AVAYA MESSAGING™

Integration with Avaya Aura CM and Session Manager 8

Release 11.0
Issue 1
Oct 2021

AVAYA MESSAGING INTEGRATION WITH AVAYA AURA CM AND SESSION MANAGER 8

Please refer to this guide when integrating Avaya Messaging with Avaya Aura CM with Session Manager 8.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

"Documentation" means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials.

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

"Hosted Service" means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK "AVAYA SOFTWARE LICENSE TERMS (Avaya Products)" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a dif-

ferent number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. “Named

User”, means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya’s sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note, unless otherwise stated, that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya’s website at: https:// support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE.

ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP:// WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of https:// support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from

Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

AVAYA MESSAGING INTEGRATION WITH AVAYA AURA CM AND SESSION

Table of Contents

AVAYA MESSAGING INTEGRATION WITH AVAYA AURA CM AND SESSION MANAGER 8

Introduction

Please follow this guide when integrating Avaya Aura CM with Session Manager Release 8.0+ with Avaya Messaging 10.7.

Reference Configuration

Figure 1 illustrates the configuration used in these notes. The sample configuration shows an enterprise with Session Manager and an Avaya Server with an Avaya Media Gateway. Endpoints include Avaya SIP IP Telephones, Avaya IP Telephones, and an Avaya Digital Telephone. An Avaya Server with Avaya Media Gateway was included in the test to include inter-switch scenarios.

Avaya Messaging is configured with the Session Manager as a trusted SIP entity.

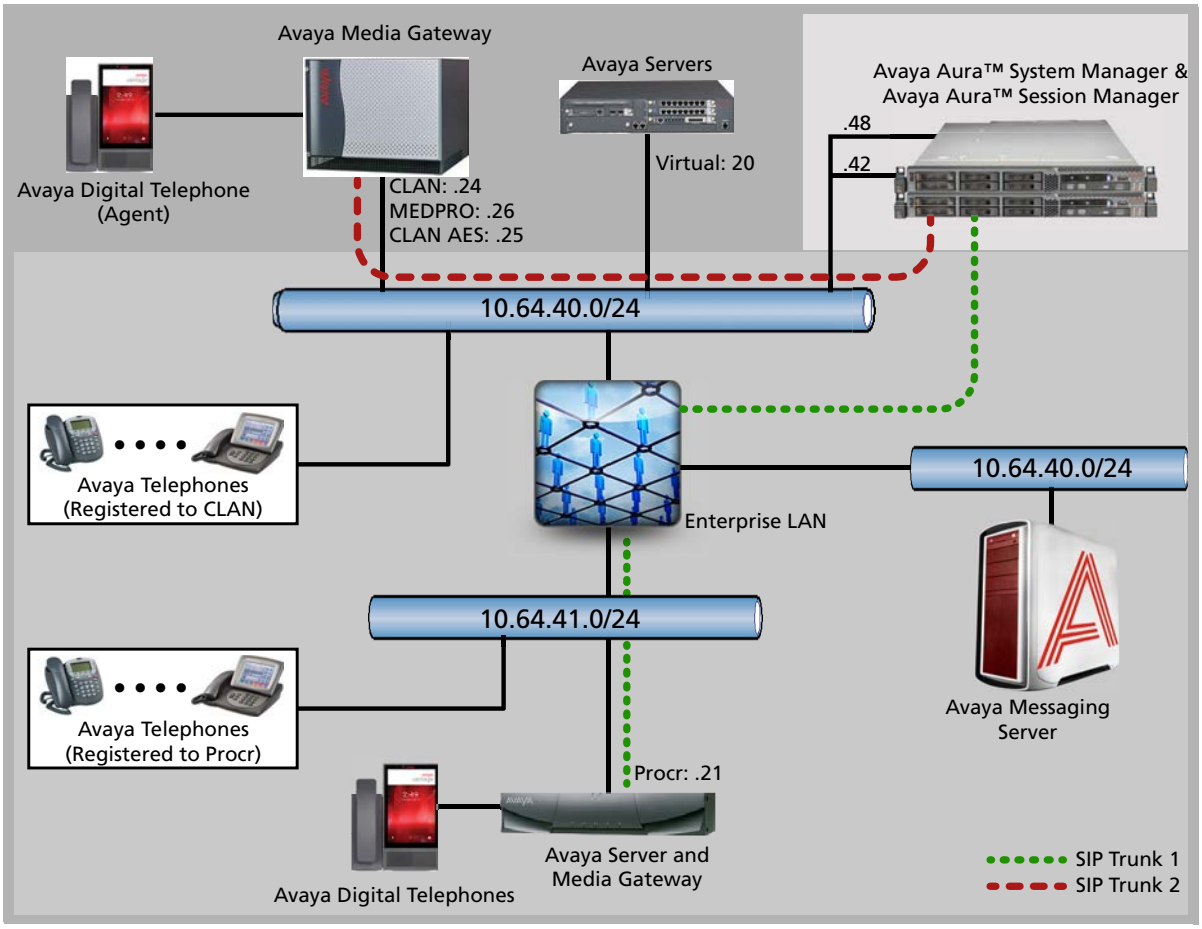


Figure 1: Test Configuration

Equipment and Software Validated

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

EQUIPMENT	SOFTWARE/FIRMWARE
Avaya Aura Communication Manager with Avaya G450 Media Gateway	Avaya Aura Communication Manager 8.0+ (R017x.01.0.532.0) with Patch 01.0.532.0-23985
Avaya Aura System Manager	Avaya Aura System Manager 7.1.2 (7.1.2.0.047222)
Avaya Aura Session Manager	Avaya Aura System Manager 7.1.2 (7.1.2.0.712004)
Avaya SIP Telephones	
9600 Series Equinox Client	7.1+ 3.4
Avaya Messaging	10.7+

PBX and Hardware Configuration

Configure Avaya Aura Communication Manager

For compliance testing, Communication Manager was set up as an **Evolution Server** (Full Call Model). This section describes the procedure for setting up a SIP trunk between Communication Manager and Session Manager. The steps include establishing an IP codec set, an IP network region, IP node name, a signaling group, a trunk group, and a SIP station. Before a trunk can be configured, it is necessary to verify that there is enough capacity remaining.

The highlights in the following screens indicate the values used during the compliance test. Default values may be used for all other fields.

These steps are performed from the Communication Manager **System Access Terminal** (SAT) interface. All SIP telephones, except Avaya Messaging, are configured as off-PBX telephones in Communication Manager.

Capacity Verification

Enter the **display system-parameters customer-options** command. Verify that there are sufficient Maximum Off-PBX Telephones – OPS licenses.

If necessary, contact an authorized Avaya account representative to obtain additional licenses.

```
display system-parameters customer-options                    Page   1 of  12
                              OPTIONAL FEATURES

    G3 Version: V17                              Software Package: Enterprise
      Location: 2                                 System ID (SID): 1
      Platform: 28                                Module ID (MID): 1

                                                          USED
                                Platform Maximum Ports: 65000 9834
                                     Maximum Stations: 41000 8285
                                Maximum XMOBILE Stations: 41000 0
                    Maximum Off-PBX Telephones - EC500: 41000 2
                    Maximum Off-PBX Telephones -   OPS: 4100  5767
                    Maximum Off-PBX Telephones - PBFMC: 41000 0
                    Maximum Off-PBX Telephones - PVFMC: 41000 0
                    Maximum Off-PBX Telephones - SCCAN: 0     0
                         Maximum Survivable Processors: 313   1
```

Scroll down to verify that the number of SIP trunks supported by the system is sufficient.

If necessary, contact an authorized Avaya account representative to obtain additional licenses.

```
display system-parameters customer-options                    Page   2 of  12
                              OPTIONAL FEATURES

IP PORT CAPACITIES                                            USED
                       Maximum Administered H.323 Trunks: 12000 0
            Maximum Concurrently Registered IP Stations: 18000 5
              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: 41000 2
                  Maximum Video Capable IP Softphones: 18000 129
                      Maximum Administered SIP Trunks: 24000 1503
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
```

IP Codec Set

This section describes the steps for administering a codec set in Communication Manager. This codec set is used in the IP network region for linking Communication Manager with Session Manager. Enter the **change ip-codec-set <c>** command, where **c** is a number between 1 and 7. IP codec sets are used in **Configure IP Network Region on page 14** for configuring the IP network region to specify which codec sets may be used within and between network regions.

Note: Avaya Messaging supports G.711MU and G.711A. These were validated during compliance testing.

```
change ip-codec-set 1                                          Page   1 of   2

                         IP Codec Set
    Codec Set: 1

    Audio          Silence       Frames   Packet
    Codec          Suppression   Per Pkt  Size(ms)
 1: G.711MU            n           2         20
 2: G711A              n           2         20
```

Configure IP Network Region

This section describes the steps for administering an IP network region in Communication Manager for communication with Session Manager. Enter the **change ip-network-region <n>** command, where **n** is a number between 1 and 250.

Configure the following:

- **Authoritative Domain** – Enter the appropriate name for the Authoritative Domain. During the compliance test, the authoritative domain was set to aam1.com. This should match the value for SIP Domain on Session Manager, in **Configure SIP Domain on page 21**.
- **Codec Set** – Set the codec set number provisioned in **IP Codec Set on page 14**.

```
change ip-network-region 1                                     Page   1 of  20
                              IP NETWORK REGION
  Region: 1       NR Group: 1
Location: 1       Authoritative Domain: aam1.com
    Name: main-cm7950
MEDIA PARAMETERS                  Intra-region IP-IP Direct Audio: yes
      Codec Set: 1                Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                       IP Audio Hairpinning? y
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

Configure IP Node Name

This section describes setting an IP node name for Session Manager in Communication Manager.
Enter the **change node-names ip** command, and add a node name for Session Manager along with its IP address.

