

Avaya Solution & Interoperability Test Lab

Application Notes for Verint Ultra with Avaya Communication Manager and Avaya Application Enablement Services using DMCC and TSAPI – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for the Verint Ultra call recorder to successfully interoperate with Avaya Communication Manager and Avaya Application Enablement Services (AES) using Device Media and Call Control as well as Telephony Service Application Programmer Interface.

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

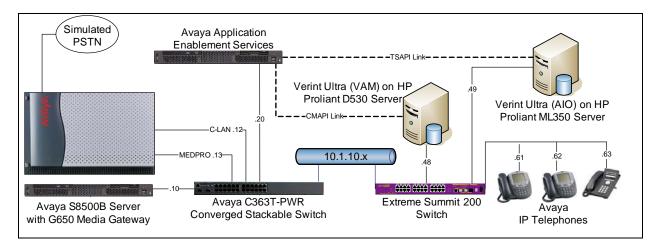
1. Introduction

These Application Notes describe the configuration steps required for the Verint Ultra call recorder to successfully interoperate with Avaya Communication Manager and Avaya Application Enablement Services (AES) using Device Media and Call Control (DMCC) as well as Telephony Service Application Programmer Interface (TSAPI).

Ultra uses TSAPI to extract Computer Telephony Integration (CTI) call event information and DMCC to retrieve the audio. Ultra uses TSAPI to invoke the Avaya Communication Manager single step conference method in order to bring the audio to the DMCC softphone stations.

The compliance test configuration consisted of an All In One (AIO) server and a Voice Acquisition Machine (VAM) server, both running Verint Ultra. The AIO server stores the recordings, the database and connects to the AES via TSAPI. The VAM connects to the AES via DMCC and receives media streams. Ultra is able to record media in both encrypted and unencrypted formats, however only unencrypted media was used in the compliance testing.

The diagram below shows the compliance test configuration.



2. Equipment and Software Validated

The following equipment and software were used for the sample configuration.

Equipment	Software
Avaya AES Server	AES 4.0
Avaya S8500 Server	Avaya Communication Manager 4.0
	(R14.00.0.730.5)
Avaya G650 Media Gateway	
IPSI TN2312BP	HW 7, FW 39
C-LAN TN799DP	HW 1, FW24
Medpro TN2302AP	HW 20, FW116
Avaya C363T-PWR Switch	4.3.12
Avaya 4610 IP Telephones (H.323)	2.8
Avaya 4602 IP Telephones (H.323)	2.3
Avaya 9620 IP Telephones (H.323)	1.5
Extreme Summit 200 Switch	Extremeware 7.5e.2.8
HP Proliant ML350 running	Windows Server 2003, Service Pack 1
Verint Ultra (AIO)	Release 10, SP1 (patches 2189, 2217, 2220,
	2245, 2252, 2273)
HP Compaq D530 running	Windows Server 2003, Service Pack 1
Verint Ultra (VAM)	Release 10, SP1 (patches 2153, 2190)

3. Configure Avaya Communication Manager

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

- Checking licensing.
- Administering CTI Link for the TSAPI Service.
- Administering DMCC softphones.

This section assumes that the link to the AES is previously administered. Information on how to do this is available in the AES Administration and Maintenance Guide, see **Section 10**.

For the compliance testing, users had physical station extensions of "10001, 10002, 10003, 10004 and 10022". The System Administration Terminal (SAT) interface was used for all Avaya Communication Manager configurations.

3.1. Check Licensing

Use the "display system-parameters customer-options" command, and verify that the **ASAI Link Core Capabilities** customer option is set to "y" on **Page 3**.

```
display system-parameters customer-options
                                                                  3 of 11
                                                           Page
                              OPTIONAL FEATURES
   Abbreviated Dialing Enhanced List? y
                                               Audible Message Waiting? n
                                           Authorization Codes? y
       Access Security Gateway (ASG)? n
       Analog Trunk Incoming Call ID? n
                                                             CAS Branch? n
A/D Grp/Sys List Dialing Start at 01? n
                                                               CAS Main? n
Answer Supervision by Call Classifier? n
                                                      Change COR by FAC? n
                                ARS? y Computer Telephony Adjunct Links? n
                ARS/AAR Partitioning? y Cvg Of Calls Redirected Off-net? y
         ARS/AAR Dialing without FAC? y
                                                            DCS (Basic)? y
         ASAI Link Core Capabilities? y
                                                      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? n
             ATM WAN Spare Processor? n
                                                                DS1 MSP? y
                                                 DS1 Echo Cancellation? n
                 Attendant Vectoring? n
       (NOTE: You must logoff & login to effect the permission changes.)
```

