



# **Application Notes for Snom M900 Multicell DECT Phones with Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and Avaya Session Border Controller for Enterprise - Issue 1.0**

## **Abstract**

These Application Notes describe the configuration steps required to integrate Snom M900 Multicell DECT Phones with Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and Avaya Session Border Controller for Enterprise. The Snom M900 Multicell Base Station was connected to the LAN which, in turn, registered M-series DECT phones directly to Avaya Aura® Session Manager via SIP. In addition, the Snom M900 Multicell Base Station was also connected to the internet which, in turn, registered M-series DECT phones to Avaya Aura® Session Manager through Avaya Session Border Controller for Enterprise as SIP Remote Workers. The base station converts IP protocol to DECT protocol and transmits phone calls to and from the M-series DECT phones. For the compliance test, the Snom M65 DECT Handsets were used.

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

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

## 1. Introduction

These Application Notes describe the configuration steps required to integrate Snom M900 Multicell DECT Phones with Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and Avaya Session Border Controller for Enterprise (SBCE). The Snom M900 Multicell Base Station was connected to the LAN which, in turn, registered M-series DECT phones directly to Avaya Aura® Session Manager via SIP. In addition, the Snom M900 Multicell Base Station was also connected to the internet which, in turn, registered M-series DECT phones to Avaya Aura® Session Manager through Avaya Session Border Controller for Enterprise as SIP Remote Workers. The base station converts IP protocol to DECT protocol and transmits phone calls to and from the M-series DECT phones.

For the compliance test, the Snom M65 DECT Handsets were used. There are other DECT M-Series handsets that share the same firmware version as the Snom M65 DECT Handset, and therefore the testing also applies to them. See Attachment 1 for additional details.

## 2. General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing. The feature testing focused on establishing calls between Snom M65 DECT Handsets and Avaya SIP/H.323 deskphones and exercising basic telephony features, such as hold, mute, and transfer. The M65 handsets gained network access via the M900 base station. Additional telephony features, such as call forward, call park/unpark, and call pickup were also verified using Communication Manager Features Access Codes (FACs).

The serviceability testing focused on verifying that the Snom M900 Multicell Base Station came back into service after re-connecting the Ethernet or rebooting the Snom M65 DECT Handsets.

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

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with this Application Note, the interface between Avaya systems and Snom M900 Multicell DECT Phones utilized enabled capabilities of TLS/SRTP.

## 2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- SIP registration of M65 DECT handsets with Session Manager in the enterprise.
- SIP registration of M65 DECT handsets with Session Manager through SBCE as remote workers.
- Calls between M65 DECT handsets and Avaya SIP/H.323 deskphones with Direct IP Media (Shuffling) enabled and disabled.
- Calls between M65 DECT handsets and the PSTN.
- Calls with TLS/SRTP enabled.
- TLS using secure PFS cipher of TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384.
- Support of G.711 and G.722 codecs.
- Proper recognition of DTMF tones.
- Basic telephony features, including hold, mute, redial, multiple calls, blind/attended transfer, conference, and long duration calls.
- Extended telephony features using Communication Manager FACs for Call Forward, Call Unpark, and Call Pickup.
- Proper system recovery after a restart of M900 and M65 DECT handsets.

## 2.2. Test Results

All test cases passed with the following observation noted:

- Currently, the Snom M900 Multicell Base Station doesn't support TLS authentication with a Subject Alternate Name (SAN) in the certificate. Therefore, the M900 was configured to accept all certificates by disabling the **Use Only Trusted Certificates** option under **Security** in the M900 configuration as described in **Section 0**.
- When Snom M900 Multicell DECT Phones are used as remote workers with Avaya SBCE, Capability Negotiation must be disabled in Avaya SBCE Media Rule, as described in **Section 8.3**, to avoid one-way audio after a Session Refresh is sent to the remote worker during an active call.

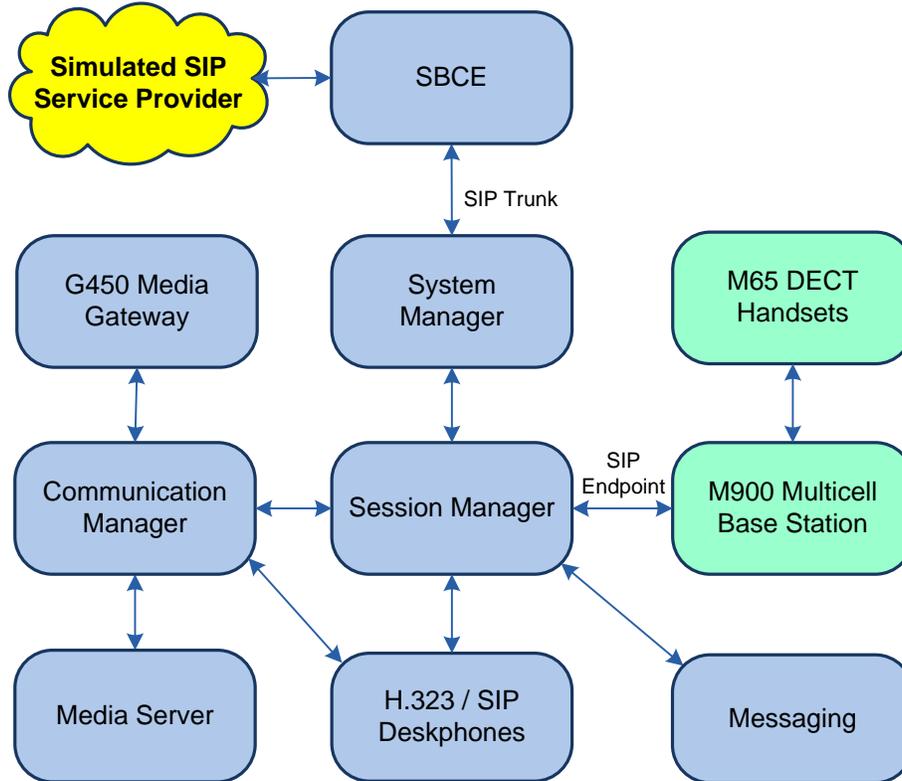
## 2.3. Support

For technical support on the Snom M900 Multicell DECT Phones, contact Snom Support via phone, email, or website.

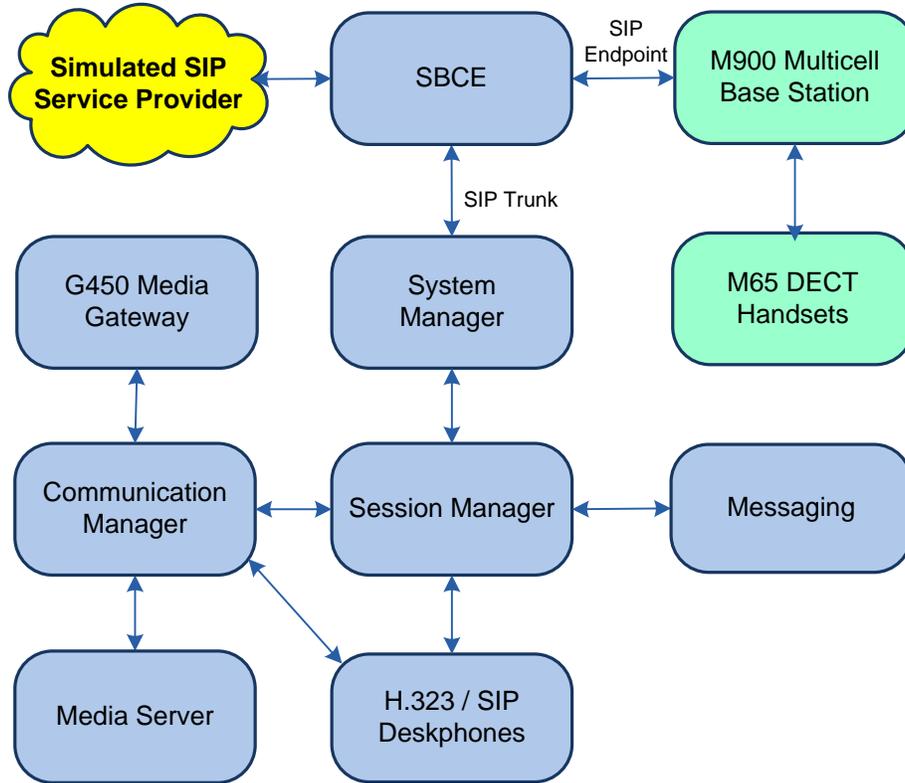
- **Phone:** +1 (339) 227-6160 Option 2
- **Web:** <https://service.snom.com>
- **Email:** [supportusa@snom.com](mailto:supportusa@snom.com)

### 3. Reference Configuration

The following diagrams illustrate sample configurations consisting of Snom M900 Multicell Base Station and Snom M65 DECT Handsets with Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and Avaya Session Border Controller for Enterprise. In **Figure 1**, the M900 registered the M65 DECT handsets directly with Session Manager. In **Figure 2**, the M900 registered the M65 DECT handsets to Session Manager through SBCE as remote workers.



**Figure 1: Snom M900 Multicell DECT Phones Registered Directly to Avaya Aura® Session Manager**



**Figure 2: Snom M900 Multicell DECT Phones Registered to Avaya Aura® Session Manager as Remote Workers**

## 4. Equipment and Software Validated

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

<b>Equipment/Software</b>	<b>Release/Version</b>
Avaya Aura® Communication Manager	8.1.3.2.0-FP3SP2
Avaya G450 Media Gateway	FW 41.24.0
Avaya Aura® Media Server	v.8.0.2.138
Avaya Aura® System Manager	8.1.3.1 Build No. – 8.1.0.0.733078 Software Update Revision No: 8.1.3.1.1012493 Service Pack 1
Avaya Aura® Session Manager	8.1.3.1.813113
Avaya Messaging	10.8 SP1 SU3
Avaya Session Border Controller for Enterprise	8.1.2.0-31-19809
Avaya 96x1 Series IP Deskphones	6.8502 (H.323) 7.1.13.0.4 (SIP)
Avaya J100 Series IP Deskphones	4.0.9.0.4 (SIP)
Snom M900 Multicell Base Station	05.30/B0002
Snom M65 DECT Handsets	05.30/B0002

## 5. Configure Avaya Aura® Communication Manager

This section provides the procedure for configuring Communication Manager. The procedure includes the following areas:

- Verify Communication Manager License
- Administer IP Node Names
- Administer IP Network Region and IP Codec Set
- Administer SIP Trunk Group to Session Manager
- Administer AAR Call Routing

Use the System Access Terminal (SAT) to configure Communication Manager and log in with appropriate credentials.

