Avaya Solution & Interoperability Test Lab

Application Notes for Configuring ISI Telemanagement Solutions Infortel Select with Avaya Aura® Communication 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® Communication Manager using Avaya Reliable Session Protocol over TCP/IP. ISI Telemanagement Solutions 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 and ISI Telemanagement Solutions Infortel Select (herein referred to as ISI Infortel Select). ISI Infortel Select Solutions 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.

Avaya Aura® Communication Manager communicates to ISI Infortel Select via an Avaya Reliable Session Protocol (RSP) session over the TCP/IP network. The RSP session provides a transport mechanism for reliable delivery of CDR records. Avaya Aura ® Communication Manager generates and sends the call records out in the RSP session while ISI Infortel Select collects, stores and processes the records at the other end.

Avaya Aura® Communication Manager can generate call detail records for intra-switch calls, inbound trunk calls and outbound trunk calls. In addition, split records can be generated for transferred calls and conference calls. ISI Infortel Select can support any CDR format provided by Avaya Aura® Communication Manager. However, during the compliance test, the unformatted format was utilized.

2. General Test Approach and Test Results

The general test approach was to manually place intra-switch calls, inbound trunk and outbound trunk calls, to and from telephones attached to the Avaya Servers, and verify that ISI Infortel Select collects the CDR records and properly classifies and reports the attributes of each call.

For serviceability testing, physical and logical links were disabled/re-enabled, Avaya Servers were reset, and ISI Infortel Select was restarted. The LSP test was performed from ISI Infortel Select using the SFTP command to the Avaya S8300D Server (LSP), and collecting the CDR records.

All executed test cases passed. ISI Infortel Select successfully collected the CDR records from Avaya Aura® Communication Manager via an RSP connection for all types of calls generated, including, intra-switch calls, inbound/outbound PSTN trunk calls, inbound/outbound private IP trunk calls, transferred calls, and conference calls.

For serviceability testing, ISI Infortel Select was able to resume collecting CDR records after failure recovery, including buffered CDR records for calls that were placed during the outages. ISI Infortel Select also successfully collected the CDR records from the Avaya S8300D Server (LSP) using the SFTP command.

2.1. Interoperability Compliance Testing

The interoperability compliance testing included features and serviceability tests. The focus of the compliance testing was primarily on verifying the interoperability between ISI Infortel Select and Communication Manager.

2.2. Test Results

The test objectives were verified. ISI Infortel Select successfully collected the CDR records from Communication Manager via an RSP connection for all types of calls generated, including, intra-switch calls, inbound/outbound PSTN trunk calls, inbound/outbound private IP trunk calls, transferred calls, and conference calls

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 configuration consists of three Avaya Servers running Avaya Aura® Communication Manager. Site A is comprised of Avaya Aura® Communication Manager running on an Avaya S8300D Server with an Avaya G450 Media Gateway.

Site B is included to provide the trunk-to-trunk test scenario, and is comprised of Avaya Aura® Communication Manager running on two Avaya S8720 Servers (duplex fail-over configuration) and an Avaya G650 Media Gateway.

Both Avaya Aura® Communication Managers are connected to an IP network comprised of an Extreme Networks Summit 48 layer 3 switch.

ISI Infortel Select, running on a Windows XP Professional system, is connected to the IP network through a firewall and has an RSP session established to Avaya Aura® Communication Manager to collect CDR records.

Each system has trunks and phones associated with it to generate calls. Avaya 4625 IP Telephones, Avaya 9600 Series IP Telephones, and Avaya 6400D Series Digital Telephones are registered to both Avaya S8700 and S8300D Servers. In addition, there is an H.323 IP trunk established between the two media servers.

Site C is comprised of an Avaya S8300D Server with an Avaya G430 Media Gateway, which has connections to an Avaya 9600 Series IP Telephone and an Avaya 6400D Series Digital Telephone. The Avaya S8300D Server with G430 gateway in Site C, installed with Local Survivable Processor (LSP) license, is set up as a LSP to Site A.

