



Avaya Solution & Interoperability Test Lab

Application Notes for FutureSoft Periscope 1.0 with Avaya Aura® Communication Manager 6.0.1 - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for FutureSoft Periscope 1.0 to interoperate with Avaya Aura® Communication Manager 6.0.1.

Periscope is a user friendly tool capable of collating and compiling of data from different sources to generate reports in a single desired format.

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

The objective of this interoperability compliance testing is to verify that FutureSoft Periscope 1.0 can interoperate with Avaya Aura® Communication Manager 6.0.1. FutureSoft Periscope interoperates with Avaya Aura® Communication Manager using Avaya Reliable Session Protocol (RSP) over TCP/IP for the collection of call detail records (CDR).

2. General Test Approach and Test Results

The general test approach was to manually place intra-switch calls, inter-switch IP Trunk calls, inbound and outbound PSTN trunk calls to and from telephones on Avaya Aura® Communication Manager systems, and verify that FutureSoft Periscope collects the CDR records and reports the correct attributes of the call.

2.1. Interoperability Compliance Testing

The interoperability compliance testing included feature and serviceability testing.

For feature testing, the ability of FutureSoft Periscope to collect and process CDR records for intra-switch calls, inter-switch calls, inbound and outbound PSTN trunk calls to and from telephones on both Communication Manager systems was evaluated.

For serviceability testing, the following were performed:

- Busied out and released the CDR links on Communication Manager.
- Disconnected and reconnected network connection to the FutureSoft Periscope server.
- Rebooted the FutureSoft Periscope server and Avaya S8800 Server.

2.2. Test Results

All test cases described in **Section 2.1** passed successfully except the following:

- After rebooting the FutureSoft Periscope server, the Avaya Reliable Data Transport Tool – Server and the FutureSoft Periscope CDR File Uploader applications have to be manually restarted.

2.3. Support

For technical support on Periscope, contact FutureSoft as shown below.

- **Web:** <http://www.futuresoftindia.com/aboutus/locations.aspx>
- **Voice:** +91-11-4222 8888
- **Email:** info@futuresoftindia.com

3. Reference Configuration

Figure 1 illustrates the network configuration used to verify the FutureSoft Periscope solution. Site A is comprised of an Avaya S8800 Server and Avaya G650 Media Gateway, and has connections to the following: Avaya 9600 and 1600 Series IP Telephones, Avaya 1400 Series Digital Telephones, and an ISDN-BRI trunk to the PSTN. FutureSoft Periscope is installed on a server running Microsoft Windows Server 2003 with Service Pack 2. Site B is comprised of an Avaya S8300D Server with Avaya G450 Media Gateway, and has connections to Avaya 9600 and 1600 Series IP Telephones. The Avaya 4548GT-PWR Ethernet Routing Switch provides Ethernet connectivity to the servers and IP telephones and Layer 3 IP routing between the two sites. An H.323 IP trunk is configured between Site A and B for the users to call between the two sites. For this testing, Site B is only used to make inter-PBX IP calls. No CDR data is collected from Site B.

