



Avaya Solution & Interoperability Test Lab

Application Notes for Noble Systems Contact Center Solution with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using SIP Trunks – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Noble Systems Contact Center Solution to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using SIP trunks.

Noble Systems Contact Center Solution is a unified customer interaction management solution. In the compliance testing, Noble Systems Contact Center Solution used SIP trunks to Avaya Aura® Session Manager for dedicated connections with agents, and for calls with the PSTN.

Readers should pay attention to Section 2, in particular the scope of testing as outlined in Section 2.1 as well as any 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 configuration steps required for Noble Systems Contact Center Solution to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using SIP trunks.

Noble Systems Contact Center Solution is a unified customer interaction management solution for multimedia business environments that combines outbound predictive dialing and inbound with blended call management. In the compliance testing, Noble Systems Contact Center Solution used SIP trunks to Avaya Aura® Session Manager for dedicated connections with agents, and for calls with the PSTN.

Noble Systems Contact Center Solution agents are administered as regular station users on Avaya Aura® Communication Manager, with desktop computers running the web-based or client version of Noble Systems Composer to perform ACD related activities such as login/logout and answer/drop calls. All ACD functionalities are provided by Noble Systems Contact Center Solution.

Noble Systems Contact Center Solution can support direct trunk connection to the PSTN or via a PBX. In the compliance testing, the connection with the PSTN for inbound/outbound calls was accomplished via Avaya Aura® Communication Manager. Inbound calls were routed by Avaya Aura® Communication Manager to Avaya Aura® Session Manager and then to Noble Systems Contact Center Solution. Noble Systems Contact Center Solution delivered the inbound calls to available agents by merging the talk paths of the inbound calls from the PSTN with the dedicated connections to the agents. Outbound calls were initiated by Noble System Contact Center Solution to Avaya Aura® Communication Manager via Avaya Aura® Session Manager, and Noble Systems Contact Center Solution delivered the answered outbound calls to available agents by merging the talk paths.

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Outbound calls were automatically launched by Contact Center Solution, whereas the inbound calls were manually made. Call controls were performed from the agent desktops or telephones to verify the various call scenarios.

The serviceability test cases were performed manually by disconnecting and reconnecting the Ethernet cables to Contact Center Solution.

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 test included feature and serviceability testing.

The feature testing included G.711MU, G.729, codec negotiation, DTMF, blind/attended transfer, blind/attended conference, inbound, outbound, and multiple agents.

The serviceability testing focused on verifying the ability of Contact Center Solution to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connections to Contact Center Solution.

2.2. Test Results

All test cases were executed and verified. The following were the observations on Contact Center Solution from the compliance testing.

- Contact Center Solution does not support media shuffling. Therefore corresponding parameters must be disabled on the relevant signaling group and network region.
- The transfer-to and conference-to agents do not receive screen updates associated with the call. Furthermore, there isn't a way for the conference-to agent to initiate a drop from the active conference call.
- The conference-from agent will see a "hang up during transfer" pop-up message, whenever the user or agent drops first from a conference call.
- PSTN user in the conference call with 2 Noble agents, if PSTN user hangs up the call, the conference call will be disconnected on all agents.
- Agent will see a "hang up during transfer" pop-up message whenever PSTN or Agent drop the call during call is put on hold.
- If Agent hangs up a call that is on hold, after reconnect agent deskphone with Composer, agent need to manually change status from Paused to Connected on Composer.

- No blind transfer support to internal or external number. Blind transfer only support for call transferred from Agent to Agent.
- Unplug agent's PC, NobleWinAgent will not response to the mouse and pop-up a window say: "Unable to connect appserver or dbserver" after plug LAN cable back, need to reboot and everything is work as normal.

2.3. Support

Technical support on Contact Center Solution can be obtained through the following:

- **Phone:** (888) 966-2539
- **Web:** <http://www.noblesys.com/contact.aspx>
- **Email:** info@noblesys.com

3. Reference Configuration

Contact Center Solution consists of multiple servers, and the compliance testing used a two-server configuration with the Composer Web Server component running on a separate server.

SIP trunks are used from Contact Center Solution to Session Manager, to reach users on Communication Manager and on the PSTN.

A five digit Uniform Dial Plan (UDP) was used to facilitate dialing with Contact Center Solution. Unique extension ranges were associated with Communication Manager Users (56xxx), and Contact Center Solution (52xxx).

The detailed administration of basic connectivity between Communication Manager and Session Manager is not the focus of these Application Notes and will not be described.

