Avaya Solution & Interoperability Test Lab

Application Notes for Verint Impact 360 with Avaya Proactive Contact and Avaya Communication Manager Using Service Observing – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Verint Impact 360 to interoperate with Avaya Proactive Contact and Avaya Communication Manager using Service Observing. Verint Impact 360 is a call recording solution for contact centers. In the compliance testing, the Verint Impact 360 used the Event Services interface from Avaya Proactive Contact to obtain information on agent states and outbound calls, and used the Avaya Communication Manager Service Observing feature via the Avaya Application Enablement Services Device, Media, and Call Control interface to capture the media associated with the outbound calls for call recording.

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 Impact 360 to interoperate with Avaya Proactive Contact and Avaya Communication Manager using Service Observing. Verint Impact 360 is a call recording solution for contact centers. In the compliance testing, the Verint Impact 360 used the Event Services interface from Avaya Proactive Contact to obtain information on agent states and outbound calls, and used the Avaya Communication Manager Service Observing feature via the Avaya Application Enablement Services (AES) Device, Media, and Call Control (DMCC) interface to capture the media associated with the outbound calls for call recording.

The Avaya Proactive Contact Event Services interface is used by Verint Impact 360 to monitor the states and outbound calls for the agents. When the agent logs into Avaya Proactive Contact to service outbound calls, Verint Impact 360 receives the notification and initiates a Service Observing request to Avaya Communication Manager via the Avaya AES DMCC interface, to add a virtual IP softphone to the dedicated audio connection between the agent and Avaya Proactive Contact. The virtual IP softphone will stay connected to the agent until the agent logs out of Avaya Proactive Contact.

When an outbound call is delivered to the agent, the Verint Impact 360 is informed of the call via call events from the Avaya Proactive Contact Event Services interface, and therefore starts the call recording using the media from the virtual IP softphone that is connected to the agent. The call events from the Avaya Proactive Contact Event Services interface are also used to determine when to stop the call recording.

Verint Impact 360 only uses the Avaya Proactive Contact Event Services to record outbound calls, therefore the compliance test only covered the recording of outbound calls from Avaya Proactive Contact.

1.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on the Verint Impact 360:

- Handling of real-time agent states and call events from Avaya Proactive Contact.
- Use of Avaya AES DMCC registration services to register and un-register the virtual IP softphones.
- Use of Avaya AES DMCC physical device services to activate Service Observing for the virtual IP softphones.
- Use of Avaya AES DMCC monitoring services and media control events to obtain the media from the virtual IP softphones.
- Proper recording, logging, and playback of outbound calls for scenarios involving basic, hold, reconnect, simultaneous, conference, and transfer calls.

The serviceability testing focused on verifying the ability of Verint Impact 360 to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet cable to Verint Impact 360.

1.2. Support

Technical support on Verint Impact 360 can be obtained through the following:

- **Phone:** (800) 776-2462
- **Email:** contactcenter@verint.com

2. Reference Configuration

Verint Impact 360 can be configured on a single server or with components distributed across multiple servers. The compliance test configuration used two servers to host Verint Impact 360 components, as shown in **Figure 1**.

The detailed administration of basic connectivity between Avaya Communication Manager and Avaya AES, and between Avaya Communication Manager and Avaya Proactive Contact, are not the focus of these Application Notes and will not be described.

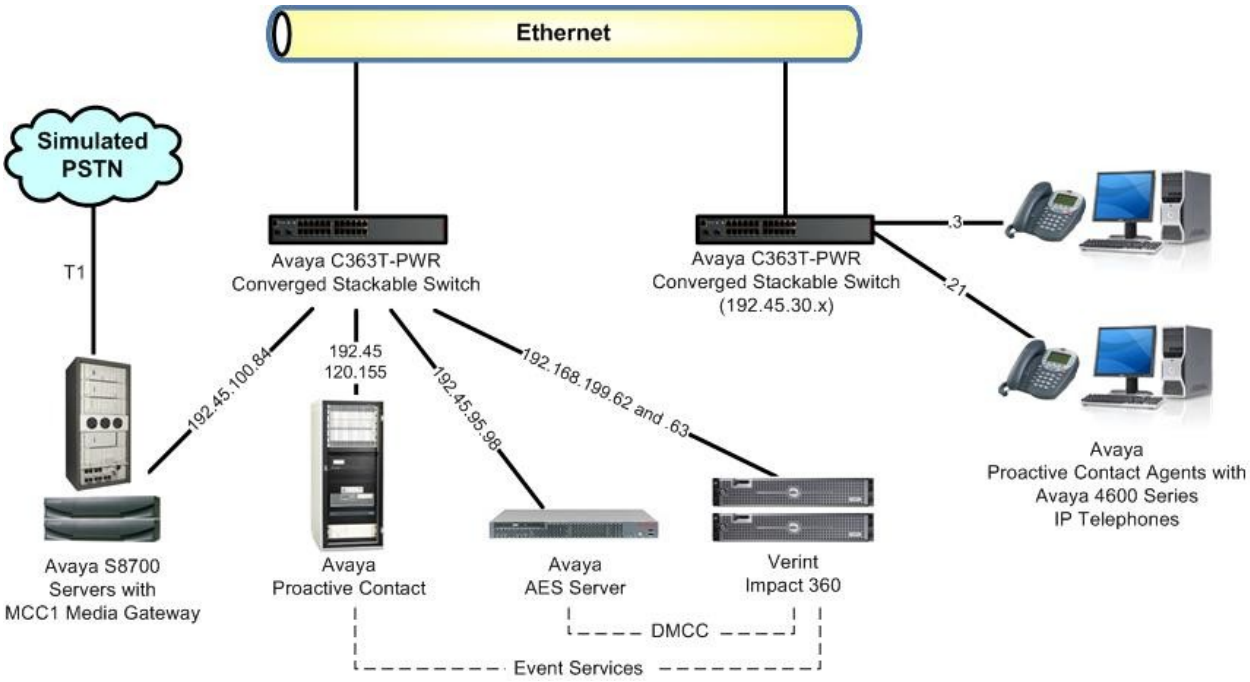


Figure 1: Verint Impact 360 with Avaya Proactive Contact and Avaya Communication Manager Using Service Observing

3. Equipment and Software Validated

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

Equipment	Software
Avaya S8700 Servers	Avaya Communication Manager 5.1.2, R015x.01.2.416.4
Avaya MCC1 Media Gateway • TN799DP C-LAN Circuit Pack • TN2302AP IP Media Processor	 HW01 FW024 HW13 FW116
Avaya Application Enablement Services	4.2
Avaya Proactive Contact with PG230 Switch	4.0
Avaya 4600 Series IP Telephones (H.323)	2.9
Verint Impact 360 • Verint Impact 360 HUB • Verint Impact 360 VoIP	 ULTRA 10 SP3 ULTRA 10 SP3

4. Configure Avaya Communication Manager

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

- Verify Avaya Communication Manager License
- Administer DMCC CTI link
- Administer feature access codes
- Administer class of restriction
- Administer agent stations
- Administer virtual IP softphones

4.1. Verify Avaya Communication Manager License

Log into the System Access Terminal (SAT) to verify that the Avaya Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the "display system-parameters customer-options" command to verify that the **Service Observing (Basic)** customer option is set to "y" on **Page 6**. If this option is not set to "y", then contact the Avaya sales team or business partner for a proper license file.

```
display system-parameters customer-options                    Page   6 of  11
                        CALL CENTER OPTIONAL FEATURES

                          Call Center Release: 5.0

                                 ACD? y                        Reason Codes? y
                       BCMS (Basic)? y               Service Level Maximizer? y
          BCMS/VuStats Service Level? y              Service Observing (Basic)? y
  BSR Local Treatment for IP & ISDN? n     Service Observing (Remote/By FAC)? y
                  Business Advocate? n              Service Observing (VDNs)? y
                    Call Work Codes? y                              Timed ACW? y
```

Navigate to **Page 10**, and verify that there is sufficient **IP_Soft** license.

```
display system-parameters customer-options                    Page  10 of  11
                     MAXIMUM IP REGISTRATIONS BY PRODUCT ID

Product ID  Rel. Limit          Used
AgentSC        : 12000          0
IP_API_A       : 12000          0
IP_API_B       : 100            0
IP_API_C       : 100            0
IP_Agent       : 12000          0
IP_IR_A        : 100            0
IP_Phone       : 12000          4
IP_ROMax       : 12000          0
IP_Soft        : 12000          0
IP_eCons       : 128            0
oneX_Comm      : 12000          0
               : 0              0
```