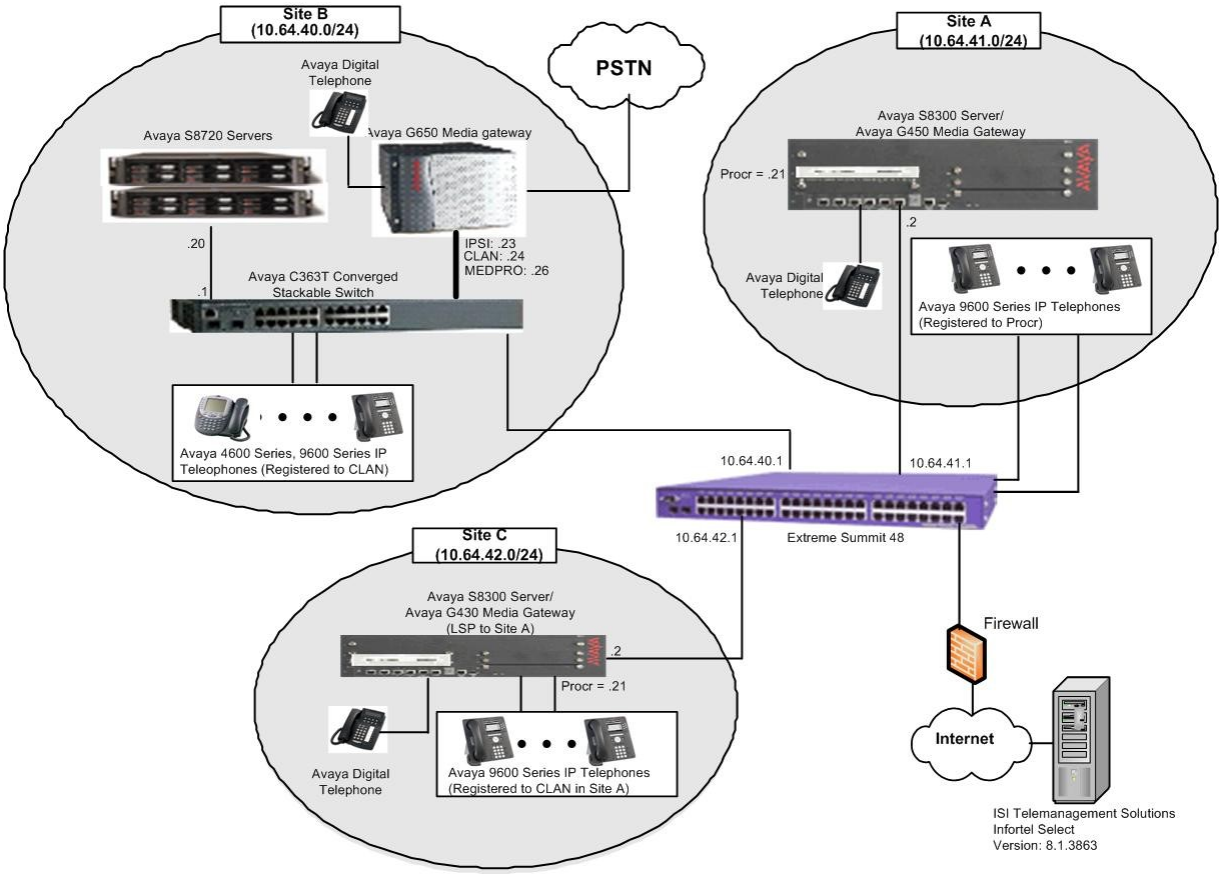


Figure 1: Test configuration for ISI Infortel Select Compliance Test

4. Equipment and Software Validated

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

Equipment		Software/Firmware
Avaya S8300D Server with Avaya G450 Media Gateway		Avaya Aura® Communication Manager 6.0.1 (R016x.00.1.510.1)
Avaya S8300D Server with Avaya G430 Media Gateway (with LSP license)		Avaya Aura® Communication Manager 6.0.1 (R016x.00.1.510.1)
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 6400D Series Digital Telephones		-
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 call detail recording (CDR) in Avaya Aura® Communication 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. Avaya Aura® Communication Manager will be configured to generate CDR records using RSP over TCP/IP to the IP address of the PC running ISI Infortel Select. For the Avaya S8300D Server, the RSP link originates at the IP address of the local processor (with node-name "procr").

Use the **change node-names ip** command to create a new node name, for example, **ISI**. This node name is associated with the IP Address of the PC running ISI Infortel Select application. Also, take note of the node name "procr". It will be used in the next step. The "procr" entry on this form was previously administered. S8300-lsp is an LSP licensed Avaya S8300D Server.

Note: Since a public IP address was used for ISI Infortel Select during the compliance test, the IP address will not be shown.

```
change node-names ip                                              Page   1 of   2
                                   IP NODE NAMES
    Name                IP Address
ISI                    x.x.x.x
default                0.0.0.0
procr                  10.64.41.21
procr6                 ::
rdtt                   10.64.43.10
s8300-lsp              10.64.42.21
```

Use the **change ip-services** command to define the CDR link to use the RSP over TCP/IP. To define a primary CDR link, provide the following information:

- **Service Type**: **CDR1** [If needed, a secondary link can be defined by setting Service Type to CDR2.]
- **Local Node**: **procr** [For the Avaya S8720 Server, set the Local Node to the node name of the CLAN board.]
- **Local Port**: **0** [The Local Port is fixed to 0 because Communication Manager initiates the CDR link.]
- **Remote Node**: **ISI** [The Remote Node is set to the node name previously defined.]
- **Remote Port**: **9000** [The Remote Port may be set to a value between 5000 and 64500 inclusive, and must match the port configured in ISI Infortel Select.]

```
change ip-services                                                Page   1 of   4

                                   IP SERVICES
 Service      Enabled     Local        Local        Remote       Remote
  Type                    Node         Port         Node         Port
AESVCS         y       procr           8765
CDR1                   procr           0        ISI              9000
CDR2                   procr           0        rdtt             9007
```

On **Page 3** enable the Reliable Session Protocol (RSP) for the CDR link by setting the **Reliable Protocol** field to **y**.

```
change ip-services                                                Page   3 of   4

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

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

Enter the **change system-parameters cdr** command from the SAT to set the parameters for the type of calls to track, and the format of the CDR data. The example below shows the settings used during the compliance test. Provide the following information:

- **CDR Date Format**: **month/day**
- **Primary Output Format**: **unformatted**
- **Primary Output Endpoint**: **CDR1**

The remaining parameters define the type of calls that will be recorded and what data will be included in the record. See reference [1] for a full explanation of each field. The test configuration used some of the more common fields described below.

- **Enable CDR Storage on Disk?**: **y** [Enable the Survivable CDR feature. Default is **n**.]
- **Use Legacy CDR Formats?**: **n** [Allows CDR formats to use 4.x CDR formats. If the field is set to **y**, then CDR formats utilize the 3.x CDR formats.]
- **Intra-switch CDR**: **y** [Allows call records for internal calls involving specific stations. Those stations must be specified in the INTRA-SWITCH CDR form.]
- **Record Outgoing Calls Only?**: **n** [Allows incoming trunk calls to appear in the CDR records along with the outgoing trunk calls.]
- **Outg Trk Call Splitting?**: **y** [Allows a separate call record for any portion of an outgoing call that is transferred or conferenced.]
- **Inc Trk Call Splitting?**: **y** [Allows a separate call record for any portion of an incoming call that is transferred or conferenced.]

