



Avaya Solution & Interoperability Test Lab

Application Notes for configuring Tiger Prism from Tiger Communications with Avaya Aura® Session Manager R7.0.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Tiger Prism from Tiger Communications to interoperate with Avaya Aura® Session Manager R7.0.1. Tiger Prism is a call logging system that records Call Detail Records (CDR) outputted by Avaya Aura® Session Manager over an IP network connection.

Readers should pay particular attention to the scope of testing as outlined in Section 2.1, as well as observations noted in Section 2.2 to ensure that their own use cases are adequately covered by this scope and results

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

These Application Notes describe the compliance-tested configuration of Tiger Prism from Tiger Communications to interoperate with Avaya Aura® Session Manager R7.0.1. These Application Notes show the Call Detail Recording (CDR) capability of Avaya Aura® Session Manager and the ability of Tiger Prism to report on the CDR it receives.

Tiger Prism is a call accounting and billing package that utilizes the CDR output from Session Manager. Tiger Prism collects, stores, and processes the CDR records to provide usage analysis, call costing and billing capabilities. Session Manager can generate CDRs for intra-switch calls, inbound trunk calls and outbound trunk calls. Tiger Prism connects to Session Manager over the local or wide area network using Secure File Transfer Protocol (SFTP). Session Manager is configured to generate CDR into files, in XML format, and save them to a specific folder on the Session Manager server. Tiger Prism using SFTP connects to the server, to access the folder and downloads XML files generated by Session Manager to the local Tiger Prism server for reports. For the compliance testing, the “Enhanced XML file” format was used as the Data File Format on Session Manager.

2. General Test Approach and Test Results

The general test approach was to manually place intra-switch calls, inbound trunk, outbound trunk calls to and from H.323 telephones controlled by Communication Manager and SIP endpoints registered to Session Manager and verify that Tiger Prism collects the CDR records and properly classifies and reports the attributes of the call. For serviceability testing LAN failures were simulated.

Session Manager R7.0.x contains interface changes related to the security of the CDR login, used to download CDR records from a Session Manager server. These changes were not backward compatible with the Avaya recommended CDR retrieval procedure of deleting CDR files once they had been retrieved. A patch was created that reverts the operation of the CDR_User back to what it was in Session Manager R6.3 and earlier. This patch was used in this configuration. Additional details on the patch and how to obtain it are available at support.avaya.com, under PSN004893u.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member’s solution.

2.1. Interoperability Compliance Testing

The interoperability compliance testing included feature and serviceability testing. The feature testing evaluated the ability of Tiger Prism to collect and process CDR records for calls over SIP trunks. The source and destination of each call was verified on the Tiger Prism application. The interoperability compliance testing includes the following cases.

- Calls between H.323 and SIP phones over SIP Trunk.
- Inbound and outbound calls to/from H.323 phones over SIP trunks to simulated PSTN.
- Inbound and outbound calls to/from SIP phones over SIP trunks to simulated PSTN.

The serviceability testing introduced failure scenarios to see if Tiger Prism could resume CDR collection after failure recovery

2.2. Test Results

All feature and performance tests passed with the following observation.

- Session Manager CDR was designed to cover calls between 2 parties, where at least one leg of the call traverses Session Manager. Calls that involve Communication Manager invoking call features (such as transfer, conference, call-forward, etc.) may not yield the expected call records by Session Manager. This design may change in future versions of Session Manager.

2.3. Support

Support from Avaya is available by visiting the website <http://support.avaya.com> and a list of product documentation can be found in **Section 10** of these Application Notes. Technical support for the Tiger Prism product can be obtained as follows.

- Tel : +44 (0)1425 891000
- Web : <http://www.tigercomms.com/departments>
- Email: enquiries@tigercomms.com

3. Reference Configuration

Figure 1 shows an Avaya Aura® Communication Manager R7.0.1 serving H.323 endpoints with an Avaya G450 Media Gateway and an Avaya Aura® Media Server R7.7 with an Avaya Aura® Session Manager R7.0.1 providing SIP endpoints and a SIP trunk to the PSTN. Tiger Prism was configured on the same IP network for the transfer of CDR data from Avaya Aura® Session Manager R7.0.1.

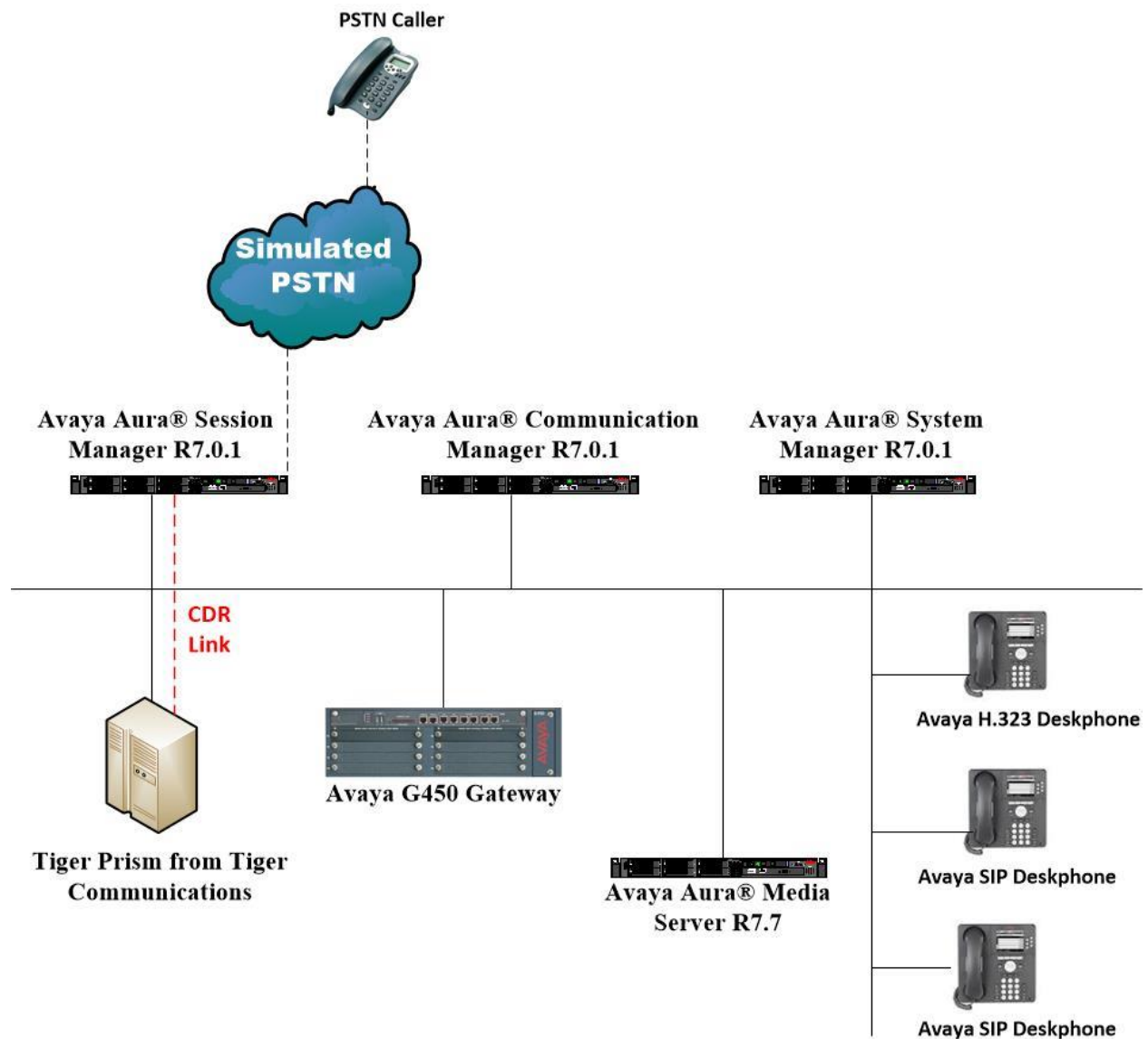


Figure 1: Network solution of Tiger Prism from Tiger Communications and Avaya Aura® Session Manager R7.0.1

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® System Manager running on a virtual server	System Manager 7.0.1.2 Build No. - 7.0.0.0.16266 Software Update Revision No: 7.0.1.2.086007 Service Pack 2
Avaya Aura® Session Manager running on a virtual server	Session Manager R7.0 SP2 Build No. – 7.0.1.2.701230
Avaya Aura® Communication Manager running on a virtual server	R7.0.1 R017x.00.0.441.0 00.0.441.0-23523
Avaya G450 Gateway	37.19.0 /1
Avaya Aura® Media Server running on a virtual server	Media Server SYSTEM R7.7.0.21 Media Server R7.7.0.350
Avaya 9608 H323 Deskphone	96x1 H323 Release 6.6.028
Avaya 9608 SIP Deskphone	96x1 SIP Release 7.0.0.39
Tiger Prism from Tiger Communications <ul style="list-style-type: none">• CallExtractionService.exe• AvayaAuraSM.exe• Collection.exe	2016.4.001.5033 Version: 1.0.62.0 Version: 13.3.5.0 Version: 13.4.1.0

5. Configure Avaya Aura® Communication Manager

There is no specific configuration necessary on Communication Manager for the collection of CDR from Session Manager. It is assumed that the SIP trunk to Session Manager is already setup. The following is a quick overview of the SIP trunk that was used during compliance testing. The steps are performed through the System Access Terminal (SAT) interface. Some screens in this section have been abridged and highlighted for brevity and clarity in presentation.

