

# Avaya Solution & Interoperability Test Lab

# **Application Notes for Configuring Avotus Enhanced Usage Reporting for Unified Communications with Avaya Aura® Communication Manager – Issue 1.0**

#### **Abstract**

These Application Notes describe the configuration procedures required to allow Avotus Enhanced Usage Reporting for Unified Communications to collect call detail records from Avaya Aura® Communication Manager using Avaya Reliable Session Protocol over TCP/IP. Avotus Enhanced Usage Reporting for Unified Communications collects, stores and processes these call records to provide usage analysis, call costing and billing capabilities.

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

Information in these Application Notes has been obtained through 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 describes a compliance-tested call detail recording (CDR) solution comprised of Avaya Aura ® Communication Manager (Communication Manager) and Avotus Enhanced Usage Reporting for Unified communications (Avotus EUR). Avotus EUR is a call accounting software application that uses call detail records from Communication Manager to provide reporting capabilities to business and IT managers to track and manage call usage and telecom expenses.

Communication Manager communicates to Avotus EUR via an Avaya Reliable Session Protocol (RSP) session over the TCP/IP network. The RSP session provides a transport mechanism for reliable delivery of CDR records. Communication Manager generates and sends the call records out in the RSP session while Avotus EUR collects, stores and processes the records at the other end.

Communication Manager can generate call detail records for intra-switch calls, inter-switch calls, inbound trunk calls and outbound trunk calls. In addition, split records can be generated for transferred calls and conferenced calls. Avotus EUR can support any CDR format provided by Communication Manager. However, during the compliance test, the expanded format was utilized.

# 2. General Test Approach and Test Results

This section describes the compliance testing used to verify interoperability of Avotus EUR application with Communication Manager. This section covers the general test approach and the test results. The testing covered feature and serviceability test cases. The feature testing covered the ability of Avotus EUR to capture and process CDR records.

The CDR records captured and displayed by Avotus EUR were compared for accuracy to the CDR records received by an Avaya Definity Reliable Data Transport Tool (RDTT), a CDR test tool. CDR records for various call types were generated, including internal calls, inbound and outbound trunk calls, PSTN calls, transferred calls, and conferenced calls. Calls were established using Avaya H.323 and SIP telephones.

The serviceability testing focused on the ability of Avotus EUR to recover from adverse conditions such as loss of network connectivity. With the use Avaya RSP, call records that were generated while Avotus EUR was disconnected from the network were not lost.

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 this DevConnect Application Note 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.

# 2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. The feature testing focused on verifying the proper parsing and displaying of expanded CDR data received from Communication Manager by Avotus EUR.

The following is a list of Interoperability tests that were performed:

- Internal calls
- Inbound Inter-Switch calls
- Outbound Inter-Switch calls
- Inbound PSTN calls
- Outbound PSTN calls
- Tandem calls to PSTN
- Hold and Resume
- Blind and Consultative Transfer
- Blind and Consultative Conference
- Call Forward
- Hunt Group calls
- Bridged Appearance
- Account codes
- Authorization codes
- Split CDR Records
- Serviceability

The serviceability testing focused on the ability of Avotus EUR to recover from adverse conditions such as loss of network connectivity, disabling and re-enabling the CDR Link and power cycling. With the use of Avaya RSP, CDR records that were generated while Avotus EUR was disconnected from the network were not lost.

#### 2.2. Test Results

All applicable test cases were executed and passed with the following observations:

- Hold time will not be included in call duration since Avotus EUR does not calculate/process hold time from Communication Manager.
- Even though Call Forward, Bridged Appearances, Hunt Groups and Split CDR are collected by Avotus EUR in their raw format, they are not processed when running the reports. Avotus EUR only processes incoming, outgoing and tandem calls for reporting purposes.
- Even though condition codes "E, G, F and I" are collected by Avotus EUR in their raw format, they are not processed when running the reports.

# 2.3. Support

Technical support for the Avotus EUR solution can be obtained by contacting Avotus:

- URL <a href="http://www.avotus.com/contact\_support.asp">http://www.avotus.com/contact\_support.asp</a>
- Phone (800) 840-2580

# 3. Reference Configuration

**Figure 1** illustrates the configuration used for the compliance test. In the sample configuration two sites, Sites A and B, are connected via a SIP trunk through Session Manager. Avotus EUR only monitors the calls at Site A. Site B is used to generate inter-site traffic across the SIP trunk.