```
change system-parameters cdr                                      Page   1 of   2
                              CDR SYSTEM PARAMETERS

 Node Number (Local PBX ID): 1                       CDR Date Format: month/day
      Primary Output Format: unformatted   Primary Output Endpoint: CDR1
    Secondary Output Format:
           Use ISDN Layouts? n                     Enable CDR Storage on Disk? y
       Use Enhanced Formats? n      Condition Code 'T' For Redirected Calls? n
      Use Legacy CDR Formats? n                   Remove # From Called Number? n
Modified Circuit ID Display? n                              Intra-switch CDR? y
                  Record Outgoing Calls Only? n     Outg Trk Call Splitting? y
  Suppress CDR for Ineffective Call Attempts? y       Outg Attd Call Record? n
      Disconnect Information in Place of FRL? n      Interworking Feat-flag? n
 Force Entry of Acct Code for Calls Marked on Toll Analysis Form? n
                                    Calls to Hunt Group - Record: member-ext
Record Called Vector Directory Number Instead of Group or Member? n
Record Agent ID on Incoming? y       Record Agent ID on Outgoing? y
     Inc Trk Call Splitting? y                   Inc Attd Call Record? n
  Record Non-Call-Assoc TSC? n            Call Record Handling Option: warning
      Record Call-Assoc TSC? n   Digits to Record for Outgoing Calls: dialed
   Privacy - Digits to Hide: 0               CDR Account Code Length: 6
```

If the Intra-switch CDR field is set to **y** on **Page 1** of the SYSTEM PARAMETERS CDR form, then use the **change intra-switch-cdr** command to define the extensions that will be subject to call detail records. In the Assigned Members field, enter the specific extensions whose usage will be tracked. To simplify the process of adding multiple extensions, the **Intra-switch CDR by COS** feature may be utilized in the SPECIAL APPLICATIONS form under the system-parameters section. To utilize this feature, contact an authorized Avaya account representative to obtain the license.

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

                                Assigned Members:   9    of 1000   administered
   Extension          Extension          Extension          Extension
   72001
   72002
   72003
   72004
   72005
   72007
   72009
   72010
   72011
```

For each trunk group for which CDR records are desired, verify that CDR reporting is enabled. Use the **change trunk-group *n*** command, where ***n*** is the trunk group number, to verify that the CDR Reports field is set to **y**. This applies to all types of trunk groups.

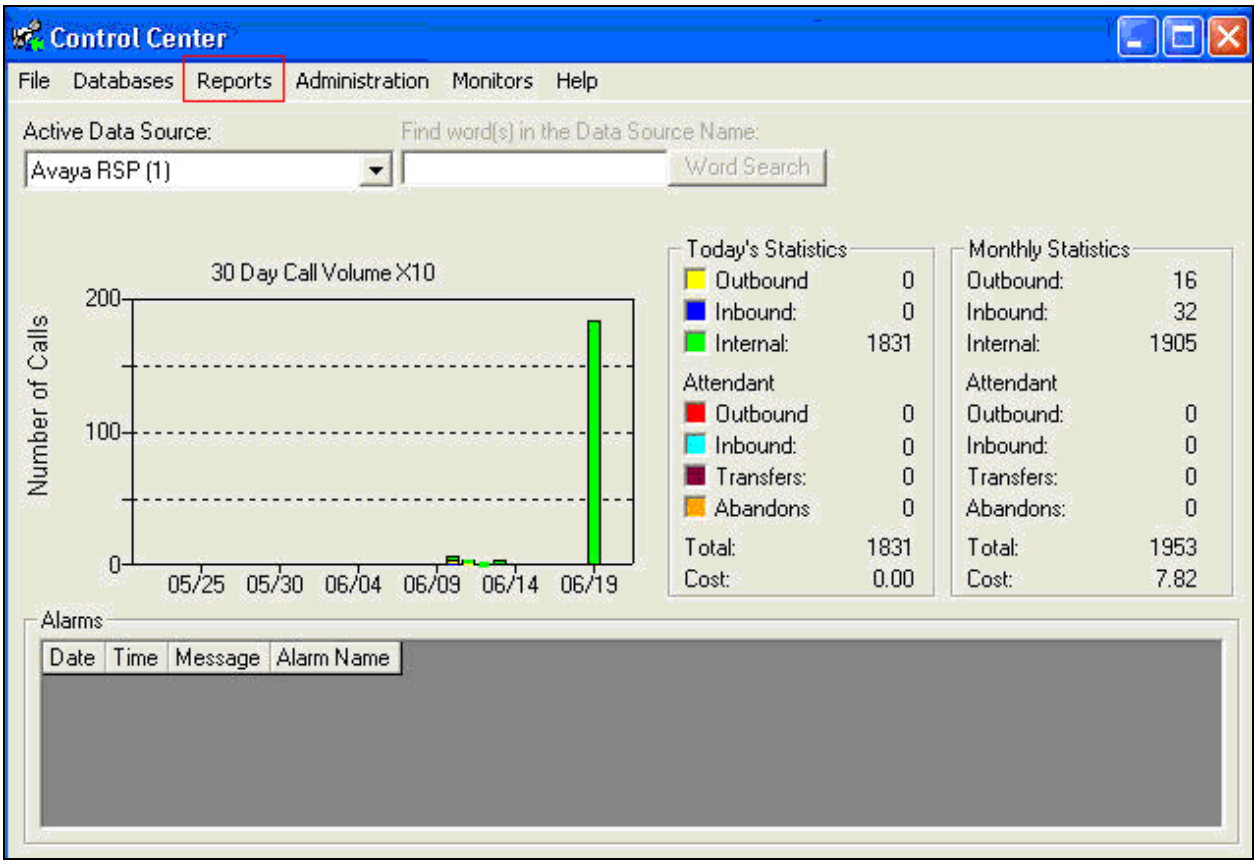
```
change trunk-group 10                                            Page   1 of  21
                                TRUNK GROUP

Group Number: 10                   Group Type: isdn          CDR Reports: y
  Group Name: S8720-IP trunk              COR: 1        TN: 1        TAC: 1010
   Direction: two-way        Outgoing Display? n         Carrier Medium: H.323
 Dial Access? y              Busy Threshold: 255  Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n
                                          Member Assignment Method: auto
                                                   Signaling Group: 10
                                                 Number of Members: 10
```