```
display node-names ip
                                IP NODE NAMES
    Name                  IP Address
AAM7461                 103.20.74.61
SM1                     10.255.248.98
SM4                     10.255.248.105
SM7954                  103.20.250.35
aes25035                10.255.250.35
aes25156                10.255.251.56
cm7944                  103.20.79.44
dc3-aes-ha-cm79         10.255.251.57
dc3-lsp                 10.255.253.37
default                 0.0.0.0
officelinx88            10.255.250.88
ol25158                 10.255.251.58
procr                   10.255.250.91
```

Configure SIP Signaling

Enter the **add signaling-group <s>** command, where **s** is an available signaling group. Configure the following:

- **Group Type** – Set to **sip**.
- **IMS Enabled** – Verify that the field is set to **n**.
- **Transport Method** – Set to **tls** (Transport Layer Security).
- **Near-end Node Name** – Set to **procr** as displayed in **Configure IP Node Name on page 15**.
- **Far-end Node Name** – Set to the Session Manager name configured in **Configure IP Node Name on page 15**.
- **Far-end Network Region** – Set to the region configured in **Configure IP Network Region on page 14**.
- **Far-end Domain** – Set to **aam1.com**. This should match the SIP Domain value in **Configure IP Network Region on page 14**.
- **Direct IP-IP Audio Connections** – Set to **n**.

```
display signaling-group 58
                               SIGNALING GROUP

Group Number: 58                    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    Peer Server: SM
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
  Near-end Node Name: procr                        Far-end Node Name: SM4
Near-end Listen Port: 5061                       Far-end Listen Port: 5061
                                               Far-end Network Region: 1

Far-end Domain: aam1.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? n
Session Establishment Timer (min): 3                       IP Audio Hairpinning? y
          Enable Layer 3 Test? y                        Initial IP-IP Direct Media? y
H.323 Station Outgoing Direct Media? n                 Alternate Route Timer (sec): 6
```

Configure Trunk Group

To configure the associated trunk group, enter the **add trunk-group <t>** command, where **t** is an available trunk group and configure the following:

- **Group Type** – Set the Group Type field to **sip**.
- **Group Name** – Enter a descriptive name.
- **TAC (Trunk Access Code)** – Set to any available trunk access code.
- **Service Type** – Set the Service Type field to **tie**.
- **Signaling Group** – Set to the Group Number field value configured in the SIGNALING GROUP form.
- **Number of Members** – The permitted range is between 0 and 255. Set to a value large enough to accommodate the number of SIP telephone extensions being used.

```
display trunk-group 58                                        Page   1 of  21
                              TRUNK GROUP

Group Number: 58                  Group Type: sip           CDR Reports: y
  Group Name: To OL25158                  COR: 1        TN: 1        TAC: *158
   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: 58
                                                  Number of Members: 10
```

- On Page 3, set the **Numbering Format** field to **private**.

```
display trunk-group 58                                        Page   3 of  21
TRUNK FEATURES
         ACA Assignment? n           Measured: none
                                                    Maintenance Tests? y


   Suppress # Outpulsing? n   Numbering Format: private
                                           UUI Treatment: service-provider
```

Configure Hunt Group

This section describes the steps for administering a hunt group in Communication Manager. Enter the **add hunt-group <h>** command, where **h** is an allocated hunt group number. The following fields were configured for the compliance test.

- **Group Name** – Enter a descriptive name.
- **Group Extension** – Enter an extension valid in the provisioned dial plan.

```
display hunt-group 92                                          Page   1 of  60
                                  HUNT GROUP

           Group Number: 58                                 ACD? n
             Group Name: OL25158                          Queue? n
        Group Extension: 58000                           Vector? n
             Group Type: ucd-mia                 Coverage Path: 58
                     TN: 1           Night Service Destination:
                    COR: 1                     MM Early Answer? n
          Security Code:                  Local Agent Preference? n
 ISDN/SIP Caller Display: mbr-name
```

On Page 2, provide the following information:

- **Message Center** – Enter **sip-adjunct**, indicating the type of messaging adjunct used for this hunt group. This value will also be used in the Station form.
- **Voice Mail Number** – Enter the Voicemail Number, which is the extension of Avaya Messaging.
- **Voice Mail Handle** –Enter the Voicemail Handle which is the extension of Avaya Messaging.
- **Routing Digit (e.g. AAR/ARS Access Code)** – Enter the AAR Access Code as defined in the Feature Access Code form.

```
display hunt-group 58                                          Page   2 of  60
                                  HUNT GROUP


                     Message Center: sip-adjunct

    Voice Mail Number        Voice Mail Handle         Routing Digits
                                                  (e.g., AAR/ARS Access Code)
    58000                    58000                     11
```

Configure Coverage Path

This section describes the steps for administering coverage path in Communication Manager. Enter the **add coverage path <s>** command, where **s** is a valid coverage path number. The Point1 value of **h58** is used to represent the hunt group number 58 created in **Configure Hunt Group on page 17**. The default values for the other fields may be used.

```
display coverage path 58
                               COVERAGE PATH

                 Coverage Path Number: 58
    Cvg Enabled for VDN Route-To Party? n        Hunt after Coverage? n
                      Next Path Number:          Linkage

COVERAGE CRITERIA
    Station/Group Status    Inside Call     Outside Call
             Active?             n              n
               Busy?             y              y
      Don't Answer?              y              y         Number of Rings: 2
                All?             n              n
 DND/SAC/Goto Cover?             y              y
   Holiday Coverage?             n              n


COVERAGE POINTS
    Terminate to Coverage Pts. with Bridged Appearances? n
  Point1: h58            Rng: 2  Point2:
  Point3:                        Point4:
  Point5:                        Point6:
```

Configure SIP Endpoint

This section describes the steps for administering SIP stations in Communication Manager and associating with OPS station extensions.

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

Configure Route Pattern

For the trunk group created in **Configure Trunk Group on page 16**, define the route pattern by entering the **change route-pattern <r>** command, where **r** is an unused route pattern number. The route pattern consists of a list of trunk groups that can be used to route a call. The following screen shows route-pattern 58 will utilize trunk group 58 to route calls. The default values for the other fields may be used.

```
display route-pattern 92                                        Page   1 of   3
                  Pattern Number: 58  Pattern Name: To OL58
    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: 58  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 Sub  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
```

Configure AAR Analysis

For the AAR Analysis Table, create the dial string that will map calls to Avaya Messaging via the route pattern created in **Configure Route Pattern on page 19**. Enter the **change aar analysis <x>** command, where **x** is a starting partial digit (or full digit). The dialed string created in the AAR Digit Analysis table should contain a map to the Avaya Messaging system extension, which is configured as 58000. During the configuration of AAR table, the Call Type field was set to **lev0**.

```
display aar analysis 58                                         Page   1 of   2
                           AAR DIGIT ANALYSIS TABLE
                                 Location: all            Percent Full: 1

