



## **Avaya Solution & Interoperability Test Lab**

---

# **Configuring Avaya one-X® Mobile SIP for iOS 6.2 as a Remote User with SRTP to Avaya Session Border Controller Advanced for Enterprise 6.2 Server with Avaya Aura® Midsize Enterprise 6.2 Server & Avaya Aura® Messaging 6.2 Server – Issue 1.1**

## **Abstract**

These Application Notes describe the configuration steps required to register the Avaya one-X® Mobile SIP for IOS as a Remote User with SRTP to the Avaya Session Border Controller Advanced for Enterprise Server with Avaya Aura® Solution for Midsize Enterprise Server and Avaya Aura® Messaging Server. The Application Notes also identifies how to configure SRTP from the Avaya one-X® Mobile SIP for IOS as a Remote User to the outside interface of the Avaya Session Border Controller Advanced for Enterprise Server and configure SRTP from the inside interface of the Avaya Session Border Controller Advanced for Enterprise Server to the Avaya Aura® Solution for Midsize Enterprise Server. The Application Note also describes how to administer Avaya Aura® Messaging Server to function with SRTP with the Avaya one-X® Mobile SIP for IOS as a Remote User with the Avaya Session Border Controller Advanced for Enterprise Server.

## Table of Contents

1.	Introduction.....	4
2.	Interoperability Tests .....	4
2.1.	Test Description and Coverage .....	4
2.1.1.	Basic IP Telephony Features .....	4
2.1.2.	Supplementary Features.....	4
2.1.3.	Messaging .....	4
2.1.4.	Test Results.....	5
3.	Reference Configuration .....	6
4.	Equipment and Software Validated .....	8
5.	Administer Avaya Aura® Communication Manager Server.....	9
5.1.	Verify OPS Capacity.....	9
5.2.	Administer Dial Plan.....	10
5.3.	Administer IP Node-Name.....	10
5.4.	Administer Signaling Group .....	11
5.5.	Administer Trunk Group.....	12
5.6.	Administer Calling Party Number Information .....	12
5.7.	Administer Route Selection .....	12
5.8.	Administer IP Network Region.....	13
5.9.	Administer IP Codec Set.....	14
5.10.	Verify Off PBX Telephone Station Mapping.....	14
5.11.	Administer Hunt Group.....	15
5.12.	Administer Coverage Path.....	16
5.13.	Administer Station Screen .....	17
5.14.	Administer SRTP on Communication Manager.....	18
5.15.	Save Translations.....	19
6.	Administer Avaya Aura® Session Manager.....	20
6.1.	Access Avaya Aura® System Manager .....	20
6.2.	Administer SIP Domain .....	21
6.3.	Administer Location.....	22
6.4.	Administer Avaya Aura® Session Manager SIP Entity .....	23
6.5.	Administer Avaya Aura® Communication Manager Server SIP Entity .....	24
6.6.	Administer Avaya Aura® Messaging SIP Entity .....	25
6.7.	Administer SIP Entity Link.....	25
6.8.	Administer Regular Expression .....	27
6.9.	Administer Routing Policy.....	28
6.10.	Administer Avaya Aura® Communication Manager as a Managed Element .....	29
6.11.	Administer Avaya Aura® Communication Manager Server Application .....	31
6.12.	Administer Avaya Aura® Communication Manager Server Application Sequence ..	32
6.13.	Synchronize Avaya Aura® Communication Manager Data .....	34
6.14.	Administer SIP User .....	35
7.	Administer Avaya Aura® Messaging Server .....	39
7.1.	Access Avaya Aura® Messaging.....	39

7.2.	Administer Telephony Integration with SRTP.....	39
7.3.	Administer Subscriber.....	41
8.	Administer Avaya Session Border Controller Advanced for Enterprise .....	43
8.1.	Access Avaya Session Border Controller Advanced for Enterprise .....	43
8.2.	Enable Interfaces on the Avaya Session Border Controller Advanced for Enterprise...	45
8.3.	Administer User Agent.....	45
8.4.	Administer Server Interworking.....	46
8.5.	Administer Phone Interworking .....	47
8.6.	Verify TLS Client Profile.....	48
8.7.	Verify TLS Server Profile .....	49
8.8.	Administer Topology Hiding for Subscriber and Server Flow .....	49
8.9.	Administer Session Manager Server Configuration.....	50
8.10.	Administer External Signaling Interface Toward Remote User.....	52
8.11.	Administer Internal Signaling Interface toward Session Manager.....	53
8.12.	Administer External Media Interface Toward Remote User.....	53
8.13.	Administer Internal Media Interface Toward Session Manager .....	54
8.14.	Administer SIP Cluster .....	55
8.15.	Administer Routing Profile Toward Session Manager for Subscriber Flow.....	58
8.16.	Administer SRTP Media Rule for the End Point Policy Group for Subscriber Flow and Server Flow .....	60
8.17.	Administer End Point Policy Group for Subscriber Flow and Server Flow .....	62
8.18.	Administer End Point Flow with Subscriber Flow .....	63
8.19.	Administer Routing Profile Toward Remote User for Server Flow .....	66
8.20.	Administer End Point Flow with Server Flow .....	66
9.	Administer Avaya one-X® Mobile SIP for IOS.....	68
9.1.	Access Wireless Network.....	68
9.2.	Administering Avaya one-X® Mobile SIP Communicator for iOS .....	69
10.	Verification Steps.....	72
11.	Conclusion .....	75
12.	Additional References.....	76

# 1. Introduction

These Application Notes describe the configuration steps required to register the Avaya one-X® Mobile SIP for IOS 6.2.2.702 as a Remote User with SRTP to the Avaya Session Border Controller Advanced for Enterprise Server 6.2.0.Q40 with Avaya Aura® Solution for Midsize Enterprise Server 6.2 and Avaya Aura® Messaging Server 6.2. These Application Notes also identify how to configure SRTP from the Avaya one-X® Mobile SIP for IOS as a Remote User to the outside interface of the Avaya Session Border Controller Advanced for Enterprise Server and configure SRTP from the inside interface of the Avaya Session Border Controller Advanced for Enterprise Server to the Avaya Aura® Solution for Midsize Enterprise Server and Avaya Aura® Messaging Server. These Application Note also describe how to administer Avaya Aura® Messaging Server to function with SRTP with the Avaya one-X® Mobile SIP for IOS as a Remote User with the Avaya Session Border Controller Advanced for Enterprise Server.

## 2. Interoperability Tests

The following sections describe the test scenario used to verify the functionality of the Avaya one-X Mobile SIP for IOS with SRTP as a Remote User with SRTP with the Avaya Session Border Controller Advanced for Enterprise Server.

### 2.1. Test Description and Coverage

This section provides an overview of the test cases performed after the installation and configuration of the Avaya one-X Mobile SIP for IOS as a Remote User with SRTP with the Avaya Session Border Controller Advanced for Enterprise Server.

#### 2.1.1. Basic IP Telephony Features

The following Basic IP Telephony Features were tested:

- Basic Calls
- Codec Negotiation
- Direct IP-IP Media Shuffling
- PPM Download
- Hold
- Drop

#### 2.1.2. Supplementary Features

The following Supplementary Features were tested:

- Call Forwarding
- Bridged Call Appearance
- Call Pickup with FAC
- TLS

#### 2.1.3. Messaging

Following Messaging Features were verified for Remote Users with SRTP with Avaya Aura® Messaging 6.2 SP1

- Login and access to mailbox
- Leave/Retrieve Voice Mail Messages with proper MWI operation
- Call Sender
- Reply
- Forward Message

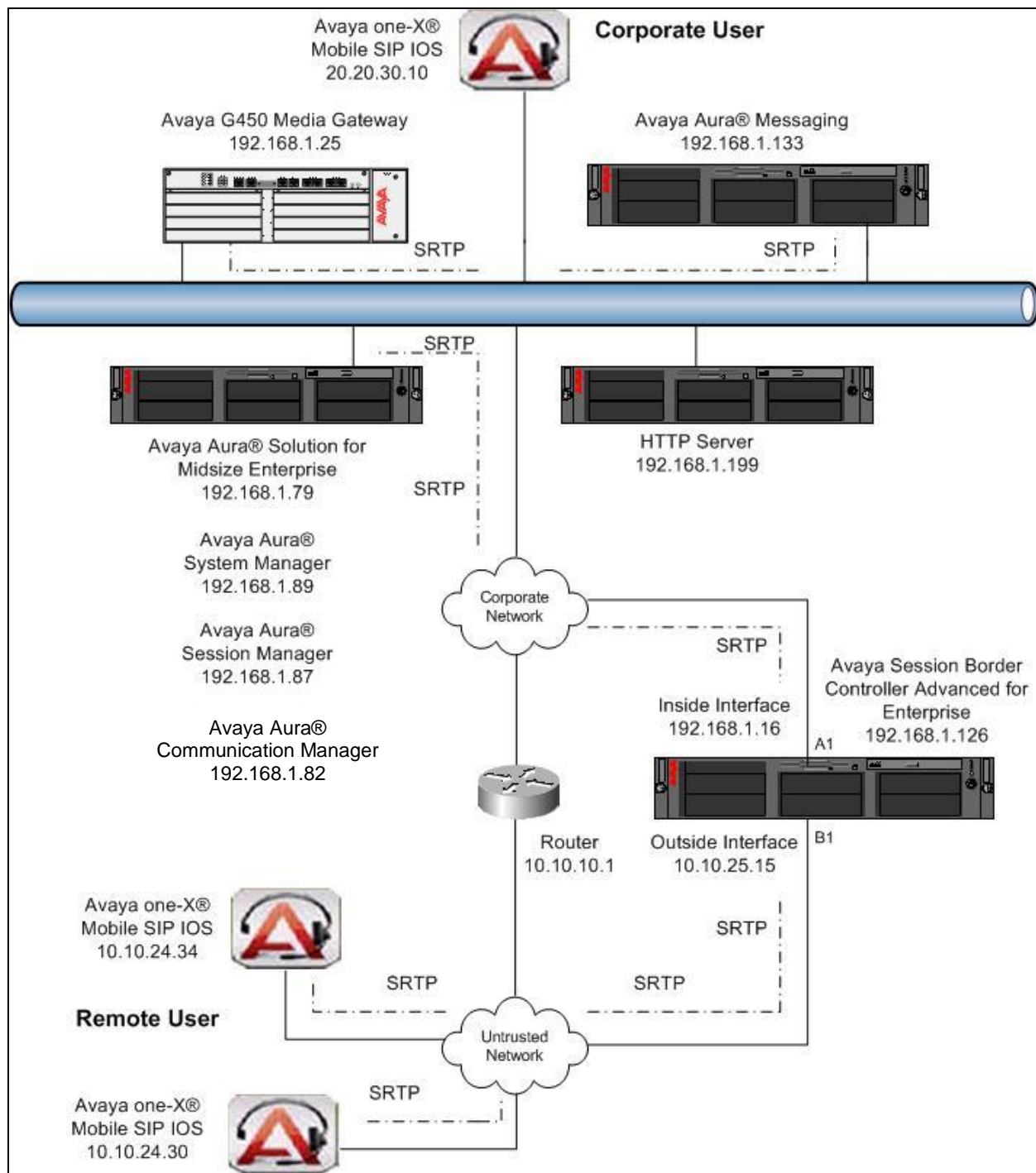
#### **2.1.4. Test Results**

All test cases passed. The following are the observations for the Avaya one-X Mobile SIP for IOS as a Remote User with SRTP registered to the Avaya Session Border Controller Advanced for Enterprise Server:

- Avaya one-X Mobile SIP for IOS as Remote User registered to the Avaya Session Border Controller Advanced for Enterprise Server uses SRTP for secure encryption of the audio.
- Avaya one-X Mobile SIP for IOS as Remote User registered to the Avaya Session Border Controller Advanced for Enterprise Server has added security as all communication uses TLS.
- The Avaya Session Border Controller Advanced for Enterprise Server is supported as an alternative to VPN in an untrusted network. The Avaya one-X Mobile SIP for IOS connects to Session Manager Server through the Avaya Session Border Controller Advanced for Enterprise Server thus making communication secure.

### 3. Reference Configuration

The configuration used in these Application Notes is shown in **Figure 1**. The Avaya Aura® Solution for Midsize Enterprise is installed on Avaya System Platform on a S8800 Server. Avaya Aura® Solution for Midsize Enterprise contains Avaya Aura® System Manager, Avaya Aura® Session Manager and Avaya Aura® Communication Manager as virtual machines running with the Avaya Aura® Solution for Midsize Enterprise. Avaya Aura® Communication Manager running as an Evolution Server is used for Off-PBX Station Mapping (OPS). Avaya Aura® Messaging is a template installed on Avaya System Platform on an S8800 Server. The Avaya Session Border Controller Advanced for Enterprise software is installed and configured on Red Hat Linux 5.6 Operating System on an S8800 Server. The diagram indicates logical signaling connections. All components in the Corporate LAN are physically connected to a single Avaya Ethernet Routing Switch (ERS) 2550T-PWR, and are administered in subnet range 192.168.1.x. The Avaya one-X Mobile SIP for IOS Application was obtained from the iTunes App Store and installed on an Apple iPhone 4S. The Avaya one-X Mobile SIP for IOS with SRTP as a Remote User registers to the B1 external interface of the Avaya Session Border Controller Advanced for Enterprise Server.



**Figure 1 Avaya one-X Mobile SIP for IOS Remote User**

## 4. Equipment and Software Validated

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

Avaya Aura®	Software
Avaya S8800 Server	Avaya Aura® Solution for Midsize Enterprise R6.2 Release 6.2.0.0.3105 Update: Service Pack 4
	Avaya Aura® System Manager R6.2 Release 6.2.16.1.1993 Update: Service Pack 4
	Avaya Aura® Session Manager R6.2 R6.2.4.0.624005 Update: Service Pack 4
	Avaya Aura® Communication Manager R16x.02.0.823.0.20199 Update: Service Pack 4
Avaya G450 Media Gateway	Avaya G450 Media Gateway Release 32.24.0
Avaya S8800 Server	Avaya Aura® Messaging R6.2 MSG 02.0.823.0-109_0102 Update: Service Pack 1
Avaya S8800 Server	Avaya Session Border Controller Advanced for Enterprise Release 6.2.0.Q40
Avaya one-X Mobile SIP iOS	Avaya one-X Mobile SIP iOS R6.2 App Release 6.2.2.702



## 5. Administer Avaya Aura® Communication Manager Server

This section highlights the important commands for defining the Avaya one-X Mobile SIP for IOS as a Remote User as an Off-PBX Station (OPS) and administering a SIP Trunk and Signaling Group to carry calls between the Avaya one-X Mobile SIP for IOS as a Remote User and the SIP endpoints registered to Session Manager on the Corporate LAN in Communication Manager Server. This section will also explain how to administer SRTP on Communication Manager so that SRTP can be used from the inside interface on the Session Border Controller Server to the Communication Manager Server on the Corporate LAN.

### 5.1. Verify OPS Capacity

Use the **display system-parameters customer-options** command to verify that **Maximum Off-PBX Telephones – OPS** has been set to the value that has been licensed, and that this value will accommodate addition of the SIP telephones. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to obtain additional capacity.

display system-parameters customer-options		Page 1 of 11
OPTIONAL FEATURES		
G3 Version: V15	Software Package: Standard	
Location: 2	RFA System ID (SID): 1	
Platform: 25	RFA Module ID (MID): 1	
		USED
Platform Maximum Ports:	44000	181
Maximum Stations:	2400	9
Maximum XMOBILE Stations:	2400	0
Maximum Off-PBX Telephones - EC500:	2400	2
<b>Maximum Off-PBX Telephones - OPS:</b>	<b>2400</b>	<b>5</b>
Maximum Off-PBX Telephones - PBFMC:	2400	2
Maximum Off-PBX Telephones - PVFMC:	2400	0

Verify that there are sufficient licenses to administer the SIP Trunk. This is the **Maximum Administered SIP Trunk** value on **Page 2** of System Parameter Customer-Options.

display system-parameters customer-options		Page 2 of 11
OPTIONAL FEATURES		
IP PORT CAPACITIES		USED
Maximum Administered H.323 Trunks:	8000	12
Maximum Concurrently Registered IP Stations:	18000	3
Maximum Administered Remote Office Trunks:	8000	0
Maximum Concurrently Registered Remote Office Stations:	18000	0
Maximum Concurrently Registered IP eCons:	128	0
Max Concur Registered Unauthenticated H.323 Stations:	100	0
Maximum Video Capable Stations:	2400	0
Maximum Video Capable IP Softphones:	100	3
<b>Maximum Administered SIP Trunks:</b>	<b>5000</b>	<b>160</b>
Maximum Administered Ad-hoc Video Conferencing Ports:	8000	0
Maximum Number of DS1 Boards with Echo Cancellation:	522	0

## 5.2. Administer Dial Plan

This section describes the **Dial Plan Analysis** screen. This is Communication Manager's way of translating digits dialed by the user. The user can determine the beginning digits and total length for each type of call that Communication Manager needs to interpret. The **Dialed String** beginning with the number **4** and with a **Total Length** of **5** digits will be used to administer the **extension** range used for the one-X Mobile SIP for IOS device.

```
display dialplan analysis
```

DIAL PLAN ANALYSIS TABLE								
Location: all			Percent Full: 1					
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
1	3	dac						
2	5	aar						
3	5	ext						
35	5	aar						
<b>4</b>	<b>5</b>	<b>ext</b>						
60	4	aar						
7	5	aar						
8	6	aar						
*	2	fac						

## 5.3. Administer IP Node-Name

This section describes **IP Node-Name**. This is where Communication Manager assigns the IP Address and node-name to Session Manager. The node-name is **SM** and the IP Address is **192.168.1.87** within Communication Manager Server. The Communication Manager Server automatically populates a processor node name to the IP Address of Communication Manager Server. This node name is **procr** with IP Address **192.168.1.82**.

```
list node-names all
```

NODE NAMES		
Type	Name	IP Address
IP	EnterpriseCM	192.168.1.6
<b>IP</b>	<b>SM</b>	<b>192.168.1.87</b>
IP	SessionM2	192.168.1.60
<b>IP</b>	<b>BSM</b>	<b>192.168.1.157</b>
IP	default	0.0.0.0
<b>IP</b>	<b>procr</b>	<b>192.168.1.82</b>

## 5.4. Administer Signaling Group

This section describes the **Signaling Group** screen. The **Group Type** was set to **sip** and the **Transport Method** was set to **tls**. Since the Avaya one-X Mobile SIP for IOS as a Remote User is using a Communication Manager Evolution Server for Off Pbx Station Mapping the **IMS Enabled** setting must be set to **n**. Since the SIP trunk is between Communication Manager Evolution Server and Session Manager the **Near-end Node Name** is the node name of the “procr” of the Communication Manager Server. The **Far-end Node Name** is the node name of the Session Manager Server. This is **SM**. The **Near-end Listen Port** and **Far-end Listen Port** are both set to port number **5061**. The **Far-end Network-Region** was set to **1**.

```
display signaling-group 120

SIGNALING GROUP

Group Number: 120          Group Type: sip
IMS Enabled? n            Transport Method: tls
    Q-SIP? n
    IP Video? y            Priority Video? n        Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y  Peer Server: SM

Near-end Node Name: procr      Far-end Node Name: SM
Near-end Listen Port: 5061     Far-end Listen Port: 5061
Far-end Network Region: 1

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? n                    IP Audio Hairpinning? n
H.323 Station Outgoing Direct Media? n    Initial IP-IP Direct Media? y
                                           Alternate Route Timer(sec): 6
```

## 5.5. Administer Trunk Group

This section describes the **Trunk Group** used to carry calls between the Avaya one-X Mobile SIP IOS as a Remote User. Trunk Group 120 was configured as a SIP Trunk with the **Group Type** set as **sip**. The trunk **Group Name** was set to **To SM**. The **Direction** of the calls was set to **two-way** as there will be calls to and from the Remote SIP Users registered to the Avaya Session Border Controller. The **Service Type** was set to **tie** as the trunk is an internal trunk between Communication Manager Evolution Server and Session Manager. The **Signaling Group** number assigned to this trunk is **120**. The **Number of Members** assigned to this trunk group is **100**. All other fields on this page are left as default.

display trunk-group 120			Page 1 of 21		
TRUNK GROUP					
Group Number: 120		Group Type: sip		CDR Reports: y	
Group Name: To SM		COR: 1		TN: 1	
Direction: two-way		Outgoing Display? n		TAC: 120	
Dial Access? n				Night Service:	
Queue Length: 0					
Service Type: tie		Auth Code? N			
		Member Assignment Method: auto			
		Signaling Group: 120			
		Number of Members: 100			

## 5.6. Administer Calling Party Number Information

Use the **change private-numbering 0** to add an **Extension Length** of **5** with **Extension code** of **4**. The **Total Length** of the CPN number was **5**. The **change private-numbering 0** command was also used to add an **Extension Code** of **8** for the Messaging hunt group number.

change private-numbering 0				Page 1 of 2	
NUMBERING - PRIVATE FORMAT					
Ext	Ext	Trk	Private	Total	
Len	Code	Grp(s)	Prefix	Len	
5	4			5	Total Administered: 2
5	8			5	

## 5.7. Administer Route Selection

Use the **change aar a 5** to administer the automatic alternate route selection to route calls between via the SIP trunk to Session Manager. Calls to the number beginning with **5** that are a **minimum** of **5** digits and a **maximum** of **5** digits in length are sent to routing pattern 120. The **Call Type** was set to **unku**.

change aar analysis 4						Page 1 of 2	
AAR DIGIT ANALYSIS TABLE							
Location: all						Percent Full: 1	
	Dialed	Total		Route	Call	Node	ANI
	String	Min	Max	Pattern	Type	Num	Reqd
4		5	5	120	unku		n

Use the **change route-pattern 120** to add **trunk group 120** to route pattern 120. Ensure the **Secure SIP** value was set to **No**.

change route-pattern 120										Page	1 of	3	
Pattern Number: 120 Pattern Name:													
SCCAN? n Secure SIP? n													
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted			DCS/	IXC		
No			Mrk	Lmt	List	Del	Digits			QSIG			
										Intw			
1:	120	0								n	user		
2:										n	user		

## 5.8. Administer IP Network Region

This section describes **IP Network Region** screen. It was decided to place the Avaya one-X Mobile SIP for iOS as a Remote User in network region 1. The **Authoritative Domain** must mirror the domain name of Session Manager. This was **silstack.com**. The codec used on the SIP endpoints were placed in **Codec Set 1**. IP Shuffling was turned on so both **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** were set to **yes**.

