Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R6.0.1 and Avaya Aura® Session Manager R6.1 to interoperate with Comdasys Mobile Convergence Solution – Issue 1.0

Abstract

These Application Notes describe the steps to configure trunking using the Session Initiation Protocol (SIP) between the Comdasys Mobile Convergence Solution with Avaya Aura® Session Manager and Avaya Aura® Communication Manager. Comdasys Mobile Convergence Solution allows GSM telephones to connect to a wireless LAN interface to be assigned an extension on the Avaya Aura® Communication Manager.

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

The Comdasys Mobile Convergence Solution together with Avaya Aura® Communication Manager and Avaya Aura® Session Manager allows "**dual mode**" mobile endpoints to act as local Avaya Aura® Communication Manager extensions. In addition to a GSM interface, such endpoints have a wireless LAN interface and a SIP client. When used within the coverage range of the local wireless LAN, incoming and outgoing calls for these endpoints are made via the mobile endpoint wireless LAN interface. When outside this coverage area, incoming and outgoing calls are made via the GSM network. When mobile endpoints enter or exit the wireless LAN coverage area, calls are "**handed over**" between the GSM and wireless LAN networks. The Comdasys Mobile Convergence Client needs to be installed on the mobile phone. Placing phone calls and feature invocation are executed transparently for the end-user either in the Wi-Fi or GSM mode.

SIP is a standards-based communications approach designed to provide a common framework to support multimedia communication. RFC 3261 is the primary specification governing this protocol. In the configuration described in these Application Notes, SIP is used as the signaling protocol between the Avaya components and the Comdasys Mobile Convergence Solution. SIP manages the establishment and termination of connections and the transfer of related information such as the desired codec, calling party identity, etc.

2. General Test Approach and Test Results

The interoperability compliance testing evaluated the ability of the Mobile Convergence Solution to carry out endpoint registration, call routing and call handover. Call handling, feature access and voice quality was performed from the Mobile Convergence Client on the mobile endpoint.

2.1. Interoperability Compliance Testing

The following tests were performed as part of the compliance testing. When appropriate, the tests were covered for calls established via the wireless LAN (WLAN) interface and the GSM interface of the client endpoints involved.

- Outgoing/incoming local/PSTN call
- Outgoing/incoming local/PSTN call rejection
- Outgoing/incoming local/PSTN call cancellation
- Call forwarding
- Supervised/blind transfer
- Consultation
- Hold/retrieve
- Manual handover from WLAN
- Automatic handover from WLAN/GSM
- Interruption to Comdasys server LAN interface
- Interruption to Comdasys server power

2.2. Test Results

All functionality and serviceability test cases were completed successfully.

2.3. Support

Support is available via the Comdasys distributor network. Details can be found at www.comdasys.com.

3. Reference Configuration

Figure 1 illustrates the network topology used during compliance testing. The Avaya solution consists of an Avaya S8800 Server running Communication Manager with Avaya G650 Media Gateway. An Avaya S8800 Server hosts Session Manager. Another Avaya S8800 Server hosts System Manager. A variety of Avaya H.323, Digital and SIP endpoints (not shown) were used in the testing. The Comdasys Mobile Convergence Solution was hosted on a Generic VMWare server.

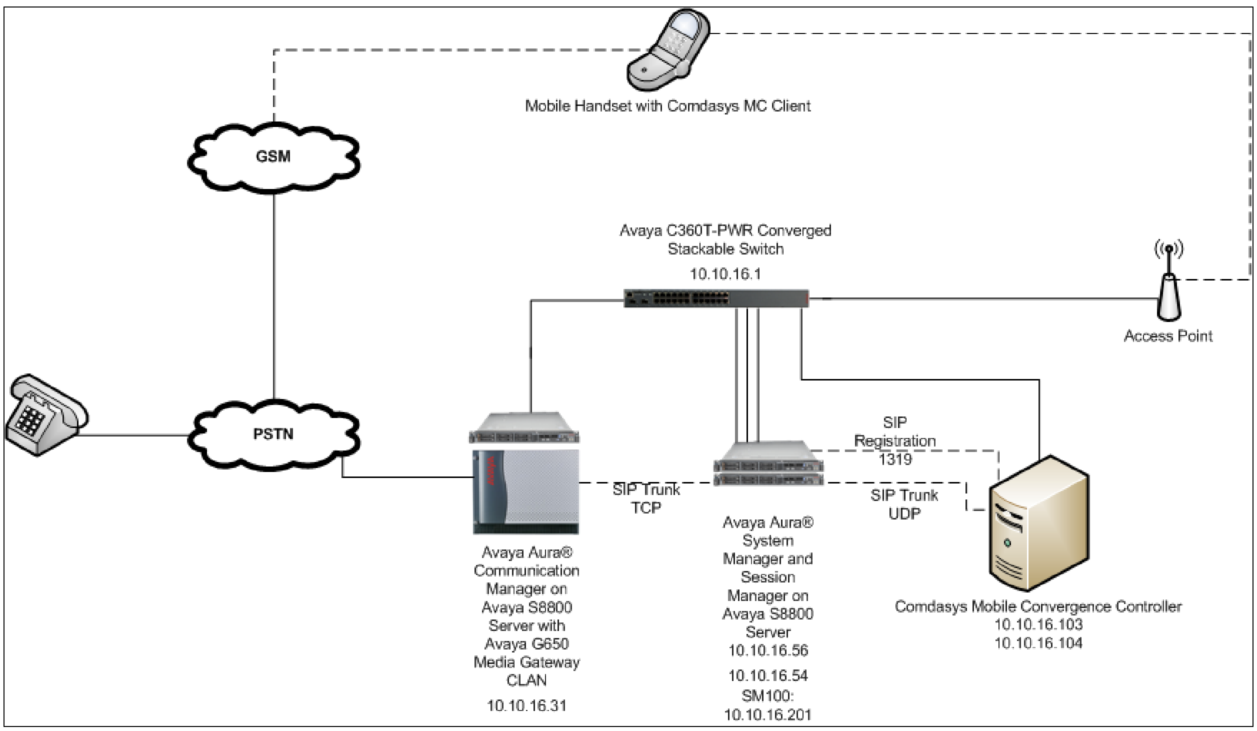


Figure 1: Avaya Aura® Communication Manager with Avaya Aura® Session Manager and Avaya Aura® System Manager and Comdasys Mobile Convergence Solution Configuration

The telephone numbers used for testing are shown in the following table.

Endpoint	Ext	PSTN Number	Station Type
A	1319	0035391482457	SIP Endpoint On MCC
B	4002	n/a	Avaya 1616
C	4001	0035391482458	Avaya 9620
PSTN	n/a	00353857412987	PSTN
Mobile Device	n/a	00353867818308	Cell Phone
Call through	n/a	0035391482456	FMC on MCC

The FMC (Fix/Mobile Convergence) call-through number is used by the Mobile Convergence Client in GSM mode to dial the Mobile Convergence Controller (MCC). All users share the same Call-Through number. The Call-Through is mandatory for initiating calls from the Client whenever it is out of Wi-Fi range.

4. Equipment and Software Validated

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

Equipment	Software
Avaya Aura® S8800 Media Server	Avaya Aura® Communication Manager R6.0.1 R16.00.1.510.1-19009
Avaya Aura® S8800 Media Server	Avaya Aura® Session Manager R6.1 SP3 6.1.3.0.613006
Avaya Aura® S8800 Media Server	Avaya Aura® System Manager R6.1 Build Number 6.1.0.0.7345-6.1.5.112 Software Update Revision Number 6.1.7.1.1260
Generic VMWare Server	Comdasys Mobile Convergence Controller Build 10684.12
BlackBerry Bold 2 9780	6.0.0.448 Comdasys MC Client 3.1.1
Nokia E71	Firmware 500.21.009 Comdasys MC Client 3.0
Apple iPhone 3g	iOS 4.2.1 Comdasys MC Client 3.1.6
Samsung Galaxy S	Android 2.1 update 1 Comdasys MC Client 2.1

5. Configure Avaya Aura® Communication Manager

The configuration and verification operations illustrated in this section were all performed using Communication Manager System Administration Terminal (SAT). The information provided in this section describes the configuration of Communication Manager for this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation as referenced in **Section 11**. The configuration operations described in this section can be summarized as follows:

- Verify System Parameters Customer Options
- Configure Node Names
- Configure SIP Signaling Group
- Configure SIP Trunk
- Configure Route Pattern
- Configure AAR
- Configure PSTN Call Through Number
- Configure Feature Access Code
- Configure Private Numbering

5.1. Verify System Parameters Customer Options

Use the **display system-parameters customer-options** command to verify that Communication Manager has permissions for features illustrated in these Application Notes. On **Page 1**, ensure that **Maximum Off-PBX Telephones** is adequate for the number of SIP endpoints as shown below.

```
display system-parameters customer-options                    Page   1 of  11
                                OPTIONAL FEATURES

     G3 Version: V16                                 Software Package: Enterprise
       Location: 2                                    System ID (SID): 1
       Platform: 28                                   Module ID (MID): 1

                                                              USED
                                Platform Maximum Ports: 65000 131
                                      Maximum Stations: 41000 23
                              Maximum XMOBILE Stations: 41000 0
                    Maximum Off-PBX Telephones - EC500: 41000 1
                    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




         (NOTE: You must logoff & login to effect the permission changes.)
```

On **Page 2** ensure that **Maximum Administered SIP Trunks** is adequate for the number of channels that are to be used on the SIP Trunk from Communication Manager to Session Manager.

```
display system-parameters customer-options                     Page   2 of  11
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                             USED
                     Maximum Administered H.323 Trunks: 12000 0
           Maximum Concurrently Registered IP Stations: 18000 12
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 414   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 18000 0
                   Maximum Video Capable IP Softphones: 18000 0
                       Maximum Administered SIP Trunks: 24000 40
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                             Maximum TN2501 VAL Boards: 128   0
                     Maximum Media Gateway VAL Sources: 250   0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   1
          Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 300   0

        (NOTE: You must logoff & login to effect the permission changes.)
```

5.2. Configure Node Names

The Application Notes assumes a C-LAN interface or equivalent is administered on Communication Manager. The Application Notes also assumes that the SM100 (Session Manager signaling interface) has been configured on Session Manager. In order to create the SIP Trunk between Communication Manager and Session Manager a node-name needs to be specified for the SM100. This will be used in **Section 5.3**. Enter the command **change node-names ip** and enter an identifying **Name** for the SM100 and its **IP address**, in this case **sesmgr-sm100** and **10.10.16.201** respectively. Take a note here of the C-LAN node name, **clancm601**.

```
change node-names ip                                            Page   1 of
2
                                  IP NODE NAMES
    Name                  IP Address
clancm601               10.10.16.31
default                 0.0.0.0
devconaes61             10.10.16.30
ipo7.0                  10.10.16.105
medprocm601             10.10.16.32
procr                   10.10.16.47
procr6                  ::
sesmgr-sm100            10.10.16.201









( 8  of 8    administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

5.3. Configure SIP Signaling Group

A signaling group must be used to specify the signaling type and node-names to be used for the SIP Trunk configured in **Section 5.4**. Enter the command **add signaling-group next**, take a note of the **Group Number**, set the **Group Type** to **sip**, **Transport Method** to **tcp**, set the **Near-end Node Name** to the node name of the C-LAN, in this case **clancm601**, and the **Far-end Node Name** to that configured in **Section 5.2**, in this case **sesmgr-sm100**. Leave all other settings as default.

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

 Group Number: 2              Group Type: sip
  IMS Enabled? n        Transport Method: tcp
        Q-SIP? n                                               SIP Enabled LSP?
n
     IP Video? n                                     Enforce SIPS URI for SRTP?
y
  Peer Detection Enabled? y  Peer Server: SM



   Near-end Node Name: clancm601            Far-end Node Name: sesmgr-sm100
 Near-end Listen Port: 5060               Far-end Listen Port: 5060
                                       Far-end Network Region:

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

5.4. Configure SIP Trunk

To route calls between Communication Manager and Session Manager the SIP trunk must use the Signaling group setup in **Section 5.3**. Enter the command **add trunk-group next**, on **Page 1** take a note of the **Group Number**, this will be used when configuring route patterns. Set the **Group Type** to **sip** and assign the trunk an identifying **Group Name.** Set the **TAC** according to the dialplan. Set the **Service Type** as **Tie** and assign the **Signaling Group** as added in **Section 5.3**, set **Number of Members** according to requirements.

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

Group Number: 2                   Group Type: sip          CDR Reports: y
  Group Name: SIP TRUNK TO SES-MGR       COR: 1        TN: 1        TAC: 702
   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: 2
                                                    Number of Members: 30
```

On **Page 2** configure **Redirect on OPTIM Failure** to **10000**. This is necessary to ensure the delay in dialing off-net does not cause the SIP trunk to disconnect the call.

```
add trunk-group next                                          Page   2 of  21
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name: auto

                                             Redirect on OPTIM Failure: 10000

            SCCAN? n                                 Digital Loss Group: 18
                      Preferred Minimum Session Refresh Interval(sec): 600

 Disconnect Supervision - In? y  Out? y


           XOIP Treatment: auto    Delay Call Setup When Accessed Via IGAR? n
```

On **Page 3** set the **Numbering Format** as **private**, configure further in **Section 5.9**.

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



                     Numbering Format: private
                                              UUI Treatment: service-provider

                                                Replace Restricted Numbers? n
                                               Replace Unavailable Numbers? n


                                Modify Tandem Calling Number: no




 Show ANSWERED BY on Display? y
```

5.5. Configure Route Pattern

When SIP users are created on Session Manager using System Manager, they are synchronized with Communication Manager as both stations and off-PBX-telephone stations. In order for calls from Communication Manager to reach the SIP stations, which register to the Session Manager, a route pattern must be created. The route pattern will use the trunk created in **Section 5.4**. Enter the command **change route-pattern x**, where **x** is an unused route pattern, configure an identifying **Pattern Name**, the **Grp No** set up in the previous Section, and an **FRL** accordingly.

```
change route-pattern 2                                          Page   1 of   3
                    Pattern Number: 2   Pattern Name: to ses-mgr
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                           DCS/ IXC
    No          Mrk Lmt List Del  Digits                                QSIG
                             Dgts                                       Intw
 1: 2    0                                                            n   user
 2:                                                                   n   user
 3:                                                                   n   user
 4:                                                                   n   user
 5:                                                                   n   user
 6:                                                                   n   user

  BCC VALUE      TSC CA-TSC   ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W      Request                                Dgts Format
                                                         Subaddress
 1: y y y y y n  n            rest                                       none
 2: y y y y y n  n            rest                                       none
 3: y y y y y n  n            rest                                       none
 4: y y y y y n  n            rest                                       none
 5: y y y y y n  n            rest                                       none
 6: y y y y y n  n            rest                                       none
```

5.6. Configure AAR

The AAR table must be configured in order that calls to SIP stations are routed using the pattern configured in **Section 5.5**. Enter the command **change aar analysis 0** to configure AAR. In this example, SIP stations are **4** digits in length, and begin with the digits **13**; calls to numbers beginning with 13 will route over route pattern **2**. Configure the **Dialed String**, **Min** and **Max**, **Route Pattern** and **Call Type** as shown below.

```
change aar analysis 0                                          Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all            Percent Full: 0

          Dialed            Total      Route     Call   Node  ANI
          String           Min  Max   Pattern    Type   Num   Reqd
    13                     4    4      2         aar          n
    201                    3    3      4         aar          n
    2456                   4    4      2         aar          n
    400                    3    3      5         aar          n
    5                      7    7      999       aar          n
    6                      7    7      999       aar          n
    7                      7    7      999       aar          n
    8                      5    5      3         aar          n
    9                      7    7      999       aar          n
                                                              n
                                                              n
                                                              n
                                                              n
                                                              n
                                                              n
```

In addition, the incoming number for call through is configured in the AAR table.

5.7. Configure PSTN Call Through Number

The trunk used to provide the PSTN Call Through Number must be configured to route the correct digits to Session Manager. Enter the command **change inc-call-handling-trmt trunk-group x** where x is the number of the PSTN trunk. In this instance, the digits provided by the PSTN network is **82456**. The required configuration in this example is for digits **2456** to route to Session Manager. To achieve this, the AAR feature access code, **5,** must be used as configured in **Section 5.8**. Upon the incoming digits being replaced with **52456**, the AAR table will be entered and digits 2456 presented to it. The call will be routed in accordance with the details in **Section 5.6**. Configure **Service/Feature** as **public-ntwrk**, **Number Len**, **Number Digits, Del** and **Insert** accordingly.

```
change inc-call-handling-trmt trunk-group 3                     Page 1 of  30
                   INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert            Per Call Night
 Feature        Len      Digits                           CPN/BN   Serv
 public-ntwrk    5  82456            all 52456
 public-ntwrk    5  82457            all 1319
 public-ntwrk    5  82458            all 4510
 public-ntwrk    5  82459            all 1300
 public-ntwrk    5  82460            all 4001
 public-ntwrk    5  82461            all 1320
 public-ntwrk    5  82462            all 1321
 public-ntwrk    5  82463            all 1322
 public-ntwrk    5  82464            all 5400
 public-ntwrk
```

5.8. Configure Feature Access Code

Enter the command **change feature-access-codes** to configure the feature access code for AAR as referenced in **Section 5.7**.

```
change feature-access-codes                                    Page   1 of  10
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code: *14
                       Answer Back Access Code: *13
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 5
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation:        Deactivation:
Call Forwarding Activation Busy/DA:        All:        Deactivation:
   Call Forwarding Enhanced Status:        Act: *11    Deactivation: *12
                         Call Park Access Code:
                       Call Pickup Access Code: *10
CAS Remote Hold/Answer Hold-Unhold Access Code:
                  CDR Account Code Access Code:
                        Change COR Access Code:
                   Change Coverage Access Code:
            Conditional Call Extend Activation:        Deactivation:
                   Contact Closure   Open Code:          Close Code:
```

5.9. Configure Private Numbering

In order to specify the calling number presented to SIP endpoints, the private numbering table must be administered. Enter the command **change private-numbering 0** for this configuration. In this example **4** digit extensions beginning with **13** are routed over SIP trunk group **2** with a total length of **4**. Enter **Ext Len, Extn Code, Trk Grp(s)** and **Total Len** accordingly. Similarly, extensions beginning with **4** which are **4** digits in length are added.