6. Configure ISI Infortel Select

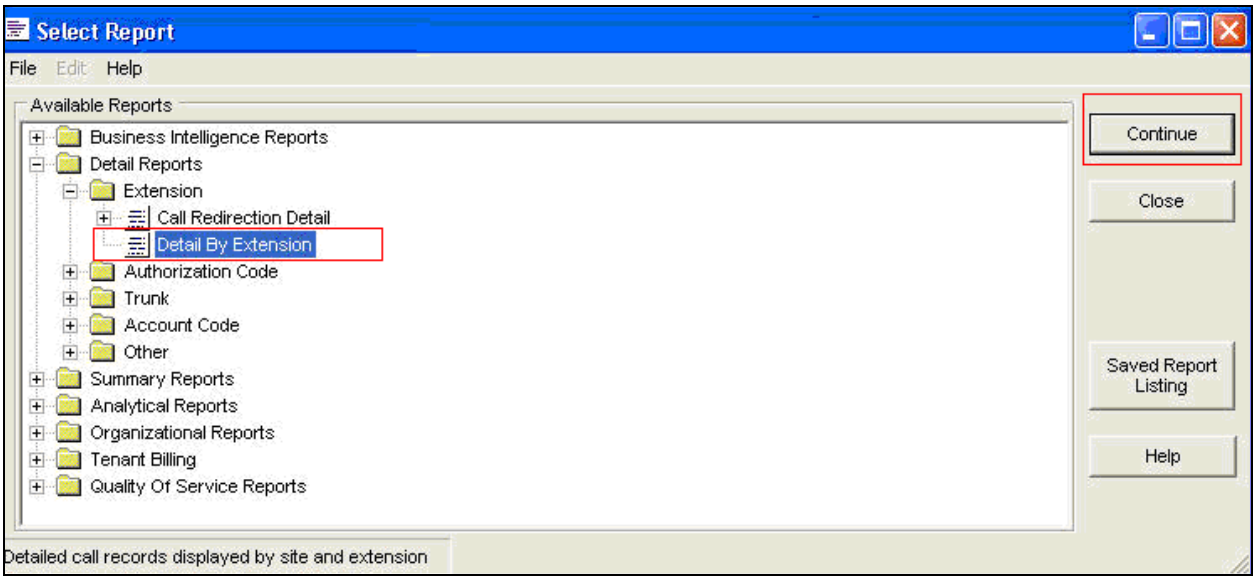
This section describes the configuration of ISI Infortel Select. ISI Telemanagement Solutions installs, configures, and customizes the Infortel Select application for end customers. Thus, this section only describes the interface configuration, so that ISI Infortel Select can receive CDR data from Avaya Aura® Communication Manager.

6.1. Configure CDR Report

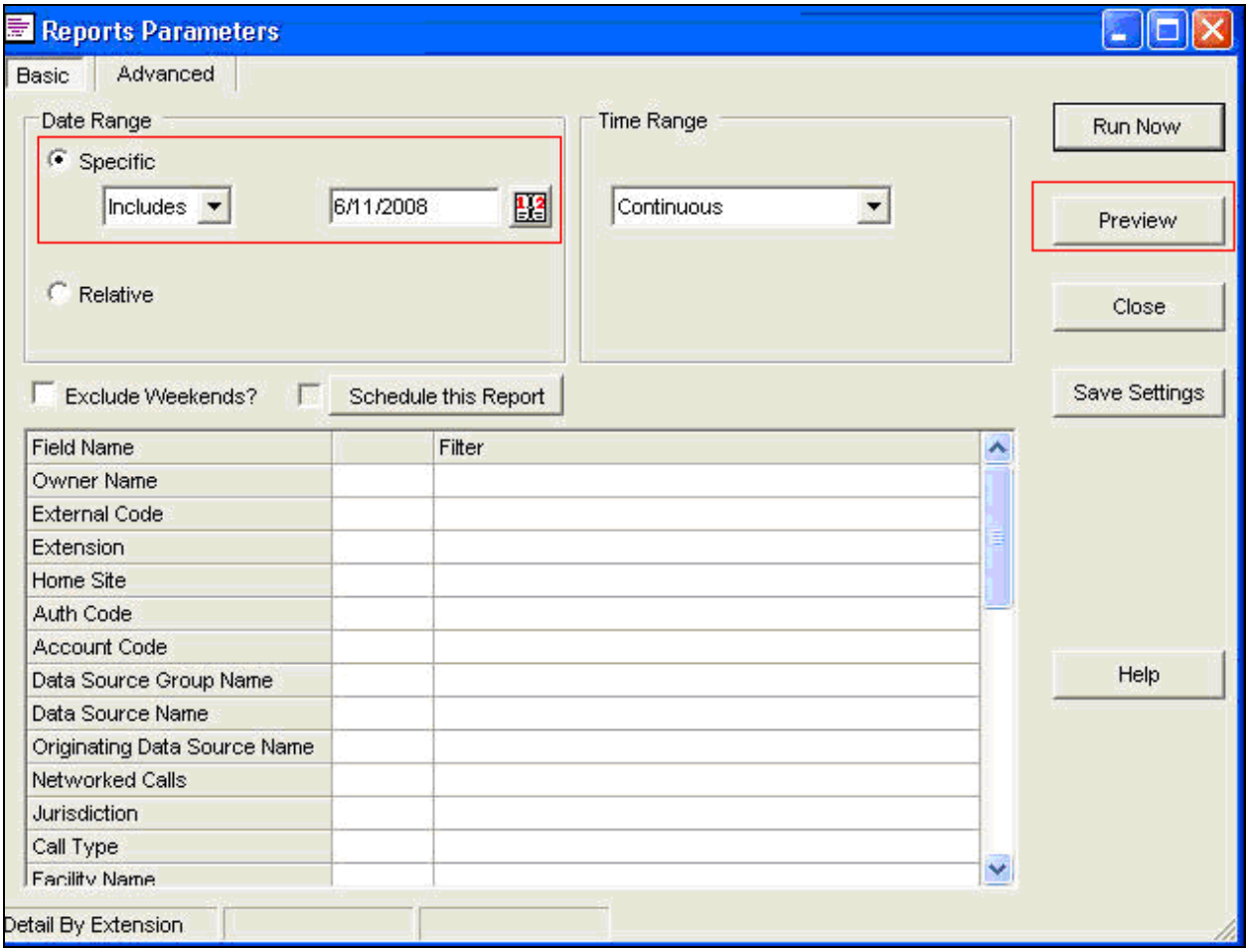
The following section describes the steps for generating the CDR reports. Navigate to **Start → Programs →Infortel Select →Control Center** to access the Control Center page. The following screen shows the Control Center page. From the Control Center page, select **Call Account Reports** (not shown) under the Reports menu.