5.1. Configure SIP Trunk

In the Node Names IP form, note the IP Address of the **procr** and the Session Manager (**SM70vmpg**). The host names will be used throughout the other configuration screens of Communication Manager and Session Manager. Type **display node-names ip** to show all the necessary node names.

display node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
AES63VMPG	10.10.40.30	
PGDECT	10.10.40.50	
SM70vmpg	10.10.40.12	
default	0.0.0.0	
procr	10.10.40.31	
procr6	::	

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is **devconnect.local**. The **IP Network Region** form also specifies the **IP Codec Set** to be used. This codec set will be used for calls routed over the SIP trunk to Session manager as **ip-network region 1** is specified in the SIP signaling group.

display ip-network-region 1		Page 1 of 20
IP NETWORK REGION		
Region: 1		
Location: 1	Authoritative Domain: devconnect.local	
Name: Default region		
MEDIA PARAMETERS	Intra-region IP-IP Direct Audio: yes	
Codec Set: 1	Inter-region IP-IP Direct Audio: yes	
UDP Port Min: 2048	IP Audio Hairpinning? n	
UDP Port Max: 3329		
DIFFSERV/TOS PARAMETERS		
Call Control PHB Value: 46		
Audio PHB Value: 46		
Video PHB Value: 26		
802.1P/Q PARAMETERS		
Call Control 802.1p Priority: 6		
Audio 802.1p Priority: 6		
Video 802.1p Priority: 5		
		AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS	RSVP Enabled? n	
H.323 Link Bounce Recovery? y		
Idle Traffic Interval (sec): 20		
Keep-Alive Interval (sec): 5		
Keep-Alive Count: 5		

In the **IP Codec Set** form, select the audio codec's supported for calls routed over the SIP trunk to Communications Portal. The form is accessed via the **change ip-codec-set n** command. Note that IP codec set 1 was specified in IP Network Region 1 shown above. Multiple codecs may be specified in the **IP Codec Set** form in order of preference; the example below includes **G.729**, **G.711MU** (mu-law) and **G.711A** (a-law), which are supported by Communications Portal.

change ip-codec-set 1

Page 1 of 2

IP Codec Set

Codec Set: 1

	Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size (ms)
1:	G.729	n	2	20
2:	G.711MU	n	2	20
3:	G.711A	n	2	20
4:				
5:				

Prior to configuring a SIP trunk group for communication with Session Manager, a SIP signaling group must be configured. Configure the Signaling Group form shown below as follows:

- Set the **Group Type** field to **sip**.
- Set the **Transport Method** to the desired transport method, for compliance testing this was set to **tls**.
- The **Peer Detection Enabled** field should be set to **y** allowing the Communication Manager to automatically detect if the peer server is a Session Manager.
- Set the **Near-end Node Name** to **procr**. This value is taken from the **IP Node Names** form shown above.
- Set the **Far-end Node Name** to the node name defined for the Session Manager (node name **SM70vmpg**), as per **Section 5.1**.
- Ensure that the recommended TLS port value of **5061** is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- In the **Far-end Network Region** field, enter the IP Network Region configured above. This field logically establishes the **far-end** for calls using this signaling group as network region 1.
- Leave the **Far-end Domain** field blank to allow Communication Manager to accept any domain.
- The **Direct IP-IP Audio Connections** field is set to **y**.
- The **Initial IP-IP Direct Media** field is set to **n**.
- The default values for the other fields may be used.

change signaling-group 1		Page 1 of 2
SIGNALING GROUP		
Group Number: 1	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? n	
Peer Detection Enabled? y	Peer Server: SM	
Near-end Node Name: procr	Far-end Node Name: SM70vmpg	
Near-end Listen Port: 5061	Far-end Listen Port: 5061	
	Far-end Network Region: 1	
Far-end Domain:		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 6	

Configure the **Trunk Group** form as shown below. This trunk group is used for calls to and from Communications Portal. Enter a descriptive name in the **Group Name** field. Set the **Group Type** field to **sip**. Enter a **TAC** code compatible with the Communication Manager dial plan. Set the **Service Type** field to **public-ntwrk**. Specify the signaling group associated with this trunk group in the **Signaling Group** field, and specify the **Number of Members** supported by this SIP trunk group. Accept the default values for the remaining fields.

change trunk-group 1		Page 1 of 21	
TRUNK GROUP			
Group Number: 1	Group Type: sip	CDR Reports: r	
Group Name: SIP TRK	COR: 1	TN: 1	TAC: *801
Direction: two-way	Outgoing Display? y		
Dial Access? n	Night Service:		
Queue Length: 0			
Service Type: public-ntwrk	Auth Code? n		
	Member Assignment Method: auto		
	Signaling Group: 1		
	Number of Members: 10		

On **Page 2** of the trunk-group form the **Preferred Minimum Session Refresh Interval (sec)** field should be set to a value mutually agreed with Presence to prevent unnecessary SIP messages during call setup. Session refresh is used throughout the duration of the call, to check the other side has not gone away, for the compliance test a value of **1800** was used.

change trunk-group 1		Page 2 of 21	
Group Type: sip			
TRUNK PARAMETERS			
Unicode Name: auto			
Redirect On OPTIM Failure: 5000			
SCCAN? n	Digital Loss Group: 18		
	Preferred Minimum Session Refresh Interval(sec): 1800		
Disconnect Supervision - In? y Out? y			
XOIP Treatment: auto Delay Call Setup When Accessed Via IGAR? N			

Settings on **Page 3** can be left as shown below.

change trunk-group 1	Page 3 of 21
TRUNK FEATURES	
ACA Assignment? n	Measured: none
	Maintenance Tests? y
Numbering Format: private	UI Treatment: shared
	Replace Restricted Numbers? n
	Replace Unavailable Numbers? n
Modify Tandem Calling Number: no	
Show ANSWERED BY on Display? y	

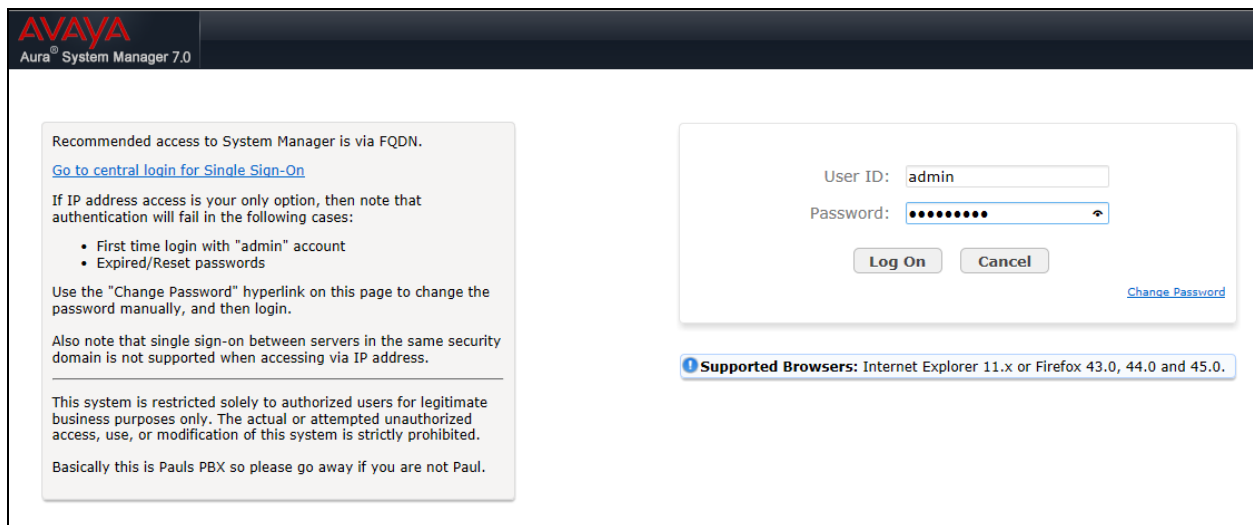
Settings on **Page 5** are as follows.

change trunk-group 1	Page 5 of 22
PROTOCOL VARIATIONS	
Mark Users as Phone? y	
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	
Send Transferring Party Information? y	
Network Call Redirection? y	
Build Refer-To URI of REFER From Contact For NCR? n	
Send Diversion Header? y	
Support Request History? y	
Telephone Event Payload Type: 101	
Convert 180 to 183 for Early Media? n	
Always Use re-INVITE for Display Updates? n	
Identity for Calling Party Display: P-Asserted-Identity	
Block Sending Calling Party Location in INVITE? n	
Accept Redirect to Blank User Destination? n	
Enable Q-SIP? n	
Interworking of ISDN Clearing with In-Band Tones: keep-channel-active	
Request URI Contents: may-have-extra-digits	

6. Configure Avaya Aura® Session Manager

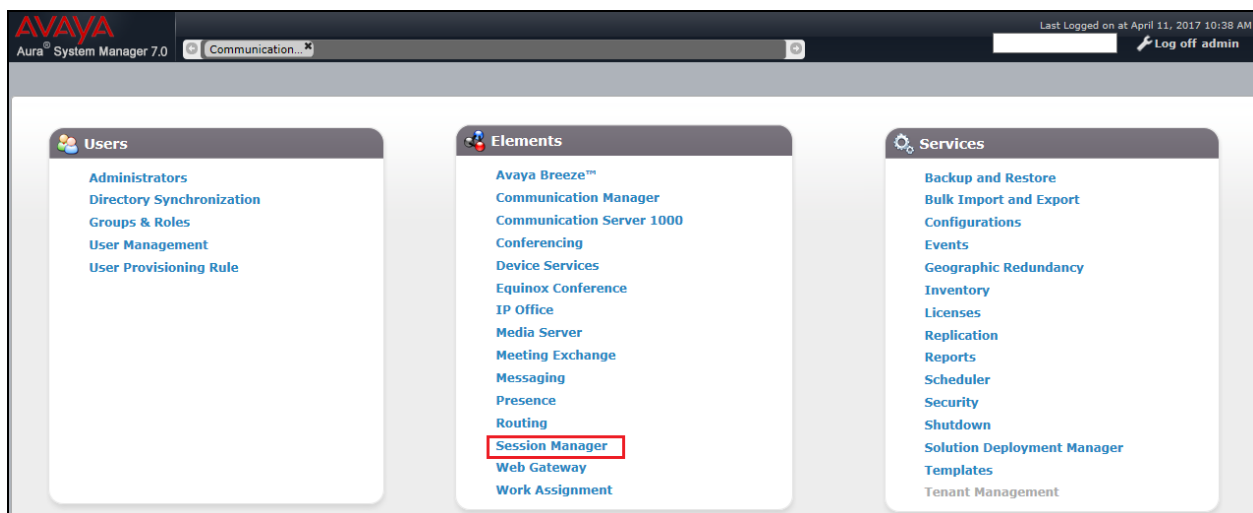
Note: For the compliance testing, the “Enhanced XML file” format of CDR was used as the Data File Format on Session Manager.

In order to make changes in Session Manager a web session is established to System Manager. Log into System Manager by opening a web browser and navigating to <http://<System Manager IP Address>/SMGR>. Enter the appropriate credentials for the **User ID** and **Password** and click on **Log On** highlighted below.

