Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avotus ICM Usage Management with Avaya Aura™ Communication Manager – Issue 1.0

Abstract

These Application Notes describe the configuration procedures required to allow Avotus ICM Usage Management to collect call detail records from Avaya Aura™ Communication Manager using Avaya Reliable Session Protocol over TCP/IP. Avotus ICM 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 describes a compliance-tested call detail recording (CDR) solution comprised of Avaya Aura ™ Communication Manager and Avotus ICM Usage Management (referred to as Avotus ICM in the ensuring text of this document). Avotus ICM 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.

Communication Manager communicates to Avotus ICM 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. Communication Manager generates and sends the call records out in the RSP session while Avotus ICM collects, stores and processes the records at the other end.

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. Avotus ICM can support any CDR format provided by Communication Manager. However, during the compliance test, the expanded format was utilized.

1.1. 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 Avotus ICM Usage Management and Communication Manager.

1.2. Support

Technical support for the Avotus ICM Usage Management solution can be obtained by contacting Avotus:

- URL – http://www.avotus.com/contact_support.asp
- Phone – (800) 840-2580

2. Reference Configuration

Figure 1 illustrates a sample configuration that was used for the compliance test. The configuration consists of three Avaya Servers running Communication Manager. Site A is comprised of Communication Manager running on an Avaya S8300D Server with an Avaya G450 Media Gateway. Site B is comprised of Communication Manager running on two Avaya S8720 Servers (duplex fail-over configuration) and an Avaya G650 Media Gateway. Each Communication Manager is connected to an IP network comprised of an Extreme Networks Summit 48 layer 3 switch. Avotus ICM running on a Windows Server 2003 Enterprise Edition is connected to the IP network at a different subnet and has a RSP session established to each Communication Manager to collect CDR records. Each system has trunks and phones associated with it to generate calls. Avaya 4600 Series IP Telephones, Avaya 9600 Series IP Telephones, and Avaya 6400D Series Digital Telephones are registered to both Avaya S8700 and S8300 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 (not shown).

The Avaya S8300D Server, installed with Local Survivable Processor (LSP) license, is set up as a LSP to Site A.

