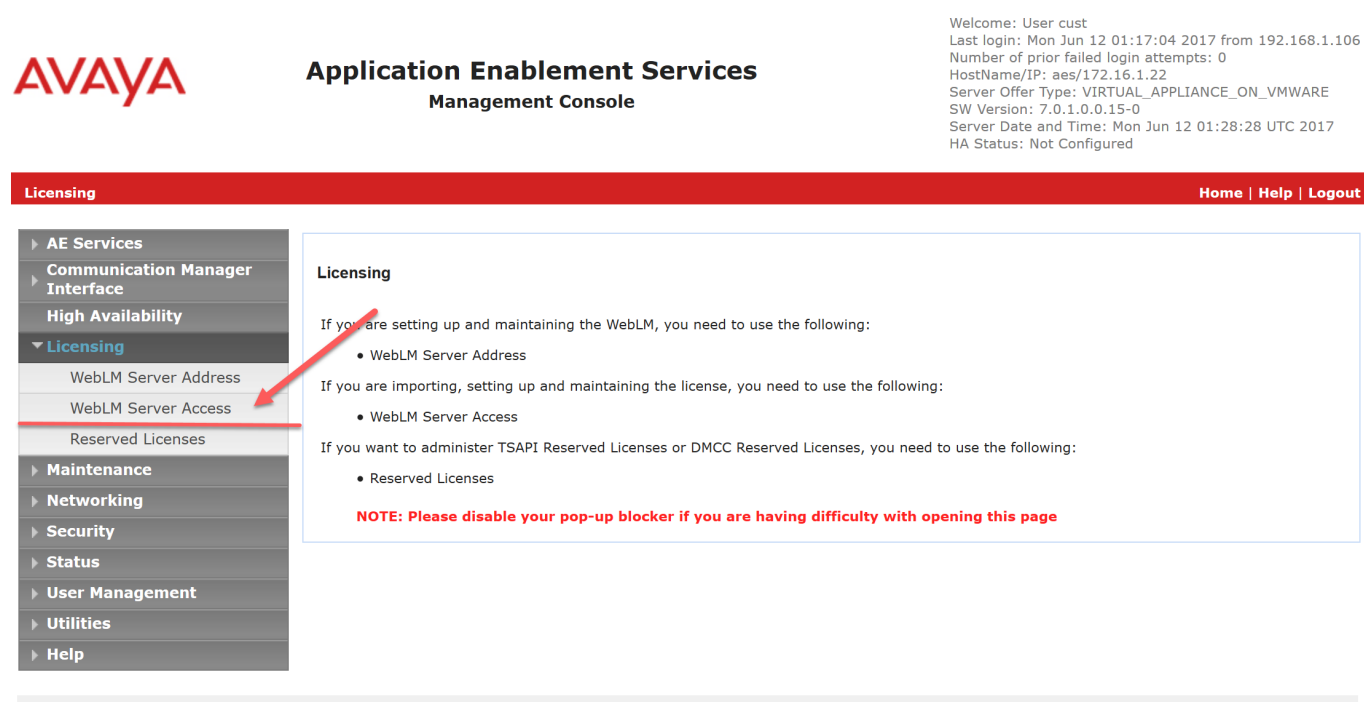
This section provides the procedures for configuring Avaya Application Enablement Services. The procedures include the following areas:

- Verify TSAPI service licensing
- Administer TSAPI link
- Obtain Tlink name
- Administer CTI user for MiaRec