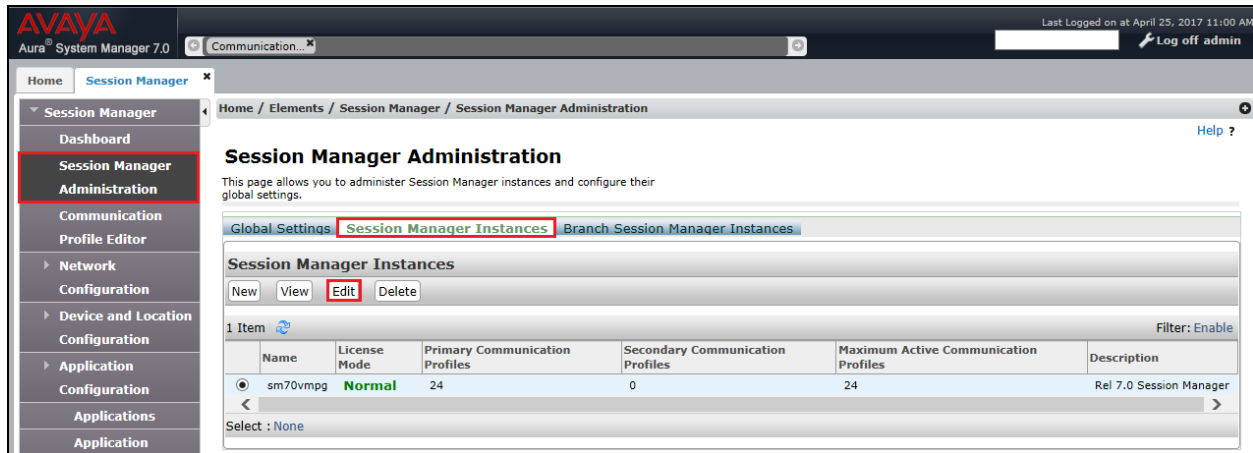


The screenshot shows the Avaya Aura System Manager 7.0 login interface. On the left, a grey box contains instructions: "Recommended access to System Manager is via FQDN. Go to central login for Single Sign-On. If IP address access is your only option, then note that authentication will fail in the following cases: • First time login with 'admin' account • Expired/Reset passwords. Use the 'Change Password' hyperlink on this page to change the password manually, and then login. Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address. This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited. Basically this is Pauls PBX so please go away if you are not Paul." On the right, a white box contains the login form with fields for "User ID" (containing "admin") and "Password" (masked with dots), and "Log On" and "Cancel" buttons. A "Change Password" link is also present. Below the form, a blue banner states "Supported Browsers: Internet Explorer 11.x or Firefox 43.0, 44.0 and 45.0."

Once logged in click on **Session Manager** highlighted below.



The Session Manager tab is displayed. In the left navigation pane select **Session Manager Administration**. When the **Session Manager Administration** page is displayed select the **Session Manager Instances** tab and then select the Session Manager instance e.g., **sm70vmpg** and click on **Edit** button to edit.



The **Edit Session Manager** page is displayed. Scroll down to the **CDR** section, check on the check box **Enable CDR** to enable the CDR feature and enter a password in the **Password** and **Confirm Password** box for the **CDR_User**. Ensure that both **Include User to User Calls** and **Include Incomplete Calls** are both ticked as shown. Click the **Commit** button at the end of the page to commit the changes.

CDR

Enable CDR ☒

User

Password

Confirm Password

Data File Format

Include User to User Calls ☒

Include Incomplete Calls ☒

Personal Profile Manager (PPM) - Connection Settings

Limited PPM Client Connection ☒

*Maximum Connection per PPM Client

PPM Packet Rate Limiting ☒

*PPM Packet Rate Limiting Threshold

Event Server

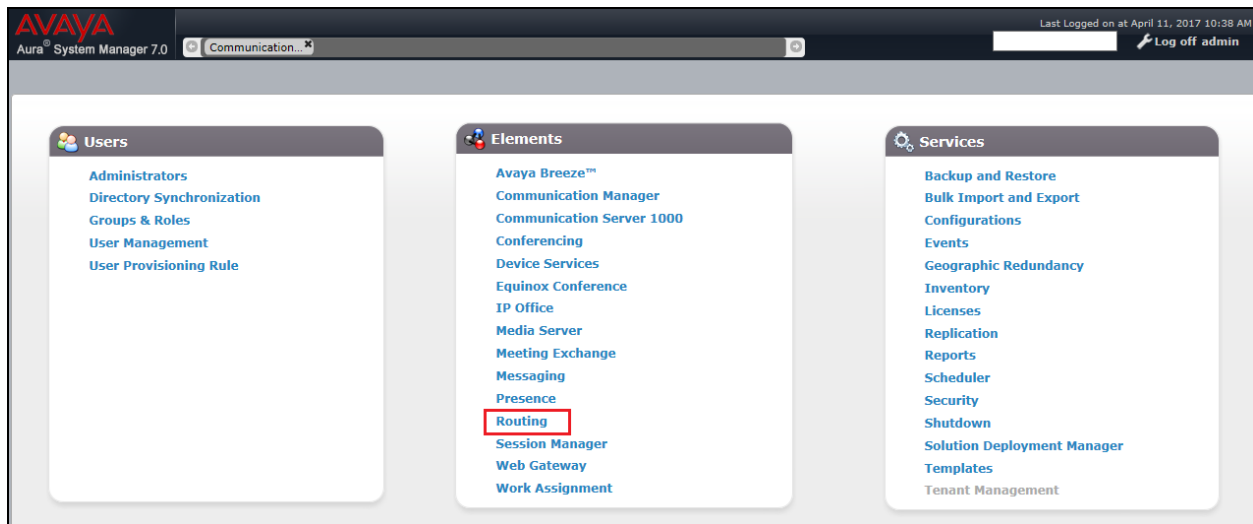
Clear Subscription on Notification Failure

* Required

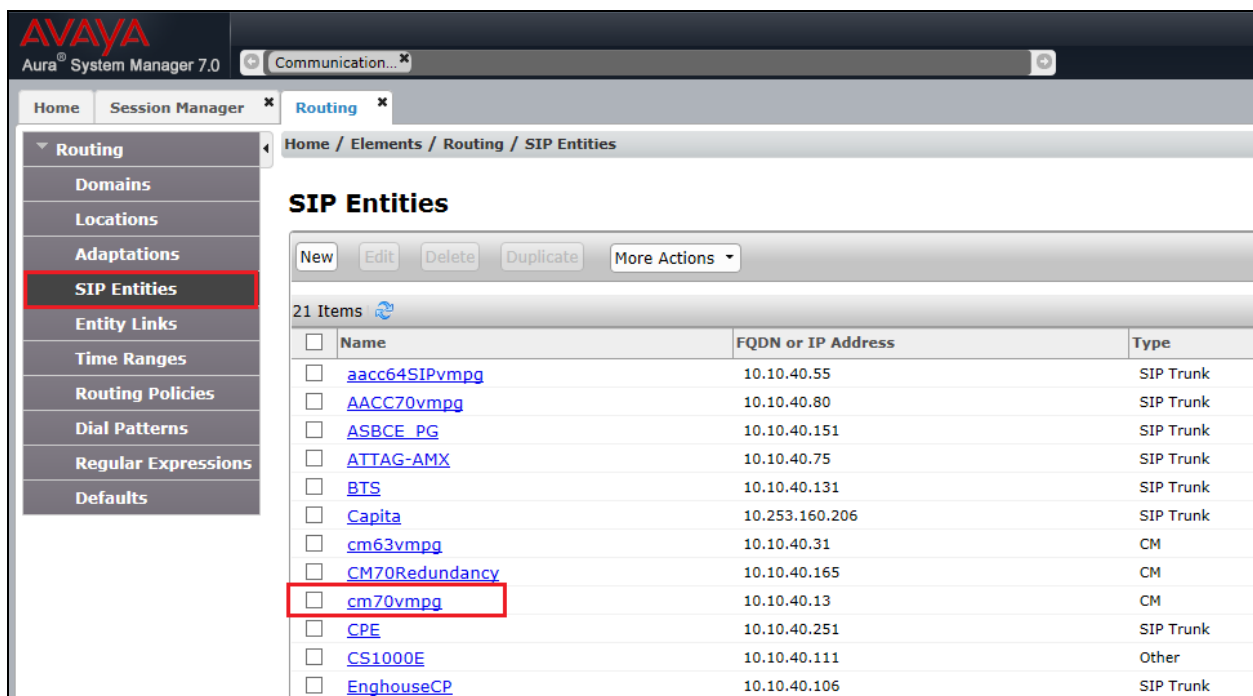
Commit

Cancel

Each SIP Entity must have their CDR enabled as well; in order to make changed to SIP Entities select **Routing** from the main page.



Click on **SIP Entities** in the left window and select the Communication Manager SIP Entity from the main window.



Change **Call Detail Recording** to **both** as shown below from the drop-down menu and click on **Commit** once finished.

