



## Avaya Solution & Interoperability Test Lab

---

# Application Notes for Tri-Line's TIM Enterprise 3.0.0.125 with Avaya Aura® Communication Manager 8.1 - Issue 1.0

### Abstract

These Application Notes describe the configuration steps required for Tri-Line's TIM Enterprise 3.0.0.125 to interoperate with Avaya Aura® Communication Manager 8.1.

TIM Enterprise is an enterprise-class call logging software that interoperates with Avaya Aura® Communication Manager over TCP/IP for the collection of Call Details Records (CDRs). TIM Enterprise listens, collects, and processes the call records generated for various types of calls.

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

The objective of this compliance test is to verify that Tri-Line's TIM Enterprise 3.0.0.125 enterprise-class call logging software can interoperate with Avaya Aura® Communication Manager 8.1. TIM Enterprise interoperates with Avaya Aura® Communication Manager over TCP/IP for the collection of Call Detail Records (CDR). During compliance testing, the CDR collection was verified with Avaya Communication Manager running in a VMware Environment.

## 2. General Test Approach and Test Results

The general test approach was to manually place intra-switch calls, inter-switch calls, inbound and outbound PSTN trunk calls to and from telephones that utilize Avaya Media Servers/Gateways, and verify that TIM Enterprise collects the CDR records and properly classifies and reports the attributes of the call. For serviceability testing, logical links were disabled/re-enabled, and media servers were rebooted.

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.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Avaya systems and the TIM Enterprise did not include use of any specific encryption features as requested by Tri-Line.

## 2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. The feature testing evaluated the ability of Tri-Line's TIM Enterprise to collect and process CDR records for various types of calls: intra-switch calls (calls between phones on the same site), outbound/inbound calls to/from the PSTN and outbound/inbound calls to/from the phones between the two sites via the IP trunk. The serviceability testing introduced failure scenarios to see if TIM Enterprise can resume CDR collection after failure recovery.

## 2.2. Test Results

All test cases passed successfully.

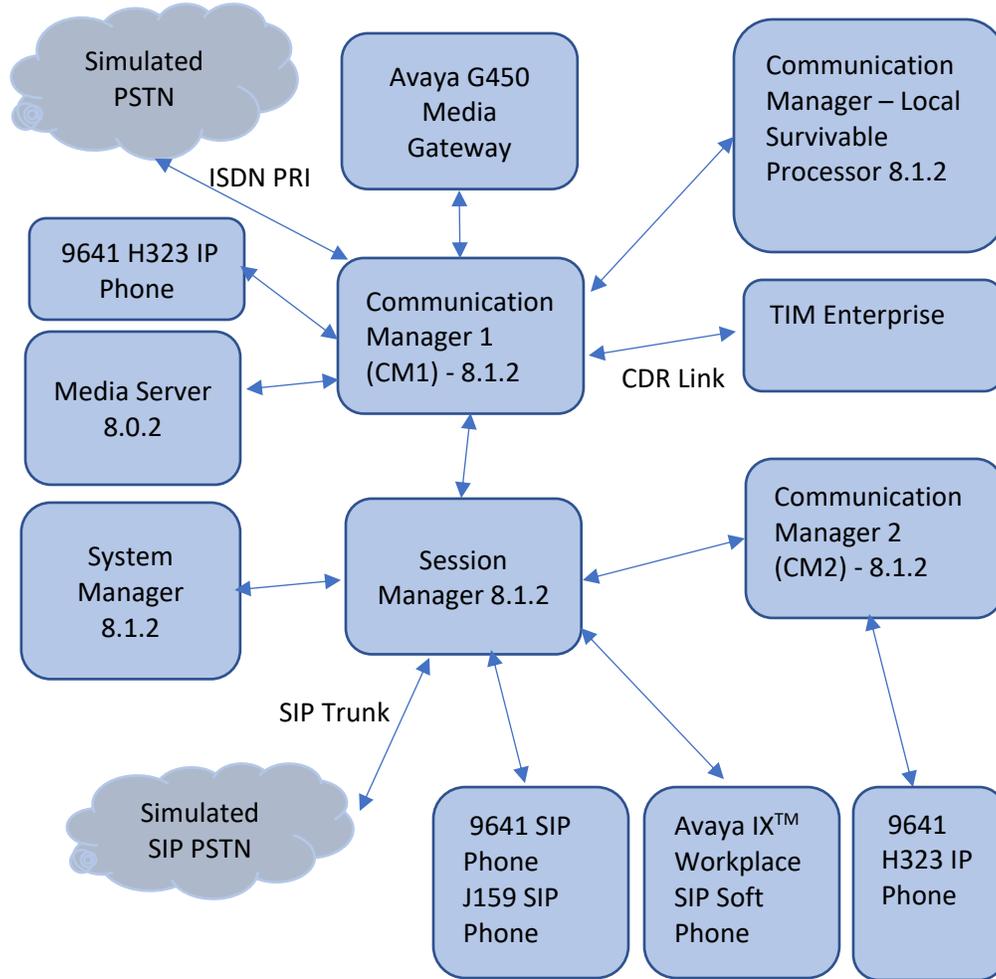
## 2.3. Support

Technical support from Tri-Line can be obtained through the following:

Phone: +44 20 7265 2626  
E-mail: [support@tri-line.com](mailto:support@tri-line.com).  
Web: <http://www.tri-line.com/>  
Address: 9-10 Telfords Yard  
The Highway  
LONDON  
E1W 2BS  
England

### 3. Reference Configuration

**Figure 1** illustrates a sample configuration that was used to compliance test the interoperability of Tri-Line’s TIM Enterprise and Avaya Communication Manager. TIM Enterprise was installed on Windows and it was connected to Communication Manager for collecting CDR records.



