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 0**, 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 ® Session Manager (Session Manager) and Avotus Enhanced Usage Reporting for Unified Communications (Avotus EUR). Avotus EUR 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.

Avotus EUR is a Call Accounting and Billing package that utilizes the CDR output from Avaya Aura® Session Manager. Avotus EUR collects, stores, and processes the CDR records to provide usage analysis, call costing and billing capabilities. Avaya Aura® Session Manager can generate Call Detail Records for intra-switch calls, inter-switch calls, inbound trunk calls and outbound trunk calls. Avotus EUR connects to Session Manager over the local or wide area network using Secure File Transfer Protocol (SFTP). Session Manager is configured to generate Call Detail Records (CDR) into files and save them to a specific folder on the Session Manager server. Avotus EUR using SFTP connects to the server to access these folders and downloads XML files generated by Session Manager, to the local Avotus EUR server for reports. For the compliance testing, the “Enhanced XML file” format was used as the Data File Format on Session Manager.

2. General Test Approach and Test Results

The general test approach was to manually place intra-switch calls, inter-switch calls, inbound trunk, outbound trunk calls to and from H323 telephones controlled by Communication Manager and SIP endpoints registered to Session Manager and verify that Avotus EUR collects the CDR records and properly classifies and reports the attributes of the call. For serviceability testing LAN failures and a restart of the Avotus EUR server were simulated.

Session Manager R7.0.x contains interface changes related to the security of the Call Detail Recording (CDR) login, used to download CDR records from a Session Manager server. These changes were not backward compatible with the Avaya recommended CDR retrieval procedure of deleting CDR files once they had been retrieved. A patch was created that reverts the operation of the CDR_User back to what it was in release 6.3 and earlier. This patch was used in this configuration. Additional details on the patch and how to obtain it are available at support.avaya.com, under PSN004893u.

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 testing included feature and serviceability testing. The feature testing evaluated the ability of Avotus EUR to collect and process CDR records for calls over SIP trunks. The source and destination of each call was verified on the Avotus EUR application. The interoperability compliance testing includes the following cases.

- Calls between H323 and SIP phones over SIP Trunk.
- Inbound and outbound calls to/from H323 phones over SIP trunks to simulated PSTN.
- Inbound and outbound calls to/from SIP phones over SIP trunks to simulated PSTN.

The serviceability testing introduced failure scenarios to see if Avotus EUR could resume CDR collection after failure recovery.

2.2. Test Results

All feature and performance tests passed with the following observation.

- Session Manager CDR was designed to cover calls between 2 parties, where at least one leg of the call traverses Session Manager. Calls that involve Communication Manager invoking call features (such as transfer, conference, call-forward, etc.) may not yield the expected call records by Session Manager. This design may change in future versions of Session Manager.

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 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 Session 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 telephones. 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.

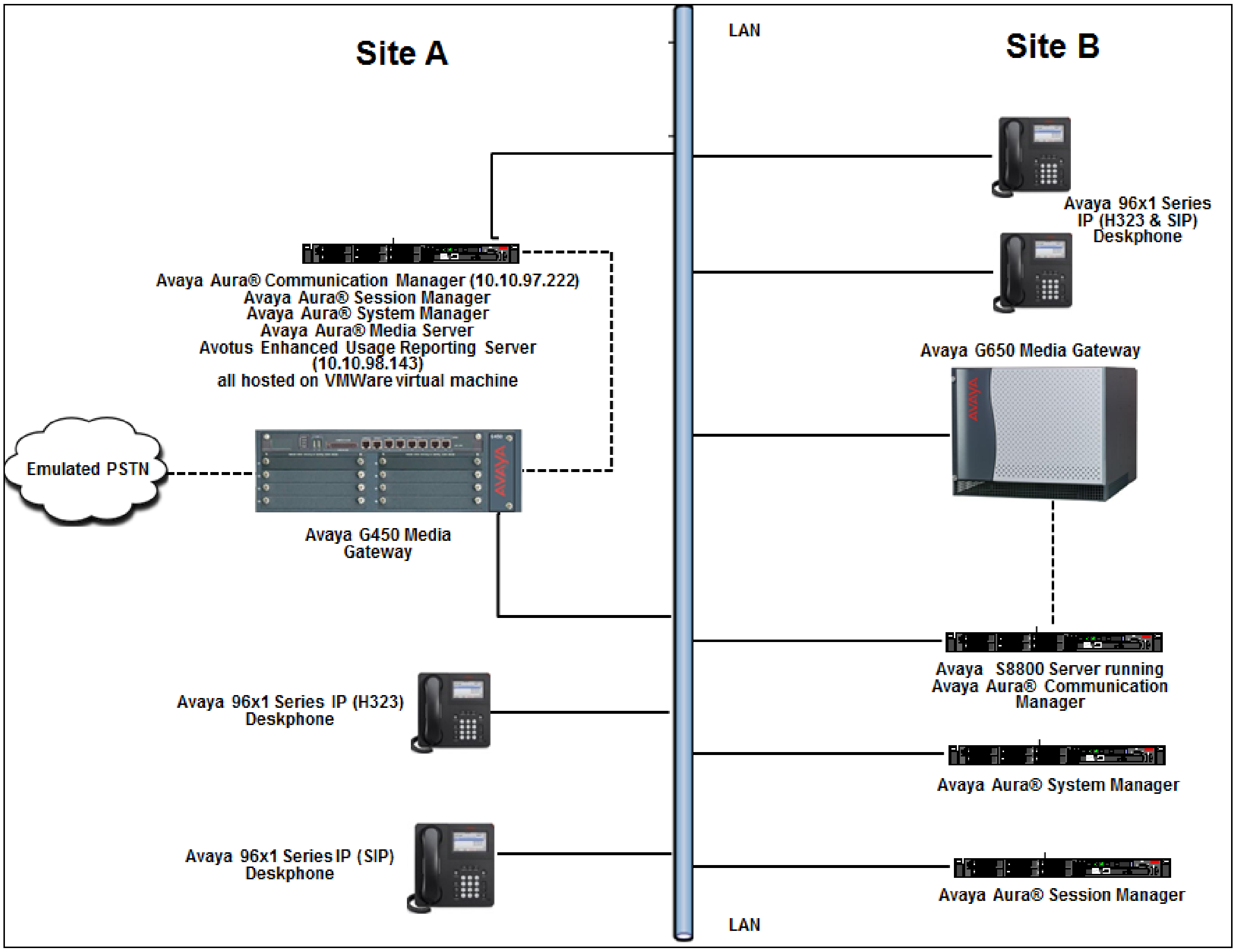

Site A
LAN
Site B
Avaya 96x1 Series IP (H323 & SIP) Deskphone
Avaya Aura® Communication Manager (10.10.97.222)
Avaya Aura® Session Manager
Avaya Aura® System Manager
Avaya Aura® Media Server
Avotus Enhanced Usage Reporting Server (10.10.98.143)
all hosted on VMWare virtual machine
Avaya G650 Media Gateway
Emulated PSTN
Avaya G450 Media Gateway
Avaya S8800 Server running Avaya Aura® Communication Manager
Avaya 96x1 Series IP (H323) Deskphone
Avaya Aura® System Manager
Avaya 96x1 Series IP (SIP) Deskphone
Avaya Aura® Session Manager
LAN

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 a virtual server	7.0.1.2.0-FP1SP2
Avaya Aura® Session Manager running on a virtual server	7.0.1.2.701230
Avaya Aura® System Manager running on a virtual server	7.0.1.2 Service Pack 2
Avaya Aura® Media Server running on a virtual server	7.7.0.375
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 running on Windows Server 2008 R2 Standard SP1 running on VMware (5.5)	9.10

5. Configure Avaya Aura® Communication Manager

There is no specific configuration necessary on Communication Manager for the collection of CDR from Session Manager. It is assumed that the SIP trunk to Session Manager is already setup. The following is a quick overview of the SIP trunk that was used during compliance testing. The steps are performed through the System Access Terminal (SAT) interface. Some screens in this section have been abridged and highlighted for brevity and clarity in presentation.

5.1. Configure SIP Trunk

In the Node Names IP form, note the IP Address of the **procr** and the Session Manager (**SM-VM**). The host names will be used throughout the other configuration screens of Communication Manager and Session Manager. Type **display node-names ip** to show all the necessary node names.

```
display node-names ip
                                  IP NODE NAMES
    Name                  IP Address
SM-VM                   10.10.97.228
procr                   10.10.97.222
procr6                  ::
```

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is **bvwdev.com**. The **IP Network Region** form also specifies the **IP Codec Set** to be used. This codec set will be used for calls routed over the SIP trunk to Session manager as **ip-network region 1** is specified in the SIP signaling group.

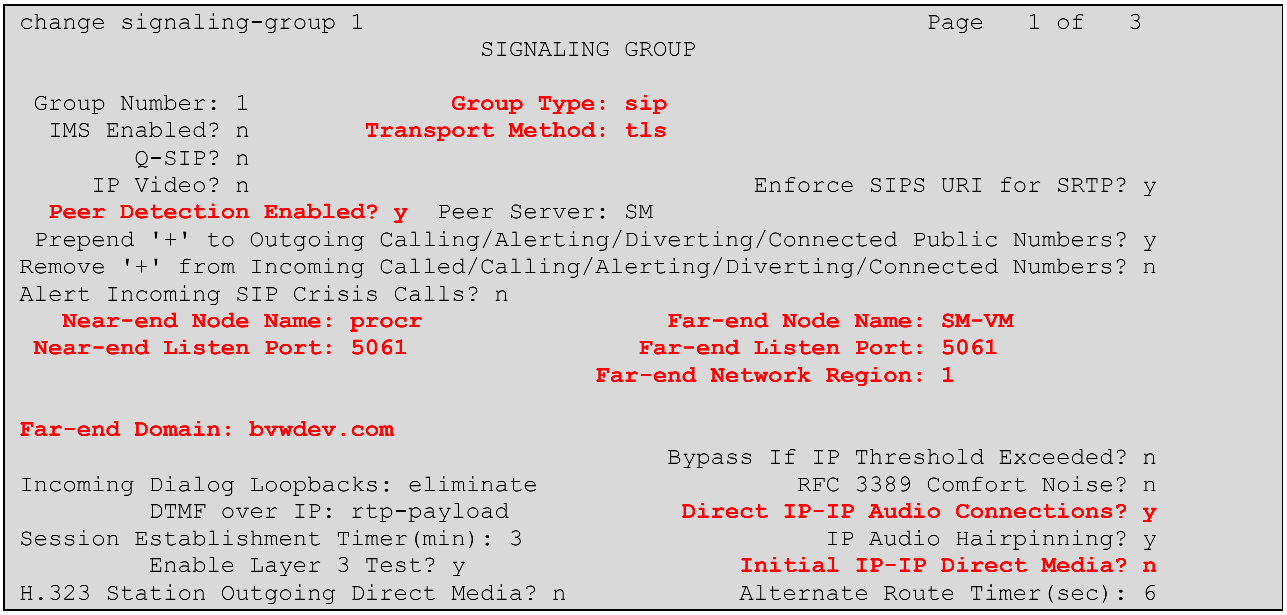
```
display ip-network-region 1                                    Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location:          Authoritative Domain: bvwdev.com
    Name: Region1                 Stub Network Region: n
MEDIA PARAMETERS                  Intra-region IP-IP Direct Audio: yes
      Codec Set: 1                Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                        IP Audio Hairpinning? y
   UDP Port Max: 8001
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

In the **IP Codec Set** form, select the audio codec's supported for calls routed over the SIP trunk to Communications Portal. The form is accessed via the **change ip-codec-set n** command. Note that IP codec set 1 was specified in IP Network Region 1 shown above. Multiple codecs may be specified in the **IP Codec Set** form in order of preference; the example below includes **G.711MU** and **G.711A**, which are supported by Communications Portal.

