



Application Notes for Configuring Avotus Enhanced Usage Reporting for Unified Communications with Avaya Aura® Session 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® Session Manager over an IP network connection. 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 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 describes a compliance-tested call detail recording (CDR) solution comprised of Avaya Aura ® Session Manager (Session Manager) and Avotus Enhanced Usage Reporting for Unified Communications (Avotus EUR). Avotus EUR is a call accounting software application that makes use of CDRs to provide reporting capabilities to business and IT managers to track and manage call usage and telecom expenses.

Avotus EUR is a call accounting and billing software application that utilizes the CDR output from Session Manager. Avotus EUR collects, stores, and processes the CDRs to provide usage analysis, call costing and billing capabilities. Session Manager can generate CDRs for intra-switch calls, inter-switch calls, inbound trunk calls and outbound trunk calls. Avotus EUR can connect to Session Manager over a local or wide area network using Secure File Transfer Protocol (SFTP). Session Manager is configured to generate CDRs and put them into files and save them to a specific folder on the Session Manager server. Avotus EUR, using SFTP, connects to the server to access the CDR files generated by Session Manager and download them to Avotus EUR server to generate reports. For the compliance testing, the “Enhanced Flat file” format was used as the Data File Format on Session Manager.

During the compliance test, SIP endpoints were included. SIP endpoints registered with Session Manager. An assumption is made that Session Manager and Avaya Aura® System Manager are already installed and basic configuration has been performed. Only steps relevant to this compliance test are described in this document.

2. General Test Approach and Test Results

The general test approach was to manually place intra-switch calls, inbound trunk and outbound trunk calls, transfer, conference, and verify that Avotus EUR collects the CDR records, and properly classifies and reports the attributes of the call. For serviceability testing, physical and logical links were disabled/re-enabled, Avaya Servers were reset, and Avotus EUR connection and its server was restarted.

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 testing included features and serviceability tests. The feature testing focused on verifying the proper parsing and displaying of CDR data by Avotus EUR for call scenarios including internal, inbound, and outbound trunk calls.

The serviceability testing focused on verifying the ability of Avotus to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to Avotus.

2.2. Test Results

All executed test cases were verified and passed.

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 a sample configuration consisting of Site 1 that includes System Manager, Session Manager, Communication Manager, Local Survivable Processor and Avaya Aura® Media Server running on Virtualized Environment, Avaya G450 Media Gateway that has PRI/T1 trunk to PSTN, Avotus EUR Call Accounting server. Avaya IP Office Server Edition running on Virtualized Environment on the Site 2 connects to Session Manager via SIP trunks.