Site A has a VMware virtual machine hosting Communication Manager, Session Manager, System Manager and Media Server. The Communication Manager is connected to an Avaya G450 Media Gateway. Site A also includes Avaya 96x1 Series H.323 and SIP Deskphones. In addition, Site A has connectivity to the PSTN. The configuration at Site B is similar to Site A and also uses the Session Manager at Site A. Avotus EUR connects via the LAN and establishes a CDR link to Communication Manager at Site A. Avotus EUR is also installed and configured on the VMware virtual machine.

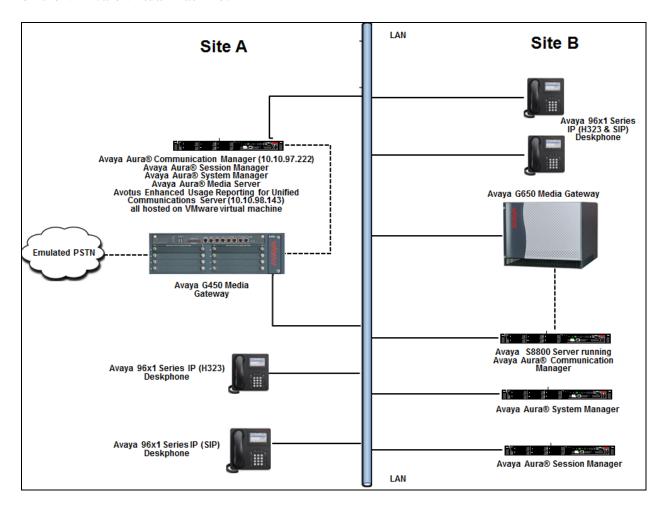


Figure 1: Test configuration for Avotus EUR Compliance Test

# 4. Equipment and Software Validated

The following equipment and software/firmware were used for the test configuration.

Equipment/Software	Release/Version
Avaya Aura® Communication Manager	7.0.1.2.0-FP1SP2
running on a virtual server	
Avaya Aura® Session Manager running on a	7.0.1.2.701230
virtual server	
Avaya Aura® System Manager running on a	7.0.1.2 Service Pack 2
virtual server	
Avaya Aura® Media Server running on a	7.7.0.375
virtual server	
Avaya G450 Media Gateway	37.41.0/1
Avaya 9611G IP Deskphones (H.323)	6.6229
Avaya 9641GS IP Deskphone (SIP)	7.0.1.1.5
Avotus Enhanced Usage Reporting for Unified	9.10
Communications running on Windows Server	
2008 R2 Standard SP1	

# 5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring CDR on Communication Manager. These steps are performed through the System Access Terminal (SAT). Communication Manager is configured to generate CDR records and send them to the IP address of the server running Avotus EUR using TCP/IP. The procedure covers the following areas:

- Administer IP Node Names
- Configure CDR Link
- Enable CDR for Intra-Switch Calls
- Enable CDR for Trunks Calls
- Configure Off-PBX-Telephone Configuration-Set

#### 5.1. Administer IP Node Names

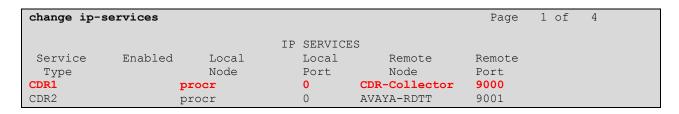
Use the **change node-names ip** command to create a new node name for the server running Avotus EUR. This node name is associated with the IP address of the server. In the sample configuration **CDR-Collector** was used for the name and **10.10.98.143** was used for the IP address. Also, take note of the node name **procr**. It will be used in the next step. The **procr** entry on this form was previously administered. The **AVAYA-RDTT** was used to setup the collection of CDR on the secondary link.

change node-name:	s ip		Page	1 of	2
		IP NODE NAMES			
Name	IP Address				
AVAYA-RDTT	10.10.98.71				
CDR-Collector	10.10.98.143				
DevvmAES	10.10.97.224				
DevvmAMS	10.10.97.232				
GW-G450	10.10.4.25				
Loopback	10.10.97.222				
SM-VM	10.10.97.228				
TFTP-Server	10.10.98.72				
default	0.0.0.0				
procr	10.10.97.222				

# 5.2. Configure CDR Link

Use the **change ip-services** command to define the CDR link between Communication Manager and Avotus EUR. To define a primary CDR link, provide the following information:

- **Service Type**: **CDR1** [If needed, a secondary link can be defined by setting Service Type to CDR2.]
- **Local Node**: **procr** [For Communication Manager used during compliance testing, set the Local Node to the node name of the processor board.]
- Local Port: 0 [The Local Port is fixed to 0 because Communication Manager initiates the CDR link.]
- **Remote Node**: **CDR-Collector** [The Remote Node is set to the node name previously defined in **Section 5.1**.]
- **Remote Port**: **9000** [The Remote Port may be set to a value between 5000 and 64500 inclusive, and must match the port configured in Avotus EUR.]



