



Avaya Solution & Interoperability Test Lab

Application Notes for Tiger Communications' Tiger 2020 Pro with Avaya Communication Manager - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Tiger Communications' Tiger 2020 Pro to interoperate with Avaya Communication Manager. Tiger 2020 Pro is a call logging system that records call detail records (CDR) outputted by Avaya Communication Manager over an IP network connection. Features and survivability were validated and performance testing was conducted in order to verify operation under light load.

Information in these Application Notes has been obtained through *DeveloperConnection* compliance testing and additional technical discussions. Testing was conducted via the *DeveloperConnection* Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the compliance-tested configuration using a Tiger Communications' Tiger 2020 Pro V5 and Avaya Communication Manager 4.0. This addresses the call detail records (CDR) capability of Avaya Communication Manager.

Tiger 2020 Pro is a Call Accounting and Billing package that utilizes the CDR Link in Communication Manager. Tiger 2020 Pro collects, stores, and processes the CDR records to provide usage analysis, call costing and billing capabilities. Survivability mode is supported via secure file transfer protocol (SFTP). When administered with the Survivable CDR feature enabled, the LSP saves the CDR information in files that are stored in a special directory on the local hard drive until the Tiger 2020 Pro remotely logs into the LSP via a special login, copies the files to its own storage device, and then goes on to process the CDR data in the same manner that it does normally. Avaya Communication Manager can generate call detail records for intra-switch calls, inbound trunk calls and outbound trunk calls. In addition, split records can be generated for transferred calls and conference calls. Tiger 2020 Pro creates a custom Avaya Communication Manager configuration file to accurately parse the CDR data. For the compliance testing, a customized format was used. Tiger 2020 Pro does not currently support Reliable Session Protocol (RSP).

An Avaya S8700 Server with an Avaya G650 Media Gateway running Avaya Communication Manager 4.0 was configured as the main server and a S8300 Server with an Avaya G250 Media Gateway was configured as the local survivable processor (LSP).

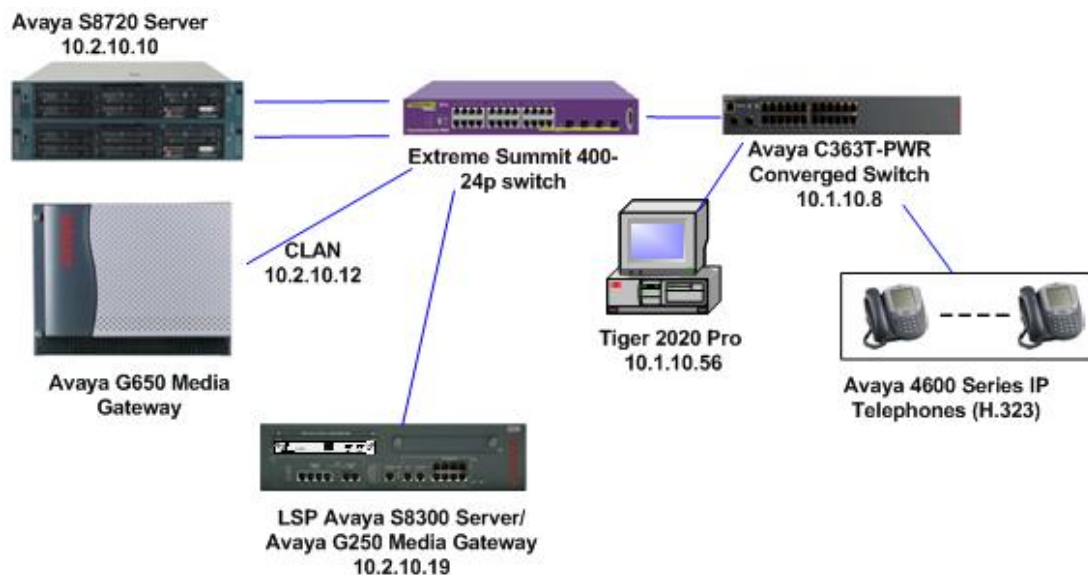


Figure 1: Tested Avaya Communication Manager System with Tiger 2020 Pro Server

2. Equipment and Software Validated

Below is a list of the equipment and software versions used within the compliance-tested network.

Equipment	Software
Avaya S8700 Server running Avaya Communication Manager.	4.0.1 (R014x.00.0.731.2)
Avaya G650 Media Gateway IPSI TN2312BP C-LAN TN799DP Medpro TN2302AP	HW 7, FW 39 HW 1, FW24 HW 20, FW116
Avaya S8300 Server with Avaya G250 Media Gateway (LSP Mode)	4.0.1 (R014x.00.0.731.2)
Extreme Summit 200 Switch	Extremeware 7.5e.2.8
Avaya C363T PWR Converged Stackable Switch	4.3.12
Avaya 46XX IP Telephones (H.323)	2.8
Avaya 96XX IP Telephones (H.323)	1.5
Tiger Communications' 2020 Pro Server	v5.0
Tiger Communications' 2020 Database	MySQL v4.1.

3. Configure Avaya Communication Manager

This section describes the steps for configuring Call Detail Recording (CDR) links, CDR system parameters, and intra-switch CDR extensions on Avaya Communication Manager. The steps are performed through the System Access Terminal (SAT) interface.


Step	Description																		
1.	<p>Enter the change node-names ip command. Create a new node name and IP address for the Tiger 2020 Pro used to collect the call detail records from Avaya Communication Manager. The node name configured below will be used in the ip-services form to specify the remote node of the CDR links.</p> <div><pre>change node-names ip</pre><div>Page 1 of 2</div><table><thead><tr><th colspan="2">IP NODE NAMES</th></tr><tr><th>Name</th><th>IP Address</th></tr></thead><tbody><tr><td>AEServer</td><td>10.1.10.20</td></tr><tr><td>Abacus</td><td>10.1.10.31</td></tr><tr><td>CDR_Server</td><td>10.1.10.56</td></tr><tr><td>IP0412a_DC1</td><td>10.1.20.10</td></tr><tr><td>S8300a_DC1</td><td>10.1.30.10</td></tr><tr><td>S8500_Val1</td><td>10.1.10.14</td></tr><tr><td>SEServer</td><td>10.1.10.22</td></tr></tbody></table></div>	IP NODE NAMES		Name	IP Address	AEServer	10.1.10.20	Abacus	10.1.10.31	CDR_Server	10.1.10.56	IP0412a_DC1	10.1.20.10	S8300a_DC1	10.1.30.10	S8500_Val1	10.1.10.14	SEServer	10.1.10.22
IP NODE NAMES																			
Name	IP Address																		
AEServer	10.1.10.20																		
Abacus	10.1.10.31																		
CDR_Server	10.1.10.56																		
IP0412a_DC1	10.1.20.10																		
S8300a_DC1	10.1.30.10																		
S8500_Val1	10.1.10.14																		
SEServer	10.1.10.22																		

