Avaya Solution & Interoperability Test Lab

# Application Notes for VeraSMART eCAS Call Accounting with Avaya Communication Server 1000 – Issue 1.0

## Abstract

These Application Notes describe the configuration steps required for the VeraSMART eCAS Call Accounting software to successfully interoperate with Avaya Communication Server 1000 Release 6.0.

VeraSMART is a call accounting software that utilizes the File Transfer Protocol or Secure File Transfer Protocol to log into Avaya Communication Server 1000 Release 6.0, to retrieve and to transfer raw SIP CDR data to VeraSMART, where the raw data is transformed into call records and made available for their end customers.

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.


©2010 Avaya Inc. All Rights Reserved.

# 1. Introduction

The overall objective of this interoperability compliance testing is to verify that the VeraSMART eCAS Call Accounting software can collect raw Call Detail Records (CDR) data output from Avaya Communication Server 1000 Data Buffer and Access (DBA) tool kits. The serviceability test was conducted to assess the reliability of the solution.

## 1.1. Interoperability Compliance Testing

The focus of the interoperability compliance testing was primarily on verifying whether the VeraSMART eCAS Call Accounting software can establish an FTP/SFTP session with Avaya Communication Server 1000 Release 6.0 to collect raw data and automatically populate this data into their reporting system.

## 1.2. Support

Technical support for VeraSMART can be obtained by contacting Veramark via email at tech_support@veramark.com or by calling 585-249-3310.

# 2. Reference Configuration

**Figure 1** illustrates the test configuration used during the compliant testing event between the Avaya CS1000 rel.6.0 and the VeraSMART rel 9.1.171.11a.

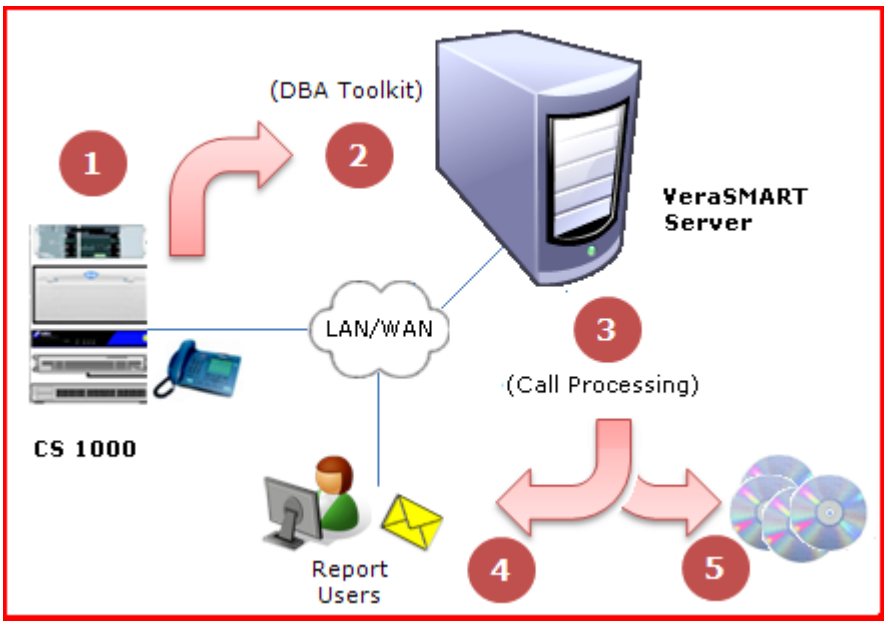



**Figure 1: Overview**


©2010 Avaya Inc. All Rights Reserved.

# 3. Equipment and Software Validated

| System | Software/Loadware Version |
|---|---|
| CS1000 | • Call Server (CPPM): 6.00RJ<br>• Signalling Server (CPPM): 6.00.18<br>• SIP Line Gateway (HP DL320) |
| Call Pilot | • CallPilot (600r): 05.00.41.29 |
| SIP softphones<br>IP phones | • 02.02.16.00<br>• 2050PC: 3.02.0045 |
| VeraSMART | • 9.1.171.11a |

# 4. Configure CS 1000 DBA CDR/Traffic Collector

This section describes the steps to configure CS 1000 Data Buffer and Access (DBA) CDR/Traffic Collector.

## 4.1. Call Server configuration settings

The CS 1000 Call Server must be configured to enable network collection of CDR or Traffic data. Note that the DBA package must also be enabled on the CS 1000 system.

1. Log into the Call Server using the admin username/password: admin/Escspv_123.
2. Enter command **ld 15.**
3. Enter **CDR_DATA** in response to TYPE.
4. Enter **YES** in response to the **CDR** prompt for **BDI** (Buffer Data Interface for CDR) (if not already yes).
5. Enter command **ld 117**. The => prompt will be shown indicating that the system is ready to accept input.
6. To enable collection of CDR data, enter **ENL BUF CDR.**

   To enable collection of Traffic data, enter **ENL BUF TRF.**
7. Corresponding operations are available to disable each feature (e.g. **DIS BUF CDR** and **DIS BUF TRF**).
8. To view the status of buffering data enter **STAT BUF.**
9. Enter command **ld 17.**


©2010 Avaya Inc. All Rights Reserved.

**LD 17**

**REQ CHG**

**TYPE PARM**

**FCDR NEW**

## 4.2. General Security Settings - CS 1000 Call Server and DBA CDR/Traffic collector

Live CDR/Traffic data and the user name and password information required for starting a live data collection are sent to the Call Server in an encrypted format using a proprietary encryption method. The CS 1000 DBA CDR/Traffic Collector supports both standard FTP and secure FTP (SFTP) for downloading the uncollected data from the Call Server (data collected while the Developer application is unavailable to receive data). Additional FTP/SFTP details are provided in **Section 6.1** of this document.

There are a number of security features on the Call Server which can impact access by the CS 1000 DBA CDR/Traffic Collector as follows:

One such feature is the configuration state of Unsecure and Secure Shells on the Call Server in Overlay 117. To configure Secure/Unsecure Shells, login to the Call Server using the admin username and password, and enter **ld 117**.

- To configure Secure Shells, enter **ENL/DIS SHELLS SECURE**
- To configure Unsecure shells, enter **ENL/DIS SHELLS UNSECURE**

## 4.3. Configure IPSec Security Settings - CS 1000 Call Server release 6.0

IPSec configurations for a Call Server can be performed through Unified Communications Manager (UCM) only. The configuration procedure is provided below.

Launch CS1000 Web Portal using IE to launch web CS1000 portal at http:// <IP address of UCM>.
Default username/password: admin/Escspv_123.

1. Login to the UCM server that manages the CS 1000 system from which the CDR/Traffic data is to be collected.


©2010 Avaya Inc. All Rights Reserved.

2. In UCM Navigator, click on **IPSec** under **CS 1000 Services** as shown below in **Figure 2**.

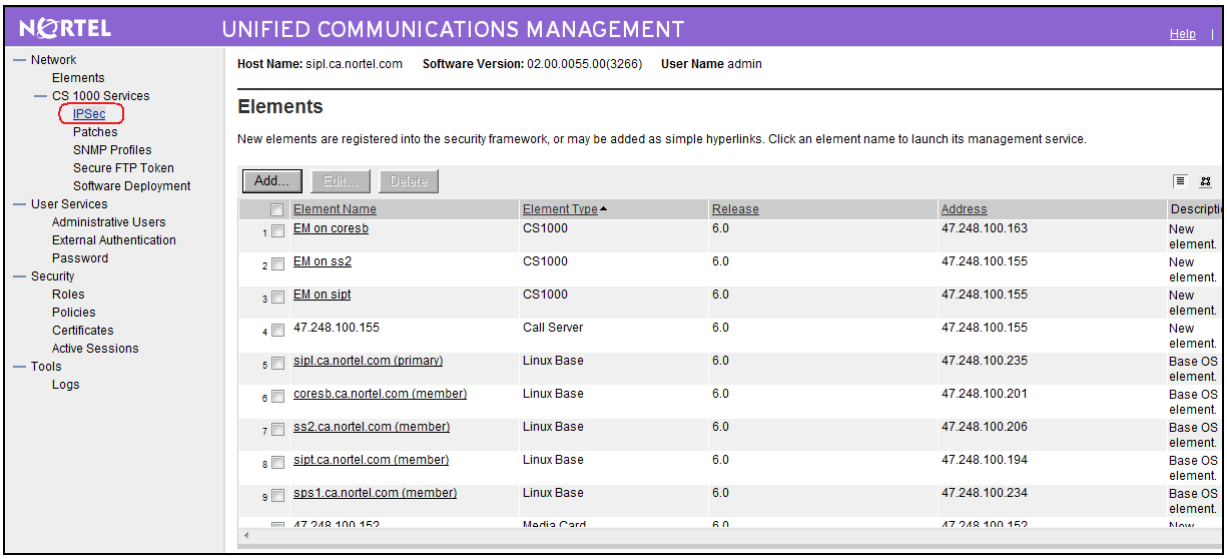



**Figure 2: IPSec on UCM Home page**

3. The Call Server, from which CDR/Traffic data will be collected, is available under the Targets section as shown in **Figure 3** below. Click on the IP Address of the Call Server to open the IPSec Configuration Details page.

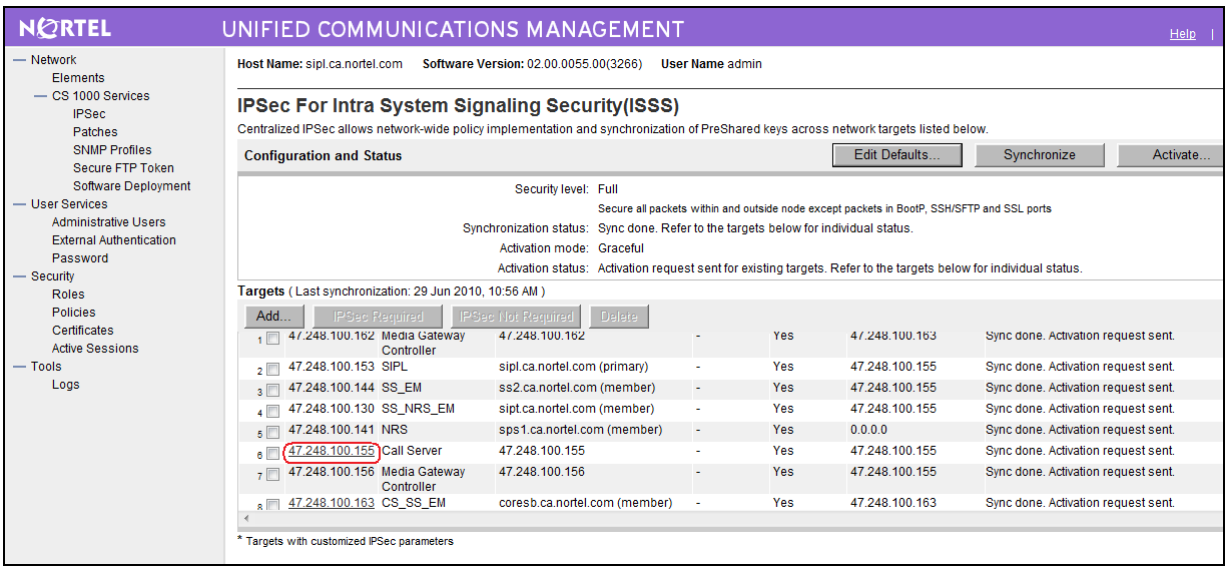



**Figure 3: IPSec for Intra System Signaling Security**


©2010 Avaya Inc. All Rights Reserved.

4. On the IPSec Configuration Details page, select the desired security level (**Full/Optimal**), provide the PreShared Key (PSK), click on the **Save and Synchronize** button as shown in **Figure 4** below to save the configuration information.

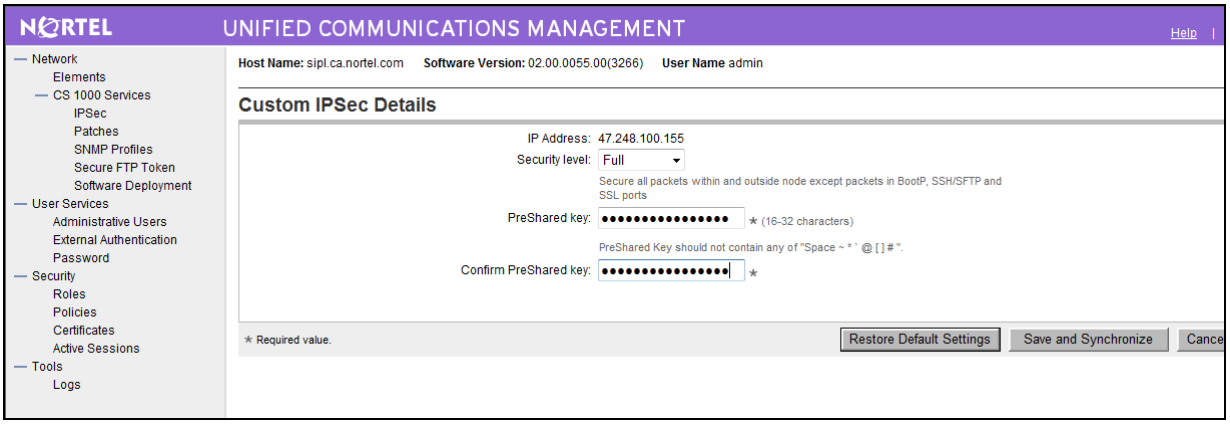



**Figure 4: Custom IPSec Details**

5. If synchronization process is successful, the Sync/Activation status for the Call Server is changed to **Sync done Activation required** as shown in **Figure 5**. In order for the change to take affect, activation is required.

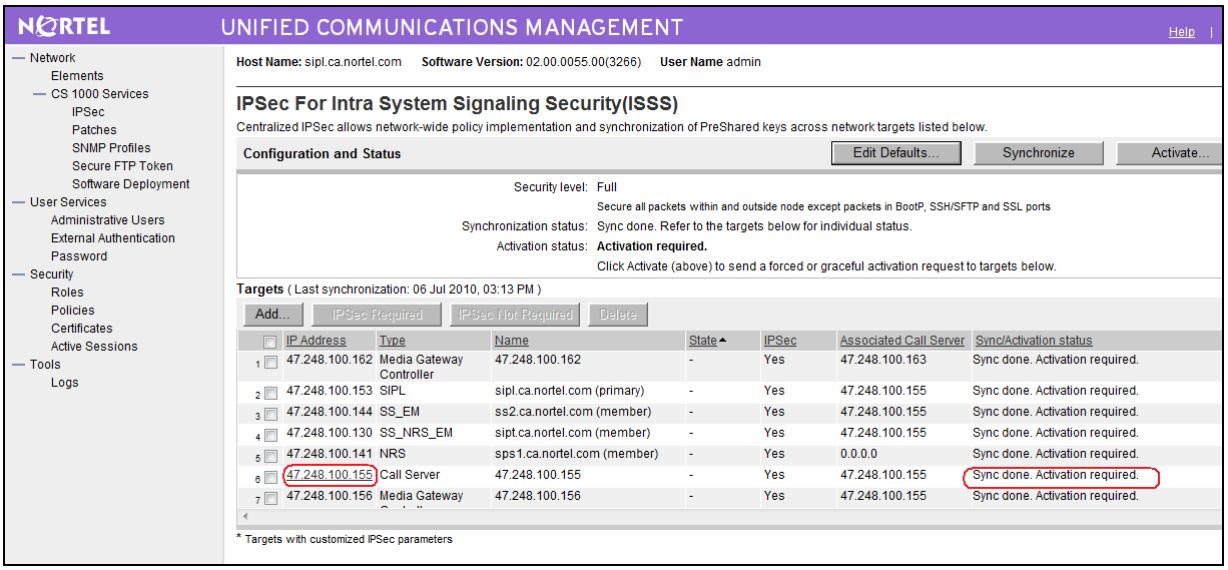



**Figure 5: IPSec Synchronization**


©2010 Avaya Inc. All Rights Reserved.