**Figure 1: Compliance Testing Configuration**

## 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 in Virtual Environment	8.1.2
Avaya Aura® Session Manager in Virtual Environment	8.1.2
Avaya Aura® Communication Manager in Virtual Environment	8.1.2
Avaya G450 Media Gateway	41.16.30
Avaya Aura® Media Server in Virtual Environment	8.0 SP2
Avaya 9608G & 9641G IP Deskphone (H.323)	6.8
Avaya IX Workplace	3.8.4.10.2
Avaya 9641 & 9621 IP Deskphone (SIP)	7.1.9
Tri-Line TIM Enterprise <ul style="list-style-type: none"><li>• Windows 2012 Server</li><li>• Chrome</li></ul>	3.0.0.125

## 5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Call Data Record (CDR) features in Avaya Communication Manager. All the configuration changes in Avaya Communication Manager are performed through the System Access Terminal (SAT). Avaya Communication Manager was configured to generate CDR records to the IP address of the TIM Enterprise server over TCP/IP. The CDR link originates at the IP address of the **procr** interface that connects to the same network where the TIM Enterprise server is located.

Use the **change node-names ip** by specifying the **Name** and the command to add a new node **Name** for the TIM Enterprise server and **IP Address** of the server.

change node-names ip		IP NODE NAMES		Page	1 of	1
Name	IP Address	Name	IP Address			
<b>TIMEnterprise</b>	<b>10. 103 .3.245</b>			.	.	.
default	0 .0 .0 .0			.	.	.
procr	10. 30 .5 .93			.	.	.

Use the **change ip-services** command to define the CDR link over TCP/IP. To define a primary CDR link, the following information should be provided:

- **Service Type: CDR1**
- **Local Node: procr**
- **Local Port: 0** [The Local Port is fixed to 0.]
- **Remote Node: TIMEnterprise** [The Remote Node is set to the node name that was created in the previous step for the TIM Enterprise server.]
- **Remote Port: 9000** [The Remote Port may be set to a value between 5000 and 64500 inclusive and must match the port configured in the TIM Enterprise server.]

**Note:** A different port number must be specified for each Communication Manager Server.

change ip-services						Page	1 of	3
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port			
CDR1		<b>procr</b>	<b>0</b>	<b>TIMEnterprise</b>	<b>9000</b>			

On **Page 3** of the ip-services form, disable the Reliable Session Protocol (RSP) for the CDR link by setting the **Reliable Protocol** field to **n**.

change ip-services							Page	3 of	3
Service Type	Reliable Protocol	Packet Timer	Resp	Session Connect Message Cntr	SPDU Cntr	Connectivity Timer			
CDR1	<b>n</b>	30		3	3	60			

Enter the **change system-parameters cdr** command from the SAT to set the parameters for the type of calls to track and the format of the CDR data. The example below shows the settings used during the compliance test. Provide the following information:

- **CDR Data Format: day/month**
- **Primary Out Format: customized**
- **Primary Output Endpoint: CDR1**

The remaining parameters define the type of calls that will be recorded and what data will be included in the record. See reference [2] for a full explanation of each field. The test configuration used some of the more common fields described below.

- **Use Legacy CDR Formats: y** [Allows CDR formats to use 5.x CDR formats. If the field is set to y, then CDR formats utilize the 3.x CDR formats.]
- **Intra-switch CDR: y** [Allows call records for internal calls involving specific stations. Those stations must be specified in the **inter-switch-cdr** form.]
- **Record Outgoing Calls Only: n** [Allows incoming trunk calls to appear in the CDR records along with the outgoing trunk calls.]
- **Outg Trk Call Splitting: y** [Allows a separate call record for any portion of an outgoing call that is transferred or conferenced.]
- **Inc Trk Call Splitting: y** [Allows a separate call record for any portion of an incoming call that is transferred or conferenced.]

```

change system-parameters cdr                                     Page 1 of 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? n
  Use Enhanced Formats? n              Condition Code 'T' For Redirected Calls? n
  Use Legacy CDR Formats? y            Remove # From Called Number? n
Modified Circuit ID Display? y          Intra-switch CDR? y
  Record Outgoing Calls Only? n        Outg Trk Call Splitting? y
  Suppress CDR for Ineffective Call Attempts? y    Outg Attd Call Record? 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: group-ext
Record Called Vector Directory Number Instead of Group or Member? n

  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
Remove '+' from SIP Numbers? y

```

On the **Page 2** of the CDR SYSTEM PARAMETERS form, define the customized CDR format as shown below.

change system-parameters cdr			Page 2 of 2		
CDR SYSTEM PARAMETERS					
Data Item - Length		Data Item - Length		Data Item - Length	
1: date	- 6	17: dialed-num	- 8	33: auth-code	- 13
2: space	- 1	18: space	- 1	34: return	- 1
3: time	- 4	19: in-trk-code	- 4	35: line-feed	- 1
4: space	- 1	20: space	- 1	36:	-
5: sec-dur	- 5	21: in-crt-id	- 3	37:	-
6: space	- 1	22: space	- 1	38:	-
7: cond-code	- 1	23: calling-num	- 5	39:	-
8: space	- 1	24: space	- 1	40:	-
9: attd-console	- 2	25: vdn	- 5	41:	-
10: space	- 1	26: space	- 1	42:	-
11: code-used	- 4	27: bcc	- 1	43:	-
12: space	- 1	28: space	- 1	44:	-
13: out-crt-id	- 3	29: ppm	- 5	45:	-
14: space	- 1	30: space	- 1	46:	-
			1		
15: code-dial	- 4	31: acct-code	- 5	47:	-
16: space	- 1	32: space	- 1	48:	-
Record length = 126					

If the Intra-switch CDR field is set to **y** in the CDR SYSTEM PARAMETERS form, use the **change intra-switch-cdr** command to define the extensions that will be subject to call detail records. In the **intra-switch-cdr** form, enter a specific extensions tracked with a CDR record. Add an entry for each additional **Extension** of interest.

change intra-switch-cdr			Page 1 of 3		
INTRA-SWITCH CDR					
Extension	Extension	Assigned Members:	4	of 5000	administered
		Extension	Extension	Extension	Extension
70000					
70009					
70010					
71000					
71001					
71002					

For each trunk group for which CDR records are desired, verify that CDR reporting is configured to generate the ring interval CDR records. Use the **change trunk-group n** command, where **n** is the trunk group number, to verify that the **CDR Reports** field is set to **r**. This applies to all types of trunk groups.