4.2. Administer DMCC CTI Link

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

```
add cti-link 15                                                Page   1 of   3
                                    CTI LINK
 CTI Link: 15
Extension: 24998
     Type: ADJ-IP
                                                                    COR: 1
     Name: Verint DMCC Link
```

4.3. Administer Feature Access Codes

Use the "change feature-access-codes" command, to enter an available feature access code for the **Service Observing Listen Only Access Code** field.

```
change feature-access-codes                                    Page   5 of  10
                              FEATURE ACCESS CODE (FAC)

                         Automatic Call Distribution Features

                    After Call Work Access Code: *13
                            Assist Access Code:
                          Auto-In Access Code: *15
                         Aux Work Access Code: *16
                            Login Access Code: *17
                           Logout Access Code: *20
                        Manual-in Access Code: *12
      Service Observing Listen Only Access Code: *05
      Service Observing Listen/Talk Access Code: *06
          Service Observing No Talk Access Code: *07
                    Add Agent Skill Access Code:
                 Remove Agent Skill Access Code:
              Remote Logout of Agent Access Code:
```

4.4. Administer Class of Restriction

Enter the "change cor n" command, where "n" is the class of restriction (COR) number used for integration with Verint Impact 360. Set the **Can Be Service Observed** and **Can Be A Service Observer** fields to "y", as shown below. For the compliance testing, this COR was assigned to the physical stations used by the Avaya Proactive Contact agents and to the virtual IP softphones used by Verint Impact 360.

```
change cor 7                                              Page   1 of  22
                            CLASS OF RESTRICTION

               COR Number: 7
          COR Description:

                      FRL: 7                                APLT? y
  Can Be Service Observed? y           Calling Party Restriction: none
Can Be A Service Observer? y            Called Party Restriction: none
        Time of Day Chart: 1       Forced Entry of Account Codes? n
         Priority Queuing? n                Direct Agent Calling? y
     Restriction Override: none       Facility Access Trunk Test? n
     Restricted Call List? n                 Can Change Coverage? y
```

4.5. Administer Agent Stations

Modify each physical station used by the Avaya Proactive Contact agents to allow the station to be service observed. Change the agent station using the "change station n" command, where "n" is the station extension number. For the COR field, enter the COR from **Section 4.4**, which allows the station to be service observed.

Repeat this section for all agent stations. In the compliance testing, two physical agent stations with extensions of "22721" and "26614" were modified.

```
change station 22721                                      Page   1 of   5
                                    STATION

Extension: 22721                        Lock Messages? n               BCC: 0
     Type: 4621                         Security Code: *                TN: 1
     Port: S00011                     Coverage Path 1:                 COR: 7
     Name: Customer                   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: 22721
           Speakerphone: 2-way               Mute Button Enabled? y
        Display Language: english               Expansion Module? n
 Survivable GK Node Name:
          Survivable COR: internal              Media Complex Ext:
   Survivable Trunk Dest? y                          IP SoftPhone? n

                                                      IP Video? n

                                               Customizable Labels? y
```

4.6. Administer Virtual IP Softphones

Add a virtual softphone 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.

- **Type:** "4602+"
- **Name:** A descriptive name.
- **Security Code:** A desired value.
- **COR:** The class of restriction number from **Section 4.4**.
- **IP SoftPhone:** "y"

```
add station 22991                                          Page   1 of   4
                                   STATION

Extension: 22991                       Lock Messages? n              BCC: 0
     Type: 4602+                       Security Code: 12345           TN: 1
     Port: S00147                    Coverage Path 1:                COR: 7
     Name: Verint Virtual Softphone 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: 22991
           Speakerphone: 1-way                Mute Button Enabled? y
        Display Language: english
 Survivable GK Node Name:
          Survivable COR: internal              Media Complex Ext:
   Survivable Trunk Dest? y                          IP SoftPhone? y

                                         IP Video Softphone? n
```

Repeat this section to administer the desired number of virtual softphones, using sequential extension numbers and the same security code for all virtual softphones. For the compliance testing, two virtual softphones were administered as shown below, to allow for two simultaneous recordings.

```
list station 22991 count 2

                                STATIONS

Ext/          Port/   Name/                        Room/         Cv1/ COR/ Cable/
 Hunt-to       Type      Surv GK NN        Move     Data Ext      Cv2  COS  Jack

22991         S00147  Verint Virtual Softphone 1                    7
               4602+                        no                      1
22992         S00139  Verint Virtual Softphone 2                    7
               4602+                        no                      1
```

5. Configure Avaya Application Enablement Services

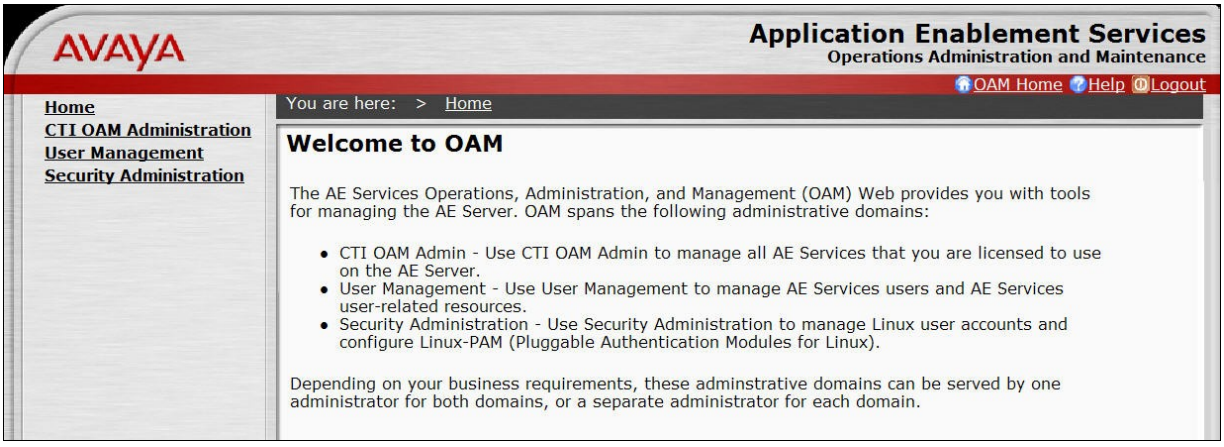
This section provides the procedures for configuring Avaya AES. The procedures include the following areas:

- Verify AES license
- Obtain H.323 gatekeeper
- Administer Verint user

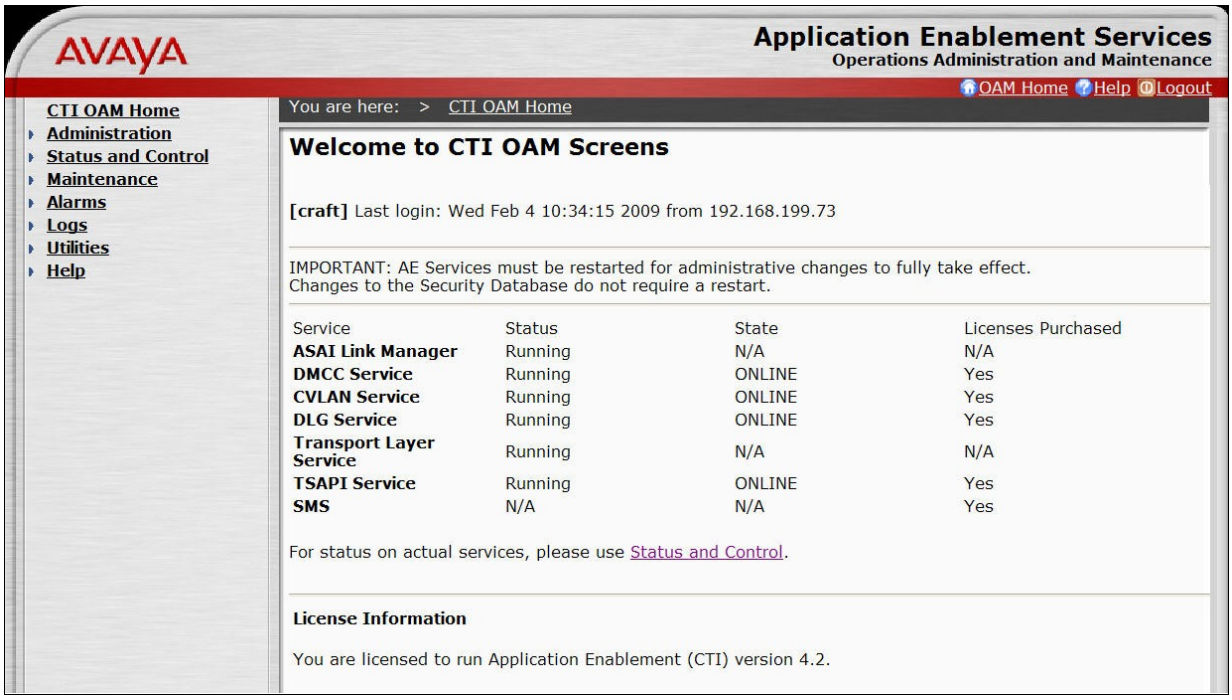
5.1. Verify AES License

Access the AES OAM web-based interface by using the URL "https://ip-address:8443/MVAP" in an Internet browser window, where "ip-address" is the IP address of the AES server. The **Logon** screen is displayed as shown below. Log in with the appropriate credentials.

