Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avotus ICM Usage Management with Avaya Aura™ Communication Manager and Avaya Aura™ Session Manager – Issue 1.0

Abstract

These Application Notes describe the configuration procedures required to allow Avotus ICM Usage Management to collect call detail records from Avaya Aura™ Session Manager.

During the compliance test, Avotus ICM connects to Avaya Aura™ Session Manager and collects, stores and processes these call records to provide usage analysis, call costing and billing capabilities.

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 describe a compliance-tested call detail recording (CDR) solution comprised of Avaya Aura ™ Communication Manager, Avaya Aura ™ Session Manager and Avotus ICM Usage Management (referred to as Avotus ICM in the ensuring text of this document).

Avotus ICM is a call accounting software application that uses call detail records to provide reporting capabilities to business and IT managers to track and manage call usage and telecom expenses.

During the compliance test, Avotus ICM connects to Session Manager and collects, stores and processes these call records to provide usage analysis, call costing and billing capabilities. All call records that pass through Session Manager will be stored in the /var/home/ftp/CDR directory in Session Manager. Avotus ICM will SFTP to Session Manager to retrieve these call records using credentials configured prior to the compliance test.

1.1. Interoperability Compliance Testing

The interoperability compliance testing included features and serviceability tests. The focus of the compliance testing was primarily on verifying capabilities of Avotus ICM to access Session Manager, retrieve current CDR data, transfer CDR raw data into Avotus ICM, and populate raw data into the CDR report.

1.2. Support

Technical support for the Avotus ICM Usage Management solution can be obtained by contacting Avotus:

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

2. Reference Configuration

Figure 1 illustrates a sample configuration that was used for the compliance test. The sample configuration shows two SIP trunks from Session Manager, one from S8300D/G450 and the other from S8720/G650.