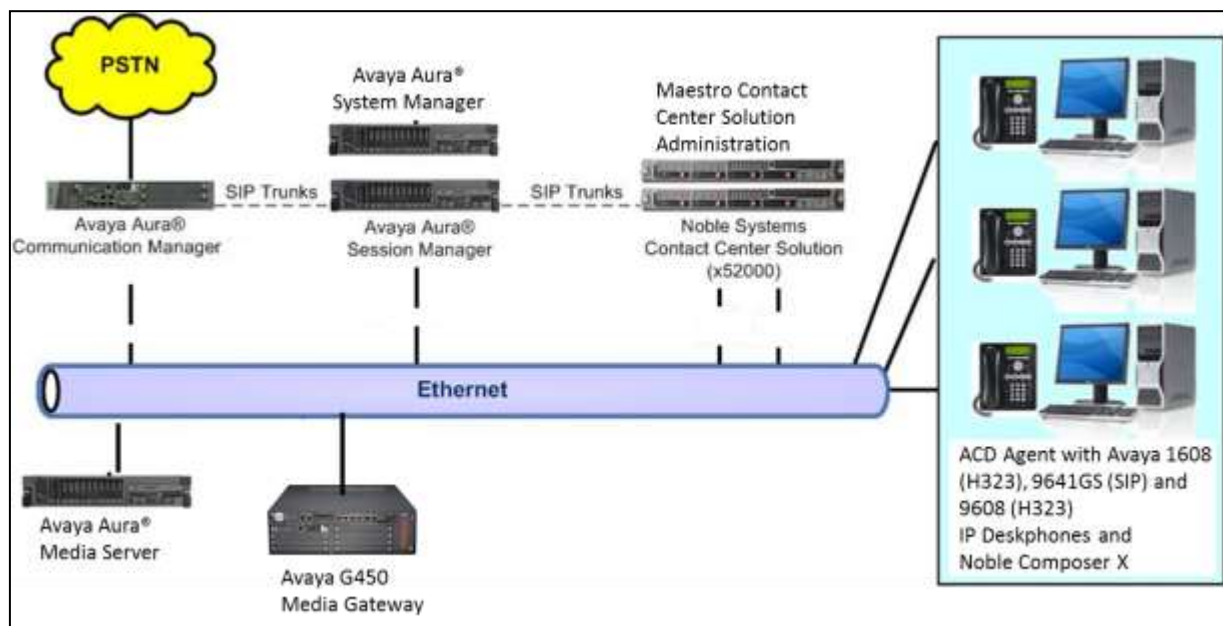


Figure 1: Noble Systems Contact Center Solution with Avaya Aura® Communication Manager and Avaya Aura® Session Manager

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 in Virtual Environment	R017x.00.0.441.0 7.0.1.0.0-FP1
Avaya G450 Media Gateway	37.19.0
Avaya Aura® Media Server in Virtual Environment	7.7.019 (FP1)
Avaya Aura® System Manager running on Virtualized Environment	7.0.1.0
Avaya Aura® Session Manager running on Virtualized Environment	7.0.1.0.701007
Avaya 9641G, IP Deskphone (SIP)	7.0.1
Avaya 9608 IP Deskphone (H.323)	6.6029
Avaya 1608-I IP Deskphones (H.323)	1.3 Release 9
The Noble Enterprise Contact Solution on CentOS	Version 10 6.7
Maestro Contact Center Solution Administration on Windows Server 2012 R2	Version 8.1 R2 64bit
Composer X Agent Desktop and Designer on Windows 10 Pro	version 3.1 2015 32Bit

5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager. The procedures include the following areas:

- Verify license
- Administer system parameters features
- Administer SIP trunk group
- Administer SIP signaling group
- Administer SIP trunk group members
- Administer IP network region
- Administer IP codec set
- Administer route pattern
- Administer private numbering
- Administer uniform dial plan
- Administer AAR analysis
- Administer ISDN trunk group
- Administer tandem calling party number

In the compliance testing, a separate set of codec, network region, trunk group, and signaling group were used for integration with Noble Systems.

5.1. Verify License

Log into the System Access Terminal (SAT) to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the “display system-parameters customer-options” command. Navigate to **Page 2**, and verify that there is sufficient remaining capacity for SIP trunks by comparing the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column.

The license file installed on the system controls the maximum permitted. If there is insufficient capacity, contact an authorized Avaya sales representative to make the appropriate changes.

display system-parameters customer-options		Page 2 of 11
OPTIONAL FEATURES		
IP PORT CAPACITIES	USED	
Maximum Administered H.323 Trunks: 12000	10	
Maximum Concurrently Registered IP Stations: 18000	3	
Maximum Administered Remote Office Trunks: 12000	0	
Maximum Concurrently Registered Remote Office Stations: 18000	0	
Maximum Concurrently Registered IP eCons: 414	0	
Max Concur Registered Unauthenticated H.323 Stations: 100	0	
Maximum Video Capable Stations: 18000	1	
Maximum Video Capable IP Softphones: 18000	0	
Maximum Administered SIP Trunks: 24000	20	
Maximum Administered Ad-hoc Video Conferencing Ports: 24000	0	
Maximum Number of DS1 Boards with Echo Cancellation: 522	0	

5.2. Administer System Parameters Features

Use the “change system-parameters features” command to allow for trunk-to-trunk transfers.

For ease of interoperability testing, the **Trunk-to-Trunk Transfer** field was set to “all” to enable all trunk-to-trunk transfers on a system wide basis. Note that this feature poses significant security risk, and must be used with caution. For alternatives, the trunk-to-trunk feature can be implemented on the Class Of Restriction or Class Of Service levels. Refer to [1] for more details.

```
change system-parameters features                               Page 1 of 19
      FEATURE-RELATED SYSTEM PARAMETERS
      Self Station Display Enabled? n
      Trunk-to-Trunk Transfer: all
      Automatic Callback with Called Party Queuing? n
Automatic Callback - No Answer Timeout Interval (rings): 3
      Call Park Timeout Interval (minutes): 10
      Off-Premises Tone Detect Timeout Interval (seconds): 20
      AAR/ARS Dial Tone Required? y

      Music (or Silence) on Transferred Trunk Calls? no
      DID/Tie/ISDN/SIP Intercept Treatment: attd
Internal Auto-Answer of Att'd-Extended/Transferred Calls: transferred
      Automatic Circuit Assurance (ACA) Enabled? n

      Abbreviated Dial Programming by Assigned Lists? n
      Auto Abbreviated/Delayed Transition Interval (rings): 2
      Protocol for Caller ID Analog Terminals: Bellcore
Display Calling Number for Room to Room Caller ID Calls? n
```


