



Avaya Solution & Interoperability Test Lab

Application Notes for configuring Metropolis OfficeWatch XT with Avaya Aura® Communication Manager R7.0 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Metropolis OfficeWatch XT to interoperate with Avaya Aura® Communication Manager 7.0. Metropolis OfficeWatch XT captures call records from Avaya Aura® Communication Manager using a Call Detail Record (CDR) link with Avaya Reliable Session Protocol (RSP) enabled for reliable transmission of call records. In turn, OfficeWatch processes the call records and generates detailed reports.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the 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 steps required to integrate Metropolis OfficeWatch XT with Avaya Aura® Communication Manager R7.0. Metropolis OfficeWatch XT captures call records from Avaya Aura® Communication Manager using a Call Detail Record (CDR) link with Avaya Reliable Session Protocol (RSP) enabled for reliable transmission of call records. OfficeWatch XT then processes the call records and generates detailed reports.

Note: For security purposes public IP addresses and phone numbers have been altered in this document.

2. General Test Approach and Test Results

This section describes the compliance testing used to verify interoperability of Metropolis OfficeWatch XT with Communication Manager and covers the general test approach and the test results. The testing covered feature and serviceability test cases. The feature testing covered the ability of OfficeWatch XT to capture and process call records.

The call records captured and displayed by OfficeWatch XT were compared for accuracy to call records received by the Avaya Reliable Data Transport CDR test tool. Call records for various call types were generated including internal calls, inbound and outbound trunk calls, PSTN calls, transferred calls and conference calls. Calls were established using H.323 and SIP telephones.

The serviceability testing focused on the ability of OfficeWatch XT to recover from adverse conditions such as loss of network connectivity. With the use of Avaya RSP, call records that were generated while OfficeWatch XT was disconnected from the network were not lost.

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 for 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 test included feature and serviceability testing. The feature testing focused on verifying the proper parsing and displaying of unformatted CDR data received from Communication Manager by OfficeWatch XT.

The following is a list of Interoperability tests that were performed:

- Internal calls
- Inbound Inter-Switch calls
- Outbound Inter-Switch calls
- Inbound PSTN calls
- Outbound PSTN calls
- Tandem calls to PSTN
- Hold
- Blind and Consultative Transfer
- Blind and Consultative Conference
- Hunt Groups
- Bridged Appearance
- Account codes
- Authorization codes
- Split CDR Records
- Serviceability

The serviceability testing focused on the ability of OfficeWatch XT to recover from adverse conditions such as loss of network connectivity, disabling and re-enabling the CDR Link and power cycling. With the use of Avaya RSP, call records that were generated while OfficeWatch XT was disconnected from the network were not lost.

2.2. Test Results

All applicable test cases were executed and passed with the following observation:

There are some differences in Communication Manager in the call records generated by SIP endpoints compared to Analog, Digital, and H.323 endpoints. As a result in certain scenarios involving SIP endpoints (e.g., two-party call, transfer, or conference), a CDR application may see more or less records, or records with condition codes/calling party other than expected. Avaya is investigating the differences and code changes may be made available in a future release pending the outcome of that investigation.

2.3. Support

For technical support on Metropolis OfficeWatch XT, contact Metropolis Customer Service by phone, through their website, or email.

Phone: (954) 414-2900 x32
Web: <http://www.metropolis.com/support.html>
Email: support2016@metropolis.com

3. Reference Configuration

Figure 1 illustrates the configuration used for the compliance test. In the sample configuration two sites, Sites A and B, are connected via a SIP trunk through Session Manager. OfficeWatch XT only monitors the calls at Site A. Site B is used to generate inter-site traffic across the SIP trunk.

Site A has a VMWare virtual machine hosting the Avaya Aura® Communication Manager, Session Manager, System Manager and Media Server. The Communication Manager is connected to an Avaya G450 Media Gateway. Site A also includes Avaya 9600 Series H.323 and SIP telephones. In addition, Site A has connectivity to the PSTN. The configuration at Site B is similar to Site A and also uses the Session Manager at Site A. OfficeWatch XT connects via the LAN and establishes a CDR link to Communication Manager at Site A. The OfficeWatch XT is also installed and configured on the VMWare virtual machine.