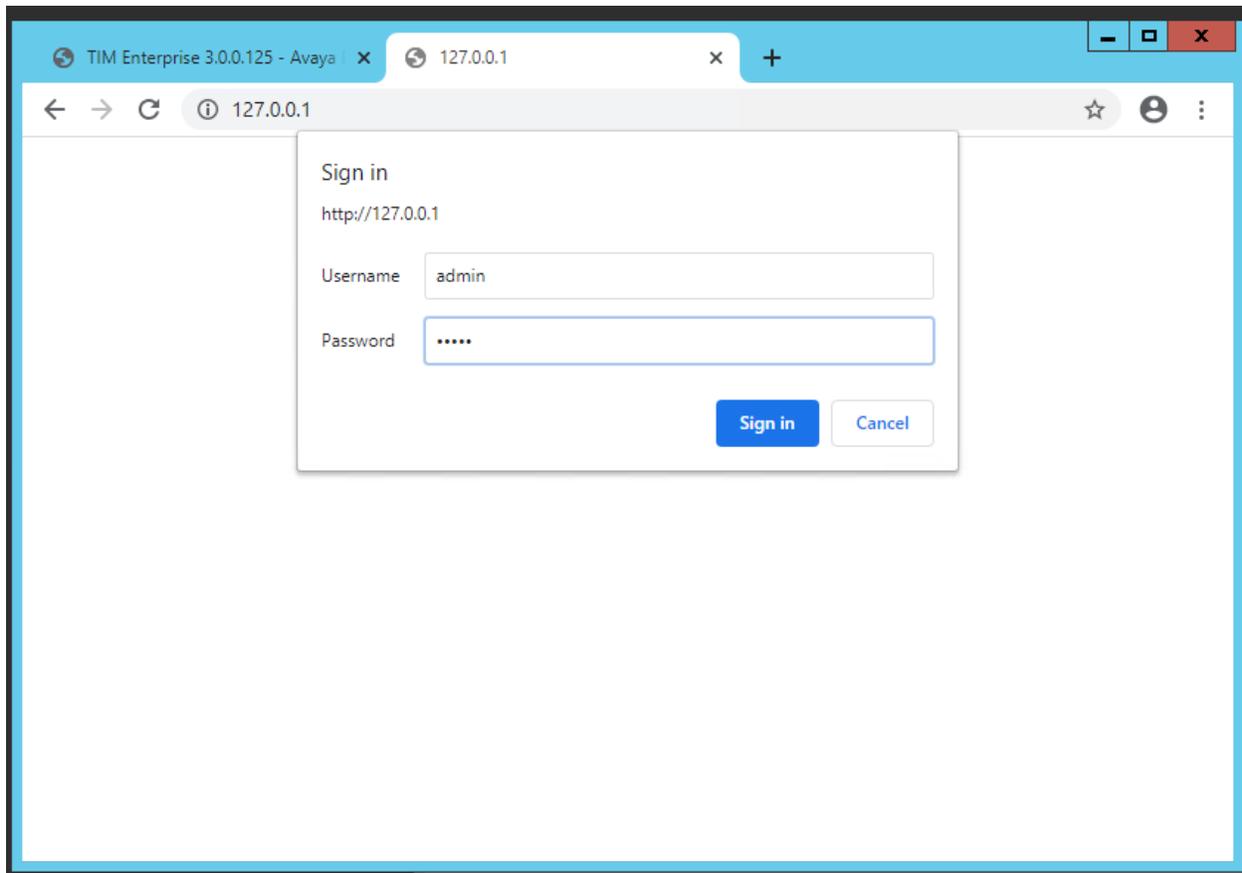
```
change trunk-group 3                                     Page 1 of 21
                                                         TRUNK GROUP
Group Number:3                                         Group Type: isdn      CDR Reports: r
  Group Name: DevC-PSTN                                COR: 1                TN: 1      TAC: #03
  Direction: two-way                                  Outgoing Display? y   Carrier Medium: PRI/BRI
  Dial Access? y                                     Busy Threshold: 255   Night Service:
Queue Length: 0
Service Type: tie                                     Auth Code? n          TestCall ITC: rest
TestCall BCC: 4                                     Far End Test Line No:
```

## 6. Configure the TIM Enterprise server

This section provides the procedures for configuring the TIM Enterprise server to receive Call Data Records (CDRs) for various call types output by the Avaya Communication Manager.

To access TIM Enterprise, open a web browser and enter the IP address of the TIM Enterprise server e.g. <http://x.x.x.x/> where x.x.x.x is the IP address of the machine running TIM Enterprise.

Enter a valid username and password in the web browser's authentication window that appears, and select **Sign in**.



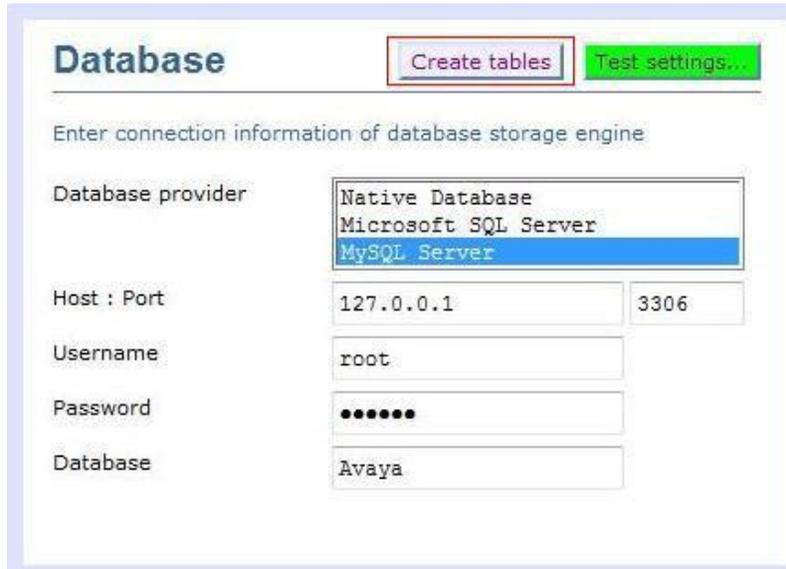
After successful login, the default **System settings** screen is displayed. This is the main screen that will be used to configure the TIM Enterprise system.

