



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager with Unison Galactrix 3.1.1 - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Avaya Aura® Communication Manager with Unison Galactrix 3.1.1.

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 configuration steps to integrate Avaya Aura® Communication Manager with UNISON Galactrix. The UNISON Galactrix application collects Call Detailed Records that are output from the Avaya Aura® Communication Manager which are stored on an IP buffer. These records are downloaded to the UNISON Galactrix application at defined intervals. UNISON Galactrix is a fully integrated communication platform with various voice, fax and billing applications that operate from a central directory. During compliance testing only the collection of Call Detailed Records was tested.

2. General Test Approach and Test Results

The general test approach was to configure the UNISON Galactrix (Galactrix) to communicate with the Avaya Aura® Communication Manager (Communication Manager) as implemented on a customer's premises. Testing focused on verifying that Call Detailed Records (CDR) are collected by the IP buffer and received in the format as generated by the Communication Manager. The Galactrix application would collect the CDR data using File transfer Protocol from the IP buffer. Various call scenarios were performed to simulate real call types as would be observed on a customer premises. See **Figure 1** for a network diagram. The interoperability compliance test included both feature functionality and serviceability tests.

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 testing included:

- Verification of connectivity between Galactrix/IP buffer and Communication Manager using a TCP connection.
- Verification that CDR data was collected as output by the Communication Manager.
- Link Failure\Recovery was also tested to ensure successful reconnection after link failure.
- CDR data collected included:
 - Internal/External phone numbers.
 - Authorization codes.
 - Charge codes.
 - Transfer/Conference details.
- Calls were completed using Avaya H323 and SIP Deskphones.

2.2. Test Results

Tests were performed to insure full interoperability between the Galactrix and Communication Manager. The tests were all functional in nature and performance testing was not included. All the test cases passed successfully.

2.3. Support

Technical support for UNISON Galactrix can be found as follows:

- Web: www.unison.co.za
- Email: unicare@unison.co.za
- Phone: +27117973000

3. Reference Configuration

Figure 1 illustrates the network topology used during compliance testing. The Avaya solution consists of a Communication Manager, System Manager, Session Manager and a G650 Gateway. The Communication Manager is configured to output Call Detail Records data over a TCP/IP port. A Node is configured on the Communication Manager to point to the Scannex IP buffer. The Call Detail Records are sent in customized format and are stored on the buffer and are retrieved by the GALACTRIX application at defined periods. A variety of Avaya 96XX H.323 and SIP Deskphones were used to generate calls. Inbound and outbound calls to the PSTN were made via a G650 Media Gateway.

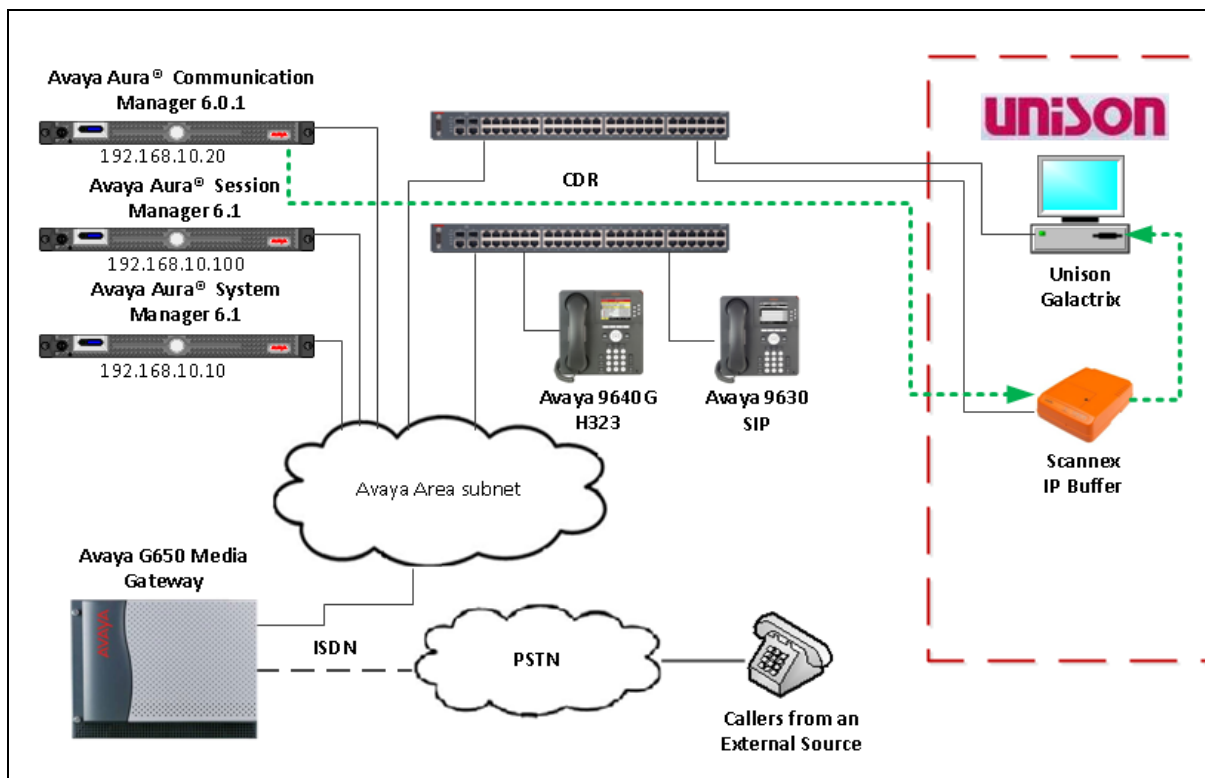


Figure 1: Avaya Aura® Communication Manager and UNISON Galactrix Reference Configuration

4. Equipment and Software Validated

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

Avaya Equipment	Software / Firmware Version
Avaya S8800 Server	Avaya Aura® Communication Manager R6.01 Build 001.1.510 SP3
Avaya S8800 Server	Avaya Aura® System Manager R6.1 Build 6.1.0.0.7345
Avaya S8800 Server	Avaya Aura® Session Manager R6.1 SP3
Avaya G650 Media Gateway <ul style="list-style-type: none">• IP Server INTFC• Control-Lan• IP Media Processor• DS1	TN2312BP HW15 FW050 TN799DP HW01 FW038 TN2602AP HW02 FW054 TN2464BP HW05 FW024
Avaya 96XX Telephones <ul style="list-style-type: none">• 9630 (H323)• 9630 (SIP)• 9640G (H323)	S3.186a S2.6.3 S2.050
UNISON Equipment	Software / Firmware Version
IBM System x3250 M2 server running Windows 2003 Server R2	UNISON Galactrix Version 3.1.1
Scannex IP Buffer	Version IPBCF2.75.199 2012-02-09 / i5.0.10

5. Avaya Aura® Communication Manager Configuration

Configuration and verification operations on the Communication Manager illustrated in this section were all performed using Avaya Site Administrator Emulation Mode. The information provided in this section describes the configuration of the Communication Manager for this solution. It is implied a working system is already in place. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**. The configuration operations described in this section can be summarized as follows:

- Create Node Name for IP buffer
- Define the CDR Link
- Change system-parameters cdr

5.1. Create Node Name for IP Buffer

A Node Name needs to be created to associate the IP buffer with the Communication Manager. Use the **change node-names ip** command to configure the following:

Page 1

- **Name** Enter an informative name i.e. **IP buffer**
- **IP address** Enter the IP address of the **IP buffer**

Press **f3** button to save the new settings.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
IP buffer	192.168.10.82	

5.2. Define the CDR Link

A CDR link needs to be defined between the Communication Manager and the IP buffer. Use the **change ip-services** command to configure the following:

- **Service Type** Enter **CDR1**
- **Local Node** Enter **procr**
- **Remote Node** Enter **Unison**
- **Remote Port** Enter **9000**

change ip-services					Page 1 of 3
IP SERVICES					
Service	Enabled	Local	Local	Remote	Remote
Type		Node	Port	Node	Port
CDR1		Procr	0	Unison	9000

Navigate to **Page 3** and set the **Reliable Protocol** field to **n**. This will disable Reliable Session Protocol (RSP) for CDR transmission. In this case, the CDR link will use TCP without RSP.

- **Reliable Protocol** Enter **n**

Press **F3** button to save the new settings.

change ip-services					Page	3 of 3
SESSION LAYER TIMERS						
Service	Reliable	Packet Resp	Session Connect	SPDU	Connectivity	
Type	Protocol	Timer	Message Cntr	Cntr	Timer	
CDR1	n	30	3	3	60	

5.3. Change system-parameters cdr

Certain parameters changes are required for Communication Manager to interoperate with Galactrix. The screen shots below show the settings used during compliance testing. Use the **change system-parameters cdr** command to configure the following:

- **CDR Date Format** Enter **day/month**
- **Primary Output Format** Enter **customized**
- **Primary Output Endpoint** Enter **CDR1**
- **Record Outgoing Calls Only** Enter **n**
- **Intra-Switch CDR** Enter **y**
- **Outg Trk Call Splitting** Enter **y**
- **Inc Trk Call Splitting** Enter **y**

change system-parameters cdr		Page 1 of 2
CDR SYSTEM PARAMETERS		
Node Number (Local PBX ID):		CDR Date Format: month/day
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? 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? y	Outg Attd Call Record? n	
Disconnect Information in Place of FRL? n	Interworking Feat-flag? n	
Force Entry of Acct Code for Calls Marked on Toll Analysis Form? y		
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? n	
Record Non-Call-Assoc TSC? n	Call Record Handling Option: warning	
Record Call-Assoc TSC? n	Digits to Record for Outgoing Calls: outpulsed	
Privacy - Digits to Hide: 0	CDR Account Code Length: 6	

Navigate to **Page 2** and enter the following information.