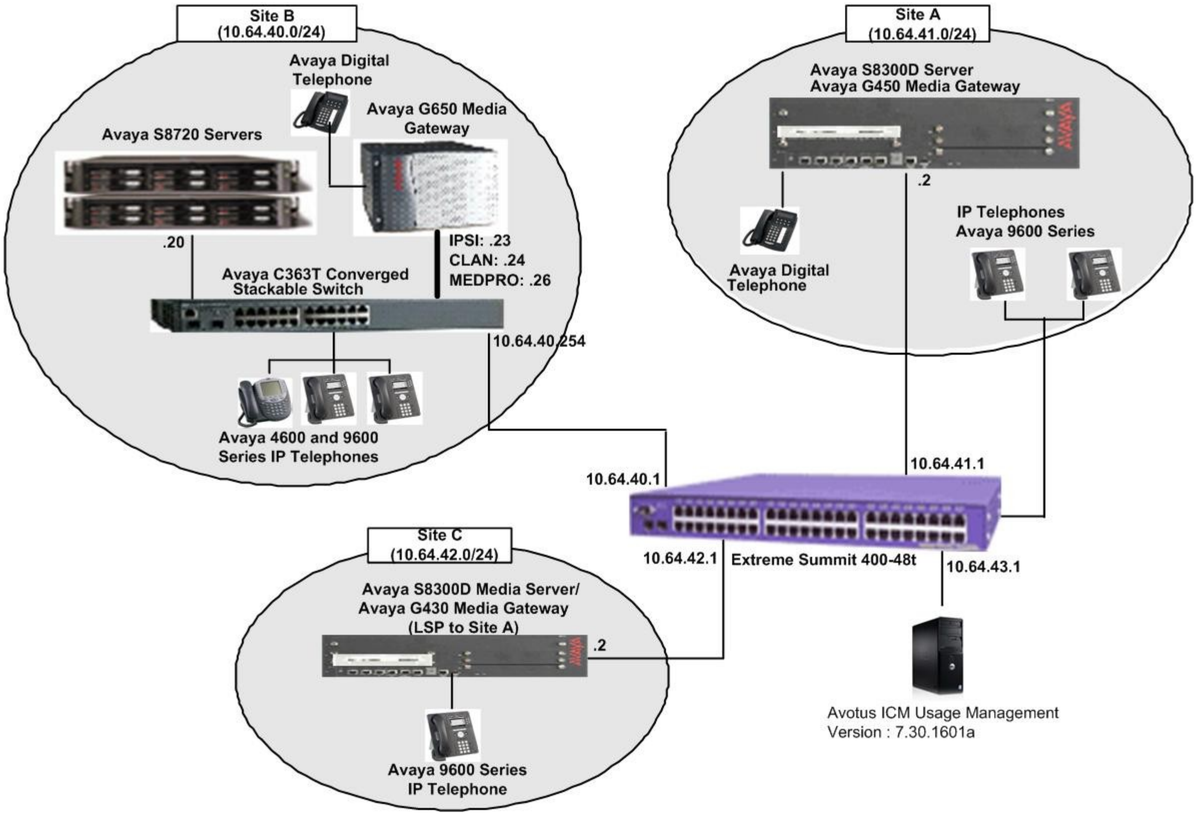


Figure 1: Test configuration for Avotus ICM Usage Management Compliance Test

3. Equipment and Software Validated

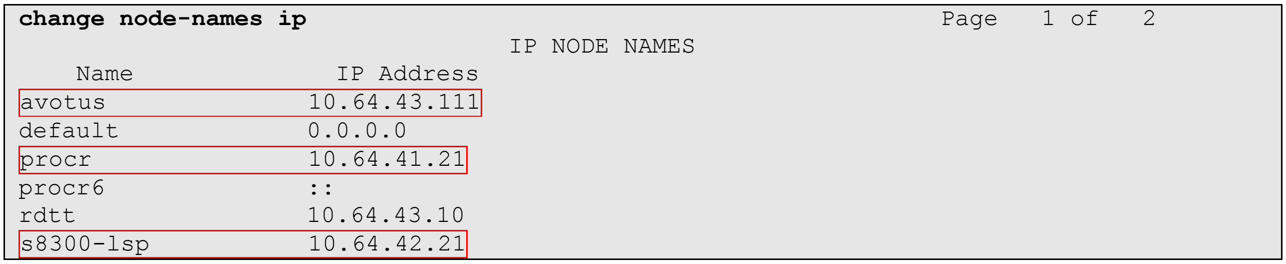
The following equipment and software/firmware were used for the test configuration.

Equipment		Software/Firmware
Avaya S8300D Server with Avaya G450 Media Gateway		Avaya Aura™ Communication Manager 6.0 (R016x.00.0.345.0) with Patch 00.0345.0-18246
Avaya S8720 Servers with Avaya G650 Media Gateway		Avaya Aura™ Communication Manager 5.2.1 (R015x.02.1.016.4)
Avaya S8300D Server with Avaya G430 Media Gateway (with LSP license)		Avaya Aura™ Communication Manager 6.0 (R016x.00.0.345.0) with Patch 00.0345.0-18246
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
Avotus ICM		7.30.1601a

4. Configure Avaya Aura™Communication Manager

This section describes the procedure for configuring call detail recording (CDR) in 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. Communication Manager will be configured to generate CDR records using RSP over TCP/IP to the IP address of the PC running Avotus ICM. For the Avaya S8720 Server, the RSP link originates at the IP address of the CLAN board. For the Avaya S8300D Server, the RSP link originates at the IP address of the local processor (with node-name “procr”).

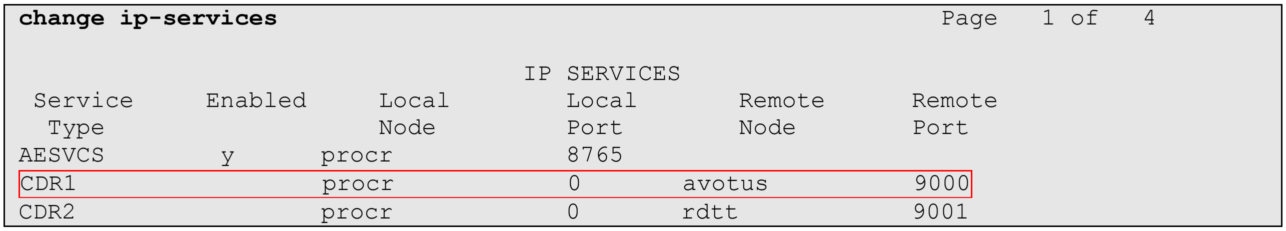
Use the **change node-names ip** command to create a new node name, for example, **avotus**. This node name is associated with the IP Address of the PC running Avotus ICM application. Also, take note of the node name “procr”. It will be used in the next step. The “procr” entry on this form was previously administered. s8300-lsp is an LSP licensed Avaya S8300D Server.



```
change node-names ip                                          Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
avotus              10.64.43.111
default             0.0.0.0
procr               10.64.41.21
procr6              ::
rdtt                10.64.43.10
s8300-lsp           10.64.42.21
```

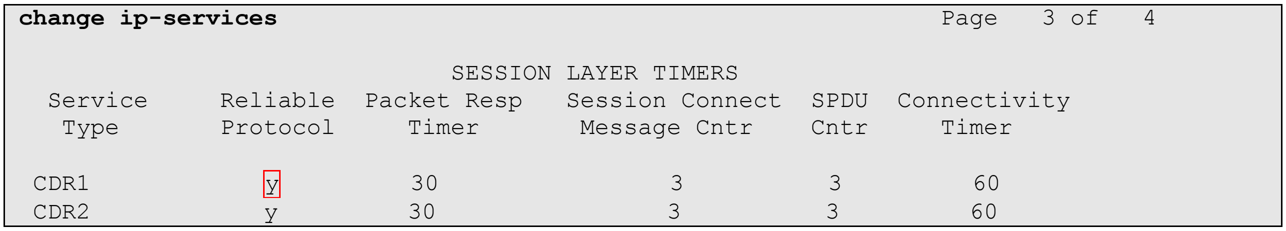
Use the **change ip-services** command to define the CDR link to use the RSP over TCP/IP. To define a primary CDR link, provide the following information:

- 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: **avotus** [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 Avotus ICM.]



```
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        avotus             9000
CDR2                   procr            0        rdtt               9001
```

On Page 3 of the ip-services form, enable the Reliable Session Protocol (RSP) for the CDR link by setting the Reliable Protocol field to **y**.