Note: Repeat the same procedure for other SIP Entities if needed

SIP Entity Details

CommitCancel

General

* Name:cm70vmpg

* FQDN or IP Address:10.10.40.13

Type:CM

Notes:

Adaptation:

Location:PGLAB

Time Zone:Europe/Dublin

* SIP Timer B/F (in seconds):4

Credential name:

Securable:☒

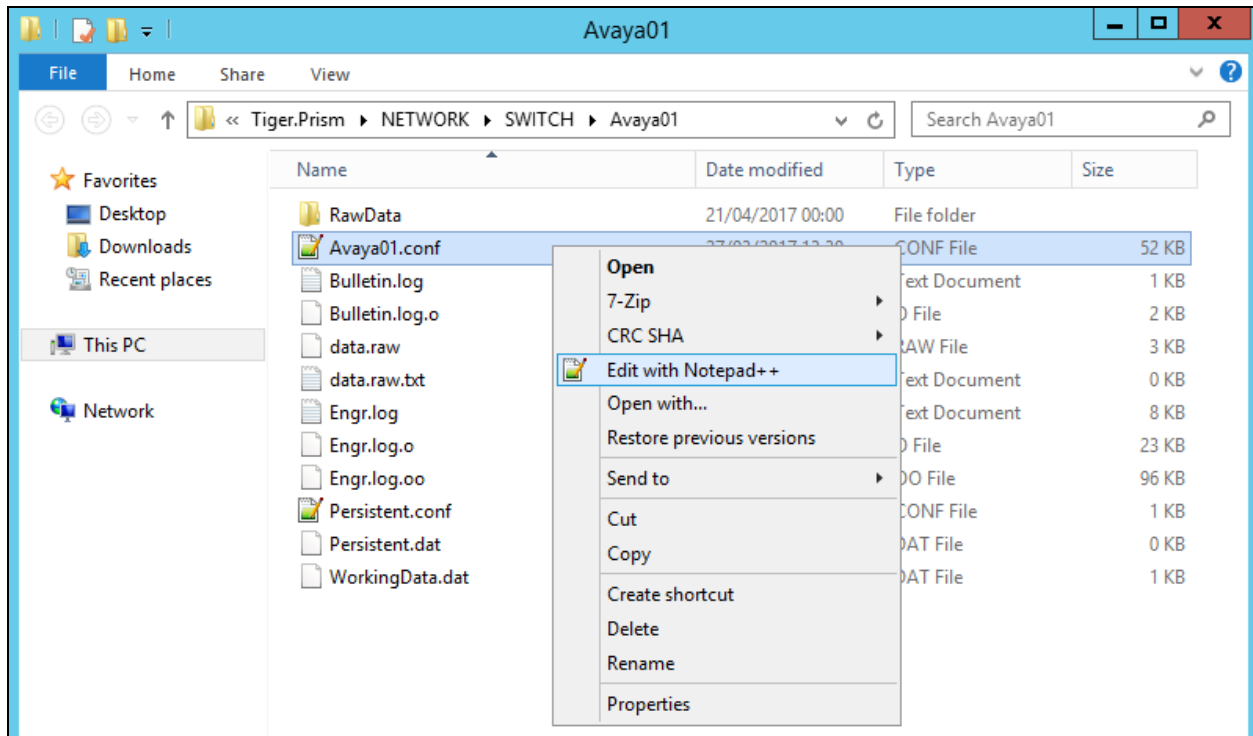
Call Detail Recording:both

7. Configure Tiger Prism

The configuration information provided in this section describes the setup of Tiger Prism to collect CDR records generated by Session Manager via SFTP.

7.1. Configure Configuration file

On the Tiger Prism server, modify the configuration file; in this case it is called D:\Tiger.Prism\network\Switch\Avaya01\Avaya01.conf.

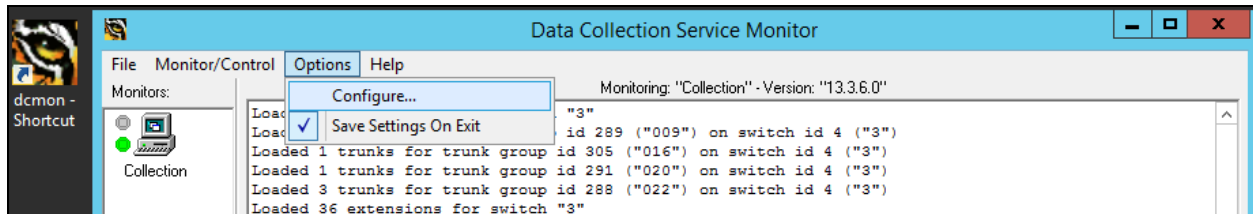


In the **[Switch]** section ensure the **Type** field is set to **AvayaAuraSM**. In the **[Input]** section the type=file, see the full details for this section below. The **[FieldDefsFile]** section should point to the location of the field definition file. This was named **AvayaAuraSM_7_XML.conf** and this file is displayed in full in **Appendix A** of these Application Notes.

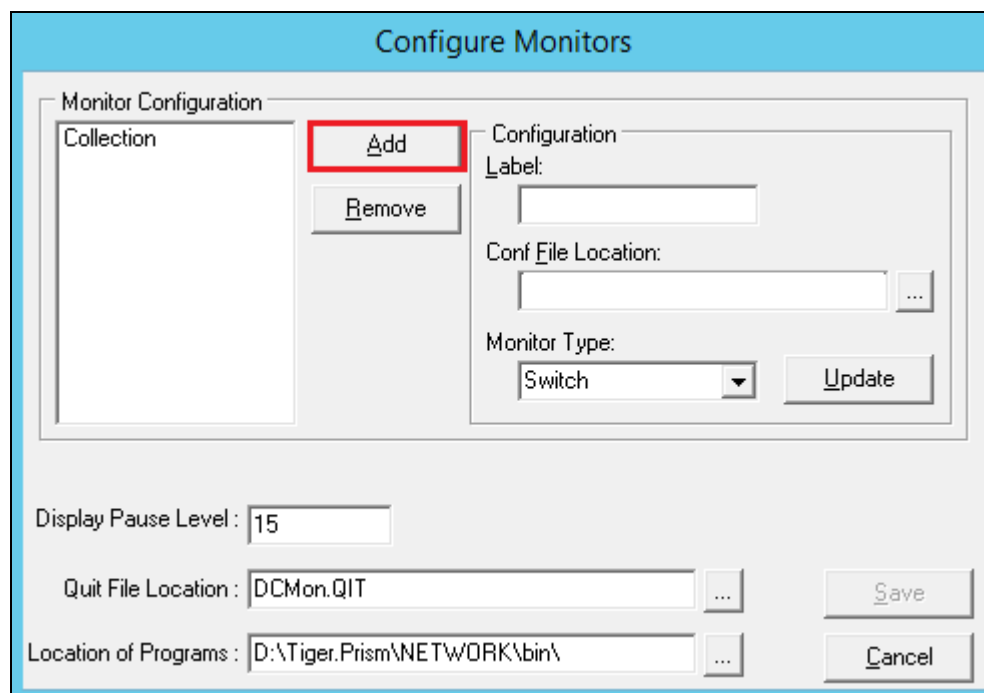
```
[Switch]  
Type=AvayaAuraSM  
Revision=7.0  
MaxCallHoldTime=60000  
MaxTandemHoldOn=30000  
MaxSectionHoldOn=60000  
RecordDiscardBlacklistHoldOn=3600000  
MaxLineLength=2000  
BreakYear=1980  
CustomerId=  
NodeId=2  
DiscardDuplicateRecords=1  
DiscardOutgoingWithNoCalledDigits=0  
RecordTenant=0  
PassTrunkGroupLength=1  
CallTimeType=0  
SequenceNumberDays=7  
SequenceNumbersHeld=7  
DefaultLatency=0  
DiversionChargedPartyRule=0  
TransferChargedPartyRule=0  
QueueDeviceIsUnanswered=0  
SkipHostNameLookup=1  
ForwardNoAnswerAfterMS=15000  
IsolatedSwitch=0  
[Input]  
Name=D:\Tiger.Prism\Network\Switch\Avaya01\Data.raw  
Type=file  
Direction=input  
ExitAtEof=0  
DeleteOnCompletion=1  
WaitForFileCreation=1  
BufferSize=1024  
TimeOut=200  
Sharing=none  
CascadeDisable=1  
[FieldDefsFile]  
Name=D:\Tiger.Prism\Network\SwitchConf\AvayaAuraSM_7_XML.conf
```


7.2. Configure Data Collection

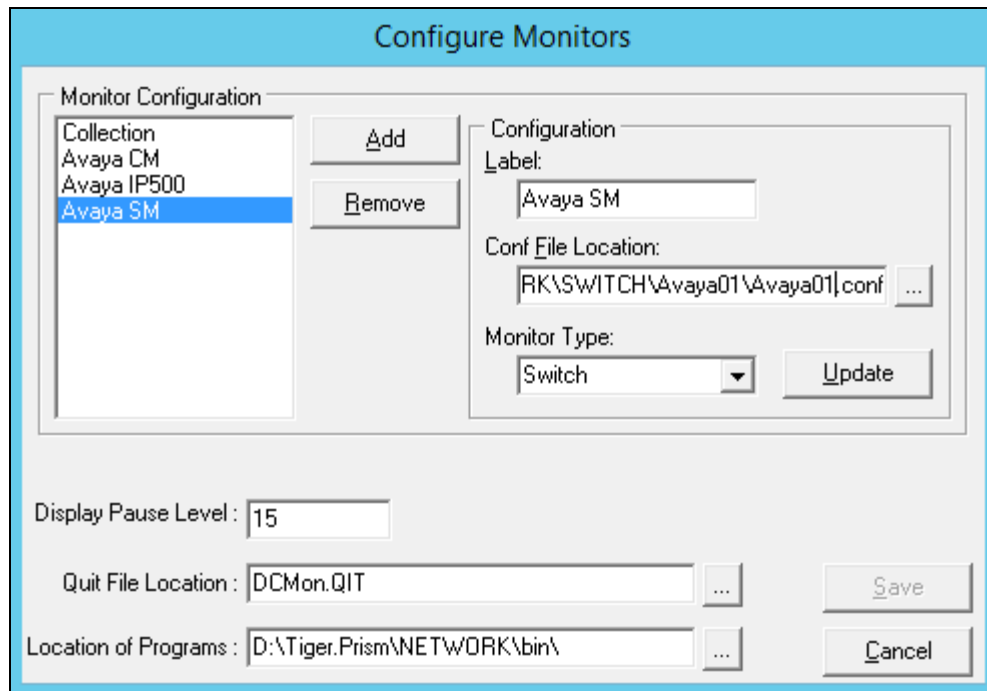
On the Tiger Prism server, open **dcmmon.exe** (this was done from a shortcut on the desktop as shown below). On the main Data Collection Monitor screen toolbar, click on **Options** → **Configure**.



There are two types of monitor types to be configured - one for the collection which interfaces with the Tiger Prism database and one for the switch which interfaces with Session Manager. In the **Configure Monitors** dialog box click the **Add** button. Below shows the addition of the interface to Session Manager.