- Enter **Data Item** and **Length** as shown in the screen below

Press **F3** button to save the new settings.

change system-parameters cdr			Page 2 of 2		
CDR SYSTEM PARAMETERS					
Data Item - Length		Data Item - Length		Data Item - Length	
1: space	- 1	17: code-dial	- 4	33: clg-num/in-tac	- 15
2: date	- 6	18: space	- 1	34: space	- 1
3: time	- 4	19: cond-code	- 1	35: attd-console	- 2
4: space	- 1	20: space	- 1	36: space	- 1
5: in-trk-code	- 4	21: feat-flag	- 1	37: code-used	- 4
6: space	- 1	22: space	- 1	38: space	- 1
7: calling-num	- 15	23: ppm	- 5	39: vdn	- 13
8: space	- 1	24: space	- 1	40: return	- 1
9: acct-code	- 15	25: out-crt-id	- 3	41: line-feed	- 1
10: space	- 1	26: space	- 1	42:	-
11: auth-code	- 7	27: in-crt-id	- 3	43:	-
12: space	- 1	28: space	- 1	44:	-
13: dialed-num	- 18	29: location-from	- 3	45:	-
14: space	- 1	30: space	- 1	46:	-
15: sec-dur	- 5	31: location-to	- 3	47:	-
16: space	- 1	32: space	- 1	48:	-
Record length = 152					

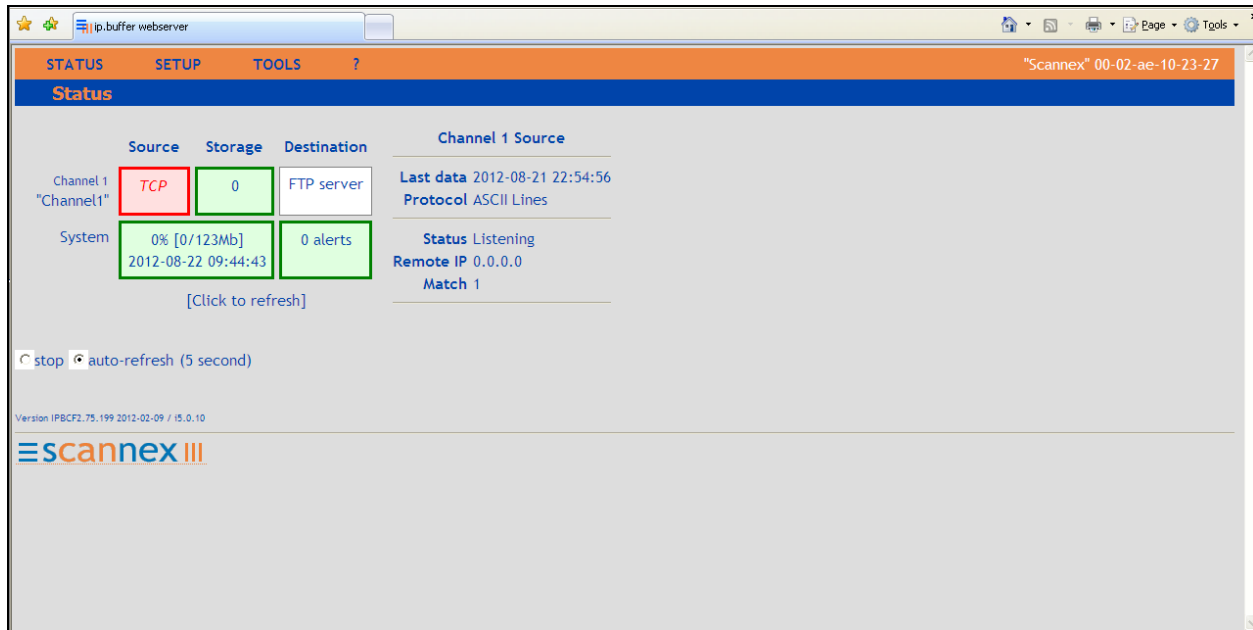
6. Configuration of Scannex IP Buffer

This section provides the procedures to configure the Scannex IP buffer. It is implied that the Scannex IP buffer is already in place and configured with an IP address on the same subnet as the Communication Manager. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**. The configuration operations described in this section can be summarized as follows:

- Logging into the Scannex IP Buffer
- Configure Channel 1
 - Select Source
 - Enter TCP/IP port
 - Select Destination

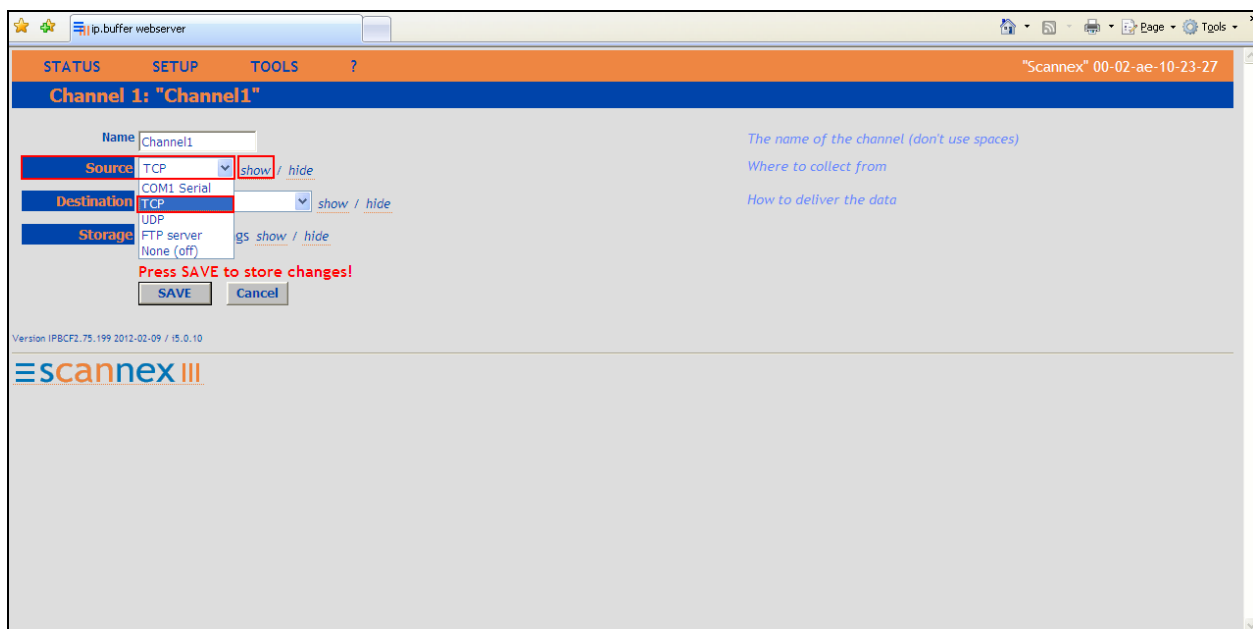
6.1. Logging into the Scannex IP Buffer

To access the web-based interface of the Scannex IP Buffer use the URL **http://192.168.10.82**. The **Management Main** page is displayed.



6.2. Configure Channel 1

Select **STATUS** followed by **Channel 1** (Not shown). Once the **Channel 1** page is opened select **TCP** from the **Source** dropdown box, then select **show**.



Once the next page opens enter **9000** in the **TCP/IP port** box. Use the scroll bar on the right side of the page and scroll to the bottom.

The screenshot shows the 'Channel 1: "Channel1"' configuration page. The 'TCP/IP' section is active, showing 'Connect' set to 'Device to ipbuffer (passive/server)', 'Address' set to 'multihome', and 'Port' set to '9000'. The 'Protocol' is set to 'ASCII Lines'. The 'Match & Send' section shows four rows for matching and sending data. A red box highlights the 'Port' field, and a red arrow points to the scroll bar on the right.

At the FTP section select **FTP server** from the **Destination** dropdown box, then select **show**.

The screenshot shows the 'Pass-through' and 'Notification' sections. The 'Destination' dropdown is set to 'FTP server'. The 'Storage' dropdown is set to 'FTP server'. The 'show' button is highlighted. A red box highlights the 'Destination' dropdown, and a red arrow points to the 'show' button.

Once the **FTP server** page opens enter **Username**, **Password**, and **Filename**. During compliance testing the default values were used.

Username – Channel1

Password – Password

Filename - Channel1.dat

Click on the **Save** button to store the changes.

The screenshot shows a web browser window titled 'ip.buffer webserver'. The 'Destination' dropdown is set to 'FTP server'. The 'FTP server' section contains the following fields: 'Username' (Channel1), 'Password' (password), and 'Filename' (channel1.dat), which are highlighted with a red box. Below these are 'Compression' (none), 'Limit' (0 kb), and 'Autodelete' (No). The 'Data Markers' section has 'Prefix' and 'Suffix' fields. The 'Data Security' section has 'Data Encryption' set to 'Unencrypted'. At the bottom, there is a 'Storage' section with 'Storage settings' and a red 'Press SAVE to store changes!' message above 'SAVE' and 'Cancel' buttons. The 'SAVE' button is highlighted with a red box.