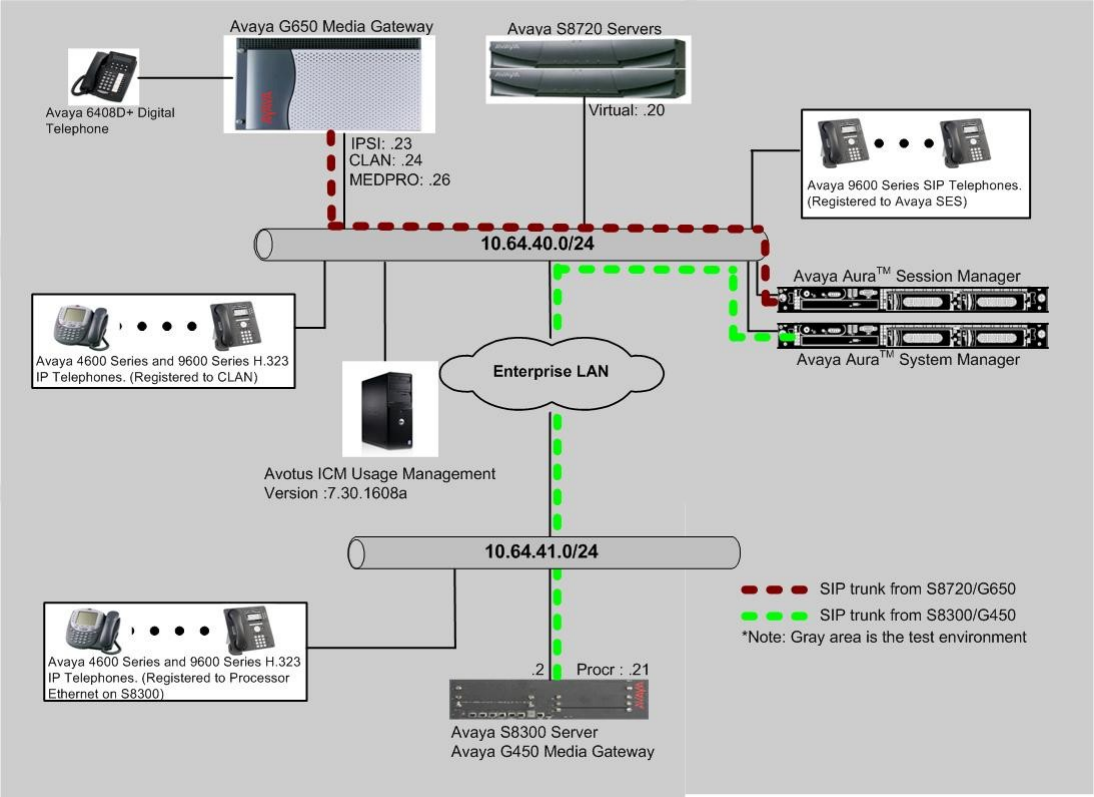


Figure 1: Test configuration for Avotus ICM Usage Management Compliance Test with Avaya Aura™ Session Manage

3. Equipment and Software Validated

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

Equipment		Software/Firmware
Avaya S8300D Server with Avaya G450 Media Gateway		Avaya Aura™ Communication Manager 6.0 (R016x.00.0.345.0) with Patch 00.0345.0-18246
Avaya S8720 Servers with Avaya G650 Media Gateway		Avaya Aura™ Communication Manager 5.2.1 (R015x.02.1.016.4)
Avaya Aura™ System Manager		Avaya Aura™ System Manager 6.0 (6.0.0.0-556)
Avaya Aura™ Session Manager		Avaya Aura™ System Manager 6.0 (6.0.0.0.600020)
Avaya 4600 Series IP Telephones		
	4625 (H.323)	2.9
Avaya 9600 Series IP Telephones		
	9620 (H.323) 9630 (H.323) 9650 (H.323)	3.1 3.1 3.1
Avaya 6400D Series Digital Telephones		-
Avaya C363T-PWR Converged Stackable Switch		4.5.14
Extreme Networks Summit 48		4.1.21
Avotus ICM		7.30.1601a

4. Configure Avaya Aura™ Communication Manager

This section describes the procedure for configuring a SIP trunk group and a SIP signaling group used for connecting to the Session Manager.

During the compliance test, the CDR data will be collected and stored in the hard disk drive of Session Manager. All calls that pass through this trunk will have their associated call data stored. These steps are performed through the System Access Terminal (SAT). These steps describe the procedure used for the Avaya S8300D Server. All steps are the same for the other Avaya Servers unless otherwise noted. For the Avaya S8720 Server, the SIP trunk terminates at the IP address of the CLAN board. For the Avaya S8300D Server, the SIP trunk terminates at the IP address of the local Ethernet Processor (with node-name "procr").

Use the **change node-names ip** command to create a new node name, for example, **SM-1**. SM-1 and procr IP addresses will be used in the next step for configuration of the signaling group.

```
add node-names ip                                              Page   1 of   2
                                IP NODE NAMES
    Name                  IP Address
CLAN                    10.64.40.24
SM-1                    10.64.40.42
avotus                  10.64.43.111
default                 0.0.0.0
procr                   10.64.41.21              ::
```

Enter the **add signaling-group <s>** command, where ***s*** is an available signaling group and configure the following:

- Group Type – Set to **sip**.
- IMS Enabled – Verify that the field is set to **n**. Setting this field to **y** will cause Communication Manager to function as a Feature Server.
- Transport Method – Set to **tls** (Transport Layer Security).
- Near-end Node Name – Set to **procr** as displayed in the IP NODE NAMES form.
- Far-end Node Name – Set to **SM-1**, the Session Manager name configured in the IP NODE NAMES form.
- Far-end Network Region – Set to the region configured in the IP NETWORK REGION form (not shown).
- Far-end Domain – Set to **avaya.com**. This should match the SIP Domain value in the IP NETWORK REGION form (not shown).
- Direct IP-IP Audio Connections – Set to **y**, since Media Shuffling is enabled during the compliance test

```
add signaling-group 92
                                SIGNALING GROUP

 Group Number: 92                Group Type: sip
  IMS Enabled? n          Transport Method: tls
        Q-SIP? n                                          SIP Enabled LSP? n
     IP Video? n                                Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM



   Near-end Node Name: procr                 Far-end Node Name: SM-1
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                         Far-end Network Region: 1

Far-end Domain: avaya.com
                                              Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                   RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                    IP Audio Hairpinning? n
         Enable Layer 3 Test? n                    Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n             Alternate Route Timer(sec): 6
```