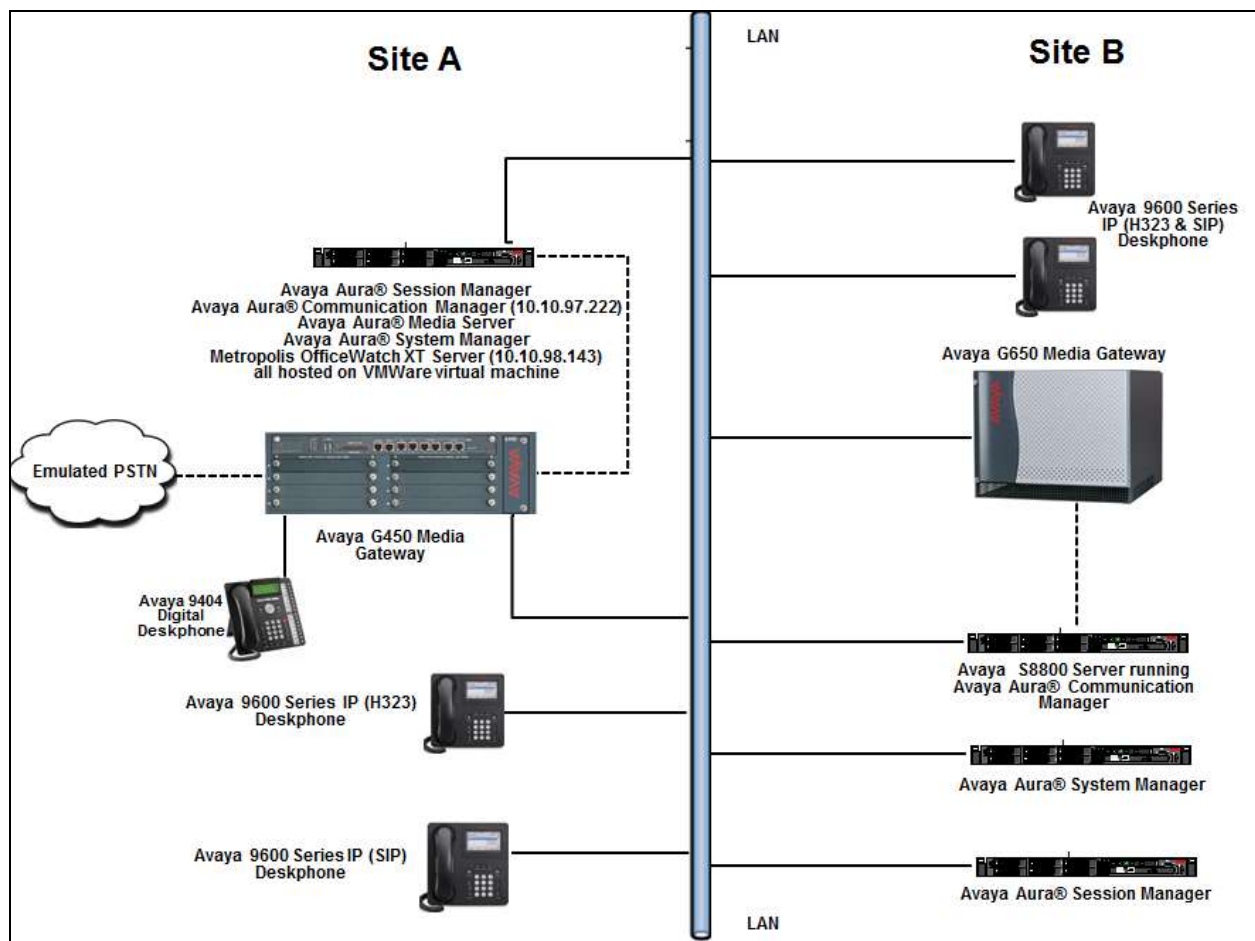


Figure 1: Metropolis OfficeWatch XT with Avaya Aura® Communication Manager

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on a virtual server	7.0.0.1.0-SP1 (R017x.00.0.441.0)
Avaya Aura® Session Manager running on a virtual server	7.0.0.0.700007
Avaya Aura® System Manager running on a virtual server	7.0.0.0
Avaya Aura® Media Server running on a virtual server	7.7.0.226
Avaya IP Deskphones: 9641 (H.323) 9608 (H.323) 9621 (SIP) 9641 (SIP)	6.6115 6.6115 7.0.0.39 7.0.0.39
Avaya 9404 Digital Deskphone	R 0.15 V21
Metropolis OfficeWatch XT running on Windows Server 2012 R2 Standard running on VMware (5.5)	2016.02.03c

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring call detail recording (CDR) on Communication Manager. These steps are performed through the System Access Terminal (SAT). Communication Manager is configured to generate CDR records and send them to the IP address of the server running OfficeWatch XT using TCP/IP. The procedure covers the following areas:

- Administer IP Node Names
- Configure CDR Link
- Enable CDR for Intra-Switch Calls
- Enable CDR for Trunks Calls
- Configure Off-PBX-Telephone Configuration-Set

5.1. Administer IP Node Names

Use the **change node-names ip** command to create a new node name for the server running OfficeWatch XT. This node name is associated with the IP Address of the server. In the sample configuration **CDR-Collector** was used for the name and **10.10.98.143** was used for the IP address. Also, take note of the node name **procr**. It will be used in the next step. The procr entry on this form was previously administered. The **AVAYA-RD TT** was used to setup the collection of CDR on the Secondary link.