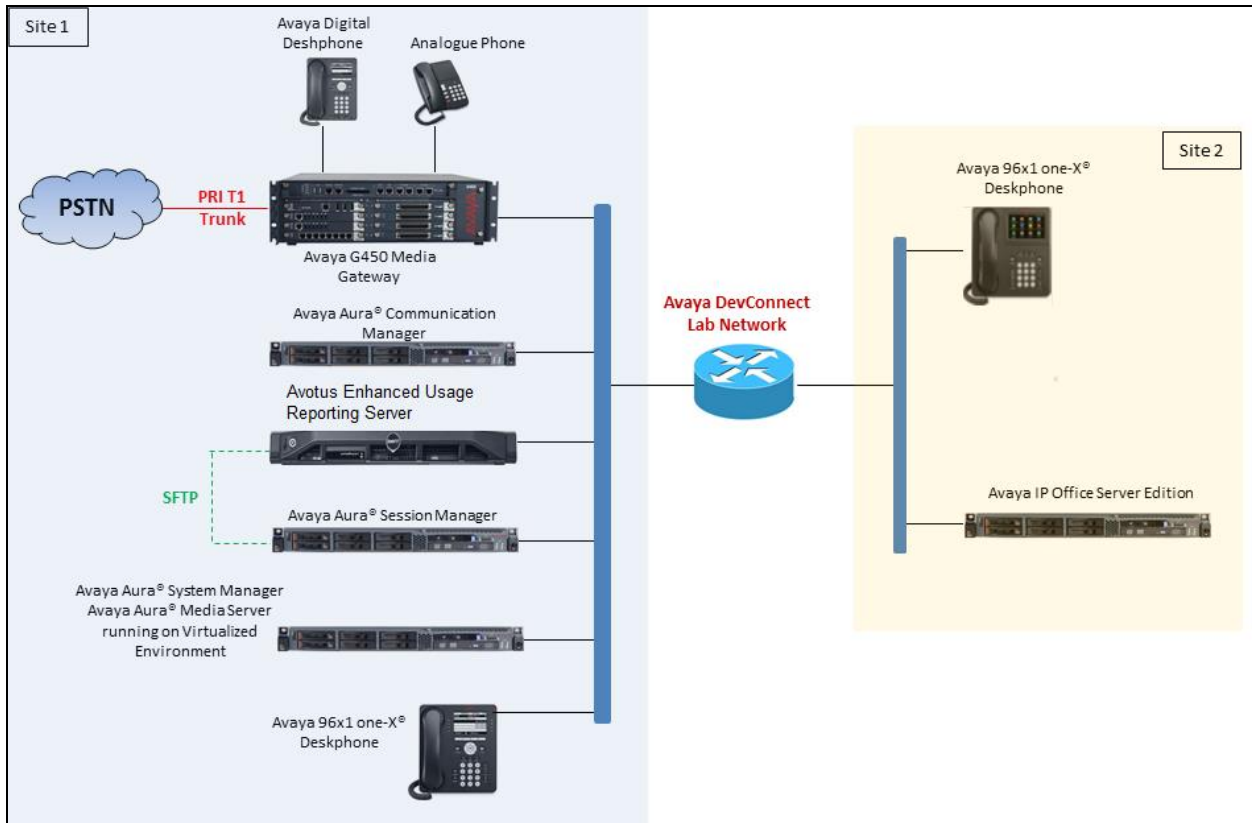


Figure 1: Test configuration for Avotus EUR Compliance Test

4. Equipment and Software Validated

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

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	8.0.0.137
Avaya G450 Media Gateway <ul style="list-style-type: none">• MGP	40.20.0
Avaya 96x1 IP Deskphones <ul style="list-style-type: none">• H323• SIP	6.7104 7.1.4.0.11
Avaya 1416 Digital Deskphone	FW1
Avotus Enhanced Unified Reporting – Call Accounting Software	ICM Version: 9.10.0001

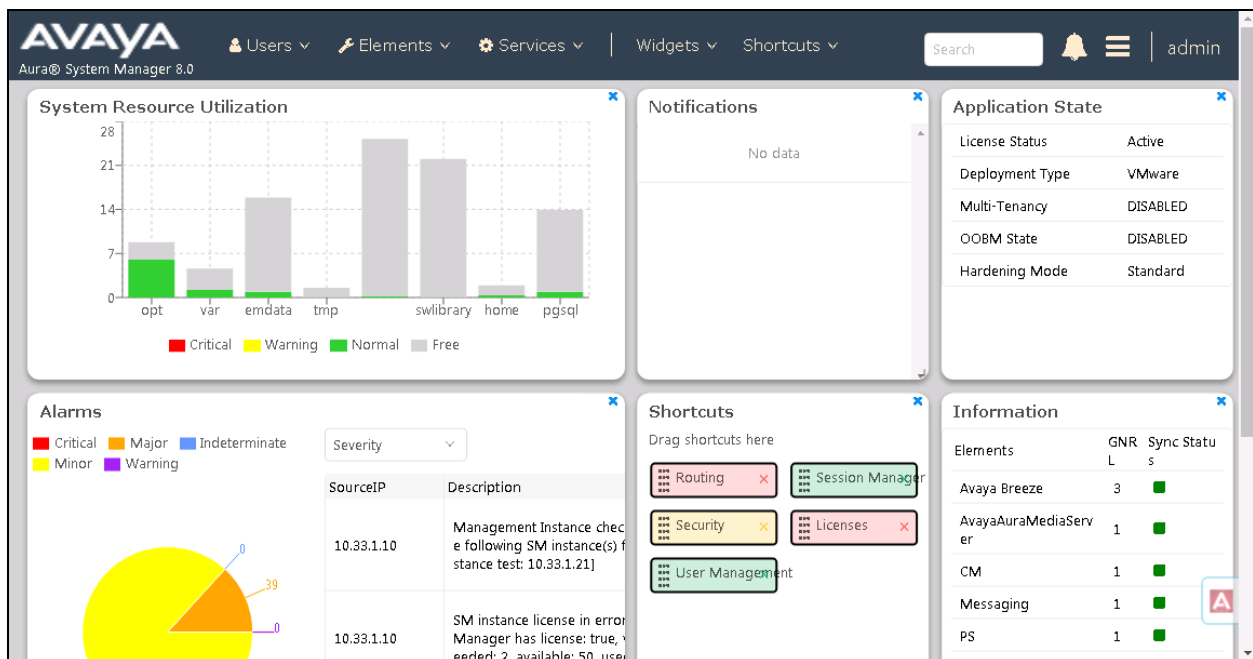
5. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. Session Manager is configured by opening a web browser to System Manager. The procedures include the following areas:

- Log in to Avaya Aura® System Manager
- Administer Call Detail Recording on Session Manager
- Administer Call Detail Recording on SIP Entity

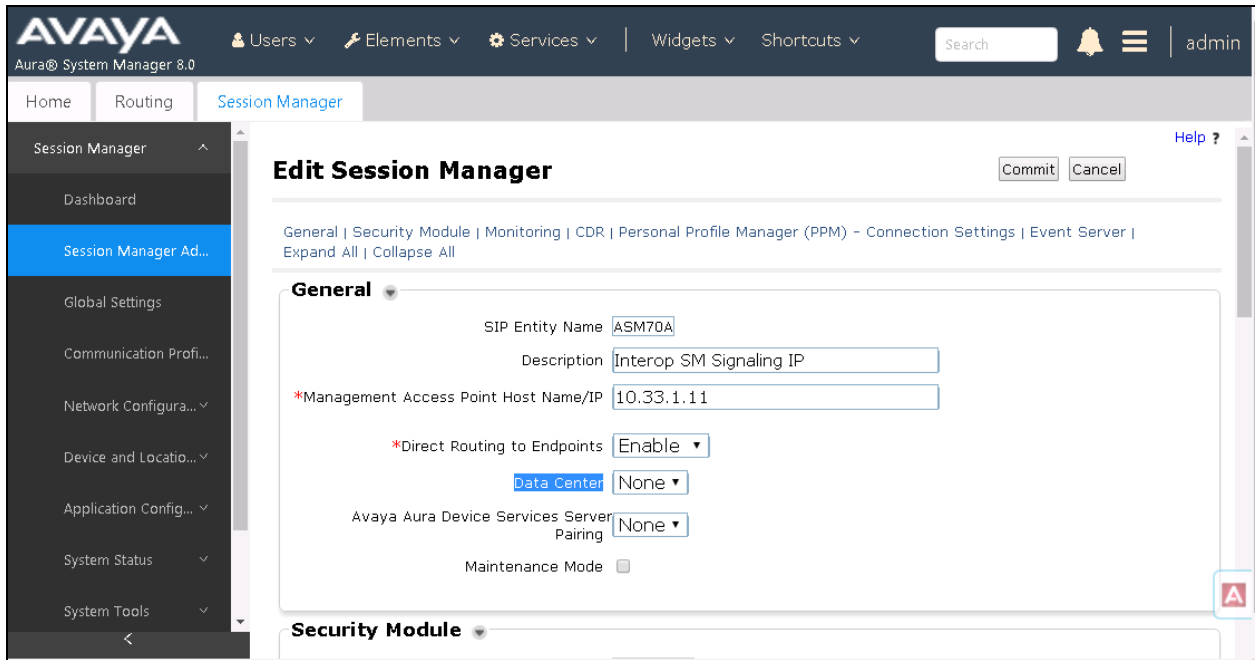
5.1. Log in to Avaya Aura® System Manager