For this solution the RSP is used. On **Page 3** of the **ip-services** form, set the **Reliable Protocol** field to **y**.

change ip-se	rvices				Page 3 of	4
Service Type	Reliable Protocol	SESSION Packet Resp Timer	LAYER TIMERS Session Connect Message Cntr	SPDU Cntr	Connectivity Timer	
CDR1 CDR2	<b>у</b> У	30 30	3 3	3 3	60 60	

Enter the **change system-parameters cdr** command to set the parameters for the type of calls to track, and for the format of the CDR data. The example below shows the settings used during the compliance test. Provide the following information:

- CDR Date Format: month/day
- Primary Output Format: expanded
- Primary Output Endpoint: CDR1

The remaining parameters define the type of calls that will be recorded and what data will be included in the record. Refer to documents in **Section 9** for a full explanation of each field. The test configuration used some of the more common fields described below.

- Use Legacy CDR Formats?: y [Allows CDR formats to use 3.x CDR formats for "y". If the field is set to "n", then CDR formats utilize the 4.x CDR formats.]
- Intra-switch CDR: y [Allows call records for internal calls involving specific stations. Those stations must be specified in the intra-switch cdr form.]
- **Record Outgoing Calls Only?**: **n** [Allows incoming trunk calls to appear in the CDR records along with the outgoing trunk calls.]
- Outg Trk Call Splitting?: y [Allows a separate call record for any portion of an outgoing call that is transferred or conferenced.]
- Inc Trk Call Splitting?: y [Allows a separate call record for any portion of an incoming call that is transferred or conferenced.]
- **CDR Account Code Length: 4** [The length may be set to a value between 1 and 15. However, during the compliance test, "4" was used.]

```
change system-parameters cdr
                                                                          Page 1 of 1
                                CDR SYSTEM PARAMETERS
Node Number (Local PBX ID):
                                                           CDR Date Format: month/day
      Primary Output Format: expanded Primary Output Endpoint: CDR1
    Secondary Output Format: unformatted Secondary Output Endpoint: CDR2
      Use ISDN Layouts? n
Use Enhanced Formats? n
Use Legacy CDR Formats? y

Enable CDR Storage on Disk? n
Condition Code 'T' For Redirected Calls? n
Remove # From Called Number? n
                                            Remove # From Called Number? n
  odified Circuit ID Display? n

Record Outgoing Calls Only? n

Suppress CDR for Ineffective Call Attempts? y

Disconnect Information in Place of FRL? n

Intra-switch CDR? y

Outg Trk Call Splitting? y

Outg Attd Call Record? y

Interworking Feat-flag? n
Modified Circuit ID Display? n
                                                                     Intra-switch CDR? y
Force Entry of Acct Code for Calls Marked on Toll Analysis Form? n
                                    Calls to Hunt Group - Record: member-ext
Record Called Vector Directory Number Instead of Group or Member? n
Record Agent ID on Incoming? n Record Agent ID on Outgoing? y
  Record Call-Assoc TSC? n Digits to Record for Outgoing Calls: dialed
   Privacy - Digits to Hide: 0
                                                   CDR Account Code Length: 4
Remove '+' from SIP Numbers? Y
```

#### 5.3. Enable CDR for Intra-Switch Calls

If the **Intra-switch CDR** field is set to **y** on **Page 1** of the **system-parameters cdr** form, then use the **change intra-switch-cdr** command to define the extensions that will be subject to call detail records. In the **Extension** field, enter the specific extensions whose usage will be tracked.

**Note:** To simplify the process of adding multiple extensions in the **Assigned Members** field, the **Intra-switch CDR by COS (SA8202)** special feature may be utilized. To utilize this feature, contact an authorized Avaya account representative to obtain the license.

change intra-switch-cdr INTRA-SWITCH CDR			<b>Page 1</b> of 3
Extension	Assic Extension	gned Members: Extension	8 of 1000 administered Extension
56103 56201			

#### 5.4. Enable CDR for Trunk Calls

For each trunk group for which CDR records are desired, verify that CDR reporting is enabled. To do this, use the **change trunk-group n** command, where **n** is the trunk group number, and verify that the **CDR Reports** field is set to **y**. This applies to all trunk group types.