Use the **add trunk-group *n*** command, where ***n*** is an available trunk group number, to configure a SIP trunk group between Communication Manager and Session Manager. Provide the following information:

- Group Type – Set the Group Type field to **sip**.
- Group Name – Enter a descriptive name.
- TAC (Trunk Access Code) – Set to any available trunk access code.
- Service Type – Set the Service Type field to **tie**.
- Signaling Group – Set to the Group Number field value configured in the SIGNALING GROUP form.
- Number of Members – Allowed value is between 0 and 255. Set to a value large enough to accommodate the number of SIP telephone extensions being used.

```
add trunk-group 92                                          Page   1 of  21
                              TRUNK GROUP

Group Number: 92                    Group Type: sip           CDR Reports: y
  Group Name: No IMS SIP trk              COR: 1        TN: 1        TAC: 1092
   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: 92
                                                     Number of Members: 10
```

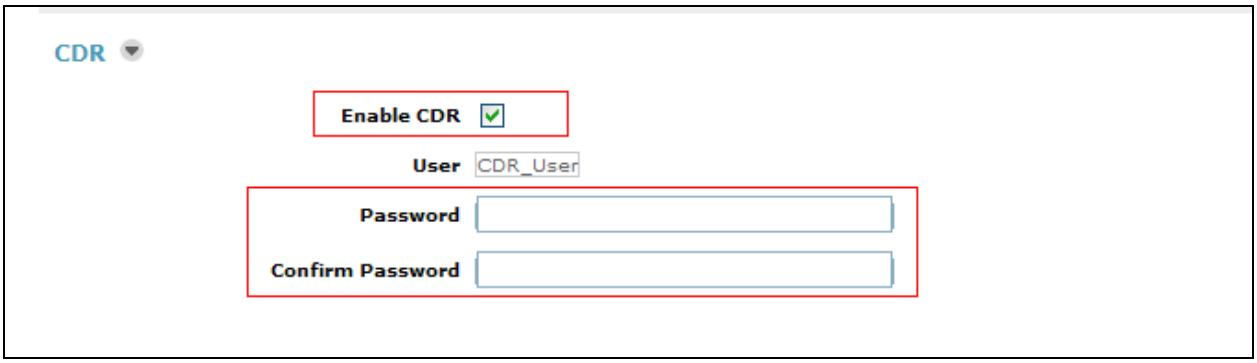
5. Configure Avaya Aura™ Session Manager

This section assumes that initial configuration on Session Manager has been performed, and Routing and Session Manager Instance are administered properly. This section will only discuss enabling the CDR configuration. To enable CDR in Session Manager, the following has to be modified:

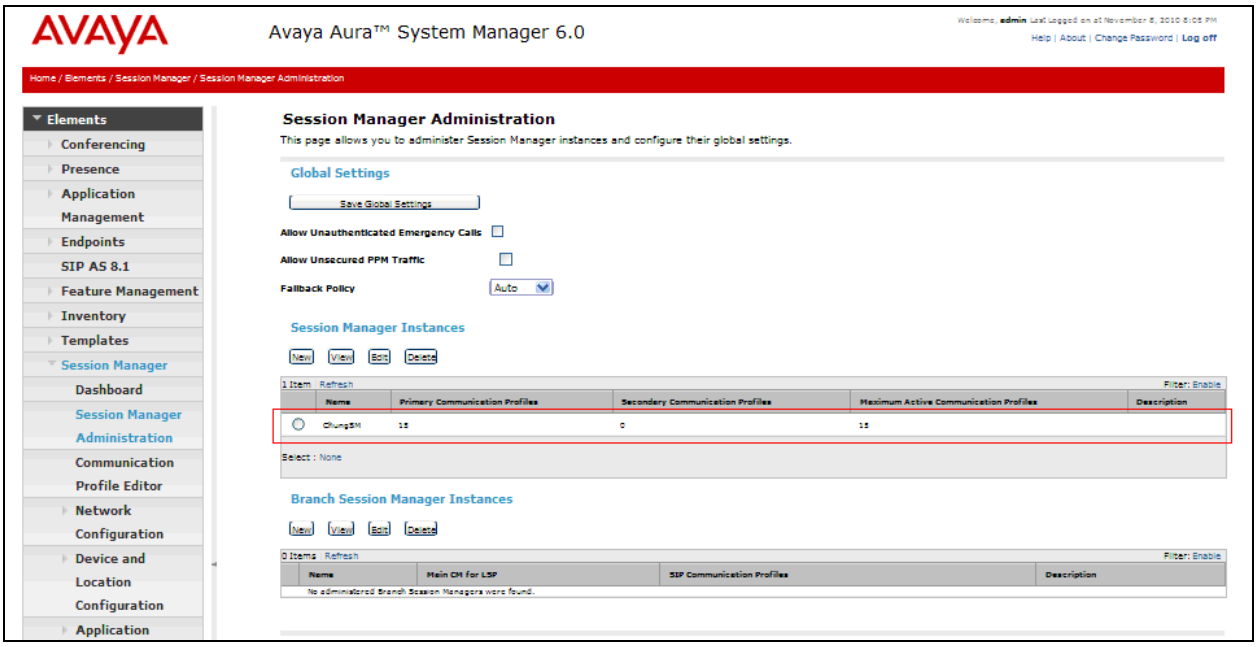
- Session Manager instances (**Elements → Session Manager → Session Manager Administration → Session Manager Instances** section)
- SIP Entities (**Routing → SIP Entities**)

Navigate to **Elements→ Session Manager → Session Manager Administration**, and click on the **Edit** button in the Session Manager Instances section to modify the configuration, so that CDR can be enabled. Under the CDR section, provide the following information:

- Check the box on the Enable CDR field.
- Provide a password for the CDR_User
- Re-enter the password.



The following screen shows the Session Manager Instances section in the Session Manager Administration page.



SIP Entities must be added for Session Manager and for each network component that has a SIP trunk provisioned to Session Manager. During the compliance test, the following SIP Entities are configured:

- Session Manager itself.
- Communication Managers (S8300D/G450 and S8720/G650)

Navigate to **Routing → SIP Entities**, and click on the **New** button to create a new SIP entity. Provide the following information:

General section

a. Enter a descriptive name in the **Name** field
b. Enter the IP address for the SIP Entity.

c. From the **Type** drop down menu select a type that best matches the SIP Entity (e.g. **CM**).
d. Enter a description in the **Notes** field if desired.
e. Select the appropriate time zone.
f. Select **both** in the Call Detail Recording field. By setting this field to both, Session Manager will collect CDR on both direction (inbound and outbound)