On **Page 10**, verify that the entry in **Limit** column for **Product ID** "IP_API_A" is greater than or equal to the number of simultaneous recordings required.

display system-parameters customer-options Page 10 of 11												
		MAX	KIMUM IP	REGISTE	RATION	IS BY	PROD	UCT	ID			
Product ID	Rel.	Limit		Used								
IP_API_A	:	100		0								
IP_API_B	:	100		0								
IP_API_C	:	100		0								
IP_Agent	:	100		0								
IP_IR_A	:	0		0								
IP_Phone	:	2400		4								
IP_ROMax	:	2400		0								
IP_Soft	:	100		0								
IP_eCons	:	1		0								
	:	0		0								
	:	0		0								
	:	0		0								
	:	0		0								
	:	0		0								
	:	0		0								
(NC	TE: Y	ou must	logoff	& login	to ef	fect	the	perm	nission	cha:	nges.)	

If either of the options above is not set appropriately, then contact the Avaya sales team or business partner and request a new license file.

3.2. Administer CTI Link for the TSAPI Service

Use the "add cti-link x" command, where "x" is an available CTI link number, to add a new CTI link. Enter an available extension number in the **Extension** field. Note that the CTI link number and extension number may vary. Enter "ADJ-IP" in the **Type** field, and a descriptive name in the **Name** field. The remaining fields may be left at their default values. Submit these changes.

```
add cti-link 3

CTI LINK

CTI Link: 3

Extension: 13300

Type: ADJ-IP

COR: 1

Name: TSAPI CTI Link 3
```

3.3. Administer DMCC Softphones

The DMCC softphones must be added in a consecutive range. The number of DMCC softphones added should be greater than or equal to the maximum number of simultaneous recordings required. Use the "add station x" command, where "x" is an available station number, to add a new DMCC softphone station. Configure the fields on **Page 1** as follows.

• **Type:** "4620"

• **Security Code:** Enter numerical code 4-8 digits in length.

• **Name:** Enter a descriptive name.

• IP SoftPhone: "y"

The remaining fields may be left at their default values. Submit these changes

add station 14001		Page	1 of 5
		STATION	
Extension: 14001		Lock Messages? n	BCC: 0
		Security Code: ****	TN: 1
Type: 4620		-	
Port: IP		Coverage Path 1:	COR: 1
Name: CMAPI Stn 1		Coverage Path 2:	cos: 1
		Hunt-to Station:	
STATION OPTIONS			
		Time of Day Lock Table:	
Loss Group:	19	Personalized Ringing Pattern:	1
		Message Lamp Ext:	14000
Speakerphone:	2-way	Mute Button Enabled?	У
Display Language:	english	Expansion Module?	n
Survivable GK Node Name:	J	<u>-</u>	
Survivable COR:	internal	Media Complex Ext:	
Survivable Trunk Dest?	V	IP SoftPhone?	v
	1		-
		IP Video Softphone?	n
		TI VIGCO BOTTPHONE:	
		Customizable Labels? y	

4. Configure Avaya AES

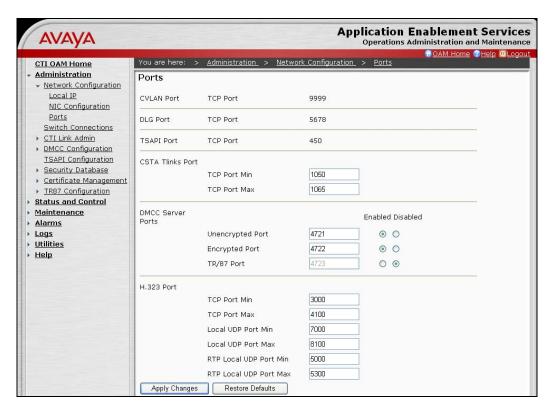
This section provides the procedures for configuring Avaya Application Enablement Services. The procedures include the following areas.

