Application Notes for Veramark VeraSmart with Avaya Communication Manager - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for the Veramark VeraSmart call accounting software to successfully interoperate with Avaya Communication Manager.

Veramark VeraSmart is a call accounting software that interoperates with Avaya Communication Manager over the Avaya Reliable Session Protocol (RSP). Call records can be generated for various types of calls. Veramark VeraSmart collects, and processes the call records. The serviceability, Local Survivable Process (LSP) mode, and performance tests were conducted to assess the reliability of the solution.

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 overall objective of this interoperability compliance testing is to verify that the Veramark VeraSmart call accounting software can interoperate with Avaya Communication Manager 5.1. Veramark VeraSmart connects to Avaya Communication Manager over the local or wide area network using a CDR link running on RSP. Avaya Communication Manager is configured to send CDR records to Veramark VeraSmart using a specific TCP/IP port. The serviceability, LSP mode, and performance tests were conducted to assess the reliability of the solution.

Figure 1 illustrates a sample configuration that was used for the compliance test. The configuration consists of three Avaya Servers running Avaya Communication Manager. Site A is comprised of Avaya Communication Manager running on Avaya S8720 Servers with an Avaya G650 Media Gateway. Site B is comprised of Avaya Communication Manager running on an Avaya S8300 Server residing in an Avaya G700 Media Gateway. Each Avaya Communication Manager is connected to an IP network comprised of an Extreme Networks Summit 48 layer 3 switch. Veramark VeraSmart is running on a Windows 2003 Server remotely connected to the IP network through a firewall, and has a RSP session established to each Avaya Communication Manager to collect CDR records. Each system has trunks and phones to generate calls. Avaya 4600 Series IP Telephones, Avaya 9600 Series IP Telephones, Avaya 6400D Series Digital Telephones, and Avaya IP agent are registered to both Avaya S8720 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 S8300 Server with an Avaya G350 Media Gateway, which has connections to an Avaya 4600 Series IP Telephone and an Avaya 6400D Series Digital Telephone. The Avaya S8300 Server, installed with Local Survivable Processor (LSP) license, is setup as a LSP to Site A.