```
change private-numbering 0                                      Page   1 of   2
                           NUMBERING - PRIVATE FORMAT

Ext Ext              Trk         Private          Total
Len Code             Grp(s)      Prefix           Len
 4  13               2                            4     Total Administered: 1
 4  4                2                            4        Maximum Entries: 540
```

6. Configure Avaya Aura® Session Manager

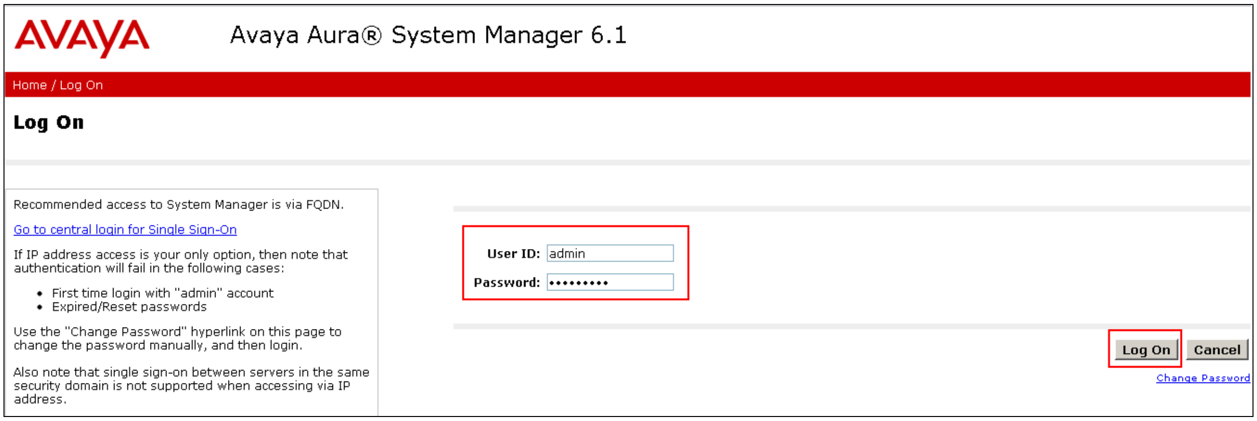
System Manager is used to configure Session Manager SIP entities and manages the connections between related SIP trunks and endpoints. It is also used to configure dial patterns and route calls according to defined rules. The configuration and verification operations illustrated in this section were all performed using the System Manager Web Interface.

This section provides the procedures for configuring Session Manager. For further reference documents, refer to **Section 11** of this document. The procedures include the following areas:

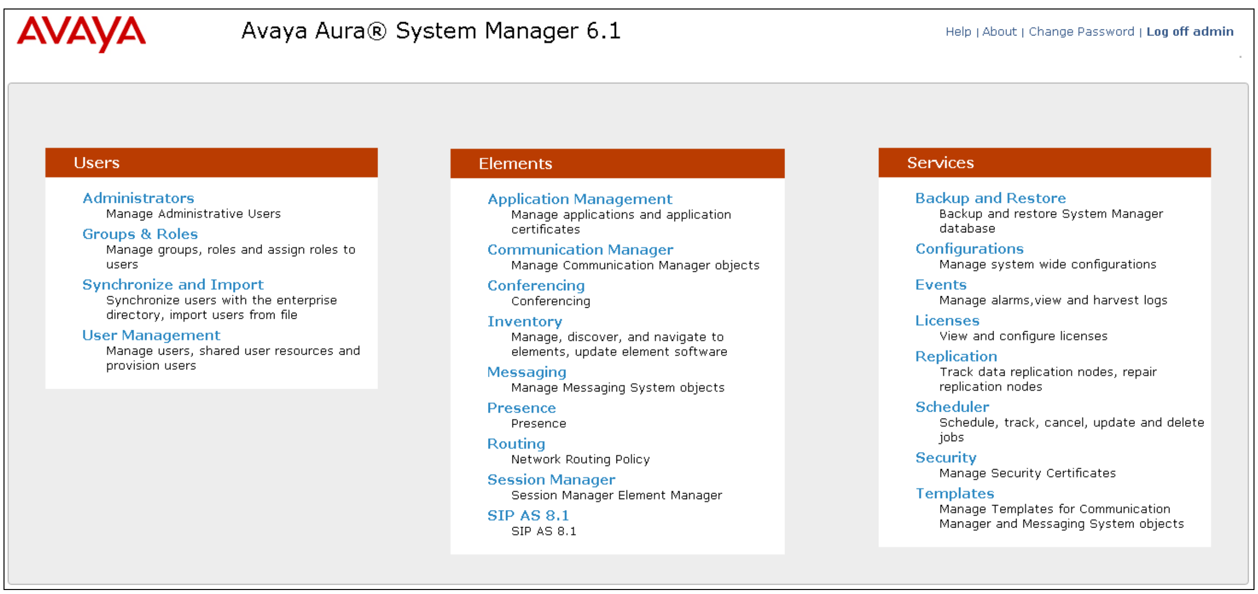
- Login to Avaya Aura® System Manager
- Administer SIP Domain
- Administer Locations
- Administer SIP Entities
- Administer Entity Links
- Administer Routing Policies
- Administer Dial Patterns
- Administer Avaya Aura® Session Manager
- Add Avaya Aura® Communications Manager
- Administer SIP Users

6.1. Login to Avaya Aura® System Manager

Login to the System Manager web interface using the System Manager IP address, in this case https://10.10.16.56/index.jsp enter the appropriate credentials and click **Log On**.

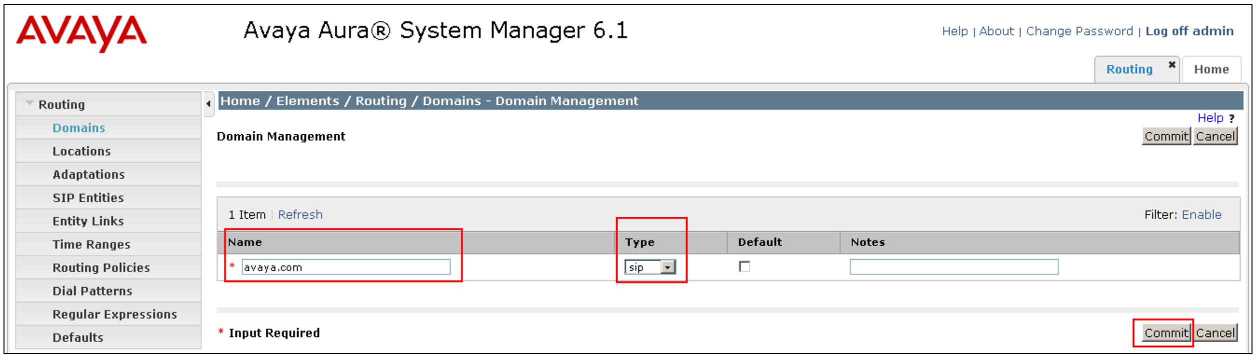


The Home screen is divided into three sections with hyperlinked categories as shown below.



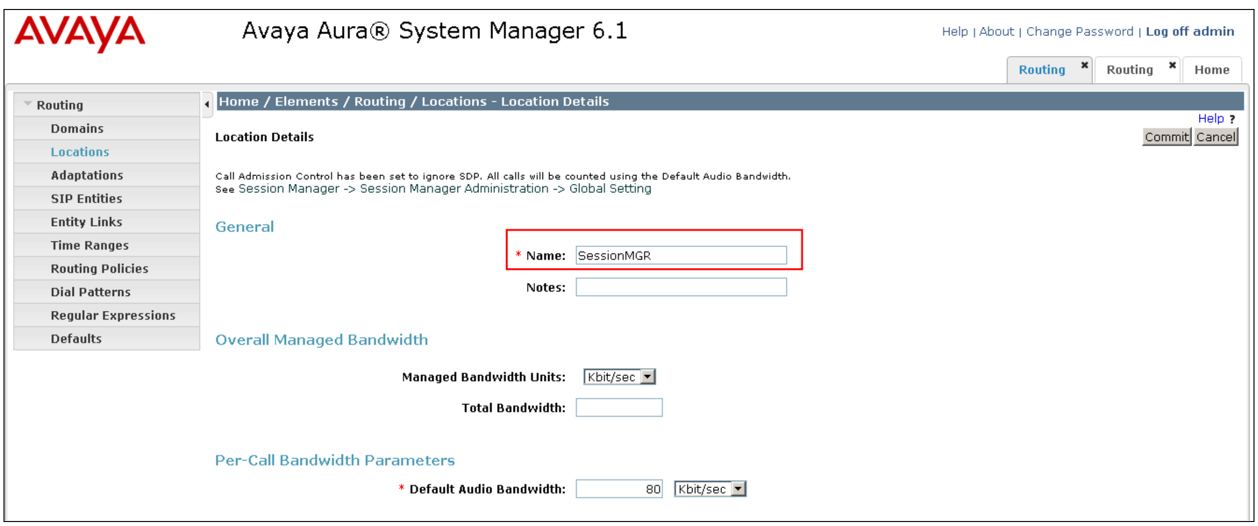
6.2. Administer SIP Domain

SIP domains are created as part of the Session Manager basic configuration. There will be at least one for which the System Manager is the authoritative SIP controller. In these sample notes it is **avaya.com**. Under the **Elements** section click **Routing → Domains → New**, enter the domain **Name,** set the **Type** as **sip** and click **Commit**.

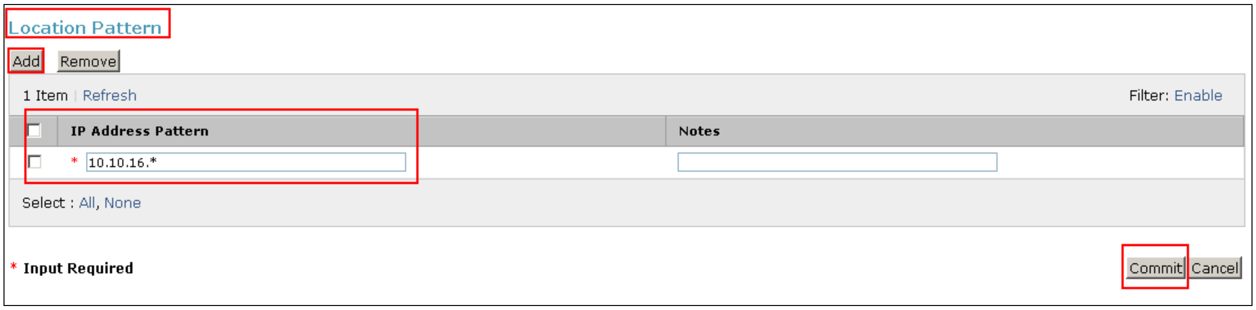


6.3. Administer Locations

Session Manager uses the origination location to determine which dial patterns to look at when routing a call. In this example, one Location has been created which will reference both the Session Manager location and the Comdasys Mobile Convergence Controller location. Navigate to **Home → Elements → Routing → Locations → New**, enter an identifying **Name**, as shown below.



At the bottom of the same page the **Location Pattern** is defined. Click **Add** and enter the IP address range used to logically identify the location. In this case the **IP Address Pattern** is **10.10.16.x** as shown below. Click **Commit** when done.

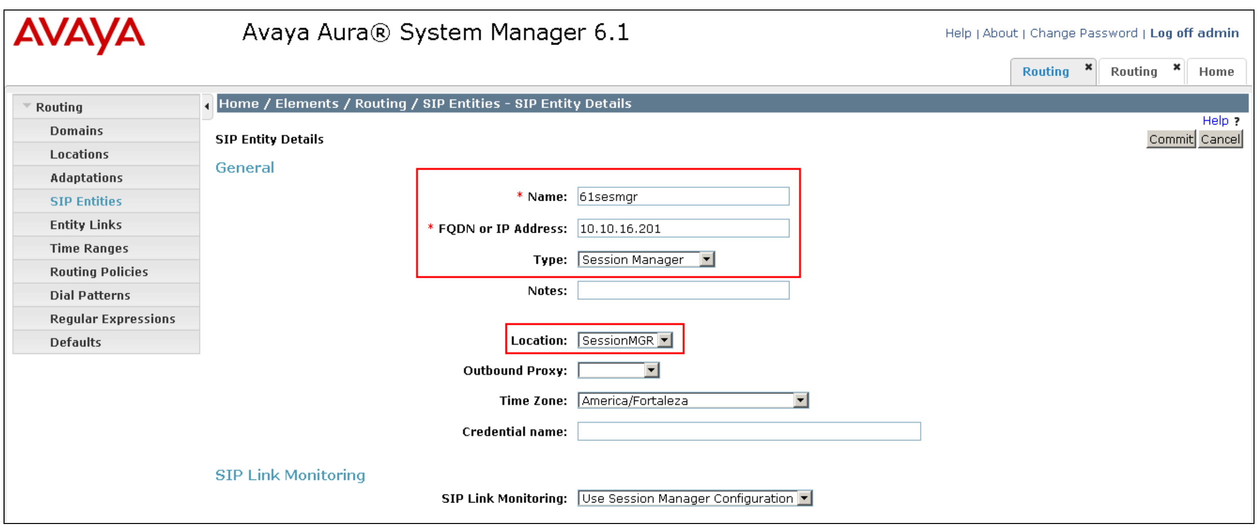


6.4. Administer SIP Entities

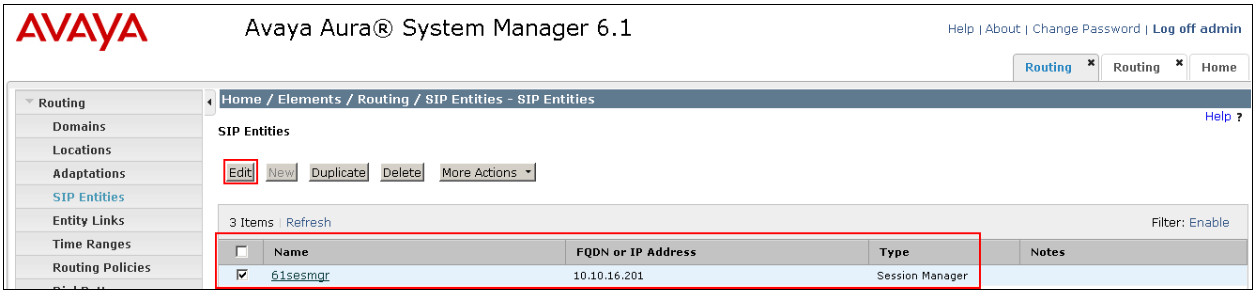
Each SIP device (other than Avaya SIP Phones) that communicates with the Session Manager requires a SIP Entity configuration. This section details the steps to create SIP Entities for the Session Manager, Communication Manager and Mobile Convergence Solution respectively.

6.4.1. Configure Avaya Aura® Session Manager Entity

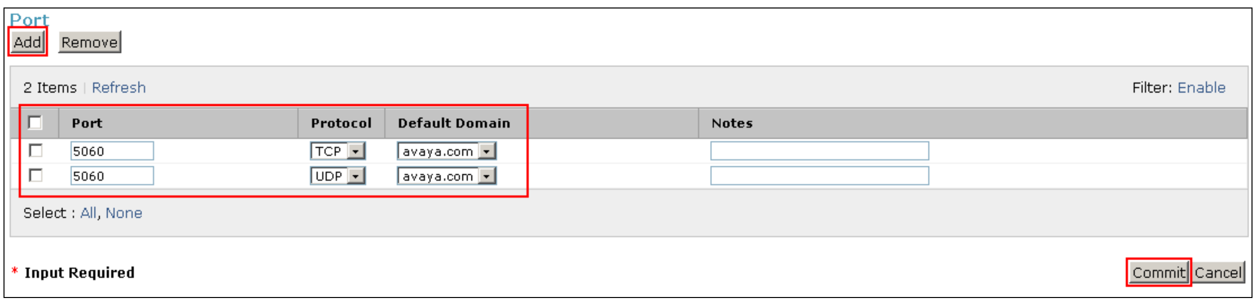
Click **Home → Elements → Routing → SIP Entities → New**, assign an identifying **Name**, the **FQDN or IP Address** for the Session Manager signaling interface, set the **Type** to **Session Manager** and the **Location** to the Location configured in **Section 6.3** and click on **Commit**.



The screen below will now be displayed, tick the box next to the entity that was just created and click **Edit.**

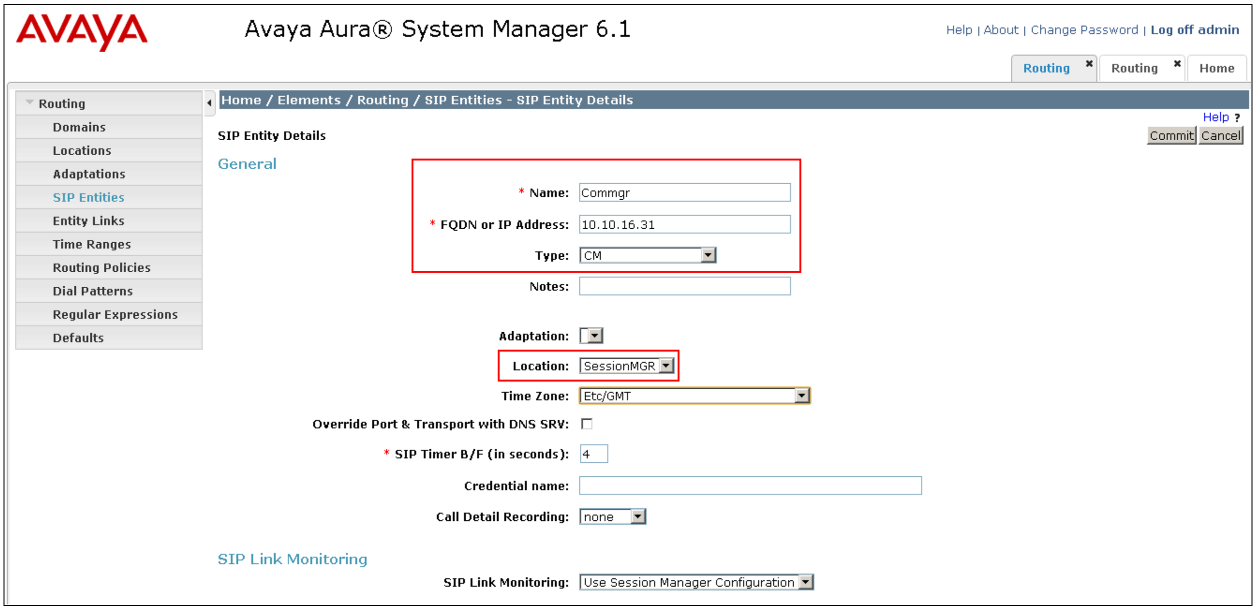


Scroll down the page until the **Port** section is displayed. Click **Add** and configure the **Port** as **5060**, the Protocol as **TCP** and the **Default Domain** as the domain configured in **Section 6.2**. This configuration corresponds with the signaling group configured in **Section 5.3**. Repeat this for the UDP connection which will be established to the Mobile Convergence Controller, as shown below. Click **Commit** when done.

