Avaya Solution & Interoperability Test Lab

Application Notes for Synergem Evolution 911 Elite™ with Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Aura® Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Synergem Evolution 911 Elite™ which were compliance tested with Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Aura® Application Enablement Services.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the procedures for configuring Synergem Evolution 911 Elite™ (Evolution 911 Elite) endpoints, which were compliance tested with Avaya Aura® Communication Manager (Communication Manager), Avaya Aura® Session Manager (Session Manager) and Avaya Aura® Application Enablement Services (AES). Evolution 911 Elite SIP endpoint registers to Session Manager via TCP. Evolution 911 Elite also uses AES' DMCC API for logging in agents for Automatic Call Distributer (ACD) functionality.

Evolution 911 Elite, Synergem's call-taking solution, is user-friendly and was designed from the ground up to optimize the capabilities delivered by a Next Generation 9-1-1 ESInet built to the i3 standards (See NENA i3 standard). Evolution 911 Elite has, at its core, Avaya Aura™ Call Center Elite. Features of Avaya Aura™ Call Center Elite are available within Evolution 911 Elite.

Evolution 911 Elite provides all of the capabilities required to execute the call taking function in a Next Generation Public Safety Answering Point (PSAP). In addition, the system supports all of the required interfaces to other functional elements in a fully developed Next Generation 9-1-1 system.

The Evolution 911 Elite user interface provides the capability to answer incoming calls, place outgoing calls, release calls, manage calls (mute, hold, conference, transfer, speed dials, etc.), provide caller location information, log into Avaya ACD and provide access to agency contact lists. The windows based GUI is user friendly and customizable by agency and end user.

These Application Notes assume that Communication Manager and Session Manager are already installed and basic configuration steps have been performed. Only steps relevant to this compliance test will be described in this document. For further details on configuration steps not covered in this document, consult references [1], [2], and [3].

2. General Test Approach and Test Results

The general test approach was to place calls to and from Evolution 911 Elite and exercise basic telephone and ACD operations. The main objectives were to verify the following:

- Registration
- Codecs (G.711MU)
- DTMF (SIP INFO)
- Inbound calls
- Outbound calls
- Hold/Resume
- Call termination (origination/destination)
- Conferences and transfers
- Agent log-in, log-out and states
- Serviceability

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

2.1. Interoperability Compliance Testing

The interoperability compliance test included features and serviceability. The focus of the interoperability compliance testing was primarily on verifying call establishment on Evolution 911 Elite. Evolution 911 Elite operations such as inbound calls, outbound calls, hold/resume, transfer, conference, and Evolution 911 Elite interactions with Session Manager, AES, and Avaya SIP, H.323, and digital telephones were verified. The serviceability testing introduced failure scenarios to see if Evolution 911 Elite can recover from failures.

2.2. Test Results

The test objectives were verified. For serviceability testing, Evolution 911 Elite operated properly after recovering from failures such as cable disconnects, and resets of Evolution 911 Elite, and Session Manager and AES. The features tested worked as expected.

2.3. Support

Technical support on Synergem Evolution 911 Elite™ can be obtained through the following:
Phone: 1-866-859-0911
Email: support@synergemtech.com
Web: www.synergemtech.com/support

3. Reference Configuration

Figure 1 illustrates a sample configuration consisting of Communication Manager, an Avaya G430 Media Gateway, a Session Manager, System Manager and Evolution 911 Elite. The solution described herein is also extensible to other Avaya Media Servers and Media Gateways. For completeness, an Avaya 9600 Series H.323 IP Deskphones and Avaya 9600 Series SIP IP Deskphones are included in **Figure 1** to demonstrate calls between the SIP-based Evolution 911 Elite and Avaya SIP, H.323, and digital telephones. For security reasons, the IP Addresses in the diagram have been changed to private IP Addresses.

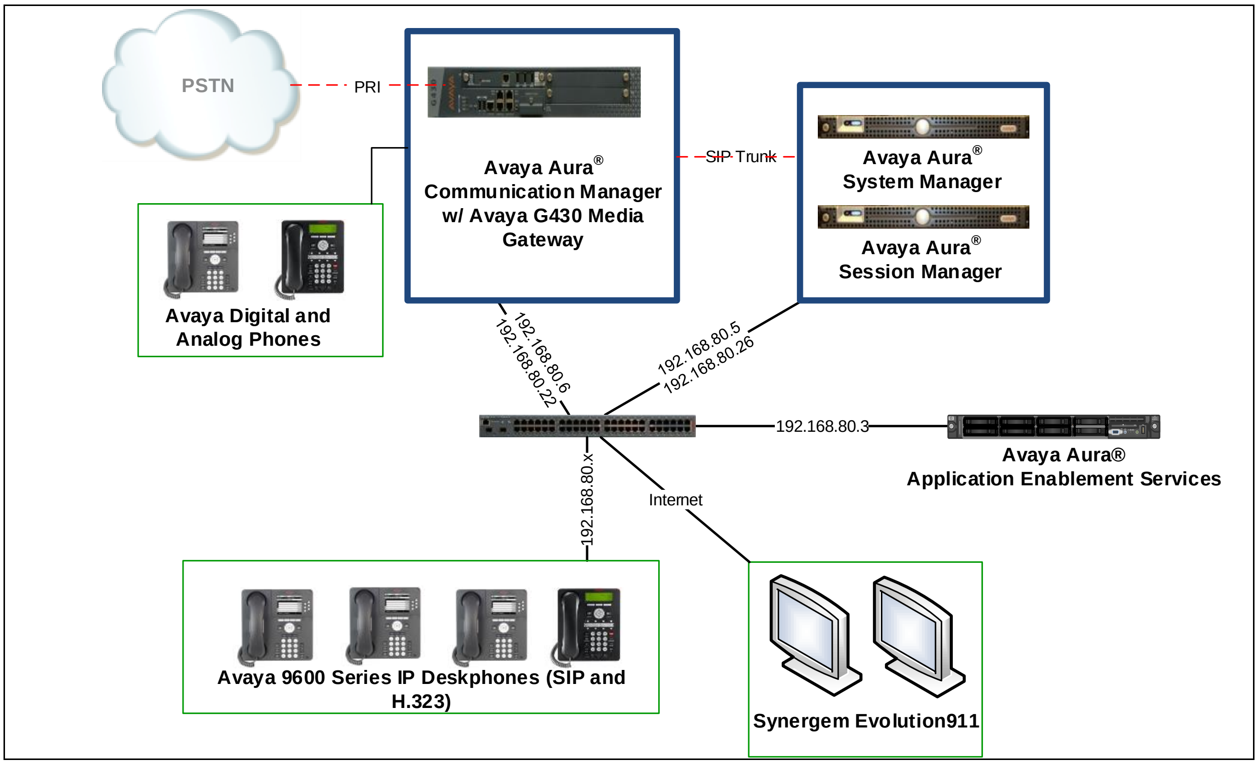


Figure 1: Test Configuration of Evolution 911 Elite by Synergem

4. Equipment and Software Validated

The following equipment and software were used for the test configuration.