Sip Link Monitoring section

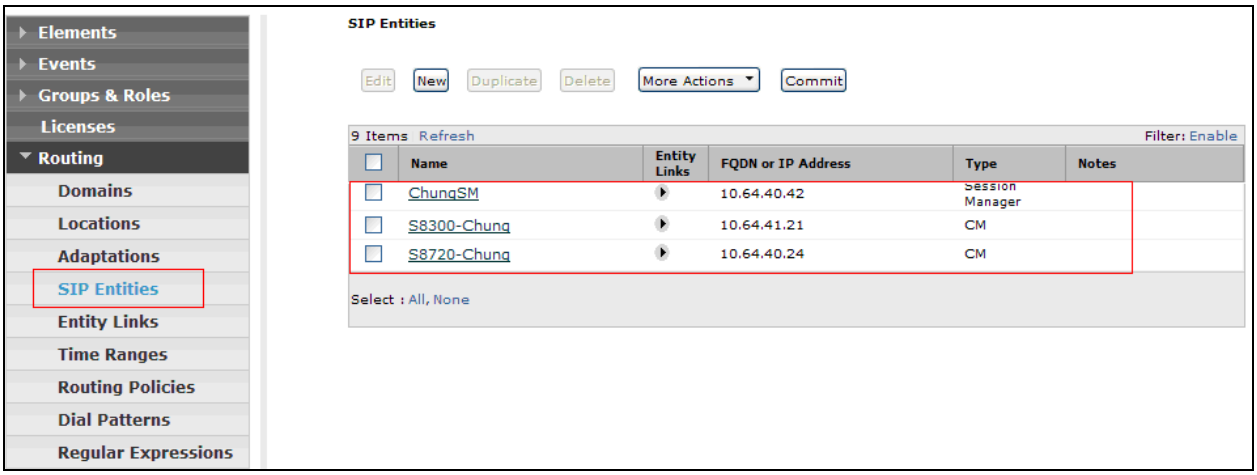
a. Select the desired option.

Port section

a. When defining a SIP Entity for Session Manager itself and **SM** is selected from the **Type** drop down menu, an additional section called **Ports** will appear. Click **Add**, then edit the fields in the resulting new row:
   - Enter the **Port** number on which the system listens for SIP requests.
   - Select the transport **Protocol** to be used.
   - Select the SIP Domain configured in the IP NETWORK REGION form (not shown) for the **Default Domain**.

b. Repeat **step a** for each Port to be configured.
c. Click on **Commit**.
d. Repeat these steps for each SIP Entity.

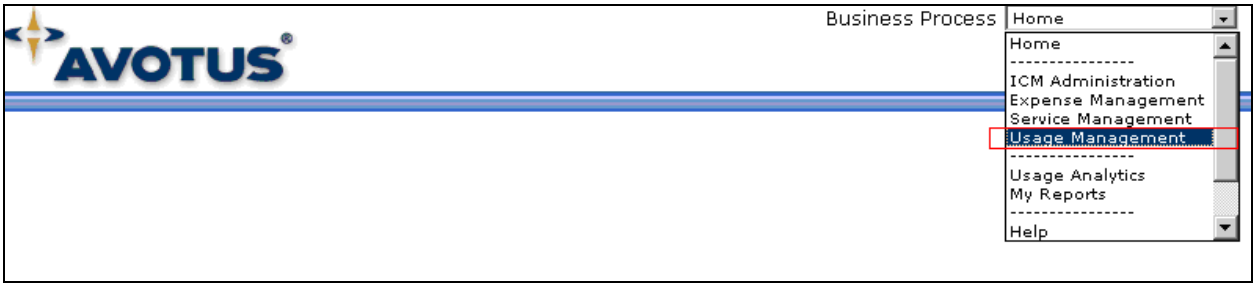
The following screen shows the SIP Entities page that lists the SIP Entities configured for the compliance test..