6. Click on the **Activate** button as shown in **Figure 6**. The Activation Detail page will appear as shown in **Figure 7**.

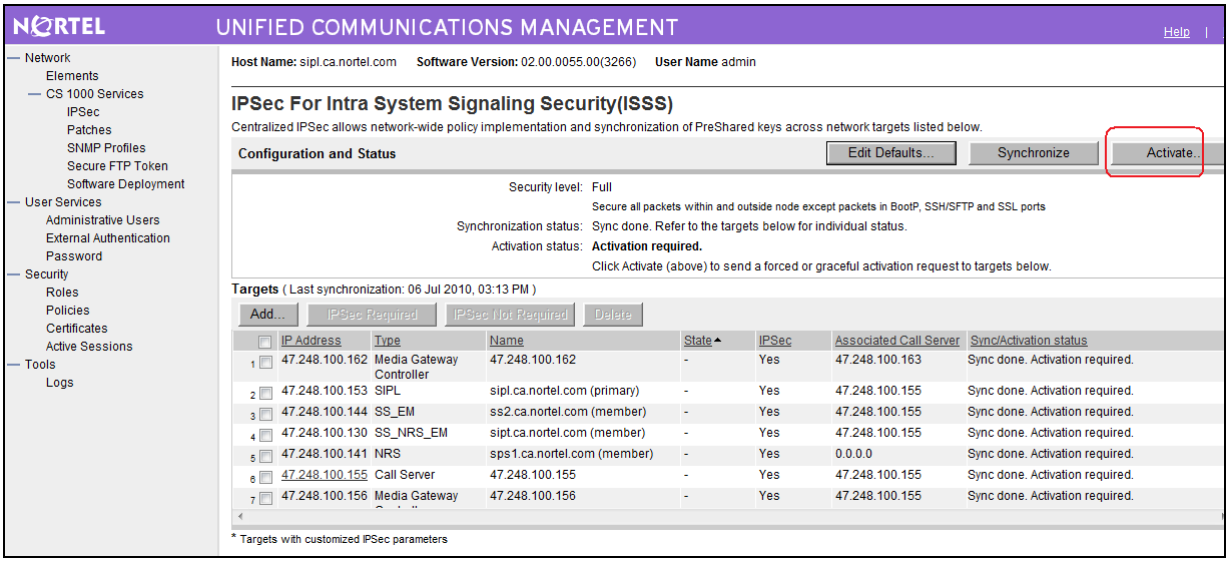



**Figure 6: IPSec Activation**

7. On the IPSec Activation Details page, choose the **Graceful** option as the Activation type and click on **Activate** button as shown in **Figure 7** below.

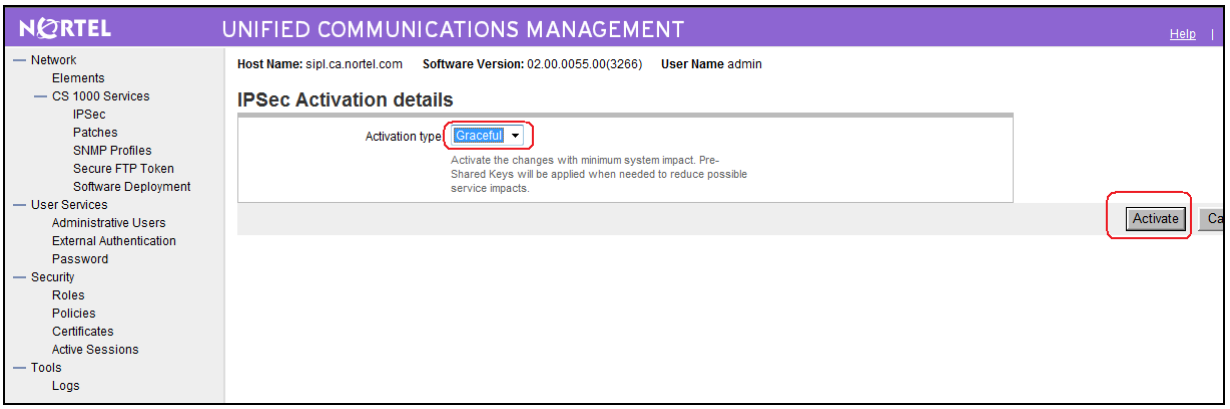



**Figure 7: Activation Type**


©2010 Avaya Inc. All Rights Reserved.

8. The Sync/Activation status of the Call Server will be changed to **Sync done. Activation request sent** as shown in **Figure 8**.

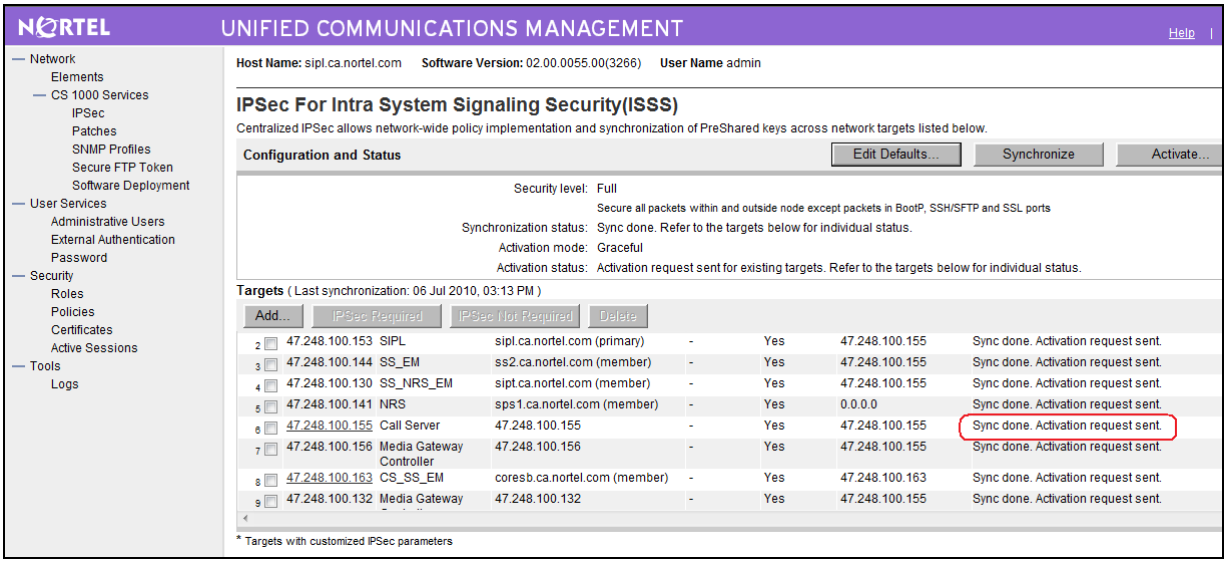



**Figure 8: Sync done. Activation request sent**

## 4.4. IPSEC Security Settings - VeraSMART's Windows OS Server or PC

To configure a PC running the DBA CDR/Traffic Collector as a trusted target in a Release 6.0 Call Server, please follow the steps below:

1. Login to the UCM server that manages the CS 1000 system from which the CDR/Traffic data is to be collected.
2. In UCM Navigator, click on **IPSec** under **CS 1000 Services**.
3. The Call Server, from which CDR/Traffic data will be collected, is available under the Targets section.


©2010 Avaya Inc. All Rights Reserved.

4. Click on the **Add** button under the Targets section as shown in **Figure 9**.

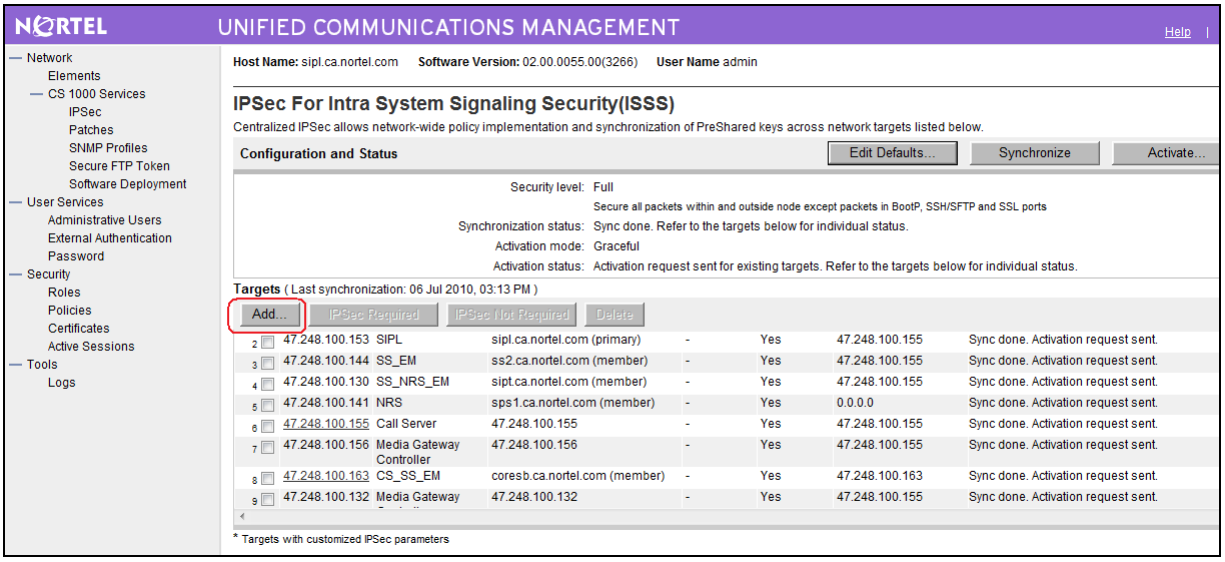



**Figure 9: New IPSec target addition**

5. On the New Manual IPSec Target page, enter the IP Address of the PC running the DBA CDR/Traffic Collector and provide the friendly name, then select **IPSec required** and click on the **Save** button as shown in **Figure 10** below.

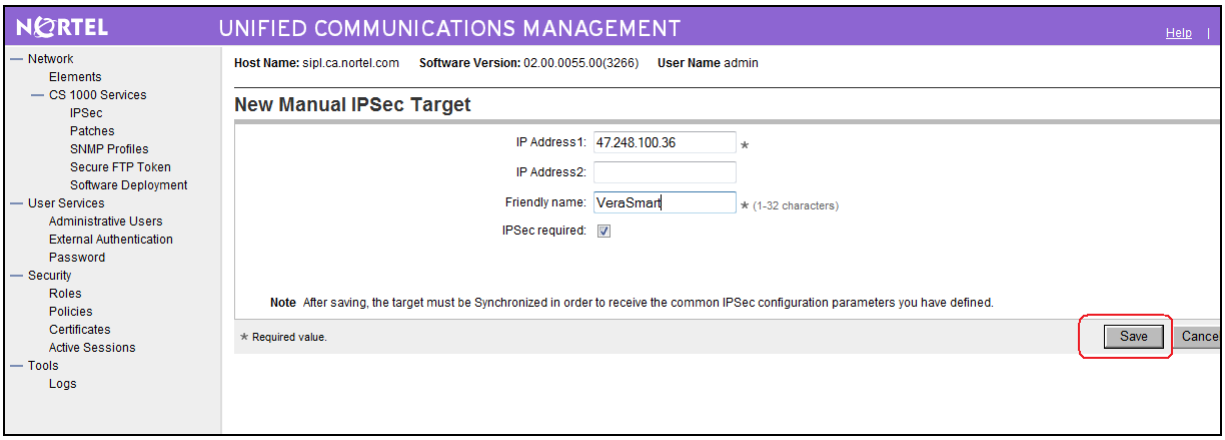



**Figure 10: Manual IPSec Target Configuration**


©2010 Avaya Inc. All Rights Reserved.

6. Click the **Edit Defaults** button in the Configuration and Status section as shown in **Figure 11**.

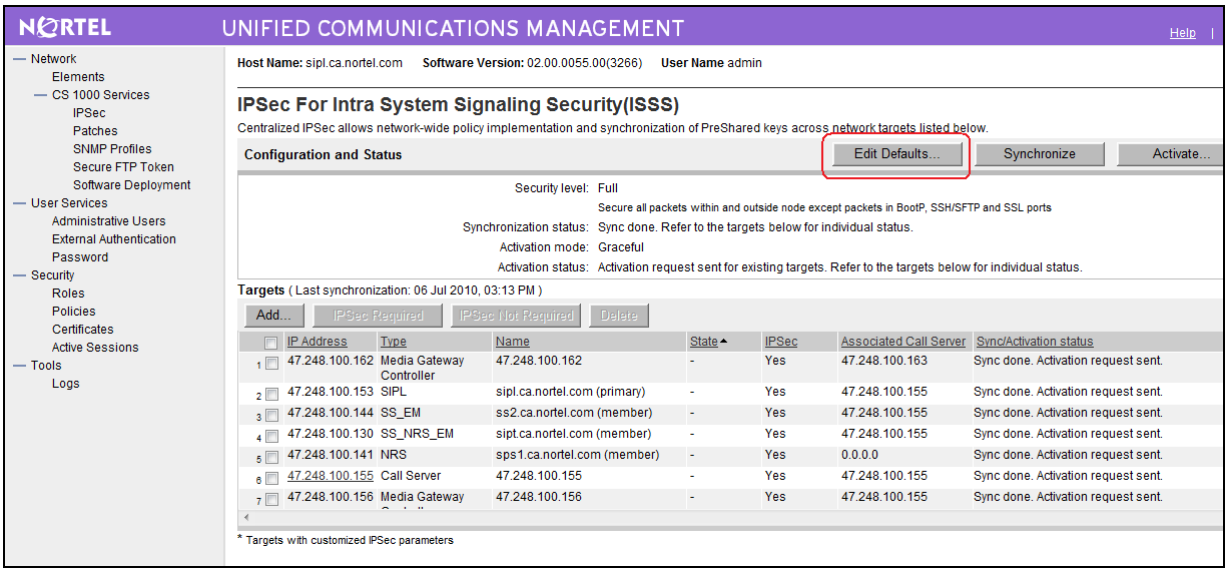



**Figure 11: Edit Defaults**

7. On the IPSec Configuration Details page, select the desired security level (**Full**/**Optimal**), enter the PSK and click on the **Save and Synchronize** button as shown in **Figure 12** below.

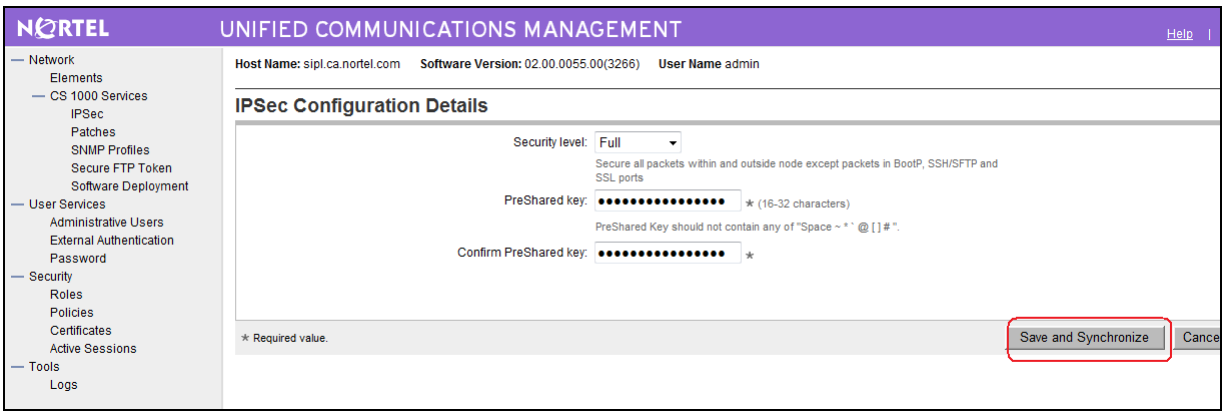



**Figure 12: PSK Save and Synchronize**

# 5. Create and configure the Windows ELAN IPSecurity policy (on Windows XP)

This section describes the steps to configure the Windows ELAN IPSecurity policy (on Windows XP).


©2010 Avaya Inc. All Rights Reserved.