The example below shows the ISDN-PRI trunk to the PSTN.

```
Change trunk-group 4

TRUNK GROUP

Group Number: 4

Group Type: isdn

CDR Reports: y

Group Name: To-IPO 36_44

COR: 1

TN: 1

TAC: #004

Direction: two-way

Outgoing Display? n

Carrier Medium: PRI/BRI

Dial Access? n

Busy Threshold: 255 Night Service:

Queue Length: 0

Service Type: tie

Auth Code? n

TestCall ITC: rest

Far End Test Line No:
```

The example below shows the SIP trunk between Sites A and B. This SIP trunk actually terminates to Session Manager, which then routes calls to Site B over another SIP trunk.

```
Change trunk-group 1

TRUNK GROUP

Group Number: 1

Group Type: sip

Group Name: Trunk to SM on VM

Direction: two-way

Dial Access? n

Queue Length: 0

Service Type: tie

Auth Code? n

Member Assignment Method: auto

Signaling Group: 1

Number of Members: 24
```

# 5.5. Configure Off-PBX-Telephone Configuration-Set

SIP endpoints and off-pbx-telephone stations will be automatically created in Communication Manager when users (SIP endpoints) are created in Session Manager.

However, the **off-pbx-telephone configuration-**set form needs to be modified. Enter **change off-pbx-telephone configuration-set** and disable the **CDR for Calls to EC500 Destination** field by setting it to **n**. Example below shows **off-pbx-telephone configuration-set 1**. The same will apply to other applicable configuration sets.

```
change off-pbx-telephone configuration-set 1
                                                                       1 of
                                                                              1
                                                                Page
                                     CONFIGURATION SET: 1
                         Configuration Set Description:
                                  Calling Number Style: network
                                  CDR for Origination: phone-number
                    CDR for Calls to EC500 Destination? n
                          Fast Connect on Origination? n
                          Post Connect Dialing Options: dtmf
                         Cellular Voice Mail Detection: timed (seconds): 4
                                         Barge-in Tone? n
                           Calling Number Verification? y
             Call Appearance Selection for Origination: primary-first
                                      Confirmed Answer? n
Use Shared Voice Connections for Second Call Answered? n
Use Shared Voice Connections for Second Call Initiated? n
              Provide Forced Local Ringback for EC500? n
                       Apply Ringback upon Receipt of: Call-Proceeding
```

# 6. Configure Avotus Enhanced Usage Reporting for Unified Communications

This section describes the configuration of Avotus EUR. Avotus installs, configures, and customizes the EUR application for the end customers. Thus, this section only describes the interface configuration, so that Avotus EUR can receive CDR data from Communication Manager. The procedure covers the following areas:

- Login to Avotus EUR
- Configure a site
- Configure script and collection
- Start collection

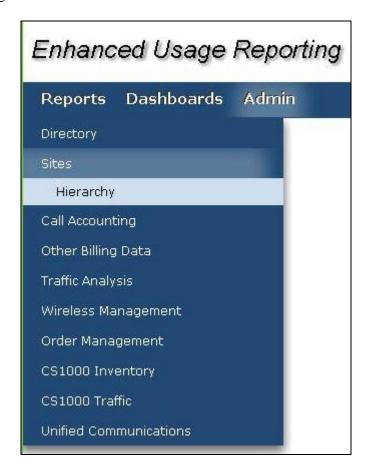
# 6.1. Login to Avotus EUR

To configure Avotus EUR, double click on the Avotus EUR icon on desktop, in and provide credentials to gain access into Avotus EUR in the window shown below.

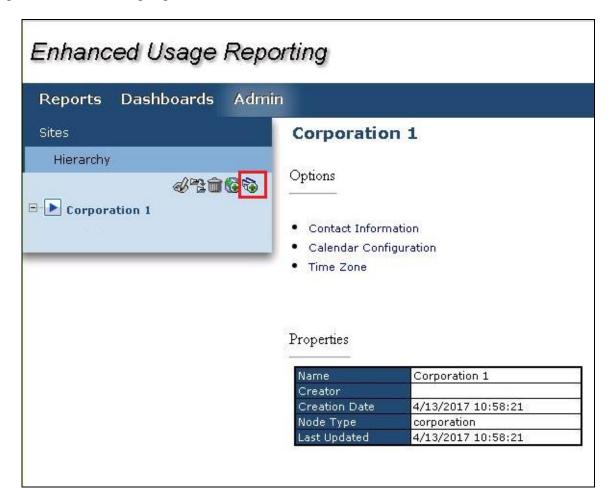


# 6.2. Configure a Site

From the **Enhanced Usage Reporting** screen shown below, navigate to **Admin**  $\rightarrow$  **Sites**  $\rightarrow$  **Hierarchy** to configure a site.