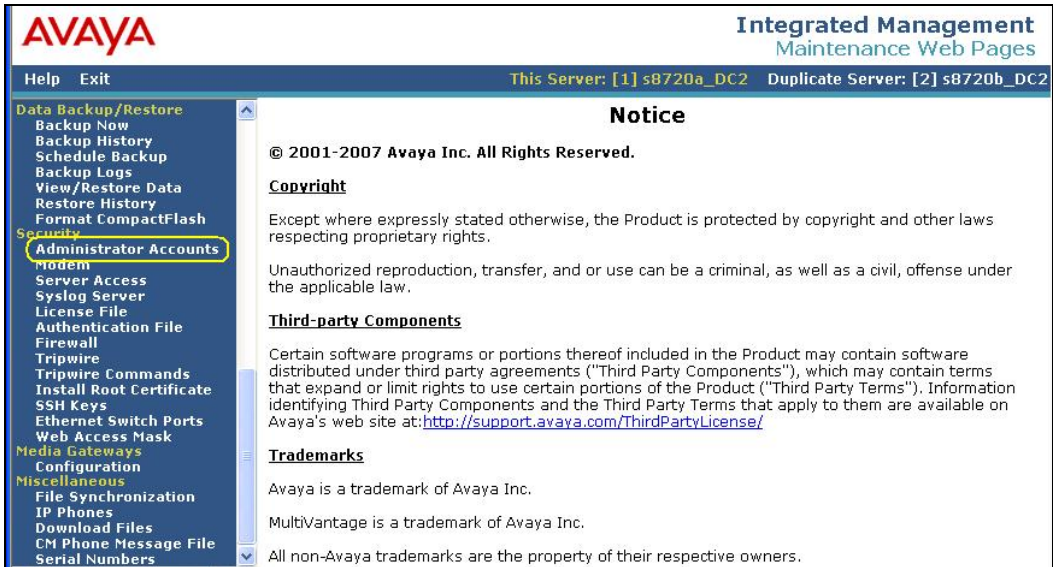
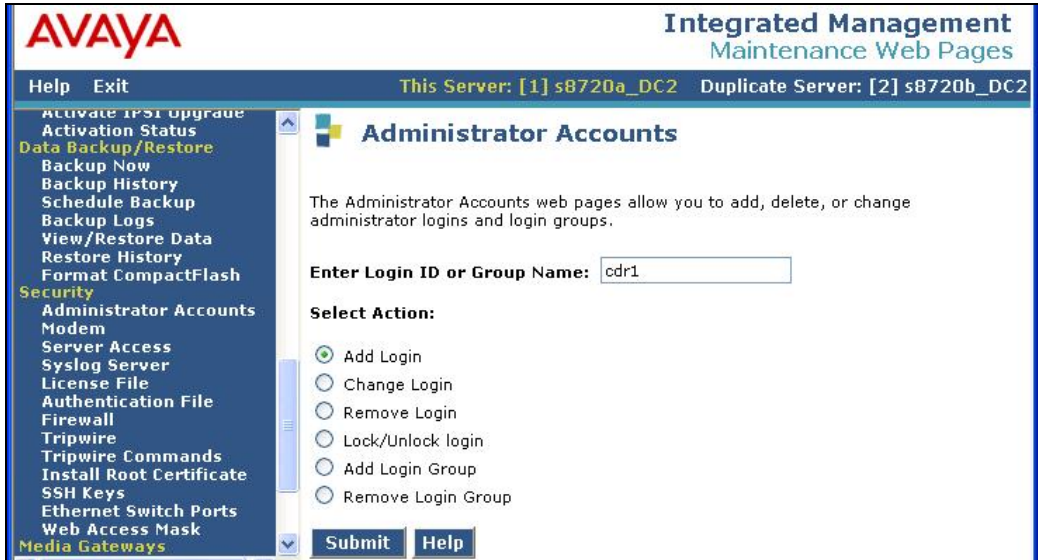
Step	Description																																																
2.	<p>Enter the change ip-services command. On page 1 of the IP SERVICES screen, define a primary CDR link by setting the Service Type to “CDR1”. A secondary link can be defined by setting Service Type to CDR2. Set Local Node to “clanla_DC1” and Remote Node to “CDR_Server” as configured in step 1 above. The Local Port is fixed at “0” and the Remote Port may be set to a value between 5000 and 64500, inclusive, but must match the port configured on the Tiger 2020 Pro in section 4, step 1.</p> <div><div>change ip-services</div><div>Page 1 of 4</div><table><thead><tr><th colspan="6">IP SERVICES</th></tr><tr><th>Service Type</th><th>Enabled</th><th>Local Node</th><th>Local Port</th><th>Remote Node</th><th>Remote Port</th></tr></thead><tbody><tr><td>SAT</td><td>y</td><td>clanla_DC1</td><td>5023</td><td>any</td><td>0</td></tr><tr><td>AESVCS</td><td>y</td><td>clanla_DC1</td><td>8765</td><td></td><td></td></tr><tr><td>CDR1</td><td></td><td>clanla_DC1</td><td>0</td><td>CDR_Server</td><td>9000</td></tr></tbody></table></div> <p>On Page 3 of the ip-services screen, disable the Reliable Session Protocol (RSP) for the CDR link by setting Reliable Protocol to “n”.</p> <div><div>change ip-services</div><div>Page 3 of 4</div><table><thead><tr><th colspan="6">SESSION LAYER TIMERS</th></tr><tr><th>Service Type</th><th>Reliable Protocol</th><th>Packet Resp Timer</th><th>Session Connect Message Cntr</th><th>SPDU Cntr</th><th>Connectivity Timer</th></tr></thead><tbody><tr><td>CDR1</td><td>n</td><td>30</td><td>3</td><td>3</td><td>30</td></tr></tbody></table></div>	IP SERVICES						Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port	SAT	y	clanla_DC1	5023	any	0	AESVCS	y	clanla_DC1	8765			CDR1		clanla_DC1	0	CDR_Server	9000	SESSION LAYER TIMERS						Service Type	Reliable Protocol	Packet Resp Timer	Session Connect Message Cntr	SPDU Cntr	Connectivity Timer	CDR1	n	30	3	3	30
IP SERVICES																																																	
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port																																												
SAT	y	clanla_DC1	5023	any	0																																												
AESVCS	y	clanla_DC1	8765																																														
CDR1		clanla_DC1	0	CDR_Server	9000																																												
SESSION LAYER TIMERS																																																	
Service Type	Reliable Protocol	Packet Resp Timer	Session Connect Message Cntr	SPDU Cntr	Connectivity Timer																																												
CDR1	n	30	3	3	30																																												


Step	Description
3.	<p>Enter the change system-parameters cdr command and set the following:</p> <ul style="list-style-type: none"> • CDR Date Format: set to “day/month”. The date format will be used for the date stamp that begins each new day of call records or in the “customized” CDR output formats (see below). • Primary Output Format: set to a format specified or “customized”. For compliance testing the “customized” format was used. • Primary Output Endpoint: set to “CDR1”. • Intra-switch CDR: set to “y” so that CDR records will be generated for calls to/from extensions that are assigned intra-switch CDR (see step 5 below). • Outg Trk Call Splitting / Inc Trk Call Splitting: set to “y” if a separate CDR record is desired for any portion of an outgoing/incoming call that is transferred or conferenced. • Enable CDR Storage on Disk: set to “y” this is to allow CDR’s to be stored on the LSP when in survivable mode. <div data-bbox="277 779 1520 1350"> <pre> change system-parameters cdr Page 1 of 2 CDR SYSTEM PARAMETERS Node Number (Local PBX ID): 1 CDR Date Format: day/month Primary Output Format: customized Primary Output Endpoint: CDR1 Secondary Output Format: Use ISDN Layouts? n Enable CDR Storage on Disk? y Use Enhanced Formats? n Condition Code 'T' For Redirected Calls? y Use Legacy CDR Formats? n Remove # From Called Number? n Modified Circuit ID Display? n Intra-switch CDR? y Record Outgoing Calls Only? n Outg Trk Call Splitting? y Suppress CDR for Ineffective Call Attempts? n Outg Attd Call Record? y Disconnect Information in Place of FRL? n Interworking Feat-flag? n Force Entry of Acct Code for Calls Marked on Toll Analysis Form? n Calls to Hunt Group - Record: member-ext Record Called Vector Directory Number Instead of Group or Member? n Record Agent ID on Incoming? y Record Agent ID on Outgoing? y Inc Trk Call Splitting? y Inc Attd Call Record? y Record Non-Call-Assoc TSC? n Call Record Handling Option: warning Record Call-Assoc TSC? n Digits to Record for Outgoing Calls: dialed Privacy - Digits to Hide: 0 CDR Account Code Length: 15 </pre> </div>