5.3. Administer SIP Trunk Group

Use the “add trunk-group n” command, where “n” is an available trunk group number, in this case “52”. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Type:** “sip”
- **Group Name:** A descriptive name.
- **TAC:** An available trunk access code.
- **Service Type:** “tie”

add trunk-group 52		Page 1 of 21	
TRUNK GROUP			
Group Number: 52	Group Type: sip	CDR Reports: y	
Group Name: Noble Systems	COR: 1	TN: 1	TAC: 1052
Direction: two-way	Outgoing Display? n		
Dial Access? n	Night Service:		
Queue Length: 0			
Service Type: tie	Auth Code? n		
	Member Assignment Method: auto		
	Signaling Group:		
	Number of Members: 0		

Navigate to Page 3, and enter “private” for Numbering Format.

add trunk-group 52		Page 3 of 21	
TRUNK FEATURES			
ACA Assignment? n	Measured: none	Maintenance Tests? y	
Numbering Format: private			
UUI Treatment: service-provider			
Replace Restricted Numbers? n			
Replace Unavailable Numbers? n			

5.4. Administer SIP Signaling Group

Use the “add signaling-group n” command, where “n” is an available signaling group number, in this case “52”. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Type:** “sip”
- **Transport Method:** “tls”
- **Near-end Node Name:** An existing C-LAN node name or “procr” in this case.
- **Far-end Node Name:** The existing Session Manager node name.
- **Near-end Listen Port:** An available port for integration with Noble Systems.
- **Far-end Listen Port:** The same port number as in **Near-end Listen Port**.
- **Far-end Network Region:** An existing network region to use with Noble Systems.
- **Far-end Domain:** The applicable domain name for the network.

For **Direct IP-IP Audio Connections**, enter “n” since Noble Systems does not support shuffling.

add signaling-group 52		Page 1 of 1
SIGNALING GROUP		
Group Number: 52	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n	SIP Enabled LSP? n	
IP Video? n	Enforce SIPS URI for SRTP? y	
Peer Detection Enabled? y	Peer Server: Others	
Near-end Node Name: procr	Far-end Node Name: SM-VM	
Near-end Listen Port: 5061	Far-end Listen Port: 5061	
	Far-end Network Region: 7	
Far-end Domain: bvwdev.com	Far-end Secondary Node Name:	
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? n	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
Alternate Route Timer(sec): 6		

5.5. Administer SIP Trunk Group Members

Use the “change trunk-group n” command, where “n” is the trunk group number from **Section 5.3**. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Signaling Group:** The signaling group number from **Section 5.4**.
- **Number of Members:** The desired number of members, in this case “10”.

add trunk-group 52		Page 1 of 21	
TRUNK GROUP			
Group Number: 52	Group Type: sip	CDR Reports: y	
Group Name: Noble Systems	COR: 1	TN: 1	TAC: 1052
Direction: two-way	Outgoing Display? n		
Dial Access? n	Night Service:		
Queue Length: 0			
Service Type: tie	Auth Code? n		
		Member Assignment Method: auto	
		Signaling Group: 52	
		Number of Members: 10	

5.6. Administer IP Network Region

Use the “change ip-network-region n” command, where “n” is the existing far-end network region number used by the SIP signaling group from **Section 5.4** (For this testing 7 was used).

For **Authoritative Domain**, enter the applicable domain for the network. Enter a descriptive **Name**. Enter “no” for **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio**, as shown below. For **Codec Set**, enter an available codec set number for integration with Noble Systems.

change ip-network-region 7

Page1 of 20

IP NETWORK REGION

Region: 7

Location: 1

Authoritative Domain: bvwdev.com

Name: Noble Systems

MEDIA PARAMETERS

Codec Set: 7

Intra-region IP-IP Direct Audio: no

Inter-region IP-IP Direct Audio: no

UDP Port Min: 2048

UDP Port Max: 3329

IP Audio Hairpinning? n

DIFFSERV/TOS PARAMETERS

Call Control PHB Value: 46

Audio PHB Value: 46

Video PHB Value: 26

Navigate to **Page 4**, and specify this codec set to be used for calls with the network region used by the Avaya endpoints and with the PSTN. There are other network regions in the compliance testing; network region “1” is used by the Avaya endpoints, and network region “4” is used with the trunk to the PSTN.

change ip-network-region 7

Page4 of 20

Source Region: 7

Inter Network Region Connection Management

I

M

G

A

t

dst codec direct WAN-BW-limits Video Intervening Dyn A G c

rgn set WAN Units Total Norm Prio Shr Regions CAC R L e

17yNoLimitn

2

3

47

5

6

77all

8

5.7. Administer IP Codec Set

Use the “change ip-codec-set n” command, where “n” is the codec set number from **Section 5.6**. Update the audio codec types in the **Audio Codec** fields as necessary. Note that Noble Systems supports the G.711 and G.729 codec variants. The codec shown below were used in the compliance testing.

change ip-codec-set 7

Page 1 of 2

IP Codec Set

Codec Set: 7

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

5.8. Administer Route Pattern

Use the “change route-pattern n” command, where “n” is an existing route pattern number to be used to reach Noble Systems, in this case “52”. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Pattern Name:** A descriptive name.
- **Grp No:** The SIP trunk group number from **Section 5.3**.
- **FRL:** A level that allows access to this trunk, with 0 being least restrictive.