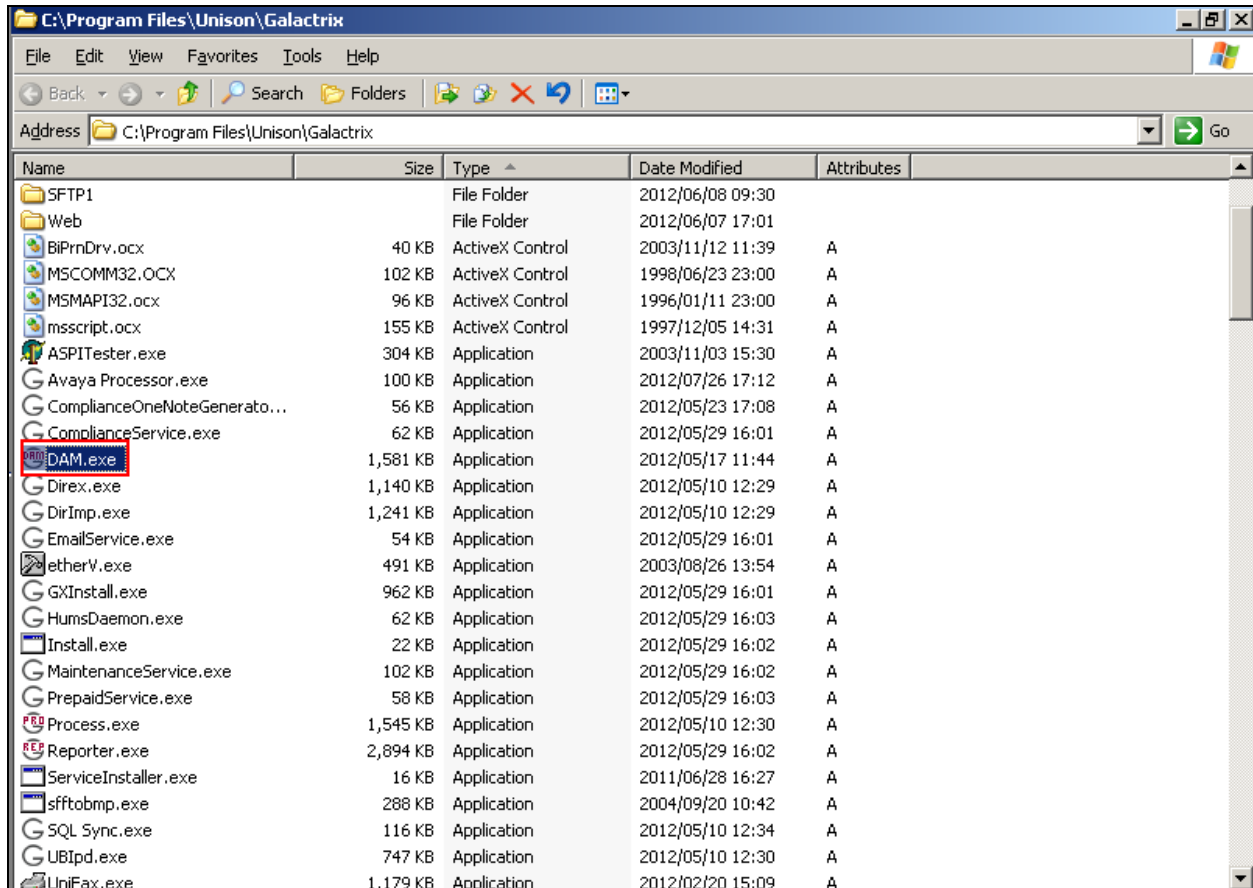
7. Configure Galactrix Server

This section describes the steps performed to configure the Galactrix Server. It is implied that the Galactrix Server software is already installed. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**. These configurations can be summarised as follows:

- Configure DAM.exe.
- Configure Avaya Processor.exe
- Configure Process.exe

7.1. Configure DAM.exe

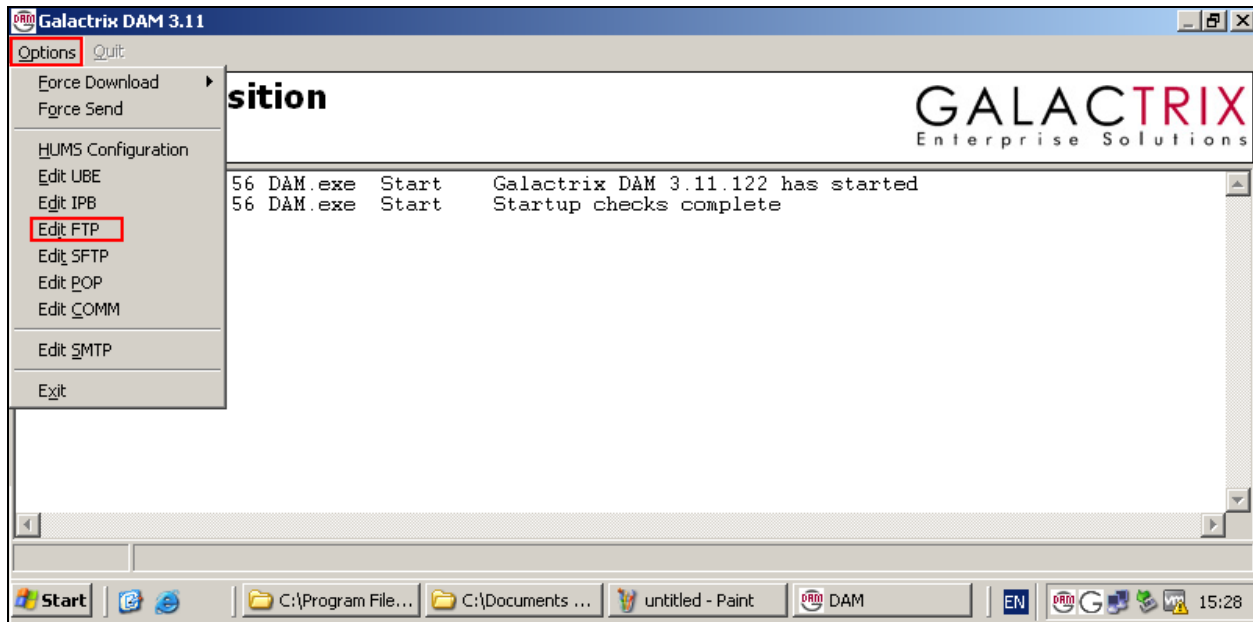
Locate and open the **DAM.exe** application. During compliance testing the **DAM.exe** was located in the Folder **C:\Program Files\Unison\Galactrix**.



Once the **DAM.exe** is opened an icon appears in the system tray, right click on the Icon and select **Show**.

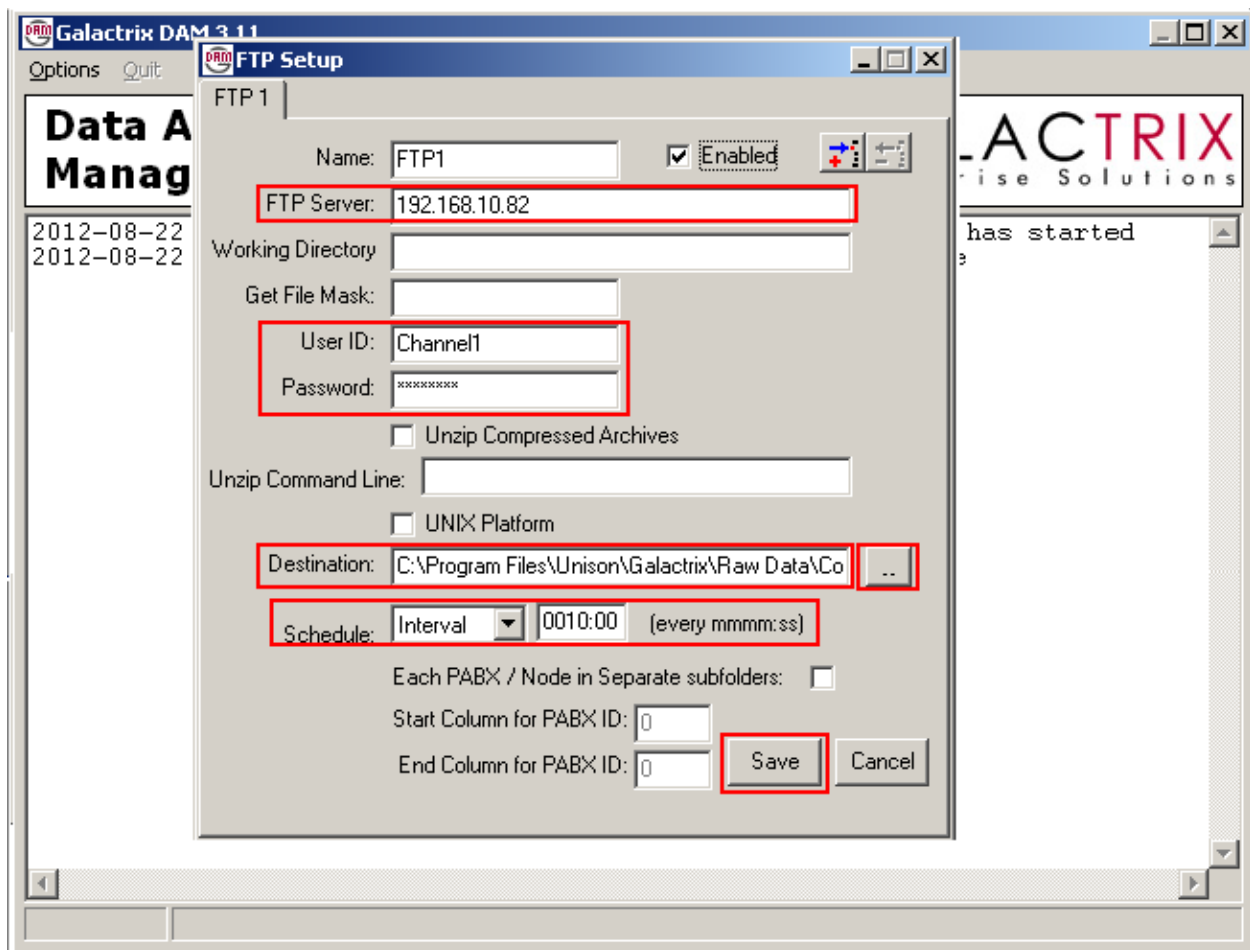


Once the **DAM.exe** Window opens select **Options** → **Edit FTP**.



