



Avaya Solution & Interoperability Test Lab

Application Notes for Noble Systems Contact Center Solution with Avaya Communication Server 1000 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 Communication Server 1000 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 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 the Noble Systems Contact Center Solution to interoperate with Avaya Communication Server 1000 and Avaya Aura® Session Manager using SIP trunks.

The 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, the Noble Systems Contact Center Solution used SIP trunks to Avaya Aura® Session Manager for calls with the PSTN.

Noble Systems Contact Center Solution agents are administered as regular station users on Avaya Communication Server 1000, 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 functionality is provided by the Noble Systems Contact Center Solution.

The Noble Systems Contact Center Solution can support a 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 Communication Server 1000. Inbound calls were routed by Avaya Communication Server 1000 to Avaya Aura® Session Manager and then to the Noble Systems Contact Center Solution. The 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 the Noble System Contact Center Solution to Avaya Communication Server 1000 via Avaya Aura® Session Manager, and the 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 the 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 the 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.

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

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

For the testing associated with this Application Note, the interface between Avaya systems and the Noble Systems Contact Center Solution did not include use of any specific encryption features as requested by Noble Systems.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

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

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

- 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.
- When a PSTN user is in the conference call with 2 Noble agents, if the PSTN user hangs up the call, the conference call will be disconnected for all agents.
- Agent will see a "hang up during transfer" pop-up message whenever the PSTN or Agent drops the call while the call is on hold.
- There is no blind transfer support to internal or external number. Blind transfer is only supported for calls transferred from Agent to Agent.

2.3. Support

Technical support on the 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

The 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 the Contact Center Solution to Session Manager, to reach users on Communication Server 1000 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 Server Users (54xxx), and Contact Center Solution (54910).

The detailed administration of basic connectivity between Communication Server 1000 and Session Manager is not the focus of these Application Notes and will not be described in this application notes. Refer to Section 10 for reference documents on how to administrate Communication Server 1000 and Session Manager.

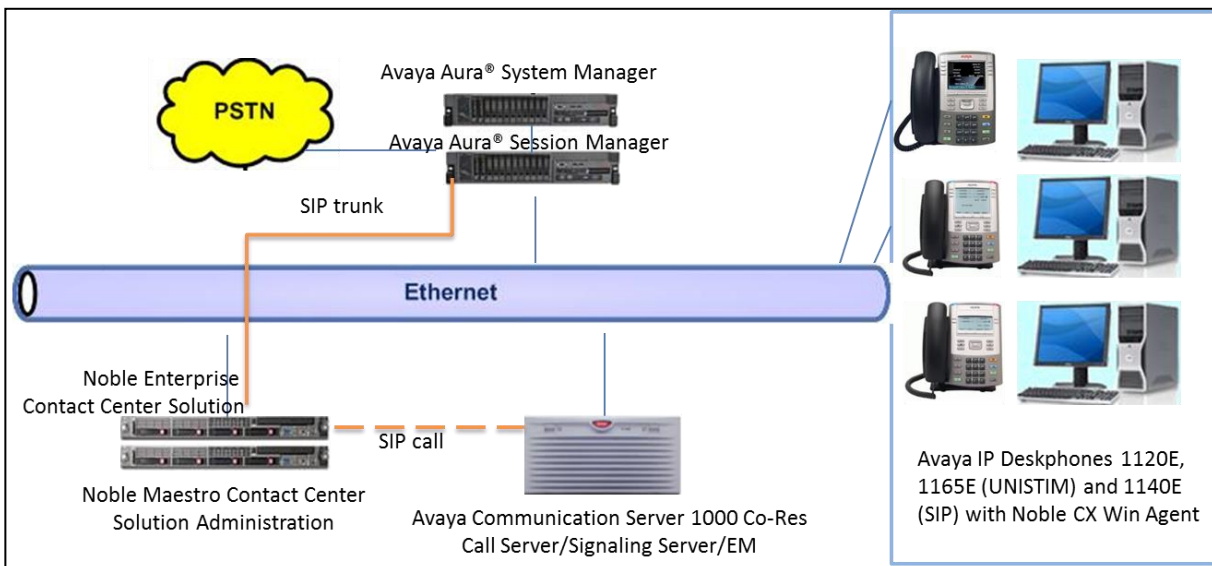


Figure 1: Noble Systems Contact Center Solution with Avaya Communication Server 1000 and Avaya Aura® Session Manager