<b>display ip-network-region 1</b>										Page	1 of	19
IP NETWORK REGION												
Region: 1												
Location: 1 <b>Authoritative Domain: silstack.com</b>												
Name:												
MEDIA PARAMETERS										<b>Intra-region IP-IP Direct Audio: yes</b>		
<b>Codec Set: 1</b>										<b>Inter-region IP-IP Direct Audio: yes</b>		
UDP Port Min: 2048										IP Audio Hairpinning? n		
UDP Port Max: 3329												
DIFFSERV/TOS PARAMETERS										RTCP Reporting Enabled? y		
Call Control PHB Value: 46										RTCP MONITOR SERVER PARAMETERS		
Audio PHB Value: 46										Use Default Server Parameters? y		
Video PHB Value: 26												
802.1P/Q PARAMETERS												
Call Control 802.1p Priority: 6												
Audio 802.1p Priority: 6												
Video 802.1p Priority: 5										AUDIO RESOURCE RESERVATION PARAMETERS		
H.323 IP ENDPOINTS										RSVP Enabled? n		
H.323 Link Bounce Recovery? y												
Idle Traffic Interval (sec): 20												
Keep-Alive Interval (sec): 5												

## 5.9. Administer IP Codec Set

This section describes the **IP Codec Set** screen. IP Codec **G.711MU**, **G.711A** and **G.729** were used for testing purposes with the Remote User SIP endpoints.

display ip-codec-set 1				Page	1 of	2
IP Codec Set						
Codec Set: 1						
Audio	Silence	Frames	Packet			
Codec	Suppression	Per Pkt	Size (ms)			
1: <b>G.711MU</b>	n	2	20			
2: <b>G.711A</b>	n	2	20			
3: <b>G.729</b>	n	2	20			

## 5.10. Verify Off PBX Telephone Station Mapping

This section show the **off-pbx-telephone station-mapping**. The Avaya one-X Mobile SIP for IOS as a Remote User extension **40040** uses off pbx **Application OPS** which is used for SIP enabled telephones. This information is populated in Communication Manager when the Avaya one-X Mobile SIP for IOS as a Remote User is administered in User Management in System Manager. The **SIP Trunk Selection** is set to **aar**. The **Config Set** which is the desired call treatment was set to **1**.

display off-pbx-telephone station-mapping 53177								Page	1 of	3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION										
Station	Appl	CC	Phone Number	Config	Trunk	Mapping	Calls			
Extension				Set	Select	Mode	Allowed			
<b>40040</b>	OPS		40040	<b>1</b>	<b>/ aar</b>	both	all			
40050	OPS		40050	1	/ aar	both	all			
40060	OPS		40060	1	/ aar	both	all			

The **Call Limit** is set to **6** as shown below. This is the maximum amount of simultaneous calls for extension 40040. The **Mapping Mode** field was set to **both** in this configuration setup. This is used to control the degree of integration between the Remote User SIP telephones. The **Calls Allowed** field was set to **all**. This identifies the call filter type for a SIP Phone. The **Bridged Calls** field was set to **none** as it was not needed for testing purposes.

display off-pbx-telephone station-mapping 53177							Page	2 of	3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION									
Station	Appl	Call	Mapping	Calls	Bridged	Location			
Extension	Name	Limit	Mode	Allowed	Calls				
<b>40040</b>	OPS	<b>6</b>	<b>both</b>	<b>all</b>	<b>none</b>				
40050	OPS	4	both	all	both				

## 5.11. Administer Hunt Group

**Hunt Group number 1** was administered and was assigned **Group Name Mango**. **Group Extension 80960** was assigned to hunt group 1. **ucd-mia** was assigned as the **Group Type**.

display hunt-group 1		Page 1 of 60
HUNT GROUP		
Group Number: 1	ACD? n	
Group Name: <b>Mango</b>	Queue? n	
Group Extension: <b>80960</b>	Vector? n	
Group Type: <b>ucd-mia</b>	Coverage Path: 1	
TN: 1	Night Service Destination:	
COR: 1	MM Early Answer? n	
Security Code:	Local Agent Preference? n	
ISDN/SIP Caller Display: mbr-name		

Select **sip-adjunct** for **Message Center**. The **Voice Mail Handle** was set to 80960 the same value as the **Group Extension** on Page 1. The **Voice Mail Handle** was set to **80960**. The **Routing Digits \*08** is used in the **Voice Mail Number** field as a Feature Access Code to access the SIP trunk the hunt group number goes out across.

display hunt-group 1		Page 2 of 60
HUNT GROUP		
Message Center: sip-adjunct		
Voice Mail Number	Voice Mail Handle	Routing Digits
		(e.g., AAR/ARS Access Code)
80960	80960	*08

## 5.12. Administer Coverage Path

Configure a coverage path for the Message Application Subscriber. Use the command **add coverage path n** where **n** is the coverage path number to be assigned. Configure a coverage point, using value **hx** where **x** is the hunt group number defined in **Section 5.11**. In this case its hunt-group 1 or **h1** as shown below.

```
add coverage path n

                                COVERAGE PATH

                                Coverage Path Number: 3
                                Cvg Enabled for VDN Route-To Party? n
                                Next Path Number:
                                Hunt after Coverage? n
                                Linkage

COVERAGE CRITERIA

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

COVERAGE POINTS
    Terminate to Coverage Pts. with Bridged Appearances? n
    Point1: h1              Rng:    Point2:
    Point3:                 Point4:
    Point5:                 Point6:
```



### 5.13. Administer Station Screen

This screen describes the **station** form setup for the Avaya one-X Mobile SIP IOS as a Remote User on Communication Manager. This information is populated on Communication Manager when user 40040 is administered in User Management in System Manager in **Section 6.14** The **Extension** used was **40040** with phone **Type 9640SIP**. **Coverage Path 1** was set to **1** as described in **Section 5.12**. The **Name** of the phone was set to **40040, 40040** and all other values on **Page 1** of the station form were left as default.

display station 40040		Page 1 of 5
STATION		
Extension: 40040	Lock Messages? n	BCC: 0
Type: 9640SIP	Security Code:	TN: 1
Port: S00010	Coverage Path 1: 1	COR: 1
Name: 40040,40040	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
	Time of Day Lock Table:	
Loss Group: 19	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 40040	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english	Expansion Module? n	
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? n	
	IP Video? n	

The **SIP Trunk** value was set to **aar** on **Page 6** of the station form.

add station 40040		Page 6 of 6
STATION		
SIP FEATURE OPTIONS		
Type of 3PCC Enabled: None		
SIP Trunk: aar		

## 5.14. Administer SRTP on Communication Manager

It was decided that SRTP would be administered from the inside interface of the Session Border controller to the Communication Manager Server. There are a number of settings on Communication Manager that need to be set in order for SRTP to function correctly. The **change system-parameters customer-option** command was used to set the **set media encryption over IP** setting on **Page 4** to **YES**.

change system-parameters customer-options		Page	4	of	11
OPTIONAL FEATURES					
Emergency Access to Attendant? y	IP Stations? y				
Enable 'dadmin' Login? y					
Enhanced Conferencing? y	ISDN Feature Plus? n				
Enhanced EC500? y	ISDN/SIP Network Call Redirection? y				
Enterprise Survivable Server? n	ISDN-BRI Trunks? y				
Enterprise Wide Licensing? n	ISDN-PRI? y				
ESS Administration? y	Local Survivable Processor? n				
Extended Cvg/Fwd Admin? y	Malicious Call Trace? y				
External Device Alarm Admin? y	<b>Media Encryption Over IP? y</b>				
Five Port Networks Max Per MCC? n	Mode Code for Centralized Voice Mail? n				
Flexible Billing? n					

The **change system-parameters ip-options** command was used to set the **Override ip-codec-set for SIP direct-media connections** setting on **Page 4** to **NO**.

change system-parameters ip-options		Page	4	of	4
IP-OPTIONS SYSTEM PARAMETERS					
SYSLOG FROM TN BOARDS					
Local Facility #: local4					
Dest #1 IP address: Port #: 514					
Dest #2 IP address: Port #: 514					
Dest #3 IP address: Port #: 514					
Override ip-codec-set for SIP direct-media connections? n					

The **change system-parameters features** command was used to set the **SDP Capability Negotiation for SRTP** setting on **Page 19** to **YES**.

change system-parameters features		Page	19	of	19
FEATURE-RELATED SYSTEM PARAMETERS					
IP PARAMETERS					
Direct IP-IP Audio Connections? y					
IP Audio Hairpinning? n					
Synchronization over IP? n					
<b>SDP Capability Negotiation for SRTP? y</b>					
SIP Endpoint Managed Transfer? y					

The **change ip-codec 1** command was used to set the **Media Encryption** setting on **Page 1** of the ip-codec setting to **1-srtp-aescm128-hmac80**.

change ip-codec-set 1

Page 1 of 2

IP Codec Set

Codec Set: 1

Audio	Silence	Frames	Packet
Codec	Suppression	Per Pkt	Size (ms)
1: G.711MU	n	2	20
2: G.711A	n	2	20
3: G.729	n	2	20
4:			
5:			
6:			
7:			

Media Encryption

1: 1-srtp-aescm128-hmac80

2:

3:

## 5.15. Save Translations

Use the **save translation** command to save these changes.

save translation	
SAVE TRANSLATION	
Command Completion Status	Error Code
Success	0

## 6. Administer Avaya Aura® Session Manager

The following steps describe configuration of the Avaya one-X Mobile SIP for IOS as a Remote User with Session Manager. This section describes administering SIP Entities between Session Manager and the Communication Manager Server in order to establish a SIP Entity link between Session Manager and the Communication Manager Server. It also discusses administering the SIP Entities between Session Manager and the Messaging Server. Administering the Avaya one-X Mobile SIP for IOS as a Remote User in User Management to register to the Avaya Session Border Controller Advanced Enterprise Server with Session Manager is also discussed.

### 6.1. Access Avaya Aura® System Manager

Access the System Manager web interface, by entering **http://<ip-addr>/SMGR** as the URL in an Internet browser, where *<ip-addr>* is the IP address of the server running System Manager graphical user interface. Log in with the appropriate **User ID** and **Password** and press the **Log On** button to access System Manager.

**AVAYA** Avaya Aura® System Manager 6.2

Home / Log On

**Log On**

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

User ID: admin

Password: [masked]

Log On Cancel

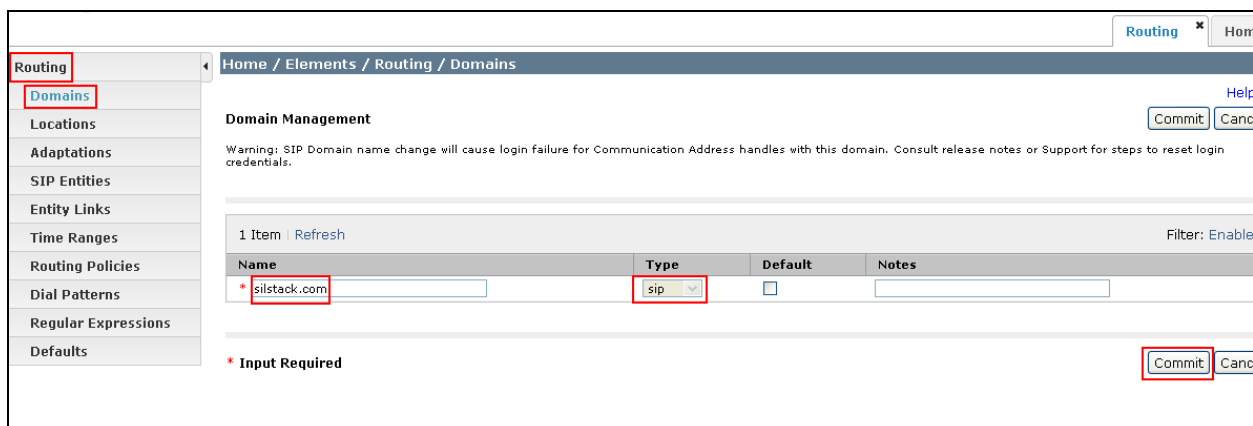
[Change Password](#)

The **main menu** of the **System Manager Graphical User Interface** is displayed in the following screenshot.



## 6.2. Administer SIP Domain

The following screenshot shows the configuration used to add a **SIP Domain**. Under the heading **Routing** on the left hand side of the system management interface of System Manager, access the sub heading **Domains**. The name of the SIP Domain used in Session Manager **silstack.com** was added. The Type was set to **sip**. Press the **Commit** button to add the SIP Domain.



### 6.3. Administer Location

To add a new Location, click on **Routing** and access the **Locations** sub heading. A location **Name Galway Stack** was added to the Session Manager. The **Default Audio Bandwidth** was set to **80Kbit/sec**. The **Commit** button was pressed to confirm changes. Locations are used to identify logical and physical locations where SIP entities reside for the purposes of bandwidth management or location based routing.

Home / Elements / Routing / Locations

**Location Details**

Call Admission Control has been set to ignore SDR. All calls will be counted using the Default Audio Bandwidth. Note: If this setting is disabled, you should return to this form to review settings for multimedia bandwidth. See Session Manager -> Session Manager Administration -> Global Settings

**General**

\* Name: Galway Stack

Notes:

**Overall Managed Bandwidth**

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

**Per-Call Bandwidth Parameters**

\* Default Audio Bandwidth: 80 Kbit/sec

Commit Cancel

User **Location Pattern** an IP Address Pattern for **192.168.1.x** was added. The **Commit** button was pressed to add the IP Address Pattern to the Location.

**Location Pattern**

Add Remove

3 Items | Refresh Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.10.99.*	
<input type="checkbox"/>	* 10.10.97.*	
<input type="checkbox"/>	* 192.168.1.*	

Select : All, None

\* Input Required

Commit Cancel

## 6.4. Administer Avaya Aura® Session Manager SIP Entity

This application note assumes that the basic installation steps for integrating Session Manager with System Manager have already been completed. The screenshot below shows what the completed Session Manager administration looks like in System Manager.

The screenshot shows the 'SIP Entity Details' page in System Manager. The left sidebar has a menu with 'Routing' selected. The main content area is titled 'SIP Entity Details' and has a 'Commit' button in the top right. The 'General' tab is active, showing fields for 'Name' (MESSM), 'FQDN or IP Address' (192.168.1.87), 'Type' (Session Manager), 'Location' (Galway Stack), 'Time Zone' (Europe/Dublin), and 'SIP Link Monitoring' (Use Session Manager Configuration). The 'Outbound Proxy' field is empty. The 'Credential name' field is also empty.

Routing

Home / Elements / Routing / SIP Entities

SIP Entity Details

Commit

General

\* Name: MESSM

\* FQDN or IP Address: 192.168.1.87

Type: Session Manager

Notes:

Location: Galway Stack

Outbound Proxy:

Time Zone: Europe/Dublin

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

The following screenshot shows what **Port** settings need to be configured for the SIP Entity. With the signaling protocol being set to **TLS** port **5061** was used in the SIP Entity SIP trunk. Press the **Commit** button.

The screenshot shows the 'Port' configuration page in System Manager. The 'Port' tab is selected. There are fields for 'TCP Failover port' and 'TLS Failover port', both empty. Below these are 'Add' and 'Remove' buttons. A table shows 3 items with columns: Port, Protocol, Default Domain, and Notes. The table has three rows: 5060 (TCP), 5060 (UDP), and 5061 (TLS). The 5061 row is highlighted. Below the table is a 'Select' dropdown set to 'All, None'. There is a section for 'SIP Responses to an OPTIONS Request' with 'Add' and 'Remove' buttons. Below this is another table with 0 items, columns: Response Code & Reason Phrase, Mark Entity Up/Down, and Notes. At the bottom, there is a '\* Input Required' message and 'Commit' and 'Cancel' buttons.

Port

TCP Failover port:

TLS Failover port:

Add Remove

3 Items | Refresh Filter: Enable

	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	TCP	silstack.com	
<input type="checkbox"/>	5060	UDP	silstack.com	
<input type="checkbox"/>	5061	TLS	silstack.com	

Select : All, None

SIP Responses to an OPTIONS Request

Add Remove

0 Items | Refresh Filter: Enable

	Response Code & Reason Phrase	Mark Entity Up/Down	Notes
--	-------------------------------	---------------------	-------

\* Input Required

Commit Cancel

## 6.5. Administer Avaya Aura® Communication Manager Server SIP Entity

The Communication Server SIP Entity is the second part of the link between the Session Manager and the Communication Manager Server. The **Name** of the SIP Entity was **MESCM**. The **FQDN or IP Address** was set to **192.168.1.82** which was the IP Address of the Communication Manager Server. The **Type** was set to **CM** for Communication Manager. The Location was set to **Galway Stack** and the **SIP Link Monitoring** was set to **Use Session Manager Configuration**. Press the **Commit** button.

Home / Elements / Routing / SIP Entities

**SIP Entity Details**

**General**

\* Name: MESCM

\* FQDN or IP Address: 192.168.1.82

Type: CM

Notes:

Adaptation:

Location: Galway Stack

Time Zone: Europe/Dublin

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: none

**SIP Link Monitoring**

SIP Link Monitoring: Use Session Manager Configuration

Commit



## 6.6. Administer Avaya Aura® Messaging SIP Entity

The following describes the Messaging SIP Entity to the Session Manager. The **Name** of the SIP Entity was **MANGO**. The **FQDN or IP Address** was set to **192.168.1.133** which was the IP Address of the Messaging Server. The **Type** was set to **Modular Messaging** for Messaging. The Location was set to **Galway Stack** and the **SIP Link Monitoring** was set to **Use Session Manager Configuration**. Press the **Commit** button.

Home / Elements / Routing / SIP Entities

**SIP Entity Details**

**General**

\* Name: MANGO

\* FQDN or IP Address: 192.168.1.133

Type: Modular Messaging

Notes:

Adaptation:

Location: Galway Stack

Time Zone: Europe/Dublin

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: none

**SIP Link Monitoring**

SIP Link Monitoring: Use Session Manager Configuration

Commit

## 6.7. Administer SIP Entity Link

To administer the SIP Entity link access the sub heading **Routing → Entity Links** on the left hand side of the Session Manager GUI. Select the **New** button.

Home / Elements / Routing / Entity Links

**Entity Links**

Edit New Duplicate Delete More Actions

26 Items | Refresh

The SIP Entity Link shown below is the link between Session Manager and the Communication Manager Server. The Name of the **Entity Link** was **SMONE-MESCM**. The **SIP Entity 1** was set to **Session Manager One**. The **Protocol** was **TLS** and the **Port** was **5061**. The **SIP Entity 2** was set to **MESCM**.