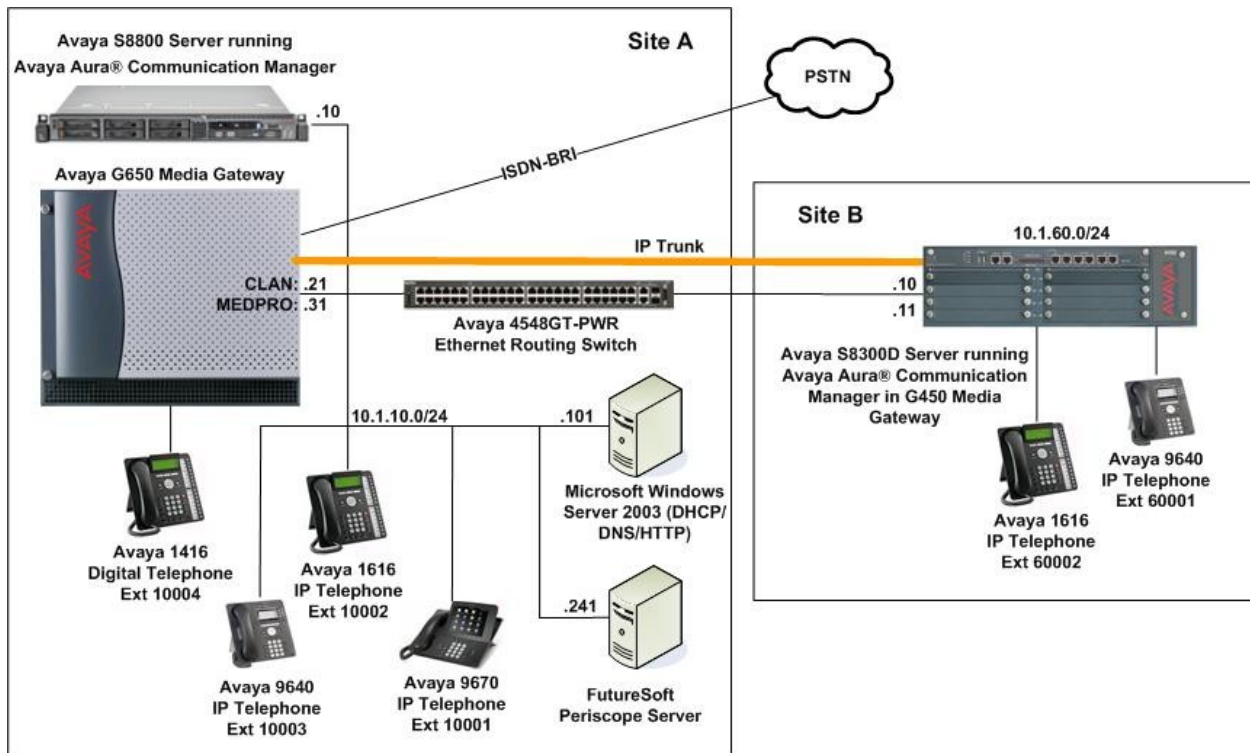


Figure 1: Test configuration for FutureSoft Periscope Solution

4. Equipment and Software Validated

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

Equipment	Software
Avaya S8800 Server	Avaya Aura® Communication Manager 6.0.1 (Service Pack 4 00.1.510.1-19100)
Avaya G650 Media Gateway <ul style="list-style-type: none"> • TN2312BP IP Server Interface • TN799DP C-LAN Interface • TN2302AP IP Media Processor • TN2602AP IP Media Processor • TN2214CP Digital Line 	- HW07, FW054 HW01, FW040 HW20, FW121 HW02, FW059 HW08, FW015
Avaya S8300D Server	Avaya Aura® Communication Manager 6.0.1 (Service Pack 4 00.1.510.1-19100)
Avaya G450 Media Gateway	31.19.2
Avaya 9600 Series IP Telephones - 9670 - 9640	3.1 SP2 (H.323) 3.1 SP2 (H.323)
Avaya 1600 Series IP Telephones - 1616	1.300B (H.323)
Avaya 1416 Digital Telephone	-
Avaya 4548GT-PWR Ethernet Routing Switch	V5.4.0.008
FutureSoft Periscope running on Microsoft Windows 2003 Server	1.0

5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Call Detail Recording (CDR) in Communication Manager. All configuration changes in Communication Manager are performed through the System Access Terminal (SAT). Communication Manager is configured to generate and send the CDR records to the IP address of the FutureSoft Periscope server using Avaya Reliable Session Protocol (RSP) over TCP/IP. For this configuration, the CDR links are configured to originate from the IP addresses of the Avaya S8800 Server (i.e. with node-name – “procr”) and terminates at the IP address of the FutureSoft Periscope server. The highlights in the following screens indicate the parameter values used during the compliance test.