change route-pattern 52												Page	1 of 3							
Pattern Number: 52												Pattern Name: Noble Systems								
SCCAN? n												Secure SIP? n								
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted					DCS/	IXC							
No			Mrk	Lmt	List	Del	Digits					QSIG								
							Dgts					Intw								
1:	52	0									n	user								
2:												n	user							
3:												n	user							
4:												n	user							
5:												n	user							
6:												n	user							
BCC VALUE												TSC	CA-TSC	ITC	BCIE	Service/Feature	PARM	No.	Numbering	LAR
0		1	2	M	4	W	Request					Dgts		Format						
												Subaddress								
1:	y	y	y	y	y	n	n	rest							none					

5.9. Administer Private Numbering

Use the “change private-numbering 0” command, to define the calling party number to send to Noble Systems. Add an entry for the trunk group defined in **Section 5.3**. In the example shown below, all calls originating from a 5-digit extension beginning with 4 and routed to trunk group 52 will result in a 5-digit calling number. The calling party number will be in the SIP “From” header.

change private-numbering 0					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext	Ext	Trk	Private	Total	
Len	Code	Grp(s)	Prefix	Len	
5	4	52		5	Total Administered: 1
					Maximum Entries: 540

5.10. Administer Uniform Dial Plan

This section provides a sample AAR routing used for routing calls with dialed digits 52xxx to Noble Systems. Note that other methods of routing may be used. Use the “change uniform-dialplan 0” command, and add an entry to specify the use of AAR for routing digits 52xxx, as shown below.

change uniform-dialplan 0					Page 1 of 2
UNIFORM DIAL PLAN TABLE					
					Percent Full: 0
Matching			Insert	Node	
Pattern	Len	Del	Digits	Net Conv Num	
52	5	0		aar n	

5.11. Administer AAR Analysis

Use the “change aar analysis 0” command, and add an entry to specify how to route calls to 52xxx. In the example shown below, calls with digits 52xxx will be routed as an AAR call using route pattern “52” from **Section 5.8**.

change aar analysis 0					Page 1 of 2
AAR DIGIT ANALYSIS TABLE					
Location: all					Percent Full: 2
	Dialed	Total	Route	Call	Node
	String	Min Max	Pattern	Type	Num
52		5 5	52	unku	n
					ANI
					Reqd

5.12. Administer ISDN Trunk Group

Use the “change trunk-group n” command, where “n” is the existing trunk group number used to reach the PSTN, in this case “450”.

Navigate to **Page 3**. For **Modify Tandem Calling Number**, enter “tandem-cpn-form” to allow for the calling party number from Noble Systems to be modified.

change trunk-group 450		Page 3 of 21	
TRUNK FEATURES			
ACA Assignment? n		Measured: none	
		Internal Alert? n	Maintenance Tests? y
		Data Restriction? n	NCA-TSC Trunk Member:
		Send Name: y	Send Calling Number: y
Used for DCS? n		Send EMU Visitor CPN? n	
Suppress # Outpulsing? n	Format: public		
UII IE Treatment: service-provider			
Replace Restricted Numbers? n			
Replace Unavailable Numbers? n			
Send Connected Number: y			
Network Call Redirection: none		Hold/Unhold Notifications? n	
Send UII IE? y		Modify Tandem Calling Number: tandem-cpn-form	
Send UCID? n			
Send Codeset 6/7 LAI IE? y			
DSN Term? n			

5.13. Administer Tandem Calling Party Number

Use the “change tandem-calling-party-num” command, to define the calling party number to send to the PSTN for tandem calls from Noble Systems.

In the example shown below, all calls originating from a 5-digit extension beginning with 5 and routed to trunk group 450 will result in a 10-digit calling number. For **Number Format**, use an applicable format, in this case “pub-unk”.

change tandem-calling-party-num					Page	1 of	8
CALLING PARTY NUMBER CONVERSION							
FOR TANDEM CALLS							
CPN		Trk				Number	
Len	Prefix	Grp(s)	Delete	Insert	Format		
5	4	450		90884	pub-unk		
5	5	450		90884	pub-unk		

6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. The procedures include the following areas:

- Launch System Manager
- Administer locations
- Administer adaptations
- Administer SIP entities
- Administer entity links
- Administer routing policies
- Administer dial patterns

6.1. Launch System Manager

Access the System Manager web interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of the System Manager server. Log in using the appropriate credentials.

The screenshot displays the Avaya Aura System Manager 7.0 login interface. The browser address bar shows the URL `https://devvmsmgr.bvwddev.com/securityserver/UI/Login?or`. The page header includes the Avaya logo and the text "Aura® System Manager 7.0".

On the left side, a disclaimer box contains the following text:

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.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

On the right side, the login form includes:

- User ID:
- Password:
- Log On button
- Reset button

At the bottom right, a box titled "Supported Browsers" lists: Internet Explorer 9.x or 10.x or 11.x or Firefox 36.0, 37.0 or 38.0.

6.2. Administer Locations

In the subsequent screen (not shown), select **Elements > Routing** to display the **Introduction to Network Routing Policy** screen below. Select **Routing > Locations** from the left pane, and click **New** in the subsequent screen (not shown) to add a new location for Noble Systems.

The **Location Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name** and optional **Notes**. In the **Location Pattern** sub-section, click **Add** and enter the applicable **IP Address Pattern**, as shown below. Retain the default values in the remaining fields.

AVAYA
Aura System Manager 7.0

Last logged on at August 1, 2014

Home Routing

Home / Elements / Routing / Locations

Location Details

Commit Cancel

Help ?