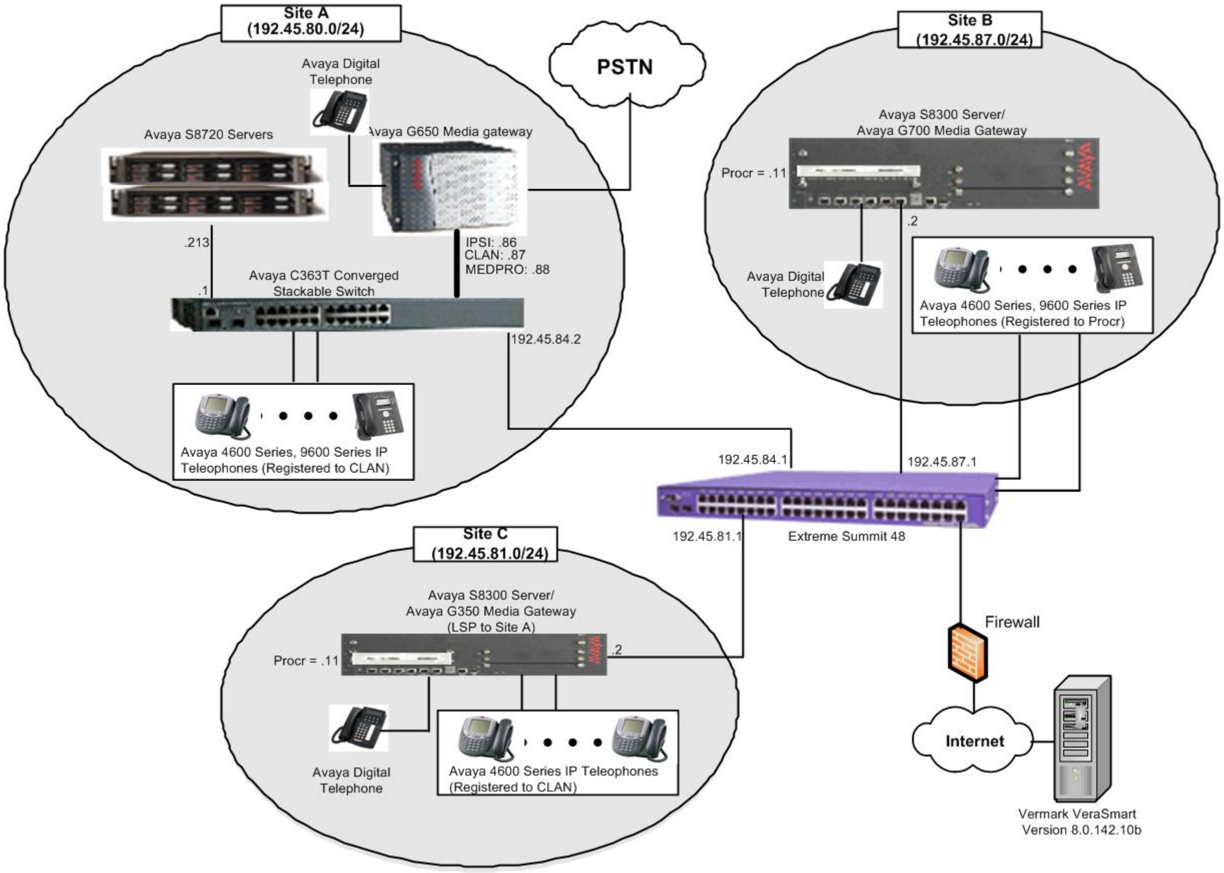


Figure 1. Test configuration of the VeraSmart with Avaya Communication Manager

2. Equipment and Software Validated

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

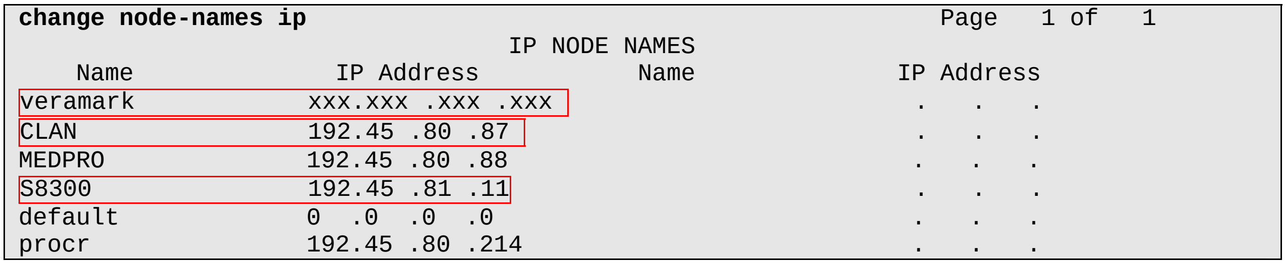
Equipment		Software
Avaya S8720 Servers		Avaya Communication Manager 5.1 (R015x.01.0.414.3 w/ SP 15962)
Avaya G650 Media Gateway		
	TN2312BP IPSI TN799DP CLAN TN2302AP MEDPRO	HW11 FW030 HW20 FW017 HW01 FW108
Avaya S8300 Server		Avaya Communication Manager 5.1 (R015x.01.0.414.3 w/ SP 15962)
Avaya G700 Media Gateway		28.17
Avaya S8300 Server (with LSP License)		Avaya Communication Manager 5.1 (R015x.01.0.414.3 w/ SP 15962)
Avaya G350 Media Gateway		26.31
Avaya 4600 Series IP Telephone		
	4620SW 4625SW	2.83 2.83
Avaya 9600 Series IP Telephone		
	9630 9650	1.5 1.5
Avaya 64xx Series Digital Telephones		
	6408D+ 6402D	- -
Analog Telephone		-
Avaya C363T Converged Stackable Switch (Layer 3)		4.5.14
Extreme Summit 48 Switch (Layer 3)		4.1.21
Veramark VeraSmart on Windows 2003 Server with Service Pack 2		8.0.142.10b

3. Configure Avaya Communication Manager

This section provides procedures for configuring the CDR feature in Avaya Communication Manager. All configuration changes in Avaya Communication Manager are performed through the System Access Terminal (SAT). These steps describe the procedure used for the Avaya S8720 Server. All steps are the same for the other Avaya Servers unless otherwise noted. Avaya Communication Manager will be configured to generate CDR records and send CDR records to the IP address of Veramark VeraSmart, using RSP over TCP/IP. For the Avaya S8720 Server, the CDR link originates at the IP address of the CLAN board, and terminates at VeraSmart. For the Avaya S8300 Server, the CDR link originates at the IP address of the local server (with node-name – "procr") and terminates at VeraSmart. The highlights in the following screens indicate the parameter values used during the compliance test.

Enter the **change node-names ip** command to create a new node name, for example, **veramark**. This node name is associated with the IP Address of VeraSmart. The IP address of S8300 is added in the IP NODE NAME form for the LSP test. The CLAN entry on this form was previously administered.

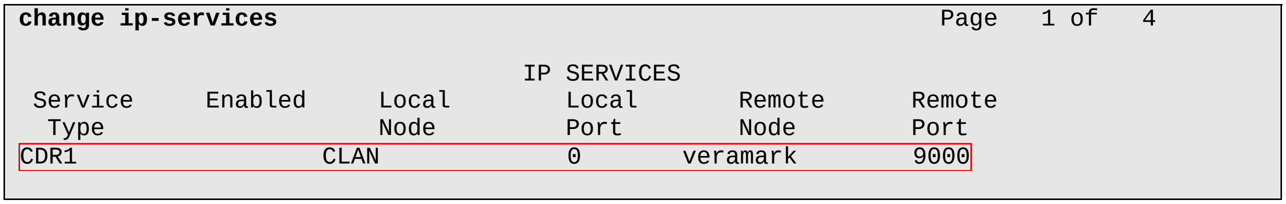
Note: *The IP address of Veramark VeraSmart is not displayed, since the test utilized a public IP address.*



```
change node-names ip                                            Page   1 of   1
                                 IP NODE NAMES
    Name                 IP Address             Name                IP Address
veramark               xxx.xxx .xxx .xxx                             .   .   .
CLAN                   192.45 .80 .87                                .   .   .
MEDPRO                 192.45 .80 .88                                .   .   .
S8300                  192.45 .81 .11                                .   .   .
default                0   .0   .0   .0                              .   .   .
procr                  192.45 .80 .214                               .   .   .
```