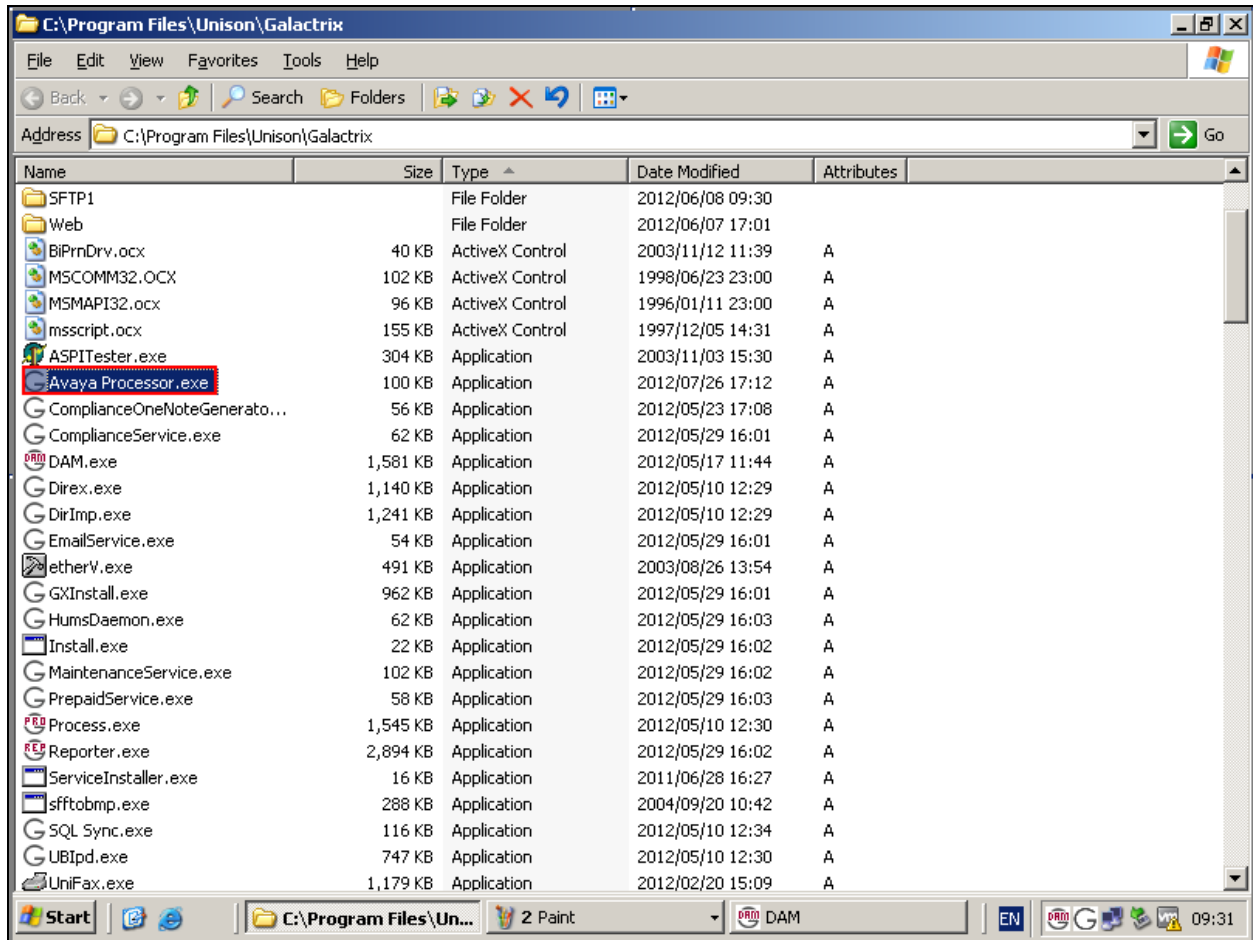
Once the **FTP Setup** window opens enter the IP address of the Scannex IP buffer in the **FTP Server** box. During compliance testing this was **192.168.10.82**. Enter the User ID and Password in the **User ID** and **Password** that were configured in **Section 6.2**. Check the **Enabled** Check box. For **Destination** browse to the folder where the CDR data is to be stored. Click the **Save** button to save the configuration.

Note: during compliance testing a collection folder was created where the CDR data was stored. The location of this folder was **C:\Program Files\Unison\Galactrix\Raw Data\Collection**

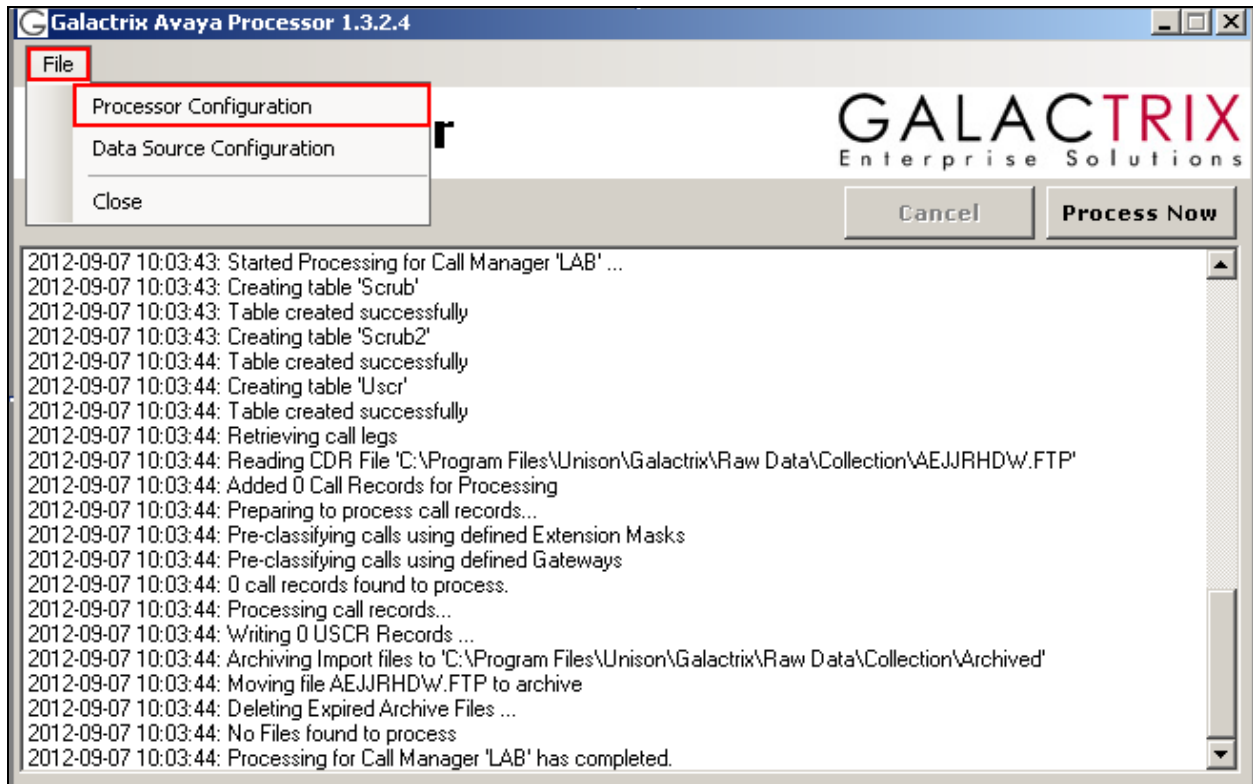


7.2. Configure Avaya Processor.exe

Locate and open the **Avaya Processor.exe** application. During compliance testing **Avaya Processor.exe** was located in the Folder **C:\Program Files\Unison\Galactrix**.



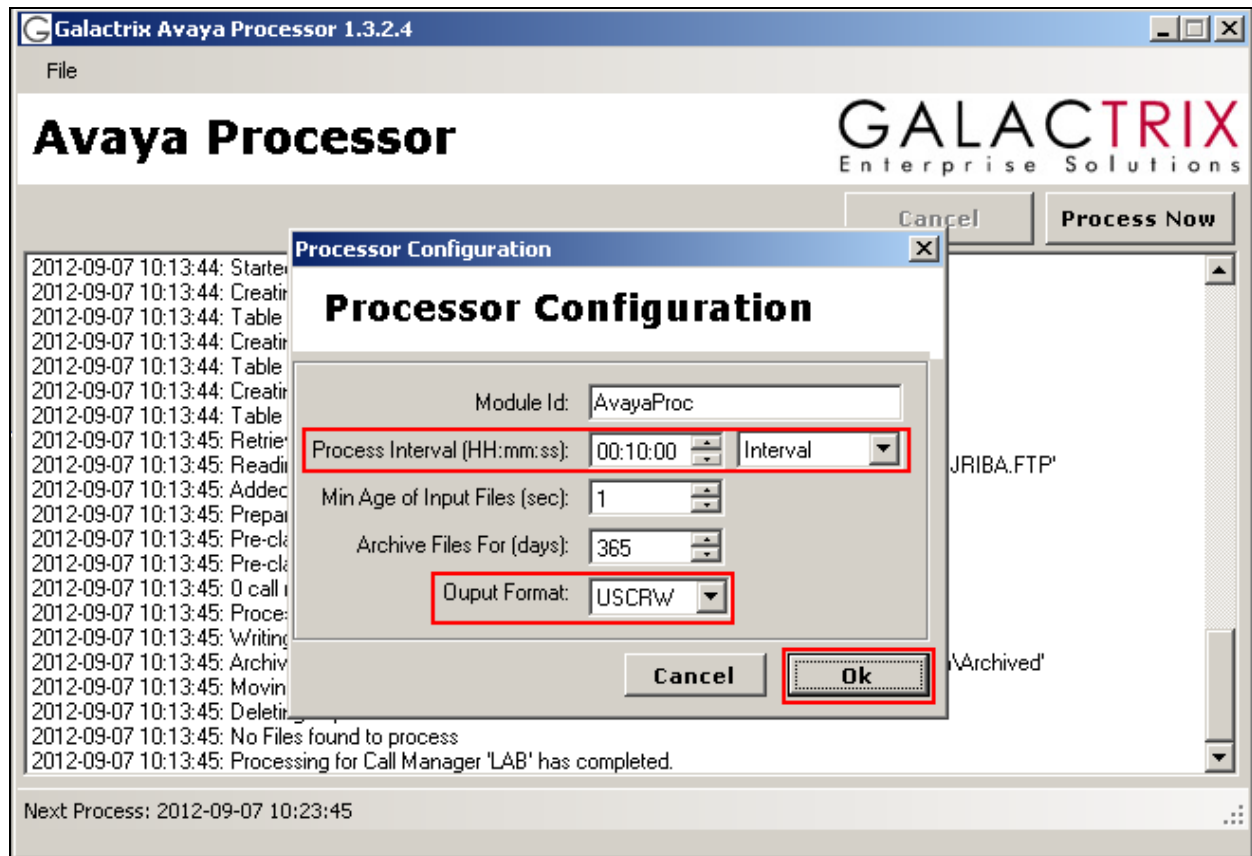
Once the **Avaya Processor** window opens select **File** followed by **Processor Configuration**.