Equipment		Software/Firmware
Avaya Aura® Communication Manager		7.0 SP3
Avaya Aura® System Manager		7.0.1.2
Avaya Aura® Session Manager		7.0.1.2
Avaya G430 Media Gateway		37.41.0
Avaya Aura® Application Enablement Services		7.0.1 Super Patch 3
Avaya 9600 Series Deskphones		
	96x1 (SIP) 96x1 (H.323) 96x0 (SIP)	7.0.1.4 6.6.4 2.6.16
Evolution 911 Elite™ by Synergem		4.0.0.35

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for setting up a SIP trunk between Communication Manager and Session Manager. The steps include setting up 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 if there is enough capacity to setup an additional trunk. 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. Evolution 911 Elite and other SIP telephones are configured as off-PBX telephones in Communication Manager.

5.1. Capacity Verification

Enter the **display system-parameters customer-options** command. Verify that there are sufficient **Maximum Off-PBX Telephones – OPS** licenses. If not, 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: 48000 28
                                      Maximum Stations: 36000 9
                              Maximum XMOBILE Stations: 36000 0
                    Maximum Off-PBX Telephones - EC500: 41000 0
                    Maximum Off-PBX Telephones -   OPS: 41000 6
                    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   0
```

On **Page 2** of the form, verify that the number of SIP trunks supported by the system is sufficient for the number of SIP trunks needed. If not, 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 4
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 128   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 36000 0
                   Maximum Video Capable IP Softphones: 18000 0
                       Maximum Administered SIP Trunks: 12000 10
  Maximum Administered Ad-hoc Video Conferencing Ports: 12000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
```

5.2. 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 communications between Communication Manager and Session Manager. Enter the **change ip-codec-set <c>** command, where **c** is a number between **1** and **7**, inclusive. IP codec sets are used in **Section 5.3** for configuring IP network region to specify which codec sets may be used within and between network regions. For the compliance testing, G.711MU was tested for verification.

```
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:
 3:
 4:
 5:
 6:
 7:
```

5.3. Configure IP Network Region

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

- **Authoritative Domain** – Enter the appropriate name for the Authoritative Domain. Set to the appropriate domain. During the compliance test, the authoritative domain is set to **avaya.com**. This should match the SIP Domain value on Session Manager, in **Section 6.1**.
- **Intra-region IP-IP Direct Audio** – Set to **yes** to allow direct IP-to-IP audio connectivity between endpoints registered to Communication Manager or Session Manager in the same IP network region. The default value for this field is **yes**.
- **Codec Set** – Set the codec set number as provisioned in **Section 5.2**.
- **Inter-region IP-IP Direct Audio** – Set to **yes** to allow direct IP-to-IP audio connectivity between endpoints registered to Communication Manager or Session Manager in different IP network regions. The default value for this field is **yes**.

```
change ip-network-region 1                                     Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1        Authoritative Domain: avaya.com
    Name: Default               Stub Network Region: n
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: 44
        Audio PHB Value: 44
        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
```

5.4. Configure IP Node Name

This section describes the steps for setting 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.

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
default             0.0.0.0
procr               192.168.80.6
procr6              ::
publicaes           192.168.80.3
publicsm            192.168.80.5
```

5.5. Configure SIP Signaling

This section describes the steps for administering a signaling group in Communication Manager for communication between Communication Manager and Session Manager. Enter the **add signaling-group <s>** command, where **s** is an available signaling group and configure the following:

- **Group Type** – Set to **sip.**
- **Transport Method –** Set to **tls**
- **Near-end Node Name** – Set to **procr**.
- **Far-end Node Name** – Set to the Session Manager name configured in **Section 5.4**.
- **Far-end Network Region** – Set to the region configured in **Section 5.3**.
- **Far-end Domain** – Set to **avaya.com**. This should match the SIP Domain value in **Section 6.1**.
- **Direct IP-IP Audio Connections** – Set to **y**, since Media Shuffling is enabled during the compliance test

```
add signaling-group 1                                        Page   1 of   3
                                SIGNALING GROUP

 Group Number: 1              Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? n                                 Enforce SIPS URI for SRTP? n
  Peer Detection Enabled? n  Peer Server: SM
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
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: publicsm
 Near-end Listen Port: 5061               Far-end Listen Port: 5061
                                       Far-end Network Region: 1

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? y
         Enable Layer 3 Test? y                   Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 6
```

5.6. Configure SIP Trunk

This section describes the steps for administering a trunk group in Communication Manager for communication between Communication Manager and Session Manager. Enter the **add trunk-group <t>** command, where **t** is an unallocated 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.
- **Outgoing Display –** Set to **y**.
- **Signaling Group** – Set to the Group Number field value configured in **Section 5.5**.
- **Number of Members –** Allowed value is between 0 and 255. Set to a value large enough to accommodate the number of SIP telephone extensions being used.

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

Group Number: 1                     Group Type: sip          CDR Reports: y
  Group Name: publicsm                     COR: 1        TN: 1        TAC: 101
   Direction: two-way        Outgoing Display? y
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type: tie                    Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 1
                                                     Number of Members: 10
```

5.7. Configure CTI-link

This section describes the steps for administering a CTI Link for AES. Enter the **add cti-link <c>** command, where **c** is an unallocated cti link.

- **Extension –** Type in an available extension number.
- **Type –** Set to **ADJ-IP**.
- **Name –** Type in a descriptive name.

```
add cti-link 1                                                    Page   1 of   3
                                    CTI LINK
 CTI Link: 1
Extension: 12090
     Type: ADJ-IP
                                                                             COR: 1

     Name: publicaes
```

5.8. Configure ip-services

This section describes configuration required to configure ip services for AES. Enter the **change ip-services** command and configure Page 4 as following:

- For a row available, configure the host name of AES in **AES Services Server** and set a password in **Password.**

```
change ip-services                                                   Page   3 of   3
                            AE Services Administration

   Server ID    AE Services        Password          Enabled    Status
                     Server
      1:      publicaes         *                    y        in use
```

6. 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.