In the screen shown below, click on **Corporation 1** (created during install time). Click on the top right **Add Site** icon highlighted below to add a site.



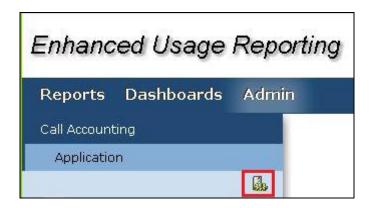
In the **Add Site** window shown below, enter an appropriate name for **Site Name** field and click on the **OK** icon highlighted below.



To assign the site created above for collection of data; navigate to Admin → Call Accounting → Application as shown in the screen below.



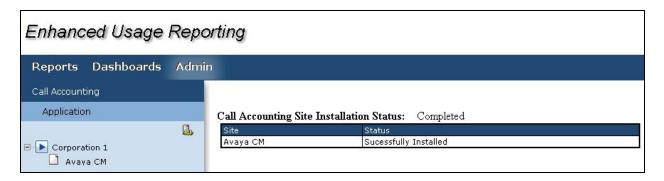
In the **Application** section, start the configuration by clicking on the **Configure** icon as highlighted in the screen below.



In the **Site Assignments** window seen below, select the server name from the drop down menu to assign it to the site. In the example below, "WIN-IB7NT8C7NJP" is the Windows server name and "Avaya CM" is the site created earlier in this section.



Screen below shows the successful assigning of the site for collection.

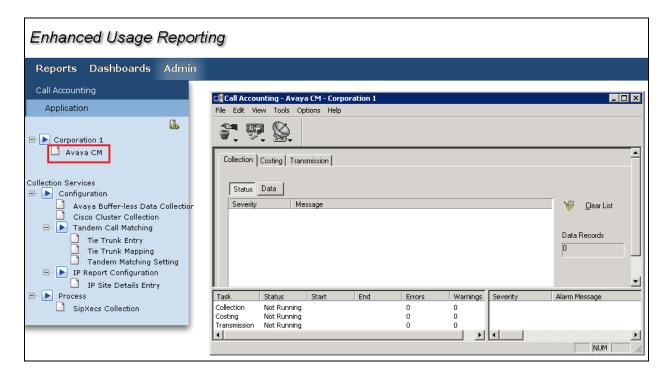


# 6.3. Configure Script and Collection

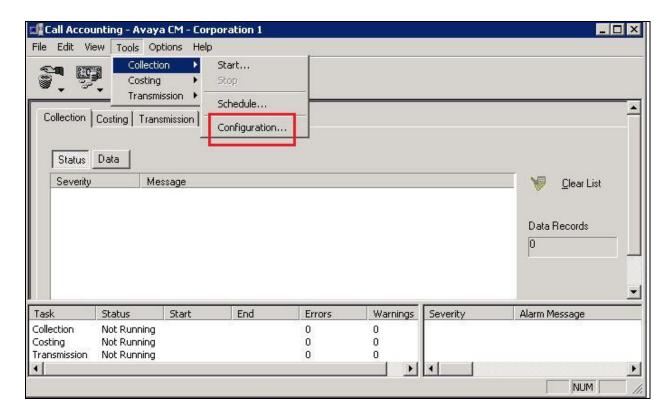
This section explains the configuring of the script and collection of the CDR records by Avotus EUR.

# 6.3.1. Configuring the Script

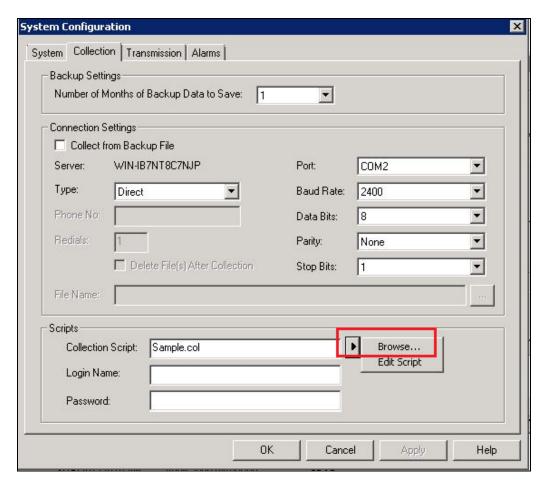
To configure the script for collection of data, navigate to Admin  $\rightarrow$  Call Accounting  $\rightarrow$  Application  $\rightarrow$  Corporation 1  $\rightarrow$  Avaya CM. The Call Accounting window is launched on the right side as shown in the screen below.