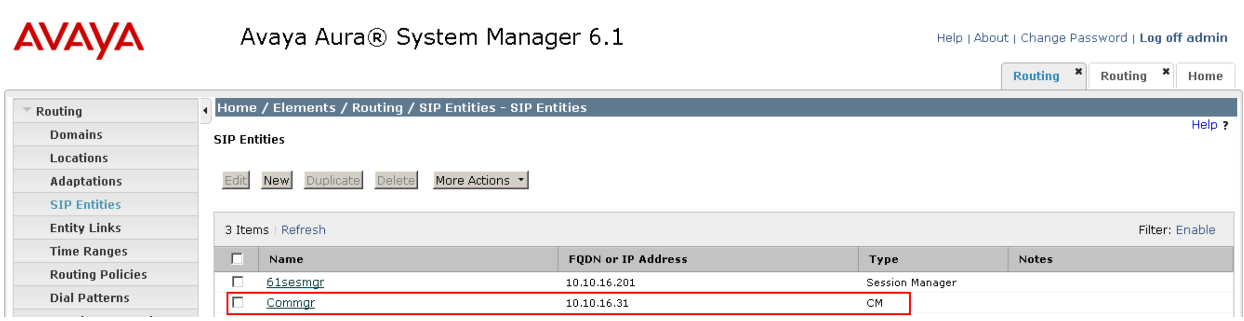


6.4.2. Configure Avaya Aura® Communication Manager Entity

Click **Home → Elements → Routing → SIP Entities → New**, assign an identifying **Name**, the **FQDN or IP Address** for the C-LAN, set the **Type** to **CM** and the **Location** to the Location configured in **Section 6.3** and click on **Commit**.

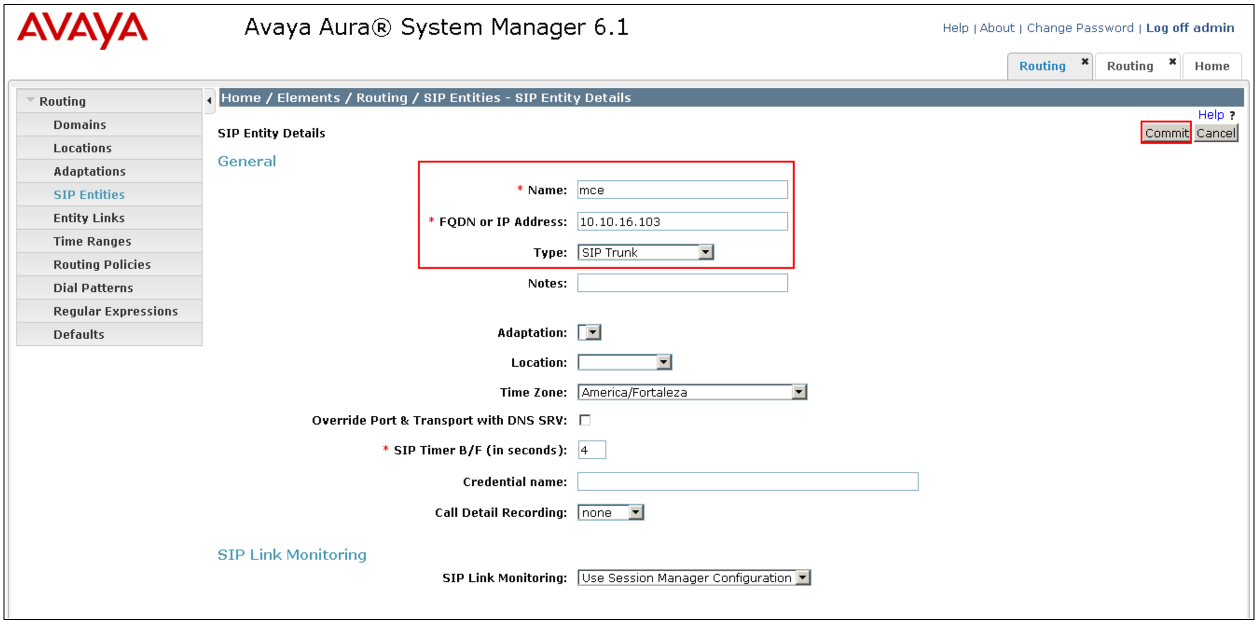


The screen below will now be displayed confirming the entry.

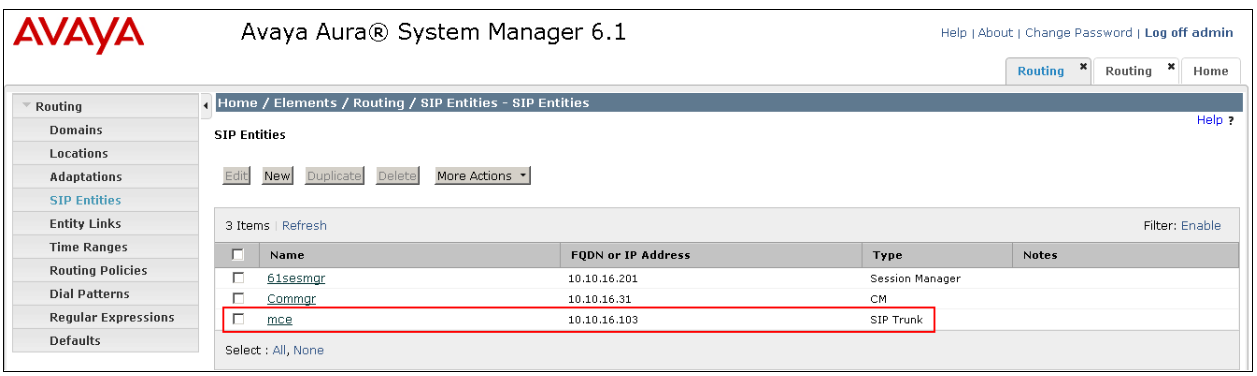


6.4.3. Configure Comdasys Mobile Convergence Controller Entity

Click **Home → Elements → Routing → SIP Entities → New**, assign an identifying **Name**, the **FQDN or IP Address** for the Mobile Convergence Controller, set the **Type** to **SIP Trunk** and set **Call Detail Recording** to **none**, leave all other settings as default and click **Commit**.



The screen below will now be displayed confirming the entry.

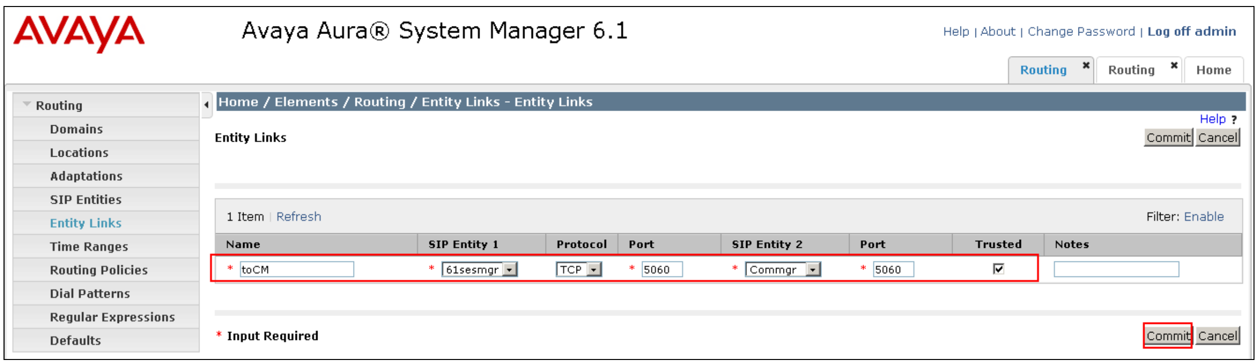


6.5. Administer SIP Entity Links

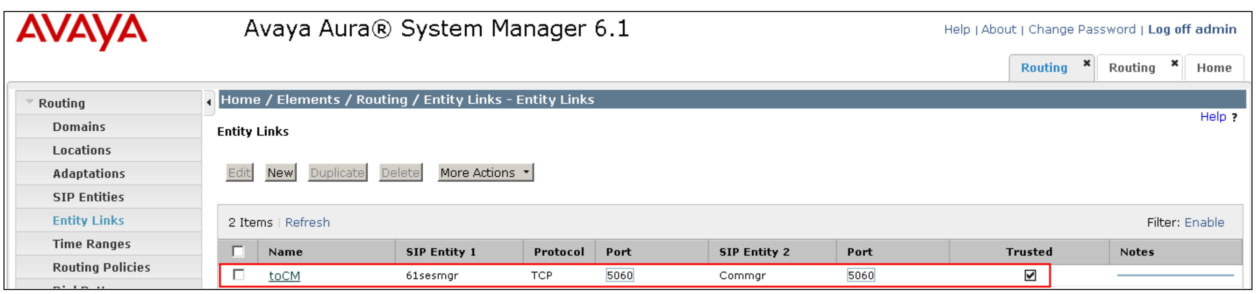
A SIP Trunk between a Session Manager and a telephony system is described by an Entity Link. An entity link needs to be created between Session Manager and both Communication Manager and the Mobile Convergence Controller.

6.5.1. Administer SIP Entity Link from Avaya Aura® Session Manager to Avaya Aura® Communication Manager

Click on **Home → Elements → Routing → Entity Links → New**, assign an identifying **Name**, choose the entity assigned to Session Manager as **SIP Entity 1**, set **Protocol** as **TCP**, enter **5060** for **Port**, choose the CM entity as **SIP Entity 2** and set **Port** to **5060**, place an arrow in the **Trusted** box. Click **Commit** when done.

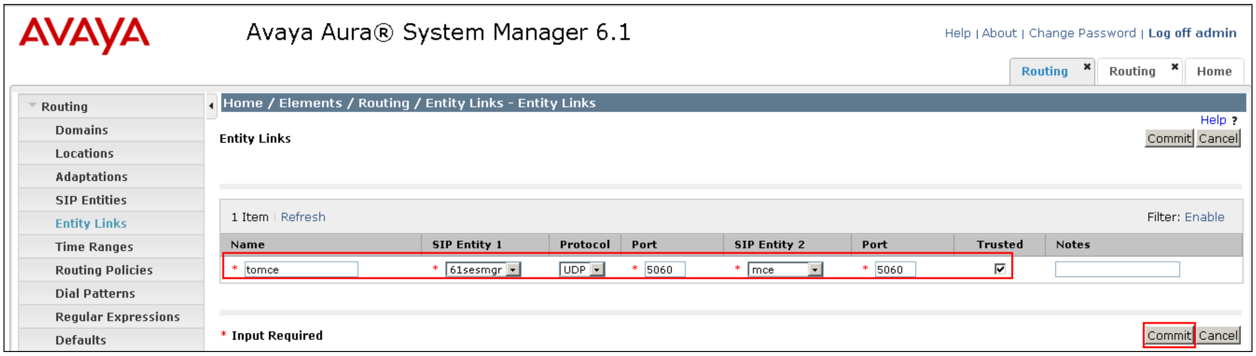


The screen below will be shown confirming the entry.

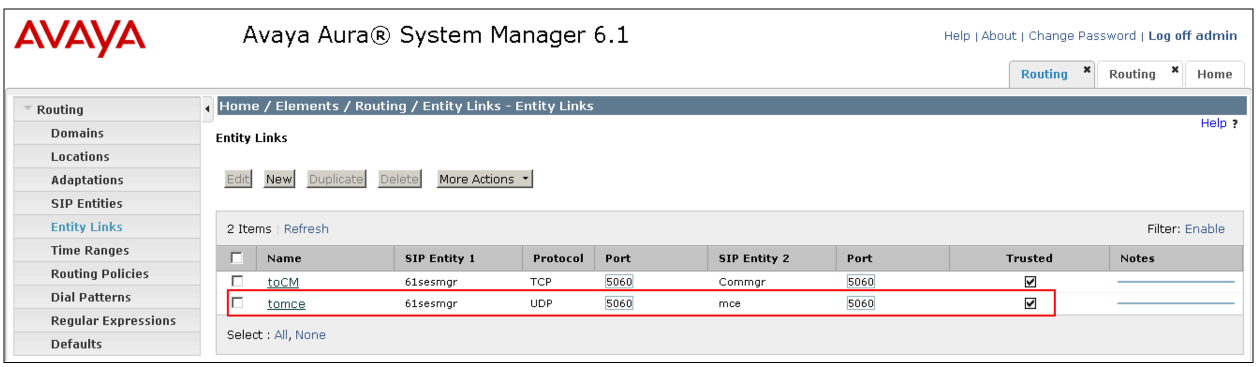


6.5.2. Administer SIP Entity Link from Avaya Aura® Session Manager to Comdasys Mobile Convergence Controller

Click on **Home → Elements → Routing → Entity Links → New**, assign an identifying **Name**, choose the entity assigned to Session Manager as **SIP Entity 1**, set **Protocol** as **UDP**, enter **5060** for **Port**, choose the Mobile Convergence Controller entity as **SIP Entity 2** and set **Port** to **5060**, place an arrow in the **Trusted** box. Click **Commit** when done. This establishes the Session Manager end of the SIP Trunk to the Mobile Convergence Controller.



The screen below will be shown confirming the entry.

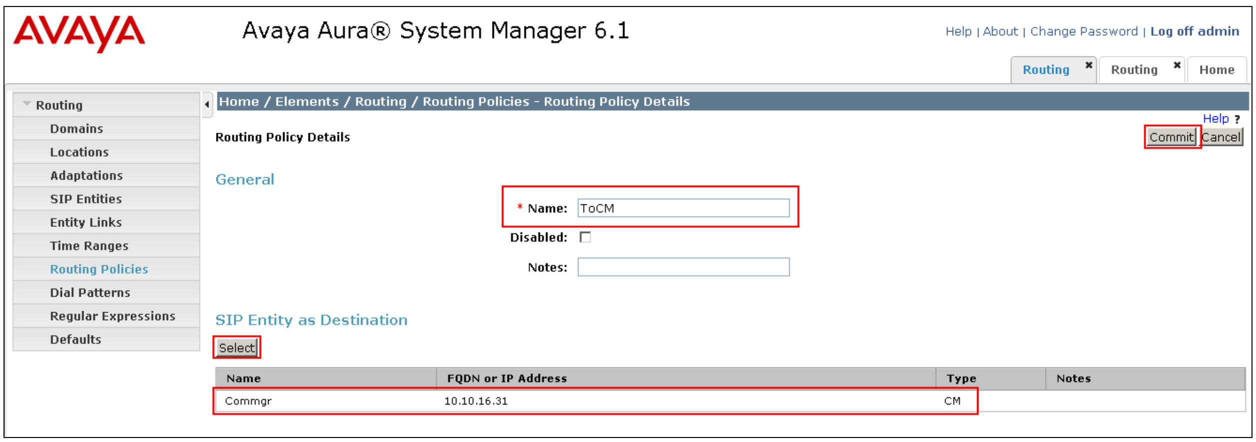


6.6. Administer Routing Policies

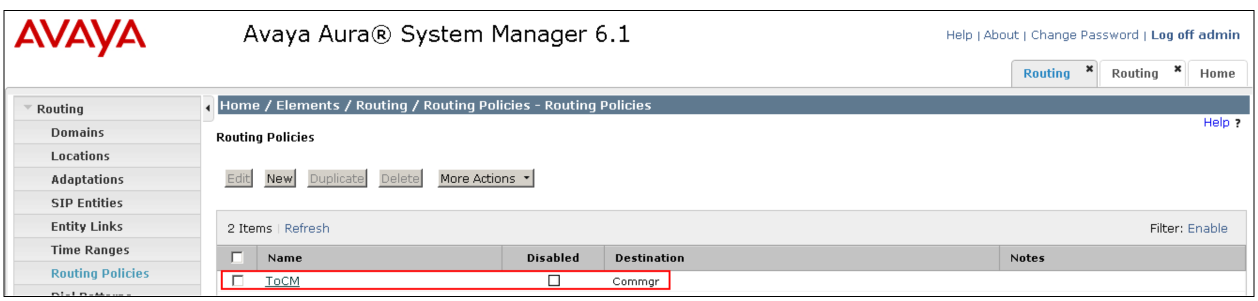
To complete the routing configuration, a Routing Policy is created. Routing policies determine how calls will be routed to an attached system. Two routing policies must be created, one for the Communications Manager and the second for the Mobile Convergence Controller. These will be associated with the Dial Patterns created in **Section 6.7**.

6.6.1. Create Routing Policy to Avaya Aura® Communication Manager

Click **Home → Elements → Routing → Routing Polices →New**, assign an indentifying **Name** for the route. Under the **SIP Entity as Destination** section, click on **Select** and choose the CM SIP Entity and click **Select**. Click **Commit** when done.

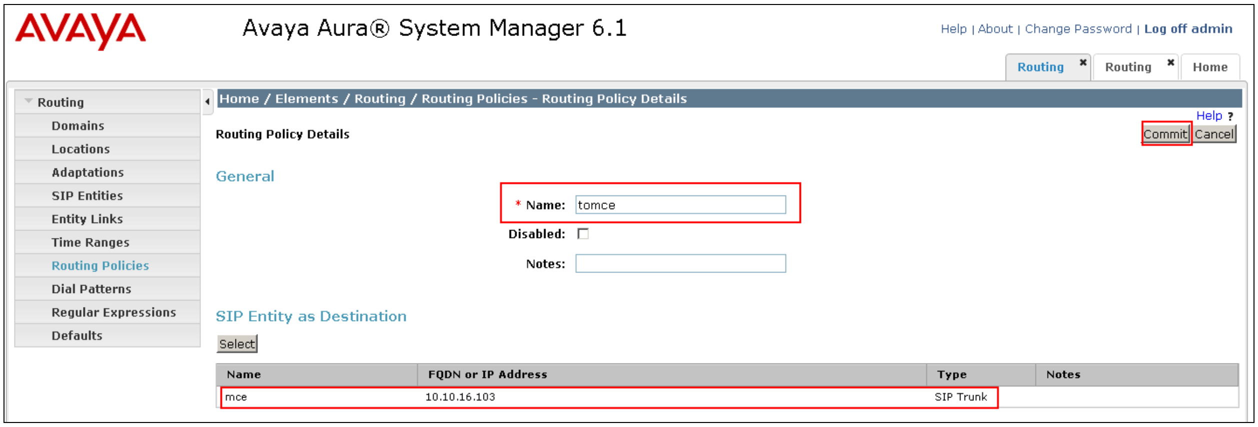


The screen below will be shown confirming the entry.

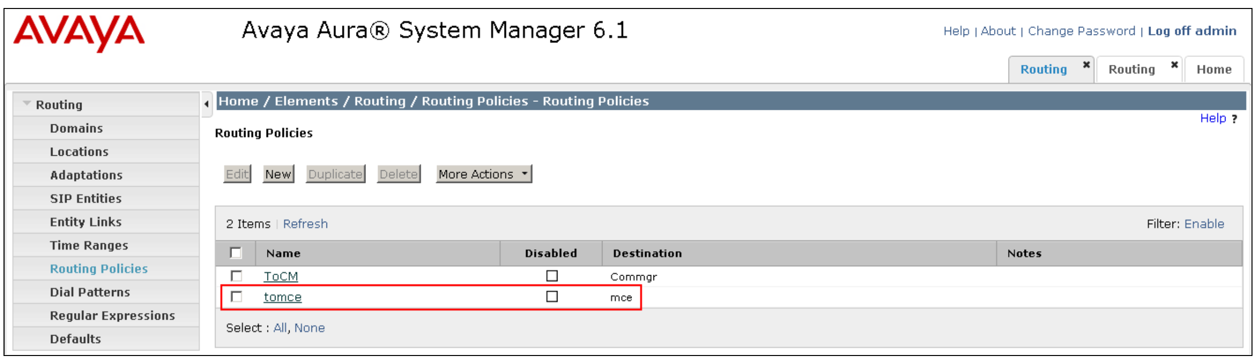


6.6.2. Create Routing Policy to Comdasys Mobile Convergence Controller

Click **Home** → **Elements** → **Routing** → **Routing Polices** →**New**, assign an indentifying **Name** for the route. In the **SIP Entity as Destination** section, click on **Select** and choose the Mobile Convergence Controller SIP Entity and click **Select**. Click **Commit** when done.



The screen below will be shown confirming the entry.

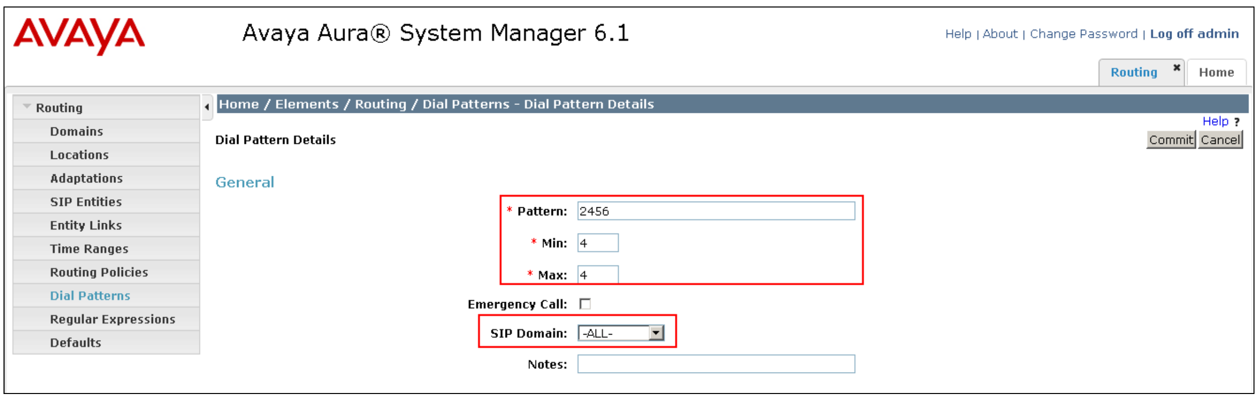


6.7. Administer Dial Patterns

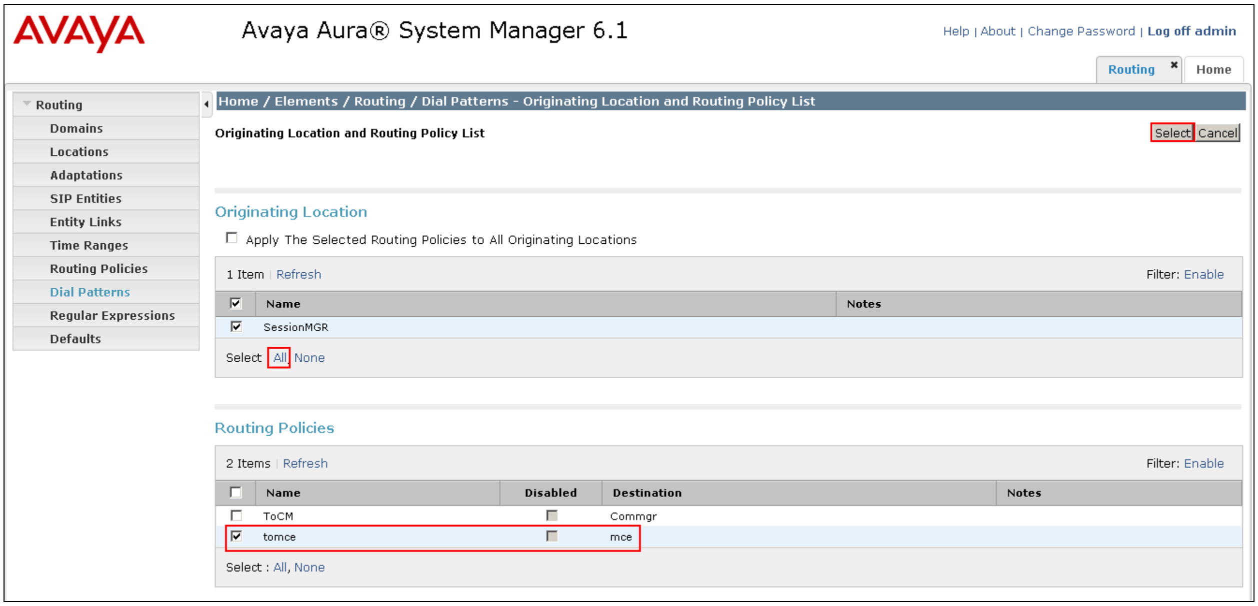
As one of its main functions, Session Manager routes SIP traffic between connected devices. Dial Patterns are created as part of the configuration to manage SIP traffic routing, which will direct calls based on the number dialed to the appropriate system.

6.7.1. Create Dial Pattern for Call Through to Comdasys Mobile Convergence Controller