change node-names ip		Page 1 of 2	
		IP NODE NAMES	
Name	IP Address		
AVAYA-RD TT	10.10.98.71		
CDR-Collector	10.10.98.143		
DevvmAES	10.10.97.224		
DevvmAMS	10.10.97.232		
GW-G450	10.10.4.25		
Loopback	10.10.97.222		
SM-VM	10.10.97.228		
TFTP-Server	10.10.98.72		
default	0.0.0.0		
procr	10.10.97.222		

5.2. Configure CDR Link

Use the **change ip-services** command to define the CDR link between Communication Manager and OfficeWatch XT. To define a primary CDR link, provide the following information:

- **Service Type: CDR1** [If needed, a secondary link can be defined by setting Service Type to CDR2.]
- **Local Node: procr** [For the Communication Manager used during compliance testing, set the Local Node to the node name of the processor board.]
- **Local Port: 0** [The Local Port is fixed to 0 because Communication Manager initiates the CDR link.]
- **Remote Node: CDR-Collector** [The Remote Node is set to the node name previously defined in **Section 5.1.**]
- **Remote Port: 9000** [The Remote Port may be set to a value between 5000 and 64500 inclusive, and must match the port configured in OfficeWatch XT.]

change ip-services						Page	1	of	4
IP SERVICES									
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port				
AESVCS	y	procr	8765						
CDR1		procr	0	CDR-Collector	9000				
CDR2		procr	0	AVAYA-RDIT	9001				

For this solution the Reliable Session Protocol (RSP) is used. On **Page 3** of the ip-services form, set the **Reliable Protocol** field to **y**.

change ip-services						Page	3	of	4
SESSION LAYER TIMERS									
Service Type	Reliable Protocol	Packet Timer	Resp	Session Connect Message Cntr	SPDU Cntr	Connectivity Timer			
CDR1	y	30		3	3	60			
CDR2	y	30		3	3	60			

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

- **CDR Date Format: month/day**
- **Primary Output Format: unformatted**
- **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 8** in **Section 9** 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 4.x CDR formats for “n”. 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 INTRA-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.]
- **CDR Account Code Length: 4** [The length may be set to a value between 1 and 15. However, during the compliance test, “4” was used.]

```

change system-parameters cdr                                     Page 1 of 1
                                CDR SYSTEM PARAMETERS

Node Number (Local PBX ID):                                     CDR Date Format: month/day
    Primary Output Format: unformatted    Primary Output Endpoint: CDR1
Secondary Output Format: unformatted    Secondary Output Endpoint: CDR2
    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? 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? 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? n           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: dialed
    Privacy - Digits to Hide: 0            CDR Account Code Length: 4
Remove '+' from SIP Numbers? Y

```

5.3. Enable CDR for Intra-Switch Calls

If the **Intra-switch CDR** field is set to **y** on **Page 1** of the **system-parameters cdr** form, then use the **change intra-switch-cdr** command to define the extensions that will be subject to call detail records. In the **Extension** field, enter the specific extensions whose usage will be tracked.

Note: To simplify the process of adding multiple extensions in the Assigned Members field, the **Intra-switch CDR by COS (SA8202)** feature may be utilized in the SPECIAL APPLICATIONS form under the system-parameters section. To utilize this feature, contact an authorized Avaya account representative to obtain the license.

change intra-switch-cdr		Page 1 of 3	
INTRA-SWITCH CDR			
Assigned Members:	8	of 1000	administered
Extension	Extension	Extension	Extension
56101			
56102			
56103			
56201			
56202			
56203			
56204			
56205			

5.4. Enable CDR for Trunk Calls

For each trunk group for which CDR records are desired, verify that CDR reporting is enabled. To do this, use the **change trunk-group *n*** command, where *n* is the trunk group number, and verify that the **CDR Reports** field is set to **y**. This applies to all trunk group types.

The example below shows the ISDN-PRI trunk to the PSTN.

```
change trunk-group 4                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 4                      Group Type: isdn      CDR Reports: y
  Group Name: To-IPO 36_44           COR: 1              TN: 1          TAC: #004
  Direction: two-way                 Outgoing Display? n    Carrier Medium: PRI/BRI
  Dial Access? n                     Busy Threshold: 255  Night Service:
Queue Length: 0
Service Type: tie                     Auth Code? n          TestCall ITC: rest
                                     Far End Test Line No:
TestCall BCC: 4
```

The example below shows the SIP trunk between Sites A and B. This SIP trunk actually terminates to Session Manager, which then routes calls to Site B over another SIP trunk.

```
change trunk-group 1                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 1                      Group Type: sip      CDR Reports: y
  Group Name: Trunk to SM on VM       COR: 1              TN: 1          TAC: #001
  Direction: two-way                 Outgoing Display? y
  Dial Access? n                     Night Service:
Queue Length: 0
Service Type: tie                     Auth Code? n
                                     Member Assignment Method: auto
                                     Signaling Group: 1
                                     Number of Members: 24
```

5.5. Configure Off-PBX-Telephone Configuration-Set

SIP endpoints and off-pbx-telephone stations will be automatically created in Communication Manager when users (SIP endpoints) are created in Session Manager.