```
change ip-codec-set 1                                          Page   1 of   2

                          IP CODEC SET
    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU          n          2        20
 2: G.711A           n          2        20
```

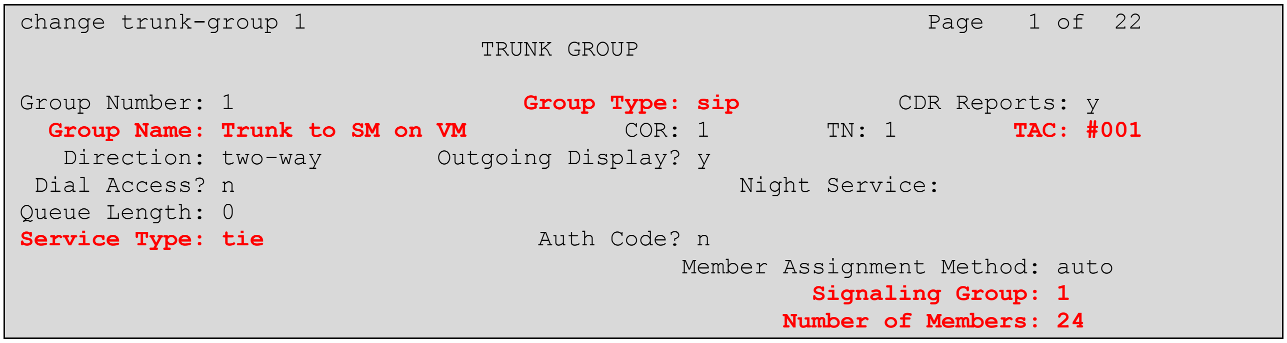
Prior to configuring a SIP trunk group for communication with Session Manager, a SIP signaling group must be configured. Configure the Signaling Group form shown below as follows:

- Set the **Group Type** field to **sip**.
- Set the **Transport Method** to the desired transport method, for compliance testing this was set to **tls**.
- The **Peer Detection Enabled** field should be set to **y** allowing the Communication Manager to automatically detect if the peer server is a Session Manager.
- Set the **Near-end Node Name** to **procr**. This value is taken from the **IP Node Names** form shown above.
- Set the **Far-end Node Name** to the node name defined for the Session Manager (node name **SM-VM**), as per **IP Node Names** form shown above.
- Ensure that the recommended TLS port value of **5061** is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- In the **Far-end Network Region** field, enter the IP Network Region configured above**.** This field logically establishes the **far-end** for calls using this signaling group as network region 1.
- Enter the **Far-end Domain** field to allow Communication Manager to accept the configured domain in Session Manager. During compliance testing **bvwdev.com** was configured in Session Manager.
- The **Direct IP-IP Audio Connections** field is set to **y**.
- The **Initial IP-IP Direct Media** field is set to **n**.
- The default values for the other fields may be used.



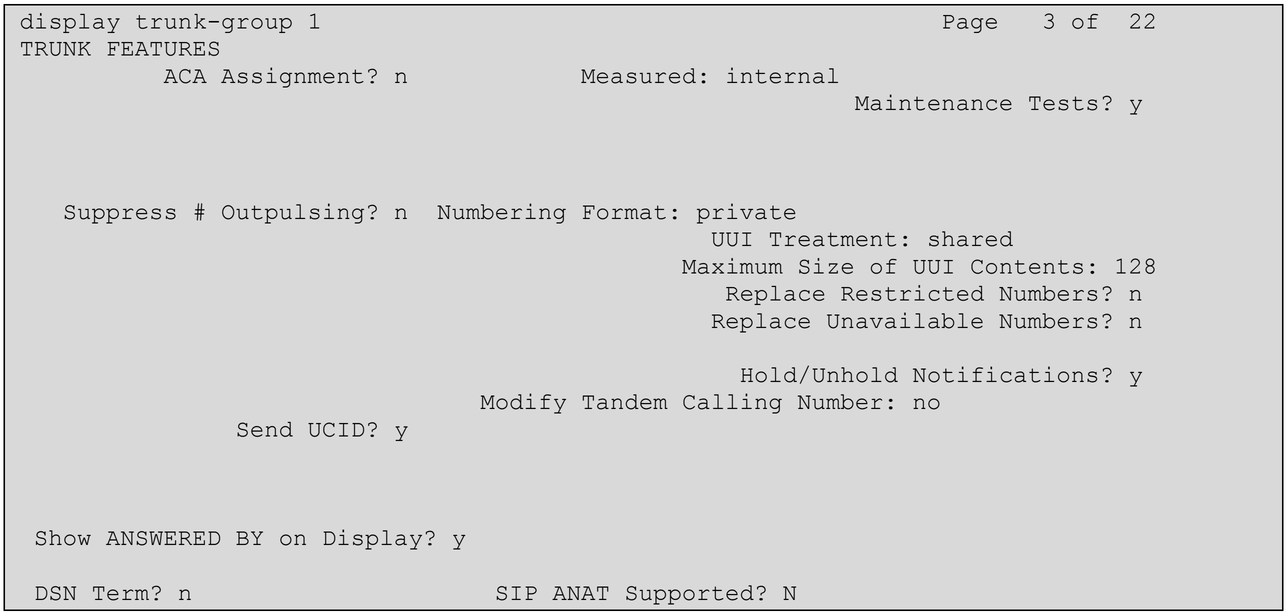
```
change signaling-group 1                                       Page   1 of   3
                                SIGNALING GROUP

 Group Number: 1              Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? n                                   Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr                 Far-end Node Name: SM-VM
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                        Far-end Network Region: 1

Far-end Domain: bvwdev.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? y
         Enable Layer 3 Test? y                   Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 6
```

Configure the **Trunk Group** form as shown below. This trunk group is used for calls to and from Communications Portal. Enter a descriptive name in the **Group Name** field. Set the **Group Type** field to **sip**. Enter a **TAC** code compatible with the Communication Manager dial plan. Set the **Service Type** field to **tie**. Specify the signaling group associated with this trunk group in the **Signaling Group** field, and specify the **Number of Members** supported by this SIP trunk group. Accept the default values for the remaining fields.



```
change trunk-group 1                                           Page   1 of  22
                                TRUNK GROUP

Group Number: 1                    Group Type: sip           CDR Reports: y
  Group Name: Trunk to SM on VM           COR: 1        TN: 1        TAC: #001
   Direction: two-way        Outgoing Display? y
 Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 1
                                                     Number of Members: 24
```

Settings on **Page 3** can be left as shown below.

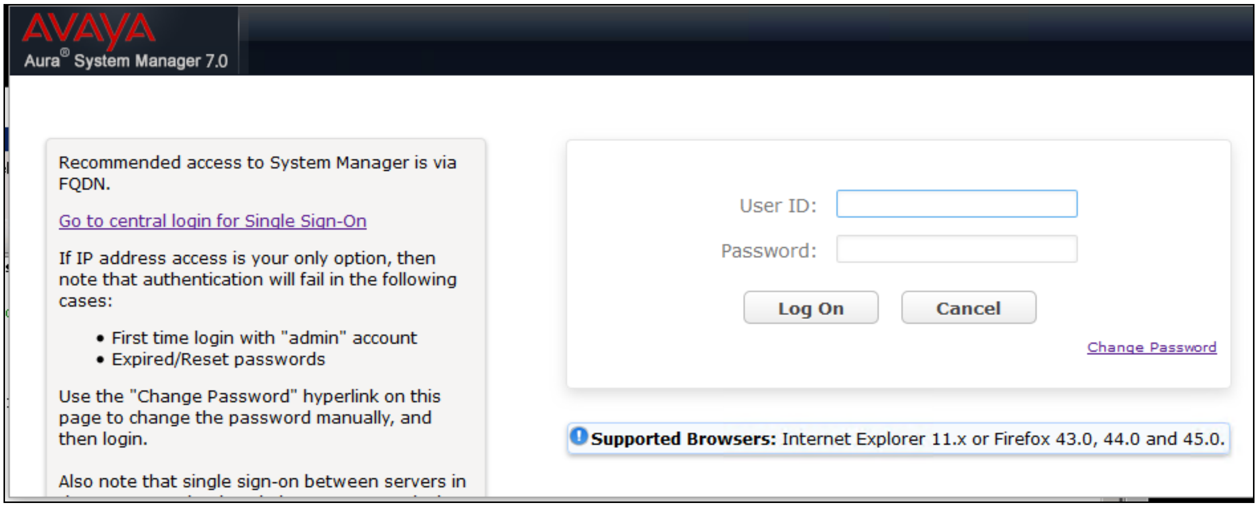


```
display trunk-group 1                                           Page   3 of  22
TRUNK FEATURES
          ACA Assignment? n            Measured: internal
                                                          Maintenance Tests? y



   Suppress # Outpulsing? n  Numbering Format: private
                                                UUI Treatment: shared
                                              Maximum Size of UUI Contents: 128
                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n

                                                  Hold/Unhold Notifications? y
                                Modify Tandem Calling Number: no
               Send UCID? y