The screenshot shows the 'System settings' interface. It is divided into four main sections: Database, Alerts, Email, and Web server. The Database section is the primary focus, containing a dropdown for 'Database provider' with 'MySQL Server' selected, and input fields for 'Host : Port' (127.0.0.1 and 3306), 'Username' (root), 'Password' (masked with dots), and 'Database' (Avaya). There are 'Create tables' and 'Test settings...' buttons. The Alerts section has input fields for 'Critical', 'Warning', and 'Information' alerts. The Email and Web server sections also have 'Test settings...' buttons.

To configure the Database settings, select the **Database provider** that will be used to store the call data on the TIM Enterprise server. In this case **MySQL Server** was specified. Type in the **Host** and **Port** number of the SQL server and enter the **Username** and **Password** for the SQL server connection. Type the name of the **Database** to connect to and click on the **Test settings** button to verify that the database details entered are valid.

This is a close-up view of the Database configuration section. It features a dropdown menu for 'Database provider' with 'MySQL Server' highlighted. Below it are input fields for 'Host : Port' (127.0.0.1 and 3306), 'Username' (root), 'Password' (masked with dots), and 'Database' (Avaya). At the top right of this section are 'Create tables' and 'Test settings...' buttons.

If the **Test settings** button comes back green the settings were correct. Prepare the database tables and indices by clicking the **Create tables** button.



**Database** Create tables Test settings...

Enter connection information of database storage engine

Database provider: Native Database, Microsoft SQL Server, **MySQL Server**

Host : Port: 127.0.0.1 3306

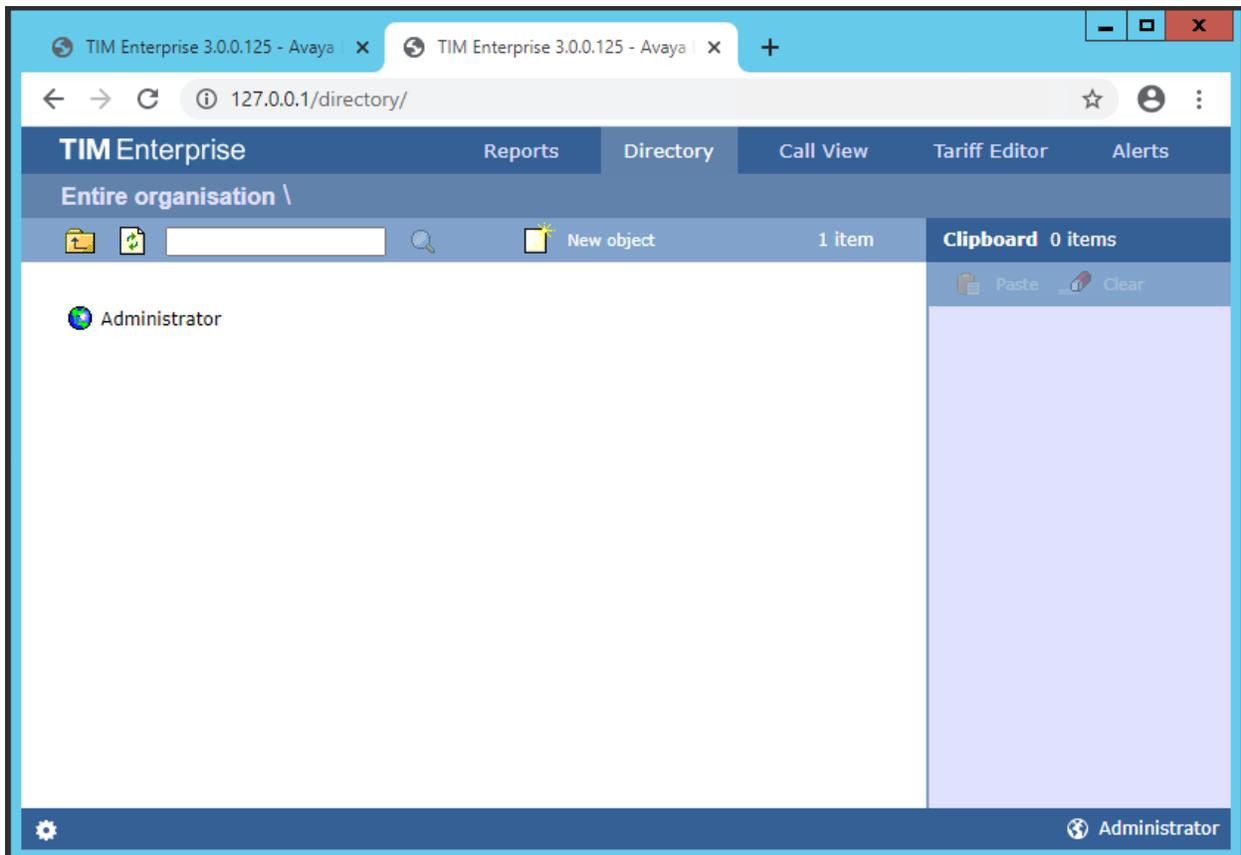
Username: root

Password: .....

