

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.

# 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

Solution & Interoperability Test Lab Application Notes ©2010 Avaya Inc. All Rights Reserved.

## 3. Equipment and Software Validated

System	Software/Loadware Version
CS1000	• Call Server (CPPM): 6.00RJ
	• Signalling Server (CPPM): 6.00.18
	• SIP Line Gateway (HP DL320)
Call Pilot	• CallPilot (600r): 05.00.41.29
SIP softphones	• 02.02.16.00
IP phones	• 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.

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 <u>Section 6.1</u> 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.

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

NØRTEL	UNIFIED COMMUNICATIO	NS MANAGEME	NT		<u>Help</u>				
— Network Elements	Host Name: sipl.ca.nortel.com Software V	<b>ersion:</b> 02.00.0055.00(3266)	User Name admin						
- CS 1000 Services	CS 1000 Services Elements								
SNMP Profiles	New elements are registered into the security	/ framework, or may be added a:	s simple hyperlinks. Click an elem	nent name to launch its management service.					
Secure FTP Token Software Deployment	Add Edit Delete				≣ 23				
- User Services	Element Name	Element Type -	Release	Address	Descripti				
Administrative Users External Authentication	1 EM on coresb	CS1000	6.0	47.248.100.163	New element.				
Password — Security	2 EM on ss2	CS1000	6.0	47.248.100.155	New element.				
Roles Policies	3 EM on sipt	CS1000	6.0	47.248.100.155	New element.				
Certificates Active Sessions	4 🔲 47.248.100.155	Call Server	6.0	47.248.100.155	New element.				
- Tools	5 m sipl.ca.nortel.com (primary)	Linux Base	6.0	47.248.100.235	Base OS element.				
Loga	e 📄 coresb.ca.nortel.com (member)	Linux Base	6.0	47.248.100.201	Base OS element.				
	7 ss2.ca.nortel.com (member)	Linux Base	6.0	47.248.100.206	Base OS element.				
	8 sipt.ca.nortel.com (member)	Linux Base	6.0	47.248.100.194	Base OS element.				
	9 sps1.ca.nortel.com (member)	Linux Base	6.0	47.248.100.234	Base OS element.				
	A7 248 100 152	Media Card	6.0	A7 9A8 100 159	Now				

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.

NØRTEL	UNIFIED COMMUNICATIO	NS MANAGEMENT					<u>Help</u>			
— Network Elements	Host Name: sipl.ca.nortel.com Software Ve	Host Name: sipl.ca.nortel.com Software Version: 02.00.0055.00(3266) User Name admin								
	IPSec For Intra System Sign Centralized IPSec allows network-wide policy	naling Security(ISSS)	of PreShared	l keys across	s network targets listed be	low.				
SNMP Profiles Secure FTP Token	Configuration and Status				Edit Defaults	Synchronize	Activate			
Software Deployment		Security level: Full								
- User Services		Secure all packet	s within and out	side node exc	ept packets in BootP, SSH/SF	TP and SSL ports				
Administrative Users	Sync	hronization status: Sync done. Ref	er to the target	s below for i	ndividual status.					
Password	Activation mode: Graceful									
- Security	Activation status: Activation request sent for existing targets. Refer to the targets below for individual status.									
Roles	Targets (Last synchronization: 29 Jun 2010, 10:56 AM)									
Policies	Add IPSec Required IPSe	c Not Required Delete								
Certificates Active Sessions	1 47.248.100.162 Media Gateway Controller	47.248.100.162	-	Yes	47.248.100.163	Sync done. Activation re	quest sent.			
— Tools	2 M 47.248.100.153 SIPL	sipl.ca.nortel.com (primary)	-	Yes	47.248.100.155	Sync done. Activation re	quest sent.			
Logs	3 🕅 47.248.100.144 SS_EM	ss2.ca.nortel.com (member)	-	Yes	47.248.100.155	Sync done. Activation re	quest sent.			
	4 0 47.248.100.130 SS_NRS_EM	sipt.ca.nortel.com (member)		Yes	47.248.100.155	Sync done. Activation re	quest sent.			
	5 A 47.248.100.141 NRS	sps1.ca.nortel.com (member)	-	Yes	0.0.0.0	Sync done. Activation re	quest sent.			
	8 (47.248.100.155) Call Server	47.248.100.155	-	Yes	47.248.100.155	Sync done. Activation re	quest sent.			
	7 47.248.100.156 Media Gateway Controller	47.248.100.156	-	Yes	47.248.100.155	Sync done. Activation re	quest sent.			
	8 A 47.248.100.163 CS_SS_EM	coresb.ca.nortel.com (member)	-	Yes	47.248.100.163	Sync done. Activation re	quest sent.			
	<									
	* Targets with customized IPSec parameters									

Figure 3: IPSec for Intra System Signaling Security

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.

NØRTEL	UNIFIED COMMUNICATIONS MANAGEMENT	Help
- Network Elements	Host Name: sipl.ca.nortel.com Software Version: 02.00.0055.00(3266) User Name admin	
IPSec	Custom IPSec Details	
Patches SNMP Profiles Secure FTP Token Software Deployment — User Services Administrative Users External Authentication Password — Security Roles Policies	IP Address: 47.248.100.155 Security level: Full  Secure all packets within and outside node except packets in BootP, SSH/SFTP and SSL ports PreShared key:  PreShared Key should not contain any of "Space ~ * "@[]#". Confirm PreShared key:  *	
Certificates Active Sessions	* Required value. Restore Default Settings Save and Synchronize	Cance
— Tools Logs		

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.