In the Select Report page, navigate to **Detail Reports → Extension → Detail by Extension.** Click the **Continue** button.

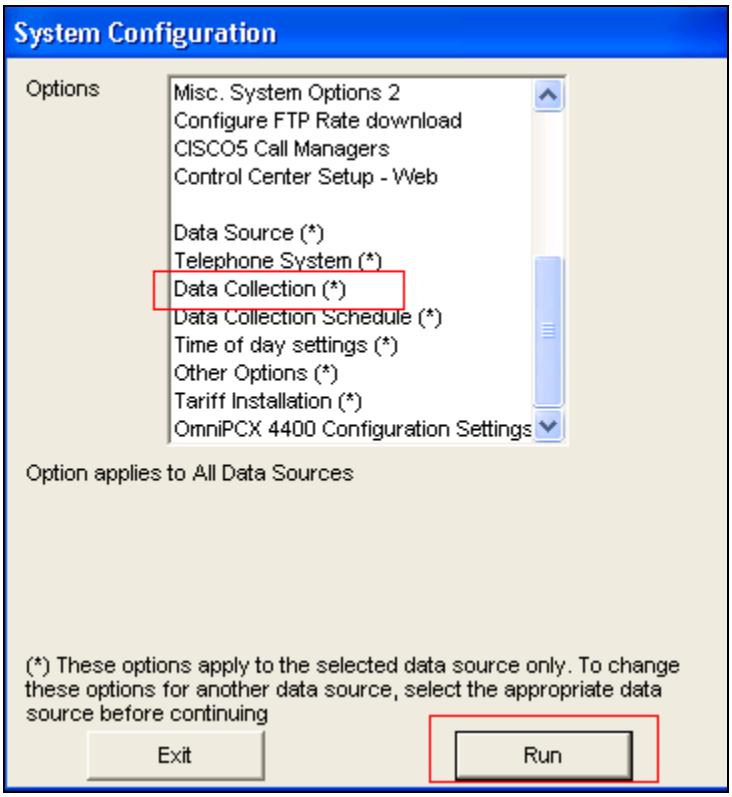


From the Reports Parameters page, click **Specific** in the Date Range section. Choose **Includes** using the drop-down menu, and select the specific date. Once completed, click the **Preview** button to view the report.

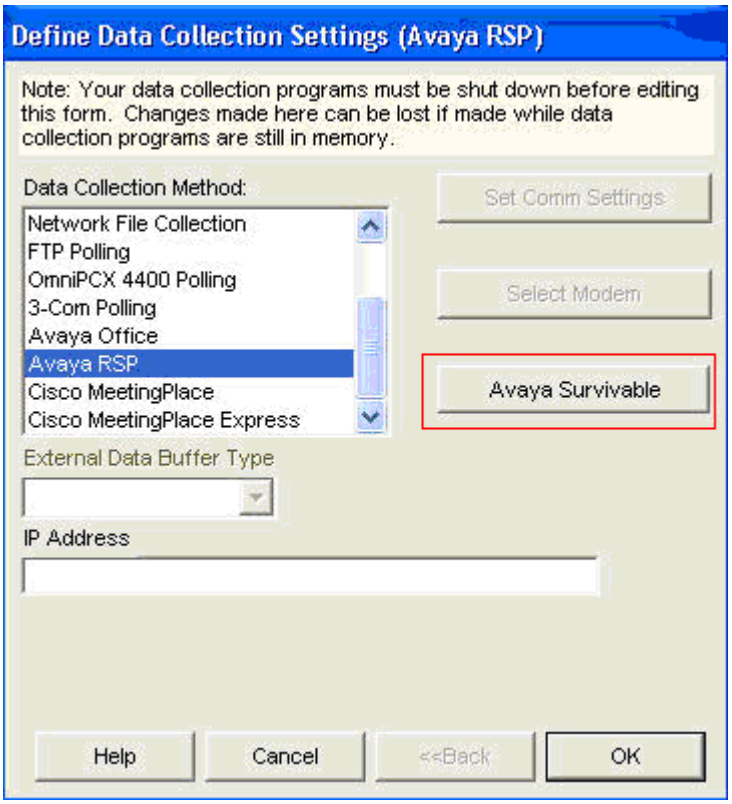


6.2. Configure Survivable LSP Data Collection

The following section describes the steps for data collection settings. Navigate to **Start → Programs →Infortel Select →System Configuration Options** to access the data collection settings page. From the System Configuration page, select **Data Collection (*)**. Click on the **Run** button.