Entity Links
Commit

1 Item | Refresh
Filter: E

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port
* SMONE-MESCM	* Session Manager One	TLS	* 5061	* MESCM	* 5061

The SIP Entity Link shown below is the link between Session Manager and the Messaging Server. The Name of the **Entity Link** was **SMONE-MANGO**. The **SIP Entity 1** was set to **Session Manager One**. The **Protocol** was **TLS** and the **Port** was **5061**. The **SIP Entity 2** was set to **MANGO**.

Entity Links
Commit

1 Item | Refresh
Filter: E

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port
* SMONE-MANGO	* Session Manager One	TLS	* 5061	* MANGO	* 5061

## 6.8. Administer Regular Expression

Select **Routing** → **Regular Expressions**. Under the **Regular Expressions** field select the **New** button.

The screenshot shows a web application interface for configuring Regular Expressions. On the left is a sidebar menu with 'Routing' and 'Regular Expressions' highlighted. The main content area has a breadcrumb trail 'Home / Elements / Routing / Regular Expressions'. Below this is a 'Regular Expressions' section with buttons for 'Edit', 'New', 'Duplicate', 'Delete', and 'More Actions'. A table below shows one item with a checkbox, a 'Pattern' column containing '80960@silstack.com', and a 'Rank Order' column containing '0'. At the bottom of the table is a 'Select : All, None' option.

	Pattern	Rank Order
<input type="checkbox"/>	80960@silstack.com	0

The **Pattern** was set to **80960@silstack.com**. The **Rank Order** was set to **0**. The **Commit** button was pressed to save the changes. This matches the Hunt Group Extension configured in **Section 5.11**.

The screenshot shows the 'Regular Expression Details' form. It has a 'General' tab. The 'Pattern' field is set to '80960@silstack.com' and the 'Rank Order' field is set to '0'. There is a 'Deny' checkbox which is unchecked. A 'Notes' field is at the bottom. In the top right corner, there are 'Commit' and 'Cancel' buttons.

\* Pattern: 80960@silstack.com

\* Rank Order: 0

Deny: ☐

Notes:

## 6.9. Administer Routing Policy

Select **Routing** → **Routing Policies**. Under the **Routing Policies** field select the **New** button.

Home / Elements / Routing / Routing Policies

**Routing Policies**

Edit New Duplicate Delete More Actions

10 Items | Refresh

<input type="checkbox"/>	Name	Disabled	Retries	Destination	Notes
<input type="checkbox"/>	AAC6	<input type="checkbox"/>	0	AACR6	
<input type="checkbox"/>	AvayaIT_CM	<input type="checkbox"/>	0	AvayaIT_CM	

Under **Routing Policies** the **SIP Entity as Destination** with the **Name** as **MANGO** and the **IP Address** as **192.168.1.133** and the **Type** set as **Modular Messaging** was selected.

Time Ranges  
Routing Policies  
Dial Patterns  
Regular Expressions  
Defaults

Disabled: ☐  
\* Retries: 0  
Notes:

**SIP Entity as Destination**

Select

Name	FQDN or IP Address	Type
MANGO	192.168.1.133	Modular Messaging

Under **Dial Patterns** the **Pattern** for **80960** with a **minimum** length of **5** digits a **maximum** length of **5** digits a **SIP Domain** as **silstack.com** and **Originating Location** as **Galway Stack** was added.

**Dial Patterns**

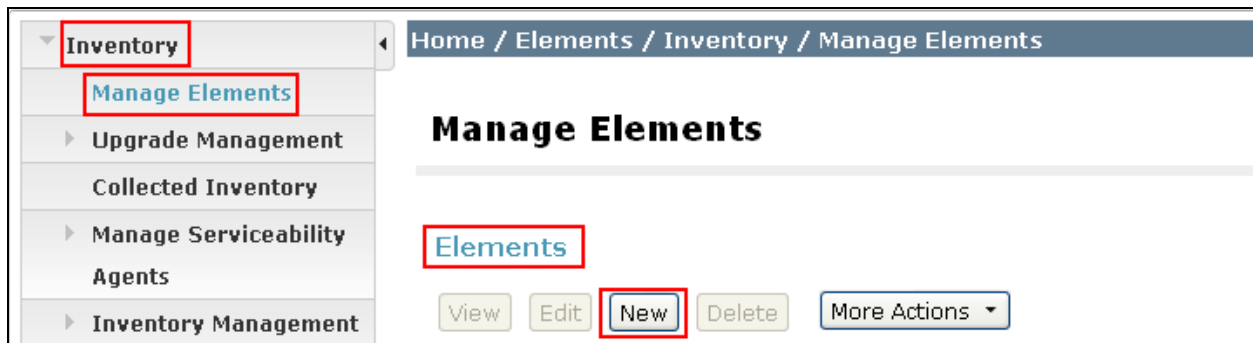
Add Remove

3 Items | Refresh

<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location
<input type="checkbox"/>	80959	5	5	<input type="checkbox"/>	silstack.com	Galway Stack
<input type="checkbox"/>	80960	5	5	<input type="checkbox"/>	silstack.com	Galway Stack

## 6.10. Administer Avaya Aura® Communication Manager as a Managed Element

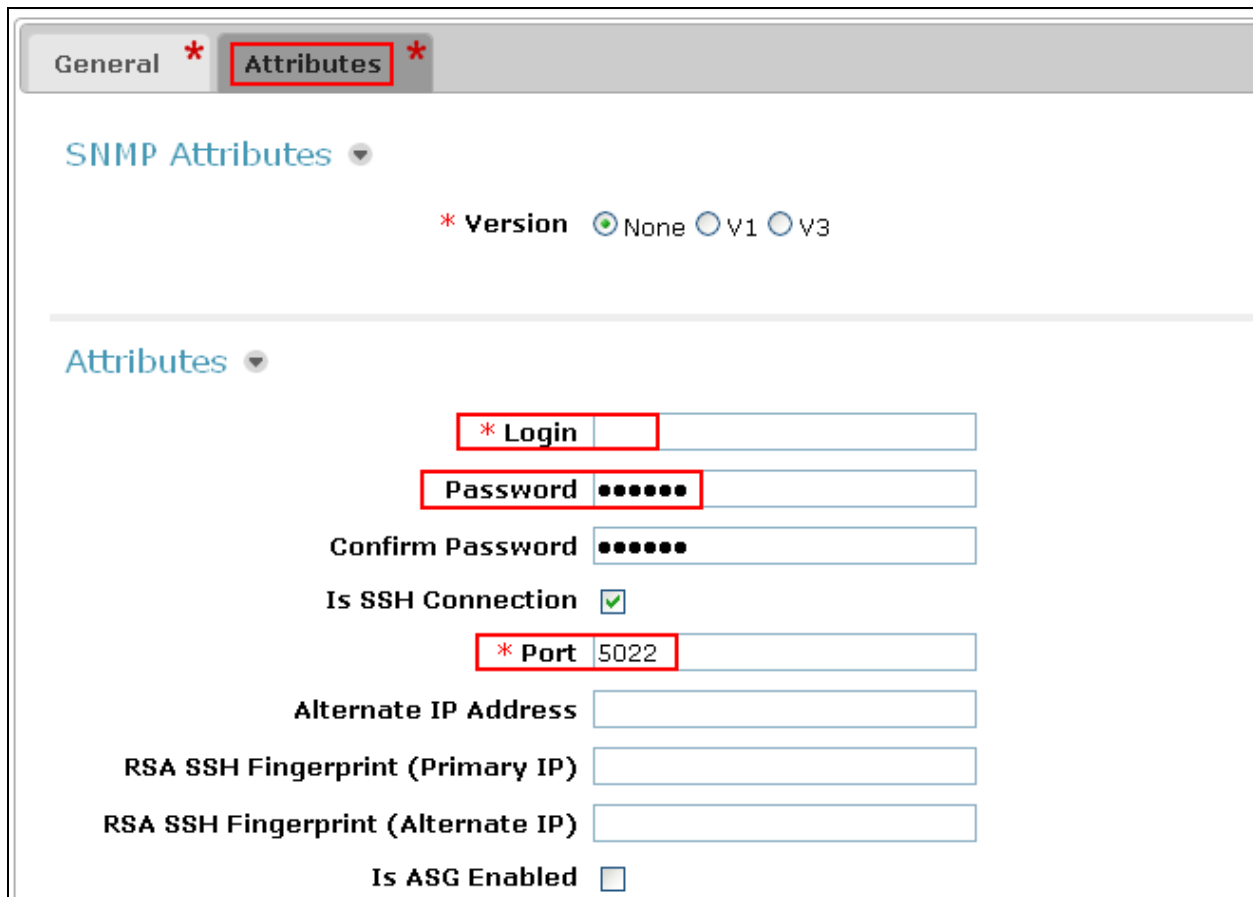
In order for Communication Manager to supply configuration and feature support to the Avaya one-X Mobile SIP for IOS as a Remote User when it registers to Session Manager, Communication Manager must be added as an application. Under the **Inventory** heading on the left hand side of the System Manager GUI access the **Manage Elements** sub heading. Under **Elements** select the **New** button.



The Manage Element **Name** was **MESCM**. The **Type** was set to **Communication Manager**. The **Node** IP Address was set to **192.168.1.82**.

The screenshot shows the 'Edit Communication Manager: CMES60' form. At the top right is a 'Commit' button. Below the title bar are two tabs: 'General' (active) and 'Attributes'. Under the 'General' tab, there are four fields: '\* Name' with the value 'MESCM', '\* Type' with the value 'Communication Manager', a 'Description' text area, and '\* Node' with the value '192.168.1.82'. All four fields are highlighted with red boxes.

Access the **Attributes** section and set the **Login**. This was the login used to access the Communication Manager Evolution Server. The **Password** was set to the password used to access the Communication Manager Evolution Server. The **Port** was set to **5022**.



General \* **Attributes** \*

SNMP Attributes ▾

\* Version ☒ None ☐ V1 ☐ V3

---

Attributes ▾

\* Login

Password

Confirm Password

Is SSH Connection ☒

\* Port

Alternate IP Address

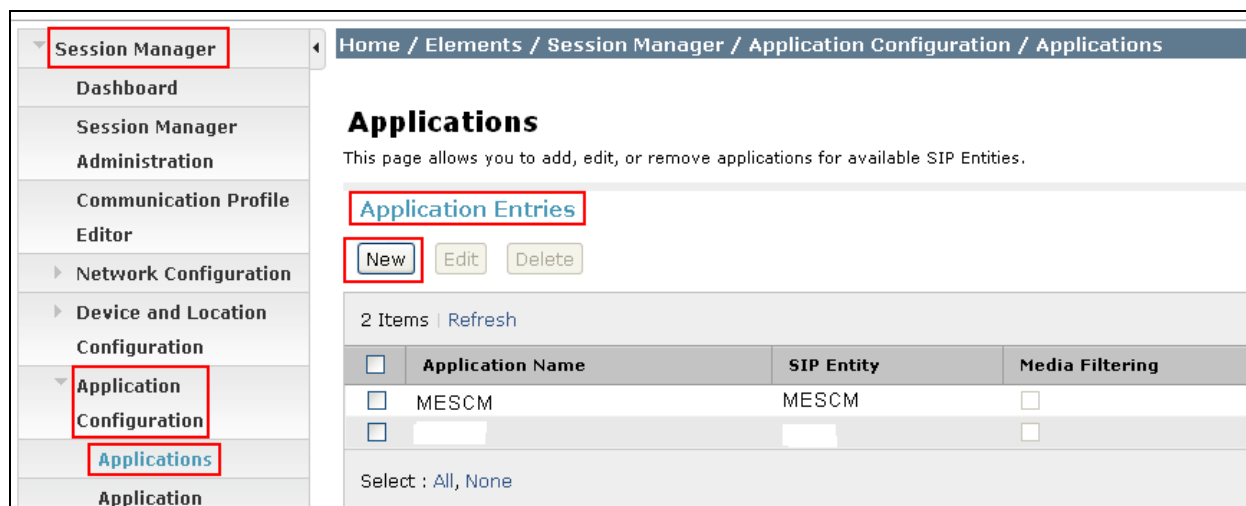
RSA SSH Fingerprint (Primary IP)

RSA SSH Fingerprint (Alternate IP)

Is ASG Enabled ☐

## 6.11. Administer Avaya Aura® Communication Manager Server Application

To configure the Communication Manager Evolution Server Application access **Session Manager** → **Application Configuration** → **Applications**. Under **Application Entries**, select the **New** button.



Home / Elements / Session Manager / Application Configuration / Applications

### Applications

This page allows you to add, edit, or remove applications for available SIP Entities.

**Application Entries**

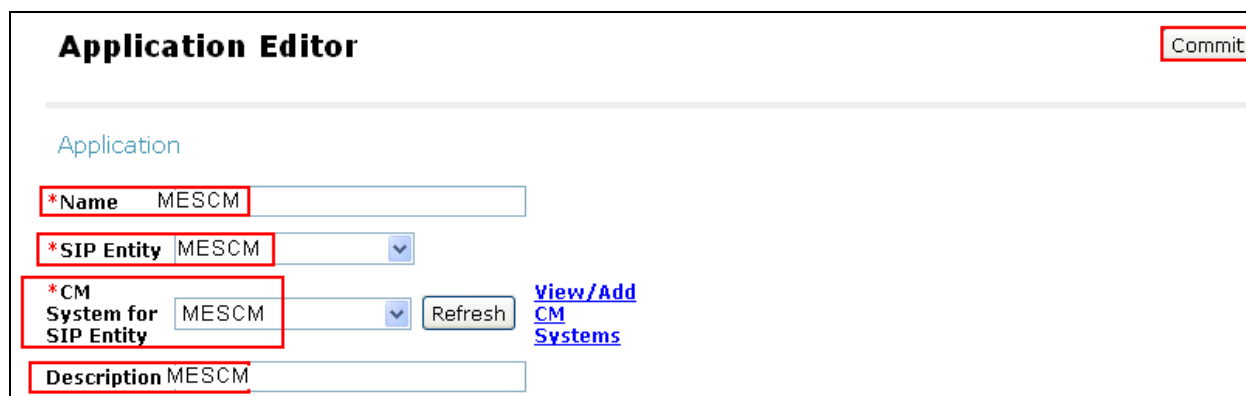
[New](#) [Edit](#) [Delete](#)

2 Items | [Refresh](#)

<input type="checkbox"/>	Application Name	SIP Entity	Media Filtering
<input type="checkbox"/>	MESCM	MESCM	<input type="checkbox"/>
<input type="checkbox"/>			<input type="checkbox"/>

Select : All, None

The **Name** of the Application was **MESCM**. The **SIP Entity** used was **MESCM**. The **CM System for SIP Entity** used was **MESCM**. The **Description** of the Application was **MESCM**.



### Application Editor

[Commit](#)

Application

\*Name MESCM

\*SIP Entity MESCM

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

Description MESCM

## 6.12. Administer Avaya Aura® Communication Manager Server Application Sequence

To configure the Communication Manager Evolution Server Application Sequence access the **Session Manager** heading on the left hand side System Manager GUI. Access the sub heading **Application Configuration** → **Application Sequences**.

The screenshot displays the Avaya Aura System Manager GUI. On the left, a navigation pane shows the 'Session Manager' menu expanded, with 'Application Configuration' and 'Application Sequences' highlighted. The main content area shows the 'Application Sequences' page, which includes a breadcrumb trail 'Home / Elements / Session Manager / Application Configuration /', a title 'Application Sequences', and a description 'This page allows you to add, edit, or remove sequences of applications.' Below this, there are buttons for 'New', 'Edit', and 'Delete'. A table lists two items: 'MESCM' and an empty row. The table has columns for 'Name' and 'Description'. At the bottom, there is a 'Select : All, None' option.

Session Manager

Dashboard

Session Manager Administration

Communication Profile Editor

Network Configuration

Device and Location Configuration

Application Configuration

Applications

Application Sequences

Home / Elements / Session Manager / Application Configuration /

### Application Sequences

This page allows you to add, edit, or remove sequences of applications.

Application Sequences

New Edit Delete

2 Items | Refresh

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	MESCM	
<input type="checkbox"/>		

Select : All, None



The Evolution Server Application Sequence **Name** was added as **MESCM**. The **Description** field was set to **MESCM**. Under the **Available Applications** field select the **plus** button to the left of the **MESCM** Name. This will then populate MESCM in the Application in this Sequence field. Select the **Commit** button to save the changes.

Application Sequence Editor

Commit

Application Sequence

\*Name MESCM

Description MESCM

Applications in this Sequence

Move First

Move Last

Remove

1 Item

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

Select : All, None

Available Applications

2 Items | Refresh Filter

	Name	SIP Entity	Description
	MESCM	MESCM	MESCM

## 6.13. Synchronize Avaya Aura® Communication Manager Data

To synchronize the Communication Manager Data access **Inventory** → **Synchronization** → **Communication System** heading on the left hand side of the System Manager GUI. Access the sub heading **Communication System**. The following screenshot shows the MESCM, the Communication Manager Evolution Server synchronized to the Session Manager by highlighting the **Initialize data for the selected devices** option and selecting the **Now** key.

The screenshot displays the Avaya Aura System Manager GUI. On the left, the navigation menu shows 'Inventory' and 'Synchronization' highlighted, with 'Communication System' selected under 'Synchronization'. The main content area is titled 'Synchronize CM Data and Configure Options'. A note states: 'Note: Please avoid any administration task on CM while sync is in progress.' Below this, a section titled 'Synchronize CM Data/Launch Element Cut Through' contains a table with one item, 'MESCM'. The table has columns for 'Element Name', 'FQDN/IP Address', 'Last Sync Time', 'Last Translation Time', 'Sync Type', and 'Sync Status'. The 'MESCM' row shows a last sync time of 'January 24, 2013 11:00:05 PM +00:00' and a last translation time of '10:00 pm THU JAN 24, 2013'. Below the table, there are three radio button options: 'Initialize data for selected devices' (selected), 'Incremental Sync data for selected devices', and 'Execute 'save trans all' for selected devices'. At the bottom, there are four buttons: 'Now', 'Schedule', 'Cancel', and 'Launch Element Cut Through'.

Home / Elements / Inventory / Synchronization / Communication System

**Synchronize CM Data and Configure Options**

Note: Please avoid any administration task on CM while sync is in progress.

Synchronize CM Data/Launch Element Cut Through

1 Item | Refresh | Show ALL Filter: Enable

	Element Name	FQDN/IP Address	Last Sync Time	Last Translation Time	Sync Type	Sync Status
<input checked="" type="checkbox"/>	MESCM	192.168.1.82	January 24, 2013 11:00:05 PM +00:00	10:00 pm THU JAN 24, 2013	Incremental	Completed

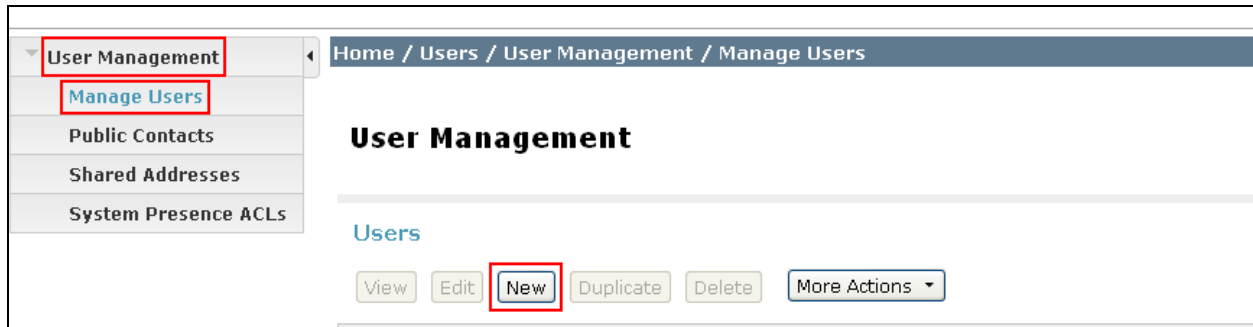
Select : All, None

☒ Initialize data for selected devices  
☐ Incremental Sync data for selected devices  
☐ Execute 'save trans all' for selected devices

Now Schedule Cancel Launch Element Cut Through

## 6.14. Administer SIP User

To add a SIP User to Session Manager, access the **User Management → Manage Users** heading on the left hand side of the System Manager GUI. Select the New button to add a new SIP User to Session Manager.



Select the **Identity** sub heading. The **Last Name** was set to **40040** and **First Name** was set to **40040**. The **Login Name** was set to **40040@silstack.com**. The **Authentication Type** was set to **Basic**.