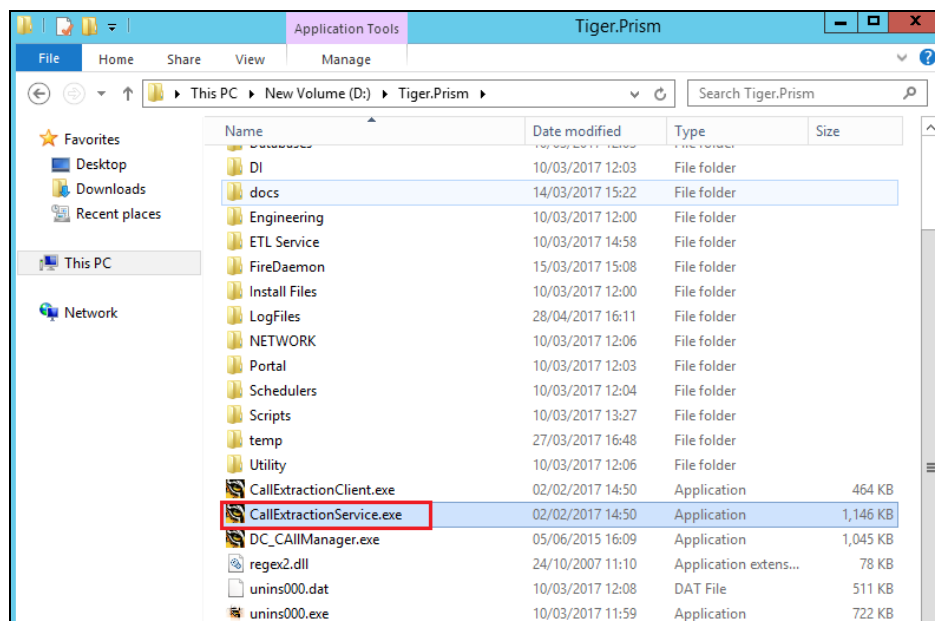


In the **Label** field enter a descriptive name for the switch monitor type. In the **Conf File Location** field enter or browse to the location of the **Avaya02.conf** file created in **Section 6.1**. The **Avaya01.conf** file for this compliance testing was located at **D:\Tiger.Prism\network\Switch\Avaya01**. For the **Monitor Type** select **Switch** from the drop-down list. The rest of the parameters can be left with their default values. Click **Save**.

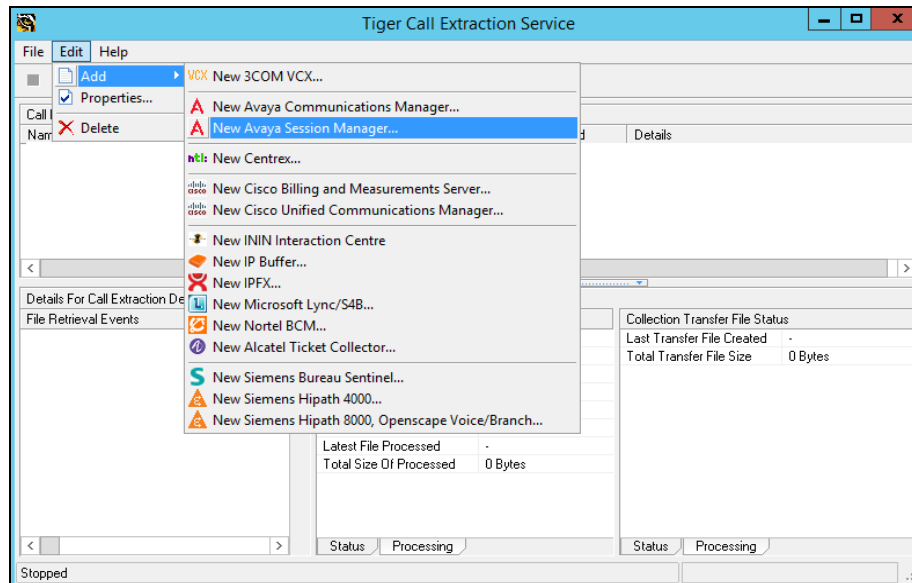


7.3. Configure Call Extraction Service

On the Tiger Prism server, open **D:\Tiger.Prism\CallExtractionService.exe**.

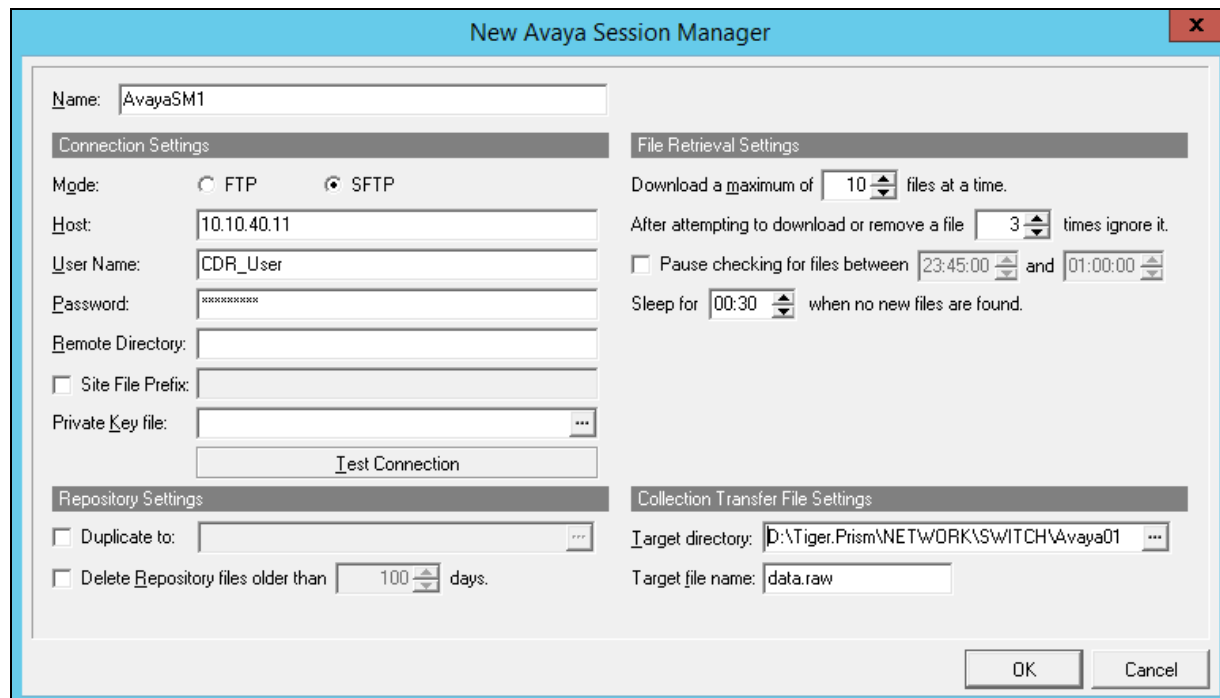


In the menus select **Edit → Add → New Avaya Session Manager**.

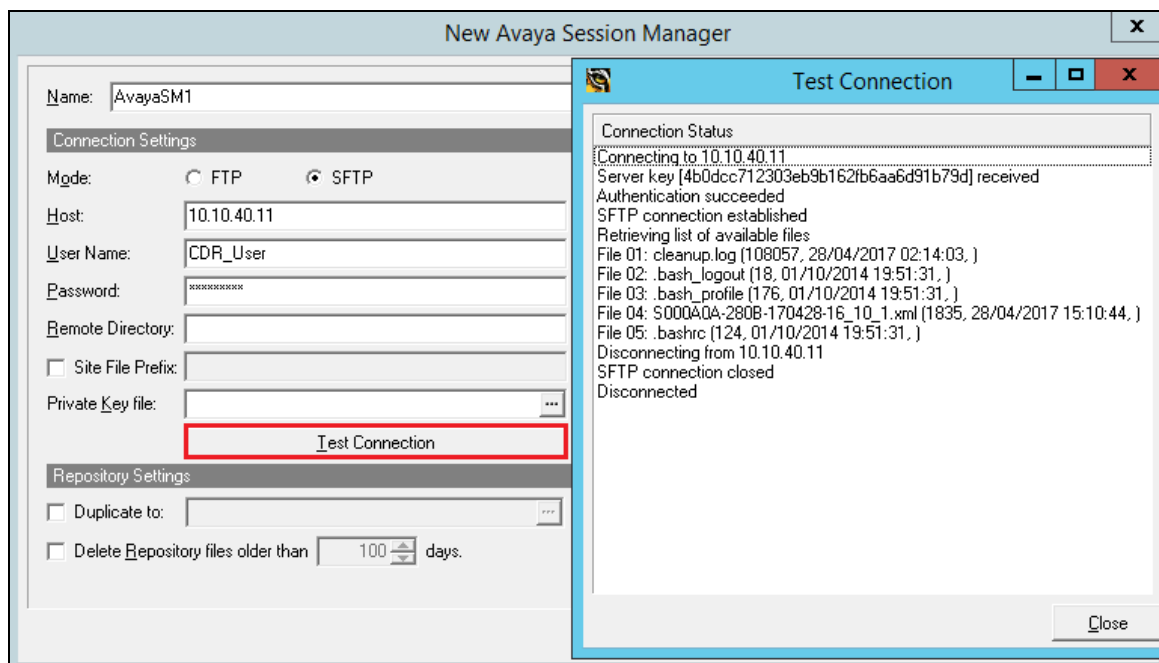


Enter the following information:

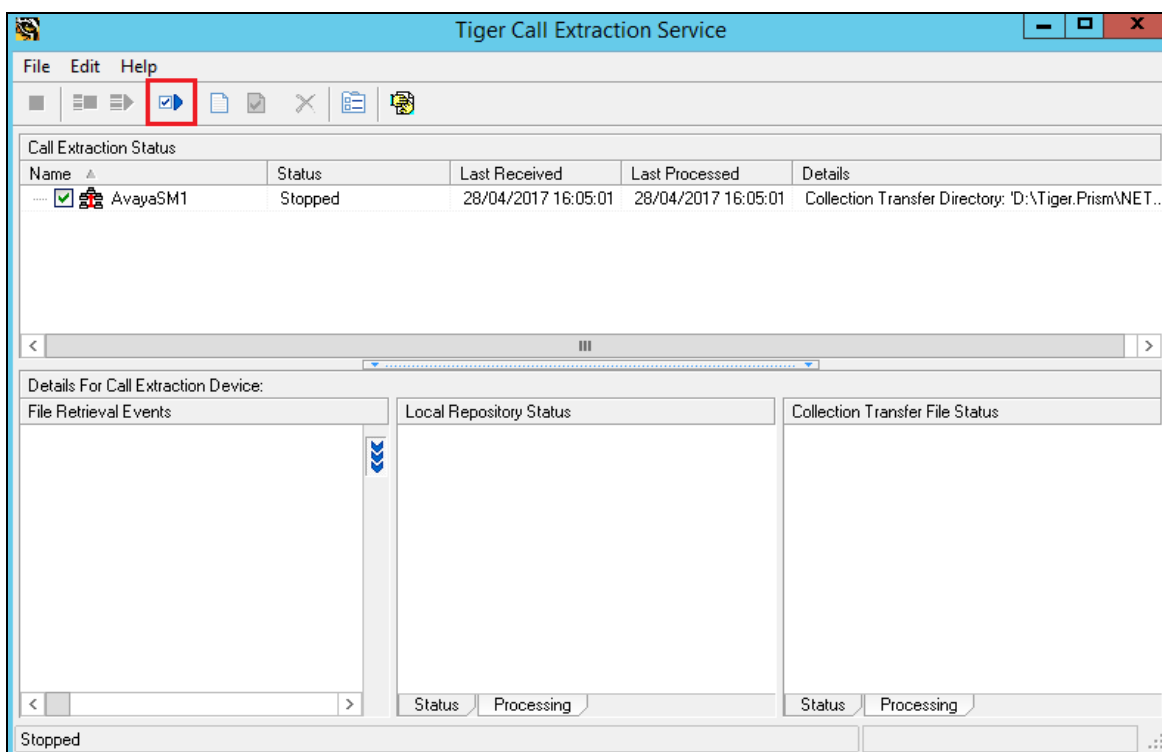
Name	Enter a suitable name.
Host	Enter the Session Managers IP Address.
User Name	This should be CDR_User .
Password	This will be the password configured in Section 6 .
Target directory	D:\Tiger.Prism\Network\Switch\Avaya01\