The **Welcome to OAM** screen is displayed next. Select **CTI OAM Administration** from the left pane.

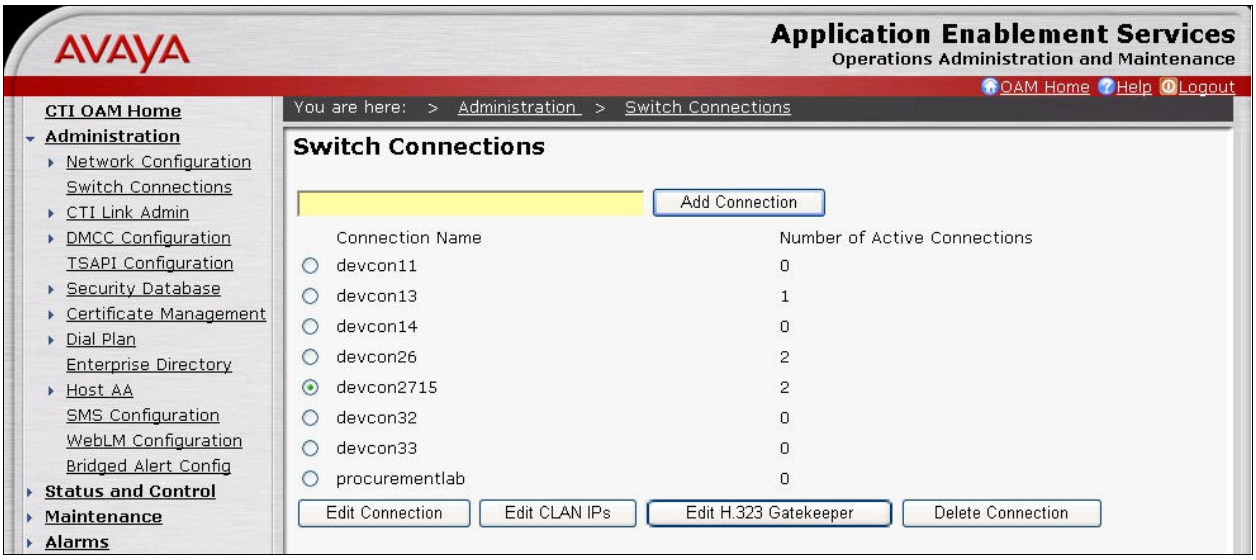


The **Welcome to CTI OAM Screens** is displayed. Verify that AES is licensed for the **DMCC Service**, as shown below. If the service is not licensed, contact the Avaya sales team or business partner for a proper license file.



5.2. Obtain H.323 Gatekeeper

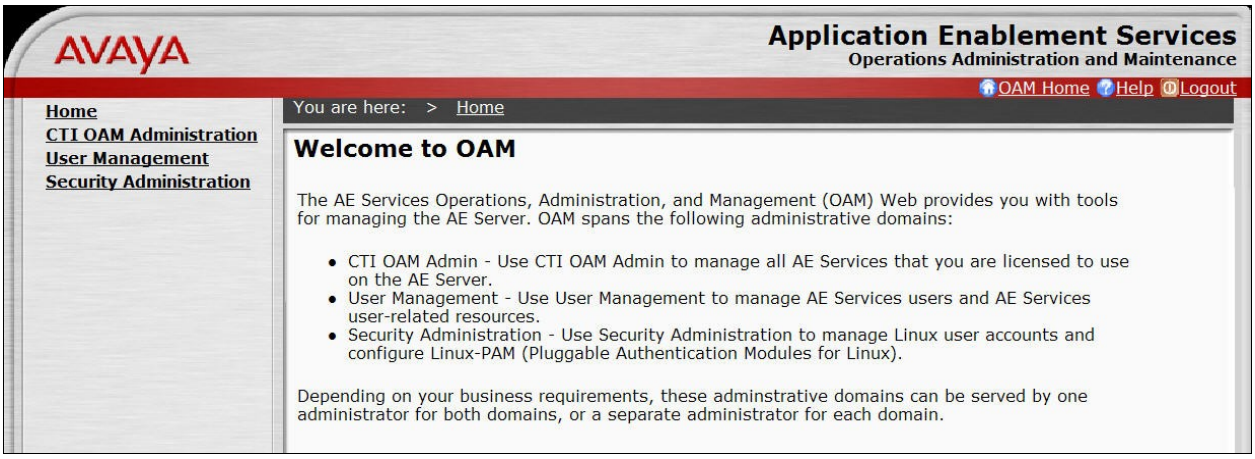
Select **Administration > Switch Connections** from the left pane. The **Switch Connections** screen shows a listing of the existing switch connections. Locate the connection name associated with the relevant Avaya Communication Manager, in this case "devcon2715", and select the corresponding radio button. Click **Edit H.323 Gatekeeper**.



The **Edit H.323 Gatekeeper** screen is displayed. Note the IP address, for this value will be used later to configure the Verint Impact 360 server.

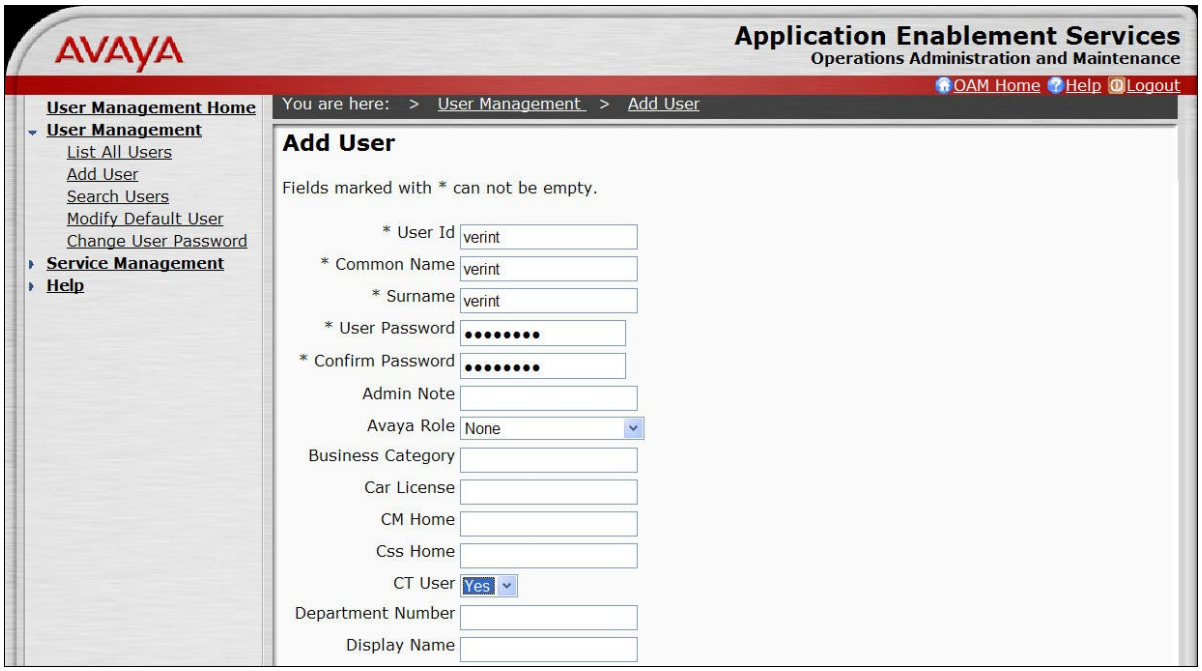
5.3. Administer Verint User

Administer a new user account for Verint Impact 360, which is created from the AES User Management web pages. Select **OAM Home**, located at the upper right corner of the screen, to display the **Welcome to OAM** screen below. Select **User Management** from the left pane.



