AVAYA

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.

KP; Reviewed:
SPOC 2/19/2019
Solution & Interoperability Test Lab Application Notes
©2019 Avaya Inc. All Rights Reserved.
1 of 29
AvotusEUR_CM80

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 makes use CDRs 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 connection. The RSP session provides a transport mechanism for reliable delivery of CDRs. Communication Manager generates and sends the CDRs in a RSP session, while Avotus EUR collects, stores and processes the CDRs at the other end.

Communication Manager can generate CDRs 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 conference 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 call records.

The CDRs captured and displayed by Avotus EUR were compared for accuracy to the CDRs received by an Avaya Definity Reliable Data Transport Tool (RDTT), a CDR test tool. CDRs for various call types were generated by manually placing internal calls, inbound and outbound trunk calls, PSTN calls, transfer calls, and conference calls. Calls were made using a PSTN line, 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, CDRs 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.

For the testing associated with this Application Note, the interface between Avaya systems and the Avotus EUR did not include use of any specific encryption features as requested by Avotus.

Encryption (TLS/SRTP) was used internally between Avaya 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
- Hunt Groups
- Bridged Appearance
- Account codes
- Authorization codes
- Split CDR Records
- CDR Records on Local Survivable Processor (LSP) as the main Communication Manager down
- 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, call 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:

- 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 – http://www.avotus.com/contact_support.asp
- Phone – (800) 840-2580

3. Reference Configuration

Figure 1 illustrates the configuration used for the compliance test. In the sample configuration two sites, Sites 1 and 2, are connected via a SIP trunk through Session Manager. Avotus EUR only monitors the calls at Site 1. Site 2 is used to generate inter-site traffic across the SIP trunk.

Site 1 has a VMWare virtualized environment hosting Communication Manager, Session Manager, System Manager and Media Server. The Communication Manager is connected to an Avaya G450 Media Gateway. Site 1 also includes Avaya 96x1 Series H.323 and SIP telephones. In addition, Site 1 has connectivity to the PSTN. The configuration at Site 2 has Avaya IP Office Server Edition. Avotus EUR connects via the LAN and establishes a CDR link to Communication Manager at Site 1. Avotus EUR is also installed and configured on VMWare virtualized environment.
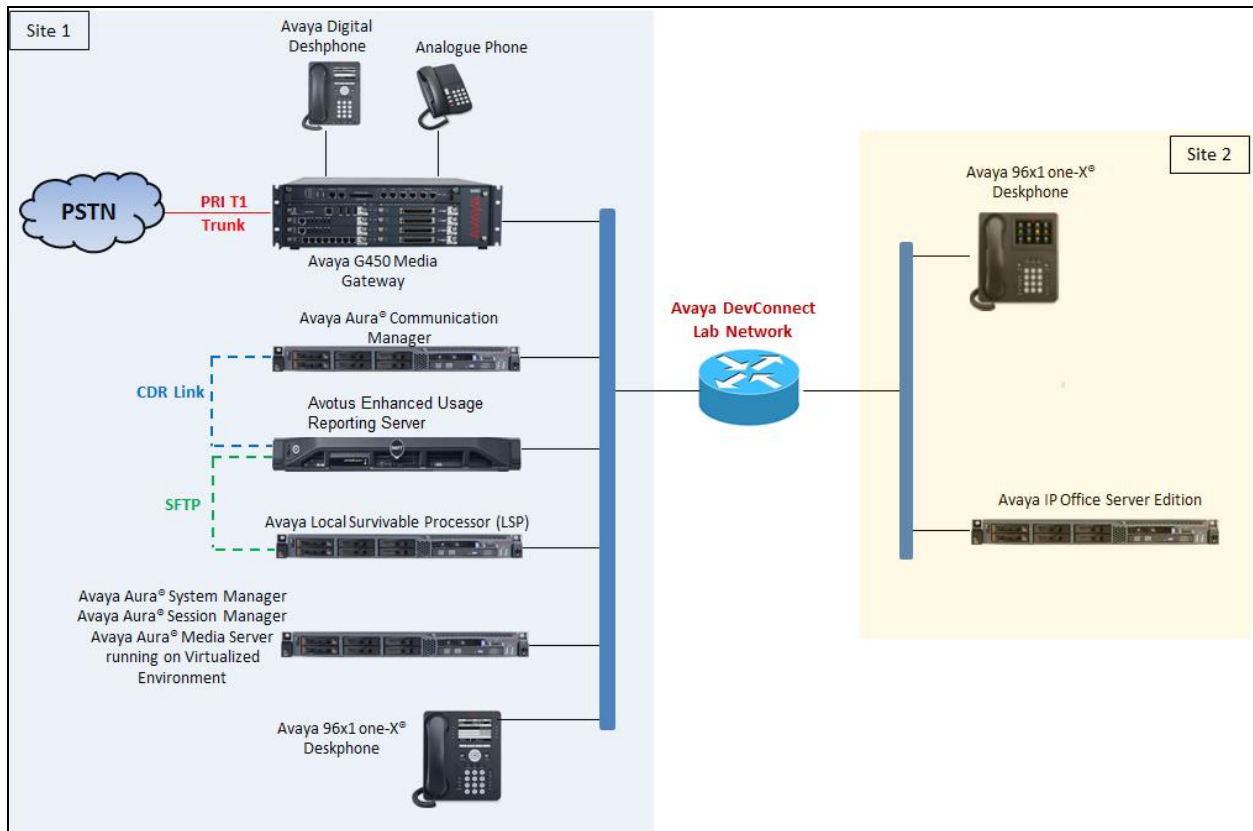
Figure 1: Test configuration for Avotus EUR Compliance Test

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 running on Virtualized Environment	8.0.1.0.0-FP1 Build 8.0.1.0.0.822.25031
Avaya Aura® System Manager running on Virtualized Environment	8.0.1.0 Build 8.0.1.0.038826
Avaya Aura® Session Manager running on Virtualized Environment	8.0.1.0 Build 8.0.1.0.801007
Avaya Aura® Media Server running on Virtualized Environment	8.0.0.173
Avaya G450 Media Gateway • MGP	 40.20.0
Avaya 96x1 IP H.323 Deskphones	6.7104
Avaya 96x1 IP SIP Deskphones	7.1.4.0.11
Avaya 1416 Digital Deskphone	FW1
Avotus Enhanced Usage Reporting – Call Accounting Software	ICM Version: 9.10.0001

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring call detail recording (CDR) in Communication Manager. These steps are performed through the System Access Terminal (SAT). Communication Manager will be configured to generate CDR records using RSP over TCP/IP to the IP address of the server running Avotus EUR call accounting software.