Step	Description																																																			
4.	<p>If Primary Output Format is set to “customized”, then on Page 2 of the system-parameters cdr screen, enter the data items in the order that the information should appear in the customized call records sent over the CDR link. For each field in the CDR record, specify the data item and length as shown below.</p> <div><div>change system-parameters cdr</div><div>Page2 of2</div><div>CDR SYSTEM PARAMETERS</div><table><thead><tr><th>Data Item - Length</th><th>Data Item - Length</th><th>Data Item - Length</th></tr></thead><tbody><tr><td>1: date - 6</td><td>17: in-trk-code - 4</td><td>33: -</td></tr><tr><td>2: time - 4</td><td>18: attd-console - 4</td><td>34: -</td></tr><tr><td>3: space - 2</td><td>19: bcc - 1</td><td>35: -</td></tr><tr><td>4: space - 2</td><td>20: clg-pty-cat - 2</td><td>36: -</td></tr><tr><td>5: sec-dur - 5</td><td>21: feat-flag - 1</td><td>37: -</td></tr><tr><td>6: cond-code - 1</td><td>22: node-num - 2</td><td>38: -</td></tr><tr><td>7: code-dial - 4</td><td>23: vdn - 8</td><td>39: -</td></tr><tr><td>8: code-used - 4</td><td>24: bandwidth - 2</td><td>40: -</td></tr><tr><td>9: dialed-num - 18</td><td>25: tsc_ct - 4</td><td>41: -</td></tr><tr><td>10: clg-num/in-tac - 15</td><td>26: return - 1</td><td>42: -</td></tr><tr><td>11: auth-code - 7</td><td>27: line-feed - 1</td><td>43: -</td></tr><tr><td>12: in-crt-id - 3</td><td>28: -</td><td>44: -</td></tr><tr><td>13: out-crt-id - 3</td><td>29: -</td><td>45: -</td></tr><tr><td>14: isdn-cc - 11</td><td>30: -</td><td>46: -</td></tr><tr><td>15: ppm - 5</td><td>31: -</td><td>47: -</td></tr><tr><td>16: acct-code - 15</td><td>32: -</td><td>48: -</td></tr></tbody></table><div>Record length = 135</div></div>	Data Item - Length	Data Item - Length	Data Item - Length	1: date - 6	17: in-trk-code - 4	33: -	2: time - 4	18: attd-console - 4	34: -	3: space - 2	19: bcc - 1	35: -	4: space - 2	20: clg-pty-cat - 2	36: -	5: sec-dur - 5	21: feat-flag - 1	37: -	6: cond-code - 1	22: node-num - 2	38: -	7: code-dial - 4	23: vdn - 8	39: -	8: code-used - 4	24: bandwidth - 2	40: -	9: dialed-num - 18	25: tsc_ct - 4	41: -	10: clg-num/in-tac - 15	26: return - 1	42: -	11: auth-code - 7	27: line-feed - 1	43: -	12: in-crt-id - 3	28: -	44: -	13: out-crt-id - 3	29: -	45: -	14: isdn-cc - 11	30: -	46: -	15: ppm - 5	31: -	47: -	16: acct-code - 15	32: -	48: -
Data Item - Length	Data Item - Length	Data Item - Length																																																		
1: date - 6	17: in-trk-code - 4	33: -																																																		
2: time - 4	18: attd-console - 4	34: -																																																		
3: space - 2	19: bcc - 1	35: -																																																		
4: space - 2	20: clg-pty-cat - 2	36: -																																																		
5: sec-dur - 5	21: feat-flag - 1	37: -																																																		
6: cond-code - 1	22: node-num - 2	38: -																																																		
7: code-dial - 4	23: vdn - 8	39: -																																																		
8: code-used - 4	24: bandwidth - 2	40: -																																																		
9: dialed-num - 18	25: tsc_ct - 4	41: -																																																		
10: clg-num/in-tac - 15	26: return - 1	42: -																																																		
11: auth-code - 7	27: line-feed - 1	43: -																																																		
12: in-crt-id - 3	28: -	44: -																																																		
13: out-crt-id - 3	29: -	45: -																																																		
14: isdn-cc - 11	30: -	46: -																																																		
15: ppm - 5	31: -	47: -																																																		
16: acct-code - 15	32: -	48: -																																																		
5.	<p>If Intra-switch CDR is enabled (Step 3), enter the command change intra-switch-cdr and enter the extensions for which intra-switch calls will generate CDR data.</p> <div><div>change intra-switch-cdr</div><div>Page1 of3</div><div>INTRA-SWITCH CDR</div><table><thead><tr><th>Extension</th><th>Assigned Members:</th><th>4</th><th>of 5000</th><th>administered</th></tr><tr><th>Extension</th><th>Extension</th><th>Extension</th><th>Extension</th><th></th></tr></thead><tbody><tr><td>10001</td><td></td><td></td><td></td><td></td></tr><tr><td>10002</td><td></td><td></td><td></td><td></td></tr><tr><td>10003</td><td></td><td></td><td></td><td></td></tr><tr><td>10004</td><td></td><td></td><td></td><td></td></tr></tbody></table></div> <p>Note: For ease of implementation, special application (SA8202) Intra-Switch CDR by COS is an optional feature that allows customers to enable intra-switch CDR for extensions that are assigned a COS with intra-switch CDR activated. The customer does not have to manually add individual extensions in the intra-switch-cdr form. The SA8202 feature also removes the 5000 extension limit for the S8500, allowing CDR records to be generated for as many extensions as are administered on the switch.</p>	Extension	Assigned Members:	4	of 5000	administered	Extension	Extension	Extension	Extension		10001					10002					10003					10004																									
Extension	Assigned Members:	4	of 5000	administered																																																
Extension	Extension	Extension	Extension																																																	
10001																																																				
10002																																																				
10003																																																				
10004																																																				

Step	Description
6.	<p>For each trunk group for which CDR records are desired, enter the command change trunk-group n, where n is the trunk group number, and set CDR Reports to “r”. CDR Reports, field valid entries are y, n, and r. Default is y.</p> <p>“y” All calls on this trunk group will generate call detail records. “n” Calls over this trunk group will not generate call detail records. “r” (ring-intvl) CDR records will be generated for both incoming and outgoing calls.</p> <p>In addition, the following ringing interval CDR records are generated:</p> <ul style="list-style-type: none"> Abandoned calls: The system creates a record with a condition code of "H," indicating the time until the call was abandoned. Answered calls: The system creates a record with a condition code of "G," indicating the interval from start of ring to answer. Calls to busy stations: The system creates a record with a condition code of "I," indicating a recorded interval of 0. <p>The example below depicts the trunk group connected to the PSTN in the sample configuration.</p> <pre> change trunk-group 19 Page 1 of 21 TRUNK GROUP Group Number: 19 Group Type: isdn CDR Reports: r Group Name: PRI to BT COR: 1 TN: 1 TAC: 719 Direction: two-way Outgoing Display? n Carrier Medium: PRI/BRI Dial Access? y Busy Threshold: 255 Night Service: Queue Length: 0 Service Type: public-ntwrk Auth Code? n TestCall ITC: rest Far End Test Line No: TestCall BCC: 4 </pre>
7.	<p>Survivable CDR feature is used to preserve the CDR records associated with calls that occur while a gateway is under the control of a Local Survivable Processor (LSP). The following steps are required to allow the calls to be stored on the LSP so they can be then retrieved via SFTP. Enter the list survivable-processor command and make a note of the LSP name in this example it is “LSP_G250”.</p> <pre> list survivable-processor SURVIVABLE PROCESSORS Name Type IP Address Reg LSP Translations Net Act Updated Rgn LSP_G250 LSP 10 .2 .10 .19 n n 1 </pre>

Step	Description																												
8.	<p>Enter change survivable-processor LSP_G250 and set the following parameters.</p> <ul style="list-style-type: none">• Service Type: set to “CDR1”, which is set as the Primary Output Endpoint in step 3.• Enabled: set to “o” for overwrite.• Store to disk: set to “y” this allows the CDR’s to be stored to the LSP disk. <div><div>change survivable-processor LSP_G250</div><div>PAGE 2 OF 3</div><table><tr><th colspan="7">SURVIVABLE PROCESSOR - IP-SERVICES</th></tr><tr><th>Service Type</th><th>Enabled</th><th>Store to disk</th><th>Local Node</th><th>Local Port</th><th>Remote Node</th><th>Remote Port</th></tr><tr><td>AESVCS</td><td>i</td><td>n</td><td>clan_01a10</td><td>8765</td><td></td><td></td></tr><tr><td>CDR1</td><td>o</td><td>y</td><td></td><td></td><td></td><td></td></tr></table></div>	SURVIVABLE PROCESSOR - IP-SERVICES							Service Type	Enabled	Store to disk	Local Node	Local Port	Remote Node	Remote Port	AESVCS	i	n	clan_01a10	8765			CDR1	o	y				
SURVIVABLE PROCESSOR - IP-SERVICES																													
Service Type	Enabled	Store to disk	Local Node	Local Port	Remote Node	Remote Port																							
AESVCS	i	n	clan_01a10	8765																									
CDR1	o	y																											
9.	<p>Use either of these following commands to save the translations to the LSP:</p> <ul style="list-style-type: none">- The save trans lsp command locally saves the translations, and performs a filesync operation to all registered LSPs.- The save trans lsp n command, where n is the IP address of a specific LSP, locally saves the translations, and performs a filesync operation to the specified LSP.																												
10.	<p>Access the Main (Avaya S8720 server) Avaya Communication Manager administration web interface by entering <i>http://<ip-addr>/</i> as the URL in an Internet browser, where <i><ip-addr></i> is the IP address of Avaya Communication Manager. Log in with the appropriate credentials to the Avaya Communication Manager web interface and click Launch Maintenance Web Interface.</p> <div></div>																												

