



Avaya Solution & Interoperability Test Lab

Application Notes for Verint® Workforce Optimization Version 15.2 with Avaya Aura® Communication Manager R7.1 and Avaya Aura® Application Enablement Services R7.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Verint® Workforce Optimization to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services 7.1.2. Verint Workforce Management is a call recording solution.

In the compliance testing, Verint® Workforce Optimization used the Telephony Services Application Programming Interface from Avaya Aura® Application Enablement Services to monitor contact center devices on Avaya Aura® Communication Manager, and used the Device, Media, and Call Control interface from Avaya Aura® Application Enablement Services along with the Single Step Conference feature to capture media associated with the monitored agents for call recording.

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

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

1. Introduction

These Application Notes describe the configuration steps required for Verint® Workforce Optimization to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services 7.1.2. Verint Workforce Optimization is a call recording solution.

In the compliance testing, Verint Workforce Optimization used the Telephony Services Application Programming Interface (TSAPI) from Avaya Aura® Application Enablement Services to monitor contact center devices on Avaya Aura® Communication Manager, and used the Device, Media, and Call Control (DMCC) interface from Avaya Aura® Application Enablement Services along with the Single Step Conference feature to capture media associated with the monitored agents for call recording.

The TSAPI interface is used by Verint Workforce Optimization to monitor skill groups and agent station extensions, and the DMCC interface is used by Verint Workforce Optimization to register virtual IP softphones. When there is an active call at the monitored agent, Verint Workforce Optimization is informed of the call via event reports from the TSAPI interface. Verint Workforce Optimization starts the call recording by using the Single Step Conference feature from the TSAPI interface to add a virtual IP softphone to the active call to obtain the media. The TSAPI event reports are also used to determine when to stop the call recordings.

2. General Test Approach and Test Results

The feature test cases were performed manually. Upon start of the Workforce application, the application automatically registers the virtual IP softphones to Communication Manager using DMCC, and requests monitoring for the skill groups and agent stations using TSAPI.

Each call was handled manually on the agent with generation of unique audio content for the recordings. Necessary user actions such as hold and reconnect were performed from the agent telephones to test the different call scenarios.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet cable to Workforce server.

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

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

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

For the testing associated with these Application Notes, the interface between Avaya systems and Verint Workforce Optimization did not include use of any specific encryption features as requested by Verint.

The encryption (TLS/SRTP) is used only between Avaya Aura systems.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. The feature testing focused on verifying the following on Workforce:

- Handling of TSAPI messages in the areas of event notification and value queries.
- Use of DMCC registration services to register the virtual IP softphones.
- Use of TSAPI call control services to activate Single Step Conference for the virtual IP softphones.
- Use of DMCC monitoring services and media control events to obtain the media from the virtual IP softphones.
- Proper recording, logging, and playback of calls for scenarios involving inbound, outbound, internal, external, ACD, non-ACD, hold, reconnect, simultaneous, conference, and transfer.

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

2.2. Test Results

All test cases were executed and verified. The following were observations on Workforce from the compliance testing.

- The internal call from H.323 station to SIP station (either one of them is monitored station or both are monitored stations by Verint call recording application) sometimes cannot be recorded. The reason is because a collision between SIP shuffling and SSC requests from call recording adjunct, CM denies SSC request on call when SIP shuffling is in progress. CM can delay the start of a shuffle up to 100ms, and the shuffle may take 200ms due to SIP delays that means that when a SSC request comes in less than 300ms after a call is answered, it can collide with the shuffle sequence. The SSC wants to add a new party to an existing call so a conference connection must be created. The workaround for this issue is to disable the shuffling on SIP signaling group used by SIP phone.

2.3. Support

Technical support on Workforce Optimization can be obtained through the following:

- **Phone:** (866) 787-2020
- **Email:** ESSupport@verint.com
- **Web:** <http://online.verint.com>

3. Reference Configuration

Figure 1 illustrates the compliance test configuration consisting of:

- Avaya Aura® Communication Manager R7.0
- Avaya Aura® Application Enablement Services R7.0
- Various IP, Digital, and analog endpoints
- Verint Workforce server installed on a standalone machine

In the compliance testing, Workforce Optimize monitored the skill group and agent station extensions shown in the table below.

Device Type	Extension
VDN	3340
Skill Group	3320
Supervisor Station	3301, 3403
Agent Station	3303, 3401
Agent ID	1000, 1001

