



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.

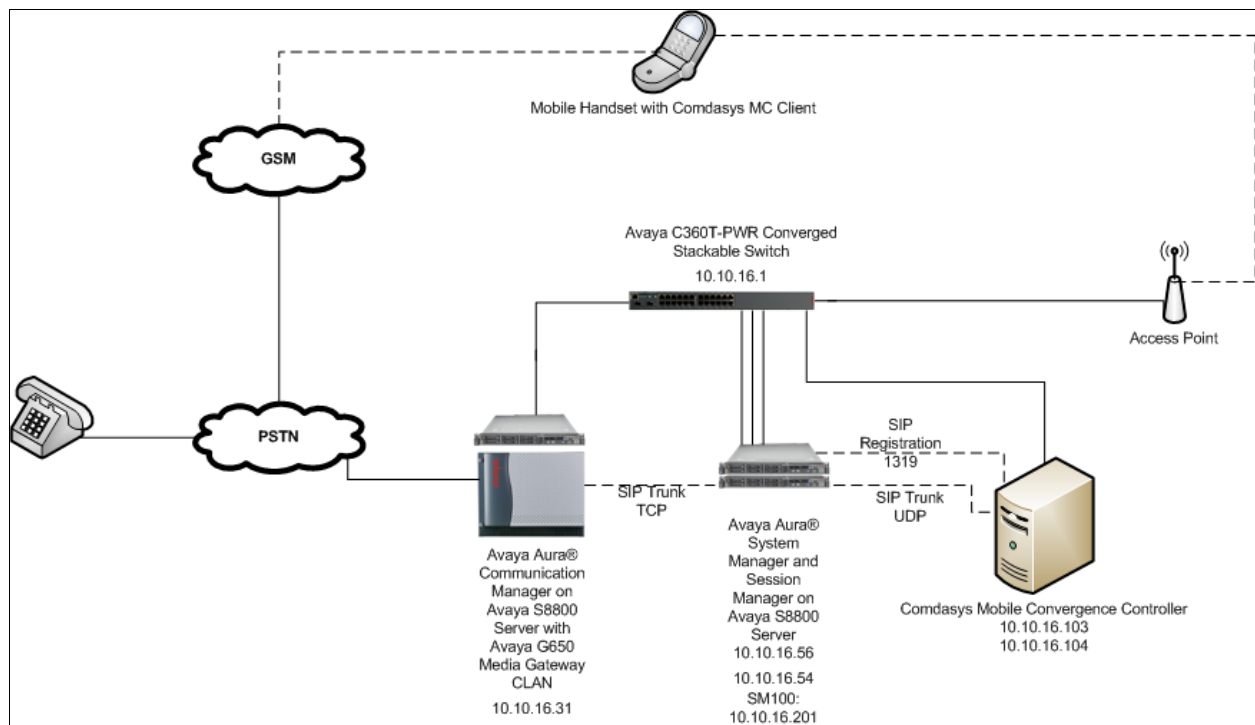


Figure 1: Avaya Aura® Communication Manager with Avaya Aura® Session Manager and Avaya Aura® System Manager and Comdasys Mobile Convergence Solution Configuration

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:		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP 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	Night Service:	
Dial Access? n			
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	
	UI 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 String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd
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/ Feature	Number Len	Number Digits	Del	Insert	Per Call CPN/BN	Night 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 Len	Ext Code	Trk Grp(s)	Private Prefix	Total Len	
4	13	2		4	Total Administered: 1
4	4	2		4	Maximum Entries: 540

6. Configure Avaya Aura® Session Manager

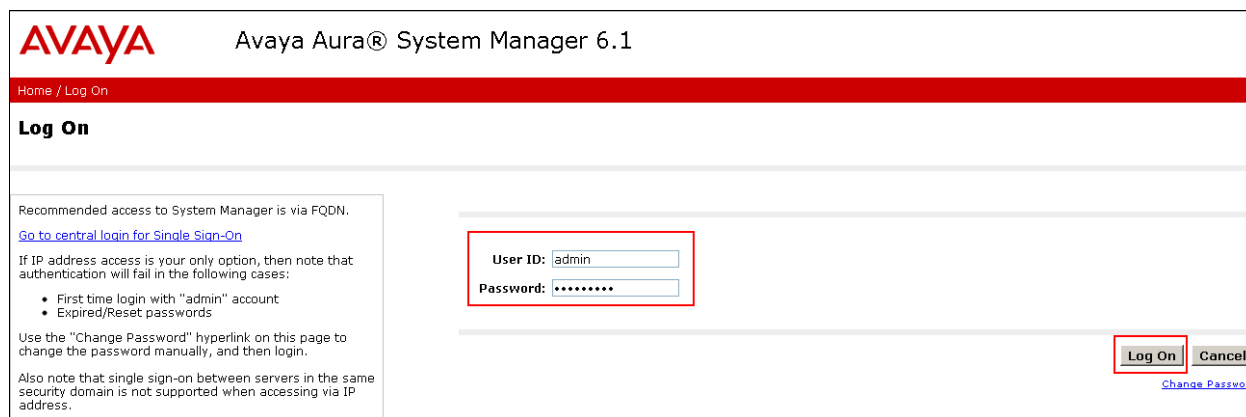
System Manager is used to configure Session Manager SIP entities and manages the connections between related SIP trunks and endpoints. It is also used to configure dial patterns and route calls according to defined rules. The configuration and verification operations illustrated in this section were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