NØRTEL	UNIFIE	D COMM	UNICATIC	NS MANA	GEMENT					<u>Help</u>
— Network Elements	Host Nam	Host Name: sipl.ca.nortel.com Software Version: 02.00.0055.00(3266) User Name admin								
— CS 1000 Services IPSec Patches	IPSec Centralize	IPSec For Intra System Signaling Security(ISSS) Centralized IPSec allows network-wide policy implementation and synchronization of PreShared keys across network targets listed below								
SNMP Profiles Secure FTP Token	Configu	ration and S	tatus					Edit Defaults	Synchronize	Activate
Secure FIP Token Software Deployment — User Services Administrative Users External Authentication Password		Security level: Full Secure all packets within and outside node except packets in BootP, SSH/SFTP and SSL ports Synchronization status: Sync done. Refer to the targets below for individual status. Activation status: Activation required.								
- Security Roles	Targets (	Targets (Last synchronization: 06 Jul 2010, 03:13 PM)								
Policies Certificates	Add	IPSec	Required IPS:	ec Not Required	Delete					
Active Sessions		P Address	Type	<u>Name</u>		State +	IPSec	Associated Call Server	Sync/Activation status	
- Tools	1 🕅 4	7.248.100.162	Media Gateway Controller	47.248.100.162		-	Yes	47.248.100.163	Sync done. Activation required.	
Logs	2 🛄 4	7.248.100.153	SIPL	sipl.ca.nortel.com	(primary)	-	Yes	47.248.100.155	Sync done. Activation required.	
	3 🕅 4	7.248.100.144	SS_EM	ss2.ca.nortel.com	(member)	-	Yes	47.248.100.155	Sync done. Activation required.	
	4 🗖 4	7.248.100.130	SS_NRS_EM	sipt.ca.nortel.com	(member)	-	Yes	47.248.100.155	Sync done. Activation required.	
	5 🛄 4	7.248.100.141	NRS	sps1.ca.nortel.com	n (member)	-	Yes	0.0.0.0	Sync done. Activation required.	
	o 🗆 🤇	7.248.100.155	Call Server	47.248.100.155		-	Yes	47.248.100.155	Sync done. Activation required.	
	7 🗖 4	7.248.100.156	Media Gateway	47.248.100.156		-	Yes	47.248.100.155	Sync done. Activation required.	_
	* Targets w	vith customized I	PSec parameters							

**Figure 5: IPSec Synchronization** 

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

N@RTEL	UNIFIED COMM	IUNICATIO	NS MANAGEMEN	т				Help	
— Network Elements	Host Name: sipl.ca.nortel.com Software Version: 02.00.0055.00(3266) User Name admin								
— CS 1000 Services IPSec Patches	IPSec For Intra System Signaling Security(ISSS) Centralized IPSec allows network-wide policy implementation and synchronization of PreShared keys across network targets listed below.								
SNMP Profiles Secure FTP Token	Configuration and St	atus				Edit Defaults	Synchronize	Activate	
Software Deployment			Security level: Full						
Administrative Lisers			Secure all pack	ets within and o	outside node exc	cept packets in BootP, SSH/SF	TP and SSL ports		
External Authentication		Sync	hronization status: Sync done. R	efer to the targ	jets below for i	ndividual status.			
Password	Activation status: Activation required.								
- Security	Click Activate (above) to send a forced or graceful activation request to targets below.								
Roles	Targets (Last synchronization: 06 Jul 2010, 03:13 PM )								
Policies	Add IPSec F	Required IPSe	c Not Required Delete						
Certificates	IP Address	Туре	Name	State -	IPSec	Associated Call Server	Sync/Activation status		
- Tools	1 47.248.100.162	Media Gateway Controller	47.248.100.162	-	Yes	47.248.100.163	Sync done. Activation required.		
Logs	2 47.248.100.153	SIPL	sipl.ca.nortel.com (primary)	-	Yes	47.248.100.155	Sync done. Activation required.		
	3 47.248.100.144	SS_EM	ss2.ca.nortel.com (member)	-	Yes	47.248.100.155	Sync done. Activation required.		
	4 47.248.100.130	SS_NRS_EM	sipt.ca.nortel.com (member)	-	Yes	47.248.100.155	Sync done. Activation required.		
	5 47.248.100.141	NRS	sps1.ca.nortel.com (member)	-	Yes	0.0.0.0	Sync done. Activation required.		
	6 <u>47.248.100.155</u>	Call Server	47.248.100.155	-	Yes	47.248.100.155	Sync done. Activation required.		
	7 47.248.100.156	Media Gateway	47.248.100.156	-	Yes	47.248.100.155	Sync done. Activation required.		
	*	~ • •						1	
	* Targets with customized IF	Sec parameters							

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.

NØRTEL	UNIFIED COMMUNICATIONS MANAGEMENT	Help
NORTEL  - Network Elements - CS 1000 Services IPSec Patches SNMP Profiles Secure FTP Token Software Deployment - User Services Administrative Users External Authentication Password - Security Roles Policies Certificates Active Sessions	UNIFIED COMMUNICATIONS MANAGEMENT Host Name: sipl.ca.norfel.com Software Version: 02.00.0055.00(3266) User Name admin IPSec Activation details Activation type Graceful  Activation type Graceful  Activate the changes with minimum system impact. Pre- Shared Keys will be applied when needed to reduce possible service impacts.	Help I Activate Ca
— Tools Logs		