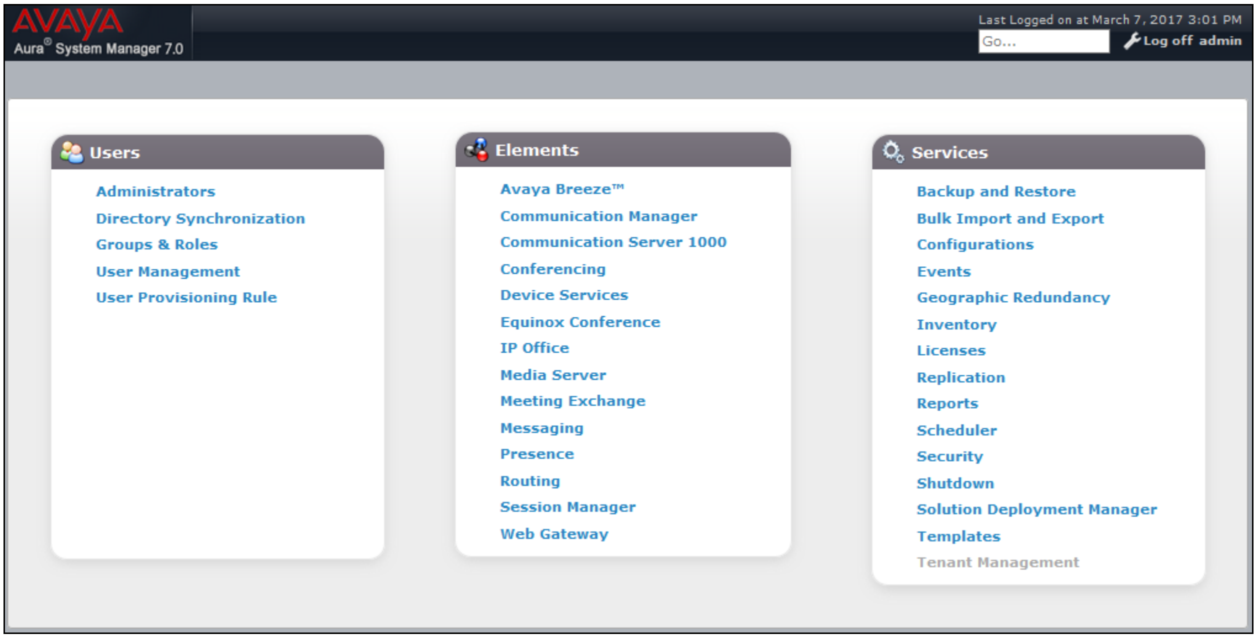
The following sections assume that Session Manager and System Manager have been installed and that network connectivity exists between the two platforms.

In this section, the following topics are discussed:

- SIP Domains
- Locations
- SIP Entities
- Entity Links
- Time Ranges
- Routing Policy
- Dial Patterns
- User Management

6.1. Configure SIP Domain

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

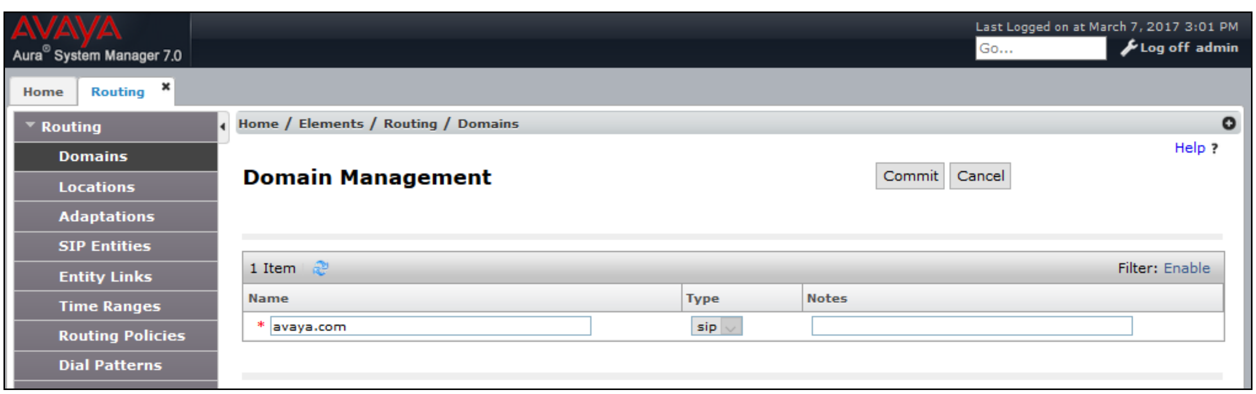


In the main menu, navigate to **Elements → Routing → Domains**, and click on the **New** button (not shown) to create a new SIP Domain. Enter the following values and use default values for remaining fields:

- **Name** – Enter the Authoritative Domain Name specified in **Section 5.3**, which is **avaya.com**.
- **Type** – Select **SIP**

Click **Commit** to save.

The following screen shows the Domains page used during the compliance test.



6.2. 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.

From the main menu, navigate to **Elements → Routing → Locations**, and click on the **New** button (not shown) to create a new SIP endpoint location.

General section

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

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

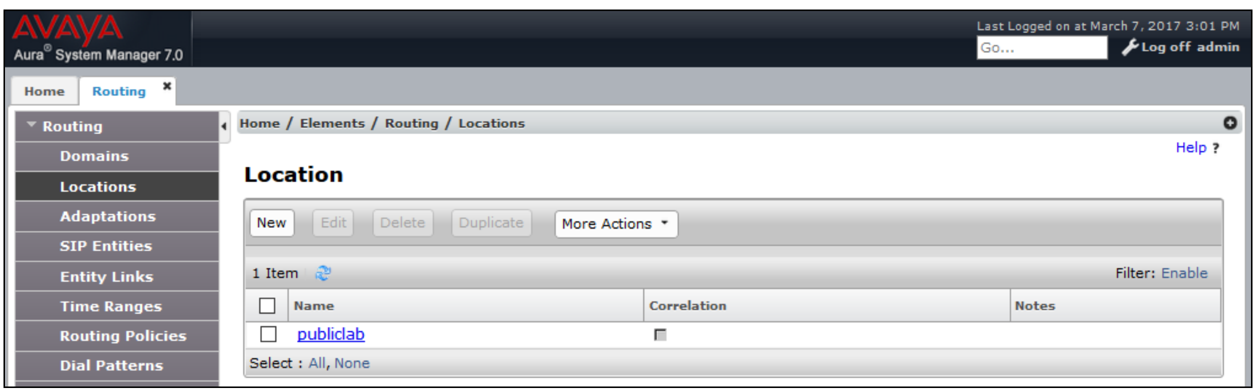
Location Pattern section

Click **Add** and enter the following values:

- Enter the IP address information for the **IP address Pattern** field (e.g. **192.168.***).
- Enter a description in the **Notes** field if desired.

Repeat steps in the Location Pattern section if the Location has multiple IP segments. Modify the remaining values on the form, if necessary; otherwise, use all the default values. Click on the **Commit** button.

The following screen shows the Locations list used during the compliance test.



6.3. 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. This entity was created prior to the compliance test.
- Communication Manager. This entity was created prior to the compliance test.

Navigate 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 remaining fields.