Access the System Manager using a web browser and entering **http://<FQDN >/SMGR**, where <FQDN> is the fully qualified domain name of System Manager. Log in using appropriate credentials (not shown) and the **Home** tab will be presented with menu options shown below.



5.2. Administer Call Detail Recording on Session Manager

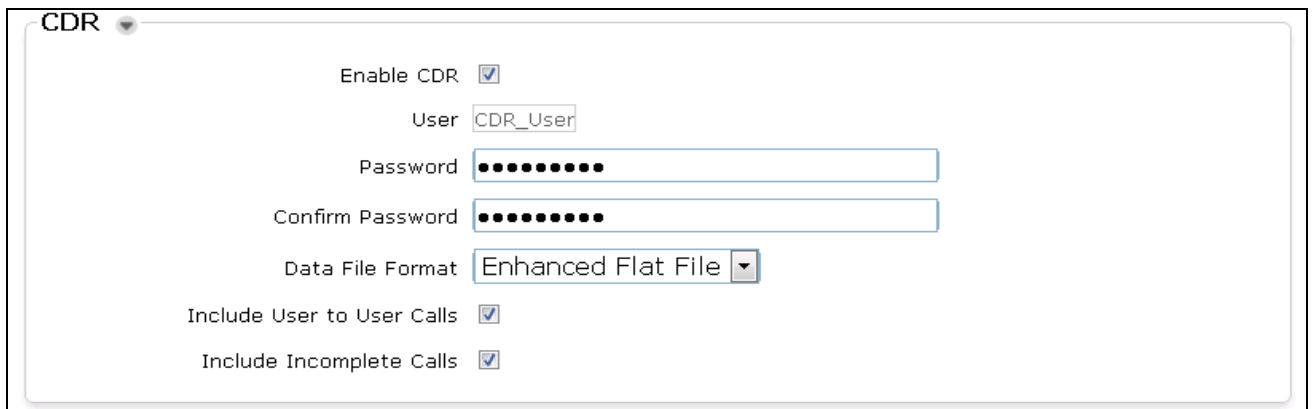
From the homepage of System Manager, navigate to **Elements** → **Session Manager**, the **Session Manager** tab is displayed. Select **Session Manager Administration** from the left pane and select a desired Session Manager entity, for example “ASM70A” from list of Session Manager entity in the right side and then select **Edit** button (not shown) to edit. The **Edit Session Manager** is displayed as below.



Scroll down to the CDR section, and do the following:

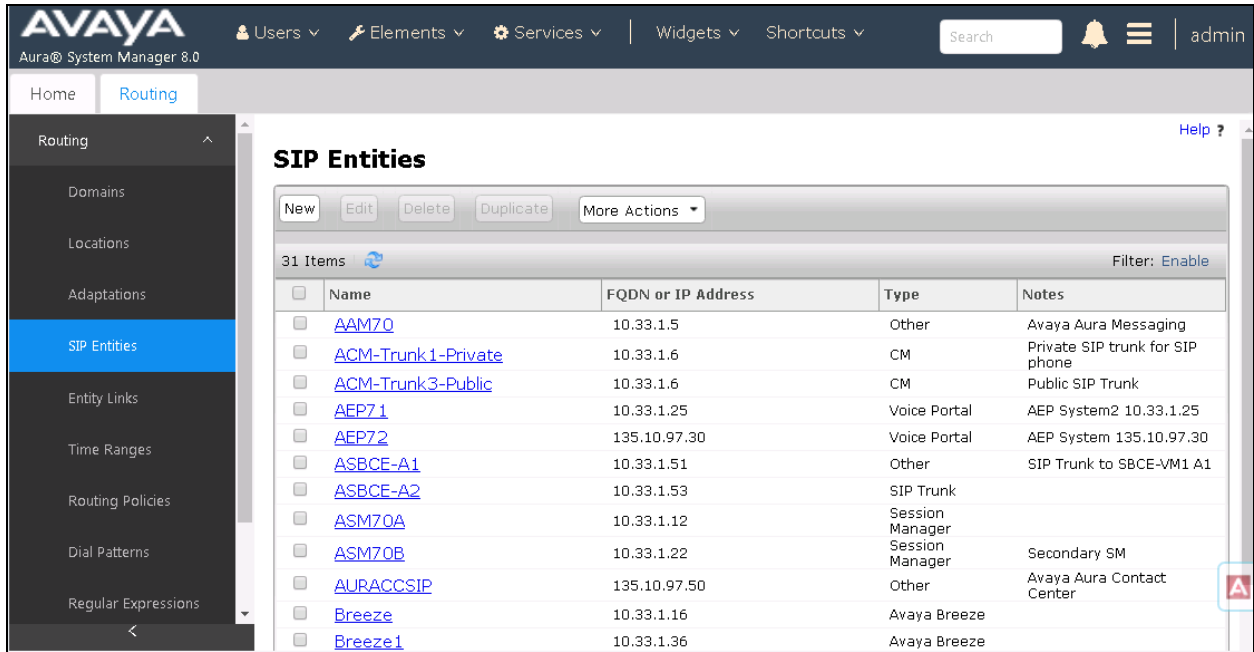
- **Enable CDR:** select the check box to enable CDR feature on Session Manager
- **Password and Confirm Password:** enter a password for user “CDR_User”
- Keep other fields at default