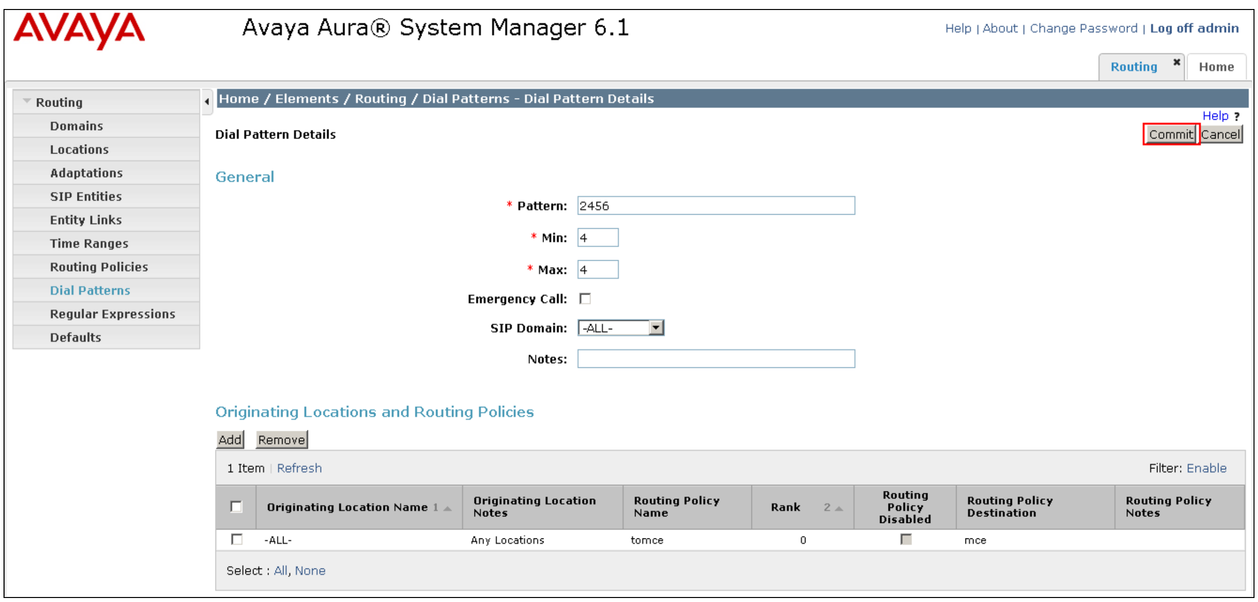
In **Section 5.6** and **Section 5.7** Communication Manager is configured to route the inbound PSTN number assigned to the Comdasys Call Through feature to Session Manager. To create a Dial Pattern to route the Call Through number from Session Manager to the Mobile Convergence Controller click **Home → Elements → Routing → Dial Patterns →New**. Under **Pattern** enter the numbers presented to Session Manager by Communication Manager for the Call Through feature in the **Patterns** box. Set **Min** and **Max** digit string length, and set **SIP Domain** to **ALL**.



In the **Originating Locations and Routing Policies** section of the web page, click **Add**. In the **Origination Location** section click **All**, in the **Routing Policies** section click the routing policy created for the Mobile Convergence Controller. Click **Select** when done.

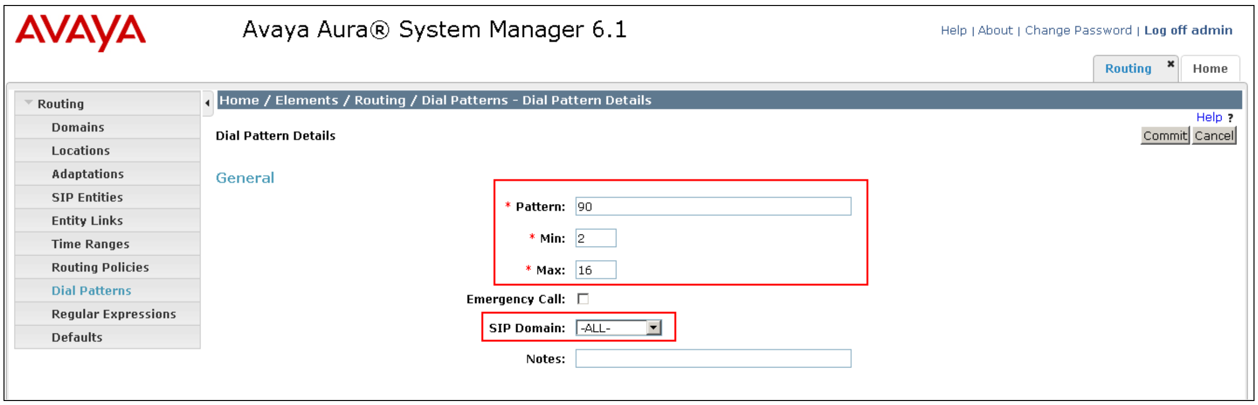


Click **Commit** when complete.

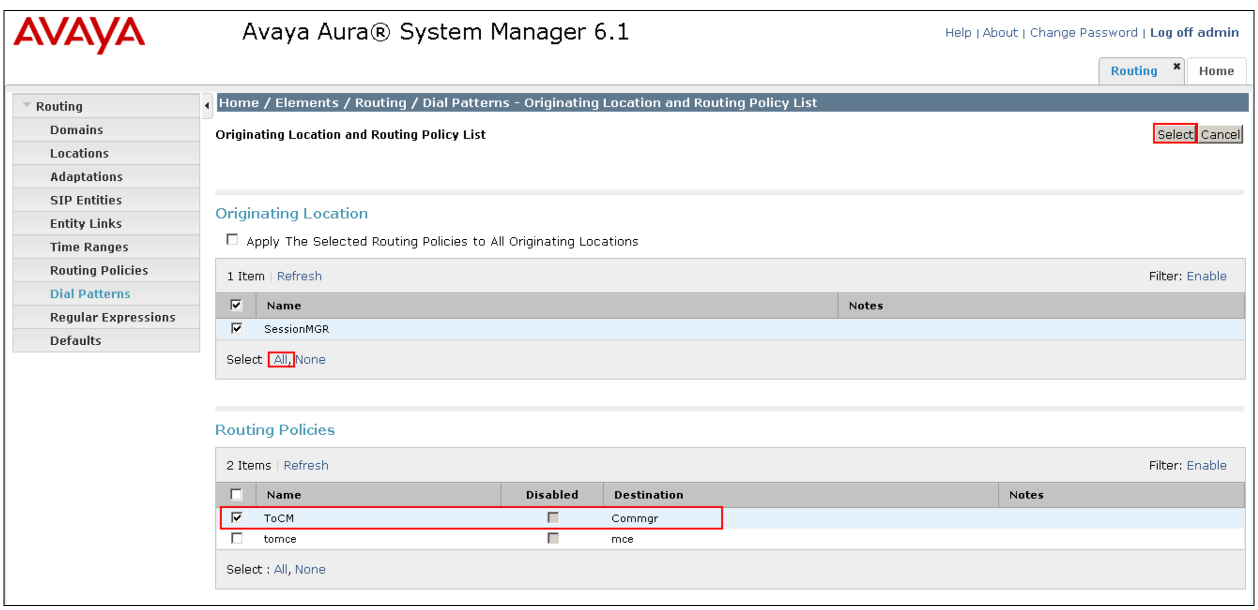


6.7.2. Create Dial Pattern to Call Mobile Device Off-net

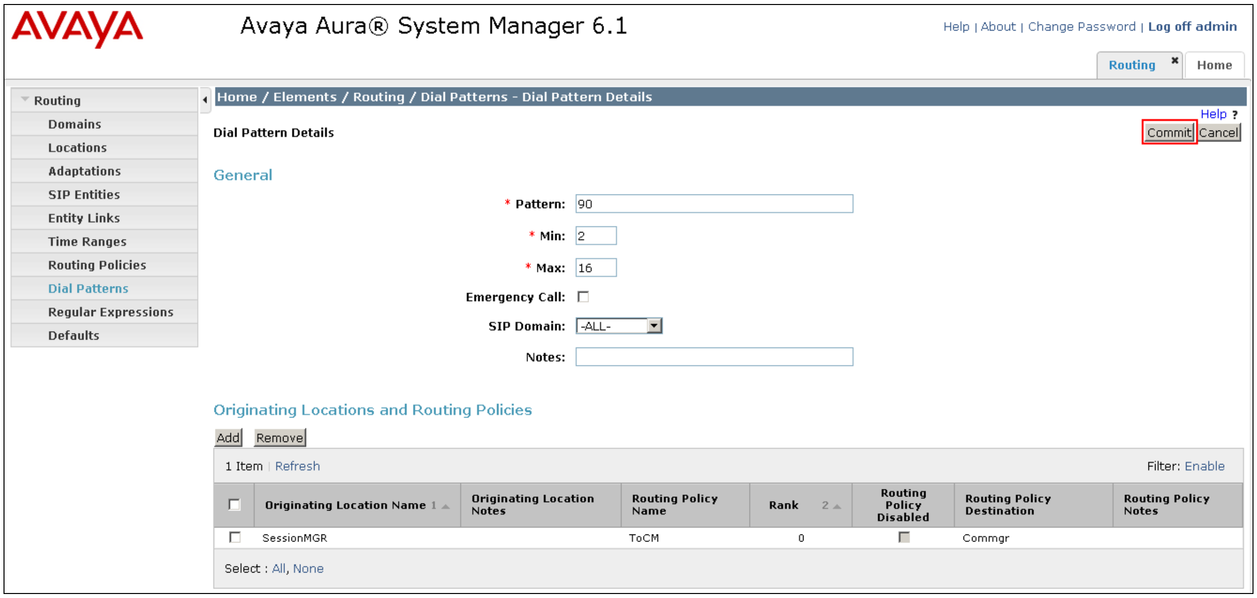
Where the Comdasys Client is not in WIFI range, a call is placed by the Mobile Convergence Controller to its corresponding Cell Phone number through Communication Manager. It is essential that a route for this is configured. Without this route, a call to the cell phone number cannot be made. Click **Home → Elements → Routing → Dial Patterns → New**. In this instance, the Communication Manager ARS code of 9 and the first digit of the cell phone number is specified. Under **Pattern** enter the digits to be presented to Communication Manager in the **Patterns** box. Set **Min** and **Max** digit string length, and set **SIP Domain** to **ALL**.



In the **Originating Locations and Routing Policies** section of the web page, click **Add**. In the **Origination Section,** click **All**, in the **Routing Policies** section click the routing policy created for Communication Manager. Click **Select** when done.



Click **Commit** when complete.



6.8. Administer Avaya Aura® Session Manager

To complete the configuration, adding the Session Manager will provide the linkage between the System Manager and Session Manager. Click **Home → Elements → Session Manager→ Session Manager Administration**. On the right hand side, under **Session Manager Instances**, click on **New**.

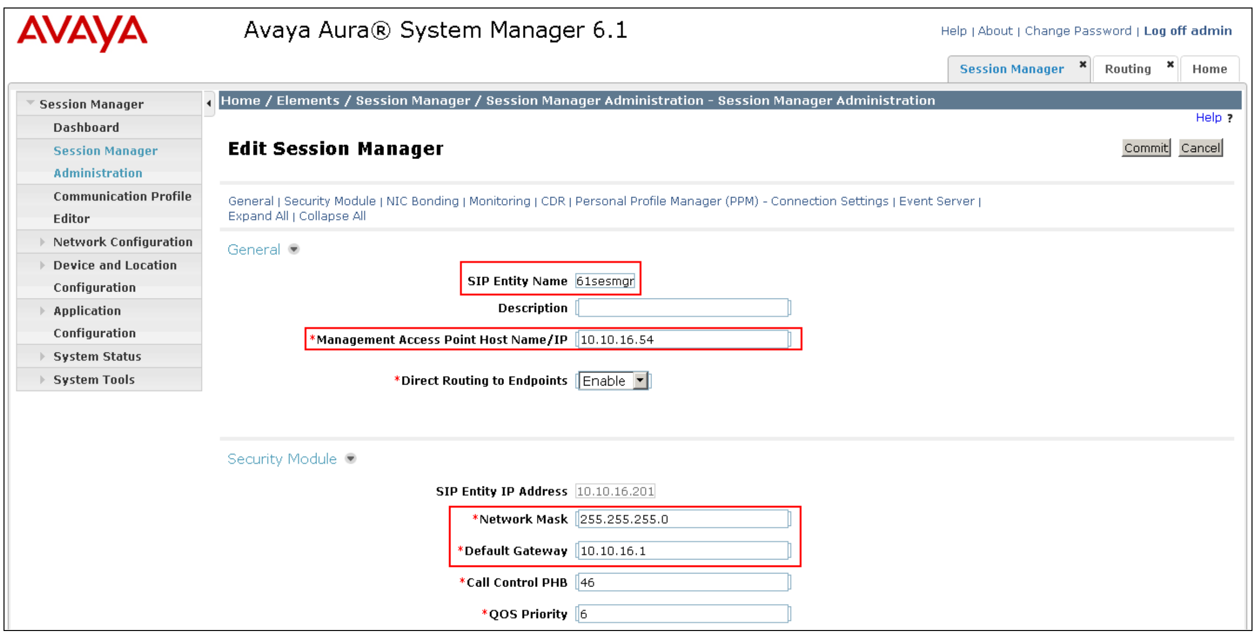
Under **General**:

- **SIP Entity name** Select the names of the SIP entity added for Session Manager
- **Management Access Point Host Name/IP** Enter the IP address of the Session Manager management interface

Under **Security Module**:

- **Network Mask** Enter the network mask corresponding to the IP address of the Session Manager
- **Default Gateway** Enter the IP address of the default gateway for Session Manager.

Use default values for the remaining fields**.**

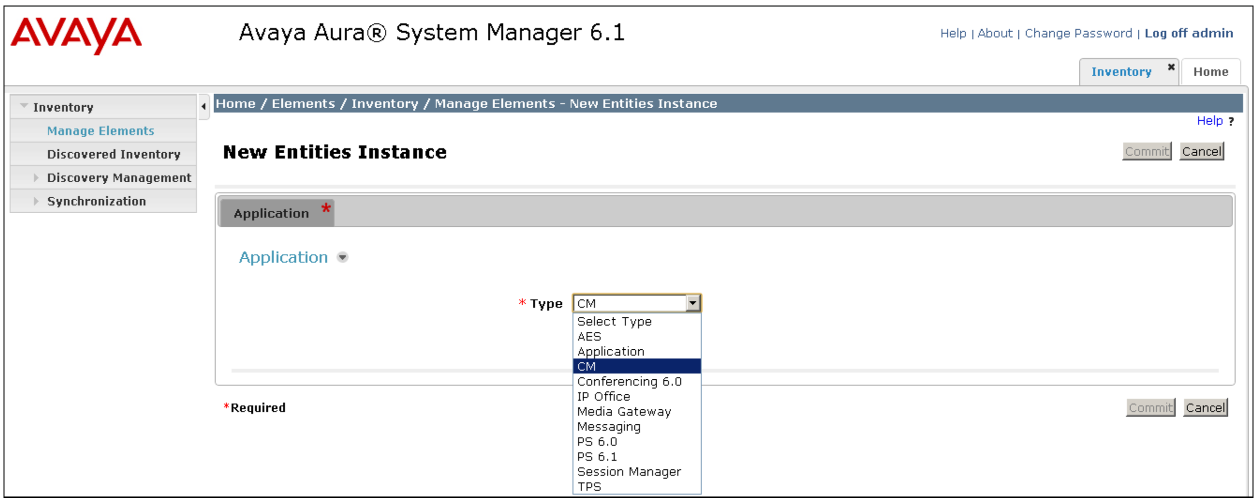


6.9. Add Avaya Aura® Communications Manager

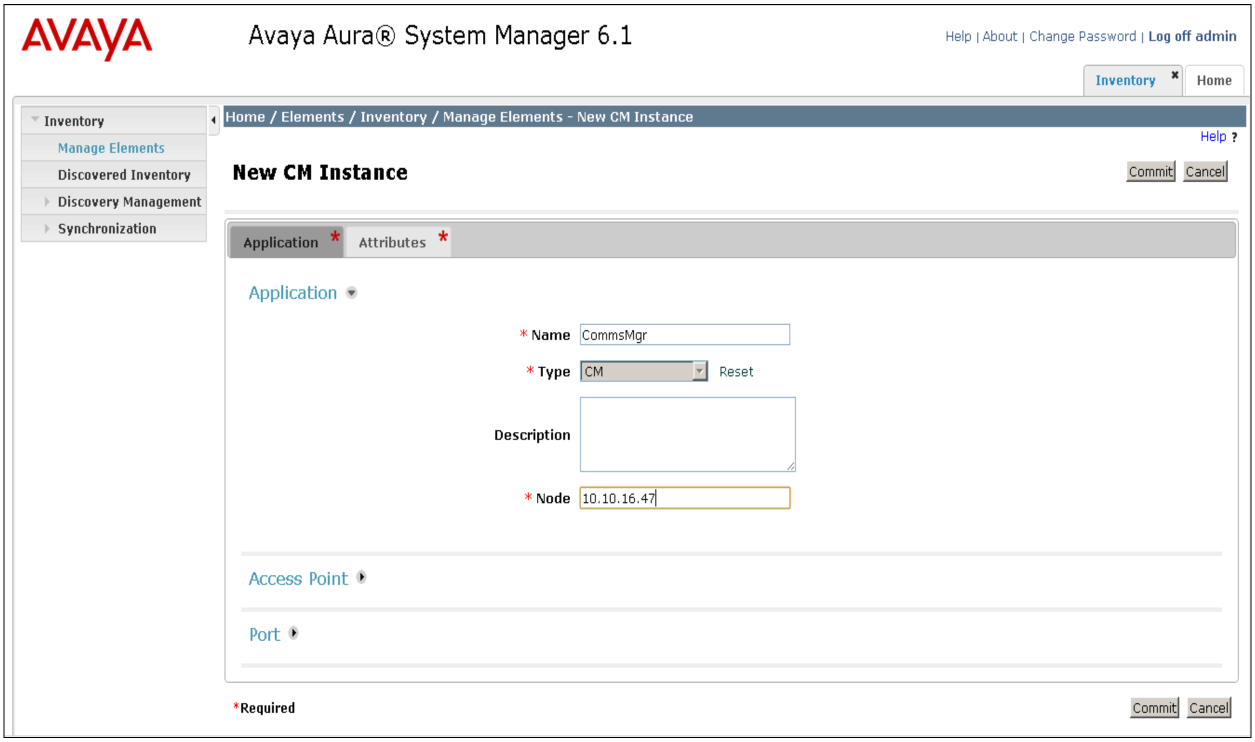
In order for Communication Manager to provide configuration and support to SIP Phones when they register to Session Manager, Communication Manager must be added as an application.

6.9.1. Create a Avaya Aura® Communication Manager Instance

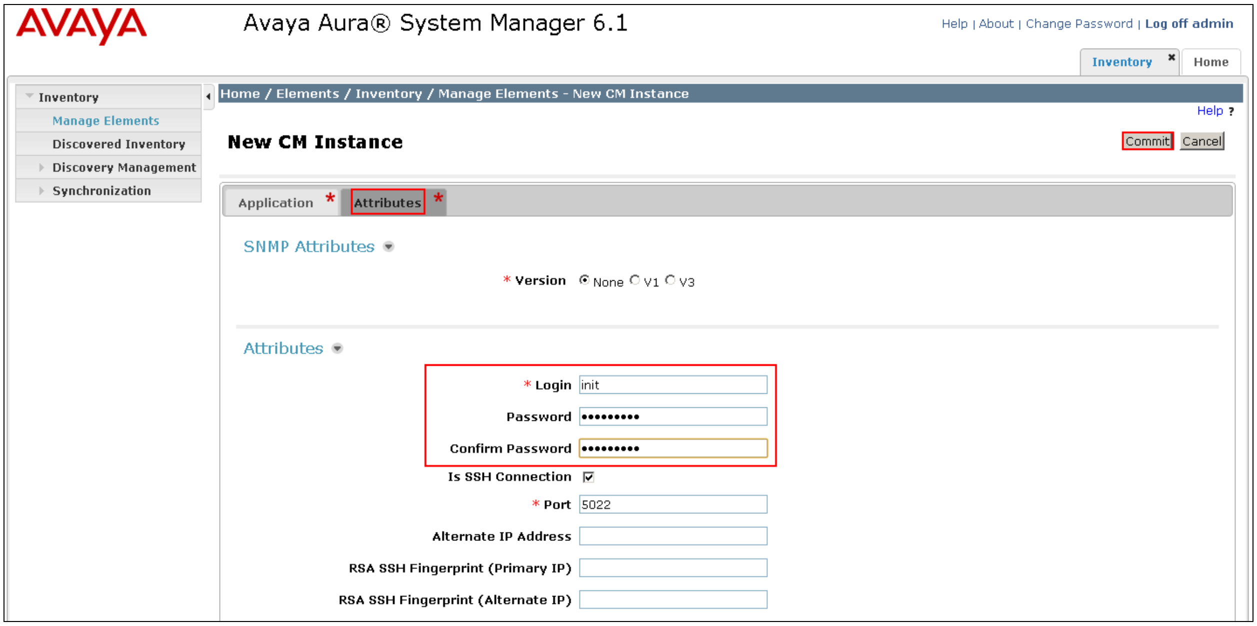
On the System Manager Managements Screen click **Home → Elements → Inventory → Manage Elements → New**. Select **CM** from the drop-down list.



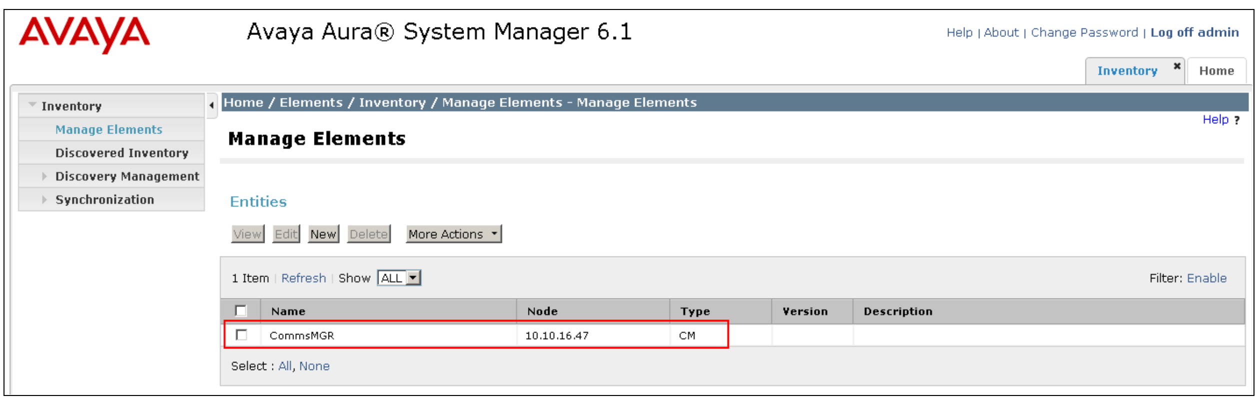
The following screen will load, enter an identifying **Name** and the IP address of the Communication Manager server as the **Node**.



Click on the **Attributes** tab and enter a valid Communication Manager **Login** and **Password**, leave all other settings as default. Click **Commit** when done.



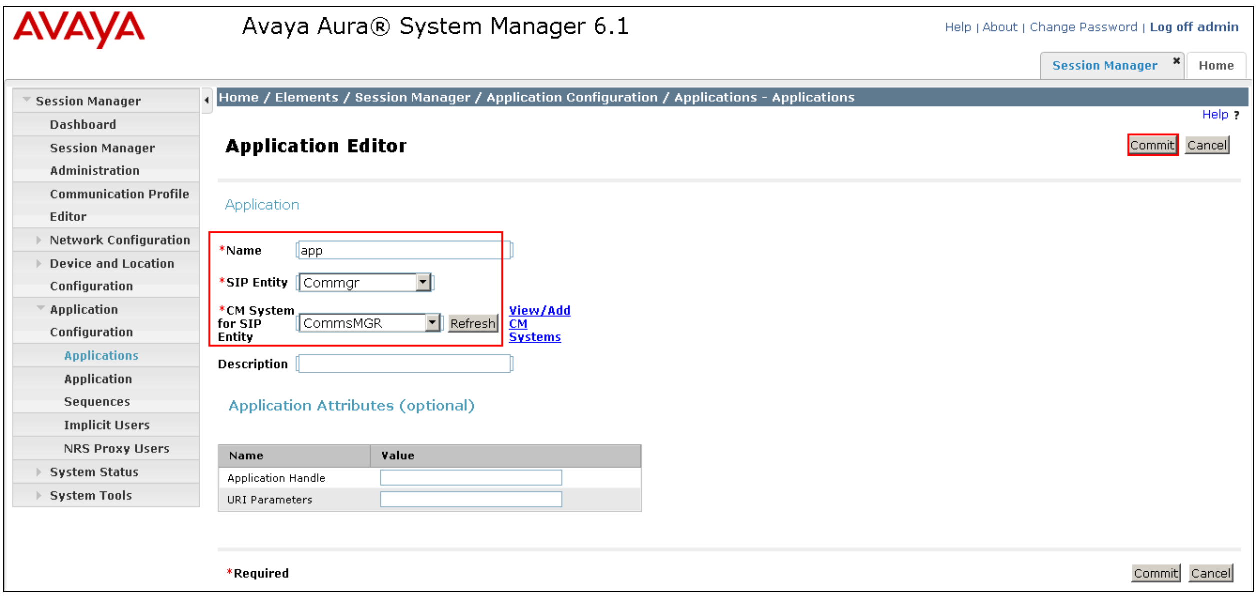
The screen below will be shown confirming the entry.



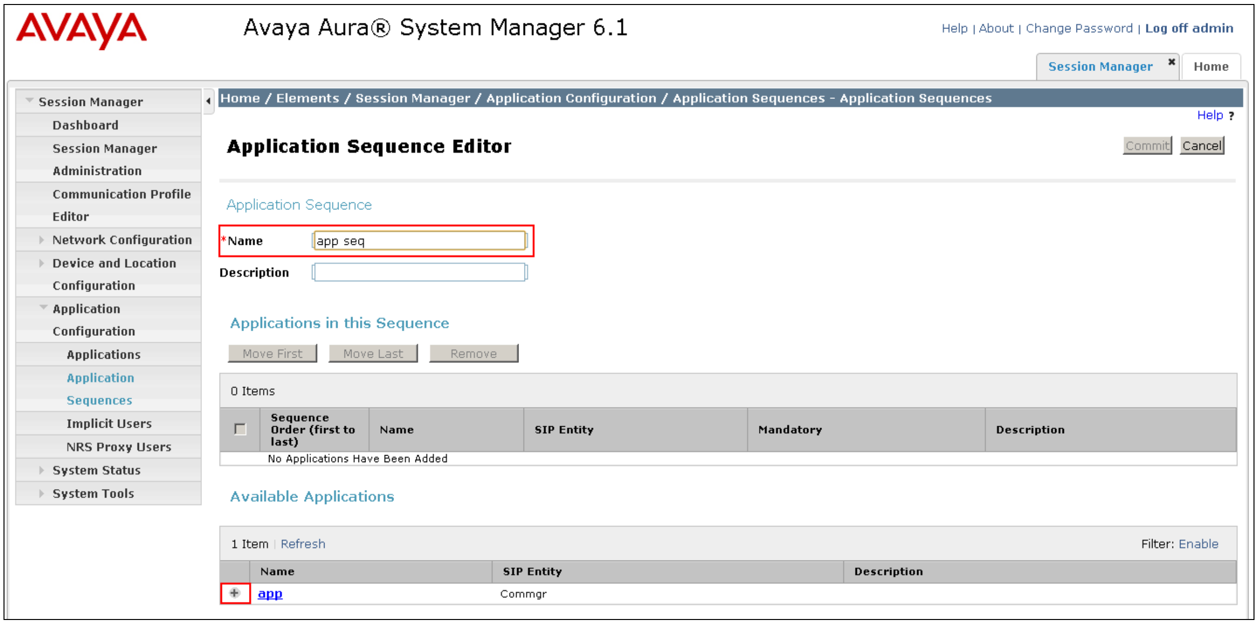
6.9.2. Create an Avaya Aura® Communication Manager Application

For Communication Manager support, further configuration of the Session Manager is required. Once complete the Session Manager will support Avaya SIP phone registration. Users are created through the Session Manager **User Management** screens. Session Manager creates corresponding stations on Communication Manager.