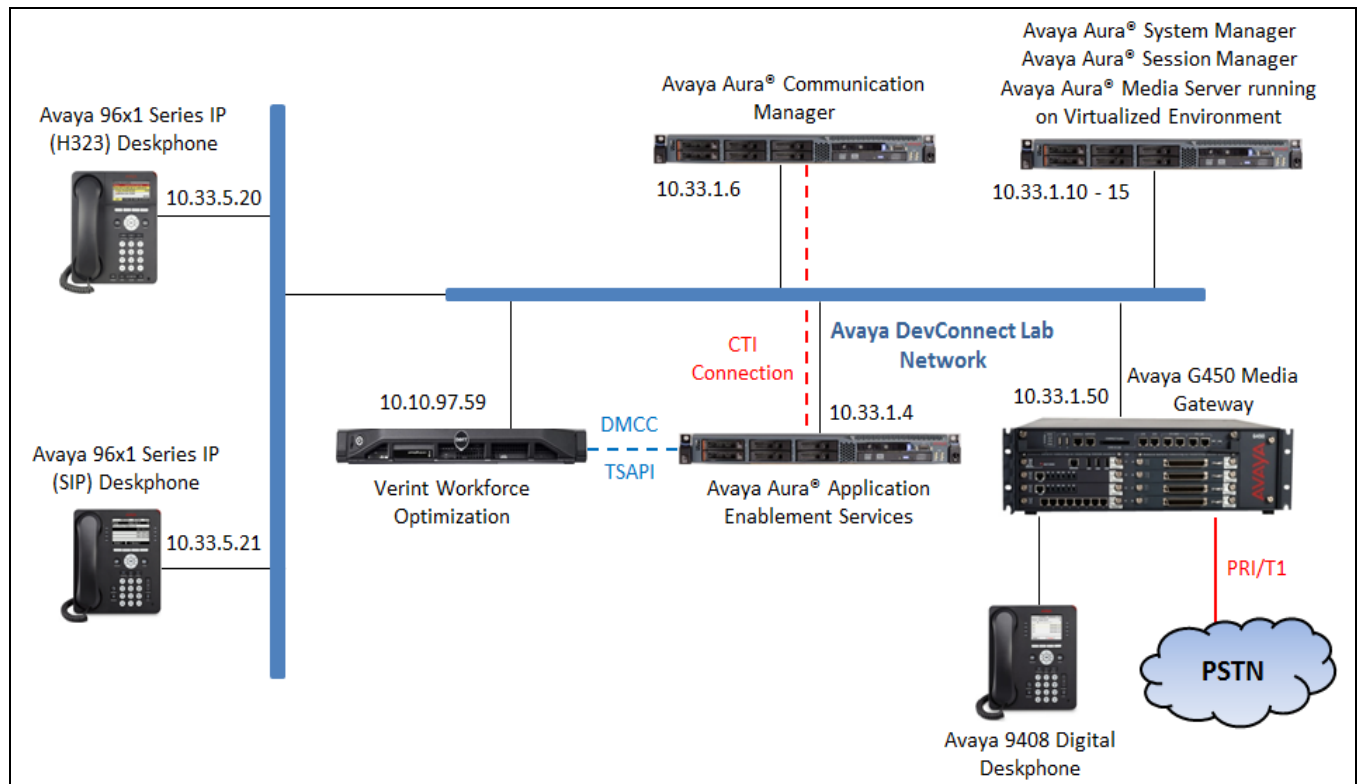


Figure 1 – Verint Workforce Optimization Test Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on virtualized environment	7.1.2.0.0.532 – FP2
Avaya Aura® Application Enablement Services running on virtualized environment	7.1.2.0.0.3
Avaya Aura® Session Manager running on virtualized environment	7.1.2.0.712004
Avaya Aura® System Manager	7.1.2.0.057353
Avaya Aura® Media Server	7.7.0.359
Avaya G450 Media Gateway	FW 38 .21 .0
Avaya 96x1 Series IP Telephone <ul style="list-style-type: none">• 96x1 (H.323)• 96x1 (SIP)	6.6506 7.1.1.0.9
Avaya 1416 Digital Telephones	FW 1
2500 analog phone	-
Verint® Workforce Optimization running on Windows 2012 Standard Server	15.2

5. Configure Avaya Aura® Communication Manager

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

- Verify Feature and License for the integration
- Administer Communication Manager System Features
- Administer IP Services for Application Enablement Services
- Administer Computer Telephony Integration (CTI) Link
- Verify Recorded Extensions
- Add Virtual Stations

All the configuration changes in this section for Communication Manager are performed through the System Access Terminal (SAT) interface. For more details on configuring Communication Manager, refer to the Avaya product documentation in **Section 10**.

5.1. Verify Feature and License

Enter the **display system-parameters customer-options** command and ensure that **Computer Telephony Adjunct Links** is set to **y**. If this option is not set to **y**, contact the Avaya sales team or business partner for a proper license file.

```
display system-parameters customer-options                                Page 4 of 12
                                OPTIONAL FEATURES

Abbreviated Dialing Enhanced List? y      Audible Message Waiting? y
Access Security Gateway (ASG)? n           Authorization Codes? y
Analog Trunk Incoming Call ID? y           CAS Branch? n
A/D Grp/Sys List Dialing Start at 01? y    CAS Main? n
Answer Supervision by Call Classifier? y    Change COR by FAC? n
ARS? y      Computer Telephony Adjunct Links? y
ARS/AAR Partitioning? y      Cvg Of Calls Redirected Off-net? y
ARS/AAR Dialing without FAC? y      DCS (Basic)? y
ASAI Link Core Capabilities? n      DCS Call Coverage? y
ASAI Link Plus Capabilities? n      DCS with Rerouting? y
Async. Transfer Mode (ATM) PNC? n
Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? y
ATM WAN Spare Processor? n            DS1 MSP? y
ATMS? y      DS1 Echo Cancellation? y
Attendant Vectoring? y
```

(NOTE: You must logoff & login to effect the permission changes.)

Each recording port or virtual station extension the recorder will use to record agent phones will require an **IP_API_A** license if not licensed on Application Enablement Services.

```
display system-parameters customer-options                               Page 11 of 12
                                MAXIMUM IP REGISTRATIONS BY PRODUCT ID

Product ID  Rel. Limit      Used
AgentSC     * : 2400        0
IP_API_A   * : 2400        0
IP_Agent    * : 2400        0
```

5.2. Administer Communication Manager System Features

Enter the **change system-parameters features** command and ensure that on page 5 **Create Universal Call ID (UCID)** is enabled and a relevant **UCID Network Node ID** (1 was used in the test) is defined. Also ensure that on page 13 that **Send UCID to ASAI** is set to **y**. Workforce relies on UCID to track complex calls (Transfers and Conferences).

```
change system-parameters features                                     Page 5 of 19
                                FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS
  Endpoint:                      Lines Per Page: 60

SYSTEM-WIDE PARAMETERS
                                Switch Name:
                                Emergency Extension Forwarding (min): 10
                                Enable Inter-Gateway Alternate Routing? n
                                Enable Dial Plan Transparency in Survivable Mode? n
                                COR to Use for DPT: station
                                EC500 Routing in Survivable Mode: dpt-then-ec500
MALICIOUS CALL TRACE PARAMETERS
                                Apply MCT Warning Tone? n    MCT Voice Recorder Trunk Group:
                                Delay Sending RElease (seconds): 0
SEND ALL CALLS OPTIONS
  Send All Calls Applies to: station    Auto Inspect on Send All Calls? n
  Preserve previous AUX Work button states after deactivation? n
UNIVERSAL CALL ID
  Create Universal Call ID (UCID)? y    UCID Network Node ID: 1
```


change system-parameters features Page 13 of 19

FEATURE-RELATED SYSTEM PARAMETERS

CALL CENTER MISCELLANEOUS

Callr-info Display Timer (sec): 10

Clear Callr-info: next-call

Allow Ringer-off with Auto-Answer? n

Reporting for PC Non-Predictive Calls? n

Agent/Caller Disconnect Tones? n

Interruptible Aux Notification Timer (sec): 3

Zip Tone Burst for Callmaster Endpoints: double

ASAI

Copy ASAI UII During Conference/Transfer? n

Call Classification After Answer Supervision? n

Send UCID to ASAI? y

For ASAI Send DTMF Tone to Call Originator? y

Send Connect Event to ASAI For Announcement Answer? n

Prefer H.323 Over SIP For Dual-Reg Station 3PCC Make Call? n

5.3. Administer IP-Services for Application Enablement Services

Add an IP-Services entry for Application Enablement Services as described below:

- Enter the **change ip-services** command.
- In the **Service Type** field, type **AESVCS**.
- In the **Enabled** field, type **y**.
- In the **Local Node** field, type the Node name **procr** for the Processor Ethernet Interface.
- In the **Local Port** field, use the default of **8765**.