On the completion, click **Commit** button to save the changes.

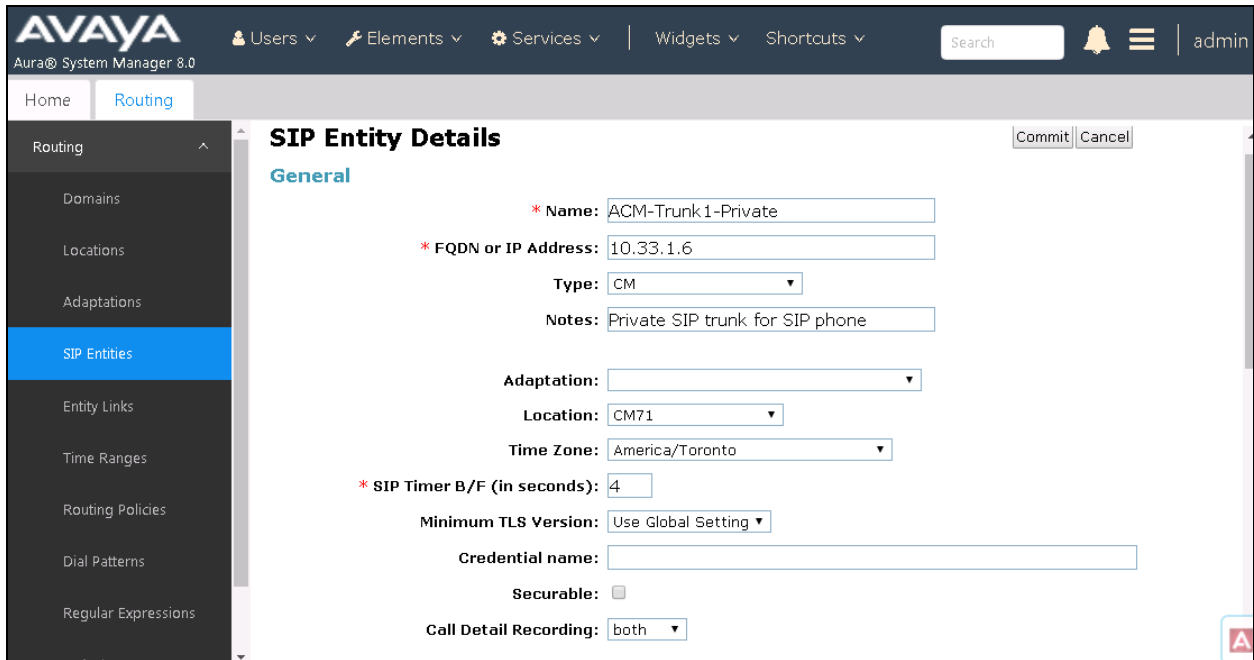


5.3. Administer Call Detail Recording on SIP Entity

From the home page of System Manager, navigate to **Elements** → **Routing**. The **Routing** tab is displayed with SIP Entities shown in the right side of window.



Select the “ACM-Trunk1-Private” SIP entity which is Communication Manager SIP entity and select “both” on the **Call Detail Recording** field. On the completion, click **Commit** button to save the change.



Repeat the procedure above for another SIP entity that wishes Session Manager to log CDR on their SIP entity. The example below is for Avaya IP Office acting like Site 2 as shown up in **Figure 1**.

The screenshot displays the Avaya Aura System Manager 8.0 interface. The top navigation bar includes the Avaya logo, user information (Users), and various menu options (Elements, Services, Widgets, Shortcuts). A search bar and a notification bell are also present. The main content area is titled "SIP Entity Details" and is currently set to the "General" tab. The configuration form includes the following fields:

- Name:** IPOSE110
- FQDN or IP Address:** 10.10.97.110
- Type:** SIP Trunk
- Notes:** (empty text area)
- Adaptation:** (empty dropdown menu)
- Location:** IPO110
- Time Zone:** America/New_York
- SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting
- Credential name:** (empty text area)
- Securable:** (unchecked checkbox)
- Call Detail Recording:** both

Buttons for "Commit" and "Cancel" are located at the top right of the form. A "Help ?" link is also visible. The left sidebar shows a navigation menu with "SIP Entities" highlighted.

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 Session Manager. The procedure covers the following areas:

- Login to Avotus EUR.
- Configure a site.
- Configure 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, and provide credentials to gain access into Avotus EUR in the Sign In window shown below.