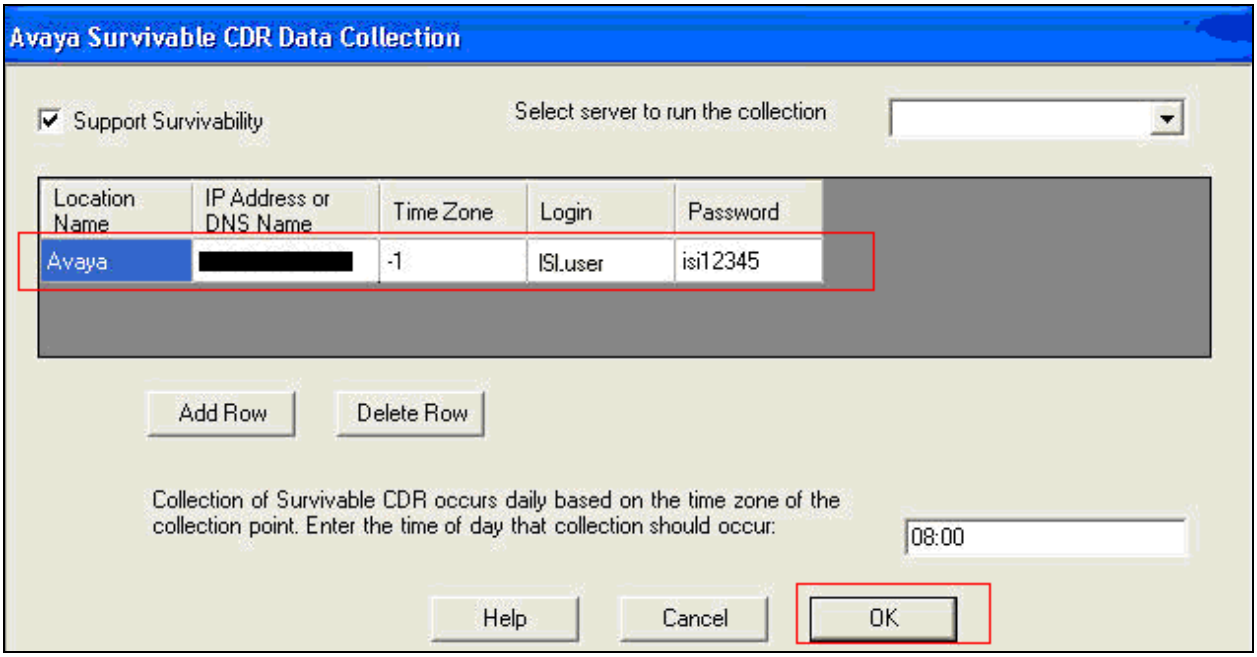
From the Define Data Collection Settings (Avaya RSP) page, select the **Avaya Survivable** button.



In the Avaya Survivable CDR Data Collection page, click on the **Add Row** button.
Provide the following information:

- **Location Name** – Enter a descriptive name
- **IP address or DNS Name** – IP address of the survivable Communication Manager. During the compliance test an S8300 Server (Processor Ethernet) IP address was utilized.
- **Time Zone** – Enter the time zone offset information.
- **Login** – Enter the login name that will be created in **Section 7.1.1**.
- **Password** – Enter the password that will be created in **Section 7.1.1**.

After completion, click on the **OK** button.



7. Configure the Avaya LSP CDR Solution

This section describes how to configure the main Avaya Aura® Communication Manager and a LSP licensed Avaya Aura® Communication Manager to perform an Avaya LSP CDR solution. This section also includes the verification steps.

7.1. Configure Avaya S8300D Server (Main) with G450 Media Gateway for the Avaya LSP Solution

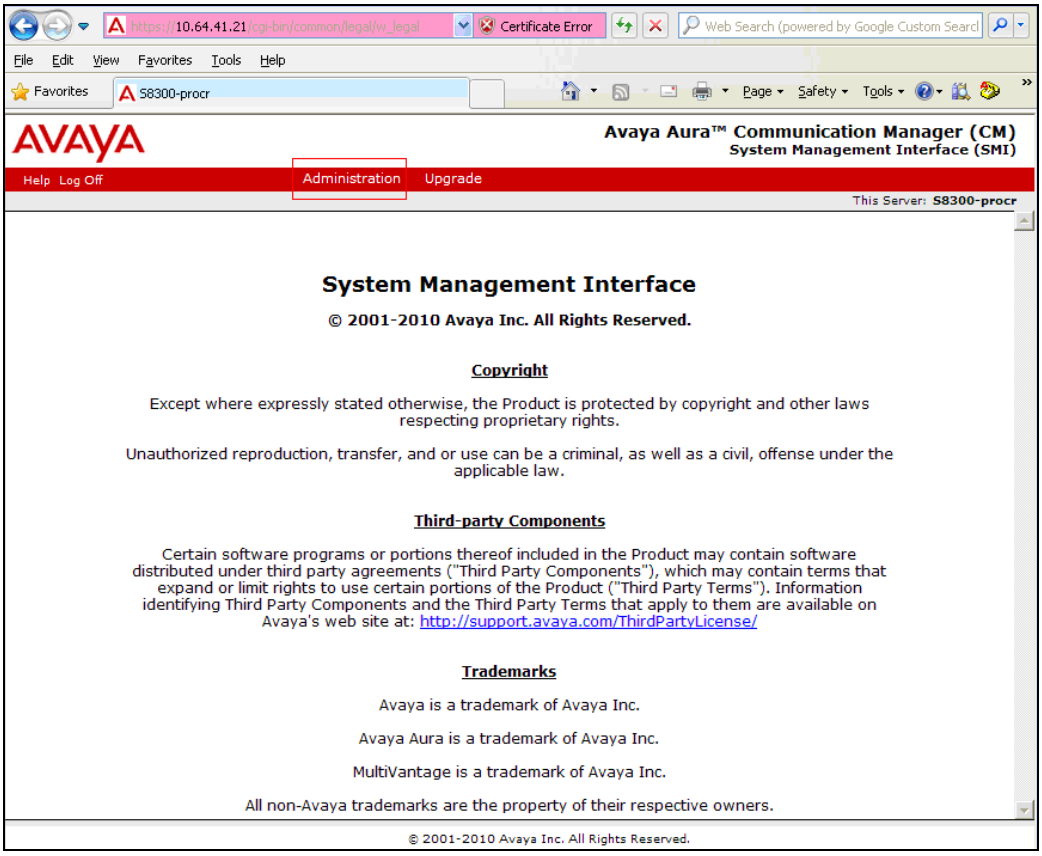
This section describes how to configure an Avaya S8300D Server with G450 Media Gateway for the Avaya LSP CDR Solution. The following steps must be performed:

- Create member credentials (username/password) for an SFTP account
- Add survivable-processor on the main Avaya S8300D Server
- Save the translation for LSP on the main Avaya S8300D Server to push translations to the LSP Server

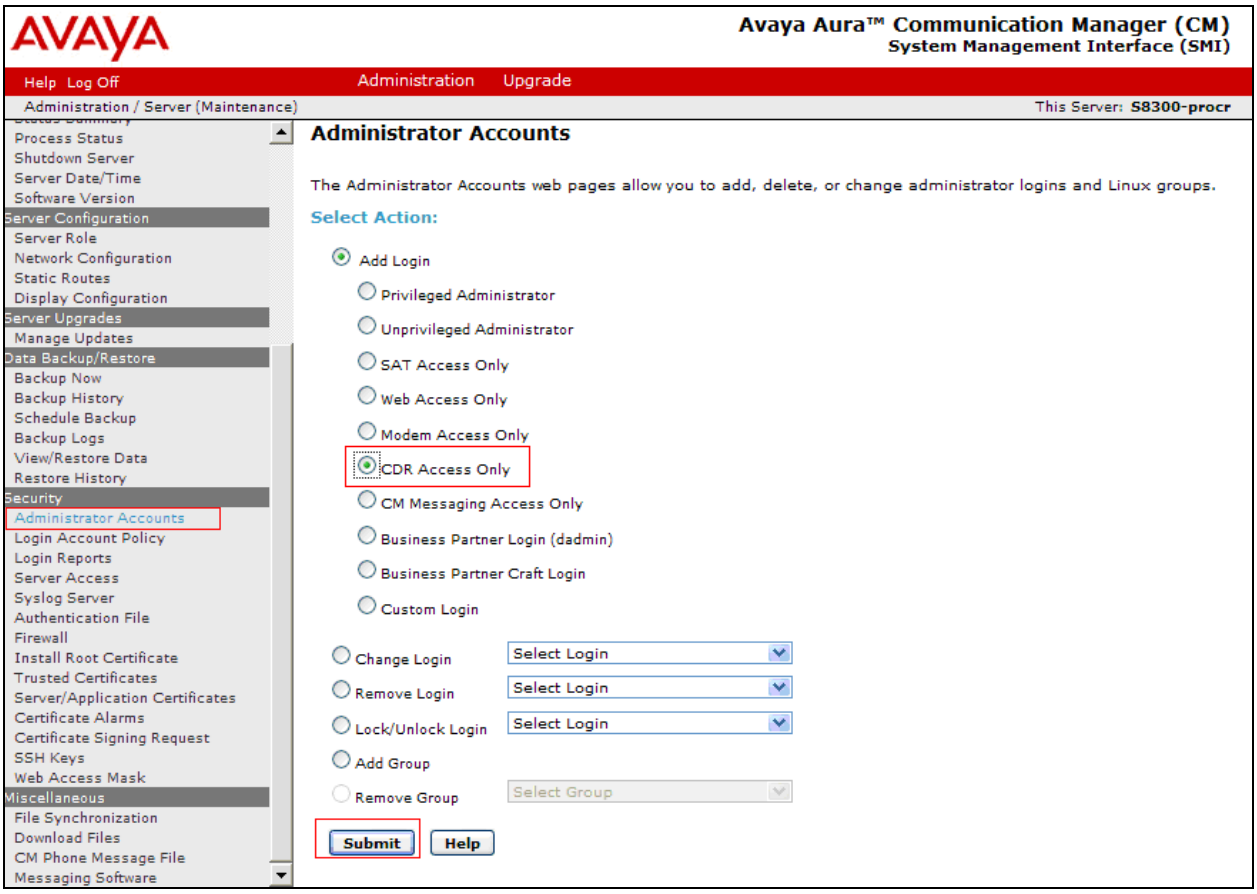
7.1.1. CDR credentials for SFTP

To create credentials, enter http://<IP address of Avaya S8300D Server> in the URL field of your browser, and log in with the appropriate credentials for accessing the Avaya Aura® Communication Manager (CM) System Management Interface (SMI) pages.

Select **Administration ➔ Server Maintenance** (not shown).