## 5.1. Create the custom IPSec MMC Console

The configuration procedure is provided below.

1. Log on to the computer as a user with administrative privileges.
2. Click **Start** on the Windows desktop.
3. Click **Run**. The Run dialog box appears.
4. Enter **MMC**.
5. Click **OK**.
6. Select **Add/Remove Snap-In** on the Console menu. The **Add/Remove Snap-In** dialog box appears.
7. Click **Add**. The **Add Standalone Snap-In** dialog box appears.
8. Select **IP Security Policy Management** in the **Add Standalone Snap-In** dialog box as shown in **Figure 13** below.

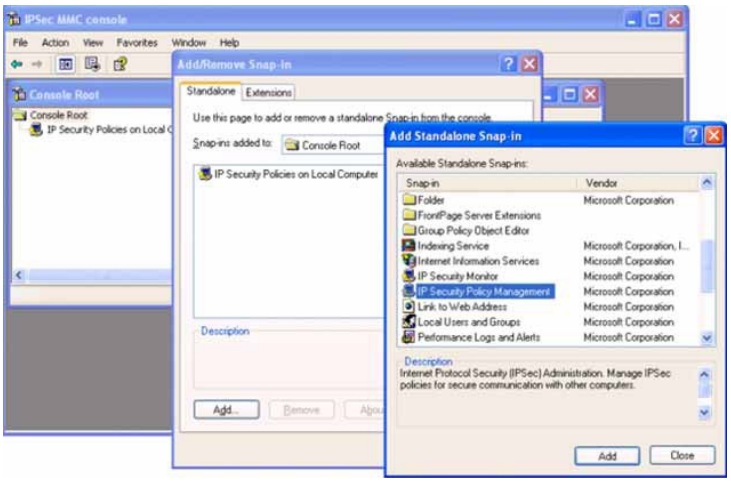



**Figure 13: Add Standalone Snap-in dialog box**

9. Click **Add**. Verify that Local Computer is selected.
10. Click **Finish**.
11. Select **IP Security Monitor** in the **Add Standalone Snap-In** dialog box.
12. Click **Add**.
13. Click **Close** to close the **Add Standalone Snap-In** dialog box.
14. Click **OK** to close the **Add/Remove Snap-In** dialog box.
15. Select **File > Save As** on the **MMC** console window.


©2010 Avaya Inc. All Rights Reserved.

16. Enter **IPSec MMC console** in the File name textbox.

17. Click **Save**.

The saved custom IPSec MMC console can be launched from **Start > Program > Administrative Tools > IPSec MMC console.msc** as shown in **Figure 14** below.

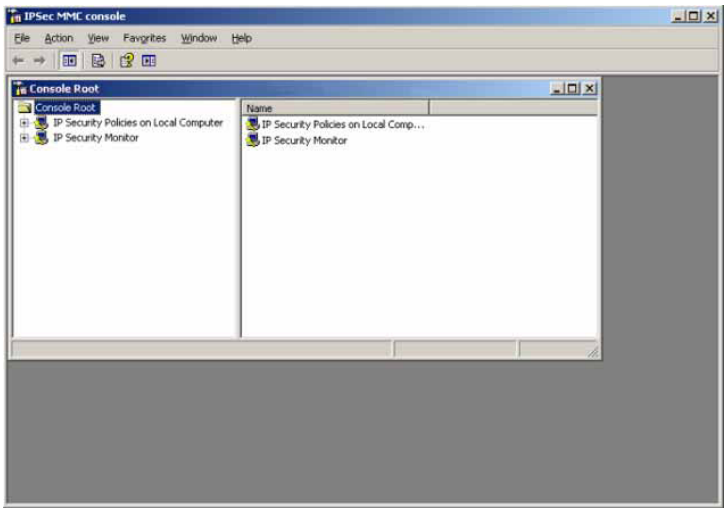



**Figure 14: IPSec MMC Console**

## 5.2. Create the Windows ELAN IPSecurity policy

The configuration procedure is provided below.

1. Log on to the computer as a user with administrative privileges.
2. Click **Start** on the Windows desktop.
3. Click **Programs**.
4. Select **Administrative Tools**.
5. Select **IPSec MMC console.msc** created in Section 5.1 above.
6. Right-click **IP Security Policies on Local Computer Policy** in the left-hand pane of the subsequent window.


©2010 Avaya Inc. All Rights Reserved.

7. Select **Create IP Security Policy**. The IP Security Policy Wizard screen appears as shown in **Figure 15** below.


**Figure 15**

8. Click **Next**

9. Enter a name in the Name text box, WINXP IP Security Policy for example as shown in **Figure 16** below.

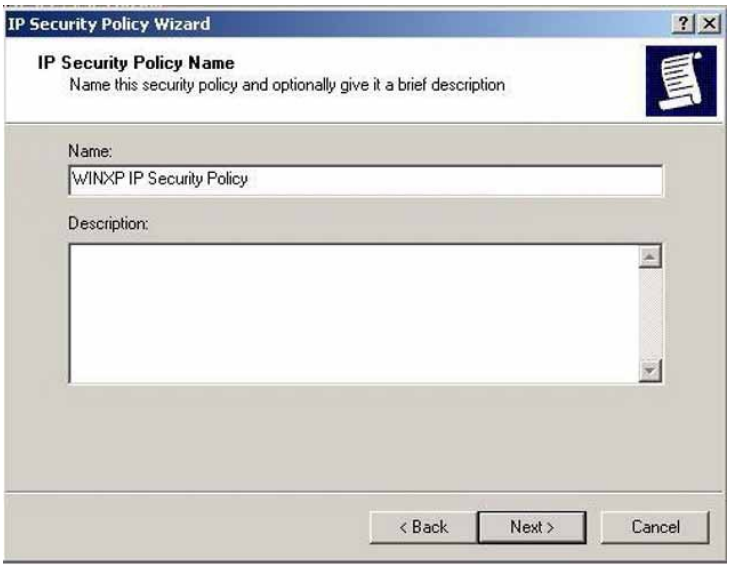



**Figure 16**

10. Enter a description in the Description text box.

11. Click **Next**.


©2010 Avaya Inc. All Rights Reserved.

12. **DO NOT place** a check mark in the **"Activate the default response rule"** check box as shown in **Figure 17** below.

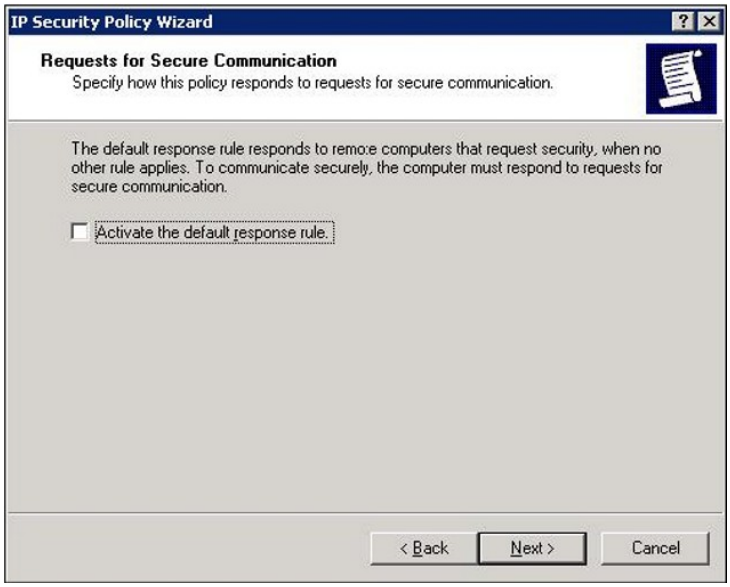



**Figure 17**

13. Click **Next.**

14. **DO NOT place** a check mark in the **"Edit properties"** check box as shown in **Figure 18**.

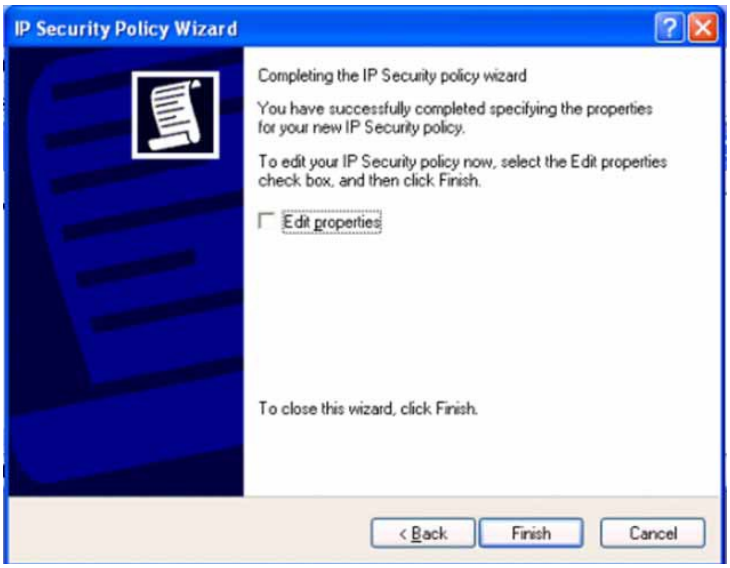



**Figure 18**

15. Click **Finish** to complete creating the Windows ELAN IPSecurity policy.

## 5.3. Configure the Windows ELAN IPSecurity policy

1. Log on to the computer as a user with administrative privileges.


©2010 Avaya Inc. All Rights Reserved.

2. Click **Start** on the Windows desktop.
3. Click **Programs**.
4. Select **Administrative Tools**.
5. Select **IPSec MMC console.msc** created in Section 5.1 above. The IPSec MMC Console window appears.
6. Right-click **WINXP IP Security Policy** in the right-hand pane of the window.
7. Click **Properties**. The dialog box WINXP IP Security Policy Properties window appears.
8. Select the Rules tab in the Properties dialog box.
9. Click **Add**. The Security Rule Wizard appears as shown in **Figure 19** below.


**Figure 19**


©2010 Avaya Inc. All Rights Reserved.

10. Click **Next**. The Security Rule Wizard Tunnel Endpoint screen appears as shown in **Figure 20** below.


**Figure 20**

11. Select **This rule does not specify a tunnel** radio button.

12. Click **Next**. The Security Rule Wizard Network Type screen appears as shown in **Figure 21** below.

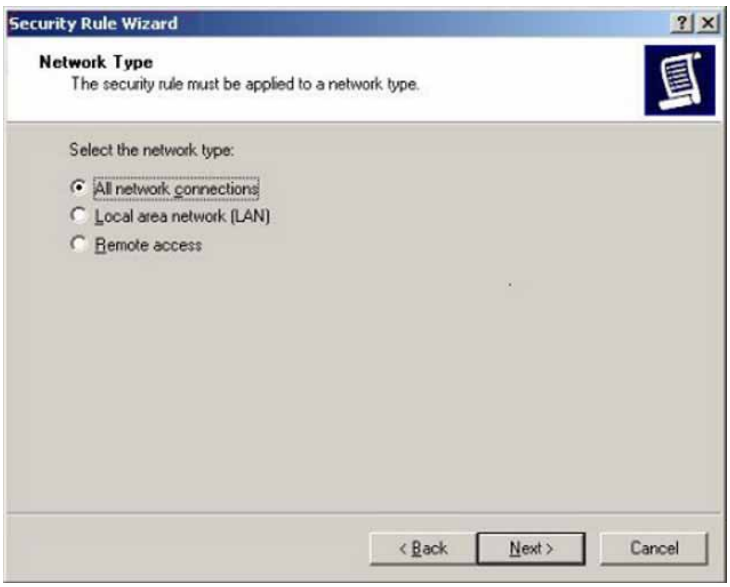



**Figure 21**

13. Click **Next**

14. Select **Use this string to protect the key exchange (Preshared key)**.


©2010 Avaya Inc. All Rights Reserved.

15. Enter the Preshared Key string used in the Communication Server 1000 IPSec policy configuration configured in **Figure 4, Section 4.3** above as shown in **Figure 22** below.


**Figure 22**

16. Click **Next**. The Security Rule Wizard IP Filter List screen appears to add a new IP filter as shown in **Figure 23** below.

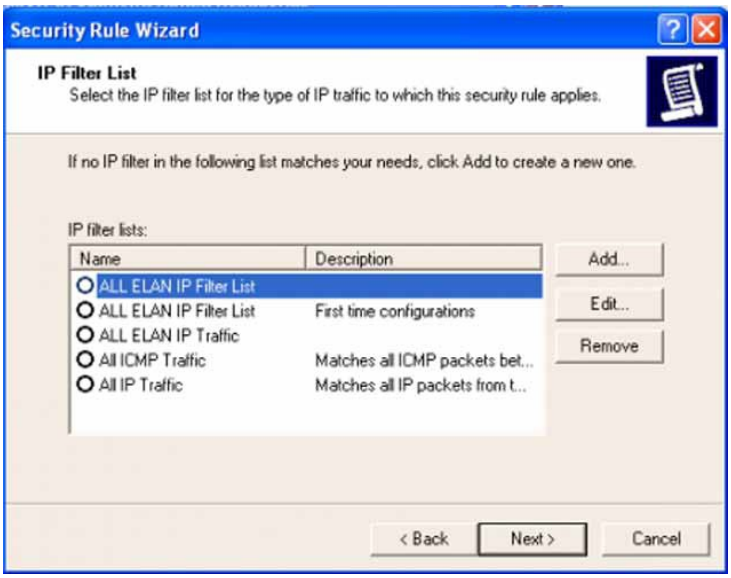



**Figure 23**


©2010 Avaya Inc. All Rights Reserved.

17. Click **Add** to create an IP filter. The IP Filter List screen appears to add the name and description as shown in **Figure 24** below.

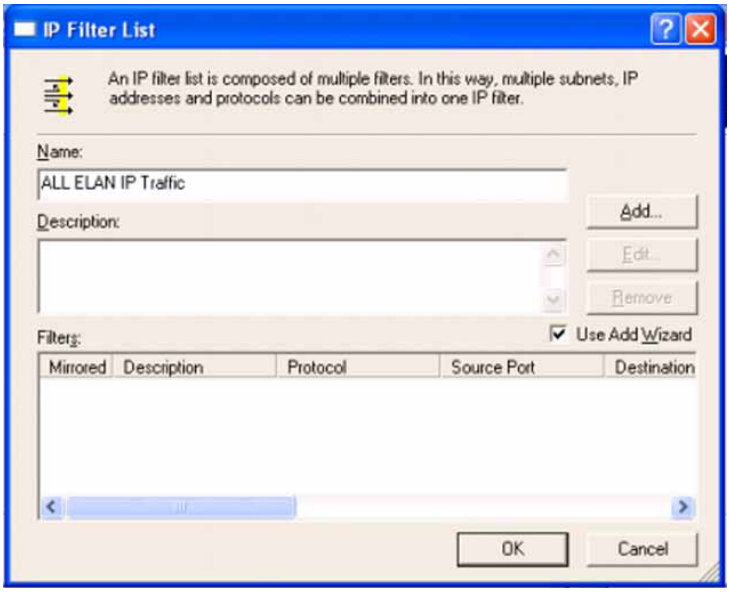



**Figure 24**

18. Enter **All ELAN IP Traffic** in the Name textbox.

19. Enter a description in the description textbox.

20. Click **Add**. The IP Filter Wizard screen appears as shown in **Figure 25** below.


**Figure 25**


©2010 Avaya Inc. All Rights Reserved.