Error: Your Session Has Expired!
Please login to continue.

Login:

Password:

Language:

SIGN IN

Access to this service is restricted to authorized users.

6.2. Configure a Site

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



In the screen shown below, **Avotus** is created by default. Click on the top right **Add Site** icon highlighted below to add a site.

The screenshot shows the 'Enhanced Usage Reporting' application interface. At the top, there are navigation tabs for 'Reports', 'Dashboards', and 'Admin'. Below these, a 'Sites' sidebar is visible with a 'Hierarchy' view and a list of sites, including 'Avotus'. The main content area is titled 'Avotus' and contains an 'Options' section with a list of links: 'Contact Information', 'Calendar Configuration', and 'Time Zone'. Below the options is a 'Properties' section with a table of site details.

Properties	
Name	Avotus
Creator	
Creation Date	11/29/2018 03:47:25
Node Type	corporation
Last Updated	11/29/2018 03:47:25

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

The screenshot shows the 'Add Site' dialog box. It features a 'Site Name' input field with the text 'Avaya SM' entered. At the bottom right of the dialog, there are two circular buttons: a checkmark (OK) and an 'X' (Cancel). The background shows the same application interface as the previous screenshot, with the 'Add Site' icon highlighted in the sidebar.

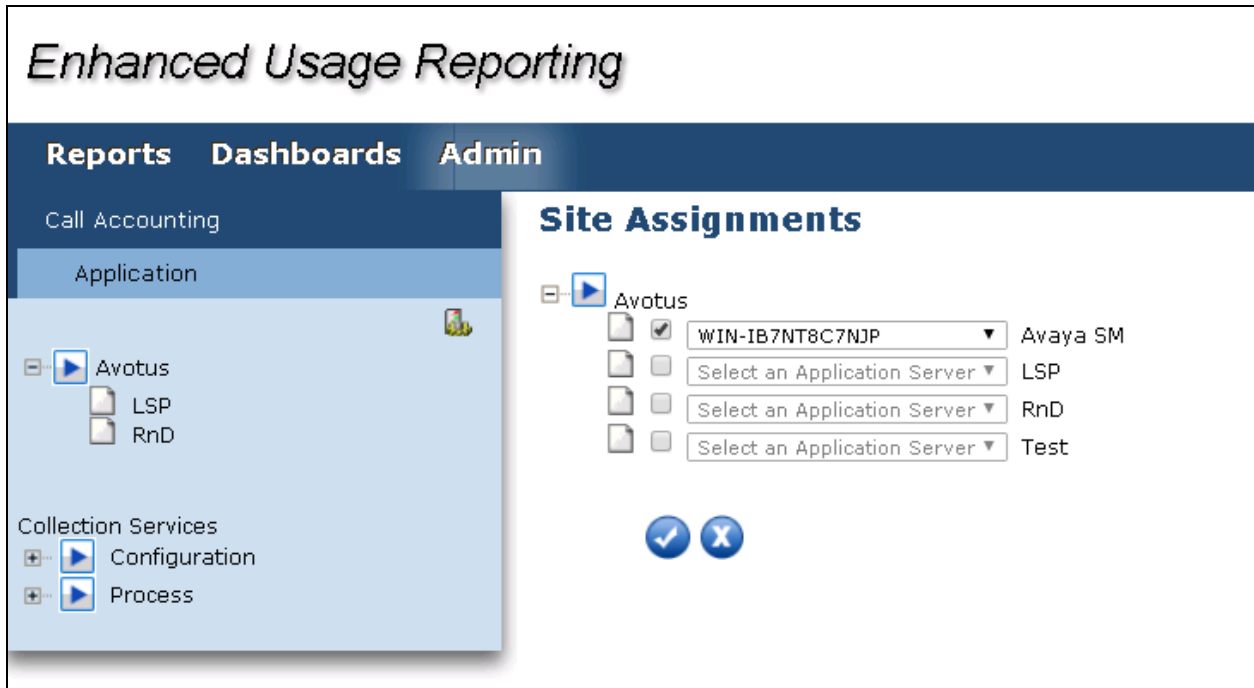
To assign the site created above for collection of data; navigate to **Admin** → **Call Accounting** → **Application** as shown in the screen below.



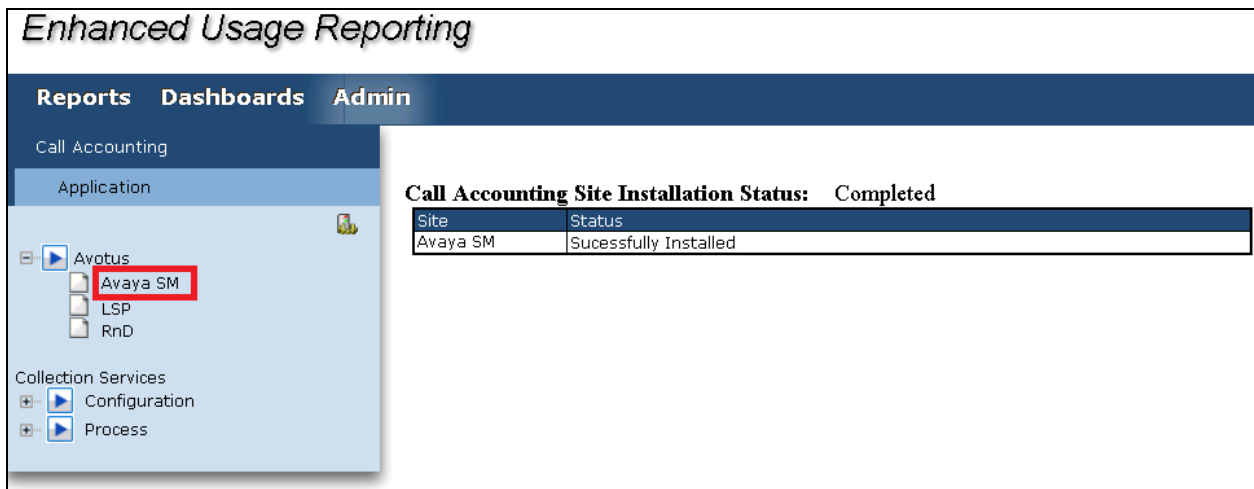
In the **Application** section, start the configuration by clicking on the **Configure** icon as highlighted in the screen below.