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Communication Server 1000	7.65P
Avaya Aura® System Manager running on Virtualized Environment	7.1
Avaya Aura® Session Manager running on Virtualized Environment	7.1
Avaya 1140E IP Deskphone (SIP)	4.4.26
Avaya 1120E, 1165E IP Deskphone (UNSTIM)	0625C94
Avaya 1165E IP Deskphones (UNSTIM)	0626C94
Noble Enterprise Contact Center Solution on Linux	Version 10 3.10.0-514.16.1.el7 64bit
Maestro Contact Center Solution Administration on Windows Server 2012 R2	Version 8.3 R2 64bit
CX Win Agent on Windows 10 Pro	version 3.1.16.1 2016 32bit

5. Configure Avaya Communication Server 1000

This section provides the procedures for configuring Communication Server 1000. The procedures include the following areas:

- Launch System Manager
- Verify Communication Server 1000 Node
- Administer Stations

5.1. 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.

System Manager

https://devvmsmgr.bvwdev.com/securityserver/UI/Login?org=dc=nortel,dc=com&go

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.

User ID:

Password:

Log On Reset

Supported Browsers: Internet Explorer 11.x or Firefox 48.0, 49.0 or 50.0.

5.2. Verify Communication Server 1000 Node

In the subsequent screen (not shown), select **Elements** → **Communication Server 1000** to display the Communication Server 1000 Elements page as shown below. Select **EM on cppm3** (where cppm3 is Communication Server 1000's name).

AVAYA

Aura® System Manager 7.1

Configurations

HomeRoutingCommunication Server 1000

Home / Elements / Communication Server 1000

Network

Elements

CS 1000 Services

Corporate Directory

IPSec

Numbering Groups

Patches

SNMP Profiles

Secure FTP Token

Software Deployment

User Services

Administrative Users

External Authentication

SAML Configuration

Password

Security

Roles

Policies

Active Sessions

Host Name: devvmsmgr.bvwdev.com

User Name: admin

Elements

New elements are registered into the security framework, or may be added as simple hyperlinks. Click an element name to launch its manage by entering a search term.

Search

Reset

Add...

Edit...

Delete

	Element Name	Element Type	Release	Address	Description
1	devvmsmgr.bvwdev.com (primary)	Base OS	7.6	10.10.97.226	Base OS element.
2	EM on cppm3	CS1000	7.6	10.10.97.78	New element.
3	cppm3.bvwdev.com (member)	Linux Base	7.6	10.10.97.150	Base OS element.
4	135.10.97.79	Media Gateway Controller	7.6	10.10.97.79	New element.

In the **CS1000 Element Manager** page, select **IP Network → Nodes: Servers, Media Cards**, verify TLAN IP address, this IP will be used to configure Noble system in Section.

Managing: 10.97.78 Username: admin
System » IP Network » IP Telephony Nodes » Node Details

Node Details (ID: 510 - SIP Line, LTPS, PD, Gateway (SIPGw))

Node ID: 510 * (0-9999)

Call server IP address: 10.10.97.78 * TLAN address type: ☒ IPv4 only
☐ IPv4 and IPv6

Embedded LAN (ELAN)
Gateway IP address: 10.10.97.65 *
Subnet mask: 255.255.255.192 *

Telephony LAN (TLAN)
Node IPv4 address: 10.10.97.149 *
Subnet mask: 255.255.255.192 *
Node IPv6 address:

IP Telephony Node Properties

- Voice Gateway (VGW) and Codecs
- Quality of Service (QoS)
- LAN
- SNTP
- Numbering Zones
- MCDN Alternative Routing Treatment (MALT) Causes

Applications (click to edit configuration)

- SIP Line
- Terminal Proxy Server (TPS)
- Gateway (SIPGw)
- Personal Directories (PD)
- Presence Publisher
- IP Media Services

* Required Value. Save Cancel

Associated Signaling Servers & Cards

Server(s) with (hostname-ELAN IP-TLAN IP) not part of the CS1000 or CS1000-HS system where this Call Server belongs: (cppm3-10.97.78-10.97.150)

Select to add Add Remove Make Leader Print Refresh

Hostname	Type	Deployed Applications	ELAN IP	TLAN IPv4	Role
<input type="checkbox"/> cppm3	Signaling_Server	NONE	10.97.78	10.97.150	Leader

Show: ☐ IPv6 address

Note: Only server(s) that are not part of any other IP telephony node and deployed application(s) that match the service(s) selected for this node are available in the servers list.

