Avaya Solution & Interoperability Test Lab

Application Notes for Configuring ISI Telemanagement Solutions Infortel Select with Avaya Aura® Communication Manager and Avaya Aura® Session Manager – Issue 1.0

Abstract

These Application Notes describe the configuration procedures required to allow ISI Telemanagement Solutions Infortel Select to collect call detail records from Avaya Aura® Session Manager.

During the compliance test, ISI Telemanagement Solutions Infortel Select 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 ISI Telemanagement Solutions Infortel Select (referred to as ISI Infortel Select in the ensuing text of this document).

ISI Infortel Select 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, ISI Infortel Select connects to Session Manager, using SFTP, 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. ISI Infortel Select will SFTP to Session Manager to retrieve these call records using credentials configured prior to the compliance test.

2. General Test Approach and Test Results

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

2.1. Interoperability Compliance Testing

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

2.2. Test Results

All executed test cases passed. ISI Infortel Select successfully collected the CDR records from Session Manager via a SFTP connection for all types of SIP calls (intra switch/ inbound/outbound) between two Communication Manager systems. For serviceability testing, ISI Infortel Select was able to resume collection of CDR records after failure recovery.

2.3. Support

Technical support for the ISI Infortel Select solution can be obtained by contacting ISI Telemanagement Solutions:

- http://www.isi-info.com/support/support.htm
- (800) 326-6183

3. 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 Communication Manager running on a S8300D Server with a G450 Media Gateway and the other from Communication Manager running on a S8720 Server with a G650 Media Gateway.

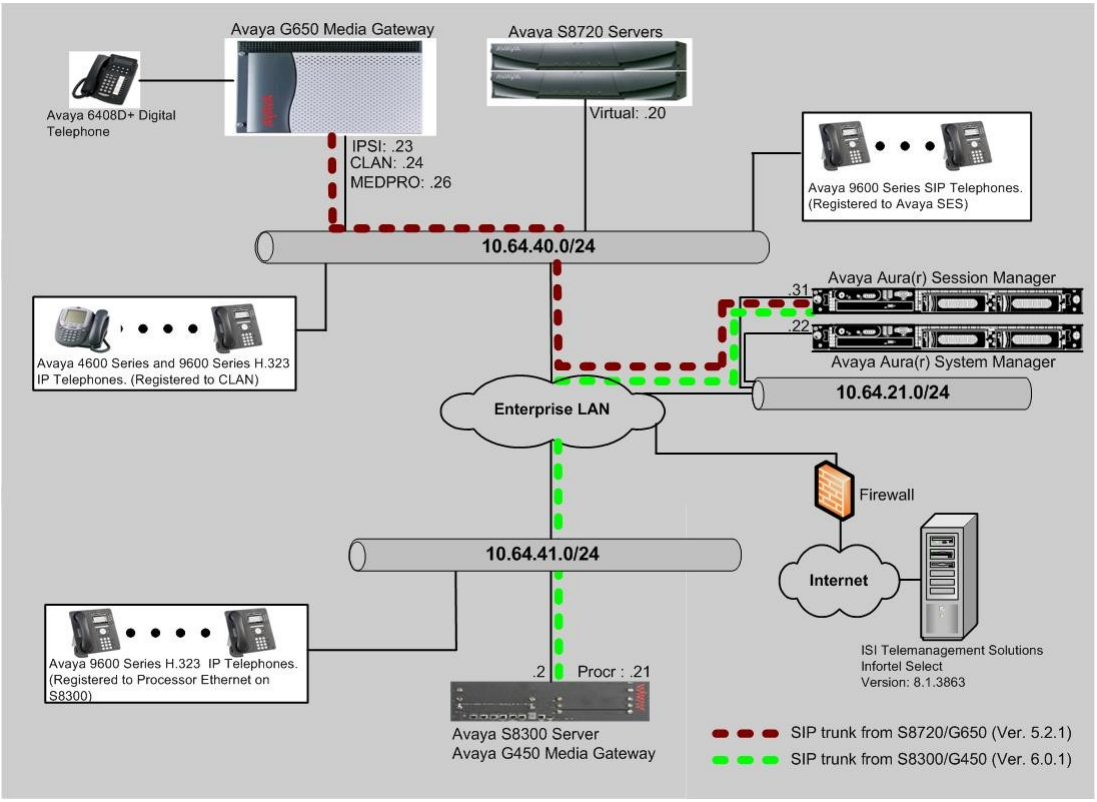


Figure 1: Test configuration for Infortel Select Compliance Test with Session Manager