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 SM” is the site created earlier in this section.



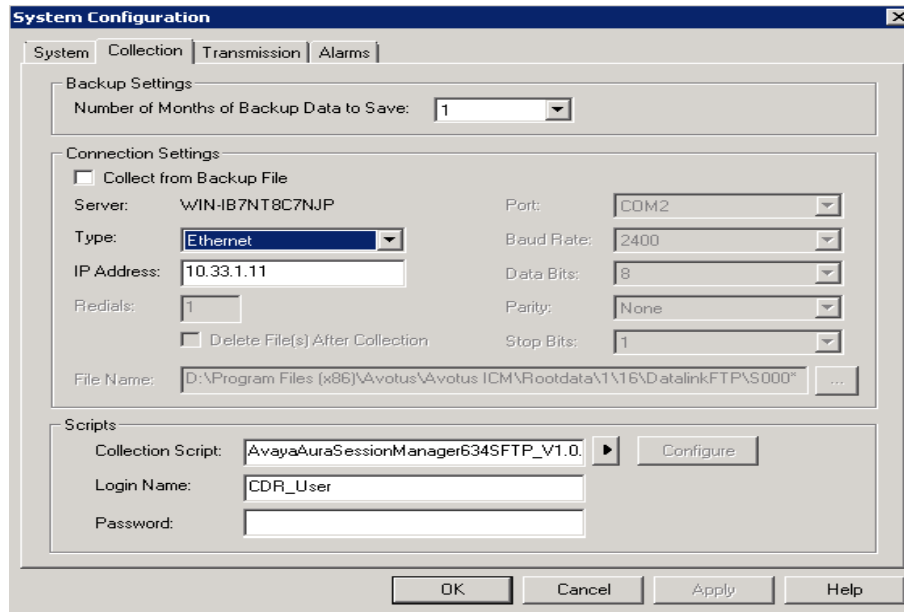
Screen below shows the successful assigning of the site for collection.



6.3. Configure Collection

6.3.1. When CDR format is “Enhanced Flat File” in Avaya Session Manager

Click on the newly assigned Site, as in the screenshot above the newly assigned Site is “Avaya SM”. This will open dialog box “System Configuration as shown below.

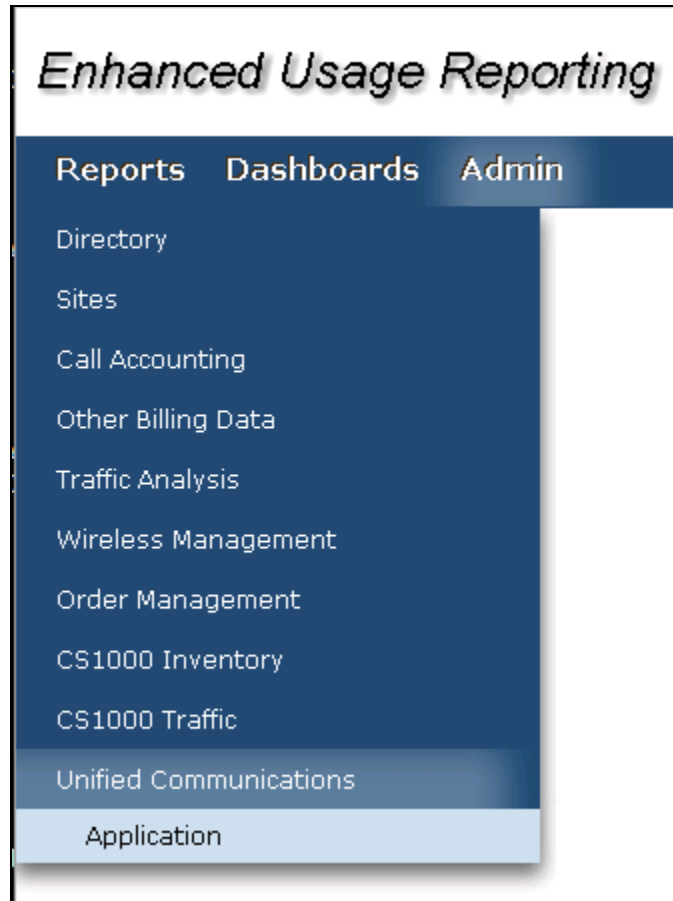


As shown in above figure, configure:

- **Type:** Ethernet
- **IP Address:** IP address of Session Manager
- **Collection Script:** AvayaAuraSessionManager634SFTP_V1.0.col.
- **Login Name:** Login ID of user configured in the “CDR feature” in Session Manager as configured in **Section 5.2**.
- **Password:** Password of user configured in the “CDR feature” in Session Manager as configured in **Section 5.2**.