3.4.1 4.1. Verify TSAPI service licensing

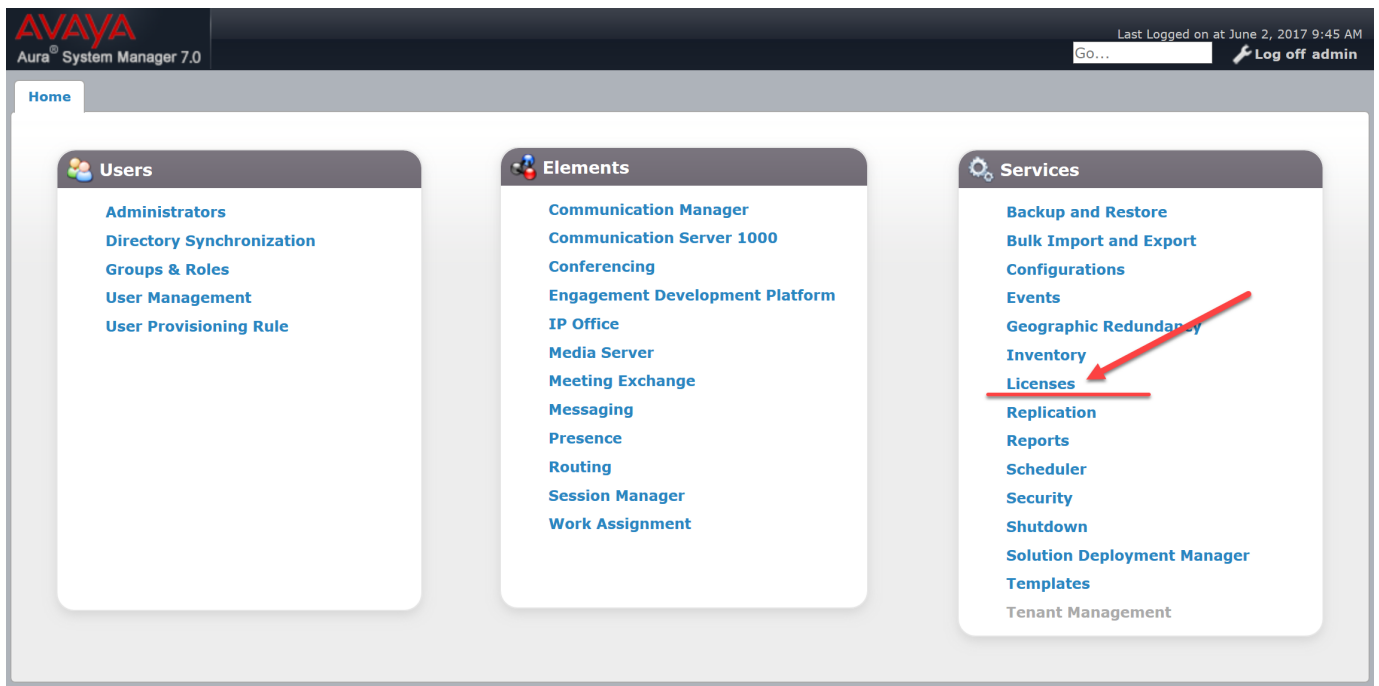
Prior to any administration, verify that the TSAPI service has been licensed properly. Open the AES OAM web interface by browsing to "https://ip-address-or-dns", where "ip-address-or-dns" is the IP address or DNS alias of the Appliation Enabledment Services server, and log in using the appropriate credentials (not shown).

Select **Licensing -> WebLM Server Access** in the left pane, to display the **Web License Manager** pop-up screen (not shown), and log in using the appropriate credentials.



Copyright Â© 2009-2016 Avaya Inc. All Rights Reserved.

If the licenses are managed centrally on the System Manager, then select **Services -> Licenses** in the System Manager home screen. Otherwise, the **Web License Manager** screen is shown immediately.



In the **Web License Manager** screen, select **Application_Enablement** under **Licenses Products** to display license capacity and current usage.

Make certain that a number of **TSAPI Simultaneous Users** (licenses) is enough. MiaRec requires TSAPI Basic license for each recorded IP Phone and softphone and for each monitored ACD Split (Hunt Group). If the TSAPI service is not licensed, contact the Avaya sales team or business partner for a proper license file.

WebLM Home	Application Enablement (CTI) - Release: 7 - SID: 10503000 (Enterprise license file)
Install license	You are here: Licensed Products > Application_Enablement > View by Feature
Licensed products	License installed on: June 2, 2017 9:47:35 AM -07:00
APPL_ENAB	
▶ Application_Enablement	
CE	
▶ COLLABORATION_ENVIRONMENT	
CMM	
▶ Communication_Manager_Messaging	
Configure Centralized Licensing	
COMMUNICATION_MANAGER	
▶ Communication_Manager	
▶ Call_Center	
Configure Centralized Licensing	
MSR	
▶ Media_Server	
PRESENCE_SERVICES	
▶ Presence_Services	
SessionManager	
▶ SessionManager	
Uninstall license	
Server properties	
Shortcuts	
Help for Installed Product	

Feature (License Keyword)	License Capacity	Currently available
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	16	16
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	1000	1000
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	3	3
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	16	16
Product Notes (VALUE_NOTES)	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiSmallServer MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_8832_vm;CtiMediumServer LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;unknown;CtiLargeServer TrustedApplications: IPS_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XM_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; PC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; OSPC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; VP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AES_UNIFIED_CC_DESKTOP,; CCE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T1_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T2_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; AVAYAVRINT_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CCT_ELITE_CALL_CTRL_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents; ANAV_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents; UNIFIED_DESKTOP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents; AACC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents; CE_AGENT_STATES_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents; TP_CLIENT_001, BasicUnrestricted, , , AgentEvents; EXT_CLIENT_001, , , , AgentEvents; EXT_CLIENT_002, , , , AgentEvents; EXT_CLIENT_003, , , , AgentEvents; EXT_CLIENT_004, , , , AgentEvents; EXT_CLIENT_005, , , , AgentEvents; AAWFO_SELECT_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted;	Not counted
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	3	3
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	1000	994
DLG (VALUE_AES_DLG)	16	16
Device Media and Call Control (VALUE_AES_DMCC_DMC)	1000	1000
AES ADVANCED MEDIUM SWITCH (VALUE_AES_AEC_MEDIUM_ADVANCED)	3	3

3.4.2 4.2. Administer TSAPI link

To administer a TSAPI link, select **AE Services -> TSAPI -> TSAPI Links** from the left pan of the **Management Console**. The **TSAPI Links** screen is displayed, as shown below. If the TSAPI Link is not configured yet, then click **Add Link** to create one.