5.3. Administer Stations

It is assumed that the Communication Server 1000 system is already in place. Please see **Section 11** for an example of 3 stations (54004, 54336 and 54400) configured on Communication Server 1000 and used during the compliance test.

6. Configure Avaya Aura® Session Manager

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

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

6.1. 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.

The screenshot displays the Avaya Aura System Manager 7.1 interface. The top navigation bar includes the Avaya logo and the text "Aura® System Manager 7.1". Below this, there are tabs for "Home" and "Routing". The "Routing" tab is active, and a sub-menu is open showing "Locations" selected. The main content area is titled "Location Details" and contains a "General" section. In the "General" section, there are two input fields: "Name" (containing "Belleville") and "Notes" (containing "Belleville DevConnect Lab"). Below these fields, there is a section titled "Dial Plan Transparency in Survivable Mode" with an "Enabled" checkbox. At the bottom of the form, there are two more fields: "Listed Directory Number" and "Associated CM SIP Entity". The "Associated CM SIP Entity" field has a search icon. The "Commit" and "Cancel" buttons are located in the top right corner of the form area.

6.2. 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 “iosrcd=10.10.98.27 odstcd=10.10.97.228, where “10.10.98.27” is the IP address of the Noble Linux server and 10.10.97.228 is the IP address of Session Manager . This will set the source and destination domains for all incoming and outgoing calls for Noble Systems.

AVAYA
Aura® System Manager 7.1

Configurations

Home / Elements / Routing / Adaptations

Adaptation Details Commit Cancel

General

* **Adaptation Name:** For_Noble

* **Module Name:** DigitConversionAdapter

Module Parameter Type: Name-Value Parameter

Name	Value
fromto	true
iosrcd	10.10.98.27
odstd	10.10.97.228

Select : All, None

6.3. 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 (Linux server).
- **Type:** “Other”
- **Adaptation:** Select the Noble Systems adaptation name from **Section 6.2**.
- **Location:** Select the Noble Systems location name from **Section 6.1**.
- **Time Zone:** Select the applicable time zone.

Home Routing x

Home / Elements / Routing / SIP Entities

SIP Entity Details

Commit Cancel

General

* Name: NobleLinux

* FQDN or IP Address: 10.10.98.27

Type: Other

Notes:

Adaptation: For_Noble

Location:

Time Zone: America/Fortaleza

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

Minimum TLS Version: Use Global Setting

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

Monitoring

SIP Link Monitoring: Use Session Manager Configuration

CRLF Keep Alive Monitoring: Use Session Manager Configuration

Supports Call Admission Control: ☐

6.4. Administer Entity Links

Add a 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, in this case “LinkToNobleLinux”.
- **SIP Entity 1:** The Session Manager entity name, in this case “DevvmSM”.
- **Protocol:** “UDP”
- **Port:** “5060”
- **SIP Entity 2:** The Noble Systems entity name from **Section 6.3**.
- **Port:** “5060”
- **Connection Policy:** “Trusted”

Home / Elements / Routing / Entity Links

Entity Links Commit Cancel

1 Item

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service
<input type="checkbox"/>	* LinkToNobleLinux	* DevvmSM	UDP	* 5060	* NobleLinux	* 5060	<input type="checkbox"/>	trusted	<input type="checkbox"/>

Select : All, None

Commit Cancel

6.5. 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 6.3** in the listing (not shown).

Retain the default values in the remaining fields.

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service
<input type="checkbox"/>	* LinkToNobleLiux	* DevvmSM	UDP	* 5060	* NobleLinux	* 5060	<input type="checkbox"/>	trusted	<input type="checkbox"/>

Select : All, None

6.6. 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:** Select available domain name.
- **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.

Home / Elements / Routing / Dial Patterns

Dial Pattern Details [Commit] [Cancel] [Help ?]