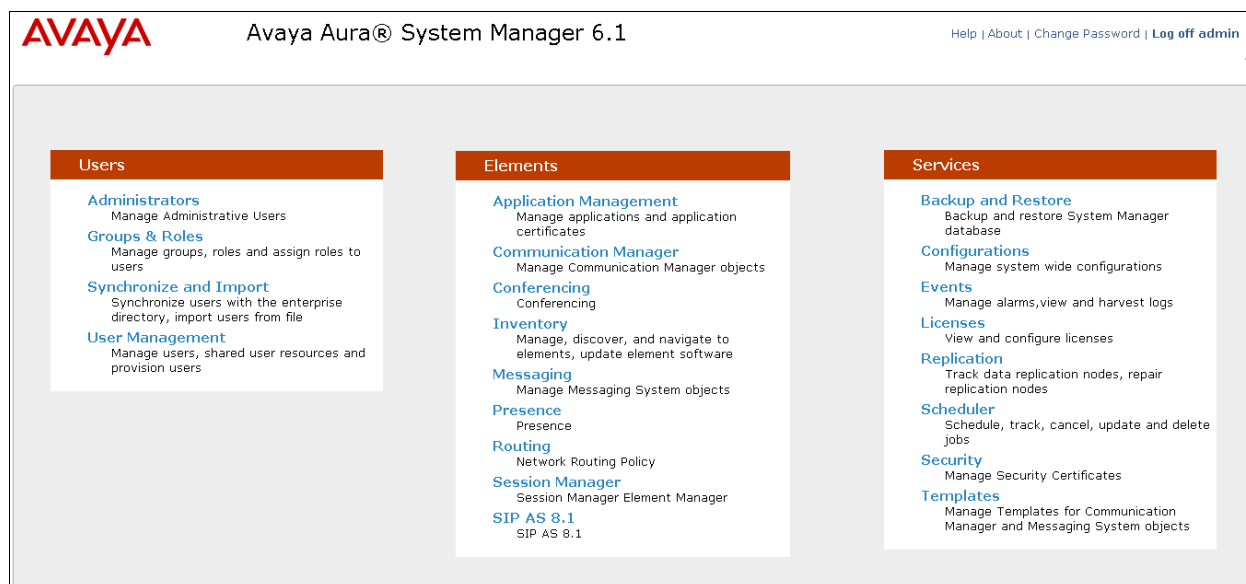
6.1. Login to Avaya Aura® System Manager

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 login page features the Avaya logo and the title 'Avaya Aura® System Manager 6.1'. A red navigation bar at the top contains the links 'Home / Log On'. Below this, a 'Log On' section is highlighted. On the left, a text box provides instructions: 'Recommended access to System Manager is via FQDN. Go to central login for Single Sign-On. If IP address access is your only option, then note that authentication will fail in the following cases: • First time login with "admin" account • Expired/Reset passwords. Use the "Change Password" hyperlink on this page to change the password manually, and then login. Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.' In the center, a red-bordered box contains the login fields: 'User ID: admin' and 'Password: *****'. To the right of these fields are 'Log On' and 'Cancel' buttons, with a 'Change Password' link below them.

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



The home screen displays the Avaya logo and title 'Avaya Aura® System Manager 6.1'. In the top right corner, there are links for 'Help | About | Change Password | Log off admin'. The main content area is divided into three columns, each with a category header and a list of sub-items:

- Users**
 - [Administrators](#)
Manage Administrative Users
 - [Groups & Roles](#)
Manage groups, roles and assign roles to users
 - [Synchronize and Import](#)
Synchronize users with the enterprise directory, import users from file
 - [User Management](#)
Manage users, shared user resources and provision users
- Elements**
 - [Application Management](#)
Manage applications and application certificates
 - [Communication Manager](#)
Manage Communication Manager objects
 - [Conferencing](#)
Conferencing
 - [Inventory](#)
Manage, discover, and navigate to elements, update element software
 - [Messaging](#)
Manage Messaging System objects
 - [Presence](#)
Presence
 - [Routing](#)
Network Routing Policy
 - [Session Manager](#)
Session Manager Element Manager
 - [SIP AS 8.1](#)
SIP AS 8.1
- Services**
 - [Backup and Restore](#)
Backup and restore System Manager database
 - [Configurations](#)
Manage system wide configurations
 - [Events](#)
Manage alarms, view and harvest logs
 - [Licenses](#)
View and configure licenses
 - [Replication](#)
Track data replication nodes, repair replication nodes
 - [Scheduler](#)
Schedule, track, cancel, update and delete jobs
 - [Security](#)
Manage Security Certificates
 - [Templates](#)
Manage Templates for Communication Manager and Messaging System objects

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**.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing × Home

Home / Elements / Routing / Domains - Domain Management

Domain Management

Commit Cancel

1 Item Refresh Filter: Enable

Name	Type	Default	Notes
* avaya.com	sip	<input type="checkbox"/>	

* Input Required

Commit Cancel

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.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing × Routing × Home

Home / Elements / Routing / Locations - Location Details

Location Details

Commit Cancel

Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth. See Session Manager -> Session Manager Administration -> Global Setting

General

* Name: SessionMGR

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Per-Call Bandwidth Parameters

* Default Audio Bandwidth: 80 Kbit/sec

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.

Location Pattern

Add Remove

1 Item Refresh Filter: Enable

IP Address Pattern	Notes
* 10.10.16.*	

Select : All, None

* Input Required

Commit Cancel

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**.

AVAYA Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing Routing Home

Home / Elements / Routing / SIP Entities - SIP Entity Details

SIP Entity Details

General

* Name: 61sesmgr

* FQDN or IP Address: 10.10.16.201

Type: Session Manager

Notes:

Location: SessionMGR

Outbound Proxy:

Time Zone: America/Fortaleza

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

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

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing * Routing * Home

Home / Elements / Routing / SIP Entities - SIP Entities

SIP Entities

Edit New Duplicate Delete More Actions ▾

3 Items Refresh Filter: Enable

<input type="checkbox"/>	Name	FQDN or IP Address	Type	Notes
<input checked="" type="checkbox"/>	61sesmgr	10.10.16.201	Session Manager	

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.