Step	Description
1.	<p>Use the change node-names ip command to add a new node name for the FutureSoft Periscope.</p> <pre> change node-names ip Page 1 of 1 IP NODE NAMES Name IP Address default 0.0.0.0 procr 10.1.10.10 Periscope 10.1.10.241 </pre>
2.	<p>Use the change ip-services command to define the CDR link. To define a primary CDR link, the following information should be provided:</p> <ul style="list-style-type: none"> • Service Type: CDR1 [If needed, a secondary link can be defined by setting Service Type to CDR2.] • Local Node: procr • Local Port: 0 [The Local Port is fixed to 0 because Communication Manager initiates the CDR link.] • Remote Node: Periscope [The Remote Node is set to the node name previously defined in Step 1.] • Remote Port: 9000 [The Remote Port may be set to a value between 5000 and 64500 inclusive, and must match the port configured in FutureSoft Periscope in Section 6.1.] <pre> change ip-services Page 1 of 4 IP SERVICES Service Type Enabled Local Node Local Port Remote Node Remote Port CDR1 procr 0 Periscope 9000 </pre>

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

```
change ip-services
```

Page 3 of 4

Service Type	Reliable Protocol	SESSION LAYER TIMERS				Connectivity Timer
		Packet Resp Timer	Session Message	Connect Cntr	SPDU Cntr	
CDR1	y	30	3	3	60	

3. Enter the **change system-parameters cdr** command to set the parameters for the type of calls to track and the format of the CDR data. The following settings were used during the compliance test.

- **CDR Date Format: month/day**
- **Primary Output Format: customized**
- **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 [2]** for a full explanation of each field. The test configuration used some of the more common fields described below.

- **Use Legacy CDR Formats? n** [Specify the use of the new Communication Manager 4.0.1 and later formats in the CDR records produced by the system.]
- **Remove # From Called Number? y** [The system will remove the pound sign (#) from the Dialed Number field of the call detail record.]
- **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: customized                            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? y
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? y
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: group-ext
Record Called Vector Directory Number Instead of Group or Member? n
Record Agent ID on Incoming? n                          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: outpulsed
Privacy - Digits to Hide: 0                             CDR Account Code Length: 7

```

On Page 2 of the CDR SYSTEM PARAMETERS form, define the customized CDR format as shown.

```

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

Data Item - Length      Data Item - Length      Data Item - Length
1: date                  - 6      17: calling-num         - 15      33:
2: space                 - 1      18: space                - 1      34:
3: time                  - 4      19: frl                  - 1      35:
4: space                 - 1      20: space                - 1      36:
5: sec-dur               - 5      21: in-crt-id           - 3      37:
6: space                 - 1      22: clg-num/in-tac      - 15     38:
7: code-used             - 4      23: vdn                  - 7      39:
8: space                 - 1      24: cond-code           - 1      40:
9: out-crt-id            - 3      25: return               - 1      41:
10: space                 - 1      26: line-feed           - 1      42:
11: code-dial            - 4      27:                      -         43:
12: dialed-num           - 23     28:                      -         44:
13: space                 - 1      29:                      -         45:
14: auth-code            - 13     30:                      -         46:
15: space                 - 1      31:                      -         47:
16: acct-code            - 15     32:                      -         48:

Record length = 130

```

4. If the **Intra-switch CDR** field is set to **y** on Page 1 of the CDR SYSTEM PARAMETERS form, then use the **change intra-switch-cdr** command to define the extensions that will be subjected to call detail records. In the **Extension** column, enter the specific extensions whose usage will be tracked with the CDR records.