          Dialed           Total     Route    Call    Node  ANI
          String          Min  Max  Pattern   Type    Num   Reqd
    58                    5    5    58        lev0          n
    59                    5    5    4         aar           n
    6                     7    7    2000      aar           n
```

Configure Avaya Aura Session Manager

This section provides the procedures for configuring Session Manager as provisioned in the reference configuration. Session Manager is comprised of two functional components: the Session Manager server and the System Manager server. All SIP call provisioning for Session Manager is performed through the System Manager Web interface and is then downloaded into Session Manager.

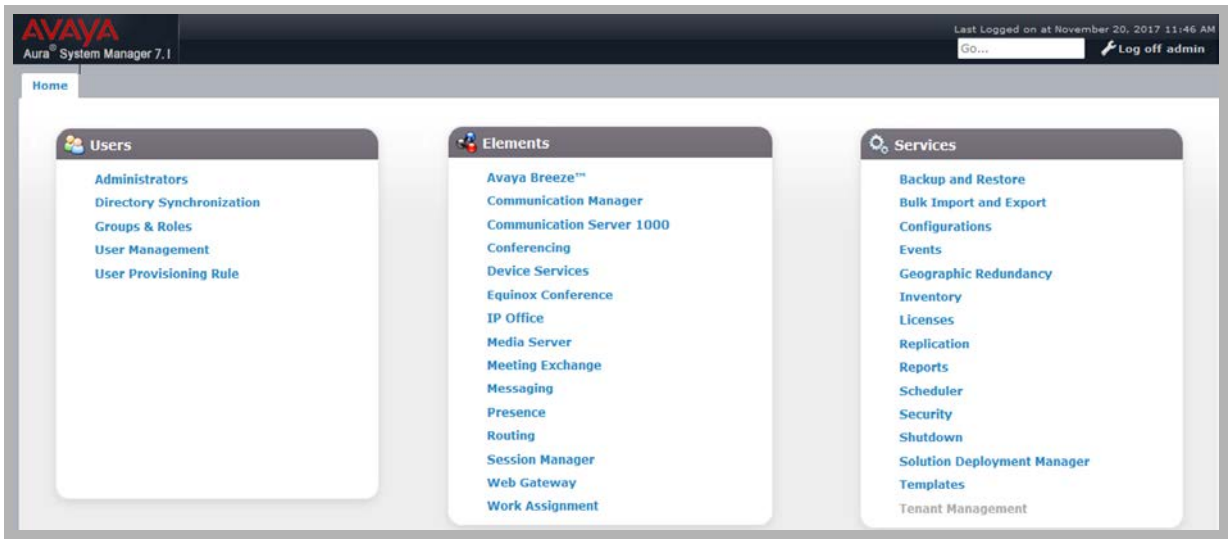
The following assumes that Session Manager and System Manager have been installed and that network connectivity exists between the two platforms.

In this section, the following topics are discussed:

- SIP Domains
- Locations
- SIP Entities
- Entity Links
- Time Ranges
- Routing Policy
- Dial Patterns
- Manage Element
- Applications
- Application Sequence
- User Management
- Synchronization

Configure SIP Domain

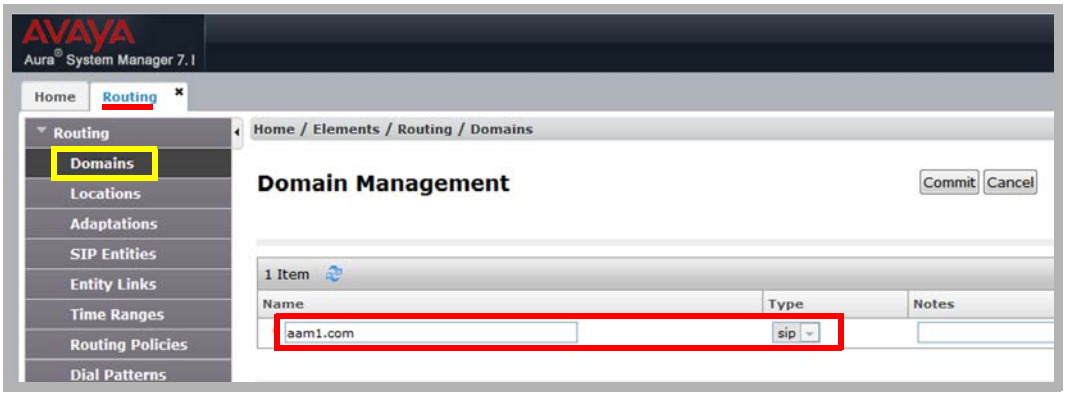
Launch a web browser, enter the following URL address **http://<IP address of System Manager>/SMGR** and log in with the appropriate credentials.



Go to **Routing > Domains**, and click on the **New** button (not shown) to create a new SIP Domain. Enter the following values and use default values for the remaining fields:

- **Name** – Enter the Authoritative Domain Name specified in **Configure IP Network Region on page 14**, which is aam1.com.
- **Type** – Select **SIP**

Click **Commit** to save. The following screen shows the Domains page used during the compliance test.



Configure Locations

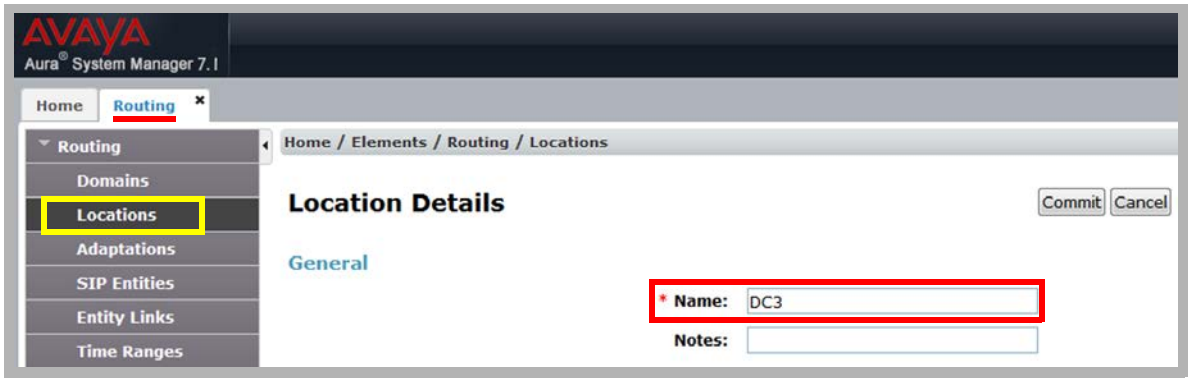
Locations are used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management or location-based routing.

Go to **Routing > Locations**, and click on the **New** button (not shown) to create a new SIP endpoint location.

General section

Enter the following values. Leave the remaining fields at their default values.

- Enter a descriptive Location name in the **Name** field (e.g. **DC3**).
- Enter a description in the **Notes** field if desired.



Configure SIP Entities

A SIP Entity must be added for Session Manager and for each network component that has a SIP trunk provisioned to Session Manager. During the compliance test, the following SIP Entities were configured:

- Session Manager itself.
- Communication Manager
- Avaya Messaging

Go to **Routing > SIP Entities**, and click on the **New** button (not shown) to create a new SIP entity. Provide the following information.

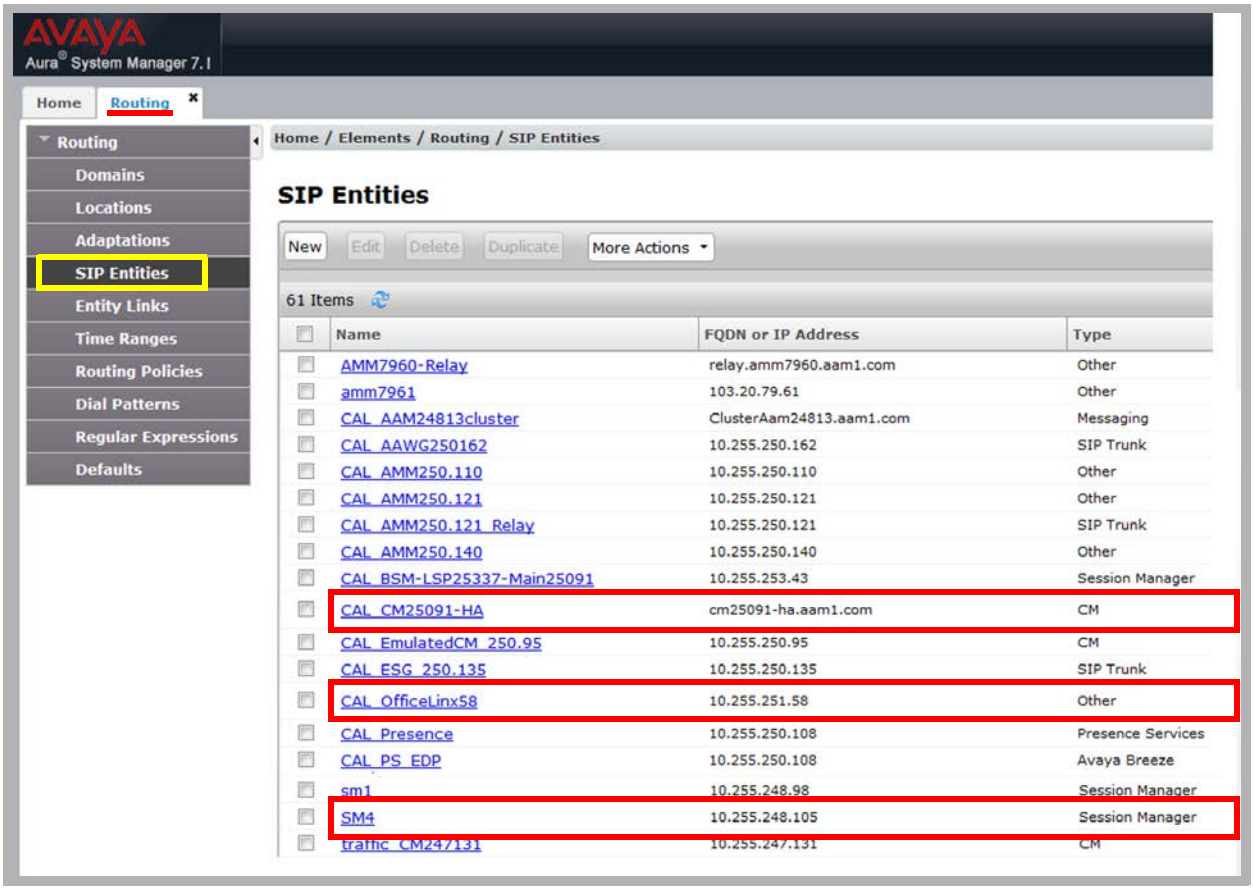
General section

Enter the following values and use default values for the remaining fields.

- Enter a descriptive Location name in the Name field.
- Enter IP address for signaling interface on each Communication Manager, virtual SM-100 interface on Session Manager, or 3rd party device on the FQDN or IP Address field.
- From the **Type** drop down menu select a type that best matches the SIP Entity:
  - For Communication Manager, select CM
  - For Session Manager, select Session Manager
  - For Avaya Messaging, select **Other**
- Enter a description in the **Notes** field if desired.
- Select the appropriate time zone.
- Accept the other default values.

Click on the **Commit** button to save each SIP entity. The following screen shows the SIP Entities page used during the compliance test.

Repeat for each new entity.



Configure Entity Links

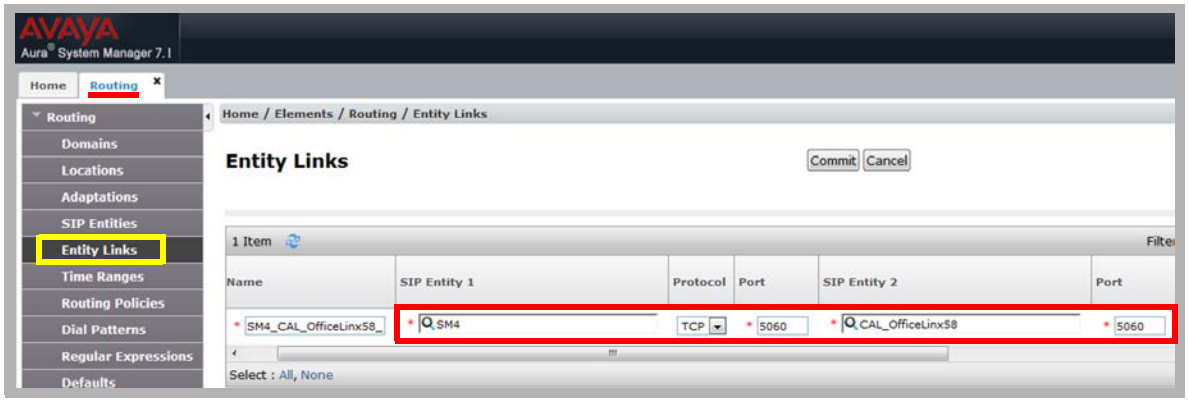
Entity Links define the connections between the SIP Entities and Session Manager. In the compliance test, the following entity links were defined from Session Manager.

- Session Manager <=> Communication Manager
- Session Manager <=> Avaya Messaging

Go to **Routing > Entity Links**, and click on the **New** button (not shown) to create a new entity link. Provide the following information:

- Enter a descriptive name in the **Name** field.
- In the **SIP Entity 1** drop down menu, select the Session Manager SIP Entity created in **Configure Entity Links on page 24** (e.g. SM4).
- In the **Protocol** drop down menu, select the protocol to be used.
- In the **Port** field, enter the port to be used (e.g. **5060** or **5061**).
  - TLS – 5061
  - UDP or TCP – 5060
- In the **SIP Entity 2** drop down menu, select one of the two entities in the bullet list above (which were created in **Configure SIP Entities on page 22**).
- In the **Port** field, enter the port to be used (e.g. **5060** or **5061**).
- Check the **Trusted** box.
- Enter a description in the **Notes** field if desired.

Click on the **Commit** button to save each Entity Link definition. The following screen shows an Entity Links page (between Session Manager and Avaya Messaging) used during the compliance test.



Repeat the steps to define Entity Links between Session Manager and Communication Manager.

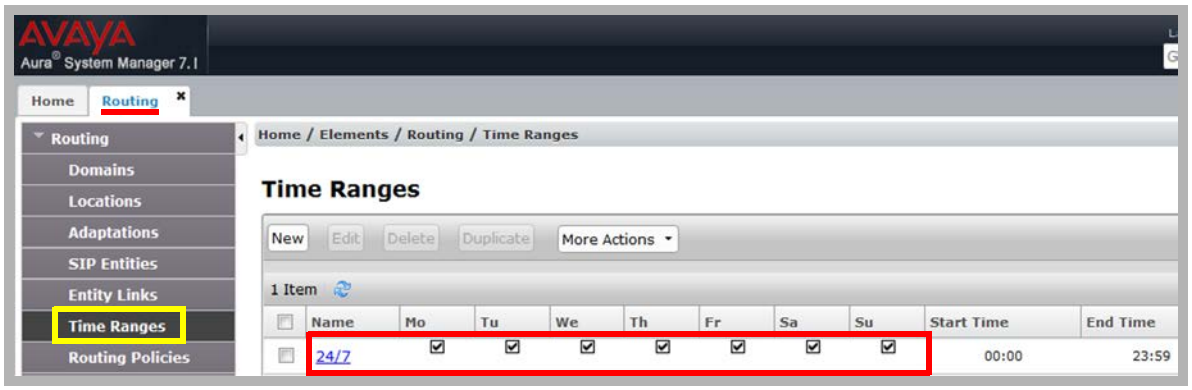
Time Ranges

The Time Ranges form allows admission control criteria to be specified for Routing Policies (**Configure Routing Policy on page 25**). In the reference configuration, no restrictions were used.

To add a Time Range, go to **Routing > Time Ranges**, and click on the **New** button (not shown). Provide the following information:

- Enter a descriptive Location name in the **Name** field (e.g. **24/7**).
- Check each day of the week.
- In the **Start Time** field, enter **00:00**.
- In the **End Time** field, enter **23:59**.
- Enter a description in the **Notes** field if desired.

Click the **Commit** button. The following screen shows the Time Range page used during the compliance test.



Configure Routing Policy

Routing Policies associate destination SIP Entities (**Configure SIP Entities on page 22**) with Time of Day admission control parameters (**Time Ranges on page 25**) and Dial Patterns (**Dial Patterns on page 26**). In the reference configuration, Routing Policies are defined for:

Inbound calls to Communication Manager.

Outbound calls to the Avaya Messaging

To add a Routing Policy, go to **Routing > Routing Policy**, and click on the **New** button (not shown) on the right. Provide the following information.