21. Click **Next**. The IP Filter Wizard IP Traffic Source screen appears as shown in **Figure 26**.

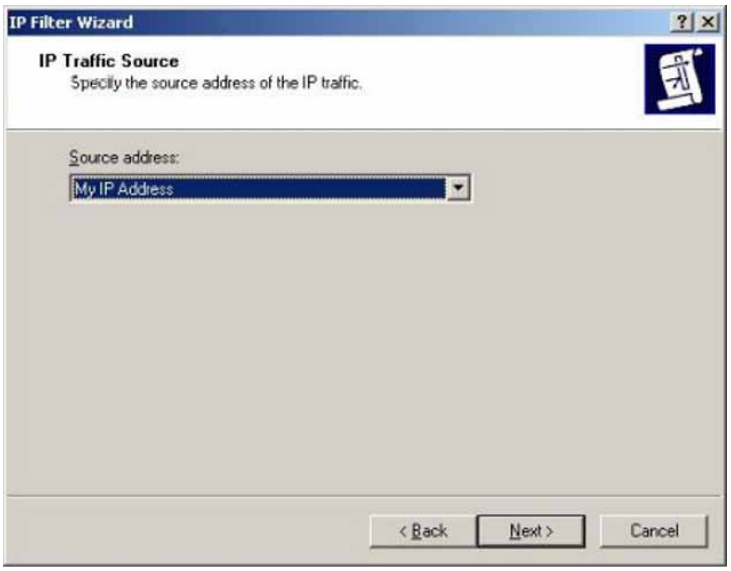



**Figure 26**

22. Select **A Specific IP Address** from the list. The subsequent IP Filter Wizard IP Traffic Source screen appears as shown in **Figure 27** below.

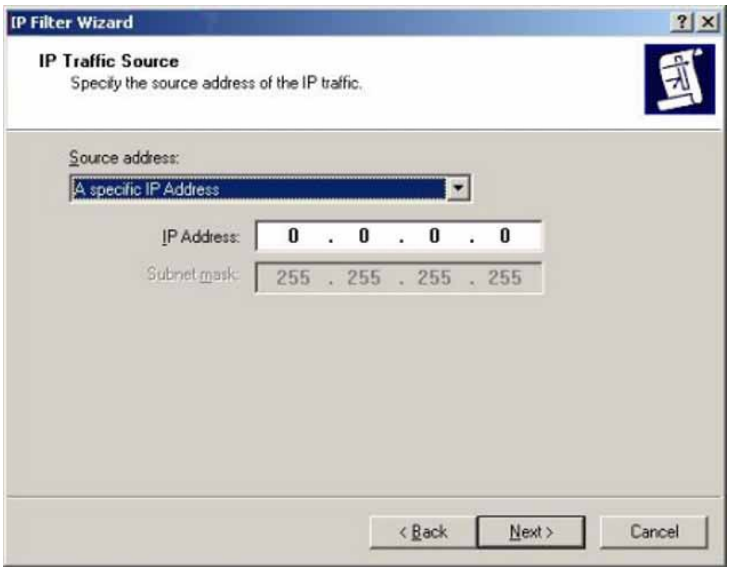



**Figure 27**

23. Enter the Windows System IP Address.

24. Click **Next**.

25. Select **A Specific IP Address** from the list.

26. Enter the Call Server ELAN IP address


©2010 Avaya Inc. All Rights Reserved.

27. Click **Next**. The IP Protocol Type screen of the Filter Wizard appears as shown in **Figure 28**.

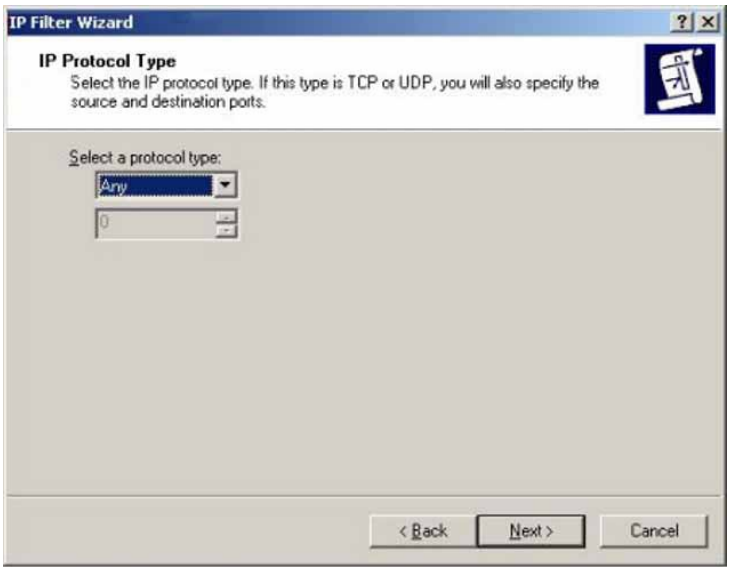



**Figure 28**

28. Select **Any** from the list.

29. Click **Next**.

30. Click **Finish** to close the IP Filter Wizard dialog box.

31. Click **OK**.

32. Select the newly created filter list **All ELAN IP traffic** in the Security Rule Wizard dialog box.

33. Click **Next**. The Filter Action dialog box appears as shown in **Figure 29** below.


**Figure 29**


©2010 Avaya Inc. All Rights Reserved.

34. Click **Add**. The Filter Action wizard appears as shown in **Figure 30**.


**Figure 30**

35. Click **Next**.

36. Enter **ELAN Security** in the Name textbox of the Filter Action window (not shown).

37. Enter a description in the Description textbox (not shown).

38. Click **Next**. The **Filter Actions General Options** dialog box appears as shown in **Figure 31** below.

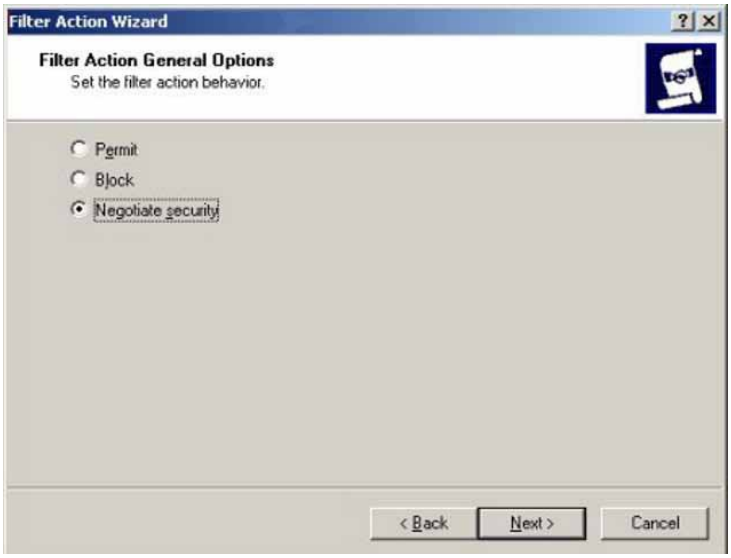



**Figure 31**

39. Select **Negotiate security**.


©2010 Avaya Inc. All Rights Reserved.

40. Click **Next**. The Communicating with computers that do not support IPSec screen of the Filter Actions Wizard appears (not shown).

41. Select "**Do not communicate with computers that do not support IPSec"** (not shown).

42. Click **Next**. The IP Traffic Security Screen window appears as shown in **Figure 32** below.

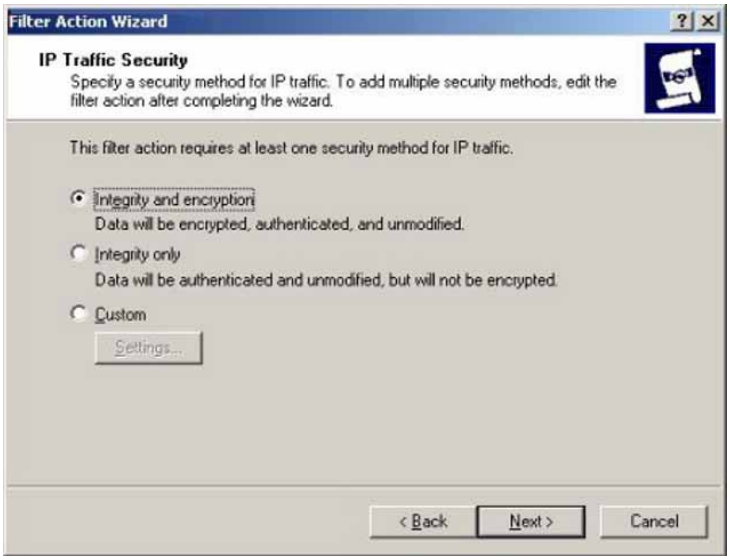



**Figure 32**

43. Select **Integrity and encryption**.

44. Click **Next**.

45. Click **Finish** to close the IP Security Filter Action Wizard.

46. Select the newly created filter action, **ELAN Security** on the Filter Action screen of the Security Rule Wizard.

47. Click **Edit**. The ELAN Security Properties dialog box appears.

48. Select the **Security Methods** tab.

- Select the **Negotiate security** radio button.
- Place a check mark in the **Accept unsecured communication, but always respond using IPSec** check box.
- Place a check mark in the **Session key perfect forward secrecy (PFS)** check box.

49. Click **OK** to close the ELAN Security Properties dialog box.

50. Select the newly created filter action, **ELAN Security** on the Filter Action screen of the Security Rule Wizard.

51. Click **Next**.


©2010 Avaya Inc. All Rights Reserved.

52. Place a check mark in the **ALL ELAN IP Traffic** check box on the WIN XP IP Security Policy Properties dialog box.

53. Click **Close** to close the Windows IP Security Policy Properties dialog box

This completes the Windows Server IP Security Policy configuration.

## 5.4. Assign WinXP IP Security policy to Windows Server

1. Log on to the computer as a user with administrative privileges.
2. Click **Start** on the Windows desktop.
3. Click **Programs**.
4. Select **Administrative Tools**.
5. Select **IPSec MMC console.msc**.
6. Select **IP Security Policies on Local Computer Policy** in the left-hand pane of the subsequent window.
7. Right-click the WINXP IP Security Policy in the right-hand pane.
8. Select **Assign** from the list. Following this action, the Policy Assigned column should show **Yes** as shown in **Figure 33** below.

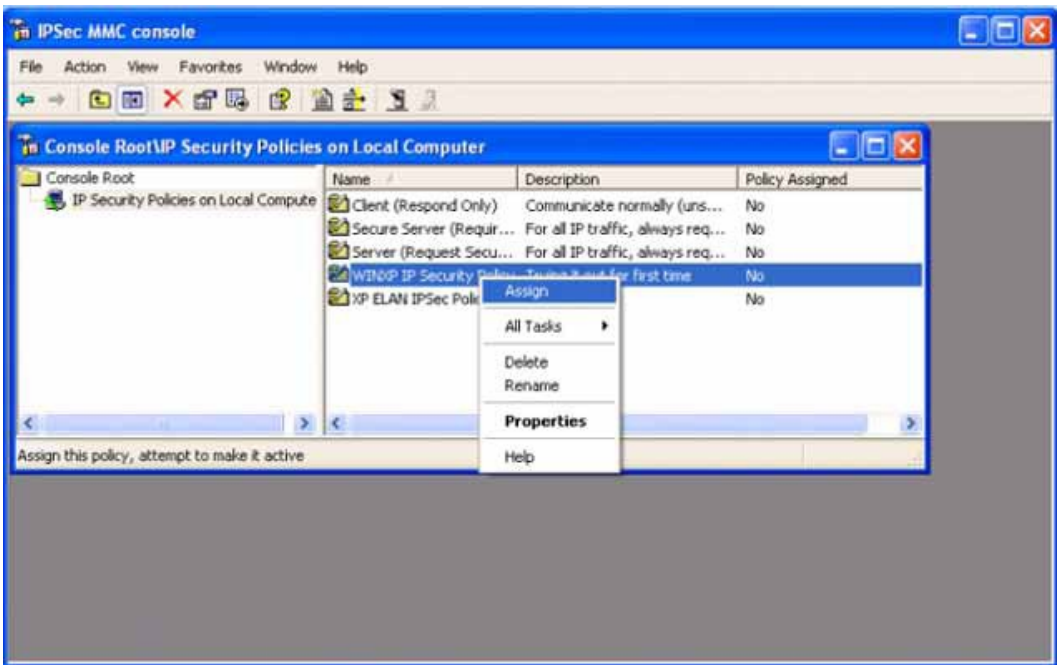



**Figure 33**

9. Open a DOS command window.


©2010 Avaya Inc. All Rights Reserved.

10. Enter **c:\>ping <M1 CS ELAN IP address> as known c:\>ping 47.248.100.155 for CS1000 Release 6.0**. The ping returns a few messages of "Negotiating IP Security" first and then the message "Reply from …". This response indicates the ping is successful as shown in **Figure 34** below.

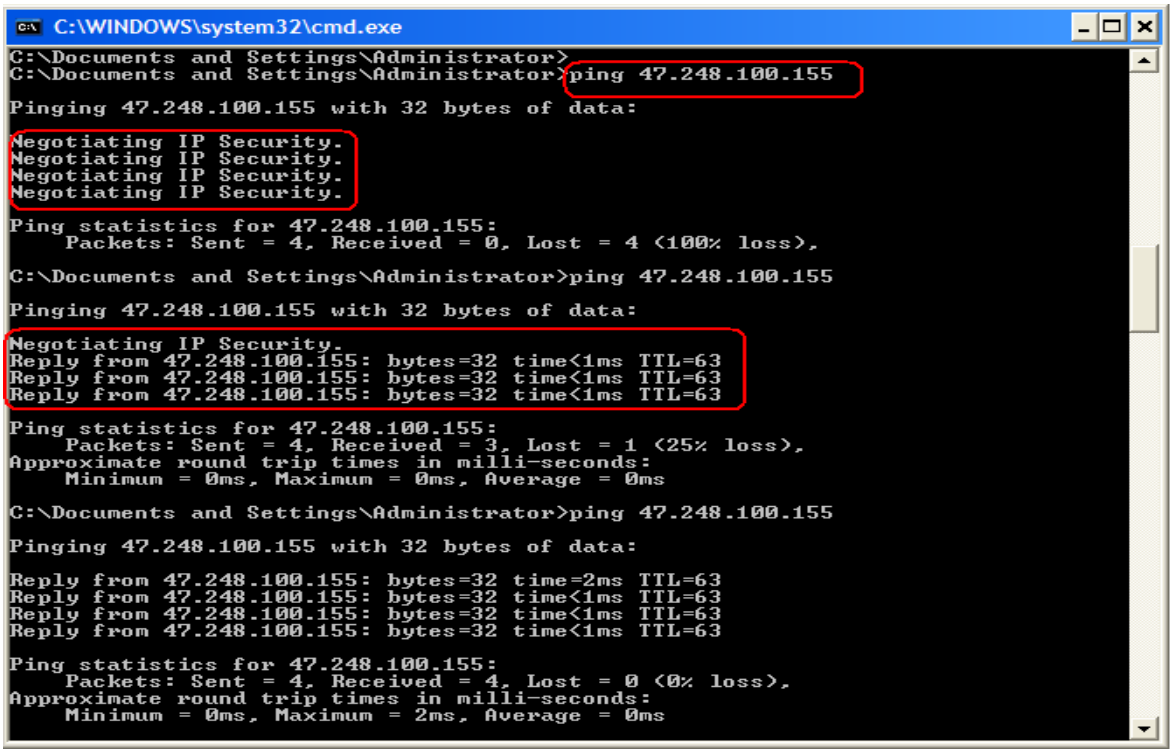



**Figure 34**

➔ The ELAN connection is now working in IPSec mode.

# 6. Collect CDR/Traffic data

There are two ways to collect CDR/Traffic data as indicated in 6.1 and 6.2 below.

## 6.1. Start a new live data session

To collect live data, a live date session must be started and configured (an active connection to a Call Server). The CS 1000 DBA CDR/Traffic Collector runs continuously during the session and provides access for the session configuration and a window for monitoring session information. To maintain a live data session, the CS 1000 DBA CDR/Traffic Collector main window must remain open at all time during the process.

This section describes the steps to collect CDR/Traffic data.

1. Select **New Session** from the File menu in the CS 1000 DBA CDR/Traffic Collector main window.


©2010 Avaya Inc. All Rights Reserved.