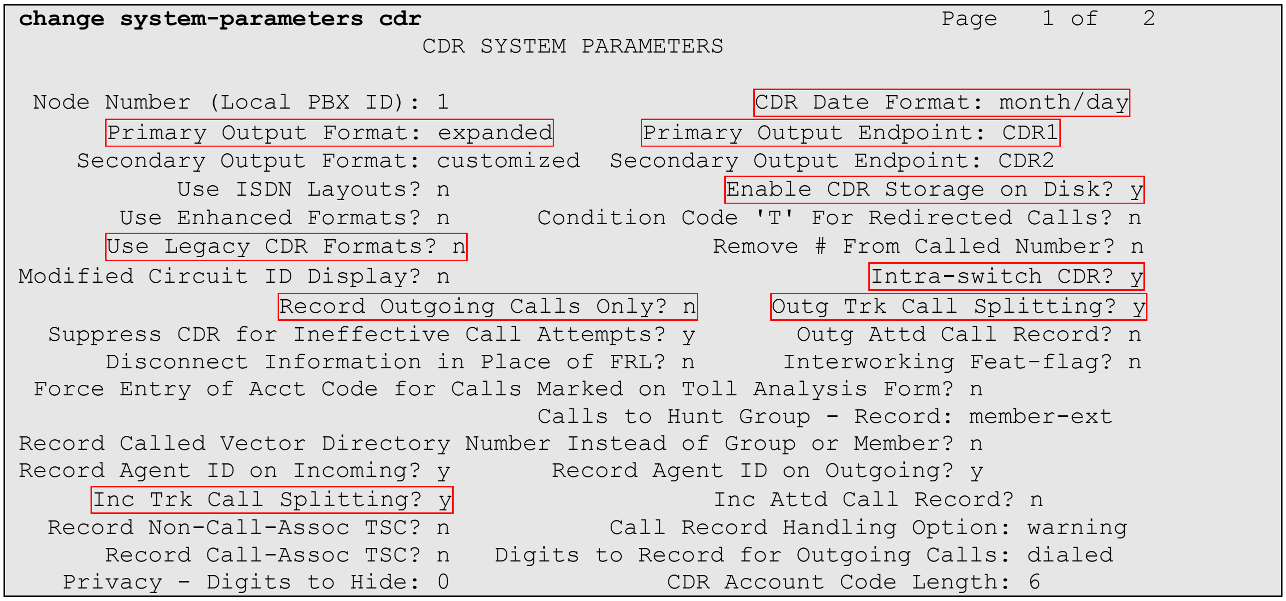
```
change ip-services                                            Page   3 of   4

                              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: **expanded**
- 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.

- 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: expanded      Primary Output Endpoint: CDR1
    Secondary Output Format: customized  Secondary Output Endpoint: CDR2
           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
```

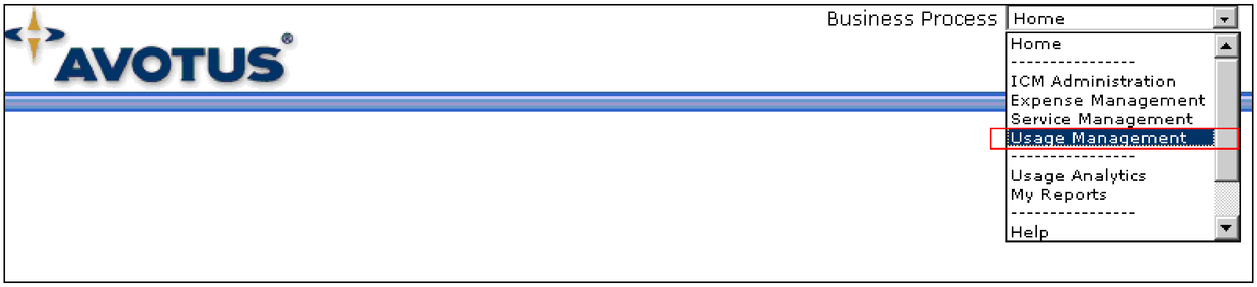
For each trunk group for which CDR records are desired, verify that CDR reporting is enabled. Use the **change trunk-group *n*** command, where ***n*** is the trunk group number, to verify that the CDR Reports field is set to **y**. This applies to all types of trunk groups.

```
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
```

5. Configure Avotus ICM Usage Management

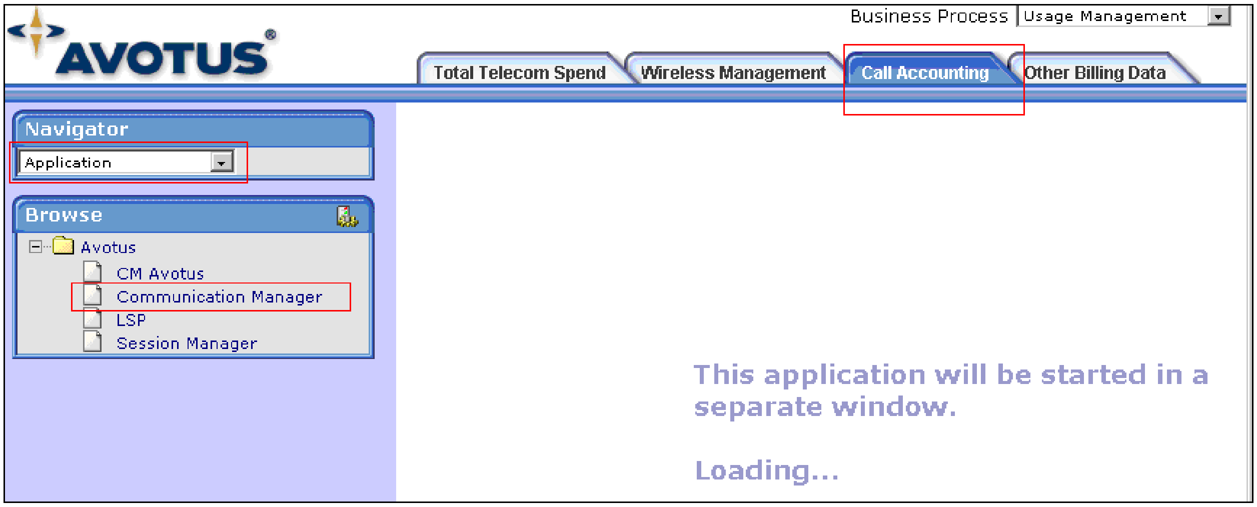
This section describes the configuration of Avotus ICM Usage management. Avotus installs, configures, and customizes the ICM Usage Management application for the end customers. Thus, this section only describes the interface configuration, so that Avotus ICM Usage Management can receive CDR data from Communication Manager.