Port

Add Remove

2 Items Refresh Filter: Enable

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	TCP ▾	avaya.com ▾	
<input type="checkbox"/>	5060	UDP ▾	avaya.com ▾	

Select : All, None

* Input Required

Commit Cancel

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**.

AVAYA Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing × Routing × Home

Home / Elements / Routing / SIP Entities - SIP Entity Details

SIP Entity Details

General

* Name: Commgr

* FQDN or IP Address: 10.10.16.31

Type: CM

Notes:

Adaptation:

Location: SessionMGR

Time Zone: Etc/GMT

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: none

SIP Link Monitoring: Use Session Manager Configuration

Commit Cancel

The screen below will now be displayed confirming the entry.

AVAYA Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing × Routing × Home

Home / Elements / Routing / SIP Entities - SIP Entities

SIP Entities

Edit New Duplicate Delete More Actions

3 Items Refresh Filter: Enable

	Name	FQDN or IP Address	Type	Notes
<input type="checkbox"/>	s1sesmgr	10.10.16.201	Session Manager	
<input checked="" type="checkbox"/>	Commgr	10.10.16.31	CM	

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**.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing x Routing x Home

Home / Elements / Routing / SIP Entities - SIP Entity Details

SIP Entity Details

General

* Name: mce

* FQDN or IP Address: 10.10.16.103

Type: SIP Trunk

Notes:

Adaptation: [v]

Location: [v]

Time Zone: America/Fortaleza

Override Port & Transport with DNS SRV: [x]

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

Credential name:

Call Detail Recording: none

SIP Link Monitoring: Use Session Manager Configuration

Commit Cancel

The screen below will now be displayed confirming the entry.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing x Routing x Home

Home / Elements / Routing / SIP Entities - SIP Entities

SIP Entities

Edit New Duplicate Delete More Actions

3 Items Refresh Filter: Enable

	Name	FQDN or IP Address	Type	Notes
<input type="checkbox"/>	61sesmgr	10.10.16.201	Session Manager	
<input type="checkbox"/>	Commgr	10.10.16.31	CM	
<input type="checkbox"/>	mce	10.10.16.103	SIP Trunk	

Select : All, None

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.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing x Routing x Home

Home / Elements / Routing / Entity Links - Entity Links

Entity Links

Commit Cancel

1 Item | Refresh

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* toCM	* 61sesmgr	TCP	* 5060	* Commgr	* 5060	<input checked="" type="checkbox"/>	

* Input Required

Commit Cancel

The screen below will be shown confirming the entry.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing x Routing x Home

Home / Elements / Routing / Entity Links - Entity Links

Entity Links

Edit New Duplicate Delete More Actions

2 Items | Refresh

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
<input type="checkbox"/> toCM	61sesmgr	TCP	5060	Commgr	5060	<input checked="" type="checkbox"/>	

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.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing x Routing x Home

Entity Links

1 Item Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* tomce	* 61sesmgr	UDP	* 5060	* mce	* 5060	<input checked="" type="checkbox"/>	

* Input Required

Commit Cancel

The screen below will be shown confirming the entry.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing x Routing x Home

Entity Links

Edit New Duplicate Delete More Actions

2 Items Refresh Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
<input type="checkbox"/>	toCM	61sesmgr	TCP	5060	Commgr	5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	tomce	61sesmgr	UDP	5060	mce	5060	<input checked="" type="checkbox"/>	

Select : All, None

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 Policies** → **New**, assign an identifying **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.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing x Routing x Home

Home / Elements / Routing / Routing Policies - Routing Policy Details

Routing Policy Details

General

* Name: ToCM

Disabled: ☐

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Commgr	10.10.16.31	CM	

The screen below will be shown confirming the entry.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing x Routing x Home

Home / Elements / Routing / Routing Policies - Routing Policies

Routing Policies

Edit New Duplicate Delete More Actions

2 Items Refresh Filter: Enable

Name	Disabled	Destination	Notes
ToCM	<input type="checkbox"/>	Commgr	

6.6.2. Create Routing Policy to Comdasys Mobile Convergence Controller

Click **Home** → **Elements** → **Routing** → **Routing Policies** → **New**, assign an identifying **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.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing x Routing x Home

Home / Elements / Routing / Routing Policies - Routing Policy Details

Routing Policy Details

General

* Name: tomce

Disabled: ☐

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
mce	10.10.16.103	SIP Trunk	

The screen below will be shown confirming the entry.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing x Routing x Home

Home / Elements / Routing / Routing Policies - Routing Policies

Routing Policies

Edit New Duplicate Delete More Actions

2 Items Refresh Filter: Enable

Name	Disabled	Destination	Notes
ToCM	<input type="checkbox"/>	Commgr	
tomce	<input type="checkbox"/>	mce	

Select: All, None

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**.