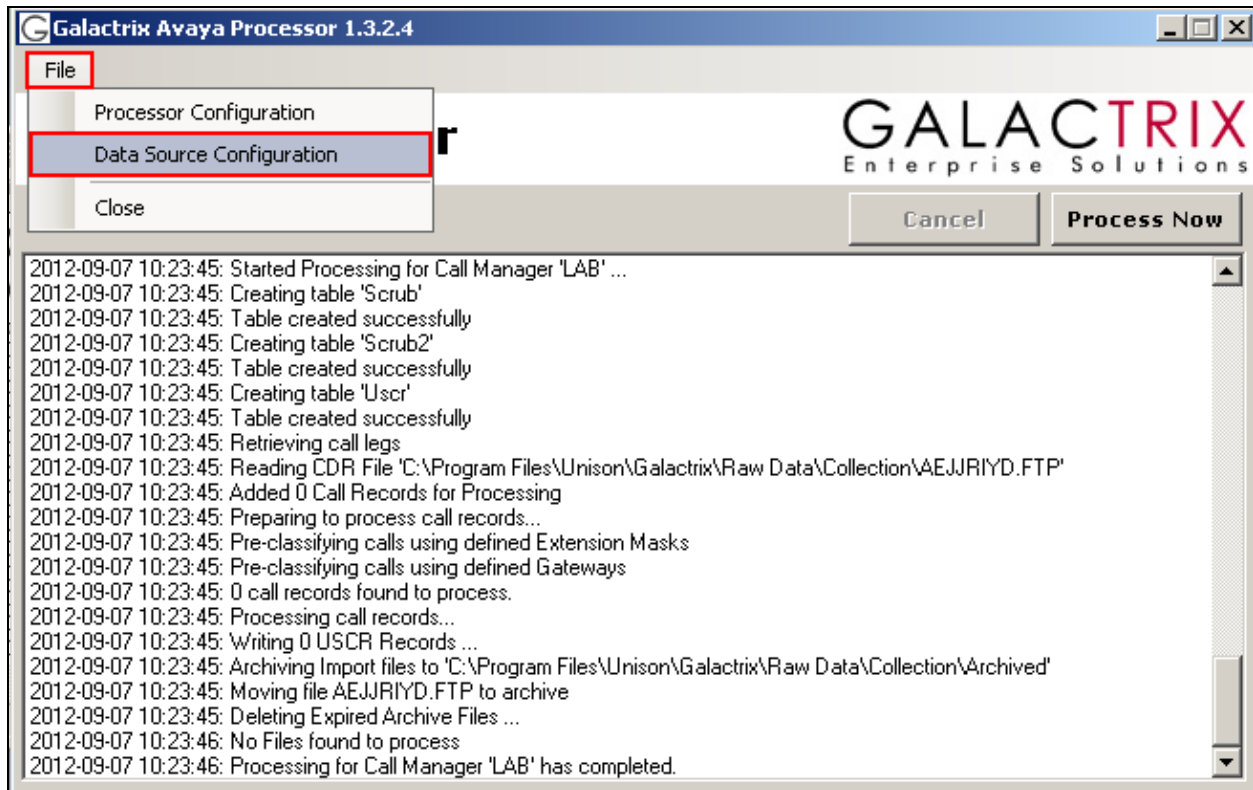
Once the **Processor Configuration** window opens enter the following:

- **Process Interval (HH:mm:ss)** – example **00:10:00** and **Interval** from the dropdown box
- **Output Format** – **USCRW**

Click the **Ok** button to save.



Select **File** followed by **Data Source Configuration**.



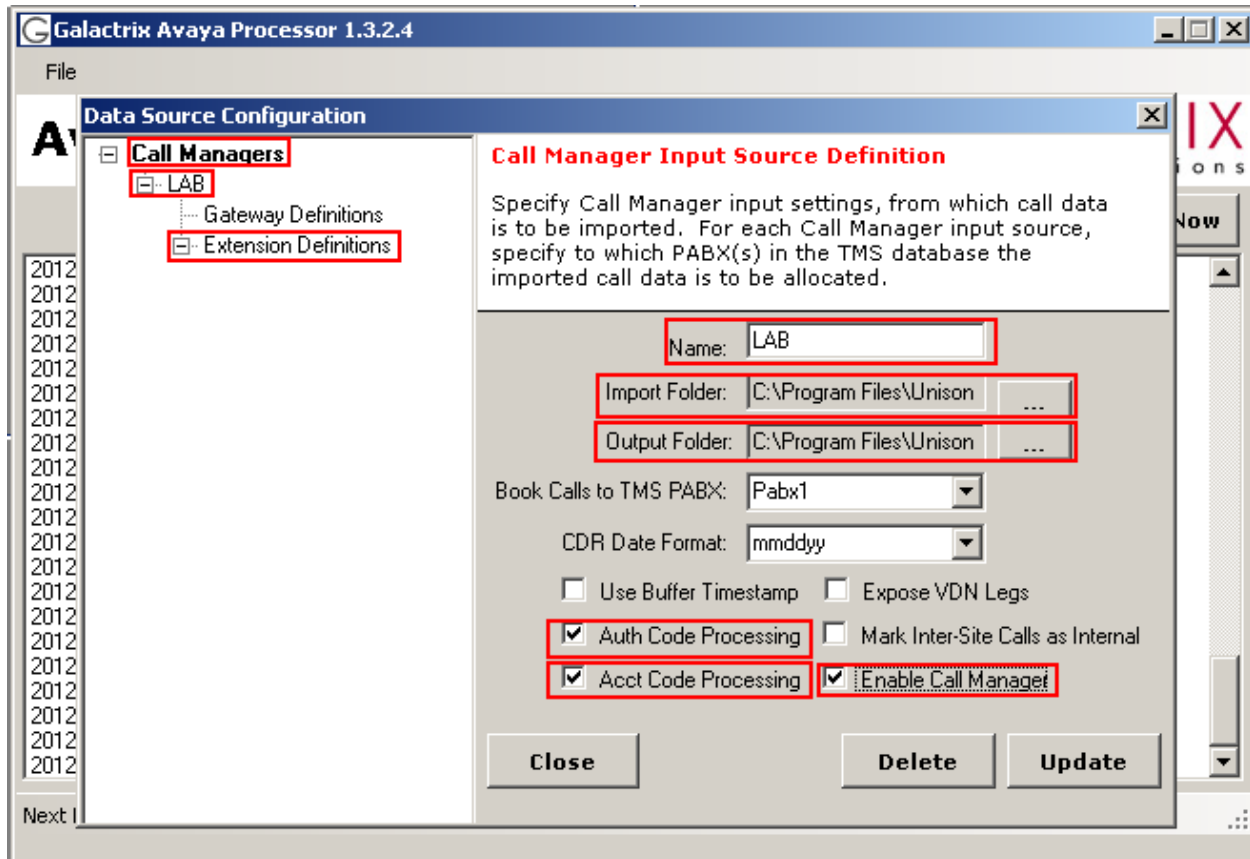
Expand **Call Managers** and select **LAB** and enter the following:

- **Name** Enter an informative name. (i.e. **LAB**)
- **Import Folder** browse to the collection folder (**C:\Program Files\Unison\Galatrix\Raw Data\Collection**)
- **Output Folder** browse to the collection folder (**C:\Program Files\Unison\Galatrix\Raw Data\Collection**)

Check the follow check boxes:

Auth Code Processing, **Acct Code Processing** and **Enable Call Manager**.

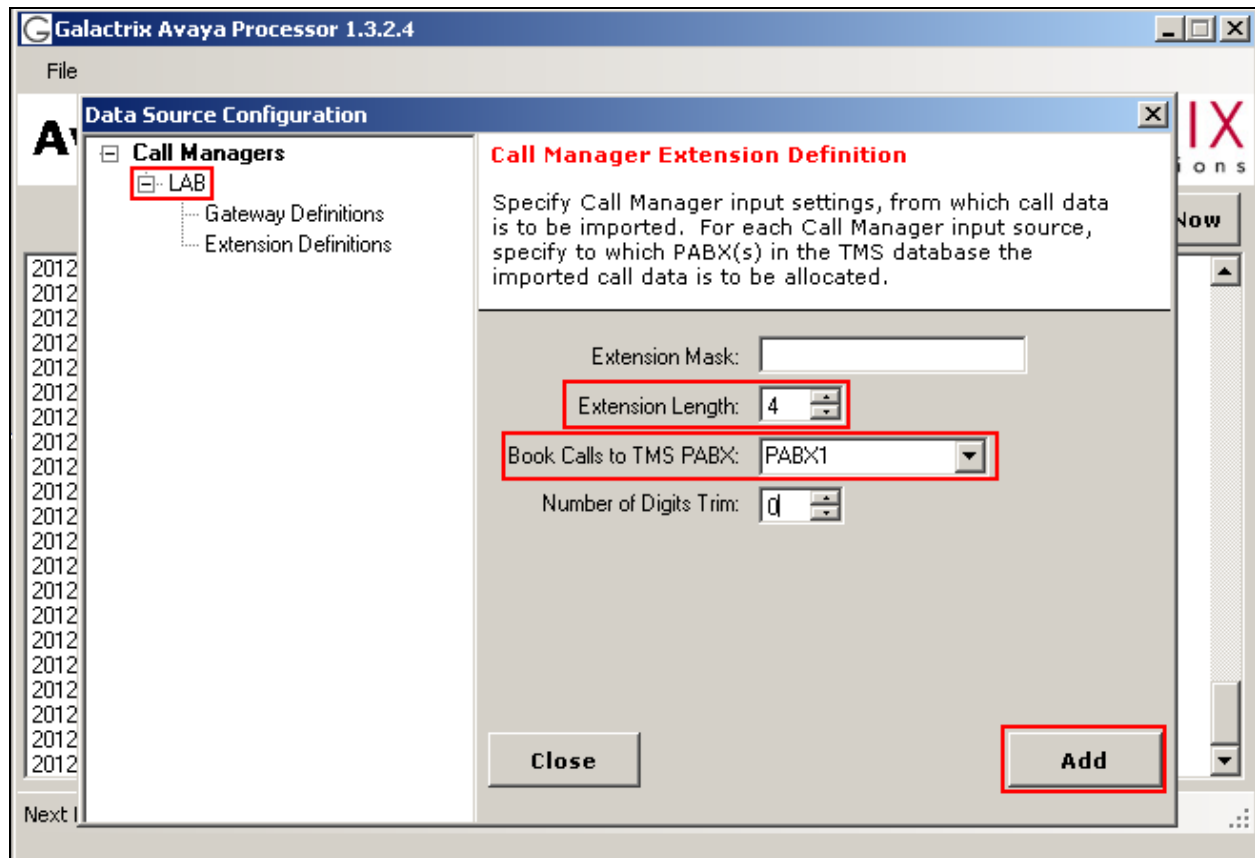
Select **Extension Definitions**.