5.1. Configure Node-Names IP

Use the **change node-names ip** command to create a new node name, for example, **Avotus**. This node name is associated with the **IP Address** of the server running the Avotus EUR application. 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.

```
change node-names ip                                         Page   1 of   2
                                   IP NODE NAMES
    Name                IP Address
AMS1               10.33.1.30
CMS18              10.33.1.20
RDTT               10.10.98.86
Avotus             10.10.98.143
default            0.0.0.0
lsp                10.33.1.17
procr              10.33.1.6
procr6             ::
```

5.2. Configure IP Services

Use the **change ip-services** command to define the CDR link to use the RSP over TCP/IP.
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**.
- **Local Port**: **0 -** The local Port is fixed to 0 because Avaya Communication Manager initiates the CDR link.
- **Remote Node**: **Avotus -** The Remote Node is set to the node name previously defined.
- **Remote Port**: **9002 -** The Remote Port may be set to a value between 5000 and 64500 inclusive and must match the port configured in the Avotus application.

```
change ip-services                                          Page   1 of   4

                              IP SERVICES
 Service       Enabled      Local         Local        Remote        Remote
  Type                      Node          Port         Node          Port
AESVCS         y      procr              8765
CDR1                  procr              0         Avotus            9002
CDR2                  procr              0         RDTT              9001
```

On **Page 3** of the ip-services form, enable the Reliable Session Protocol for the primary CDR link that is configured for Avotus EUR by setting the **Reliable Protocol** field to "y"

```
change ip-services                                          Page   3 of   4

                          SESSION LAYER TIMERS
 Service      Reliable  Packet Resp  Session Connect  SPDU  Connectivity
  Type        Protocol    Timer       Message Cntr    Cntr     Timer

 CDR1            y          30              3           3        60
 CDR2            y          30              3           3        60
```

5.3. Configure System Parameters CDR

Enter the **change system-parameters cdr** command from the SAT to set the parameters for the type of calls to track and 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. See reference [2] for a full explanation of each field. The test configuration used some of the more common fields described below.

- **Enable CDR Storage on Disk?** Set to "y", this field must be enabled so that CDR data can be saved into a file in the local survivable processor when the main Communication Manager becomes inactive
- **Use Legacy CDR Formats?** Set to "n" **-** Allows CDR formats to use 4.x CDR formats. If the field is set to "y", then CDR formats utilize the 3.x CDR formats
- **Intra-switch CDR** set to "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?** Set to "n" **-** Allows incoming trunk calls to appear in the CDR records along with the outgoing trunk calls
- **Inc Trk Call Splitting?** Set to "y" **-** Allows a separate call record for any portion of an incoming call that is transferred or conferenced
- **Call Account Code Length** Set to "5" **-** The length may be set to a value between 1 and 15. However, during the compliance test, "5" was used

```
change system-parameters cdr
                          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                     Enable CDR Storage on Disk? y
       Use Enhanced Formats? n      Condition Code 'T' For Redirected Calls? n
       Use Legacy CDR Formats? n                  Remove # From Called Number? n
Modified Circuit ID Display? n                              Intra-switch CDR? y
                Record Outgoing Calls Only? n      Outg Trk Call Splitting? y
  Suppress CDR for Ineffective Call Attempts? y       Outg Attd Call Record? y
      Disconnect Information in Place of FRL? y      Interworking Feat-flag? n
 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? y
Record Agent ID on Incoming? n       Record Agent ID on Outgoing? y
     Inc Trk Call Splitting? y                   Inc Attd Call Record? n
  Record Non-Call-Assoc TSC? n          Call Record Handling Option: warning
      Record Call-Assoc TSC? n   Digits to Record for Outgoing Calls: dialed
   Privacy - Digits to Hide: 0                   CDR Account Code Length: 5
Remove '+' from SIP Numbers? y
```

5.4. Configure Intra-Switch CDR

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 Assigned Members field, enter the specific extensions whose usage will be tracked.

```
change intra-switch-cdr                                      Page   1 of   3
                           INTRA-SWITCH CDR

                              Assigned Members:   15   of 5000   administered
   Extension          Extension            Extension          Extension
   3301
   3302
   3303
   3401
   3402
Use 'list intra-switch-cdr' to see all members, 'add intra-switch-cdr' to add
new members and 'change intra-switch-cdr <ext>' to change/remove other members
```

5.5. Configure Off-PBX-Telephone Configuration Set

SIP endpoints and off-pbx-telephone stations will be automatically created in Communication manager when SIP endpoints were created in Session Manager. However, the off-pbx-telephone configuration-set form needs to be modified in order to call records of SIP endpoint are generated correctly. Enter **change off-pbx-telephone configuration-set 1**and set **CDR for Origination to "none"** and disable the **CDR for Calls to EC500 Destination?** to "n".

```
change off-pbx-telephone configuration-set 1                   Page   1 of   1

                                CONFIGURATION SET: 1

                      Configuration Set Description:
                             Calling Number Style: network
                             CDR for Origination: none
                  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

              Location to Route Incoming Overlap Calls: station-location-if-set
```

5.6. Enable CDR in Trunk Group

Enter the command **change trunk-group <id>** which the <id> is the trunk number that needs to be modified. Set **CDR Report** field to "y" to enable call record for calls going in and out from this trunk group. Note that this field is set to "y" by default.

```
change trunk-group 1                                          Page   1 of  21
                             TRUNK GROUP

Group Number: 1                      Group Type: sip        CDR Reports: y
  Group Name: For-Private                  COR: 1      TN: 1      TAC: #01
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                     Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n
                                          Member Assignment Method: auto
                                                   Signaling Group: 1
                                                 Number of Members: 14
```

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 the Avotus server, [Avotus ICM icon], and provide credentials to gain access into Avotus EUR in the Sign In window shown below.

6.2. Configure a Site

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

Solution & Interoperability Test Lab Application Notes
©2019 Avaya Inc. All Rights Reserved.
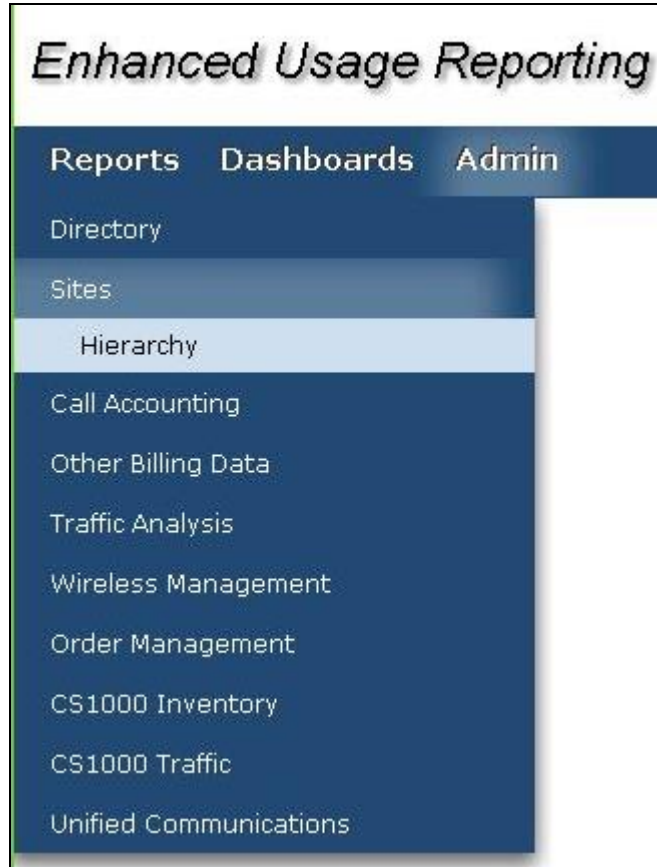
In the screen shown below, click on **Avotus** (created during install time). Click on the top right **Add Site** icon highlighted below to add a site.