```
change intra-switch-cdr                                     Page 1 of 3
                                     INTRA-SWITCH CDR
Assigned Members: 4 of 5000 administered
Extension      Extension      Extension      Extension
10001
10002
10003
10004
```

5. 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.

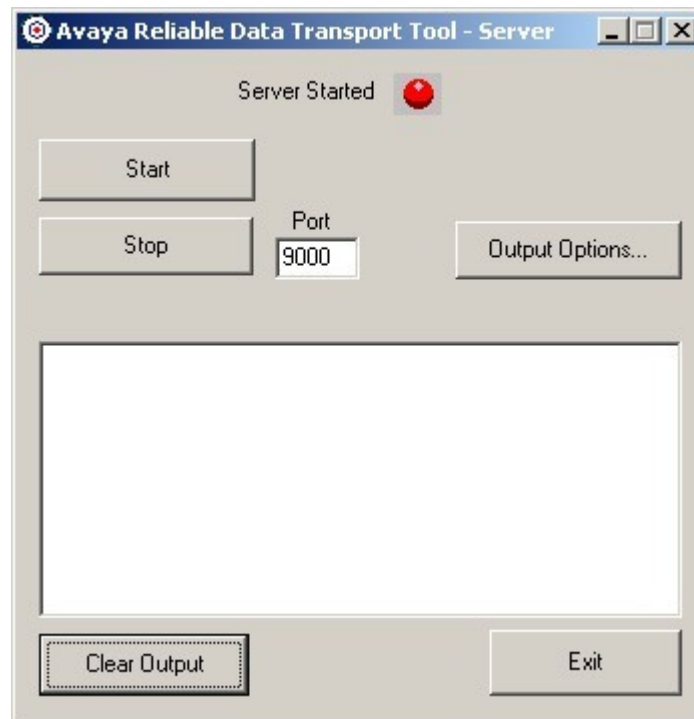
```
change trunk-group 1                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 1          Group Type: isdn          CDR Reports: y
Group Name: PSTN - BRI   COR: 95          TN: 1          TAC: #01
Direction: two-way      Outgoing Display? n      Carrier Medium: PRI/BRI
Dial Access? y          Busy Threshold: 255      Night Service:
Queue Length: 0
Service Type: public-ntwrk      Auth Code? n          TestCall ITC: rest
Far End Test Line No:
TestCall BCC: 4
```


6. Configure FutureSoft Periscope

This section describes the configuration of FutureSoft Periscope. Periscope uses the Avaya Reliable Data Transport Tool – Server application to collect the CDR records from Communication Manager and write the CDR records to a folder on the Periscope server. The CDR records are then imported into the Periscope database using the Periscope CDR File Uploader application.

6.1. Configure Avaya Reliable Data Transport Tool - Server

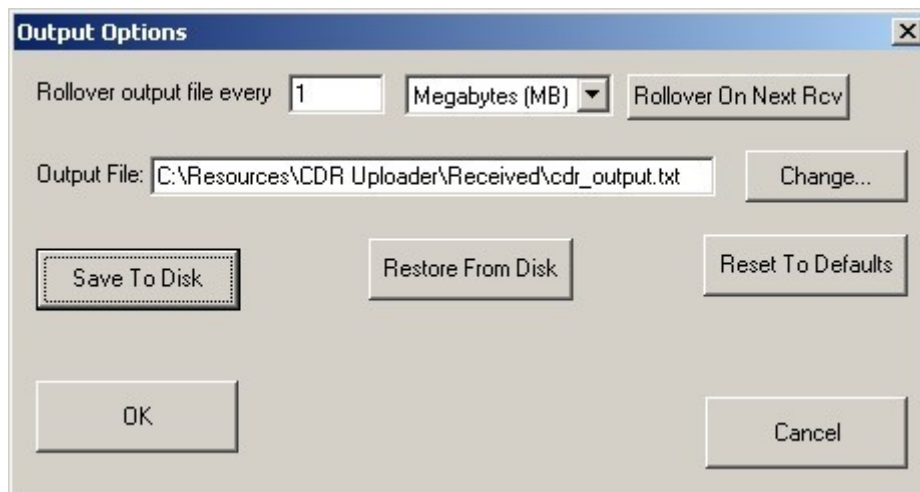
Login as an administrator on the Periscope server, and click **Start** → **All Programs** → **Avaya Reliable Data Transport Tool** → **Server Executable** to launch the application. Set **Port** to **9000** to match the setting on Communication Manager in **Section 5 Step 2**. Click **Output Options**.