**Figure 7: Activation Type** 

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

N@RTEL	UNIFIED COMMUNICATIO	ONS MANAGEMENT					<u>Help</u>		
Network     Elements     CS 1000 Services     IPSec	Host Name: sipl.ca.nortel.com Software Version: 02.00.0055.00(3266) User Name admin IPSec For Intra System Signaling Security(ISSS)								
Patches	Centralized IPSec allows network-wide policy implementation and synchronization of PreShared keys across network targets listed below.								
SIMP Profiles Secure FTP Token	Configuration and Status				Edit Defaults	Synchronize	Activate		
SIMP Profiles Secure FTP Token Software Deployment User Services Administrative Users External Authentication Password Security Roles Policies Certificates Active Sessions Tools Logs	Syn Targets (Last synchronization: 06 Jul 2010, Add PSec Required PSi 2 47.248.100.153 SIPL 3 47.248.100.144 SS_EM 4 7.248.100.130 SS_NRS_EM 5 47.248.100.135 Call Server 7 47.248.100.155 Call Server 7 47.248.100.155 Call Server 8 47.248.100.155 Call Server 9 47.248.100.132 Media Gateway Controller 8 47.248.100.132 Media Gateway	Security level: Full Secure all packe chronization status: Sync done. Re Activation mode: Graceful Activation mode: Graceful Activation status: Activation requ 03:13 PM ) en for Required Delete sipil ca.nortel.com (member) sipil ca.nortel.com (member) sps1 ca.nortel.com (member) 47:248.100.155 47:248.100.155	s within and ou er to the targe est sent for ex - - - - - - - - - - - - - - - - - - -	tside node exits below for isting targets Yes Yes Yes Yes Yes Yes Yes Yes Yes	Cept packets in BootP, SSH/S individual status. 8. Refer to the targets belo 47.248.100.155 47.248.100.155 0.0.0 47.248.100.155 47.248.100.155 47.248.100.155 47.248.100.155 47.248.100.155	FTP and SSL ports w for individual status. Sync done. Activation requ Sync done. Activation requ	est sent. est sent. est sent. est sent. est sent. est sent. est sent.		
	* Targets with customized IPSec parameters								

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.

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

NØRTEL	UNIFIED COMMUNICATIO	ONS MANAGEMENT	-		Help				
— Network Elements	Host Name: sipl.ca.nortel.com Software V	Version: 02.00.0055.00(3266) Use	er Name admin						
— CS 1000 Services IPSec Patches	IPSec For Intra System Signaling Security(ISSS) Centralized IPSec allows network-wide policy implementation and synchronization of PreShared keys across network targets listed below.								
SNMP Profiles Secure FTP Token	Configuration and Status			Edit Defaults	Synchronize Activate				
Secure i i Protein Software Deployment — User Services Administrative Users External Authentication Password — Security Roles Policies Certificates Active Sessions — Tools Logs	Syn Targets (Last synchronization: 06 Jul 2010,	Security level: Full Secure all packe chronization status: Sync done. Ref Activation mode: Graceful Activation status: Activation requi 03:13 PM)	is within and outside no fer to the targets belo est sent for existing t	de except packets in BootP, SSH/ w for individual status. argets. Refer to the targets bel	SFTP and SSL ports ow for individual status.				
	Aud         Tesses regulation         Tess           2         47.248.100.153         SIPL         3           3         47.248.100.154         SS_EM           4         74.248.100.144         SS_EM           5         47.248.100.141         NRS           6         47.248.100.155         Call Server           7         47.248.100.155         Call Server           7         47.248.100.156         Media Gateway Controller           8         47.248.100.153         CS_SS_EM           9         47.248.100.132         Media Gateway           4         47.248.100.132         Media Gateway	sipi.ca.nortel.com (primary) ss2.ca.nortel.com (member) sipi.ca.nortel.com (member) sps1.ca.nortel.com (member) 47.248.100.155 47.248.100.156 coresb.ca.nortel.com (member) 47.248.100.132	- Yes - Yes - Yes - Yes - Yes - Yes - Yes	47 248.100.155 47 248.100.155 47 248.100.155 0.0.0 47 248.100.155 47 248.100.155 47 248.100.163 47 248.100.155	Sync done. Activation request sent. Sync done. Activation request sent.				

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.

NØRTEL	UNIFIED COMMUNICATIONS MANAGEMENT	Help
— Network Elements	Host Name: sipl.ca.norfel.com Software Version: 02.00.0055.00(3266) User Name admin	
<ul> <li>— CS 1000 Services IPSec</li> </ul>	New Manual IPSec Target	
Patches SNMP Profiles Secure FTP Token	IP Address1: 47.248.100.36 * IP Address2:	
Software Deployment — User Services Administrative Users	Friendly name: VeraSmart * (1-32 characters)	
External Authentication Password — Security	ir-Secreduied.	
Roles Policies	Note After saving, the target must be Synchronized in order to receive the common IPSec configuration parameters you have defined.	-
Active Sessions	* Required value.	Cance
- Iools Logs		

Figure 10: Manual IPSec Target Configuration

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

	UNIFIED COM	IUNICATIO	ONS MANAGEMEN	Т				<u>Help</u>		
— Network Elements	Host Name: sipl.ca.nortel	l.com Software V	Version: 02.00.0055.00(3266) U	ser Name adr	min					
- CS 1000 Services IPSec	IPSec For Intra	System Sig	naling Security(ISSS	;) ion of PreSha	red keys across	network targets listed bel	low			
SNMP Profiles Secure FTP Token	Configuration and St	atus				Edit Defaults	Synchronize	Activate		
Software Deployment			Security level: Full							
- User Services			Secure all pac	kets within and	outside node exc	ept packets in BootP, SSH/SF	TP and SSL ports			
Administrative Users		Syn	chronization status: Sync done. F	efer to the targ	gets below for in	ndividual status.				
External Authentication			Activation mode: Graceful							
- Security		Activation status: Activation request sent for existing targets. Refer to the targets below for individual status.								
Roles	Targets (Last synchroni	Targets (Last synchronization: 06 Jul 2010, 03:13 PM )								
Policies	Add IPSec	Required IPS:	ec Not Required Delete							
Active Sessions	IP Address	Type	Name	State +	IPSec	Associated Call Server	Sync/Activation status			
- Tools	1 47.248.100.162	Media Gateway Controller	47.248.100.162	-	Yes	47.248.100.163	Sync done. Activation request se	ent.		
Logs	2 47.248.100.153	SIPL	sipl.ca.nortel.com (primary)	-	Yes	47.248.100.155	Sync done. Activation request se	ent.		
	3 47.248.100.144	SS_EM	ss2.ca.nortel.com (member)	-	Yes	47.248.100.155	Sync done. Activation request se	ent.		
	4 47.248.100.130	SS_NRS_EM	sipt.ca.nortel.com (member)	-	Yes	47.248.100.155	Sync done. Activation request se	ent.		
	5 47.248.100.141	NRS	sps1.ca.nortel.com (member)	-	Yes	0.0.0.0	Sync done. Activation request se	ent.		
	8 <u>47.248.100.155</u>	Call Server	47.248.100.155	-	Yes	47.248.100.155	Sync done. Activation request se	ent.		
	7 7 47.248.100.156	Media Gateway	47.248.100.156	-	Yes	47.248.100.155	Sync done. Activation request se	ent.		
	*	· · ·								
	* Targets with customized IF	Sec parameters								