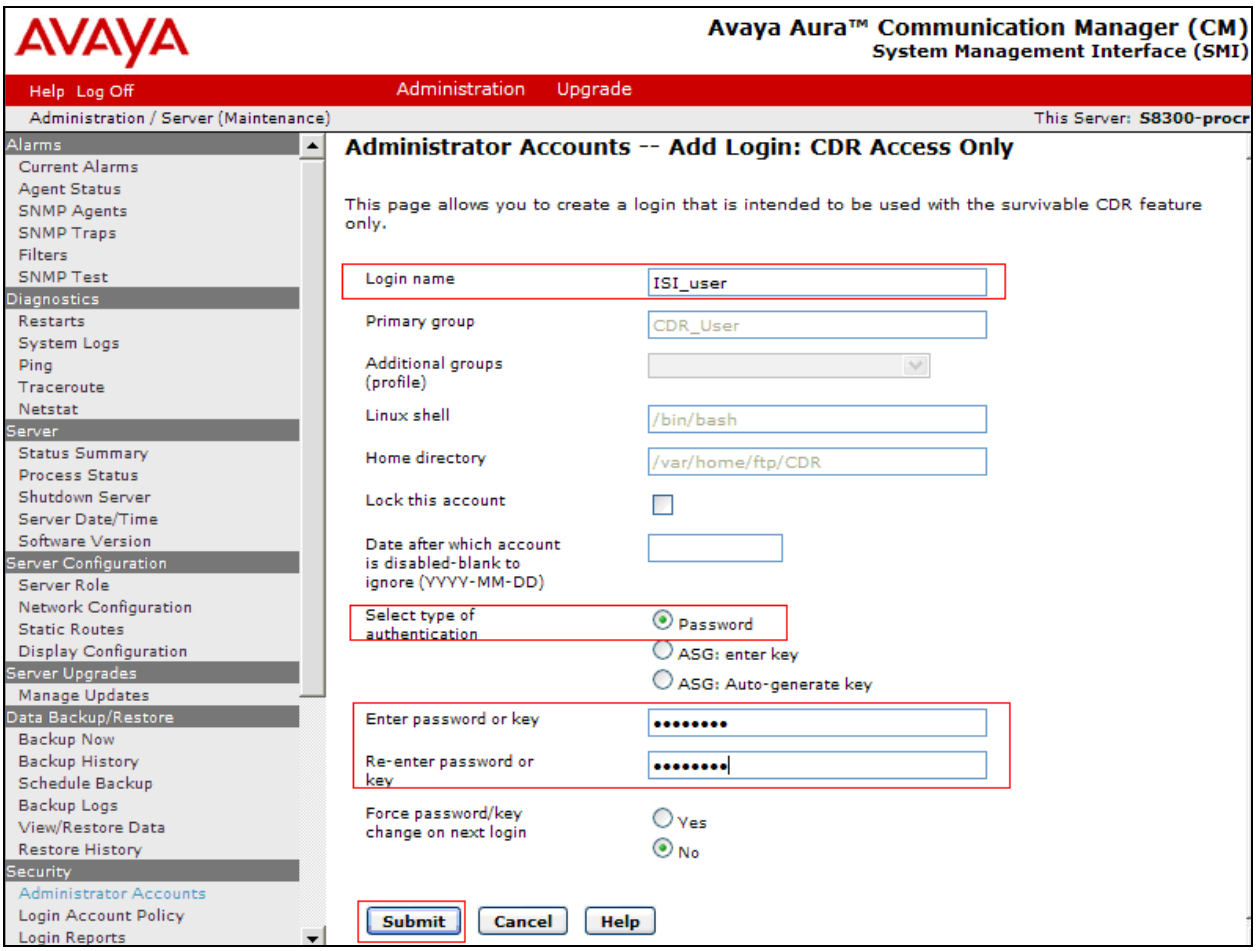
Select the **Administrator Accounts** link under the Security section on the left pane.
In the Administrator Accounts page, provide a type of login and click **Submit.**



On the Administrator Accounts—Add Login:CDR Access Only page, provide the following information:

- **Create a Login Name**
- **Select type of authentication** – Password was selected.
- **Enter the password**
- **Re-enter the password**

Click the **Submit** button.



7.1.2. Survivable-Processor Form

Using SAT, enter the **add survivable-processor s8300-lsp** command, where S8300 is an LSP licensed Avaya S8300D Server, configured in **Section 5**.

```
add survivable-processor s8300-lsp                                Page   1 of   3
                              SURVIVABLE PROCESSOR

Type: lsp          Cluster ID/MID: 2     Processor Ethernet Network Region:3


 V4 Node Name: s8300-lsp       Address: 10.64.42.21
 V6 Node Name:                 Address:
```

On Page 2, change the **Enabled** field to **o**, and the **Store to dsk** field to **y**.

```
add survivable-processor s8300-lsp                                Page   2 of   3
                    SURVIVABLE PROCESSOR - IP-SERVICES
 Service    Enabled Store   Local             Local    Remote            Remote
  Type              to dsk  Node              Port     Node              Port
  CDR1        o       y
  CDR2        o       y
```

After the configuration steps in **Section 7.1.1** and **7.1.2** are completed, run the **save translation all** command so that the translations in the Avaya S8300D Server will be pushed to the LSP licensed Avaya S8300D Server.

7.2. Verification from the Avaya S8300D Server for the Avaya LSP Solution

This section describes how to verify the Avaya LSP CDR solution from the LSP Server.
Enter the **display ip-services** command on the LSP Server.

```
display ip-services                                                Page   1 of   4

                                    IP SERVICES
 Service     Enabled     Local        Local       Remote      Remote
  Type                   Node         Port        Node        Port
CDR1                  procr            0       ISI             9000
CDR2                  procr            0       rdtt            9007
```

Enter the **display survivable-processor s8300-lsp** command and verify that the survivable-processor S8300 form in Avaya S8300D and LSP Servers are identical.

```
display survivable-processor s8300-lsp                            Page   2 of   3
                    SURVIVABLE PROCESSOR - IP-SERVICES
 Service    Enabled Store   Local             Local    Remote            Remote
  Type              to dsk  Node              Port     Node              Port
  CDR1        o       y
  CDR2        o       y
```

8. Verification Steps

The following steps may be used to verify the configuration:

- On the SAT of each Avaya Media Server, enter the **status cdr-link** command and verify that the CDR link state is up.
- Place a call and verify that ISI Infortel Select 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.
- Place internal, inbound trunk and outbound trunk calls to and from various telephones, generate an appropriate report in ISI Infortel Select, and verify the report's accuracy.

9. Conclusion

These Application Notes describe the procedures for configuring ISI Infortel Select to collect call detail records from Avaya Aura® Communication Manager running on Avaya Servers. ISI Infortel Select 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*, Release 6.0, Issue 8.0, June 2010, Document Number 555-245-205

[2] *Administering Avaya Aura® Communication Manager* Release 6.0, Issue 6.0, June 2010, Document Number 03-300509.

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.