



Avaya Solution & Interoperability Test Lab

Application Notes for Centurion CARES 14.03 with Avaya Aura® Communication Manager 7.1 and Avaya Aura® Session Manager 7.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for the Centurion CARES 14.03 to interoperate with Avaya Aura® Communication Manager 7.1 and Avaya Aura® Session Manager 7.1. Centurion CARES is a contact center solution.

In the compliance testing, Centurion CARES used the SIP trunk interface from Avaya Aura® Session Manager to provide IVR and ACD capabilities.

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 Centurion CARES 14.03 to interoperate with Avaya Aura® Communication Manager 7.1 and Avaya Aura® Session Manager 7.1. CARES is a contact center solution.

In the compliance testing, CARES used the SIP trunk interface from Session Manager to provide IVR and ACD capabilities.

Agents are administered as station users on Communication Manager and have desktops running the Centurion CARES Client application. The CARES Client application is used by agents to log into CARES, to set proper work modes, and to control subsequent calls.

Inbound ACD calls are routed by Communication Manager and Session Manager over the SIP trunk to CARES, with CARES providing relevant IVR call treatment such as greeting announcement and supporting PSTN callers' use of DTMF digits to navigate the menu.

Upon requested by PSTN caller to connect with an agent, CARES determines an available agent for the call, establishes a dedicated audio connection over the SIP trunk with the agent telephone when necessary, and bridges the audio path of the agent connection with the customer connection at CARES. Agents are required to use their desktops to perform all subsequent call controls and ACD related activities. The dedicated audio connections with agents stay in place until agents log out of CARES. All SIP communications on CARES are supported using the Dialogic PowerMedia Host Media Processing (HMP) SIP stack.

CARES also support outbound promotional campaign calls, with outbound calls launched by CARES and with call classifications supported by Dialogic PowerMedia HMP.

2. General Test Approach and Test Results

The feature test cases were performed manually. Incoming calls were made from the PSTN to CARES. DTMF input were manually input from callers for proper IVR navigation and menu selection, including request to connect with an agent. Manual call controls from the CARES Client application were exercised to verify features such as answering and transferring of calls.

The serviceability test cases were performed manually by disconnecting and reconnecting the Ethernet connection to CARES.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

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

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

For the testing associated with these Application Notes, the interfaces between Avaya and Centurion did not include use of any specific encryption features as requested by Centurion.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing included OPTIONS, DTMF, G.711MU, media shuffling, session refresh, ANI, dialing ahead, agent work modes, screen pop, hold/resume, music on hold, mute/unmute, blind/supervised transfer, supervised conference, multiple agents, queuing, internal call, long duration, and outbound campaign calls.

The serviceability testing focused on verifying the ability of CARES to recover from adverse conditions, such as disconnecting and reconnecting the Ethernet connection to CARES.

2.2. Test Results

All test cases were executed, and the following were observations on CARES:

- Depending on the customer network, a delay may need to be added to the beginning of the inbound call flow for PSTN callers to hear the entire greeting announcement. See **Section 7.6** for more details.
- By design, the PSTN calling party number does not populate at the conference-to agent desktop.
- In the serviceability scenario, for an agent that had a call that was dropped during an Ethernet outage to the CARES server, the desktop can no longer be used to answer subsequent calls post server recovery and with agent work state toggled between Idle – Pre-work and Pending ACD Call. When this occurs, the workaround is to manually drop the dedicated connection with CARES from the agent telephone, exit from the CARES Client application and log back in.

2.3. Support

Technical support on CARES can be obtained through the following:

- **Phone:** +1 (262) 317-5678
- **Email:** support@centurioncares.com

3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**. SIP trunk was used between Session Manager and CARES and the applicable domain name was “avaya.com”.

A 5-digits Uniform Dial Plan (UDP) was used to facilitate routing with CARES. Unique extension ranges were assigned to stations users on Communication Manager (6xxxx) and to the CARES main number (54000).

The configuration of Session Manager is performed via the web interface of System Manager. The detailed administration of basic connectivity between Communication Manager, System Manager, and Session Manager is not the focus of these Application Notes and will not be described.

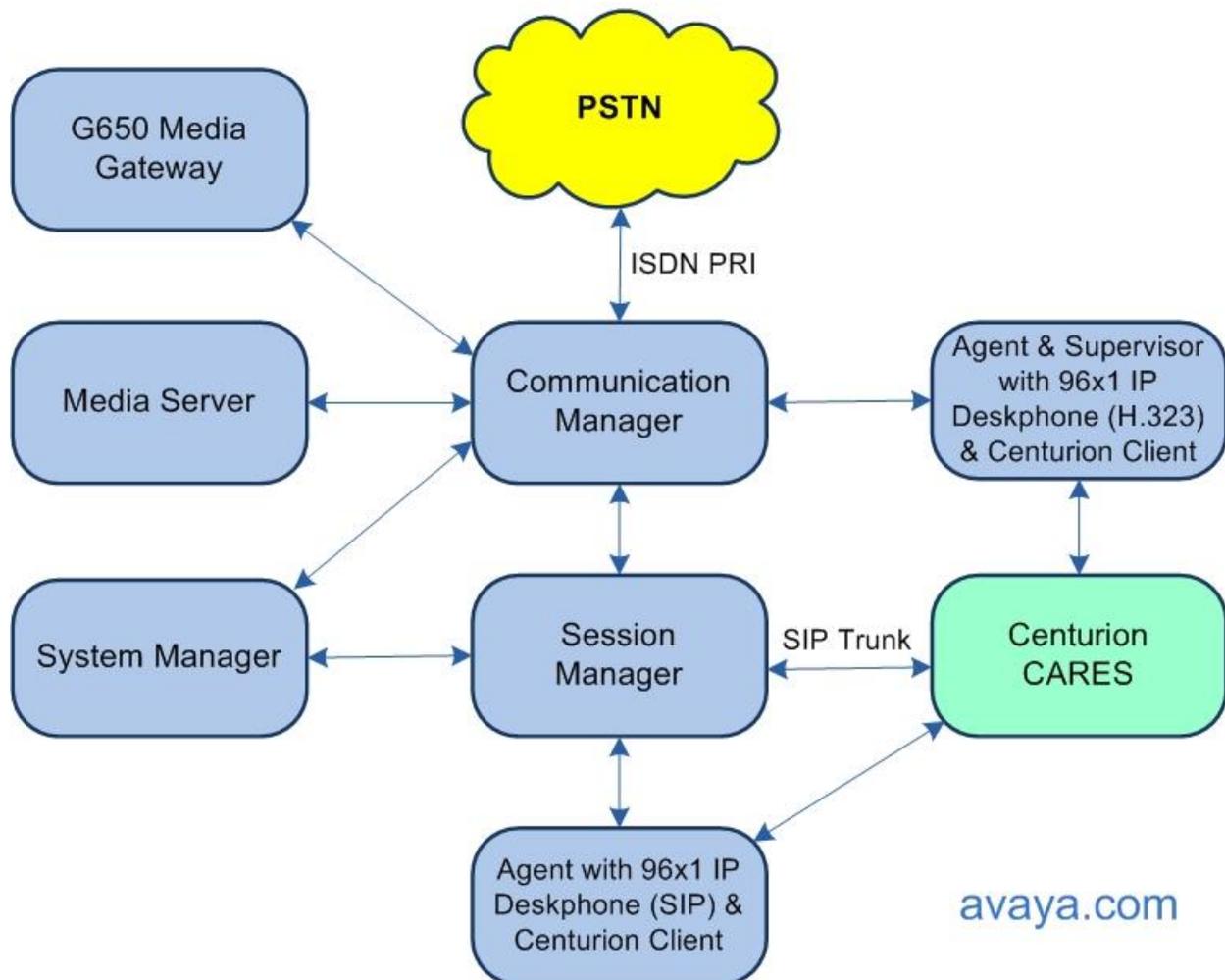


Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager in Virtual Environment	7.1 (7.1.3.3.0.532.25082)
Avaya G650 Media Gateway	NA
Avaya Aura® Media Server in Virtual Environment	8.0.0.205
Avaya Aura® Session Manager in Virtual Environment	7.1 (7.1.3.3.713307)
Avaya Aura® System Manager in Virtual Environment	7.1 (7.1.3.3.069127)
Avaya 9611G & 9641G IP Deskphone (H.323)	6.8202
Avaya 9641G IP Deskphone (SIP)	7.1.6.1.3
Centurion CARES on Microsoft Windows Server 2016 <ul style="list-style-type: none">• Base Package• CARES Server• Dialogic PowerMedia HMP	14.03 Standard 14.03.279 14.03.1720 3.0.395
Centurion CARES Client on Microsoft Windows 10	14.03.1739 Pro