 Show ANSWERED BY on Display? y

 DSN Term? n                     SIP ANAT Supported? N
```

6. Configure Avaya Aura® Session Manager

Note: For the compliance testing, the "Enhanced XML file" format was used as the Data File Format on Session Manager.

In order to make changes in Session Manager, a web session is established to System Manager. Log into System Manager by opening a web browser and navigating to http://<System Manager IP Address>/SMGR. Enter the appropriate credentials for the **User ID** and **Password** and click on **Log On** button.



Recommended access to System Manager is via FQDN.

If IP address access is your only option, then note that authentication will fail in the following cases:

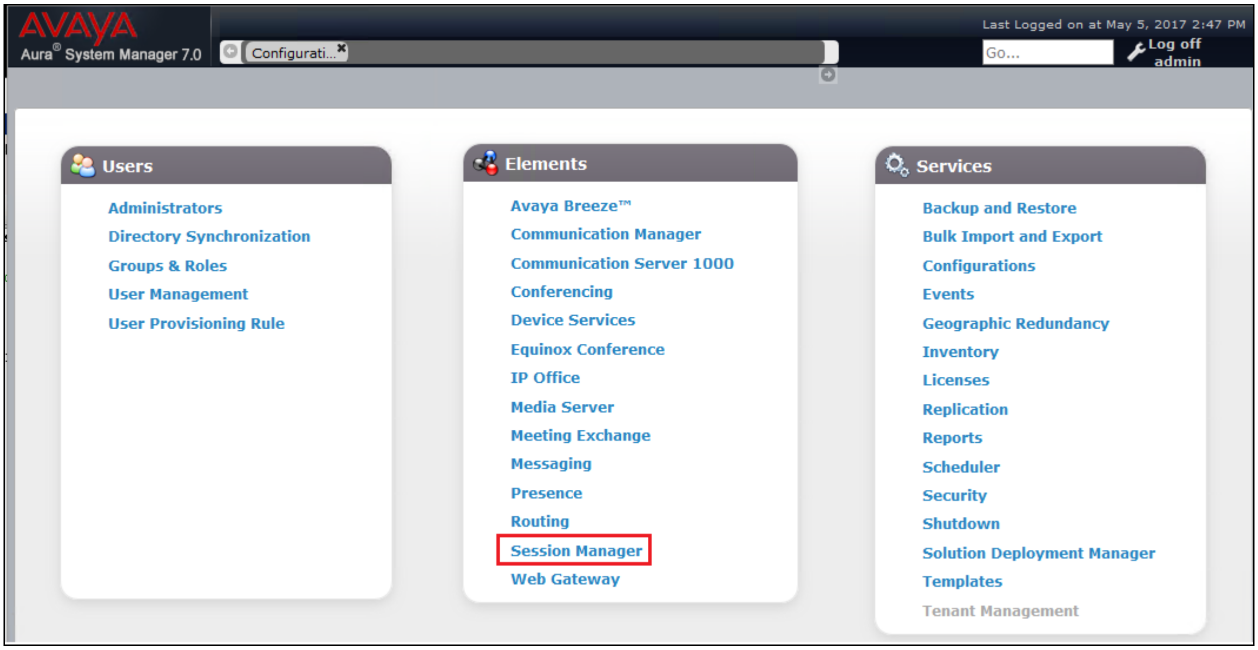
- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

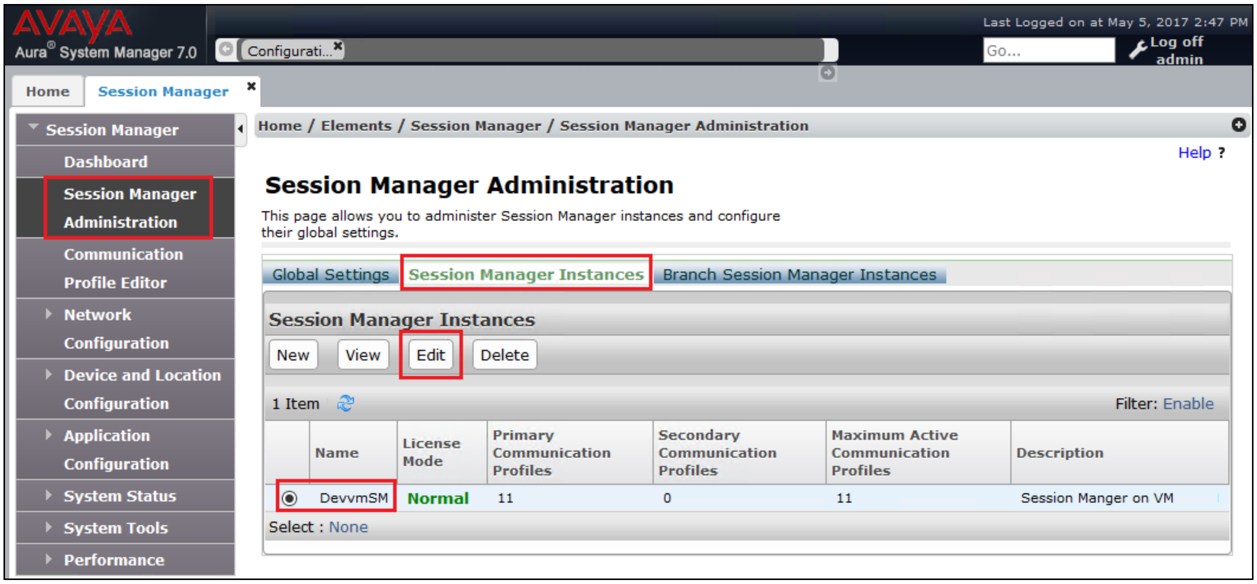
Also note that single sign-on between servers in

Supported Browsers: Internet Explorer 11.x or Firefox 43.0, 44.0 and 45.0.

Once logged in click on **Session Manager** under **Elements** column as shown below.



The Session Manager tab is displayed. In the left navigation pane select **Session Manager Administration**. When the **Session Manager Administration** page is displayed select the **Session Manager Instances** tab and then select the Session Manager instance e.g., **DevvmSM** and click on **Edit** button to edit.



Home / Elements / Session Manager / Session Manager Administration

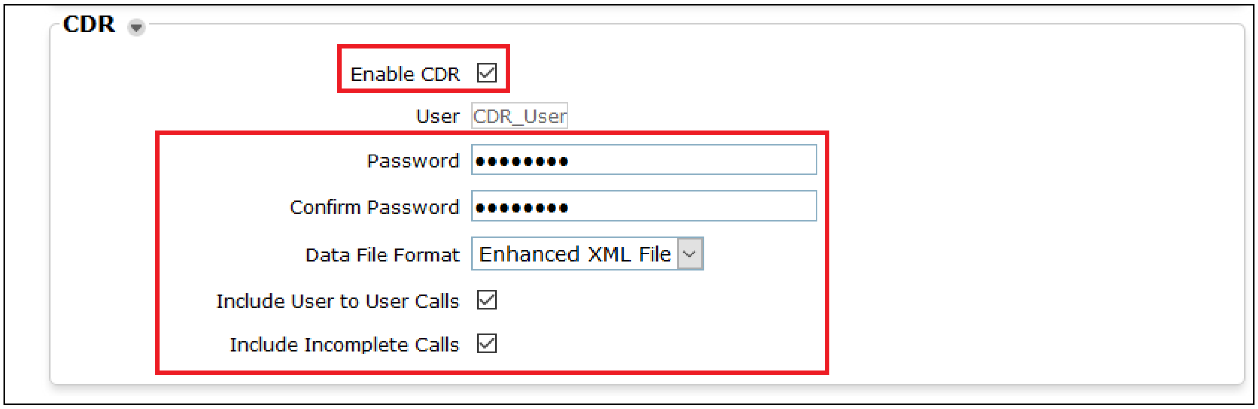
Session Manager Administration

This page allows you to administer Session Manager instances and configure their global settings.

Session Manager Instances

	Name	License Mode	Primary Communication Profiles	Secondary Communication Profiles	Maximum Active Communication Profiles	Description
●	DevvmSM	Normal	11	0	11	Session Manger on VM

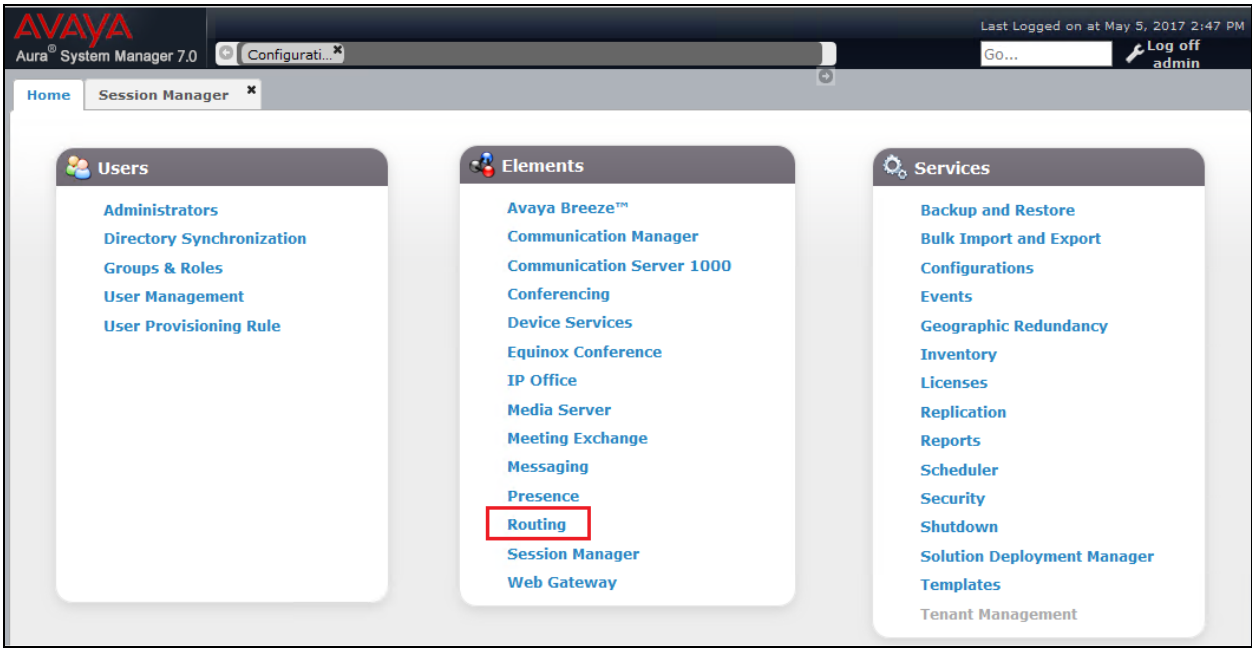