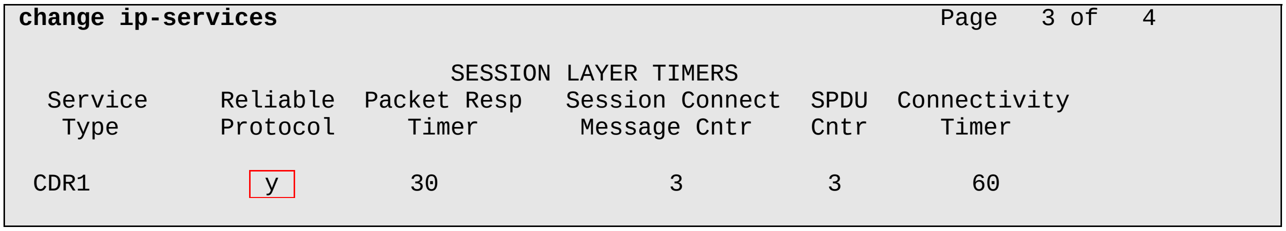
Enter the **change ip-services** command to define the CDR link to use RSP over TCP/IP. The following information should be provided:

- Service Type: CDR1 [If needed, a secondary link can be defined by setting Service Type to CDR2.]
- Local Node: **CLAN** [For Avaya S8720 Server, the Local Node is set to the node name of the CLAN board. If Avaya S8300 Server was utilized, set the Local Node to **procr**.]
- Local Port: 0 [The Local Port is fixed to 0.]
- Remote Node: **veramark** [The Remote Node is set to the node name defined previously.]
- Remote Port: **9000** [The Remote Port may be set to a value between 5000 and 64500 inclusive and must match the port configured in VeraSmart.]



```
change ip-services                                              Page   1 of   4

                                  IP SERVICES
 Service      Enabled     Local        Local        Remote       Remote
  Type                    Node         Port         Node         Port
CDR1                   CLAN            0        veramark         9000
```

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



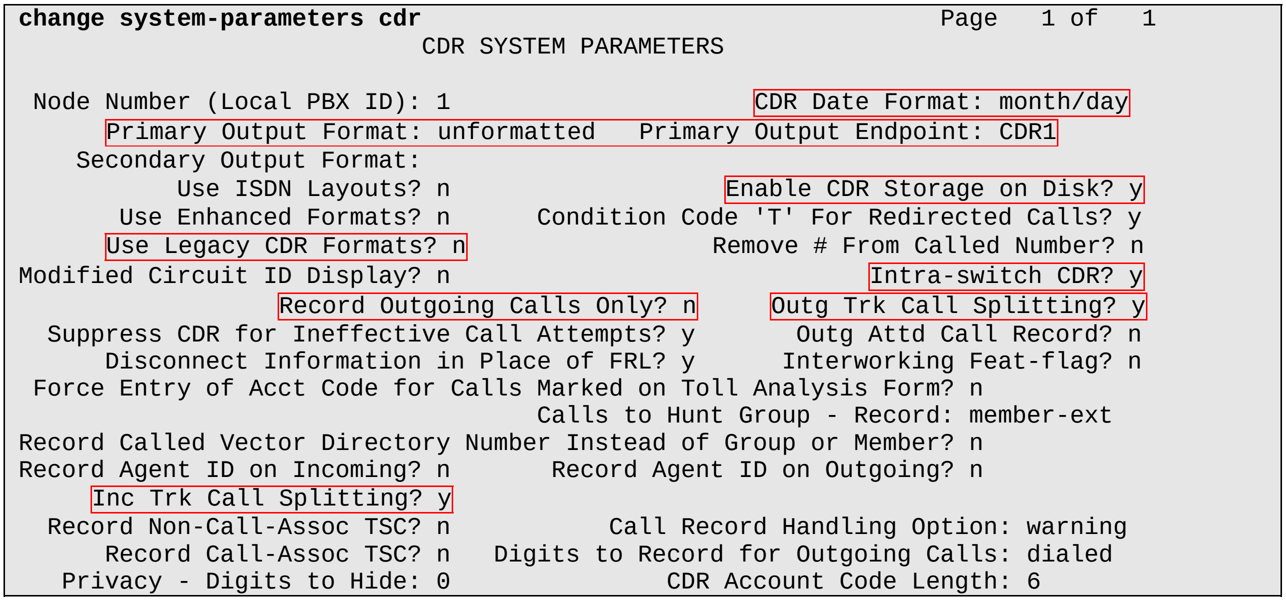
```
change ip-services                                              Page   3 of   4

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

 CDR1             y         30                3           3        60
```

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 [2] for a full explanation of each field. The test configuration used some of the more common fields described below.