5. Configure Avaya Aura® Communication Manager

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

- Verify license
- Administer node names
- Administer codec set
- Administer network region
- Administer SIP trunk group
- Administer SIP signaling group
- Administer SIP trunk group members
- Administer route pattern
- Administer private numbering
- Administer uniform dial plan
- Administer AAR analysis
- Administer PSTN trunk group
- Administer tandem calling party number

In the compliance testing, the Avaya endpoints used encrypted signaling connections with encrypted media. A separate set of codecs set, network region and network region map were created for integration with CARES.

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 capacity for SIP trunks by comparing the **Maximum Administered SIP Trunks** 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.

<code>display system-parameters customer-options</code>		Page 2 of 12
OPTIONAL FEATURES		
IP PORT CAPACITIES		USED
Maximum Administered H.323 Trunks:	4000	10
Maximum Concurrently Registered IP Stations:	2400	2
Maximum Administered Remote Office Trunks:	4000	0
Max Concurrently Registered Remote Office Stations:	2400	0
Maximum Concurrently Registered IP eCons:	68	0
Max Concur Reg Unauthenticated H.323 Stations:	100	0
Maximum Video Capable Stations:	2400	0
Maximum Video Capable IP Softphones:	2400	3
Maximum Administered SIP Trunks:	4000	50
Max Administered Ad-hoc Video Conferencing Ports:	4000	0
Max Number of DS1 Boards with Echo Cancellation:	80	0

5.2. Administer Node Names

Use the “change node-names ip” command. Note the **Name** and **IP Address** of the processor or existing C-LAN circuit pack that will be used for connectivity to CARES, in this case “procr” and “10.64.150.14”.

Also note the **Name** and **IP Address** of the Session Manager signaling interface, in this case “sm15018” and “10.64.150.18”.

```
change node-names ip                                     Page 1 of 2
                                                    IP NODE NAMES
  Name          IP Address
ams1509        10.64.150.9
cm102201       10.64.102.201
cms15012       10.64.150.12
default        0.0.0.0
ipol15050     10.64.10.50
msgserver      10.64.150.15
procr         10.64.150.14
procr6         ::
sm102204       10.64.102.204
sm15018       10.64.150.18
```

5.3. Administer Codec Set

Administer a codec set for integration with CARES. Use the “change ip-codec-set n” command, where “n” is an existing codec set number to use for interoperability.

For **Audio Codec**, enter the pertinent G.711 variant as shown below. Note that G.711 is the only codec type supported by CARES. For **Media Encryption** and **Encrypted SRTCP**, retain the default values of “none” and “enforce-unenc-srtcp” as shown below. Retain the default values for the remaining fields.

```
change ip-codec-set 4                                   Page 1 of 2
                                                    IP MEDIA PARAMETERS
Codec Set: 4
  Audio          Silence      Frames      Packet
  Codec          Suppression  Per Pkt    Size (ms)
1: G.711MU      n             2           20
2:
3:
4:
5:
6:
7:
  Media Encryption          Encrypted SRTCP: enforce-unenc-srtcp
1: none
```

5.4. Administer Network Region

Administer a network region for integration with CARES. Use the “change ip-network-region n” command, where “n” is an existing network region number to use for interoperability.

Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Authoritative Domain:** The SIP domain from **Section 3**.
- **Name:** A descriptive name.
- **Codec Set:** The codec set number from **Section 5.3**.

```
change ip-network-region 4                                     Page 1 of 20
                                     IP NETWORK REGION
Region: 4              NR Group: 4
Location:              Authoritative Domain: avaya.com
Name: CARES                Stub Network Region: n
MEDIA PARAMETERS      Intra-region IP-IP Direct Audio: yes
Codec Set: 4                Inter-region IP-IP Direct Audio: yes
                        IP Audio Hairpinning? n
UDP Port Min: 2048
UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26
```

Navigate to **Page 4**, and specify the same codec set number to be used for calls with network regions used by Avaya endpoints and by the trunk with the PSTN. In the compliance testing, network region “1” was used by the Avaya endpoints and by the trunk with the PSTN.

```
change ip-network-region 4                                     Page 4 of 20

Source Region: 4      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
1  4   y   NoLimit
2
3
4  4
5
6
7
8
```

5.5. Administer SIP Trunk Group

Use the “add trunk-group n” command, where “n” is an available trunk group number, in this case “54”. 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 54                                     Page 1 of 4
                                     TRUNK GROUP
Group Number: 54                Group Type: sip                CDR Reports: y
  Group Name: SIP trunk to CARES  COR: 1                TN: 1                TAC: 154
  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 54                                     Page 3 of 4
TRUNK FEATURES
  ACA Assignment? n                Measured: none
                                     Maintenance Tests? y

  Suppress # Outpulsing? n  Numbering Format: private
                                     UUI Treatment: service-provider
                                     Replace Restricted Numbers? n
                                     Replace Unavailable Numbers? n
                                     Hold/Unhold Notifications? y
                                     Modify Tandem Calling Number: no

Show ANSWERED BY on Display? y
```

5.6. Administer SIP Signaling Group

Use the “add signaling-group n” command, where “n” is an available signaling group number, in this case “54”. 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:** The processor node name from **Section 5.2**.
- **Far-end Node Name:** The Session Manager node name from **Section 5.2**.
- **Near-end Listen Port:** An available port for integration with CARES.
- **Far-end Listen Port:** The same port number as in **Near-end Listen Port**.
- **Far-end Network Region:** The network region number from **Section 5.4**.
- **Far-end Domain:** The domain name from **Section 3**.

```
add signaling-group 54                                     Page 1 of 2
                                                         SIGNALING GROUP

Group Number: 54                Group Type: sip
IMS Enabled? n                  Transport Method: tls
Q-SIP? n
IP Video? n                      Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y PeerServer: Others
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? n
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? y
Alert Incoming SIP Crisis Calls? n
Near-end Node Name: procr        Far-end Node Name: sm15018
Near-end Listen Port: 5054      Far-end Listen Port: 5054
Far-end Network Region: 4

Far-end Domain: avaya.com

Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate RFC 3389 Comfort Noise? n
DTMF over IP: rtp-payload       Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3 IP Audio Hairpinning? n
Enable Layer 3 Test? y          Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n Alternate Route Timer(sec): 6
```

5.7. Administer SIP Trunk Group Members

Use the “change trunk-group n” command, where “n” is the trunk group number from **Section 5.5**. 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 5.6**.
- **Number of Members:** The desired number of members, in this case “10”.

```
change trunk-group 54                                     Page 1 of 4
                                     TRUNK GROUP
Group Number: 54           Group Type: sip           CDR Reports: y
  Group Name: SIP Trunk to CARES           COR: 1           TN: 1           TAC: 154
  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: 54
                                     Number of Members: 10
```

5.8. Administer Route Pattern

Use the “change route-pattern n” command, where “n” is an existing route pattern number to be used for integration with CARES, in this case “54”. 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 5.5**.
- **FRL:** A level that allows access to this trunk, with 0 being least restrictive.
- **Numbering Format:** “lev0-pvt”

```
change route-pattern 54                                     Page 1 of 3
                                     Pattern Number: 54 Pattern Name: CARES
  SCCAN? n           Secure SIP? N           Used for SIP stations? n
Grp FRL NPA Pfx Hop Toll No. Inserted           DCS/ IXC
No           Mrk Lmt List Del Digits           QSIG
                                     Dgts           Intw
1: 54 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
1: y y y y y n n           rest           lev0-pvt none
2: 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 CARES. Add an entry for the trunk group defined in **Section 5.5**.