Note that if installations using CLAN connectivity, each CLAN interface would require similar configuration.

change ip-services Page 1 of 3

IP SERVICES

Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port
AESVCS	y	procr	8765		

On Page 3 of the IP Services form, enter the following values:

- In the **AE Services Server** field, type the host name of the Application Enablement Services server.
- In the **Password** field, type the same password to be administered on the Application Enablement Services server in **Section 6, Step 1**.
- In the **Enabled** field, type **y**.

change ip-services				Page	3 of	3
AE Services Administration						
Server ID	AE Services Server	Password	Enabled	Status		
1:	aes70	*	y	in use		
2:	aesvm63	*	y	idle		
3:	aesvm70	*	y	idle		
4:	aes7	*	y	idle		

5.4. Administer Computer Telephony Integration (CTI) Link

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

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

add cti-link 1		Page 1 of 3	
CTI LINK			
CTI Link: 1			
Extension: 3332			
Type: ADJ-IP			
Name: AES70			COR: 1

5.5. Verify Recorded Extensions

All stations (H.323 and Digital) that will be recorded using the Multiple Registration method must have **IP Softphone** enabled, and the application needs to know the **Security Code** in order to successfully register. For stations (SIP and Analog) that are unable to support Softphone, or which the administrator prefers to record using Single Step Conference, leave the **IP Softphone** setting disabled. Use the **display station n** command to verify information, or **change station n** to make changes if necessary.

display station 3301		Page 1 of 6
STATION		
Extension: 3301	Lock Messages? n	BCC: 0
Type: 9641	Security Code: *	TN: 1
Port: S00011	Coverage Path 1:	COR: 1
Name:	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: 3301	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english	Button Modules: 1	
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	

5.6. Add Virtual Stations

Virtual stations are used by Workforce to do Single Step Conference based call recording for stations. Add a virtual station using **the add station <n>** command; where <n> is an available extension number. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- In the **Type** field, enter a station type such as **9640**
- In the **Name** field, enter a descriptive name for e.g. **DMCC Station 1**
- In the **Security Code** field, enter a desired value
- Set the **IP SoftPhone** field to **y**


display station 3317		Page 1 of 5
STATION		
Extension: 3317	Lock Messages? n	BCC: 0
Type: 9640	Security Code: *	TN: 1
Port: S00019	Coverage Path 1:	COR: 1
Name: DMCC Station 1	Coverage Path 2:	COS: 1
	Hunt-to Station:	Tests? y
STATION OPTIONS		
Loss Group: 19	Time of Day Lock Table:	
	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 3317	
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	

6. Configure Avaya Aura® Application Enablement Services

All administration of Application Enablement Services is performed via a web browser. Enter <https://<ip-addr>> in the URL field of a web browser where <ip-addr> is the IP address of the Application Enablement Services server. After a login step, the **Welcome to OAM** page is displayed. Note that all navigation is performed by clicking links in the Navigation Panel on the left side of the screen, context panels will then appear on the right side of the screen.

The procedures fall into the following areas:

- Configure Communication Manager Switch Connections
- Configure TSAPI Link
- Obtain TSAPI Link
- Configure CT user
- Confirm TSAPI and DMCC Licenses

**Application Enablement Services**
Management Console

Welcome: User cust
Last login: Fri Jan 19 14:16:17 2018 from ntpsrv.bvwdev.co
Number of prior failed login attempts: 0
HostName/IP: aes70/10.33.1.4
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.2.0.0.3-0
Server Date and Time: Tue Jan 23 13:47:13 EST 2018
HA Status: Not Configured

Home

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Welcome to OAM

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

- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- High Availability - Use High Availability to manage AE Services HA.
- Licensing - Use Licensing to manage the license server.
- Maintenance - Use Maintenance to manage the routine maintenance tasks.
- Networking - Use Networking to manage the network interfaces and ports.
- Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.
- Status - Use Status to obtain server status informations.
- User Management - Use User Management to manage AE Services users and AE Services user-related resources.
- Utilities - Use Utilities to carry out basic connectivity tests.
- Help - Use Help to obtain a few tips for using the OAM Help system

Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain.

6.1. Configure Communication Manager Switch Connections

To add links to Communication Manager, navigate to the **Communication Manager Interface** → **Switch Connections** page and enter a name for the new switch connection (e.g. **interopCM**) and click the **Add Connection** button (not shown). The **Connection Details** screen is shown. Enter the **Switch Password** configured in **Section 5.3** and check the **Processor Ethernet** box if using the **procr** interface. Click **Apply**.

Communication Manager Interface | Switch Connections Home | Help | Logout

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

Connection Details - interopCM

Switch Password

Confirm Switch Password

Msg Period Minutes (1 - 72)

Provide AE Services certificate to switch ☒

Secure H323 Connection ☐

Processor Ethernet ☒

Apply Cancel

The display returns to the **Switch Connections** screen which shows that the **interopCM** switch connection has been added.

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services
Communication Manager Interface
Switch Connections
Dial Plan
High Availability
Licensing
Maintenance
Networking

Switch Connections

Add Connection

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> interopCM	Yes	30	1
<input type="radio"/> server1	Yes	30	1

Edit Connection Edit PE/CLAN IPs Edit H.323 Gatekeeper Delete Connection Survivability Hierarchy

Click the **Edit PE/CLAN IPs** button on the **Switch Connections** screen to configure the **procr** or **CLAN** IP Address(es) for TSAPI message traffic. The **Edit Processor Ethernet IP** screen is displayed. Enter the IP address of the **procr** interface and click the **Add/Edit Name or IP** button.