The screenshot shows the 'Identity' subheading form. The 'Identity' subheading is highlighted with a red rectangle. The form contains the following fields and values:

- Last Name:** 40040 (highlighted with a red rectangle)
- First Name:** 40040 (highlighted with a red rectangle)
- Middle Name:** (empty field)
- Description:** (empty text area)
- Status:** Offline
- Update Time:** November 29, 2012 11:
- Login Name:** 40040@silstack.com (highlighted with a red rectangle)
- Authentication Type:** Basic (highlighted with a red rectangle)

Next, click on the **Communication Profile** Tab. Select the **Communication Profile** sub heading. The **Communication Profile Password** was set. Select the **Done** button to save the changes.

Identity \* **Communication Profile** \* Membership Contacts

Communication Profile ▼

Communication Profile Password: ●●●●●●

Confirm Password: ●●●●●●

New Delete **Done** Cancel

Select the **Communication Address** heading. The **Type** was set to **Avaya E.164**. The **Fully Qualified Address** was set to **+353917740040@silstack.com**. The **Add** button was pressed to save the changes.

**Communication Address** ▼

New Edit Delete

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

Type: Avaya E.164 ▼

\* Fully Qualified Address: +353917740040 @ silstack.com ▼

**Add** Cancel

Select **Session Manager Profile** heading was selected. The **Primary Session Manager** was set to **MESSM**. This equates to the Session Manager SIP entity. The **Origination Application Sequence** was set to **MESCM**. The **Termination Application Sequence** was set to **MESCM**. The **Home Location** was set to **Galway Stack**.

☒ **Session Manager Profile**

\* **Primary Session Manager** MESSM

**Secondary Session Manager** (None)

**Origination Application Sequence** MESCM

**Termination Application Sequence** MESCM

**Conference Factory Set** (None)

**Survivability Server** (None)

\* **Home Location** Galway Stack

In order for the Station Profile template information to be pushed from the Session Manager down to the Communication Manager Evolution Server, **enable** the **CM Endpoint Profile** box. The **System** was set to **MESCM**. This is the Communication Manager Server Element Name. The **Extension** was set to **40040** and the **Template** and **Set Type** was set to **9640SIP**.

☒ **CM Endpoint Profile**

\* **System** MESCM

\* **Profile Type** Endpoint

**Use Existing Endpoints** ☐

\* **Extension** 40040 **Endpoint Editor**

**Template** Select/Reset

**Set Type** 9640SIP

Click on **Endpoint Editor** and under **Feature Options** the settings were left as default.

**General Options (G) \*** **Feature Options (F)** **Site Data (S)** **Abbreviated Call Dialing (A)**

**Enhanced Call Fwd (E)** **Button Assignment (B)** **Group Membership (M)**

**Active Station Ringing** single  
**MWI Served User Type** Select  
**Per Station CPN - Send Calling Number** Select  
**IP Phone Group ID**  
**Remote Soft Phone Emergency Calls** as-on-local  
**LWC Reception** spe  
**AUDIX Name**  
**Speakerphone** 2-way  
**Short/Prefixed Registration Allowed** Select

**Auto Answer** none  
**Coverage After Forwarding** system  
**Display Language** english  
**Hunt-to Station**  
**Loss Group** 19  
**Survivable COR** internal  
**Time of Day Lock Table** Select  
**Voice Mail Number**

**Features**

- ☐ Always Use
- ☐ IP Audio Hairpinning
- ☐ Bridged Call Alerting
- ☐ Bridged Idle Line Preference
- ☒ Coverage Message Retrieval
- ☐ Data Restriction
- ☒ Survivable Trunk Dest
- ☐ Bridged Appearance Origination Restriction
- ☐ Idle Appearance Preference
- ☒ IP SoftPhone
- ☒ LWC Activation
- ☐ CDR Privacy
- ☒ Direct IP-IP Auto Connection
- ☐ H.320 Conversion
- ☐ IP Video Softphone

Within **Button Assignments** a value of **5 call-appr** buttons were set. A **call-fwd** button and a **call-pkup** button were also assigned. The **Done** button was pressed

**General Options (G) \*** **Feature Options (F)** **Site Data (S)** **Abbreviated Call Dialing (A)**

**Enhanced Call Fwd (E)** **Button Assignment (B)** **Group Membership (M)**

**Main Buttons** **Feature Buttons** **Button Modules**

Button	Value	Extension P	Rg
1	call-appr		
2	call-appr		
3	call-appr		
4	call-appr		
5	call-appr		
6	call-fwd		
7	call-pkup	h	no-ring
8	None		

**\*Required**

**Done** **Cancel**

Press the **Commit** button to save the changes.

**Delete Endpoint on Unassign of Endpoint from User or on Delete User** ☒

**Messaging Profile** **Messaging Profile**

**Commit** **Cancel**

## 7. Administer Avaya Aura® Messaging Server

This section highlights the important commands for administering Avaya Aura Messaging to function correctly with SRTP and adding a subscriber for the Avaya one-X Mobile SIP for IOS as a Remote User to the Messaging Server.

### 7.1. Access Avaya Aura® Messaging

Access the Messaging web interface, by entering **http://<ip-addr>** as the URL in an Internet browser, where *<ip-addr>* is the IP address of the server running the Messaging graphical user interface. Log in with the appropriate **Login ID** and **Password** and press the **Logon** button to access the Messaging Server.



The screenshot shows a web browser window with the URL `https://192.168.1.133/cgi-bin/common/login/webLogin`. The Avaya logo is in the top left corner. A red banner at the top contains the text "Log Off". The main content area features a "Logon" box with the following fields and buttons:

- Logon ID:** A text input field containing the value "init".
- Password:** A password input field containing eight dots.
- Logon:** A button located at the bottom right of the "Logon" box.

Under the Administration heading select **Messaging**.



### 7.2. Administer Telephony Integration with SRTP

Select **Telephony Integration** under the Telephony Settings heading on the left hand side of the Messaging Graphical User Interface. Under **BASIC CONFIGURATION** the **Switch Integration Type** was set to **SIP**. Under **SIP SPECIFIC CONFIGURATION** the **Transport**

**Method** was set to **TLS**. The **Connection 1** setting was set to **192.168.1.87**, the IP Address of the Session Manager. The **Port** was set to **5061**. The **Messaging Address** was set to **192.168.1.133**. The **SIP Domain** was set to **silstack.com**. The **Save** button was selected to save the changes.

The **Show Advanced Options** setting was selected.

Under the **Advanced Options** settings the **Media Encryption** setting was set to **srtp-aescm128-hmac80**. The **Media Encryption During CapNeg** setting was **Enabled**. The **Save** button was selected to save these changes to the Messaging Server. Note that the Messaging Server needed to be stopped and started for these SRTP changes to take effect on the Messaging Server.



<input type="button" value="Save"/> <input type="button" value="Help"/> <input type="button" value="Hide Advanced Options"/>	
<b>ADVANCED OPTIONS</b>	
<u>Quality Of Service</u>	Call Control PHB <input type="text" value="46"/> Audio PHB <input type="text" value="46"/>
<u>UDP Port Range</u>	Start <input type="text" value="8000"/> End <input type="text" value="8410"/>
<u>Media Encryption</u>	<input type="text" value="srtp-aescm128-hmac80"/>
<u>SIP INFO for DTMF</u>	<input type="text" value="Ignore"/>
<u>Media Encryption During CapNeg</u>	<input type="text" value="Enabled"/>
<u>Supported Header includes "replaces"</u>	<input type="text" value="no"/>
<u>Monitor Far-end OPTIONS messages</u>	<input type="text" value="no"/> Proactive Interval <input type="text" value="0"/>
<u>Inactive Link Actions</u>	<input type="text" value="Alarm Only"/>

### 7.3. Administer Subscriber

To add a subscriber to the Messaging Server select **User Management**. Under the **Add User/Info Mailbox** heading select the **Add** button.

Administration / Messaging	
<ul style="list-style-type: none"> <li>Messaging System (Storage) <ul style="list-style-type: none"> <li><b>User Management</b></li> <li>Class of Service</li> <li>Sites</li> <li>Topology</li> <li>Storage Destinations</li> <li>System Policies</li> <li>Enhanced List Management</li> <li>System Mailboxes</li> <li>System Ports and Access</li> <li>User Activity Log Configuration</li> </ul> </li> <li>Reports (Storage) <ul style="list-style-type: none"> <li>Users</li> <li>Info Mailboxes</li> <li>Remote Users</li> <li>Uninitialized Mailboxes</li> <li>Login Failures</li> <li>Locked Out Users</li> </ul> </li> <li>Server Information <ul style="list-style-type: none"> <li>System Status (Storage)</li> <li>System Status (Application)</li> <li>Alarm Summary</li> <li>Voice Channels (Application)</li> <li>Cache Statistics (Application)</li> </ul> </li> <li>Server Settings (Storage)</li> </ul>	<h2>User Management</h2> <p><b>License Status</b> License mode: Normal</p> <p><b>Edit User/Info Mailbox</b> Edit a user's properties. Possible identifiers are: mailbox number.</p> <p>Identifier: <input type="text"/></p> <p><input type="button" value="Edit"/></p> <p><b>Add User/Info Mailbox</b></p> <p>Add a new user: <input type="button" value="Add"/></p> <p>Add a new Info Mailbox:</p>

The **First Name** was set to **40040**. The **Last Name** was set to **40040**. The **Mailbox Number** was set to **40040**. The **Extension** was set to **40040**. The **Class of Service** was set to **Standard**.

**User Management > Properties for New User**

**User Properties**

First name: 40040

Last name: 40040

Display name: one-X Mobile SIP for IOS

ASCII name:

Site: Default

Mailbox number: 40040

Extension: 40040

☒ Include in Auto Attendant directory

Additional extensions:

Class of Service: Standard

Pronounceable name: one-X Mobile SIP for IOS

The **MWI enabled** setting was set to **Yes**. The **New password** was set to the password of the subscriber mailbox for the Avaya one-X Mobile SIP for IOS as a Remote User. The **User must change voice messaging password on next logon** setting was **enabled**. The **Save** button was pressed to save these changes.

MWI enabled: Yes

Miscellaneous 1:

Miscellaneous 2: init

New password: .....

Confirm password:

☒ User must change voice messaging password at next logon

☐ Voice messaging password expired

☐ Locked out from voice messaging

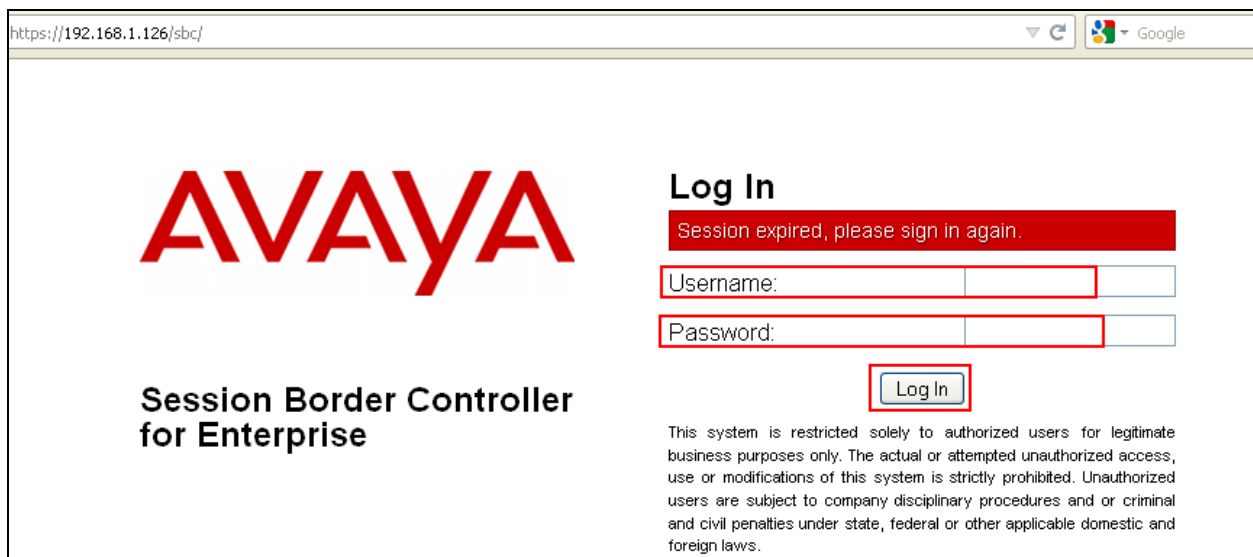
Save Delete

## 8. Administer Avaya Session Border Controller Advanced for Enterprise

This section highlights the important steps for administering Avaya one-X Mobile SIP for IOS as a Remote User with SRTP to register to the Session Border Controller Server. It was decided that the Avaya one-X Mobile SIP for IOS as a Remote User would be administered with SRTP from the remote endpoint to the outside interface on the Session Border Controller and with SRTP from the inside interface to the Communication Manager Server. This section will document administering the media rule with SRTP to be used on the outside and inside interfaces on the Session Border Controller. It will also document the steps needed to administer signaling and media interfaces to the Session Manager and Remote User. It will highlight the steps required to configure Routing Profiles and End Point Policy Groups needed to be assigned to Subscriber and Server Flows within an End Point Flow. An asterisk (\*) used in the option field for this section indicates that any or all choices for that parameter are acceptable. It is assumed that IP Addresses for all ports have been assigned during installation.

### 8.1. Access Avaya Session Border Controller Advanced for Enterprise

Access the Avaya Session Border Controller Advanced web interface, by entering **https://<ip-addr>** as the URL in an Internet browser, where *<ip-addr>* is the Management IP address of the server running the Avaya Avaya Session Border Controller Advanced graphical user interface. Log in with the appropriate **Username** and **Password** and press the **Log In** button to access the server.



https://192.168.1.126/sbc/

**AVAYA**

**Session Border Controller  
for Enterprise**

**Log In**

Session expired, please sign in again.

Username:

Password:

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws.

The following page is displayed.

Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log

## Session Border Controller for Enterprise

**Dashboard**

- Administration
- Backup/Restore
- System Management
  - Global Parameters
  - Global Profiles
  - SIP Cluster
  - Domain Policies
  - TLS Management
  - Device Specific Settings

**Dashboard**

Application DEBUG level log messages are currently enabled on one or more subsystems. Leaving this log level enabled for extended periods of time may cause severe performance degradation.

Information	
System Time	02:11:03 PM GMT <a href="#">Refresh</a>
Version	6.2.0.Q40
Build Date	Thu Mar 14 15:50:47 UTC 2013

Installed Devices
EMS
MCS

Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
MCS: Server DOS Detected - Pending Threshold Crossed
MCS: Server DOS Detected - Pending Threshold Crossed
MCS: Request Timeout

Select **Device Specific Settings**→**Network Management**→**Add** to add the IP Address of the Session Border Controller Server interfaces.

Dashboard Administration Backup/Restore System Management Global Parameters Global Profiles SIP Cluster Domain Policies TLS Management **Device Specific Settings**

**Network Management**

Media Interface

**Network Management: MCS**

Devices MCS

**Network Configuration** **Interface Configuration**

Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from [System Management](#).

A1 Netmask	A2 Netmask	B1 Netmask	B2 Netmask
255.255.255.224		255.255.255.0	

[Add](#) [Save](#)

IP Address	Public IP	Gateway	Interface
			A1
			B1

The IP Address of the **A1** inside interface was set to **192.168.1.16**. The IP Address of the **B1** outside interface was set to **10.10.25.15**.

Device Specific Settings **Network Management** Media Interface Signaling Interface Signaling Forking

**Network Management**

Media Interface

Signaling Interface

Signaling Forking

**Network Configuration** **Interface Configuration**

Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from [System Management](#).

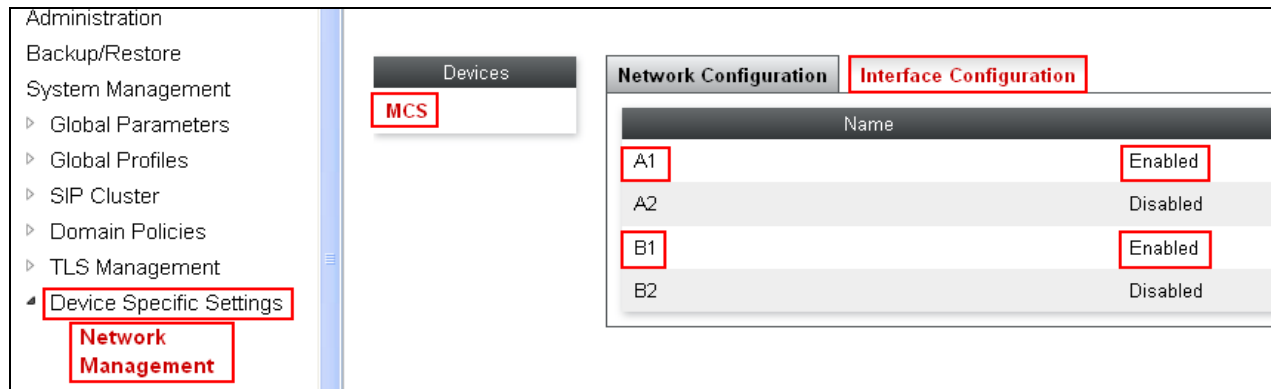
A1 Netmask	A2 Netmask	B1 Netmask	B2 Netmask
255.255.255.224		255.255.255.0	

[Add](#) [Save](#)

IP Address	Public IP	Gateway	Interface
192.168.1.16		192.168.1.1	A1
10.10.25.15		10.10.25.1	B1

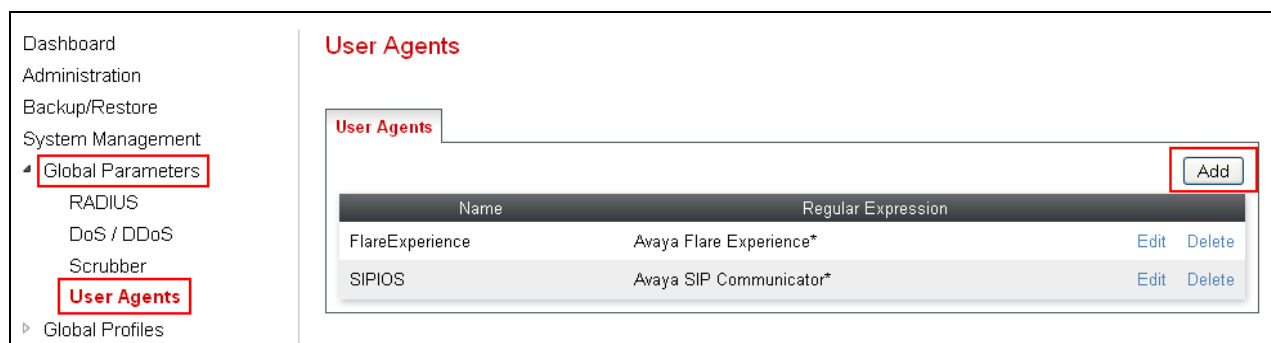
## 8.2. Enable Interfaces on the Avaya Session Border Controller Advanced for Enterprise

Select **Device Specific Settings**→**Network Management**→**Interface Configuration**. The **A1** internal interface was **Enabled** by selecting the **Toggle State** button. The **B1** external interface was also **Enabled** by selecting the **Toggle State** button.



## 8.3. Administer User Agent

A User Agent was added for Avaya one-X Mobile SIP for IOS to allow the Avaya one-X Mobile SIP for IOS remote user access the network. To administer a User Agent for Avaya one-X Mobile SIP for IOS under **Global Parameters** select the **User Agents** heading. Select the **Add** button.



The **Name** was set to **SIPIOS** and the **Regular Expression** was set to **Avaya SIP Communicator\***. The **Finish** button was selected to save the changes.

**Add User Agent** X

**WARNING:** Invalid or incorrectly entered regular expressions may cause unexpected results.

Note: This regular expression is case-sensitive.

**Ex:**  
 Avaya one-X Deskphone  
 Aastra.\*  
 Cisco-CP7970G[0-9]{3}  
 RTC/1.1RTC/1.2

Name

SIPIOS

Regular Expression

Avaya SIP Communicat

Finish

## 8.4. Administer Server Interworking

An Interworking Profile was used to manipulate headers for compatibility purposes. It was decided to use an existing Server Interworking Profile named **avaya-ru** and clone this Server Interworking Profile. To clone the Server Interworking select **Global Profiles**→**Server Interworking**→**avaya-ru**→**Clone**.

- Dashboard
- Administration
- Backup/Restore
- System Management
- Global Parameters
- Global Profiles
- Domain DoS
- Fingerprint
- Server Interworking
- Phone Interworking

Interworking Profiles: cs2100

Add

Interworking Profiles

cs2100

avaya-ru

OCS-Edge-Server

cisco-ccm

cups

Sipera-Halo

Clone

It is not recommended to edit the defaults. Try cloning or adding a new profile instead.