The **Edit Session Manager** page is displayed. Scroll down to the **CDR** section, check on the check box **Enable CDR** to enable the CDR feature and enter a password in the **Password** and **Confirm Password** box for the **CDR_User**. Ensure that both **Include User to User Calls** and **Include Incomplete Calls** are both ticked as shown. If the site does not want to capture user to user calls or incomplete calls, then these boxes need not be checked. Click the **Commit** button (not shown) at the end of the page to commit the changes.



CDR

Enable CDR	☑
User	CDR_User
Password	••••••••
Confirm Password	••••••••
Data File Format	Enhanced XML File
Include User to User Calls	☑
Include Incomplete Calls	☑

Each SIP Entity must have their CDR enabled as well; in order to make changed to SIP Entities select **Routing** from Elements column as shown below.


AVAYA Aura® System Manager 7.0 | Configurati... | Last Logged on at May 5, 2017 2:47 PM | Go... | Log off admin

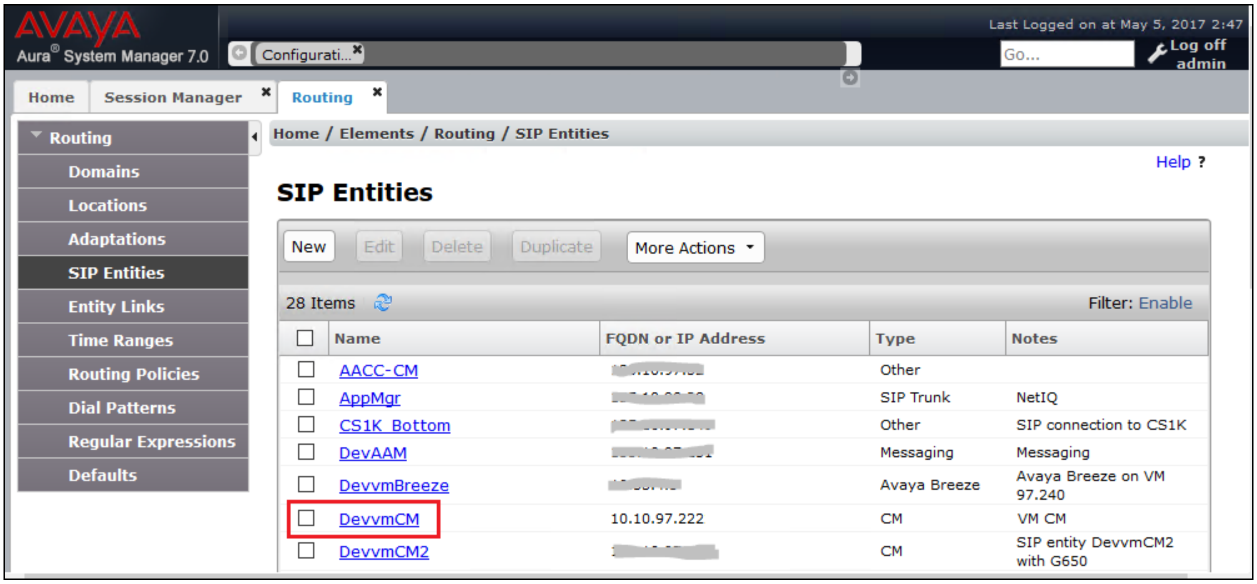
Home | Session Manager

Users
- Administrators
- Directory Synchronization
- Groups & Roles
- User Management
- User Provisioning Rule

Elements
- Avaya Breeze™
- Communication Manager
- Communication Server 1000
- Conferencing
- Device Services
- Equinox Conference
- IP Office
- Media Server
- Meeting Exchange
- Messaging
- Presence
- Routing
- Session Manager
- Web Gateway

Services
- Backup and Restore
- Bulk Import and Export
- Configurations
- Events
- Geographic Redundancy
- Inventory
- Licenses
- Replication
- Reports
- Scheduler
- Security
- Shutdown
- Solution Deployment Manager
- Templates
- Tenant Management

Click on **SIP Entities** in the left window and select the Communication Manager SIP Entity from the main window and click on the **Edit** button. In the example below, it is **DevvmCM**.


AVAYA Aura® System Manager 7.0 | Configurati... | Last Logged on at May 5, 2017 2:47 | Go... | Log off admin

Home | Session Manager | Routing

Routing: Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, Defaults

Home / Elements / Routing / SIP Entities | Help ?

SIP Entities

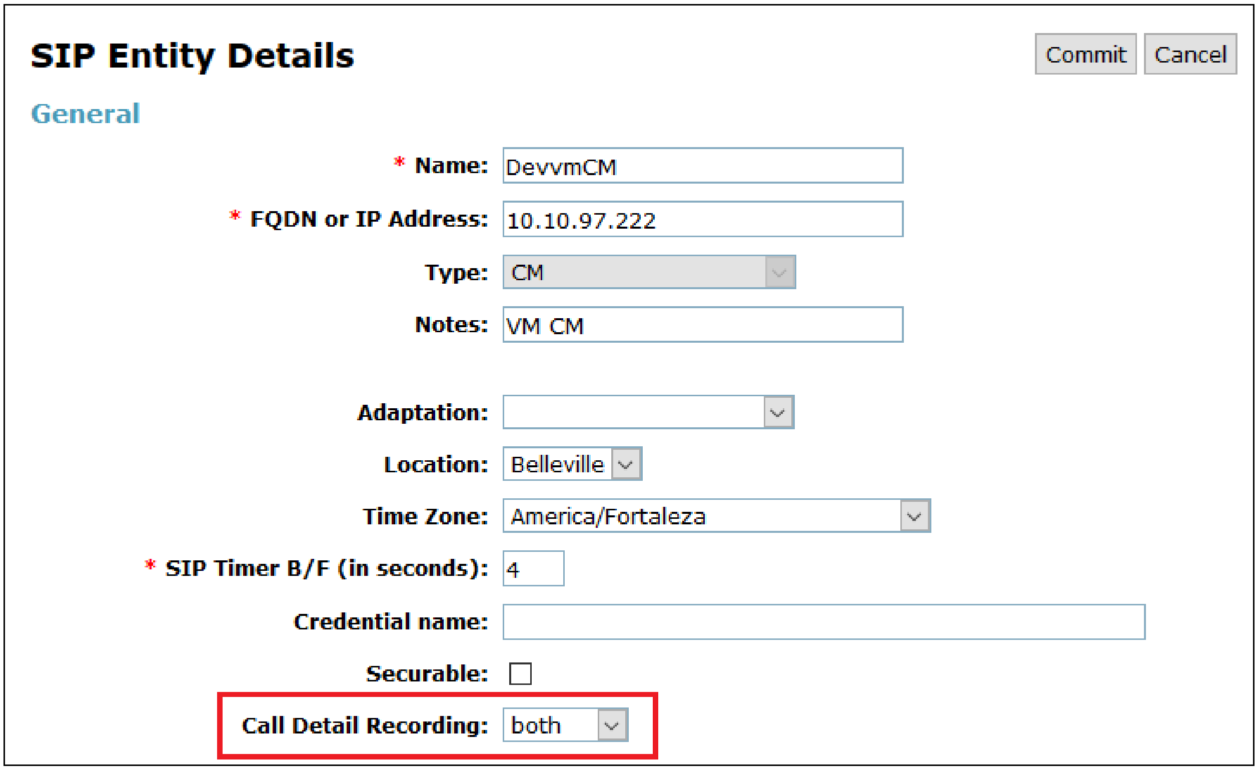
New | Edit | Delete | Duplicate | More Actions

28 Items | Filter: Enable

□	Name	FQDN or IP Address	Type	Notes
□	AACC-CM	[redacted]	Other	
□	AppMgr	[redacted]	SIP Trunk	NetIQ
□	CS1K_Bottom	[redacted]	Other	SIP connection to CS1K
□	DevAAM	[redacted]	Messaging	Messaging