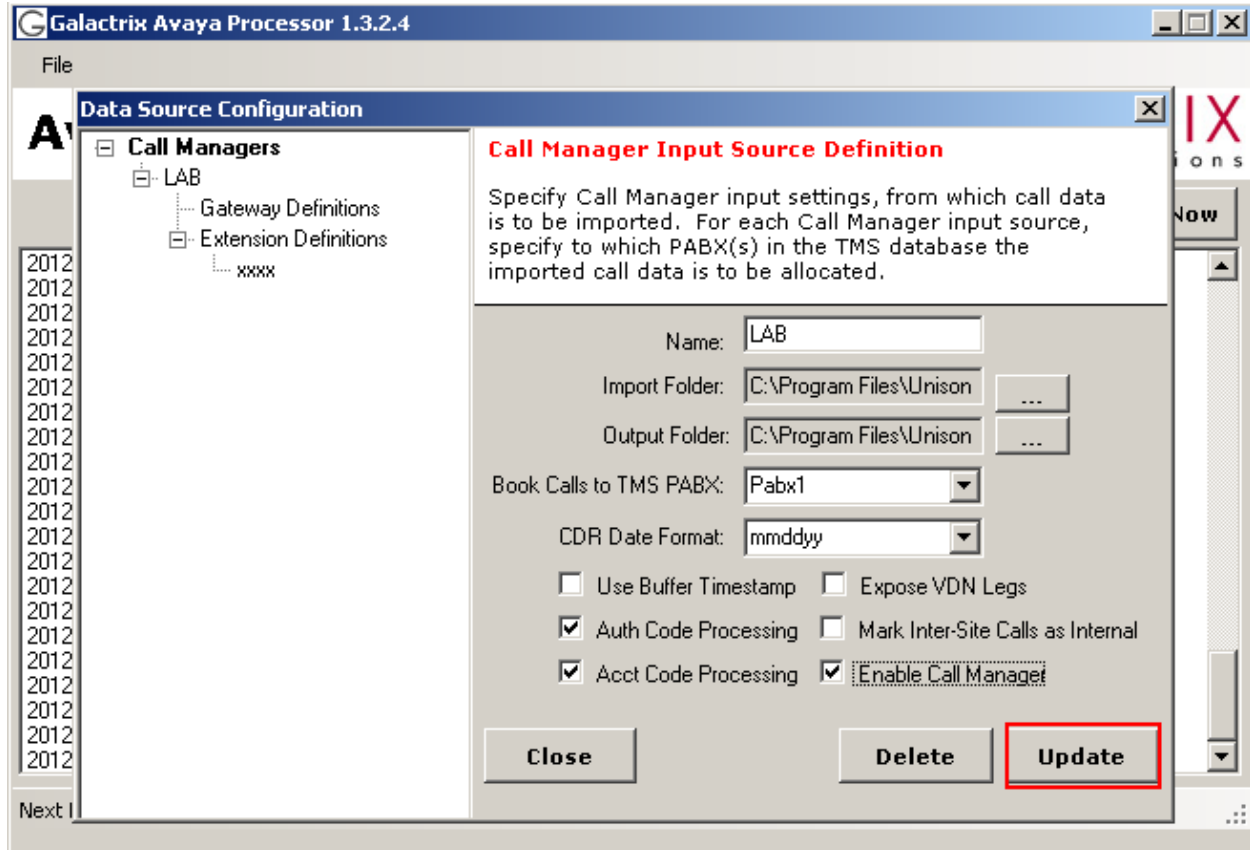
Once the **Extension Definitions** window opens enter the following:

- **Extension Length** Enter the extension length (i.e. **4**)
- **Book Calls to TMS PABX** Select **PABX1** from the dropdown box

Click the **Add** button. Select **LAB**.

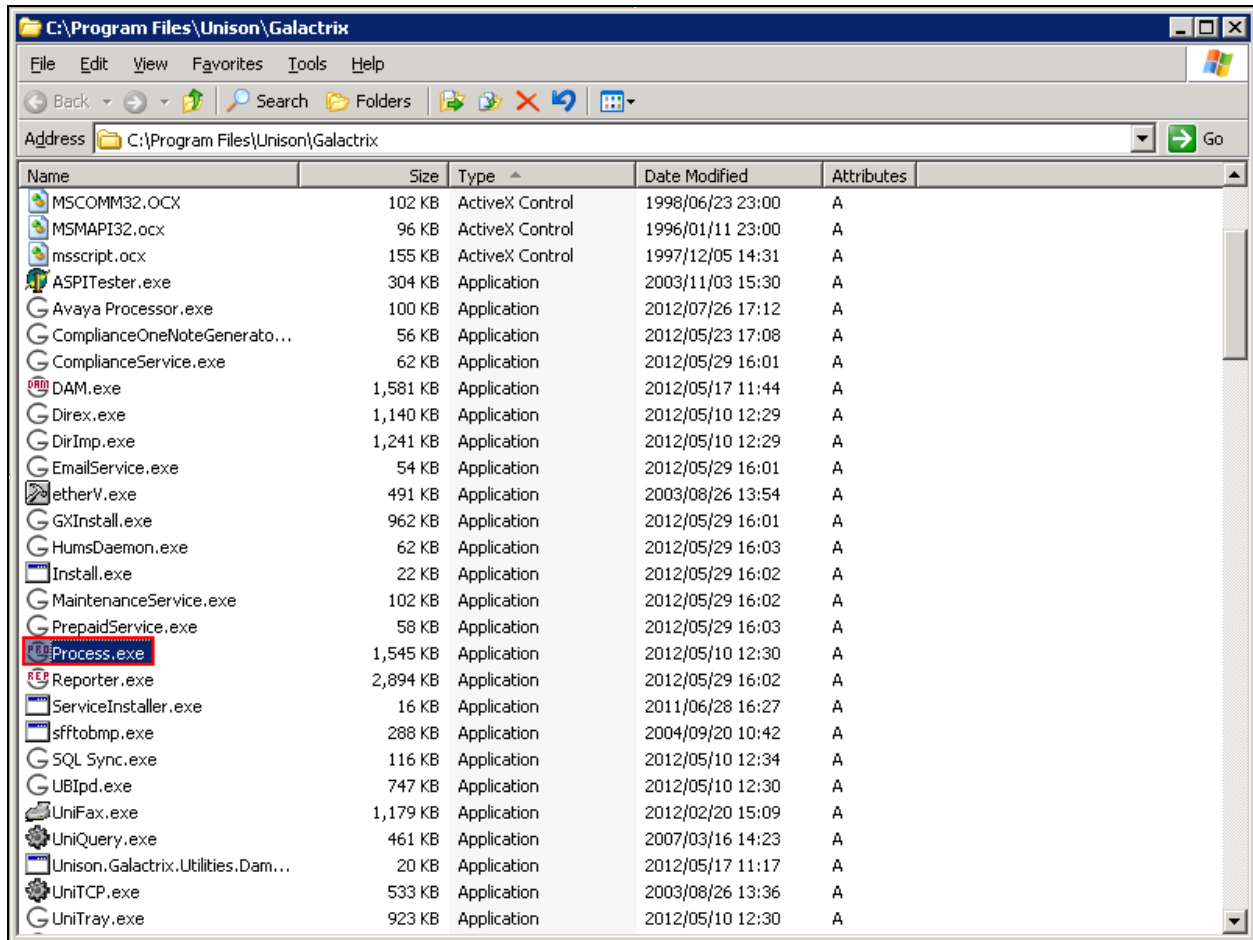


Once the **LAB** window opens select **Update** to save the configuration.



7.3. Configure Process.exe

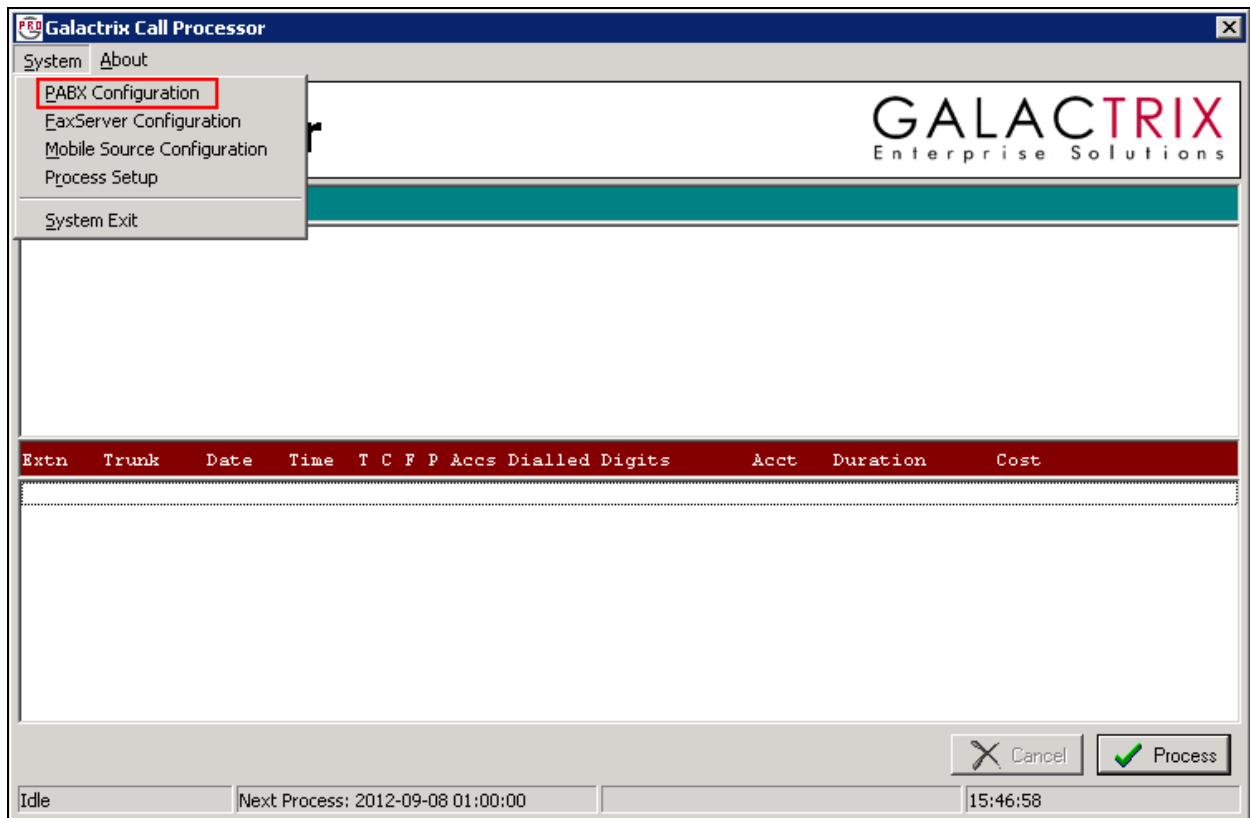
Locate and open the **Process.exe** application. During compliance testing **Process.exe** was located in the Folder **C:\Program Files\Unison\Galactrix**.