General

Timers

URI Manipulation

Header Manipulation

Advanced

General	
Hold Support	RFC3264
180 Handling	None
181 Handling	None
182 Handling	None

The **Profile Name** selected was **avaya-ru**. The **Clone Name** was set to **avaya-ruSIPIOS**. The **Finish** button was selected to save the changes.

**Clone Profile** X

Profile Name

avaya-ru

Clone Name

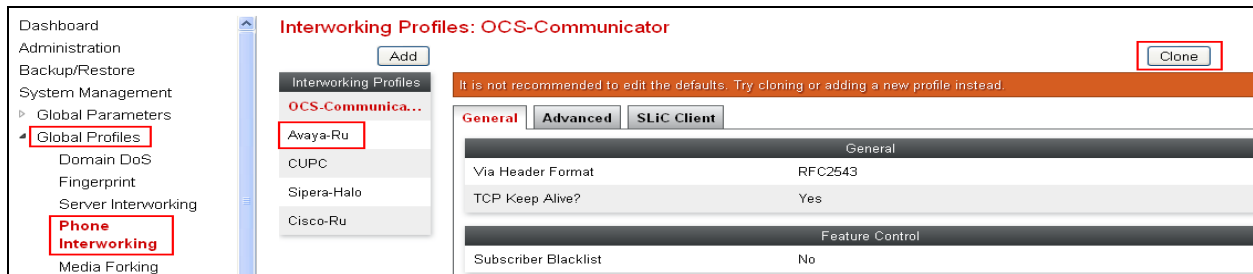
avaya-ruSIPIOS

Finish

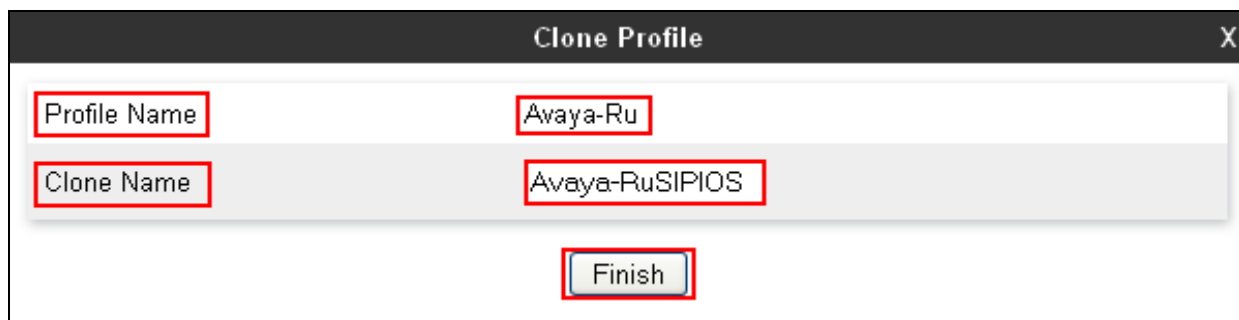
All values for the Server Interworking Profile were left as default.

## 8.5. Administer Phone Interworking

A Phone Interworking allows the user to edit specific SIP signaling message parameters to allow interoperability between endpoints and SIP implementations. It was decided to use an existing Phone Interworking Profile named **Avaya-Ru** and clone this Phone Interworking Profile. To clone the Phone Interworking select **Global Profiles**→**Phone Interworking**→**Avaya-Ru**→**Clone**.



The **Profile Name** selected was **Avaya-Ru**. The **Clone Name** was set to **Avaya-RuSIPIOS**. The **Finish** button was selected to save the changes.



The settings for the Phone Interworking Profile were left as default.

## 8.6. Verify TLS Client Profile

A Client Profile is needed to allow the Avaya one-X Mobile SIP for IOS as a Remote User to participate in a secure TLS session. The Session Border Controller has a pre installed Avaya client profile as part of the Session Border Controller software named AvayaSBCClient. It was decided to use this pre installed Avaya client profile for configuration purposes. Select **TLS Management**→**Client Profiles**→**AvayaSBCClient**. The **Profile Name** was **AvayaSBCClient**. The AvayaSBCClient profile contained the **Certificate** named **AvayaSBC.crt**. The AvayaSBCClient profile also contained the **Peer Certificate Authorities** root CA certificate named **AvayaSBCCA.crt**. These certificates are all Avaya signed certificates and trusted by other Avaya Servers.

The screenshot displays the Avaya SBC configuration interface. On the left is a navigation menu with the following items: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, SIP Cluster, Domain Policies, TLS Management (highlighted with a red box), Certificates, Client Profiles (highlighted with a red box), Server Profiles, and Device Specific Settings. The main content area is titled "Client Profiles: AvayaSBCClient" in red. It features an "Add" button and a "Client Profiles" tab. Below the tab is a list of client profiles, with "AvayaSBCClient" highlighted by a red box. To the right of the list is a "Click here to add a description." link. The "AvayaSBCClient" profile is expanded, showing the following details:

Client Profile	
Click here to add a description.	
TLS Profile	
Profile Name	AvayaSBCClient
Certificate	AvayaSBC.crt
Certificate Info	
Peer Verification	Required
Peer Certificate Authorities	AvayaSBCCA.crt



## 8.7. Verify TLS Server Profile

To allow the Avaya one-X Mobile SIP for IOS as a Remote User to participate in a secure TLS session a TLS Server Profile was also used. The Session Border Controller has a pre installed Avaya server profile as part of the Session Border Controller software. It was decided to use this pre installed Avaya server profile for configuration purposes. Select **TLS Management**→**Server Profiles**→**AvayaSBCServer**. The **Profile Name** was **AvayaSBCServer**. The AvayaSBCServer profile contained the **Certificate** named **AvayaSBC.crt**.

The screenshot shows the Avaya SBC configuration interface. On the left is a navigation menu with options: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, SIP Cluster, Domain Policies, TLS Management (selected), Certificates, Client Profiles, Server Profiles (highlighted), and Device Specific Settings. The main area is titled "Server Profiles: AvayaSBCServer". It features an "Add" button and a list of server profiles: "Server Profiles", "AvayaSBCServer" (highlighted), and "https". The "AvayaSBCServer" profile is expanded, showing a "Server Profile" section with a "Click here to add a description." link. Below this is a "TLS Profile" section with fields for "Profile Name" (AvayaSBCServer) and "Certificate" (AvayaSBC.crt), both highlighted. Further down is a "Certificate Info" section with "Peer Verification" set to "None". At the bottom is a "Renegotiation Parameters" section.

## 8.8. Administer Topology Hiding for Subscriber and Server Flow

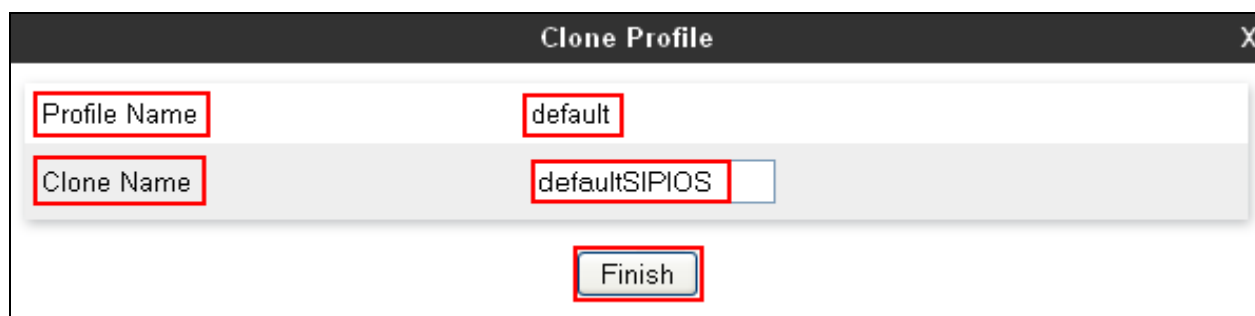
Topology Hiding is a UC-Sec security feature which allows the user to change certain key SIP messages parameters to hide how the enterprise network map appears to the outside world. The Topology Hiding created will be applied to the Subscriber and Server flow. It was decided to use an existing topology hiding named **default** and clone this Topology hiding Profile. To clone the Topology Hiding Profile select **Global Profiles**→**Topology Hiding**→**default**→**Clone**.

The screenshot shows the Avaya SBC configuration interface for "Topology Hiding Profiles: default". The left navigation menu includes: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (selected), Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, Routing, Server Configuration, Topology Hiding (highlighted), Signaling, and Manipulation. The main area is titled "Topology Hiding Profiles: default" and includes an "Add" button and a list of profiles: "Topology Hiding Profiles", "default" (highlighted), "cisco\_th\_profile", and "silstack". A "Clone" button is highlighted in the top right. A warning message states: "It is not recommended to edit the defaults. Try cloning or adding a new profile instead." Below this is a "Topology Hiding" table with the following data:

Header	Criteria	Replace Action	Overwrite Value
To	IP/Domain	Auto	---
From	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
Request-Line	IP/Domain	Auto	---

An "Edit" button is located at the bottom right of the table.

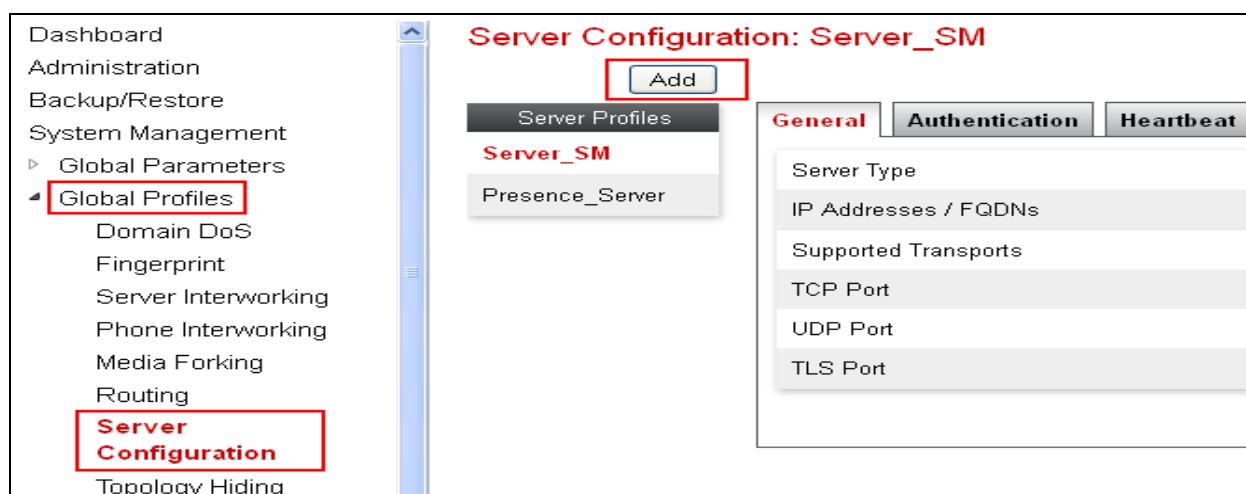
The **Profile Name** was set to **default**. The **Clone Name** was set to **defaultSIPIOS**. The **Finish** button was selected to save the changes.



A dialog box titled "Clone Profile" with a close button (X) in the top right corner. It contains two text input fields: "Profile Name" with the value "default" and "Clone Name" with the value "defaultSIPIOS". Below these fields is a "Finish" button. Red boxes highlight the "Profile Name" field, the "Clone Name" field, and the "Finish" button.

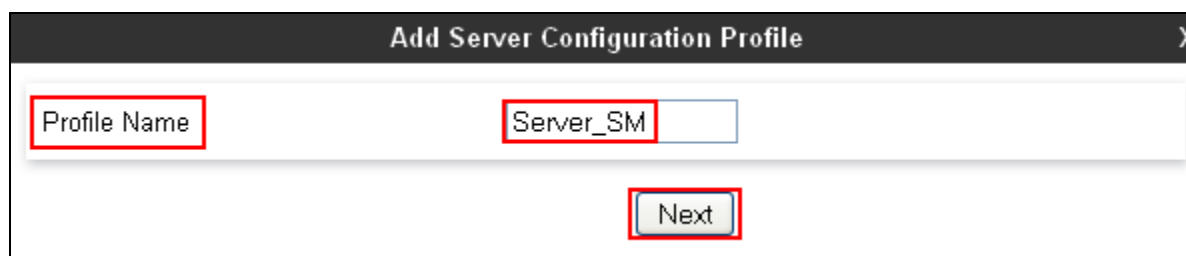
## 8.9. Administer Session Manager Server Configuration

This section describes creating a Call Server Profile for the Avaya Session Manager Server on the Avaya Session Border Controller. Select **Global Profiles**→**Server Configuration**→**Add**.



A screenshot of the "Server Configuration: Server\_SM" interface. On the left is a navigation menu with items: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (selected), Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, Routing, Server Configuration (highlighted in red), and Topology Hiding. The main area shows a list of "Server Profiles" with "Server\_SM" and "Presence\_Server". An "Add" button is highlighted with a red box. To the right are tabs for "General", "Authentication", and "Heartbeat". The "General" tab is active, showing fields for "Server Type", "IP Addresses / FQDNs", "Supported Transports", "TCP Port", "UDP Port", and "TLS Port".

The **Profile Name** was set to **Server\_SM**. The **Next** button was selected to continue to the next page.



A dialog box titled "Add Server Configuration Profile" with a close button (X) in the top right corner. It contains a text input field for "Profile Name" with the value "Server\_SM". Below this field is a "Next" button. Red boxes highlight the "Profile Name" field and the "Next" button.

The Server Configuration Server\_SM was administered in this section. The **Server Type** was set to **Call Server**. The **IP address** was set to **192.168.1.87**. This was the Signaling Interface of the

Session Manager. The **Supported Transports** was set to **TLS**. The **TLS Port** was set to **5061**. The **Next** button was selected to continue to the next page.

**Add Server Configuration Profile - General**

Server Type: Call Server

IP Addresses / Supported FQDNs: 192.168.1.87

Supported Transports: ☐ TCP, ☐ UDP, ☒ TLS

TCP Port:

UDP Port:

TLS Port: 5061

Back Next

The **Enable Grooming** setting was also **Enabled**. The **Interworking Profile** value was set to **avaya-ruSIPIOS**. The **TLS Client Profile** was set to **AvayaSBCClient**. The **TLS Connection Type** was set to **SUBID**. The **Finish** button was selected.

**Add Server Configuration Profile - Advanced**

Enable DoS Protection: ☐

Enable Grooming: ☒

Interworking Profile: avaya-ruSIPIOS

TLS Client Profile: AvayaSBCClient

Signaling Manipulation Script: None

TLS Connection Type: ☒ SUBID, ☐ PORTID, ☐ MAPPING

Back Finish

## 8.10. Administer External Signaling Interface Toward Remote User

The section explains administering a signaling interface to the Avaya one-X Mobile SIP for IOS as a Remote User endpoint. Select **Device Specific Settings**→**Signaling Interface**→**Add**.

Backup/Restore  
System Management  
‣ Global Parameters  
‣ Global Profiles  
‣ SIP Cluster  
‣ Domain Policies  
‣ TLS Management  
‣ **Device Specific Settings**  
  Network Management  
  Media Interface  
  **Signaling Interface**

Devices  
MCS

**Signaling Interface** Add

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	Edit	Delete
Int_Sig_intf_Call_Srv		5060	5060	5061	AvayaSBCServer		
Ext_Sig_intf_Remote_Phone	10.10.25.15	5060	5060	5061	AvayaSBCServer	Edit	Delete

The **Name** was set to **Ext\_Sig\_intf\_Remote\_Phone**. The **IP Address** was set to **10.10.25.15**. This was the IP Address of the B1 external interface of the Avaya Avaya Session Border Controller. The **TLS Port** was set to **5061**. The **TLS Profile** was set to **AvayaSBCServer**. The **Finish** button was pressed to save the changes.

**Name** Ext\_Sig\_Intf\_Remote

**IP Address** 10.10.25.15

**TCP Port** 5060  
Leave blank to disable

**UDP Port** 5060  
Leave blank to disable

Enable Stun ☐

**TLS Port** 5061  
Leave blank to disable

**TLS Profile** AvayaSBCServer

Enable Shared Control ☐

Shared Control Port

**Finish**

## 8.11. Administer Internal Signaling Interface toward Session Manager

This section explains administering a signaling interface to the Session Manager Server. Select **Device Specific Settings**→**Signaling Interface**→**Add**. The **Name** was set to **Int\_Sig\_intf\_Call\_Srv**. The **IP Address** was set to **192.168.1.16**. This was the IP Address of the A1 internal interface of the Avaya Session Border Controller. The **TLS Port** was set to **5061**. The **TLS Profile** was set to **AvayaSBCServer**. The **Finish** button was pressed to save the changes.

Add Signaling Interface	
Name	Int_Sig_intf_Call_Srv
IP Address	192.168.1.16
TCP Port Leave blank to disable	5060
UDP Port Leave blank to disable	5060
TLS Port Leave blank to disable	5061
Cluster TLS Only for use with Cisco SIP Clusters	<input type="checkbox"/>
Enable Stun Requires a UDP Port	<input type="checkbox"/>
TLS Profile	AvayaSBCServer
<b>Finish</b>	

## 8.12. Administer External Media Interface Toward Remote User

The section explains administering a media interface to the Avaya one-X Mobile SIP for IOS as a Remote User. Select **Device Specific Settings**→**Media Interface**→**Add**.

<div>Backup/Restore</div> <div>System Management</div> <div>Global Parameters</div> <div>Global Profiles</div> <div>SIP Cluster</div> <div>Domain Policies</div> <div>TLS Management</div> <div>Device Specific Settings</div> <div>Network Management</div> <div>Media Interface</div> <div>Signaling Interface</div>	<div>Devices</div> <div>MCS</div>	<div>Media Interface</div> <div>Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from <a href="#">System Management</a>.</div> <div>Add</div> <table border="1"><thead><tr><th>Name</th><th>Media IP</th><th>Port Range</th><th>Edit</th><th>Delete</th></tr></thead><tbody><tr><td>Int_Med_intf_Call_Srv</td><td></td><td>35000 - 40000</td><td></td><td></td></tr><tr><td>Ext_Med_intf_Remote_Phone</td><td>10.10.25.15</td><td>35000 - 40000</td><td></td><td></td></tr></tbody></table>	Name	Media IP	Port Range	Edit	Delete	Int_Med_intf_Call_Srv		35000 - 40000			Ext_Med_intf_Remote_Phone	10.10.25.15	35000 - 40000		
	Name	Media IP	Port Range	Edit	Delete												
	Int_Med_intf_Call_Srv		35000 - 40000														
	Ext_Med_intf_Remote_Phone	10.10.25.15	35000 - 40000														

The **Name** was set to **Ext\_Med\_intr\_Remote\_Phone**. The **IP Address** was set to **10.10.25.15**. The **Port Range** was set to **35000 – 40000**. The **Finish** button was selected to save the changes.

The screenshot shows a dialog box titled "Add Media Interface" with a close button (X) in the top right corner. It contains three input fields and a button. The "Name" field has the text "Ext\_Med\_intf\_RemotePt". The "IP Address" field has a dropdown menu showing "10.10.25.15". The "Port Range" field has two input boxes with "35000" and "40000" separated by a hyphen. Below these fields is a "Finish" button.

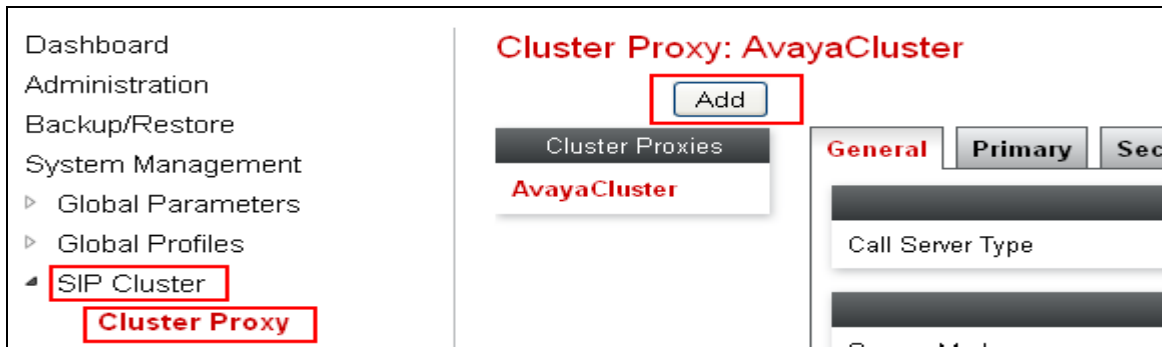
### 8.13. Administer Internal Media Interface Toward Session Manager

This section explains administering a media interface to the Session Manager Server. Select **Device Specific Settings**→**Media Interface**→**Add Media**. The **Name** was set to **Int\_Med\_intr\_Call\_Srv**. The **IP Address** was set to **192.168.1.16**. The **Port Range** was set to **35000 – 40000**. The **Finish** button was selected to save the changes.