The **Welcome to the User Management home page** screen is displayed, as shown below.

Select **User Management > Add User** from the left pane. In the **Add User** screen shown below, enter descriptive values for the **User Id**, **Common Name**, **Surname**, **User Password**, and **Confirm Password** fields. For the **CT User** field, select "Yes" from the drop-down list. Retain the default value in the remaining fields. Click **Apply** at the bottom of the screen (not shown below).



6. Configure Verint Impact 360

This section provides the procedures for configuring Verint Impact 360. The procedures include the following areas:

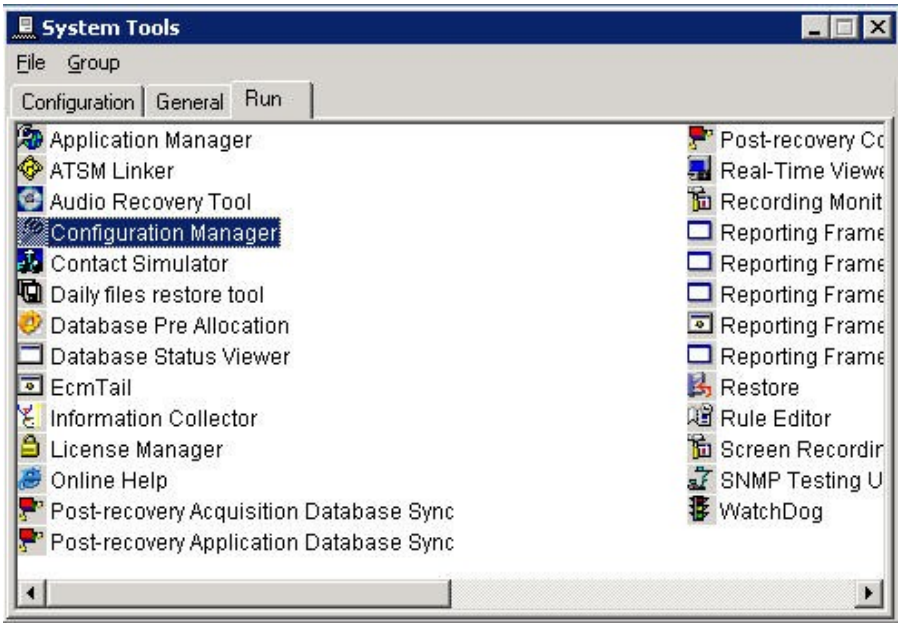
- Launch Configuration Manager
- Administer acquisition configuration
- Administer recording control
- Generate and distribute configuration
- Launch IntelliLink Configuration
- Administer Communication Manager connection
- Administer Proactive Contact connection

The configuration of Verint Impact 360 is performed by Verint technicians. The procedural steps are presented in these Application Notes for informational purposes.

6.1. Launch Configuration Manager

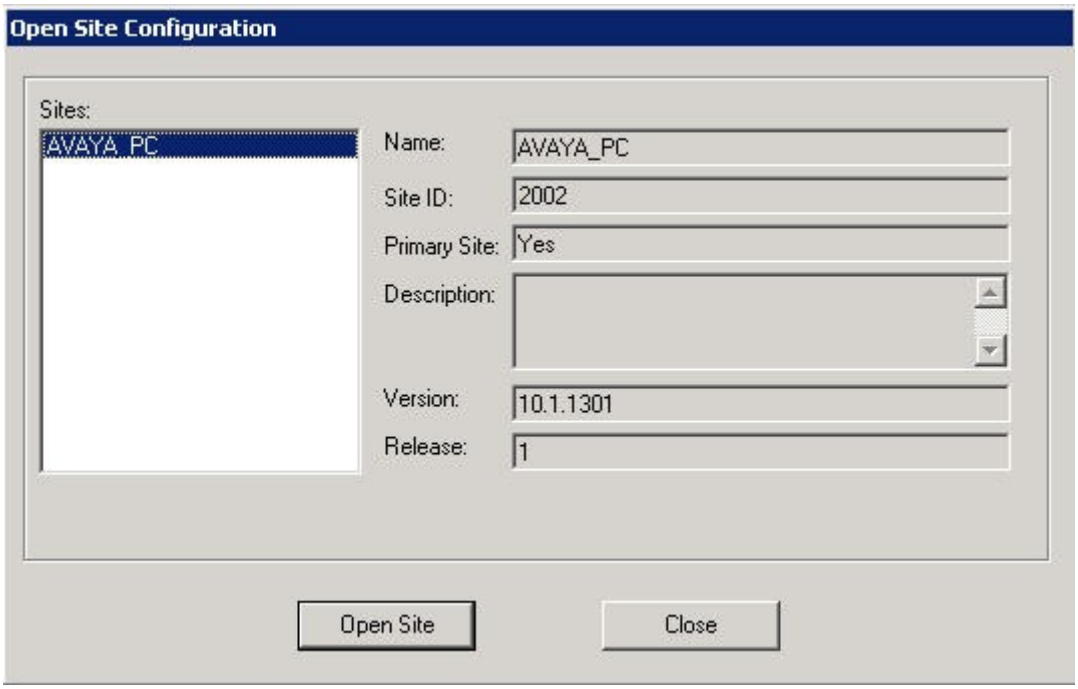
From the Verint Impact 360 server running the HUB component, double-click on the **System Tool** icon shown below, which is created as part of the installation.

The **System Tools** screen is displayed. Select the **Run** tab, followed by **Configuration Manager** to launch the application.



In the **Configuration Manager Login** screen, enter the appropriate credentials.

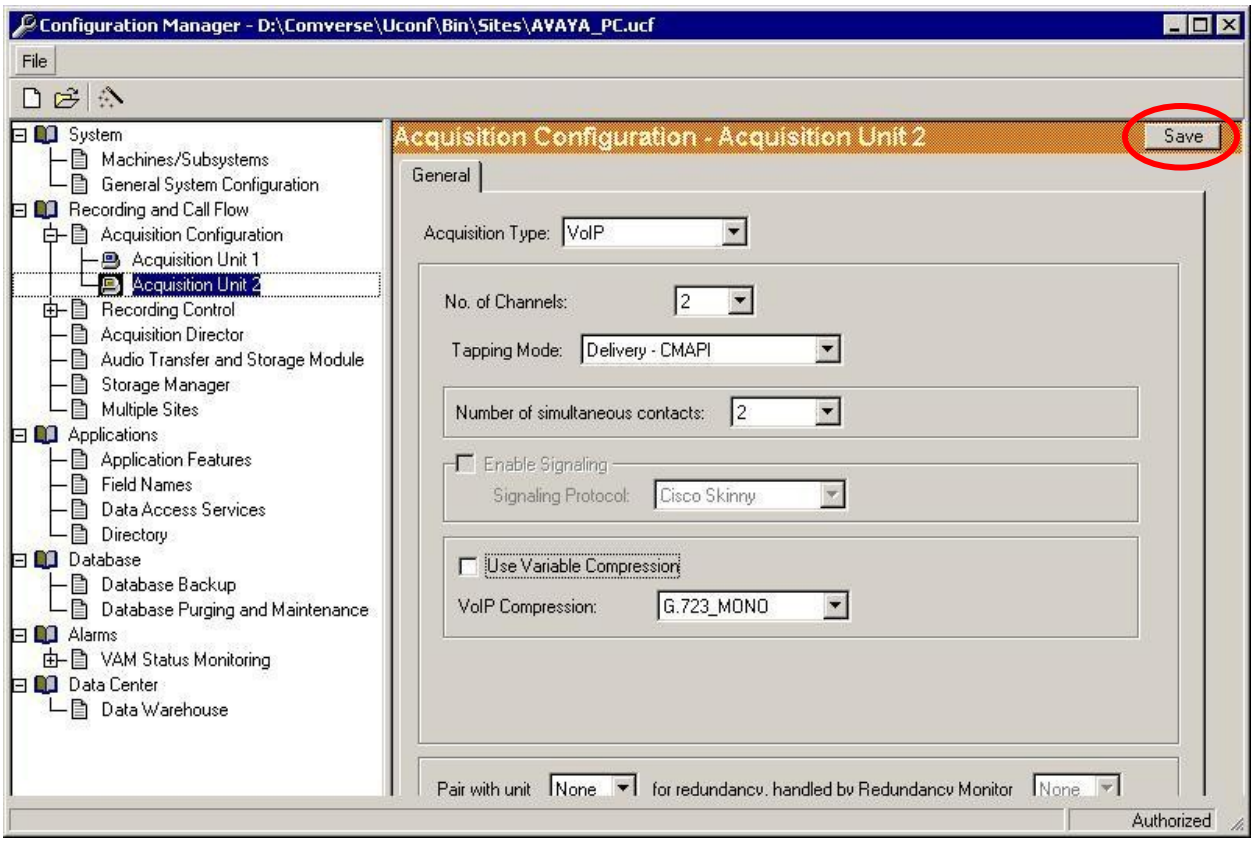
The **Open Site Configuration** screen is displayed next. Select the appropriate site under **Sites** and click **Open Site**. Note that the applicable sites are created by the Verint technicians as part of the initial configuration.