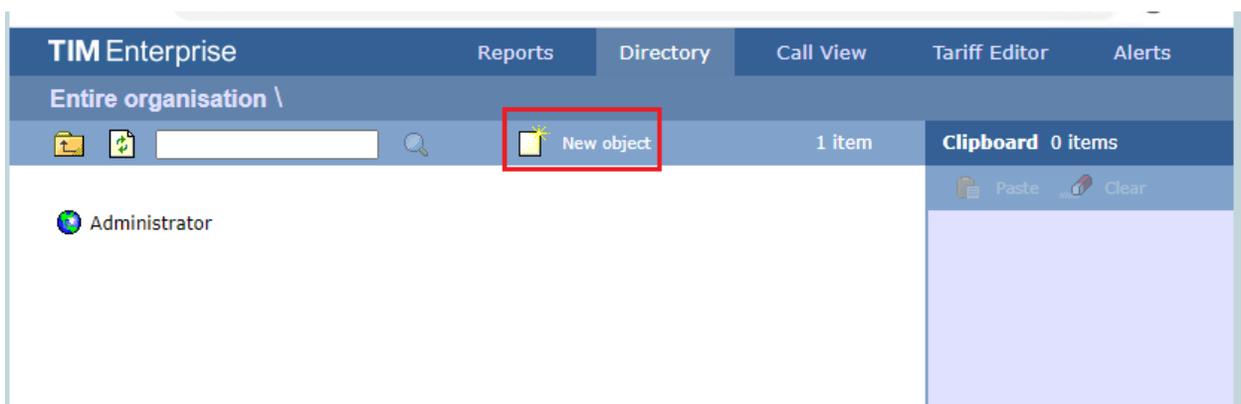
Database: Avaya

When the tables are created successfully, the alert will be displayed. Click **OK**. (Not shown)  
This completes the configuration of the Database settings on TIM Enterprise. The next task is to configure the Directory settings.

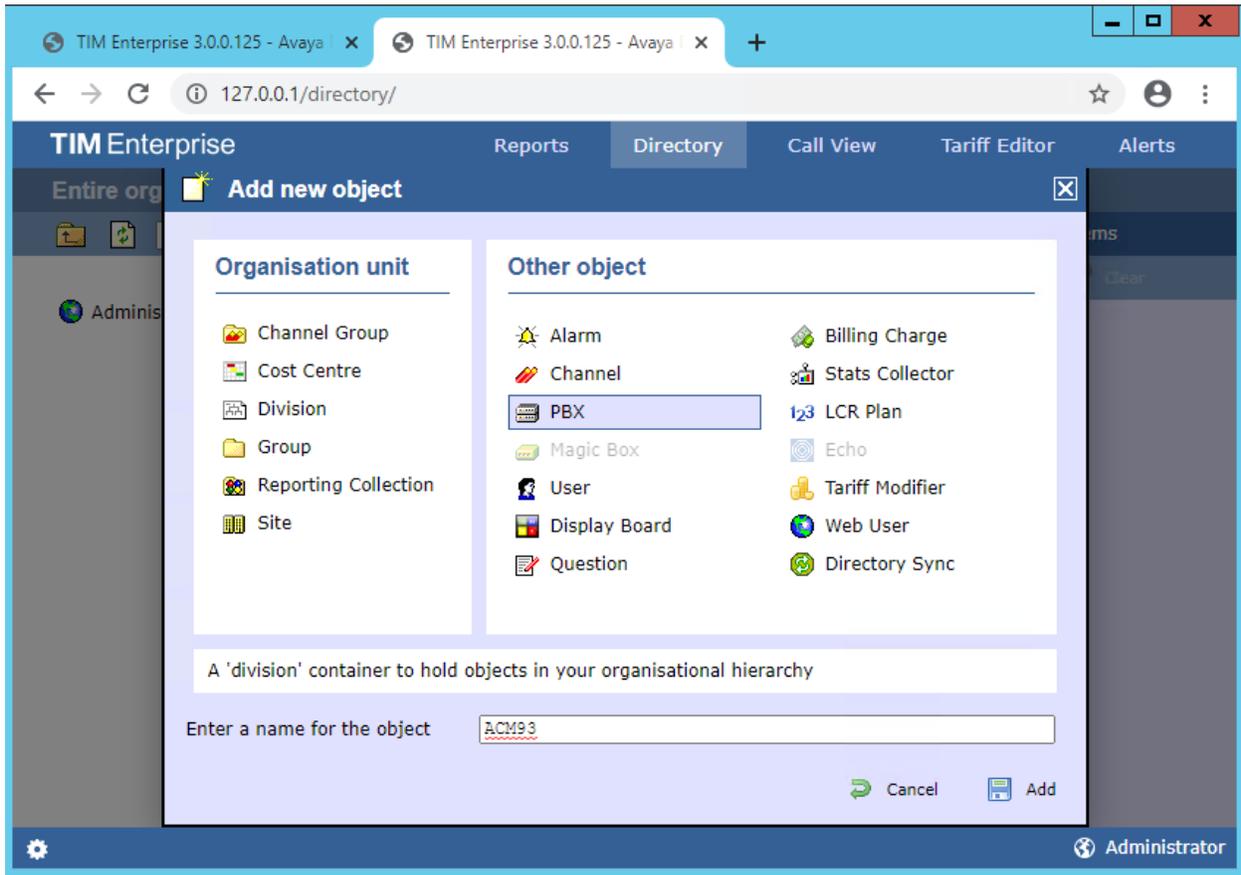
To configure the Directory settings, click on the **Directory** tab in the TIM Enterprise toolbar.



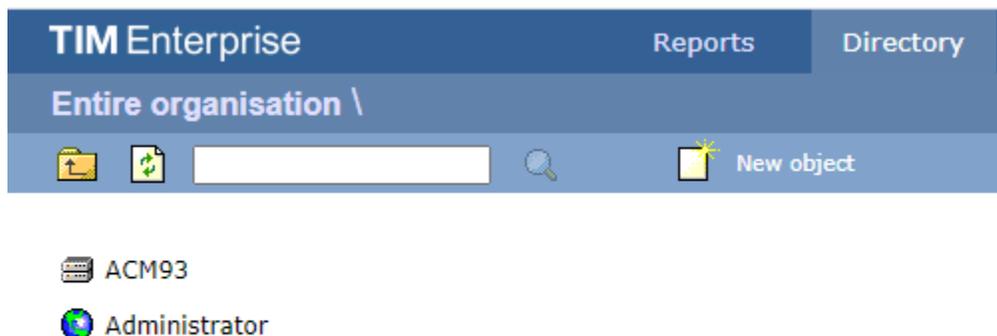
On the Directory screen that is displayed, click on **New Object**.