In the example shown below, all calls originating from a 5-digit extension beginning with 6 and routed to trunk group 54 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  2
  5  5
  5  6          54          5
Total Administered: 3
Maximum Entries: 540

```

5.10. Administer Uniform Dial Plan

This section provides a sample AAR routing used for routing calls with dialed digits 54000 to CARES. Note that other routing methods may be used. Use the “change uniform-dialplan 0” command and add an entry to specify the use of AAR for routing of digits 54000, as shown below.

```

change uniform-dialplan 0                                     Page 1 of 2
                                UNIFORM DIAL PLAN TABLE
                                Percent Full: 0

Matching      Len Del      Insert      Node
Pattern       Len Del      Digits      Net Conv Num
54000         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 54000. In the example shown below, calls with digits 54000 will be routed as an AAR call using route pattern “54” 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      ANI
String      Min Max    Pattern    Type      Num      Reqd
54000      5  5        54        aar      n

```

5.12. Administer PSTN 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 “97”. Navigate to **Page 3**.

For **Modify Tandem Calling Number**, enter “tandem-cpn-form” to allow modification of calling party number for calls to the PSTN.

```

change trunk-group 97                                     Page 3 of 21
TRUNK FEATURES
  ACA Assignment? n           Measured: none           Wideband Support? n
                               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: private
  Outgoing Channel ID Encoding: preferred  UII IE Treatment: shared
                               Maximum Size of UII IE Contents: 128
                               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? y                   BSR Reply-best DISC Cause Value: 31
  Send Codeset 6/7 LAI IE? y          Dsl Echo Cancellation? n
  Apply Local Ringback? n           US NI Delayed Calling Name Update? n
  Show ANSWERED BY on Display? y     Invoke ID for USNI Calling Name: variable

```

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 CARES.

By default, CARES sends the agent’s internal extension on CARES as calling party number for manual outbound calls placed by the agent, and sends a blank calling party number for outbound campaign calls launched by CARES.

In the example shown below, all tandem calls to the PSTN will have up to 4-digits of calling party number deleted and replaced with “3035354000”, which takes care of the blank and 4-digits calling party number (4xxx) sent by CARES. Note that alternatively CARES can be configured to send a specific calling party number for outbound campaign calls, in which case the calling party number modification only needs to be for the CARES internal agent extensions.