**Note:** It is assumed that basic configuration, such as voicemail coverage, has already been configured. The SIP station configuration for the Snom M900 Multicell DECT Phones is performed through Avaya Aura® System Manager in **Section 6.2**.

### 5.1. Verify Communication Manager License

Using the SAT, verify that the Off-PBX Telephones (OPS) option is enabled on the **system-parameters customer-options** form. The license file installed on the system controls these options. If a required feature is not enabled, contact an authorized Avaya sales representative.

On **Page 1**, verify that the number of OPS stations allowed in the system is sufficient for the number of SIP endpoints that will be deployed.

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

G3 Version: V18                                     Software Package: Enterprise
Location: 2                                         System ID (SID): 1
Platform: 28                                       Module ID (MID): 1

                                                USED
Platform Maximum Ports: 48000                       1309
Maximum Stations: 36000                             36
Maximum XMOBILE Stations: 36000                     0
Maximum Off-PBX Telephones - EC500: 41000           0
Maximum Off-PBX Telephones - OPS: 41000           22
Maximum Off-PBX Telephones - PBFMC: 41000           0
Maximum Off-PBX Telephones - PVFMC: 41000           0
Maximum Off-PBX Telephones - SCCAN: 0                0
Maximum Survivable Processors: 313                   0

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

On Page 5, verify that the **Media Encryption Over IP** option is enabled.

```
change system-parameters customer-options                               Page 5 of 12
                                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                                   Media Encryption Over IP? y
  Five Port Networks Max Per MCC? n                               Mode Code for Centralized Voice Mail? n
    Flexible Billing? y
  Forced Entry of Account Codes? y                                 Multifrequency Signaling? y
  Global Call Classification? y                                   Multimedia Call Handling (Basic)? y
    Hospitality (Basic)? y                                       Multimedia Call Handling (Enhanced)? y
  Hospitality (G3V3 Enhancements)? y                             Multimedia IP SIP Trunking? y
    IP Trunks? y

IP Attendant Consoles? y
(NOTE: You must logoff & login to effect the permission changes.)
```

## 5.2. Administer IP Node Names

In the **IP Node Names** form, assign an IP address and host name for Communication Manager (*procr*) and Session Manager (*devcon-sm*). The host names will be used in other configuration screens of Communication Manager.

```
change node-names ip                                               Page 1 of 2
                                IP NODE NAMES

Name          IP Address
default       0.0.0.0
devcon-aes    10.64.102.119
devcon-ams    10.64.102.118
devcon-sm    10.64.102.117
procr       10.64.102.115
procr6        ::

( 6 of 6 administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

### 5.3. Administer IP Network Region and IP Codec Set

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is *avaya.com*. By default, **IP-IP Direct Audio** (shuffling) is enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in Avaya G450 Media Gateway or Avaya Aura® Media Server. The **IP Network Region** form also specifies the **IP Codec Set** to be used for calls routed over the SIP trunk to Session Manager.

```

change ip-network-region 1                                     Page 1 of 20
                                                           IP NETWORK REGION
  Region: 1          NR Group: 1
Location: 1        Authoritative Domain: avaya.com
  Name:              Stub Network Region: n
MEDIA PARAMETERS      Intra-region IP-IP Direct Audio: yes
  Codec Set: 1      Inter-region IP-IP Direct Audio: yes
  UDP Port Min: 2048          IP Audio Hairpinning? n
  UDP Port Max: 50999
DIFFSERV/TOS PARAMETERS
  Call Control PHB Value: 46
  Audio PHB Value: 46
  Video PHB Value: 26
802.1P/Q PARAMETERS
  Call Control 802.1p Priority: 6
  Audio 802.1p Priority: 6
  Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS      RSVP Enabled? n
  H.323 Link Bounce Recovery? y
  Idle Traffic Interval (sec): 20
  Keep-Alive Interval (sec): 5
  Keep-Alive Count: 5
  
```

In the **IP Codec Set** form, select the audio codec type supported for calls routed over the SIP trunk to the M900. The form is accessed via the **change ip-codec-set 1** command. Note that IP codec set '1' was specified in IP Network Region '1' shown above. The default settings of the **IP Codec Set** form are shown below. The M900 was tested using G.711 and G.722 codecs. Specify the desired codecs in the **IP Codec Set** form as per customer requirements.

```

change ip-codec-set 1                                     Page 1 of 2
                                                           IP CODEC SET
  Codec Set: 1
  Audio      Silence      Frames      Packet
  Codec      Suppression    Per Pkt    Size (ms)
1: G.711MU      n          2          20
2:
3:
  
```

To enable SRTP, include set *1-srtp-aescm128-hmac80* and *2-srtp-aescm128-hmac32*, and *none* under **Media Encryption**. The *none* setting allows calls with IP endpoints that don't support media encryption to be supported.

<b>Media Encryption</b>	<b>Encrypted SRTCP: best-effort</b>
1: 1-srtp-aescm128-hmac80	
2: 2-srtp-aescm128-hmac32	
3: none	

## 5.4. Administer SIP Trunk to Session Manager

Prior to configuring a SIP trunk group for communication with Session Manager, a SIP signaling group must be configured. Configure the **Signaling Group** form as follows:

- Set the **Group Type** field to *sip*.
- Set the **IMS Enabled** field to *n*.
- The **Transport Method** field was set to *tls*.
- Specify Communication Manager (*procr*) and the Session Manager as the two ends of the signaling group in the **Near-end Node Name** field and the **Far-end Node Name** field, respectively. These field values are taken from the **IP Node Names** form.
- Ensure that the TLS port value of *5061* is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- The preferred codec for the call will be selected from the IP codec set assigned to the IP network region specified in the **Far-end Network Region** field.
- Enter the domain name of Session Manager in the **Far-end Domain** field. In this configuration, the domain name is *avaya.com*.
- The **Direct IP-IP Audio Connections** field was enabled on this form.
- The **DTMF over IP** field should be set to the default value of *rtp-payload*.

Communication Manager supports DTMF transmission using RFC 2833. The default values for the other fields may be used.

```
add signaling-group 10                                     Page 1 of 2
                                                         SIGNALING GROUP
Group Number: 10                                         Group Type: sip
IMS Enabled? n                                           Transport Method: tls
Q-SIP? n
IP Video? Y                                             Priority Video? n           Enforce SIPS URI for SRTP? n
Peer Detection Enabled? y Peer Server: SM                Clustered? n
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
Near-end Node Name: procr                               Far-end Node Name: devcon-sm
Near-end Listen Port: 5061                               Far-end Listen Port: 5061
                                                         Far-end Network Region: 1
Far-end Domain: avaya.com
Incoming Dialog Loopbacks: eliminate                    Bypass If IP Threshold Exceeded? n
                                                         RFC 3389 Comfort Noise? n
DTMF over IP: rtp-payload                               Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
Enable Layer 3 Test? y                                  Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n                 Alternate Route Timer(sec): 6
```

Configure the **Trunk Group** form as shown below. This trunk group is used for SIP calls to M900 and Avaya SIP deskphones. Set the **Group Type** field to *sip*, set the **Service Type** field to *public-ntwrk* or *tie*, specify the signaling group associated with this trunk group in the **Signaling Group** field, and specify the **Number of Members** supported by this SIP trunk group. Configure the other fields in bold and accept the default values for the remaining fields.

```

add trunk-group 10                                     Page 1 of 22
                                     TRUNK GROUP
Group Number: 10                                     Group Type: sip                                     CDR Reports: y
Group Name: To devcon-sm                             COR: 1                                     TN: 1                                     TAC: 1010
Direction: two-way                                   Outgoing Display? n
Dial Access? n                                       Night Service:
Queue Length: 0
Service Type: public-ntwrk                           Auth Code? n
Member Assignment Method: auto
Signal Group: 10
Number of Members: 10

```

### 5.5. Administer AAR Call Routing

SIP calls to Session Manager are routed over a SIP trunk via AAR call routing. Configure the AAR analysis form and enter add an entry that routes digits beginning with “78” to route pattern 10 as shown below.

```

change aar analysis 78                               Page 1 of 2
                                     AAR DIGIT ANALYSIS TABLE
                                     Location: all                                     Percent Full: 1

```

Dialed String	Total		Route Pattern	Call Type	Node Num	ANI Reqd
	Min	Max				
<b>78</b>	<b>5</b>	<b>5</b>	<b>10</b>	<b>lev0</b>		<b>n</b>

Configure a preference in **Route Pattern 10** to route calls over SIP trunk group 10 as shown below.