General section

- Enter a human friendly descriptive label in the **Name** field.
- Enter a description in the **Notes** field if desired.

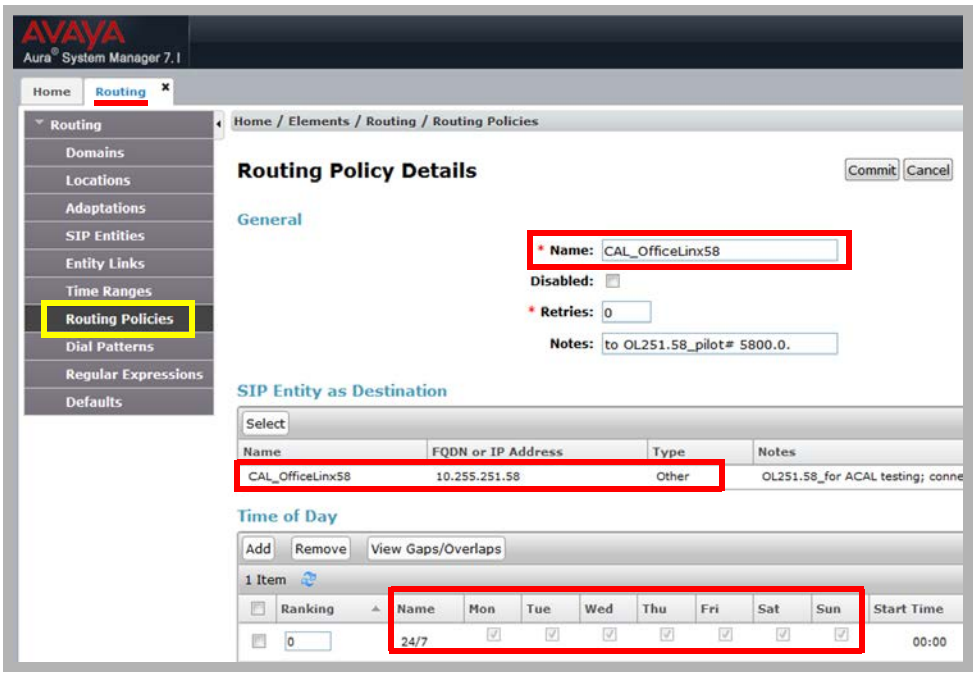
SIP Entity as Destination section

- Click the **Select** button.
- Select the SIP Entity that will be the destination for this call (not shown).
- Click the **Select** button and return to the Routing Policy Details form.

Time of Day section

- Leave as default values.

Click **Commit** to save the Routing Policy definitions. The following screen shows the Routing Policy used for Avaya Messaging during the compliance test.



Repeat the steps to define a routing policy to Communication Manager.

Dial Patterns

Dial Patterns define digit strings to be matched for inbound and outbound calls. In addition, the domain in the request URI is also examined. In the compliance test, the following dial patterns are defined from Session Manager.

- 71xxx – SIP endpoints in Avaya Communication Server.
- 58000 – Avaya Messaging voicemail number.

To add a Dial Pattern, select **Routing > Dial Patterns** and click on the **New** button (not shown) on the right. During the compliance test, a 5 digit dial plan was used. Provide the following information:

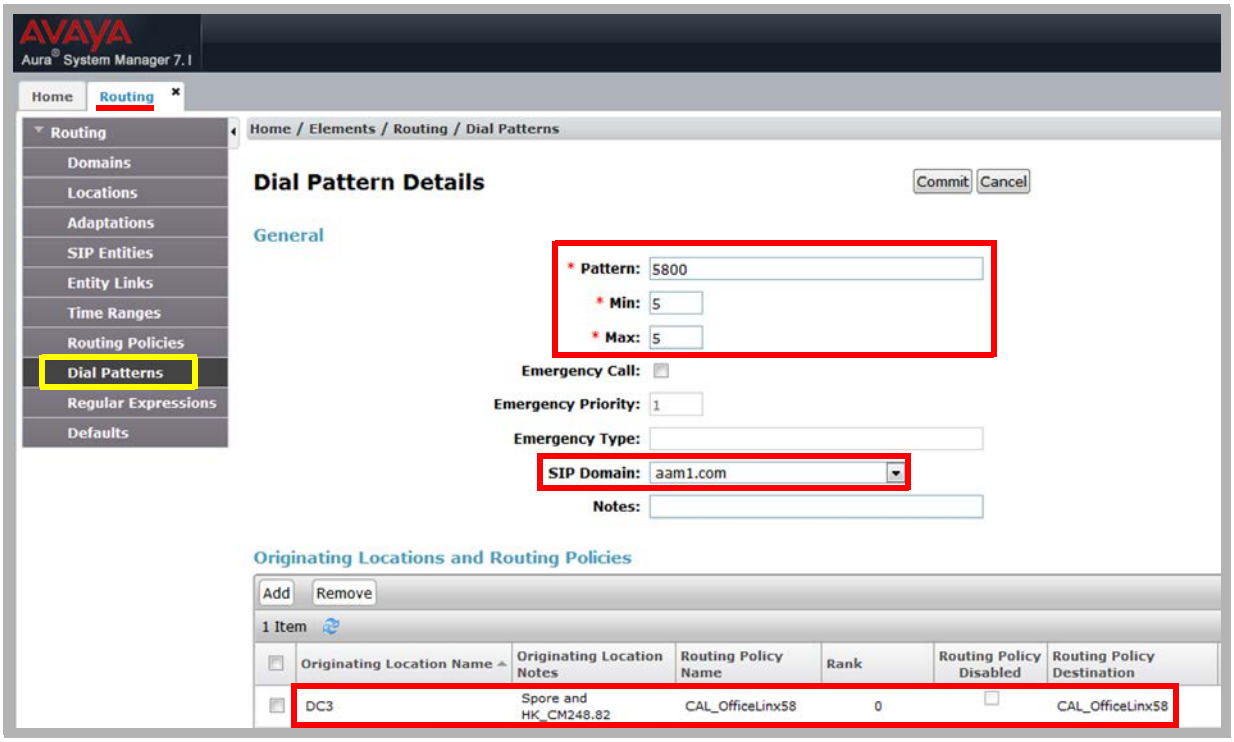
General section

- Enter a unique pattern in the **Pattern** field (e.g. **5800**).
- In the **Min** field enter the minimum number of digits (e.g. **5**).
- In the **Max** field enter the maximum number of digits (e.g. **5**).
- In the **SIP Domain** field drop down menu select the domain that will be contained in the Request URI received by Session Manager from Communication Manager.
- Enter a description in the **Notes** field if desired.

Originating Locations and Routing Policies section

- Click on the **Add** button and a window will open (not shown).
- Click on the boxes for the appropriate Originating Locations (see **Configure Locations on page 22**), and Routing Policies (see **Configure Routing Policy on page 25**) that pertain to this Dial Pattern.
  - Location **DC3**.
  - Routing Policies **CAL_Avaya Messaging58**.
  - Click on the **Select** button and return to the Dial Pattern window.

Click the **Commit** button to save the new definition. The following screen shows the dial pattern used for Avaya Messaging during the compliance test.



Configure Managed Elements

To define a new Managed Element, navigate to **Elements > Inventory > Manage Elements**.

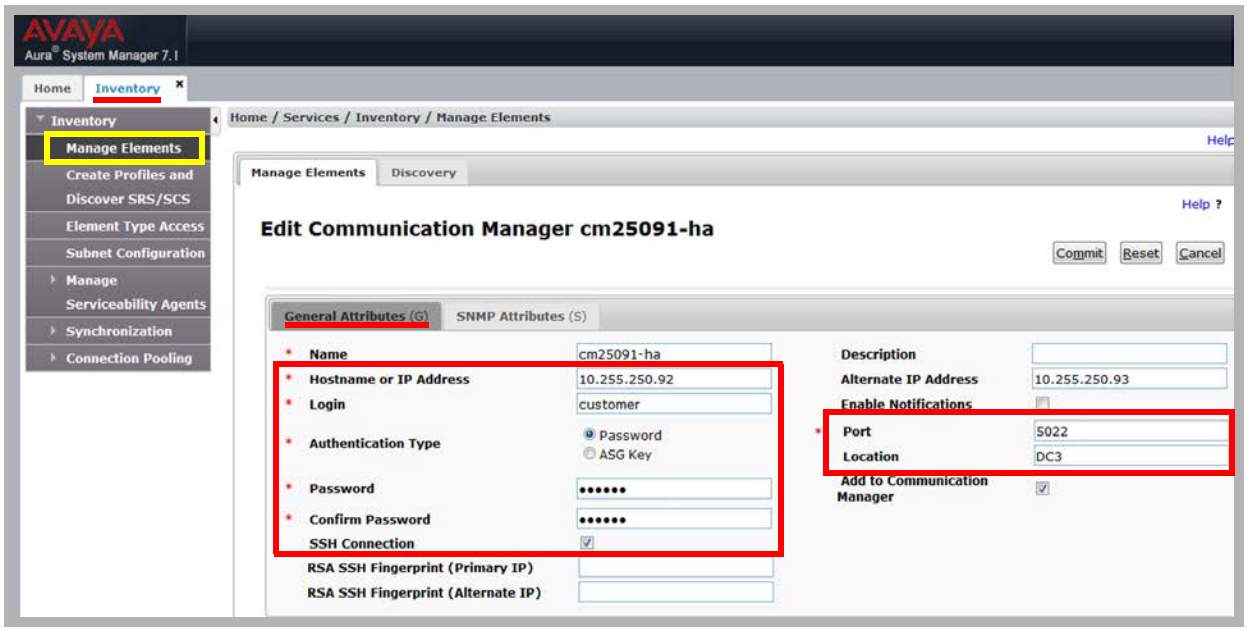
Click on the **New** button (not shown) to open the **New Entities** Instance page.

In the **New Entities Instance** Page:

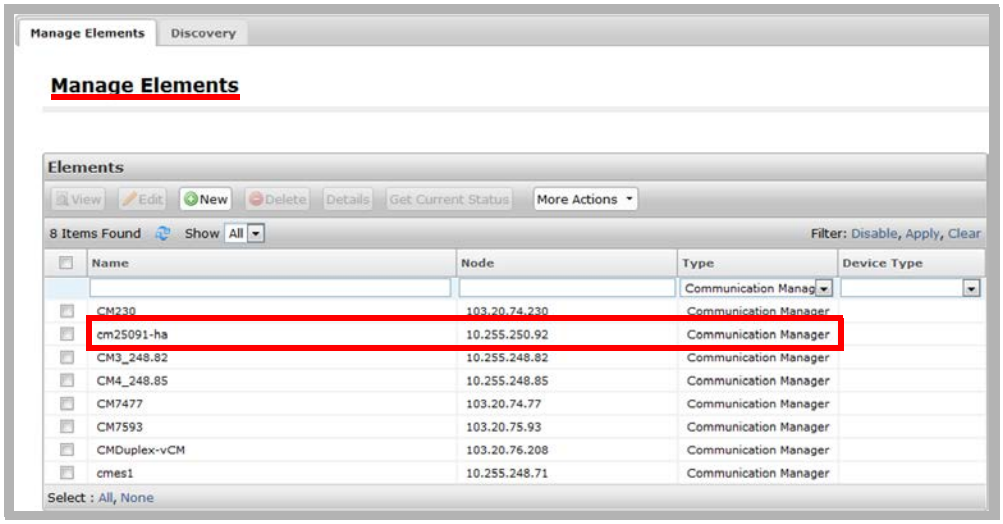
- In the **Type** field, select **CM** using the drop-down menu. The **New CM Instance** page opens (not shown).

In the New CM Instance Page, provide the following information:

- **Name** – Enter name for Communication Manager Feature Server.
- **Description** - Enter a description if desired.
- **Hostname or IP Address** – Enter the IP address of the administration interface. During the compliance test, the procr IP address (10.255.250.92, Note: CM-Duplex was used) was utilized.