```

change tandem-calling-party-num                          Page 1 of 9
          CALLING PARTY NUMBER CONVERSION
          FOR TANDEM CALLS
          Incoming Outgoing
          Number   Trunk
          Format   Group(s)   Delete   Insert
Len Prefix
any  any           97       4       3035354000
          pub-unk

```

6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager, which is performed via the web interface of System Manager. The procedures include the following areas:

- Launch System Manager
- Administer locations
- Administer SIP entities
- 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 System Manager. Log in using the appropriate credentials.

Recommended access to System Manager is via FQDN.

[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

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:

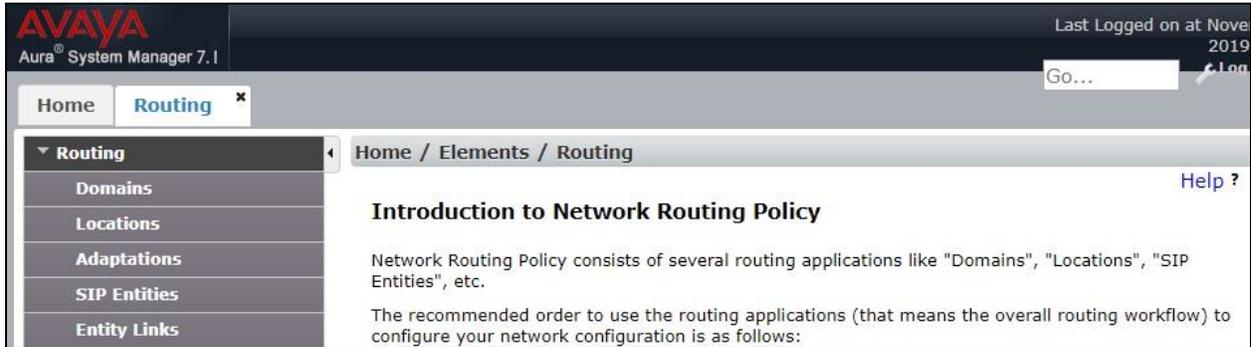
Password:

[Change Password](#)

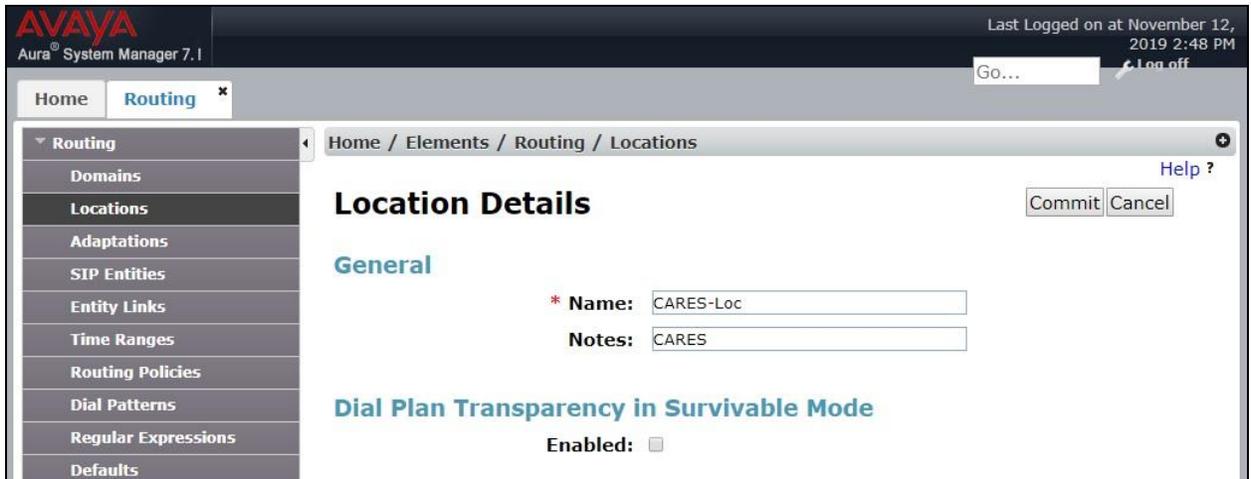
Supported Browsers: Internet Explorer 11.x or Firefox 48.0, 49.0 and 50.0.

6.2. Administer Locations

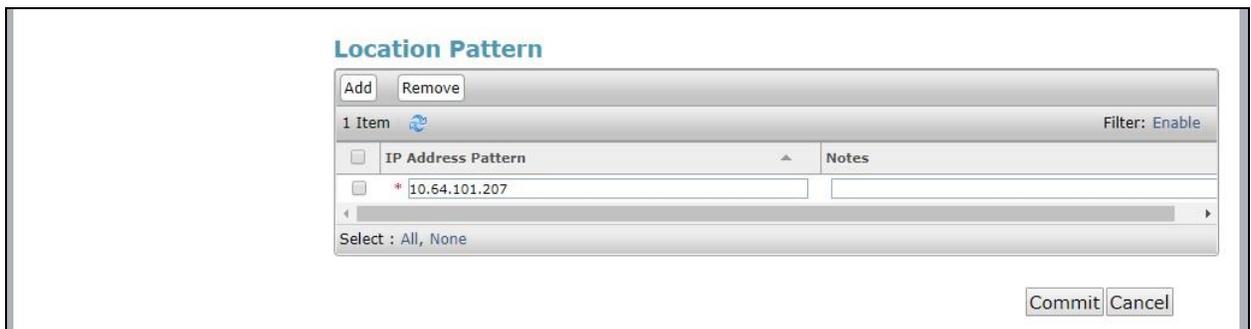
In the subsequent screen (not shown), select **Elements** → **Routing** to display the **Introduction to Network Routing Policy** screen below. Select **Routing** → **Locations** from the left pane and click **New** in the subsequent screen (not shown) to add a new location for CARES.



The **Location Details** screen is displayed next. In the **General** sub-section, enter a descriptive **Name** and optional **Notes**.



Scroll down to the **Location Pattern** sub-section and click **Add**. For **IP Address Pattern**, enter the IP address of CARES as shown below. Retain the default values in the remaining fields.



6.3. Administer SIP Entities

Add two SIP entities, one for CARES and one for the new SIP trunk with Communication Manager.

6.3.1. SIP Entity for CARES

Select **Routing** → **SIP Entities** from the left menu and click **New** in the subsequent screen (not shown) to add a new SIP entity for CARES.

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 CARES.
- **Type:** “SIP Trunk”
- **Location:** Select the CARES location name from **Section 6.2**.
- **Time Zone:** Select the applicable time zone.

The screenshot shows the Avaya Aura System Manager 7.1 interface. The top navigation bar includes the Avaya logo, the text "Aura System Manager 7.1", and the user's login information: "Last Logged on at November 12, 2019 2:48 PM" and "Log off". The main content area is titled "SIP Entity Details" and is divided into two sections: "General" and "Loop Detection". The "General" section contains the following fields:

- Name:** CARES
- FQDN or IP Address:** 10.64.101.207
- Type:** SIP Trunk
- Notes:** (empty)
- Adaptation:** (empty)
- Location:** CARES-Loc
- Time Zone:** America/New_York
- SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting
- Credential name:** (empty)
- Securable:**
- Call Detail Recording:** egress

The "Loop Detection" section is currently empty. The left navigation menu shows "Routing" selected, with "SIP Entities" highlighted. The breadcrumb trail at the top reads "Home / Elements / Routing / SIP Entities".

Scroll down to the **Entity Links** sub-section and click **Add** to add an entity link. 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 “sm15018”.
- **Protocol:** “UDP”
- **Port:** “5060”
- **SIP Entity 2:** The CARES entity name from this section.
- **Port:** “5060”
- **Connection Policy:** “trusted”

Note that CARES only support UDP in the current release.

Entity Links

Override Port & Transport with DNS SRV:

Add Remove

1 Item Filter: Enable

	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
<input type="checkbox"/>	* SM-CARES	sm15018	UDP	* 5060	CARES	* 5060	trusted

Select : All, None

SIP Responses to an OPTIONS Request

Add Remove

0 Items Filter: Enable

Response Code & Reason Phrase	Mark Entity Up/Down	Notes

Commit Cancel

6.3.2. SIP Entity for Communication Manager