Step	Description
11.	<p>In the Security section click on Administrator Accounts.</p>  <p>The screenshot shows the Avaya Integrated Management Maintenance Web Pages interface. The left sidebar contains a menu with categories: Data Backup/Restore, Security, Modem, Server Access, Syslog Server, License File, Authentication File, Firewall, Tripwire, Tripwire Commands, Install Root Certificate, SSH Keys, Ethernet Switch Ports, Web Access Mask, Media Gateways, Configuration, Miscellaneous, File Synchronization, IP Phones, Download Files, CM Phone Message File, and Serial Numbers. The 'Security' category is expanded, and 'Administrator Accounts' is highlighted. The main content area displays a 'Notice' section with copyright information and a 'Third-party Components' section.</p>
12.	<p>In the Enter Login or Group Name field enter a name that will be used by the Tiger 2020 to login in Section 4, Step 9. Select the Add Login radio button and click Submit.</p>  <p>The screenshot shows the Avaya Integrated Management Maintenance Web Pages interface for the 'Administrator Accounts' section. The left sidebar is the same as in the previous screenshot, but 'Administrator Accounts' is now selected. The main content area has a heading 'Administrator Accounts' and a description: 'The Administrator Accounts web pages allow you to add, delete, or change administrator logins and login groups.' Below this is a form with the label 'Enter Login ID or Group Name:' and a text input field containing 'cdr1'. Underneath is a 'Select Action:' section with several radio buttons: 'Add Login' (selected), 'Change Login', 'Remove Login', 'Lock/Unlock login', 'Add Login Group', and 'Remove Login Group'. At the bottom of the form are 'Submit' and 'Help' buttons.</p>

Step	Description
13.	<p>In the login group field, enter “CDR_User”, leave the additional groups field blank. Click on the CDR access only radio button. Click on the password radio button and enter the desired password twice this will be used by the Tiger 2020 Pro to access the survivable CDR file on the LSP. All other remaining fields can be left with their default values. Click the Add button at the bottom of the page (not shown). The account details created on the Main Avaya Communication Manage will be propagated to the LSP.</p>  <p>The screenshot shows the Avaya Integrated Management Maintenance Web Pages interface. The left sidebar contains a navigation menu with categories like Data Backup/Restore, Security, Media Gateways, and Miscellaneous. The main content area is titled 'Administrator Logins -- Add Login'. It contains a description of the page and a form to add a new administrator login. The form fields are as follows:</p> <ul style="list-style-type: none"> Login ID: cdr1 login group: CDR_User additional groups: (empty field) shell access: <ul style="list-style-type: none"> <input type="radio"/> no shell access. <input type="radio"/> standard shell access. <input checked="" type="radio"/> CDR access only. <input type="radio"/> remote login. lock this account: <input type="checkbox"/> date (YYYY-MM-DD) on which account is disabled (blank to ignore): (empty field) select type of authentication: <ul style="list-style-type: none"> <input checked="" type="radio"/> password <input type="radio"/> ASG enter key or password: (empty field) re-enter key or password: (empty field) force password/key change on first login: <ul style="list-style-type: none"> <input type="radio"/> yes <input checked="" type="radio"/> no

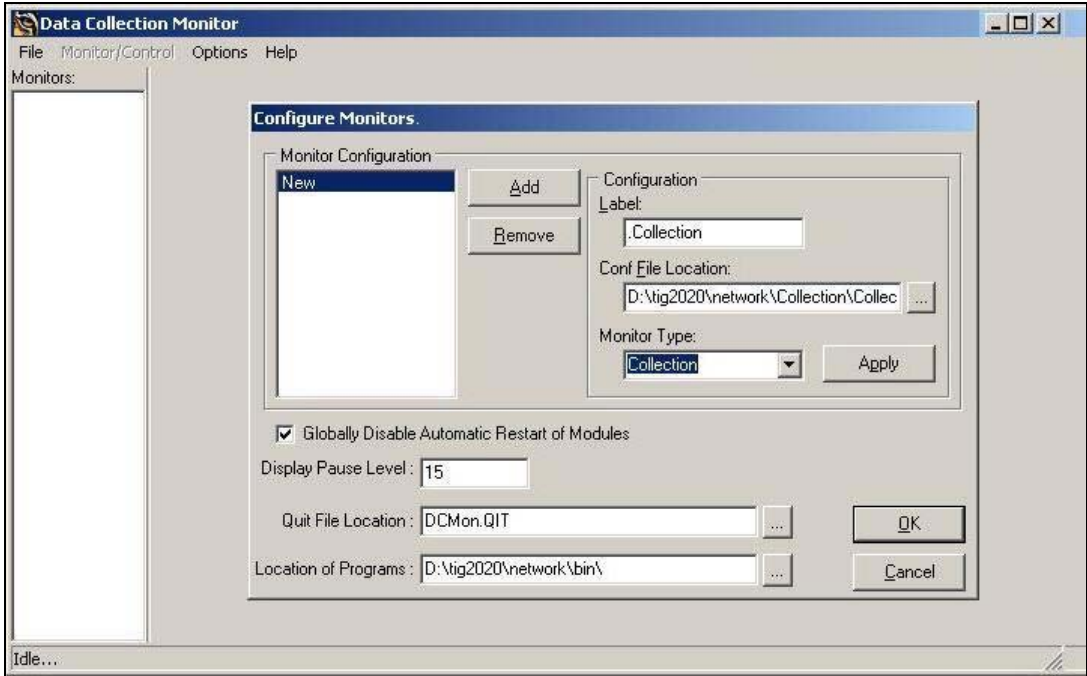
4. Configure Tiger 2020 Pro

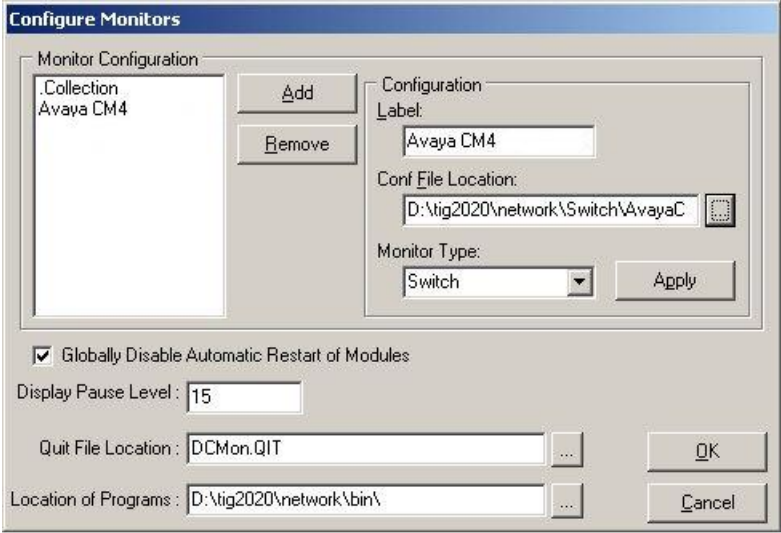
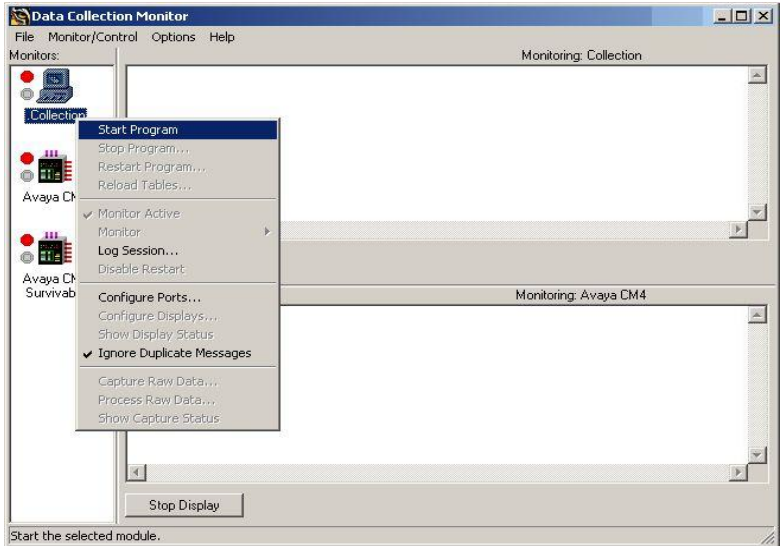
The configuration information provided in this section describes the steps required to set up Tiger 2020 Pro to collect CDR records generated by Avaya Communication Manager over a TCP/IP link.