Application Enablement Services Management Console

Welcome: User cust
Last login: Mon Jun 12 01:17:04 2017 from 192.168.1.106
Number of prior failed login attempts: 0
HostName/IP: aes/172.16.1.22
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.0.15-0
Server Date and Time: Mon Jun 12 01:32:42 UTC 2017
HA Status: Not Configured

AE Services | TSAPI | TSAPI Links
Home | Help | Logout

▼ AE Services

- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▼ TSAPI
 - TSAPI Links
 - TSAPI Properties
- ▶ TWS

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
<input checked="" type="radio"/> 1	cm2	1	7	Unencrypted

Add Link
Edit Link
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 "cm2" is selected. For **Switch CTI Link Number**, select the CTI Link number from **Section 3.1**. Make sure that **ASAI Link Version** is 6 or higher. Retain the default values in the remaining fields.



Application Enablement Services Management Console

Welcome: User cust
Last login: Mon Jun 12 01:17:04 2017 from 192.168.1.106
Number of prior failed login attempts: 0
HostName/IP: aes/172.16.1.22
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.0.15-0
Server Date and Time: Mon Jun 12 01:34:52 UTC 2017
HA Status: Not Configured

AE Services | TSAPI | TSAPI Links
Home | Help | Logout

▼ AE Services

- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▼ TSAPI
 - TSAPI Links
 - TSAPI Properties
- ▶ TWS

Add TSAPI Links

Link
2

Switch Connection
cm2

Switch CTI Link Number
1

ASAI Link Version
7

Security
Unencrypted

Apply Changes
Cancel Changes

3.4.3 4.3. Obtain Tlink name

Select **Security** -> **Security Database** -> **Tlinks** from the left pane. The **Tlinks** screen shows a listing of the Tlink names. Locate the Tlink Name associated with the switch connection to Avaya Communication Manager. 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 the MiaRec server.

In this case, the associated Tlink name is "AVAYA#CM2#CSTA#AES". Note the use of the switch connection "CM2" from **Section 4.2** as part of the Tlink name.

If Tlink doesn't exist, then follow instructions in **AE Services Administration** in document **Application Enablement Services Administration and Maintenance Guide** available at <http://support.avaya.com>



Application Enablement Services Management Console

Welcome: User cust
Last login: Mon Jun 12 01:28:24 2017 from 192.168.1.106
Number of prior failed login attempts: 0
HostName/IP: aes/172.16.1.22
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.0.15-0
Server Date and Time: Mon Jun 12 02:49:03 UTC 2017
HA Status: Not Configured

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

Tlinks

Tlink Name

☒ AVAYA#CM2#CSTA#AES[Delete Tlink](#)

3.4.4 4.4. Administer CTI user for MiaRec

Select **User Management -> 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**. Retain the default value of **"None"** for **Avaya Role**, and select **"Yes"** from the **CT User** drop-down list. Click **Apply** at the bottom of the screen (not shown below). Make a note of the User Id and Password, to be used later for configuring the MiaRec server.



Application Enablement Services Management Console

Welcome: User cust
Last login: Mon Jun 12 01:28:24 2017 from 192.168.1.106
Number of prior failed login attempts: 0
HostName/IP: aes/172.16.1.22
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.0.15-0
Server Date and Time: Mon Jun 12 02:40:09 UTC 2017
HA Status: Not Configured

User Management | User Admin | Add User

Home | 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 Id	miarec
* Common Name	miarec
* Surname	miarec
* 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	

Next, you need to change the security level for the CTI User as it needs to have unrestricted access privileges.

Select **Administration -> Security Database -> CTI Users -> List All Users** from the left pane. Choose the previously created CTI user, and click **Edit**.



Application Enablement Services Management Console

Welcome: User cust
Last login: Mon Jun 12 01:28:24 2017 from 192.168.1.106
Number of prior failed login attempts: 0
HostName/IP: aes/172.16.1.22
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.0.15-0
Server Date and Time: Mon Jun 12 02:44:07 UTC 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**
 - Control
 - CTI Users**
 - List All Users**
 - Search Users
 - Devices

CTI Users

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

Edit List All

The **Edit CTI User** screen appears. Tick the **Unrestricted Access** box and **Apply Changes** at the bottom of the screen.



Application Enablement Services Management Console

Welcome: User cust
Last login: Mon Jun 12 01:28:24 2017 from 192.168.1.106
Number of prior failed login attempts: 0
HostName/IP: aes/172.16.1.22
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.0.15-0
Server Date and Time: Mon Jun 12 02:45:12 UTC 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**
 - Control
 - ▣ **CTI Users**
 - **List All Users**
 - Search Users
 - Devices

Edit CTI User

User Profile:	User ID	miarec
	Common Name	miarec
	Worktop Name	NONE ▾
	Unrestricted Access	<input checked="" type="checkbox"/>
Call and Device Control:	Call Origination/Termination and Device Status	Any ▾
Call and Device Monitoring:	Device Monitoring	Any ▾
	Calls On A Device Monitoring	Any ▾
	Call Monitoring	<input checked="" type="checkbox"/>
Routing Control:	Allow Routing on Listed Devices	None ▾
<input type="button" value="Apply Changes"/> <input type="button" value="Cancel Changes"/>		