```

change route-pattern 10                                     Page 1 of 3
      Pattern Number: 10      Pattern Name: To devcon-sm
  SCCAN? n      Secure SIP? n      Used for SIP stations? n

  Grp FRL NPA Pfx Hop Toll No.  Inserted      DCS/ IXC
  No      Mrk Lmt List Del  Digits      QSIG
                                         Intw
1: 10    0
2:
3:
4:
5:
6:

      BCC VALUE  TSC CA-TSC      ITC BCIE Service/Feature  PARM Sub  Numbering LAR
      0 1 2 M 4 W      Request      Dgts  Format
1: y y y y y n  n      rest      unk-unk  none
2: y y y y y n  n      rest      none
3: y y y y y n  n      rest      none
4: y y y y y n  n      rest      none
  
```

## 6. Configure Avaya Aura® Session Manager

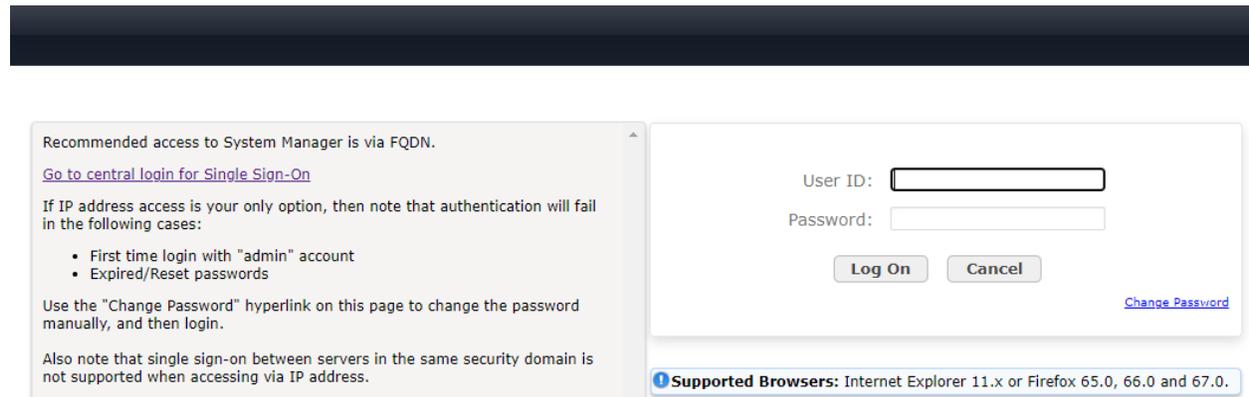
This section provides the procedure for configuring Session Manager. The procedures include the following areas:

- Launch System Manager
- Set Network Transport Protocol for M900 Multicell DECT Phones
- Administer SIP User

**Note:** It is assumed that basic configuration of Session Manager has already been performed. This section will focus on the configuration of a SIP user for the Snom solution.

### 6.1. Launch System Manager

Access the System Manager Web interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of the System Manager server. Log in using the appropriate credentials.



## 6.2. Set Network Transport Protocol for M900 Multicell DECT Phones

From the System Manager **Home** screen, select **Elements** → **Routing** → **SIP Entities** and edit the SIP Entity for Session Manager shown below.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.1', and menu items for Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile 'admin' are also visible. The left sidebar shows a navigation tree with 'Routing' selected, and 'SIP Entities' highlighted. The main content area is titled 'SIP Entity Details' and contains two sections: 'General' and 'Monitoring'. The 'General' section includes fields for Name (devcon-sm), IP Address (10.64.102.117), SIP FQDN, Type (Session Manager), Notes, Location (Thornton), Outbound Proxy, Time Zone (America/New\_York), Minimum TLS Version (Use Global Setting), and Credential name. The 'Monitoring' section includes SIP Link Monitoring and CRLF Keep Alive Monitoring, both set to 'Use Session Manager Configuration'. Buttons for 'Commit' and 'Cancel' are located at the top right of the form.

Scroll down to the **Listen Ports** section and verify that the transport network protocol used by M900 is specified in the list below. For the compliance test, the solution used TLS network transport.

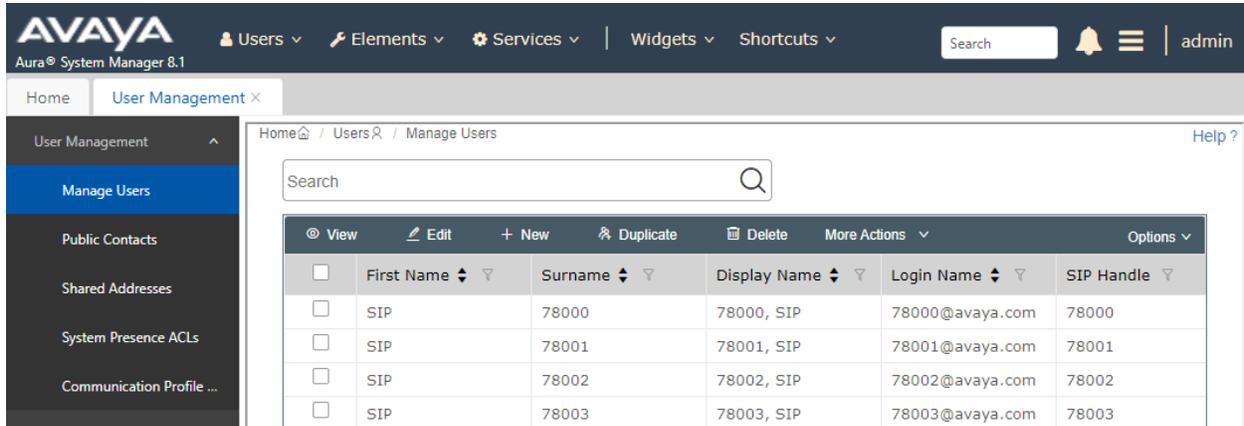
### Listen Ports

<input type="checkbox"/>	Listen Ports	Protocol	Default Domain	Endpoint	Notes
<input type="checkbox"/>	5060	TCP	avaya.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	5060	UDP	avaya.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	5061	TLS	avaya.com	<input checked="" type="checkbox"/>	

Select : All, None

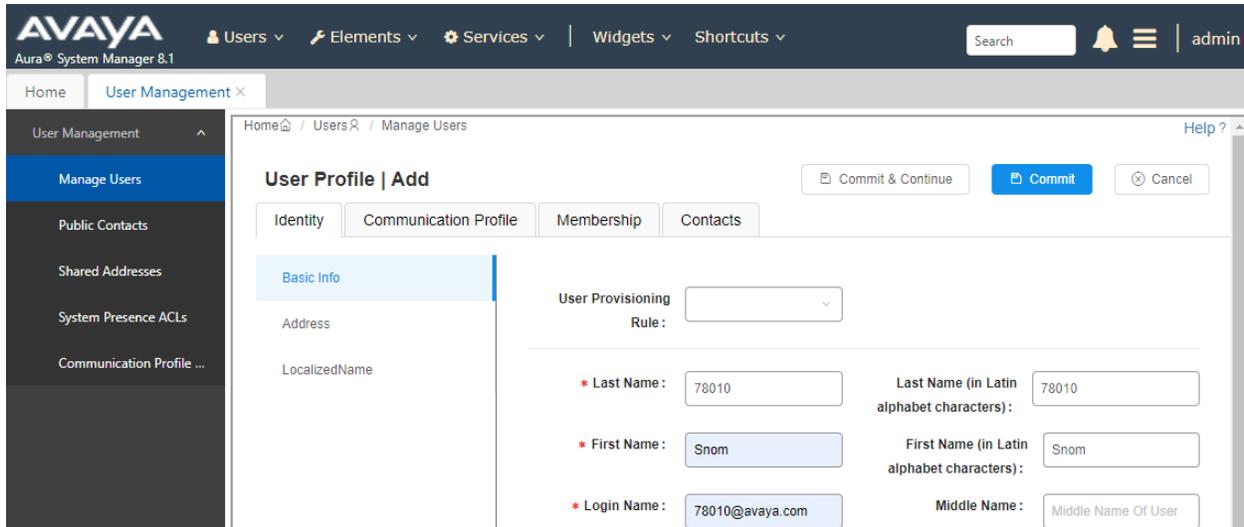
### 6.3. Administer SIP User

In the **Home** screen (not shown), select **Users** → **User Management** → **Manage Users** to display the **User Management** screen below. Click **New** to add a user.



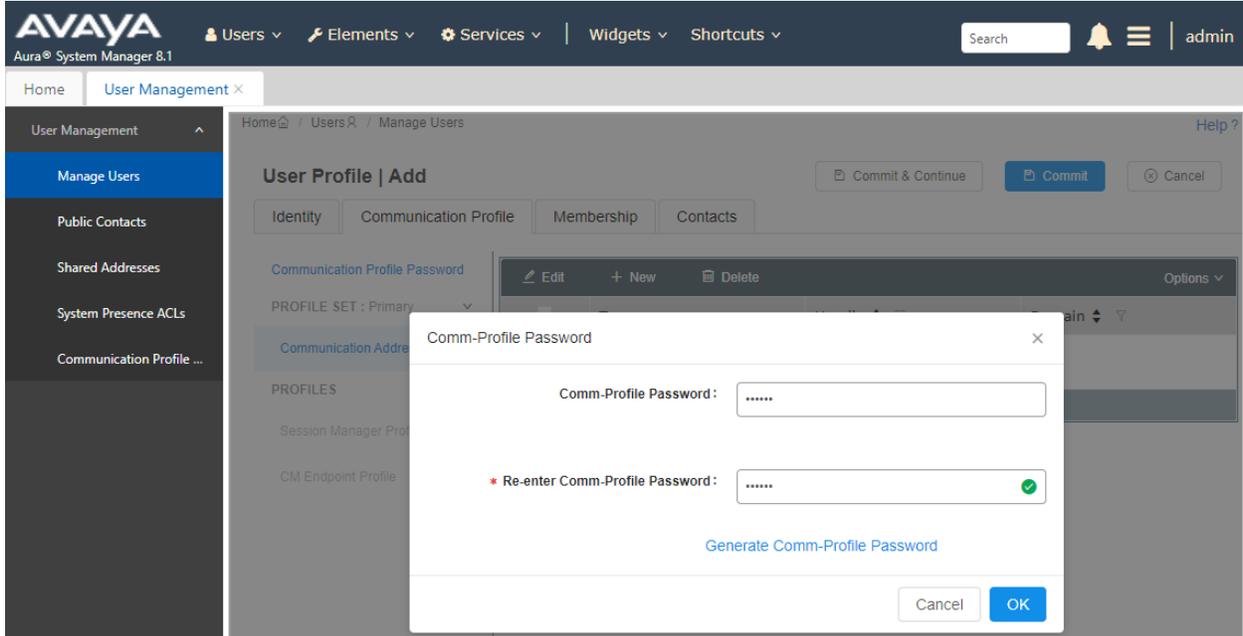
#### 6.3.1. Identity

The **New User Profile** screen is displayed. Enter desired **Last Name** and **First Name**. For **Login Name**, enter “<ext>@<domain>”, where “<ext>” is the desired M900 SIP extension and “<domain>” is the applicable SIP domain name from **Section 5.3**. Retain the default values in the remaining fields.



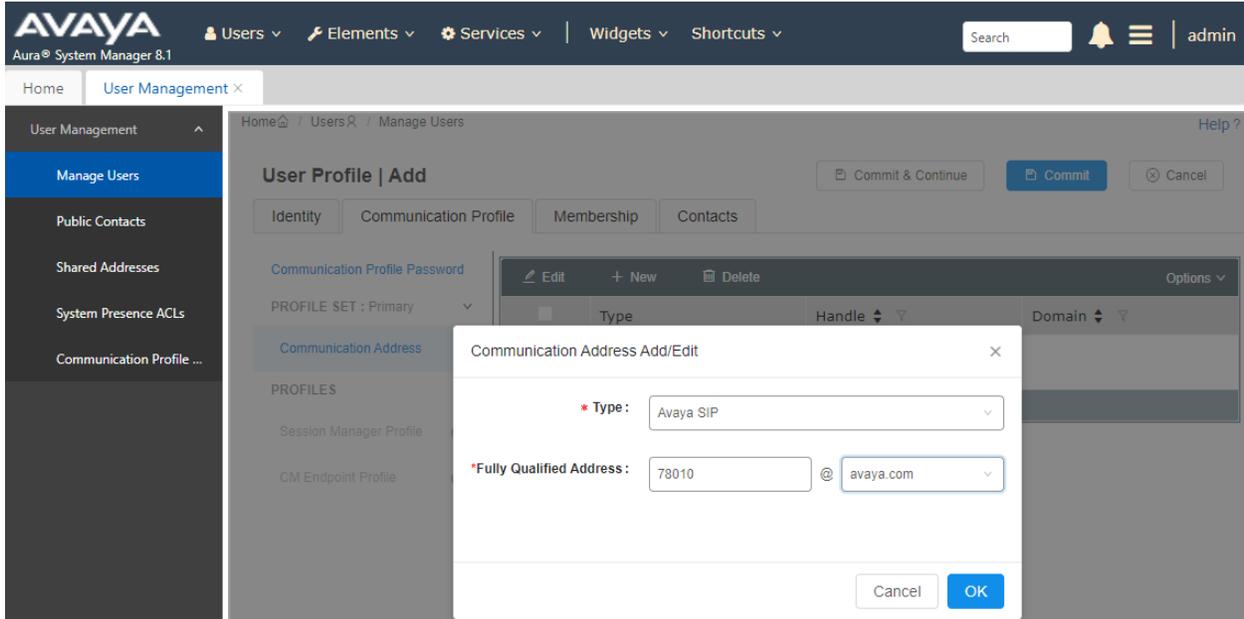
### 6.3.2. Communication Profile

Select the **Communication Profile** tab. Next, click on **Communication Profile Password**. For **Comm-Profile Password** and **Re-enter Comm-Profile Password**, enter the desired password for the SIP user to use for registration. Click **OK**.



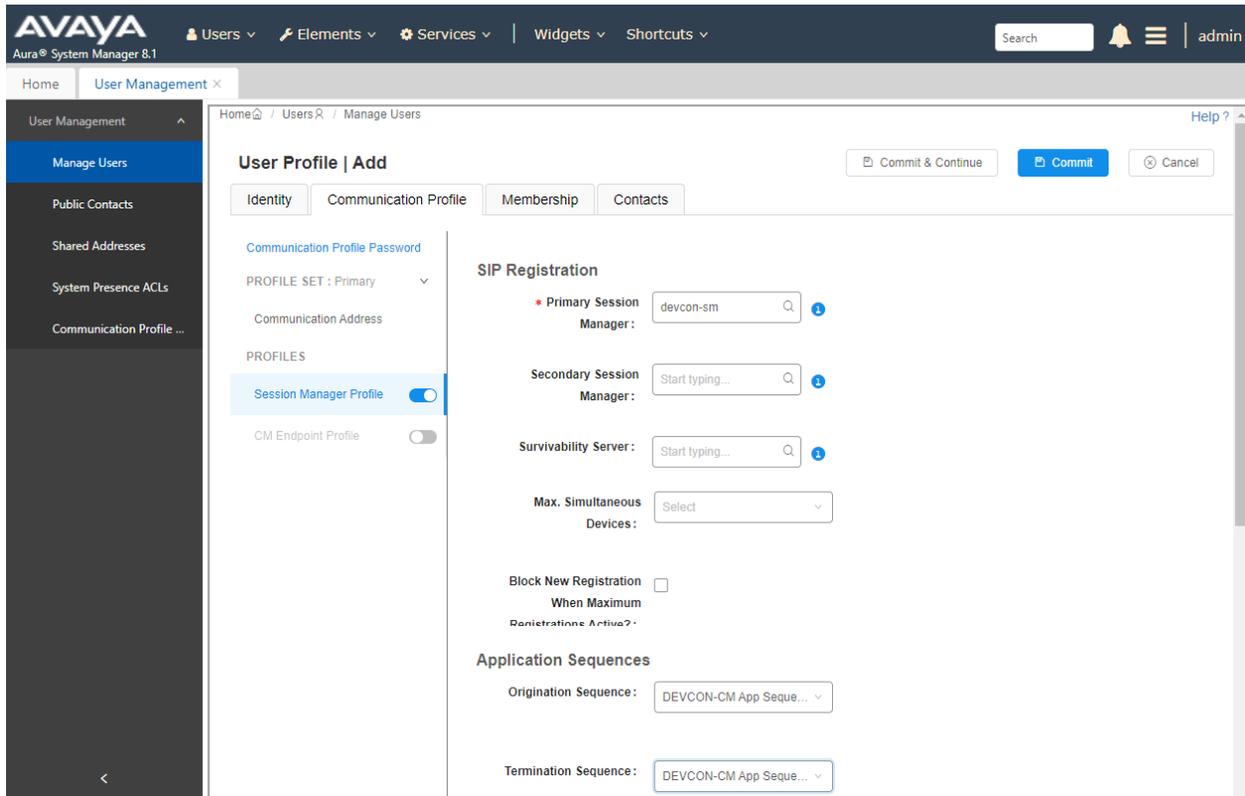
### 6.3.3. Communication Address

Click on **Communication Address** and then click **New** to add a new entry. The **Communication Address Add/Edit** dialog box is displayed as shown below. For **Type**, select *Avaya SIP*. For **Fully Qualified Address**, enter the SIP user extension and select the domain name to match the login name from **Section 6.3.1**. Click **OK**.

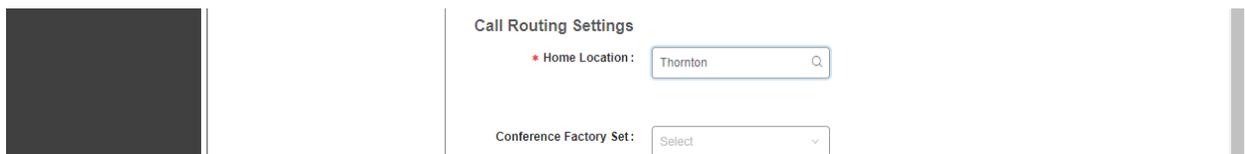


### 6.3.4. Session Manager Profile

Click on toggle button by **Session Manager Profile**. For **Primary Session Manager**, **Origination Application Sequence**, **Termination Application Sequence**, and **Home Location**, select the values corresponding to the applicable Session Manager and Communication Manager. Retain the default values in the remaining fields.



Scroll down to the **Call Routing Settings** section to configure the **Home Location**.