Communication Manager Interface | Switch Connections Home | Help | Logout

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

Edit Processor Ethernet IP - interopCM

10.10.1.6

Name or IP Address	Status
10.10.1.6	In Use

Click the **Edit H.323 Gatekeeper** button on the **Switch Connections** screen to configure the **procr** or **CLAN** IP Address(es) for DMCC registrations. The **Edit H.323 Gatekeeper** screen is displayed. Enter the IP address of the **procr** interface and click the **Add Name or IP** button.

Communication Manager Interface | Switch Connections Home | Help | Logout

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

Edit H.323 Gatekeeper - interopCM

Name or IP Address

☒ 10.10.1.6

6.2. Configure TSAPI Link

To configure a TSAPI link, select **AE Services** → **TSAPI** → **TSAPI Links** from the left pane. The TSAPI Links screen is displayed, as shown below. Click **Add Link**

The screenshot shows the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the text "Application Enablement Services Management Console". On the right, a welcome message for "User cust" is displayed, along with login details and system status. The main navigation bar shows "AE Services | TSAPI | TSAPI Links" and links for "Home | Help | Logout". The left sidebar lists "AE Services" with sub-items: CVLAN, DLG, DMCC, SMS, TSAPI (expanded), TSAPI Links (selected), TSAPI Properties, and TWS. The main content area is titled "TSAPI Links" and contains a table with the following data:

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
1	interopcm	1	7	Both

Below the table are three buttons: "Add Link", "Edit Link", and "Delete Link".

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 “interopcm” is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.4**. Retain the default values in the remaining fields, and click **Apply Changes**.

The screenshot shows the "Edit TSAPI Links" configuration page. The left sidebar is identical to the previous screenshot, with "TSAPI Links" selected. The main content area is titled "Edit TSAPI Links" and contains the following fields:

- Link: 1
- Switch Connection: interopcm (dropdown)
- Switch CTI Link Number: 1 (dropdown)
- ASAI Link Version: 7 (dropdown)
- Security: Both (dropdown)

At the bottom are three buttons: "Apply Changes", "Cancel Changes", and "Advanced Settings".

6.3. Obtain TSAPI Link

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

In this case, the associated unencrypted Tlink name is “AVAYA#INTEROPCM#CSTA#AES70”. Note the use of the switch connection “interopcm” from **Section 6.1** as part of the Tlink name.

The screenshot displays the Avaya Workforce Management console interface. The top navigation bar is red with the text "Security | Security Database | Tlinks". On the left, a sidebar menu lists various system components, with "Security" expanded to show "Security Database", which in turn has "Tlinks" selected. The main content area is titled "Tlinks" and contains a "Tlink Name" section with two radio button options: "AVAYA#INTEROPCM#CSTA#AES70" (which is selected) and "AVAYA#INTEROPCM#CSTA-S#AES70". Below these options is a "Delete Tlink" button.

6.4. Configure CT User

In the Navigation Panel, select **User Management** → **User Admin** → **Add User**. The **Add User** panel will display as shown below. Enter an appropriate **User Id**, **Common Name**, **Surname**, and **User Password**. Select **Yes** from the **CT User** dropdown list.

Click **Apply** (not shown) at the bottom of the pages to save the entries.

User Management | User Admin | List All Users

▶ 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

Edit User

* User Id	<input type="text" value="verint"/>
* Common Name	<input type="text" value="Verint"/>
* Surname	<input type="text" value="User"/>
User Password	<input type="password" value="•••••"/>
Confirm Password	<input type="password" value="•••••"/>
Admin Note	<input type="text"/>
Avaya Role	<input type="text" value="None"/>
Business Category	<input type="text"/>
Car License	<input type="text"/>
CM Home	<input type="text"/>
Css Home	<input type="text"/>
CT User	<input type="text" value="Yes"/>
Department Number	<input type="text"/>
Display Name	<input type="text"/>
Employee Number	<input type="text"/>
Employee Type	<input type="text"/>
Enterprise Handle	<input type="text"/>
Given Name	<input type="text"/>
Home Phone	<input type="text"/>

If the Security Database (SDB) is enabled on Application Enablement Services, set the Verint user account to Unrestricted Access to enable any device (station, ACD extension, DMCC virtual station) to be used implicitly. This step avoids the need to duplicate administration.

Navigate to **Security → Security Database → CTI Users → List All Users** and select the **verint** user and click **Edit**.

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 type="radio"/> breeze	Breeze	NONE	NONE
<input type="radio"/> ctiuser	CTI	NONE	NONE
<input type="radio"/> test	test	NONE	NONE
<input checked="" type="radio"/> verint	Verint	NONE	NONE

EditList All

On the **Edit CTI User** panel, check the **Unrestricted Access** box and click the **Apply Changes** button. Click **Apply** when asked to confirm the change on the **Apply Changes to CTI User Properties** dialog.

Security | Security Database | CTI Users | List All Users

▶ 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

Edit CTI User

User Profile:

User ID
Common Name
Worktop Name
Unrestricted Access

verint
Verint
NONE
☒

Call and Device Control:

Call Origination/Termination and Device Status

None

Call and Device Monitoring:

Device Monitoring
Calls On A Device Monitoring
Call Monitoring

None
None
☐

Routing Control:

Allow Routing on Listed Devices

None

Apply Changes

Cancel Changes

6.5. Confirm TSAPI and DMCC Licenses

Workforce uses a DMCC (**VALUE_AES_DMCC_DMC**) license for each recording port. Additionally, a TSAPI Basic (**VALUE_AES_TSAPI_USERS**) license is used for each agent station being monitored. If **VALUE_AES_DMCC_DMC** is licensed on Application Enablement Services, then an **IP_API_A** is generally not required on Communication Manager. Please consult product offer documentation for more details. If the licensed quantities are not sufficient for the implementation, contact the Avaya sales team or business partner for a proper license file.

From the left pane menu on Application Enablement Services Management Console, click **Licensing → WebLM Server Access**. A **Web License Manager** login window is displayed. Enter proper credentials to log in. Click **Licensed products → APPL_ENAB → Application Enablement** from the left pane. The Application Enablement Services license is displayed in the right pane. Ensure that there are enough **VALUE_AES_DMCC_DMC** and **VALUE_AES_TSAPI_USERS** licenses available.