6.3.2. When CDR format is “Enhanced XML File” in Avaya Session Manager

To configure the collection for data, navigate to **Admin** → **Unified Communications** → **Application** as shown in the screen below.



From the left navigation menu, click on **Avaya Collection** and from the right window of **Avaya IM Data Collection** click on **Add Configuration Setting** and configure the following values,

- **Site:** Select the site configured in **Section 6.2**.
- **Configuration Name:** Type a descriptive name.
- **Collection For:** Select “Avaya Expanded CDR XML” from the drop-down menu.
- **Extension length:** During compliance testing default value was retained.
- **File Protocol:** Ensure “SFTP” is selected from the drop-down menu.
- **Host Name:** Management IP address of Session Manager.
- **Port Number:** During compliance testing default value was retained.
- **User Name:** The default user name created in Session Manager in **Section 5.2**.
- **Password:** The password configured in **Section 5.2** for the CDR user.

Complete the configuration by clicking on the **Save** button.

The screenshot displays the Avotus Enhanced Usage Reporting interface. The top navigation bar includes 'Reports', 'Dashboards', and 'Admin'. The left sidebar shows 'Unified Communications' and 'Application' sections, with 'Avaya Collection' highlighted under 'COLLECTION SERVICES'. The main content area is titled 'Avaya IM Data Collection' and contains a 'Configuration Setting Details' section. The 'Edit Configuration Setting' form includes the following fields: Site (Avotus/Avaya SM), Configuration Name (SM Collection), Collection For (Avaya Expanded CDR XML), Extension length (5), File Protocol (SFTP), Host Name (10.33.1.11), Port Number (22), User Name (CDR_User), and Password (masked with asterisks). 'Save' and 'Reset' buttons are located at the bottom of the form. A 'Schedule Collection Configuration' section is visible below the form.

6.4. Start Collection

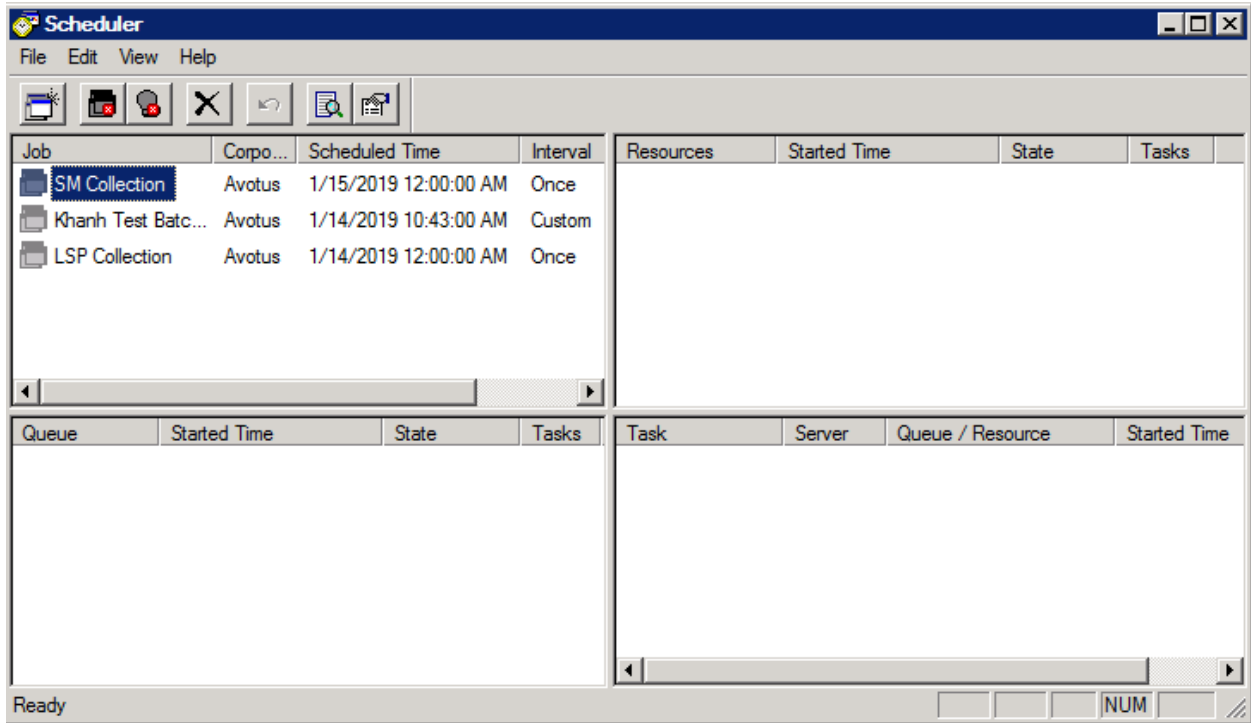
From the left navigation menu, click on **Avaya Collection** and from the right hand window of **Avaya IM Data Collection** click on **Schedule Collection Configuration** and configure the following values,

- **Job Name:** Type a descriptive job name.
- **Description:** Provide a description for the collection job.
- **Start Date (YYYY/MM/DD):** Provide a start date.
- **Start Time (HH MM):** Provide a start time.
- **Interval Type:** Select an interval frequency for the collection.

Retain default values for all other fields and click on the **Save** button.