2. The New Session Properties window appears as shown in **Figure 35** below.

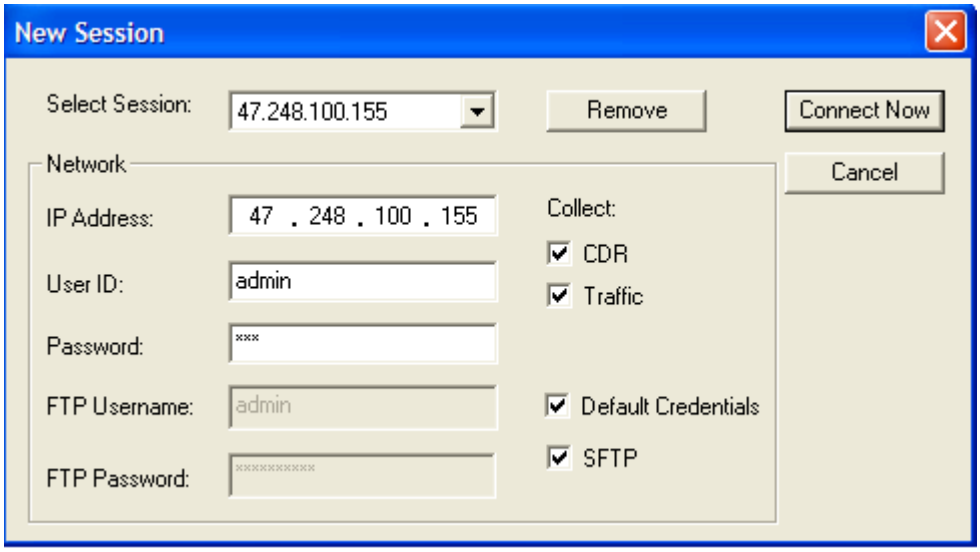



**Figure 35**

3. Enter the ELAN IP address of the Call Server in the **IP Address** box.

4. Enter the login name in the **User ID b**ox.

5. Enter the login password in the **Password** box.

6. Enter the FTP/SFTP Username in the **FTP Username** box.

7. Enter the FTP/SFTP Password in the **FTP Password** box.

8. Select the type of data to be collected by clicking on the **CDR** and/or **Traffic** boxes under the **Collect** heading.

9. Click on **Connect Now** to connect to the Call Server and begin a live data session.

*User account to be used for FTP/SFTP task is dependant on the Call Server to which the CS 1000 DBA CDR/Traffic collector is connecting.*

**Note:**
- For FTP sessions, select only the "Default Credentials" checkbox.
- For SFTP sessions, select both "Default Credentials" and "SFTP" check boxes.

## 6.2. Command Line options

Command Line options are provided to enable you to manage the CS 1000 DBA CDR/Traffic Collector sessions from a third party application. The command to create a new live data session is given below:

**dba <options> <ipaddress> <cs username> <cs password> [ftptype=] [ftpname=username] [ftppwd=password] [datatype=cdr]**


©2010 Avaya Inc. All Rights Reserved.

options: -c establishes a new connection
-r closes an established connection
ipaddress: ELAN IP Address of the CS 1000 Call Server
cs username: CS 1000 Call Server user name
cs password: CS 1000 Call Server password
ftptype: **Simple** for normal **FTP**
**Secure** for **SFTP**
ftpname: Username to establish FTP or SFTP connection
ftppwd: Password of FTP or SFTP user
datatype: **cdr** for CDR data collection
**trf** for traffic data collection
**all** for both CDR and traffic data collection

The parameters *cs username*, cs *password, ftptype, ftpname, ftppwd* and *datatype* are only required when establishing a DBA CDR/Traffic Collector data collection session. They are not required when closing a session.

Also, the parameters *ftptype, ftpname, ftppwd* and *datatype* are optional. They are provided with identifiers as shown in the example below. If these parameters are not provided, the CS 1000 DBA CDR/Traffic Collector uses normal FTP with the default credentials. Both CDR and traffic data collection are enabled.

Examples (with fictitious ELAN IP Address, User Accounts and Passwords):
CLI command to establish a session using normal FTP Connection:
**dba –c 47.248.100.155 admin Escspv_123 ftptype=simple ftpname=admin ftppwd=Escspv_123 type=all**
CLI command to establish a session using normal FTP with default credentials for both CDR and TRF data collection:
**dba –c 47.248.100.155 admin Escspv_123**
CLI command to establish a session using secure FTP Connection:
**dba –c 47.248.100.155 admin Escspv_123 ftptype=secure ftpname= admin ftppwd= Escspv_123 type=all**
CLI command to terminate an existing live connection:
**dba –r 47.248.100.155**


©2010 Avaya Inc. All Rights Reserved.

## 6.3. View session data

During a live session, you can view the collected CDR and Traffic data as well as the session data-collection statistics, as shown in **Figure 36** below in the sample session window.

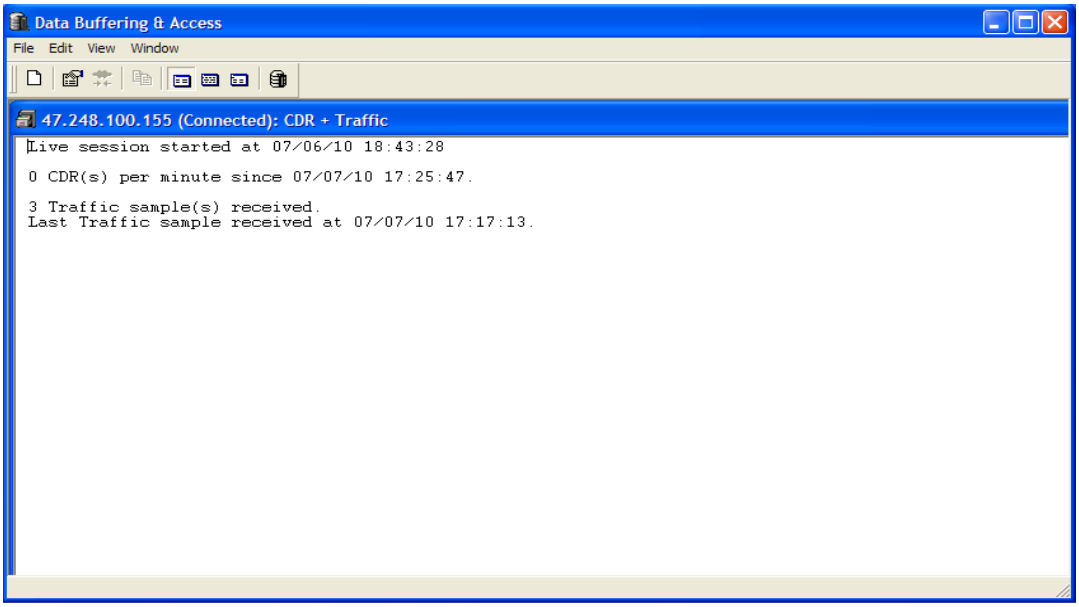



**Figure 36: Data Buffering and Access**

# 7. Use of Collected CDR and Traffic data

The CDR and Traffic data collected from a CS 1000 Call Server can be processed by VeraSMART following the guidelines in this section.

The CDR and Traffic data files are stored on the server, which is running the CS 1000 DBA CDR/Traffic Collector, and are located in a folder named with the CS 1000 Call Server IP address. For example "\<DBA root folder>\47.248.100.155". The following data file names are used:

- **detail1.img** — for CDR data
- **traffic.dmp** — for Traffic data

The CS 1000 DBA CDR/Traffic Collector collects data from the CS 1000 Call Server continuously and merges the data into the **detail1.img** and **traffic.dmp** files every 30 seconds (or the interval value configured in **DbaConfig.properties** file). If the data file is being used by another application, the merge is done at the next merge interval.


©2010 Avaya Inc. All Rights Reserved.

# 8. Configure VeraSMART eCAS

This section describes the configuration of the VeraSMART eCAS Call Accounting application.

To configure VeraSMART, launch a web browser, enter **http://<IP address of Veramark VeraSMART server>** as URL, and log in with the appropriate credentials as shown in **Figure 37** below.

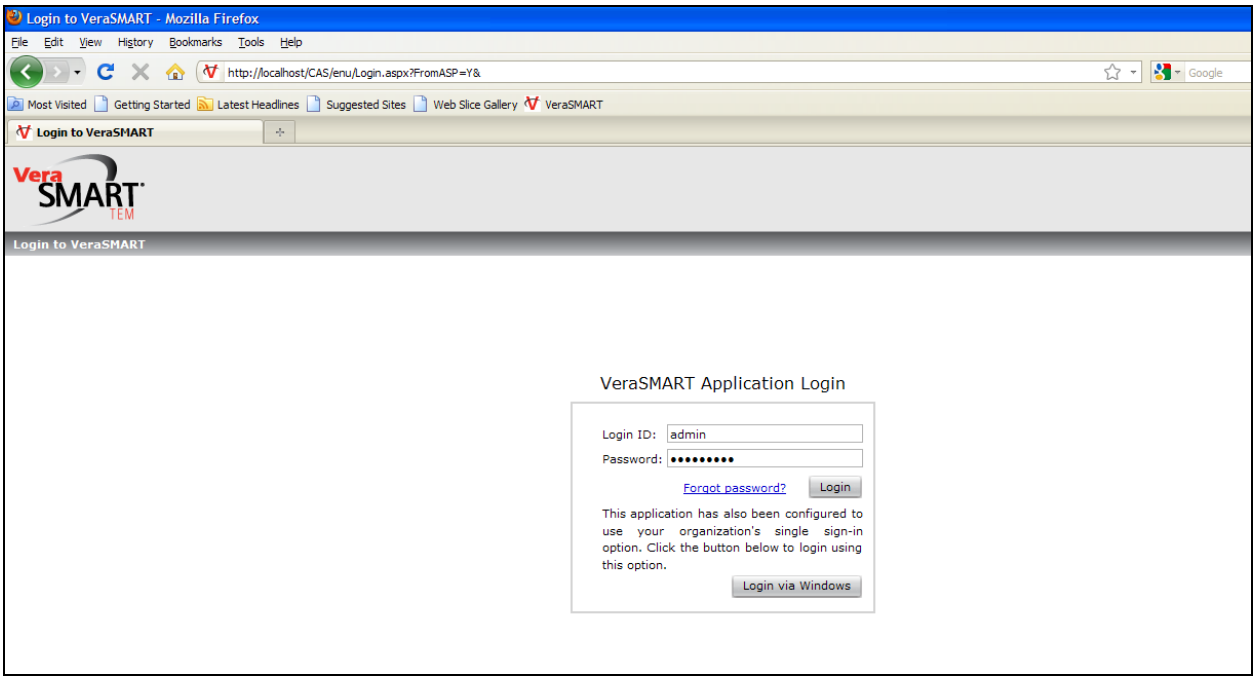



**Figure 37**


©2010 Avaya Inc. All Rights Reserved.

After logging in successfully, from the Main window, click on the **Call Accounting** > **Call Collection > CDR Source** link as shown in **Figure 38** and **Figure 39** below.

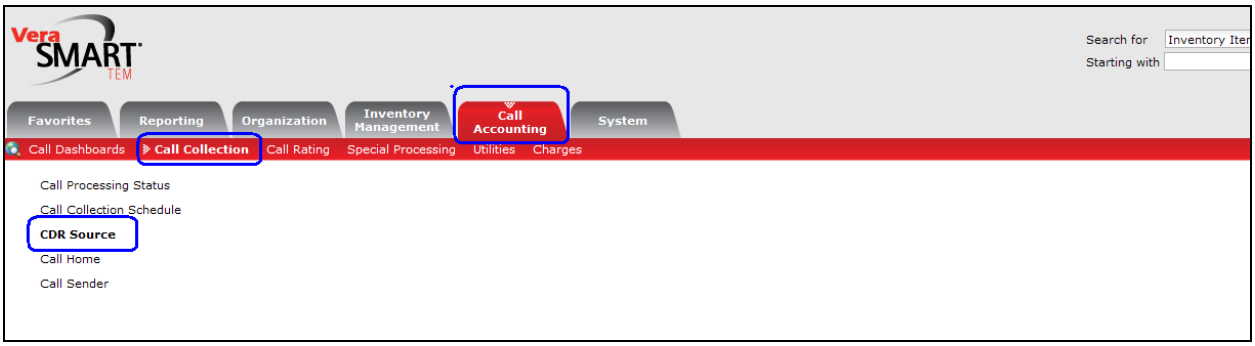



**Figure 38**

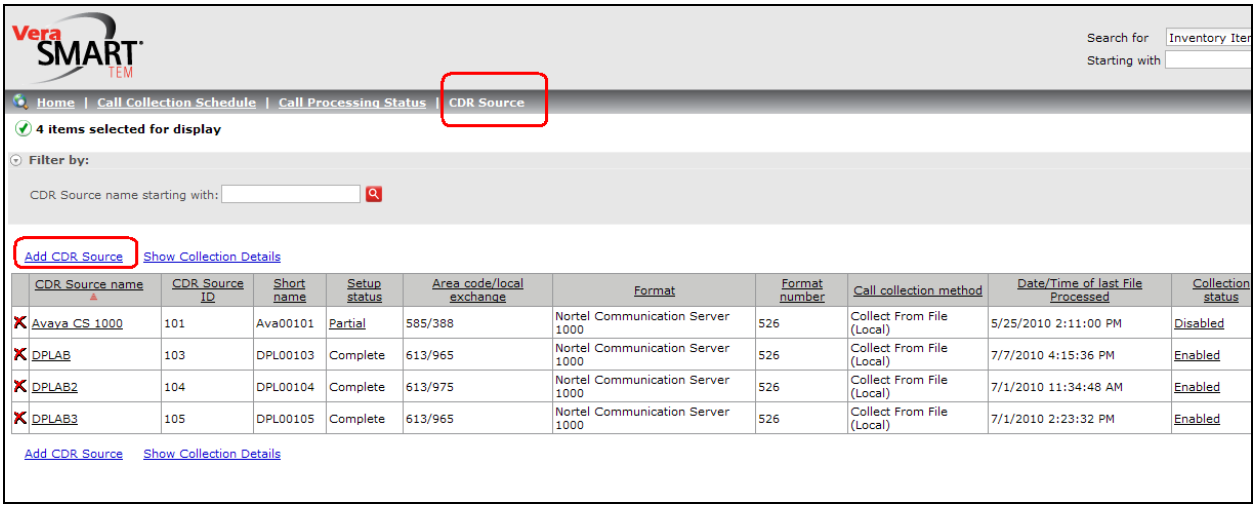



**Figure 39**


©2010 Avaya Inc. All Rights Reserved.

In the CDR Source window, click on the **Add CDR Source** link as shown in **Figure 40** below.

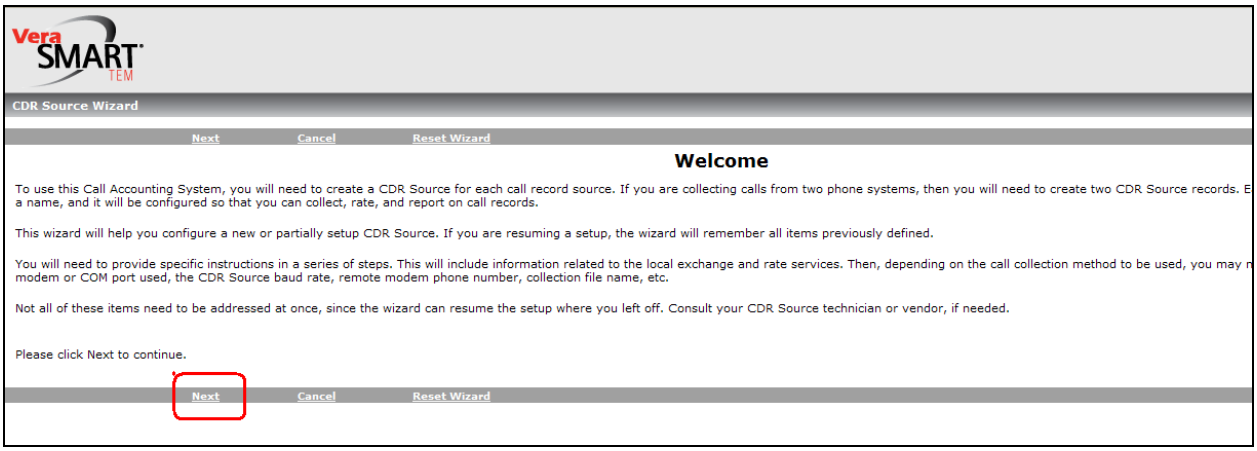



**Figure 40**

In the CDR Source Wizard, keep clicking the **Next** button that appears on the bottom menu bar until the **Identify the source of the call** is displayed. Enter the information for CDR Source Name, Area Code, and Local exchange fields. On the drop down menu list of the **Local rate method** attribute, choose option 'None' from the menu list as shown in **Figure 41** below.