Once the **Process.exe** is opened an icon appears in the system tray, right click on the Icon and select **Show**.



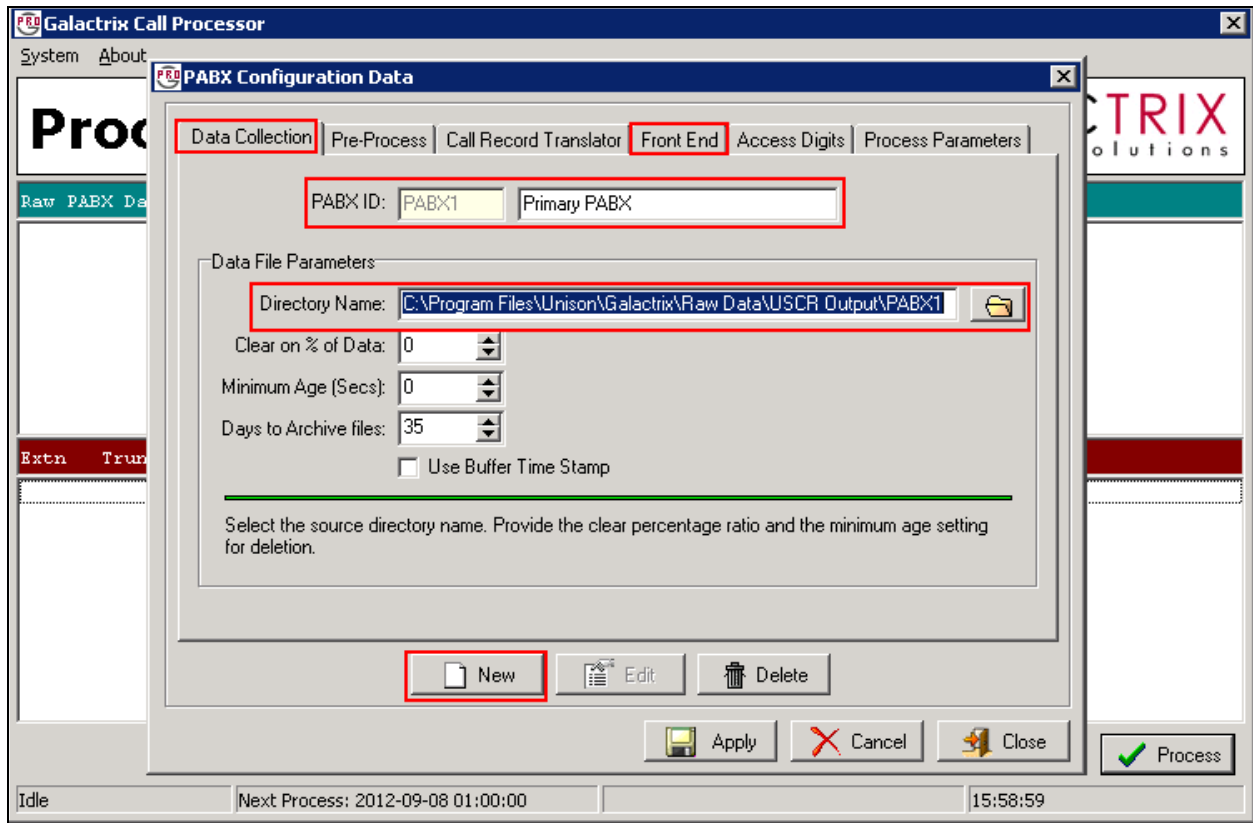
Once the **Galactrix Call Processor** window opens click on **System** followed by the **PABX Configuration**.



Once the **PABX Configuration Data** windows click on the **Data Collection** tab followed by the **New** button. Enter the following:

- **PABX** Enter PABX1 and give an informative name. (i.e. **Primary PABX**)
- **Directory Name** Browse to **Unison\Galactrix\Raw Data\USCR Output\PABX1**

Click on the **Front End** tab.



Once the **Front End** tab opens enter the following:

- **Site Code** Select **LAB** and **Avaya Lab** from the dropdown boxes
- **PABX Format** Select **USCRW** from the dropdown box
- **Parameter 1** Enter **acct**
- **Parameter 2** Enter **auth**

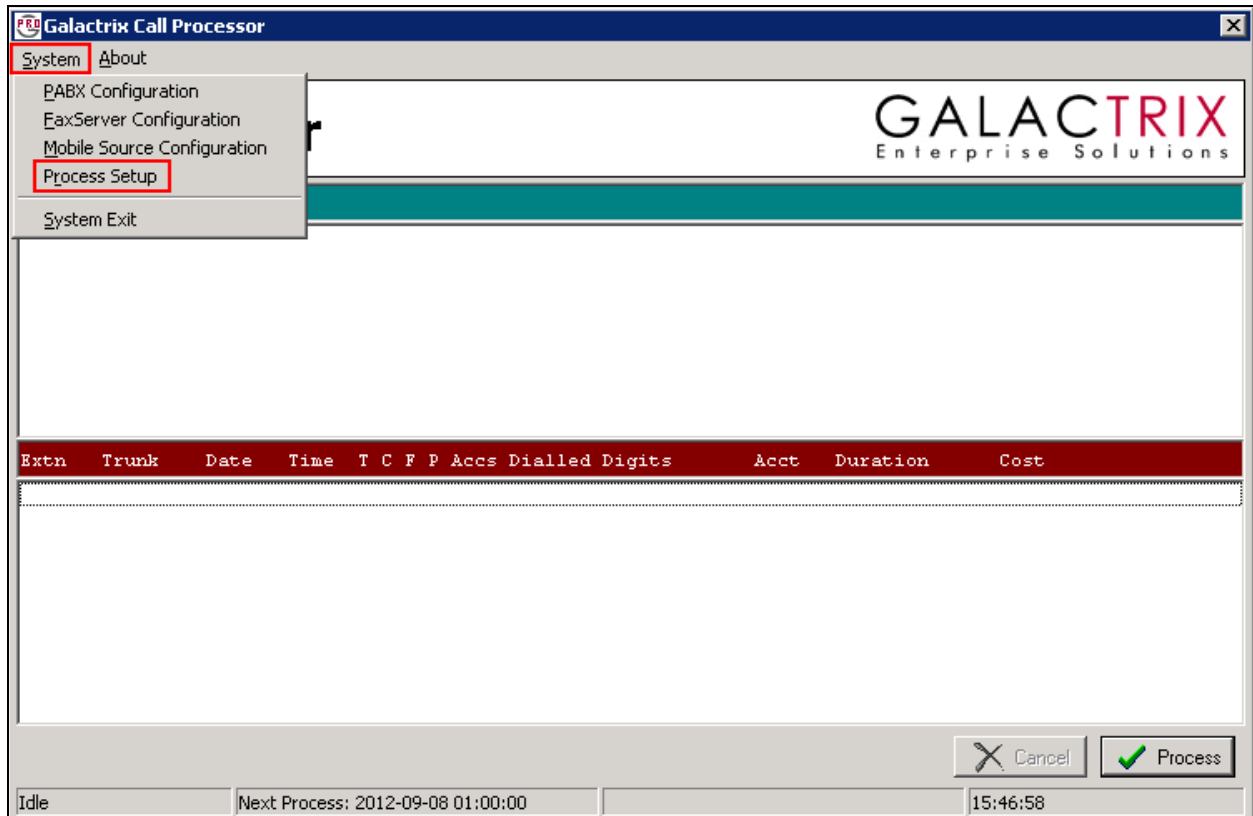
Click the **Apply** button to save followed by the **Close** button.

The screenshot shows the 'Galactrix Call Processor' application window with the 'PABX Configuration Data' dialog box open. The 'Front End' tab is selected. The configuration fields are as follows:

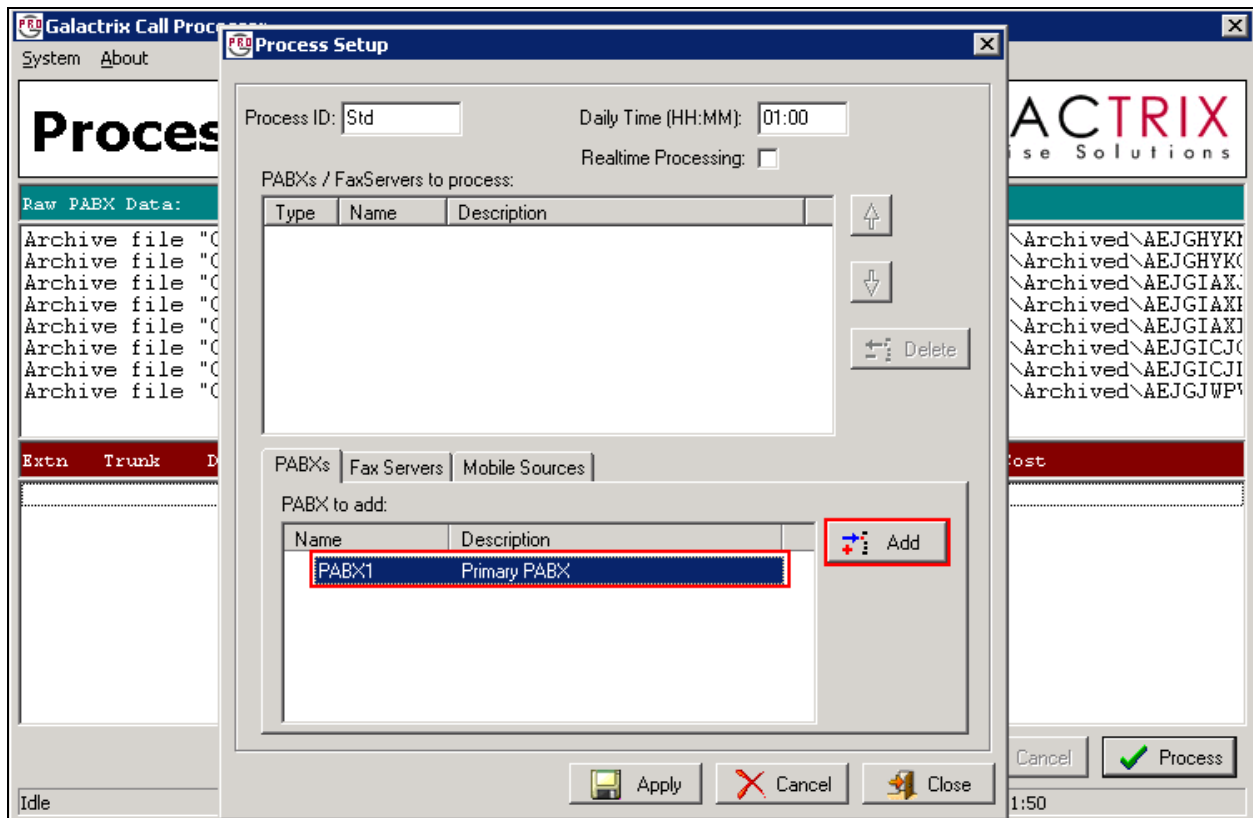
- Site Code:** LAB (dropdown), Avaya Lab (dropdown)
- Default Dept:** 9999 (dropdown), Default department for LAB (dropdown)
- Default Cost Table:** (empty dropdown)
- Internal Call Cost Table:** (empty dropdown)
- PABX Format:** USCRW (dropdown), Unison Standard Call Record - Wide Format
- Parameter 1:** acct
- Parameter 2:** auth
- Parameter 3:** (empty text box)