Select **Test Connection** to confirm the login details have been entered correctly. A new window should pop up showing the SFTP connection being **established** correctly as shown below.

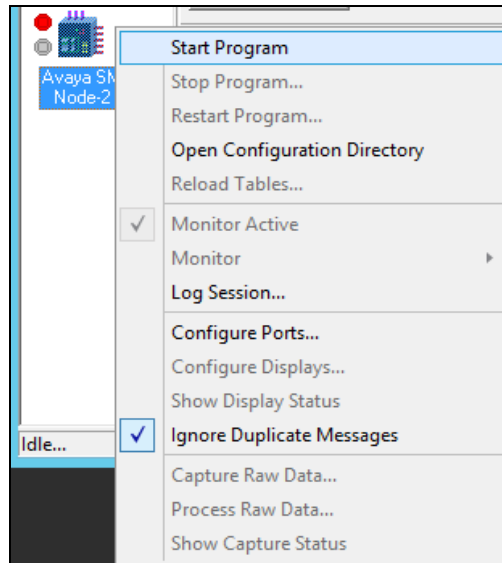


Start the Extraction by clicking in the toolbar.

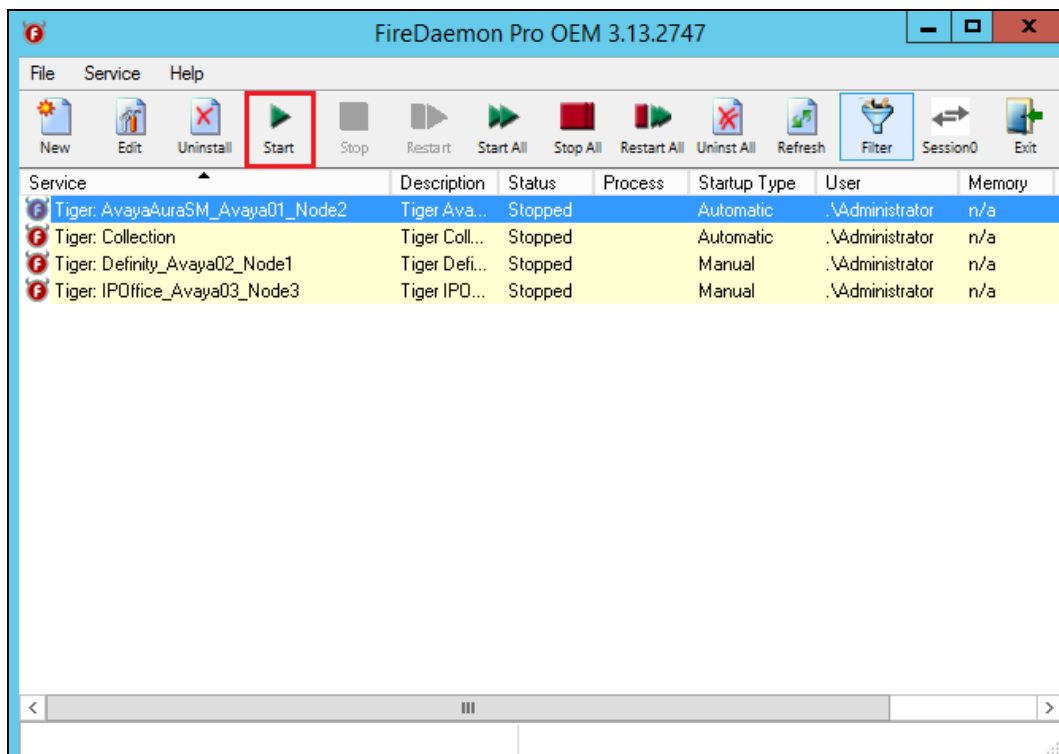


7.4. Start Data Collection

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 SM**.



Start the **Tiger: AvayaAuraSM** node as shown below. From the same screen start the **Tiger:Collection** also.

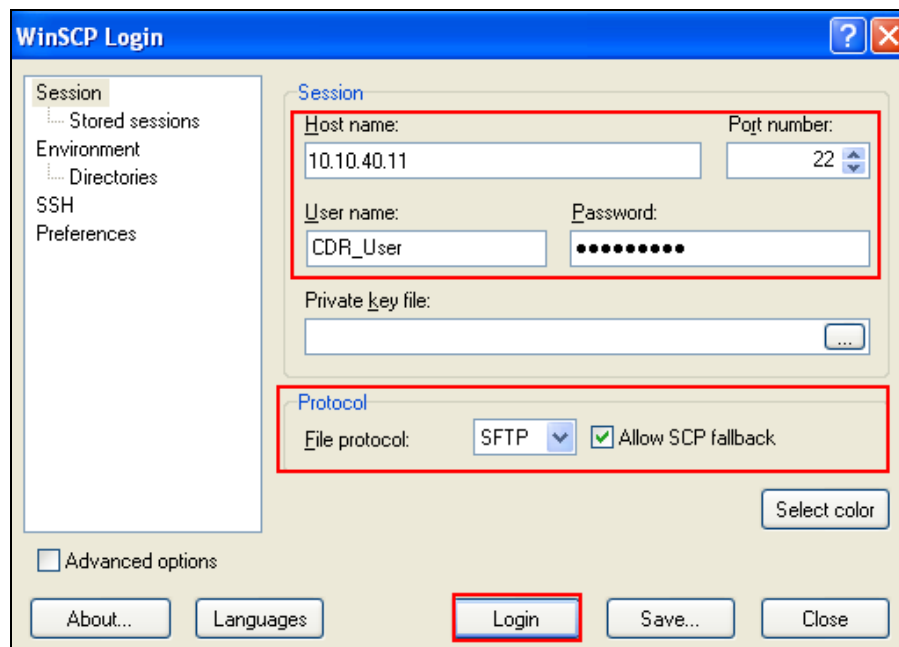


8. Verification

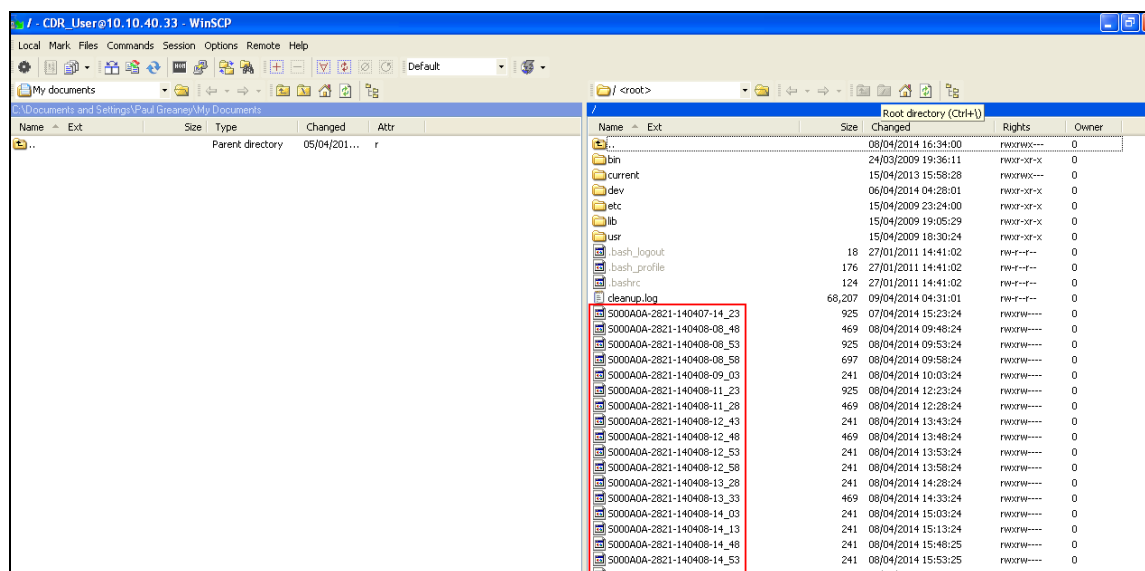
The following steps may be used to verify the configuration.

8.1. CDR information is being collected by Session Manager

Use a secure FTP application, e.g., WinSCP to connect to Session Manager by using the CDR_User and password to access the special folder that store the CDR files.



Place some different kinds of call; wait some minutes for Session Manager to generate the CDR files. There should be a list of files present as shown below.



8.2. Verify Data Collection Monitor Status

Place a call and verify that Tiger Prism 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. Verify that the **Collection** and **Avaya SM** display a green status symbol indicating they are online. Confirm that the raw data in the bottom pane is tabulated accordingly for the database in the top pane.

The screenshot shows the 'Data Collection Service Monitor' application. The left sidebar lists three monitors: 'Collection' (green), 'Avaya SM Node-2' (green), and 'Avaya IP500 Node-3' (red). The main area contains two monitoring panes.