AVAYA Avaya Aura® System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Routing](#) [Home](#)

Home / Elements / Routing / Dial Patterns - Dial Pattern Details [Help ?](#)

Dial Pattern Details [Commit](#) [Cancel](#)

General

* Pattern: 2456

* Min: 4

* Max: 4

Emergency Call: ☐

SIP Domain: ALL

Notes:

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.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing Home

Home / Elements / Routing / Dial Patterns - Originating Location and Routing Policy List

Originating Location and Routing Policy List

Select Cancel

Originating Location

☐ Apply The Selected Routing Policies to All Originating Locations

1 Item Refresh Filter: Enable

<input checked="" type="checkbox"/>	Name	Notes
<input checked="" type="checkbox"/>	SessionMGR	

Select All None

Routing Policies

2 Items Refresh Filter: Enable

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input type="checkbox"/>	ToCM	<input type="checkbox"/>	Commgr	
<input checked="" type="checkbox"/>	tomce	<input type="checkbox"/>	mce	

Select: All, None

Click **Commit** when complete.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing Home

Home / Elements / Routing / Dial Patterns - Dial Pattern Details

Dial Pattern Details

Commit Cancel

General

* Pattern: 2456

* Min: 4

* Max: 4

Emergency Call: ☐

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	tomce	0	<input type="checkbox"/>	mce	

Select: All, None

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**.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Dial Patterns - Dial Pattern Details

Dial Pattern Details

General

* Pattern: 90

* Min: 2

* Max: 16

Emergency Call: ☐

SIP Domain: ALL

Notes:

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.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Dial Patterns - Originating Location and Routing Policy List

Originating Location and Routing Policy List

Originating Location

☐ Apply The Selected Routing Policies to All Originating Locations

1 Item Refresh Filter: Enable

Name	Notes
SessionMGR	

Select: All, None

Routing Policies

2 Items Refresh Filter: Enable

Name	Disabled	Destination	Notes
ToCM	<input type="checkbox"/>	Commgr	
tomce	<input type="checkbox"/>	mce	

Select: All, None

Click **Commit** when complete.

AVAYA Avaya Aura® System Manager 6.1 Help | About | Change Password | **Log off admin**

Routing Home

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing / Dial Patterns - Dial Pattern Details

Dial Pattern Details

Help ?
Commit **Cancel**

General

* Pattern: 90

* Min: 2

* Max: 16

Emergency Call: ☐

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh

Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	SessionMGR		ToCM	0	<input type="checkbox"/>	Commgr	

Select : All, None

RCP; Reviewed:
SPOC 9/1/2011

Solution & Interoperability Test Lab Application Notes
©2011 Avaya Inc. All Rights Reserved.

30 of 51
Comdasys-CM6SM6

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.

AVAYA Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Session Manager x Routing x Home

Home / Elements / Session Manager / Session Manager Administration - Session Manager Administration

Edit Session Manager Commit Cancel

General | Security Module | NIC Bonding | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server | Expand All | Collapse All

General

SIP Entity Name 61sesmgr

Description

*Management Access Point Host Name/IP 10.10.16.54

*Direct Routing to Endpoints Enable

Security Module

SIP Entity IP Address 10.10.16.201

*Network Mask 255.255.255.0

*Default Gateway 10.10.16.1

*Call Control PHB 46

*QOS Priority 5

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.

AVAYA Avaya Aura® System Manager 6.1 Help | About | Change Password | Log off admin

Inventory * Home

Home / Elements / Inventory / Manage Elements - New Entities Instance Help ?

New Entities Instance Commit Cancel

Application *

Application

* Type

- CM
- Select Type
- AES
- Application
- CM
- Conferencing 6.0
- IP Office
- Media Gateway
- Messaging
- PS 6.0
- PS 6.1
- Session Manager
- TPS

*Required Commit Cancel

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

The screenshot shows the Avaya Aura System Manager 6.1 web interface. The top header includes the Avaya logo, the product name 'Avaya Aura® System Manager 6.1', and links for 'Help | About | Change Password | Log off admin'. A breadcrumb trail reads 'Home / Elements / Inventory / Manage Elements - New CM Instance'. The left sidebar contains a tree view with 'Inventory' expanded, showing 'Manage Elements' (selected), 'Discovered Inventory', 'Discovery Management', and 'Synchronization'. The main content area is titled 'New CM Instance' and contains two tabs: 'Application' (active) and 'Attributes'. The 'Application' tab has a dropdown menu labeled 'Application' with a right-pointing arrow. Below this are four required fields, each marked with a red asterisk: 'Name' (text box with 'CommsMgr'), 'Type' (dropdown menu with 'CM' selected and a 'Reset' button), 'Description' (text area), and 'Node' (text box with '10.10.16.47'). Below these fields are three more sections, each with a dropdown arrow: 'Access Point', 'Port', and an unlabeled section. At the bottom left, a legend indicates '* Required'. At the bottom right, there are 'Commit' and 'Cancel' buttons.

AVAYA Avaya Aura® System Manager 6.1 Help | About | Change Password | Log off admin

Inventory * Home

Home / Elements / Inventory / Manage Elements - New CM Instance Help ?

New CM Instance Commit Cancel

Application * Attributes *

Application ▾

* Name CommsMgr

* Type CM Reset

Description

* Node 10.10.16.47

Access Point ▾

Port ▾

* Required Commit Cancel

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

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Inventory x Home

Home / Elements / Inventory / Manage Elements - New CM Instance

New CM Instance

Application * **Attributes** *

SNMP Attributes

* Version ☒ None ☐ V1 ☐ V3

Attributes

* Login

Password

Confirm Password

Is SSH Connection ☒

* Port

Alternate IP Address

RSA SSH Fingerprint (Primary IP)

RSA SSH Fingerprint (Alternate IP)

Commit **Cancel**

The screen below will be shown confirming the entry.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Inventory x Home

Home / Elements / Inventory / Manage Elements - Manage Elements

Manage Elements

Entities

[View](#) [Edit](#) [New](#) [Delete](#) [More Actions](#)

1 Item | Refresh | Show **ALL**

Filter: Enable

<input type="checkbox"/>	Name	Node	Type	Version	Description
<input type="checkbox"/>	CommsMGR	10.10.16.47	CM		

Select : All, None

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.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Session Manager * Home

Home / Elements / Session Manager / Application Configuration / Applications - Applications

Help ?