□	DevvmBreeze	[redacted]	Avaya Breeze	Avaya Breeze on VM 97.240
□	DevvmCM	10.10.97.222	CM	VM CM
□	DevvmCM2	[redacted]	CM	SIP entity DevvmCM2 with G650

Change **Call Detail Recording** to **both** as shown below from the drop-down menu and click on **Commit** once finished.

Note: Repeat the same procedure for other SIP Entities if needed



SIP Entity Details

General

* Name:	DevvmCM
* FQDN or IP Address:	10.10.97.222
Type:	CM
Notes:	VM CM
Adaptation:	
Location:	Belleville
Time Zone:	America/Fortaleza
* SIP Timer B/F (in seconds):	4
Credential name:	
Securable:	□
Call Detail Recording:	both

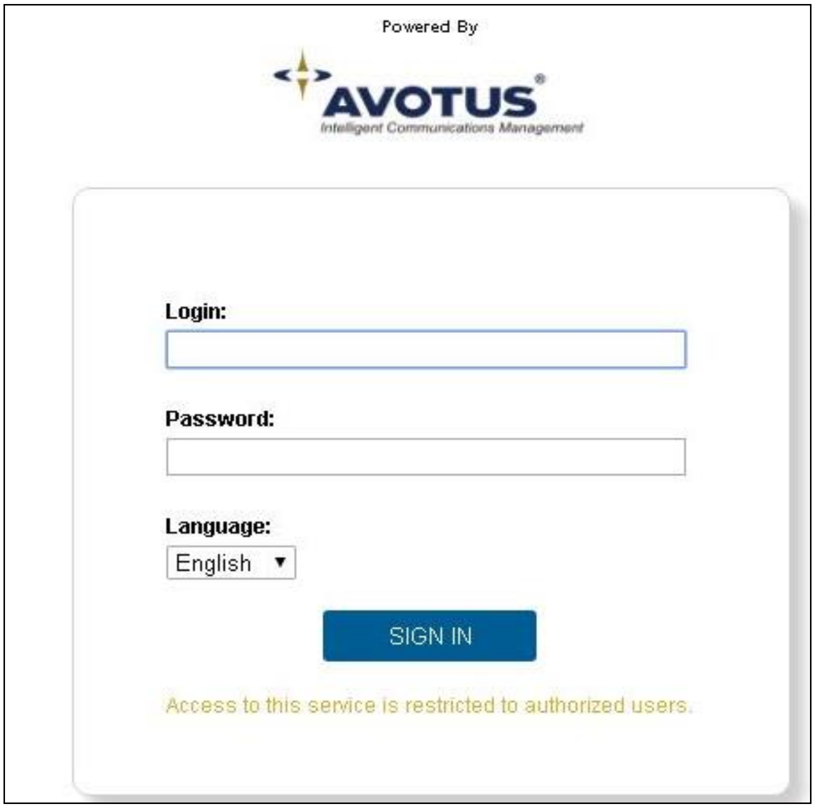
7. Configure Avotus Enhanced Usage Reporting for Unified Communications

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 script and collection
- Start collection.

7.1. Login to Avotus EUR

To configure Avotus EUR, double click on the Avotus EUR icon on desktop (show below) and provide credentials to gain access into Avotus EUR in the Sign In window shown further below.

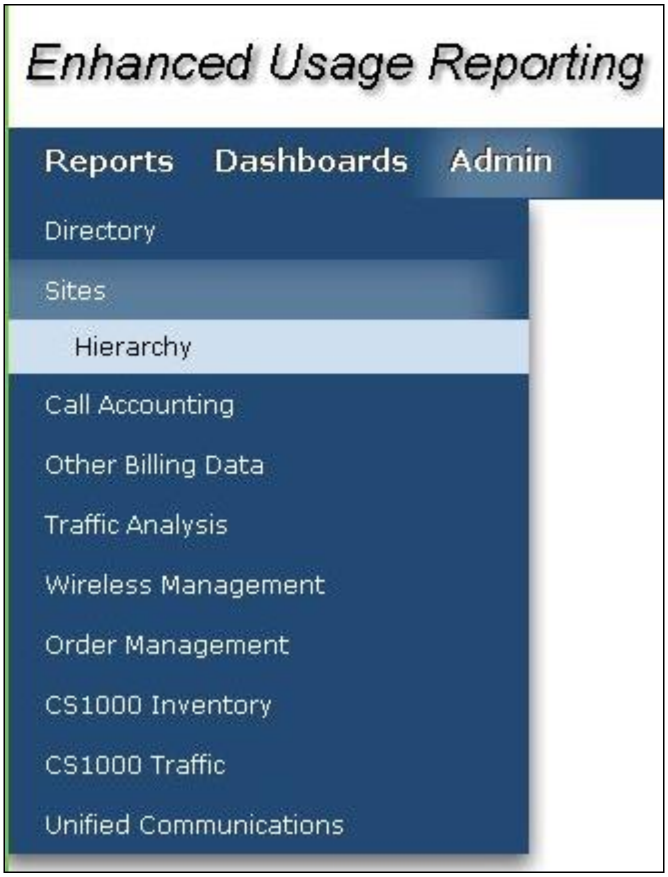


Language: English

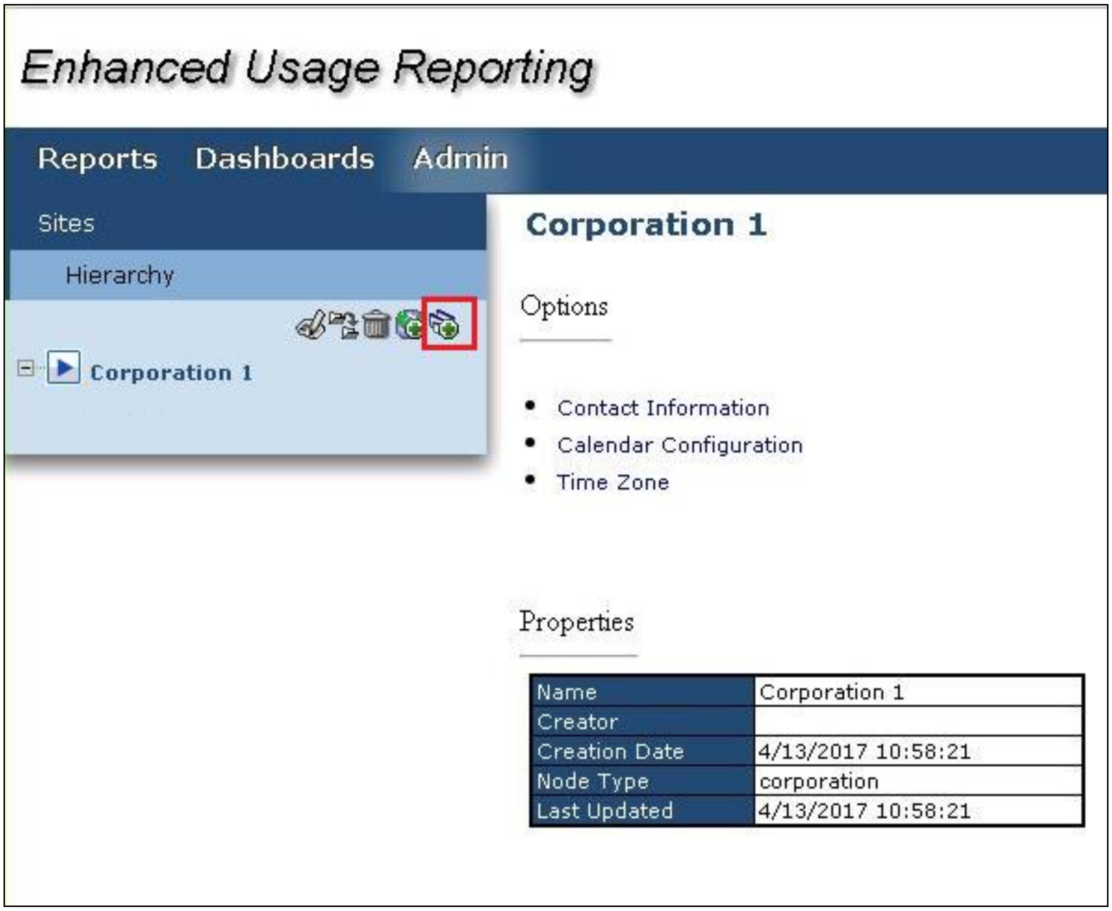
Access to this service is restricted to authorized users.

7.2. 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, **Corporation 1** is created by default. Click on the top right **Add Site** icon highlighted below to add a site.



Corporation 1

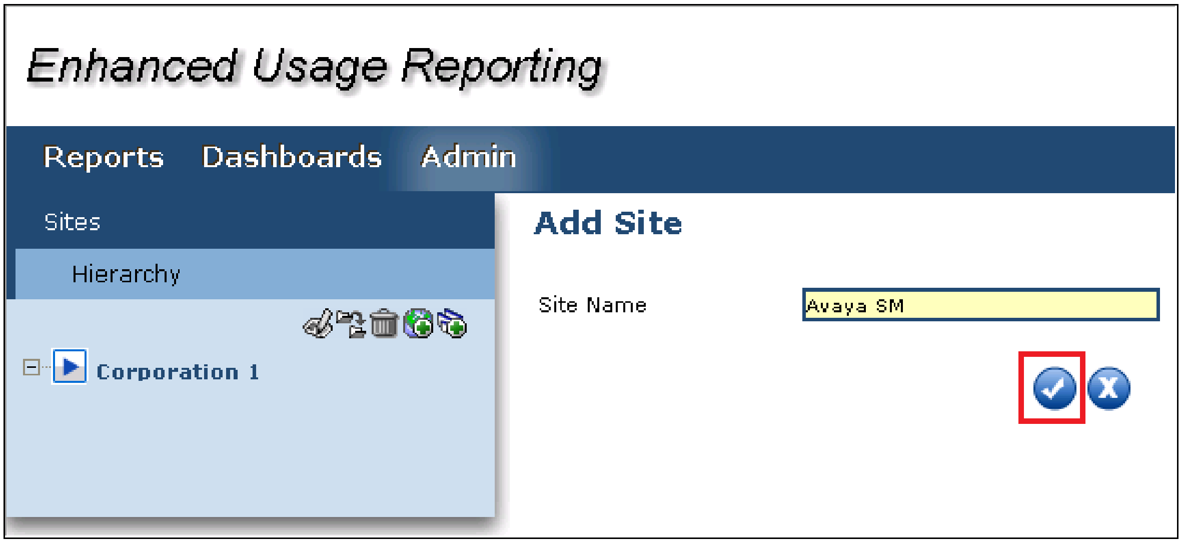
Options

- Contact Information
- Calendar Configuration
- Time Zone

Properties

Name	Corporation 1
Creator	
Creation Date	4/13/2017 10:58:21
Node Type	corporation
Last Updated	4/13/2017 10:58:21

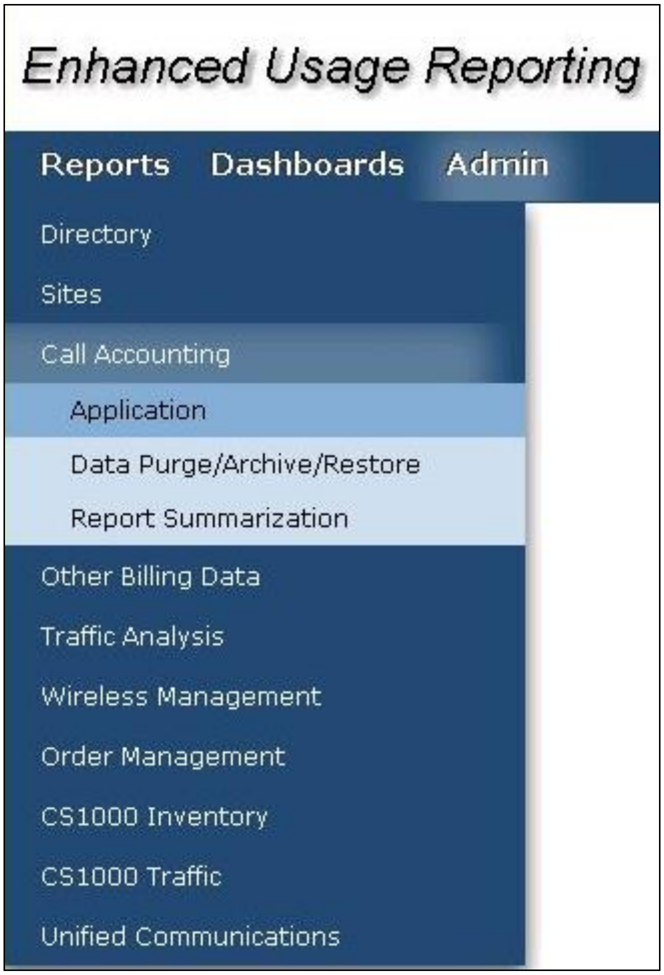
In the **Add Site** window shown below, enter an appropriate name for **Site Name** field and click on the **OK** icon highlighted below.



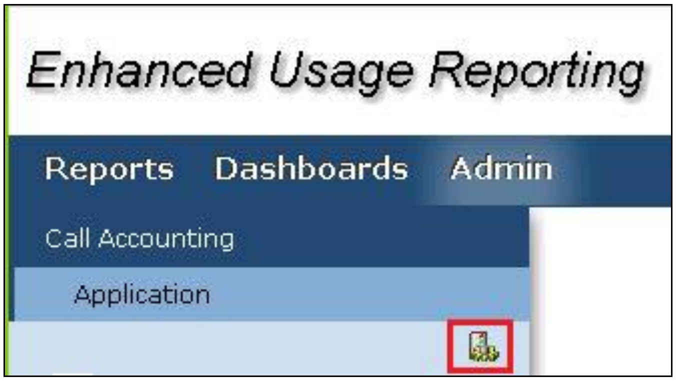
Add Site

Site Name: Avaya SM

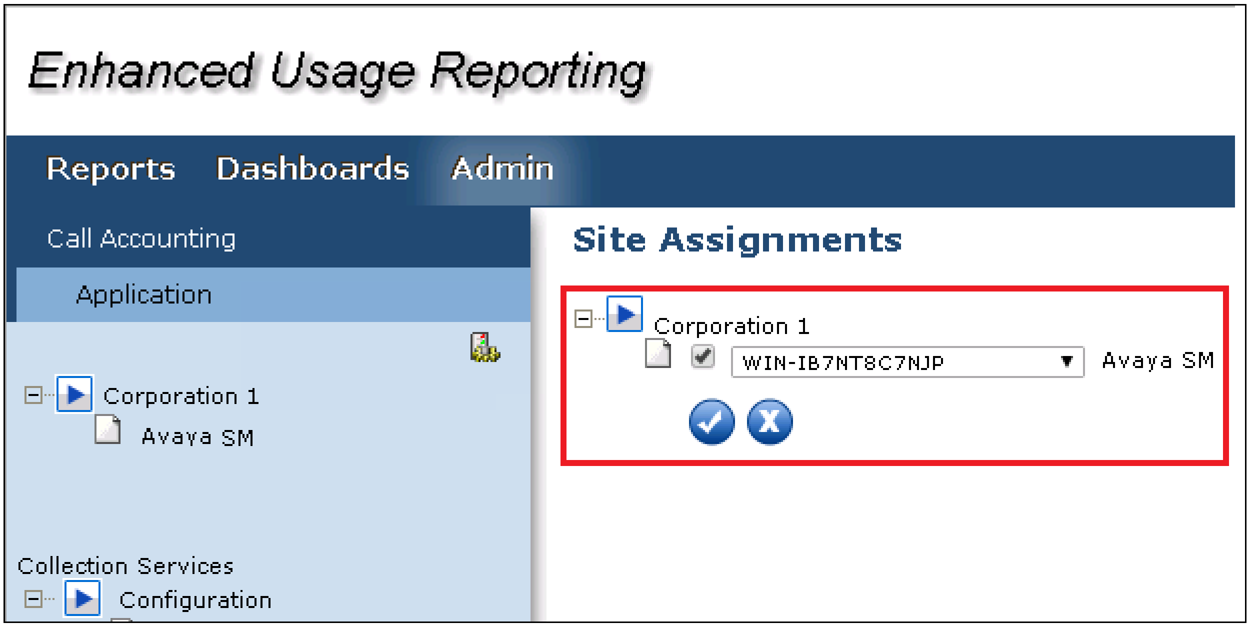
To assign the site created above for collection of data; navigate **to Admin → Call Accounting → Application** as shown in the screen below.



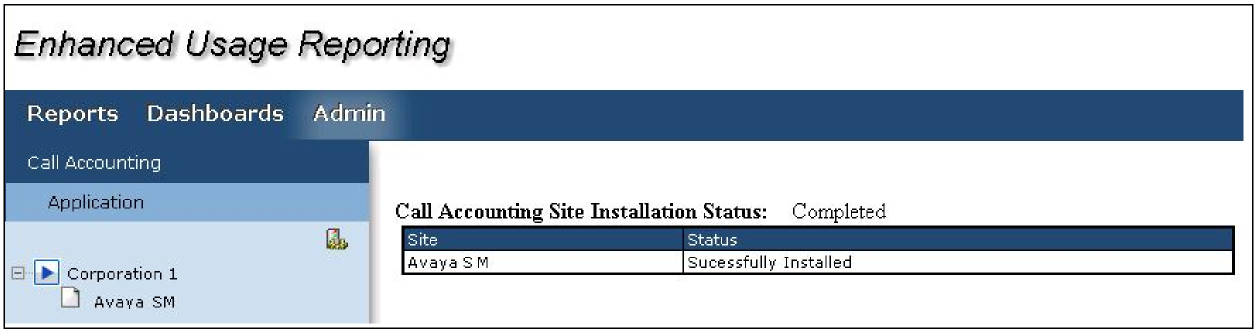