6.2. Administer Acquisition Configuration

The **Configuration Manager** screen is displayed. Select **Recording and Call Flow > Acquisition Configuration > Acquisition Unit 2** from the left pane, to display the **Acquisition Configuration – Acquisition Unit 2** screen. Enter the following values for the specified fields, and retain the default values for the remaining fields. Click **Save**.

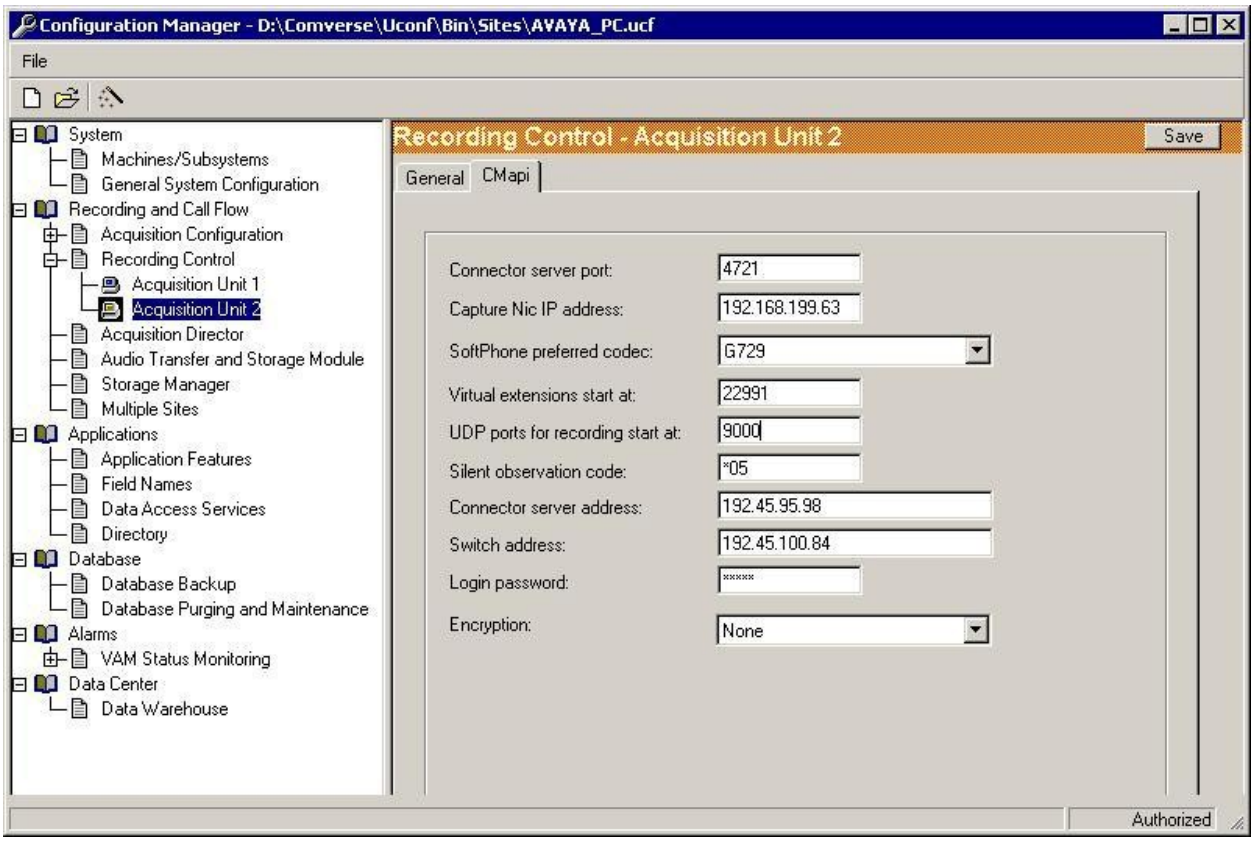
- **No. of Channels:** The number of virtual softphones from **Section 4.6**.
- **Tapping Mode:** "Delivery – CMAPI"
- **Number of simultaneous contacts:** The number of virtual softphones from **Section 4.6**.
- **VoIP Compression:** Select a desired VoIP compression.



6.3. Administer Recording Control

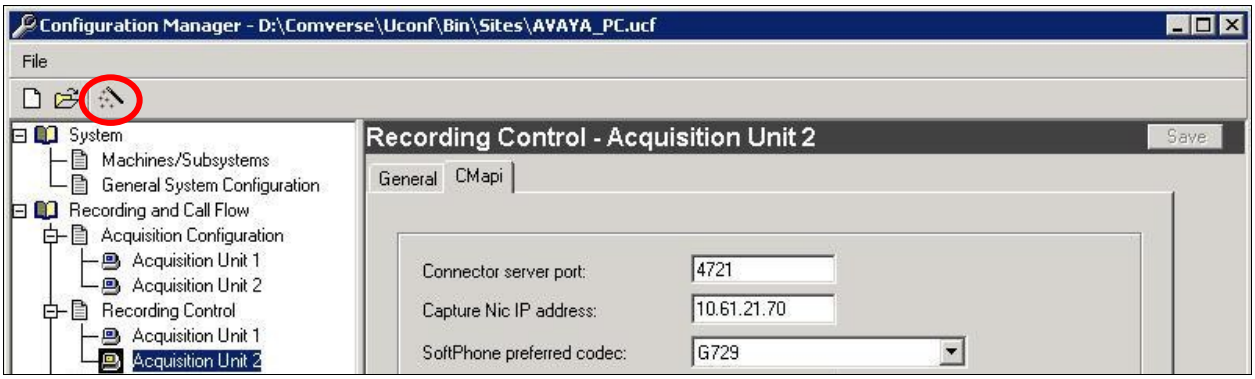
From the **Configuration Manager** screen, select **Recording and Call Flow > Recording Control > Acquisition Unit 2** from the left pane, to display the **Recording Control – Acquisition Unit 2** screen. Select the **CMapi** tab. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Virtual extensions start at:** The starting virtual softphone extension from **Section 4.6**.
- **Silent observation code:** The Service Observing Listen Only code from **Section 4.3**.
- **Connector server address:** The IP address of the Avaya AES server.
- **Switch address:** The IP address of the H.323 gatekeeper from **Section 5.2**.
- **Login password:** The password for the virtual softphones from **Section 4.6**.

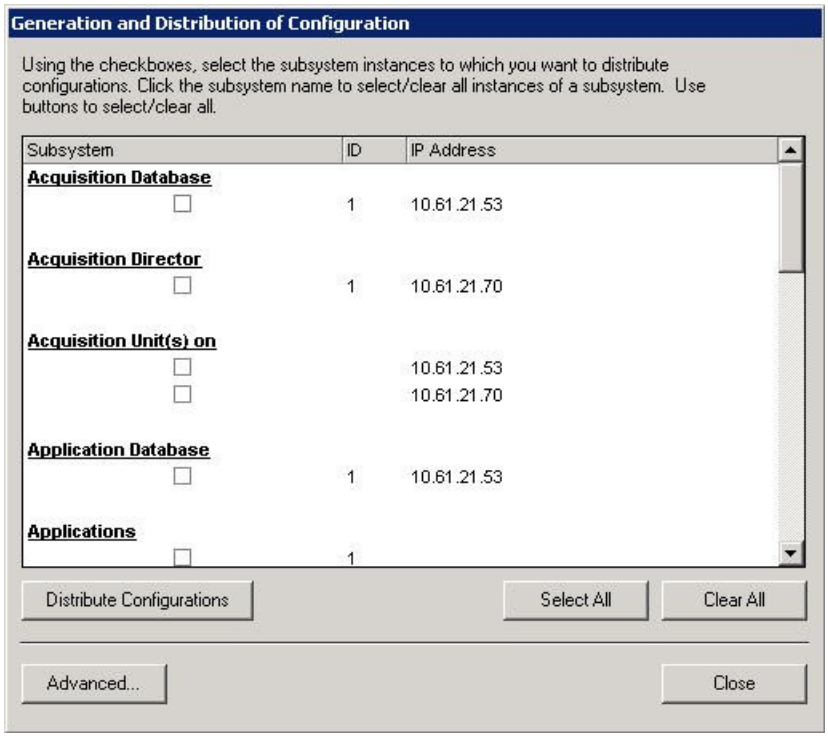


6.4. Generate and Distribute Configuration

Click on the **Generate and Distribute Configuration To Site** icon circled below.