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

License installed on: July 7, 2017 3:09:24 PM +00:00

License File Host IDs: XXXXXXXXXX

Feature (License Keyword)	License Capacity	Currently available
Device Media and Call Control (VALUE_AES_DMCC_DMC)	100	97
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	100	100
AES HA LARGE (VALUE_AES_HA_LARGE)	10	10
AES ADVANCED MEDIUM SWITCH (VALUE_AES_AEC_MEDIUM_ADVANCED)	100	100
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	100	100
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	100	100
AES HA MEDIUM (VALUE_AES_HA_MEDIUM)	10	10
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	100	100
DLG (VALUE_AES_DLG)	100	100
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	100	95
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	100	100

7. Configure Verint® Workforce Management

The initial configuration of the Workforce server is typically performed by Verint system engineer or authorized installers. These Application Notes will only cover the steps necessary to configure the Workforce solution to interoperate with Communication Manager and Application Enablement Services.

The steps include:

- Launch Verint Workforce Web Management
- Configure Data Sources
- Configure TSAPI and DMCC Adapters

7.1. Launch Verint Workforce Web Management

Local configurations of the Recorder and Recorder Integration adapters are managed via the Recorder Manager Web application. This can be accessed directly via a shortcut on the server desktop, or it can be launched from the Enterprise Manager Installation hierarchy.

If launched directly via the shortcut, enter the login name of **superuser** and the appropriate password. If launched from Enterprise Manager, it utilizes SSO and logs you in automatically.

The screenshot displays the Verint Recorder Manager Web Management interface. The top navigation bar includes the Verint logo, a refresh icon, a printer icon, and links for Preferences, Help, and Sign out. The main navigation menu has tabs for STATUS, SYSTEM MANAGEMENT, OPERATIONS, ALARMS, and GENERAL SETUP. The STATUS tab is active, showing a 'Status Summary' section. Below this, a message states: 'Information: This Recorder is managed by win-s7uefselpf8 Enterprise Manager'. The 'STATUS SUMMARY' section indicates the last update was on 01/23/2018 at 3:24 PM. The 'System Info' section lists details such as Host Name (WIN-S7UEFSELPF8), Serial # (441001), and Server Role(s) (Archive Database, Biometrics Database, Central Archive, Contact Database, Contact OLTP Database, Content Server, EM Core, Framework Applications, Framework Database, Framework Integration Service, IP Recorder, Interaction Applications, Interaction Data Warehouse, Interaction Flow Manager, QM Database, Recorder Core, Recorder Data Center APIs, Recorder Ingestion Web Service, Recorder Integration Service, Screen Recorder, Streaming Service, System). The 'Active Alarm Count' is 117, indicated by a red alarm icon. The 'System Utilization' section shows CPU Usage (2%), Memory Used (11084/12287 MB), Audio Recordings (0/100), and Screen Recordings (0/50). The 'Current Activity' section lists lag times for Compression, Consolidation, Local Archive, and Centralized Archive, all showing 0 minutes with green status icons. At the bottom right, there are 'Update' and 'Edit Thresholds' buttons.

System Info	
Host Name	WIN-S7UEFSELPF8
Serial #	441001
Server Role(s)	Archive Database, Biometrics Database, Central Archive, Contact Database, Contact OLTP Database, Content Server, EM Core, Framework Applications, Framework Database, Framework Integration Service, IP Recorder, Interaction Applications, Interaction Data Warehouse, Interaction Flow Manager, QM Database, Recorder Core, Recorder Data Center APIs, Recorder Ingestion Web Service, Recorder Integration Service, Screen Recorder, Streaming Service, System
Active Alarm Count	117

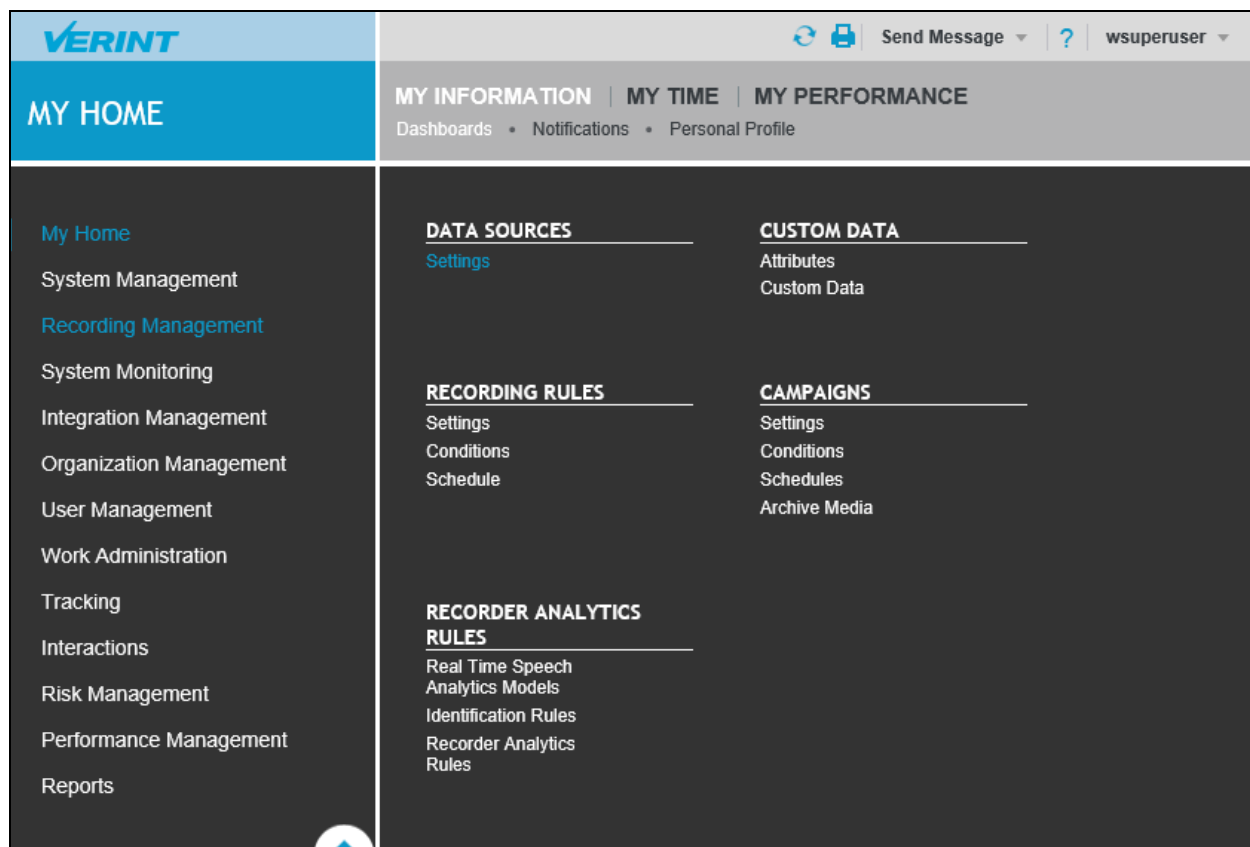
System Utilization	
CPU Usage (%)	(2%)
Memory Used (MB)	(11084/12287)
Audio Recordings	(0/100)
Screen Recordings	(0/50)