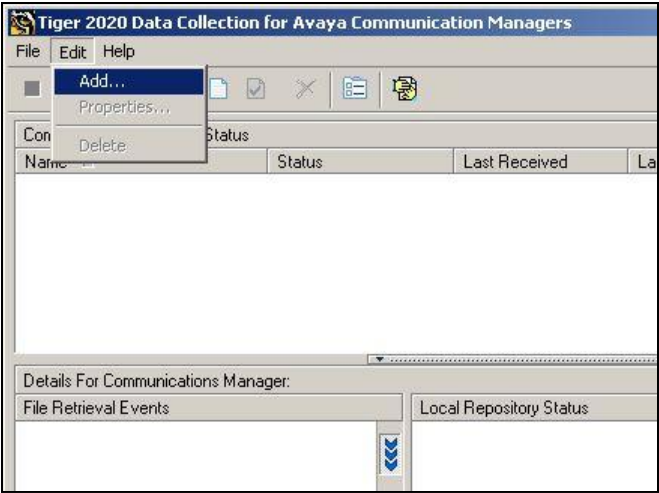
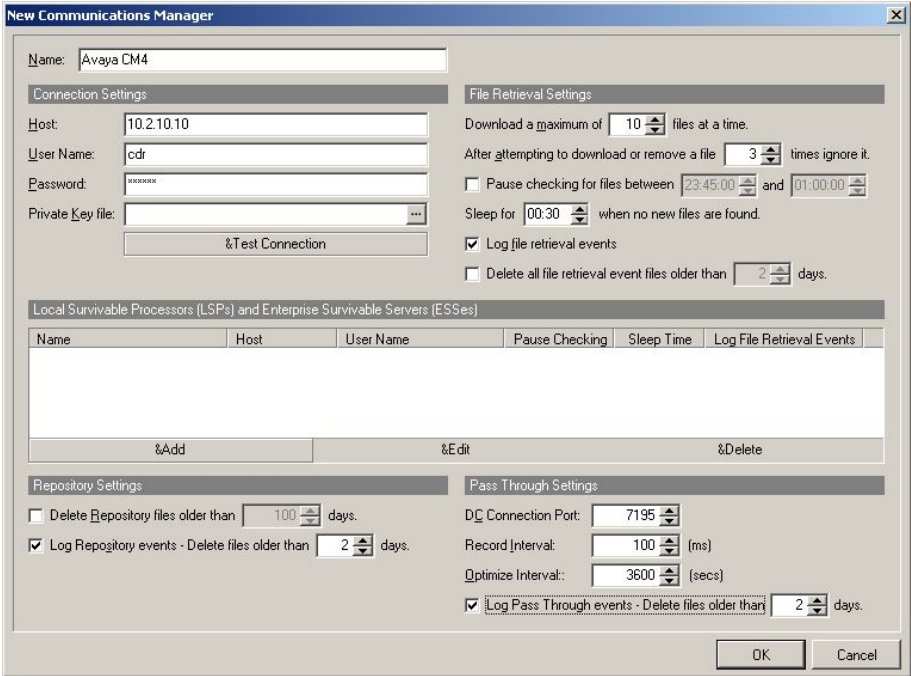
Step	Description
1.	<p>On the Tiger 2020 Pro server, modify the AvayaCM.conf file in the directory D:\tig2020\network\Switch\AvayaCM. In the [Switch] section ensure the Type field is set to “Definity”. In the [Input] section enter the Address of the Avaya Communication Manager CLAN “10.1.10.12” and the Port number “9000” configured in Section 3, Step 2. The CreateAs field is set to “Server”. The [FieldDefsFile] section should point to the location of the field definition file. This was named CM4_standard.conf.</p> <div><p>Contents of AvayaCM.conf</p><pre>[Switch] Type=Definity Revision=1.0 MaxCallHoldTime=120000 MaxTandemHoldOn=30000 MaxSectionHoldOn=7200000 RecordDiscardBlacklistHoldOn=3600000 MaxLineLength=2000 BreakYear=1980 NodeId=1 DiscardDuplicateRecords=1 DiscardOutgoingWithNoCalledDigits=0 CallTimeType=0 SequenceNumbersHeld=28 DefaultLatency=0 [Input] Name=AvayaCM4 Socket Input Type=Socket Direction=Input Protocol=TCP Address=10.1.10.12 Port=9000 CreateAs=Server Mode=Stream Sharing=readwrite BufferSize=1024 TimeOut=200 Sharing=none Blocking=0 NormalReadResetInterval=1200000 InitialReadResetInterval=3600000 [FieldDefsFile] Name=D:\tig2020\Network\SwitchConf\definity\CM4_Standard.conf</pre></div>

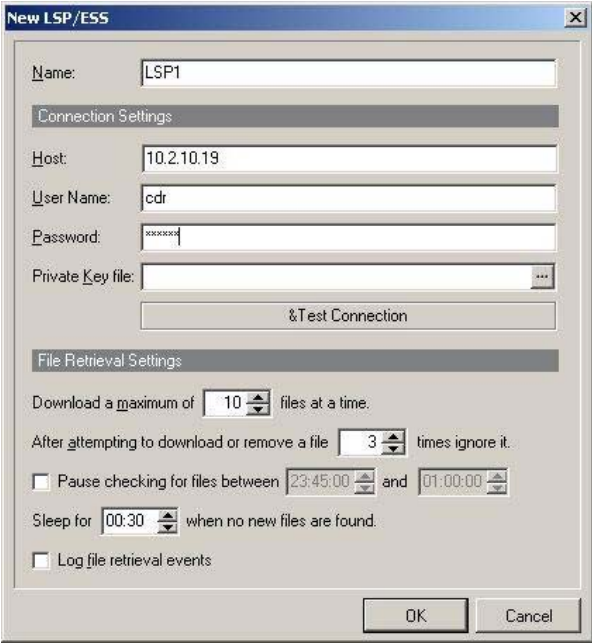
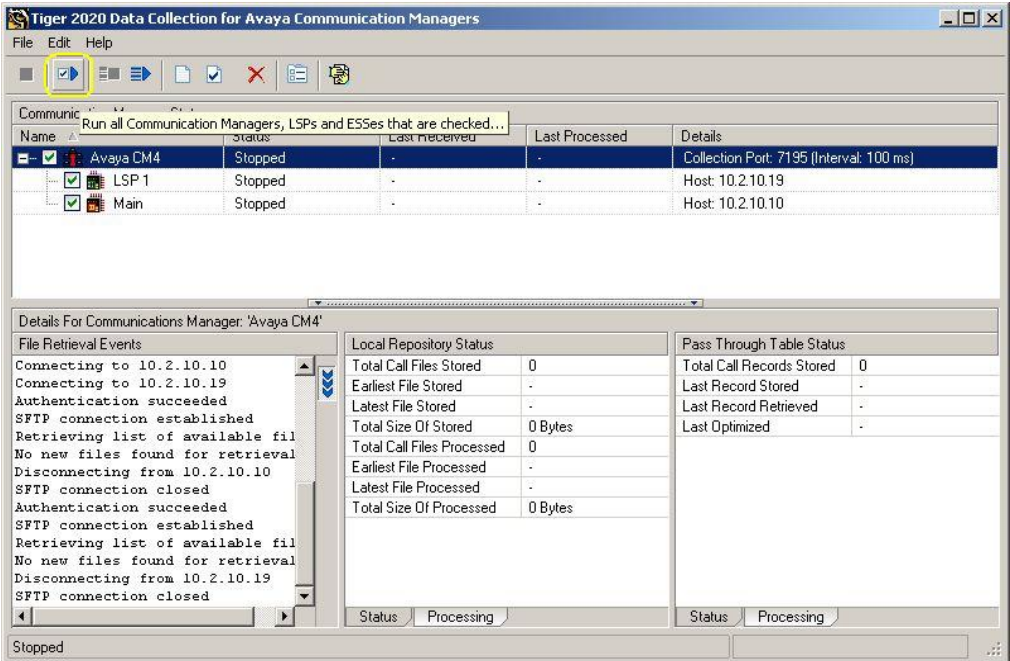
Step	Description
2.	<p>Survivable CDR data files can be retrieved by Tiger 2020 Pro from Avaya Communication Manager using SFTP. Modify the AvayaCM_Survivable.conf file in the directory D:\tig2020\network\Switch\AvayaCM_Survivable. In the [Switch] section ensure the Type field is set to “Definity”. In the [Input] section set the Hostname as “localhost” and the Port number “7195” this will be used in the Tiger 2020 Pro configuration in step . The CreateAs field is set to “Client”. The [FieldDefsFile] section should point to the location of the field definition file. This was named CM4_standard.conf.</p> <div data-bbox="277 520 1520 1581" style="border: 1px solid black; padding: 10px;"> <p>Contents of AvayaCM_Survivable.conf</p> <pre> [Switch] Type=Definity Revision=1.0 MaxCallHoldTime=120000 MaxTandemHoldOn=30000 MaxSectionHoldOn=7200000 RecordDiscardBlacklistHoldOn=3600000 MaxLineLength=2000 BreakYear=1980 NodeId=1 DiscardDuplicateRecords=1 DiscardOutgoingWithNoCalledDigits=0 CallTimeType=0 SequenceNumbersHeld=28 DefaultLatency=0 [Input] Name=AvayaCM_Survivable Socket Input Type=Socket Direction=Input Protocol=TCP Hostname=localhost Port=7195 CreateAs=Client Mode=Stream Sharing=readwrite BufferSize=1024 TimeOut=200 Sharing=none Blocking=0 NormalReadResetInterval=1200000 InitialReadResetInterval=3600000 [FieldDefsFile] Name=D:\tig2020\Network\SwitchConf\definity\CM4_Standard.conf </pre> </div>