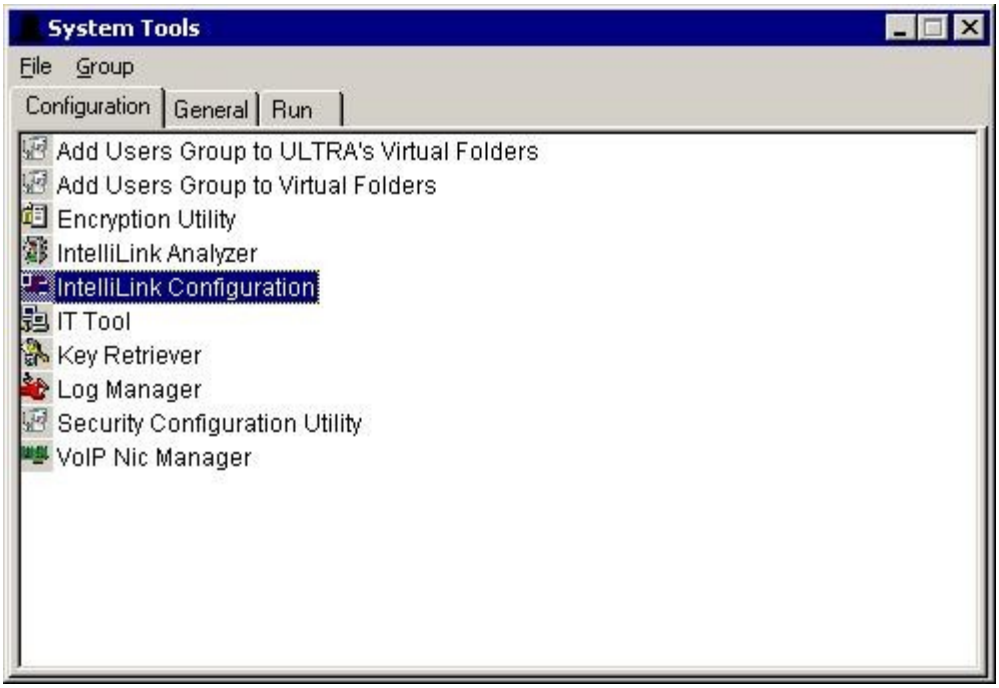
The **Generation and Distribution of Configuration** screen is displayed. Click **Select All**, followed by **Distribute Configurations** to distribute the updated configuration to all components. Reboot all Verint Impact 360 servers.



6.5. Launch IntelliLink Configuration

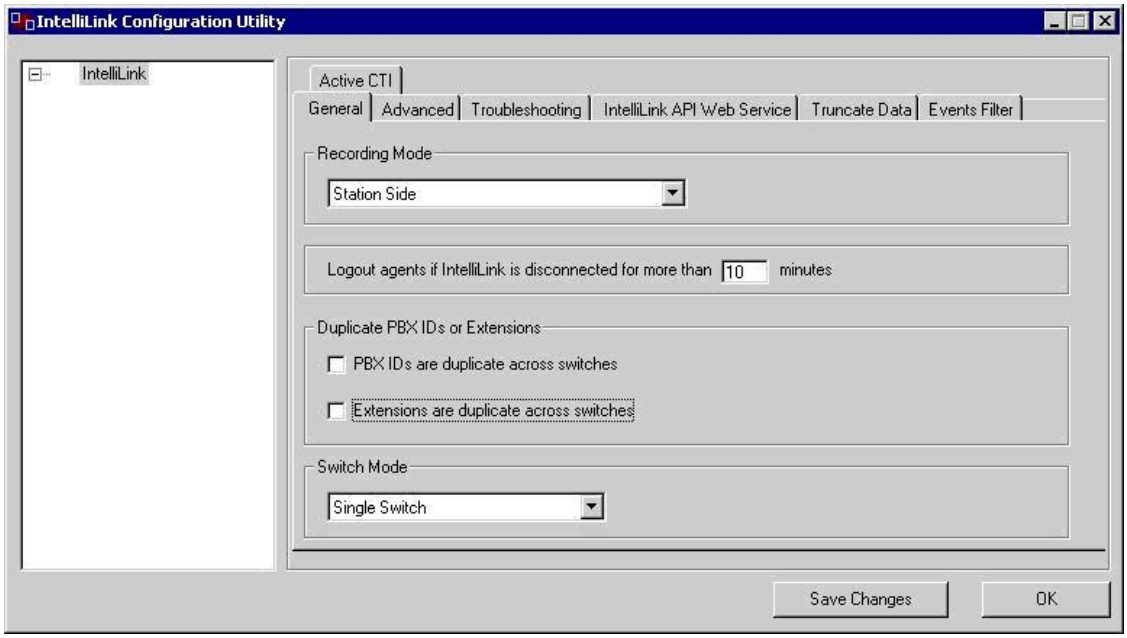
From the Verint Impact 360 server running the VoIP component, double-click on the **System Tool** icon shown below, which is created as part of the installation.

The **System Tools** screen is displayed. Select the **Configuration** tab, followed by **IntelliLink Configuration** to launch the application.



6.6. Administer Communication Manager Connection

The **IntelliLink Configuration Utility** screen is displayed. Right click on **IntelliLink** in the left pane, and select **New** to create a new switch connection.

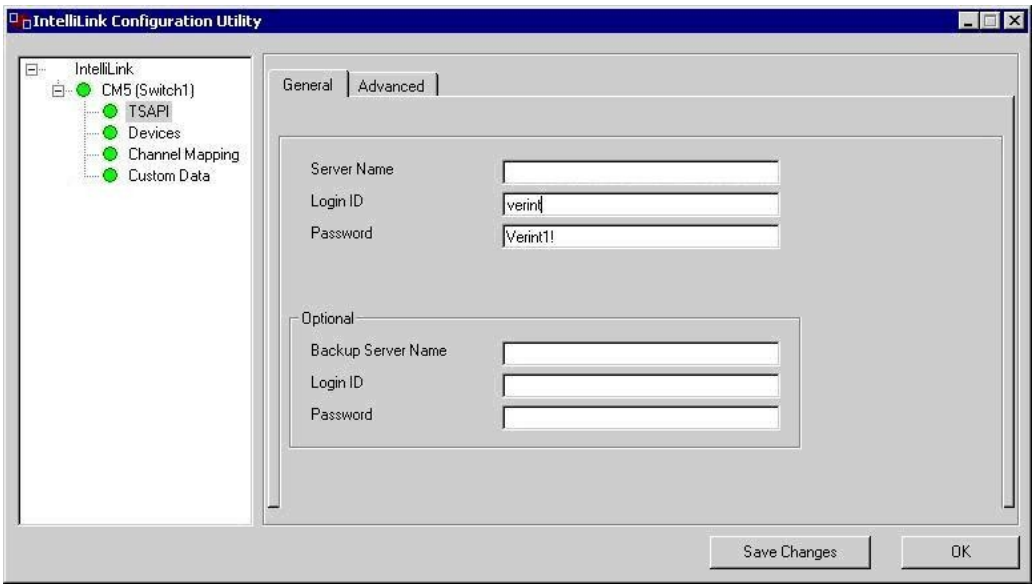


The **IntelliLink Configuration Wizard** screen is displayed (not shown). Select **Avaya Communication Manager**, and click **Next**.