Application Editor

Commit Cancel

Application

*Name

*SIP Entity

*CM System for SIP Entity Refresh [View/Add CM Systems](#)

Description

Application Attributes (optional)

Name	Value
Application Handle	<input type="text"/>
URI Parameters	<input type="text"/>

* Required

Commit Cancel

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.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Session Manager * Home

Home / Elements / Session Manager / Application Configuration / Application Sequences - Application Sequences

Application Sequence Editor

Application Sequence

*Name: app seq

Description:

Applications in this Sequence

Move First Move Last Remove

0 Items

Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
No Applications Have Been Added				

Available Applications

1 Item Refresh Filter: Enable

Name	SIP Entity	Description
+ app	Commgr	

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

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Session Manager * Home

Home / Elements / Session Manager / Application Configuration / Application Sequences - Application Sequences

Application Sequence Editor

Application Sequence

*Name: app seq

Description:

Applications in this Sequence

Move First Move Last Remove

1 Item

Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
<input type="checkbox"/>	app	Commgr	<input checked="" type="checkbox"/>	

Select : All, None

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**.

The screenshot shows the Avaya Aura® System Manager 6.1 interface. The top navigation bar includes the Avaya logo, the title 'Avaya Aura® System Manager 6.1', and links for 'Help', 'About', 'Change Password', and 'Log off admin'. The left sidebar contains a tree view with 'Inventory' selected, showing sub-items like 'Manage Elements', 'Discovered Inventory', 'Discovery Management', 'Synchronization', 'Communication System', and 'Messaging System'. The main content area has a breadcrumb trail: 'Home / Elements / Inventory / Synchronization / Communication System - Synchronize CM Data and Configure Options'. Below this is a section titled 'Synchronize CM Data and Configure Options' with a link to 'Synchronize CM Data/Launch Element Cut Through'. A table lists synchronization items, with one item 'CommsMGR' highlighted. Below the table, there are radio buttons for 'Initialize data for selected devices', 'Incremental Sync data for selected devices', and 'Save Translations for selected devices'. At the bottom, there are buttons for 'Now', 'Schedule', 'Cancel', and 'Launch Element Cut Through'.

	Element Name	FQDN/IP Address	Last Sync Time	Last Translation Time	Sync Type	Sync Status	Location	Software Version
<input checked="" type="checkbox"/>	CommsMGR	10.10.16.47	July 25, 2011 12:00:08 AM +01:00	10:00 pm SUN JUL 24, 2011	Incremental	Completed		R016x.00.1.510.1

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

The screenshot shows the 'New User Profile' form in the 'Identity' tab. The form includes fields for Last Name (Comdasys), First Name (Blackberry), Middle Name, Description, Login Name (1319@avaya.com), Authentication Type (Basic), Password, Confirm Password, Localized Display Name, Endpoint Display Name, Honorific, Language Preference, and Time Zone. Red boxes highlight the Last Name, First Name, Login Name, Authentication Type, Password, and Confirm Password fields.

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.

The screenshot shows the 'New User Profile' form in the 'Communication Profile' tab. The form includes fields for Communication Profile Password and Confirm Password. Red boxes highlight these two fields.

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**.

Communication Address ▾

New **Edit** **Delete**

<input type="checkbox"/>	Type	Handle	Domain
No Records found			

Type: Avaya SIP ▾
 * Fully Qualified Address: 1319 @ avaya.com ▾

Add **Cancel**

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

Communication Address ▾

New **Edit** **Delete**

<input type="checkbox"/>	Type	Handle	Domain
<input type="checkbox"/>	Avaya SIP	1319	avaya.com

Select : All, None

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**.

Session Manager Profile ▾

* Primary Session Manager 61sesmgr ▾

Secondary Session Manager (None) ▾

Origination Application Sequence app seq ▾
 Termination Application Sequence app seq ▾

Survivability Server (None) ▾

* Home Location SessionMGR ▾

Primary	Secondary	Maximum
7	0	7

Primary	Secondary	Maximum

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.

☒ **Endpoint Profile** ▼

* **System** CommsMGR ▼

* **Profile Type** Endpoint ▼

Use Existing Endpoints ☐

* **Extension** 1319 Endpoint Editor

* **Template** DEFAULT_9620SIP_CM_6_0 ▼

Set Type 9620SIP

Security Code

* **Port** IP

Voice Mail Number

Delete Endpoint on Unassign of Endpoint from User or on Delete User. ☐

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

AVAYA Avaya Aura® System Manager 6.1 Help | About | Change Password | Log off admin

User Management * Home

Home / Users / User Management / Manage Users - User Management Help ?

User Management

Users

[View](#) [Edit](#) [New](#) [Duplicate](#) [Delete](#) [More Actions](#) Advanced Search

7 Items [Refresh](#) Show **ALL** Filter: Enable

<input type="checkbox"/>	Status	Name	Login Name	E164 Handle	Last Login
<input type="checkbox"/>		Akemi, Hanson	1300@avaya.com	1300	
<input type="checkbox"/>		Comdasys, Android	1321@avaya.com	1321	
<input type="checkbox"/>		Comdasys, Blackberry	1319@avaya.com	1319	
<input type="checkbox"/>		Comdasys, iPhone	1320@avaya.com	1320	
<input type="checkbox"/>		Comdasys, Nokia	1322@avaya.com	1322	
<input type="checkbox"/>		Default Administrator	admin		
<input type="checkbox"/>		Harry, Potter	1350@avaya.com	1350	

Select : All, None

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 Sync 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.