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

KP; Reviewed:
SPOC 2/19/2019
Solution & Interoperability Test Lab Application Notes
©2019 Avaya Inc. All Rights Reserved.
14 of 29
AvotusEUR_CM80

To assign the site created above for collection of data; navigate **to Admin → Call Accounting → Application** as shown in the screen below.
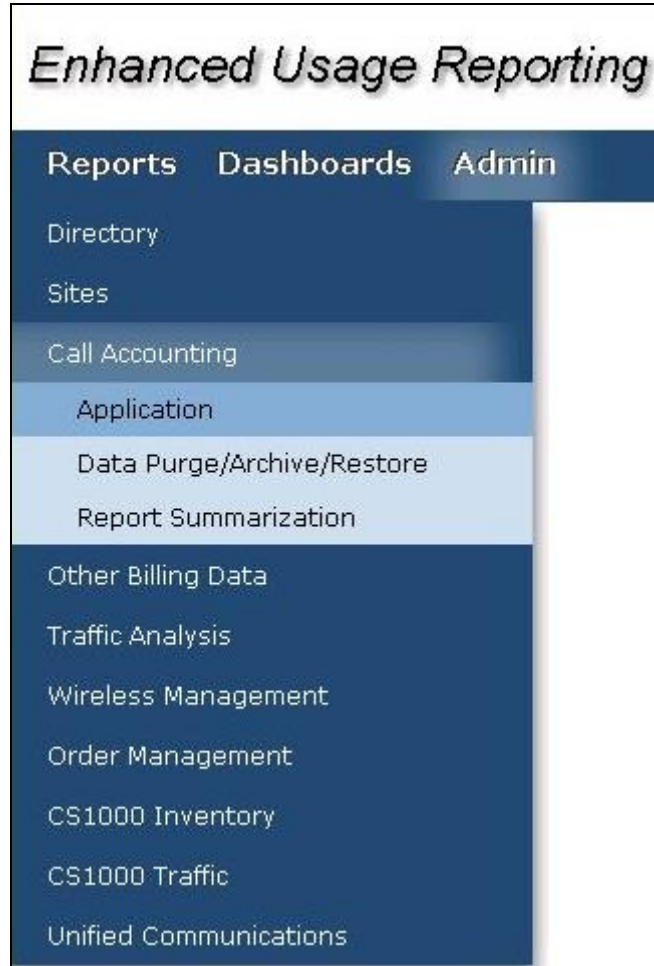
In the **Application** section, start the configuration by clicking on the **Configure** icon as highlighted in the screen below.