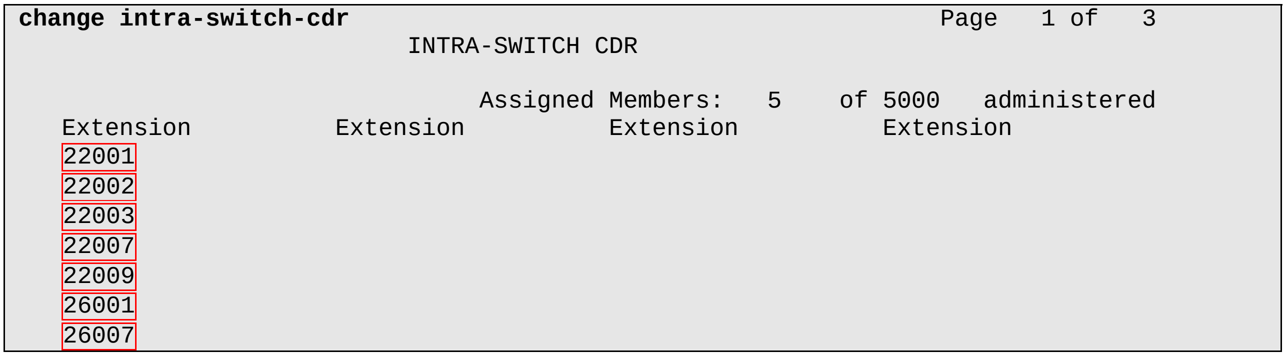
- Enable CDR Storage on Disk?: **y** [Enable the Survivable CDR feature. Default is **n**.]
- Use Legacy CDR Formats?: **n** [Allows CDR formats to use 5.x CDR formats. If the field is set to **y**, then CDR formats utilize the 3.x CDR formats.]
- Intra-switch CDR: **y** [Allows call records for internal 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   1
                            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? y
      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? y      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? n       Record Agent ID on Outgoing? n
     Inc Trk Call Splitting? y
  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
```

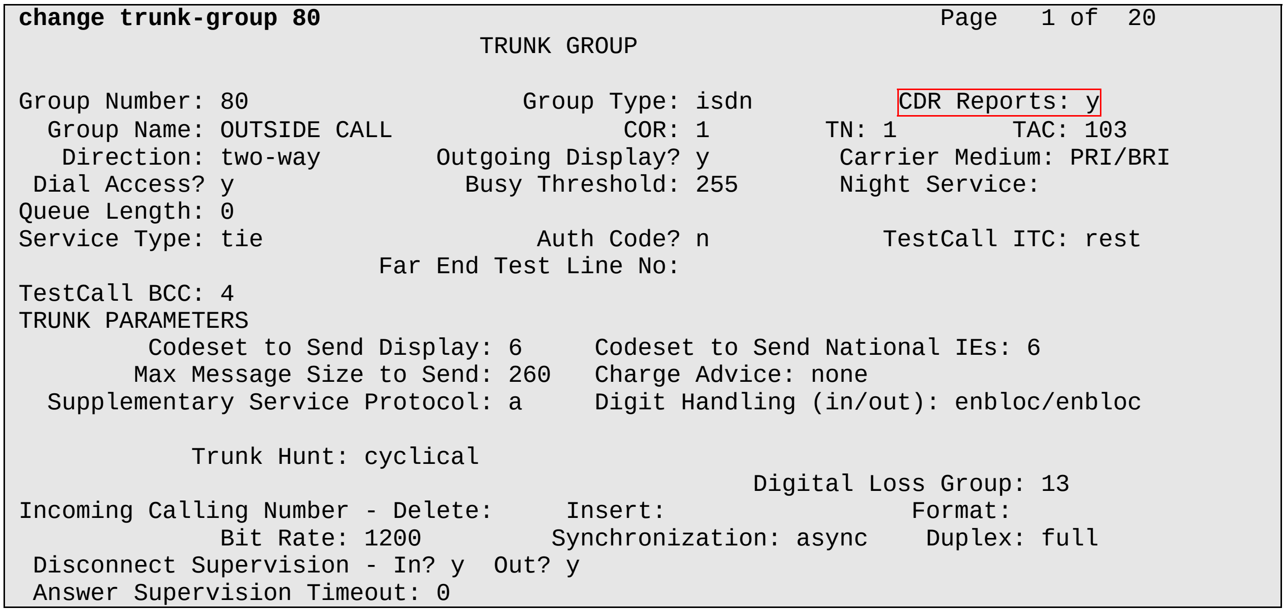
If the Intra-switch CDR field is set to **y** on Page 1 of the system-parameters cdr form, then enter the **change intra-switch-cdr** command to define the extensions that will be subject to call detail records. In the Assigned Members field, enter the specific extensions whose usage will be tracked.

Note: *To simplify the process of adding multiple extensions in the Extension field, 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:   5    of 5000   administered
   Extension            Extension            Extension            Extension
   22001
   22002
   22003
   22007
   22009
   26001
   26007
```

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 80                                           Page   1 of  20
                                TRUNK GROUP

Group Number: 80                   Group Type: isdn          CDR Reports: y
  Group Name: OUTSIDE CALL                COR: 1        TN: 1        TAC: 103
   Direction: two-way        Outgoing Display? y         Carrier Medium: PRI/BRI
 Dial Access? y                Busy Threshold: 255       Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n            TestCall ITC: rest
                         Far End Test Line No:
TestCall BCC: 4
TRUNK PARAMETERS
         Codeset to Send Display: 6     Codeset to Send National IEs: 6
        Max Message Size to Send: 260   Charge Advice: none
  Supplementary Service Protocol: a     Digit Handling (in/out): enbloc/enbloc