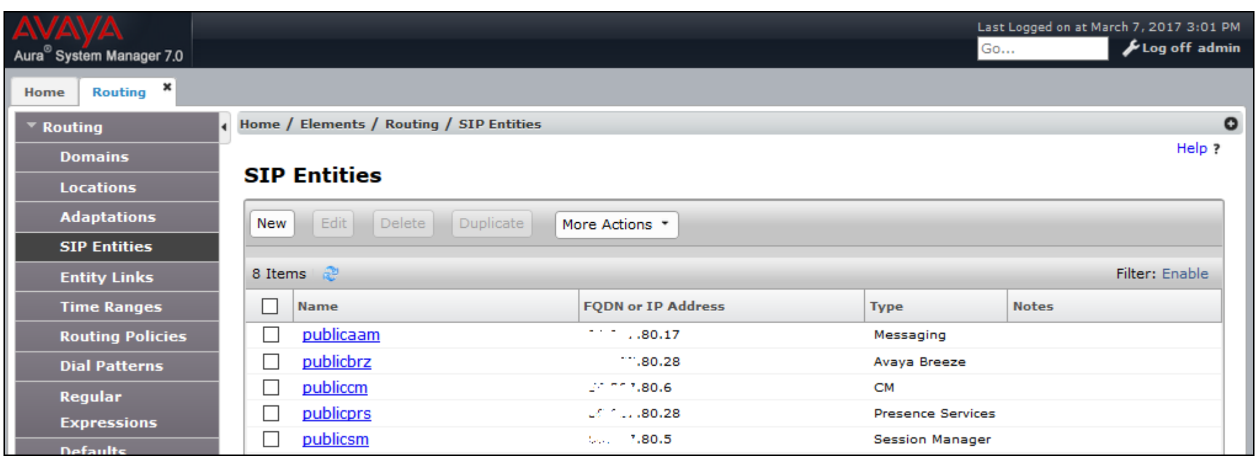
- Enter a descriptive Entity name in the **Name** field.
- Enter IP address for signaling interface on each Communication Manager, Session Manager, or 3rd party device in the **FQDN or IP Address** field
- From the **Type** drop down menu select a type that best matches the SIP Entity.
  - For Communication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

SIP Link Monitoring section

- 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 all the steps for each new entity.



The IP Addresses in the screen capture above have been brushed for security reasons.

6.4. Configure Entity Links

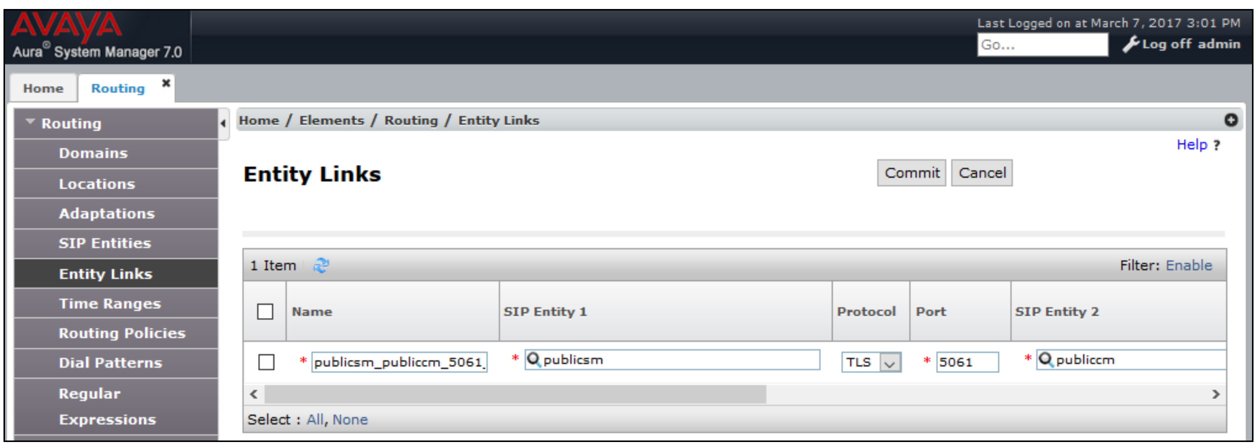
Entity Links define the connections between the SIP Entities and Session Manager. In the compliance test, the following entity links are defined from Session Manager.

- Session Manager ⇔ Communication Manager. This entity link was created prior to the compliance test.

Navigate 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 shown in **Section 6.3** (e.g. **publicsm**).
- 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 Communication Manager SIP entity
- In the **Port** field, enter the port to be used (e.g. **5060** or **5061**).
- Enter a description in the **Notes** field if desired.
- Accept the other default values.

Click on the **Commit** button to save each Entity Link definition.



Repeat the steps to define Entity Link using a different protocol.

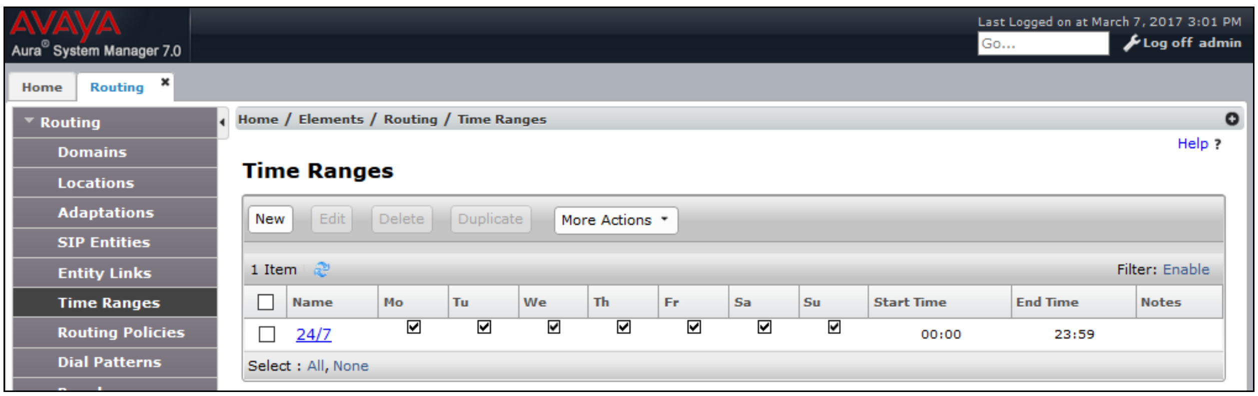
6.5. Time Ranges

The Time Ranges form allows admission control criteria to be specified for Routing Policies (**Section 6.6**). In the reference configuration, no restrictions were used.

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

- Enter a descriptive Time Range 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.



6.6. Configure Routing Policy

Routing Policies associate destination SIP Entities (**Section 6.3**) with Time of Day admission control parameters (**Section 6.5**) and Dial Patterns (**Section 6.7**). In the reference configuration, Routing Policies are defined for:

- Calls to/from Communication Manager.