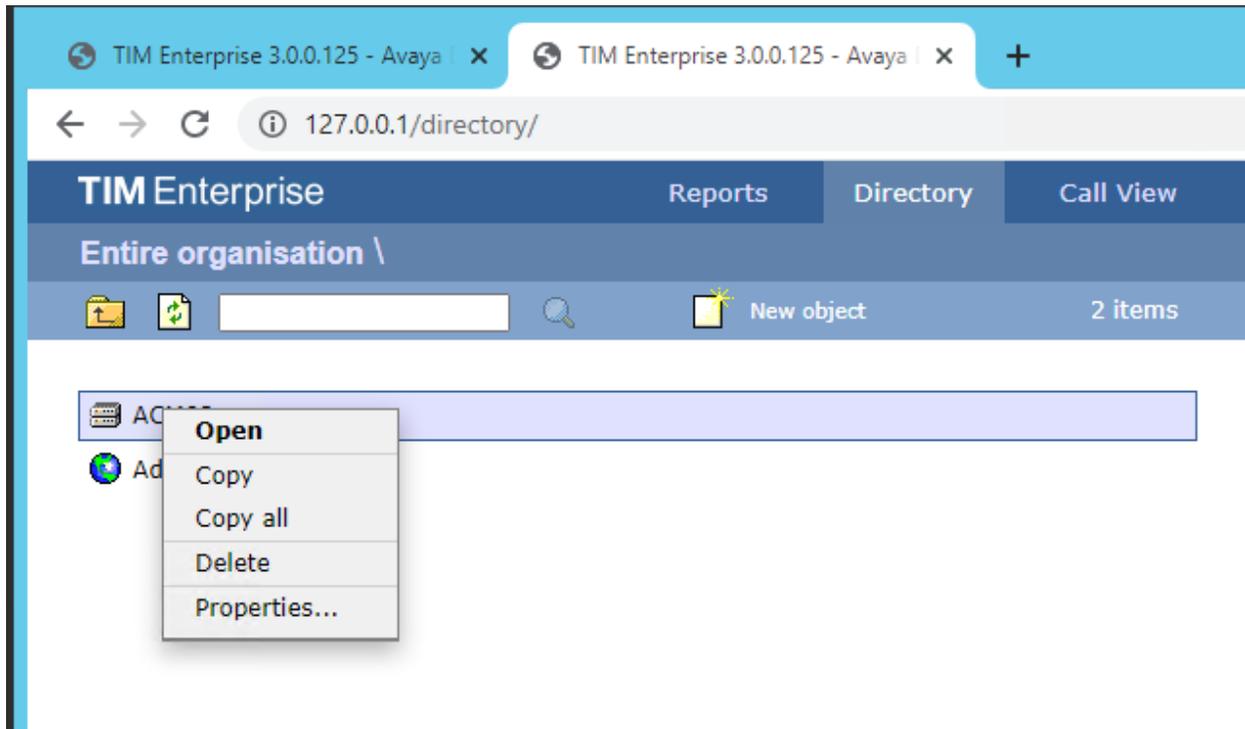
On the **Add new object** window that appears, select **PBX**. In the field, **Enter a name for the object**, enter **ACM93** and click the **Add** button as shown below.



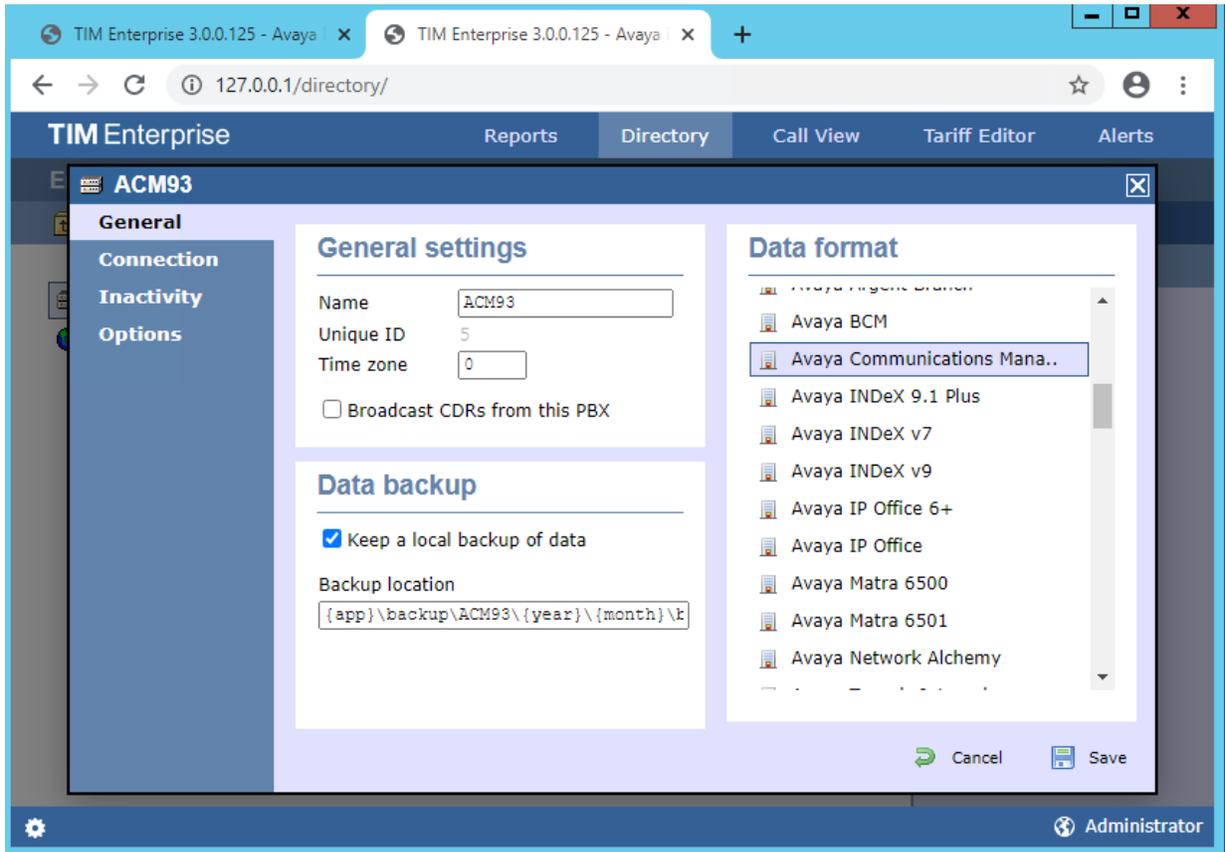
The **ACM93** will appear in the Directory as shown below.