However, the off-pbx-telephone configuration-set form needs to be modified. Enter **change off-pbx-telephone configuration-set** and disable the **CDR for Calls to EC500 Destination?** field by setting it to *n*.

change off-pbx-telephone configuration-set 1	Page 1 of 1
CONFIGURATION SET: 1	
Configuration Set Description:	
Calling Number Style: network	
CDR for Origination: phone-number	
CDR for Calls to EC500 Destination? n	
Fast Connect on Origination? n	
Post Connect Dialing Options: dtmf	
Cellular Voice Mail Detection: timed (seconds): 4	
Barge-in Tone? n	
Calling Number Verification? y	
Call Appearance Selection for Origination: primary-first	
Confirmed Answer? n	
Use Shared Voice Connections for Second Call Answered? n	
Use Shared Voice Connections for Second Call Initiated? n	
Provide Forced Local Ringback for EC500? n	
Apply Ringback upon Receipt of: Call-Proceeding	

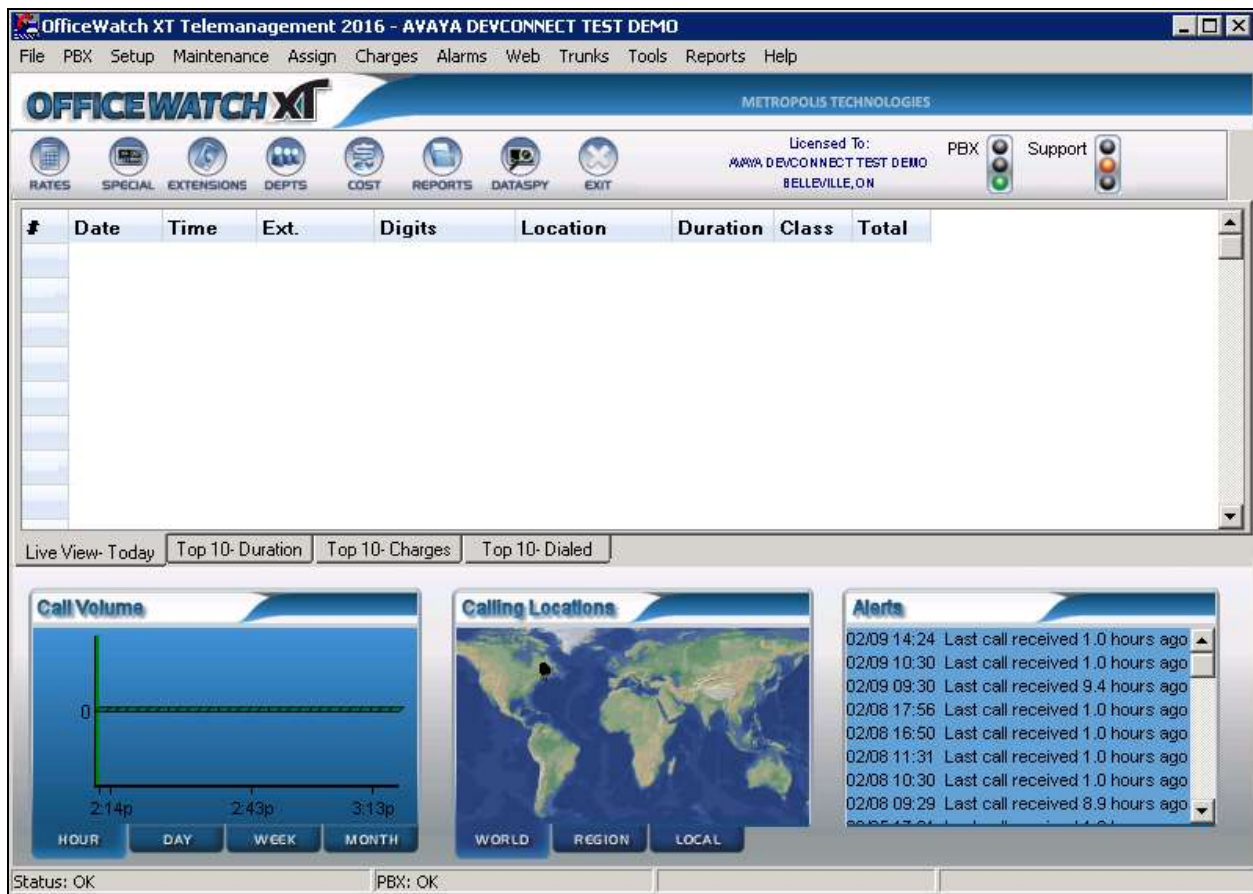
6. Configure Metropolis OfficeWatch XT

This section provides the procedures for configuring Metropolis OfficeWatch XT. The procedures include the following areas:

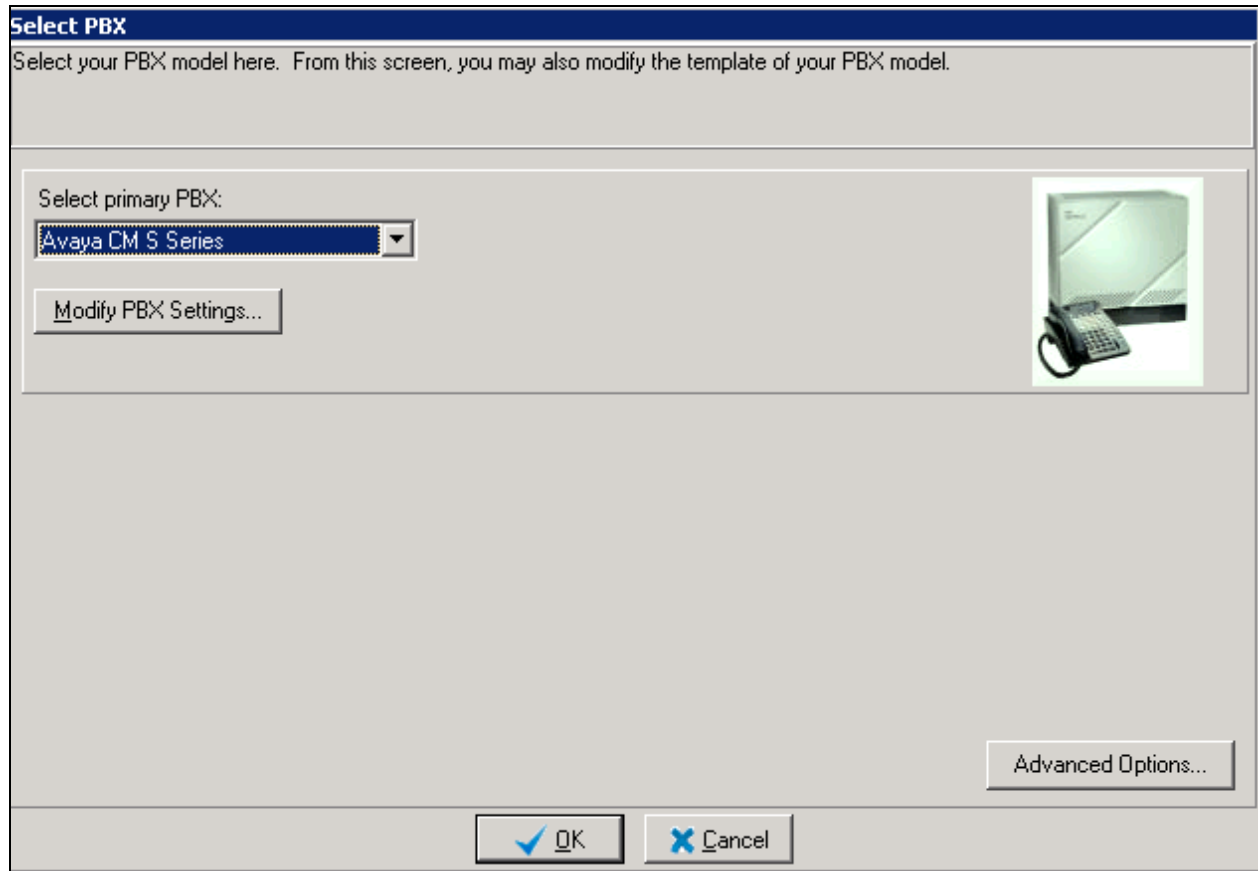
- Administer PBX
- Administer Customization
- Administer Grace Periods

6.1. Administer PBX

From the Metropolis OfficeWatch XT server, launch **OfficeWatch XT** to display the **OfficeWatch XT Telemanagement 2016 – AVAYA DEVCONNECT TEST DEMO** screen as shown below. Select **PBX → Select PBX...** from the top menu.