Current Activity	
Compression Lag Time (Min)	0
Consolidation Lag Time (Min)	0
Local Archive Lag Time (Days)	
Centralized Archive Lag Time (Days)	

7.2. Configure Data Source

Enterprise wide configurations are managed in the Enterprise Manager web application. This can be accessed by pointing your browser to <http://<hostname>/wfo/ui>.

To configure a Data Source, log in to the Enterprise Manager web-based application from Workforce server, enter username **wsuperuser** and it appropriate password to log in the Enterprise Manager (not shown), from the home page navigate to **My Home → Recording Management → Data Sources → Settings** as shown in the screenshot below.



In the **Settings** page, select **Create Data Source** button to create a new data source. The **Data Source Type** pop-up is displayed; select **Phone** in the **Type** field and **Avaya Communication Manager/Definity** in the **Switch/Sub Type** field. Click on **Select** button on completion.

Data Source Type	
Type	Phone
Switch/Sub Type	Avaya Communication Manager/Definity
<div>Select Cancel</div>	

Provide the following values for the specific fields and retain the default values for the remaining fields.

- **Name** – enter a described name, e.g. **AvayaCM** in this case
- **Time Zone** – select a proper time zone in the dropdown menu
- **Associated Integration Service Installations** – select the **Recorder Integration Service** check box

On the completion, click **Save** button.

VERINT

RECORDING MANAGEMENT

DATA SOURCES | CUSTOM DATA | RECORDING RULES | CAMPAIGNS

Settings • Member Groups • Phones • Data Source Groups • Agents • Import Status

DATA SOURCE SETTINGS: AvayaCM

Data Source Name

AvayaCM

Type: Phone

Switch/Sub Type: Avaya Communication Manager/Definity

Name: AvayaCM

Description:

Time Zone: (GMT-05:00) Eastern Time (US & Canada)

Data Source Parent: No Parent

Recorder Settings

Recorder TDM Settings

WFM Settings

TimeZone Settings

Device IP Configuration

Associated Integration Service Installations

☐ Enterprise

☐ WFO Site

☐ consolidated

☒ Recorder Integration Service

Advanced Settings

Import Export Reports Create Data Source Delete Data Source Save Revert

7.2.1. Configure Data Source – Member Groups

To create a member group, select **Member Group** link from the **Data Sources** page. In the compliance test, two member groups were created, one for extension recording resource and the other for selective extension pool.

The screenshot below shows the extension recording resource (ERR) group member. Provide the following values for the specific fields.

- **Name** – enter a descriptive name for e.g. **ERR**
- **Recorder Control Type** – select **Single Step Conference** in the dropdown menu
- **Share Recorders** – check the check box **IP Recorder**
- **Assigned Phones** – click on **Assign & Create Phones** to add virtual DMCC stations 3317, 3318, and 3319 to the list.

VERINT

RECORDING MANAGEMENT

DATA SOURCES | **CUSTOM DATA** | **RECORDING RULES** | **CAMPAIGNS**

Settings • Member Groups • Phones • Data Source Groups • Agents • Import Status

EDIT EXTENSION RECORDING RESOURCE: ERRFind Installation:

Data Source Name

AvayaCM

Settings

Name: ERR

Description:

Recorder Control Type: Single Step Conference

CLAN Boards:

Recorder Selection Expression: Attribute: Select Attribute Expression:

Shared Recorders

☐ Enterprise

☐ WFO Site

☐ consolidated

☒ IP Recorder

Assigned Phones

Extensions Primary/Secondary	Recording Mode
3317	Recording Resource
3318	Recording Resource
3319	Recording Resource

Test Regular Expression Assign & Create Phones Unassign Phones Save Cancel Rev

The screenshot below shows the selective recording pool (SEP) group member, provide the following values for the specific fields.

- **Name** – enter a descriptive name for e.g. **SEP**
- **Recorder Fallback Type** – select **On CTI Disconnection** in the dropdown menu
- **Associated Membergroups** – select the check box on the **ERR** which is the extension recording group created above.
- **Assigned Extension** – click on **Assign & Create Phones** to add extensions in the CM switch that will be monitored and recorded.

The screenshot displays the Verint Recording Management web interface. The left sidebar shows 'Data Source Name' with 'AvayaCM' selected. The main content area is titled 'EDIT SELECTIVE EXTENSION POOL: SEPFind Installation:'. The 'Settings' section includes fields for Name (SEP), Description, Recorder Selection Expression, and Recorder Fallback Type (On CTI Disconnection (Performance)). Below this, the 'Associated Membergroups' section shows a table with one entry: ERR (Extension Recording Resource), which is checked. The 'Assigned Extensions' section shows a table with four entries: 3301, 3303, 3401, and 3403, all with a Recording Mode of 'Record'. At the bottom, there are buttons for 'Assign & Create Phones', 'Unassign Phones', 'Save', 'Cancel', and 'Revert'.

Verint
RECORDING MANAGEMENT

DATA SOURCES | CUSTOM DATA | RECORDING RULES | CAMPAIGNS
Settings • Member Groups • Phones • Data Source Groups • Agents • Import Status

Send Message ? wsuperuser

EDIT SELECTIVE EXTENSION POOL: SEPFind Installation:

Data Source Name
AvayaCM

Settings

Name: SEP

Description:

Recorder Selection Expression: Attribute: Select Attribute Expression:

Recorder Fallback Type: On CTI Disconnection (Performance)

Associated Membergroups

Membergroup Name	Type
<input checked="" type="checkbox"/> ERR	Extension Recording Resource

Assigned Extensions

Extensions Primary/Secondary	Recording Mode
3301	Record
3303	Record
3401	Record
3403	Record

Assign & Create Phones Unassign Phones Save Cancel Revert

7.2.2. Configure Data Sources – Phones

To create a new phone, click on **Phones** link from the **DATA SOURCES** page. The **Phones** section is displayed, select **Create** button (not shown). The **PHONE: New Phone** page is displayed, in the **Primary Extension** section, enter the following values for the fields below.