3.5 5. Configure MiaRec Call Recording System

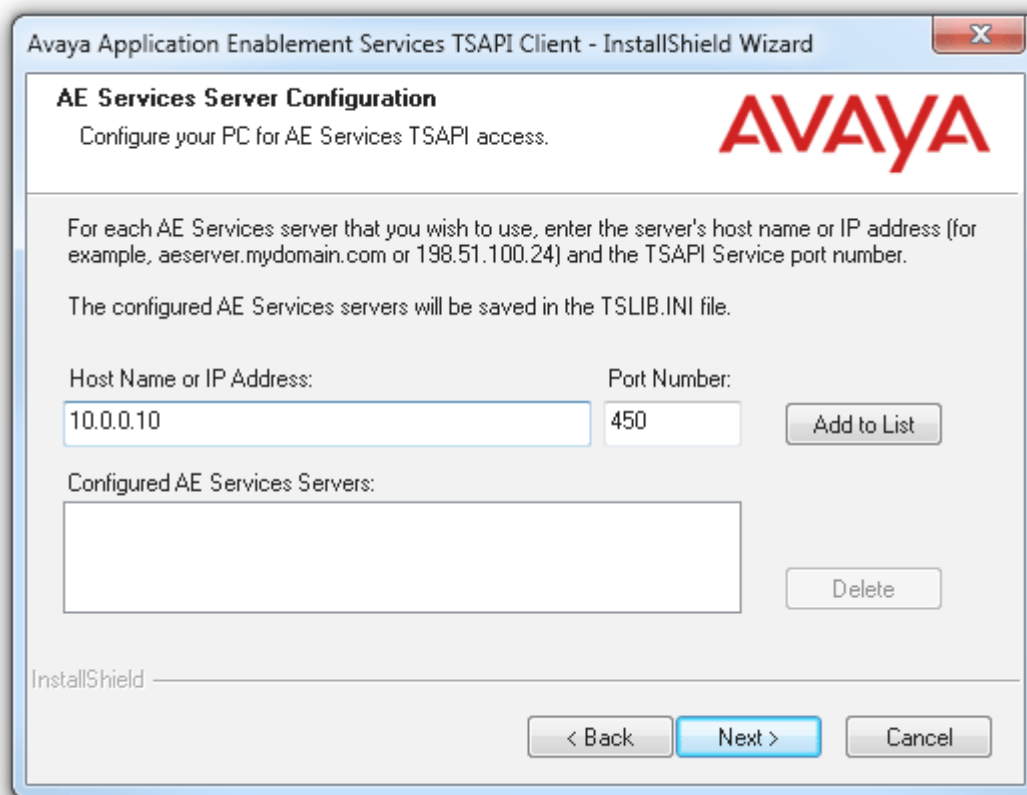
This section presents configuration steps for MiaRec call recording system. It is assumed that MiaRec is already installed on the server. The procedures include the following areas:

- Install AES TSAPI Client
- Administer MiaRec TSAPI link to AES

3.5.1 5.1. Install AES TSAPI Client

Download Application Enablement Services TSAPI Client from <http://support.avaya.com>