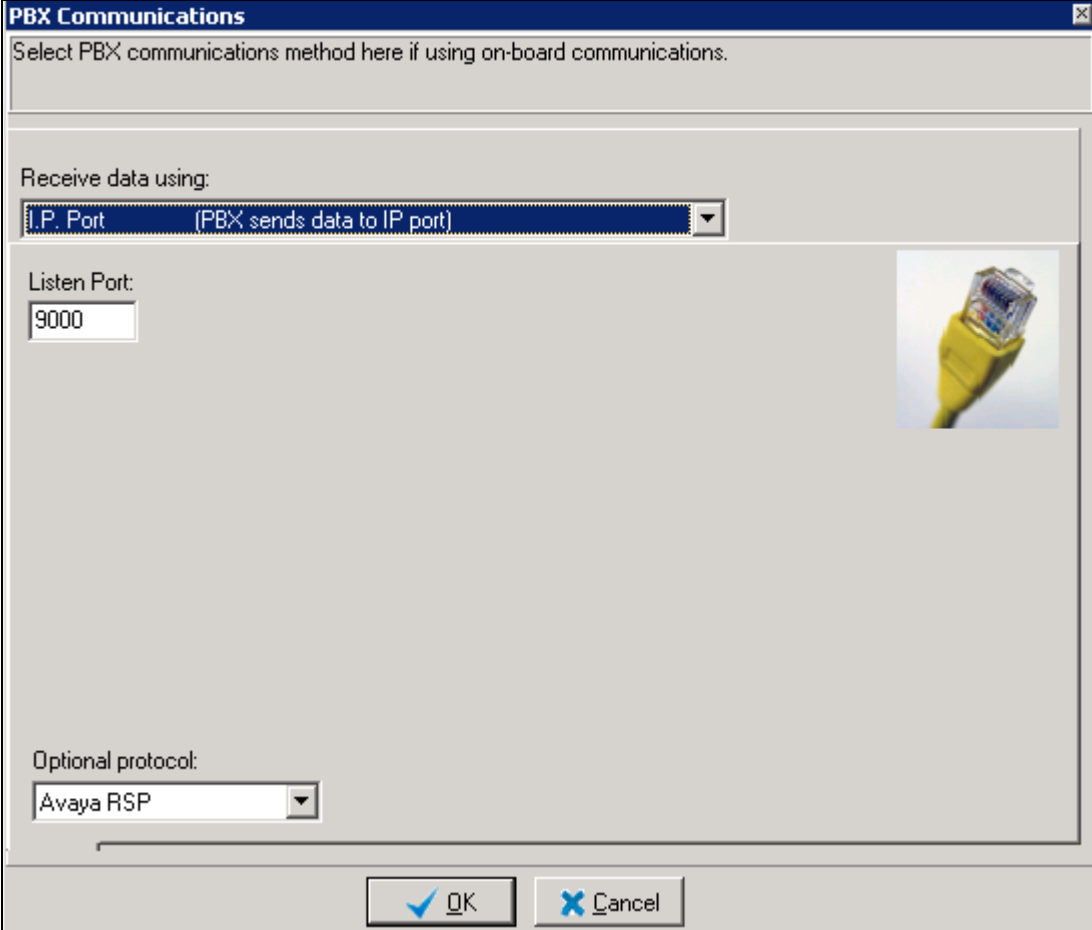
The **Select PBX** screen is displayed next. In the **Select primary PBX** drop-down box select **Avaya CM S Series** and then click **OK**.



Select **PBX → PBX Communications...** from the top menu of the **OfficeWatch XT Telemanagement 2016 – AVAYA DEVCONNECT TEST DEMO** screen (not shown). Enter the following values for the specified fields.

- **Receive data using:** *I.P. Port (PBX sends data to IP port)*
- **Listen Port:** The remote port number from **Section 5.2**
- **Optional protocol:** *Avaya RSP*

Click **OK** when finished.



PBX Communications

Select PBX communications method here if using on-board communications.

Receive data using:
I.P. Port (PBX sends data to IP port)

Listen Port:
9000

Optional protocol:
Avaya RSP

OK Cancel

On the **OfficeWatch XT Telemanagement 2016 – AVAYA DEVCONNECT TEST DEMO** screen, select **PBX → Select PBX...** from the top menu (not shown). Click the **Modify PBX Settings...** button (not shown).

The **Modify PBX – Avaya CM S Series** screen is displayed. Note that in a live customer environment, CDR data may start appearing in the top portion of the screen. Select the **Outgoing** tab.

For **Extension Length**, enter the maximum number of digits used for internal extensions on Communication Manager. As the calling number field in the CDR record is right-justified and ends at position 42, adjust the **Extension Pos** value accordingly. In the compliance testing, calling numbers with 5-digit extensions appear in position 38-42 in the CDR records.

For **Digits**, enter “18” for **Pos** and “16” for **Length** as shown below. This will match to any number in the dialed number field in position 18-33 of the CDR record.

Retain the default values in the remaining fields.

Modify PBX - Avaya CM S Series

Avaya CM S Series ☐ Show live cursor ☐ Column View ☐ Show newest CDR

Data Received from PBX Position = 15

Time	Pos	Format	Extension	Pos	Length
00:00 02/09	1	3) hhmm	38	5	
09:26 02/09	1	26) Use Today's Date	18	16	
10:27 02/09	5	14) hmnt(tenths)	14	4	

Use out trigger file on:

Select the **Incoming** tab. For **Extension Length**, enter the maximum number of digits used for the internal extensions on Communication Manager. The dialed number field in the CDR record is right-justified and ends at position 32, adjust the **Extension Pos** value accordingly. In the compliance testing, dialed numbers with 5-digit extensions appear in position 28-32 in the CDR records.