- Administering Port Properties.
- Administering TSAPI Link.
- Restarting Avaya AES.
- Administering CTI user.

This section assumes that the link to the Avaya Communication Manager is previously administered. Information on how to do this is available in the AES Administration and Maintenance Guide, see **Section 10**.

4.1. Administer Port Properties

Initialize the AES OAM web interface by browsing to "http://x.x.x.x/8443/MVAP/index.jsp", where "x.x.x.x" is the IP address of the AES, and log in (not shown). From the **OAM Home** screen (not shown) select **CTI OAM Admin** to bring up the **CTI OAM Home** menu. From the **CTI OAM Home** menu, select **Administration** > **Network Configuration** > **Ports**. On the **Ports** screen, select the **Enabled** radio button next to the **Unencrypted Port** field. The remaining fields may be left at their default values. Once completed, click **Apply Changes**.

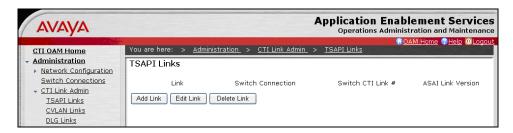


On the **Apply Changes to Port Properties** screen, click **Apply**. Do not restart the AES at this time.



4.2. Administer TSAPI Link

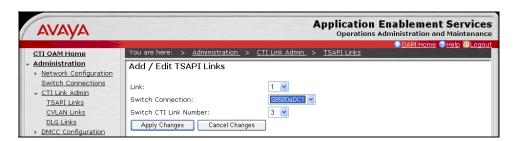
From the CTI OAM Home menu, select Administration > CTI Link Admin > TSAPI Links. On the TSAPI Links screen, click Add Link



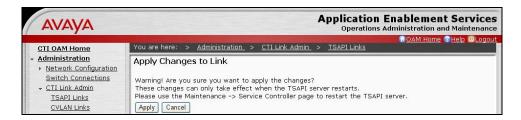
On the Add/Edit TSAPI Links screen, enter the following values.

- **Link:** Use the drop-down list to select an unused link number.
- **Switch Connection:** Choose the switch connection being used from the drop-down list.
- Switch CTI Link Number: Corresponding CTI link number configured in Section 3.2.

Once completed, click Apply Changes.



On the **Apply Changes to Link** screen, click **Apply**. Do not restart the TSAPI server at this time.



4.3. Restart Avaya AES

The AES must be restarted to effect the changes made in **Sections 4.1** and **4.2**. From the **CTI OAM Home** menu, select **Maintenance** > **Service Controller**. On the **Service Controller** screen, click **Restart AE Server**.



On the **Restart AE Server** screen, click **Restart**.



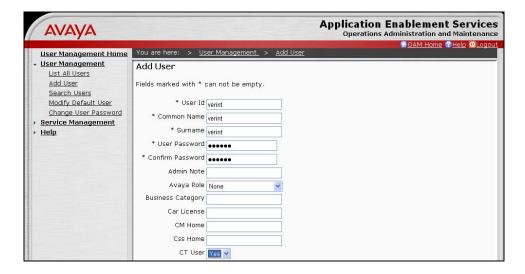
Wait at least 10 minutes and select **Maintenance > Service Controller**. On the **Service Controller** screen, verify that all services are showing "Running" in the **Controller Status** column.

4.4. Add CTI User

A user name and password are required for Ultra to communicate with the AES. This is set up via the User Management main menu which is accessed by clicking on **OAM Home** in the red bar on any AES screen, followed by clicking on **User Management** (not shown). From the **User Management** menu, select **Add User** and configure the following fields.

- User Id: Enter a login name to be used by Ultra to access the AES.
- Common Name: A descriptive name.
- **Surname:** A descriptive name.
- User Password: Enter a password to be used by Ultra to access the AES.
- **Confirm Password:** Re-enter the password.
- Avaya Role: Use the default value of "None".
- **CT User:** Select "Yes" from the drop down list.

The remaining fields may be left at their default values. Once completed, click **Apply** (not shown) at the bottom of the screen.



5. Configure Verint Ultra

This section provides the procedures for configuring Verint Ultra. The procedures include the following areas.