6. Configure Avotus ICM Usage Management

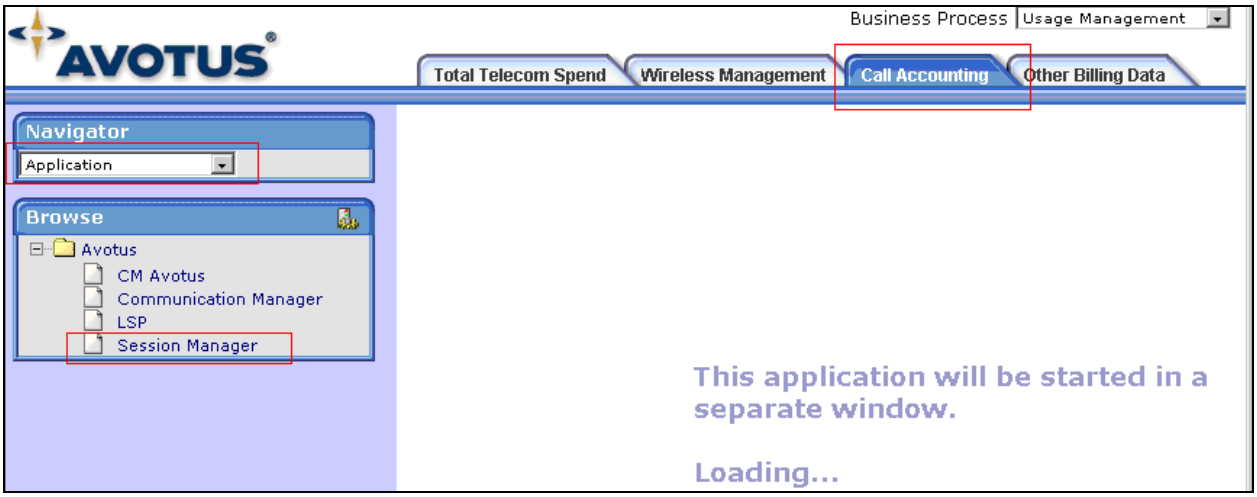
This section describes the configuration of Avotus ICM Usage management. Avotus installs, configures, and customizes the ICM Usage Management application for the end customers. Thus, this section only describes the interface configuration, so that Avotus ICM Usage Management can collect CDR data, using SFTP, from Session Manager.

To configure Avotus ICM Usage Management, double click on the Avotus ICM Usage Management icon,  , and provide credentials to gain access into Avotus ICM Usage Management. Select **Usage Management** using the drop-down menu.