Top Pane: Monitoring: "Collection" - Version: "13.3.6.0"

Opened file "D:\Tiger.Prism\Network\Collection\WorkingData.dat", size 0, offset 0
Closing file "D:\Tiger.Prism\Network\Collection\WorkingData.dat", size 0, offset 0
Input port \\.\mailslot\tiger\collect\input has been suspended.
Input port \\.\mailslot\tiger\collect\input has been resumed.

Line	Time	OG	IC	IT	OG	IC	IT	OG	IC	IT	OG	IC	IT	OG	IC	IT	OG	IC	IT
1	26	OG	17/04/21	15:57:02	0:00	0:00:05	E-7000												
1	27	IC	17/04/21	15:57:14	0:02	0:00:05	T-*801001	2016											
Monitor port opened.																			
1	28	IT	17/04/21	16:15:36	0:00	0:00:08	E-7000												
1	29	OG	17/04/21	16:15:45	0:00	0:00:04	E-7001												
1	30	IC	17/04/21	16:15:53	0:01	0:00:04	T-*801001	2016											
1	31	IC	17/04/21	16:16:13	0:01	0:00:06	T-*801001	2016											

Stop Display

Bottom Pane: Monitoring: "Avaya CM" - Processing Exe: "Definity" - Version: "13.3.6.0" - Field Definitions: "CM6_SA8201.conf"

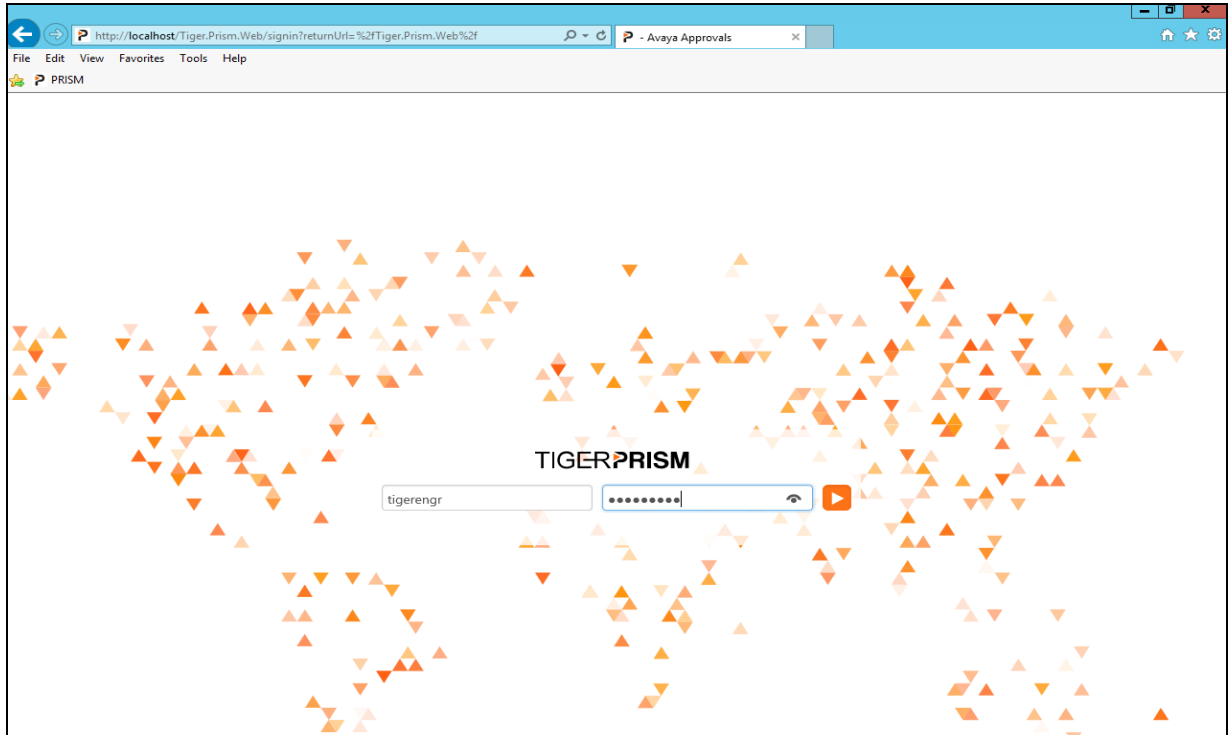
Waiting for connection from 10.10.40.13 on port 9000...
Input port Avaya CM 02 Socket Input has been suspended.
Cannot open \\.\mailslot\tiger\collect\input: GetLastError() = 2
Input port Avaya CM 02 Socket Input has been resumed.
Connection established from 10.10.40.13 on port 9000.

Time	OG	IC	IT	OG	IC	IT	OG	IC	IT	OG	IC	IT	OG	IC	IT	OG	IC	IT
15:57 21/04	210417155707	000057	8*801	2016	7000	007	0	0										
	210417155716	00002G		7100	2016	001	0	0										
	210417155721	000059		7100	2016	001	0	0										
	210417161544	000080		7100	7000													
	210417161549	000047	8*801	2016	7001	002	0	0										
	210417161554	00001G		7000	2016	001	0	0										
	210417161558	000049		7000	2016	001	0	0										
	210417161614	00001G		7001	2016	001	0	0										
	210417161620	000069		7001	2016	001	0	0										
	210417161627	00003G		7102	2016	001	0	0										
	210417161631	000049		7102	2016	001	0	0										

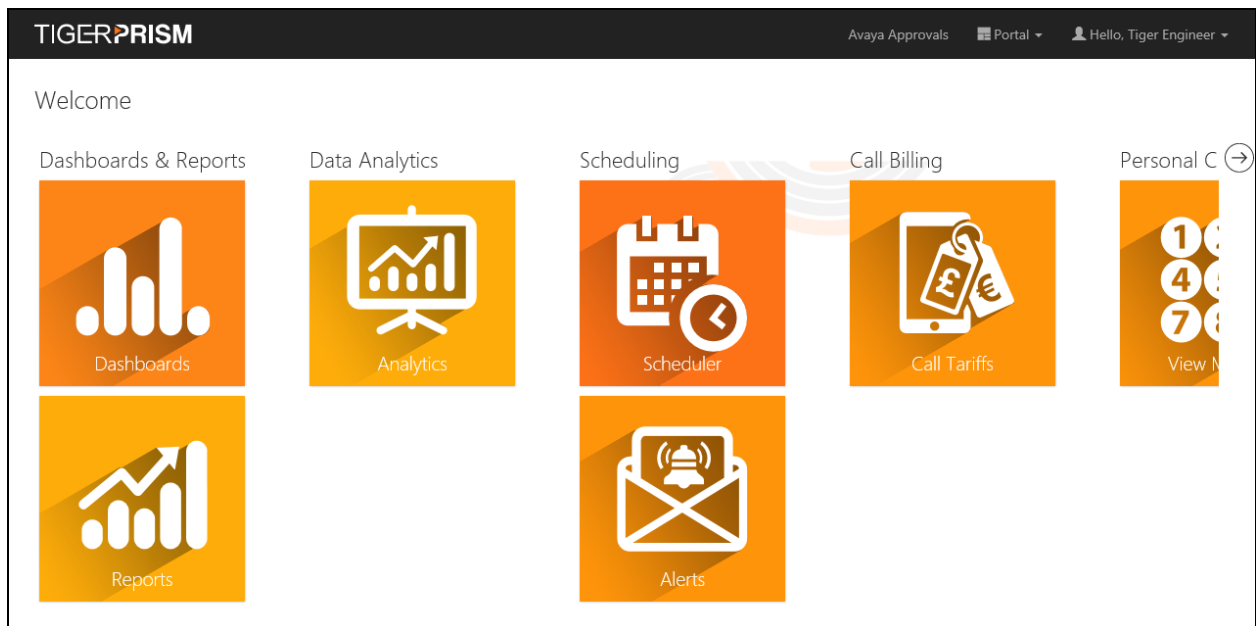
Stop Display

8.3. Verify Report/Billing Information Accuracy

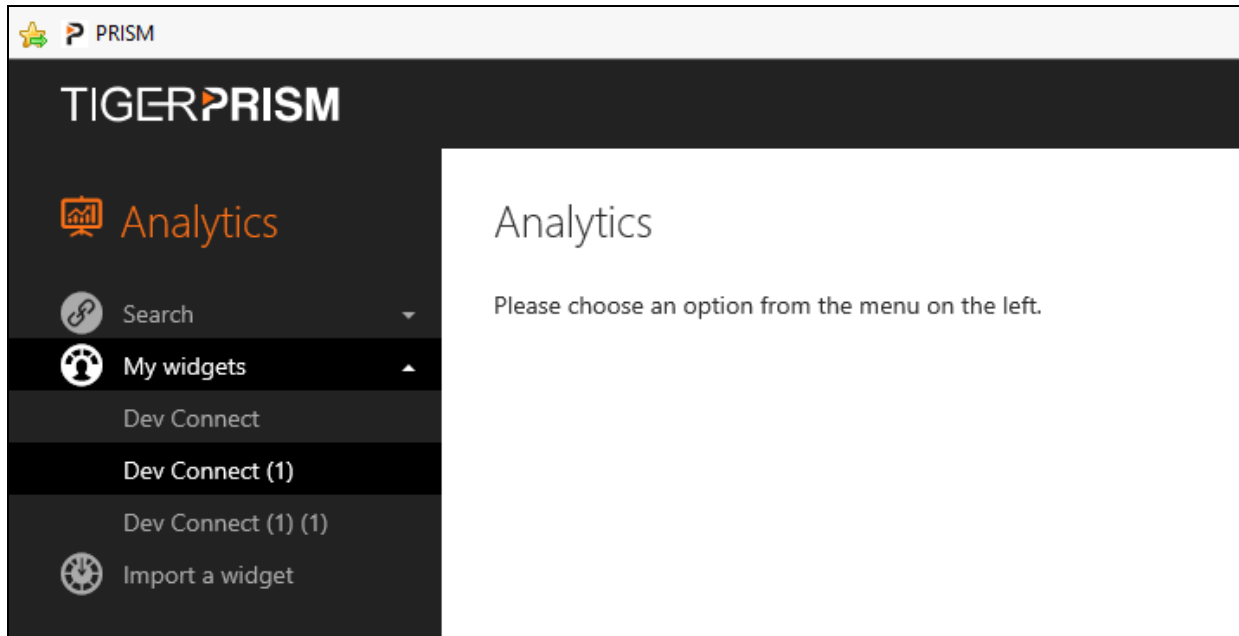
Open a web browser to the Tiger Prism server as shown below. Enter the appropriate credentials and click on the login icon.