General

* Name: Belleville

Notes: Belleville DevConnect Lab

Dial Plan Transparency in Survivable Mode

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

6.3. Administer Adaptations

Select **Routing > Adaptations** from the left pane, and click **New** in the subsequent screen (not shown) to add a new adaptation for Noble Systems.

The **Adaptation Details** screen is displayed. In the **General** sub-section, enter a descriptive **Adaptation name**. For **Module name**, select “DigitConversionAdapter”.

For **Module parameter**, enter “osrcd=bvwdev.com odstcd=bvwdev.com, where “bvwdev.com” is the applicable domain. This will set the source and destination domains for all incoming and outgoing calls for Noble Systems.

The screenshot shows the Avaya Aura System Manager 7.0 interface. The left navigation pane is expanded to 'Routing', and the 'Adaptations' sub-item is selected. The main content area displays the 'Adaptation Details' form. The 'General' tab is active. The 'Adaptation Name' field contains 'For_Noble'. The 'Module Name' dropdown is set to 'DigitConversionAdapter'. The 'Module Parameter Type' dropdown is set to 'Name-Value Parameter'. Below these fields is a table with columns 'Name' and 'Value'. The table contains three rows: 'fromto' with value 'true', 'osrcd' with value 'bvwdev.com', and 'odstd' with value 'bvwdev.com'. At the bottom of the table is a 'Select' dropdown set to 'All'. Below the table are fields for 'Egress URI Parameters' and 'Notes'. The top right of the screen shows the user is logged in as 'Last logged in at August 1, 2016 9:02 AM' and has a 'Log off' button.

Name	Value
fromto	true
osrcd	bvwdev.com
odstd	bvwdev.com

6.4. Administer SIP Entities

Add new SIP entity for Noble Systems.

Select **Routing > SIP Entities** from the left pane, and click **New** in the subsequent screen (not shown) to add a new SIP entity for Noble Systems.

The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **FQDN or IP Address:** The IP address of the Contact Center Solution server.
- **Type:** “Other”
- **Adaptation:** Select the Noble Systems adaptation name from **Section 6.3**.
- **Location:** Select the Noble Systems location name from **Section 6.2**.
- **Time Zone:** Select the applicable time zone.

AVAYA
Aura® System Manager 7.0

Last Logged on at Au

Go...

Home Routing x

Home / Elements / Routing / SIP Entities

SIP Entity Details

Commit Cancel

General

* Name: Noble

* FQDN or IP Address: 10.10.98.28

Type: Other

Notes:

Adaptation: For_Noble

Location:

Time Zone: America/Fortaleza

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

Credential name:

Securable: ☐

Call Detail Recording: none

CommProfile Type Preference:

Loop Detection

Loop Detection Mode: On

Loop Count Threshold: 5

Loop Detection Interval (in msec): 200

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

6.5. Administer Entity Links

Add new entity link for Noble Systems.

Select **Routing > Entity Links** from the left pane, and click **New** in the subsequent screen (not shown) to add a new entity link for IPC. The **Entity Links** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **SIP Entity 1:** The Session Manager entity name, in this case “SM_Noble”.
- **Protocol:** “UDP”
- **Port:** “5060”
- **SIP Entity 2:** The Noble Systems entity name from **Section .**
- **Port:** “5060”
- **Connection Policy:** “Trusted”

The screenshot shows the Avaya Aura System Manager 7.0 interface. The left navigation pane is expanded to 'Routing', and 'Entity Links' is selected. The main area displays the 'Entity Links' configuration page. At the top, there are 'Commit' and 'Cancel' buttons. Below this is a table with columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, DNS Override, and Port. The table contains one entry with the following values: Name: SM_Noble, SIP Entity 1: DevvmSH, Protocol: UDP, Port: 5060, SIP Entity 2: Noble, DNS Override: (unchecked), and Port: 5060. Below the table, there is a 'Select: All, None' dropdown. At the bottom of the page, there are 'Commit' and 'Cancel' buttons.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port
SM_Noble	DevvmSH	UDP	5060	Noble	<input type="checkbox"/>	5060

6.6. Administer Routing Policies

Add new routing policy for Noble Systems.

Select **Routing > Routing Policies** from the left pane, and click **New** in the subsequent screen (not shown) to add a new routing policy for Noble Systems.

The **Routing Policy Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name**.

In the **SIP Entity as Destination** sub-section, click **Select** and select the Noble Systems entity name from **Section 6.4** in the listing (not shown).

Retain the default values in the remaining fields.

AVAYA
Aura System Manager 7.0

Last Logged on at August 1, 2016 9:00 AM
Log off admin

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit Cancel

Help ?

General

* Name: Route_to Noble

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Noble	10.10.98.28	Other	

Time of Day

Add Remove View Gaps/Overlaps

1 Item

Filter: Enable

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	24/7							00:00	23:59	Time Range 24/7

6.7. Administer Dial Patterns

Add a new dial pattern for Noble Systems.

Select **Routing > Dial Patterns** from the left pane, and click **New** in the subsequent screen (not shown) to add a new dial pattern to reach Noble Systems. The **Dial Pattern Details** screen is displayed. In the **General** sub-section, enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Pattern:** A dial pattern to match.
- **Min:** The minimum number of digits to be matched.
- **Max:** The maximum number of digits to be matched.
- **SIP Domain:** The signaling group domain name from **Section 5.4**.
- **Notes:** Any desired description.

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create a new policy for reaching Noble Systems as shown below.