For **Digits**, enter “33” for **Pos** and “11” for **Length** as shown below. This will match to any number in the calling number field in position 33-43 of the CDR record.

Retain the default values in the remaining fields.

Modify PBX - Avaya CM S Series

Avaya CM S Series ☐ Show live cursor ☐ Column View ☐ Show newest CDR

Data Received from PBX

Time	Pos	Format	Extension	Pos	Length
00:00 02/09					
09:26 02/09					
10:27 02/09					
10410007C	561025149626104	1001	0	#004	0
10410003C	561015149626104	1001	0	#004	0
10440006C	562045149626104	1001	0	#004	0
10440003C	56202 56204	8888	1001	0	#001
105100047	6E004 15149626104 56102	1	0194	0	M00
10530000E	6 15149626104 56102	1	0	0	000
105500027	6E004 15149626104 56102	1	0214	0	M00

Outgoing Incoming Model Filters Translations Misc. Site Assignments CDR Filter Aux 1 Aux 2

Time: Pos: 1 Format: 3) hhmm Extension: Pos: 28 Length: 5

Date: Pos: 1 Format: 26) Use Today's Date Digits: Pos: 33 Length: 11

Duration: Pos: 5 Format: 14) hmm(tenths) Trunk: Pos: 79 Length: 4

Call is incoming if: Pos: 33 Text: doesn't contain ~

Pos: 41 Text: contains ~

Incoming if short field: Pos: 0 Length: 0 Min Digits: 0 Exception list:

Use in trigger file on: Pos: 0 Length: 0

Basic Fields Extended Fields Stages Filters

6.2. Administer Customization

From the **OfficeWatch XT Telemanagement 2016 – AVAYA DEVCONNECT TEST DEMO** screen shown in **Section 6.1**, select **Setup → Call Processing Options...** from the top menu to display the **Call Processing Options** screen.

Check **Process Incoming calls** and **Process extension-to-extension (internal) calls**, if desired. Set the appropriate value for **Maximum Internal Extension Length**, and retain the default values in the remaining fields. The screenshot below shows the settings used for the compliance testing.

Call Processing Options

Various features for processing calls can be enable or disabled in this screen depending on specific needs. For multi-site operation, each site may be configured independently from other sites.

Processing | Rounding | Translations | Misc.

- ☒ Process Incoming calls
- ☐ Charge Incoming calls
- ☒ Process free calls
- ☒ Process extension-to-extension (internal) calls
 - Maximum Internal Extension Length:
- ☐ Mirror and store both sides of internal calls

☐ Centralize billing sites

Multi Site Options:

Load from Site: Apply to Site:

6.3. Administer Grace Periods

From the **OfficeWatch XT Telemanagement 2016 – AVAYA DEVCONNECT TEST DEMO** screen shown in **Section 6.1**, select **Setup → Grace Periods...** from the top menu to display the **Grace Periods** screen. Modify the grace period value for each type of call if desired. Note that calls with duration shorter than the grace period will not be logged. The screenshot below shows the settings used for the compliance testing. The value of “1” was used during compliance testing.

Grace Periods

Calls which are shorter than the grace period are ignored and usually indicate busy or ring-out calls.

Grace Periods

Internal: 1 seconds

Local: 1 seconds

Local Toll: 1 seconds

In-State: 1 seconds

Long Distance: 1 seconds

International: 1 seconds

Multi Site Options:

Load from Site: Primary Site

Apply to Site: Primary Site

Apply

OK Cancel

7. Verification Steps

This section provides tests that can be performed to verify proper configuration of Communication Manager and OfficeWatch XT.

7.1. Verify Avaya Aura® Communication Manager

The CDR status of Communication Manager can be checked by running the **status cdr-link** command. The **Link State** should be **up** as shown below.

status cdr-link	
CDR LINK STATUS	
Primary	Secondary
Link State: up	up
Date & Time: 2016/02/09 14:21:44	2016/02/09 11:14:54
Forward Seq. No: 80	80
Backward Seq. No: 0	0
CDR Buffer % Full: 0.00	0.00
Reason Code: OK	OK

The primary CDR link can be disabled with the command **busyout cdr-link primary** and enabled with the command **release cdr-link primary** as shown below.