At the bottom right of the dialog, it says 'pbxproc.dll 139-SA20110527-V2'. Below the configuration fields are buttons for 'New', 'Edit', and 'Delete'. At the very bottom of the dialog are buttons for 'Apply', 'Cancel', and 'Close'. The 'Apply' and 'Close' buttons are highlighted with red boxes. In the background, a 'Process' button with a green checkmark is visible. The status bar at the bottom of the application window shows 'Idle', 'Next Process: 2012-09-08 01:00:00', and '16:26:18'.

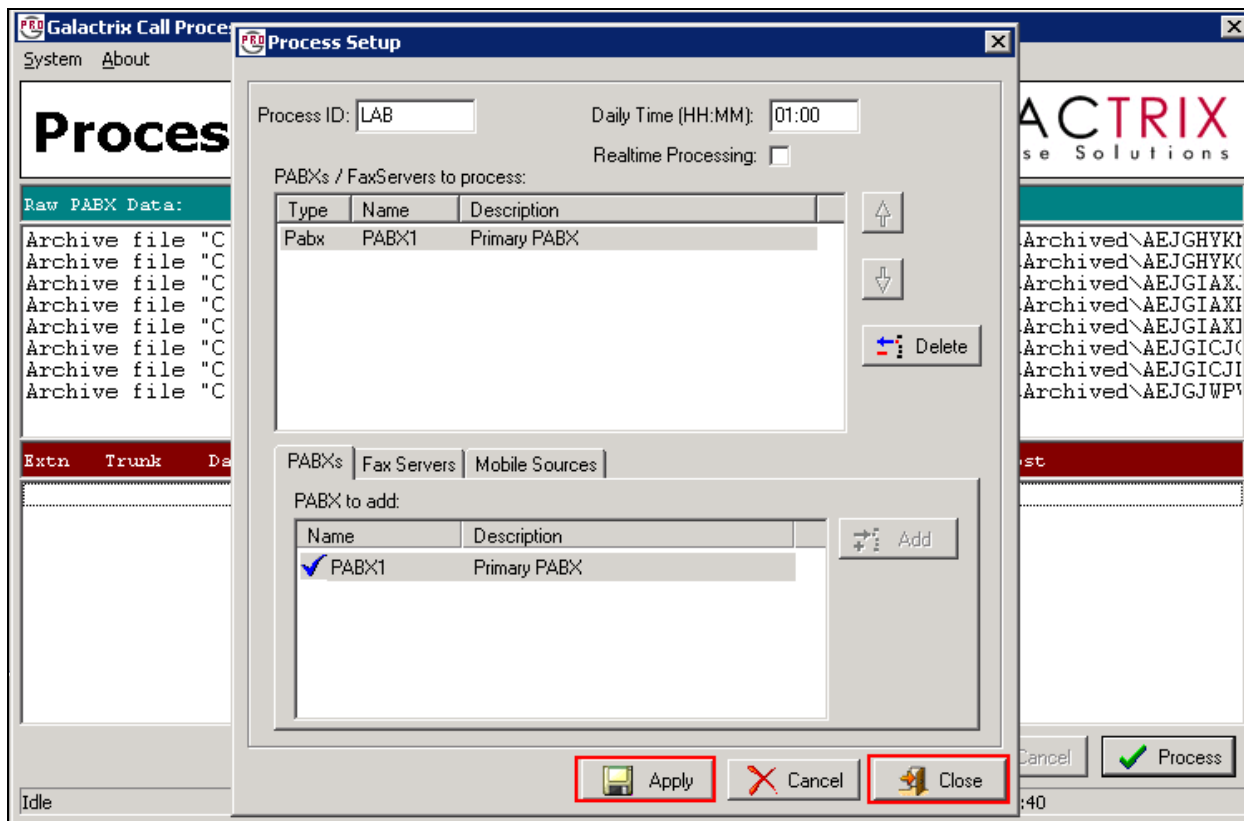
Once the PABX Configuration setup is completed click on **S**ystem followed by the **P**rocess Setup.



Once the **Process Setup** window opens enter **LAB** in the **Process ID** field, then highlight **PABX1** and click on the **Add** button.



Once the **PABX** is added click on the **Apply** button to save followed by the **Close** button.



8. Verification Steps

This section provides tests that can be performed to verify correct configuration of the Avaya and UNISON Galactrix solution.

8.1. Verify the Avaya Aura® Communication Manager CDR Link

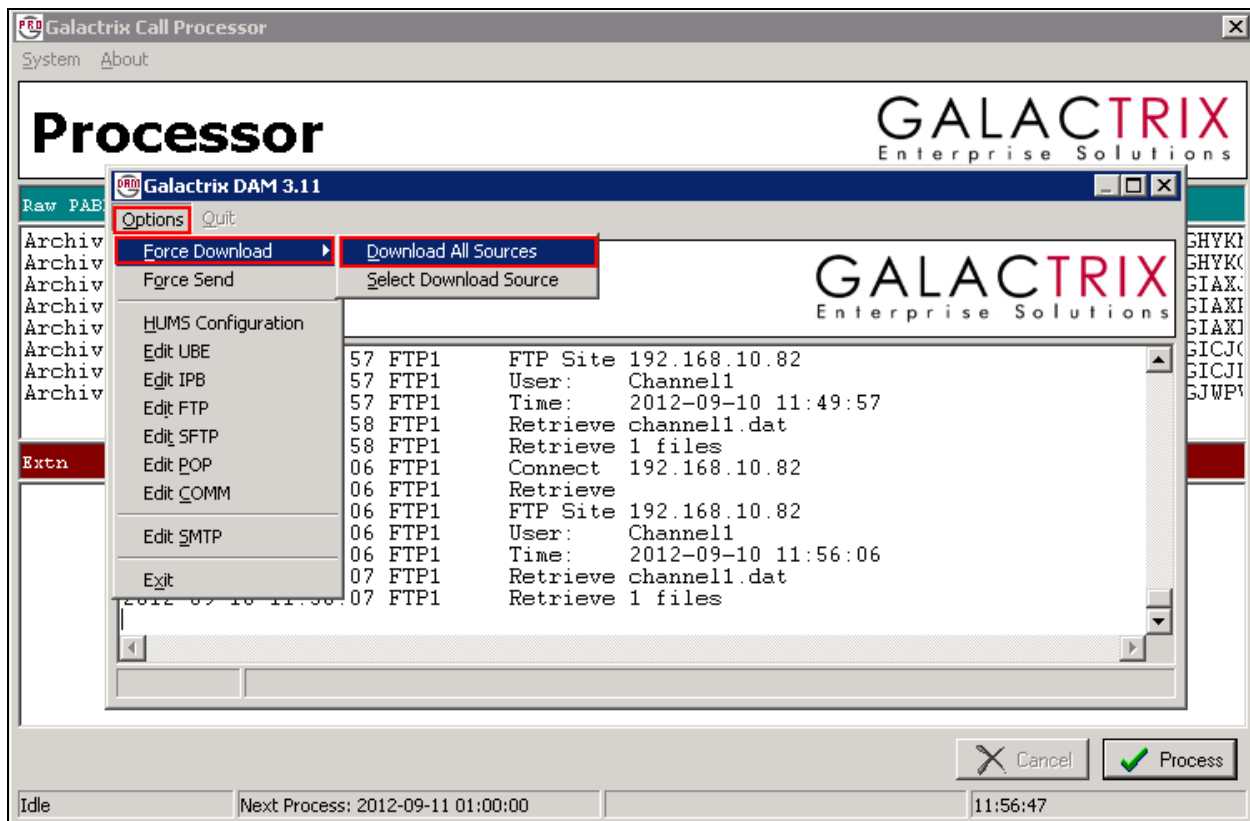
Use the **status cdr-link** command to verify that the link between the Communication Manager and the IP buffer is in service. **Link State: up** and **Reason Code: OK** confirms successful connection.

status cdr-link		
CDR LINK STATUS		
	Primary	Secondary
Link State:	up	CDR administered
Number of Retries:	999	
Date & Time:	2011/12/15 17:32:12	0000/00/00 00:00:00
Forward Seq. No:	0	0
Backward Seq. No:	0	0
CDR Buffer % Full:	0.03	0.00
Reason Code:	OK	

8.2. Verify Galactrix Downloads File from the IP Buffer

The following is carried out on the Galactrix to ensure that the stored CDR data on the IP buffer can be retrieved. Open DAM.exe and select **Options** followed by **Force Download** → **Download all Sources**. Verify the time and IP Address of the FTP Site of the new file once downloaded.

Note: IP Address should be of the IP buffer



9. Conclusion

A full and comprehensive set of feature functional test cases were performed during Compliance testing. UNISON Galactrix 3.1.1 is considered compliant with Avaya Aura® Communication Manager All test cases have passed and met the objectives outlined in **Section 2.2**.

10. Additional References

These documents form part of the Avaya official technical reference documentation suite. Further information may be had from <http://support.avaya.com> or from your Avaya representative.

[1] *Administering Avaya Aura® Communication Manager 03-300509 Release 6.0 Issue 6.0 System Management Reference*

[2] *Administering Avaya Aura® Session Manager 03-603324 Release 6.1 Issue 1.0*

Contact UNISON at +27117973000 for Product Documentation relating to Galactrix and Scannex IP buffer.

©2012 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.