### 6.3.5. CM Endpoint Profile

Click on the toggle button by **CM Endpoint Profile**. For **System**, select the value corresponding to the applicable Communication Manager. For **Extension**, enter the SIP user extension from **Section 6.3.1**. For **Template**, select *9641SIP\_DEFAULT\_CM\_8\_1*. For **Port**, click and select *IP*. Retain the default values in the remaining fields. Click on the Endpoint Editor (i.e, Edit icon in Extension field) to configure the **Coverage Path**.

The screenshot displays the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, navigation menus for Users, Elements, Services, Widgets, and Shortcuts, a search bar, and a user profile for 'admin'. The main content area is titled 'User Profile | Add' and features several tabs: Identity, Communication Profile, Membership, and Contacts. The 'Communication Profile' tab is active, showing a 'Communication Profile Password' section with a dropdown for 'PROFILE SET : Primary' and a 'Communication Address' field. Below this is a 'PROFILES' section with two toggle switches: 'Session Manager Profile' (disabled) and 'CM Endpoint Profile' (enabled). The main configuration area contains the following fields and options:

- System:** devcon-cm
- Profile Type:** Endpoint
- Extension:** 78010 (with an edit icon)
- Set Type:** 9641SIP
- Port:** IP
- Template:** 9641SIP\_DEFAULT\_CM\_8\_1
- Security Code:** Enter Security Code
- Preferred Handle:** Select
- Voice Mail Number:** (empty field)
- Sip Trunk:** aar
- Use Existing Endpoints:**
- Calculate Route Pattern:**
- SIP URI:** Select
- Delete on Unassign from User or on Delete User:**
- Override Endpoint Name and Localized Name:**
- Allow H.323 and SIP Endpoint Dual Registration:**

Buttons for 'Commit & Continue', 'Commit', and 'Cancel' are located at the top right of the form.

Navigate to the **General Options** tab and set the **Coverage Path 1** field to the voicemail coverage path. Click **Done** to return to the previous web page and then **Commit** to save the configuration (not shown).

* System	devcon-cm	* Extension	78010
* Template	9641SIP_DEFAULT_CM_8_1	* Set Type	9641SIP
* Port	IP	* Security Code	
Name			

[Display Extension Ranges](#)

<b>General Options (G)</b> *	Feature Options (F)	Site Data (S)	Abbreviated Call Dialing (A)	Enhanced Call Fwd (E)
Button Assignment (B)	Profile Settings (P)	Group Membership (M)		
* Class of Restriction (COR)	1	* Class Of Service (COS)	1	
* Emergency Location Ext	78010	* Message Lamp Ext.	78010	
* Tenant Number	1	Type of 3PCC Enabled	None	
* SIP Trunk	Qaar	Coverage Path 1	15	
Coverage Path 2		Localized Display Name		
Lock Message	<input type="checkbox"/>	Enable Reachability for Station Domain Control	system	
Multibyte Language	Not Applicable			
SIP URI				
Attendant	<input type="checkbox"/>			
<b>Primary Session Manager</b>				
IPv4:		IPv6:		
<b>Secondary Session Manager</b>				
IPv4:		IPv6:		

\*Required

**Done**

## 6.4. Administer Remote Access

**Note:** This section is applicable for remote workers only.

Remote Access is used by Session Manager to map a SIP proxy's public IP Address to a Session Manager private SIP addresses. In the System Manager **Home** page, navigate to **Elements** → **Session Manager** → **Network Configuration** → **Remote Access**.

On the **Remote Access Configuration** screen, click **New** (not shown). Enter a descriptive name (e.g., *Remote Worker*). In the **SIP Proxy Mapping Table** section, click **New** and enter the Avaya SBCE public IP address used for remote workers (e.g., *10.64.101.102*). For **Session Manager (Reference C)**, select the Session Manager instance being used. In the reference configuration a single Session Manager instance is used, and it is already selected. In the **SIP Proxy Private IP Addresses** section, click **New** and enter the Avaya SBCE private IP address used for remote workers (e.g., *10.64.102.108*).

**Remote Access Configuration** Commit Cancel

\*Name:   
Note:

[Click to open Remote Access Reference Map](#)

**SIP Proxy Mapping**

**SIP Proxy Mapping Table**

New Delete

<input type="checkbox"/>	SIP Proxy Public Address (Reference A)	Session Manager (Reference C)	IP Address Family (Reference C)
<input type="checkbox"/>	<input type="text" value="10.64.101.102"/>	devcon-sm	IPv4

Select : All, None

**SIP Proxy Private IP Addresses**

New Delete

<input type="checkbox"/>	SIP Private Address (Reference B)	SBC Type	Securable	Note
<input type="checkbox"/>	<input type="text" value="10.64.102.108"/>	Avaya SBC	<input type="checkbox"/>	<input type="text"/>

Select : All, None

\*Required Commit Cancel

## 7. Configure Avaya SIP Deskphones

The 46xxsettings.txt file is used to specify certain system parameters. It is used by Avaya H.323 and SIP Deskphones, but this section will cover four parameters that are applicable to SIP deskphones only.

- **SDPCAPNEG** Specifies whether SDP capability negotiation is supported. By default, it is enabled.
- **ENFORCE\_SIPS\_URI** Enable this option to support SIPS URI.
- **MEDIAENCRYPTION** Specifies the media encryption (SRTP) options supported. In the example below, *aescm128-hmac80* (option 1) and *aescm128-hmac32* (option 2) are supported as specified in the **IP Codec Set** in **Section 5.3**.
- **ENCRYPT\_SRTCP** Enable this option to encrypt SRTCP.