Step	Description
3.	<p>The field definition file contains the fields that match the configured fields in the customized CDR parameters on Avaya Communication Manager in Section 3, Step 4.</p> <div data-bbox="280 338 1516 1551" style="border: 1px solid black; padding: 10px;"> <p>Contents of CM4_Standard.conf</p> <pre> [FieldDefs] DATE_END_DAY=1:0.2,I # Day part of End Date DATE_END_MONTH=1:2.2,I # Month part of End Date DATE_END_YEAR=1:4.2,I # Year part of End Date TIME_END_HOUR=1:6.2,I # Hour part of End Time TIME_END_MIN=1:8.2,I # Minute part of End Time SEC_DUR=1:14.5,I # Duration in seconds COND_CODE=1:19.1,C # Condition Code CODE_DIAL=1:20.4,C # Access Code Dialed CODE_USED=1:24.4,C # Access Code Used DIALED_NUM=1:28.18,C # Dialed digits CLG_NUM_IN_TAC=1:46.15,C # Calling Number or Incoming Trunk Group Access Code AUTH_CODE=1:61.7,C # Authorisation Code IN_CRT_ID=1:68.3,C # Incoming Circuit Id OUT_CRT_ID=1:71.3,C # Outgoing Circuit Id ISDN_CC=1:74.11,C # ISDN Call Charge PPM=1:85.5,C # Meter Units ACCT_CODE=1:90.15,C # Account Code IN_TRK_CODE=1:105.4,C # Incoming Trunk Code ATTD_CONSOLE=1:109.4,C # Console Number BCC=1:113.1,C # ISDN Bearer Capability Class CLG_PTY_CAT=1:114.2,C # Calling Party Category FEAT_FLAG=1:116.1,C # ISDN Feature Flag NODE_NUM=1:117.2,C # Node Number VDN=1:119.8,C # Vector Directory Number BANDWIDTH=1:127.2,C # Number of 64Kbps channels used TSC_CT=1:129.4,C # Packet count # Date Record Format # 1 # 01234567890 # HH:MM DD/MM # 13:45 25/10 DATAREC_HOUR=2:0.2,I # Hour part of time DATAREC_HMSEP=2:2.1,F=: # Time separator DATAREC_MIN=2:3.2,I # Minute part of time DATAREC_DAY=2:6.2,I # Day part of date DATAREC_DMSEP=2:8.1,F=/ # Date separator DATAREC_MONTH=2:9.2,I # Month part of date </pre> </div>

Step	Description
4.	<p>On the Tiger 2020 Pro server, navigate to d:\tig2020\network\bin and click on dcmon.exe file to launch the Tiger 2020 Pro data collection configuration. On the main Data Collection Monitor screen toolbar, click on Options → Configure.</p> <p>There are two types of monitor types to be configured - one for the collection which interfaces with the Tiger 2020 database and one for the switch which interfaces with Avaya Communication Manager. In the Configure Monitors dialog box click the Add button. In the Label field enter a descriptive name for the collection monitor type. In the Conf File Location field enter or browse to the location of the collection.conf file. The collection.conf file during this compliance testing was located at D:\tig2020\network\collection. For the Monitor Type select “Collection” from the drop down list. The rest of the parameters can be left with their default values. Click Apply.</p> 

Step	Description
5.	<p>Click on the Add button. In the Label field enter a descriptive name for the switch monitor type. In the Conf File Location field enter or browse to the location of the AvayaCM.conf file modified in Step 1. The AvayaCM.conf file during this compliance testing was located at D:\tig2020\network\Switch\AvayaCM. For the Monitor Type select “Switch” from the drop down list. The rest of the parameters can be left with their default values. Click Apply</p> 
6.	<p>Repeat the above step for Avaya CM Survivable. In the Conf File Location field enter or browse to the location of the AvayaCM_Survivable.conf file modified in Step 2. Once added Click OK.</p>
7.	<p>In the main Data Collection Monitor screen. Right click on the collection monitor icon labeled Collection and select Start Program. Do the same for the switch monitor icon labeled Avaya CM and Avaya CM Survivable. Section 6, Step 2 verifies the CDR link is up between Tiger 220 Pro and the CLAN.</p> 

Step	Description
8.	<p>On the Tiger 2020 Pro server, navigate to d:\tig2020 and click on DC_AvayaCommsManager.exe file to launch the Tiger 2020 Pro SFTP configuration. In the Tiger 2020 Data Collection screen tool bar click on Edit → Add.</p> 
9.	<p>Enter a descriptive name for the main Avaya Communication server in the Name field. In the Host field enter the IP address of the main Avaya Communication server. In the User Name and Password field enter the username and password configured in Section 3, Steps 12 and 13. In the Pass Through Settings section, DC Connection Port field enter the port number configured in the step2 in the AvayaCM_Survivable.conf file.</p> 

Step	Description
10.	<p>Click the &Add button to enter the details of the LSP server. Enter a descriptive name for the LSP server in the Name field. In the Host field enter the IP address of the LSP server. In the User Name and Password field enter the username and password configured in Section 3, Steps 13 and 14. The remaining parameters can be left with their default values. Click OK.</p> 
11.	<p>Click on the Run button shown in the screen below. The frequency in which Tiger 2020 Pro checks for new survivable CDR files can be configured (not shown).</p> 

5. Interoperability Compliance Testing

The interoperability compliance testing included feature and serviceability testing. The feature testing evaluated the ability of Tiger 2020 Pro to collect and process CDR records for various types of calls. The source and destination of each call was verified on the Tiger 2020 application. The serviceability testing introduced failure scenarios to see if Tiger 2020 Pro could resume CDR collection after failure recovery.

5.1. General Test Approach

The general test approach was to manually place intra-switch calls, inbound trunk, outbound trunk calls, conference calls, transfer calls, and forwarded calls to and from telephones controlled by Avaya Communication Manager and verify that Tiger 2020 Pro collects the CDR records and properly classifies and reports the attributes of the call. For serviceability testing, logical links were disabled/re-enabled. Light load testing and link integrity testing were also carried out.