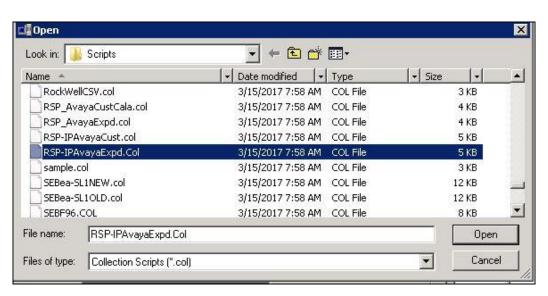
From the **Call Accounting** window navigate to **Tools**  $\rightarrow$  **Collection**  $\rightarrow$  **Configuration** as shown below.



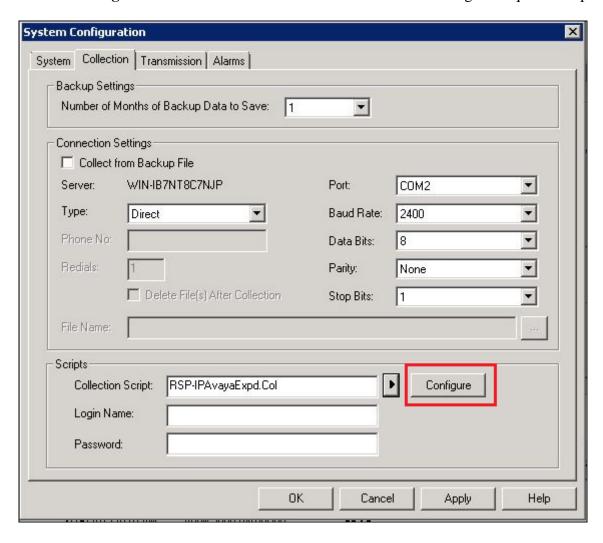
From the **System Configuration** window as shown below, navigate to **Collection** tab and under the section **Scripts**, click the **Browse** icon to select a script for **Collection Script**.



From the **Scripts** folder that is launched as shown below, select the **RSP-IPAvayaExpd.Col** script.



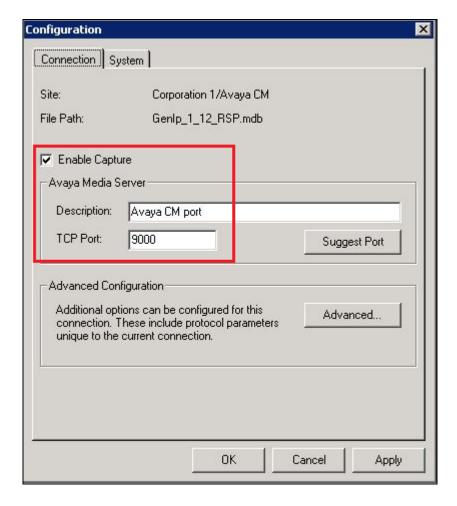
Click on the **Configure** button as shown in the screen below after selecting the required script.



In the Configuration window as seen below, configure the following under the Connection tab,

- Ensure **Enable Capture** is checked.
- **Description**: Provide a detailed description.
- **TCP Port**: Enter "9000" as this is the port configured in Communication Manager in **Section 5.2**.

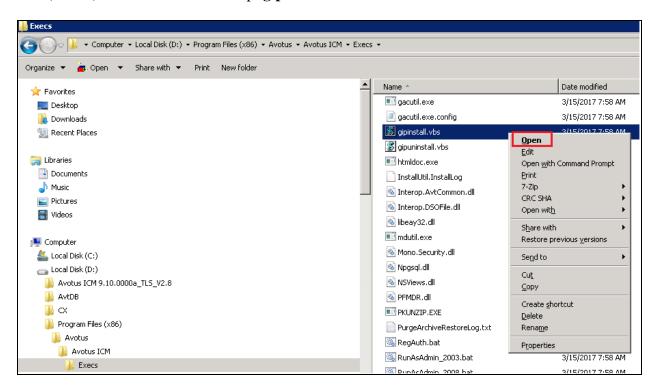
Click on the **Apply** button.