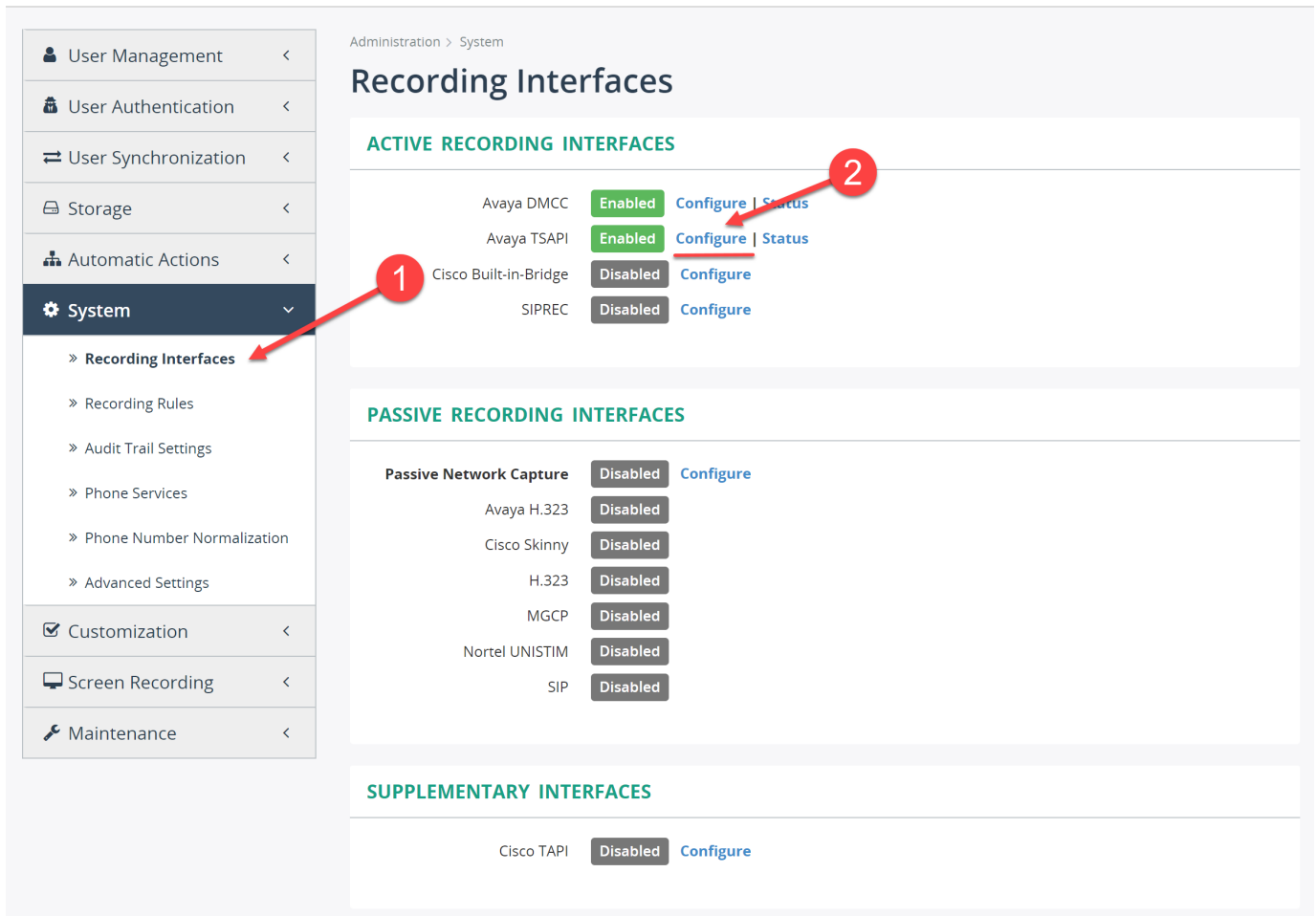
Install it on MiaRec server. During installation enter the IP address of the Avaya AES server in the **Host Name or IP Address** field, retaining the default port of 450 (see below screenshot). Click **Add to List** and then **Next** to finish installation.



3.5.2 5.2. Administer MiaRec link to AES

Navigate in the MiaRec web interface to **Administration -> System -> Recording Interfaces** and click the **Configure** link for the **Avaya TSAPI** interface.

Administration



Administration > System

Recording Interfaces

ACTIVE RECORDING INTERFACES

Interface	Status	Actions
Avaya DMCC	Enabled	Configure Status
Avaya TSAPI	Enabled	Configure Status
Cisco Built-in-Bridge	Disabled	Configure
SIPREC	Disabled	Configure

PASSIVE RECORDING INTERFACES

Interface	Status	Actions
Passive Network Capture	Disabled	Configure
Avaya H.323	Disabled	
Cisco Skinny	Disabled	
H.323	Disabled	
MGCP	Disabled	
Nortel UNISTIM	Disabled	
SIP	Disabled	

SUPPLEMENTARY INTERFACES

Interface	Status	Actions
Cisco TAPI	Disabled	Configure

In the **Configure Recording Interface (Avaya TSAPI)** screen, configure the following settings:

- Option **Enable** should be checked.
- Option **TSAPI Link** should point to the obtained TLink in the **Section 3.5. Obtain Tlink name**.
- Option **TSAPI login** and "TSAPI password**" should be set to the credentials of CTI user created in **Section 3.6. Administer CTI user for MiaRec**.
- Option **Media Source** should be set to **Passive - port mirroring**.
- Option **Monitored phones** should list all recorded extensions, comma-separated. A range of extensions is supported, like 3000-3100, 5001, 5002.
- Option **Monitored ACD Splits** should list all ACDs, which the recorded users may login to. MiaRec monitors ACDs for login/logout events. A range value is supported, like 4900-49100, 55000, 56000.
- Option **Ignore dialing phase** could be enabled to avoid recording of initial dialing phase of the outgoing call scenario.
- Retain default settings for other values.

Administration > System > Recording Interfaces

Configure Recording Interface

Enable *

☒ Enable Avaya TSAPI recording

TSAPI Link

AVAYA#CM2#CSTA#AES

TSAPI link, like AVAYA#SWITCH1#CSTA#SERVERNAME1

TSAPI login

miarec

TSAPI account name

TSAPI password

.....

TSAPI account password

Media Source

☒ Passive - port mirroring

☐ DMCC

Monitored phones

3000-3100,5001,5002

A range of monitored phones (comma-separated). Example: 3000-3100,5001,5002

Monitored ACD Splits

49000-49100,55000,56000

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.