- Administer DMCC Recording Parameters
- Administer TSAPI Link

This section assumes that the system is delivered as an All In One (AIO) server, which stores the database and connects to the AES using TSAPI, and a Voice Acquisition Machine (VAM), which receives the media streams from the AES using DMCC. Information on how to do this is available in the Verint Ultra documentation as noted in **Section 10**. The entire configuration is done on the AIO server and exported to the VAM.

5.1. Administer DMCC Recording Parameters

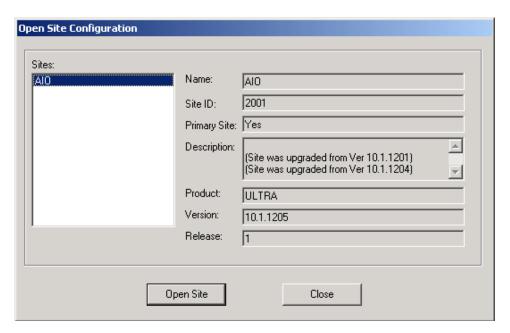
Configuring the DMCC recording is achieved by running the Ultra Configuration Manager. To activate the manager, double-click the **System Tools** shortcut on the desktop (not shown). Select the **Run** tab and double-click **Configuration Manager**.



In the **Configuration Manager Login** dialogue box, enter the password of a user with administrative permissions for Ultra.



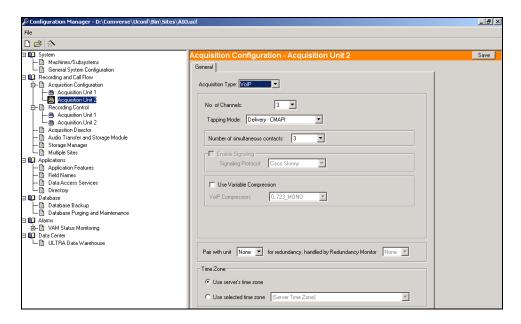
In the **Open Site Configuration** dialog box, ensure that the correct site is highlighted and click **Open Site**.



In the left pane of the **Configuration Manager** screen, expand **Recording and Call Flow** and **Acquisition Configuration**. Select the acquisition unit installed on the VAM (for the compliance testing **Acquisition Unit 2** was used). Configure the fields in the **Acquisition Configuration** pane as follows.

- Acquisition Type: "VoIP"
- **No. of Channels:** Enter a value equal to the number of DMCC softphones added in **Section 3.3**.
- **Tapping Mode:** "Delivery CMAPI"
- **Number of Simultaneous Contacts:** Enter a value less than or equal to the number of channels.

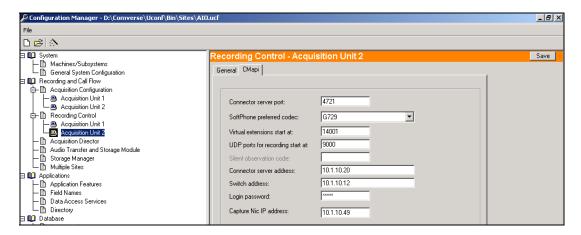
The remaining fields may be left at their default values. Once completed, click Save.



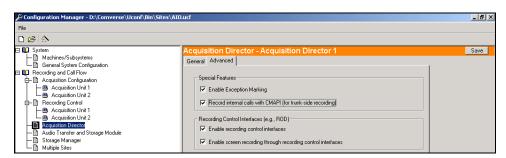
In the left pane of the **Configuration Manager** screen, expand **Recording and Call Flow** and **Recording Control**. Select the acquisition unit installed on the VAM (for the compliance testing **Acquisition Unit 2** was used). Configure the fields in the **Cmapi** tab of the **Recording Control** pane as follows.

- **Virtual extensions start at:** Enter the extension number of the first DMCC softphone of the consecutive range configured in **Section 3.3**.
- **Connector server address:** Enter the IP address of the AES.
- **Switch address:** Enter the IP address of the C-LAN board.
- **Login password:** Enter the security code for the DMCC softphones configured in **Section 3.3**.
- **Capture NIC IP address:** Enter the IP address of the VAM.