To add a Routing Policy, navigate to **Routing → Routing Policies**, and click on the **New** button (not shown) on the right. Provide the following information:

General section

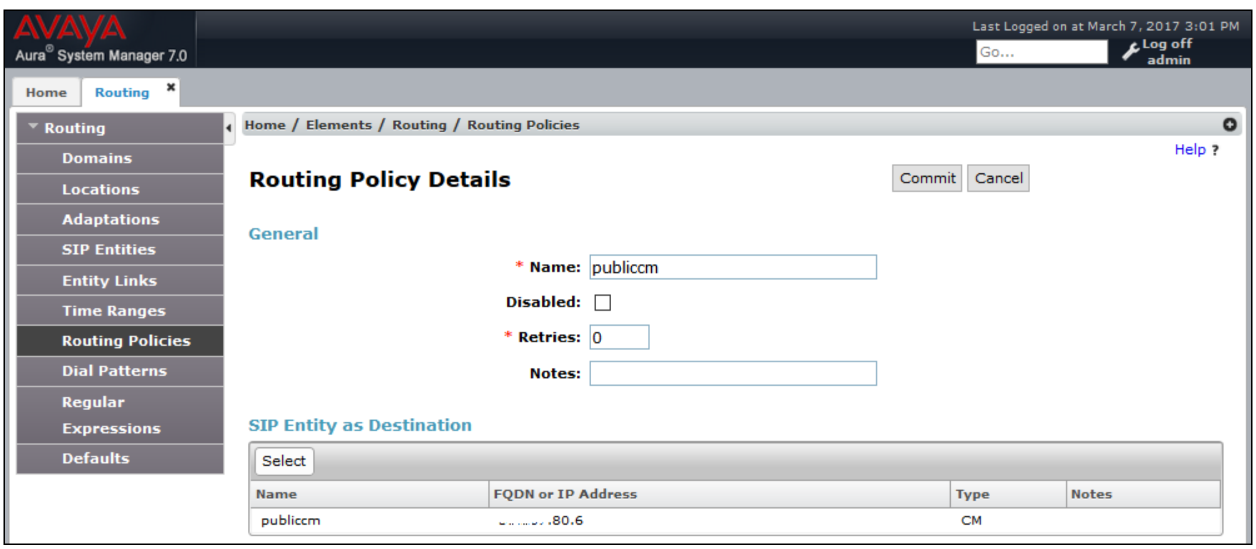
- Enter a descriptive name in the **Name** field.
- Enter a description in the **Notes** field if desired.

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 default values.

Click **Commit** to save Routing Policy definition. The following screen shows the Routing Policy used for the entity, **publiccm**, during the compliance test.



The IP Addresses in the screen capture above have been brushed for security reasons.

6.7. Dial Patterns

Dial Patterns define digit strings to be matched for 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.

- 91 – Routing for calls over to PSTN

To add a Dial Pattern, select **Routing → Dial Patterns,** and click on the **New** button (not shown) on the right.

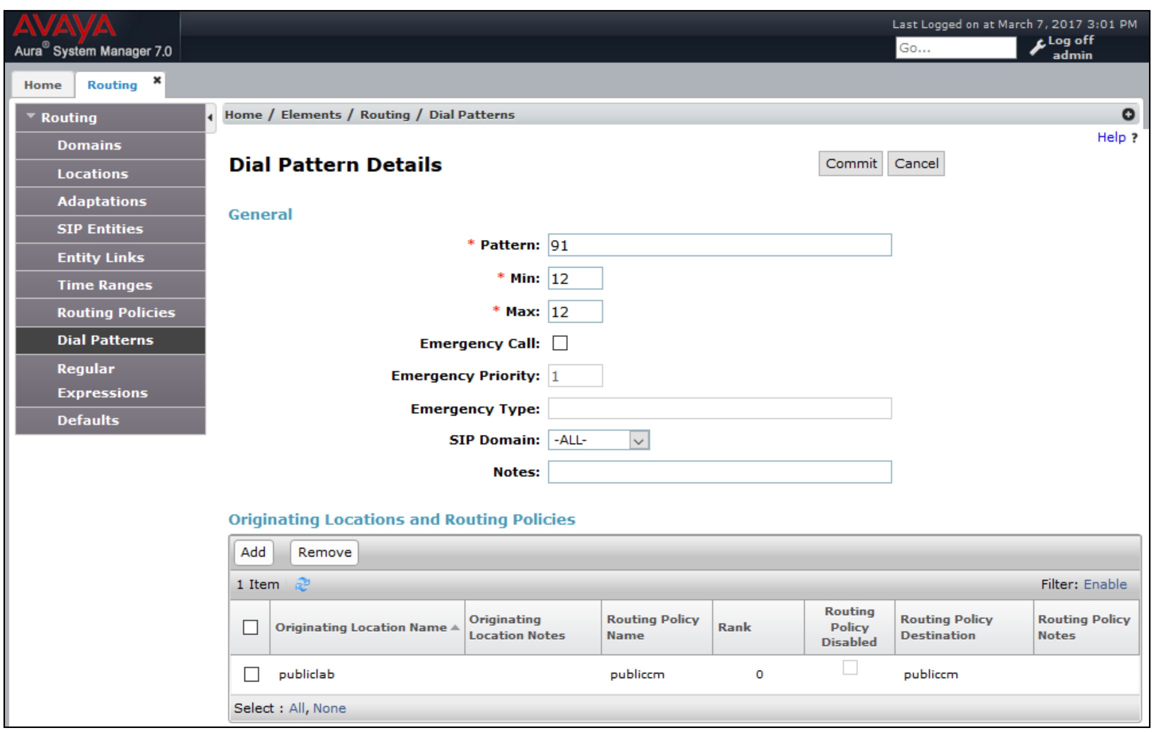
<u>General section</u>

- Enter a unique pattern in the **Pattern** field (e.g. **91**).
- In the **Min** field enter the minimum number of digits (e.g. **12**).
- In the **Max** field enter the maximum number of digits (e.g. **12**).
- In the **SIP Domain** field drop down menu select **-ALL-**
- Enter a description in the **Notes** field if desired.

<u>Originating Locations and Routing Policies section</u>

- Click on the **Add** button and a window will open (not shown).
- Click on the boxes for the appropriate Originating Locations, and Routing Policies (see **Section 6.6**) that pertain to this Dial Pattern.
  - Originating Location –Check the **Apply The Selected Routing Policies to All Originating Locations** box.
  - Routing Policies **publiccm**.
  - 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 Communication Manager during the compliance test.