The screenshot shows a dialog box titled "Add Media Interface" with a close button (X) in the top right corner. It contains three input fields and a button. The "Name" field has the text "Int\_Med\_intf\_Call\_srv". The "IP Address" field has a dropdown menu showing "192.168.1.16". The "Port Range" field has two input boxes with "35000" and "40000" separated by a hyphen. Below these fields is a "Finish" button.

## 8.14. Administer SIP Cluster

This section describes creating a SIP Cluster. The SIP Cluster will be administered with secure mode to use TLS for SIP. This allows the user to use https for the endpoint configuration download. A TLS Server Profile will be created to allow the user to download PPM information to the Avaya one-X Mobile SIP for IOS as a Remote User. Select **SIP Cluster**→**Cluster Proxy**→**Add**.



The **Cluster Name** was set to **AvayaCluster**. The **Callserver Type** was set to **Avaya**. The **Next** button was selected to continue to the next page.

A screenshot of the 'Add SIP Cluster' dialog box. It has a title bar 'Add SIP Cluster' with a close button 'X'. Inside, there are two input fields: 'Cluster Name' with the value 'AvayaCluster' and 'Callserver Type' with the value 'Avaya'. Both fields are highlighted with red boxes. At the bottom right is a 'Next' button (highlighted with a red box).

The **Secure Mode** was **Enabled** to allow TLS for SIP. The **Domain Name** was set to **silstack.com**. The **Finish** button was selected to save the changes.

The screenshot shows the 'Add SIP Cluster' dialog box with the 'Security Information' tab selected. The 'Secure Mode' checkbox is checked and labeled 'Enabled'. The 'Domain Name' field contains 'silstack.com'. The 'Configuration Update Interval' is set to '15' minutes. At the bottom, there are 'Back' and 'Next' buttons.

Security Information	
Secure Mode	<input checked="" type="checkbox"/> Enabled

Miscellaneous Information	
Domain Name	silstack.com
Configuration Update Interval	15 minutes

Back Next

The **Device Name** was set to **MCS**. The **Device IP** was set to **10.10.25.15**. This was the B1 external interface of the Avaya Avaya Session Border Controller. The **Configuration Server Client Address** was set to **192.168.1.16**. This was the A1 internal interface of the Avaya Session Border Controller. The **Next** button was selected to continue to the next page.

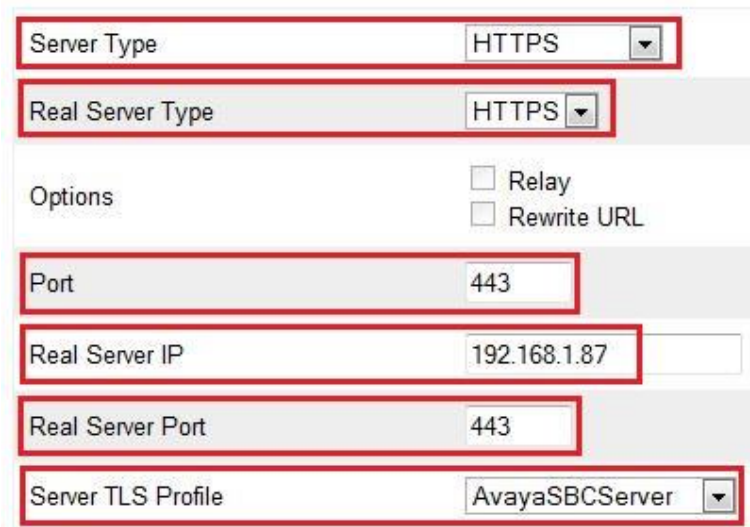
The screenshot shows the 'Add SIP Cluster' dialog box with the 'Miscellaneous Information' tab selected. The 'Device Name' dropdown is set to 'MCS'. The 'Device IP' dropdown is set to '10.10.25.15'. The 'Configuration Server Client Address' dropdown is set to '192.168.1.16'. At the bottom, there are 'Back' and 'Next' buttons.

Device Name	MCS
Device IP	10.10.25.15
Configuration Server Client Address	192.168.1.16

Back Next



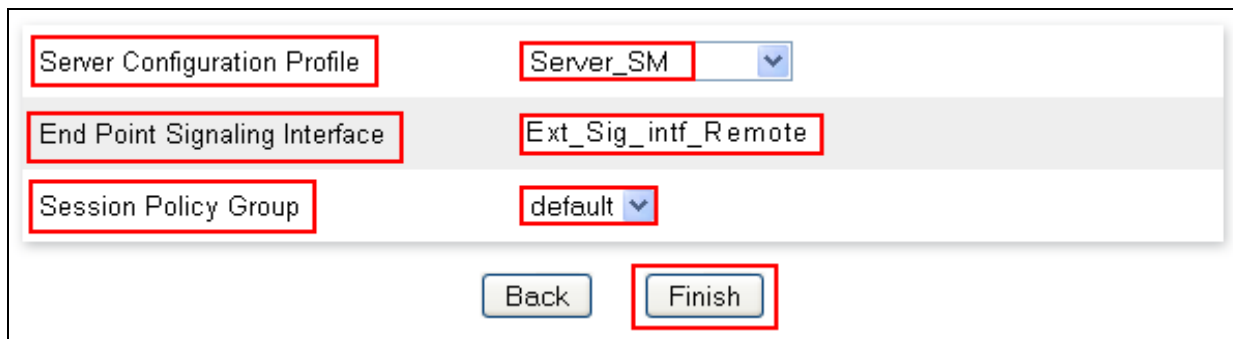
The **Server Type** was set to **HTTPS**. The **Real Server Type** was set to **HTTPS**. The **UC-Sec Port** was set to **443**. The **Real Server IP** was set to **192.168.1.87**. This is the IP Address of Session Manager . The **Real Server Port** was set to **443**. The **Server TLS Profile** was set to **AvayaSBCServer**. The **Finish** button was selected to save the changes.



The screenshot displays a configuration form with several fields and options. The fields are arranged vertically, with labels on the left and values on the right. The values are: Server Type: HTTPS, Real Server Type: HTTPS, Port: 443, Real Server IP: 192.168.1.87, Real Server Port: 443, and Server TLS Profile: AvayaSBCServer. There are also two unchecked checkboxes labeled 'Relay' and 'Rewrite URL' under the 'Options' section. Red rectangular boxes highlight each of these fields.

Server Type	HTTPS
Real Server Type	HTTPS
Options	<input type="checkbox"/> Relay <input type="checkbox"/> Rewrite URL
Port	443
Real Server IP	192.168.1.87
Real Server Port	443
Server TLS Profile	AvayaSBCServer

The Session Manager **Server Configuration Profile** was set to **Server\_SM**. The **End Point Signaling Interface** was set to **Ext\_Sig\_intf\_Remote\_Phone**. The **Session Policy Group** was set to **default**. The **Finish** button was selected to save the changes.



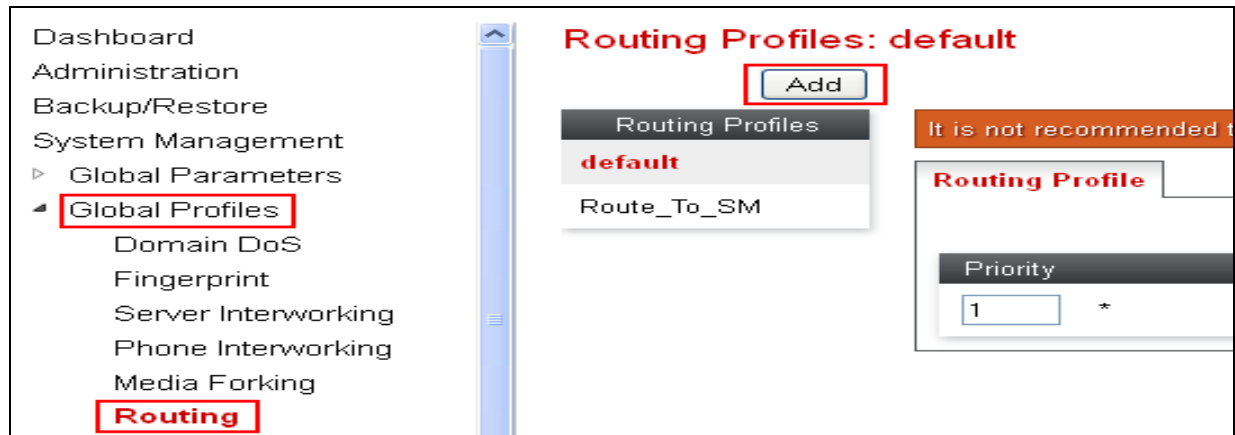
The screenshot shows the final configuration settings for the Session Manager. The fields are: Server Configuration Profile: Server\_SM, End Point Signaling Interface: Ext\_Sig\_intf\_Remote, and Session Policy Group: default. At the bottom, there are two buttons: 'Back' and 'Finish'. Red rectangular boxes highlight the labels of the three fields and the 'Finish' button.

Server Configuration Profile	Server_SM
End Point Signaling Interface	Ext_Sig_intf_Remote
Session Policy Group	default

Back Finish

## 8.15. Administer Routing Profile Toward Session Manager for Subscriber Flow

A Routing Profile is administered to the Session Manager and must be assigned to the Subscriber Flow. Select **Global Profiles**→**Routing**→**Add**.



The **Profile Name** was set to **Route\_To\_SM**. The **Next** button was selected to continue to the next page.



The **URI Group** was set to \* to indicate all URI groups were acceptable. The **Next Hop Server 1** was set to **192.168.1.87**. This was the IP Address of the Signaling Interface of the Session Manager. The **Routing Priority based on Next Hop Server** value was **Enabled**. The **Outgoing Transport** was set to **TLS**. The **Finish** button was selected to save the changes.

Routing Profile

Each URI group may only be used once per Routing Profile.

Next Hop Routing

URI Group

\*

Next Hop Server 1  
IP, IP:Port, Domain, or Domain:Port

192.168.1.87

Next Hop Server 2  
IP, IP:Port, Domain, or Domain:Port

Routing Priority based on  
Next Hop Server

☒

Use Next Hop  
for In Dialog Messages

☐

Ignore Route Header  
for Messages Outside Dialog

☐

NAPTR

☐

SRV

☐

Outgoing Transport

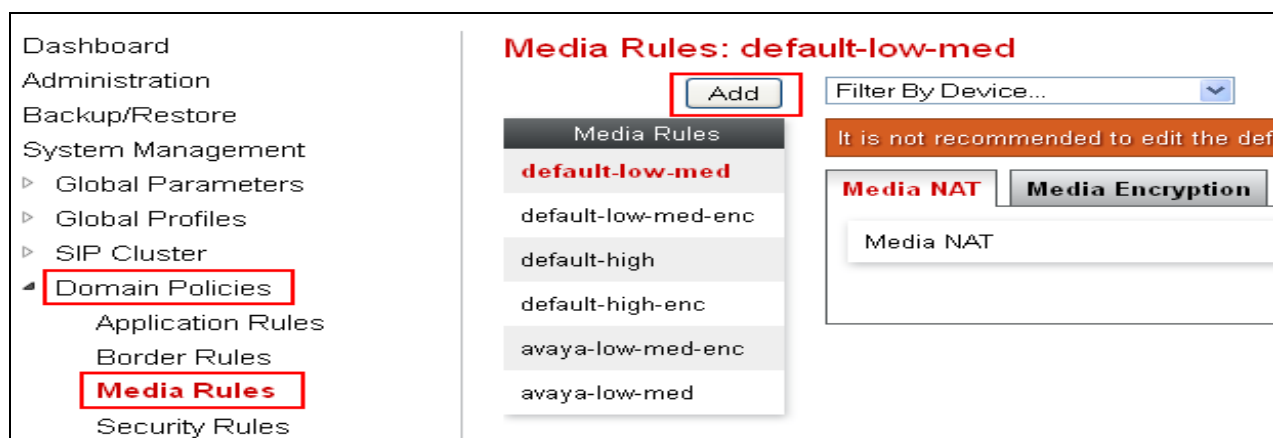
☒ TLS ☐ TCP ☐ UDP

Back

Finish

## 8.16. Administer SRTP Media Rule for the End Point Policy Group for Subscriber Flow and Server Flow

A specific Media Rule is administered and assigned to the End Point Policy Group which will be assigned to the Subscriber and Server Flows. Since the Avaya one-X Mobile SIP for iOS as a Remote User is registering to the Avaya Session Border Controller using TLS, it was decided that the Avaya one-X Mobile SIP for IOS as a Remote User would be administered to use SRTP. It was also decided that SRTP would be administered from inside interface of the Session Border controller to the Communication Manager Server. Therefore a media rule called SRTPSIP is administered with SRTP and assigned to the End Point Policy Group and then assigned to the Subscriber and Server Flows. This ensures the B1 outside interface to the Avaya one-X Mobile SIP for IOS as a Remote User will use SRTP media encryption and the A1 inside interface to the Session Manager and Communication Manager Servers will also use SRTP media encryption. To add a Media rule select **Domain Policies**→**Media Rules**→**Add**.



The **Rule Name** was set to **SIPIOS**. The **Next** button was selected to continue to the next page.

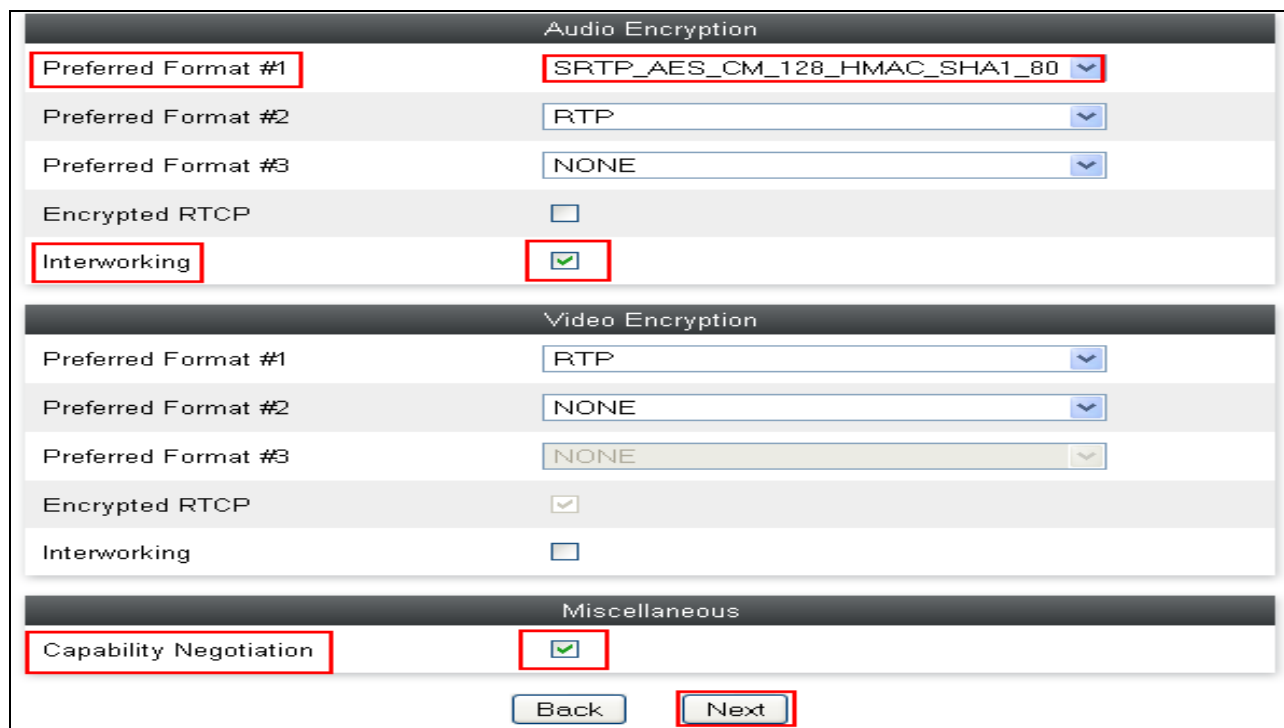


The **Media Nat** value had the **Learn Media IP dynamically** setting **Enabled**. The **Next** button was selected to continue to the next page.



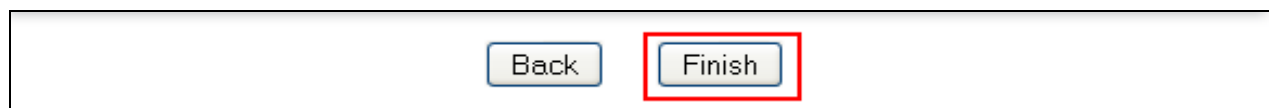
The screenshot shows a window titled "Media Rule" with a close button (X) in the top right corner. Inside the window, there is a section for "Media NAT" with two radio button options: "Enforce Signaling and Media IP correlation" (which is unselected) and "Learn Media IP dynamically" (which is selected). Below these options are two buttons: "Back" and "Next". The "Next" button is highlighted with a red rectangle.

The **Preferred Format #1** value was set to **SRTP\_AES\_CM\_128\_HMAC\_SHA1\_80**. The **Interworking** setting was **Enabled**. The **Capability Negotiation** setting was also **Enabled**. The **Next** button was selected to proceed to the next page.



The screenshot shows a configuration window with three sections: "Audio Encryption", "Video Encryption", and "Miscellaneous". In the "Audio Encryption" section, "Preferred Format #1" is set to "SRTP\_AES\_CM\_128\_HMAC\_SHA1\_80", "Preferred Format #2" is "RTP", "Preferred Format #3" is "NONE", "Encrypted RTCP" is unchecked, and "Interworking" is checked. In the "Video Encryption" section, "Preferred Format #1" is "RTP", "Preferred Format #2" is "NONE", "Preferred Format #3" is "NONE", "Encrypted RTCP" is checked, and "Interworking" is unchecked. In the "Miscellaneous" section, "Capability Negotiation" is checked. At the bottom of the window are "Back" and "Next" buttons, with the "Next" button highlighted by a red rectangle.

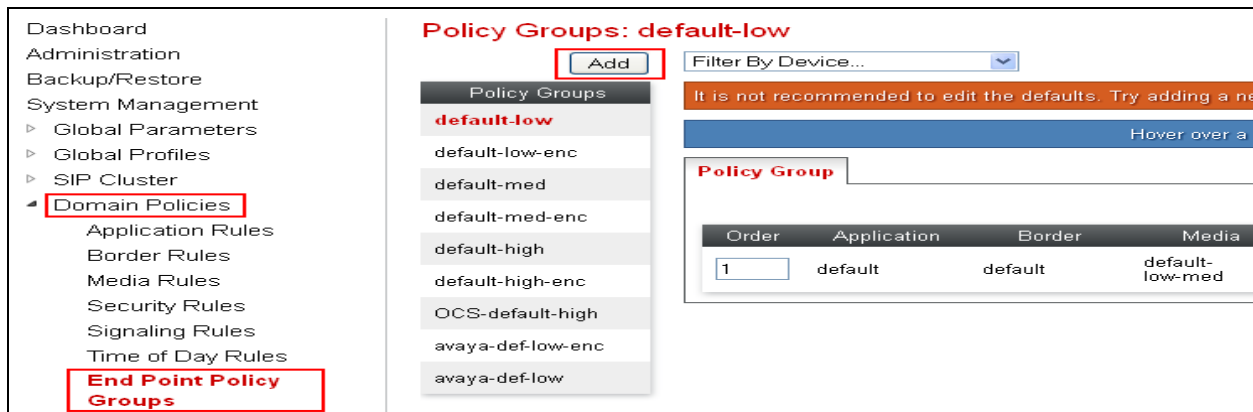
The Media Anomaly, the Media Silencing and the Media QoS settings were all disabled on the Media Rule. The **Finish** was selected to save the changes.



The screenshot shows a simple navigation bar with two buttons: "Back" and "Finish". The "Finish" button is highlighted with a red rectangle.

## 8.17. Administer End Point Policy Group for Subscriber Flow and Server Flow

An End Point Policy Group called SRTPSIPIOS was administered to be assigned to the Subscriber and Server Flow. To add an End Point Policy Group select **Domain Policies**→**End Point Policy Group**→**Add**.



The **Group Name** was set to **SRTPSIPIOS**. The **Next** button was selected to continue to the Next page.



The **Media Rule** called **SIPIOS** was assigned to the End Point Policy Group called SRTPSIPIOS. All other settings were set as default. The **Finish** button was selected to save the changes.