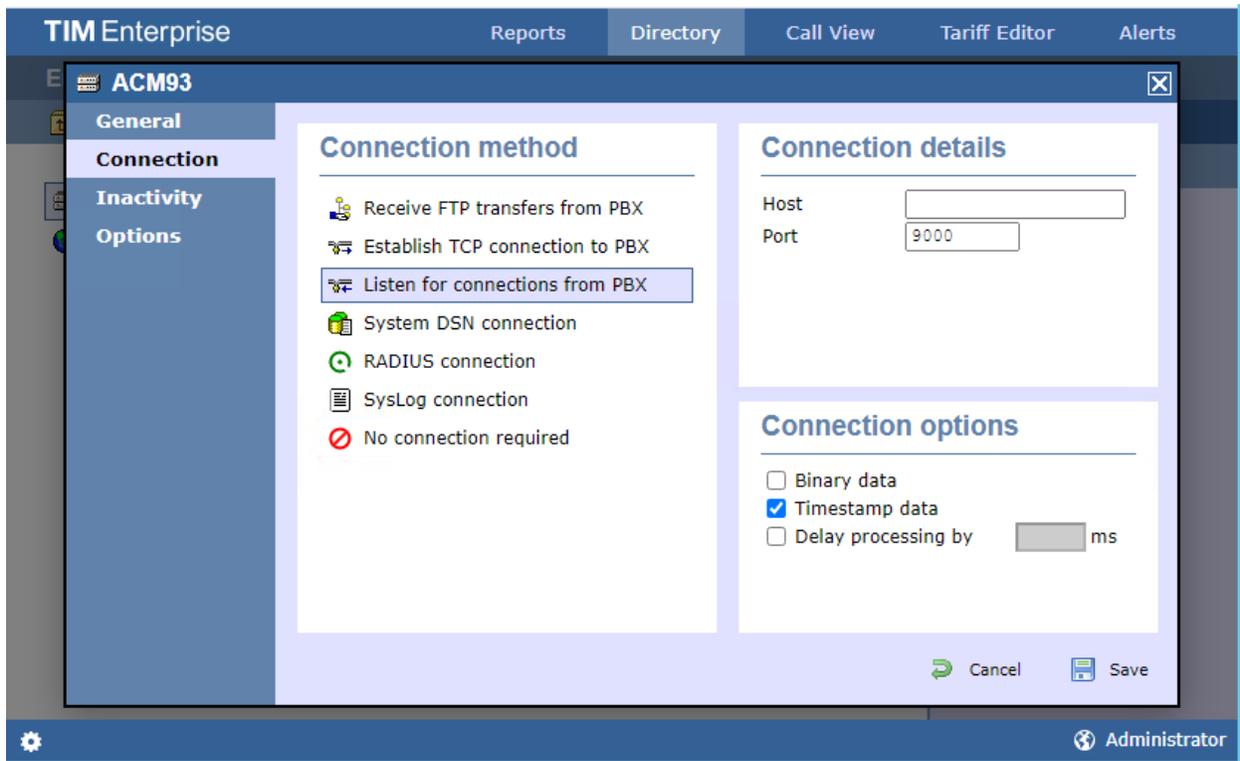
To configure TIM Enterprise to receive information from Avaya Communication Manager, click on the **ACM93** object and select **Properties** as shown below.



A new **ACM93** window will appear with default **General** tab displayed. Under the **Data format** section of the **General** tab, select **Avaya Communications Manager**.



Click on the **Connection** tab on the left hand side. In the screen that appears select **Listen for connections from PBX** and enter the **Port** number as configured for the CDR link in **Section 5**. Check the **Timestamp data** check-box and click **Save**.



Repeat the above steps to add a new directory for the second Avaya Communication Manager.

## 7. Verification Steps

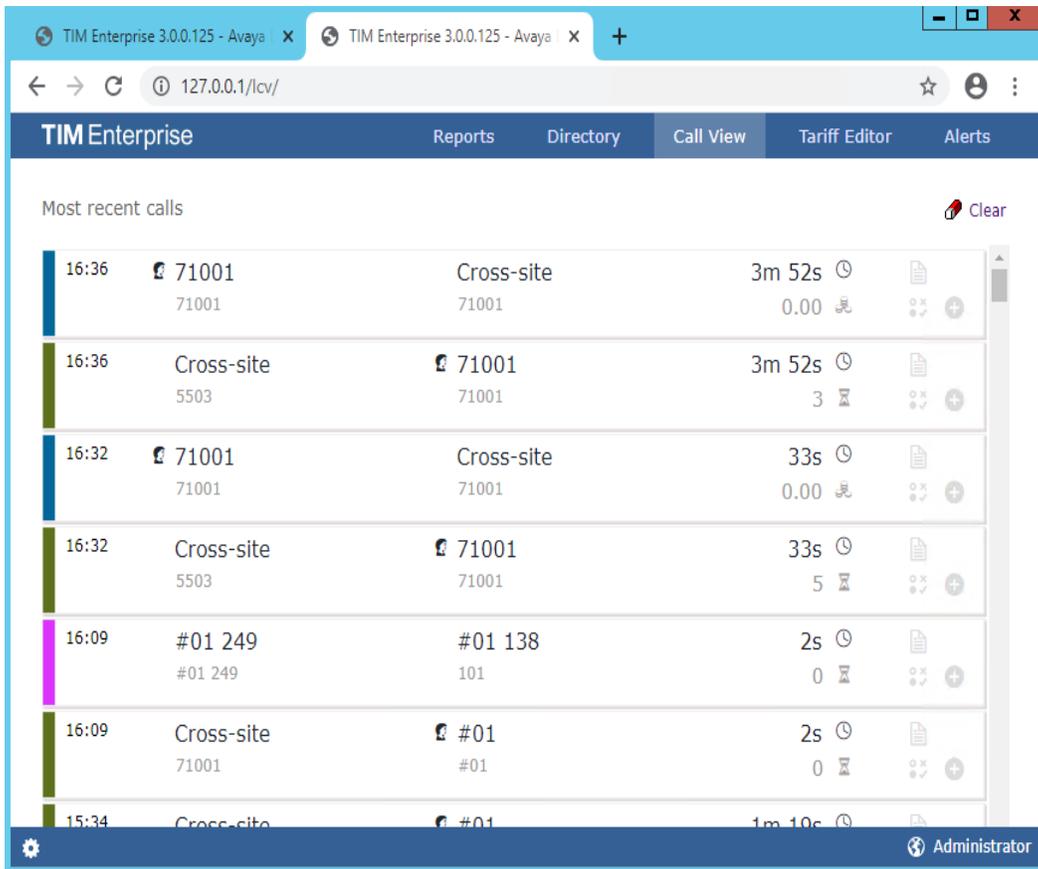
The following steps may be used to verify the configuration:

- Use the **ping** utility on the TIM Enterprise server to verify the IP connectivity to the Avaya Communication Manager Servers.
- Using the **status cdr-link** command verify that the Primary CDR **Link State** shows **up**.

```

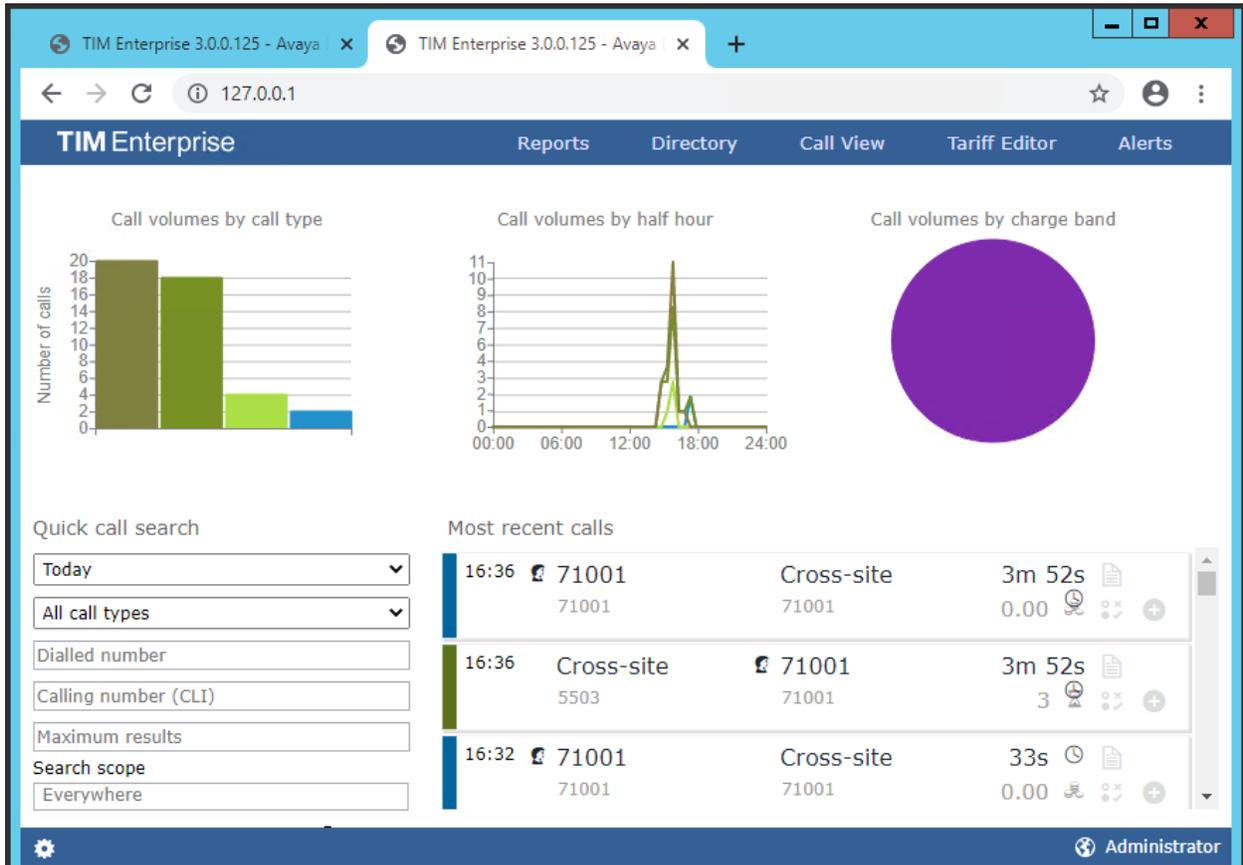
status cdr-link
                                CDR LINK STATUS
                                Primary                Secondary
                                Link State: up          down
                                Date & Time: 2020/07/14 18:10:14    0000/00 /00 00: 00: 00
                                Forward Seq. No: 254                0
                                Backward Seq. No: 325                0
                                CDR Buffer % Full: 0.00              0.00
                                Reason Code: OK
  
```

- Place a call and verify that TIM Enterprise receives the raw CDR record for the call. Compare the values of data fields in the raw CDR record with TIM Enterprise’s Call View by selecting the **Call View** tab on the TIM Enterprise toolbar (not shown).





Place internal, inbound trunk and outbound trunk calls to and from various telephones, view TIM Enterprise and verify the report's accuracy.



## 8. Conclusion

These Application Notes describe the procedures for configuring Tri-Line's TIM Enterprise to collect call detail records from Avaya Communication Manager. TIM Enterprise successfully passed all compliance testing.

## 9. Additional References

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

[1] *Feature Description and Implementation For Avaya Communication Manager*, Release 8.1.

[2] *Administrator Guide for Avaya Communication Manager*, Release 8.1.

---

**©2020 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](mailto:devconnect@avaya.com).