General

* Pattern: 54910

* Min: 5

* Max: 5

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: bvwdev.com

Notes:

Originating Locations and Routing Policies

[Add] [Remove]

1 Item [Filter: Enable]

<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	RouteToNobleLinux	0	<input type="checkbox"/>	NobleLinux	

Select : All, None

7. Configure Noble Systems Contact Center Solution

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

- Administer mappings
- Launch Maestro
- Administer routing

The configuration of the 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 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:** “map1”
- **technology:** “SIP”
- **pattern:** “\b\d{x}\b” where “x” is the number of digits in the station extensions.
- **suffix:** “@10.10.97.149, IP address of Communication Server 1000 in **Section 5.2**.”
- **format:** The desired codec, in this case “ULAW”.

In the compliance testing, the agent station extensions on Communication Server 1000 were “54xxxx”.


```
<Map name="map 1"
technology="SIP"
pattern="\b\d{10}\b|\b\d{11}\b" prefix="" suffix="@10.10.97.149" formats="ULAW"
maxNumberOfUses="10000" beginningChannelNumber="-1" endingChannelNumber="-1"
stripDigits="0" supportsInbound="true" supportsOutbound="true" />
```

7.2. 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.

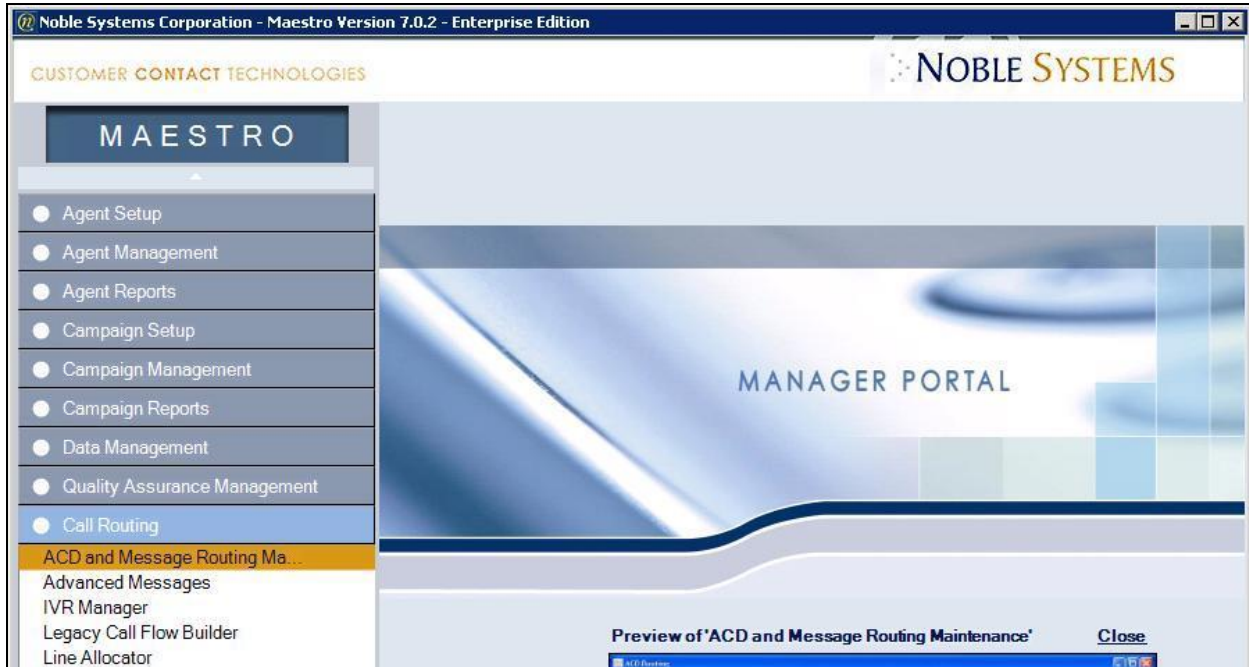


The screen below is displayed. Enter the appropriate credentials.

The image shows the Maestro login screen. At the top, there is a header bar with 'CUSTOMER CONTACT TECHNOLOGIES' on the left and 'NOBLE SYSTEMS' on the right. The main area is a dark blue rectangle with white text. It contains a 'Username' field with 'ADmin' entered, a 'Password' field with five dots, and a 'Remember Information' checkbox. Below these fields are links for 'Change Password' and 'Change DSN'. At the bottom right are 'Login' and 'Cancel' buttons. At the bottom left, it says 'Maestro - Version: 8.3.0.87' and 'Host: avayafort1'.

7.3. 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 group number.
- **Group:** The applicable group number.
- **Campaign:** "TAT"
- **Description:** A desired description.