The screenshot shows the Avaya Aura System Manager 6.1 interface. The left sidebar contains a navigation menu with 'Inventory' expanded, showing 'Manage Elements', 'Discovered Inventory', 'Discovery Management', 'Synchronization', 'Communication System', and 'Messaging System'. The main content area is titled 'Synchronize CM Data and Configure Options' and shows a breadcrumb trail: 'Home / Elements / Inventory / Synchronization / Communication System - Synchronize CM Data and Configure Options'. Below the title, there are links for 'Synchronize CM Data/Launch Element Cut Through | Configuration Options | Expand All | Collapse All'. A section titled 'Synchronize CM Data/Launch Element Cut Through' contains a table with 1 item. The table has columns: 'Element Name', 'FQDN/IP Address', 'Last Sync Time', 'Last Translation Time', 'Sync Type', 'Sync Status', 'Location', and 'Software Version'. The row for 'CommsMGR' shows a 'Sync Status' of 'Completed'. Below the table, there are three radio buttons: 'Initialize data for selected devices', 'Incremental Sync data for selected devices' (which is selected), and 'Save Translations for selected devices'. At the bottom, there are buttons for 'Now', 'Schedule', 'Cancel', and 'Launch Element Cut Through'.

Element Name	FQDN/IP Address	Last Sync Time	Last Translation Time	Sync Type	Sync Status	Location	Software Version
CommsMGR	10.10.16.47	July 26, 2011 11:06:36 AM +01:00	10:00 pm MON JUL 25, 2011	Incremental	Completed		R016x.00.1.510.1

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.

The screenshot shows the 'NETWORK' tab selected in the top navigation bar. Under 'LAN Interface 1', the 'Basic Settings' section is expanded. It contains fields for 'IP address' (10.10.16.103) and 'Netmask' (255.255.255.0). There is a 'NAT' checkbox which is unchecked. A 'Save' button is located at the bottom right of the 'Basic Settings' section. Below this, the 'DHCP Server Settings' section is collapsed.

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.

The screenshot shows the 'VIRTUAL INTERFACES' tab selected in the top navigation bar. Under 'Virtual Interfaces', the 'Configured Virtual Interfaces' section is expanded. It displays a table with the following data:

Local Interface	Number(VLAN ID)	IP address	Netmask	802.1Q VLAN	
LAN 1	1	10.10.16.104	255.255.255.0	Disabled	

Below the table is an 'Add Interface' button.


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**.

Setting	Value
Enable Call-Through Early Media	<input checked="" type="checkbox"/>
Enable Client Early Media	<input checked="" type="checkbox"/>
Enable busy sound in Wifi	<input checked="" type="checkbox"/>
Disable Inband DTMF Detection	<input checked="" type="checkbox"/>
Disable Number Converter	<input type="checkbox"/>
Enable DTMF invoked Handover	<input type="checkbox"/>
Unavailable Timeout	<input type="text"/>
DTMF Duration	<input type="text"/>
RTP payload-type for DTMF	<input type="text"/>
Disable "recommend handover" feature	<input type="checkbox"/>
Confirm SIM Switch with SMS	<input type="checkbox"/>
Force Ringing on Early Media	<input type="checkbox"/>
Use P-Asserted Identity	<input type="checkbox"/>
Activate APN	<input type="checkbox"/>
Process rinstance-tag	<input type="checkbox"/>
Number of GSM-digits to match	<input type="text" value="9"/>
Don't send P-Asserted Identity	<input type="checkbox"/>
Don't send P-Preferred Identity	<input type="checkbox"/>
Don't send Remote-Party ID	<input type="checkbox"/>

Save


7.3. Configure Numbering Profiles

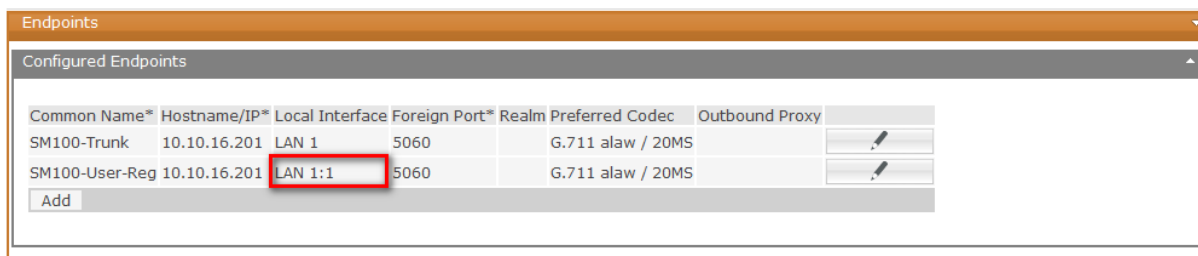
Numbering profiles are configured according to the country of implementation. Click **Telephony** → **Numbering Profiles** → **Add**, enter a **Name** to identify the locale, the international **Country Code**, the **Country Prefix** used for dialing international numbers, the local **Area Prefix**, 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.

Name*	Country Code	Country Prefix	Area Code	Area Prefix	Outgoing Prefix	Fixed Prefix	Internal Length*	Minimal Outgoing Format	
Ireland	353	00	0	9		4		Subscriber	

Add

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 **Preferred 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.




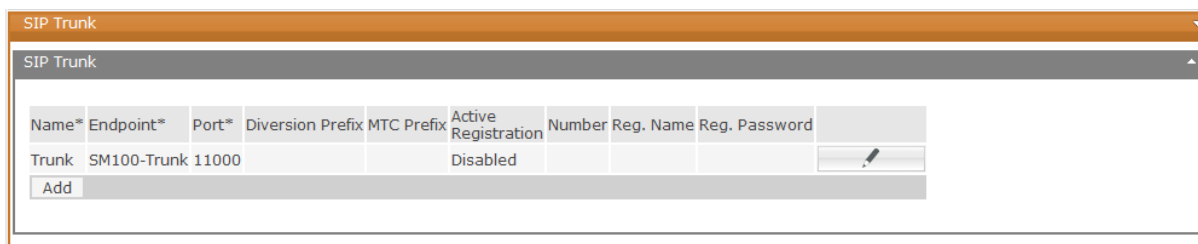
The screenshot shows the 'Endpoints' configuration window. It contains a table titled 'Configured Endpoints' with the following data:

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	

Below the table is an 'Add' button.