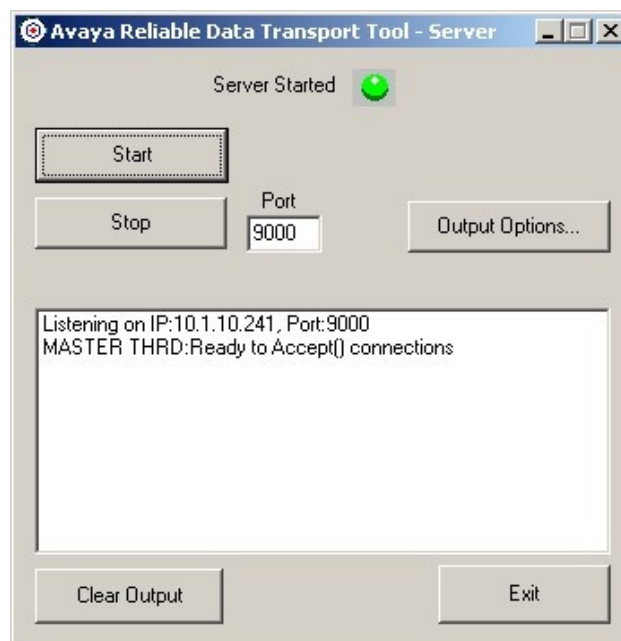
This window configures the option of saving the CDR records to a file. Configure as follows and click **Save To Disk** to save the settings. Then click **OK**.

- **Rollover output file every:** The CDR record file rolls over to a new file when it reaches a certain file size, e.g. 1 Megabyte (1 MB). This value is selected based on the expected CDR records generated by Communication Manager.
- **Output File:** Specify a folder and file name on the Periscope server to store the output files. For this testing, **C:\Resources\CDR Uploader\Received\cdr_output.txt** was used. Note that when rollover happens, the new file name follows the format as shown below:

cdr_output_<yyyymmddhhmmss>.txt

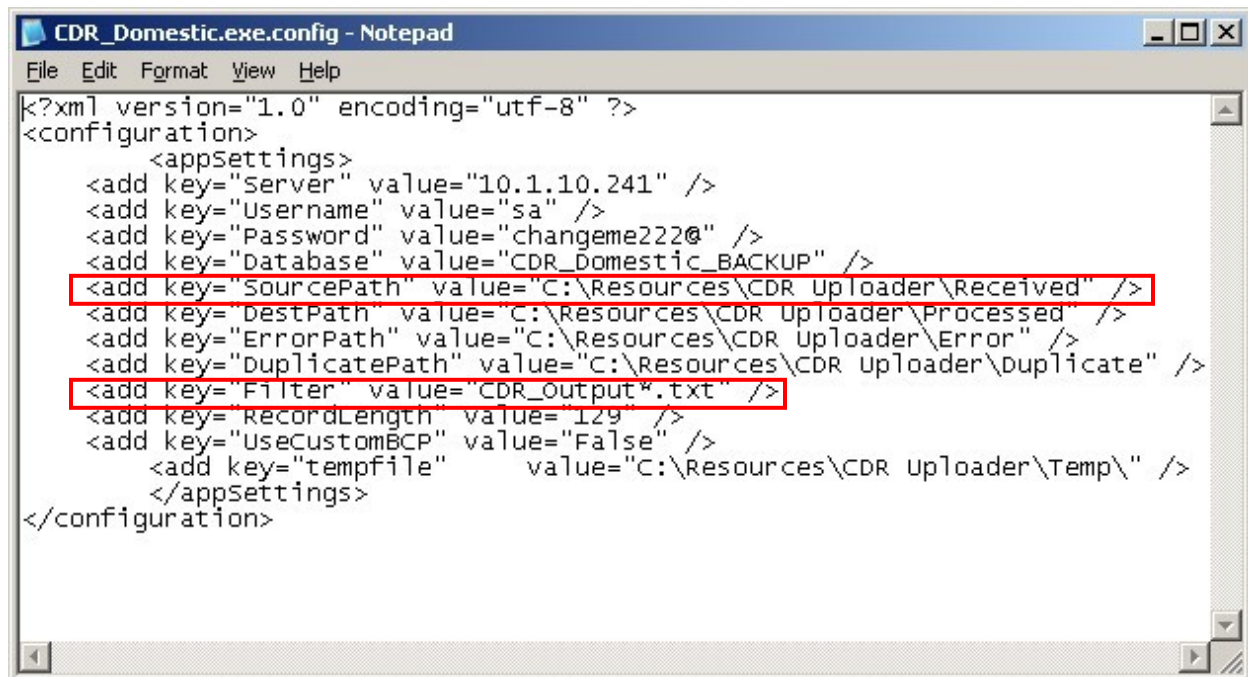


At the main window, click **Start**. The **Server Started** indicator will turn green as shown below.



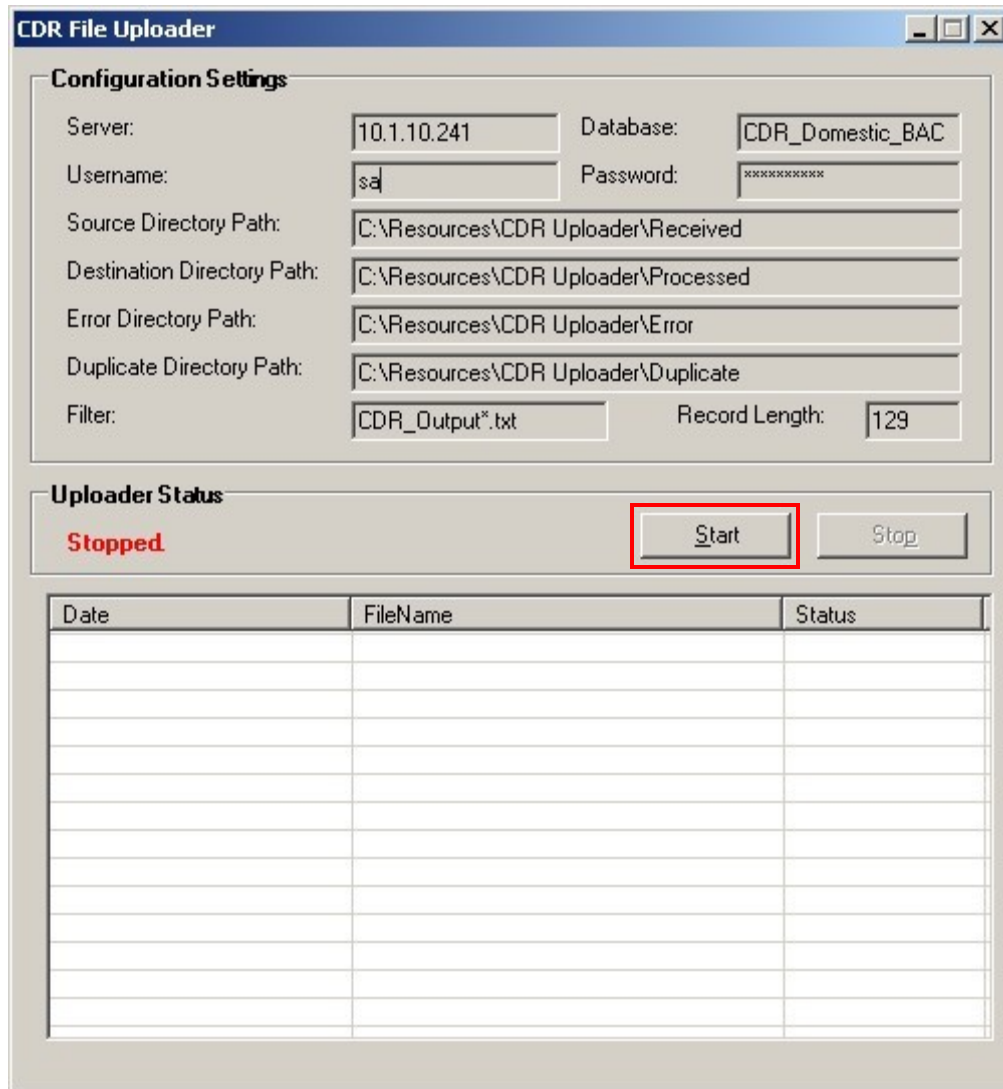
6.2. Configure Periscope CDR File Uploader

Edit the file **CDR_Domestic.exe.config** located in the folder **C:\Resources\CDR Uploader** using Notepad. Configure the **SourcePath** and **Filter** fields to match the **Output File** field configured in **Section 6.1**. For example, in this testing the **SourcePath** and **Filter** values were set to **C:\Resources\CDR Uploader\Received** and **CDR_Output*.txt** respectively as shown below so that all matching files in that folder will be processed by the CDR File Uploader application. The **Server**, **Username**, **Password** and **Database** fields are set to the appropriate values to upload the CDR records into the Microsoft SQL2005 database. Accept the default values for the rest of the fields.