Select **Routing** → **SIP Entities** from the left menu and click **New** in the subsequent screen (not shown) to add a new SIP entity for Communication Manager. Note that this SIP entity is used for integration with CARES.

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 processor IP address from **Section 5.2**.
- **Type:** “CM”
- **Location:** Select the applicable location for Communication Manager.
- **Time Zone:** Select the applicable time zone.

The screenshot shows the Avaya Aura System Manager 7.1 interface. The top header displays the Avaya logo, "Aura System Manager 7.1", and the user's login information: "Last Logged on at November 12, 2019 2:48 PM" and "Log off". The navigation menu on the left includes "Home", "Routing", "Domains", "Locations", "Adaptations", "SIP Entities", "Entity Links", "Time Ranges", "Routing Policies", "Dial Patterns", "Regular Expressions", and "Defaults". The main content area is titled "SIP Entity Details" and includes a "Commit" button and a "Cancel" button. The "General" section contains the following fields:

- * Name: DR-CM-5054
- * FQDN or IP Address: 10.64.150.14
- Type: CM
- Notes:
- Adaptation:
- Location: Lab
- Time Zone: America/New_York
- * SIP Timer B/F (in seconds): 4
- Minimum TLS Version: Use Global Setting
- Credential name:
- Securable:
- Call Detail Recording: none

The "Loop Detection" section is visible at the bottom of the form.

Scroll down to the **Entity Links** sub-section and click **Add** to add an entity link. 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 “sm15018”.
- **Protocol:** The signaling group transport method from **Section 5.6**.
- **Port:** The signaling group far-end listen port number from **Section 5.6**.
- **SIP Entity 2:** The Communication Manager entity name from this section.
- **Port:** The signaling group near-end listen port number from **Section 5.6**.
- **Connection Policy:** “trusted”

Entity Links

Override Port & Transport with DNS SRV:

Add Remove
Filter: Enable

1 Item

	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
<input type="checkbox"/>	* SM-CM-5054	sm15018	TLS	* 5054	DR-CM-5054	* 5054	trusted

Select : All, None

SIP Responses to an OPTIONS Request

Add Remove
Filter: Enable

0 Items

Response Code & Reason Phrase	Mark Entity Up/Down	Notes

6.4. Administer Routing Policies

Add two routing policies, one for CARES and one for the new SIP trunk with Communication Manager.

6.4.1. Routing Policy for CARES

Select **Routing** → **Routing Policies** from the left pane and click **New** in the subsequent screen (not shown) to add a new routing policy for CARES. The **Routing Policy Details** screen is displayed.

In the **General** sub-section, enter a descriptive **Name**. Enter optional **Notes** and retain the default values in the remaining fields.

In the **SIP Entity as Destination** sub-section, click **Select** and select the CARES entity name from **Section 6.3.1**. The screen below shows the result of the selection.

AVAYA
Aura® System Manager 7.1

Last Logged on at November 12, 2019 2:48 PM
Go... Log off

Home Routing

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit Cancel Help ?

General

* Name:

Disabled:

* Retries:

Notes:

SIP Entity as Destination

Select

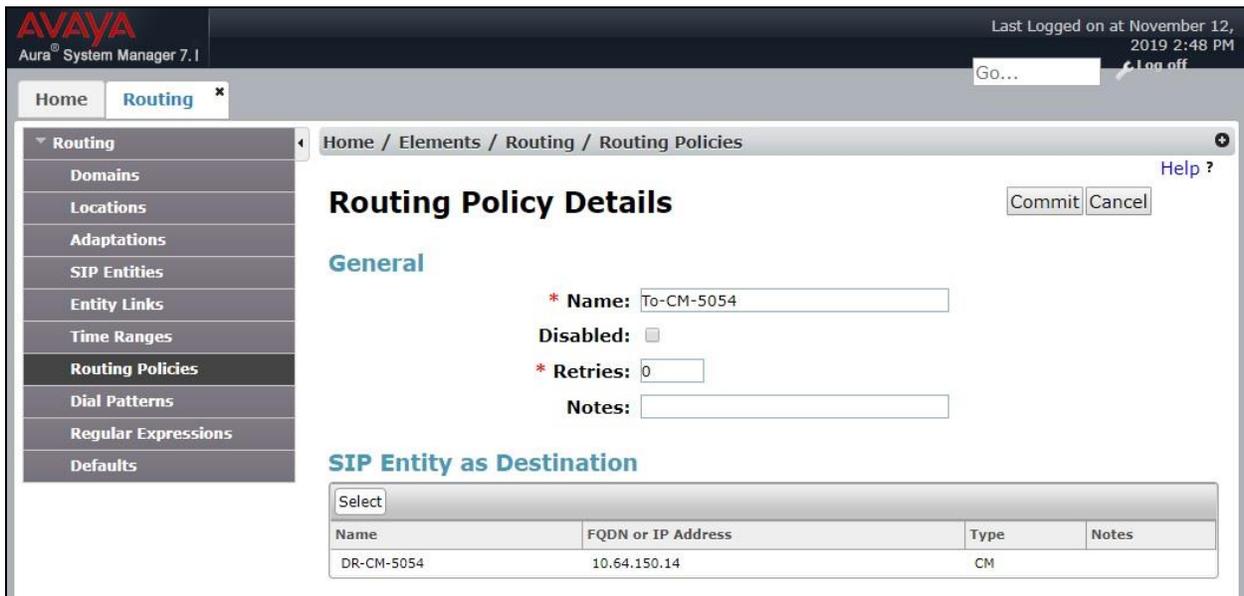
Name	FQDN or IP Address	Type	Notes
CARES	10.64.101.207	SIP Trunk	

6.4.2. Routing Policy for Communication Manager

Select **Routing** → **Routing Policies** from the left pane and click **New** in the subsequent screen (not shown) to add a new routing policy for Communication Manager. The **Routing Policy Details** screen is displayed.

In the **General** sub-section, enter a descriptive **Name**. Enter optional **Notes** and retain the default values in the remaining fields.

In the **SIP Entity as Destination** sub-section, click **Select** and select the Communication Manager entity name from **Section 6.3.2**. The screen below shows the result of the selection.



AVAYA
Aura[®] System Manager 7.1

Last Logged on at November 12, 2019 2:48 PM
Go... Log off

Home Routing

Routing
Domains
Locations
Adaptations
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns
Regular Expressions
Defaults

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit Cancel

General

* Name: To-CM-5054

Disabled:

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
DR-CM-5054	10.64.150.14	CM	

6.5. Administer Dial Patterns

Add a new dial pattern for CARES and update existing dial patterns for Communication Manager to allow calls from CARES.

6.5.1. Dial Pattern for CARES

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 CARES. 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:** The CARES main number from **Section 3**.
- **Min:** The minimum number of digits to match.
- **Max:** The maximum number of digits to match.

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create an entry for reaching CARES. In the compliance testing, the entry allowed for call origination from Communication Manager resources in location “Lab”. The CARES routing policy from **Section 6.4.1** was selected as shown below.

The screenshot displays the Avaya Aura System Manager 7.1 interface. The top navigation bar shows 'Home' and 'Routing' (selected). The breadcrumb trail is 'Home / Elements / Routing / Dial Patterns'. The main content area is titled 'Dial Pattern Details' and includes 'Commit' and 'Cancel' buttons. The 'General' section contains the following fields:

- * Pattern: 54000
- * Min: 5
- * Max: 5
- Emergency Call:
- Emergency Priority: 1
- Emergency Type:
- SIP Domain: -ALL-
- Notes:

The 'Originating Locations and Routing Policies' section features an 'Add' button and a table with the following data:

<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"/>	Lab	To-CARES		0	<input type="checkbox"/>	CARES	

At the bottom of the table, it says 'Select : All, None'.

6.5.2. Dial Pattern for Communication Manager

Select **Routing** → **Dial Patterns** from the left pane and click on the applicable dial pattern for Communication Manager in the subsequent screen, in this case dial pattern “6” (not shown). The **Dial Pattern Details** screen is displayed.

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create a new entry as necessary for calls from CARES. In the compliance testing, the new entry allowed for call origination from the CARES location from **Section 6.2** and the Communication Manager routing policy from **Section 6.4.2** were selected as shown below. Retain the default values in the remaining fields.

Repeat this section to make similar changes to applicable Communication Manager dial pattern to reach the PSTN. In the compliance testing, CARES will add the prefix “91” for outbound campaign calls to the PSTN, and therefore the existing dial pattern for “91” was also changed (not shown below).

The screenshot displays the Avaya Aura System Manager 7.1 interface. The top navigation bar shows 'Home' and 'Routing' (selected). The breadcrumb trail is 'Home / Elements / Routing / Dial Patterns'. The main content area is titled 'Dial Pattern Details' and includes 'Commit' and 'Cancel' buttons. The 'General' section contains the following fields:

- * Pattern: 6
- * Min: 5
- * Max: 5
- Emergency Call:
- Emergency Priority: 1
- Emergency Type: [Empty]
- SIP Domain: -ALL-
- Notes: To CM7

The 'Originating Locations and Routing Policies' section features an 'Add' button and a table with 2 items. The table has columns for 'Originating Location Name', 'Originating Location Notes', 'Routing Policy Name', 'Rank', 'Routing Policy Disabled', 'Routing Policy Destination', and 'Routing Policy Notes'. The 'CARES-Loc' row is highlighted with a red box.

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
CARES-Loc	CARES	To-CM-5054	0	<input type="checkbox"/>	DR-CM-5054	
Lab		cm15014	0	<input type="checkbox"/>	cm15014	

7. Configure Centurion CARES

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

- Launch web interface
- Administer trunk
- Administer trunk node
- Administer dial plan
- Administer outbound campaign parameter
- Administer inbound call flow

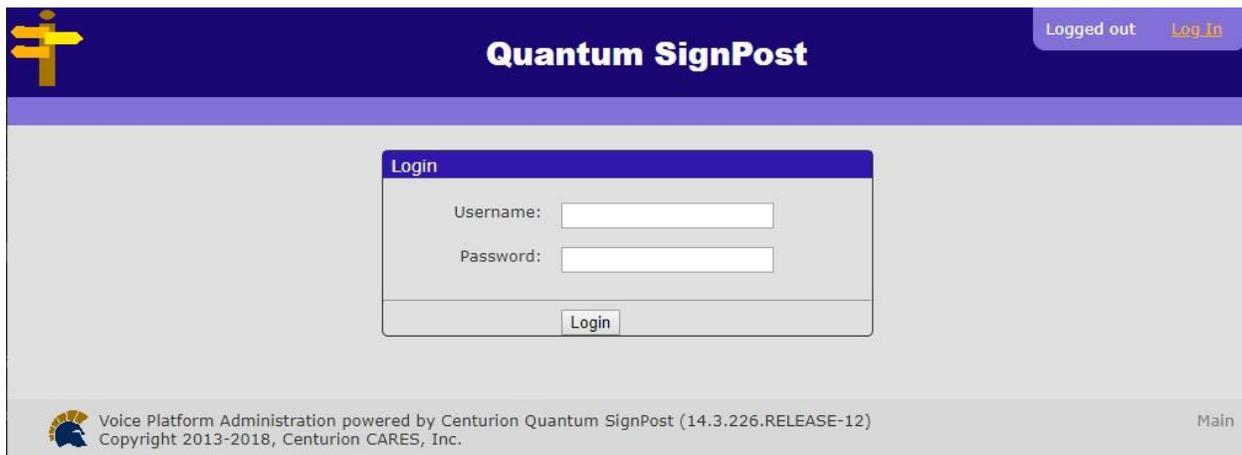