Figure 11: Edit Defaults

 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.

NØRTEL	UNIFIED COMMUNICATIONS MANA	GEMENT	Help
— Network Elements	Host Name: sipl.ca.nortel.com Software Version: 02.00.0055.	00(3266) User Name admin	
<ul> <li>— CS 1000 Services</li> <li>IPSec</li> </ul>	<b>IPSec Configuration Details</b>		
Patches SNMP Profiles	Security level:	Full v	
Secure FTP Token Software Deployment		Secure all packets within and outside node except packets in BootP, SSH/SFTP and SSL ports	
- User Services	PreShared key:	**************************************	
Administrative Users External Authentication		PreShared Key should not contain any of "Space ~ * ` @ [] # ".	
Password	Confirm PreShared key:	*	
- Security Roles			
Policies			2
Active Sessions	* Required value.	Save and Synchronize	Cance
— Tools			1
Logs			

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).

Solution & Interoperability Test Lab Application Notes ©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.

DiPSec MMC console			. 🗆 🖂	
File Action View Favorites ↔ →	Mindow Help Add/Remove Snap:In	2 🗙		
Console Root	Standalone Extensions Use this page to add or remove a standalone Smpirit added to Controle Root	Snapin from the console Add Standalone Snap-In Available Standalone Snap-in: Snap-in Folder FondPage Server Extensions Statistic Statistics Statistics Proceeding Paley Dispet Edite Internet Homation Services Proceeding Monitor Proceeding Monitor Proceedi	Vendor Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation	
	Add. Benove Abou	Decorption     Terrorent Organic Adets     Decorption     Internet Protocol Security (IPSec) Adm     policies for secure communication with	Microsoft Corporation s inistration. Manage IPSec other computers.	N 6 9

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.

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.

Ta IPSec MMC console Ele Action View Favorites Window ( ← → III E3 (2) III	140 1	LOX
Te Console Root	Name IP Security Policies on Local Comp P Security Monitor	

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 <u>Section 5.1</u> above.
  - 6. Right-click **IP Security Policies on Local Computer Policy** in the left-hand pane of the subsequent window.

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

IP Security Policy Wizard	?×
	Welcome to the IP Security Policy Wizard
	This wizard helps you create an IP Security policy. You will specify the level of security to use when communicating with specific computers or groups of computers (subnets), and for particular IP traffic types.
	To continue, click Next.
	<u>≪B</u> ack <u>Next&gt;</u> Cancel

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.

Name this security p	olicy and optional	ly give it a brief de	scription	
Name:				
WINXP IP Security	Policy			
Description				
- 11				*

Figure 16

- 10. Enter a description in the Description text box.
- 11. Click Next.

QT; Reviewed: SPOC 9/13/2010 Solution & Interoperability Test Lab Application Notes ©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.

Requests for Secure Communication		=
Specify how this policy responds to rea	uests for secure communication.	
The default response rule responds to other rule applies. To communicate ser secure communication.	emo:e computers that request se curely, the computer must respond	curity, when no I to requests for
Activate the default response rule.		

Figure 17

- 13. Click Next.
- 14. DO NOT place a check mark in the "Edit properties" check box as shown in Figure 18.

IP Security Policy Wizard	
	Completing the IP Security policy wizard You have successfully completed specifying the properties for your new IP Security policy. To edit your IP Security policy now, select the Edit properties check box, and then click Finish.
	To close this wizard, click Finish.
	< Back Finish Cancel

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.

QT; Reviewed:	Solution & Interoperability Test Lab Application Notes	
SPOC 9/13/2010	©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 <u>Section 5.1</u> 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.

Security Rule Wizard	<u>?</u> ×
	Welcome to the Create IP Security Rule Wizard         A security rule governs how and when security is invoked based upon criteria, such as the source, destination, and type of IP traffic, in the security rule's IP filter list.         A security rule contains a collection of security actions that are activated when a communication matches the criteria in the IP filter list.         Security actions: <ul> <li>IP tunneling attributes</li> <li>Authentication methods</li> <li>Filter actions</li> </ul> To continue, click Next.
	< Back Next > Cancel

Figure 19

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

Ti	el Endpoint he tunnel endpoint is the tunneling computer closest to the IP traffic destination, s specified by the security rule's IP filter list.
Ar	IPSec tunnel allows packets to traverse a public or private internetwork with the
se	curity level of a direct, private connection between two computers.
Sp	secify the tunnel endpoint for the IP Security rule:
•	This rule does not specify a tunnel
C	The tunnel endpoint is specified by this [P address:
	0.0.0.0

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.

curity Rule Wizard			?
Network Type The security rule must be applied to a petwo	rk hine		
The second role mass be applied to a nervo	in type.		-
Select the network type:			
All network connections			
C Local area network (LAN)			
C Bemote access			
	< <u>B</u> ack	<u>N</u> ext>	Cancel

Figure 21

#### 13. Click Next

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

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.

uthentication Method		E
To add multiple authentication methods, IP Security rule wizard.	edit the security rule after comple	ting the
Set the initial authentication method for th	is security rule:	
C Active Directory default (Kerberos V5	protocol)	
Use a certificate from this certification	authority (CA):	
		Blowse
Use this string to protect the key excl	ange (preshared key):	
TmServerIpsecConfiguration		~
		×

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.