In the **Application** section, start the configuration by clicking on the **Configure** icon as highlighted in the screen below.



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.



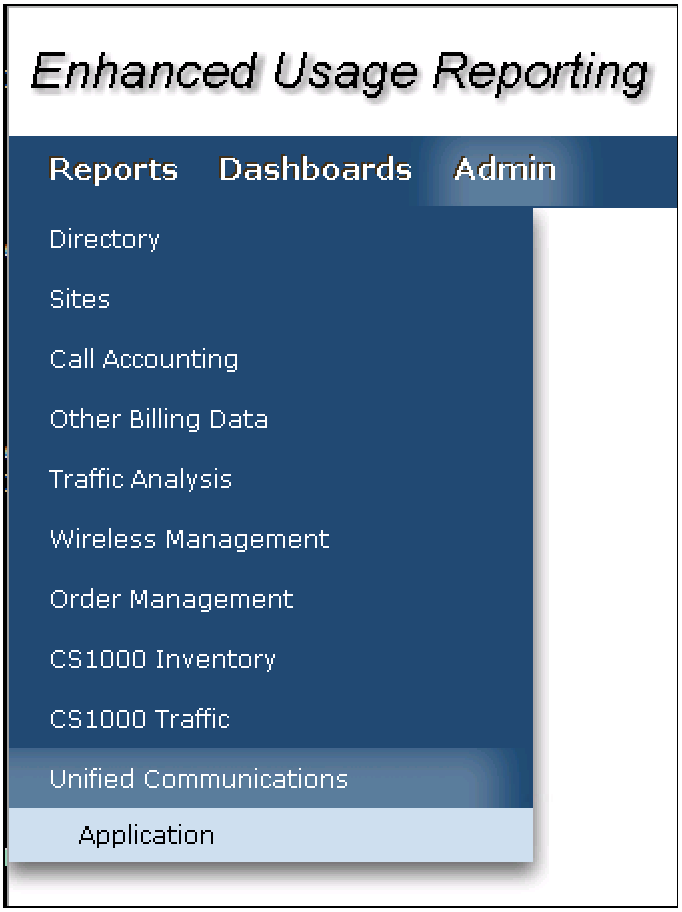
Call Accounting Site Installation Status: Completed

Site	Status
Avaya S M	Sucessfully Installed

7.3. Configure Collection and Service

7.3.1. Configuring Collection

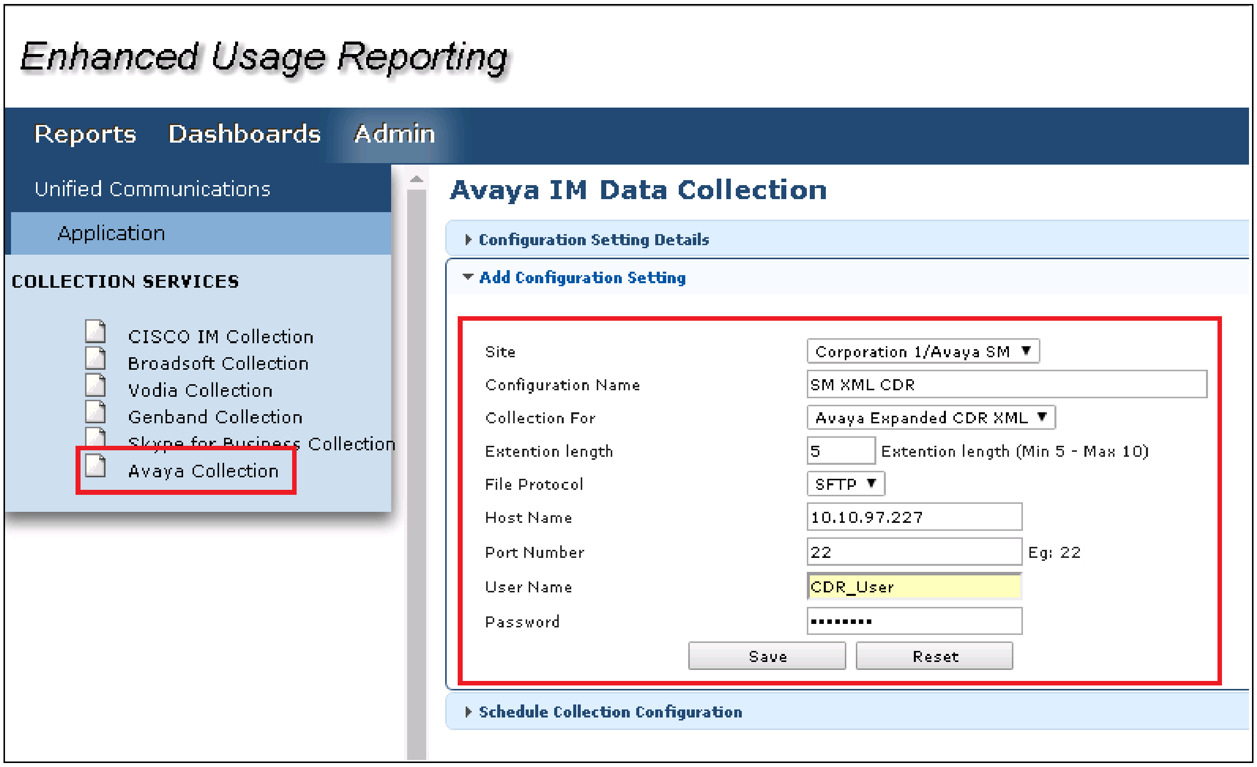
To configure the collection for data, navigate to **Admin → Unified Communications → Application** as shown in the screen below.



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

- **Site**: Select the site configured in **Section 7.2**.
- **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 were 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 6**.
- **Password**: The password configured in **Section 6** for the CDR user.

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



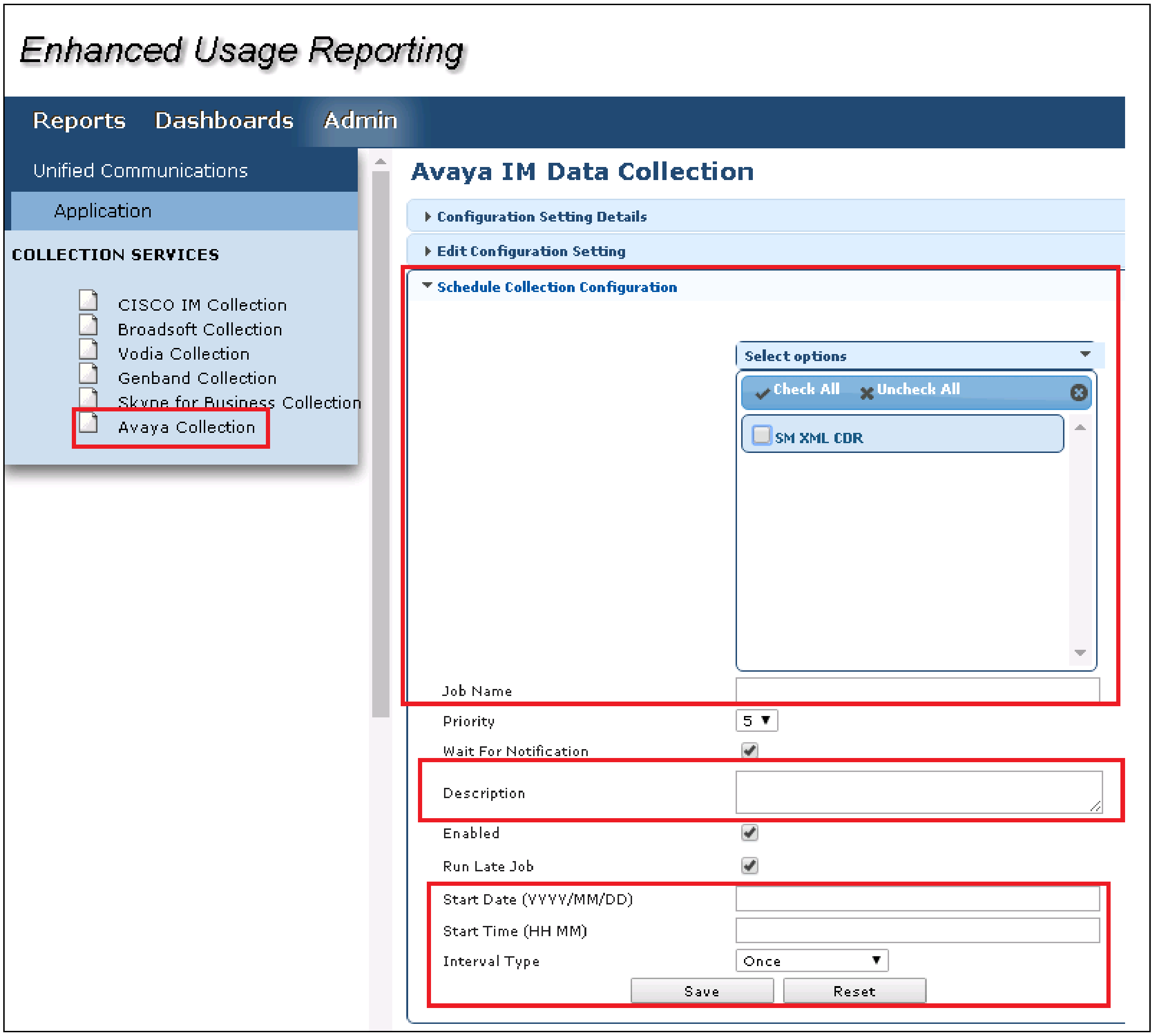
Site	Corporation 1/Avaya SM ▼
Configuration Name	SM XML CDR
Collection For	Avaya Expanded CDR XML ▼
Extention length	5 Extention length (Min 5 - Max 10)
File Protocol	SFTP ▼
Host Name	10.10.97.227
Port Number	22 Eg: 22
User Name	CDR_User
Password	••••••••

7.4. 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,

- **Select Options**:	Select the configuration configured in **Section 7.3**.
- **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.

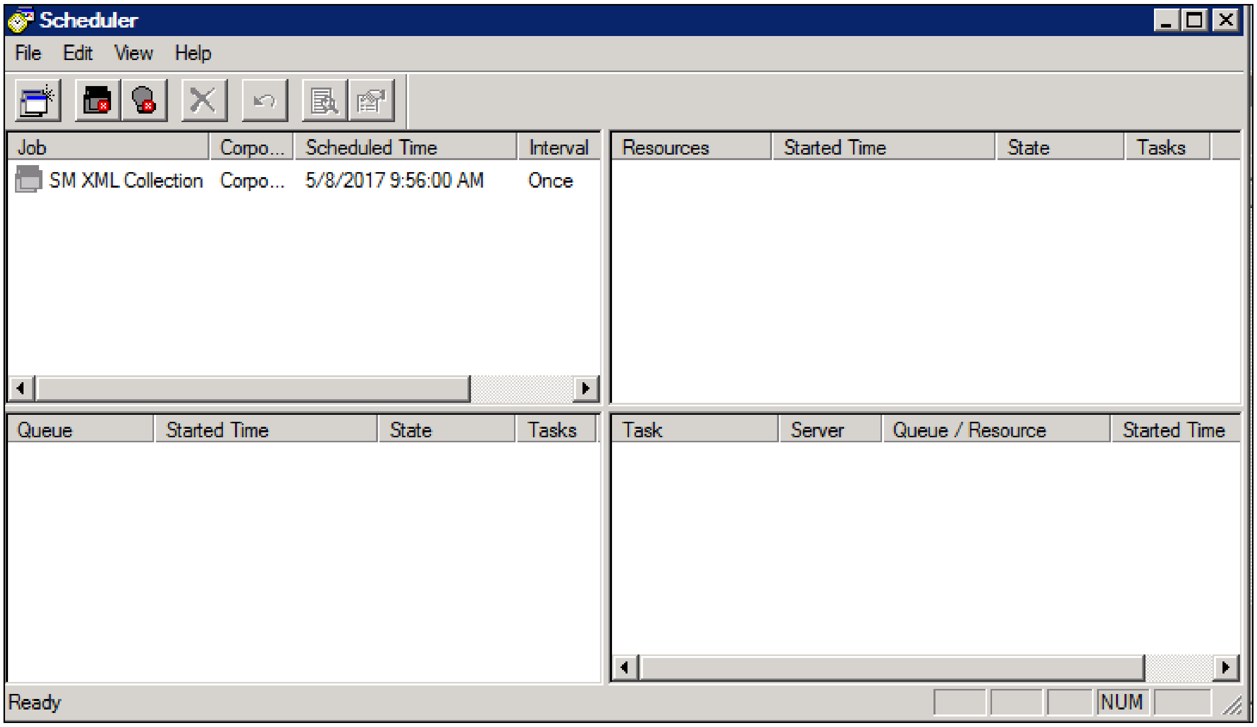
Retain default values for all other fields and click on the **Save** button.



□ SM XML CDR

Job Name	
Priority	5
Wait For Notification	☑
Description	
Enabled	☑
Run Late Job	☑
Start Date (YYYY/MM/DD)	
Start Time (HH MM)	
Interval Type	Once

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



Job	Corpo...	Scheduled Time	Interval
SM XML Collection	Corpo...	5/8/2017 9:56:00 AM	Once

Resources	Started Time	State	Tasks

Queue	Started Time	State	Tasks

Task	Server	Queue / Resource	Started Time

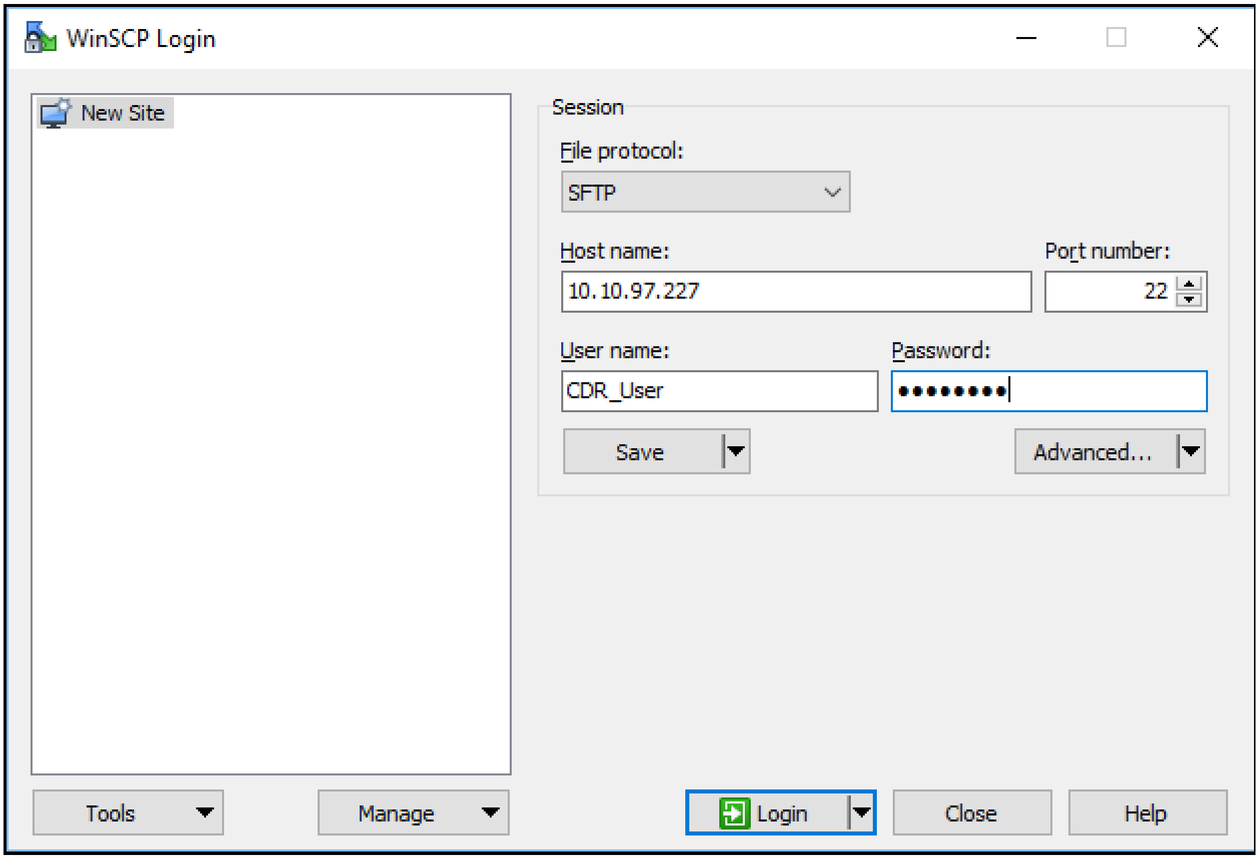
The collected raw CDR data can be found in the "Avaya_XML_Collection_Backup" folder, which is under the "/Rootdata/<Corporation number>/<Site number>" folder.