The detailed administration of the Dialogic resource and of contact center resources such as splits, skills, agents, and outbound campaigns are assumed to be in place and are not covered in these Application Notes.

The configuration of CARES is typically performed by the Centurion implementation team, and the procedural steps are presented in these Application Notes for informational purposes.

7.1. Launch Web Interface

Access the CARES web interface by using the URL <https://ip-address:8443> in an Internet browser window, where “ip-address” is the IP address of the CARES server.

The **Quantum SignPost** screen is display. Log in using the appropriate credentials.



Quantum SignPost

Logged out [Log In](#)

Login

Username:

Password:

Voice Platform Administration powered by Centurion Quantum SignPost (14.3.226.RELEASE-12)
Copyright 2013-2018, Centurion CARES, Inc. [Main](#)

7.2. Administer Trunk

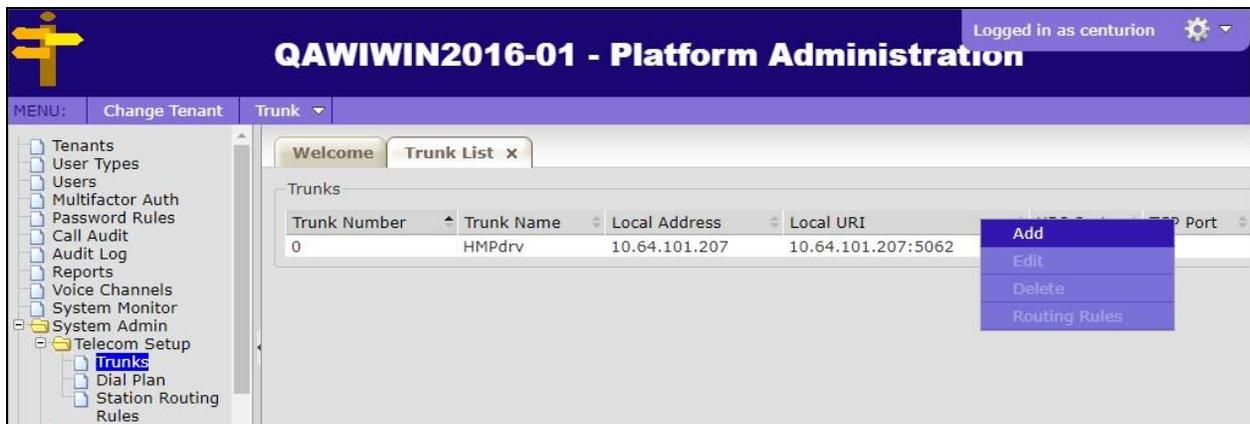
The screen below is displayed. Select **Platform Administration**.



The **Welcome** tab is displayed in the right pane, as shown below.

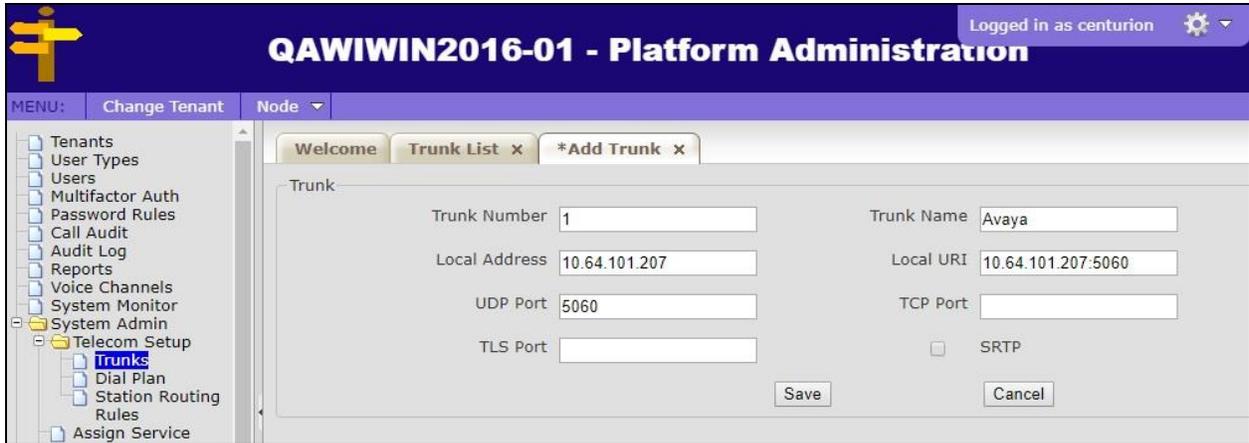


Select **System Admin** → **Telecom Setup** → **Trunks** in the left pane to display the **Trunk List** tab in the right pane. A list of existing trunks is displayed. Right click in the Trunks area and select **Add** to add a new trunk.



The **Add Trunk** tab is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Trunk Number:** The next available trunk number, in this case “1”.
- **Trunk Name:** A descriptive trunk name.
- **Local Address:** IP address of the CARES server.
- **Local URI:** IP address of the CARES server and protocol port from **Section 6.3.1**.
- **UDP Port:** UDP protocol port from **Section 6.3.1**.



7.3. Administer Trunk Node

The **Trunk List** tab is displayed again. Right click on the newly added trunk from **Section 7.2** and select **Edit**.



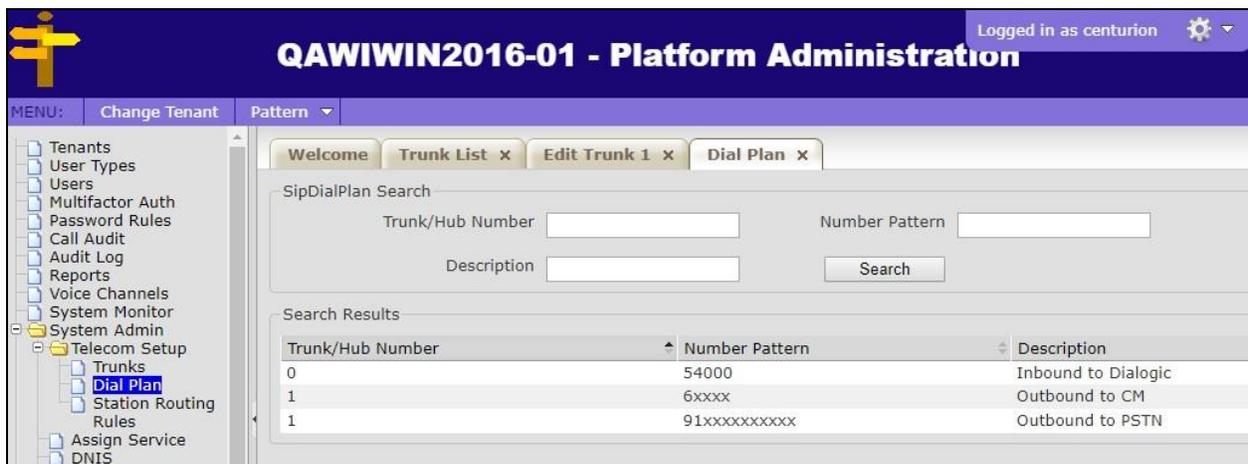
The **Edit Trunk** tab is displayed (content not shown below). Right click in the **Trunk Nodes** area and select **Add** (not shown) to display the **Add Node** tab. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Node Number:** “0”
- **Node Name:** A descriptive node name.
- **Address:** IP address of Session Manager signaling interface from **Section 5.2**.
- **Port:** The transport port number from **Section 6.3.1**.
- **URI:** IP address of Session Manager signaling interface and protocol port.



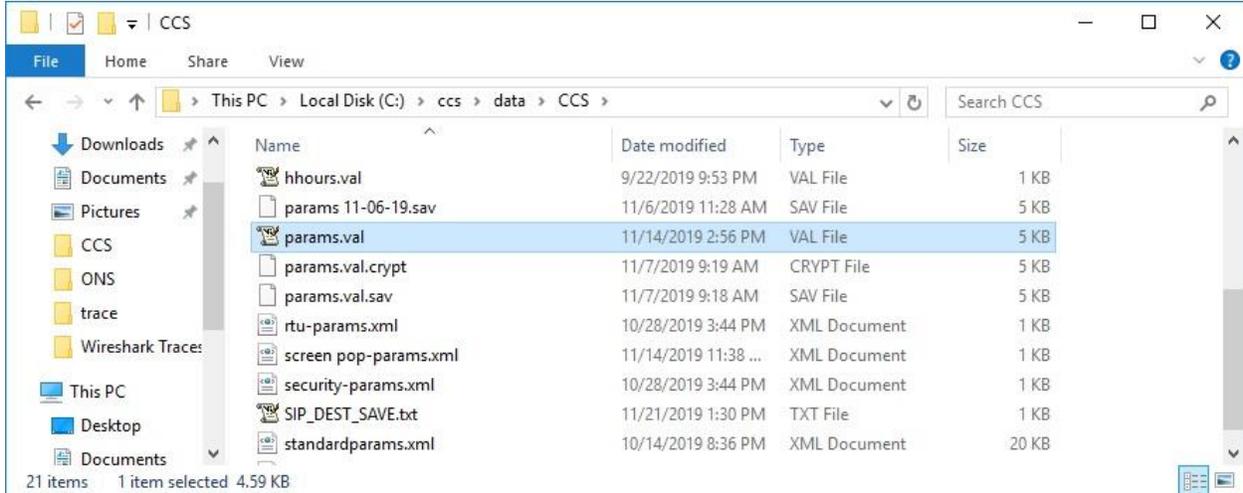
7.4. Administer Dial Plan

Select **System Admin** → **Telecom Setup** → **Dial Plan** from the left pane to display the **Dial Plan** tab. Create entries for inbound calls to the CARES main number 54000, outbound calls to agent station extensions 6xxxx on Communication Manager, and outbound calls to the PSTN with applicable network prefix. Three dial plan entries were created in the compliance testing as shown below.

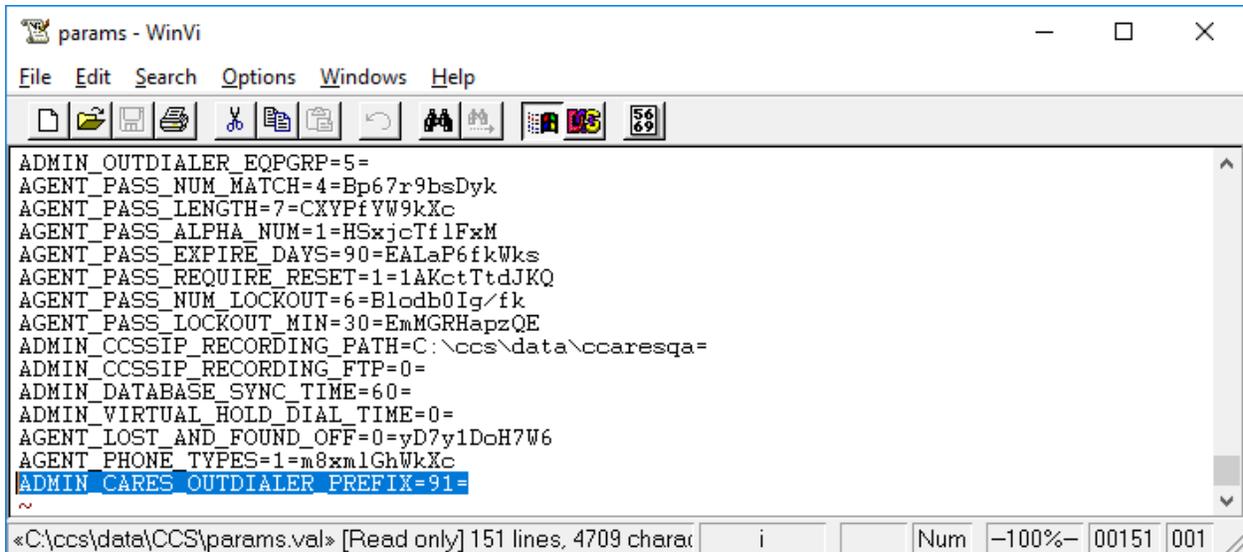


7.5. Administer Outbound Campaign Parameter

From the CARES server, navigate to the C:\ccs\data\CCS directory to locate the **params.val** file shown below.



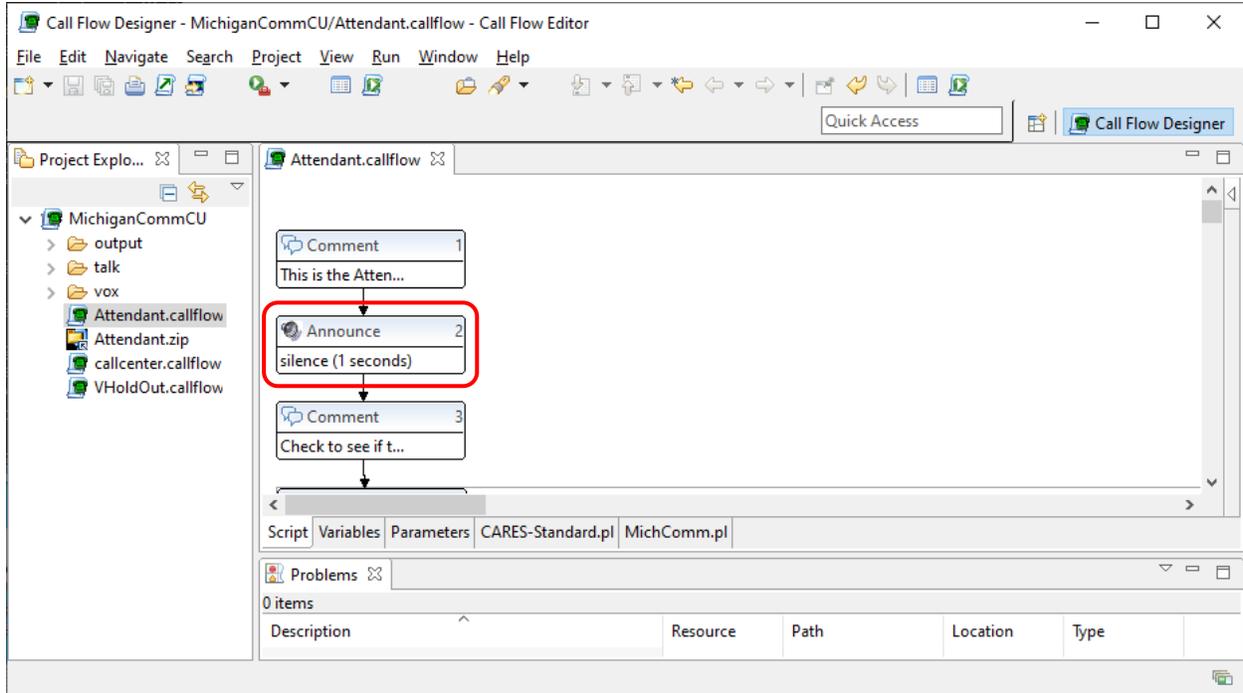
Open the **params** file with the Notepad application. Scroll down to the bottom of the file, and set **ADMIN_CARES_OUTDIALER_PREFIX** to the network dialing prefix to reach the PSTN, in this case “91” as shown below.



7.6. Administer Inbound Call Flow

Depending on the customer network, a delay may need to be added to the inbound call flow so that the greeting announcement played to PSTN callers can be heard in its entirety. Update the inbound call flow if necessary.

In the compliance testing, a one-second delay was added to the beginning of the inbound call flow as shown below.



8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Session Manager, and CARES.

8.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify status of the SIP trunk group by using the “status trunk n” command, where “n” is the trunk group number administered in **Section 5.5**. Verify that all ports are in the “in-service/idle” state as shown below.