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.




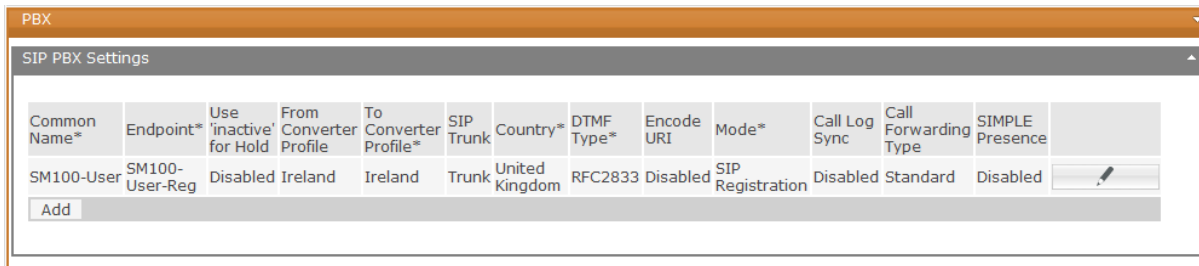
The screenshot shows the 'SIP Trunk' configuration window. It contains a table titled 'SIP Trunk' with the following data:

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


Below the table is an 'Add' button.

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.




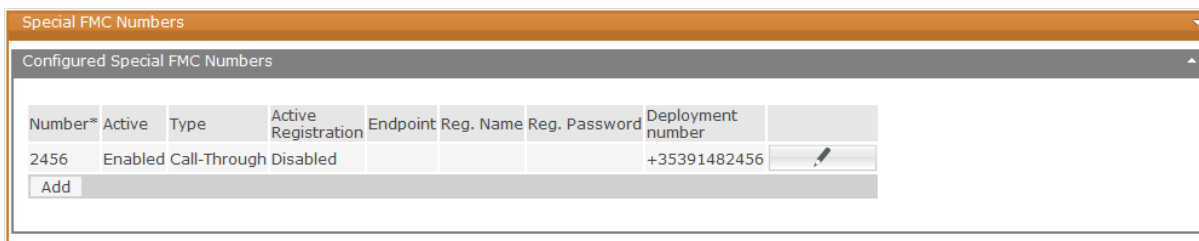
The screenshot shows the 'PBX' configuration window with the 'SIP PBX Settings' tab selected. The settings are as follows:

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	


Below the table is an 'Add' button.

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.




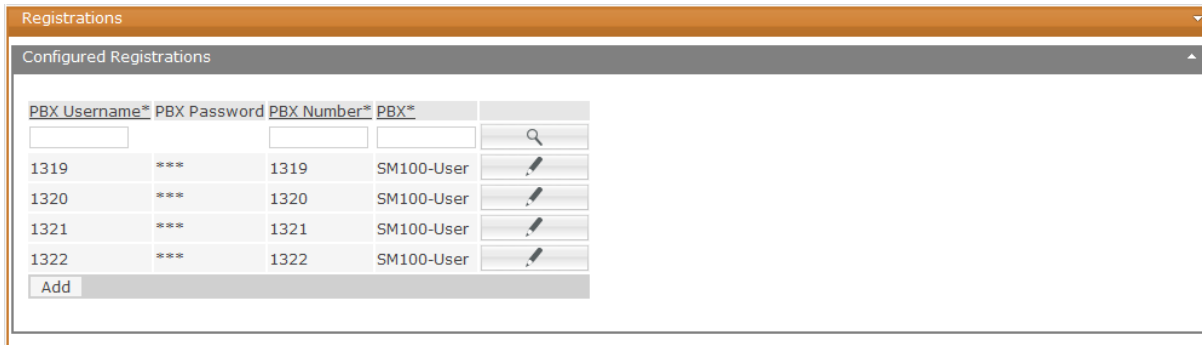
The screenshot shows the 'Special FMC Numbers' configuration window with the 'Configured Special FMC Numbers' tab selected. The settings are as follows:

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

Below the table is an 'Add' button.

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.

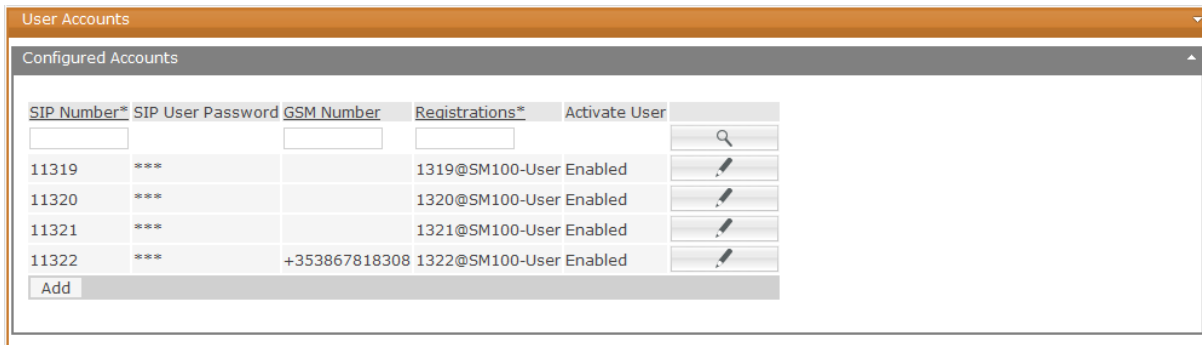


PBX Username*	PBX Password	PBX Number*	PBX*
1319	****	1319	SM100-User
1320	****	1320	SM100-User
1321	****	1321	SM100-User
1322	****	1322	SM100-User

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.