3.5.3 5.2. Enable passive recording

Navigate in the MiaRec web interface to **Administration -> System -> Recording Interfaces** and enable the following protocols:

- Passive network capture
- Avaya H.323
- H.323
- SIP (required if some of phones have SIP firmware)

Administration

User Management <

User Authentication <

User Synchronization <

Storage <

Automatic Actions <

System >

» Recording Interfaces

» Recording Rules

» Audit Trail Settings

» Phone Services

» Phone Number Normalization

» Advanced Settings

Customization <

Screen Recording <

Maintenance <

Administration > System

Recording Interfaces

ACTIVE RECORDING INTERFACES

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

PASSIVE RECORDING INTERFACES

Passive Network Capture	Enabled	Configure
Avaya H.323	Enabled	Configure
Cisco Skinny	Disabled	Configure
H.323	Enabled	Configure
MGCP	Disabled	Configure
Nortel UNISTIM	Disabled	Configure
SIP	Disabled	Configure

3.6 6. Verification

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

3.6.1 6.1. Verify Avaya Communication Manager

On Avaya Communication Manager, verify the status of the administered CTI links by using the **"status aescvs cti-link"** command. The link status should show **"no"** for maintenance busy (**Mnt Busy**) and the **Service State** should indicate **"established"**.

```
status aescvs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	4	no	aes-server1	established	15	15

The **"status aescvs interface"** command should indicate the interface is **listening**.

```
status aescvs interface
```

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

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

```
status aescvs link
```

AE SERVICES LINK STATUS						
Srvr/ Link	AE Services Server	Remote IP	Remote Port	Local Node	Msgs Sent	Msgs Rcvd
01/01	aes-server1	10.0.0.25	43909	procr	224	209

Once the MiaRec call recording application is running, the **"list monitored-station"** command will show each station, which is monitored by MiaRec via TSAPI interface.