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

6.3.1. Configuring the Script

To configure the script for collection of data, navigate to **Admin → Call Accounting → Application → Avotus → Avaya CM**. The **Call Accounting** window is launched as shown in the screen below.
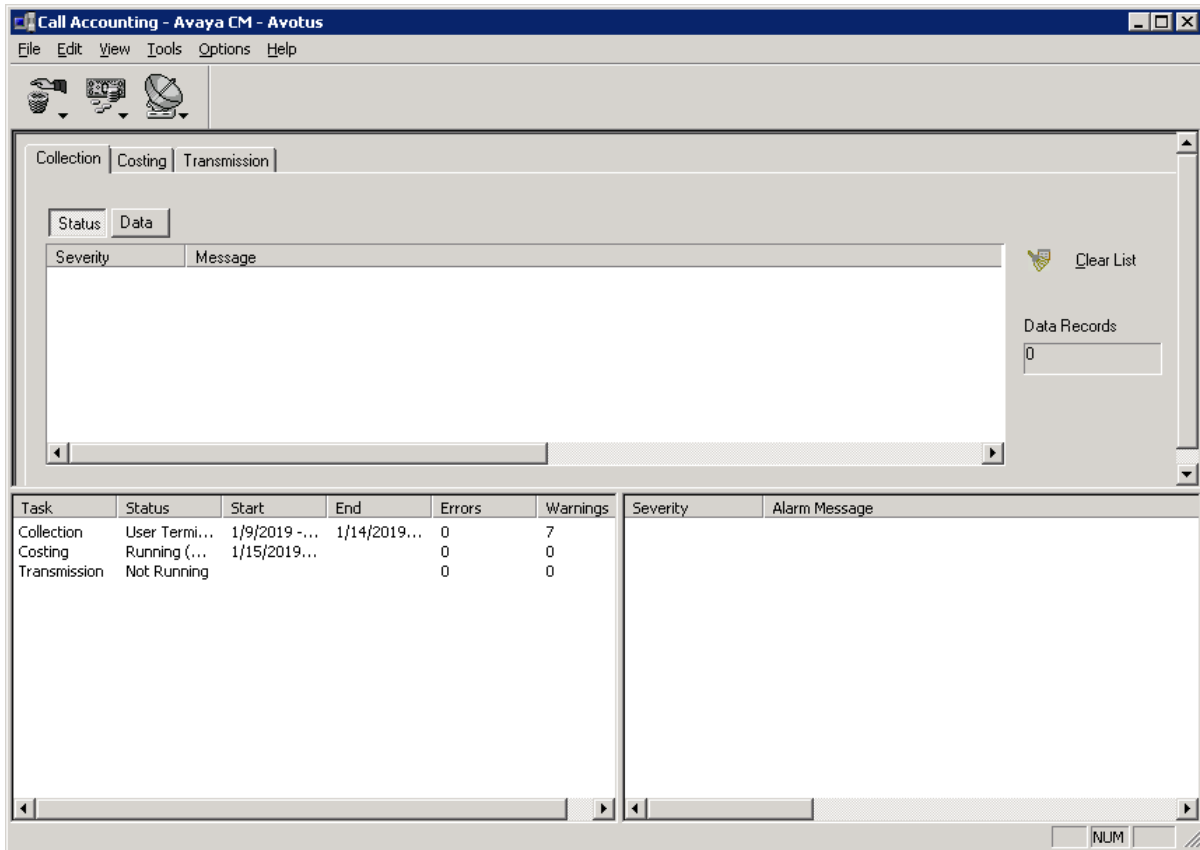
From the **Call Accounting** window navigate to **Tools → Collection → Configuration** as shown below.
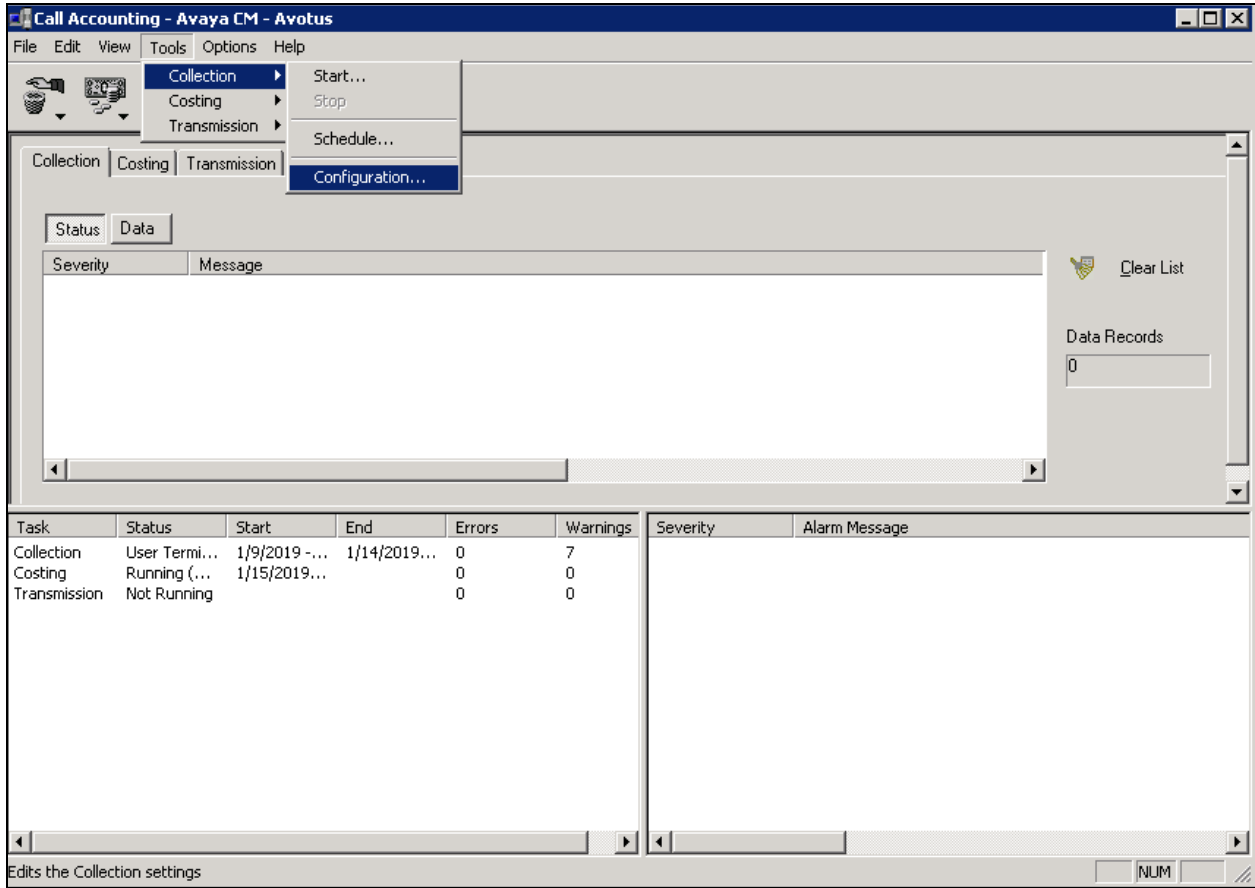