5.2. Test Results

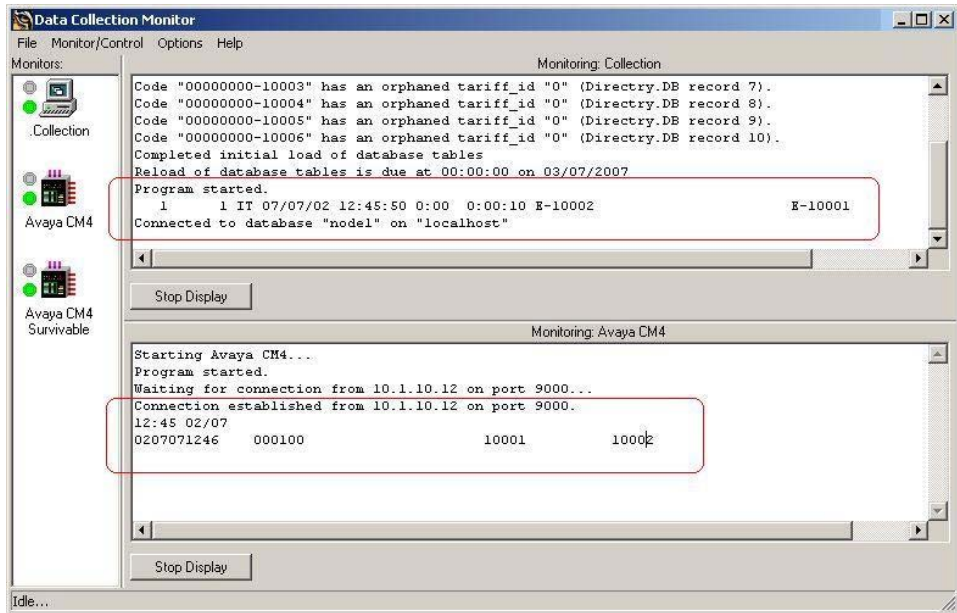
All feature and performance tests passed. The Tiger 2020 Pro successfully captured and processed call records from Avaya Communication Manager. Tiger 2020 Pro also successfully processed the CDR data, performed call costing, and produced call accounting reports.

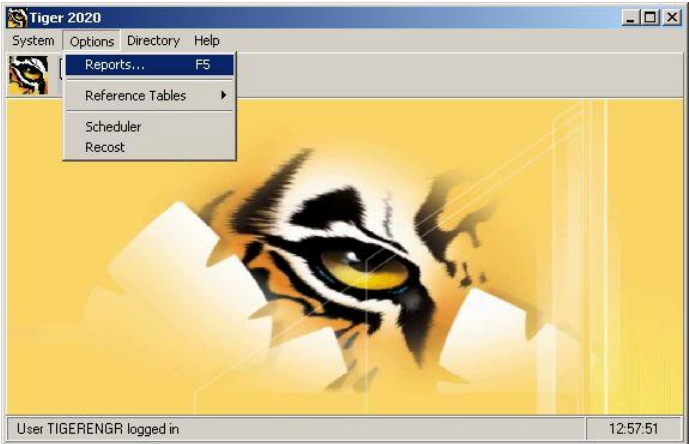
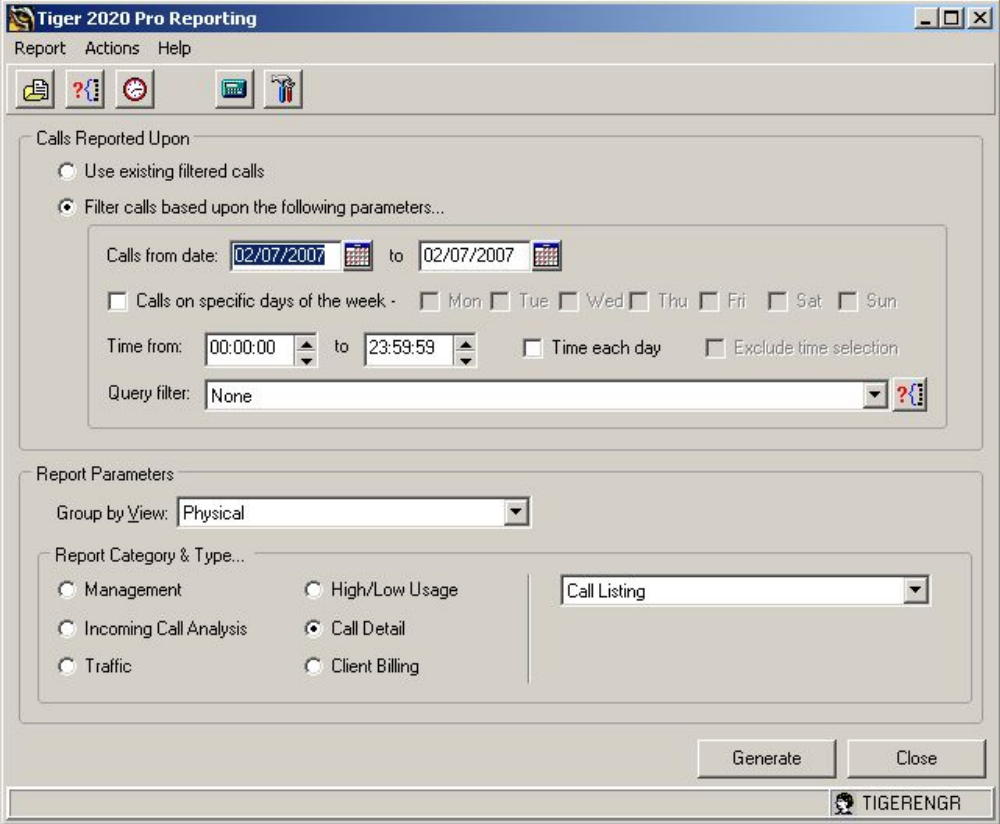
Tiger 2020 Pro successfully collected the CDR records from Avaya Communication Manager for all types of calls generated including intra-switch calls, inbound/outbound PSTN trunk calls, inbound/outbound private IP trunk calls, transferred calls, and conference calls. For serviceability testing, Tiger 2020 Pro was able to resume collecting CDR records after failure, but not for CDR records for calls that were placed during the outages between the Avaya Communication Manager and Tiger 2020 Pro as only the standard CDR link was used as the Avaya Communication Manager Reliable Session Protocol is not supported. During the fail over of the Main Avaya Communication Manager to the LSP, CDR records that were created and stored on the LSP were successfully retrieved and processed by the Tiger 2020 during the fail back to the Main Avaya Communication Manager. The Tiger 2020 Pro continued collecting the CDR records from the Main Avaya Communication Manager.

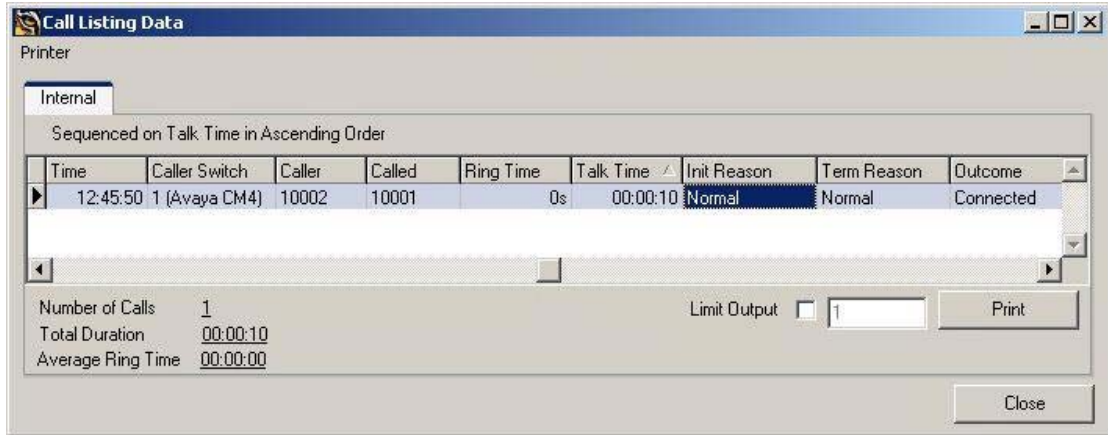
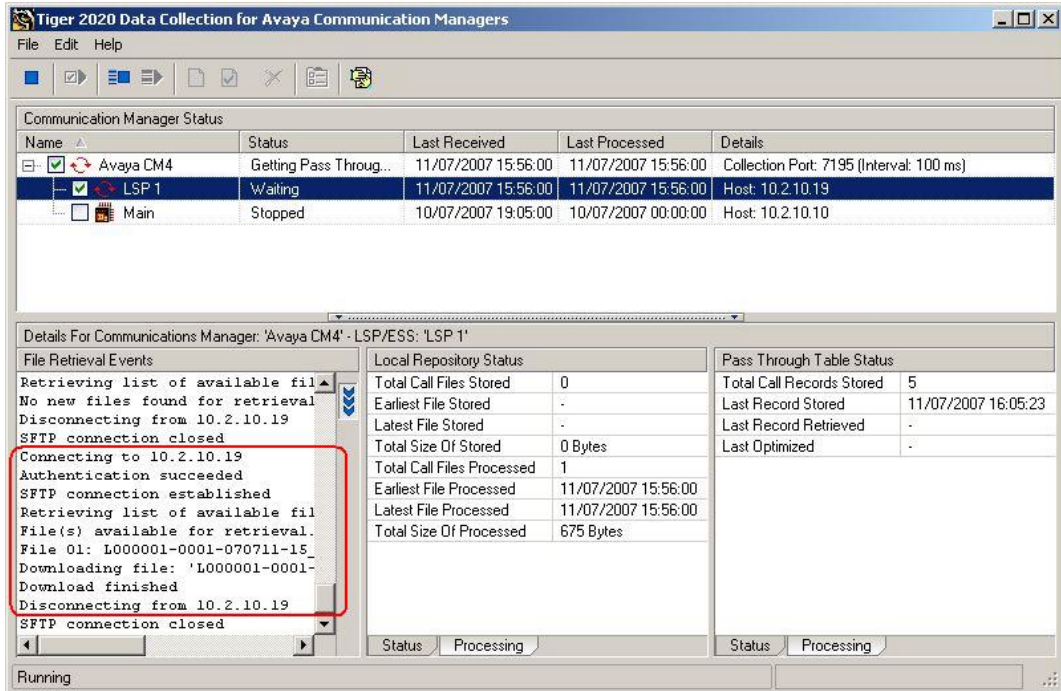
Note: As shown in Section 3, Step 2, the Avaya Communication Manager Reliable Session Protocol (RSP) was disabled for compatibility with Tiger 2020 Pro. With RSP disabled, the communication protocol is not as robust and there is a higher chance of loss of CDR records if there is a network failure.