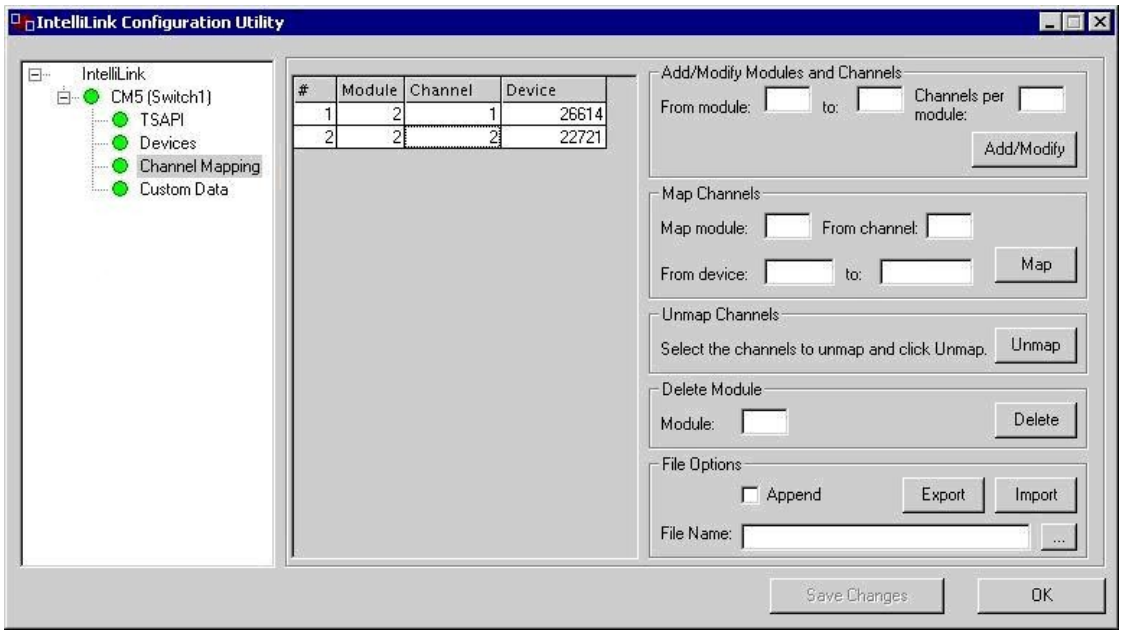
In the subsequent screen (not shown), select **TSAPI** for protocol, and click **Next**. Note that the TSAPI selection includes the DMCC.

The screen below is displayed. Enter a desired name for S**witch Name**, and click **Next**.

The **IntelliLink Configuration Utility** screen is displayed again, and updated with the newly added switch connection shown in the left pane. Select **CM5 (Switch1) > TSAPI** from the left pane. Select the **General tab** in the right pane. For **Login ID** and **Password**, enter the Verint user credentials from **Section 5.3**. Click **Save Changes**.

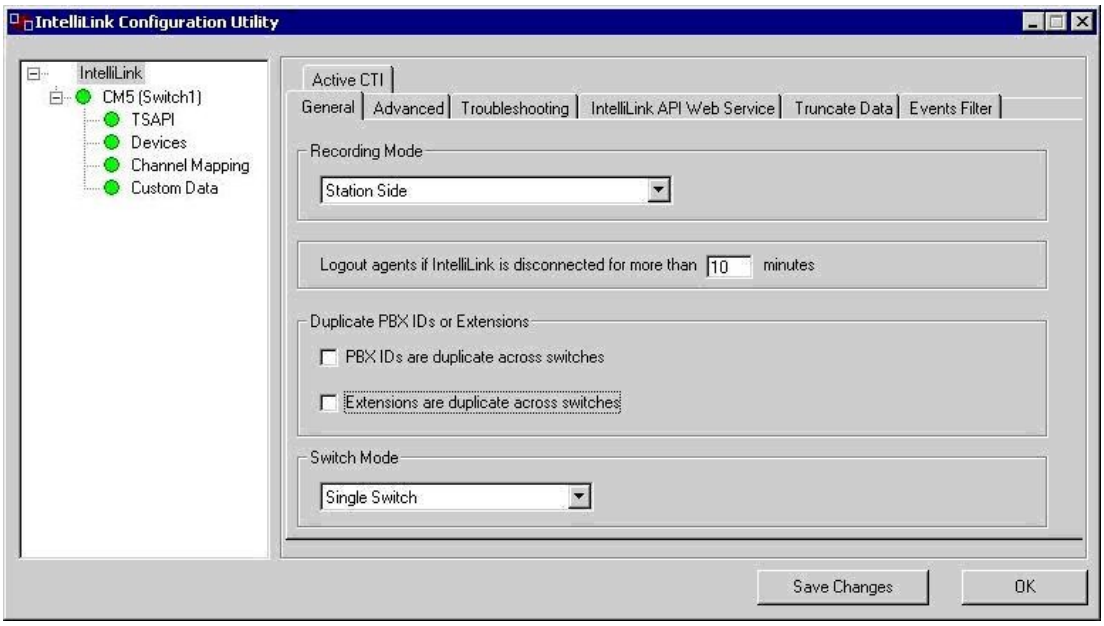


Select **CM5 (Switch1) > Channel Mapping** from the left pane. Use the **Add/Modify Modules and Channels** and the **Map Channels** sections to assign the physical agent stations from **Section 4.5** to relevant modules and channels. This will associate a virtual softphone with each physical agent station. In the compliance testing, two channels for module "2" were used, with module "2" denoting audio recording. The screen below is shown after entering the values and clicking **Save Changes**.



6.7. Administer Proactive Contact Connection

From the **IntelliLink Configuration Utility** screen, right-click on **IntelliLink** in the left pane, and select **New** to create a new switch connection.

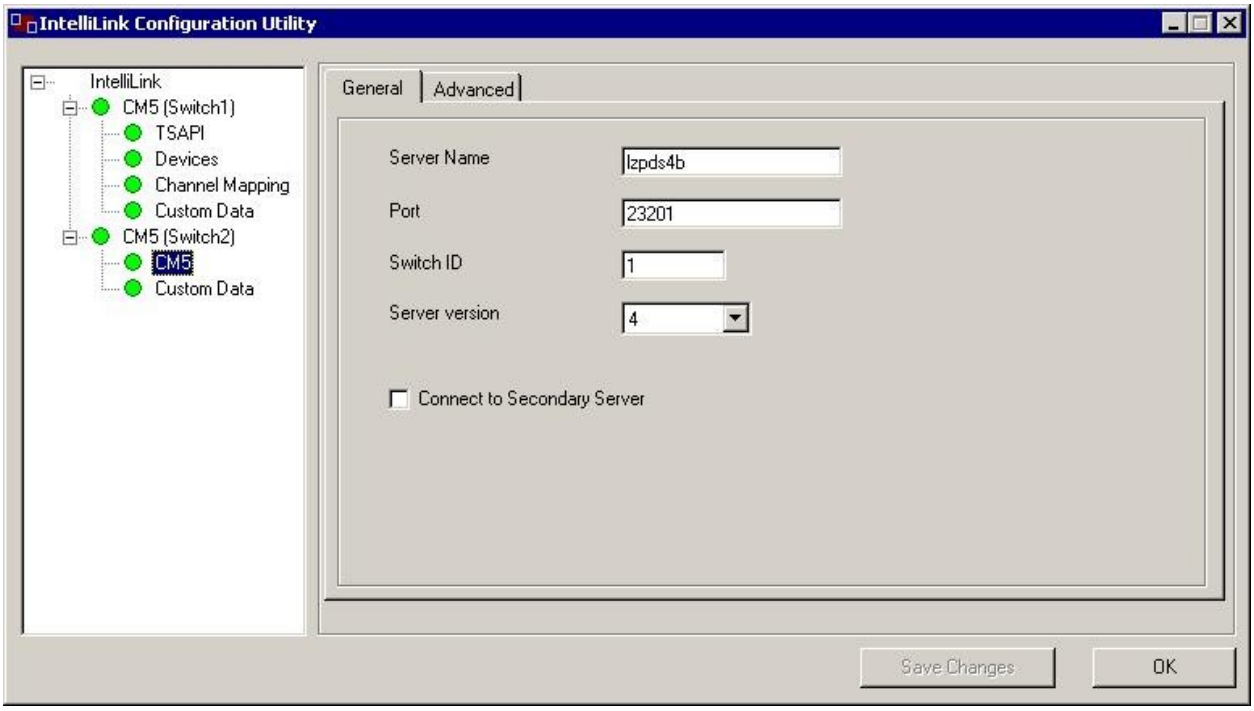


The **IntelliLink Configuration Wizard** screen is displayed (not shown). Select **Avaya PDS**, and click **Next**.

The screen below is displayed. For **Switch Name**, select the same switch name from **Section 6.6**, and click **Next**.

The **IntelliLink Configuration Utility** screen is displayed again, and updated with the newly added switch connection shown in the left pane. Select **CM5 (Switch2) > CM5** from the left pane. Select the **General tab** in the right pane. Enter the following values for the specified fields, and retain the default values for the remaining fields. Click **Save Changes**.