The screenshot shows the ACD Routing screen with a table of routing entries. The table has the following columns: ListId, DNIS, Group, Campaign, Δ, Open Message, Closed Message, Description, MaxHold, and NextDNIS. The data rows are as follows:

ListId	DNIS	Group	Campaign	Δ	Open Message	Closed Message	Description	MaxHold	NextDNIS
1	1000	1	JON		(None)	(None)	DIAL NOW		
11111	g1	2	TAT		2 -	(None)			
11113	1002	1	TAT		(None)	(None)	DIAL NOW		
11112	1001	1	TAT		(None)	(None)	DEFAULT OUT...		
11114	0000000000	1	TAT		1 -	2 -	Inbound Def		
11115	g2	256	TAT		1 -	2 -	HOLD		

At the bottom of the screen, there are buttons for 'Add', 'Delete', 'Show Voice Mail', 'Message Routing', 'Apply', 'OK', and 'Exit'. The version number '8.3.0' and host 'avayafort1' are also displayed.

8. Verification Steps

This section provides steps that can be performed to verify proper configuration of Communication Server 1000, Session Manager, and the Contact Center Solution.

8.1. Verify Avaya Communication Server 1000

Using PuTTY, enter the IP address of the server to be connected, in this case, it is IP from **Section 5.2**, 10.10.97.149 and click Open.

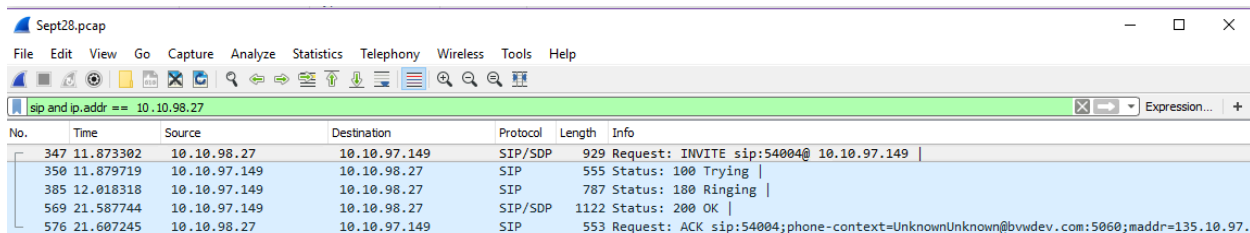
Once in the server, login as admin2 .

Check nettools status by running the command `harden nettools status`.

If status is not enabled then enable it by running the command, `harden nettools on`.

Type: `tcpdump -i any -s 0 -w <out PCAP file>` (<out PCAP file> is desired name of the file which will contain captured packets).

Using WinAgent to connect to agent's phone as described in **Section 8.3**. Below is a wireshark trace that shows that WinAgent successfully connected to Agent's phone extension 54004.

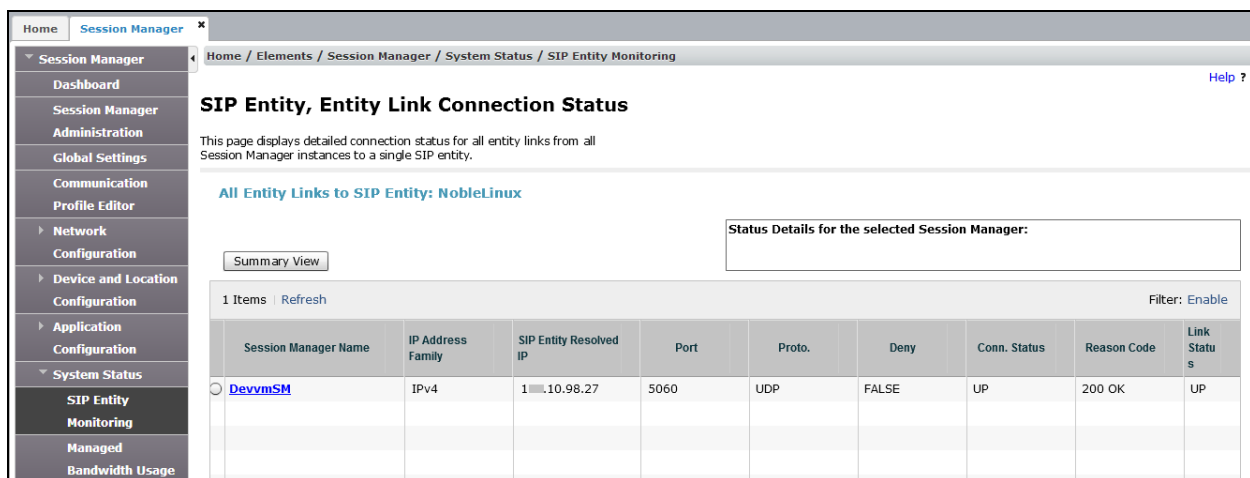


The image shows a Wireshark packet capture window titled 'Sept28.pcap'. The filter is 'sip and ip.addr == 10.10.98.27'. The packet list shows five packets:

No.	Time	Source	Destination	Protocol	Length	Info
347	11.873302	10.10.98.27	10.10.97.149	SIP/SDP	929	Request: INVITE sip:54004@ 10.10.97.149
350	11.879719	10.10.97.149	10.10.98.27	SIP	555	Status: 100 Trying
385	12.018318	10.10.97.149	10.10.98.27	SIP	787	Status: 180 Ringing
569	21.587744	10.10.97.149	10.10.98.27	SIP/SDP	1122	Status: 200 OK
576	21.607245	10.10.98.27	10.10.97.149	SIP	553	Request: ACK sip:54004;phone-context=UnknownUnknown@bvvdev.com:5060;maddr=135.10.97.

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 shows the 'SIP Entity, Entity Link Connection Status' page in the Avaya Session Manager interface. The left navigation pane shows 'Session Manager' expanded, with 'System Status' selected. The main content area shows the 'SIP Entity, Entity Link Connection Status' page for the 'NobleLinux' SIP entity. The page displays a table of entity links with the following data:

Session Manager Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
DevvmSM	IPv4	10.10.98.27	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.

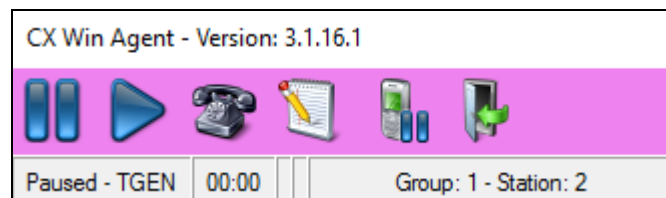
From the agent PC, access the Composer window interface by right click on **NobleWinAgent** icon, select **Run as Administrator**. The **Welcome to Composer X** screen is displayed. Click **Login**.



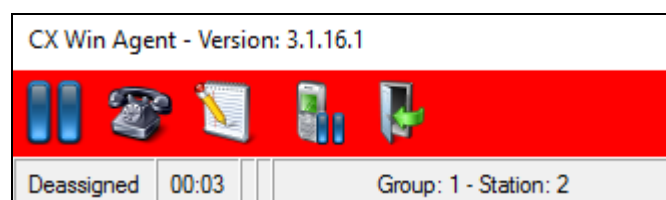
The pop-screen below is displayed. For **User Name** and **Password**, enter the appropriate agent credentials. For **Extension**, enter an available agent station extension from **Section 5.3**, and click **Log On**.

A screenshot of the 'Agent Login' dialog box. It has a title bar with 'Agent Login' and a close button. The form contains the following fields: 'User Name' with the value 'T10', 'Password' with masked characters '•••••', 'Group #' with a dropdown menu showing '1', 'Ext Type' with a dropdown menu showing 'Phone', and 'Extension' with the value '54004'. A 'Log On' button is located at the bottom right of the form.

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.