**Policy Group**

Application Rule: default

Border Rule: default

**Media Rule: SIPIOS**

Security Rule: default-low

Signaling Rule: default

Time of Day Rule: default

Back Finish

## 8.18. Administer End Point Flow with Subscriber Flow

The End Point Flow allows the user to determine how calls will be handled on the Session Border Controller. Select **Device Specific Settings**→**End Point Flow**→**Subscriber Flow**→**Add**.

**Subscriber Flows**

Update Add

Hover over a row to see its description

Priority	Flow Name	URI Group	Source Subnet	User Agent	End Point Policy Group				
1	Flow_Flare	URI_RTP	*	FlareCommunicator	avaya-def-low	View	Clone	Edit	Delete
2	Flow_ADVD	URI_RTP	*	Avaya A175	avaya-def-low	View	Clone	Edit	Delete
3	Flow_SIPIOS	URI_RTP	*	1XC SIP IOS	avaya-def-low	View	Clone	Edit	Delete
4	Flow_Remote	*	*	*	avaya-def-low-enc	View	Clone	Edit	Delete

The **Flow Name** was set to **SIPIOS**. The **URI Group** was set to \*. The **User Agent** was set to **SIPIOS**. The **Signaling Interface** was set to **Ext\_Sig\_intf\_Remote\_Phone**. The **Next** button was selected to continue to the next page.

Criteria	
Flow Name	SIPIOS
URI Group	*
User Agent	SIPIOS
Source Subnet Ex: 192.168.0.1/24	*
Via Host Ex: domain.com, 192.168.0.1/24	*
Contact Host Ex: domain.com, 192.168.0.1/24	*
Signaling Interface	Ext_Sig_Intf_Remote
Next	

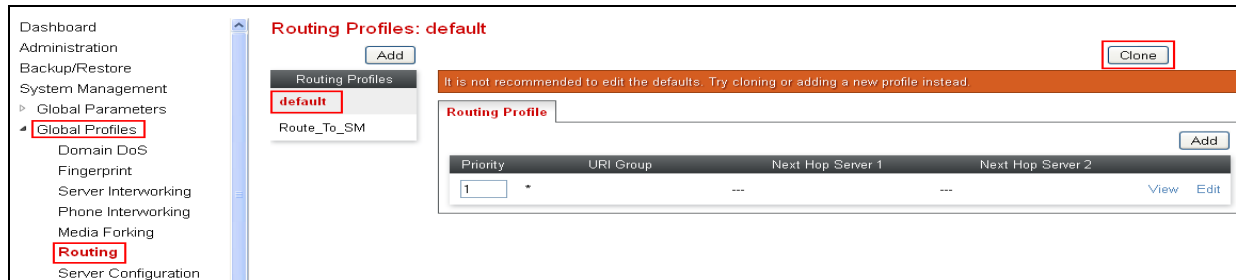


The **Media Interface** was set to **Ext\_Med\_intf\_Remote\_Phone**. The **End Point Policy Group** was set to **SRTPSIPIOS**. The **Routing Profile** was set to **Route\_To\_SM**. The **Topology Hiding Profile** was set to **defaultSIPIOS**. The **Phone Interworking Profile** was set to **Avaya\_RuSIPIOS**. The **TLS Client Profile** was set to **AvayaSBCCClient**. The **Finish** button was selected to save the changes.

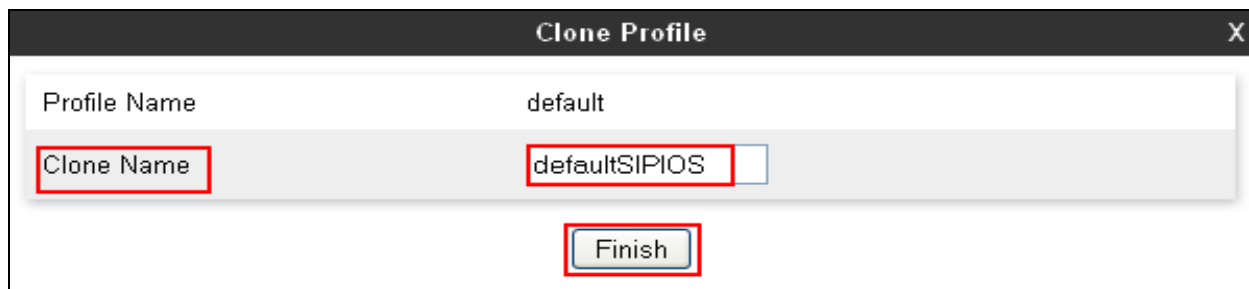
Source	<input checked="" type="radio"/> Subscriber <input type="radio"/> Click To Call
Methods Allowed Before REGISTER	INFO MESSAGE NOTIFY OPTIONS
Media Interface	Ext_Med_Intf_Remote
End Point Policy Group	SRTPSIPIOS
SIP Cluster Flow	<input type="checkbox"/>
Routing Profile	Route_To_SM
Optional Settings	
Topology Hiding Profile	defaultSIPIOS
Phone Interworking Profile	Avaya-RuSIPIOS
TLS Client Profile	AvayaSBCCClient
File Transfer Profile	None
Signaling Manipulation Script	None
<input type="button" value="Back"/> <input type="button" value="Finish"/>	

## 8.19. Administer Routing Profile Toward Remote User for Server Flow

A Routing Profile is administered to the Remote User and must be assigned to the Server Flow. It was decided to use an existing Routing Profile called **default** and clone this Routing Profile. To clone the Routing Profile select **Global Profiles**→**Routing**→**default**→**Clone**.



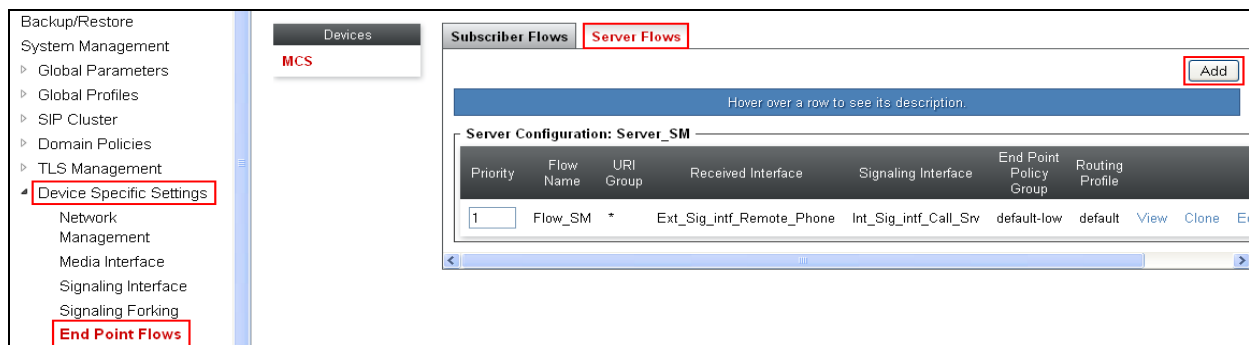
The **Profile Name** selected was **default**. The **Clone Name** was set to **defaultSIPIOS**. The **Finish** button was selected to save the changes.



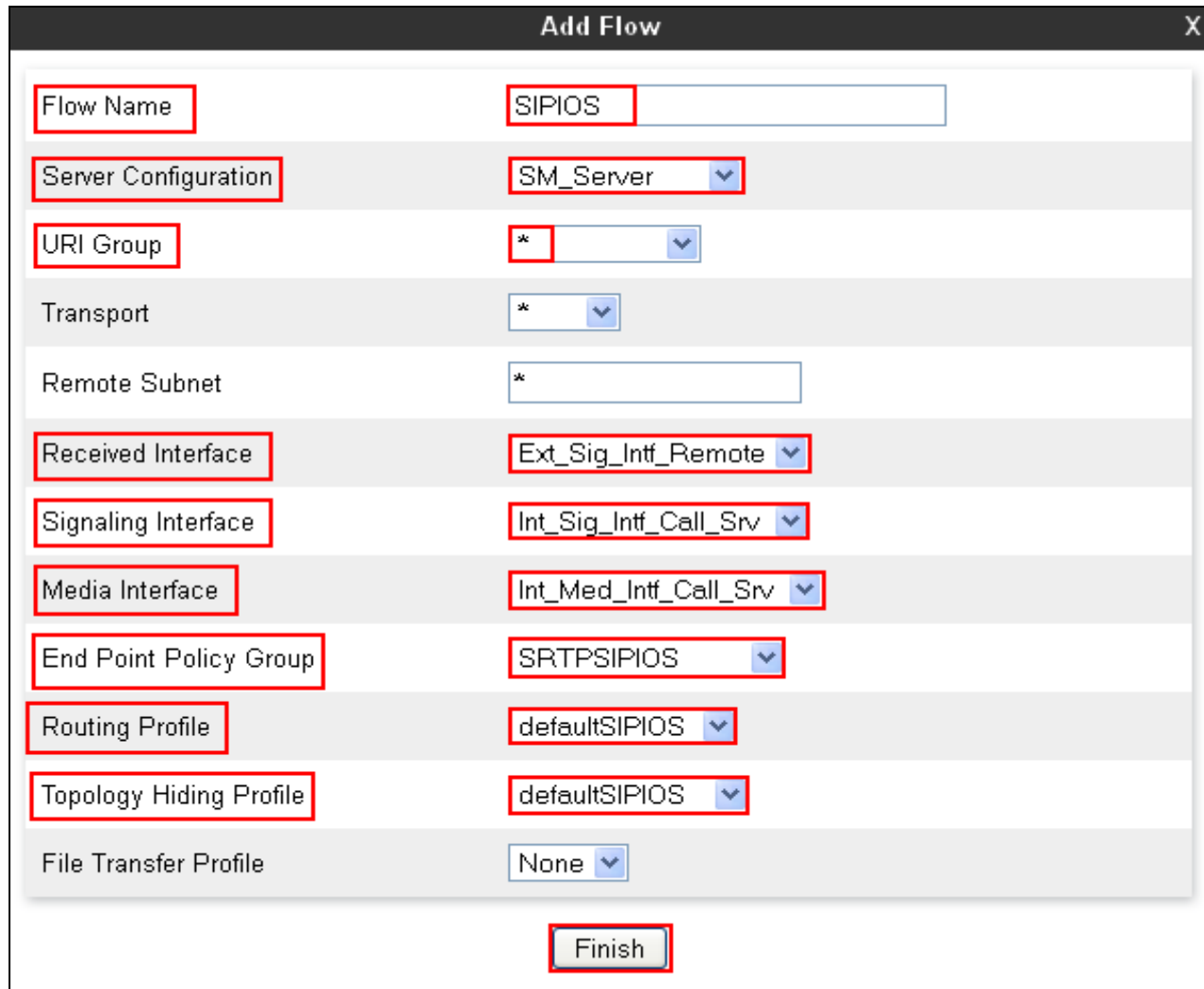
All values for the Routing Profile were left as default.

## 8.20. Administer End Point Flow with Server Flow

To administer the Server Flow to the End Point Flow select **Device Specific Settings**→**End Point Flow**→**Server Flow**→**Add**.



The **Flow Name** was set to **SIPIOS**. The **Server Configuration** was set to **Server\_SM**. The **URI Group** was set to **\***. The **Received Interface** was set to **Ext\_Sig\_intf\_Remote\_Phone**. The **Signaling Interface** was set to **Int\_sig\_intf\_Call\_Srv**. The **Media Interface** was set to **Int\_Med\_intf\_Call\_Srv**. The **End Point Policy Group** was set to **SRTPSIPIOS**. The **Routing Policy** was set to **defaultSIPIOS**. The **Topology Hiding Profile** was set to **defaultSIPIOS**. The **Finish** button was selected to save the changes.



The screenshot shows a window titled "Add Flow" with a close button (X) in the top right corner. The window contains a list of configuration fields, each with a label on the left and a value or dropdown on the right. Red rectangular boxes highlight the labels and the corresponding value areas for the following fields: Flow Name, Server Configuration, URI Group, Received Interface, Signaling Interface, Media Interface, End Point Policy Group, Routing Profile, Topology Hiding Profile, and the Finish button. The "Transport" field is also present but not highlighted. The values are: Flow Name: SIPIOS; Server Configuration: SM\_Server; URI Group: \*; Transport: \*; Remote Subnet: \*; Received Interface: Ext\_Sig\_Intf\_Remote; Signaling Interface: Int\_Sig\_Intf\_Call\_Srv; Media Interface: Int\_Med\_Intf\_Call\_Srv; End Point Policy Group: SRTPSIPIOS; Routing Profile: defaultSIPIOS; Topology Hiding Profile: defaultSIPIOS; File Transfer Profile: None.

Field	Value
Flow Name	SIPIOS
Server Configuration	SM_Server
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Ext_Sig_Intf_Remote
Signaling Interface	Int_Sig_Intf_Call_Srv
Media Interface	Int_Med_Intf_Call_Srv
End Point Policy Group	SRTPSIPIOS
Routing Profile	defaultSIPIOS
Topology Hiding Profile	defaultSIPIOS
File Transfer Profile	None

Finish

## 9. Administer Avaya one-X® Mobile SIP for IOS

This section highlights the important commands for administering Avaya one-X® Mobile SIP for IOS to set up a sip account and register to the Session Border Controller Advanced for Enterprise Server. It also describes configuring the Avaya one-X® Mobile SIP for IOS to connect to the SILsecure\$ wireless network. This Application Notes assumes that the Avaya one-X® Mobile SIP for IOS App has already been downloaded to an iPhone 4S handset.

### 9.1. Access Wireless Network

Access the **Settings** heading on the iPhone4S handset.



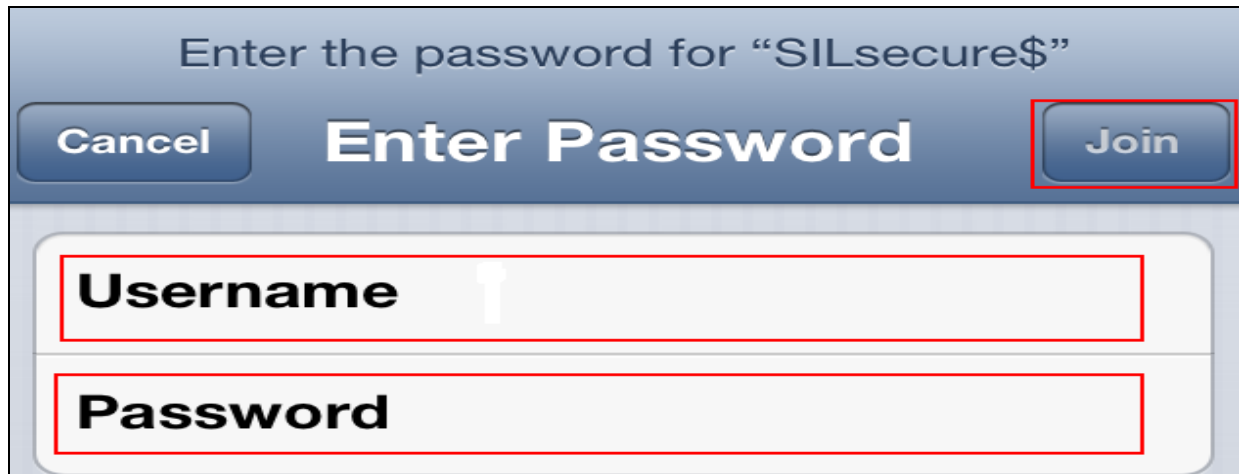
Under the **Wi-Fi Networks** and select the **Choose a Network** heading.



The **SILsecure\$** wireless network was selected.

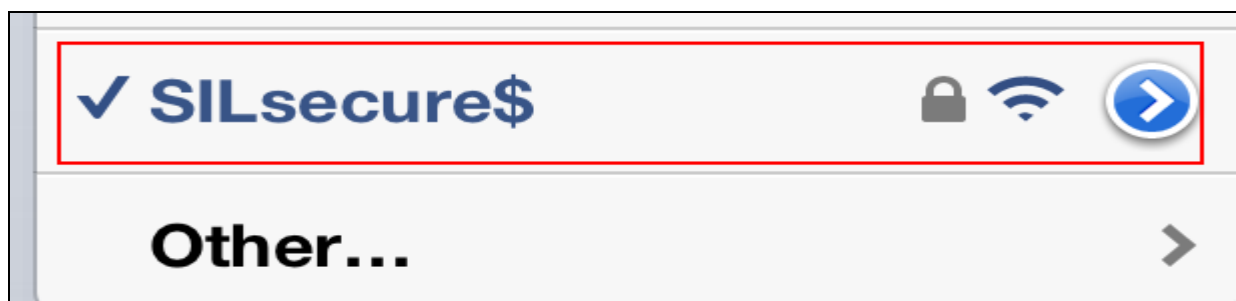


The **Username** and **Password** was entered and the **Join** button was selected.



The screenshot shows a dialog box titled "Enter the password for 'SILsecure\$'". It has a blue header bar with a "Cancel" button on the left, the title "Enter Password" in the center, and a "Join" button on the right. Below the header, there are two input fields: "Username" and "Password". Both fields are outlined with a red border. The "Join" button is also outlined with a red border.

The Avaya one-X Mobile SIP for IOS had joined the **SILsecure\$** wireless network.



## 9.2. Administering Avaya one-X® Mobile SIP Communicator for iOS

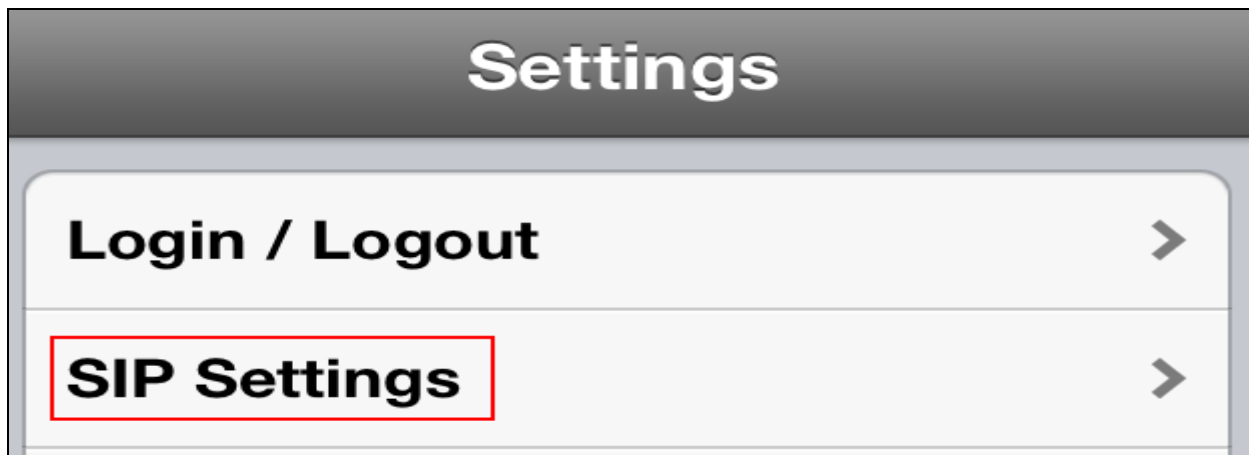
It is assumed that the Avaya one-X® Mobile SIP for IOS has already been downloaded to an iPhone 4S handset. Select the Avaya one-X® Mobile SIP for IOS heading on the iPhone 4S.



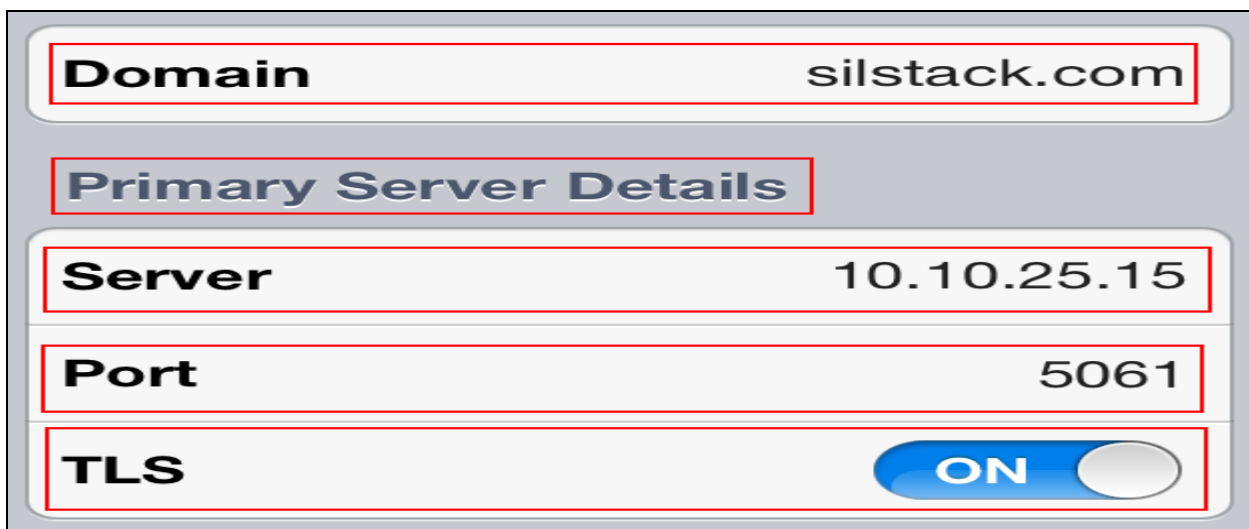
Select the **Settings** heading at the bottom of the screen.