```
## SDPCAPNEG specifies whether or not SDP capability negotiation is enabled.
## Value Operation
## 0 SDP capability negotiation is disabled
## 1 SDP capability negotiation is enabled (default)
## This parameter is supported by:
## J129 SIP R1.0.0.0 and later
## 96x1 SIP R6.0 and later
## H1xx SIP R1.0 and later
## 96x0 SIP R2.6 and later
SET SDPCAPNEG 1
##
## ENFORCE_SIPS_URI specifies whether a SIPS URI must be used for SRTP.
## Value Operation
## 0 Not enforced
## 1 Enforced (default)
## This parameter is supported by:
## J129 SIP R1.0.0.0 and later; not applicable for 3PCC environment
## 96x1 SIP R6.0 and later
## H1xx SIP R1.0 and later
## 96x0 SIP R2.6 and later
SET ENFORCE_SIPS_URI 1
##
## MEDIAENCRYPTION specifies which media encryption (SRTP) options will be supported.
## Up to 2 or 3 options may be specified in a comma-separated list.
## 2 options are supported by:
## 1. Prior releases to 96x1 SIP 7.0.0
## 2. H1xx SIP R1.0 and later
## 3. 96x0 SIP R1.0 to R2.6.14.1
## 3 options are supported by 96x1 SIP R7.0.0 and later, H1xx SIP R1.0.1 and later
## and J129 SIP R1.0.0.0 and later.
## For 96x0 SIP R2.6.14.5 and later, up to 3 options may be specified, but only the
## first two supported options are used.
## Options should match those specified in CM IP-codec-set form.
## 1 = aescm128-hmac80
## 2 = aescm128-hmac32
## 3 = aescm128-hmac80-unauth
## 4 = aescm128-hmac32-unauth
## 5 = aescm128-hmac80-unenc
## 6 = aescm128-hmac32-unenc
## 7 = aescm128-hmac80-unenc-unauth
```