- **Server Name:** The host name of the Avaya Proactive Contact server.
- **Switch ID:** The switch number for the Communication Manager connection.
- **Server version:** "4"



7. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the Verint Impact 360 application, the application automatically registers the virtual IP softphones to Avaya Communication Manager using Avaya AES DMCC, obtains the current status on Avaya Proactive Contact using Event Services, and initiates Service Observing to add a virtual IP softphone to each logged in agent using Avaya AES DMCC.

For the manual part of the testing, each outbound call was handled manually on the agent with generation of unique audio content for the recordings. Necessary agent actions such as hold and reconnect were performed from the agent desktop to test the different call scenarios.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet cables to the Verint Impact 360 servers.

The verification of tests included using the Verint Impact 360 logs for proper message exchanges, and using the Verint Impact 360 web interface for proper logging and playback of the calls.

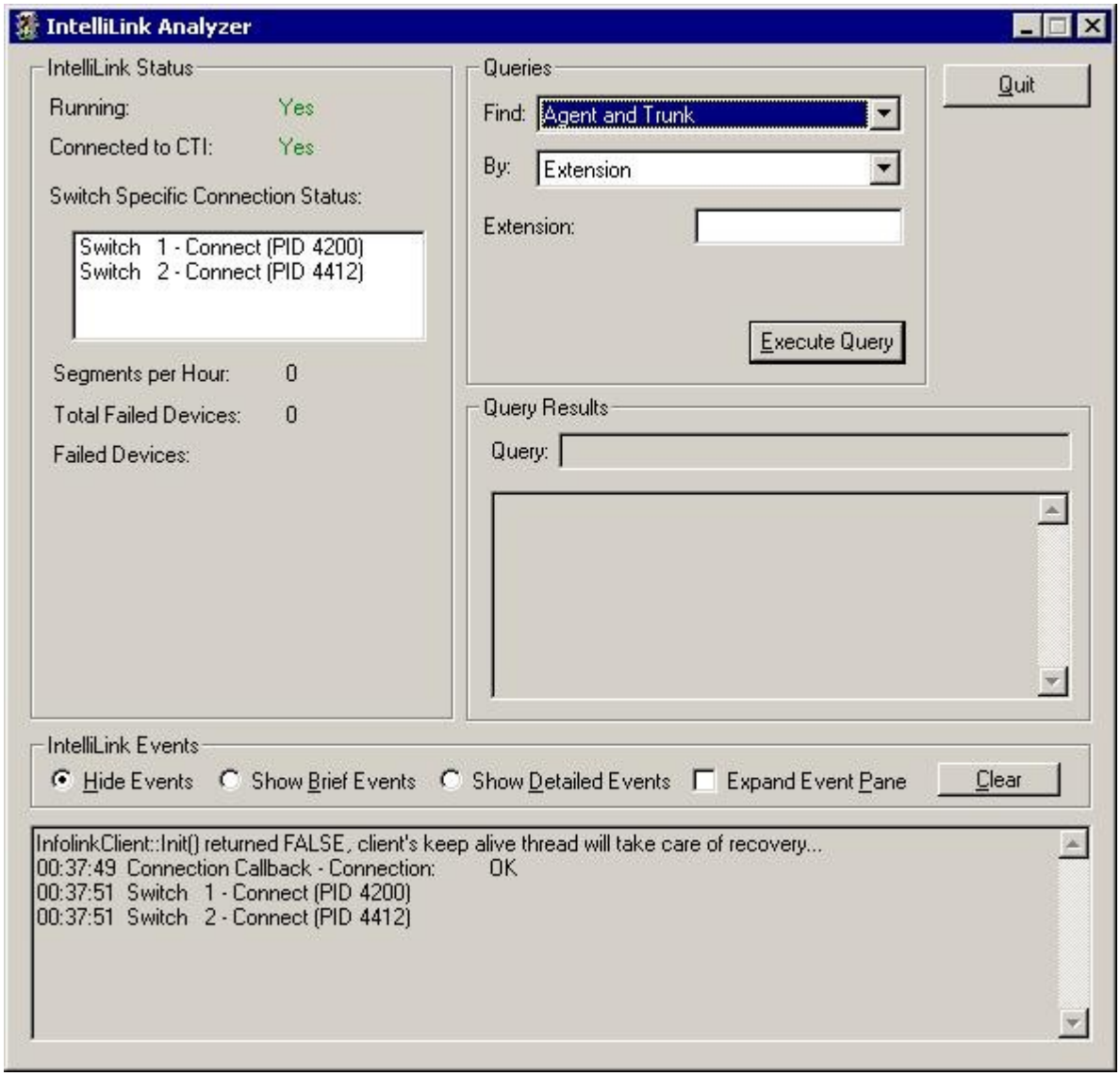
All test cases were executed and passed.

8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Communication Manager, Avaya AES, and Verint Impact 360.

Follow the procedures in **Section 6.5** to launch **System Tools** from the Verint Impact 360 server running the VoIP component, and select **IntelliLink Analyzer**.

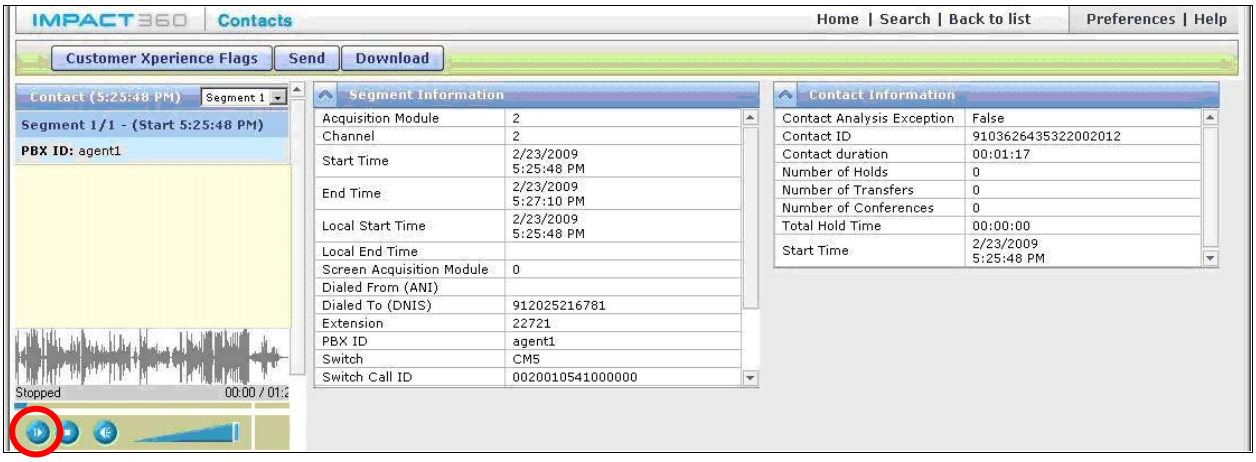
The **IntelliLink Analyzer** screen is displayed. Verify that the **Running** and **Connected to CTI** status are "Yes", as shown below. Also verify that the **Switch Specific Connection Status** section shows both switch connections to be "Connect".



Launch an outbound job on Avaya Proactive Contact, and log an agent in to handle an outbound call. Launch the Verint Impact 360 web interface with the hostname or IP address of the Verint Impact 360 server running the VoIP component, and log in with the appropriate credentials.

The **Contacts** screen displays a list of the call recordings. Verify that the first entry reflects the last call, with proper values in the **Start Time**, **Duration**, **Dial To (DNIS)**, and **Extension** fields. Double click on the entry to view the details.

Click the play icon highlighted below to verify the proper playback of the call recording.



9. Conclusion

These Application Notes describe the configuration steps required for Verint Impact 360 to successfully interoperate with Avaya Proactive Contact and Avaya Communication Manager using Service Observing. All feature and serviceability test cases were completed.

10. Additional References

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

1. *Administrator Guide for Avaya Communication Manager*, Document 03-300509, Issue 4.0, Release 5.0, January 2008, available at http://support.avaya.com.

2. *Avaya MultiVantage Application Enablement Services Administration and Maintenance Guide*, Release 4.2, Document ID 02-300357, Issue 10, May 2008, available at http://support.avaya.com.

3. *Avaya Proactive Contact Release 4.0 Administering Avaya Proactive Contact*, January 2008, available at http://support.avaya.com.

4. Verint Impact 360 documentation is available upon request to Verint technical support.

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.