            Trunk Hunt: cyclical
                                                   Digital Loss Group: 13
Incoming Calling Number - Delete:     Insert:                Format:
              Bit Rate: 1200        Synchronization: async    Duplex: full
 Disconnect Supervision - In? y  Out? y
 Answer Supervision Timeout: 0
```

4. Configure the Avaya LSP Solution

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

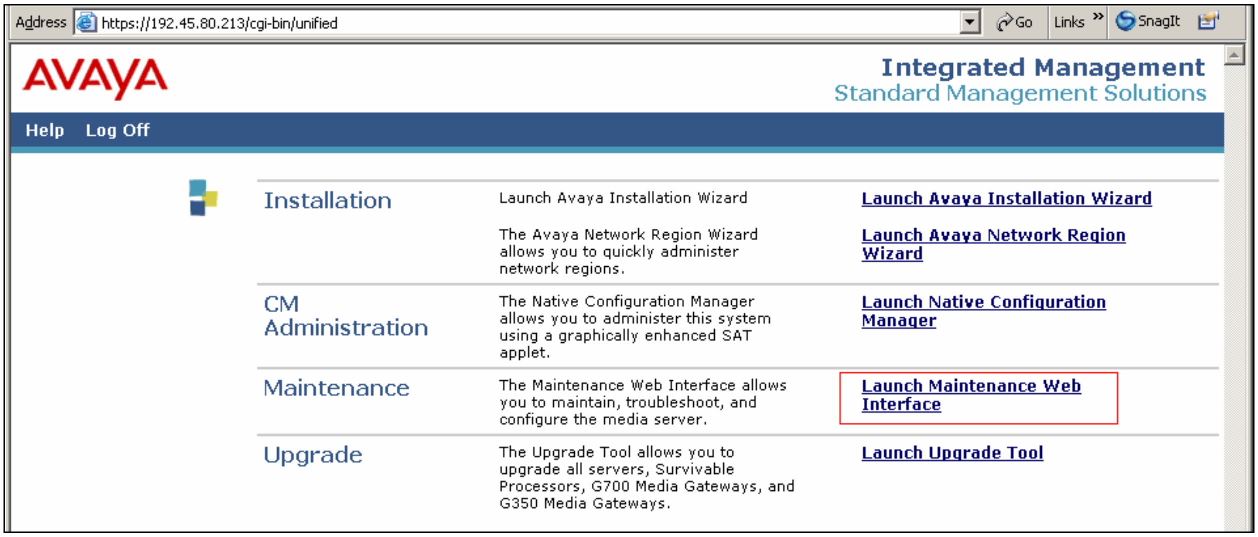
4.1. Configure the S8720 Server with G650 Media Gateway for the Avaya LSP Solution

This section describes how to configure the S8720 Server with a G650 Media Gateway for the Avaya LSP CDR Solution. The following steps must be performed:

- Create member credentials (username/password) for a sftp account
- Change "survivable-processor <assigned Survivable Processor node-name>" form
- Save the translation for LSP

4.1.1. CDR credentials for sftp

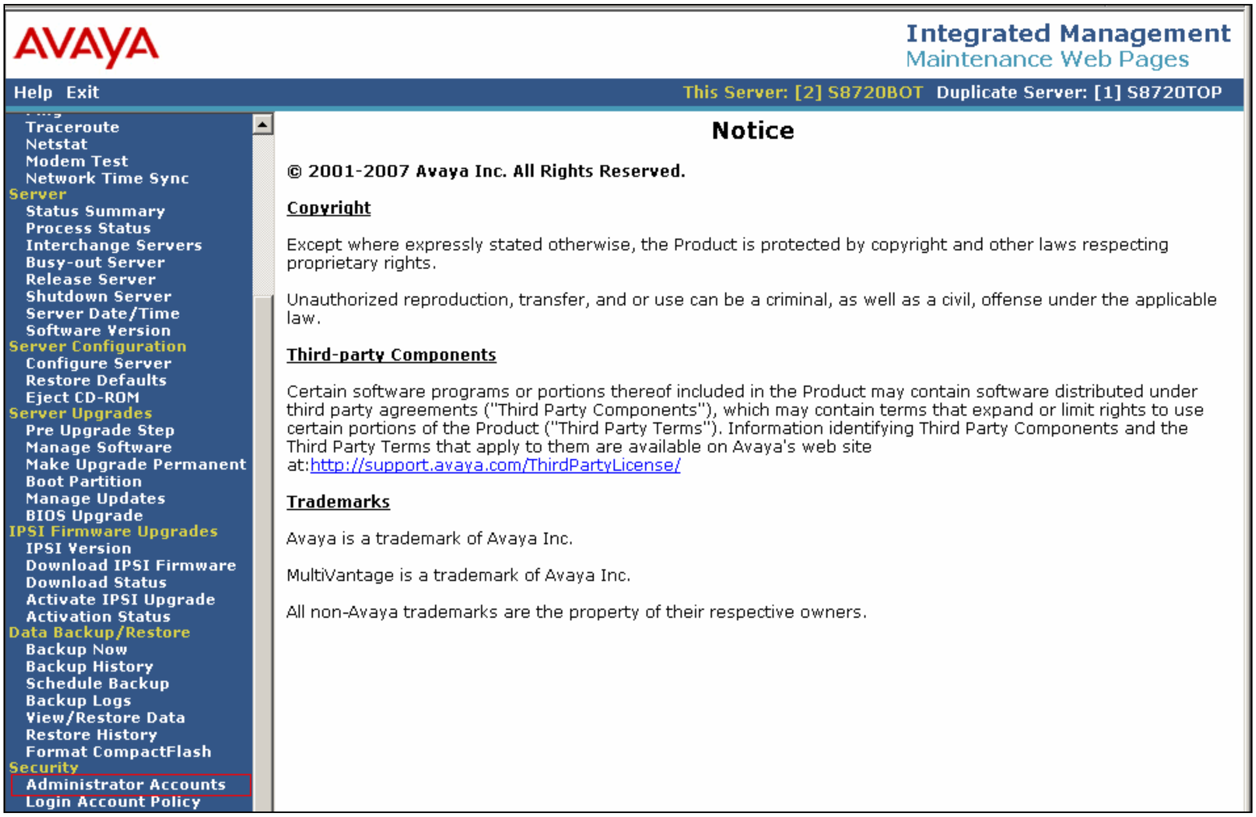
To create credentials, enter https://<IP address of Avaya S8720 Server> in the URL, and log in with the appropriate credentials for accessing the Integrated Management Standard Management Solutions pages. Select the **Launch Maintenance Web Interface** link.