Once logged in, click on **Analytics**.



From the left-hand menu select **Search** → **Legs** (not shown). This will display the calls for the current day. For the testing a widget was created; this is a custom saved report with the required fields for verification testing added to the displayed. In the example below **DevConnect (1)** was created and selected to be displayed.



The following is a report run for the previous month showing all the data for calls for that month.

TIGERPRISM

Analytics

Search

My widgets

Dev Connect

Dev Connect (1)

Dev Connect (1) (1)

Import a widget

Avaya Approvals

Modules

Hello, Tiger Engineer

Dev Connect (1)

Tree

1.Avaya IVT

Select by

Quick dates

Dates

This month

	Leg start	Call direction	Calling digits	Called digits	Talk time	Ring time	Call outcome	Initial
	05/04/2017 11:57:13	Incoming	3000	7000	0:00:00	0:00:02	Connected	Norn
	05/04/2017 11:57:15	Tandem	3000	7000	0:00:01.195	0:00:00	Connected	Norn
	05/04/2017 11:59:32	Tandem	3000	7000	0:00:19.303	0:00:00	Connected	Norn
	05/04/2017 11:59:43	Tandem	7000	3006	0:00:08.015	0:00:00	Connected	Norn
	05/04/2017 11:59:51	Tandem	3000	3006	0:00:51.373	0:00:00	Connected	Norn
	07/04/2017 13:17:20	Internal	7000	7001	0:00:06	0:00:00	Connected	Norn
	07/04/2017 13:17:36	Internal	7000	7102	0:00:13	0:00:00	Connected	Norn
	07/04/2017 13:17:36	Incoming	7000	7102	0:00:13.453	0:00:00	Connected	Norn
	07/04/2017 13:17:54	Internal	7102	7100	0:00:08	0:00:00	Connected	Norn
	07/04/2017 13:17:54	Internal	7102	7100	0:00:07.562	0:00:00	Connected	Norn
	07/04/2017 13:18:06	Internal	7100	7001	0:00:06	0:00:00	Connected	Norn
	07/04/2017 13:18:06	Outgoing	7100	7001	0:00:05.765	0:00:00	Connected	Norn
	07/04/2017 13:24:52	Tandem	7001	2016	0:00:08.659	0:00:00	Connected	Norn
	07/04/2017 13:24:53	Outgoing	7001	2016	0:00:08	0:00:00	Connected	Norn
	07/04/2017 13:25:06	Outgoing	7100	2016	0:00:18	0:00:00	Connected	Norn

1

2

3

4

5

...

50

items per page

9. Conclusion

These Application Notes describe the required configuration steps for Avaya Aura® Session Manager R7.0.1 and Tiger Prism from Tiger Communications to collect Call Detail records from Avaya Aura® Session Manager. All test cases completed successfully with the observations and exceptions noted in **Section 2.2**.

10. 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>.

- *Administering Avaya Aura® Session Manager*, Release 7.0.1

Tiger Prism product information is available from <http://www.tigercomms.com>

Appendix A

AvayaAuraSM_7_XML.conf

```
#####
# Configuration file for the Avaya Aura Session Manager switch for Release
# 6.3.4 XML format output.
#
# Created by: I.D.Hay on 6th December 2016
#
# $Revision: 4158 $
# $Author: ihay $
# $Date: 2017-02-03 15:27:48 +0000 (Fri, 03 Feb 2017) $
#
# (c) 2017 Tiger Communications plc
#####

#####
# Format of entries is "N:S,L,T" or "S,L", where:
# "N" is the line number
# "S" is the offset of the field's starting position in the line
# "L" is the length of the field
# "T" is the field type, with valid values
# "I" is interpreted as a decimal integer
# "i" is blank or interpreted as a decimal integer
# "X" is interpreted as a hexadecimal integer
# "x" is blank or interpreted as a hexadecimal integer
# "C" is an interpreted character string
# "B" is blank space
# "F=value" is the fixed character string "value"
# "f=value" is blank or the fixed character string "value"
# "V=value" is a variable length string, terminated by the string "value"
# "v=value" is blank or a variable length string, terminated by the string
"value"
# "W=value" is a variable length decimal integer, terminated by the string
"value"
# "w=value" is blank or a variable length decimal integer, terminated by the
string "value"
# "H=value" is a variable length hexadecimal integer, terminated by the string
"value"
# "h=value" is blank or a variable length hexadecimal integer, terminated by the
string "value"
#####

[SwitchInfo]
SwitchName=Avaya Aura Session Manager
SwitchVersion=6.3.4
ProgramName=AvayaAuraSM
ProgramVersion=13.2.2.0

[Description]
0=This is the field definitions for the Avaya Aura Session Manager Release 6.3.4 XML

[SampleData]
0= <?xml version="1.0" encoding="UTF-8"?>
1= <calls xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
2= <call>
3= <call_time>2002-05-30T09:30:10Z</call_time>
4= <duration>PT3H27M1.246S</duration>
```

```

5=          <condition_code>4</condition_code>
6=          <parties>
7=              <dialled_number>3035389999</dialled_number>
8=              <calling_number>9702251234</calling_number>
9=          </parties>
10=         <sip_entities>
11=             <terminating>cm4</terminating>
12=             <originating>cm7</originating>
13=         </sip_entities>
14=         <feature_flag>4</feature_flag>
15=         <bcc>M</bcc>
16=         <ma_uui>0</ma_uui>
17=         <resource_flag>0</resource_flag>
18=         <bandwidth>31</bandwidth>
19=         <av_gsid>f652e050-a876-11e2-b585-00145e3e9b22</av_gsid>
20=         <ip_addresses>
21=             <calling>10.42.35.111</calling>
22=             <called>123.43.1.76</called>
23=         </ip_addresses>
24=         <usage>
25=             <voice>Y</voice>
26=             <video>N</video>
27=             <fax>N</fax>
28=             <text>N</text>
29=             <other>N</other>
30=         </usage>
31=         <codec>1</codec>
32=         <tenant_ids>
33=             <calling>Joe's Bar and Grill</calling>
34=             <called>One Hour Dry Cleaning</called>
35=         </tenant_ids>
36=     </call>
37= </calls>

```

```

[FieldDefs]
XML_HEADER_START=3:0.15,F='<?xml version="'
XML_HEADER_MAJOR_VERSION=3:15.1,W='.'
XML_HEADER_MINOR_VERSION=3:17.1,W='"'
XML_HEADER_ENCODING=3:-1.1,V='>'
# XML_HEADER_MINOR_VERSION=3:17.1,W='"' encoding=""
# XML_HEADER_ENCODING=3:29.1,V='>'
XML_LINE=4:0.200,C
DATE_TIME_YEAR=5:0.4,W='-'
DATE_TIME_MONTH=5:5.2,W='-'
DATE_TIME_DAY=5:8.2,W='T'
DATE_TIME_HOUR=5:11.2,W=':'
DATE_TIME_MINUTE=5:14.2,W=':'
DATE_TIME_SECOND=5:17.2,I
DATE_TIME_TIMEZONE=5:19.6,C
DATE_TIME_TZ_DIRECTION=6:0.1,C
DATE_TIME_TZ_HOUR=6:1.2,W=':'
DATE_TIME_TZ_MINUTE=6:4.2,I

# Unused fields
END_HOUR=1:-1.2,I
END_MINUTE=1:-1.2,I
DUR_HOUR=1:-1.1,I
DUR_MINUTE=1:-1.2,I
DUR_TENTH_MINUTE=1:-1.1,I
CONDITION_CODE=1:-1.1,C
DIALLED_NUMBER=1:-17.15,C
CALLING_NUMBER=1:-12.10,C

```

```

TERM_SIP_ENTITY=1:-18.7,C
ORIG_SIP_ENTITY=1:-17.7,C
FEATURE_FLAG=1:-13.1,C
BCC=1:-12.1,C
MA_UUI=1:-13.1,C
RESOURCE_FLAG=1:-14.1,C
BANDWIDTH=1:-104.2,I
AV_GSID=1:-108.36,C
CALLING_PARTY_IP=1:-170.15,C
CALLED_PARTY_IP=1:-111.15,C
CALL_TIME=1:-1.2,C
DURATION=1:-1.2,I
CODEC=1:-1.2,C
VOICE=1:-1.2,C
VIDEO=1:-1.2,C
FAX=1:-1.2,C
TEXT=1:-1.2,C
OTHER=1:-1.2,C
CALLING_TENANT=1:-1.2,C
CALLED_TENANT=1:-1.2,C

DATAREC_HOUR=2:-1.2,W=':'
DATAREC_MINUTE=2:-1.2,W=' '
DATAREC_MONTH=2:-1.2,W='/'
DATAREC_DAY=2:-1.2,I

#####
# Format of [XmlSections] entries is "<XML section>=<configuration section>"
#####
[XmlSections]
calls=CallsTags
call=CallTags
parties=PartiesTags
sip_entities=SipEntitiesTags
ip_addresses=IpAddressesTags
usage=UsageTags
tenant_ids=TenantIdsTags

#####
# Format of [*Tags] entries is "<FieldName>=<XML tag>,T", where
# "T" is any of the non-blank field types mentioned above
#####
[CallsTags]
# No tags in this section

[CallTags]
CALL_TIME=call_time,C
DURATION=duration,C
CONDITION_CODE=condition_code,C
FEATURE_FLAG=feature_flag,C
BCC=bcc,C
MA_UUI=ma_uui,C
RESOURCE_FLAG=resource_flag,C
BANDWIDTH=bandwidth,I
AV_GSID=av_gsid,C
CODEC=codec,C

[PartiesTags]
DIALLED_NUMBER=dialed_number,C
CALLING_NUMBER=calling_number,C

```

```
[SipEntitiesTags]
TERM_SIP_ENTITY=terminating,C
ORIG_SIP_ENTITY=originating,C
```

```
[UsageTags]
VOICE=voice,C
VIDEO=video,C
FAX=fax,C
TEXT=text,C
OTHER=other,C
```

```
[TenantIdsTags]
CALLING_TENANT=calling,C
CALLED_TENANT=called,C
```

```
[IpAddressesTags]
CALLING_PARTY_IP=calling,C
CALLED_PARTY_IP=called,C
```

©2017 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.