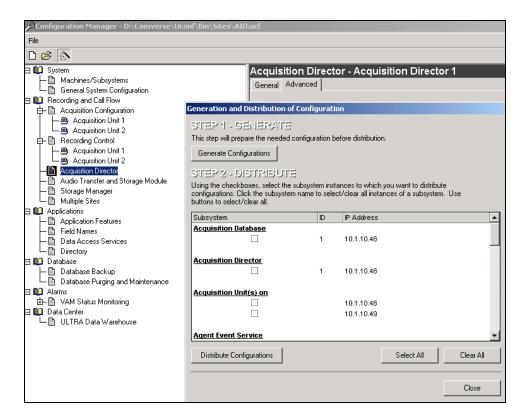
The remaining fields may be left at their default values. Once completed, click **Save**.



In the left pane of the Configuration Manager screen, expand Recording and Call Flow. Select Acquisition Director and, in the right pane, select the Advanced tab. Check the Record internal calls with CMAPI (for trunk side recording) checkbox. The remaining fields may be left at their default values. Once completed, click Save.

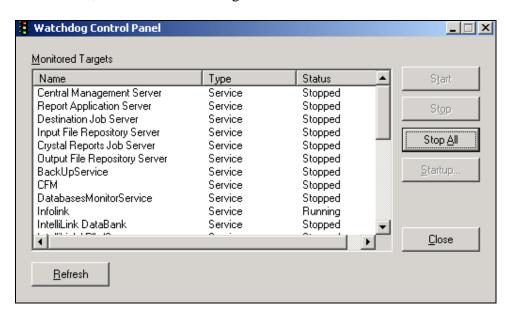


Once the configuration is completed on the AIO, it needs to be distributed to the VAM. In the taskbar of the **Configuration Manager** screen, click the rightmost button. In the **Generation and Distribution of Configuration** screen, click **Select All** and then click **Generate Configurations**.



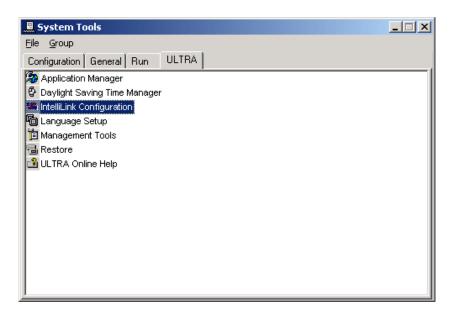
Once the generation is complete, a **Generation Report** dialog box (not shown) will appear, verifying that the generation was successful. Close the **Generation Report** dialog box to return to the **Generation and Distribution of Configuration** screen. Click **Distribute Configurations**.

The final step is to restart the Ultra services. On the **Run** tab of the **System Tools** screen (shown above), select **Ultra WatchDog**. On the **Watchdog Control Panel** click **Stop All** and wait for the **Status** column to show "Stopped" for all services. Scroll down to the **Watchdog** service (not shown) and click **Start**, wait for the watchdog to start all the services.

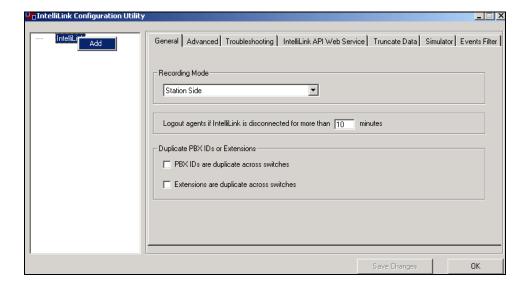


5.2. Administer TSAPI Link

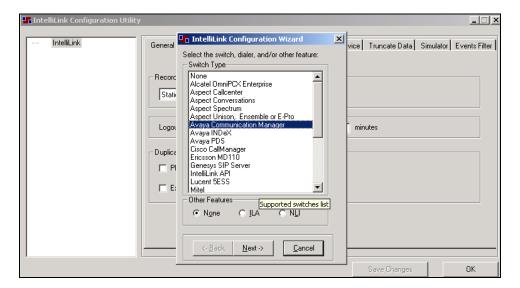
Configuring the TSAPI link is achieved by running the **IntelliLink Configuration Utility**. To activate the manager, double-click the **System Tools** shortcut on the desktop (not shown). Select the **Ultra** tab and double-click **IntelliLink Configuration**.