From the **System Configuration** window as shown below, navigate to **Collection** tab and under the section **Scripts**, launch the **Browse** icon to select a script for **Collection Script**.
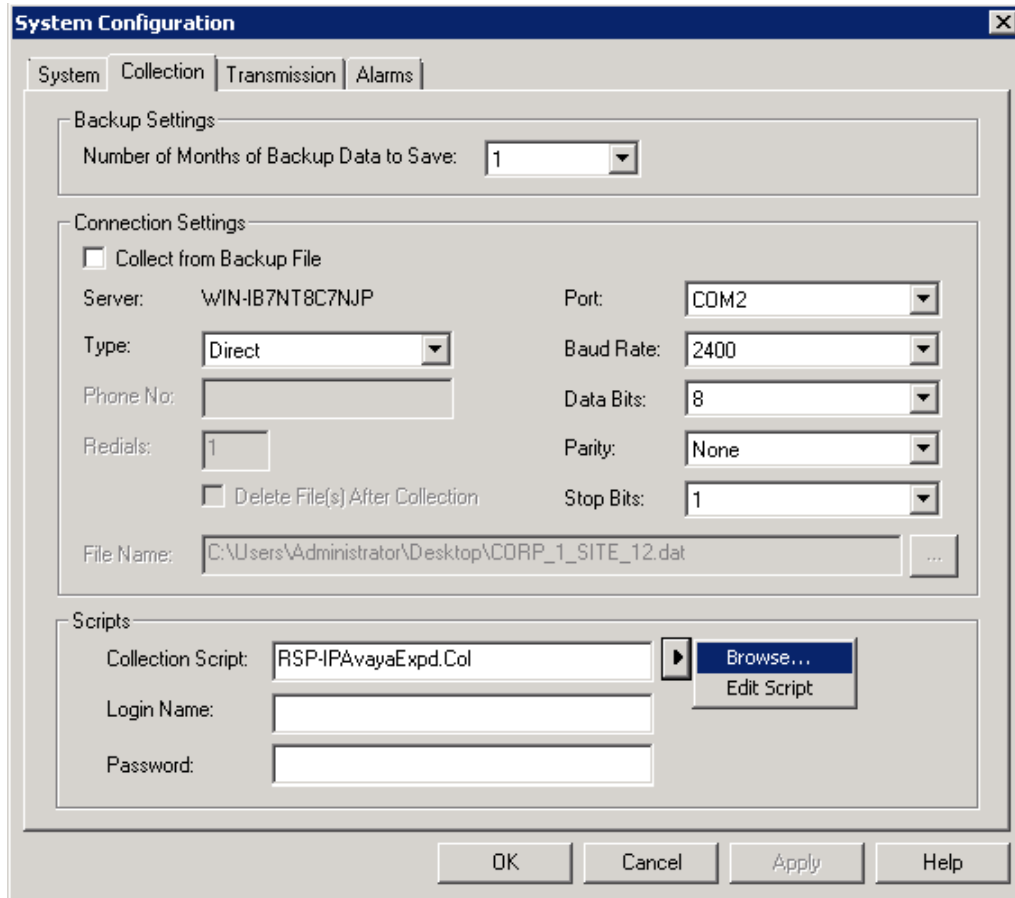
From the **Scripts** folder that is launched as shown below, select the **RSP-IPAvayaExpd.Col** script.
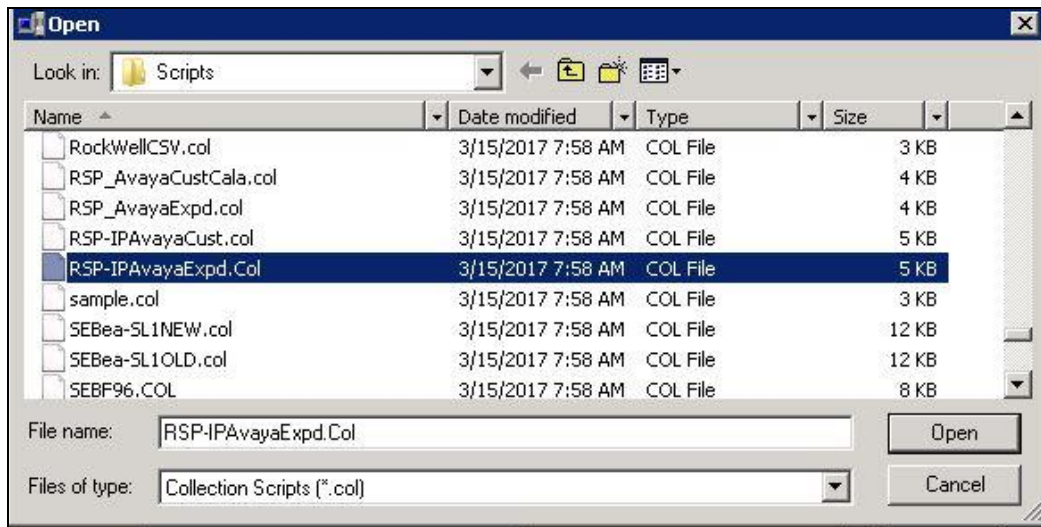
Click on the **Configure** button as shown in the screen below after selecting the required script.
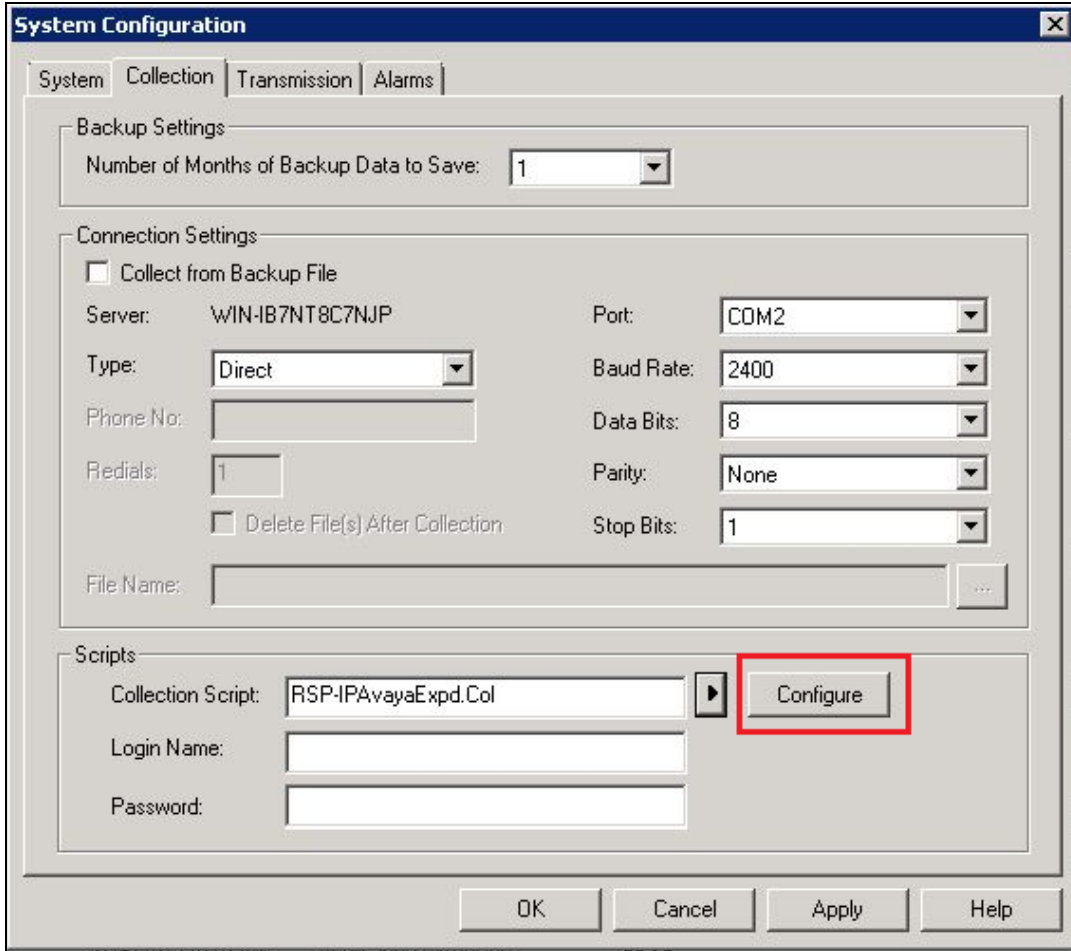
In the **Configuration** window as seen below, configure the following under the **Connection** tab,