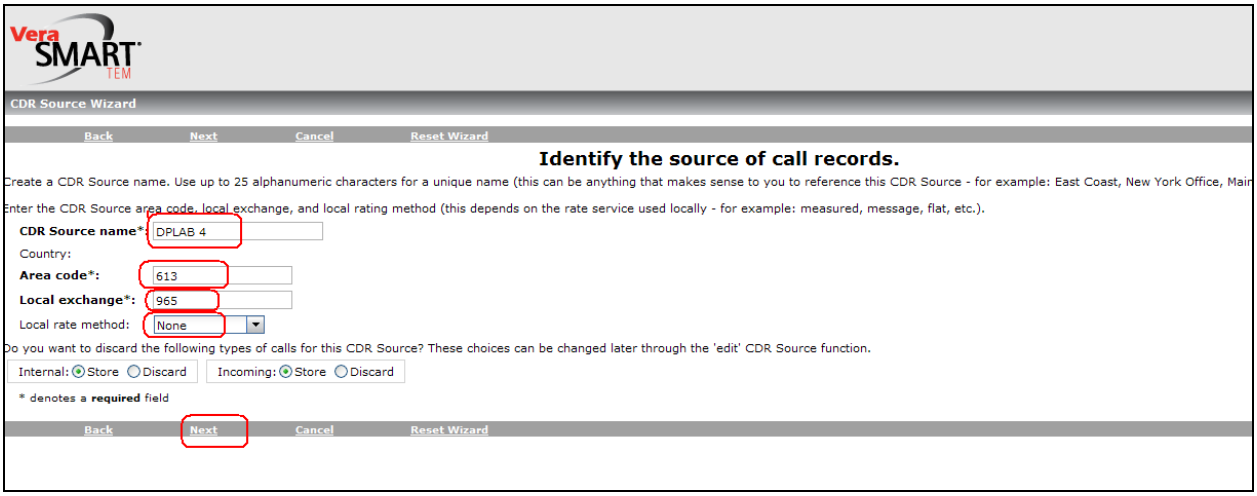



**Figure 41**


©2010 Avaya Inc. All Rights Reserved.

Click on the **Next** button until the **Select the CDR Source manufacturer** is displayed. From the drop down menu list of the **Manufacturer** attribute, select'Nortel' as shown in **Figure 42** below.

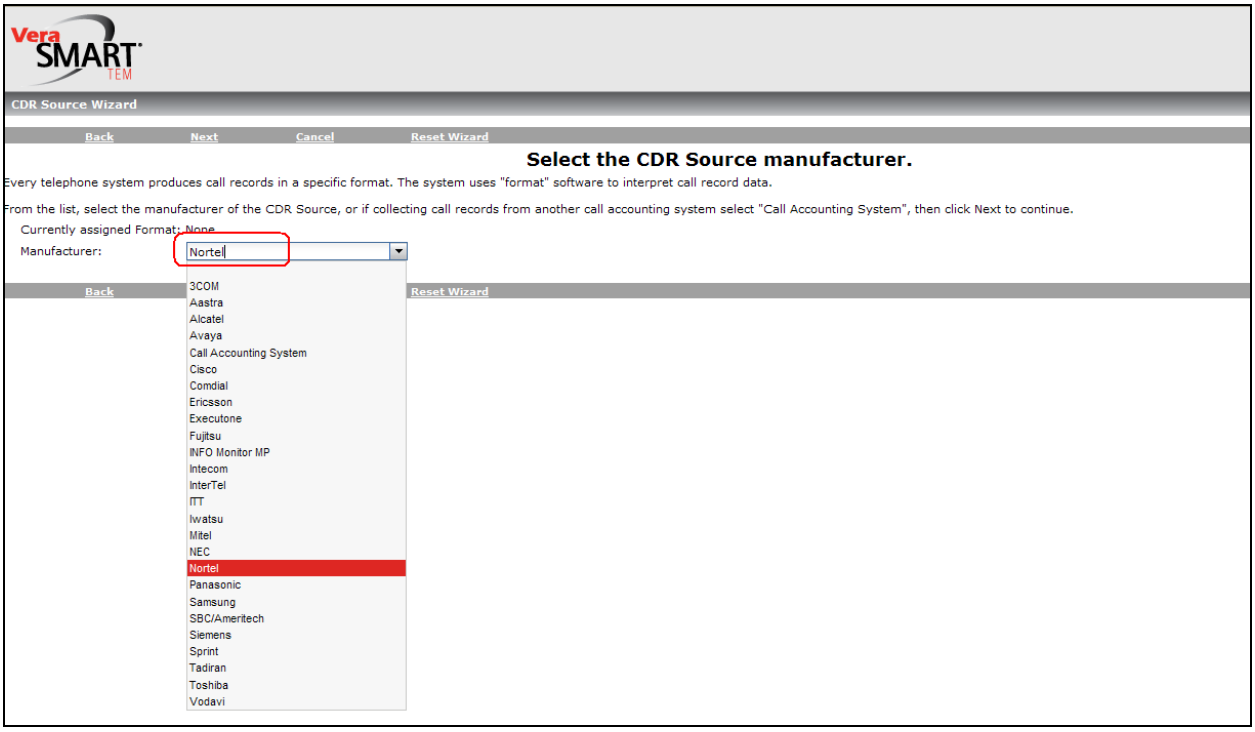



**Figure 42**

In the "Select the CDR Source manufacturer" page, continue to click the **Next** button as shown in **Figure 43** below.

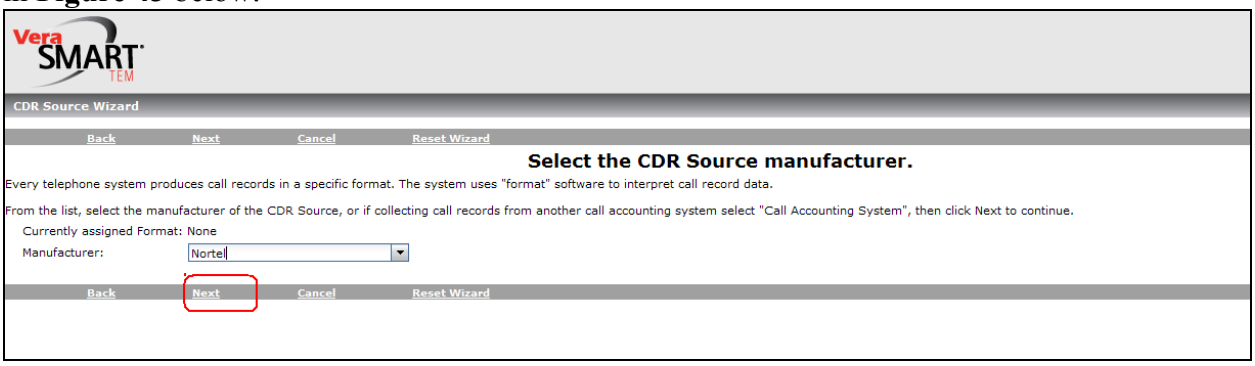



**Figure 43**


©2010 Avaya Inc. All Rights Reserved.

The "**Select the call record format**" page will appear. Choose the "Nortel Communication Server 1000" entry from the table shown in **Figure 44** below by clicking on the radio button.

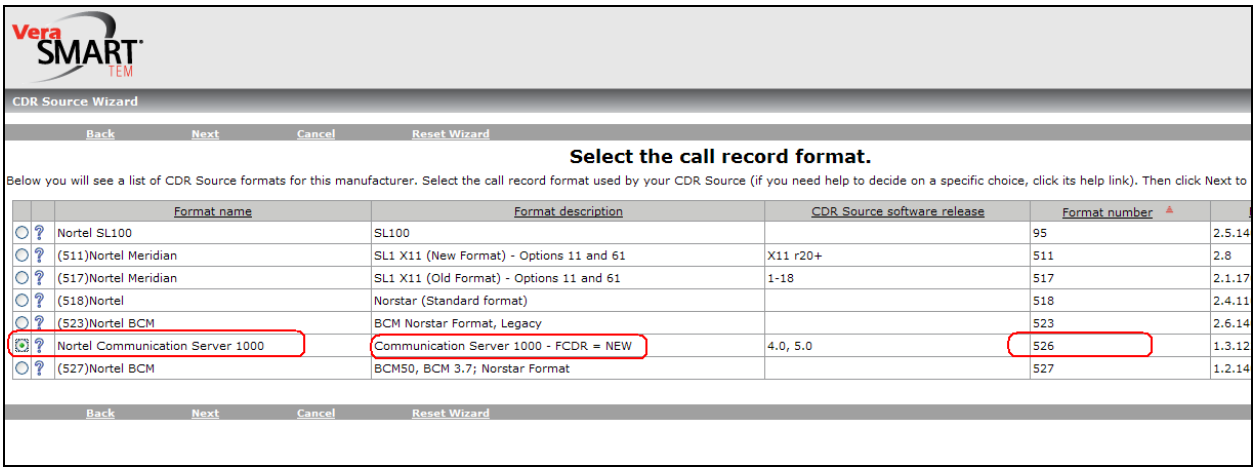



**Figure 44**

Continue to click the **Next** button until the "**Select the call collection Method**" page is displayed. Click on the circular radio button of the "Collect From File (Local)" entry in the table as shown in **Figure 45**.

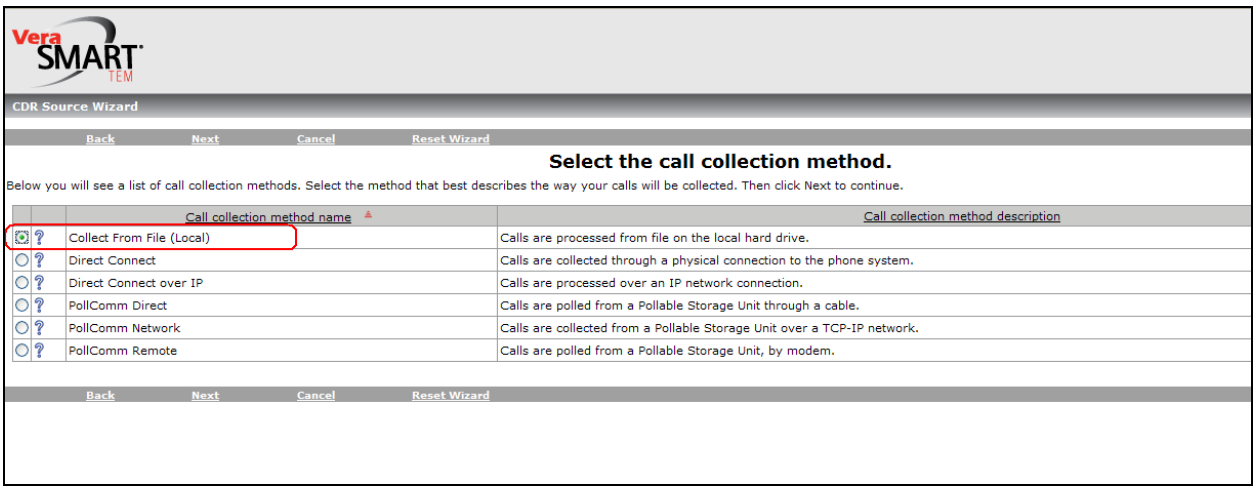



**Figure 45**


©2010 Avaya Inc. All Rights Reserved.

In the **Select the call collection method** page, click on the **Next** button on the bottom menu bar until the CRD Source Wizard page is as shown in **Figure 46**. At the **Collection file name and path** attribute, browse to the file name and path containing the CDR raw data as shown on **Figure 46** below.

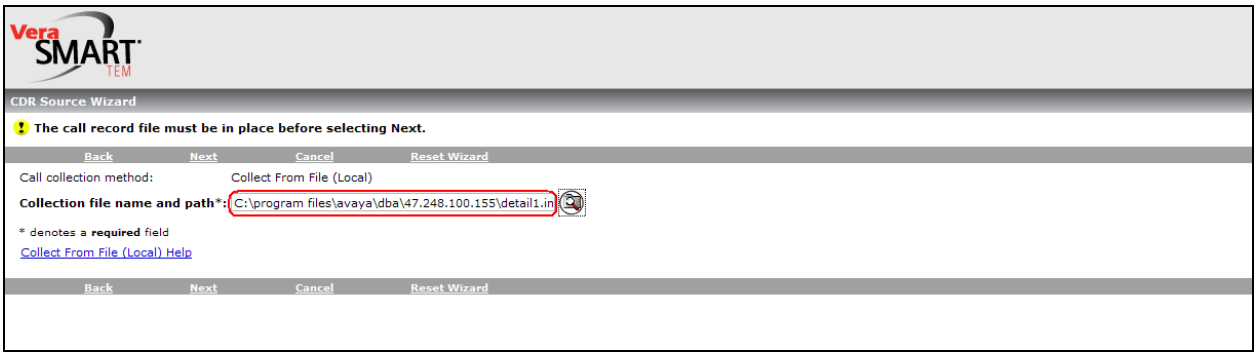



**Figure 46**

To ensure that there is a record stored in the CDR directory. The CDR directory is located in **\Home location\avaya\dba\<IP of Elan Call Server>\detail1.img**


©2010 Avaya Inc. All Rights Reserved.

The following two windows in **Figure 47** and **Figure 48** shows the raw CDR data being collected from the Call Server.

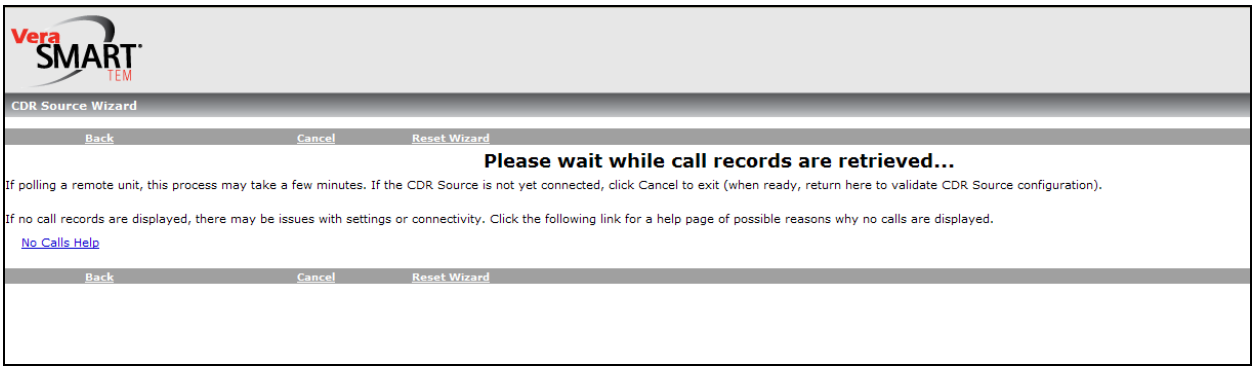



**Figure 47**

Click on the **Next** link.