Address https://192.45.80.213/cgi-bin/unified
Go
Links
SnagIt
AVAYA
Integrated Management
Standard Management Solutions
Help
Log Off

Installation	Launch Avaya Installation Wizard	Launch Avaya Installation Wizard
	The Avaya Network Region Wizard allows you to quickly administer network regions.	Launch Avaya Network Region Wizard
CM Administration	The Native Configuration Manager allows you to administer this system using a graphically enhanced SAT applet.	Launch Native Configuration Manager
Maintenance	The Maintenance Web Interface allows you to maintain, troubleshoot, and configure the media server.	Launch Maintenance Web Interface
Upgrade	The Upgrade Tool allows you to upgrade all servers, Survivable Processors, G700 Media Gateways, and G350 Media Gateways.	Launch Upgrade Tool

Select the **Administrator Accounts** link under the Security section.



Notice

© 2001-2007 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/

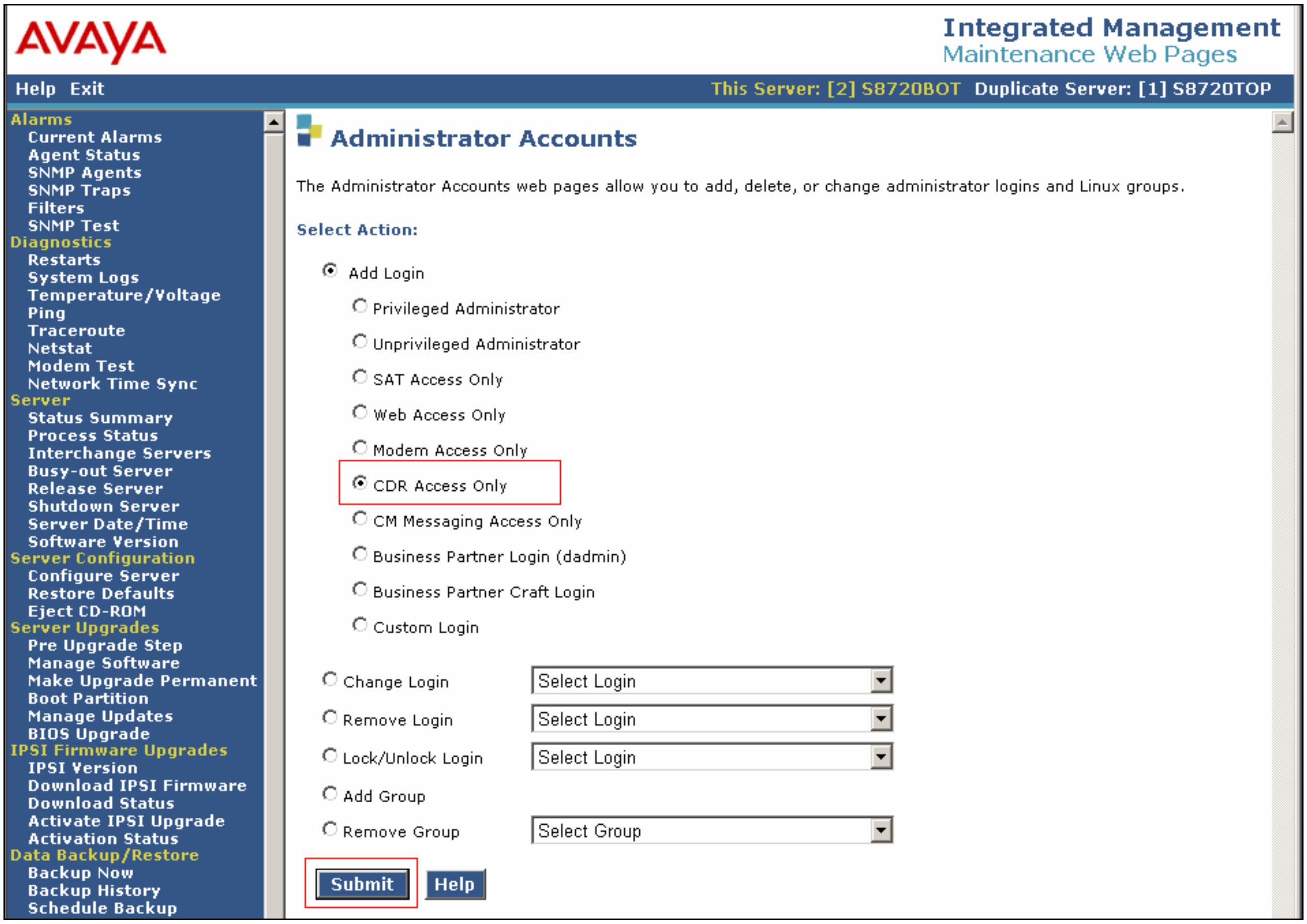
Trademarks

Avaya is a trademark of Avaya Inc.