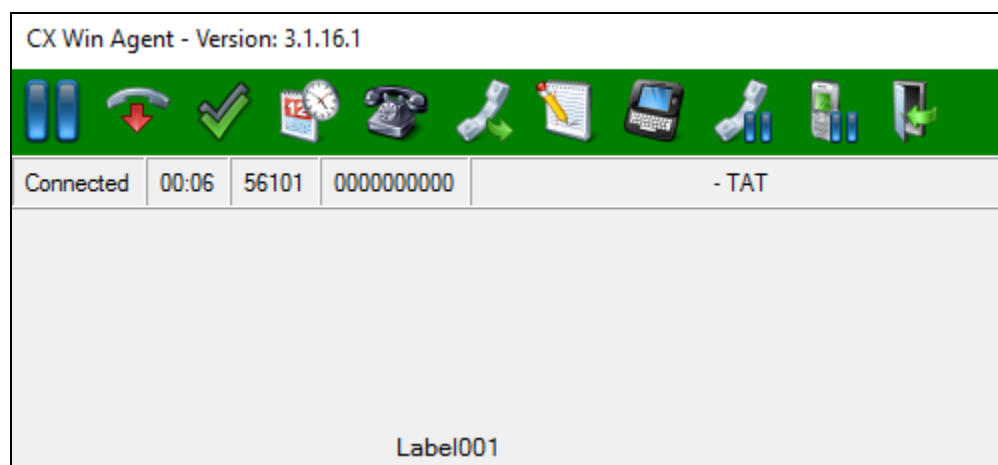


Answer the call at the agent's telephone. Verify that the screen is updated to reflect agent successfully logged into the Contact Center Solution, and is waiting for a call, as shown below.



Verify that the 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 the Noble Systems Contact Center Solution to successfully interoperate with Avaya Communication Server 1000 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. Avaya Communication Server 1000 Co-resident Call Server and Signaling Server Fundamentals Release 7.6 NN43001-509 Issue 04.04 June 2016.
2. Avaya Communication Server 1000 Element Manager System Reference - Administration Release 7.6 NN43001-632 Issue 06.08 November 2016.
3. Avaya Communication Server 1000 SIP Line Fundamentals Release 7.6 N43001-508 Issue 04.04 December 2016.
4. Administering Avaya Aura® Session Manager Release 7.1.1 Issue 2 August 2017.
5. Administering Avaya Aura® System Manager for Release 7.1.1 Release 7.1.1 Issue 6 August 2017.
6. Noble Systems Composer User Manual, available at <http://nobleusersgroup.noblesys.com>.

11. Station details

Station details used during compliance test:

User 1 (SIP) extension 54004

```
REQ: prt
TYPE: uext
TN    104 0 0 3
UXTY
DATE
PAGE
DES

DES   YES
TN    104 0 00 03   VIRTUAL
TYPE UEXT
CDEN  8D
CTYP  XDLC
CUST  0
UXTY  SIPL
MCCL  YES
SIPN  1
SIP3  0
FMCL  0
TLSV  0
SIPU  54004
NDID  510
SUPR  NO
SUBR  DFLT MWI RGA CWI MSB
UXID
NUID
NHTN
CFG_ZONE 00001
CUR_ZONE 00001
MRT
ERL    3
ECL    0
VSIT   NO
FDN    23001
TGAR   1
LDN    NO
NCOS   7
SGRP   0
RNPG   0
SCI    0
SSU
```



```

XLST
SCPW 1234
SFLT NO
CAC_MFC 0
CLS UNR FBD WTA LPR MTD FNA HTD TDD HFD CRPD
    MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
    POD SLKD CCSD SWD LND CNDD
    CFTA SFD MRD DDV CNID CDCA MSID DAPA BFED RCBF
    ICDD CDMD LLCN MCTD CLBD AUTU
    GPUD DPUD DNDD CFXA ARHD CLTD ASCD
    CPFA CPTA ABDD CFHA FICD NAID BUZZ AGRD MOAD
    UDI RCC HBTD AHA IPND DDGA NAMA MIND PRSD NRWD NRCF NROD
    DRDD EXR0
    USMD USRD ULAD CCBD RTDD RBDD RBHD PGND OCBF FLXD FTTC DNDY
DNO3 MCBN
    FDSD NOVD VOLA VOUD CDMR PRED RECD MCDD T87D SBMD ELMD
    MSNV FRA PKCH MWTB DVLD CROD ELCD VMSA
CPND_LANG ENG
RCO 0
EFD
HUNT 23000
EHT
LHK 0
PLEV 02
PUID
UPWD
DANI NO
AST
IAPG 0
AACS NO
ITNA NO
DGRP
MLWU_LANG 0
MLNG ENG
DNDR 0
KEY 00 SCR 54004 0 MARP
    01 HOT U 2654004 MARP 0
    02
    03
    04
    05
    06
    07
    08
    09
    10

```

```
11
12
13
14
15
16
17 TRN
18 AO6
19 CFW 16 23000
20 RGA
21 PRK
22 RNP
23
24 PRS
25 CHG
26 CPN
27
28
29
30
31
DATE 19 DEC 2016
```