```
status trunk 54
```

TRUNK GROUP STATUS			
Member	Port	Service State	Mtce Connected Ports Busy
0054/001	T00021	in-service/idle	no
0054/002	T00022	in-service/idle	no
0054/003	T00023	in-service/idle	no
0054/004	T00024	in-service/idle	no
0054/005	T00025	in-service/idle	no
0054/006	T00026	in-service/idle	no
0054/007	T00027	in-service/idle	no
0054/008	T00028	in-service/idle	no
0054/009	T00029	in-service/idle	no
0054/010	T00030	in-service/idle	no

Verify status of the SIP signaling group by using the “status signaling-group n” command, where “n” is the signaling group number administered in **Section 5.6**. Verify that the **Group State** is “in-service” as shown below.

```
status signaling-group 54
```

STATUS SIGNALING GROUP	
Group ID:	54
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. Click on the CARES entity name from **Section 6.3.1**.

Home / Elements / Session Manager / System Status / SIP Entity Monitoring

SIP Entity Link Monitoring Status Summary

This page provides a summary of Session Manager SIP entity link monitoring status.

SIP Entities Status for All Monitoring Session Manager Instances

Run Monitor

1 Item Filter: Enable

Session Manager	Type	Monitored Entities					Total
		Down	Partially Up	Up	Not Monitored	Deny	
<input type="checkbox"/> sm15018	Core	4	0	10	1	0	15

Select : All, None

All Monitored SIP Entities

Run Monitor

14 Items Filter: Enable

<input type="checkbox"/> SIP Entity Name
<input checked="" type="checkbox"/> CARES

The **SIP Entity, Entity Link Connection Status** screen is displayed. Verify that the **Conn Status** and **Link Status** are “UP” as shown below.

Home / Elements / Session Manager / System Status / SIP Entity Monitoring

SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

Status Details for the selected Session Manager:

All Entity Links to SIP Entity: CARES

Summary View

1 Item Filter: Enable

Session Manager Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/> sm15018	IPv4	10.64.101.207	5060	UDP	FALSE	UP	200 OK	UP

Select : None

8.3. Verify Centurion CARES

From the agent PC, double-click on the CARES Client shortcut shown below, which was created as part of CARES Client installation.



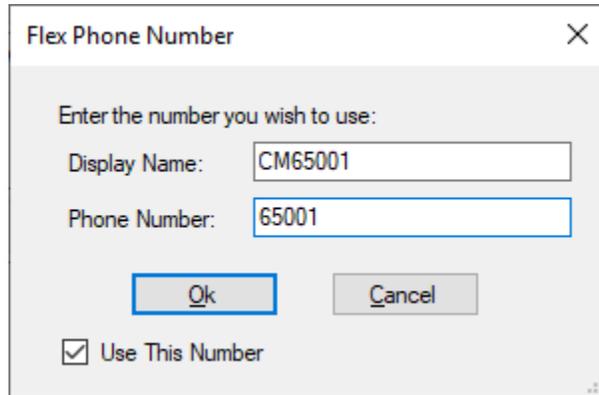
The **Cares Login** screen is displayed. Log in using the appropriate agent credentials.

A dialog box titled "Cares Login". It has a light gray background. At the top, it says "Server Name: Call Center". Below that, there are two input fields: "Login:" and "Password:". Below the input fields, there is a checkbox with the text "I want to change my password.". At the bottom, there are three buttons: "Login", "Cancel", and "Settings".

The screen below is displayed next. Upon initial log in, select **Tools** → **Flex Settings** → **Add New Number**.

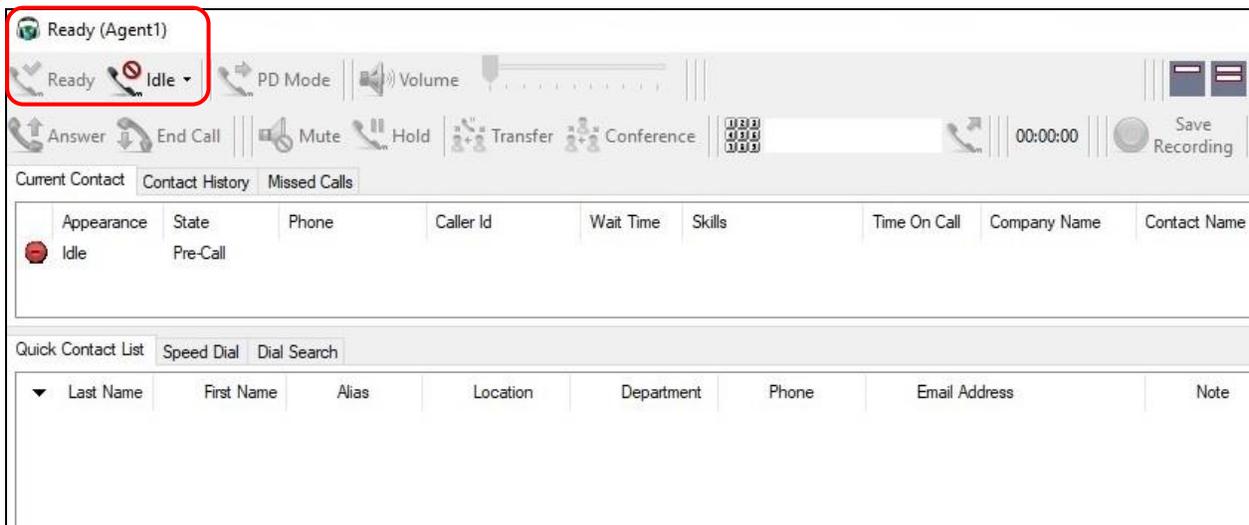
A screenshot of the CARES Agent Desktop Interface. The top bar shows the agent's status as "Idle - Pre-work (Agent1)". Below the status bar, there are various call control icons: Ready, Idle, PD Mode, Volume, Answer, End Call, Mute, Hold, Transfer, Conference, and Save Recording. A "Tools" button is highlighted with a red box. Below the call control bar, there is a "Current Contact" section with a table showing contact details. Below that, there is a "Quick Contact List" section with a table showing a list of contacts. The "Tools" button is highlighted with a red box.

The **Flex Phone Number** pop-up box is displayed. For **Display Name**, enter a descriptive name. For **Phone Number**, enter the pertinent station user extension on Communication Manager, in this case “65001”. Check **Use This Number**.



A dialog box titled "Flex Phone Number" with a close button (X) in the top right corner. The text "Enter the number you wish to use:" is displayed above two input fields. The "Display Name:" field contains the text "CM65001". The "Phone Number:" field contains the text "65001". Below the input fields are two buttons: "Ok" and "Cancel". At the bottom left, there is a checked checkbox labeled "Use This Number".

Select **Ready** from the screen below and verify that the screen is updated to reflect **Ready**.



A screenshot of an agent's interface. The top status bar shows "Ready (Agent1)" with a red box around it, and a dropdown menu with "Ready" and "Idle" options. Other icons include "PD Mode", "Volume", "Answer", "End Call", "Mute", "Hold", "Transfer", "Conference", and "Save Recording". Below the status bar are tabs for "Current Contact", "Contact History", and "Missed Calls". A table displays contact information with columns: Appearance, State, Phone, Caller Id, Wait Time, Skills, Time On Call, Company Name, and Contact Name. The "Appearance" column shows a red circle icon and the text "Idle". Below this is a "Quick Contact List" section with tabs for "Speed Dial" and "Dial Search". A table below this section has columns: Last Name, First Name, Alias, Location, Department, Phone, Email Address, and Note.

Establish an incoming trunk call from PSTN with CARES. Verify that the calling party hears the appropriate IVR greeting.

Enter the DTMF digit to select the option associated with connection to an agent. Verify that CARES place a call to the available agent if not already connected, and that the agent desktop is updated to reflect a ringing ACD call along with the PSTN calling party number as shown below. Select **Answer**.

ACD Ringing (Agent1)

Ready Idle PD Mode Volume

Answer End Call Mute Hold Transfer Conference 00:00:02 Save Recording

Appearance	State	Phone	Caller Id	Wait Time	Skills	Time On Call	Company Name	Contact Name
ACD Call	Ringing	19089532103				00:00:02		

Quick Contact List Speed Dial Dial Search

Last Name	First Name	Alias	Location	Department	Phone	Email Address	Note
-----------	------------	-------	----------	------------	-------	---------------	------

Verify that the agent is connected to the PSTN caller with two-way talk path, and that the agent desktop is updated to reflect the call in the **Connected** state.

ACD Connected (Agent1)

Ready Idle PD Mode Volume

Answer End Call Mute Hold Transfer Conference 00:00:27 Save Recording

Appearance	State	Phone	Caller Id	Wait Time	Skills	Time On Call	Company Name	Contact Name
ACD Call	Connected	19089532103				00:00:27		

Quick Contact List Speed Dial Dial Search

Last Name	First Name	Alias	Location	Department	Phone	Email Address	Note
-----------	------------	-------	----------	------------	-------	---------------	------

9. Conclusion

These Application Notes describe the configuration steps required for Centurion CARES 14.03 to successfully interoperate with Avaya Aura® Communication Manager 7.1 and Avaya Aura® Session Manager 7.1. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

10. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Release 7.1.3, Issue 8, August 2019, available at <http://support.avaya.com>.
2. *Administering Avaya Aura® Session Manager*, Release 7.1.3, Issue 5, July 2018, available at <http://support.avaya.com>.
3. *CARES Client*, Version 14.3, 6/12/19, available at <ftp://caresdl:download@ftp.centurioncares.com/pub/Documentation>.

©2019 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.