- **Extension** – enter CM stations that is monitored and recorded by Workforce, these stations configured in **Section 5.5**
- **Recording Mode** – select **Record** from the dropdown menu

On the completion, click **Save** button.

RECORDING MANAGEMENT

DATA SOURCES | **CUSTOM DATA** | **RECOI** < >

Settings • Member Groups • Phones • Data Source Groups • Agents • Import Status

PHONE: New Phone ☒

Primary Extension

Extension	3301
Recording Mode	Record
LAN (Screen) Data Source	Select LAN (Screen) Data Source
Workstation Name	

Secondary Extensions

#	Extension	Recording Mode
1		Record

Repeat the same procedure above to create a new phone for the virtual DMCC station which is configured in **Section 5.6**. The **Recording Mode** is set to **Recording Resource**.

RECORDING MANAGEMENT

DATA SOURCES | CUSTOM DATA | RECORDING

Settings • Member Groups • Phones • Data Source Groups • Agents • Import Status

PHONE: New Phone

Primary Extension

Extension: 3317

Recording Mode: Recording Resource

LAN (Screen) Data Source: Select LAN (Screen) Data Source

Workstation Name:

Secondary Extensions

#	Extension	Recording Mode
1		Record

Add Delete

Save Cancel Revert

In the compliance test, the following extensions were configured as Record (3301, 3303, 3401 and 3404) and Recording Resource (3317, 3318, and 3319).

PHONES: AvayaCMView: All Find Phone:

Extensions	Primary/Secondary	Recording Mode	Member Groups	LAN (Screen) Data Source
3301		Record	SEP	
3303		Record	SEP	
3317		Recording Resource	ERR	
3318		Recording Resource	ERR	
3319		Recording Resource	ERR	
3401		Record	SEP	
3403		Record	SEP	

7.3. Configuration TSAPI and DMCC Adapter

From the top menu of the **Recorder Manager** application, navigate to **General Setup** → **Integration Adapters** → **Settings**. The adapter setting is displayed in the middle of the page. Workforce call recording utilizes both DMCC and TSAPI interfaces for monitoring stations and for recording calls.

The screen below show the TSAPI adapter was created for the testing. Note that Avaya TSAPI client application needs to be installed on the server as a prerequisite.

- **Data Source** – select AvayaCM as configured in **Section 7.2**
- **Avaya CT Service Id** – enter to the TSAPI link as shown in **Section 6.3**
- **Login Name** – enter the **verint** user as configured in **Section 6.4**
- **Login Password** – enter the password of **verint** user as configured on **Section 6.4**

The screenshot shows the 'Integration Adapters' settings page in the Verint Recorder Manager. The page has a top navigation bar with 'STATUS', 'SYSTEM MANAGEMENT', 'OPERATIONS', 'ALARMS', and 'GENERAL SETUP'. Below this is a sub-navigation bar with 'Settings' and 'Attributes'. The main content area is titled 'ADAPTER: TSAPI'. On the left, there is a table listing adapters:

Adapter Name	Status	Target Sta
DMCC	Started	Start
TSAPI	Started	Start

On the right, the 'Settings' section for the TSAPI adapter is displayed. It includes the following fields:

- Adapter Name: TSAPI
- Description: Avaya CT (TSAPI) Adapter
- Adapter Type: TSAdapter
- Run From: Integration Service
- Startup Type: Automatic
- DataSource: AvayaCM
- Avaya CT Service Id: AVAYA#INTEROPCM#CSTA#AES70
- Backup Service Id: (empty)
- Login Name: verint
- Login Password: (masked with dots)
- Monitor Only Logged In Extensions: (checkbox)

Below the settings is an 'Advanced Settings' section. At the bottom right, there are buttons for 'Start', 'Stop', 'Restart', 'Create', 'Save', and 'Delete'.

Select DMCC adapter from the left pane, the DMCC settings is displayed in the right side of the page. Enter the following values for the specific fields and retain the default values for the remaining fields.

- Data Source – select **AvayaCM** from the dropdown menu
- **AES Server Hostname** – enter the IP address of AES server
- **AES Username** – enter the **verint** user as configured in **Section 6.4**
- **AES Password** – enter the password of verint user as configured in **Section 6.4**
- **Avaya CM Switch Name** – enter the name of CM switch, in this case it is **interopcm**
- **User Extension as Device Passcode** – check the check box to use the extension as the passcode to register virtual DMCC station to Avaya CM.

The screenshot shows the Verint Integration Adapters configuration interface. On the left, a table lists available adapters. The main area displays the settings for the selected DMCC adapter.

Adapter Name	Status	Target State
DMCC	Started	Start
TSAPI	Started	Start

ADAPTER: DMCC

Settings

Adapter Name: DMCC

Description: Avaya DMCC (CMAPI) Adapter

Adapter Type: AvayaCMAPIAdapter

Run From: Integration Service

Startup Type: Automatic

Data Source: AvayaCM

AES Server Hostname: 10.33.1.4

Use Secure DMCC: ☐

AES Username: verint

AES Password: [Masked]

Use Backup Server: ☐

Backup Server Hostname: server2

Avaya CM Switch Name: INTEROPCM

Use Extension As Device Passcode: ☒

Phone Passcode: [Empty field]

Device Media Codec: G.711 Mu-law

RTP Encryption: No Encryption

Buttons: Start Stop Restart Create Save Delete

8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services, and Verint Workforce.