To configure Avotus ICM Usage Management, double click on the Avotus ICM Usage Management icon, , and provide credentials to gain access into Avotus ICM Usage Management. Select **Usage Management** using the drop-down menu.



From the Avotus Home page, click the **Call Accounting** tab on the top. From the left pane, select **Application** under the Navigator section. Then, choose an appropriate call accounting system. The following screen shows the call accounting system for **Communication Manager**.

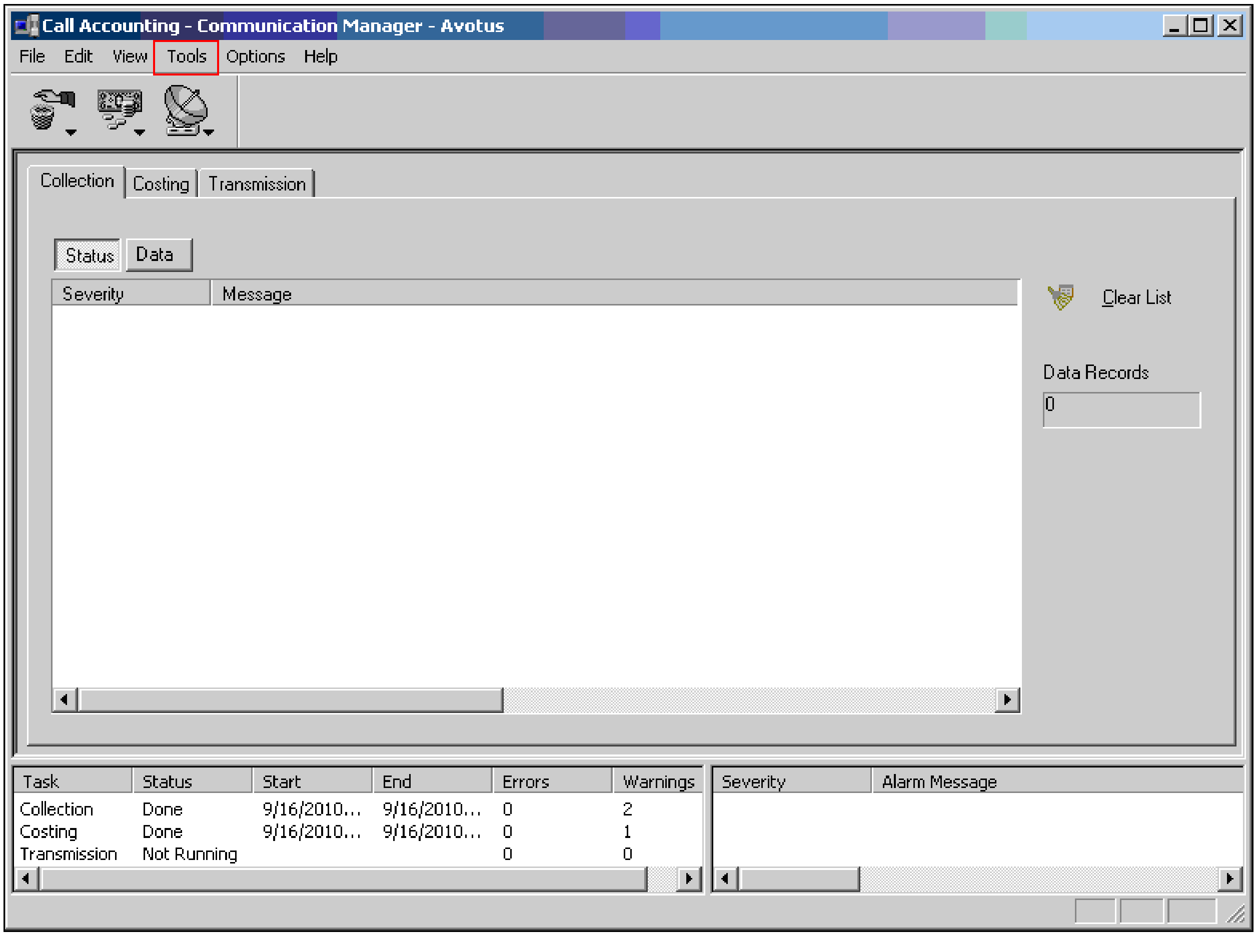
By selecting the call accounting system, the Call Accounting-Communication Manager- Avotus page appears.



This application will be started in a separate window.

Loading...