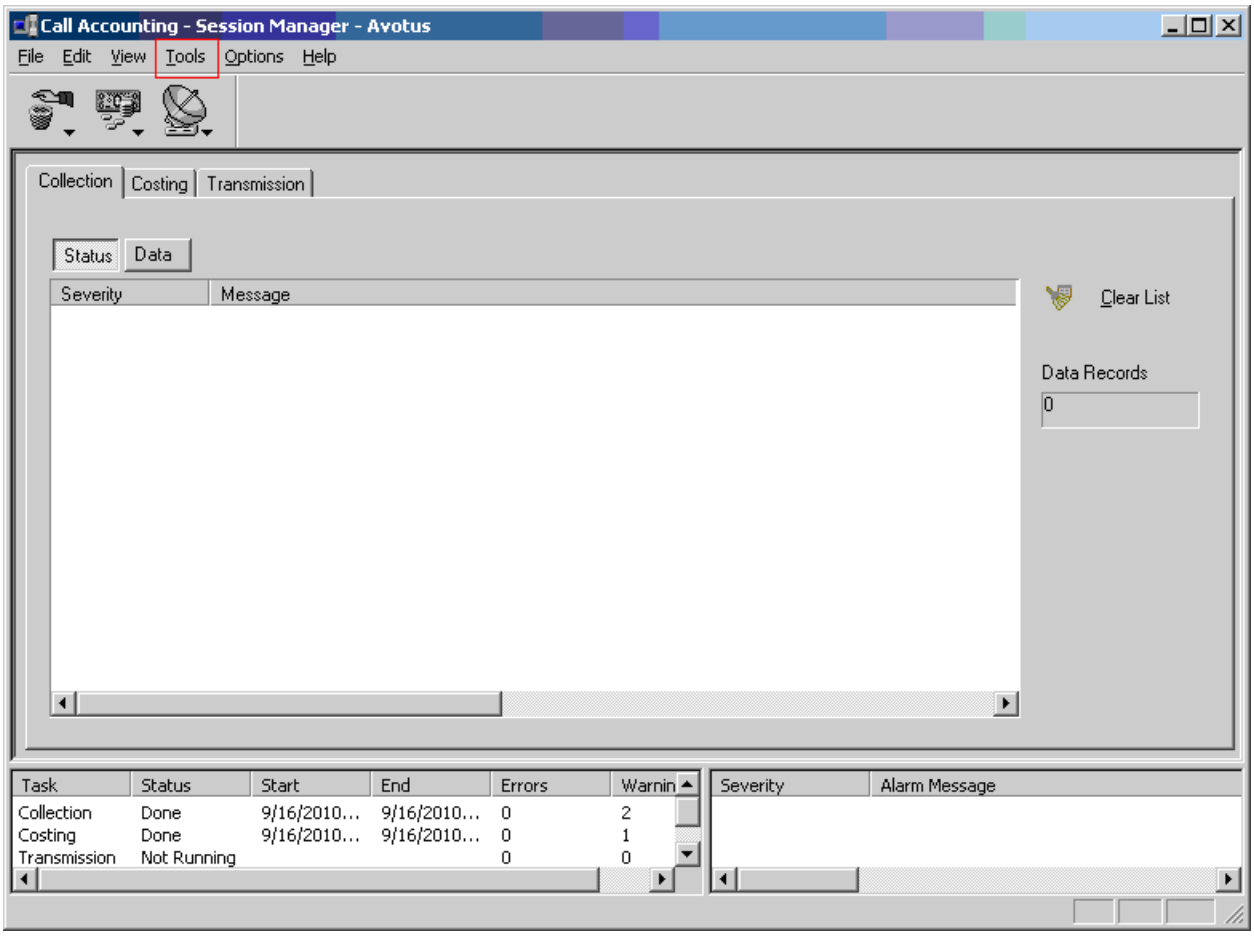


From the Avotus Home page, click the **Call Accounting** tab on the top. From the left pane, select **Application** under the Navigator section. Then, choose an appropriate call accounting system. The following screen shows the call accounting system for **Session Manager**.

By selecting the call accounting system, the Call Accounting-Session Manager- Avotus page appears.