- Ensure **Enable Capture** is checked.
- **Description**: Provide a detailed description.
- **TCP Port**: Enter "9002" as this is the port configured in Communication Manager in **Section** Error! Reference source not found..

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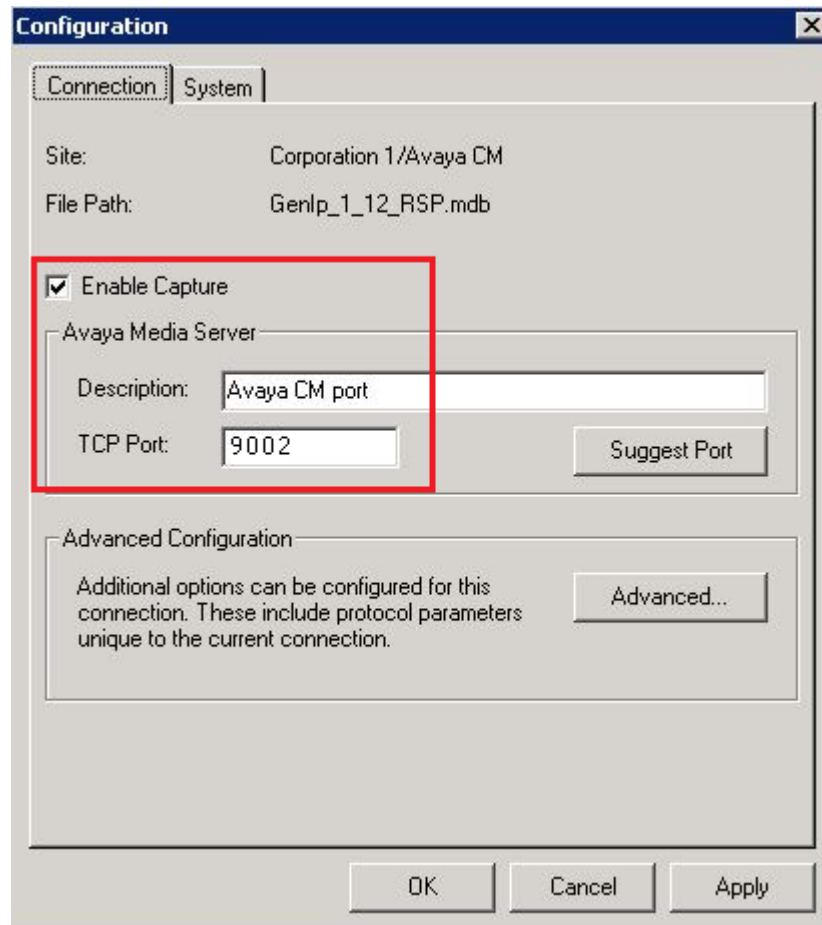
Also retain default values for all other fields in the **System Configuration** window shown earlier in this section and click on the **OK** button.