- **Login** – Enter the username for administration access.
- **Password** – Enter password used for administration access.
- **Confirm Password** – Repeat value entered in above field.
- **Is SSH Connection** – Enable the checkbox.
- **Port** – Verify **5022** has been entered as default value.



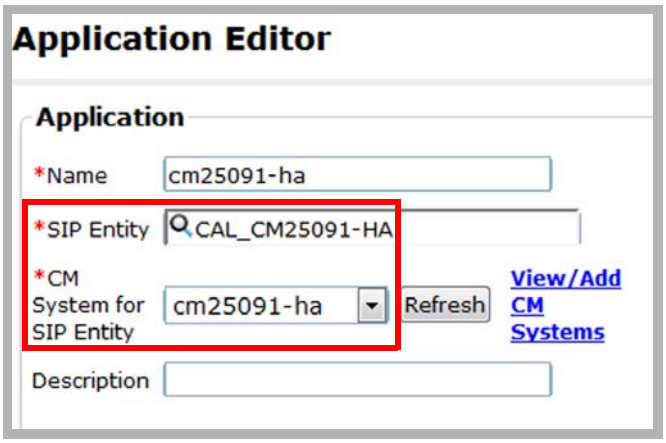
Click **Commit** to save the element. The following screen shows the element created, cm25091-ha, during the compliance test.



Configure Applications

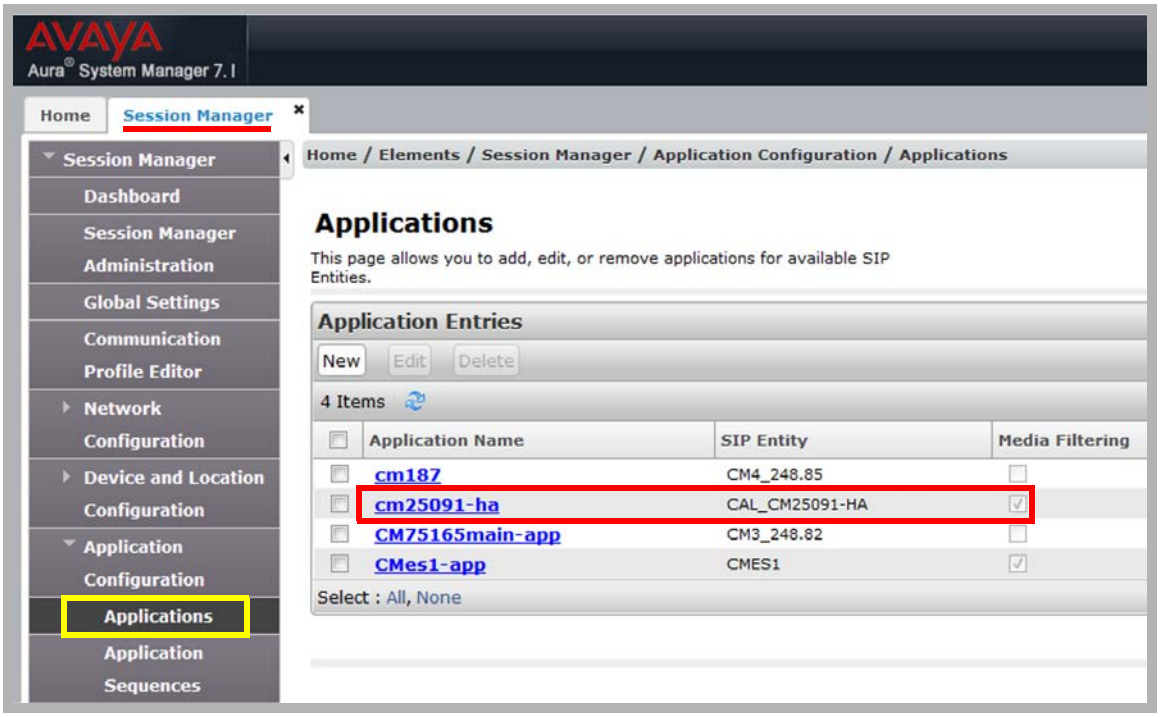
To define a new Application, go to **Elements > Session Manager > Application Configuration > Applications**. Click **New** (not shown) to open the Applications Editor page. Provide the following information.

- Application Editor section
  - **Name** – Enter name for the application.
  - **SIP Entity** - Select SIP Entity for the Communication Manager Feature Server defined in **Configure SIP Entities on page 22**
  - **CM System for SIP Entity** – Select name of Managed Element defined for Communication Manager in **Configure Managed Elements on page 28**
  - **Description** – Enter description if desired.



- Leave fields in the Application Attributes (optional) section blank.

Click the **Commit** button to save the Application. The screen below shows the Application, CM-FS defined for Communication Manager.



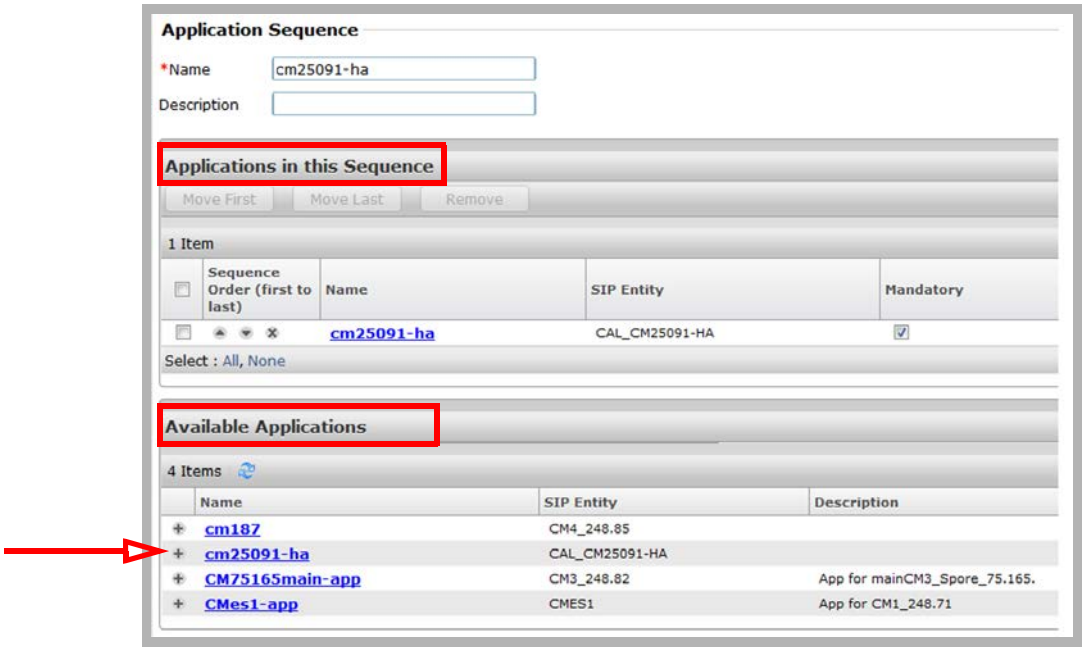
Define Application Sequence

Go to **Elements > Session Manager > Application Configuration > Application Sequences**.
Click **New** (not shown) and provide the following information.

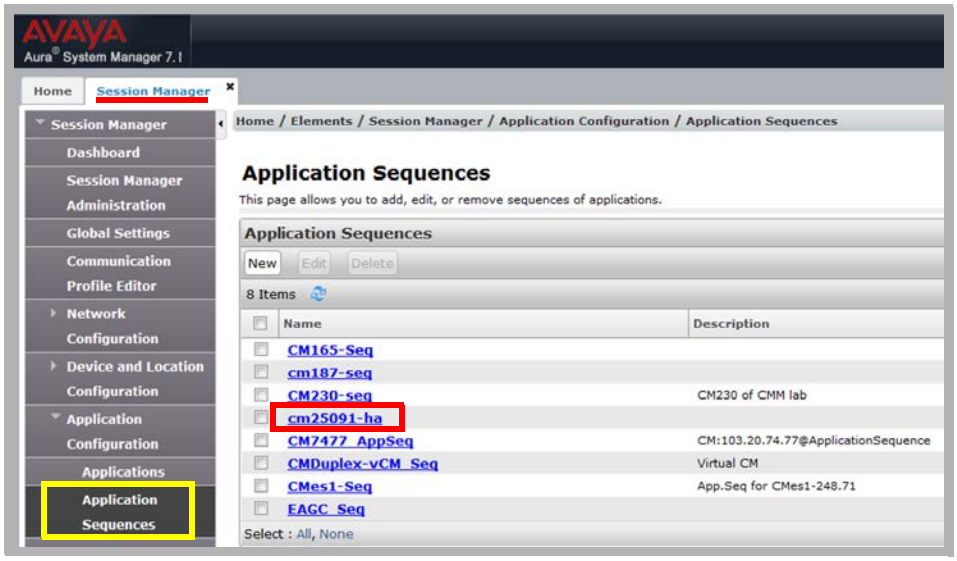
- Application Sequence section
  - **Name** – Enter name for the application.
  - **Description** – Enter description, if desired.

- Available Applications section
  - Click the **+** icon associated with the Application for Communication Manager defined in **Configure Applications on page 30** to select this application.
  - Verify a new entry is added to the Applications in this Sequence table as shown below.

Click the **Commit** button to save the new Application Sequence.



The screen below shows the Application Sequence, CM-FS defined during the compliance test.



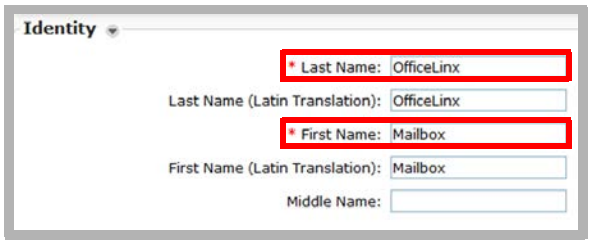
Repeat these steps if multiple applications are needed as part of the Application Sequence.

Configure SIP Users

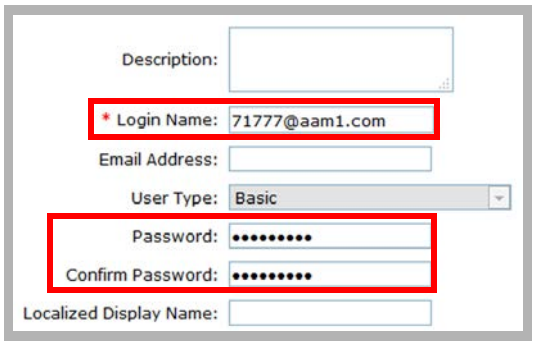
Add new SIP users for each 9600-Series SIP station. Alternatively, use the option to automatically generate the SIP station after adding a new SIP user.

To add new SIP users, go to **Users > Manage Users**.
Click **New (not shown)** and provide the following information.

- Identity section
  - **Last Name** – Enter last name of user.
  - **First Name** - Enter first name of user.



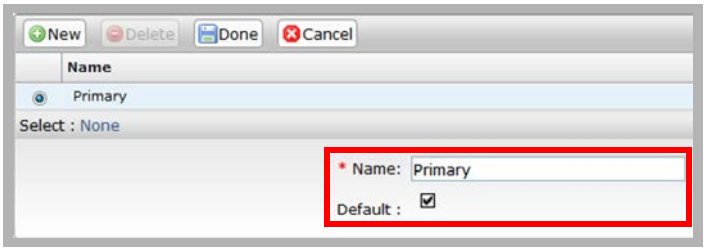
  - **Login Name** – Enter extension number@sip domain defined in **Configure IP Network Region on page 14**.
  - **Authentication Type** – Verify **Basic** is selected.
  - **SMGR Login Password** – Enter password to be used to log into System Manager.
  - **Confirm Password** – Repeat value entered above.



- Communication Profile section

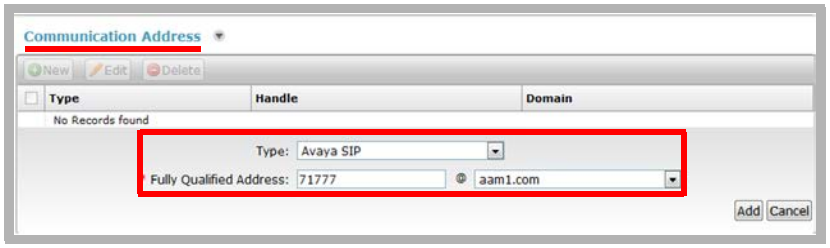