4. 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 6.0.1 (R016x.00.1.510.1)
Avaya Aura® System Manager		Avaya Aura® System Manager 6.1 (6.1.5.0)
Avaya Aura® Session Manager		Avaya Aura® Session Manager 6.1 (6.1.0.0.610023)
Avaya S8720 Servers with Avaya G650 Media Gateway		Avaya Aura® Communication Manager 5.2.1 (R015x.02.1.016.4)
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 9600 Series IP SIP Telephones		
	9620 (SIP) 9630 (SIP)	2.6.4 2.6.4
Avaya C363T-PWR Converged Stackable Switch		4.5.14
Extreme Networks Summit 48		4.1.21
ISI Telemanagement Solutions Infortel Select on Windows XP Professional Version 2002 with Service Pack 3		8.1.3863

5. Configure Avaya Aura® Communication Manager

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

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 S8300D Server, the SIP trunk terminates at the IP address of the local Ethernet Processor (with node-name “procr”). For the Avaya S8720 Server, the SIP trunk terminates at the IP address of the CLAN board.

Use the **change node-names ip** command to create a new node name, for example, **SM-2**. SM-2 and procr IP addresses will be used in the next step for configuration of the signaling group.

```
change node-names ip                                          Page   1 of   2
                                   IP NODE NAMES
    Name                IP Address
CLAN                  10.64.40.24
SM-1                  10.64.40.42
SM-2                  10.64.21.31
default               0.0.0.0
procr                 10.64.41.21
```