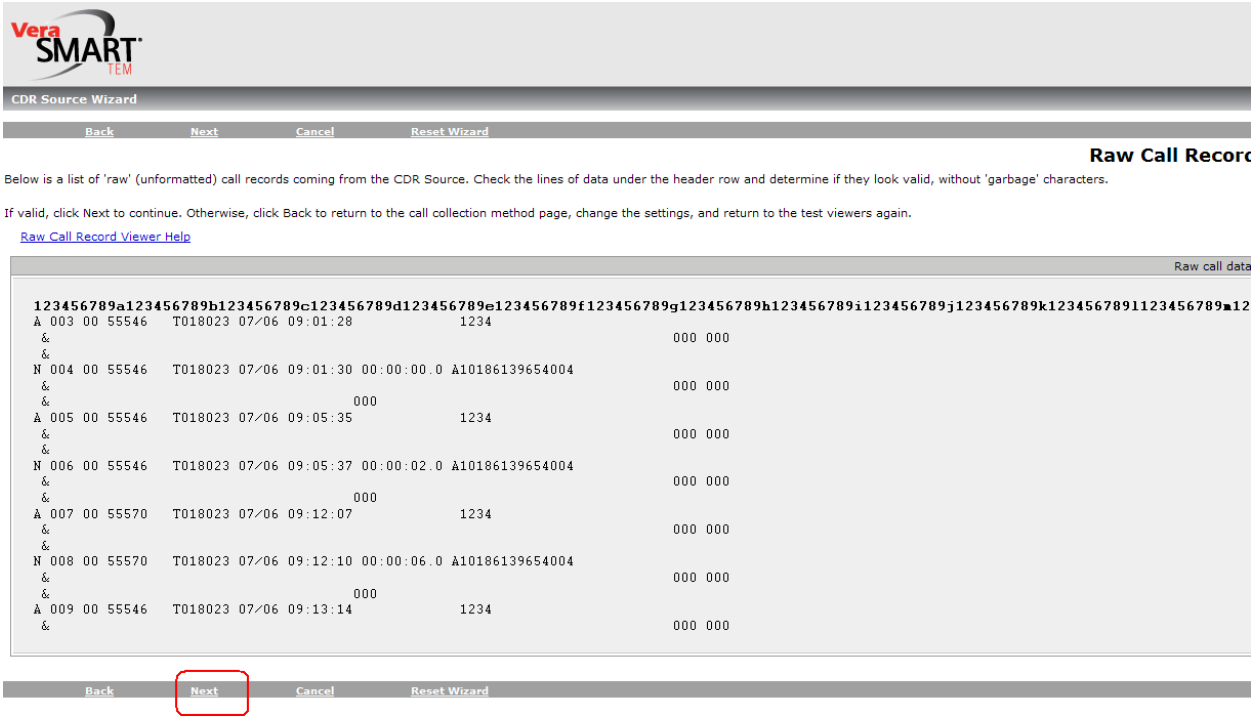
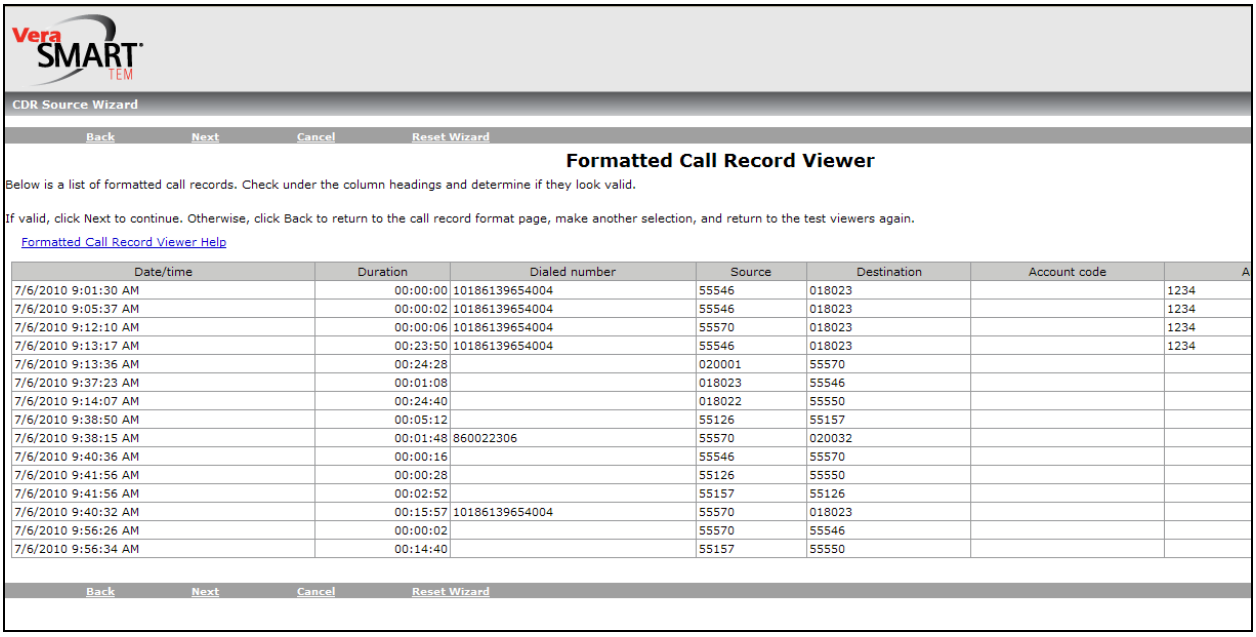



**Figure 48**


©2010 Avaya Inc. All Rights Reserved.

**Figure 49** shows the CDR report from VeraSMART.




| Date/time | Duration | Dialed number | Source | Destination | Account code | A |
|---|---|---|---|---|---|---|
| 7/6/2010 9:01:30 AM | 00:00:00 | 10186139654004 | 55546 | 018023 | | 1234 |
| 7/6/2010 9:05:37 AM | 00:00:02 | 10186139654004 | 55546 | 018023 | | 1234 |
| 7/6/2010 9:12:10 AM | 00:00:06 | 10186139654004 | 55570 | 018023 | | 1234 |
| 7/6/2010 9:13:17 AM | 00:23:50 | 10186139654004 | 55546 | 018023 | | 1234 |
| 7/6/2010 9:13:36 AM | 00:24:28 | | 020001 | 55570 | | |
| 7/6/2010 9:37:23 AM | 00:01:08 | | 018023 | 55546 | | |
| 7/6/2010 9:14:07 AM | 00:24:40 | | 018022 | 55550 | | |
| 7/6/2010 9:38:50 AM | 00:05:12 | | 55126 | 55157 | | |
| 7/6/2010 9:38:15 AM | 00:01:48 | 860022306 | 55570 | 020032 | | |
| 7/6/2010 9:40:36 AM | 00:00:16 | | 55546 | 55570 | | |
| 7/6/2010 9:41:56 AM | 00:00:28 | | 55126 | 55550 | | |
| 7/6/2010 9:41:56 AM | 00:02:52 | | 55157 | 55126 | | |
| 7/6/2010 9:40:32 AM | 00:15:57 | 10186139654004 | 55570 | 018023 | | |
| 7/6/2010 9:56:26 AM | 00:00:02 | | 55570 | 55546 | | |
| 7/6/2010 9:56:34 AM | 00:14:40 | | 55157 | 55550 | | |

**Figure 49**

Click on the **Finish** link as shown in **Figure 50** to complete the CDR configuration for VeraSMART

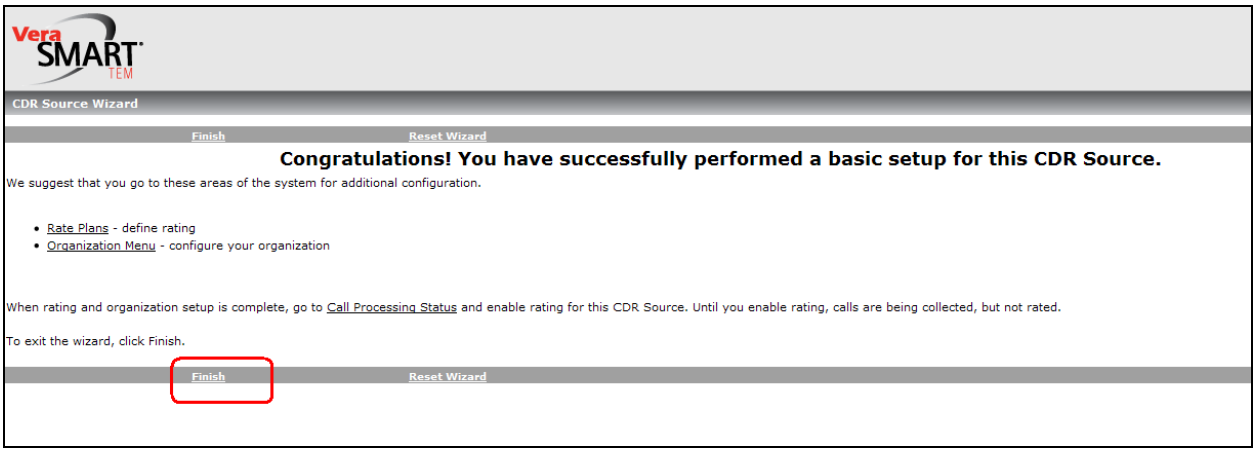



**Figure 50**


©2010 Avaya Inc. All Rights Reserved.

Return to the Home page of CDR Source, click on the new created CDR Source Name, enable "Call Collection Status" and "Rating Status" as shown in **Figure 51** and **Figure 52**. Click "Save" to keep the configuration.

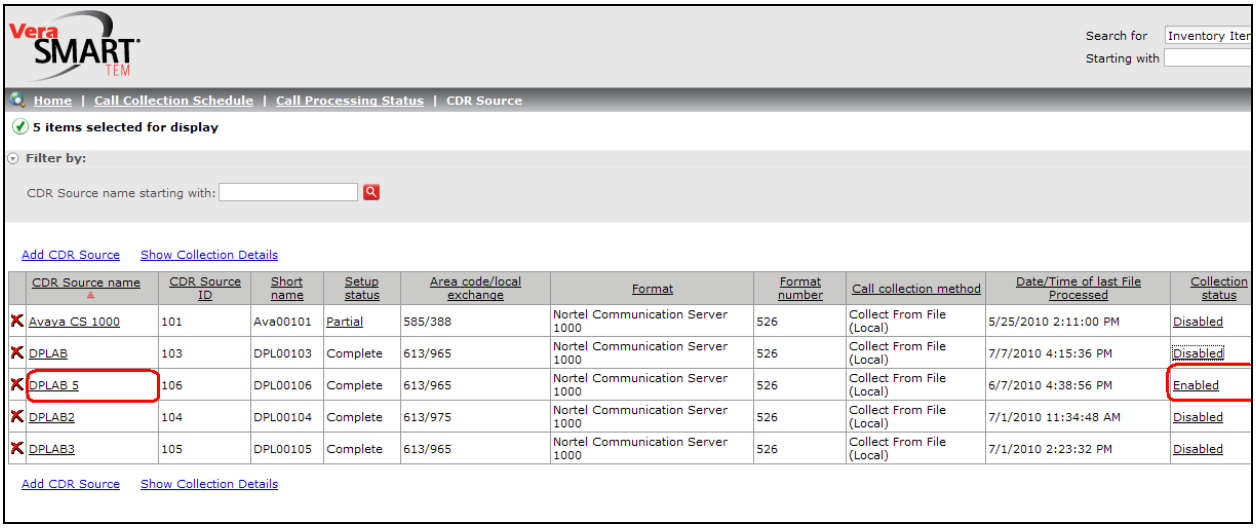



**Figure 51**


**Figure 52**

# 9. Create report on VeraSMART

This section describes the steps to create a VeraSMART report from CDR raw data.


©2010 Avaya Inc. All Rights Reserved.

From the Main window, click on the **Reporting Tab > Reporting > Create/Run Reports** link as shown in **Figure 53**.

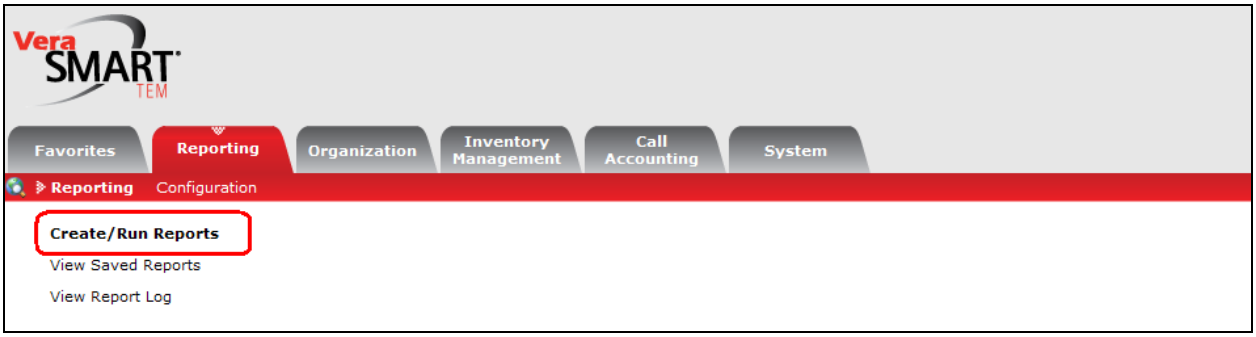



**Figure 53**

On the "**System Reports**" tab, click on the "Call Search Report" as shown in **Figure 54** below.

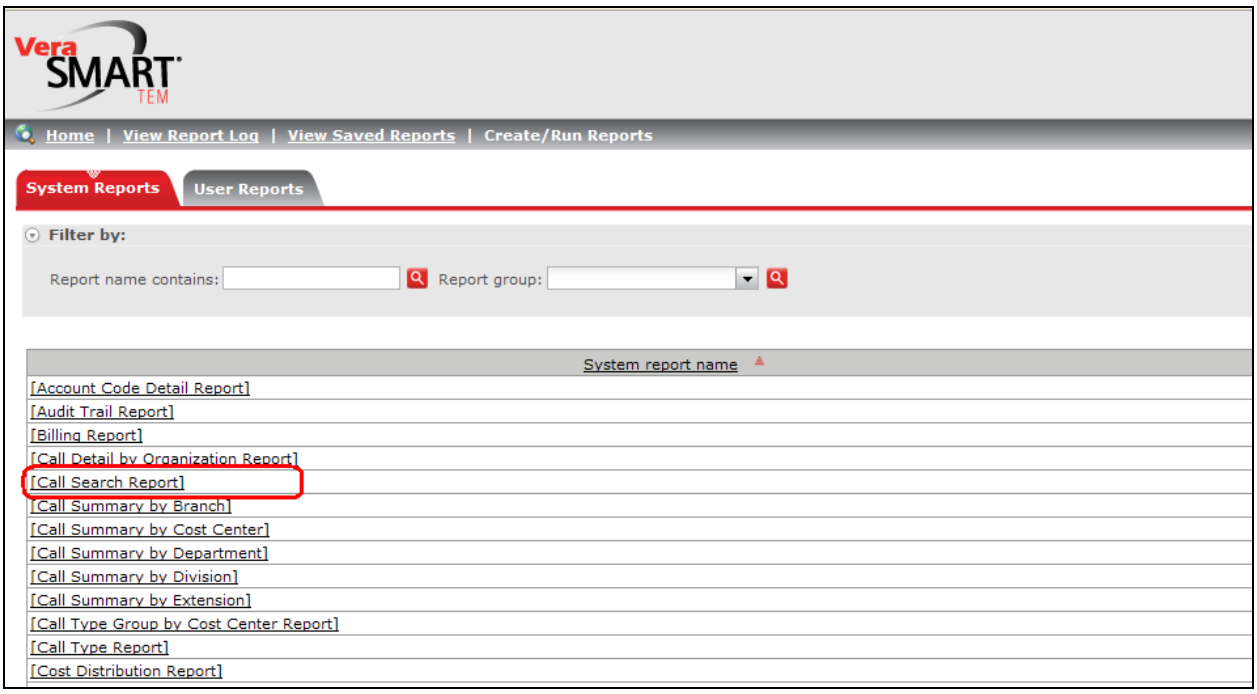



**Figure 54**


©2010 Avaya Inc. All Rights Reserved.

Click on the "**Advanced Criteria**" link to display more criteria for the report as shown in **Figure 55**.