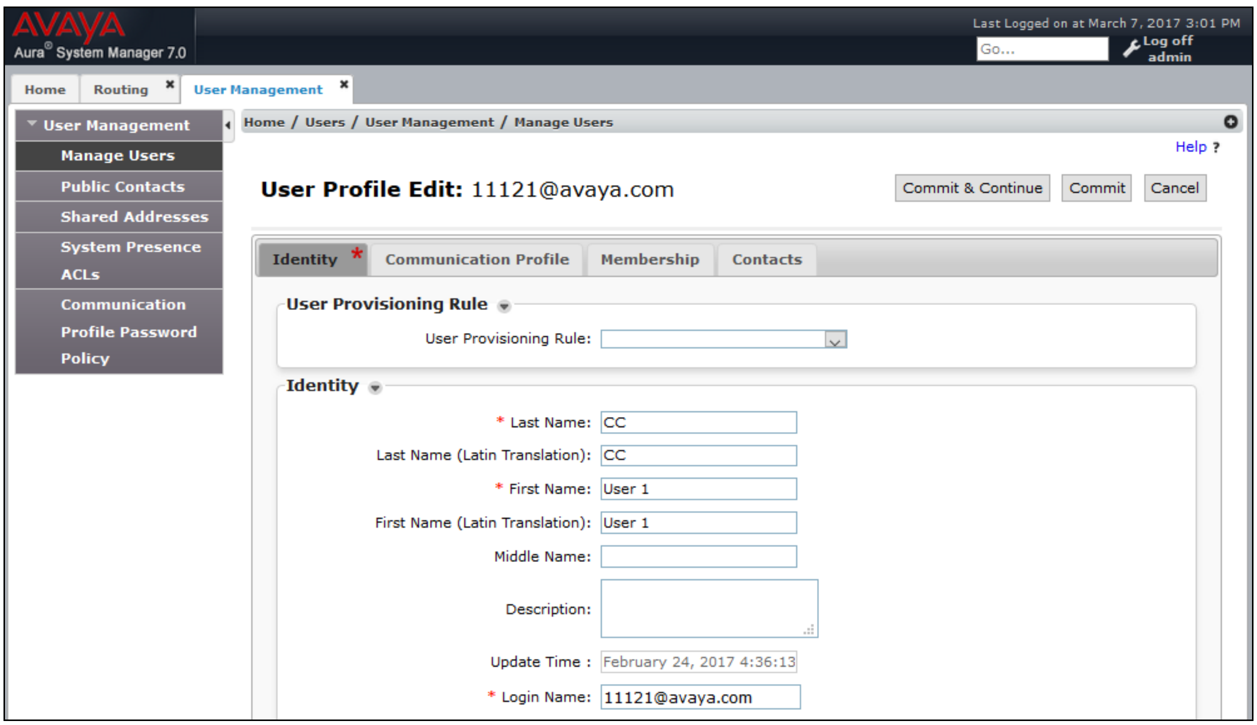


6.8. Configure SIP Users

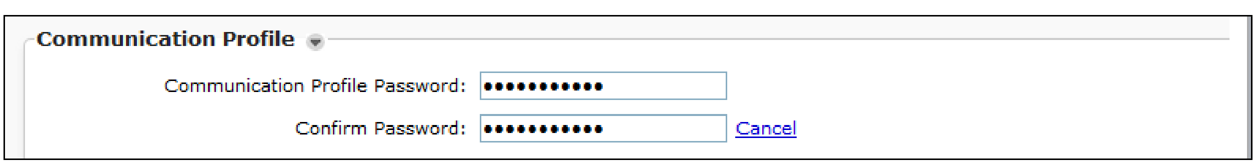
During the compliance test, no special users were created for this solution. All users were created prior to the compliance test. However, the steps to configure a user are included.
Add new SIP users for each Synergem Evolution 911 Elite Endpoint.

To add new SIP users, Navigate to **Home → Users → User Management→ 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 name. The domain name is defined in **Section 5.3**.

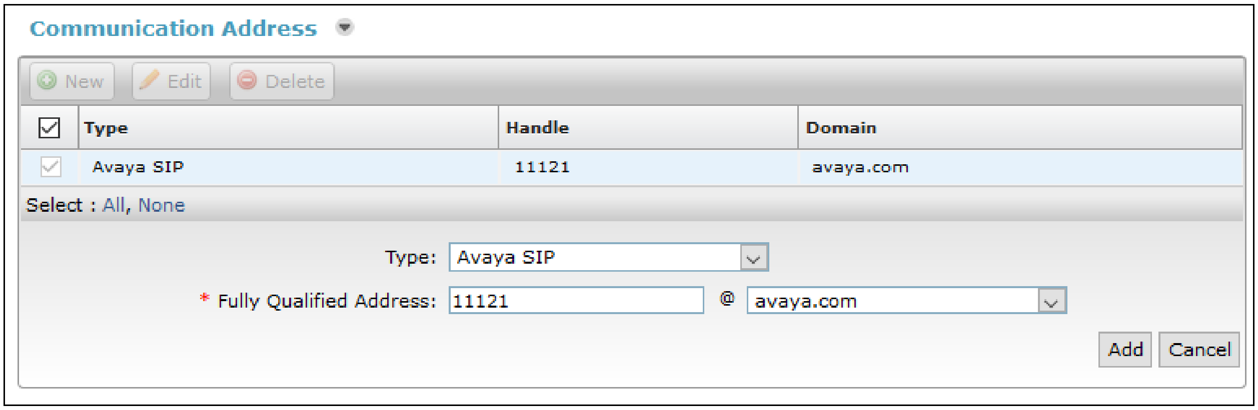


- Communication Profile section
  Provide the following information:
  - **Communication Profile Password** – Enter a numeric value used to logon to SIP telephone.
  - **Confirm Password** – Repeat numeric password