Enter the **add signaling-group <s>** command, where <*s*> is an available signaling group number 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-2**, 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** (default), since Media Shuffling was 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-2
 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:SIP trk to SM              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
```

6. Configure Avaya Aura® Session Manager

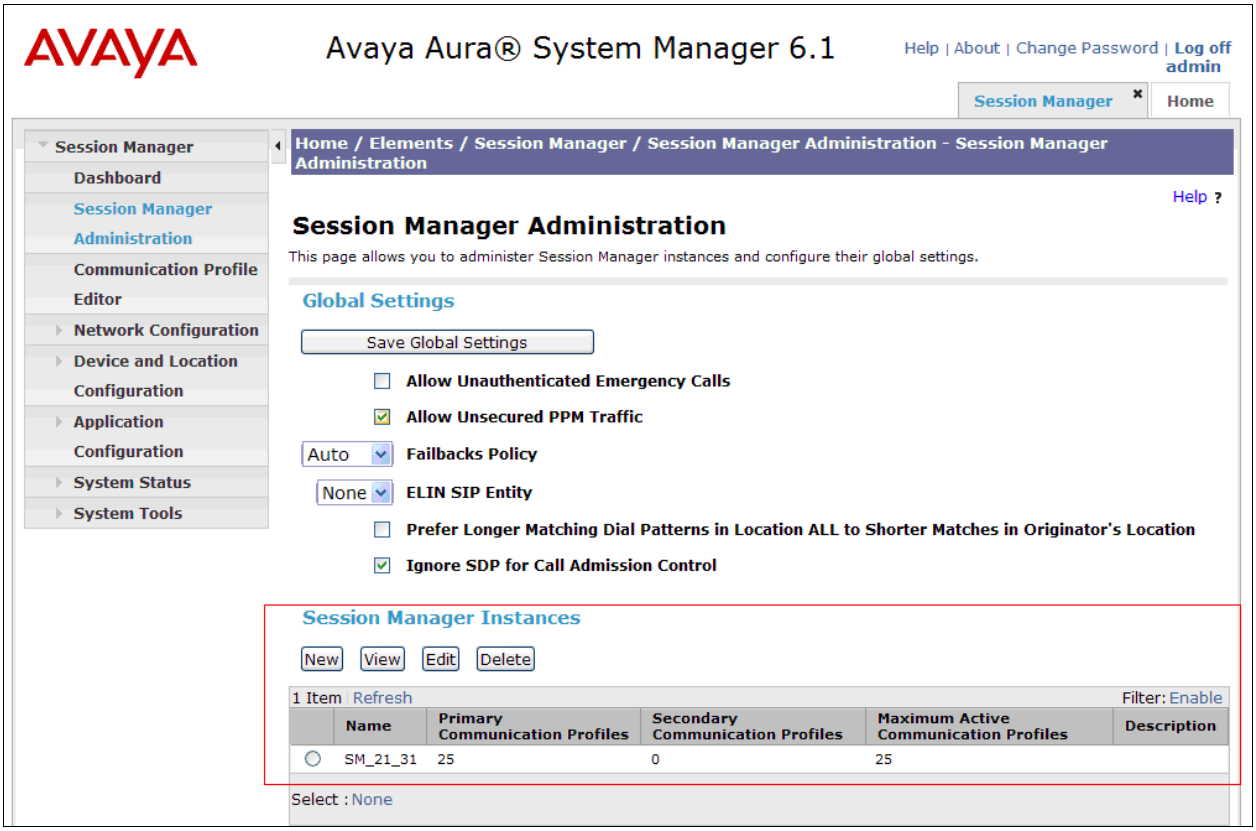
This section assumes that initial configuration on Session Manager has been performed, and Routing and Session Manager Instance are administered properly. This section will only discuss enabling the CDR configuration. During the compliance test, the CDR data will be collected and stored in the hard disk drive of Session Manager. All calls that pass through this trunk will have their associated call data stored. 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

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:

- Communication Manager (Procr in the S8300D/G450)
- Communication Manager (CLAN in the S8720/G650)

Every SIP entity, that collects CDR data, has to be enabled and specified which direction of calls (ingress/egress/both/none) will be stored.

Navigate to **Routing → SIP Entities**, and click on the **New** button (not shown) to create a new SIP entity. Provide the following information:

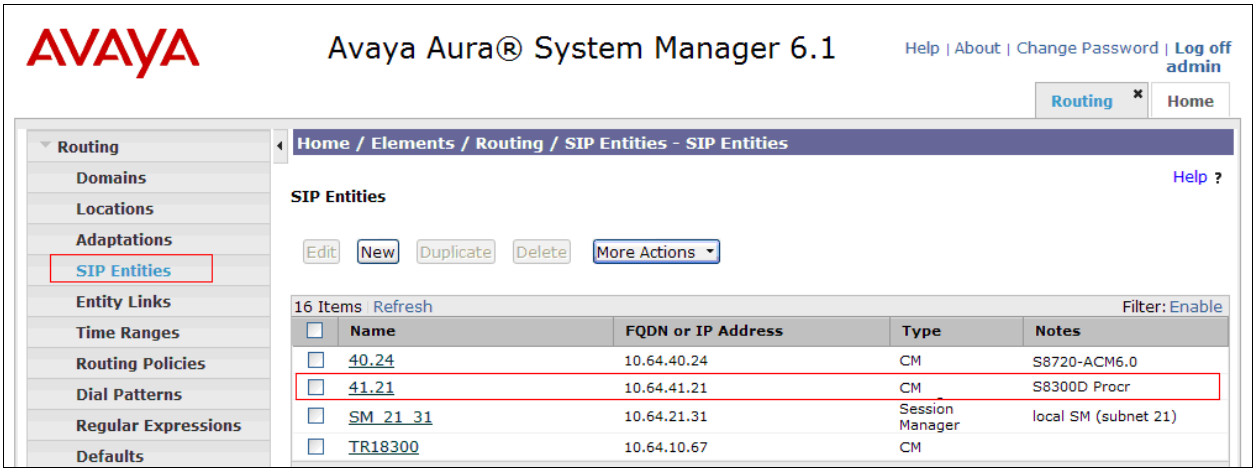
General

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

a. Select the desired option.

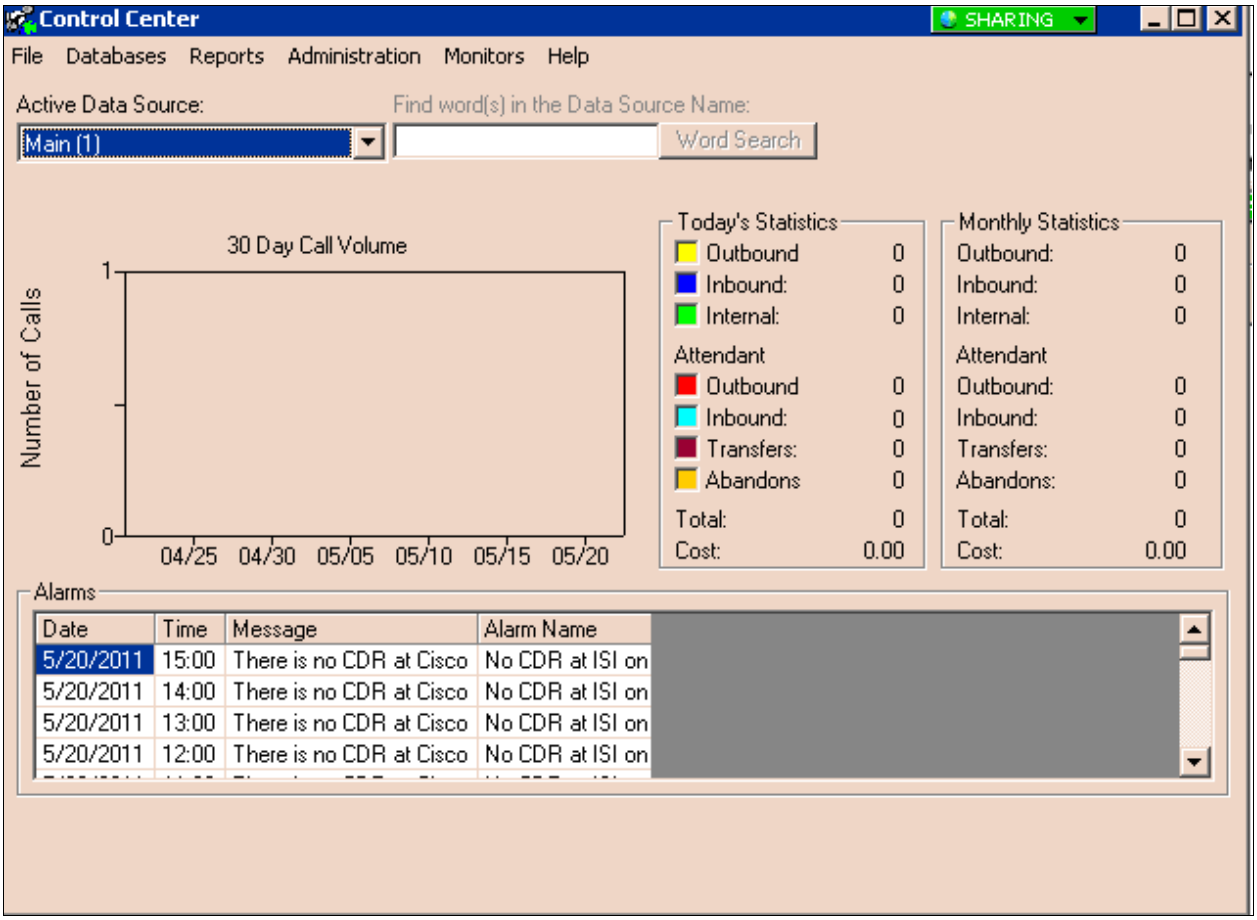
The following screen shows the SIP Entities page that lists the SIP Entities configured for the compliance test.



7. Configure ISI Telemanagement Solutions Infortel Select

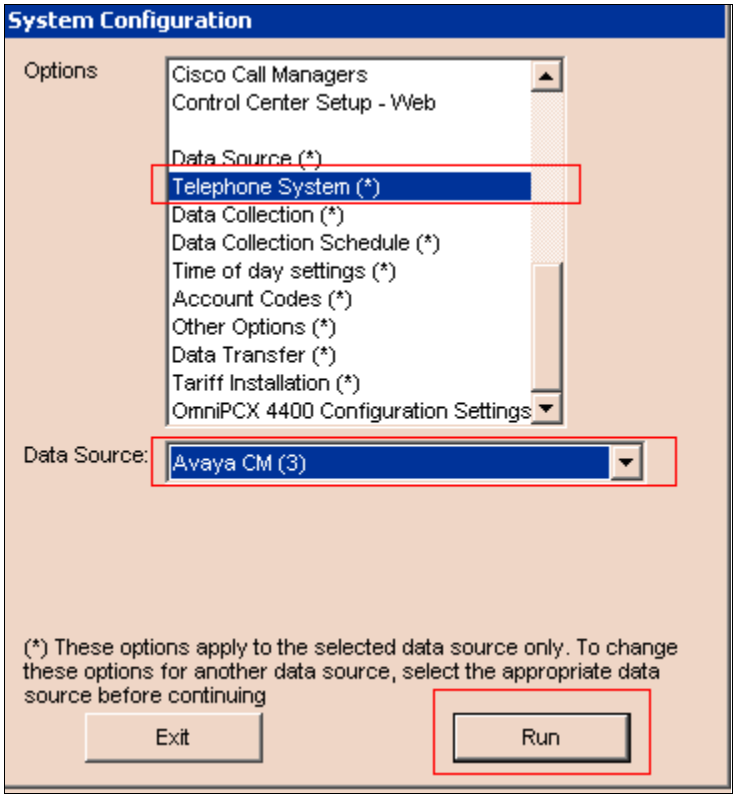
This section describes the configuration of ISI Infortel Select. ISI installs, configures, and customizes the Infortel Select application for the end customers. Thus, this section only describes the interface configuration so that ISI Infortel Select can collect CDR data using SFTP from Session Manager.