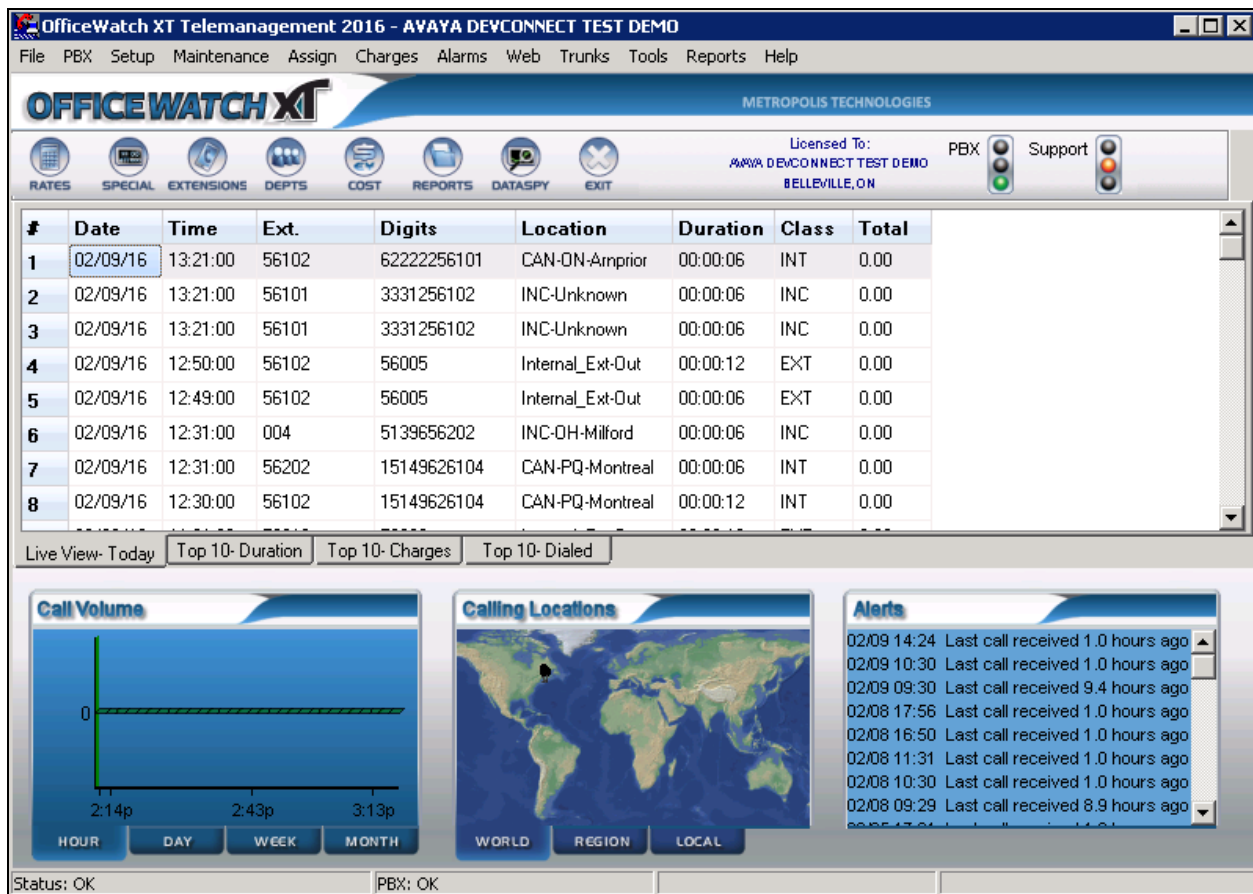
busyout cdr-link primary				
COMMAND RESULTS				
Port	Maintenance Name	Alt. Name	Result	Error Code
	PRI-CDR		PASS	

release cdr-link primary				
COMMAND RESULTS				
Port	Maintenance Name	Alt. Name	Result	Error Code
	PRI-CDR		PASS	

7.2. Verify Metropolis OfficeWatch XT

Make and complete a few phone calls, including internal calls, inbound calls from the PSTN, and outbound calls to the PSTN.

From the **OfficeWatch XT Telemanagement 2016 – AVAYA DEVCONNECT TEST DEMO** screen verify that an entry is displayed for each completed call.



8. Conclusion

These Application Notes describe the steps required to configure Metropolis OfficeWatch XT to interoperate with Avaya Aura® Communication Manager R7.0, including establishing a CDR link with Avaya Reliable Session Protocol (RSP) enabled and capturing/processing call records. All feature and serviceability test cases described in **Section 2.1** were passed with the observations pointed in **Section 2.2**.

9. Additional References

This section references the product documentation relevant to these Application Notes.

Product documentation for Avaya products may be found at <http://support.avaya.com>.

Avaya

1. *Implementing Avaya Aura® Session Manager* Document ID 03-603473.
2. *Administering Avaya Aura® Session Manager*, Doc ID 03-603324.
3. *Deploying Avaya Aura® System Manager*, Release 7.0.
4. *Administering Avaya Aura® System Manager for Release 7.0*, Release 7.0.
5. *Quick Start Guide to Using the Avaya Aura® Media Server with Avaya Aura® Communication Manager*.
6. *Deploying and Updating Avaya Aura® Media Server Appliance*, Release 7.7.
7. *Administering Avaya Aura® Communication Manager*, Release 7.0, 03-300509.
8. *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 7.0, 555-245-205.

Metropolis OfficeWatch Call Accounting User Guide, available at <http://www.metropolis.com>.

©2016 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.