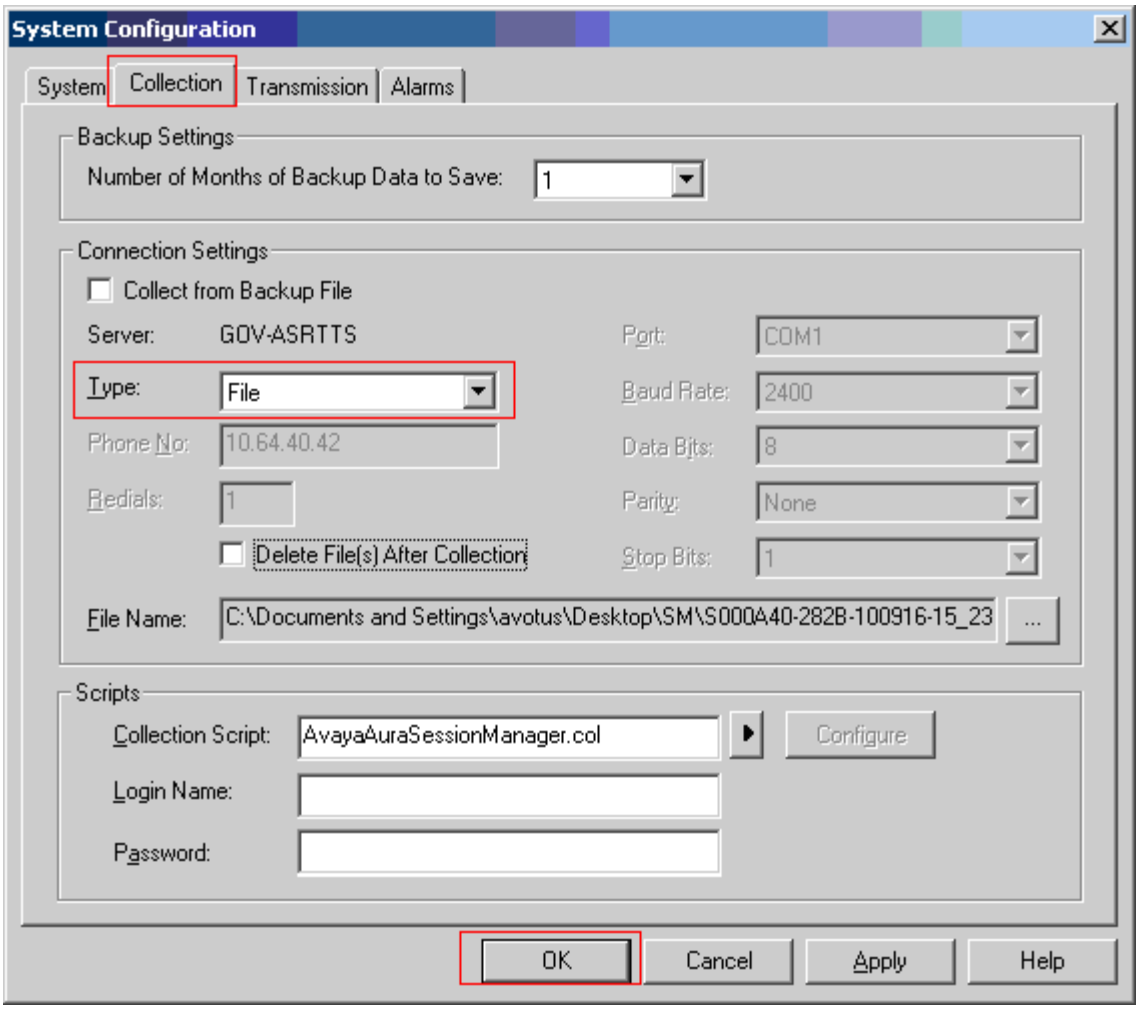


On the Call Accounting-Session Manager- Avotus page, navigate to **Tools → Collection → Configuration** (not shown), and the System Configuration page appears



On the System Configuration Page, Select the **Collection** tab. Under the Connection Settings section, select File using the drop down menu

Click on the **OK** button to save the changes.



7. General Test Approach and Test Results

The general test approach was for Avotus ICM to manually SFTP into Session Manager using the credentials that were provided to Avotus ICM during the Session Manager configuration. Once, Avotus ICM collects raw data, Avotus ICM transforms raw data into call records and makes them available for the end customers. For serviceability testing, Session Manager was reset and Avotus ICM was restarted.

All executed test cases passed. Avotus ICM successfully collected the CDR records from Session Manager via a SFTP connection for all types of SIP calls between two Communication Managers. For serviceability testing, Avotus ICM was able to resume collection of CDR records after failure recovery.

8. Verification Steps

The following steps may be used to verify the configuration:

- On the SAT of each Avaya Media Server, enter the **status trunk** command and verify that the SIP trunk state is **in-service/idle**.
- Place a call and the call goes through the trunk, and the call can be connected via Session Manager.
- The CDR raw data is stored in the /var/home/ftp/CDR directory

9. Conclusion

These Application Notes describe the procedures for configuring Avotus ICM to collect call detail records from Session Manager. Avotus ICM successfully passed the compliance test.

10. Additional References

The following Avaya product documentation can be found at http://support.avaya.com.

[1] *Avaya Aura™ Communication Manager Feature Description and Implementation*, Issue 6, August 20010, Document Number 555-245-205
[2] *Administering Avaya Aura™ Communication Manager* Release 6.0, Issue 6.0, June 2010, Document Number 03-300509.
[3] *Administering Avaya Aura™ System Manager*, Release 6.0, June 2010.
[4] *Administering Avaya Aura™ Session Manager*, Release 6.0, Issue 3, August 2010, Document Number 03-603324

The following ICM product documentation is available from Avotus. Visit http://www.avotus.com for company and product information.

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.