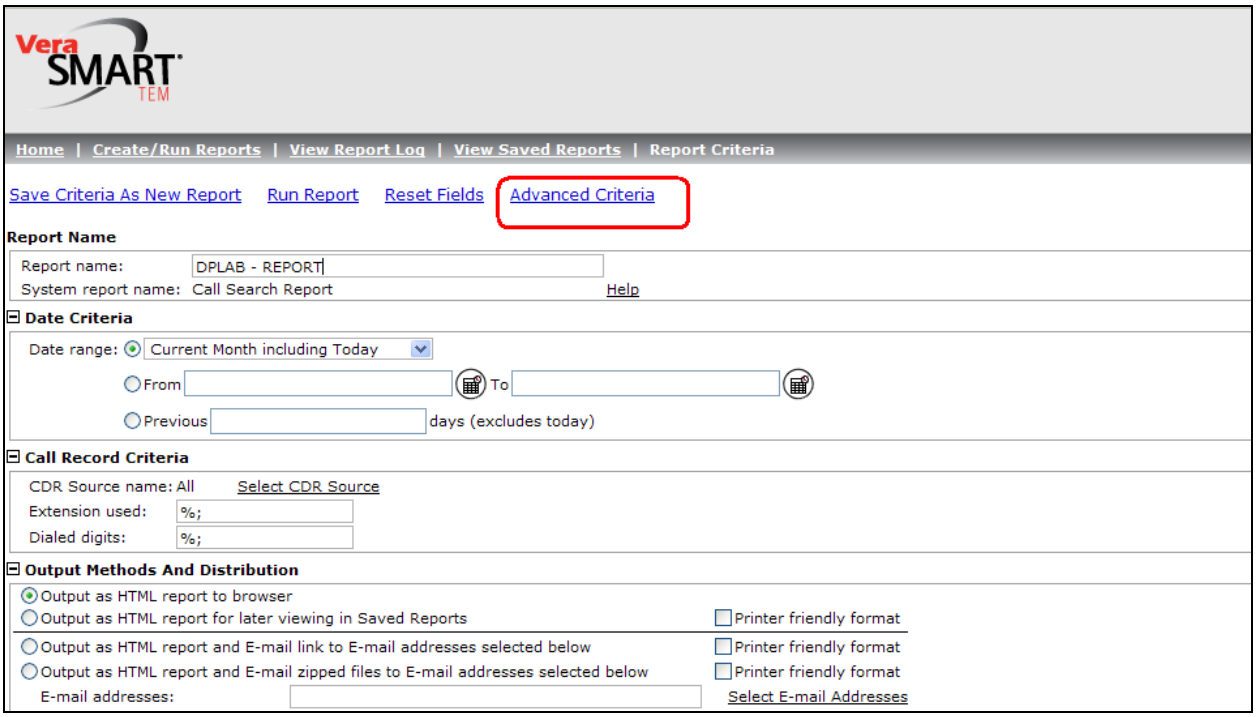



**Figure 55**

Provide the "**Report Name**" as shown in **Figure 56**.

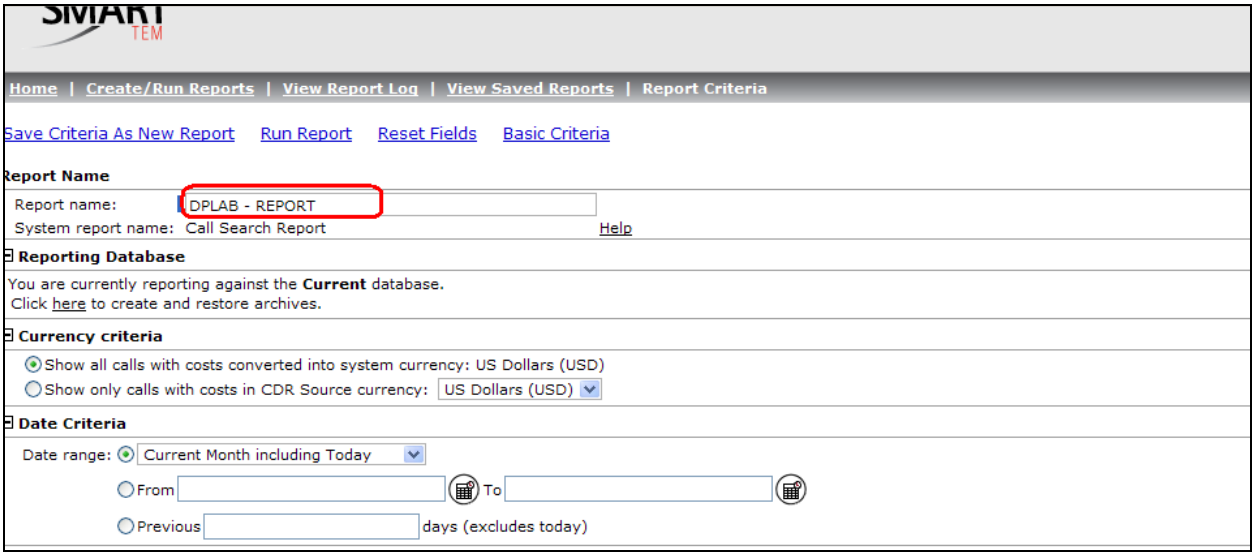



**Figure 56**


©2010 Avaya Inc. All Rights Reserved.

On the "**Details to include in Report**" tree, select some fields to display in the report such as Extension Used, Abandoned, Queue Time, Ring Time, and Unanswered as shown in **Figure 57**.

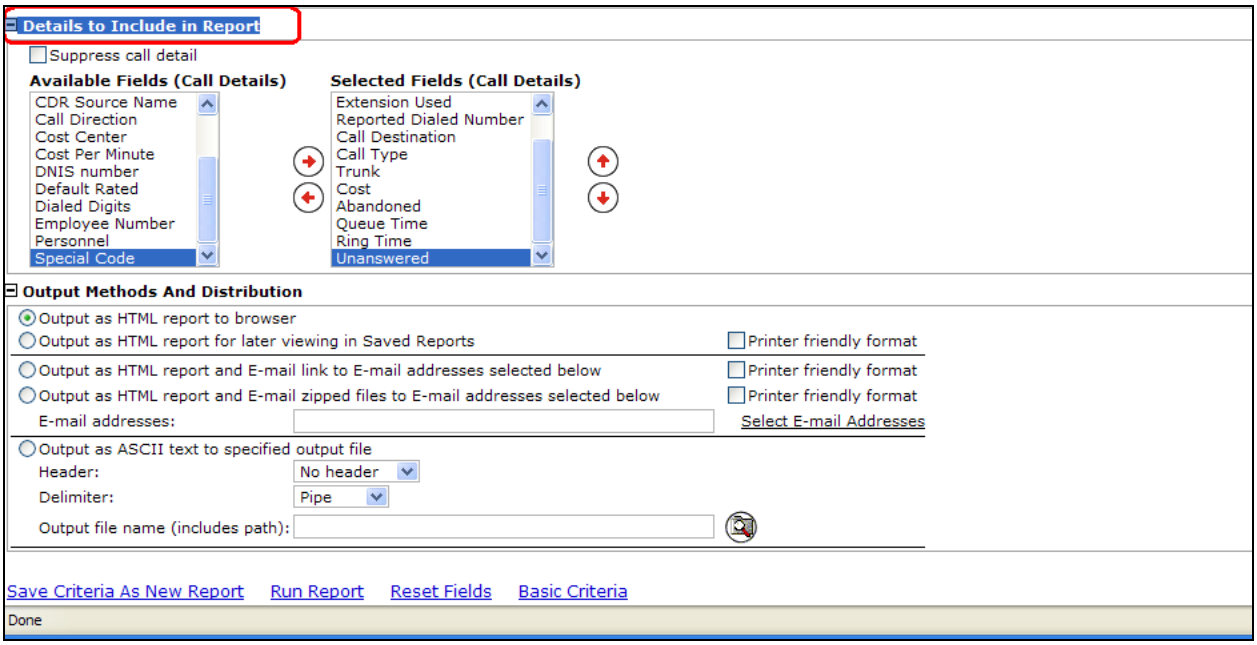



**Figure 57**

Click on the "**Run Report**" link to create the report as shown in **Figure 58** below.

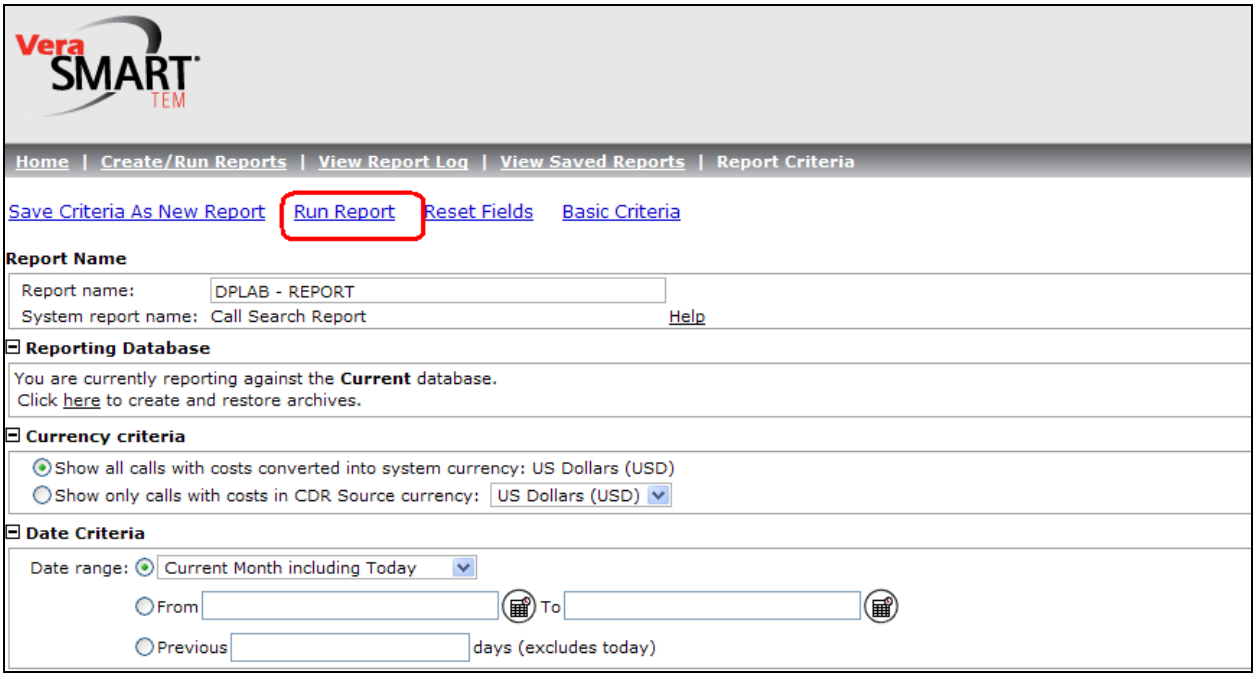



**Figure 58**


©2010 Avaya Inc. All Rights Reserved.

**Figure 59** following shows the final CDR report from VeraSMART.

**DPLAB - REPORT**

**Veramark Technologies, Inc.** Search Criteria

Page 1 of 1

| Start Date/Time | Duration | Extension Used | Reported Dialed Number | Call Destination | Call Type | Tr |
|---|---|---|---|---|---|---|
| 7/1/2010 8:10:05 AM | 13:18:10 | 55570 | 55550 | | Internal | |
| 7/1/2010 8:10:05 AM | 13:18:10 | 55570 | 55550 | | Internal | |
| 7/1/2010 8:10:05 AM | 13:18:10 | 55570 | 55550 | | Internal | |
| 7/1/2010 8:22:40 AM | 0:00:06 | 55546 | 55570 | | Internal | |
| 7/1/2010 8:22:40 AM | 0:00:06 | 55546 | 55570 | | Internal | |
| 7/1/2010 8:22:40 AM | 0:00:06 | 55546 | 55570 | | Internal | |
| 7/1/2010 8:36:39 AM | 0:00:34 | 55546 | 55570 | | Internal | |
| 7/1/2010 9:02:20 AM | 0:07:12 | 55546 | 55570 | | Internal | |
| 7/1/2010 9:05:27 AM | 0:01:28 | 55546 | 55550 | | Internal | |
| 7/1/2010 9:34:50 AM | 0:02:14 | 55570 | | | Incoming | 020001 |
| 7/1/2010 9:36:00 AM | 0:00:36 | 55546 | | | Incoming | 020002 |
| 7/1/2010 9:36:46 AM | 0:00:04 | 55546 | | | Incoming | 020002 |
| 7/1/2010 9:37:22 AM | 0:00:24 | 55546 | 860-022306 | OTTAWAHULL, ON | CANADA | 020032 |
| 7/1/2010 9:37:55 AM | 0:00:04 | 55570 | 860-022306 | OTTAWAHULL, ON | CANADA | 020032 |
| 7/1/2010 9:45:48 AM | 0:00:02 | 55570 | 860-022306 | OTTAWAHULL, ON | CANADA | 020032 |
| 7/1/2010 9:46:01 AM | 0:00:04 | 55570 | | | Incoming | 020001 |
| 7/1/2010 2:21:01 PM | 0:00:26 | 55550 | 55126 | | Internal | |
| 7/1/2010 2:22:19 PM | 0:02:26 | 55546 | 55570 | | Internal | |

**Figure 59**

# 10. General Test Approach and Test Results

The compliance testing included FTP/SFTP operation to allow the VeraSMART application to collect raw CDR data output from the CS1000 Call Server via the DBA/Traffic collector tool. The serviceability test introduced failure scenarios to see if the VeraSMART application can resume CDR collection after recovery.

## 10.1. General test approach

The general test approach was to allow the VeraSMART application to manually FTP/SFTP into the CS1000 Call Server using the credentials that were provided to VeraSMART during the CS1000 Call Server configuration. Once the VeraSMART collects raw data, the VeraSMART transforms raw data into call records available for end customers.

## 10.2. Test Results

All executed test cases passed. VeraSMART successfully collected the CDR records from Avaya Communication Server 1000 Release 6.0 via an FTP/SFTP connection for all types of calls between


©2010 Avaya Inc. All Rights Reserved.

Avaya Communication Server 1000 SIP Line Release 6.0 and PSTN on both SIP Phone and IP Phone. For serviceability testing, VeraSMART was able to resume collection of CDR records after failure recovery including buffered CDR records for calls that were placed during the outages.

The following observation was made during the compliance testing:

- When an user makes a call such as an Abandoned, On-hold, Unanswered or Transfer call with long ring time, the values of the Abandoned, Queue Time, Ring Time and Unanswered fields are not recorded into the raw CDR file from the Call Server. Therefore, the corresponding columns on VeraSMART report always show Zero.

# 11. Verification Steps

This section includes some steps that can be followed to verify the solution is working.

- Make several SIP calls between Avaya Communication Server 1000 SIP Line Release 6.0 and the PSTN on both SIP phone and IP Phone and verify that call records were stored in CDR directory.
- VeraSMART was able to FTP/SFTP into Avaya Communication Server 1000 SIP Line Release 6.0, pull raw data, transfer raw data to VeraSMART, and transform them into a report.

# 12. Conclusion

All of the executed test cases have passed and met the objectives outlined in **Section 10.1**, with some exceptions outlined in **Section 10.2**. The outstanding issues are being investigated by VeraSMART and Avaya design teams. Some of these issues are considered as exceptions. The VeraSMART eCAS Call Accounting software version 9.1.171.11a is considered compliant with CS1000 Release 6.0.

# 13. Additional References

Product documentation for Avaya products may be found at:
http://support.nortel.com/go/main.jsp

*[1] Communication Server 1000 SIP Line Fundamental, Release 6.0, Revision 01.08, February 09, 2010, Document Number NN43001-508*

*[2] Communication Server 1000 ISDN Primary Rate Interface Installation and Commissioning, Revision 01.03, August 01, 2007, Document Number NN43001-301*


©2010 Avaya Inc. All Rights Reserved.

*[3] The CS1000 Data Buffering and Access CDR/Traffic Toolkit*

*https://devconnect.avaya.com/public/dyn/d_dyn.jsp?fn=655*

Product information for VeraSMART products can be found at
http://www.veramark.com


©2010 Avaya Inc. All Rights Reserved.

**©2010 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.