If no IP filter in the following list	matches your needs, click Add to creat	e a new one.
IP filter lists:		
Name	Description	Add
O ALL ELAN IP Filter List	First time configurations	Edit
O ALL ELAN IP Traffic	Matches all ICMP packets bet	Remove
O All IP Traffic	Matches all IP packets from t	
1		

Figure 23

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.

				I IP Traffic	ALL ELAN
dd				ĸ	Description
dit	~				
move	2				
Wizard	Iv Use				Filter <u>s</u> :
stination	et	Source	Protocol	Description	Mirrored
1 17	rt Use	Source	Protocol	Description	Filter <u>s</u> : Mirrored

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

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

IP Traffic Source		-
Specify the source address of the IP	traffic.	7
Source address:		
My IP Address		
	< <u>₿</u> ack <u>N</u> ext> Canc	el
	- Idew - Gano	-

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.

Traffic Source Specify the source address	of the IP	tra	ffic.						
Source address:									
A specific IP Address						-			
IP Address:	0	×.	0	4	0		0		
Subnet mask:	255		255		255		255		
					25 0.07			_	

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

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

IP Filter Wizard	?×
IP Protocol Type Select the IP protocol type. If this type is TCP or UDP, you will also specify the source and destination ports.	Ē
Select a protocol type:	
< Back Next >	Cancel

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.

Security	y Rule Wizard		? ×
Filte	r Action Select the filter action for this secu	irity rule.	
	If no filter action in the following lis Select Use Add Wizard to create a	t matches your needs, click Add to a filter action using the wizard.	create a new one.
1	Filter Actions:	<b>v</b>	Use Add <u>W</u> izard
	Name	Description	Add
	O ELAN Security	a	
	O Permit	Permit unsecured IP packets t	<u>E</u> dit
	O Request Security (Optional) O Require Security	Accepts unsecured communi Accepts unsecured communi	Remove
		< <u>B</u> ack Nex	t> Cancel

Figure 29

Solution & Interoperability Test Lab Application Notes ©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.

	? ×
	67
c Dark Navi Cance	
	< <u>Back</u> <u>Next&gt;</u> Cance

Figure 31

39. Select Negotiate security.

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.

ID Tes	His Security	-
Sp filte	ecity a security method for IP traffic. To add multiple security methods, edit the er action after completing the wizard.	16
Th	s filter action requires at least one security method for IP traffic.	
¢	Integrity and encryption	
	Data will be encrypted, authenticated, and unmodified.	
C	Integrity only	
	Data will be authenticated and unmodified, but will not be encrypted.	
C	Custom	
	Settings	

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.

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.

onsole Root	Name /	Description		Policy Assigned	
IP Security Policies on Local Compute	Clent (Respond Only Secure Server (Request Secure Content)	<ul> <li>Communicate r ir For all IP trafficu</li> <li>For all IP trafficu</li> </ul>	ormally (uns c, always req c, always req	No No No	
	WINDP IP Security P	Astion	r first time	No	
	XP ELAN IPSec Pole	All Tasks +		No	
		Delete Rename			
<>	¢	Properties			>
	difference in the	Help			

Figure 33

9. Open a DOS command window.

Solution & Interoperability Test Lab Application Notes ©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.

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

New Session			
Select Session:	47.248.100.155	Remove	Connect Now
Network			Cancel
IP Address:	47 . 248 . 100 . 155	Collect:	
		💌 CDR	
User ID:	admin	💌 Traffic	
Password:	XXX		
FTP Username:	admin	🔽 Default Credentials	
FTP Password:	жжение	SFTP	



- 3. Enter the ELAN IP address of the Call Server in the IP Address box.
- 4. Enter the login name in the User ID box.
- 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 dependent 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]

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

#### 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.

# 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.

🕹 Login to VeraSMART - Mozilla Firefox	
Ele Edit View Higtory Bookmarks Tools Help	
😮 🕞 🕈 🖒 🕅 http://ocalhost/CAS/enu/Login.aspx?fromASP=Y&.	Google
🔊 Most Visited 🗋 Getting Started 🔊 Latest Headlines 🗋 Suggested Sites 🗋 Web Slice Gallery 材 VeraSMART	
√ Login to VeraSHART	
Vera SMART.	
Login to VeraSMART	
VeraSMART Application Login	
Login ID: admin	
Password:	
Forgot password? Login	
This application has also been configured to	
use your organization's single sign-in option. Click the button below to login using	
this option.	
Login via Windows	

Figure 37

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.