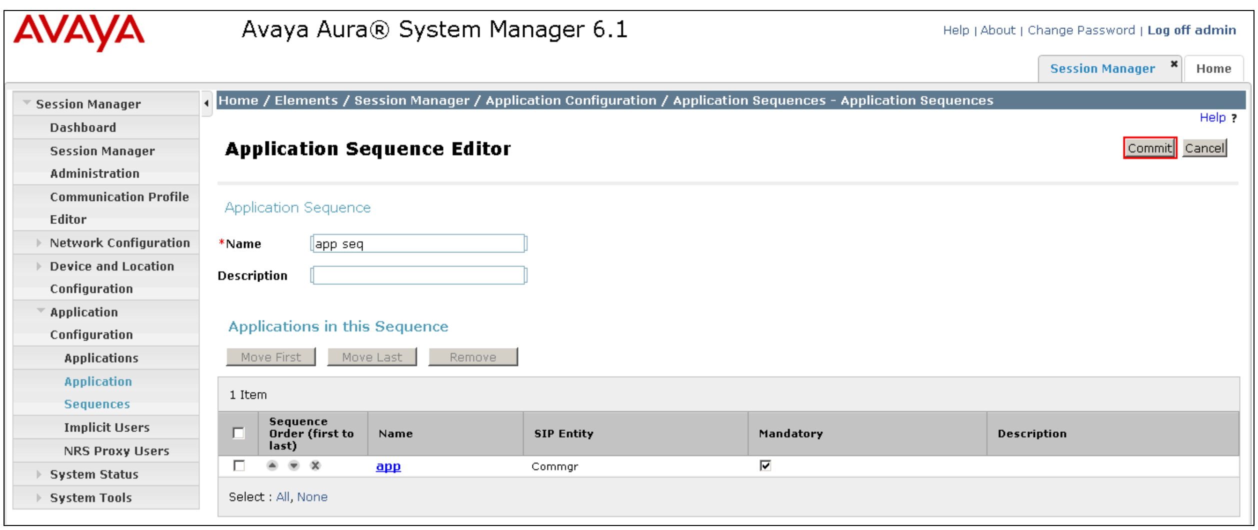
Configuration of the Communication Manager Application via Session Manager is a two stage sequence, with the Application being created first, followed by the Application Sequence. Click **Home → Elements → Session Manager → Application Configuration → Applications → New**. For **Name** enter a suitable identifier. For **SIP Entity** select the SIP Entity of Communication Manager from the drop-down list. Select the Communication Manager Instance created in **Section 6.9.1** from the **CM System for SIP Entity** drop-down list. Click **Commit** to save.



To configure the Application Sequences Configuration click **Home → -Elements → -Session Manager → Application Configuration → Applications Sequences →New**. For **Name** enter a suitable identifier. In the **Available Applications** section, select the **+** sign beside the **Application** that is to be added to this sequence.

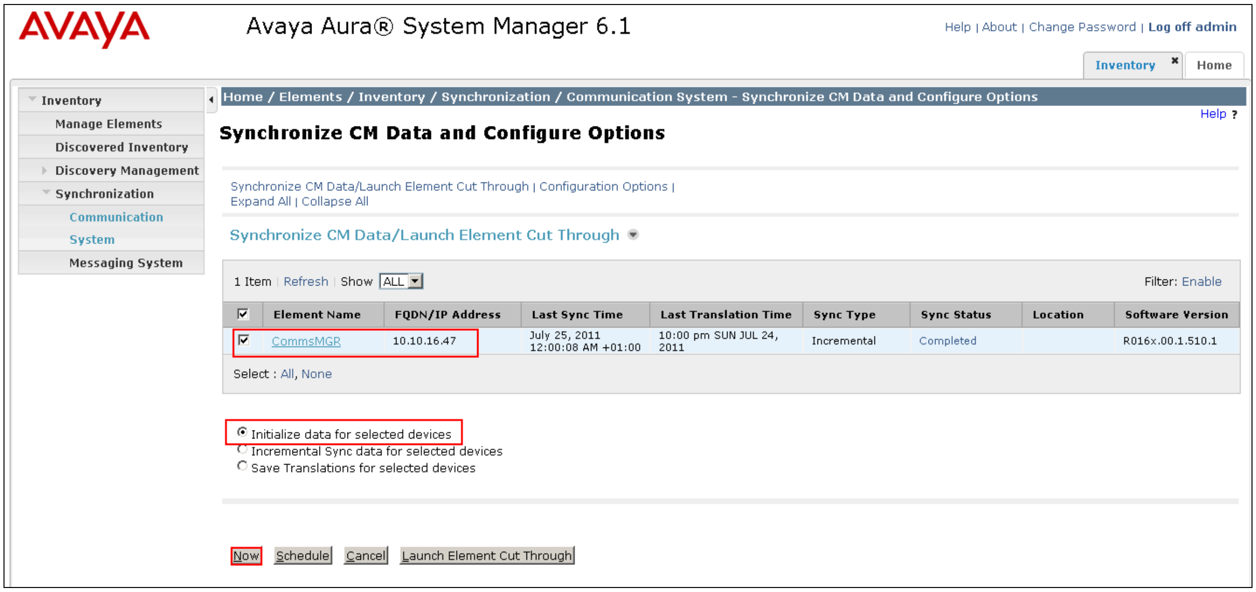


Verify that the **Applications in this Sequence** is updated correctly. Click **Commit** to save.



6.9.3. Synchronize Avaya Aura® Communication Manager Data

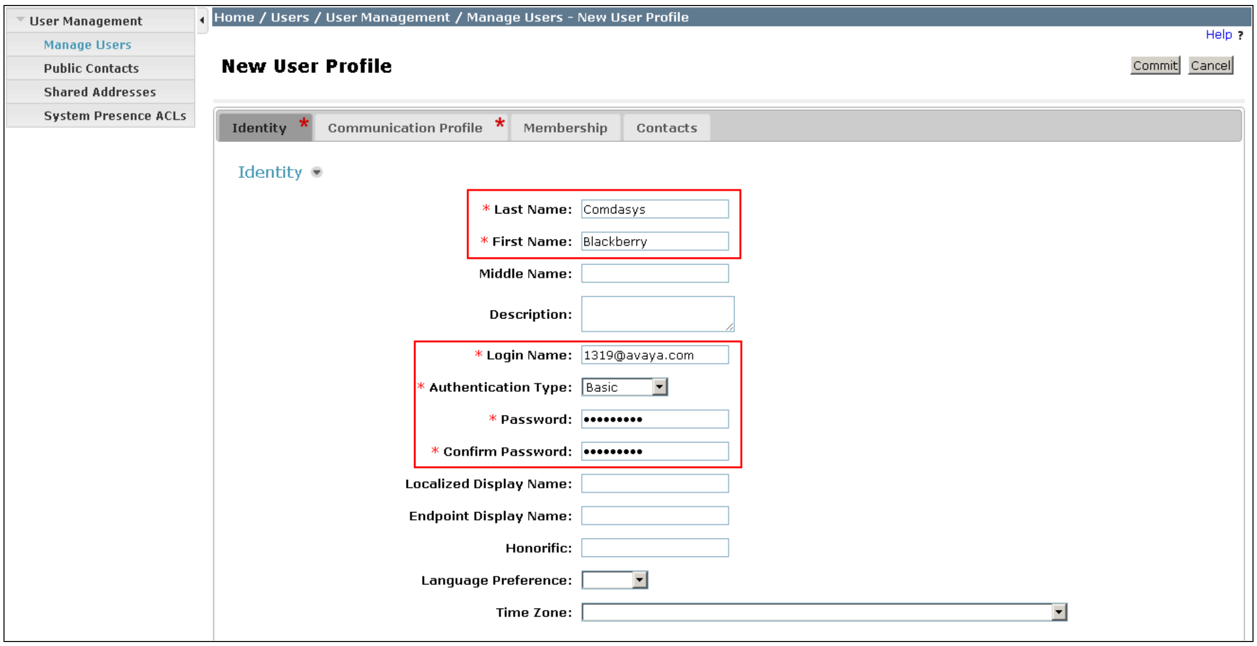
On the System Manager click **Home → Elements→Inventory → Synchronization → Communication System**. Select the appropriate **Element Name** and select **Initialize data for selected devices**. Then click on **Now**.



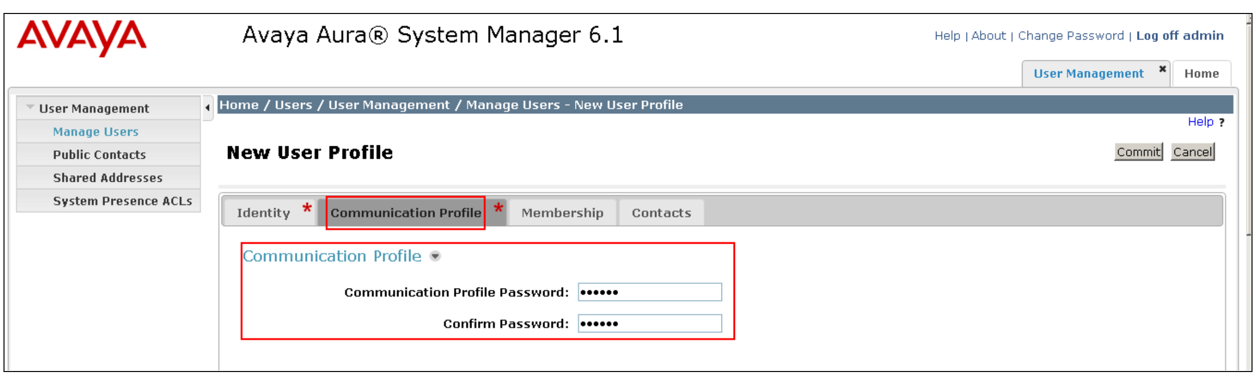
6.10. Administer SIP Users

SIP Users must be added via System Manager and the details will be updated on Session Manager and Communication Manager. Click **Home → Users → User Management → Manage Users → New**. In the **Identity** tab enter the following information and use defaults for other fields.

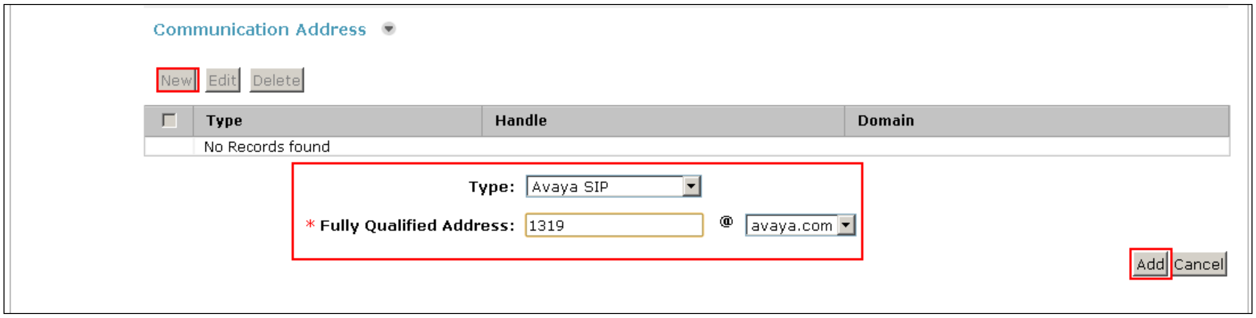
- **Last Name** Enter a last name
- **First Name** Enter a first name
- **Login Name** Enter the desired extension number in the format extension@domain.com where the domain was defined in **Section 6.2**
- **Password** Any password



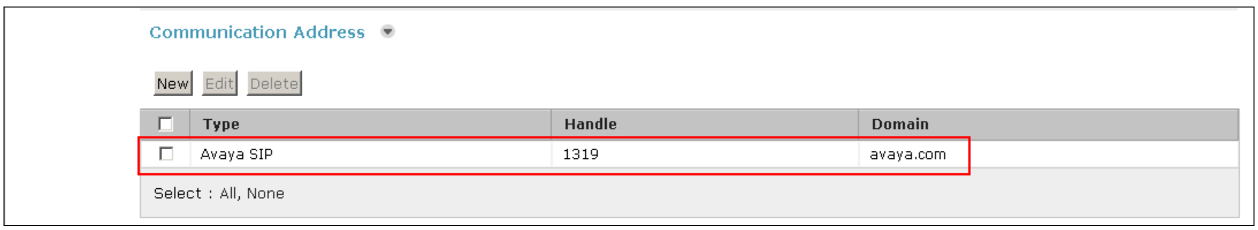
Click on the **Communication Profile** tab, configure the **Communication Profile Password**. This is the password you will use to log in the SIP user agent using the Mobile Convergence Controller.



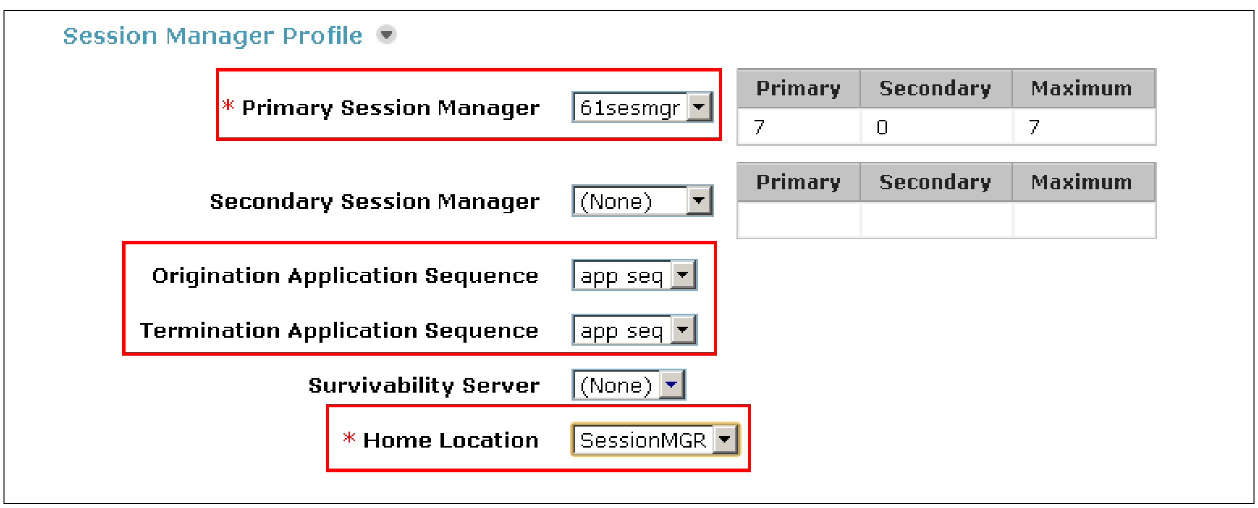
In the **Communication Address** section of the same page, click on **New**. For **Fully Qualified Address** enter the extension number and select the proper domain as configured for the **Login Name** in the **Identity** tab. Click **Add**.



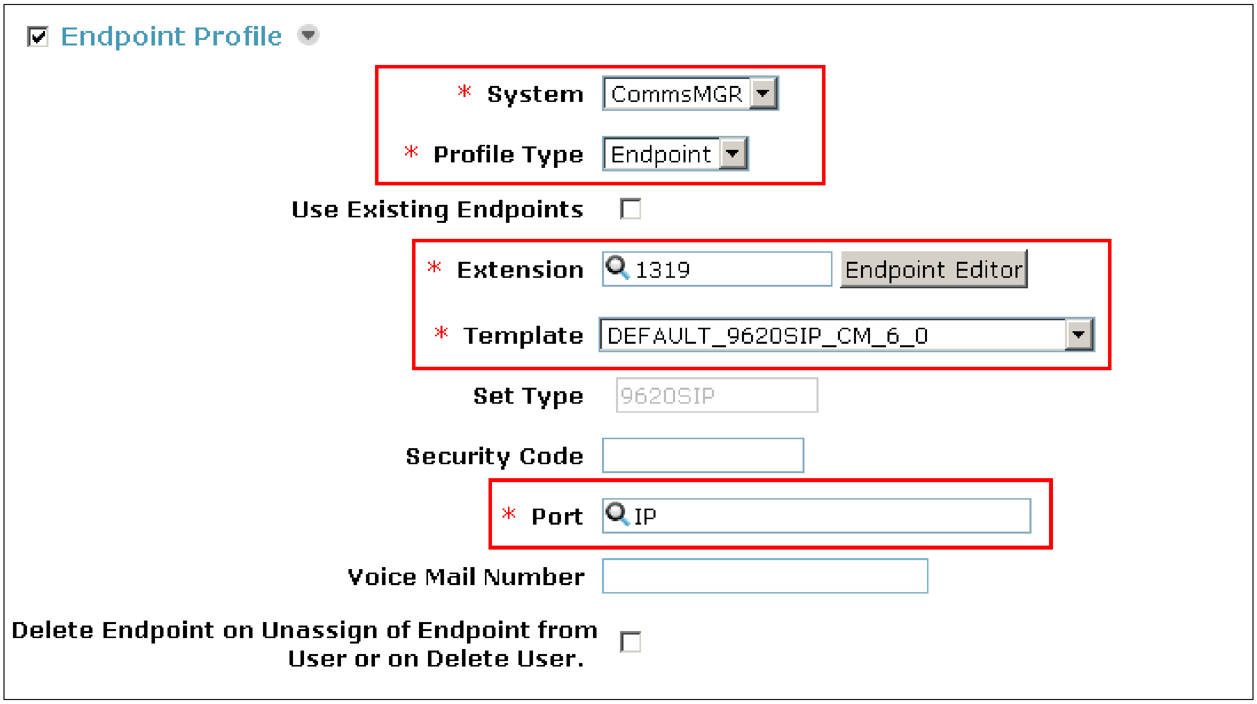
The page will display the added **Communication Address**.



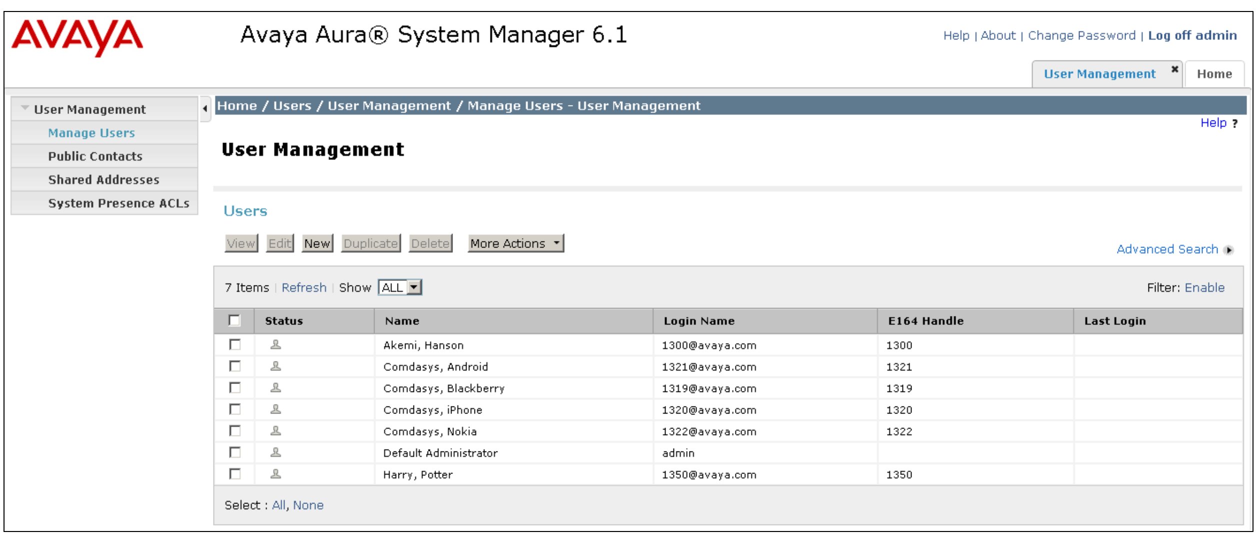
Place a tick in the **Session Manager Profile** box to expand the section. For **Primary Session Manager** select from the drop-down box the entity configured in **Section 6.4.1**. Set the **Origination Application Sequence** and **Termination Application Sequence** to the application sequence configured in **Section 6.9.2**. Set the **Home Location** as the location configured in **Section 6.3**.



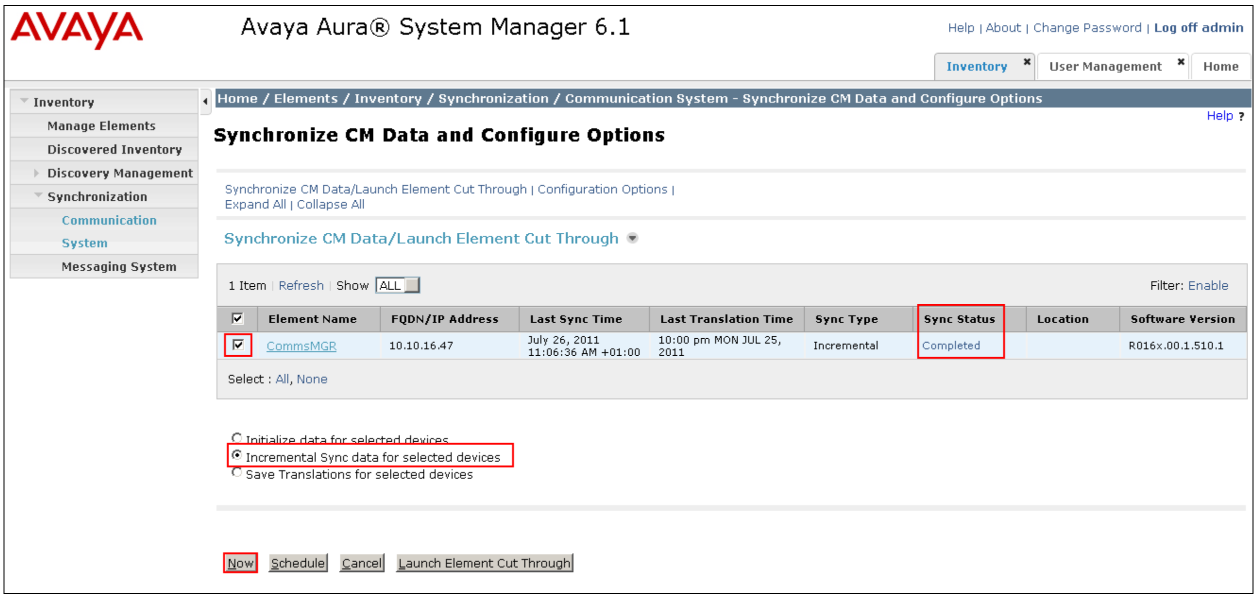
In the **Endpoint Profile** section of the same page, from the **System** drop-down box select the element configured as the CM instance in **Section 6.9.1**, set the **Profile Type** as **Endpoint**, enter the extension number configured, in this case 1319, in the **Extension** field and select the **Template** to be used for this endpoint, in this case **DEFAULT_9620SIP_CM_6_0**, set the **Port** as **IP**. Click on **Commit** (not shown) when done.



Repeat these steps for each SIP user to be added. The screen below summarizes the added SIP **Users**.



If the users cannot logon, ensure that both synchronization of SIP endpoints to Communication Manager and replication to Session Manager have occurred. For Communication Manager synchronisation confirmation, click **Home → Inventory → Synchronization → Communication System**, ensure that the **Sync Status** is **Completed**. If not, click the radio button next to **Incremental Synch data for selected devices**, click the tick box next to the **Element Name** configured in **Section 6.9.1** and click on **Now**. The **Sync Status** will show **Completed** once a full synchronisation of the data configured on System Manager has been sent to Communication Manager.