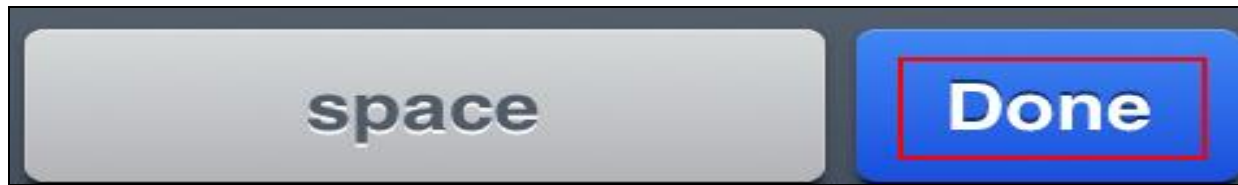
Select the heading **SIP Settings**.



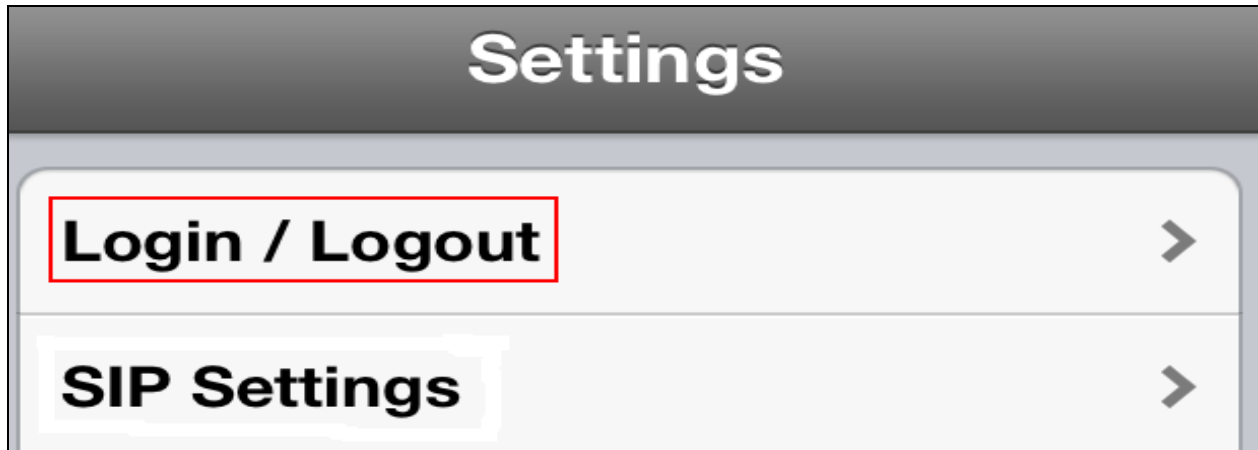
The **Domain** was set to **silstack.com**. Under the **Primary Server Details** the **Server** was set to **10.10.25.15**. The **Port** was set to **5061** and the protocol was set to **TLS**.



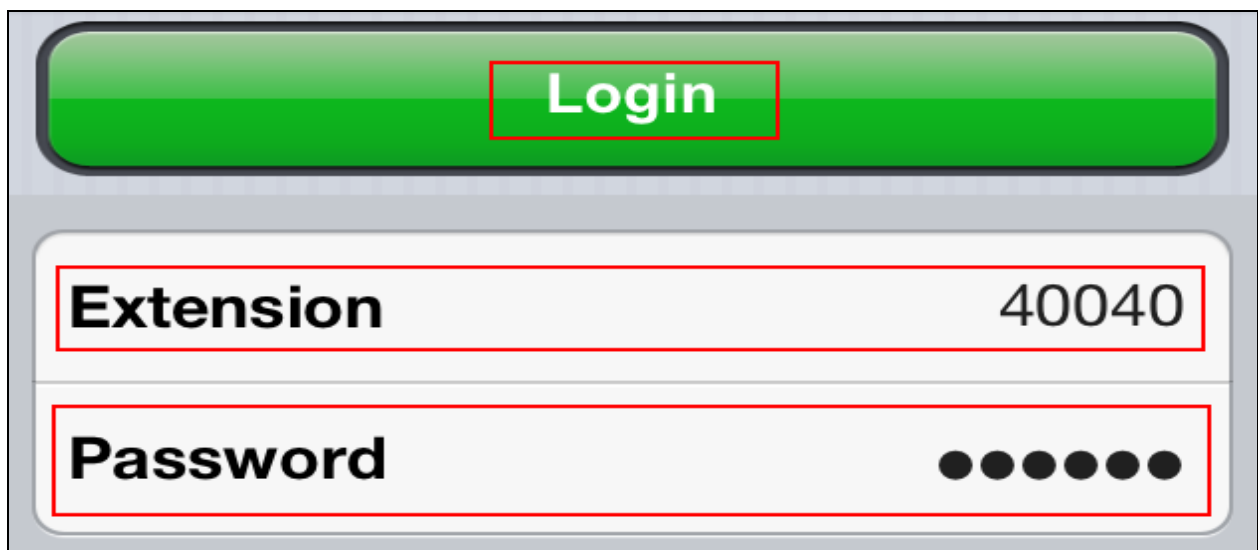
The **Done** button was selected.



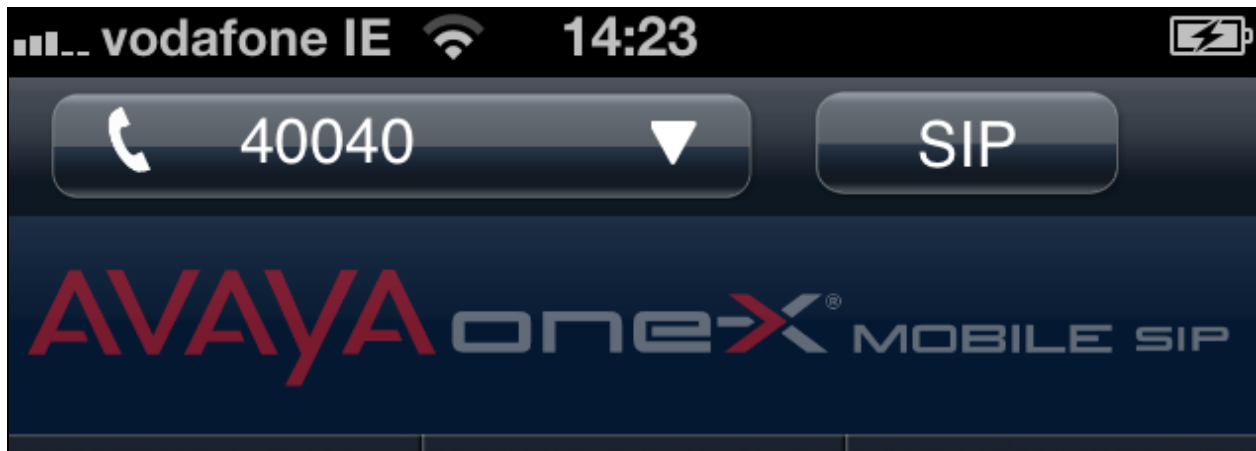
The **Login / Logout** heading was selected.



The **Extension** was set to **40040** and the **Password** was set. The **Login** button was selected.



The Avaya one-X Mobile SIP for IOS was seen to register to the Session Border Controller Server.



## 10. Verification Steps

The following six verification steps were tested using the sample configuration. The following steps can be used to verify installation in the field.

1. Verified the Avaya one-X Mobile SIP for IOS as a Remote User with SRTP obtained an IP Address from the SILsecure\$ wireless network.
2. Verified the Avaya one-X Mobile SIP for IOS as a Remote User with SRTP was registered to the Avaya Session Border Controller Advanced for Enterprise Server.
3. Verified the Avaya one-X Mobile SIP for IOS as a Remote User with SRTP registered to the Avaya Session Border Controller Advanced for Enterprise Server was seen to use SRTP from the Remote User to the outside interface of the Avaya Session Border Controller Advanced for Enterprise Server.
4. Verified the Avaya one-X Mobile SIP for IOS as a Remote User with SRTP registered to the Avaya Session Border Controller Advanced for Enterprise Server was seen to use SRTP from the inside interface of the Avaya Session Border Controller Advanced for Enterprise Server to the Avaya Communication Manager Server.
5. Verified that a message could be left on the Avaya one-X Mobile SIP for IOS as a Remote User with SRTP registered to the Avaya Session Border Controller Advanced for Enterprise Server and that the MWI was seen to function correctly for Basic Messaging.
6. Verified the PPM button information was seen on the Avaya one-X Mobile SIP for IOS as a Remote User with SRTP registered to the Avaya Session Border Controller Advanced for Enterprise Server.



Verified the Avaya one-X Mobile SIP for IOS as a Remote User with SRTP obtained an IP Address from the SILsecure\$ wireless network.

**Wi-Fi** **SILsecure\$**

**Forget this Network**

**IP Address**

**DHCP** **BootP** **Static**

**IP Address** 10.10.24.34

**Subnet Mask** 255.255.255.0

Verified that **extension 40040** was seen to register to the Avaya Session Border Controller Advanced for Enterprise Server.

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

User Registrations

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

AST Device Notifications:

Reboot

Reload

Failback

As of 3:27 PM

22 Items

Refresh

Show 15

Filter: Enable

<input type="checkbox"/>	Details	Address	Login Name	First Name	Last Name	Location	IP Address	AST Device	<div>Reboot</div>
<input type="checkbox"/>	► Show	---	40071@silstack.com	R3	40071	Galway Stack	---	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	► Show	---	40030@silstack.com	40030	40030	Galway Stack	---	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	► Show	---	40072@silstack.com	R3	40072	Galway Stack	---	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	► Show	40040@silstack.com	40040@silstack.com	40040	40040	Galway Stack	192.168.1.16:5061	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)
<input type="checkbox"/>	► Show	---	40031@silstack.com	E2	40031	Galway Stack	---	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	► Show	---	40073@silstack.com	R4	40073	Galway Stack	---	<input type="checkbox"/>	<input type="checkbox"/>

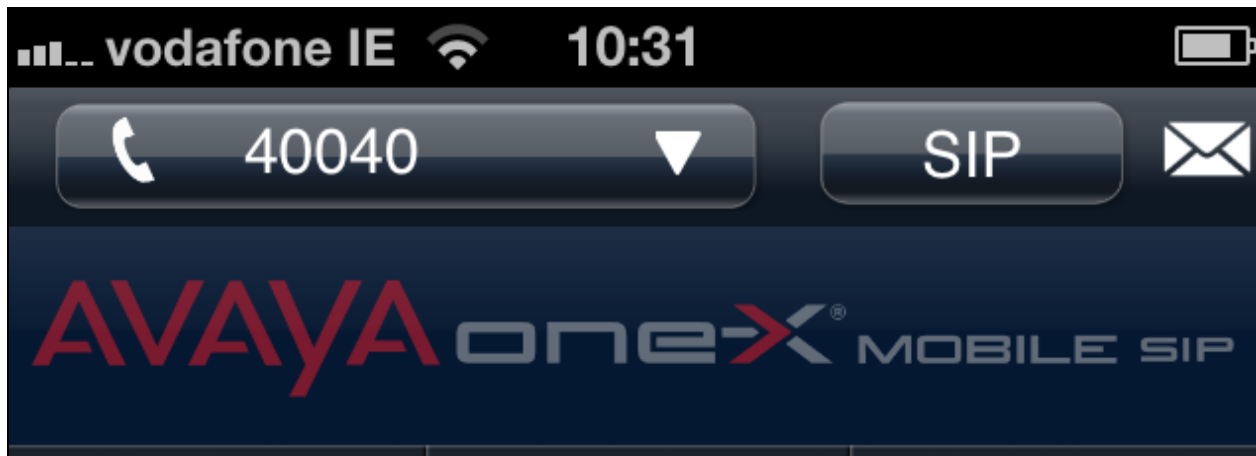
Verified the Avaya one-X Mobile SIP for IOS as a Remote User with SRTP registered to the Avaya Session Border Controller Advanced for Enterprise Server was seen to use SRTP from the Remote User to the outside interface IP Address 10.10.25.15 of the Avaya Session Border Controller Server.

Time	10.10.24.34	10.10.25.15	10.10.24.30	Comment
58.671	(49172)	INVITE	(5061)	SIP From: <sips:40040@silstack.com To:<sips:40040@silstack.com;avaya-cm-fnu=off-hook
58.673	(49172)	100 Trying	(5061)	SIP Status
58.716	(49172)	183 Session Progress	(5061)	SIP Status
59.990	(49172)	100 Trying	(5061)	SIP Status
60.005	(49172)	484 Address Incomplete	(5061)	SIP Status
60.067	(49172)	INVITE SDP (ISACRTPType-103 q722 g711U g722)	(49207)	SIP From: "40040, 40040" <sips:40040@10.10.25.15:5061 To:<sips:40070@10.10.25.15:5061
60.193	(5061)	100 Trying	(49207)	SIP Status
60.426	(5061)	180 Ringing	(49207)	SIP Status
60.451	(49172)	180 Ringing	(5061)	SIP Status
61.567	(49172)	180 Ringing SDP ()	(5061)	SIP Status
61.615	(9580)	SRTP (q711U)	(35296)	SRTP Num packets:17 Duration:0.320s SSRC:0x27DE0B7C
62.931	(9580)	SRTP (q711U)	(35296)	SRTP Num packets:23 Duration:0.441s SSRC:0x7524A92B
63.364	(5061)	200 OK SDP ()	(49207)	SIP Status
63.456	(49172)	200 OK SDP ()	(5061)	SIP Status
63.533	(9580)	SRTP (q711U)	(35296)	SRTP Num packets:25 Duration:0.465s SSRC:0x7524A92B
63.533	(35282)	SRTP (q711U)	(48666)	SRTP Num packets:24 Duration:0.321s SSRC:0x7524A92B
63.766	(5061)	ACK	(49207)	SIP Request
64.129	(35282)	SRTP (ISAC)	(48666)	SRTP Num packets:54 Duration:3.147s SSRC:0x8CF97D2B
64.129	(9580)	SRTP (ISAC)	(35296)	SRTP Num packets:51 Duration:2.971s SSRC:0x8CF97D2B
65.025	(9580)	SRTP (ISAC)	(35296)	SRTP Num packets:35 Duration:2.096s SSRC:0x90CD2663
65.025	(35282)	SRTP (ISAC)	(48666)	SRTP Num packets:37 Duration:2.208s SSRC:0x90CD2663
67.089	(49172)	100 Trying	(5061)	SIP Status
67.122	(49172)	200 OK SDP ()	(5061)	SIP Status
67.156	(9580)	SRTP (ISAC)	(35296)	SRTP Num packets:4 Duration:0.182s SSRC:0x8CF97D2B
67.168	(5061)	INVITE	(49207)	SIP From: "40040, 40040" <sips:40040@10.10.25.15:5061 To:<sips:40070@10.10.25.15:5061
67.181	(9580)	SRTP (ISAC)	(35296)	SRTP Num packets:2 Duration:0.052s SSRC:0x90CD2663
67.244	(5061)	100 Trying	(49207)	SIP Status
67.298	(5061)	200 OK SDP (ISACRTPType-103 q722 g711U g722)	(49207)	SIP Status

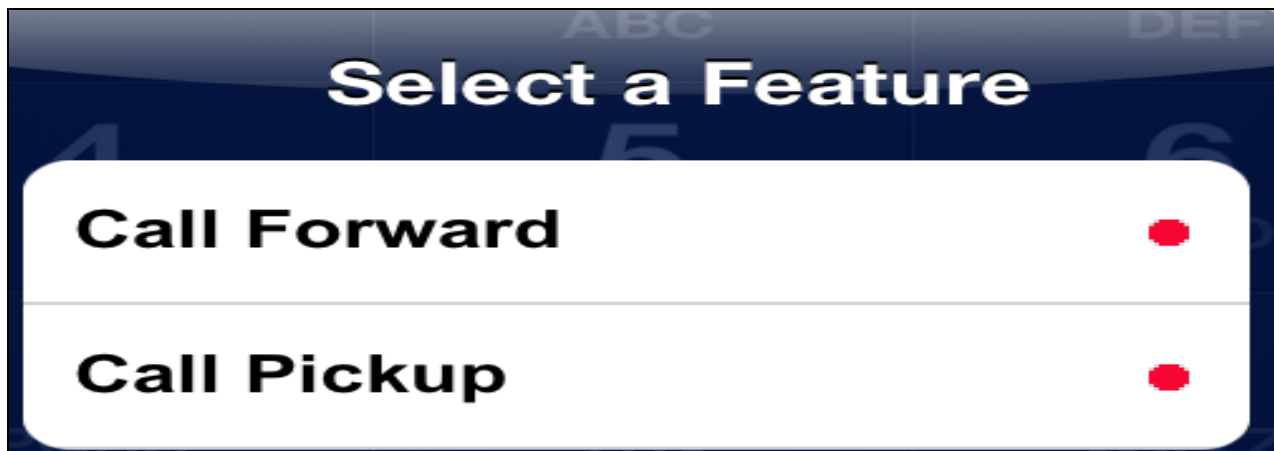
Verified the Avaya one-X Mobile SIP for IOS as a Remote User with SRTP registered to the Avaya Session Border Controller Advanced for Enterprise Server was seen to use SRTP from the inside interface IP Address 192.168.1.16 of the Avaya Session Border Controller Server to the Avaya Communication Manager Server.

status trunk 120/113	Page 3 of 3
SRC PORT TO DEST PORT TALKPATH	
src port: T00155	
T00155:TX:192.168.1.16:35134/g722-64/20ms/1-srtp-aescm128-hmac80	
T00291:RX:192.168.1.16:35132/g722-64/20ms/1-srtp-aescm128-hmac80	

Verified that a message could be left on the Avaya one-X Mobile SIP for IOS as a Remote User with SRTP registered to the Avaya Session Border Controller Advanced for Enterprise Server and that the MWI was seen to function correctly for Basic Messaging.



Verified the PPM button information was seen on the Avaya one-X Mobile SIP for IOS as a Remote User with SRTP registered to the Avaya Session Border Controller Advanced for Enterprise Server.



## 11. Conclusion

These Application Notes describe the configuration steps required to register the Avaya one-X® Mobile SIP for IOS as a Remote User with SRTP to the Avaya Session Border Controller Advanced for Enterprise Server with Avaya Aura® Solution for Midsize Enterprise Server and Avaya Aura® Messaging Server. These Application Notes also identify how to configure SRTP from the Avaya one-X® Mobile SIP for IOS as a Remote User to the outside interface of the Avaya Session Border Controller Advanced for Enterprise Server and configure SRTP from the inside interface of the Avaya Session Border Controller Advanced for Enterprise Server to the Avaya Aura® Solution for Midsize Enterprise Server and Avaya Aura® Messaging Server.

These Application Notes also describe how to administer Avaya Aura® Messaging Server to function with SRTP with the Avaya one-X® Mobile SIP for IOS as a Remote User with the Avaya Session Border Controller Advanced for Enterprise Server. Please refer to **Section 2.1.4** for the observations associated with Avaya one-X Mobile SIP for IOS as a Remote User with SRTP registered to the Avaya Session Border Controller Advanced for Enterprise Server.

## 12. Additional References

This section references Avaya documentation relevant to these Application Notes. Additional Avaya product documentation is available at <http://support.avaya.com>.

- [1] Administering Avaya Session Border Controller for Enterprise, January 2013, Release 6.2, Issue 2.
- [2] Administering Avaya one-X® Mobile SIP for IOS, November 2012, Release 6.2, Issue 1.
- [3] Administering Avaya Aura® System Manager, July 2012 Issue 2.0
- [4] Administering Avaya Aura® Session Manager, February 2012, Document Number 03-603324
- [5] Administering Avaya Aura® Communication Manager, February 2012, Document Number 03-603479
- [6] Administering Avaya Aura® Messaging, December 2011

---

**©2014 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 Solution & Interoperability Test Lab at [interoplabinotes@list.avaya.com](mailto:interoplabinotes@list.avaya.com)