Vera SMART.	Search for Inventory I Starting with
Favorites Reporting Organization Inventory Call Accounting System	
Call Processing Status	
CDR Source Call Home	
Call Sender	





Figure 39

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

Vera SMART.
CDR Source Wizard
Next Cancel Reset Wizard
Welcome
To use this Call Accounting System, you will need to create a CDR Source for each call record source. If you are collecting calls from two phone systems, then you will need to create two CDR Source records. E a name, and it will be configured so that you can collect, rate, and report on call records.
This wizard will help you configure a new or partially setup CDR Source. If you are resuming a setup, the wizard will remember all items previously defined.
You will need to provide specific instructions in a series of steps. This will include information related to the local exchange and rate services. Then, depending on the call collection method to be used, you may n modem or COM port used, the CDR Source baud rate, remote modem phone number, collection file name, etc.
Not all of these items need to be addressed at once, since the wizard can resume the setup where you left off. Consult your CDR Source technician or vendor, if needed.
Please click Next to continue.
Next Carel Basel Wood

#### 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.

Vera SMART				
CDR Source Wizard				
Back	<u>Next</u>	Cancel	<u>Reset Wizard</u>	
				Identify the source of call records.
Create a CDR Source nam	ne. Use up to 25 alp	hanumeric characters	for a unique name	(this can be anything that makes sense to you to reference this CDR Source - for example: East Coast, New York Office, Main
CDR Source area CDR Source name* Country: Area code*: Local exchange*: Local rate method: Do you want to discard the	a code, local exchar DPLAB 4 613 965 None • e following types of	rge, and local rating m	ethod (this dependence? These choices	Is on the rate service used locally - for example: measured, message, flat, etc.). : can be changed later through the 'edit' CDR Source function.
* denotes a required fie	eld	Store Obiscard		
<u>Back</u>	Next	<u>Cancel</u>	<u>Reset Wizard</u>	

#### Figure 41

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.

Vera SMART		
CDR Source Wizard		
Back	Next Cancel	Reset Witzerd
Duck	<u>next</u> <u>conce</u>	Select the CDP Source manufacturer
Eveny telephone system produ	uces call records in a specific format. T	he sustem uses "format" activities to internet call record data
Livery telephone system prout	aces can records in a specific format.	ne system uses format soltware to interpret can record data.
From the list, select the manu	facturer of the CDR Source, or if collec	ting call records from another call accounting system select "Call Accounting System", then click Next to continue.
Currently assigned Format	None	
Manufacturer:	Nortel	
Back	3COM	Reset Wizard
	Aastra	
	Avava	
	Call Accounting System	
	Cisco	
	Comdial	
	Ericsson	
	Executone	
	Fuiitsu	
	INFO Monitor MP	
	Intecom	
	InterTel	
	пт	
	Iwatsu	
	Mitel	
	NEC	
	Nortel	
	Panasonic	
	Samsung	
	SBC/Ameritech	
	Siemens	
	Sprint	
	Tadiran	
1	I OSNIDA	
	vodavi	

#### Figure 42

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



#### Figure 43

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.

Vera S	MART							
CDR 50	burce Wizard							
Below y	Back Noxt Cancel Roset Wizard Select the call record format. elow you will see a list of CDR Source formats for this manufacturer. Select the call record format used by your CDR Source (if you need help to decide on a specific choice, click its help link). Then click Next to							
	Format name	Format description	CDR Source software release	Format number				
0?	Nortel SL100	SL100		95	2.5.14			
0?	(511)Nortel Meridian	SL1 X11 (New Format) - Options 11 and 61	X11 r20+	511	2.8			
0?	(517)Nortel Meridian	SL1 X11 (Old Format) - Options 11 and 61	1-18	517	2.1.17			
0?	(518)Nortel	Norstar (Standard format)		518	2.4.11			
0?	(523)Nortel BCM	BCM Norstar Format, Legacy	_	523	2.6.14			
0?	Nortel Communication Server 1000	Communication Server 1000 - FCDR = NEW	4.0, 5.0	526	1.3.12			
0?	(527)Nortel BCM	BCM50, BCM 3.7; Norstar Format		527	1.2.14			
	<u>Back Next Cancel</u>	Reset Wizard						

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**.

Vera SI	MART.					
CDR Sou	urce Wizard					
	<u>Back Next</u>	Cancel Reset Wizard				
			Select the call collection method.			
Below you	u will see a list of call collection method	s. Select the method that best des	cribes the way your calls will be collected. Then click Next to continue.			
	Call collection met	hod name 🄺	Call collection method description			
• ?	Collect From File (Local)		Calls are processed from file on the local hard drive.			
0 ?	Direct Connect		Calls are collected through a physical connection to the phone system.			
○?	Direct Connect over IP		Calls are processed over an IP network connection.			
0?	PollComm Direct		Calls are polled from a Pollable Storage Unit through a cable.			
0?	PollComm Network		Calls are collected from a Pollable Storage Unit over a TCP-IP network.			
0?	PollComm Remote		Calls are polled from a Pollable Storage Unit, by modem.			
	<u>Back Next</u>	Cancel Reset Wizard				

Figure 45

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** 

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

Vera SMART.		
CDR Source Wizard		
Back	Cancel	Reset Wizard
		Please wait while call records are retrieved
If polling a remote unit, this process may tak	ke a few minutes. If t	the CDR Source is not yet connected, click Cancel to exit (when ready, return here to validate CDR Source configuration).
If no call records are displayed, there may b	e issues with setting	s or connectivity. Click the following link for a help page of possible reasons why no calls are displayed.
No Calls Help		
Back	Cancel	Reset Wizard

Figure 47

Click on the Next link.

Back	Next	<u>Cancel R</u>	leset Wizard	
				Raw Call Re
s a list of 'raw' (uni	formatted) call record	is coming from the CDF	Source. Check the lines of data u	inder the header row and determine if they look valid, without 'garbage' characters.
click Next to conti	nue. Otherwise, click	Back to return to the c	all collection method page, change	the settings, and return to the test viewers again.
Call Record Viewe	r Help			
				Raw
3456789a123	456789b1234567	89c123456789d12	23456789e123456789f1234	456789g123456789h123456789i123456789j123456789k123456789l1234567
003 00 55546	1018023 07/06	09:01:28	1234	000 000
004 00 55546	T018023 07/06	09:01:30 00:00:0	0.0 A10186139654004	000.000
		000		000 000
005 00 55546	T018023 07/06	09:05:35	1234	
				000 000
006 00 55546	T018023 07/06	09.05.37 00.00.0	12 0 310186139654004	
000 00 00010	1010020 01.00	07.00.01 00.00.0		000 000
		000		
007 00 55570	T018023 07/06	09:12:07	1234	000 000
				000 000
008 00 55570	T018023 07/06	09:12:10 00:00:0	6.0 A10186139654004	
				000 000
009 00 55546	T019023 07/06	09-12-14	1234	

Figure 48

Figure 49 shows the CDR report from VeraSMART.