8. Verification Steps

The following steps may be used to verify the configuration.

8.1. CDR information is being collected by Avaya Aura® Session Manager

Use a secure FTP application, e.g., WinSCP to connect to Session Manager by using the CDR_User and password to access the special folder that store the CDR files.



File protocol: SFTP

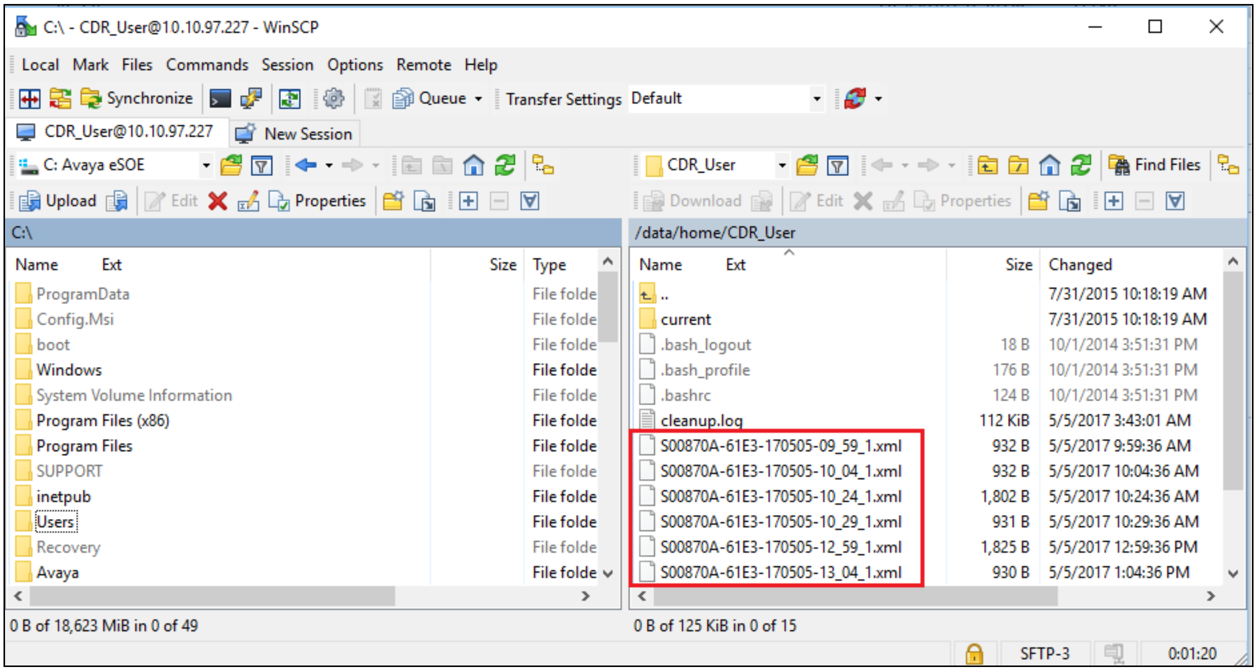
Host name: 10.10.97.227

Port number: 22

User name: CDR_User

Password: •••••••••

Place some different kinds of call; wait a few minutes for Session Manager to generate the CDR files. There should be a list of files present as shown below.



C:\

Name	Ext	Size	Type
ProgramData			File folde
Config.Msi			File folde
boot			File folde
Windows			File folde
System Volume Information			File folde
Program Files (x86)			File folde
Program Files			File folde
SUPPORT			File folde
inetpub			File folde
Users			File folde
Recovery			File folde
Avaya			File folde

0 B of 18,623 MiB in 0 of 49

/data/home/CDR_User

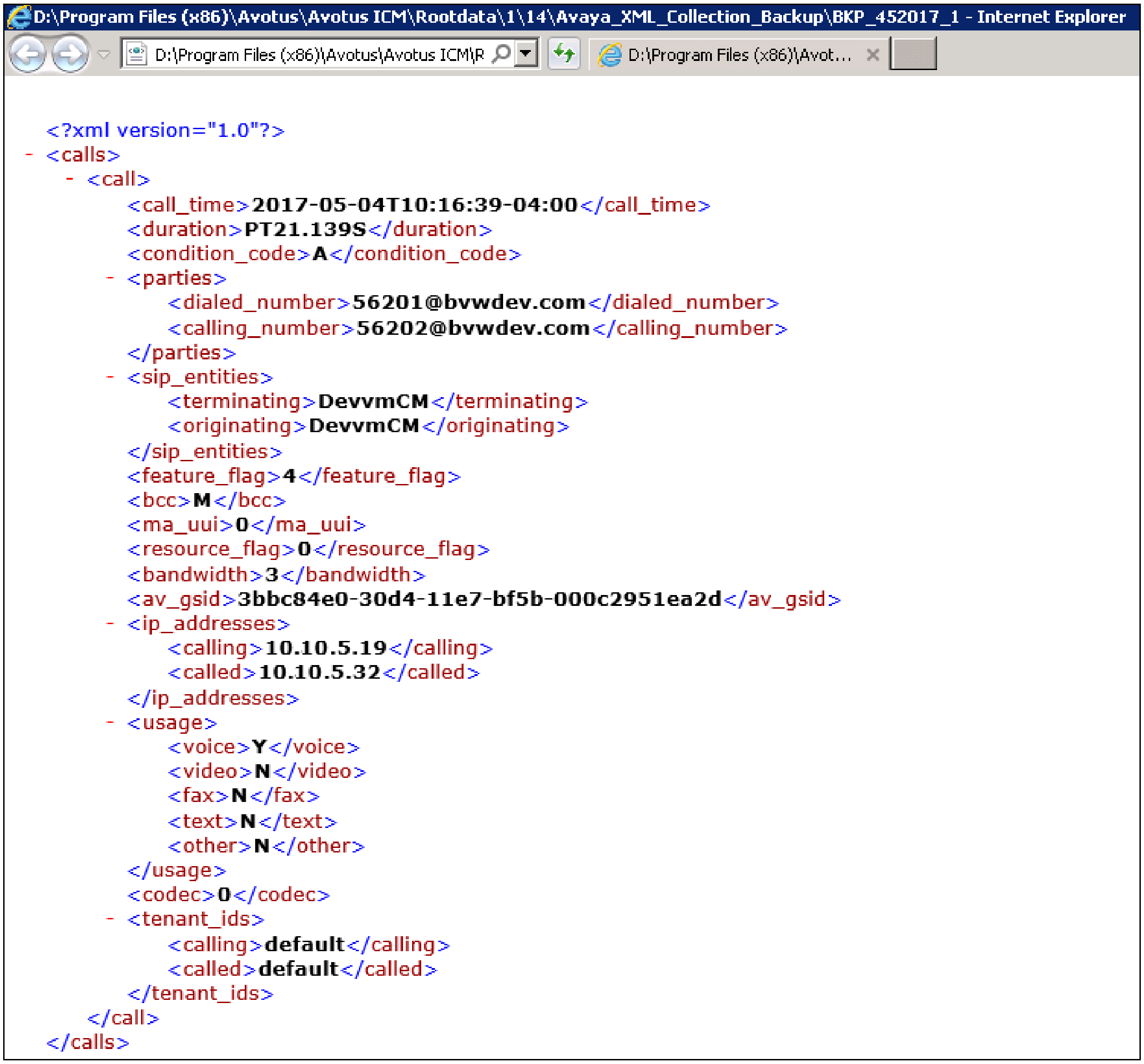
Name	Ext	Size	Changed
..			7/31/2015 10:18:19 AM
current			7/31/2015 10:18:19 AM
.bash_logout		18 B	10/1/2014 3:51:31 PM
.bash_profile		176 B	10/1/2014 3:51:31 PM
.bashrc		124 B	10/1/2014 3:51:31 PM
cleanup.log		112 KiB	5/5/2017 3:43:01 AM
S00870A-61E3-170505-09_59_1.xml		932 B	5/5/2017 9:59:36 AM
S00870A-61E3-170505-10_04_1.xml		932 B	5/5/2017 10:04:36 AM
S00870A-61E3-170505-10_24_1.xml		1,802 B	5/5/2017 10:24:36 AM
S00870A-61E3-170505-10_29_1.xml		931 B	5/5/2017 10:29:36 AM
S00870A-61E3-170505-12_59_1.xml		1,825 B	5/5/2017 12:59:36 PM
S00870A-61E3-170505-13_04_1.xml		930 B	5/5/2017 1:04:36 PM

0 B of 125 KiB in 0 of 15

SFTP-3 0:01:20

8.2. CDR Information Collected by Avotus Enhanced Usage Reporting for Unified Communications

Place internal, inbound trunk and outbound trunk calls to and from various telephones (SIP and H.323) 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 Session Manager XML file.


D:\Program Files (x86)\Avotus\Avotus ICM\Rootdata\1\14\Avaya_XML_Collection_Backup\BKP_452017_1 - Internet Explorer
D:\Program Files (x86)\Avotus\Avotus ICM\R
D:\Program Files (x86)\Avot...