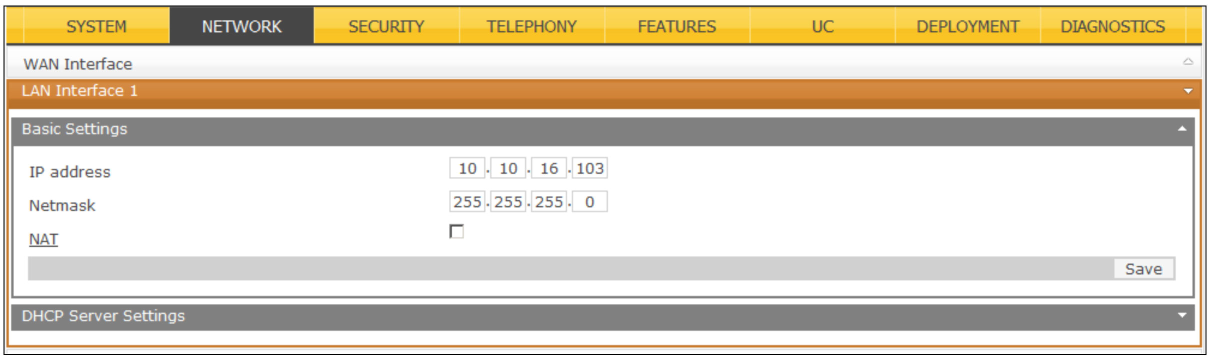
For Session Manager replication confirmation, click **Home → Services → Replication** and confirm that the **Synchronization Status** is displayed as **Synchronized** (not shown). If it is not, click the tick box next to the **Replica Group** and click **Repair**. This will force synchronization of the data from System Manager to Session Manager.

7. Configure Comdasys Mobile Convergence Controller

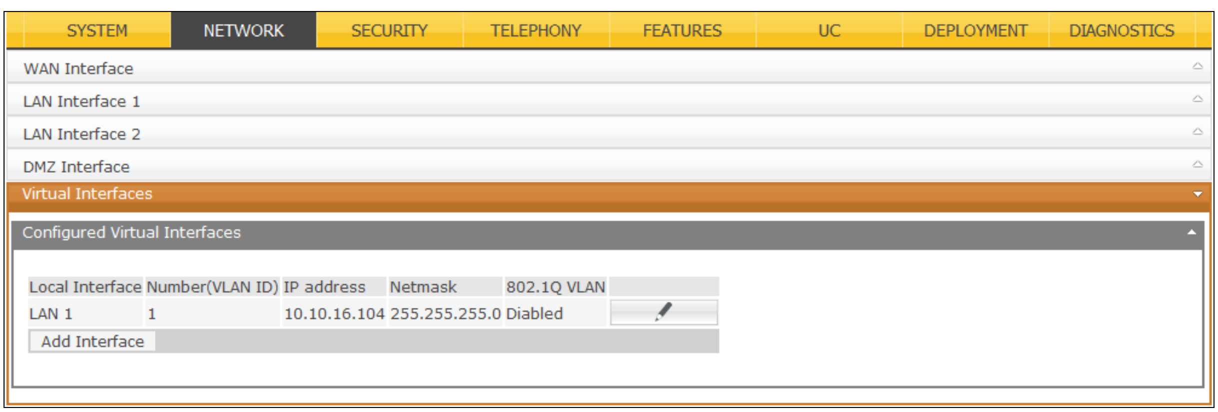
These Application Notes assume a Mobile Convergence Controller was supplied by Comdasys. All administration of the Mobile Convergence Controller is performed through its web interface. Login to the Mobile Convergence Controller web interface using its IP address, in this case https://10.10.16.103/, and enter the appropriate credentials to log on.

7.1. Administer LAN Interfaces

Two IP addresses on the LAN interface are required, one for the SIP Trunk connection to Session Manager and another one for the SIP user registrations. Click **Network → LAN Interface 1** and enter a valid **IP address** and **Netmask**, click **Save** when complete.

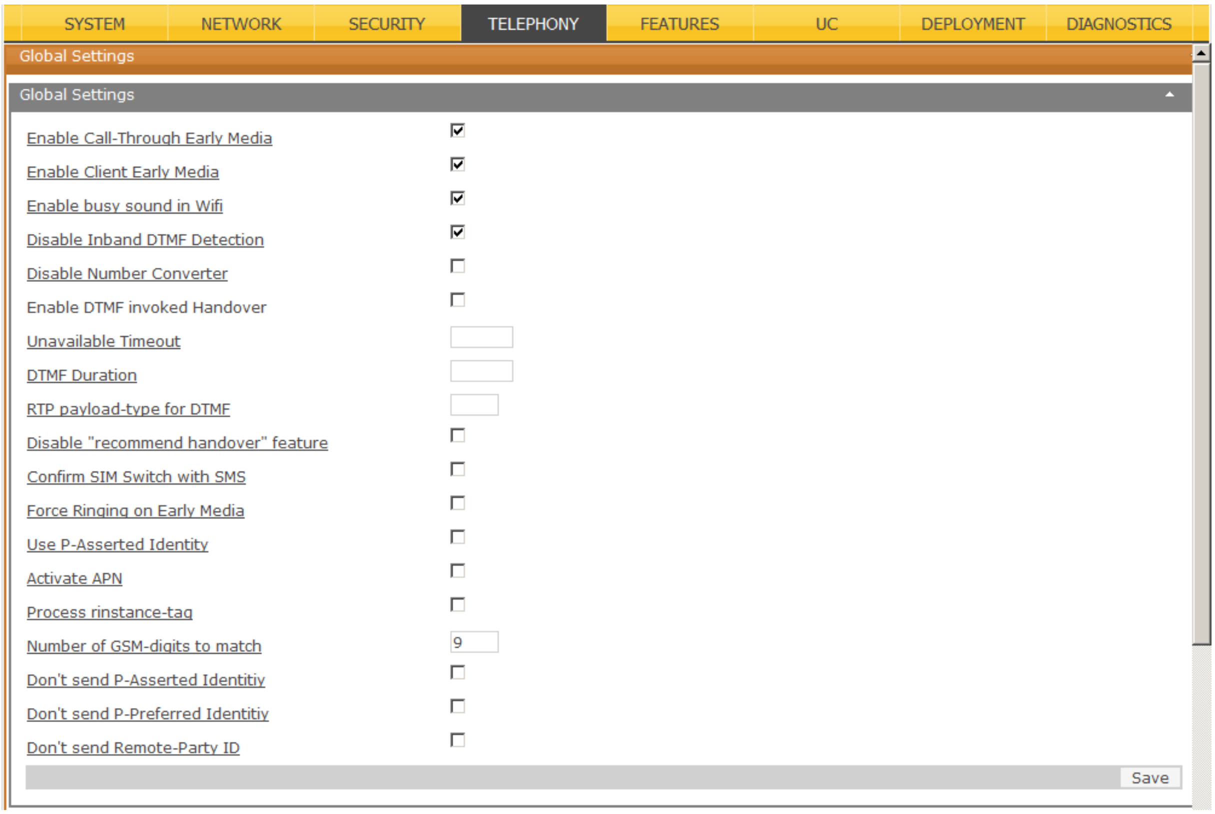


Click **Network → Virtual Interfaces → Add Interface**, select **LAN1** from the drop-down list, enter a valid **VLAN ID**, **IP address** and **Netmask** and click on  to commit. The screen below will be displayed for confirming the entry.



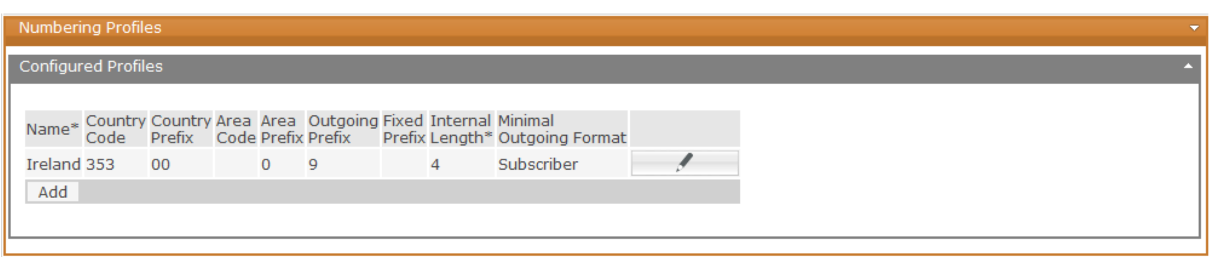
7.2. Configure Global Settings

Click **Telephony → Global Settings** to setup the global settings as indicated on the screenshot below. For details explaining the options, consult the Mobile Convergence Administrator Manual referenced in **Section 11**.



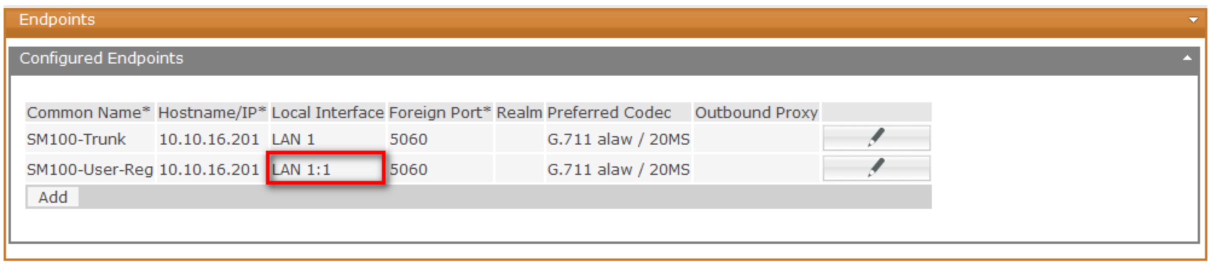
7.3. Configure Numbering Profiles

Numbering profiles are configured according to the country of implementation. Click **Telephony → Numbering Profiles → Add**, enter a **Name** to identify the locale, the international **Country Code**, the **Country Prefix** used for dialing international numbers, the local **Area Prefix**, the **Outgoing Prefix** assigned on Communication Manager (in this case the ARS Feature access code), the **Internal Length** of extensions used on Communication Manager and set **Minimal Outgoing Format** to **Subscriber**. Click on  to commit, as shown below.



7.4. Configure Endpoints

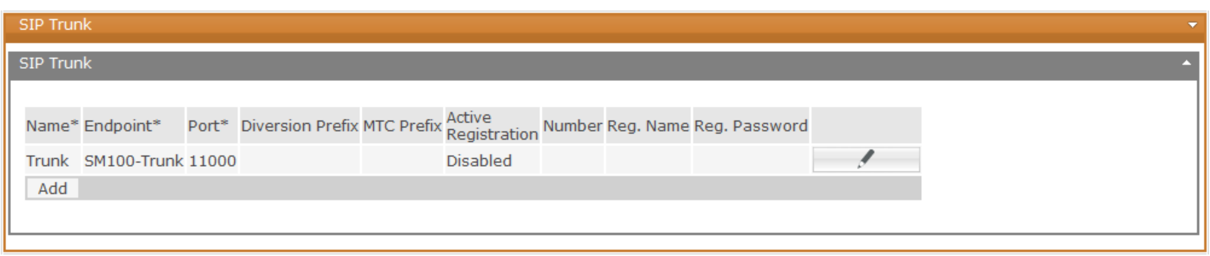
Endpoints must be configured on the Mobile Convergence Controller. One endpoint must be configured for both the SIP trunk and the SIP user registrations. Click **Telephony → Endpoints → Add**, assign a **Common Name** to identify this endpoint, set the **Hostname IP** as the IP address of the SM100 (Session Manager's signaling interface), enter the port used for SIP trunk termination and SIP user registrations as the **Foreign Port,** and choose a **Prefered Codec**. For the SIP trunk the **Local Interface** must be configured as **LAN 1**, for the SIP user registrations, the **Local Interface** must be set as the virtual interface configured in **Section 7.1**, in this case denoted as **LAN 1:1**. Click on ✓ to commit.


Endpoints
Configured Endpoints

Common Name*	Hostname/IP*	Local Interface	Foreign Port*	Realm	Preferred Codec	Outbound Proxy	
SM100-Trunk	10.10.16.201	LAN 1	5060		G.711 alaw / 20MS		
SM100-User-Reg	10.10.16.201	LAN 1:1	5060		G.711 alaw / 20MS		
Add							

7.5. Configure SIP Trunk

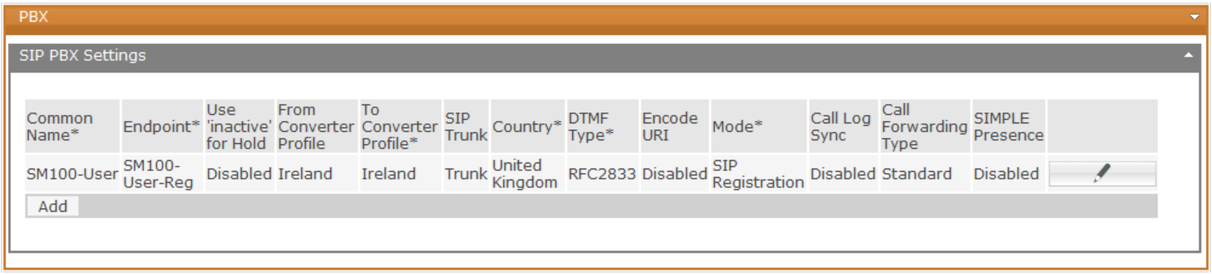
The SIP Trunk will be used whenever the Mobile Convergence Controller needs to call one of its mobiles which is not connected in Wi-Fi mode. Click **Telephony → SIP Trunk → New**. Assign an identifying **Name,** configure the **Endpoint** as the trunk endpoint configured in **Section 7.4**, choose a local **Port** number. The **Port** number is the local port on the Mobile Convergence Controller side. Click on ✓ to commit.


SIP Trunk
SIP Trunk

Name*	Endpoint*	Port*	Diversion Prefix	MTC Prefix	Active Registration	Number	Reg. Name	Reg. Password	
Trunk	SM100-Trunk	11000			Disabled				