CDR Source Wizard						
Back Next	Cancel Reset	Wizard				
		Formatte	d Call Record	l Viewer		
elow is a list of formatted call records. Check	under the column headings a	and determine if they look valid				
clow is a list of formatical call records. Check	ander the column headings t	na determine in they look valid.				
valid, click Next to continue. Otherwise, click	Back to return to the call red	ord format page, make another sel-	ection, and return to th	ne test viewers again.		
Formatted Call Record Viewer Help						
Deta liine e	Duration	Distant surplus	0	Destination	A	
Date/time	Duration	Dialed number	Source	Destination	Account code	1004
7/6/2010 9:01:30 AM	00:00:00	10186139654004	55546	018023		1234
7/6/2010 9:03:37 AM	00:00:02	10186139654004	55540	018023		1234
7/6/2010 9:12:10 AM	00:00:00	10186139654004	55570	010023		1234
7/6/2010 9:13:17 AM	00:23:30	10186139634004	020001	55570		1234
7/6/2010 9:13:30 AM	00.24.20		020001	55570		
7/D/ZUTU 9:37:23 AM	00:01:08		010023	55546		
7/6/2010 0:14:07 AM	(101) - 10 - 10 - 10 - 10 - 10 - 10 - 10		010022	00000		
7/6/2010 9:14:07 AM	00:24:40		55106	55453		
7/6/2010 9:14:07 AM 7/6/2010 9:38:50 AM	00:24:40	000000000	55126	55157		
7/6/2010 9:14:07 AM 7/6/2010 9:38:50 AM 7/6/2010 9:38:50 AM 7/6/2010 9:38:15 AM	00:24:40 00:05:12 00:01:48	860022306	55126 55570	55157 020032		
7/6/2010 9:14:07 AM 7/6/2010 9:38:50 AM 7/6/2010 9:38:15 AM 7/6/2010 9:40:36 AM	00:24:40 00:05:12 00:01:48 00:00:16	860022306	55126 55570 55546	55157 020032 55570		
7/6/2010 9:14:07 AM 7/6/2010 9:38:50 AM 7/6/2010 9:38:55 AM 7/6/2010 9:40:36 AM 7/6/2010 9:41:56 AM	00:24:40 00:05:12 00:01:48 00:00:16 00:00:28	860022306	55126 55570 55546 55126	55157 020032 55570 55550		
7/6/2010 9:14:07 AM 7/6/2010 9:38:50 AM 7/6/2010 9:38:55 AM 7/6/2010 9:40:36 AM 7/6/2010 9:41:56 AM 7/6/2010 9:41:56 AM	00:24:40 00:05:12 00:01:48 00:00:16 00:00:28 00:02:52	860022306	55126 55570 55546 55126 55157	55157 020032 55570 55550 55126 02002		
7/6/2010 9:14:07 AM 7/6/2010 9:38:50 AM 7/6/2010 9:38:55 AM 7/6/2010 9:40:56 AM 7/6/2010 9:41:56 AM 7/6/2010 9:41:56 AM 7/6/2010 9:41:56 AM	00:24:40 00:05:12 00:01:48 00:00:16 00:00:28 00:02:52 00:15:57	860022306	55126 55570 55546 55126 55157 55570 55570	55157 020032 55570 55550 55126 018023 555		
76/2010 9:14:07 AM 76/2010 9:38:50 AM 7/6/2010 9:38:15 AM 7/6/2010 9:40:36 AM 7/6/2010 9:41:56 AM 7/6/2010 9:41:56 AM 7/6/2010 9:40:32 AM 7/6/2010 9:56:26 AM	00:24:40 00:05:12 00:01:48 00:00:16 00:00:28 00:02:55 00:15:57	860022306 10186139654004	55126 55570 55546 55126 55157 55570 55570 55570	55157 020032 55570 55550 55126 018023 55546		

#### Figure 49

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

Vera SMART TEM
CDR Source Wizard
Finish Reset Wizard
Congratulations! You have successfully performed a basic setup for this CDR Source.
We suggest that you go to these areas of the system for additional configuration.
<ul> <li><u>Rate Plans</u> - define rating</li> <li><u>Organization Menu</u> - configure your organization</li> </ul>
When rating and organization setup is complete, go to Call Processing Status and enable rating for this CDR Source. Until you enable rating, calls are being collected, but not rated.
To exit the wizard, click Finish.
Finish Reset Wizard

#### Figure 50

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.