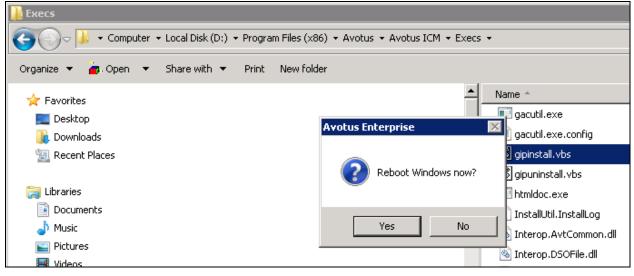


Also retain default values for all other fields in the **System Configuration** window shown earlier in this section and click on the **OK** button.

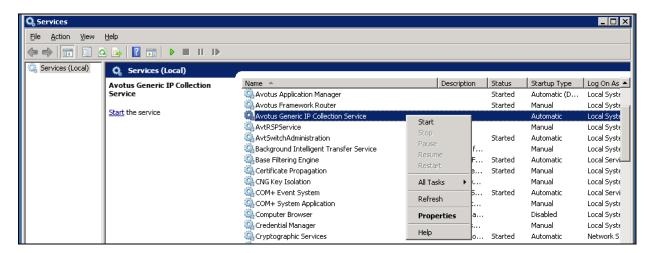
# 6.3.2. Installing the Avotus Generic IP Collection Service

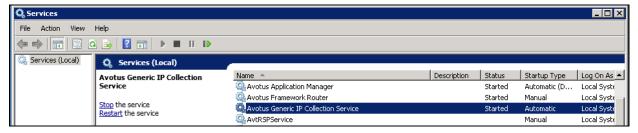
To install the Avotus Generic IP Collection Service, navigate to "<Avotus install folder>\Avotus ICM\Execs\" folder and run the script **gipinstall.vbs** as shown in the screens below.



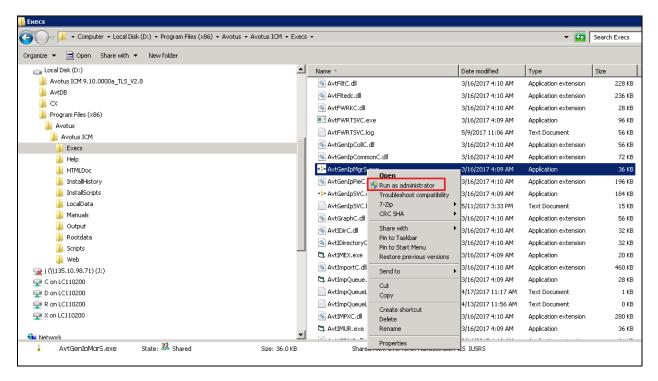


Once the rebooting of the system is completed, the **Avotus Generic IP Collction Service** will be installed under Windows Services as shown in the screen below. Start this service and ensure it is running.

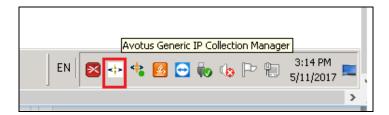




To view the status of Avotus EUR connection with Avaya RSP session, navigate to "<Avotus install folder>\Avotus ICM\Execs" and run the **AvtGenIpMgrS.exe** as shown in the screen below.



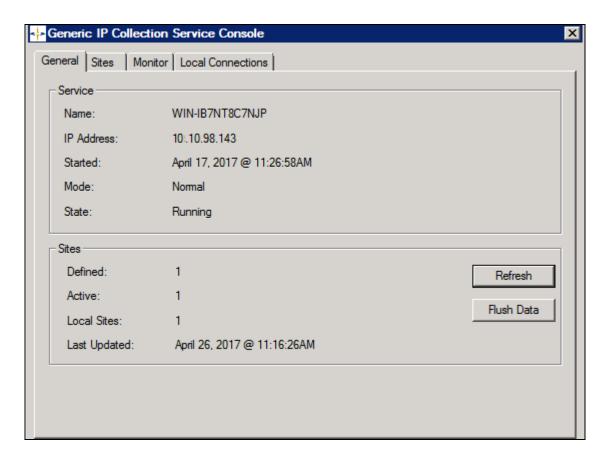
An icon will appear in the task bar / System tray of Windows by the name of **Avotus Generic IP Collection Manager** as shown in the screen below.



Right click on this icon and click on **Show Collection Console** option as shown below.