Add									

7.6. Configure PBX Profile

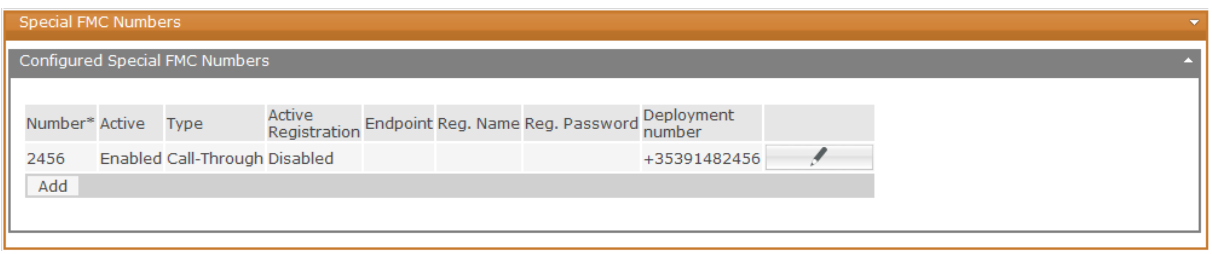
A new PBX must be added in order for SIP registrations to be made from the Mobile Convergence Controller. Click **Telephony → PBX → Add**. Assign a **Common Name** to identify this profile, select the user registration endpoint configured in **Section 7.4** as the **Endpoint**, select the numbering profile configured in **Section 7.3** as the **From Converter Profile**, select the SIP trunk configured in **Section 7.5** as the **SIP Trunk**, select the **Country** of choice, and choose **SIP Registration** as the **Mode**. Click on ✓ to commit.



Common Name*	Endpoint*	Use 'inactive' for Hold	From Converter Profile	To Converter Profile*	SIP Trunk	Country*	DTMF Type*	Encode URI	Mode*	Call Log Sync	Call Forwarding Type	SIMPLE Presence	
SM100-User	SM100-User-Reg	Disabled	Ireland	Ireland	Trunk	United Kingdom	RFC2833	Disabled	SIP Registration	Disabled	Standard	Disabled	
Add													

7.7. Configure Special FMC Number

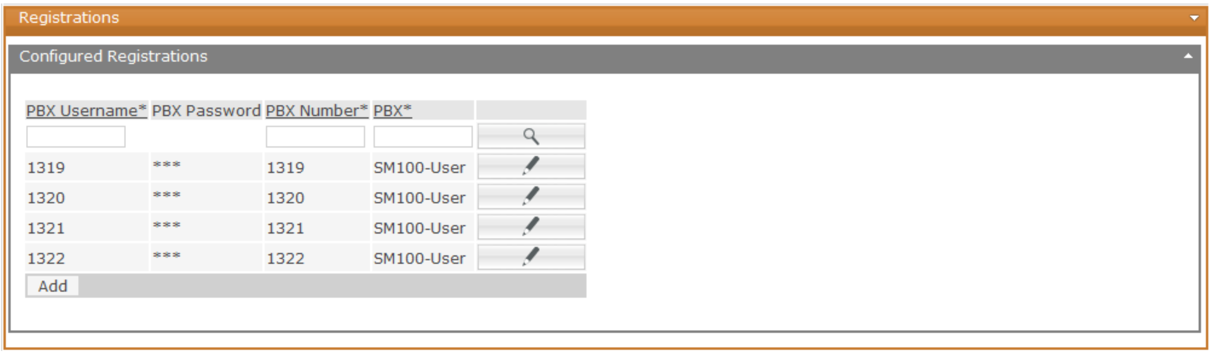
The Special FMC Number is mandatory. This single number will be shared by all users to access the call through service. Click **Telephony → Special FMC Numbers → Add**. Configure the **Number** as it is presented from Session Manager as described in **Section 6.7.1**, tick the **Enabled** box, set the **Type** as **Call-Through** and assign the **Deployment Number** as defined by its PSTN Number. Click on ✓ to commit.



Number*	Active	Type	Active Registration	Endpoint	Reg. Name	Reg. Password	Deployment number	
2456	Enabled	Call-Through	Disabled				+35391482456	
Add								

7.8. Configure SIP Registrations

Each Mobile Convergence Controller user requires a SIP registration. Click **Telephony → Registrations → Add**, assign a **PBX Username, PBX Password** and **PBX Number** as configured in **Section 6.10**. Assign a **PBX** profile as administered in **Section 7.6**. Click on to commit. Perform this task for each user required.



Registrations

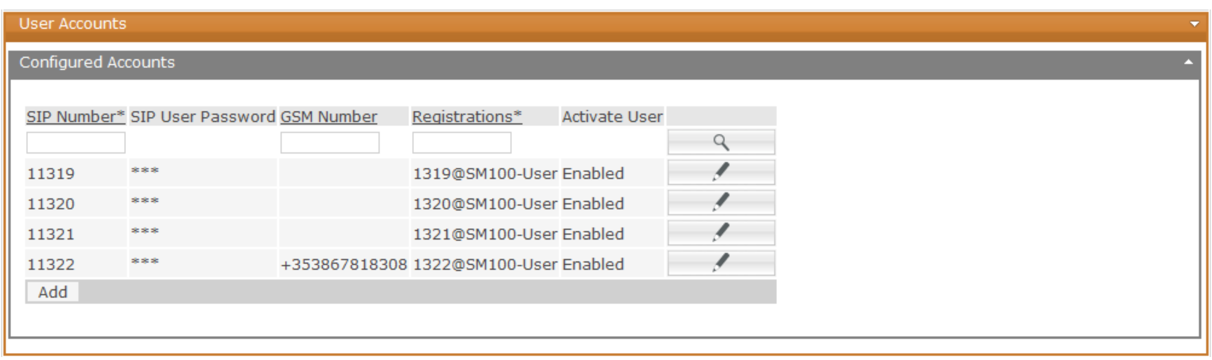
Configured Registrations

PBX Username*	PBX Password	PBX Number*	PBX*
1319	***	1319	SM100-User
1320	***	1320	SM100-User
1321	***	1321	SM100-User
1322	***	1322	SM100-User

Add

7.9. Configure SIP User Accounts

In addition to the Session Manager user account, each mobile user must use a different account to register to the Mobile Convergence Controller. It can be any username (numbers and/or letters). This user name will never show up on the PBX side. In this instance, the Session Manager SIP User extension number was prefixed with a 1. Click **Telephony → User Accounts → Add**, enter the **SIP Number**, **SIP User Password, GSM Number** as required, and the registration this SIP user should map to in the **Registrations** field. Click on to commit. Perform this task for each user required. Note that in this instance only one GSM SIM was available for testing.



User Accounts

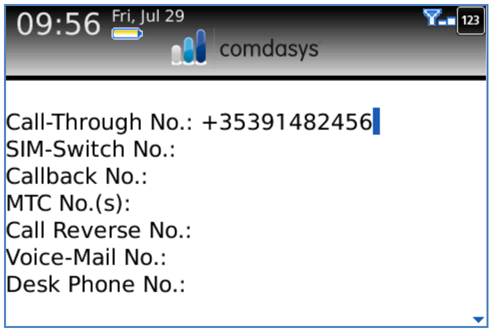
Configured Accounts

SIP Number*	SIP User Password	GSM Number	Registrations*	Activate User
11319	***		1319@SM100-User	Enabled
11320	***		1320@SM100-User	Enabled
11321	***		1321@SM100-User	Enabled
11322	***	+353867818308	1322@SM100-User	Enabled

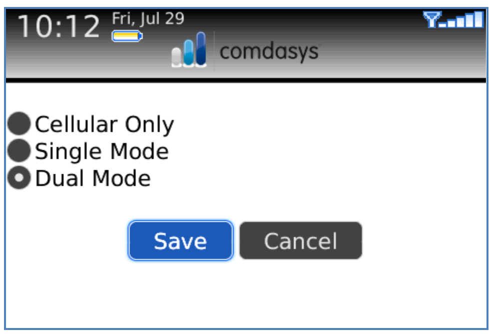
Add

8. Configure Comdasys Mobile Convergence Client

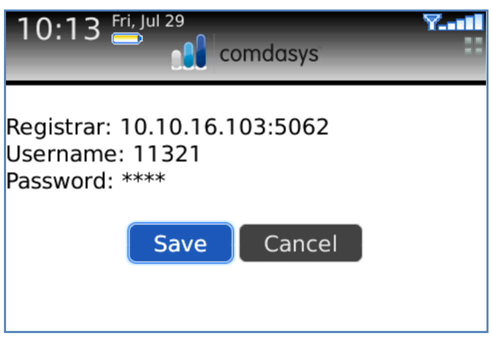
The setup of the MC Clients is not part of this document and might differ depending on the used phone platforms. However, the mandatory settings for Blackberry user, extension 11321 are described below. The **Call-Through No** must be configured in international format.



The **Dual Mode** setting tells the Client to operate over Wi-Fi, as well as GSM when in range.



Configure the **Registrar**, **Username** and **Password** as configured on the Mobile Convergence Controller, as shown below.



9. Verification Steps

This section provides the tests that can be performed to verify correct configuration of Avaya and Mobile Convergence Controller solution.

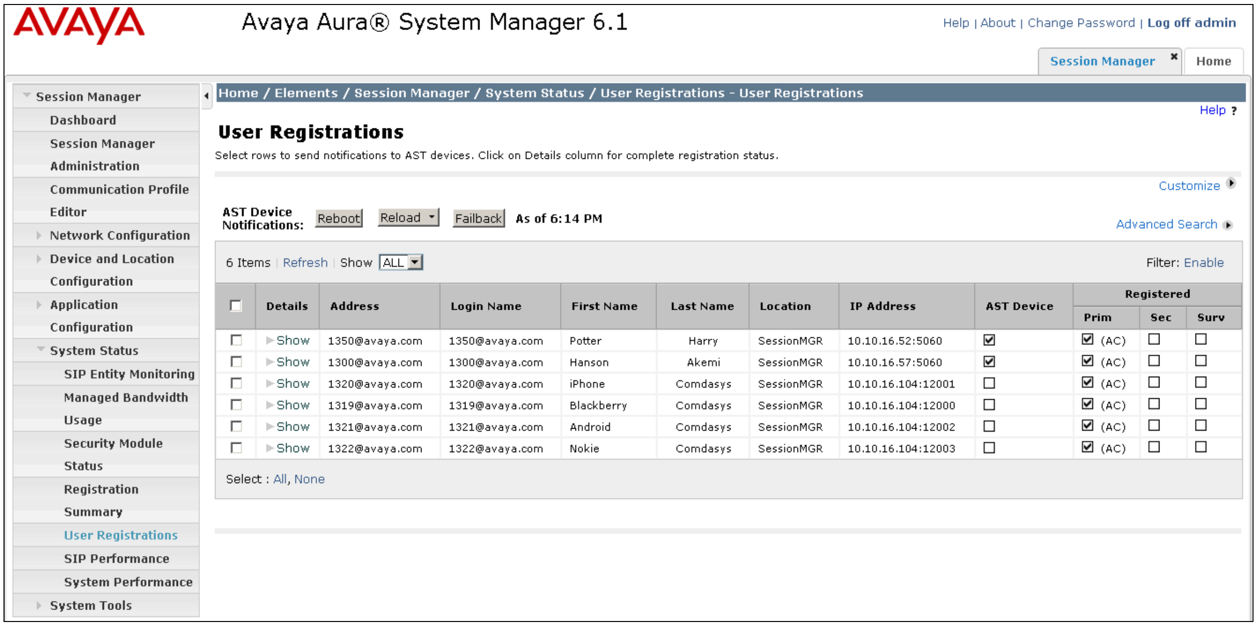
9.1. Verify Avaya Aura® Communication Manager SIP Trunk

Enter the command **status trunk x** where x is the trunk configured in **Section 5.4**. Confirm all channels are **in-service/idle**.