```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <appSettings>
    <add key="Server" value="10.1.10.241" />
    <add key="Username" value="sa" />
    <add key="Password" value="changeme222@" />
    <add key="Database" value="CDR_Domestic_BACKUP" />
    <add key="SourcePath" value="C:\Resources\CDR Uploader\Received" />
    <add key="DestPath" value="C:\Resources\CDR Uploader\Processed" />
    <add key="ErrorPath" value="C:\Resources\CDR Uploader\Error" />
    <add key="duplicatePath" value="C:\Resources\CDR Uploader\Duplicate" />
    <add key="Filter" value="CDR_Output*.txt" />
    <add key="RecordLength" value="129" />
    <add key="UseCustomBCP" value="False" />
    <add key="tempfile" value="C:\Resources\CDR Uploader\Temp\" />
  </appSettings>
</configuration>
```

Launch the CDR File Uploader application by double-clicking **CDR_Domestic.exe** located in the folder **C:\Resources\CDR Uploader**. Click **Start**. The CDR File Uploader application will begin to monitor the configured folder and upload any matching CDR record files to the SQL2005 database.



7. Verification Steps

The following steps may be used to verify the configuration:

- Use the **ping** utility on the FutureSoft Periscope server to verify the IP connectivity to the Avaya S8800 Server.
- On the SAT of Avaya S8800 Server, enter the **status cdr-link** command and verify that the **Link State** shows **up** for the Primary CDR Link that is used.