On the Call Accounting-Communication Manager- Avotus page, navigate to **Tools → Collection → Configuration** (not shown), and the System Configuration page appears

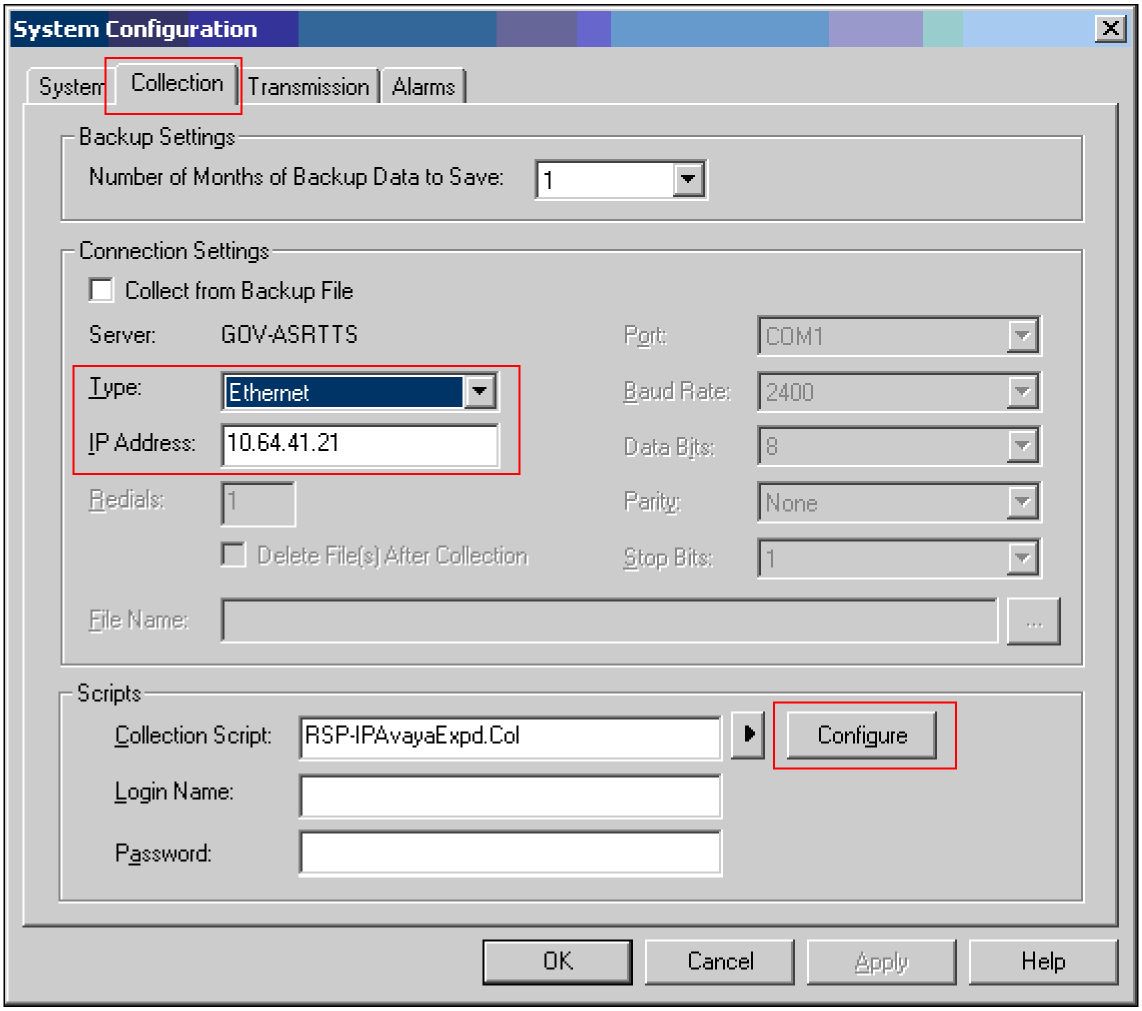


Task	Status	Start	End	Errors	Warnings
Collection	Done	9/16/2010...	9/16/2010...	0	2
Costing	Done	9/16/2010...	9/16/2010...	0	1
Transmission	Not Running			0	0

On the System Configuration Page, Select the **Collection** tab and provide the following information:

- Type – Select **Ethernet** using the drop down menu.
- IP Address – Enter the IP address where CDR data is coming from. During the compliance test, the IP address of the “procr” node on the Avaya S8300D Server was utilized (see **Section 4**). For the Avaya S8720 Servers with G650 Media Gateway, the IP address of the CLAN board should be specified here.

To configure the listening port, click on the **Configure** button.



Number of Months of Backup Data to Save: 1

□ Collect from Backup File

Server: GOV-ASRTTS

Type: Ethernet

IP Address: 10.64.41.21

Redials: 1

□ Delete File(s) After Collection

Port: COM1

Baud Rate: 2400

Data Bits: 8

Parity: None

Stop Bits: 1

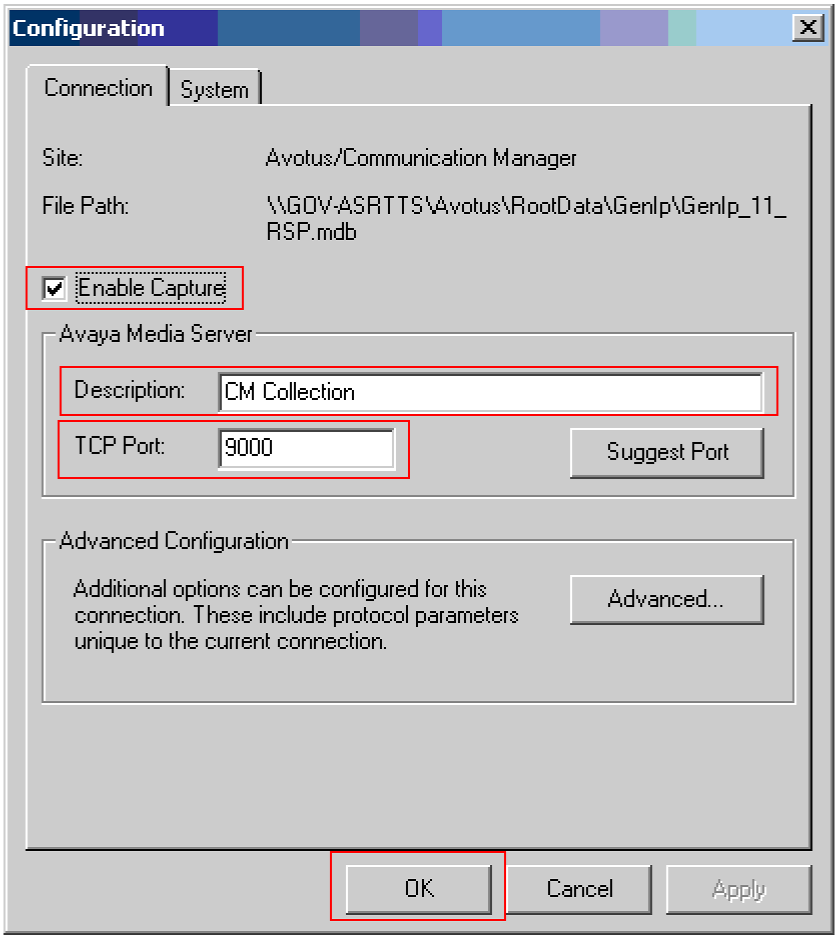
File Name:

Collection Script: RSP-IPAvayaExpd.Col

Login Name:

Password:

On the Configuration page, check on the **Enable Capture** box. Under the Avaya Media Server section, provide Description and TCP Port number. During the compliance test, port **9000** was utilized. Click on the **OK** button to save the changes.



Site: Avotus/Communication Manager

File Path: \\GOV-ASRTTS\Avotus\RootData\GenIp\GenIp_11_RSP.mdb

☑ Enable Capture

Avaya Media Server

Description: CM Collection

TCP Port: 9000

Advanced Configuration

Additional options can be configured for this connection. These include protocol parameters unique to the current connection.

6. Configure the Avaya LSP CDR Solution

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

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

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

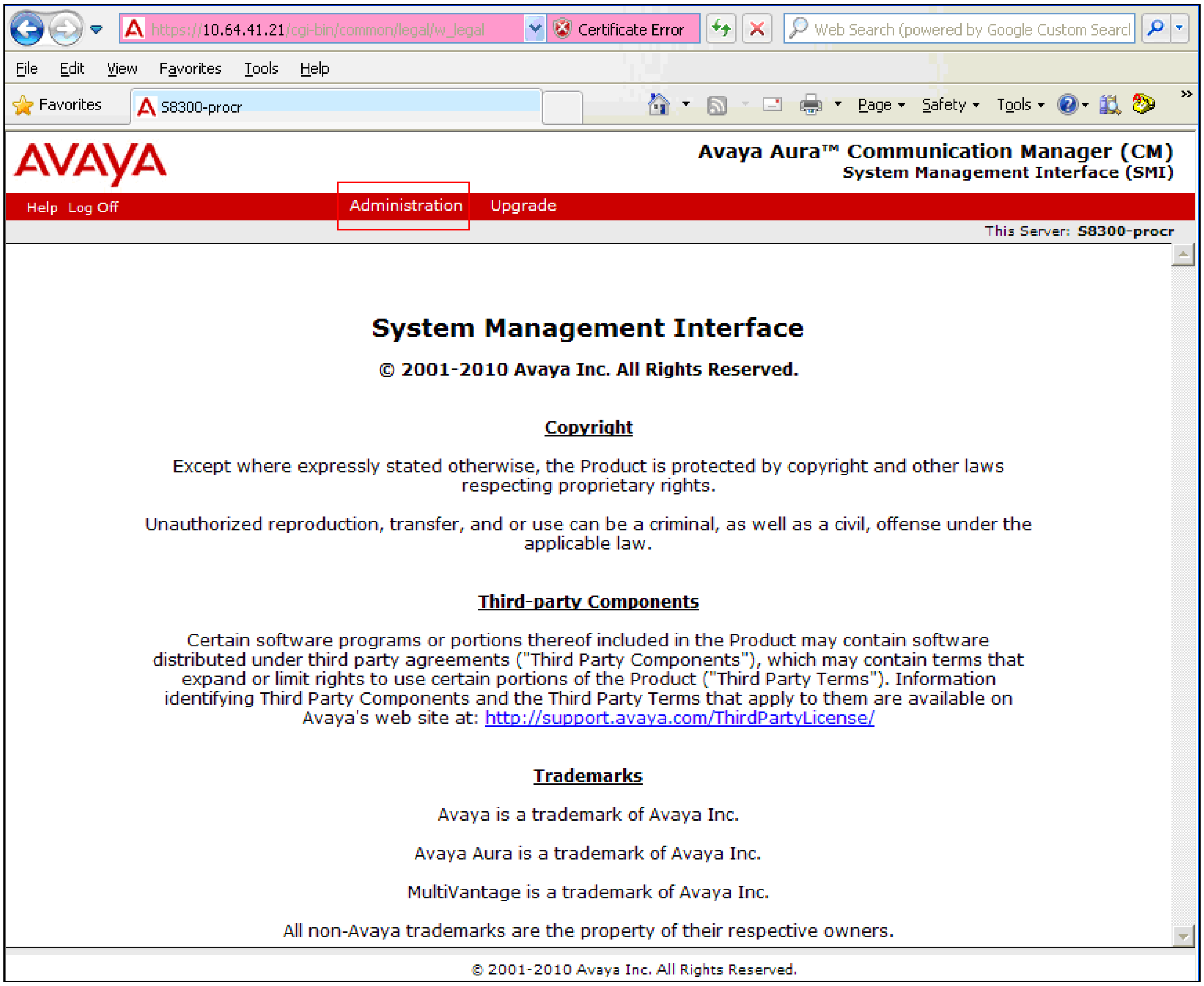
- Create member credentials (username/password) for a SFTP account
- Add survivable-processor on the main Avaya S8300D Server