```

##      8 = aescm128-hmac32-unenc-unauth
##      9 = none (default)
##     10 = aescm256-hmac80
##     11 = aescm256-hmac32
## Options 10 and 11 are supported by 96x1 SIP R7.0.0 and later, H1xx SIP R1.0.1 and
## later and J129 SIP R1.0.0.0 and later.
## Note: The list of media encryption (SRTP) options is ordered from high (left) to
## the low (right) options. The phone will publish this list in the SDP-OFFER
## or choose from SDP-OFFER list according to the list order defined in
## MEDIAENCRYPTION. Please note that Avaya Communication Manager has the capability
## to change the list order in the SDP-OFFER (for audio only) when the SDP-OFFER pass
## through CM.
## This parameter is supported by:
##     Avaya Equinox 3.1.2 and later; supported values: 1,2,9,10 and 11. The default
##     value is 1,2,9.
##     Avaya Vantage Basic Application SIP R1.0.0.0 and later; supported values:
##     1,2,9,10 and 11. The default value is 1,2,9.
##     J129 SIP R1.0.0.0 and later
##     96x1 SIP R6.0 and later
##     H1xx SIP R1.0 and later
##     96x0 SIP R1.0 and later
SET MEDIAENCRYPTION 1,2,9
##
## ENCRYPT_SRTP specifies whether RTCP packets are encrypted or not. SRTP is only
## used if SRTP is enabled using
## MEDIAENCRYPTION (values other than 9 (none) are configured).
## This parameter controls RTCP encryption for RTCP packets exchanged between peers.
## RTCP packets sent to Voice Monitoring Tools are always sent unencrypted.
## Value Operation
## 0          SRTP is disabled (default).
## 1          SRTP is enabled.
## This parameter is supported by:
##     Avaya Equinox 3.1.2 and later
##     96x1 SIP R7.1.0.0 and later
##     Avaya Vantage Basic Application SIP R1.0.0.0 and later
##     J129 SIP R1.0.0.0 and later
SET ENCRYPT_SRTP 1

```

## 8. Configure Avaya Session Border Controller for Enterprise

This section covers the configuration of Avaya SBCE. Avaya SBCE provides SIP connectivity to remote workers, Session Manager, VoIP Service Provider. This section will focus on the configuration for remote workers, including:

- Launch SBCE Web Interface
- Administer Topology Hiding
- Administer Media Rules
- Administer End Point Policy Groups
- Administer Media Interfaces
- Administer Signaling Interfaces
- Administer End Point Flows
- Administer TLS Management

**Note:** For security reasons, public IP addresses will be blacked out in these Application Notes.

### 8.1. Launch SBCE Web Interface

Access the SBCE web interface by using the URL **https://<ip-address>/sbc** in a web browser, where <ip-address> is the IP address of the SBCE management interface. The screen below is displayed. Log in using the appropriate credentials.



### Session Border Controller for Enterprise

#### Log In

Username:

WELCOME TO AVAYA SBC

Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel.

Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials.

© 2011 - 2020 Avaya Inc. All rights reserved.

After logging in, the **Dashboard** will appear as shown below. All configuration screens of the SBCE are accessed by navigating the menu tree in the left pane. Select **Device** → **SBCE** from the top menu.

Device: EMS ▾
Alarms
Incidents
Status ▾
Logs ▾
Diagnostics
Users
Settings ▾
Help ▾
Log Out

## Session Border Controller for Enterprise

**EMS Dashboard**

- Software Management
- Device Management
  - System Administration
  - Templates
- Backup/Restore
- Monitoring & Logging

### Dashboard

Information	
System Time	10:13:48 AM EDT <a href="#">Refresh</a>
Version	8.1.2.0-31-19809
GUI Version	8.1.2.0-19794
Build Date	Tue Dec 08 09:11:07 UTC 2020
License State	✔ OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	10/11/2021 10:10:45 EDT
Failed Login Attempts	0

Installed Devices
EMS
SBCE

Active Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
None found.

[Add](#)

Notes
No notes found.

## 8.2. Administer Topology Hiding

A topology hiding profile is created to replace IP addresses in the SIP URI, From, and To headers sent in a SIP Invite from remote workers. This topology hiding profile is specified in the End Point Flows in **Section 8.7**.

To create a new **Topology Hiding** profile, navigate to **Configuration Profiles → Topology Hiding**. Click **Add**. In the example below, the IP address in the **Request-Line**, **To**, and **From** headers are overwritten with the domain (e.g., *avaya.com*).

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes "Device: SBCE", "Alarms", "Incidents", "Status", "Logs", "Diagnostics", "Users", "Settings", "Help", and "Log Out". The main header displays "Session Border Controller for Enterprise" and the "AVAYA" logo.

The left sidebar contains a navigation menu with the following items: EMS Dashboard, Software Management, Device Management, Backup/Restore, System Parameters, Configuration Profiles (expanded), Domain DoS, Server Interworking, Media Forking, Routing, **Topology Hiding** (highlighted), Signaling Manipulation, URI Groups, SNMP Traps, Time of Day Rules, FGDN Groups, Reverse Proxy Policy, URN Profile, Recording Profile, Services, Domain Policies, TLS Management, Network & Flows, DMZ Services, and Monitoring & Logging.

The main content area is titled "Topology Hiding Profiles: Session Manager". It features an "Add" button, a "Click here to add a description." link, and "Rename", "Clone", and "Delete" buttons. A list of profiles is shown, with "default" and "Session Mana..." visible. The "Session Mana..." profile is selected, displaying a table of configuration rules:

Header	Criteria	Replace Action	Overwrite Value
Request-Line	IP/Domain	Overwrite	avaya.com
Refer-To	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---
To	IP/Domain	Overwrite	avaya.com
From	IP/Domain	Overwrite	avaya.com
Via	IP/Domain	Auto	---

An "Edit" button is located below the table.

### 8.3. Administer Media Rules

A media rule defines the processing to be applied to the selected media. A media rule is one component of the larger endpoint policy group defined in **Section 8.4**. For the compliance test, a new media rule was created to support RTP and SRTP to be used for both remote workers and Session Manager.

To view an existing rule, navigate to **Domain Policies** → **Media Rules** in the left pane. In the center pane, select the rule (e.g., *RTP-SRTP*) to be viewed. The contents of the *RTP-SRTP* media rule are described below. The **Encryption** tab was configured as shown below.

**Note:** Capability Negotiation must be disabled to avoid one-way audio during an active call after a Session Refresh is sent to an M65 DECT phone registered as a remote worker.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. At the top, there is a navigation bar with 'Device: SBCE' and various menu items like 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. Below this is the main header 'Session Border Controller for Enterprise' and the 'AVAYA' logo.

The left sidebar shows a navigation tree with 'Domain Policies' expanded to 'Media Rules'. The 'RTP-SRTP' rule is selected. The main content area shows the configuration for this rule, with the 'Encryption' tab active. The configuration is divided into three sections: 'Audio Encryption', 'Video Encryption', and 'Miscellaneous'.

Section	Property	Value
Audio Encryption	Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80 RTP
	Encrypted RTCP	<input checked="" type="checkbox"/>
	MKI	<input type="checkbox"/>
	Lifetime	Any
	Interworking	<input checked="" type="checkbox"/>
	Symmetric Context Reset	<input checked="" type="checkbox"/>
Video Encryption	Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80
	Encrypted RTCP	<input type="checkbox"/>
	MKI	<input type="checkbox"/>
	Lifetime	Any
	Interworking	<input checked="" type="checkbox"/>
Miscellaneous	Key Change in New Offer	<input type="checkbox"/>
	Capability Negotiation	<input type="checkbox"/>

The **Codec Prioritization** tab was configured as shown below.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

## Session Border Controller for Enterprise

AVAYA

- EMS Dashboard
- Software Management
- Device Management
- Backup/Restore
- System Parameters
- Configuration Profiles
- Services
- ▾ Domain Policies
  - Application Rules
  - Border Rules
  - Media Rules**
  - Security Rules
  - Signaling Rules
  - Charging Rules
  - End Point Policy Groups
  - Session Policies
- TLS Management
- Network & Flows
- DMZ Services
- Monitoring & Logging

### Media Rules: RTP-SRTP

Add Rename Clone Delete

Click here to add a description.

Encryption **Codec Prioritization** Advanced QoS

**Audio Codec**

Codec Prioritization

**Video Codec**

Codec Prioritization

Edit

## 8.4. Administer End Point Policy Groups

An endpoint policy group is a set of policies that will be applied to traffic between the SBCE and an endpoint (e.g., remote workers). An endpoint policy group must be created for remote workers and Session Manager. The endpoint policy group is applied to the traffic as part of the endpoint flows defined in **Section 8.7**.

To create a new group, navigate to **Domain Policies** → **End Point Policy Groups** in the left pane. In the right pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new group, followed by the **Policy Group** window (not shown) to configure the group parameters. Once complete, the settings will displayed. To view the settings of an existing group, select the group from the list. The settings will appear in the right pane.

The new endpoint policy group, named *RTP-SRTP*, is shown below and is assigned the *RTP-SRTP* media rule configured above.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Device: SBCE', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header reads 'Session Border Controller for Enterprise' with the AVAYA logo on the right. A left-hand navigation menu lists various management options, with 'End Point Policy Groups' highlighted in red. The main content area is titled 'Policy Groups: RTP-SRTP' and features an 'Add' button, 'Rename', 'Clone', and 'Delete' buttons. A 'Policy Groups' tab is active, and a link says 'Click here to add a description.' An 'Edit Policy Set' modal window is open, showing the following configuration:

Setting	Value
Application Rule	default
Border Rule	default
Media Rule	RTP-SRTP
Security Rule	default-low
Signaling Rule	default
Charging Rule	None
RTCP Monitoring Report Generation	Off

The modal window also includes a 'Finish' button. In the background, a 'Summary' button and a 'RTCP Mon Gen' status indicator (set to 'Off') are visible.

## 8.5. Administer Media Interfaces

A media interface defines an IP address and port range for transmitting media. Create separate Media Interfaces for the public and private IP interfaces used to support the Remote Workers.