```
status cdr-link
                CDR LINK STATUS
                Primary                Secondary
                Link State: up         CDR not administered
                Date & Time: 2011/11/10 17:21:33    0000/00/00 00:00:00
                Forward Seq. No: 52                0
                Backward Seq. No: 0                0
                CDR Buffer % Full: 0.00            0.00
                Reason Code: OK
```

- Place an outgoing PSTN trunk call and verify that FutureSoft Periscope receives the CDR record for the call. Login to FutureSoft Periscope using a browser (shown below) and compare the values of data fields in the CDR record with the expected values and verify that they match.

CDR Query Output													
Records : 1 - 27 of 27											BACK		
Page : 1 of 1											DOWNLOAD		
ROW_DATETIME	DURATION	CODE_USED	OUT_CRT_ID	CODE_DIALED	CALLEDNUMBER	AUTHCODE	ACCT_CODE	EXTENSION	FRL_IN_CRT_ID	CLG_NUM	VDN	FILEID	cdrCondCode
12/13/2011 11:49:00 AM	22	#01	003	9	68728680			10099	7	10099	48	7	

- Place internal, inbound trunk, and outbound trunk calls to and from various telephones, generate an appropriate report in FutureSoft Periscope and verify the report's accuracy.

8. Conclusion

These Application Notes describe the procedures for configuring FutureSoft Periscope 1.0 to collect call detail records from Avaya Aura® Communication Manager 6.0.1. FutureSoft Periscope successfully passed the compliance testing.

9. Additional References

This section references the Avaya documentation that is relevant to these Application Notes.

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

- [1] *Administering Avaya Aura® Communication Manager*, Release 6.0, June 2010, Document Number 03-300509, Issue 6.0.
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 6.0, June 2010, Document Number 555-245-205, Issue 8.0.

Product information on FutureSoft Periscope can be found at <http://www.futuresoftindia.com/solutions/telecom/periscope.html>.

The following documents are available from FutureSoft upon request.

- [3] *FutureSoft Periscope User Manual*.
- [4] *FutureSoft Periscope Installation Guide*.

©2012 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.