MultiVantage is a trademark of Avaya Inc.

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

In the Administrator Accounts page, check **CDR Access Only** box under the Add Login section. Select **Submit**



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

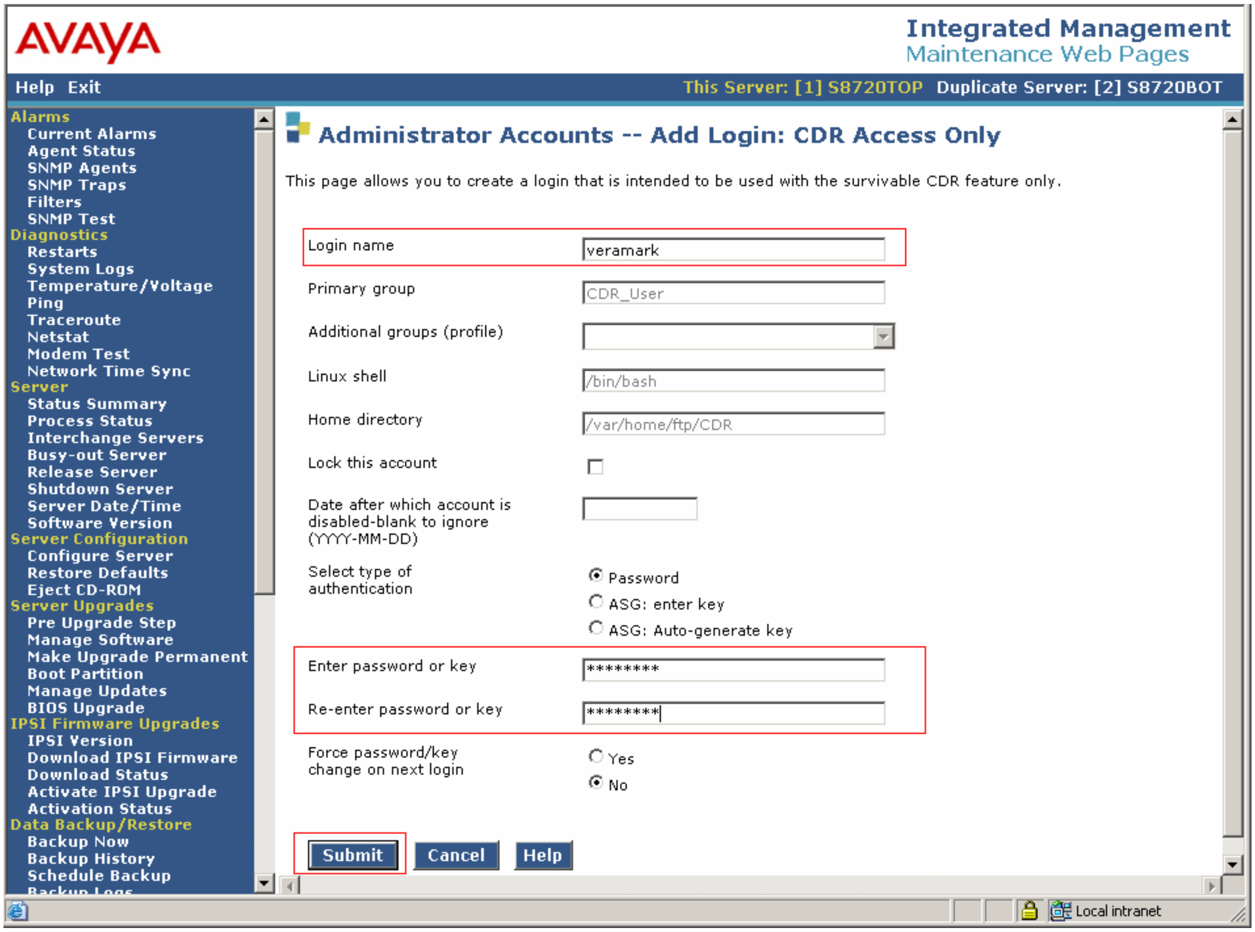
○ Change Login — Select Login
○ Remove Login — Select Login
○ Lock/Unlock Login — Select Login
○ Add Group
○ Remove Group — Select Group

In the Administrator Accounts –Add Login: CDR Access Only page, provide the following information:

- Login name
- Enter password or key
- Re-enter password or key

The above credentials will be utilized to access the LSP licensed Avaya Communication Manager.

Click on **Submit**



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	veramark
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

Submit Cancel Help

4.1.2. Survivable-Processor Form

Enter the **change survivable-processor S8300** command, where **S8300** is an LSP licensed Avaya S8300 Server, configured in **Section 3**. Make sure that the Enabled field is set to **o** (overwrite), and the Store to dsk field is to **y**.