Verify there is a default entry identified as the Primary profile for the new SIP user. If an entry does not exist, select New and enter values for the following required attributes:

  - **Name** – Enter **Primary**.
  - **Default** – **Enable** the check box.

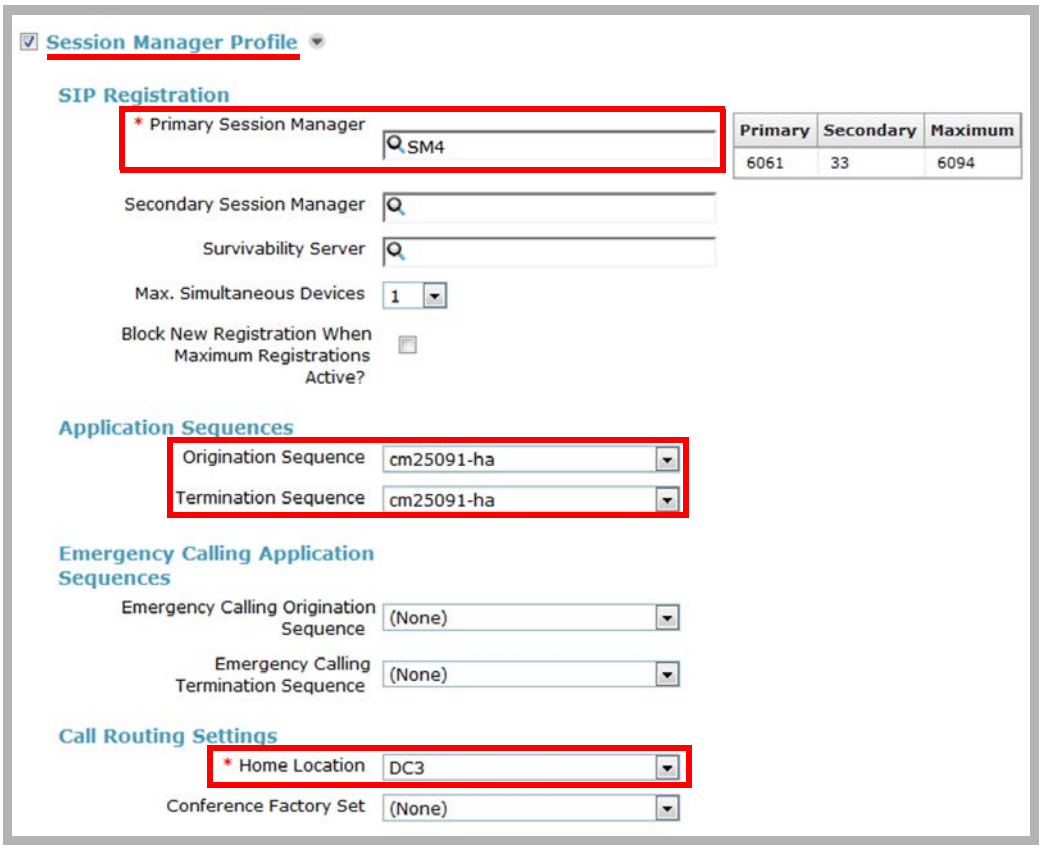


- Communication Address sub-section
  Select **New** to define a **Communication Address** for the new SIP user. Provide the following information:
  - **Type** – Select **Avaya SIP** using the dropdown menu.
  - **Fully Qualified Address** – Enter same extension number and domain used for Login Name, created previously.

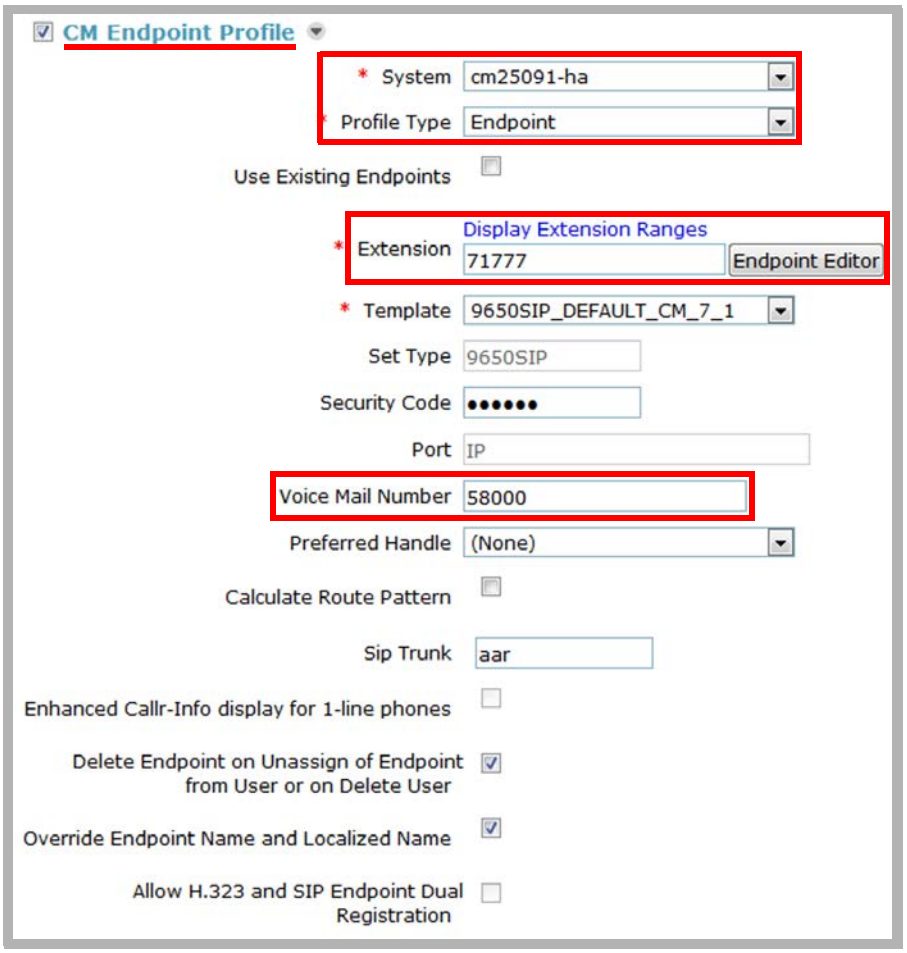
Click the **Add** button to save the Communication Address for the new SIP user.



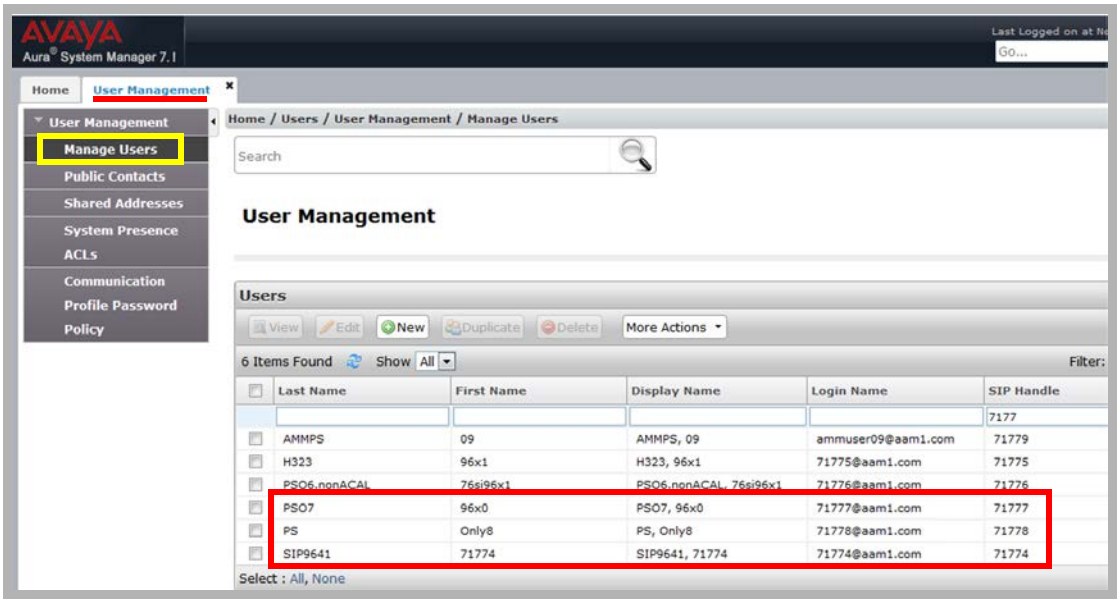
- Session Manager Profile section
  - **Primary Session Manager** – Select one of the Session Managers.
  - **Secondary Session Manager** – Leave this field empty.
  - **Origination Application Sequence** – Select the Application Sequence defined in **Define Application Sequence on page 31** for Communication Manager.
  - **Termination Application Sequence** – Select the Application Sequence defined in **Define Application Sequence on page 31** for Communication Manager.
  - **Survivability Server** – Leave this field empty.
  - **Home Location** – Select Location defined in **Configure Locations on page 22**.



- CM Endpoint Profile section
  - **System** – Select Managed Element defined in **Configure Managed Elements on page 28** for Communication Manager Feature Server.
  - **Use Existing Endpoints** - Leave this unchecked to automatically create a new endpoint when a new user is created. Otherwise, check the box if an endpoint is already defined in Communication Manager.
  - **Extension** - Enter same extension number used in this section.
  - **Template** – Select template for type of SIP phone.
  - **Security Code** – Enter a numeric value used to logon to a SIP telephone.
  - **Port** – Select **IP** from the drop down menu.
  - **Voice Mail Number** – Enter the **Voicemail Number** of the Avaya Messaging server (e.g. 58000).
  - **Delete Station on Unassign of Endpoint** – Check the box to automatically delete a station when Endpoint Profile is un-assigned from user.



Click **Commit** to save the definition of the new user. The following screen shows the created users during the compliance test.

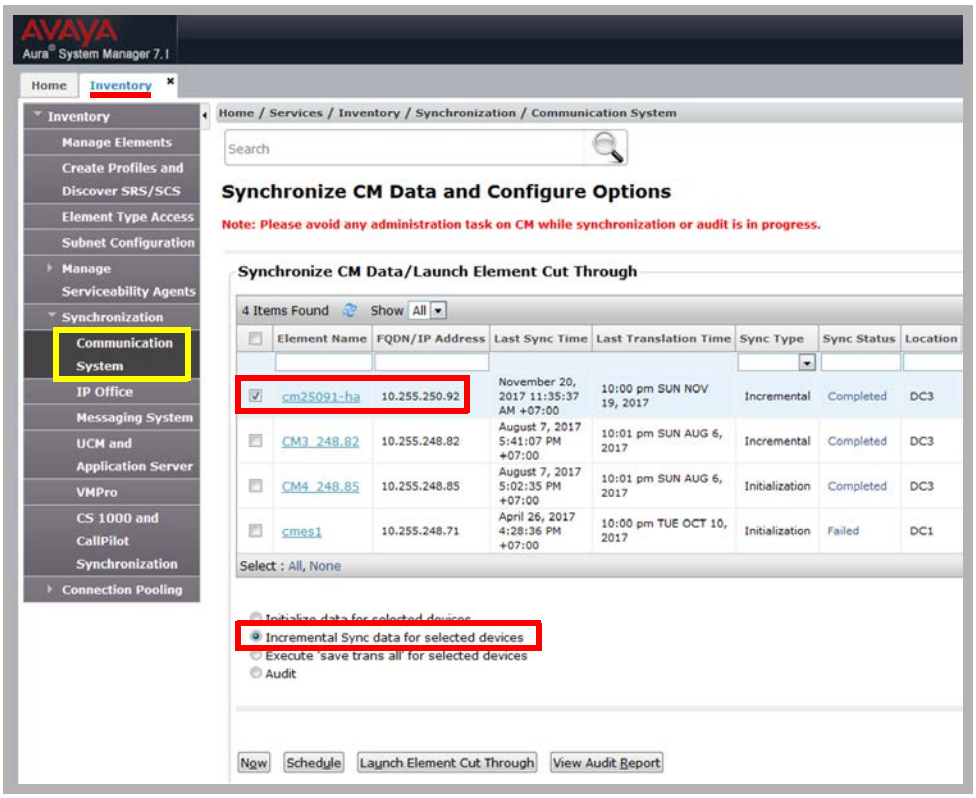


Synchronization Changes with Avaya Aura Communication Manager

After completing these changes in System Manager, perform an on demand synchronization.
Go to **Elements > Inventory > Synchronization > Communication System**.

On the **Synchronize CM Data and Configure Options** page, expand the **Synchronize CM Data/Launch Element Cut Through** table:

- Enable the radio button to select the **Incremental Sync data for selected devices** option. Click **Now** to start the synchronization.
- Use the **Refresh** button in the table header to verify status of the synchronization.
- Synchronization has successfully finished when the Sync. Status column shows **Completed**.



Avaya Messaging Configuration