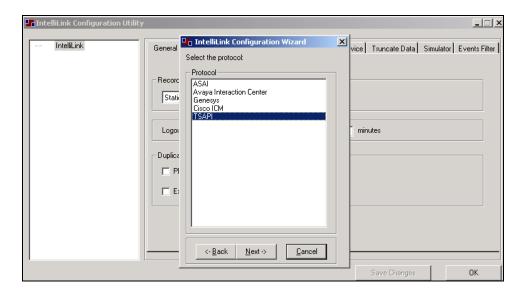
In the left pane of the **IntelliLink Configuration Utility** screen, right-click on **IntelliLink** and select **Add** to run the **IntelliLink Configuration Wizard**.



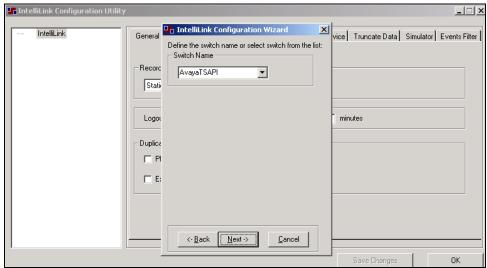
Select Avaya Communication Manager from the Switch Type list and click Next.



Select TSAPI from the Protocol list and click Next.



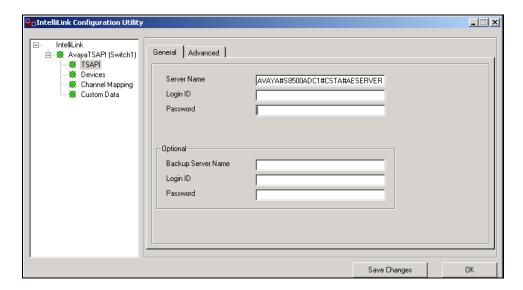
Enter a descriptive name for the connection in the **Switch Name** field and click **Next**.



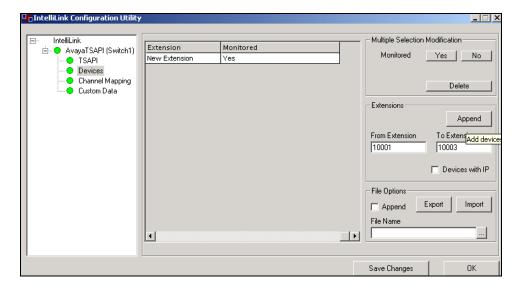
A Confirmation dialog box appears (not shown), click **OK** to complete the wizard and return to the **IntelliLink Configuration Utility**. In the left pane of the **IntelliLink Configuration Utility**, expand **IntelliLink** and the switch name created above. Click **TSAPI** and configure the fields on the **General** tab as follows.

- **Server Name:** Enter the Tlink string "AVAYA#SWITCHNAME#CSTA#AESNAME", where "SWITCHNAME" is the hostname of the server running Avaya Communication Manager and where AESNAME is the hostname of the AES.
- Login ID: Enter the user ID of the CTI user created in Section 4.4.
- **Password:** Enter the password of the CTI user created in **Section 4.4**.

The remaining fields may be left at their default values. Once completed, click **Save Changes**.



In the left pane of the **IntelliLink Configuration Utility**, click **Devices**. Enter the first extension in a range of extensions to be recorded in the **From Extension** field. Enter the last extension in a range of extensions to be recorded in the **To Extension** field. Click **Append**. Repeat this process for every range of extensions to be recorded. Once completed, click **Save Changes**.



6. Interoperability Compliance Testing

The interoperability compliance test included feature, performance and serviceability testing.

The feature testing focused on the ability of Verint Ultra to record calls to and from internal and external telephones and replay the voice recordings correctly.

The serviceability testing focused on verifying the ability of Verint Ultra to recover from an outage condition, such as busying out the CTI link and disconnecting the Ethernet cable for the CTI link.

The performance testing involved placing calls to 30 IP stations over a four hour period, achieving a Busy Hour Call Completion (BHCC) rate of approximately 3000.

6.1. General Test Approach

All feature and serviceability test cases were performed manually.

For feature testing, basic telephony operations such as answer, hold/retrieve, transfer, and conference were exercised on inbound and outbound calls as well between internal calls.

For serviceability testing, calls were placed before, during and after the outages and the recordings checked for accuracy.

For performance testing, a call generator placed inbound calls over an E1 trunk to simulated IP telephones over a four hour period.

6.2. Test Results

All feature, serviceability and performance tests successfully passed.