```
list monitored-station
```

MONITORED STATION							
Station Ext	Association 1 CTI Link	CRV	Association 2 CTI Link	CRV	Association 3 CTI Link	CRV	Association 4 CTI Link
32129	1	10					
32130	1	9					
32131	1	22					
32132	1	7					

3.6.2 6.2. Verify Avaya Application Enablement Services

On Application Enablement Services, verify the status of the switch connection by selecting **Status -> Status and Control -> Switch Conn Summary** from the left pane. Verify that the **Conn State** is **"Talking"** for the switch connection associated with Avaya Communication Manager, and that the **Associations** column reflects the total number of monitored skill groups and agent stations as configured previously.



Application Enablement Services Management Console

Welcome: User cust
Last login: Mon Jun 12 21:23:45 2017 from 192.168.1.106
Number of prior failed login attempts: 0
HostName/IP: aes/172.16.1.22
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.0.15-0
Server Date and Time: Mon Jun 12 22:22:49 UTC 2017
HA Status: Not Configured

Status | Status and Control | Switch Conn 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
 - User Management

Switch Connections Summary

☐ Enable page refresh every 60 seconds

	Switch Conn	Conn State	Processor Ethernet	Since	Online/Offline	Active/Standby/ Admin'd TEP Conns	Num of TCI Conns	SSL	Msgs To Switch	Msgs From Switch	Msg Period
<input checked="" type="radio"/>	cm2	Talking	Yes	Tue Jun 6 14:51:55 2017	Online	1 / 0 / 1	2	Enabled	615	630	30

Online Offline Connection Details Per Service Connections Details

Verify the status of the TSAPI link by selecting **Status -> Status and Control -> TSAPI Service Summary** from the left pane. Verify the **Conn Status** is **"Talking"** as shown below.



Application Enablement Services Management Console

Welcome: User cust
Last login: Mon Jun 12 21:23:45 2017 from 192.168.1.106
Number of prior failed login attempts: 0
HostName/IP: aes/172.16.1.22
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.0.15-0
Server Date and Time: Mon Jun 12 22:24:06 UTC 2017
HA Status: Not Configured

Status | Status and Control | TSAPI 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**
 - User Management

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	cm2	1	Talking	Tue Jun 6 14:51:55 2017	Online	17	6	15	15	30

Online Offline

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

TSAPI Service Status TLink Status User Status

Verify the status of the CTI User by selecting **Status -> Status and Control -> TSAPI Service Summary** from the left pane. Click the **User Status** button (not shown below). The **CTI User Status** screen is displayed. Verify that an open session exists for the CTI user created for MiaRec as shown below. This verification step assumes that MiaRec application is configured properly and running.



Application Enablement Services Management Console

Welcome: User cust
Last login: Mon Jun 12 21:23:45 2017 from 192.168.1.106
Number of prior failed login attempts: 0
HostName/IP: aes/172.16.1.22
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.0.15-0
Server Date and Time: Mon Jun 12 22:28:54 UTC 2017
HA Status: Not Configured

[Status](#) | [Status and Control](#) | [TSAPI 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**

CTI User Status

☐ Enable page refresh every secondsCTI Users

Open Streams 3

Closed Streams 50

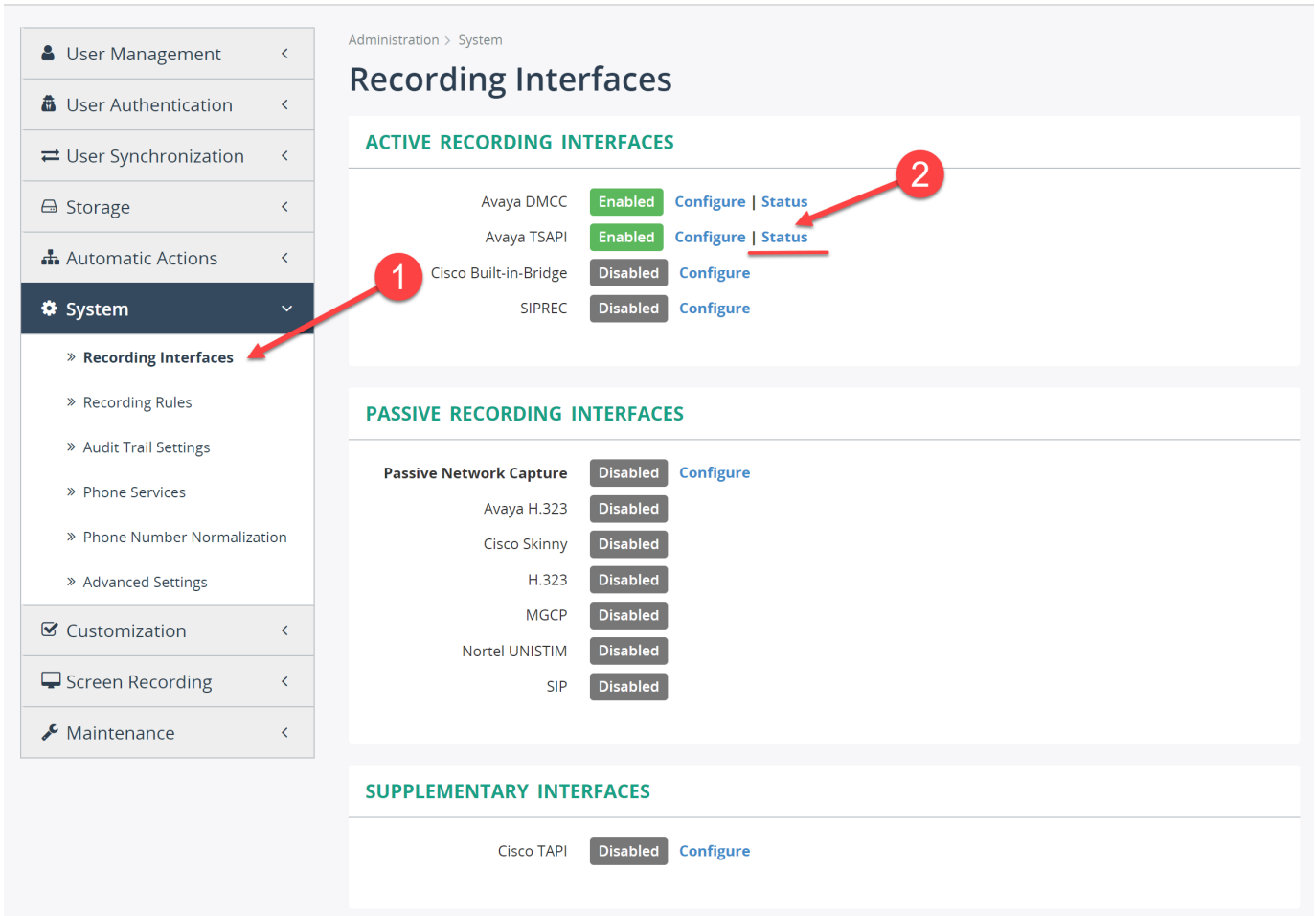
Open Streams

Name	Time Opened	Time Closed	Tlink Name
miarec	Mon 12 Jun 2017 09:41:57 PM UTC		AVAYA#CM2#CSTA#AES
DMCCLCSUserDoNotModify	Tue 06 Jun 2017 02:51:44 PM UTC		AVAYA#CM2#CSTA#AES
DMCCLCSUserDoNotModify	Tue 06 Jun 2017 02:51:44 PM UTC		AVAYA#CM2#CSTA#AES

3.6.3 6.3. Verify TSAPI device monitoring status in MiaRec

Navigate in the MiaRec web interface to **Administration -> System -> Recording Interfaces** and click the **Status** link for the **Avaya TSAPI** interface.

Administration



Administration > System

Recording Interfaces

ACTIVE RECORDING INTERFACES

Interface	Status	Actions
Avaya DMCC	Enabled	Configure Status
Avaya TSAPI	Enabled	Configure Status
Cisco Built-in-Bridge	Disabled	Configure