6.3.2. Installing the Avotus Generic IP Collection Service

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

KP; Reviewed:
SPOC 2/19/2019

Solution & Interoperability Test Lab Application Notes
©2019 Avaya Inc. All Rights Reserved.

22 of 29
AvotusEUR_CM80
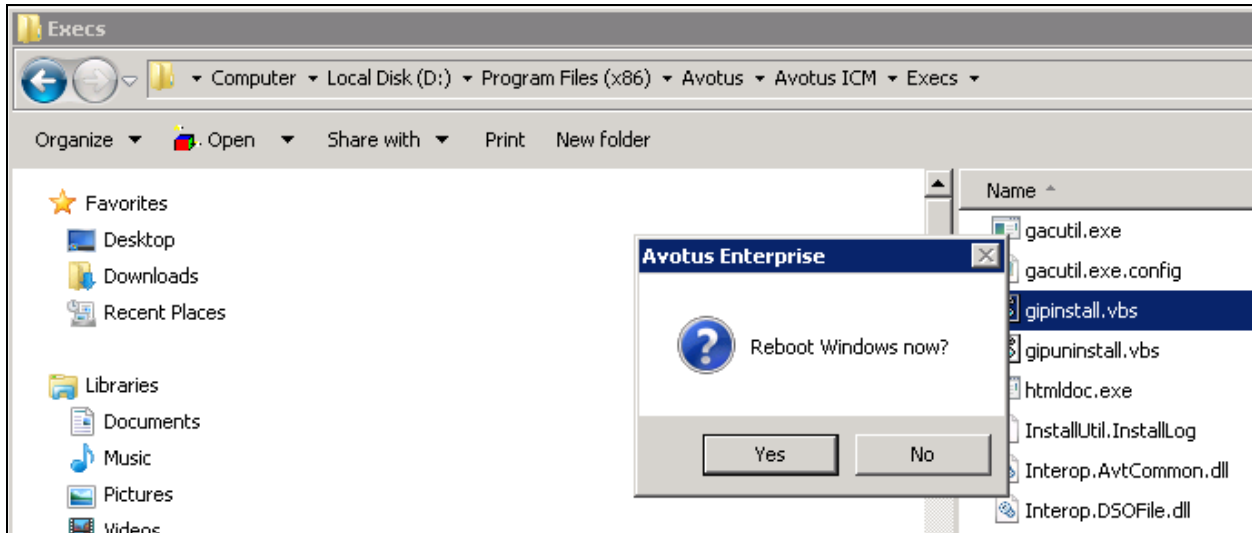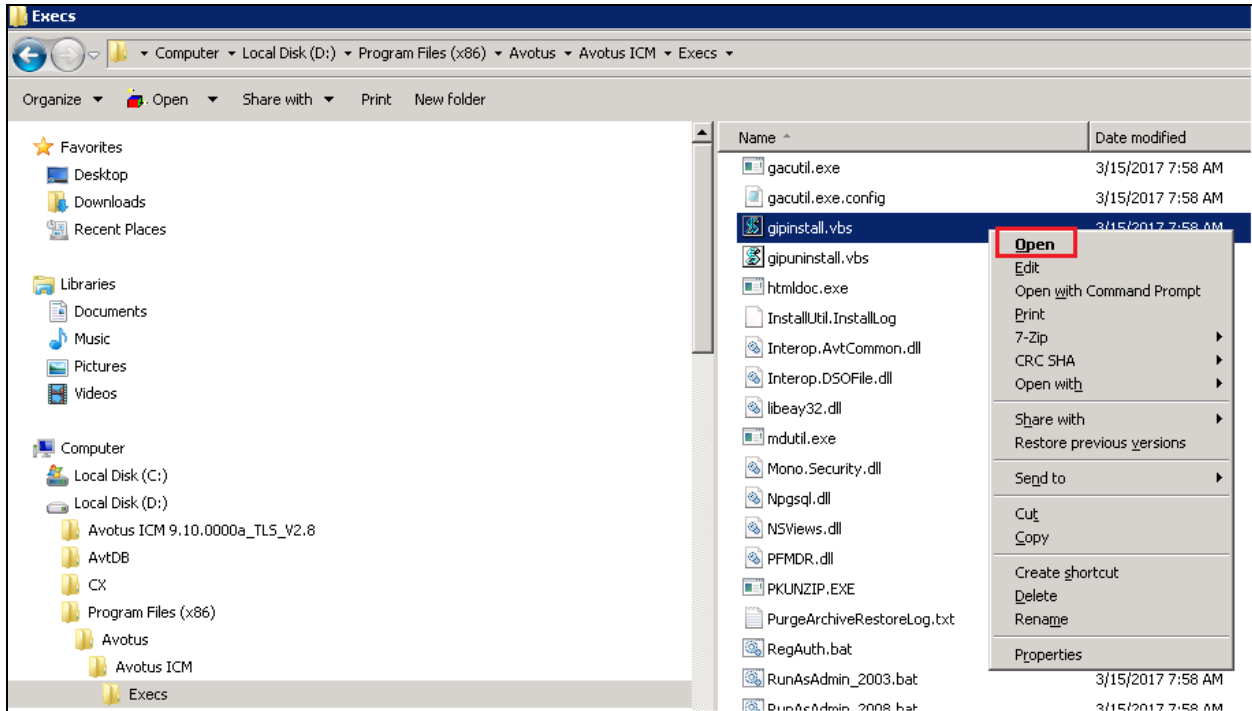
Once the rebooting of the system is completed, the **Avotus Generic IP Collction Service** will be installed under Windows Services as shown in the screen below. Start this service and ensure it is running.
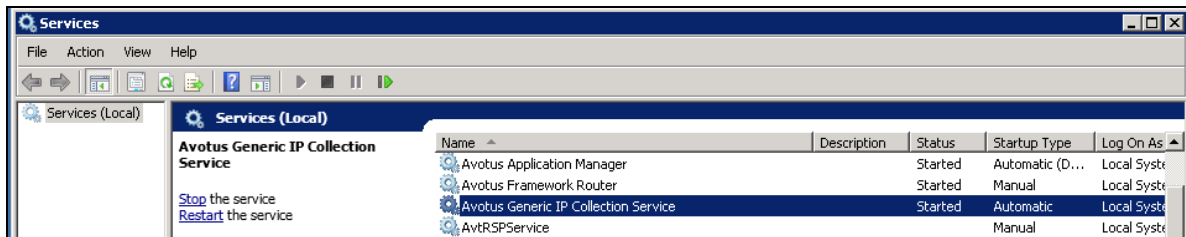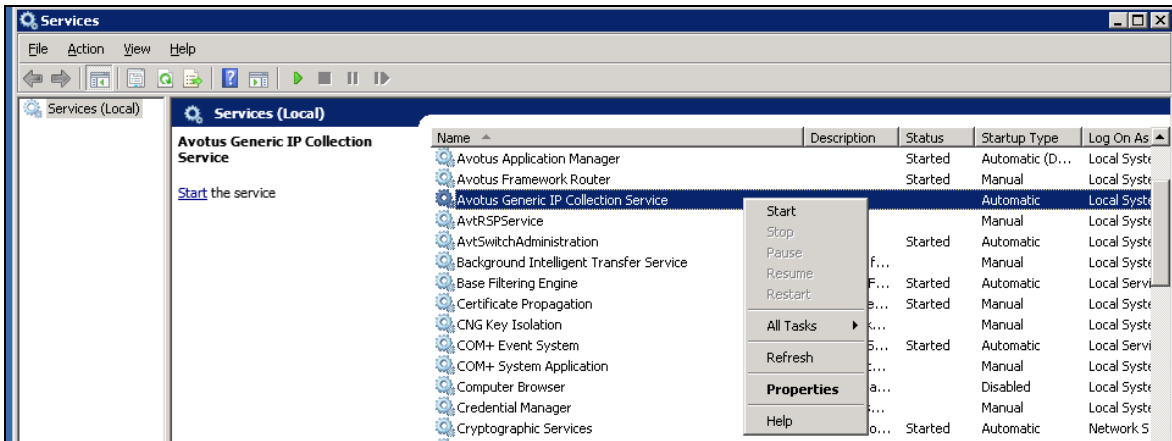
To view the status of Avotus EUR connection with Avaya RSP session, navigate to "<Avotus install folder>\Avotus ICM\Execs" and run the **AvtGenIpMgrS.exe** as shown in the screen below.
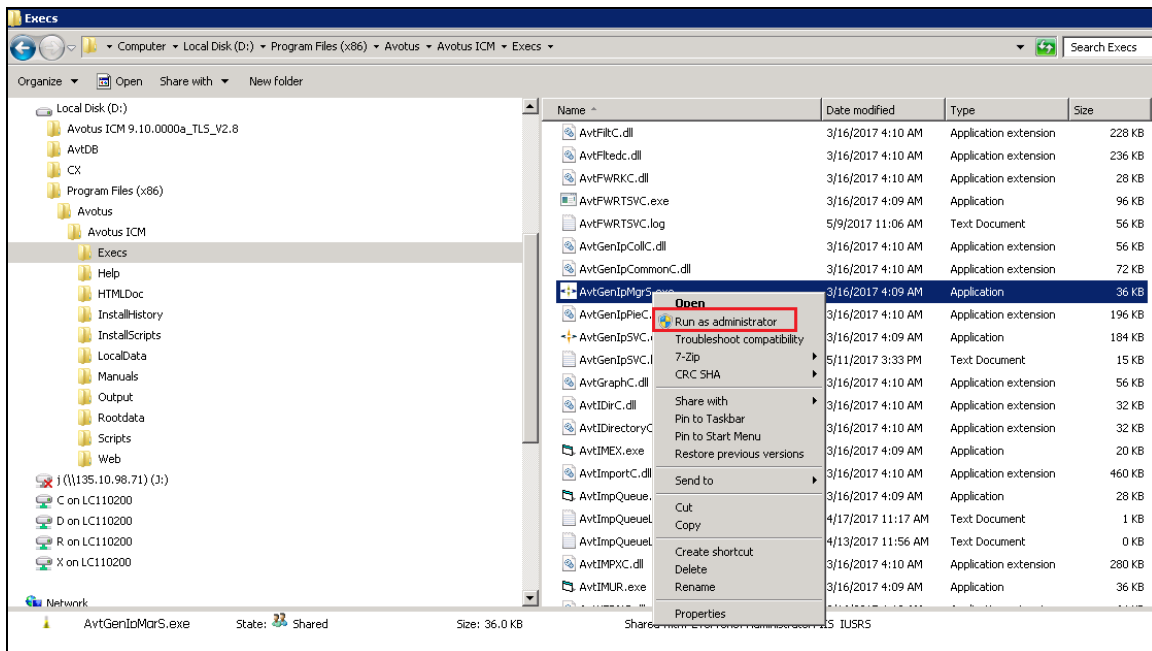
An icon will appear in the task bar / System tray of Windows by the name of Avotus Generic IP Collection Manager as shown in the screen below.
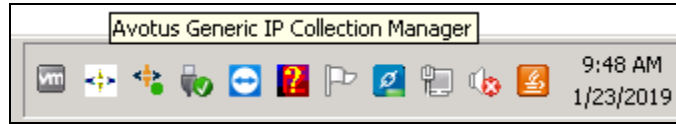
Right click on this icon and click on Show Collection Console option as shown below.
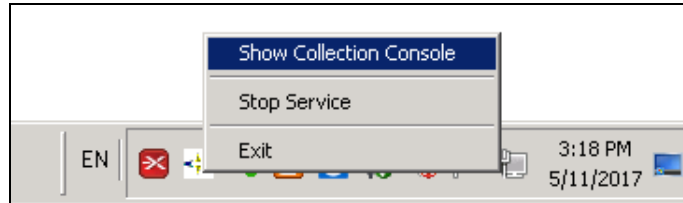
The Generic IP Collection Service Console will appear in the Interactive Desktop as shown below. User can click on the different tabs to view the status.
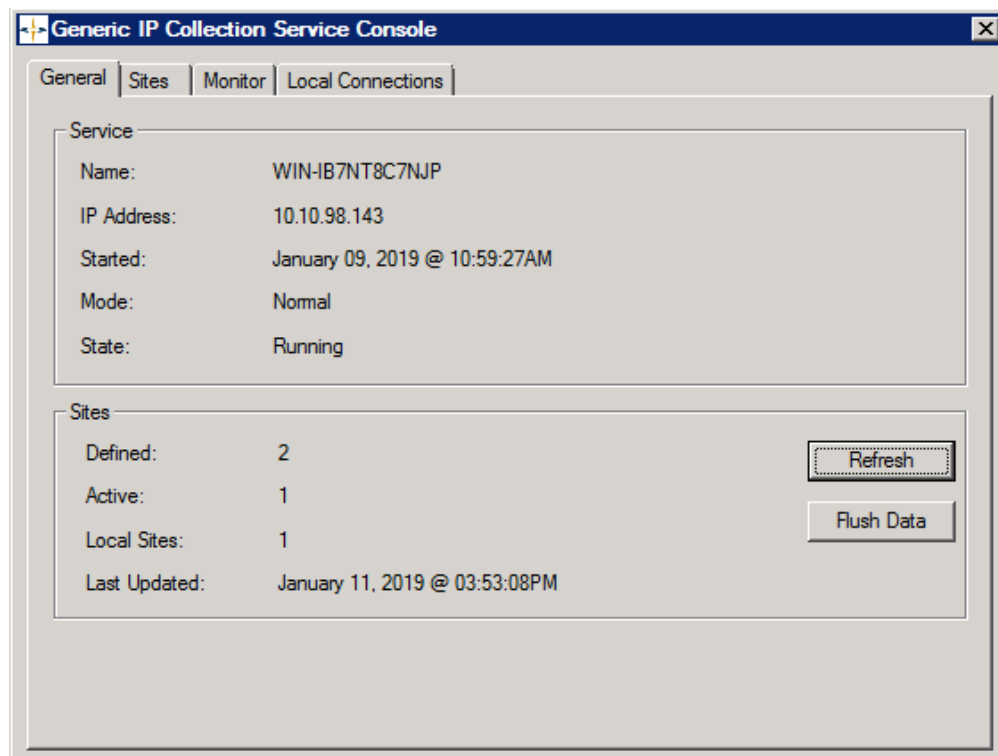
6.4. Start Collection