```
change survivable-processor S8300                               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
```

After **Section 4.1.1** and **4.1.2** are completed, run either the **save translation all** or **save translation lsp** command, so that the translation in Avaya S8720 Server will be pushed to the LSP licensed Avaya S8300 Server.

To confirm whether the translation is pushed to the LSP licensed Avaya Communication manager, execute the **list survivable-processor** command, and check the last Translations Updated field. The following shows a sample screen, resulted from performing the above command.

```
list survivable-processor

                             SURVIVABLE PROCESSORS
 Name           Type        IP Address     Reg LSP          Translations     Net
                                               Act          Updated          Rgn

 S8300           LSP        192.45 .81 .11  y   n           22:00 9/8/2008    1
```

4.2. Verification from the Avaya S8300 Server for the Avaya LSP Solution

This section describes how to verify the Avaya LSP CDR solution from the Avaya S8300 Server. Enter the **display ip-services** command. Notice that the Local Node field is changed to **procr**.

```
display  ip-services                                              Page   1 of   4

                                   IP SERVICES
 Service     Enabled     Local        Local       Remote      Remote
  Type                   Node         Port        Node        Port
CDR1                    procr         0       veramark        9000
```

Enter the **display survivable-processor S8300** command, and verify that the survivable-processor S8300 form in Avaya S8720 and S8300 Servers are identical.

```
display survivable-processor S8300                              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
```

4.3. Verification from the Avaya Media Gateway for the Avaya LSP Solution

This section describes how to verify the Avaya LSP CDR solution from the Avaya G350 Media Gateway. Telnet into the media gateway and run the **show mgc** command. As the following screen showed, the active controller has changed from 192.45.80.87 (prior to LSP) to 192.45.81.11 (post LSP).

```
G350-001(super)# sh mgc

CALL CONTROLLER STATUS
-------------------------------------------
Registered          : YES
Active Controller   : 192.45.81.11
H248 Link Status    : UP
H248 Link Error Code: 0x0

CONFIGURED MGC HOST
---------------------
192.45.80.87
192.45.81.11
-- Not Available --
-- Not Available --
```

5. Configure Veramark VeraSmart

This section describes the operation of Veramark VeraSmart. The VeraSmart connects to Avaya Communication Manager via RSP over the TCP/IP port. CDR data is sent from Avaya Communication Manager (CLAN port) into the VeraSmart where the raw data is transformed into call records, which are then immediately available for reporting. Veramark installs, configures, and customizes the VeraSmart application for their customers; therefore the details are not included in these Application Notes.

The following documents are available for configuring interfaces to communicate with Avaya Communication Manager.

- VeraSmart Reliable Session Protocol Interface Setup – Reference [3]
- VeraSmart Avaya Survivable CDR Interface Setup – Reference [4]

6. Interoperability Compliance Testing

The compliance test included feature, serviceability, performance, and LSP testing. The feature testing evaluated the ability of VeraSmart to collect and process CDR records for various types of calls. The unformatted format was utilized during the compliance test. The serviceability test introduced failure scenarios to see if the VeraSmart can resume CDR collection after recovery. The performance test utilized bulk call volumes to generate a substantial amount of CDR records. The Avaya LSP solution was tested by removing the CLAN board in the Avaya G650 Media Gateway.

6.1. General Test Approach

The general test approach was to manually place intra-switch and inter-switch calls, inbound trunk and outbound trunk calls to and from telephones attached to the Avaya Servers, and verified that VeraSmart collected the CDR records and properly classified and reported the attributes of the call. For serviceability testing, physical and logical links were disabled/re-enabled, Avaya Servers were reset and VeraSmart was restarted. The LSP test was performed from VeraSmart using the sftp command to Avaya S8300 Server (LSP) to collect the CDR records. For performance testing, a call generator was used to place calls over an extended period of time.

6.2. Test Results

All executed test cases passed. Veramark VeraSmart successfully collected the CDR records from Avaya 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, Veramark VeraSmart was able to resume collection of CDR records after failure recovery including buffered CDR records for calls that were placed during the outages. Veramark VeraSmart also successfully collected the CDR records from the Avaya S8300 Server using the sftp command. Performance tests verified that Veramark VeraSmart could collect call records during a sustained, high volume of calls.

7. Verification Steps

The following steps may be used to verify the configuration:

- On the SAT of the Avaya S8720 Server, enter the **status cdr-link** command and verify that the CDR link state is up.
- Place a call and verify that Veramark VeraSmart received CDR records for the call. Compare the values of the data fields in the CDR record with the expected values, and verify that they match.
- Place internal, inbound trunk, and outbound trunk calls to and from various telephones, generate an appropriate report in Veramark VeraSmart, and verify the report's accuracy.

8. Support

Technical support for VeraSmart can be obtained by contacting Veramark via email at tech_support@veramark.com or by calling 585 381-0115.

9. Conclusion

These Application Notes describe the procedures for configuring Veramark VeraSmart to collect call detail records from Avaya Communication Manager running on Avaya Servers. Veramark VeraSmart successfully passed all compliance testing.

10. References

This section references the Avaya and Veramark documentation that are relevant to these Application Notes.

The following Avaya product documentation can be found at http://support.avaya.com .
[1] *Administrator Guide for Avaya Communication Manager*, Issue 4, January 2008, Document Number 03-300509.
[2] *Feature Description and Implementation For Avaya Communication Manager*, Issue 6, January 2008, Document Number 555-245-205

The following documents are utilized for installation and configuration of Veramark VeraSmart.
[3] VeraSmart Reliable Session Protocol Interface Setup
[4] VeraSmart Avaya Survivable CDR Interface Setup

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.