- Save the translation for LSP on the main Avaya S8300D Server to push translation to the LSP Server

6.1.1. CDR credentials for SFTP

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

Select **Administration → Server (Maintenance)**.


https://10.64.41.21/cgi-bin/common/legal/w_legal
Certificate Error
Web Search (powered by Google Custom Searc
File Edit View Favorites Tools Help
Favorites
S8300-procr
Page Safety Tools
Avaya Aura™ Communication Manager (CM)
System Management Interface (SMI)
Help Log Off
Administration
Upgrade
This Server: S8300-procr

System Management Interface

© 2001-2010 Avaya Inc. All Rights Reserved.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights.

Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Third-party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them are available on Avaya's web site at: http://support.avaya.com/ThirdPartyLicense/

Trademarks

Avaya is a trademark of Avaya Inc.

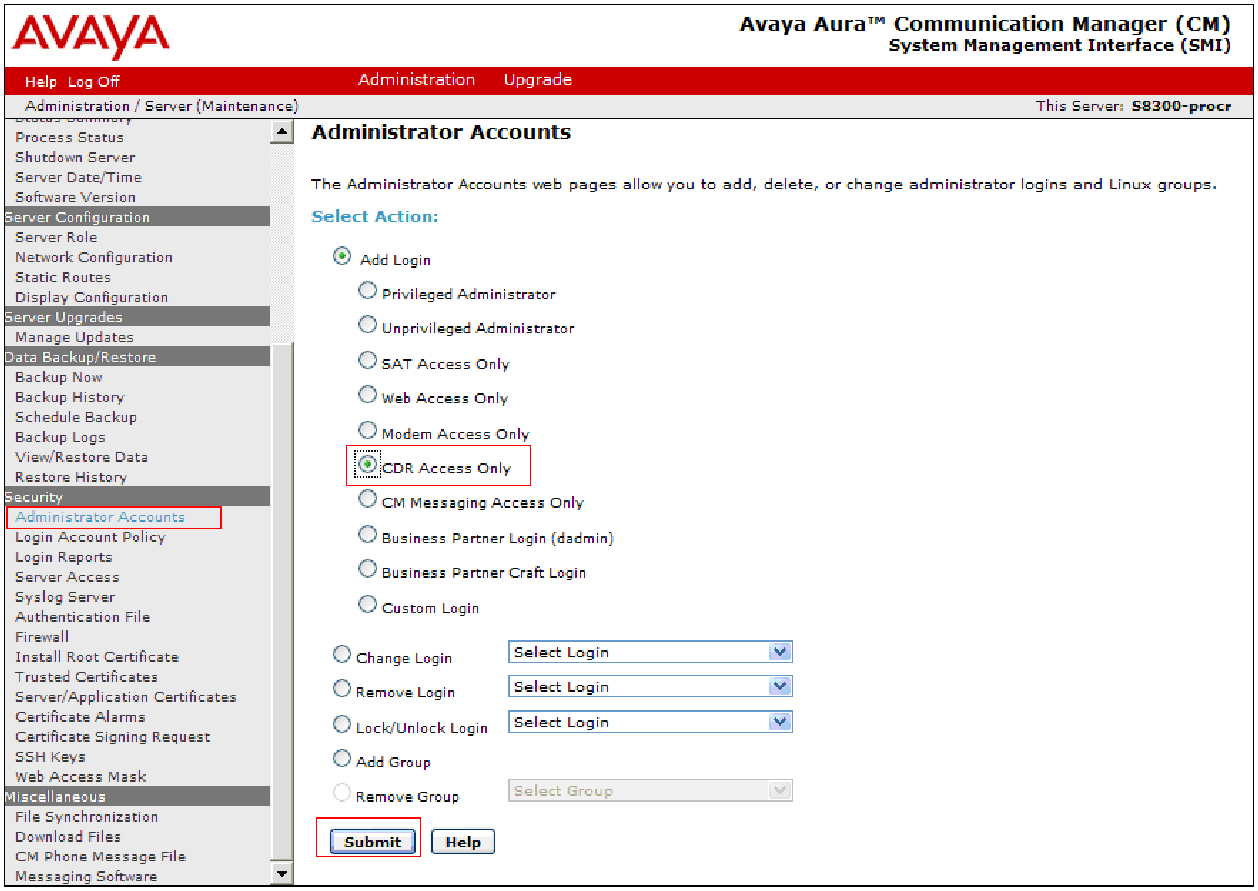
Avaya Aura is a trademark of Avaya Inc.

MultiVantage is a trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners.

© 2001-2010 Avaya Inc. All Rights Reserved.

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.**



Avaya Aura™ Communication Manager (CM)
System Management Interface (SMI)

Administrator Accounts

The Administrator Accounts web pages allow you to add, delete, or change administrator logins and Linux groups.