```
  <?xml version="1.0"?>
- <calls>
  - <call>
      <call_time>2017-05-04T10:16:39-04:00</call_time>
      <duration>PT21.139S</duration>
      <condition_code>A</condition_code>
    - <parties>
        <dialed_number>56201@bvwdev.com</dialed_number>
        <calling_number>56202@bvwdev.com</calling_number>
      </parties>
    - <sip_entities>
        <terminating>DevvmCM</terminating>
        <originating>DevvmCM</originating>
      </sip_entities>
      <feature_flag>4</feature_flag>
      <bcc>M</bcc>
      <ma_uui>0</ma_uui>
      <resource_flag>0</resource_flag>
      <bandwidth>3</bandwidth>
      <av_gsid>3bbc84e0-30d4-11e7-bf5b-000c2951ea2d</av_gsid>
    - <ip_addresses>
        <calling>10.10.5.19</calling>
        <called>10.10.5.32</called>
      </ip_addresses>
    - <usage>
        <voice>Y</voice>
        <video>N</video>
        <fax>N</fax>
        <text>N</text>
        <other>N</other>
      </usage>
      <codec>0</codec>
    - <tenant_ids>
        <calling>default</calling>
        <called>default</called>
      </tenant_ids>
    </call>
  </calls>
```

9. 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 2.1** were passed with the observations pointed in **Section 2.2**.

10. Additional References

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

Product documentation for Avaya products may be found at http://support.avaya.com.

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,
http://avotus.com/telecom-enhanced-usage-reporting.asp

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.