AVAYA
Aura® System Manager 7.0

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

General

* Pattern: 52

* Min: 2

* Max: 36

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: bvwdev.com

Notes: Route call to Noble

Originating Locations and Routing Policies

Add Remove

1 Item

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Belleville	Belleville DevConnect Lab	Route_to_Noble	0	<input type="checkbox"/>	Noble	

Select: All, None

7. Configure Noble Systems Contact Center Solution

This section provides the procedures for configuring Contact Center Solution. The procedures include the following areas:

- Administer domain resolution
- Administer mappings
- Launch Maestro
- Administer calling number
- Administer routing

The configuration of Contact Center Solution is typically performed by Noble Systems technicians. The procedural steps are presented in these Application Notes for informational purposes.

7.1. Administer Domain Resolution

Log in to the Linux shell of the Contact Center Solution server with the appropriate credentials. Navigate to the **/etc** directory. Open the **hosts** file, and add an entry to resolve the network domain of Noble Contact Center Solution Linux server as shown below.

```
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1          localhost
20.32.39.170      sipfort
10.10.97.28       avayafdev1 avayafdev1.noblesys.com
```

7.2. Administer Mappings

Navigate to the `/etc/asterisk` directory. Open the `hannibal.xml` file, and navigate to the stations mapping entry. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Map name:** “AVAYASTations”
- **technology:** “SIP”
- **pattern:** “\b\d{x}\b” where “x” is the number of digits in the station extensions.
- **suffix:** The applicable network domain, in this case “bvwddev.com”.
- **format:** The desired codec, in this case “G729” followed by “ULAW”.

In the compliance testing, the agent station extensions on Communication Manager were “4xxxx”.

```
<?xml version="1.0"?>

<TechnologyMap>
  <!-- The following is a list of examples for the various technology types -->

  <Map name="AVAYASTations" technology="SIP" pattern="\b.*\b" prefix=""
suffix="@135.10.97.228" formats="ULAW|ALAW|GSM" maxNumberOfUses="50"
hannibalChanBeg="-1" hannibalChanEnd="-1" beginningChannelNumber="-1"
endingChannelNumber="-1" supportsInbound="true" supportsOutbound="true" />

</TechnologyMap>
```


7.3. Launch Maestro

From the Contact Center Solution server, launch the Maestro application by double-clicking the **Maestro** icon shown below, which was created as part of installation.



The screen below is displayed. Enter the appropriate credentials.

The image shows the Maestro login screen. At the top, it says 'CUSTOMER CONTACT TECHNOLOGIES' and 'NOBLE SYSTEMS'. Below this, there are fields for 'Username' (containing 'Admin') and 'Password' (containing six dots). There is a checkbox labeled 'Remember Information' which is checked. At the bottom, there are links for 'Change Password', 'Change DSN', 'Login', and 'Cancel'. Below the links, it says 'Maestro - Version: 8.1.3.1' and 'Host: avaya1dev1'.

7.4. Administer Calling Number

The **MANAGER PORTAL** screen is displayed next. Double click on **Campaign Setup** > **Campaign Maintenance** in the left pane.



The **Campaign Maintenance** screen is displayed. Select **JON- Jon Test** and click **Update Campaign**.

Campaign Maintenance - Version: 8.1.3.1

Manage Campaigns

Create a new or update, remove, copy an existing Campaign by selecting a Campaign then pressing the desired action.

CGEN - Composer GEN
DGEN - DCB GEN APPL
GEN - GEN, REGULAR/BLENDED SCHEDULAR
JON - Jon Test
PGEN - generic w/ pc charge
TAT - DIAL TESTING APPLICATION

New Campaign
Update Campaign
Remove Campaign
Copy Campaign

Exit < Back Next > Finish

The **Campaign Maintenance** screen is updated. Select **Dialing Rules** to display the screen below. For **Phone Number**, enter the applicable extension to be used as calling party extension for outbound calls from Noble Systems, in this case “52000”.

Campaign Maintenance - Version: 8.1.3.1

Dialing Rules for Campaign JON

Camp Info	Pacing	Camp Dialing	Camp Holding	Call Back
CB Scan	Screening	Dialing Rules	Disposition	CB Window

Select Campaign Fetch Program:

fetchall - FETCHALL v10.0.5-6

[Launch Dialing Filters \(Fetch\)](#)

Enter ANI To Be Displayed On Customer's Caller ID: (ISDN lines only)