To start collection of CDR data, from the **Call Accounting** window navigate to **Tools →
Collection → Start** as shown in the screen below.
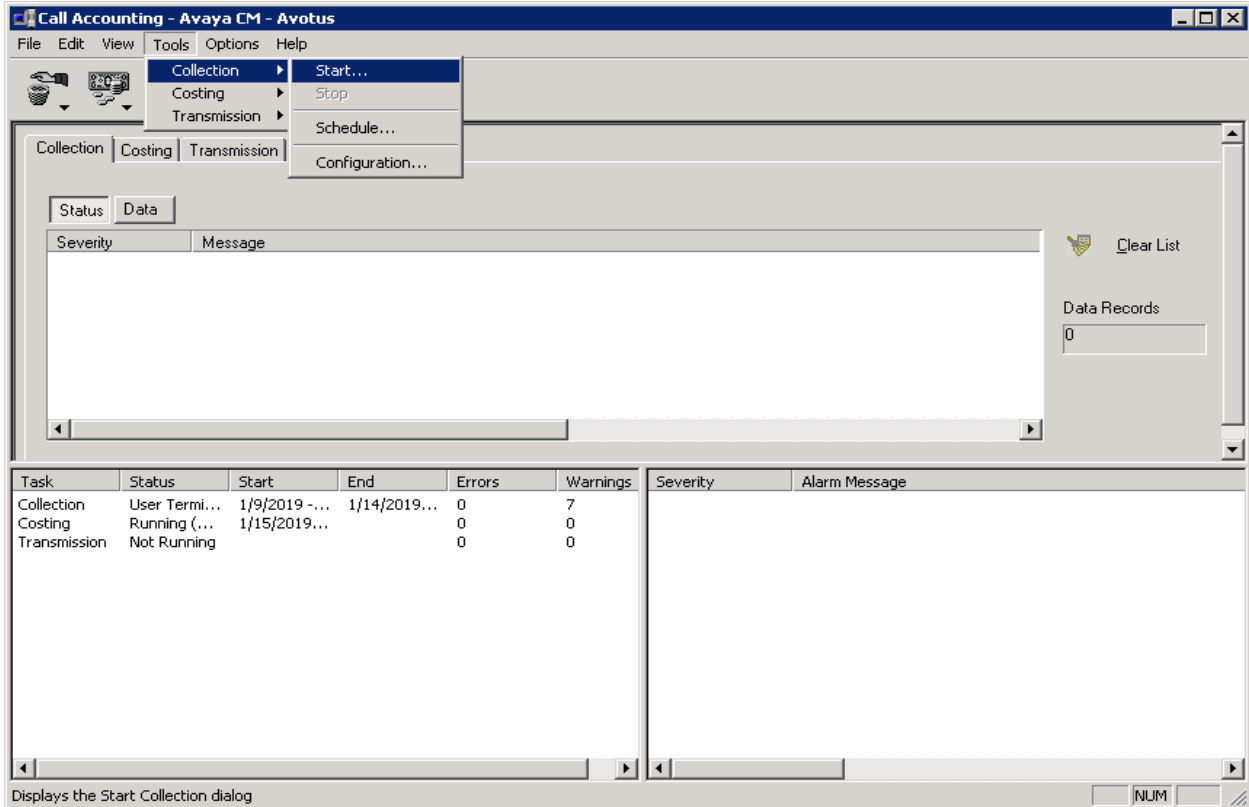
In the **Start Collection** window as shown below, select the **Collect new call records in real-
time** option and click on the **Start** button.
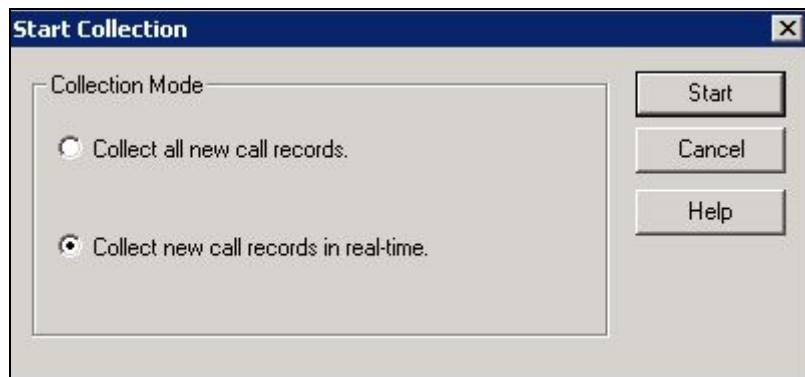
The collected raw CDR data can be found in the "CallAccountingBackup" folder, which is under
the "/Rootdata/<Corporation number>/<Site number>" folder.

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: 2019/01/11 16:23:10         2019/01/11 16:44:18
  Forward Seq. No: 97                          97
 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. The screen below shows the raw CDR data collected by Avotus EUR which was then compared with the CDR data collected by the Avaya RDTT.

- To show the call records in the report that were processed, from the main menu navigate to **Reports → Call Accounting → Diagnostic → Collected Call Records**. The Collected Call Records is displayed (not shown), enter the start date and end day and click on **Run Report** button. The screen below shows the detail report of the Collected Called Records.

KP; Reviewed:
SPOC 2/19/2019

Solution & Interoperability Test Lab Application Notes
©2019 Avaya Inc. All Rights Reserved.

27 of 29
AvotusEUR_CM80

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 Reliable Session Protocol 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 Avaya and Avotus documentation that are relevant to these Application Notes. Product documentation for Avaya Aura® Communication Manager, including the following, is available at: http://support.avaya.com/
[1] *Administering Avaya Aura® Communication Manager*, Document 03-300509, Issue 10, Release 8.0, August 2018
[2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Document 555-245-205, Issue 9.0, Release 8.0, August 2018

Product documentation for Avotus products may be found at,
http://avotus.com/telecom-enhanced-usage-reporting.asp

KP; Reviewed:
SPOC 2/19/2019

Solution & Interoperability Test Lab Application Notes
©2019 Avaya Inc. All Rights Reserved.

29 of 29
AvotusEUR_CM80