V	SMART								Search for Starting with	Inventory Iter
٢	<u>Home</u>   <u>Call Coll</u>	ection Schedul	<u>e   Call Pr</u>	ocessing St	atus   CDR Source					
Q	) 5 items selected f	for display								
•	Filter by:									
	CDR Source name st	arting with:		٩						
4	Add CDR Source S	how Collection D	etails							
	CDR Source name	CDR Source ID	Short name	Setup status	Area code/local exchange	Format	Format number	Call collection method	Date/Time of last File Processed	Collection status
×	Avaya CS 1000	101	Ava00101	Partial	585/388	Nortel Communication Server 1000	526	Collect From File (Local)	5/25/2010 2:11:00 PM	Disabled
×	DPLAB	103	DPL00103	Complete	613/965	Nortel Communication Server 1000	526	Collect From File (Local)	7/7/2010 4:15:36 PM	Disabled
×	DPLAB 5	106	DPL00106	Complete	613/965	Nortel Communication Server 1000	526	Collect From File (Local)	6/7/2010 4:38:56 PM	Enabled
×	DPLAB2	104	DPL00104	Complete	613/975	Nortel Communication Server 1000	526	Collect From File (Local)	7/1/2010 11:34:48 AM	Disabled
×	DPLAB3	105	DPL00105	Complete	613/965	Nortel Communication Server 1000	526	Collect From File (Local)	7/1/2010 2:23:32 PM	Disabled
4	Add CDR Source S	how Collection D	<u>etails</u>							

Figure 51



Figure 52

# 9. Create report on VeraSMART

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

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

Vera SMART TEM
Favorites Reporting Organization Inventory Call Management Accounting System
Create/Run Reports View Saved Reports View Report Log



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

Vera SMART.
🍕 <u>Home</u>   <u>View Report Log</u>   <u>View Saved Reports</u>   Create/Run Reports
System Reports User Reports
⊙ Filter by:
Report name contains:
System report name 🔺
[Account Code Detail Report]
[Audit Trail Report]
[Billing Report]
[Call Detail by Organization Report]
[Call Search Report]
[Call Summary by Branch]
[Call Summary by Cost Center]
[Call Summary by Department]
[Call Summary by Division]
[Call Summary by Extension]
[Call Type Group by Cost Center Report]
ICall Type Report
ICost Distribution Report]

#### Figure 54

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

Vera SMART.				
Home   Create/Run Reports   View Report Log   View Saved Reports   Report Criteria				
Save Criteria As New Report Run Report Reset Fields Advanced Criteria				
Report Name				
Report name: DPLAB - REPORT				
System report name: Call Search Report <u>Help</u>				
⊟ Date Criteria				
Date range: 🛞 Current Month including Today 🛛 💌				
OPrevious days (excludes today)				
🗆 🗆 Call Record Criteria				
CDR Source name: All Select CDR Source				
Extension used: %;				
Dialed digits: %;				
Output Methods And Distribution				
Output as HTML report to browser				
Output as HTML report for later viewing in Saved Reports				
Output as HTML report and E-mail link to E-mail addresses selected below				
Output as HTML report and E-mail zipped files to E-mail addresses selected below				
E-mail addresses: Select E-mail Addresses				

Figure 55

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

SIVIANI			
Home   <u>Create/Run Reports</u>   <u>View Report Log</u>   <u>View Saved Reports</u>   Report Criteria			
Save Criteria As New Report Run Report Reset Fields Basic Criteria			
Report Name			
Report name: DPLAB - REPORT			
System report name: Call Search Report Help			
Reporting Database			
You are currently reporting against the <b>Current</b> database. Click <u>here</u> to create and restore archives.			
Currency criteria			
Show all calls with costs converted into system currency: US Dollars (USD)			
◯ Show only calls with costs in CDR Source currency: US Dollars (USD) ▼			
Date Criteria			
Date range: 💿 Current Month including Today 🛛 💌			
O Previous days (excludes today)			

Figure 56

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**.

Details to Include in Report					
Suppress call detail					
Available Fields (Call Details) Selected Fields (Call Details)					
CDR Source Name					
Call Direction Reported Dialed Number Cost Center Call Destination					
Cost Per Minute Call Type					
DNIS number Trunk					
Dialed Digits					
Employee Number Queue Time					
Personnel Ring Time					
Output Methods And Distribution					
Output as HTML report to browser					
Output as HTML report for later viewing in Saved Reports	Printer friendly format				
Output as HTML report and E-mail link to E-mail addresses selected below	Printer friendly format				
Output as HTML report and E-mail zipped files to E-mail addresses selected below	Printer friendly format				
E-mail addresses:	Select E-mail Addresses				
Output as ASCII text to specified output file					
Header: No header 💌					
Delimiter: Pipe 💌					
Output file name (includes path):					
Construit de New Persent - Persent - Persent Fielde - Persie Criteria					
Save Criteria As New Report Run Report Reset Fields Basic Criteria					
Done					

Figure 57

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

Vera SMART TEM			
Home   Create/Run	<u>n Reports</u>   <u>View Report Log</u>   <u>View Saved Reports</u>   Report Criteria		
Save Criteria As New Report Run Report Reset Fields Basic Criteria			
Report name:	DPLAB - REPORT		
System report name:	Call Search Report Help		
Reporting Database	8		
You are currently repor Click <u>here</u> to create an	rting against the <b>Current</b> database. Id restore archives.		
E Currency criteria			
Show all calls with	costs converted into system currency: US Dollars (USD)		
◯ Show only calls wi	th costs in CDR Source currency: US Dollars (USD) 💌		
🗆 Date Criteria			
Date range: 📀 Current Month including Today 🛛 💌			
○ From			
○ Previo	days (excludes today)		

#### Figure 58

Solution & Interoperability Test Lab Application Notes ©2010 Avaya Inc. All Rights Reserved.

Veramark Technologies, Inc			DPLAB - REPORT Search Criteria			
	Page 1 of 1					
<u>Start Date/Time</u>	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 following shows the final CDR report from VeraSMART.

#### 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

QT; Reviewed:	Solution & Interoperability Test Lab Application Notes	40 of 43
07/15/2010	©2010 Avaya Inc. All Rights Reserved.	VeraSMARTCS1000

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: <u>http://support.nortel.com/go/main.jsp</u>

[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

[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 <a href="http://www.veramark.com">http://www.veramark.com</a>

#### ©2010 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by  $\mathbb{R}$  and <sup>TM</sup> 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 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 <u>devconnect@avaya.com</u>.