SIPREC	Disabled	Configure

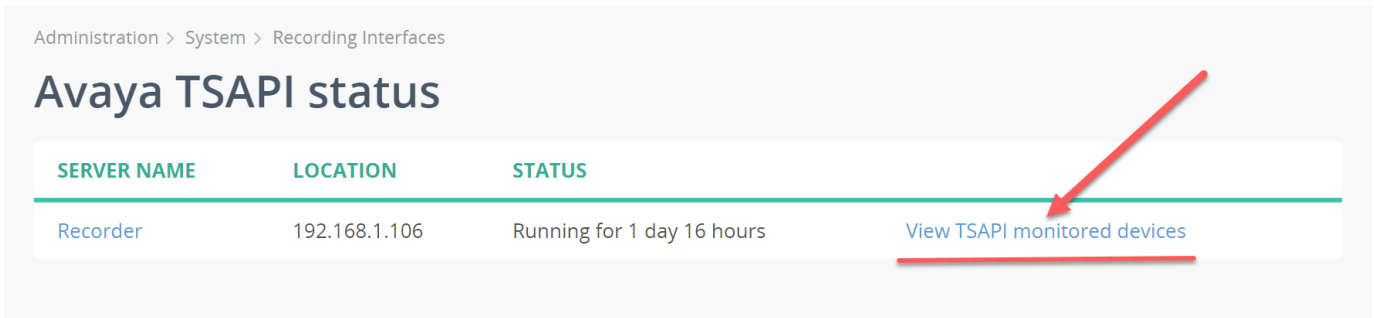
PASSIVE RECORDING INTERFACES

Interface	Status	Actions
Passive Network Capture	Disabled	Configure
Avaya H.323	Disabled	
Cisco Skinny	Disabled	
H.323	Disabled	
MGCP	Disabled	
Nortel UNISTIM	Disabled	
SIP	Disabled	

SUPPLEMENTARY INTERFACES

Interface	Status	Actions
Cisco TAPI	Disabled	Configure

In the **Avaya TSAPI status** screen, click the **View TSAPI monitored devices** link for the appropriate recorder instance (the screenshot below shows one instance).



Administration > System > Recording Interfaces

Avaya TSAPI status

SERVER NAME	LOCATION	STATUS	
Recorder	192.168.1.106	Running for 1 day 16 hours	View TSAPI monitored devices

In the **Avaya TSAPI monitored devices** screen, verify the status of the monitored devices. If any of devices shows a **failed** state, then click the extension link in that window to see the detailed error message.

Administration > System > Recording Interfaces > Avaya TSAPI status

Avaya TSAPI monitored devices

Recorder Name: **Recorder**Host IP: **192.168.1.106**Status: **Running for 1 day 17 hours**

Monitored Devices

Search by Extension

Search



0-7 of 7



EXTENSION	DEVICE NAME	AGENT ID	AGENT NAME	MONITOR STATE	TSAPI IP	ACTIVE CALLS	TOTAL CALLS	LAST EVENT TIME
3001	User Two			active	192.168.1.104	1	4	1 minute 10 seconds ago
3000	Phone One			active	192.168.1.103	1	5	1 minute 10 seconds ago
49000				failed		0	0	5 seconds ago
3003	User 3003			active		0	0	5 seconds ago
3002	User 3			active		0	0	5 seconds ago

The error message describes the actual reasons of failure. Read the message and apply appropriate corrections. For example, the message in the following screenshot says that device identifier (extension) is not valid. In this case, remove this extension from the **Monitored Phones** list in configuration.

Administration > System > Recording Interfaces > Avaya TSAPI status > Recorder DEV1

Avaya TSAPI monitored device

Extension: **49000**Media Source: **dmcc**

Device Name

Agent ID

Agent Name

Monitor State **failed**

H.323 IP

TSAPI IP

Active Calls **0**Total Calls **0**Last Event Time **1 minute 6 seconds ago**Monitor Start Time **1 minute 6 seconds ago**Error Code **12**

Error **INVALID_CSTA_DEVICE_IDENTIFIER (12) An invalid device identifier (extension) has been specified**

Recommendations **Check a list of monitored phones inside configuration file**

If the **Avaya TSAPI monitored devices** screen shows none of devices (neither successfully monitored nor failed), then probably the TSAPI link connection is not established to AES server. In this case, navigate to **Administration -> Maintenance -> System Log** and check any error messages. The screenshot below shows that the TSAPI login/password is invalid. Make the appropriate corrections to the configuration.

Wide view 

Administration

User Management <

User Authentication <

User Synchronization <

Storage <

Automatic Actions <

System <

Customization <

Screen Recording <

Maintenance <

» System Log

» System Status

Administration > Maintenance

System Log

2017/06/11 - 2017/06/11

Select a Severity

Select a Type

Search

Delete

0-1 of 1 < >

<input type="checkbox"/>	SEVERITY	DATE	SOURCE & TYPE	MESSAGE
<input type="checkbox"/>	Error	Today 4:55 PM	Recorder Protocol:Avaya::TSAPI	Failed to establish a connection to Avaya AES Server: TSERVER_BAD_PASSWORD_OR_LOGIN (25) The password, login, or both did not pass the TSAPI Service authentication checks. Check the TSAPI password and login settings inside configuration file

20 per page

0-1 of 1 < >

3.6.4 6.4. Check MiaRec trace log

MiaRec provides detailed logging for troubleshooting purposes. Navigate to **Administration -> Maintenance -> Troubleshooting** to enable log in MiaRec.

3.7 7. Additional references

- **Administering Avaya Communication Manager** (available at <http://support.avaya.com>)
- **Application Enablement Services Administration and Maintenance Guide** (available at <http://support.avaya.com>)
- **Application Enablement Services TSAPI, JTAPI and CVLAN Client and SDK Installation Guide** (available at <http://support.avaya.com>)