The screenshot displays the Avotus Enhanced Usage Reporting interface. The top navigation bar includes 'Reports', 'Dashboards', and 'Admin'. The left sidebar shows 'Unified Communications' and 'Application' menus, with 'Avaya Collection' highlighted under 'COLLECTION SERVICES'. The main content area is titled 'Configuration Setting Details' and contains a 'Schedule Collection Configuration' form. The form fields are: Job Name (text input), Priority (dropdown set to 5), Wait For Notification (checkbox checked), Description (text area), Enabled (checkbox checked), Run Late Job (checkbox checked), Start Date (YYYY/MM/DD) (text input), Start Time (HH MM) (text input), and Interval Type (dropdown set to Once). 'Save' and 'Reset' buttons are at the bottom.

The collection job is created in the scheduler as shown below.



The collected raw CDR data can be found in the “Avaya_XML_Collection_Backup” folder, which is under the “/Rootdata/<Corporation number>/<Site number>” folder.

7. Verification Steps

The following steps may be used to verify the configuration:

- Make several different types of calls such as between local stations, outgoing call via SIP trunk, and incoming call via PSTN and verify that call records were collected from Avotus EUR and shown up in the report.
- 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

Enhanced Usage Reporting		AVOTUS® Intelligent Communications Management							
Reports	Dashboards	Admin							
My Reports			2019-Jan-21 16:22:06	Extension / 3408	Trunk / ACM-Trunk1-Private	96149674303	0:54	0:00	0:00
Call Accounting			2019-Jan-21 16:27:42	Extension / 3401	Extension / 4300	3401	0:18	0:00	0:00
Billing			2019-Jan-21 16:28:36	Extension / 3408	Extension / 3410	3408	10:04:24	0:00	0:00
Posted Billing			2019-Jan-21 16:32:12	Extension / 3410	Extension / 3408	3410	7:48	0:00	0:00
Charge Backs			2019-Jan-21 16:36:36	Extension / 3408	Extension / 3410	3408	10:04:24	0:00	0:00
Call Summary			2019-Jan-21 16:50:00	Extension / 3410	Extension / 3408	3410	8:00	0:00	0:00
Call Detail			2019-Jan-21 16:58:24	Extension / 3408	Extension / 3301	3408	4:36	0:00	0:00
Top N			2019-Jan-21 17:00:18	Extension / 3408	Extension / 3401	3408	0:42	0:00	0:00
External Party			2019-Jan-21 17:01:12	Extension / 3408	Extension / 3301	3408	0:48	0:00	0:00
Performance Monitoring			2019-Jan-21 17:02:36	Extension / 3408	Extension / 3403	3408	10:04:24	0:00	0:00
Diagnostic			2019-Jan-21 17:03:24	Extension / 3408	Extension / 3401	3408	2:36	0:00	0:00
Unified Communications			2019-Jan-21 17:16:00	Extension / 3408	Extension / 3301	3408	0:00	0:00	0:00
Wireless Management			2019-Jan-21 17:17:00	Extension / 3408	Extension / 3301	3408	6:00	0:00	0:00
Traffic Analysis			2019-Jan-21 17:25:00	Extension / 3408	Extension / 3301	3408	2:00	0:00	0:00
Total Telecom Spend			2019-Jan-21 17:30:12	Extension / 3408	Extension / 3301	3408	5:48	0:00	0:00
Order Management			2019-Jan-21 17:36:18	Extension / 3403	Extension / 3408	3403	4:42	0:00	0:00
Other Billing Data			2019-Jan-22 02:28:36	Extension / 3408	Extension / 3410	3408	10:04:24	0:00	0:00
			2019-Jan-22 02:36:36	Extension / 3408	Extension / 3410	3408	10:04:24	0:00	0:00
			2019-Jan-22 03:02:36	Extension / 3408	Extension / 3403	3408	10:04:24	0:00	0:00
			2019-Jan-22 14:42:30	Trunk / ACM-Trunk1-Private	Extension / 3401	6149674309	1:30	0:00	0:00
			2019-Jan-22 14:43:06	Extension / 4309	Extension / 3301	4309	2:54	0:00	0:00
			2019-Jan-22 14:43:54	Extension / 4309	Extension / 3301	4309	6:06	0:00	0:00
			2019-Jan-22 15:08:12	Extension / 4305	Extension / 3406	4305	0:48	0:00	0:00
			2019-Jan-22 15:08:18	Extension / 3406	Extension / 4305	3406	1:42	0:00	0:00
			2019-Jan-22 15:13:18	Extension / 4307	Extension / 3406	4307	1:42	0:00	0:00
			2019-Jan-22 20:54:00	Extension / 3408	Extension / 3410	3408	1:39:00	0:00	0:00
			2019-Jan-22 21:02:00	Extension / 3408	Extension / 3410	3408	1:39:00	0:00	0:00
			2019-Jan-22 21:28:00	Extension / 3408	Extension / 3403	3408	1:39:00	0:00	0:00
							Summary	69:09:18	0:00

8. Conclusion

These Application Notes describe the steps required to configure Avotus Enhanced Usage Reporting for Unified Communications to interoperate with Avaya Aura® Session Manager and capturing/processing call records. All feature and serviceability test cases described in **Section** Error! Reference source not found. were passed with the observations pointed in **Section** Error! Reference source not found..

9. Additional References

This section references the Avaya and Resource Software International 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® Session Manager*, Document 03-300509, Issue 10, Release 8.0, August 2018

[2] *Administering Avaya Aura® System Manager*, 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>

©2019 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ 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.