SIP Config Tool

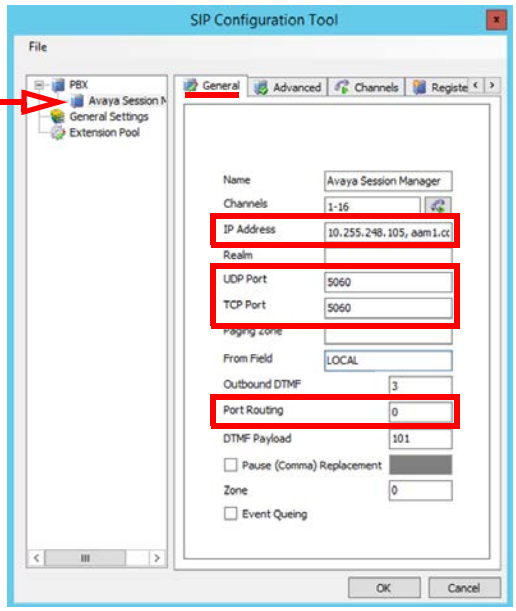
This section describes the interface configuration allowing Avaya Messaging to communicate with the Avaya Aura Session Manager. Highlighted values are the ones that were configured for the compliance test.

Integration of Avaya Messaging with Avaya Aura Session Manager is done from Avaya Messaging's SIP Configuration Tool.

Open **Start > All program > Avaya Messaging > SIP Configurator**.

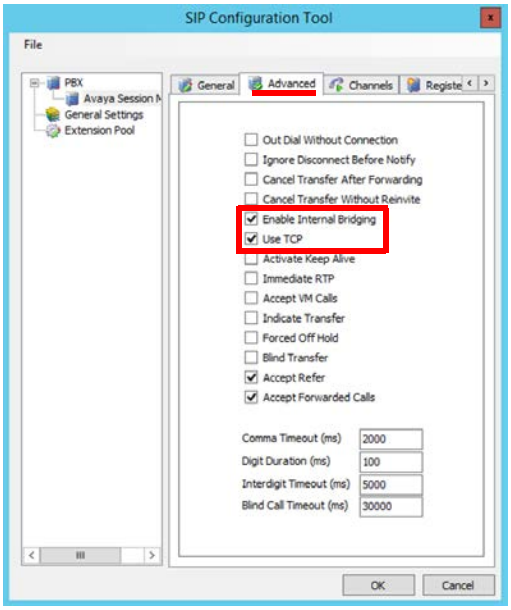
Select **Avaya** under PBX in the left pane.

Provide the following information:



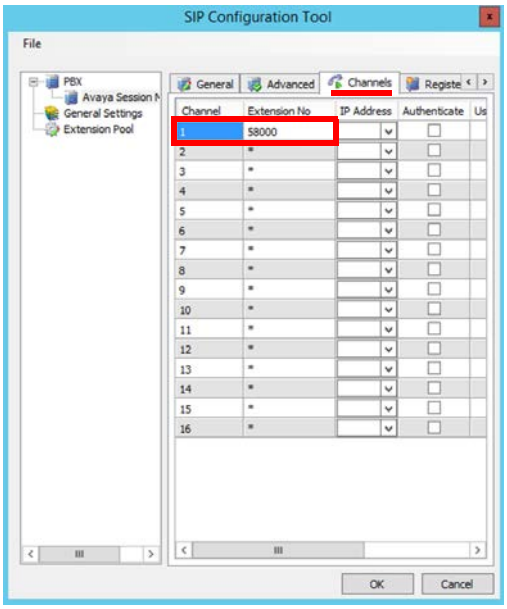
- **IP Address** – Enter the **IP address** and **Domain** in the field.
- **UDP Port** – Enter **5060**.
- **TCP Port** – Enter **5060**.
- **Port Routing** - Enter **0**.

Click the **Advanced** tab in the right pane, and enable the following:



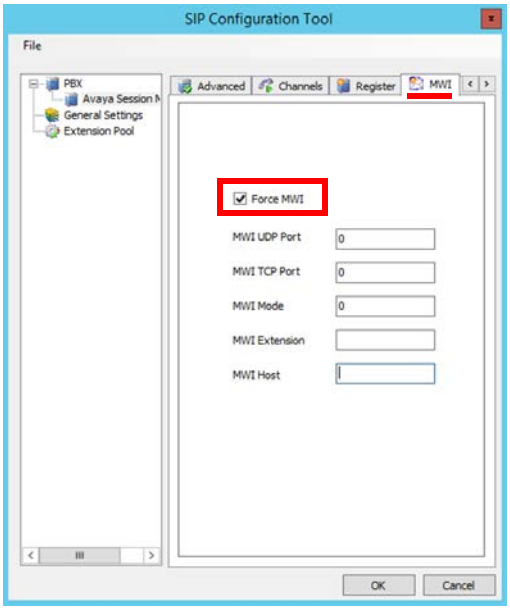
- **Enable Internal Bridging**
- **Use TCP**

On the **Channels** tab, and provide the Avaya Messaging extension. During the compliance test, extension 58000 was used for the Avaya Messaging extension.

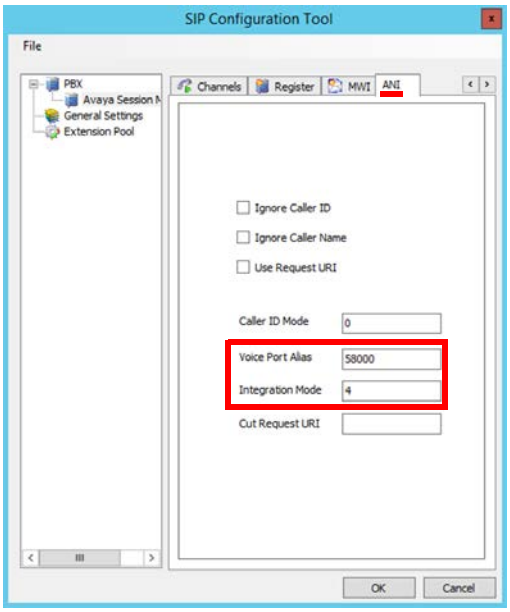


On the **MWI** tab, and check the **Force MWI** check box.

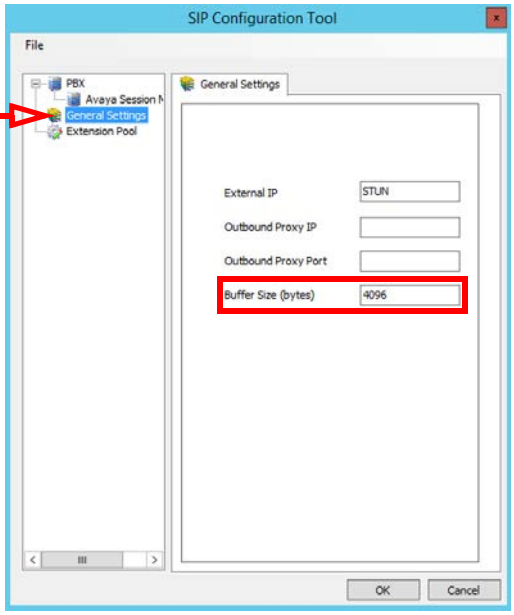
Click on the **OK** button.



On the **ANI** tab, enter the Hunt Group in the **Voice Port Alias** field. Verify that **Integration Mode** is set to **4**.



Go to the **General Settings** menu and enter **4096** for the **Buffer Size** field.



Verification Steps

The following steps may be used to verify the integration:

- From the Communication Manager SAT, use the status signaling-group command to verify that the SIP signaling group is in-service.
- From the Communication Manager SAT, use the status trunk-group command to verify that the SIP trunk group is in-service.
- Verify that calls can be placed to Avaya Messaging and key features are working.
    - Place a call to the Avaya Messaging main service number. Log on as a new mailbox user and complete the mailbox initialization process.
    - Place a call to this CM station. Test for no answer and that the call is passed to Avaya Messaging. Hear the greeting of the called party's mailbox and verify that you are able to record a message.
    - Ensure that the MWI on client telephones is updated properly based upon mailbox status.
    - Log onto an Avaya Messaging mailbox and retrieve messages, manage message lists, create/modify greetings and so on.
    - Dial into the Avaya Messaging voice menu or directory service numbers, then transfer out to a CM station or off-net destination.
- Verify with the list trace tac command that calls are using the correct trunk and coverage.

Additional References

Product documentation for Avaya products may be found at:

http://support.avaya.com

Product documentation for Avaya Messaging may be found at:

http://resources.zang.io

APPENDIX A: REVISION HISTORY

Date	Issue	Change Summary
5 April, 2019	10.7 (1)	● Initial document release.
3 December, 2020	10.8 (2)	● Correct an issue with configuring SIP (IP-IP Direct Audio should be N.
1 October, 2021	10.8 (3)	● Updated SIP configuration to specify setting Port Routing = 0.