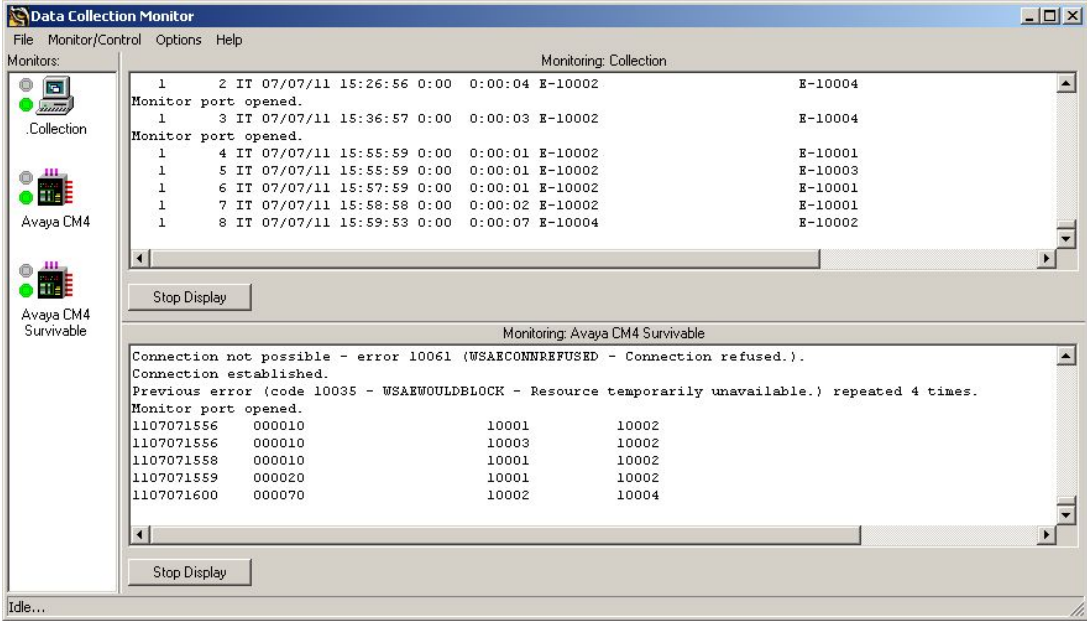
6. Verification Steps

The following steps may be used to verify the configuration

Step	Description
1.	<p>On the SAT, enter the status cdr-link command to verify that the CDR link state is up.</p> <pre> status cdr-link CDR LINK STATUS Primary Secondary Link State: up CDR not administered Number of Retries: Date & Time: 0 /0 /0 0 :0 :0 0 /0 /0 0 :0 :0 Forward Seq. No: 0 0 Backward Seq. No: 0 0 CDR Buffer % Full: 0.19 0.00 Reason Code: </pre>
2.	<p>Place a call and verify that Tiger 2020 Pro received the CDR record for the call and then processed the call. Compare the values of data fields in the CDR record with the expected values and verify that the values match as shown below.</p> 

Step	Description
3.	<p>On the Tiger 2020 Pro server, click on Start → Programs → Tiger 2020 → Tiger 2020. Enter the appropriate user name and password. On the Tiger 2020 screen tool bar, click Options → Reports.</p> 
4.	<p>On the Tiger 2020 Pro Reporting screen, select date and time. From the Report Category & Type section, select the Call Detail radio button and select Call Listing from the drop down list. Click on the Generate button.</p> 

Step	Description																		
5.	<p>The following screen displayed the processed CDR results.</p>  <p>The screenshot shows a window titled "Call Listing Data" with a "Printer" button. It has a tab labeled "Internal" and a subtitle "Sequenced on Talk Time in Ascending Order". Below this is a table with the following data:</p> <table><tr><th>Time</th><th>Caller Switch</th><th>Caller</th><th>Called</th><th>Ring Time</th><th>Talk Time</th><th>Init Reason</th><th>Term Reason</th><th>Outcome</th></tr><tr><td>12:45:50</td><td>1 (Avaya CM4)</td><td>10002</td><td>10001</td><td>0s</td><td>00:00:10</td><td>Normal</td><td>Normal</td><td>Connected</td></tr></table> <p>Below the table, there are summary statistics: Number of Calls: 1, Total Duration: 00:00:10, and Average Ring Time: 00:00:00. There is also a "Limit Output" checkbox set to 1 and a "Print" button. A "Close" button is at the bottom right.</p>	Time	Caller Switch	Caller	Called	Ring Time	Talk Time	Init Reason	Term Reason	Outcome	12:45:50	1 (Avaya CM4)	10002	10001	0s	00:00:10	Normal	Normal	Connected
Time	Caller Switch	Caller	Called	Ring Time	Talk Time	Init Reason	Term Reason	Outcome											
12:45:50	1 (Avaya CM4)	10002	10001	0s	00:00:10	Normal	Normal	Connected											
6.	<p>The screen below shows that survivable CDR file was successfully downloaded from the LSP server and that five records are stored on the Tiger 2020 PR server ready to be processed.</p>  <p>The screenshot shows a window titled "Tiger 2020 Data Collection for Avaya Communication Managers". It has a menu bar (File, Edit, Help) and a toolbar. The main area is divided into several sections:</p> <ul style="list-style-type: none">Communication Manager Status: A table showing the status of various managers.Details For Communications Manager: 'Avaya CM4' - LSP/ESS: 'LSP 1'<ul style="list-style-type: none">File Retrieval Events: A log showing the process of retrieving files from 10.2.10.19. A red box highlights the following events:Local Repository Status: A table showing the status of the local repository.Pass Through Table Status: A table showing the status of the pass through table. <p>At the bottom, there are status buttons for "Status" and "Processing", and a "Running" indicator.</p>																		

Step	Description
7.	<p>The screen below shows the five survivable CDR records processed.</p> 

7. Support

If technical support is required for the Tiger Communications' Tiger 2020 Pro server, contact their Technical Support Department.

Email: support@tigercomms.com

Phone: +44 1425 891 000 (When prompted select Option 2)

8. Conclusion

These Application Notes describe the required configuration steps for the Tiger 2020 Pro to collect call detail records from Avaya Communication Manager. Tiger 2020 Pro V5 was successfully compliance tested with Avaya Communication Manager 4.0.1.

9. Additional References

This section references the product documentations that are relevant to these Application Notes.

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

- *Administrator Guide for Avaya Communication Manager (4.0)*, Document ID 03-300509, Issue 3.1, February 2007.

Tiger Communications' 2020 Pro Product information is available from www.tigercomms.com

©2007 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 DeveloperConnection Program at devconnect@avaya.com.