User 2 (UNISTIM) extension 54336

```
DES 1140E
TN 096 0 00 23 VIRTUAL
TYPE 1140
CDEN 8D
CTYP XDLC
CUST 0
NUID
NHTN
CFG_ZONE 00001
CUR_ZONE 00001
MRT
ERL 8
ECL 0
FDN
TGAR 1
LDN NO
NCOS 1
SGRP 0
RNPG 1
SCI 0
SSU
XLST
SCPW
```

```

SFLT NO
CAC_MFC 0
CLS_ CTD FBD WTA LPR PUA MTD FND HTD TDD HFD CRPD
      MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
      POD SLKD CCSD SWD LND CNDA
      CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBF
      ICDD CDMD LLCN MCTD CLBD AUTU
      GPUD DPUD DNDA CFXD ARHD CLTD ASCD
      CPFA CPTA ABDD CFHD FICD NAID BUZZ AGRD MOAD
      UDI RCC HBTD AHD IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
      DRDD EXR0
      USMD USRD ULAD CCBF RTDD RBDD RBHD PGND OCBF FLXD FTTC DNDY DNO3
MCBN
      FDSD NOVD VOLA VOUD CDMR PRED RECD MCDD T87A SBMD
      KEM3 MSNV FRA PKCH MUTA MWTD DVLD CROD ELCD VMSA
CPND_LANG ENG
RCO_ 0
HUNT
PLEV 02
PUID
UPWD
DANI NO
AST 00
IAPG 1
AACS NO
ITNA NO
DGRP
MLWU_LANG 0
MLNG ENG
DNDR 0
KEY 00 SCR 54336 0 MARP
      CPND
          CPND_LANG ROMAN
          NAME DN 54008
          XPLN 23
          DISPLAY_FMT FIRST, LAST
01
02
03
04
05
06
07
08 RNP
09
10
11
12
13
14

```

15
16
17 TRN
18 AO6
19
20 RGA
21 PRK
22 RNP
23
24 PRS
25 CHG
26 CPN
27
28
29
30
31

User 3 (UNISTIM) extension 56400

REQ: prt

TYPE: 2050PC

TN 96 0 2 0

DATE

PAGE

DES

MODEL_NAME

EMULATED

KEM_RANGE

DES AGENT

TN 096 0 02 00 VIRTUAL

TYPE 2050PC

CDEN 8D

CTYP XDLC

CUST 0

NUID

NHTN

CFG_ZONE 00001

CUR_ZONE 00001

MRT

ERL 0

ECL 0

FDN

TGAR 1

LDN NO

NCOS 7

SGRP 0

```

RNPG 0
SCI 0
SSU
XLST
SCPW
SFLT NO
CAC_MFC 0
CLS CTD FBD WTA LPR MTD FND HTD TDD HFA CRPD
    MWD LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
    POD SLKD CCSD SWD LND CNDA
    CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBF
    ICDD CDMD LLCN MCTD CLBD AUTU
    GPUD DPUD DNDA CFXD ARHD CNTD CLTD ASCD
    CPFA CPTA ABDD CFHD FICD NAID BUZZ AGRD MOAD
    UDI RCC HBTD AHD IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
    DRDD EXR0
    USMD USRD ULAD CCBF RTDD RBDD RBHD PGND OCBF FLXD FTTC DNDY
DNO3 MCBN
    FDSD NOVD VOLA VOUD CDMR PRED RECD MCDD T87D SBMD
    KEM3 MSNV FRA PKCH MUTA MWTD DVLD CROD ELCD VMSA
CPND_LANG ENG
HUNT
PLEV 02
PUID
UPWD
DANI NO
SPID NONE
AST 00 03
IAPG 0
AACS NO
ITNA NO
DGRP
PRI 01
MLWU_LANG 0
MLNG ENG
DNDR 0
KEY 00 ACD 54901 0 1000
    AGN
    01 NRD
    02 MSB
    03 SCR 54400 0 MARP
        CPND
            CPND_LANG ROMAN
            NAME 54400, Phone
            XPLN 23
            DISPLAY_FMT FIRST, LAST

```

04
05
06
07
08
09
10
11
12
13
14
15
16
17 TRN
18 AO6
19 CFW 16 54405
20 RGA
21 PRK
22 RNP
23
24 PRS
25 CHG
26 CPN
27
28
29
30
31

©2017 Avaya Inc. All Rights Reserved.

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

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