7. Verification Steps

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

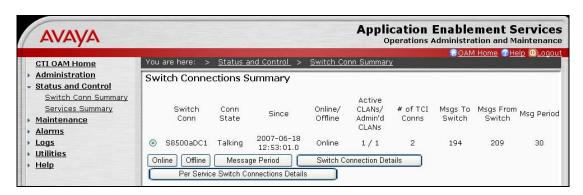
7.1. Verify Avaya Communication Manager

Verify the status of the administered CTI link by using the "status aesvcs cti-link" command. The **Service State** should show as "established".



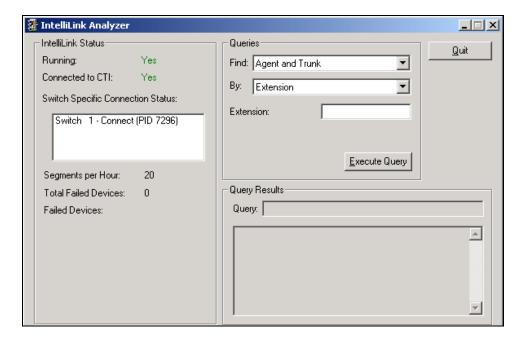
7.2. Verify Avaya Application Enablement Services

From the **AES OAM Admin** menu, verify the status of the administered CTI link by selecting **Status and Control > Switch Conn Summary**. The **Conn State** should show "Talking".



7.3. Verify Verint Ultra

Double-click the **System Tools** shortcut on the desktop (not shown). Select the **Configuration** tab (not shown) and double-click **IntelliLink Analyzer**. The **Running** and **CTI** fields should both show "Yes". Any devices that Ultra fails to monitor will be shown under **Failed Devices**.

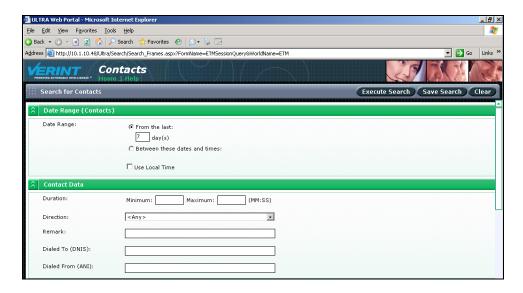


7.4. Replaying the Voice Recordings

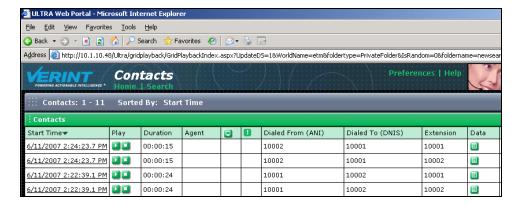
IntelliPortal is a browser-based application allowing the actual recordings that have taken place to be both inspected for data and voice content.

From any networked PC, open a browser window and enter "http://x.x.x.x/Ultra", where "x.x.x.x" is the IP address of the AIO, into the address bar. Log in to the web client using a user name with administrative privileges (not shown).

On the **Ultra Web Portal Welcome** screen, select **Search** from the menu (not shown). Enter a date range for the search on the **Search for Contacts** screen and click **Execute Search**.



Recordings made during the date range entered above will be listed in the **Contacts** screen. To bring up further information and an embedded media player (not shown), click in the **Start Time** column of a recording.



8. Support

If technical support is required for Verint Ultra, contact Verint Technical Support. Full details are available at http://www.verint.com.

9. Conclusion

These Application Notes describe the configuration steps required for the Verint Ultra call recorder to successfully interoperate with Avaya Communication Manager and Avaya Application Enablement Services (AES) using Device Media and Call Control (DMCC) and Telephony Service Application Programmer Interface (TSAPI). All features, serviceability and performance test cases were completed and passed successfully.

10. Additional References

This section references the product documentations that are relevant to these Application Notes.

- Documentation for Avaya Communication Manager (4.0), Media Gateways and Servers, Document ID 03-300151, Issue 6, February 2007, available at: http://support.avaya.com.
- Avaya Application Enablement Services 4.0 Administration and Maintenance Guide, Document ID 02-300357, Issue 6, February 2007.
 http://support.avaya.com.
- Verint Ultra product documentation is available on request from Verint. http://www.verint.com.

©2007 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and TM 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 Developer *Connection* Program at devconnect@avaya.com.