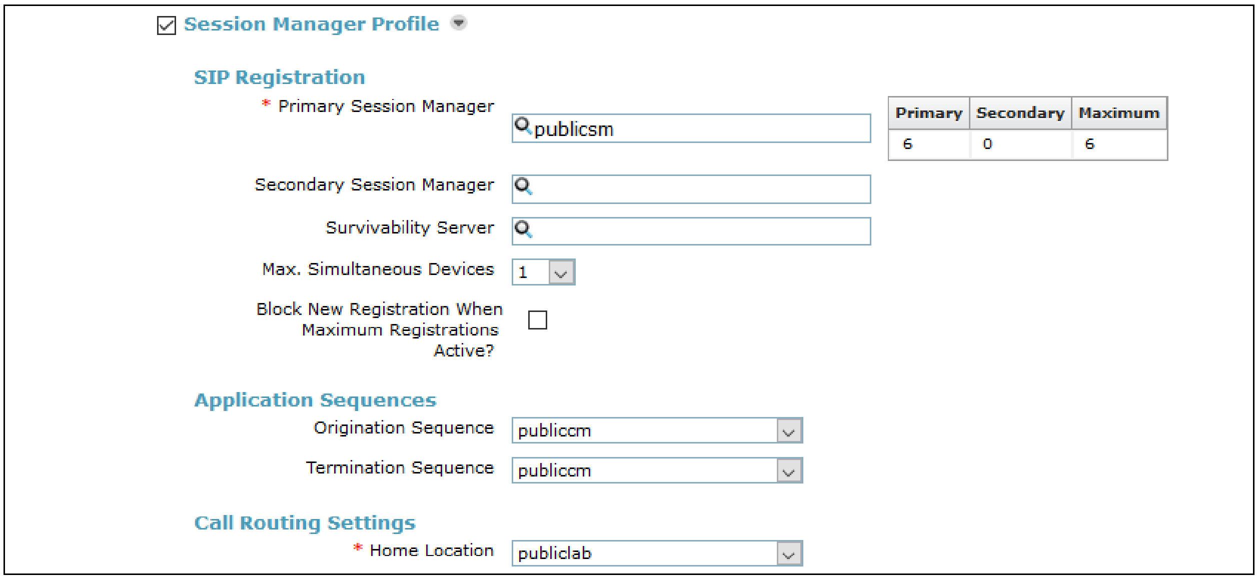


- <u>Communication Address sub-section</u>
  Select **New** to define a **Communication Address** for the new SIP user, and provide the following information.
    - **Type** – Select **Avaya SIP** using drop-down menu.
    - **Fully Qualified Address** – Enter same extension number and domain used for Login Name, created previously.

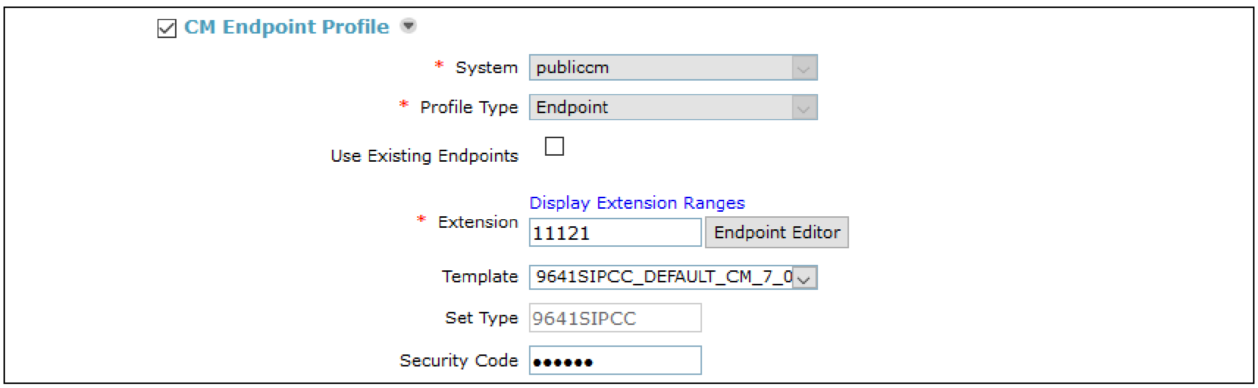
  Click the **Add** button to save the Communication Address for the new SIP user.



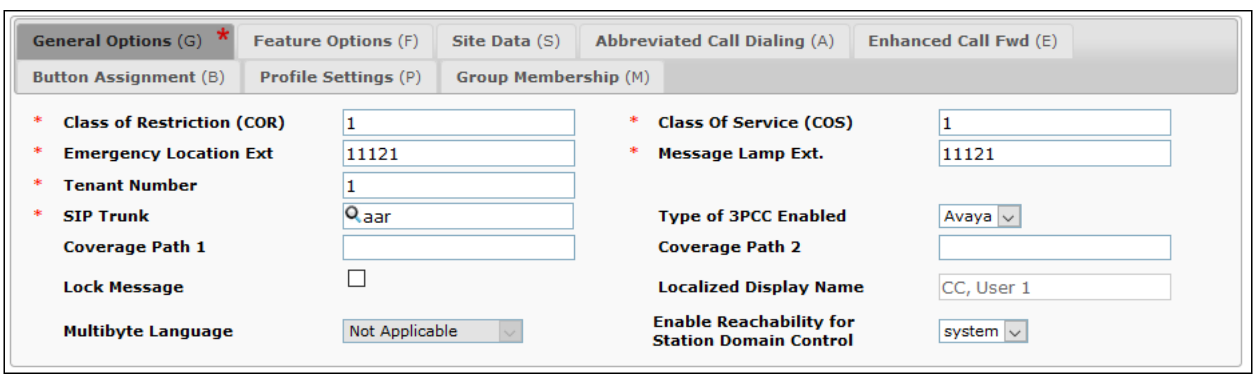
- Session Manager Profile section
  - **Primary Session Manager** – Select one of the Session Managers.
  - **Secondary Session Manager** – Select **(None)** from drop-down menu.
  - **Origination Application Sequence –** Select Application Sequence defined (not shown) for Communication Manager.
  - **Termination Application Sequence** – Select Application Sequence defined (not shown) for Communication Manager.
  - **Survivability Server** – Select **(None)** from drop-down menu.
  - **Home Location** – Select Location defined in **Section 6.2**.



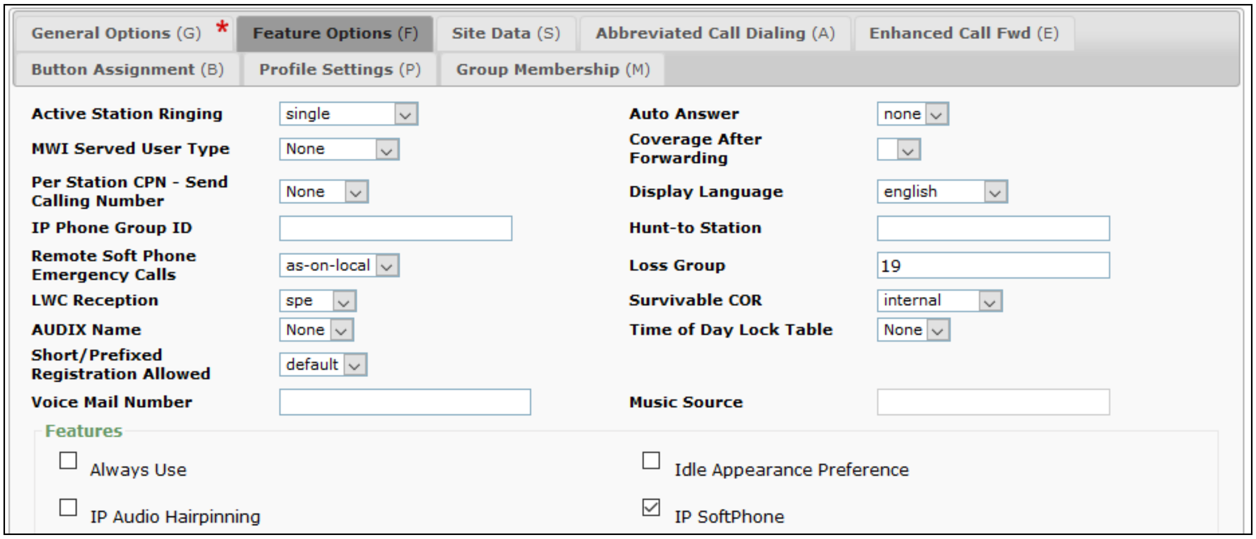
- <u>CM Endpoint Profile section</u>
  - **System** – Select Managed Element defined in **System Manager** (not shown) for Communication Manager.
  - **Use Existing Endpoints -** Leave unchecked to automatically create a new endpoint on Communication Manager when the new user is created. Or else, check the box if endpoint is already defined in Communication Manager.
  - **Extension** - Enter same extension number used in this section.
  - **Template** – Select template for type of SIP phone. During the compliance test, 9461SIPCC_DEFAULT_CM_7_0 was selected. Note that SIPCC represents that ACD functionality can be used by the endpoint.
  - **Security Code** – Enter numeric value.
  - **Port** – Select **IP** from the drop down menu
  - **Delete Station on Unassign of Endpoint** – Check the box to automatically delete station when Endpoint Profile is un-assigned from user.