Navigate to **Start** ➔ **Programs** ➔**Infortel Select** to launch the **Control Center** application. From Control Center, select **Administration** ➔ **System Configuration Option**.

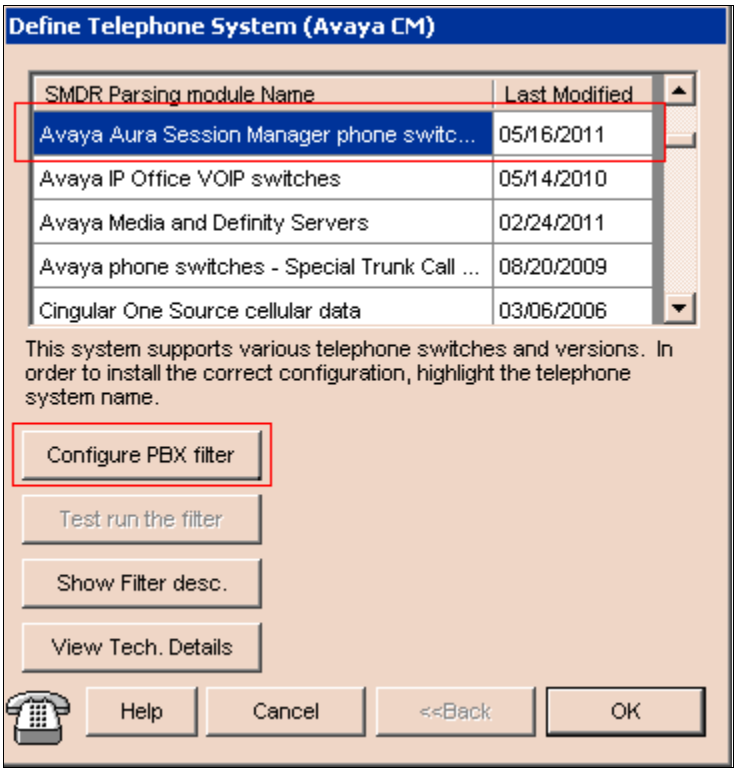


From the System Configuration window, select **Telephone System(*).** In the **Data Source** field select your applicable Data Source from the drop down list. During the compliance test, **Avaya CM(3)** was utilized as the Data Source.

Click on the **Run** button.



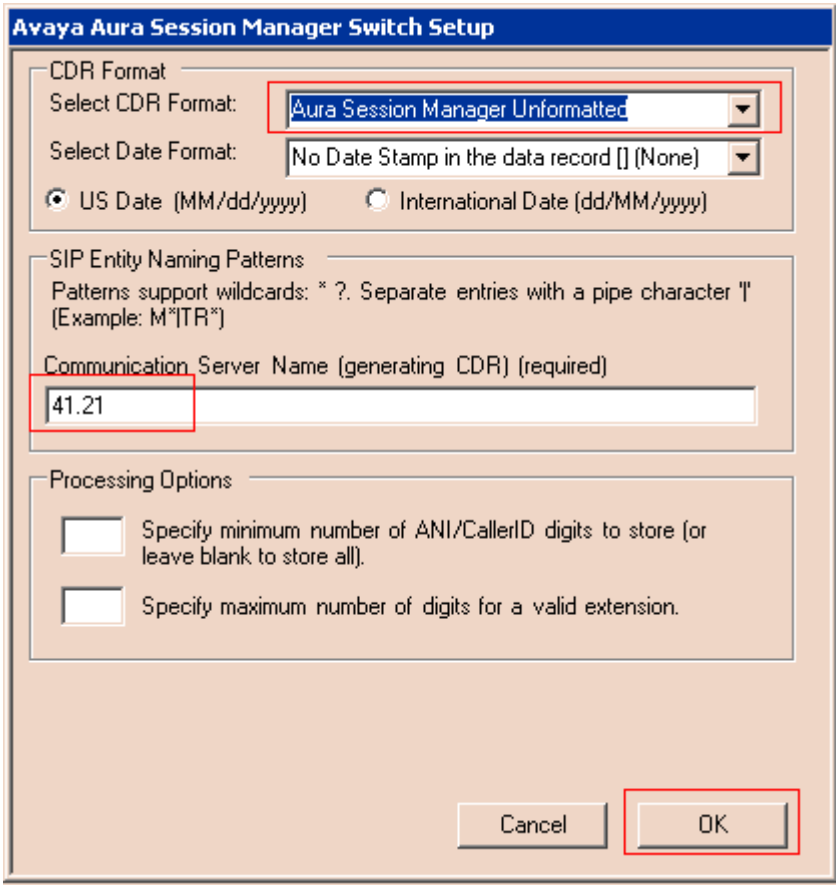
From the **Define Telephone System** window, select **Avaya Aura Session Manager phone switch**. To set the filter in ISI Infortel Select, select the **Configure PBX filter** button.



In the **Avaya Aura Session Manager Switch Setup** window, select **Aura Session Manager Unformatted** from the drop down list. Enter the SIP entity that will be monitored. This entity information will specify whether the call is inbound or out bound whenever the condition code is **9**. During the compliance test, the following methods were utilized:

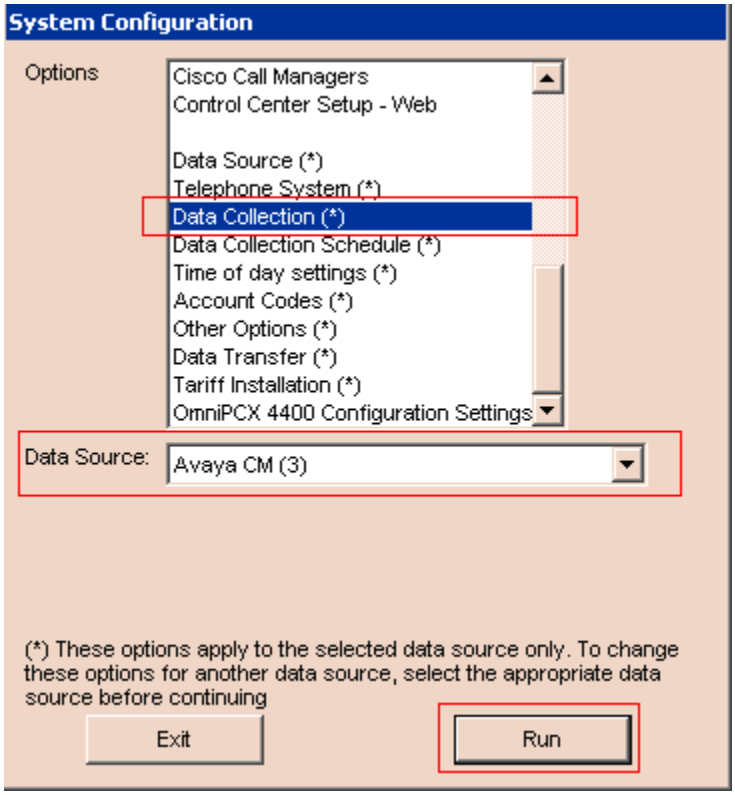
- If Originating and Terminating SIP entities are 41.21, the call is an intra switch call.
- If Originating SIP entity is 41.21 and Terminating SIP entity is other than what is specified in the filter section, the call is outbound.
- If Terminating SIP entity is 41.21 and Originating SIP entity is other than what is specified in the filter section, the call is inbound.

Click the **OK** button.



The following describes the SFTP configuration in ISI Infortel Select. From the System Configuration window, select **Data Collection(*).** In the **Data Source** field, select the applicable Data Source from the drop down list. During the compliance test, **Avaya CM(3)** was utilized as a Data Source.

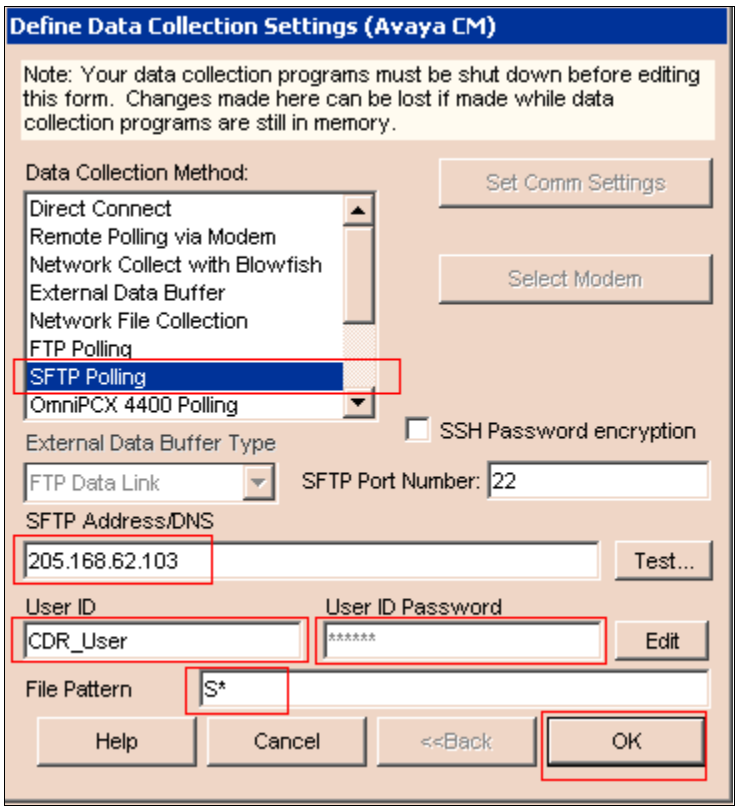
Click on the **Run** button.



From the Define Data Collection Settings window, select **SFTP Polling** as a Data Collection Method and provide the following information:

- **SIP Address/DNS** - Enter the IP address of Session Manager on the field
- **User ID** – Enter the user name created in **Section 6**.
- **User ID Password** – Enter the password created in **Section 6**.
- **File Pattern** – Automatic SFTP script will collect all files that start with **S***.

Click on the **OK** button.



8. Verification Steps

The following steps may be used to verify the configuration:

- Enter the **status trunk** command and verify that the SIP trunk state is **in-service/idle**.
- Place a call that is routed over the SIP trunk to Session Manager.
- Verify the CDR raw data that is stored in the /var/home/ftp/CDR directory on Session Manager.

9. Conclusion

These Application Notes describe the procedures for configuring ISI Infortel Select to collect call detail records from Session Manager. ISI Infortel Select passed the compliance test.

10. Additional References

[1] *Avaya Aura® Session Manager Call Detail Recording Interface,* Issue 1.1, 28 March 2011

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.