8.1. Verify Avaya Aura® Communication Manager

Verify that the interface on Communication Manager to Application Enablement Services is enabled and in **listening** status (use the **status aesvcs cti-link** command on the Communication Manager SAT).

```
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	aes70	established	75	75

Verify the registration status of the recording devices by using the **list registered-ip-stations** command. Verify that there is an entry for each virtual IP softphone from **Section 5.6**, with the client IP address of Application Enablement Services as **Station IP Address**, as shown below.

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

REGISTERED IP STATIONS					
Station Ext or Orig Port	Set Type/ Net Rgn	Prod ID/ Release	Skt	Station IP Address/ Gatekeeper IP Address	
3317	9640	IP_API_A	tcp	10.33.1.4	
	1	3.2040		10.33.1.6	
3318	9640	IP_API_A	tcp	10.33.1.4	
	1	3.2040		10.33.1.6	
3319	9640	IP_API_A	tcp	10.33.1.4	
	1	3.2040		10.33.1.6	

8.2. Verify Avaya Aura® Application Enablement Services

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

Verify the **Status** is *Talking* for the TSAPI link administered in **Section 6.2**, and that the **Associations** column reflects the number of monitored devices (4 stations, 1 hunt group number and 1 VDN) from **Section Error! Reference source not found.**

The screenshot shows the 'TSAPI Service Summary' page. On the left is a navigation pane with 'Status' expanded. The main area is titled 'TSAPI Link Details' and includes a refresh toggle set to 60 seconds. Below this is a table with the following data:

	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	interopcm	1	Talking	Fri Jan 5 16:05:17 2018	Online	17	6	74	74	30

Below the table are 'Online' and 'Offline' buttons. At the bottom, there are buttons for 'TSAPI Service Status', 'TLink Status', and 'User Status'.

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.

In the lower portion of the screen, verify that the **User** column shows an active session with the **verint** user name from **Section 6.4**, and that the **# of Associated Devices** column reflects the number of recording softphones from **Section 7.2.2**.

The screenshot shows the 'DMCC Service Summary – Session Summary' page. It includes summary statistics and a table of active sessions.

Summary Statistics:

- Service Uptime: 18 days, 23 hours 48 minutes
- Number of Active Sessions: 2
- Number of Sessions Created Since Service Boot: 157071
- Number of Existing Devices: 3
- Number of Devices Created Since Service Boot: 15

Table of Active Sessions:

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	F8A724539E9EF4C27 826F6B240629141-157070	breeze	Khepri Call Server Connector	10.33.1.46	XML Encrypted	0
<input type="checkbox"/>	832DBAEBDC79809A7 7C8A0813DA1609D-139882	verint	ContactStore	10.10.97.59	XML Unencrypted	3

At the bottom are buttons for 'Terminate Sessions' and 'Show Terminated Sessions'.

8.3. Verify Recording and Playback

To verify call recordings, log in to Enterprise Manager web-based application from Workforce server, enter username **wsuperuser** and its appropriate password to log in the Enterprise Manager (not shown), and from the home page navigate to **My Home → Risk Management → ANALYZE → Search**. In the **Search** page, select **Advanced Search** (not shown), the Advanced Search pop-up is displayed, check on the check box **Search Outside Visibility** and select **Search** button.

The screenshot shows the 'ADVANCED SEARCH' window. On the left is the 'INTERACTIONS FILTER' sidebar with options: Employees (selected), Targets, Customers, Date Range, Folders, Interactions, Custom Data, Biometrics, and Switches. The main area is titled 'EMPLOYEES' and contains a list of employees: 1000, Agent; 1001, Agent; and 1002, Agent. Below the list is a checkbox labeled 'Search Outside Visibility' which is checked. At the bottom, the search criteria are displayed as 'Search For: Search Outside Visibility true, Date Range 3 Days'. There are buttons for 'Clear All Parameters', 'Search', 'Save As', and 'Cancel'.

The **Search Results** page shows all recordings in range of 3 days. Each recording contains information of call such as Start Time, Duration, Direction, Employee, Dialed From, Dialed To, Extension...etc.

VERINT RISK MANAGEMENT

ANALYZE | CONFIGURE

Search | Folders

Back to: [Search](#)

SEARCH RESULTS

SEARCH RESULTS Retrieved 7 Interactions | [Advanced Search](#) | [New Search](#) | [Save Search](#)

Start Time	Duration	Direction	Employee	Interaction Type	Dialed From (...)	Dialed To (DN...)	Extension
01/23/2018 03:08:41 PM	01:37	↔	1000, Agent	📞	3401	3303	3303
01/23/2018 03:07:24 PM	02:16	↔	1001, Agent	📞	4603	3340	3401
01/22/2018 07:10:19 PM	02:48	↔		📞	3403	6149674306	3403
01/22/2018 07:09:48 PM	00:13	↔		📞	4301	3301	3301
01/22/2018 07:04:17 PM	02:02	↔	1001, Agent	📞	4603	3340	3401
01/22/2018 06:56:28 PM	01:45	↔		📞	4603	3403	3403
01/22/2018 06:49:33 PM	02:32	↔	1000, Agent	📞	4234684603	4179673340	3303

INTERACTION | Date/Time: 01/23/2018 03:08:41 PM | [1000, Agent](#) | [7](#)

00:00 / 01:34 [🔍](#) [🔊](#) [⏮](#) [⏪](#) [⏩](#) [⏭](#) X 1.0

Select one of recordings by clicking on a date and time link of the recording in the **Start Time** column. The **Interaction Review** page is displayed as shown in the screenshot below. In the **Interaction** section, hit the play icon to play the recording and the **Tags** section in bottom left of the page that contains all events of the recording from Alerting, Connected to Disconnected.

Back to: [Search](#) > [Search Results](#)

INTERACTION REVIEW

INTERACTION | 2/2 | Date/Time: 01/23/2018 03:08:41 PM | [1000, Agent](#) | [7](#)

00:00 / 01:34 [🔍](#) [🔊](#) [⏮](#) [⏪](#) [⏩](#) [⏭](#) X 1.0

TAGS

☒ Annotations ☒ Events

- [-00:03 Alerting](#)
- [00:00 Connected](#)
- [00:24 Call Conferenced](#)
- [00:57 Disconnected](#)

SCREEN

No screen available

9. Conclusion

These Application Notes describe the procedures for configuring Verint® Workforce Optimization to monitor and record calls placed to and from agents and phones on Avaya Aura® Communication Manager. In the configuration described in these Application Notes, Verint uses the Device and Media Control Services of Avaya Aura® Application Enablement Services to perform recording. All feature and serviceability test cases were completed and passed with the observations noted in **Section 2.2**.

10. Additional References

Product documentation for Avaya products may be found at <http://support.avaya.com>.

1. *Administering Avaya Aura® Communication Manager*, Release 7.0, 03-300509.
2. *Administering and Maintaining Avaya Aura® Application Enablement Services*, Release 7.0.

Product documentation related to Workforce Optimization can be obtained directly from Verint.

©2018 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.