- <u>Endpoint Editor:</u>
  - Under the **General Options** tab**, Type of 3PCC Enabled –** Select **Avaya,** which enabled 3PCC functionality for DMCC.



- Endpoint Editor:
    - Under the **Feature options** tab**,** check box for **IP SoftPhone.**



Select **Done** followed by **Commit** (not shown) to save the changes.

7. Configure Synergem Evolution 911 Elite™

The configuration of Evolution 911 Elite is performed by Synergem for the customer when the customer purchases Evolution 911 Elite. The information in this section is included simply as a reference.

AvayaAESDMCC	1
AvayaAESIPAddress	192.168.80.3
AvayaAESIPPort	4721
AvayaAESLogin	synergem
AvayaAESPassword	*******
AvayaAESProtocol	6.3
AvayaAESSecureSocket	0
AvayaAESSessionCleanupDelay	60
AvayaAESSessionDuration	180
AvayaAESSessionName	Evolution911
AvayaAgentDefaultWorkMode	1
AvayaAgentInitialWorkMode	3
AvayaAllowCertificateNameMismatch	1
AvayaControllableByOtherSessions	1
AvayaDashboardCritical	2
AvayaDashboardWarning	1
AvayaFACAgentWorkModesAfterCallWork	800
AvayaFACAgentWorkModesAssist	801
AvayaFACAgentWorkModesAutoIn	802
AvayaFACAgentWorkModesAuxWork	803
AvayaFACAgentWorkModesLogin	804
AvayaFACAgentWorkModesLogout	805
AvayaFACAgentWorkModesManualIn	806
AvayaFACServiceObservingByLocationListenOnly	811
AvayaFACServiceObservingByLocationListenTalk	812
AvayaFACServiceObservingListenOnly	807
AvayaFACServiceObservingListenTalk	808
AvayaFACServiceObservingNextCallListenOnly	810
AvayaFACServiceObservingNoTalk	809

AvayaStartAutoKeepAlive	1
AvayaSwitchIP	192.168.80.6
AvayaSwitchName	publiccm
AvayaTerminalMediaControl	0
AvayaTerminalRequestedDependencyMode	1
AvayaTerminalTelecommuteNumber	

8. Verification Steps

The following steps may be used to verify the configuration:

- Verify that Evolution 911 Elite successfully registers with Session Manager by following the **Session Manager → System Status → User Registrations** link on the System Manager Web Interface.

User Registrations

Select rows to send notifications to devices. Click on Details column for complete registration status.

Customize

View | **Default** | Force Unregister | **AST Device Notifications:** | Reboot | Reload | Failback | **As of 11:57 AM** | Advanced Search

6 Items | Show All | Filter: Enable

☐	Details	Address	First Name	Last Name	Actual Location	IP Address	Remote Office	Shared Control	Simult. Devices	AST Device	Registered		
											Prim	Sec	Surv
☐	Show	11122@avaya.com	User 2	CC	publiclab		☐	☐	1/1	☐	☑ (AC)	☐	☐
☐	Show	11121@avaya.com	User 1	CC	publiclab		☐	☐	1/1	☐	☑ (AC)	☐	☐
☐	Show	---	User 1	Tango	---	---	☐	☐	0/3	☐	☐	☐	☐
☐	Show	---	User 2	Tango	---	---	☐	☐	0/3	☐	☐	☐	☐
☐	Show	---	User 1	Avaya	---	---	☐	☐	0/1	☐	☐	☐	☐
☐	Show	---	User 2	Avaya	---	---	☐	☐	0/1	☐	☐	☐	☐

Select : All, None

- Place calls to and from Synergem Evolution 911 Elite and verify that the calls are successfully established with two-way talk path.
- While calls are established, Enter **status trunk <t:r>** command on Communication Manager, where **t** is the SIP trunk group configured in **Section 5.6**, and **r** is trunk group member. This will verify whether the call is shuffled or not.

```
status trunk 1/8                                                Page   3 of   3
                          SRC PORT TO DEST PORT TALKPATH
src port: T00008
T00008:TX:[Endpoint 1 IP Address]:27056/g711u/20ms
T00001:RX:[Endpoint 2 IP Address]:5004/g711u/20ms
```

- Verify the Evolution 911 Elite successfully starts monitors for stations via TSAPI on the CTI link by using **list monitored-station** command.

```
list monitored-station

                               MONITORED STATION

   Associations:     1       2       3       4       5       6       7       8
                 CTI     CTI     CTI     CTI     CTI     CTI     CTI     CTI
Station Ext      Lnk CRV Lnk CRV Lnk CRV Lnk CRV Lnk CRV Lnk CRV Lnk CRV Lnk CRV
---------------- ------- ------- ------- ------- ------- ------- ------- -------
11121            1  0007
11122            1  0001
12221            1  0006
12222            1  0004
```

9. Conclusion

Evolution 911 Elite was compliance tested with Communication Manager and Session Manager, and Application Enablement Services Synergem Evolution 911 Elite functioned properly for feature and serviceability. During compliance testing, Evolution 911 Elite successfully registered with Session Manager, placed and received calls to and from SIP and non-SIP telephones, and executed other telephony features like three-way conference, hold, etc.

10. Additional References

The following Avaya product documentation can be found at http://support.avaya.com

[1] *Administering Avaya Aura® Communication Manager*, Release 7.0.1.
[2] *Administering Avaya® Session Manager*, Release 7.0.1
[3] *Administering Avaya® System Manager*, Release 7.0.1

The following documentation was provided by Synergem and is available through Synergem Support.

[4] *Synergem EV911 Elite Installation Instructions*
[5] *Synergem EV911 Elite User Guide*

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.