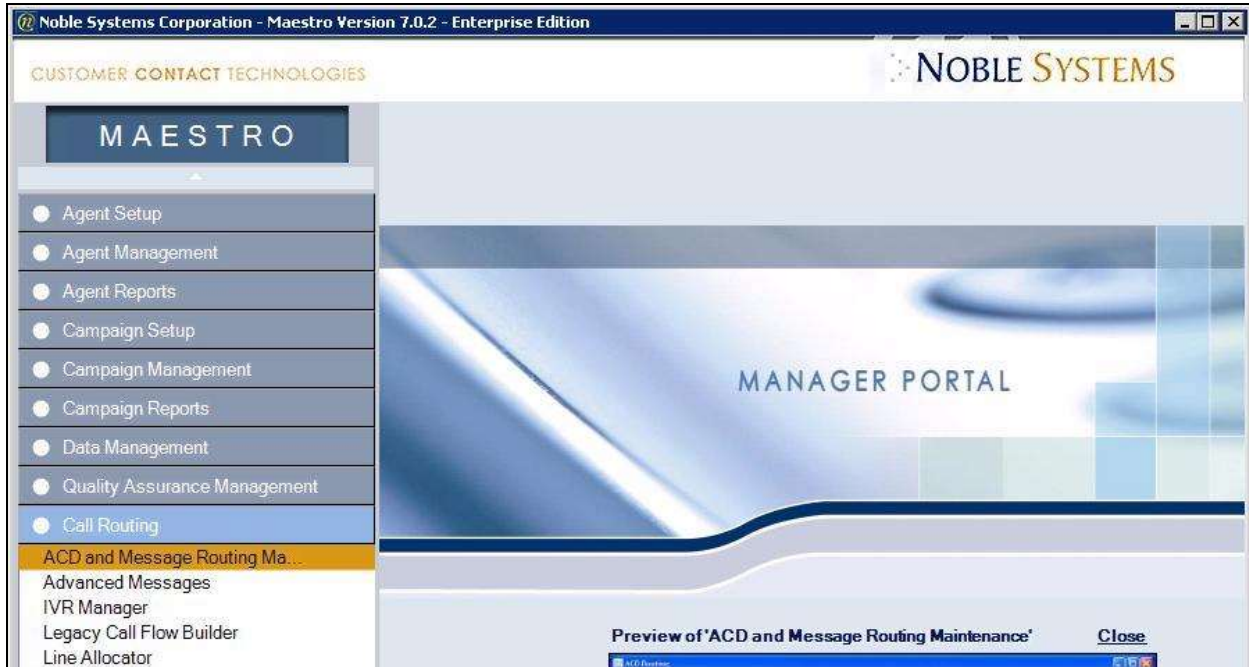
Phone Number 52000

Caller Name

Cancel Finish

7.5. Administer Routing

From the **MANAGER PORTAL** screen, double-click on **Call Routing > ACD and Message Routing Maintenance** from the left pane.



The **ACD Routing** screen is displayed. Select **Add** from the bottom of the screen (not shown) to add a new entry. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **ListId:** A desired and unique value.
- **DNIS:** The assigned Contact Center Solution extension from **Section 4**.
- **Group:** The applicable group number, in this case '1'.
- **Campaign:** "INB"
- **Description:** A desired description.

ACD Routing								
ListId	DNIS	Group	Campaign	Open Message	Closed Message	Description	MaxHold	NextDNIS
▶ 11113	52000	1	JON	2 -	2 -	inbound to g1		
80012563	g2	256	JON	2 -	(None)	Hold Group		
80010991	5556	1	JON	(None)	(None)	DEFAULT OUT...		
80012560	g1	256	JON	2 -	(None)	Hold Group		
11111	5557	2	JON	2 -	(None)	DEFAULT OUT...		
80012562	5559	2	JON	(None)	(None)	DIAL NOW		
11110	5554	1	JON	(None)	(None)	DIAL NOW		
80012561	52001	2	JON	2 -	2 -	inbound to g2		
80020990	g2	99	JON	2 -	(None)	hold		
80010990	g1	99	JON	2 -	(None)	hold		

8. Verification Steps

This section provides tests that can be performed to verify proper configuration of Communication Manager, Session Manager, and Contact Center Solution.

8.1. Verify Avaya Aura® Communication Manager

From the SAT interface, verify the status of the SIP trunk groups by using the “status trunk n” command, where “n” is the trunk group number administered in **Section 5.3**. Verify that all trunks are in the “in-service/idle” state as shown below.

```
status trunk 52
```

TRUNK GROUP STATUS			
Member	Port	Service State	Mtce Connected Ports Busy
0052/001	T00021	in-service/idle	no
0052/002	T00022	in-service/idle	no
0052/003	T00023	in-service/idle	no
0052/004	T00024	in-service/idle	no
0052/005	T00025	in-service/idle	no
0052/006	T00026	in-service/idle	no
0052/007	T00027	in-service/idle	no
0052/008	T00028	in-service/idle	no
0052/009	T00029	in-service/idle	no
0052/010	T00030	in-service/idle	no

Verify the status of the SIP signaling groups by using the “status signaling-group n” command, where “n” is the signaling group number administered in **Section 5.4**. Verify that the signaling group is “in-service” as indicated in the **Group State** field shown below.

```
status signaling-group 52
```

STATUS SIGNALING GROUP	
Group ID:	52
Group Type:	sip
Group State:	in-service

8.2. Verify Avaya Aura® Session Manager

From the System Manager home page (not shown), select **Elements > Session Manager** to display the **Session Manager Dashboard** screen (not shown). Select **Session Manager > System Status > SIP Entity Monitoring** from the left pane to display the **SIP Entity Link Monitoring Status Summary** screen. The **SIP Entity, Entity Link Connection Status** screen is displayed. Verify that **Conn Status** and **Link Status** are “Up”, as shown below.

The screenshot displays the 'SIP Entity, Entity Link Connection Status' page. The left sidebar contains a navigation menu with 'Session Manager' expanded, showing options like Dashboard, Administration, Communication, Profile Editor, Network Configuration, Device and Location Configuration, Application Configuration, and System Status. Under 'System Status', 'SIP Entity Monitoring' is selected. The main content area has a breadcrumb trail: 'Home / Elements / Session Manager / System Status / SIP Entity Monitoring'. The title is 'SIP Entity, Entity Link Connection Status'. Below the title, it states: 'This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.' A link 'All Entity Links to SIP Entity: Noble' is present. A 'Summary View' button is shown. A table displays the connection status for the selected Session Manager, 'DevcomSM'. The table has columns: Session Manager Name, SIP Entity Resolved IP, Port, Proto., Deny, Conn. Status, Reason Code, and Link Status. The row for 'DevcomSM' shows '100.10.98.28', '5060', 'UDP', 'FALSE', 'UP', '200 OK', and 'UP'.

Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
DevcomSM	100.10.98.28	5060	UDP	FALSE	UP	200 OK	UP

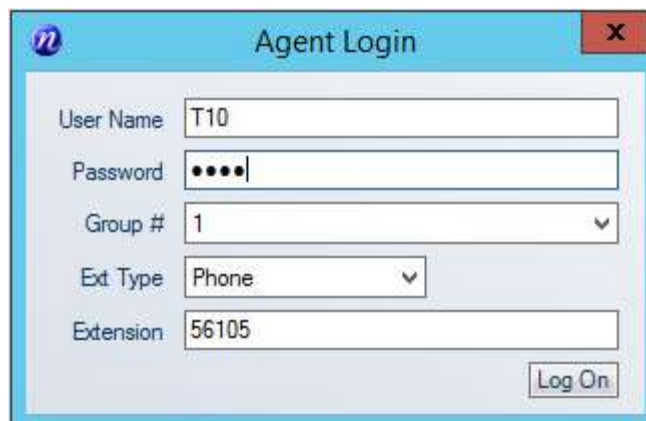
8.3. Verify Noble Systems Contact Center Solution

Prior to verification, start an outbound campaign on Contact Center Solution.

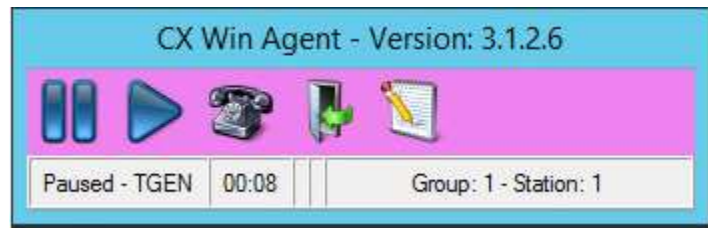
From the agent PC, access the Composer web-based interface by using the URL “http://ip-address/NobleWebAgent” in an Internet browser window, where “ip-address” is the IP address of the Composer Web Server. The **Welcome to Composer 9** screen is displayed. Click **Login**.



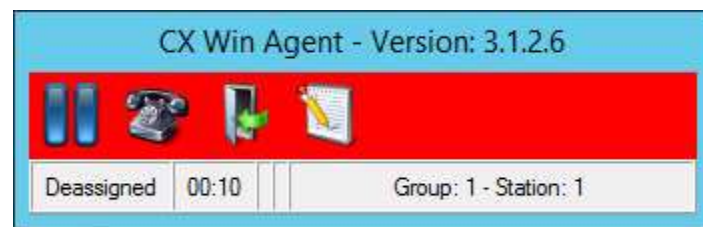
The pop-screen below is displayed. For **User Name** and **Password**, enter the appropriate agent credentials. For **Group**, select the applicable group number, in this case “1”. Select “Other” for **Ext Type**. For **Extension**, enter an available agent station extension from **Section** □, and click **Log On**.



The screen is updated as shown below. Click on the **Resume** icon to log into Contact Center Solution. Verify that Contact Center Solution initiates a dedicated connection to the agent, with the call ringing at the agent's telephone.

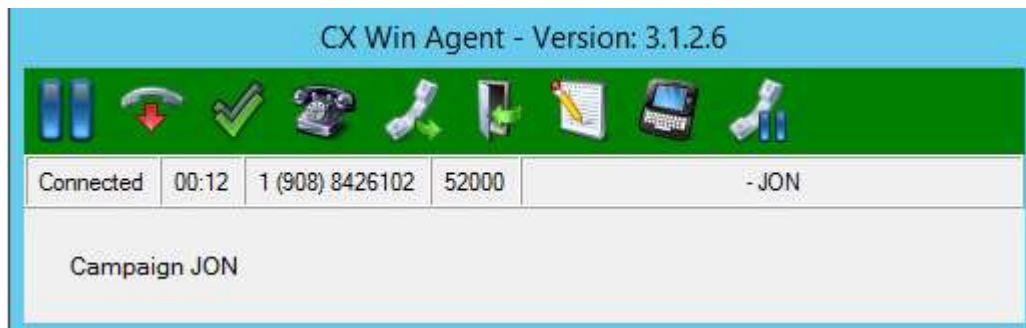


Answer the call at the agent's telephone. Verify that the screen is updated to reflect agent successfully logged into Contact Center Solution, and is waiting for a call, as shown below.



Verify that Contact Center Solution successfully placed an outbound call to a PSTN user, with the call ringing at the PSTN user.

Answer the call at the PSTN user. Verify that the agent is connected to the PSTN user with two-way talk paths, and that the agent screen is updated to reflect the connected call, as shown below.



9. Conclusion

These Application Notes describe the configuration steps required for Noble Systems Contact Center Solution to successfully interoperate with Avaya Aura® Communication Manager using Avaya Aura® Session Manager. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

10. Additional References

This section references the product documentation that is relevant to these Application Notes. Documentation for Avaya products may be obtained via <http://support.avaya.com>.

1. Administering Avaya Aura® Communication Manager, Release 7.0.3, Document 03-300509, Issue 10, June 2016.
2. Administering Avaya Aura® Session Manager, Release 7.0, Issue 7, Jan 2016.
3. *Noble Systems Composer 9 version 2011.1.1 User Manual*, Revised June 27, 2011, available at <http://nobleusersgroup.noblesys.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.