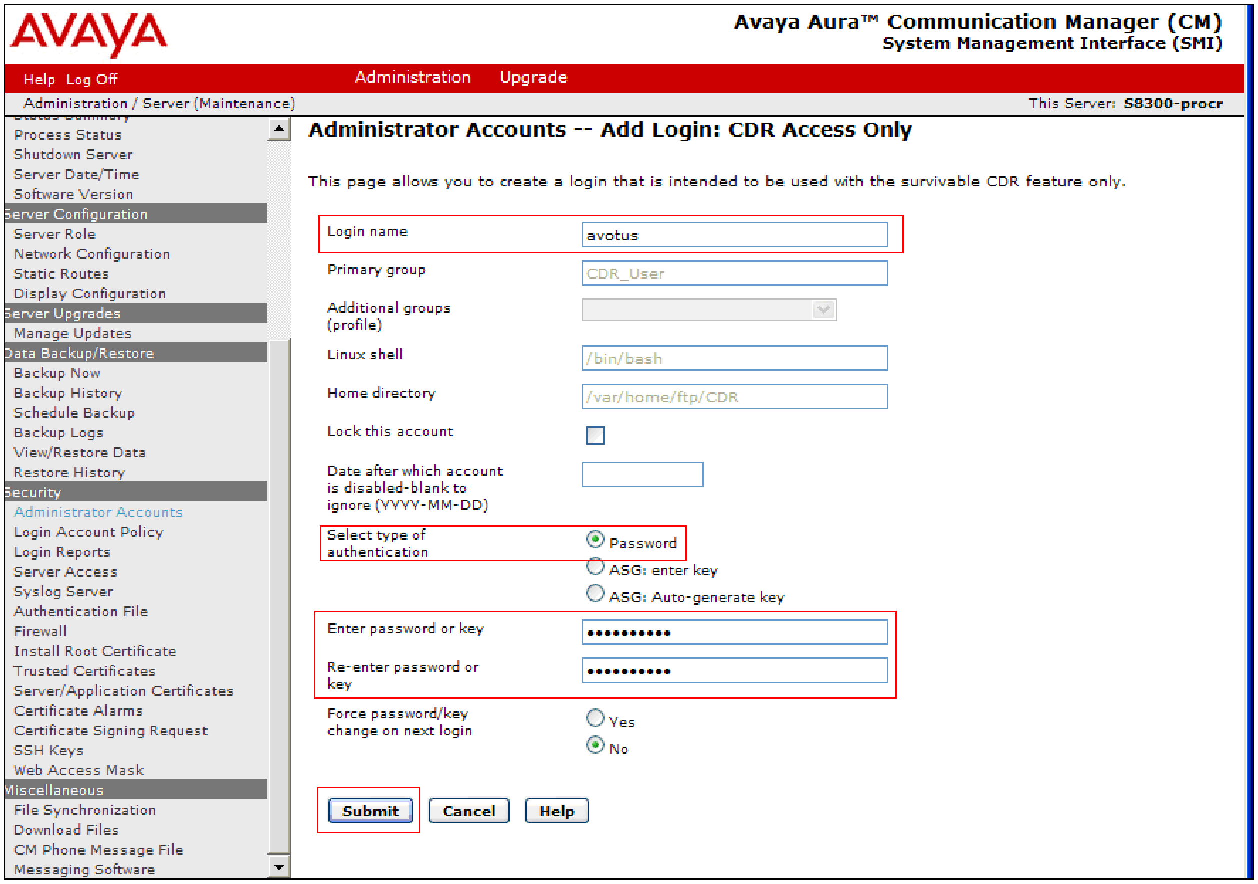
Select Action:

- ● Add Login
  - ○ Privileged Administrator
  - ○ Unprivileged Administrator
  - ○ SAT Access Only
  - ○ Web Access Only
  - ○ Modem Access Only
  - ● CDR Access Only
  - ○ CM Messaging Access Only
  - ○ Business Partner Login (dadmin)
  - ○ Business Partner Craft Login
  - ○ Custom Login
- ○ Change Login — Select Login
- ○ Remove Login — Select Login
- ○ Lock/Unlock Login — Select Login
- ○ Add Group
- ○ Remove Group — Select Group

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.



Administrator Accounts -- Add Login: CDR Access Only

This page allows you to create a login that is intended to be used with the survivable CDR feature only.

Login name	avotus
Primary group	CDR_User
Additional groups (profile)	
Linux shell	/bin/bash
Home directory	/var/home/ftp/CDR
Lock this account	□
Date after which account is disabled-blank to ignore (YYYY-MM-DD)	
Select type of authentication	● Password ○ ASG: enter key ○ ASG: Auto-generate key
Enter password or key	••••••••••
Re-enter password or key	••••••••••
Force password/key change on next login	○ Yes ● No

6.1.2. 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 4**.

```
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 6.1.1** and **6.1.2** are completed, run the **save translation all** command, so that the translation in Avaya S8300D Server will be pushed to the LSP licensed Avaya S8300D Server.

6.2. 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        avotus          9000
CDR2                     procr          0        rdtt            9001
```

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
```

7. 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 Avotus ICM 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 Avotus ICM was restarted. The LSP test was performed from the Avotus ICM using the SFTP command to the Avaya S8300 Server (LSP), and collecting the CDR records.

All executed test cases passed. Avotus ICM successfully collected the CDR records from Communication Manager via a 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, Avotus ICM was able to resume collecting CDR records after failure recovery including buffered CDR records for calls that were placed during the outages. Avotus ICM also successfully collected the CDR records from the Avaya S8300 Server using the SFTP command.

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 Avotus ICM 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 Avotus ICM, and verify the report's accuracy.

9. Conclusion

These Application Notes describe the procedures for configuring Avotus ICM to collect call detail records from Communication Manager running on Avaya Servers. Avotus ICM 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, Issue 6, August 2010, Document Number 555-245-205
[2] *Administering Avaya Aura™ Communication Manager* Release 6.0, Issue 6.0, June 2010, Document Number 03-300509.

The following ICM product documentation is available from Avotus. Visit http://www.avotus.com for company and product information.

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.