```
status trunk 2                                                   Page   1

                                TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy

0002/001 T00009   in-service/idle    no
0002/002 T00010   in-service/idle    no
0002/003 T00011   in-service/idle    no
0002/004 T00012   in-service/idle    no
0002/005 T00013   in-service/idle    no
0002/006 T00014   in-service/idle    no
0002/007 T00015   in-service/idle    no
0002/008 T00016   in-service/idle    no
0002/009 T00017   in-service/idle    no
0002/010 T00018   in-service/idle    no
0002/011 T00019   in-service/idle    no
0002/012 T00020   in-service/idle    no
0002/013 T00021   in-service/idle    no
0002/014 T00022   in-service/idle    no
```

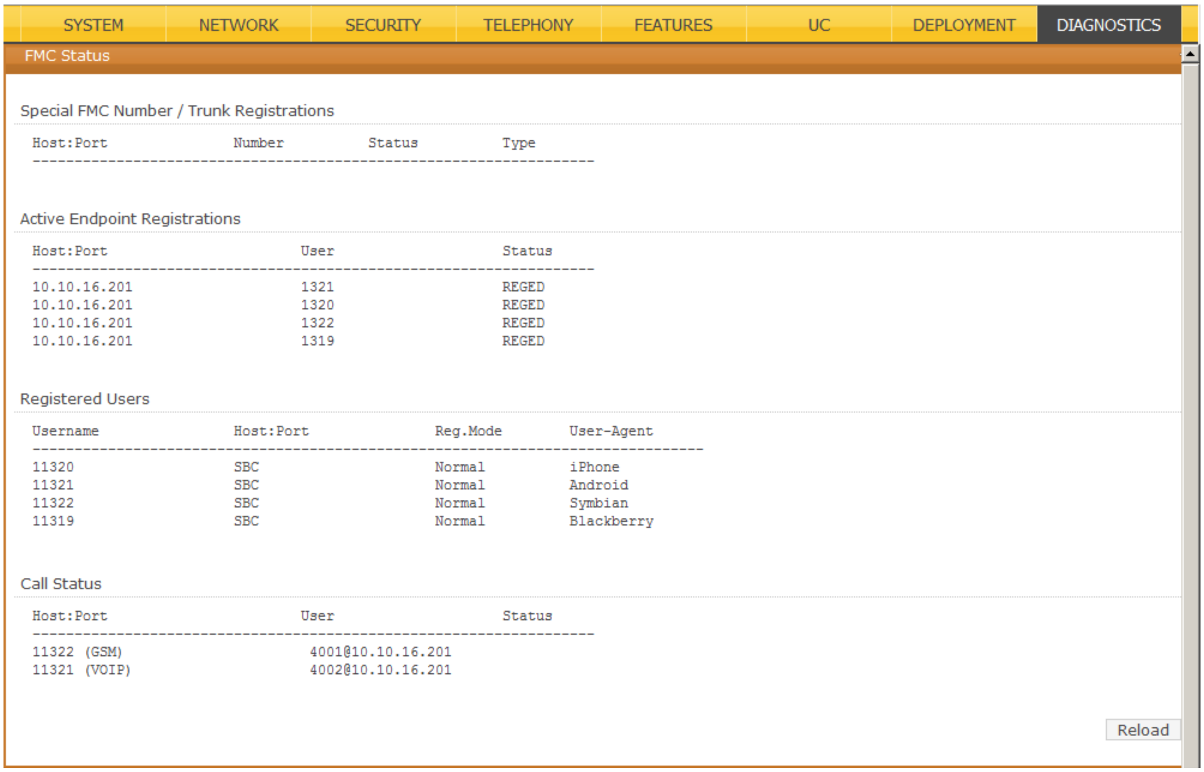
9.2. Verify Avaya Aura® Session Manager SIP User Registrations

Click on **Elements → Session Manager → System Status → User Registrations**. Confirm all the administered Mobile Convergence registrations are registered.



9.3. Verify Comdasys Mobile Convergence Controller Active Endpoint Registrations, Registered Users and VoIP/GSM Call Status

Click on **Diagnostics**. Confirm **Active Endpoint Registrations** match the SIP Users added on Session Manager, **Registered Users** match the Users administered on Mobile Convergence Controller, and confirm **Call Status** of both **GSM** and **VoIP** delivered calls.



10. Conclusion

These Application Notes describe the configuration steps required for the Comdasys Mobile Convergence Controller to successfully interoperate with Avaya Aura® Communication Manager, Avaya Aura® System Manager and Avaya Aura® Session Manager. All functionality and serviceability test cases were completed successfully.

11. Additional References

Product documentation for Avaya products may be found at http://support.avaya.com.

[1] Administering Avaya Aura® Communication Manager – Release 6.0, Issue 6.0, June 2010
[2] Administering Avaya Aura® Session Manager – Release 6.1, Issue 1, November 2010
[3] Comdasys Mobile Convergence Administrator Manual
http://ftp.comdasys.com/pub/documentation/FMC_series/
[4] Comdasys Mobile Convergence Client Manuals:
http://ftp.comdasys.com/pub/documentation/MC_Client/

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.