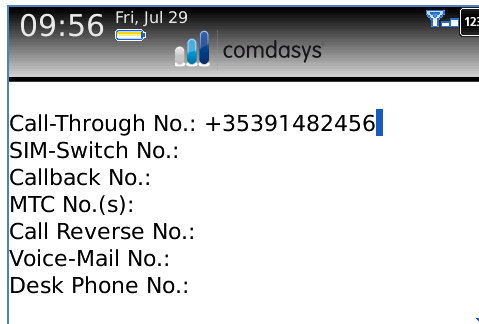


SIP Number*	SIP User Password	GSM Number	Registrations*	Activate User
11319	****		1319@SM100-User Enabled	
11320	****		1320@SM100-User Enabled	
11321	****		1321@SM100-User Enabled	
11322	****	+353867818308	1322@SM100-User Enabled	

Add

8. Configure Comdasys Mobile Convergence Client

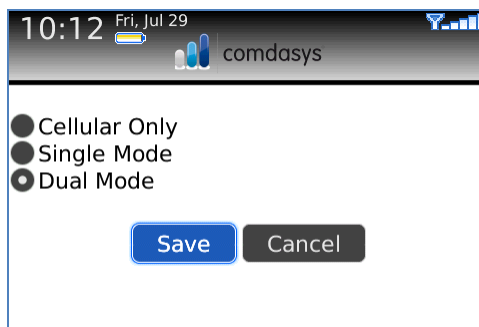
The setup of the MC Clients is not part of this document and might differ depending on the used phone platforms. However, the mandatory settings for Blackberry user, extension 11321 are described below. The **Call-Through No** must be configured in international format.



09:56 Fri, Jul 29 comdasys

Call-Through No.: +35391482456
SIM-Switch No.:
Callback No.:
MTC No.(s):
Call Reverse No.:
Voice-Mail No.:
Desk Phone No.:

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

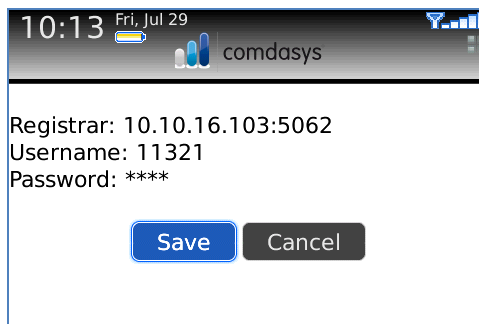


10:12 Fri, Jul 29 comdasys

☐ Cellular Only
☐ Single Mode
☒ Dual Mode

Save Cancel

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



10:13 Fri, Jul 29 comdasys

Registrar: 10.10.16.103:5062
Username: 11321
Password: ****

Save Cancel

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.

AVAYA

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Session Manager

Home

Session Manager

Dashboard

Session Manager

Administration

Communication Profile

Editor

Network Configuration

Device and Location

Configuration

Application

Configuration

System Status

SIP Entity Monitoring

Managed Bandwidth

Usage

Security Module

Status

Registration

Summary

User Registrations

SIP Performance

System Performance

System Tools

Home / Elements / Session Manager / System Status / User Registrations - User Registrations

Help ?

User Registrations

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

Customize

AST Device Notifications: Reboot Reload Fallback As of 6:14 PM

Advanced Search

6 Items Refresh Show ALL Filter: Enable

	Details	Address	Login Name	First Name	Last Name	Location	IP Address	AST Device	Registered		
									Prim	Sec	Surv
<input type="checkbox"/>	Show	1350@avaya.com	1350@avaya.com	Potter	Harry	SessionMGR	10.10.16.52:5060	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	1300@avaya.com	1300@avaya.com	Hanson	Akemi	SessionMGR	10.10.16.57:5060	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	1320@avaya.com	1320@avaya.com	iPhone	Comdasys	SessionMGR	10.10.16.104:12001	<input type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	1319@avaya.com	1319@avaya.com	Blackberry	Comdasys	SessionMGR	10.10.16.104:12000	<input type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	1321@avaya.com	1321@avaya.com	Android	Comdasys	SessionMGR	10.10.16.104:12002	<input type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	1322@avaya.com	1322@avaya.com	Nokie	Comdasys	SessionMGR	10.10.16.104:12003	<input type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>

Select : All, None

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.

SYSTEM	NETWORK	SECURITY	TELEPHONY	FEATURES	UC	DEPLOYMENT	DIAGNOSTICS
FMC Status							
Special FMC Number / Trunk Registrations							
Host:Port	Number	Status	Type				

Active Endpoint Registrations							
Host:Port	User	Status					

10.10.16.201	1321	REGED					
10.10.16.201	1320	REGED					
10.10.16.201	1322	REGED					
10.10.16.201	1319	REGED					
Registered Users							
Username	Host:Port	Reg.Mode	User-Agent				

11320	SBC	Normal	iPhone				
11321	SBC	Normal	Android				
11322	SBC	Normal	Symbian				
11319	SBC	Normal	Blackberry				
Call Status							
Host:Port	User	Status					

11322 (GSM)	4001@10.10.16.201						
11321 (VOIP)	4002@10.10.16.201						
Reload							

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/

©2011 Avaya Inc. All Rights Reserved.

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

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