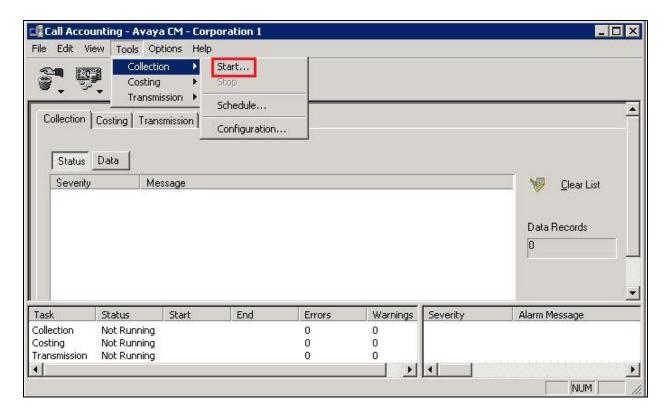


The **Generic IP Collection Service Console** will appear as shown below. User can click on the different tabs to view the status.

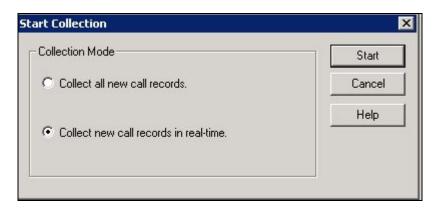


#### 6.4. Start Collection

To start collection of CDR data, from the **Call Accounting** window navigate to **Tools** → **Collection** → **Start** as shown in the screen below. This window is invoked as shown in **Section** 6.3.1.



In the **Start Collection** window as shown below, select the **Collect new call records in real-time** option and click on the **Start** button.



The collected raw CDR data can be found in the "CallAccountingBackup" folder, which is under the "/Rootdata/<Corporation number>/<Site number>" folder (not shown).

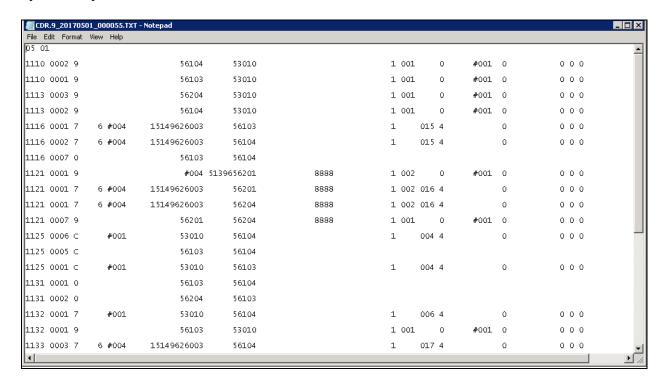
# 7. Verification Steps

The following steps may be used to verify the configuration:

On the SAT of Communication Manager, enter the **status cdr-link** command and verify that the CDR link state is up as shown below.

```
status cdr-link
                                CDR LINK STATUS
                   Primary
                                                Secondary
      Link State: up
                                                up
      Date & Time: 2017/05/01 11:34:05
                                                2017/05/01 15:48:43
 Forward Seq. No: 22
Backward Seq. No: 0
                                                0
CDR Buffer % Full:
                    0.00
                                                  0.00
     Reason Code: OK
                                                OK
```

Place internal, inbound trunk and outbound trunk calls to and from various telephones and verify that Avotus EUR received the CDR record for the call. Compare the values of data fields in the CDR record with the expected values and verify that the values match. Screen below shows the raw CDR data collected by Avotus EUR which was then compared with the CDR data collected by the Avaya RDTT.



#### 8. Conclusion

These Application Notes describe the steps required to configure Avotus Enhanced Usage Reporting for Unified Communications to interoperate with Avaya Aura® Communication Manager, including establishing a CDR link with Avaya RSP enabled and capturing/processing call records. All feature and serviceability test cases described in **Section 2.1** were passed with the observations pointed in **Section 2.2**.

#### 9. Additional References

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

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

- 1. Administering Avaya Aura® Session Manager, Release 7.0.1 Issue 2, May 2016.
- 2. Deploying Avaya Aura® System Manager, Release 7.0.1 Issue 2, August 2016.
- 3. Administering Avaya Aura® System Manager for Release 7.0.1, Release 7.0.1 Issue 3, January 2017.
- 4. Administering Avaya Aura® Communication Manager, Release 7.0.1, 03-300509, Issue 2.1, August 2016.
- 5. Avaya Aura® Communication Manager Feature Description and Implementation, Release 7.0.1, 555-245-205, Issue 3, October 2016.

Product documentation for Avotus products may be found at, <a href="http://avotus.com/telecom-enhanced-usage-reporting.asp">http://avotus.com/telecom-enhanced-usage-reporting.asp</a>

#### ©2017 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 DevConnect Program at devconnect@avaya.com.