Navigate to **Networks & Flows** → **Media Interface** to define a new Media Interface. During the Compliance Testing the following interfaces were defined. For security reasons, public IP addresses have been blacked out. The media interfaces used for this solution are listed below.

- **PrivateMediaRW:** Interface used by Session Manager to send and receive media for remote workers.
- **PublicMediaRW:** Interface used by remote workers to send and receive media.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

### Session Border Controller for Enterprise

AVAYA

EMS Dashboard  
Software Management  
Device Management  
Backup/Restore  
▸ System Parameters  
▸ Configuration Profiles  
▸ Services  
▸ Domain Policies  
▾ TLS Management  
    Certificates  
    Client Profiles  
    Server Profiles  
    SNI Group  
▾ Network & Flows  
    Network Management  
    **Media Interface**  
    Signaling Interface

#### Media Interface

Name	Media IP Network	Port Range		
PrivateMedia	10.64.102.106 Private-A1 (A1, VLAN 0)	35000 - 40000	Edit	Delete
PublicMedia	10.64.101.101 Public-B1 (B1, VLAN 0)	35000 - 40000	Edit	Delete
PublicMediaB2	[REDACTED] Public-B2 (B2, VLAN 0)	35000 - 40000	Edit	Delete
PrivateMediaRW	10.64.102.108 Private-A1 (A1, VLAN 0)	35000 - 40000	Edit	Delete
PublicMediaRW	10.64.101.102 Public-B1 (B1, VLAN 0)	35000 - 40000	Edit	Delete

## 8.6. Administer Signaling Interfaces

A signaling interface defines an IP address, protocols and listen ports that the SBCE can use for signaling. Create a Signaling Interface for both the outside and inside IP interfaces to support remote workers.

Navigate to **Networks & Flows** → **Signaling Interface** to define a new **Signaling Interface**. During the Compliance Testing the following interfaces were defined. For security reasons, public IP addresses have been blacked out. The signaling interfaces used for this solution are listed below.

- **Private Signaling RW:** Interface used by Session Manager to send and receive calls for remote workers.
- **PublicSignalingRW:** Interface used for remote workers to send and receive calls.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes "Device: SBCE", "Alarms", "Incidents", "Status", "Logs", "Diagnostics", "Users", "Settings", "Help", and "Log Out". The main header displays "Session Border Controller for Enterprise" and the Avaya logo. A left-hand navigation menu lists various management options, with "Signaling Interface" highlighted in red. The main content area is titled "Signaling Interface" and contains a table of configured interfaces. The table has columns for Name, Signaling IP Network, TCP Port, UDP Port, TLS Port, and TLS Profile. Each row also includes "Edit" and "Delete" links. The "PublicSignalingB2" row has a blacked-out IP address.

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile		
PublicSignaling	10.64.101.101 Public-B1 (B1, VLAN 0)	5060	5060	---	None	Edit	Delete
PublicSignalingB2	[Redacted] Public-B2 (B2, VLAN 0)	5060	5060	5061	sbceExternalB2	Edit	Delete
PublicSignalingRW	10.64.101.102 Public-B1 (B1, VLAN 0)	5060	5060	5061	sbceExternalB1	Edit	Delete
PrivateSignaling	10.64.102.106 Private-A1 (A1, VLAN 0)	5060	5060	5061	sbceInternal	Edit	Delete
PrivateSignalingRW	10.64.102.108 Private-A1 (A1, VLAN 0)	5060	5060	5061	sbceInternal	Edit	Delete

## 8.7. Administer End Point Flows

End Point Flows determine the path to be followed by the packets traversing through Avaya SBCE. These flows combine the different sets of rules and profiles previously configured to be applied to the SIP traffic traveling in each direction.

### 8.7.1. Administer Subscriber Flows

To create a new **Subscriber Flow** for remote workers, navigate to **Network & Flows → End Point Flows** and select the **Subscriber Flows** tab. Click **Add**.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. At the top, there is a navigation bar with the following items: Device: SBCE, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. Below the navigation bar, the page title is "Session Border Controller for Enterprise" and the Avaya logo is visible in the top right corner.

The main content area is titled "End Point Flows" and contains two tabs: "Subscriber Flows" (selected) and "Server Flows". An "Add" button is located in the top right corner of the main content area.

A warning message is displayed: "Modifications made to an End-Point Flow will only take effect on new registrations or re-registrations." Below this is a blue bar with the text "Hover over a row to see its description." A table with the following columns is shown:

Priority	Flow Name	URI Group	Source Subnet	User Agent	End Point Policy Group	
1	Remote Worker	*	*	*	RTP-SRTP	<a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a>

The left sidebar contains the following navigation items: EMS Dashboard, Software Management, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management (with sub-items: Certificates, Client Profiles, Server Profiles, SNI Group), Network & Flows (with sub-items: Network Management, Media Interface, Signaling Interface, and End Point Flows).

The following screen shows the **Remote Worker** Subscriber Flow created in the sample configuration. This flow uses the interfaces, policies, and profiles defined in previous sections.

**View Flow: Remote Worker** X

Criteria		Optional Settings	
Flow Name	Remote Worker	TLS Client Profile	sbceExternalB1
URI Group	*	Signaling Manipulation Script	None
User Agent	*		
Source Subnet	*		
Via Host	*		
Contact Host	*		
Signaling Interface	PublicSignalingRW		

Profile	
Source	Subscriber
Methods Allowed Before REGISTER	
User Agent	*
Media Interface	PublicMediaRW
Secondary Media Interface	None
End Point Policy Group	RTP-SRTP
Routing Profile	Session Manager
Presence Server Address	---

## 8.7.2. Administer Server Flows

To create a new **Server Flow** for Session Manager, navigate to **Network & Flows** → **End Point Flows** and select the **Server Flows** tab. Click **Add**.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

# Session Border Controller for Enterprise

- EMS Dashboard
- Software Management
- Device Management
- Backup/Restore
- System Parameters
- Configuration Profiles
- Services
- Domain Policies
- TLS Management
  - Certificates
  - Client Profiles
  - Server Profiles
  - SNI Group
- Network & Flows
  - Network Management
  - Media Interface
  - Signaling Interface
  - End Point Flows**
  - Session Flows
  - Advanced Options
- DMZ Services
- Monitoring & Logging

### End Point Flows

Subscriber Flows

Server Flows

Add

Modifications made to a Server Flow will only take effect on new sessions.

Hover over a row to see its description.

**SIP Server: PSTN-SIP**

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile					
1	PSTN-SIP Flow	*	PrivateSignaling	PublicSignaling	RTP-SRTP	Session Manager	View	Clone	Edit	Delete	

**SIP Server: Session Manager**

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile					
1	Session Manager Flow	*	PublicSignaling	PrivateSignaling	RTP-SRTP	PSTN-SIP	View	Clone	Edit	Delete	
2	Remote Worker Flow	*	PublicSignalingRW	PrivateSignalingRW	RTP-SRTP	default	View	Clone	Edit	Delete	

The following screen shows the **Remote Worker Flow** Server Flow created in the sample configuration. This flow uses the interfaces, policies, and profiles defined in previous sections.

Criteria		Profile	
Flow Name	Remote Worker Flow	Signaling Interface	PrivateSignalingRW
Server Configuration	Session Manager	Media Interface	PrivateMediaRW
URI Group	*	Secondary Media Interface	None
Transport	*	End Point Policy Group	RTP-SRTP
Remote Subnet	*	Routing Profile	default
Received Interface	PublicSignalingRW	Topology Hiding Profile	Session Manager
		Signaling Manipulation Script	None
		Remote Branch Office	Any
		Link Monitoring from Peer	<input type="checkbox"/>

## 8.8. Administer TLS Management

There is no additional configuration required to support TLS between SBCE and the M900 Multicell DECT Phones as remote workers. The M900 was configured to accept all certificates.

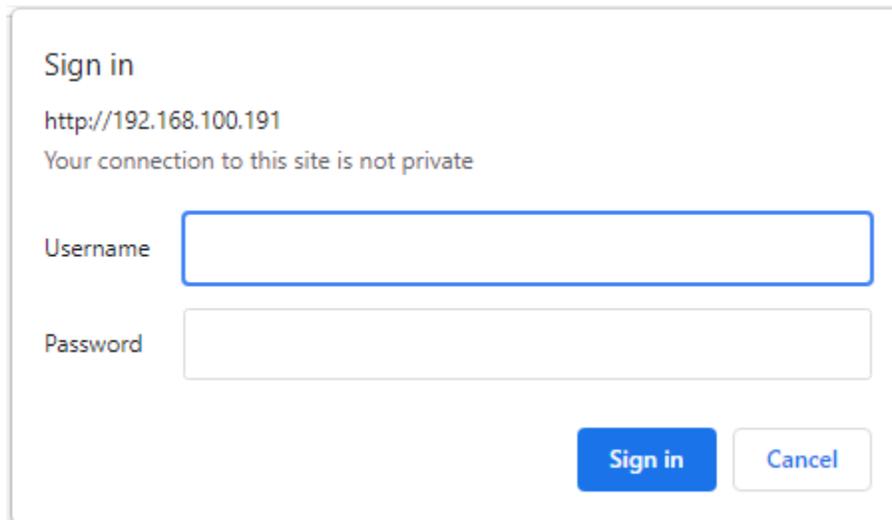
## 9. Configure Snom M900 Multicell DECT Phones

This section provides the procedure for configuring the M900. The procedure covers the following areas:

- Open web user interface
- Administer network settings
- Administer Country/Time Settings
- Administer Servers
- Add Extensions
- Administer Security

### 9.1. Open Web User Interface

The Snom M900 Multicell Base Station was configured through the web user interface by using the URL “http://ip-address” in an Internet browser window, where “ip-address” is the IP address of the base station. Log in using the appropriate credentials and then click **OK**.



The screenshot shows a web browser window with a "Sign in" dialog box. The URL bar displays "http://192.168.100.191" and a warning message states "Your connection to this site is not private". Below the URL bar, there are two input fields: "Username" and "Password". At the bottom right of the dialog box, there are two buttons: "Sign in" (highlighted in blue) and "Cancel".

## 9.2. Administer Network Settings

To configure network settings, click **Network** in the left pane. The M900 is pre-configured to use DHCP, but a static IP address may be used. For the compliance test, DHCP was used as shown below.

**SNOM M900**

Home/Status  
Extensions  
Servers  
**Network**  
Management  
Firmware Update  
Country  
Security  
Central Directory  
Multi Cell  
Dial Plans  
Repeaters  
Alarm  
Statistics  
Generic Statistics  
Diagnostics  
Configuration  
Syslog  
SIP Log  
Logout

### Network Settings

**IP Settings**  
DHCP/Static IP:   
IP Address:   
Subnet Mask:   
Default Gateway:   
DNS (Primary):   
DNS (Secondary):   
MDNS:

**NAT Settings**  
Enable STUN:   
STUN Server:   
STUN Bindtime Determine:   
STUN Bindtime Guard:   
Enable RPORT:   
Keep alive time:

**VLAN Settings**  
ID:   
User Priority:   
Synchronization:

**DHCP Options**  
Plug-n-Play:

**TCP Options**  
TCP Keep Alive Interval:

**Discovery**  
LLDP-MED Send:   
LLDP-MED Send delay:   
VLAN via LLDP-MED:

**SIP/RTP Settings**  
Use Different SIP Ports:   
RTP Collision Detection:   
Always reboot on check-sync:   
Outbound Proxy Mode:   
Failover SIP Timer B:   
Failover SIP Timer F:   
Failover Reconnect Timer:   
Local SIP port:   
SIP ToS/QoS:   
RTP port:   
RTP port range:   
RTP ToS/QoS:   
SIP registration mode:

### 9.3. Administer Country/Time Settings

Navigate to **Country** in the left pane to configure the Time Server and set the correct time.

**Note:** It is important to use correct date and time of the system when using trusted certificates. In case of undefined time/date, the certificate validation can fail.

**snom M900**

**Country/Time Settings**

Select country:

State / Region:

Notes:

Select Language:

Time Server:

Allow broadcast NTP:

Refresh time (h):

Set timezone by country/region:

Timezone:

Set DST by country/region:

Daylight Saving Time (DST):

DST Fixed By Day:

DST Start Month:

DST Start Date:

DST Start Time:

DST Start Day of Week:

DST Start Day of Week Last in Month:

DST Stop Month:

DST Stop Date:

DST Stop Time:

DST Stop Day of Week:

DST Stop Day of Week Last in Month:

## 9.4. Administer Servers

To configure SIP server, click **Servers** in the left pane, and then click **Add Server** (not shown). Configure the following fields:

- **Server Alias:** Specify a server alias (e.g., *devcon-sm*).
- **Registrar:** Specify the SIP server proxy IP address (e.g., *10.64.102.117*). Specifying the port number is optional.
- **SIP Transport:** Set to *TLS*.
- **Codec Priority:** Specify the codec priority. For the compliance test, G.711 and G.722 were verified.

**Note:** With the configuration specified above, the M900 will send the IP address in the SIP URI and From/To headers of SIP Invite message. To send the domain instead, configure the domain (e.g., *avaya.com*) in **Registrar** and the SIP server proxy IP address in **Outbound Proxy**.

The screenshot shows the 'M900' web interface with a sidebar on the left containing navigation options: Home/Status, Extensions, Servers, Network, Management, Firmware Update, Country, Security, Central Directory, Multi Cell, Dial Plans, Repeaters, Alarm, Statistics, Generic Statistics, Diagnostics, Configuration, Syslog, SIP Log, and Logout. The main content area is titled 'Servers' and lists three servers: 'devcon-sm' (10.64.102.117), 'devcon-sbc' (10.64.101.102), and 'ipose' (10.64.102.90). Below these is 'ipo500v2' (192.168.100.90) and links for 'Add Server' and 'Remove Server'. The configuration for 'devcon-sm' is shown in a table-like format with various settings and their values:

Setting	Value
Server Alias:	devcon-sm
NAT Adaption:	Enabled
Registrar:	10.64.102.117
Outbound Proxy:	
Conference Server:	
Call Log Server:	
Music on Hold Server:	
Reregistration time (s):	3600
Deregister After Failback:	Disabled
SIP Session Timers:	Enabled
Session Timer Value (s):	3600
Dial Plan ID:	2
Use SIP as XSI Authentication:	Disabled
SIP Transport:	TLS
Signal TCP Source Port:	Enabled
Use One TCP Connection per SIP Extension:	Disabled
RTP from own base station:	Disabled
Keep Alive:	Enabled
Show Extension on Handset Idle Screen:	Enabled
Hold Behaviour:	RFC 3264
Remote Ring Tone Control:	Enabled
Attended Transfer Behaviour:	Hold 2nd Call
Semi-Attended Transfer Behaviour:	Allow Semi-Attended Transfer
Use Own Codec Priority:	Disabled
DTMF Signalling:	RFC 2833
DTMF Payload Type:	101
Remote Caller ID Source Priority:	PAI - FROM
Enable Blind Transfer:	Enabled
XSI User Services:	Enabled
Codec Priority:	G711U G711A G726 G722

Codecs are listed in a scrollable list. A note at the bottom states: '- Max number of codecs is 5'.

Scroll down to configure the following fields:

- **Secure RTP:** Set to *Enabled*.
- **SRTP Crypto Suites:** Specify the supported Crypto Suites as shown below.

Accept the default values for the remaining fields. Restart the M900 after saving the changes to Servers.

RTP Packet Size:	20 ms
Secure RTP:	Enabled
Secure RTP Auth:	Enabled
SRTP Crypto Suites:	AES_CM_128_HMAC_SHA1_32 AES_CM_128_HMAC_SHA1_80
Media Security:	Disabled
Media Security only for TLS:	Disabled
Client Initiated Connections (RFC5626):	Disabled

## 9.5. Administer Extensions

To create an extension for an M65 handset, click **Extensions** in the left pane to display the **Extensions** page below. Click **Add extension**.

Snom
M900

- Home/Status
- Extensions
- Servers
- Network
- Management
- Firmware Update
- Country
- Security
- Central Directory
- Multi Cell
- Dial Plans
- Repeaters

### Extensions

AC:

---

Add extension

Idx	IPEI	Handset State	Handset Type FW Info	FWU Progress	VoIP Idx	Extension	Display Name	Server	Server Alias	State		
<input type="checkbox"/>	1	0328DCAF32	Present@RPN00	M65 530.2	Complete	<input type="checkbox"/>	1	78010		10.64.102.117	devcon-sm	SIP Registered@RPN00
<input type="checkbox"/>	2	0328DCAF77	Present@RPN00	M65 530.2	Complete	<input type="checkbox"/>	2	78011		10.64.102.117	devcon-sm	SIP Registered@RPN00
<input type="checkbox"/>	3	0328DCAF5A	Present@RPN00	M65 530.2	Complete	<input type="checkbox"/>	3	78012		10.64.102.117	devcon-sm	SIP Registered@RPN00

[Check All /](#)
[Check All Extensions /](#)  
[Uncheck All](#)
[Uncheck All Extensions](#)

---

With selected: [Delete Handset\(s\)](#) [Register Handset\(s\)](#) [Deregister Handset\(s\)](#) [Start SIP Registration\(s\)](#) [SIP Delete Extension\(s\)](#)

In the **Add Extension** page, configure the following fields:

- **Line name:** Specify a line name for extension (e.g., 78010).
- **Extension:** Enter SIP extension (e.g., 78010).
- **Authentication User Name:** Specify the user name (e.g., 78010) used to register with Session Manager.
- **Authentication Password:** Specify the password used to register with Session Manager.
- **Mailbox Name:** Specify the mailbox number for the SIP user (e.g., 78010).
- **Mailbox Number:** Specify the voicemail number (e.g., 78600).
- **Server:** Specify the SIP server proxy configured in **Section 9.4**.

## 9.6. Administer Security

Navigate to Security in the left pane to disable **Use Only Trusted Certificates** as shown below. This will allow all certificates received from Session Manager to be accepted. This setting must be disabled, because the M900 currently doesn't support a SAN in the certificate as mentioned in **Section 2.2**. Since the **Use Only Trusted Certificates** option is disabled, there's no need to download TLS certificates to the M900.

**Note:** It is important to use correct date and time of the system when using trusted certificates. In case of undefined time/date, the certificate validation can fail.

Alarm

Statistics

Generic Statistics

Diagnostics

Configuration

Syslog

SIP Log

Logout

### Trusted Root Certificates

Idx	Issued To	Issued By	Valid Until	
<input type="checkbox"/>	0	Avaya	Avaya	23/03 08:59:21 2040
<input type="checkbox"/>	1	Chambers of Commerce Root	Chambers of Commerce Root	30/09 16:13:44 2037
<input type="checkbox"/>	2	Chambers of Commerce Root - 2008	Chambers of Commerce Root - 2008	31/07 12:29:50 2038
<input type="checkbox"/>	3	Global Chambersign Root	Global Chambersign Root	30/09 16:14:18 2037
<input type="checkbox"/>	4	Global Chambersign Root - 2008	Global Chambersign Root - 2008	31/07 12:31:40 2038
<input type="checkbox"/>	5	Actalis Authentication Root CA	Actalis Authentication Root CA	22/09 11:22:02 2030
<input type="checkbox"/>	6	Amazon Root CA 1	Amazon Root CA 1	17/01 00:00:00 2038
<input type="checkbox"/>	7	Amazon Root CA 2	Amazon Root CA 2	26/05 00:00:00 2040
<input type="checkbox"/>	8	Amazon Root CA 3	Amazon Root CA 3	26/05 00:00:00 2040
<input type="checkbox"/>	9	Amazon Root CA 4	Amazon Root CA 4	26/05 00:00:00 2040
<input type="checkbox"/>	10	Starfield Services Root Certificate Authority - G2	Starfield Services Root Certificate Authority - G2	31/12 23:59:59 2037
<input type="checkbox"/>	11	IdenTrust Public Sector Root CA 1	IdenTrust Public Sector Root CA 1	16/01 17:53:32 2034
<input type="checkbox"/>	12	ISRG Root X1	ISRG Root X1	04/06 11:04:38 2035
<input type="checkbox"/>	13	Izonna.com	Izonna.com	12/12 08:27:25 2037

[Check All](#) / [Uncheck All](#)  
With selected: [Delete Certificate\(s\)](#)

**Import Root Certificate:**  
Filename:  No file chosen

Use Only Trusted Certificates:   Disabled ▼

---

**Secure Web Server:**  
HTTPS:   Disabled ▼

---

**Password:**  
Username:   
Current Password:   
New Password:   
Confirm Password:

## 10. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Aura® Communication Manager, Avaya Aura® Session Manager, Avaya Aura® Session Border Controller for Enterprise and Snom M900 Multicell DECT Phones.

1. Verify that M65 handsets have successfully registered with Session Manager. In System Manager, navigate to **Elements** → **Session Manager** → **System Status** → **User Registrations** to check the registration status.

The screenshot shows the Avaya System Manager 8.1 interface. The main content area is titled "User Registrations" and contains a table of 22 items. The table has the following columns: Details, Address, First Name, Last Name, Actual Location, IP Address, Remote Office, Shared Control, Simult. Devices, AST Device, and Registered (Prim, Sec, Surv, Visiting). Two rows are highlighted with a red box, representing Snom handsets with IP addresses 192.168.100.191.

Details	Address	First Name	Last Name	Actual Location	IP Address	Remote Office	Shared Control	Simult. Devices	AST Device	Registered			
										Prim	Sec	Surv	Visiting
<a href="#">Show</a>	---	Agent	78004	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<a href="#">Show</a>	---	WFC	78051	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<a href="#">Show</a>	---	WFC	78050	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<a href="#">Show</a>	78030@avaya.com	Agent	78030	---	192.168.100.49	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<a href="#">Show</a>	78003@avaya.com	SIP	78003	---	192.168.100.64	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<a href="#">Show</a>	---	Equinox	78040	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<a href="#">Show</a>	78011@avaya.com	Snom	78011	---	192.168.100.191	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<a href="#">Show</a>	78010@avaya.com	Snom	78010	---	192.168.100.191	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- If the M65 handsets are registered to Session Manager through SBCE as remote workers, the **Remote Office** box should be checked as shown below.

- If the M65 handsets are registered to Session Manager through SBCE as remote workers, SBCE also displays the user registrations. From the EMS web interface, navigate to **Status** → **User Registrations** to view the SIP registrations for remote workers as shown below.

AOR	SIP Instance	SBC Device	SM Address	Registration State
78010@10.64.101.102	---	SBCE	10.64.102.117(NONE)	REGISTERED
78011@10.64.101.102	---	SBCE	10.64.102.117(NONE)	REGISTERED
78012@10.64.101.102	---	SBCE	10.64.102.117(NONE)	REGISTERED

- Alternatively, the registration status of the M65 handsets may be viewed on the M900 web user interface as shown below. Navigate to **Extensions** in the left pane to view the registration status.

**Extensions**

AC:

Add extension

Idx	IPEI	Handset State	Handset Type FW Info	FW Progress	VoIP Idx	Extension	Display Name	Server	Server Alias	State	
<input type="checkbox"/>	1	0328DCAF32	Present@RPN00	M65 530.2	Complete	<input type="checkbox"/>	1	78010	10.64.102.117	devcon-sm	SIP Registered@RPN00
<input type="checkbox"/>	2	0328DCAF77	Present@RPN00	M65 530.2	Complete	<input type="checkbox"/>	2	78011	10.64.102.117	devcon-sm	SIP Registered@RPN00
<input type="checkbox"/>	3	0328DCAF5A	Present@RPN00	M65 530.2	Complete	<input type="checkbox"/>	3	78012	10.64.102.117	devcon-sm	SIP Registered@RPN00

[Check All /](#) [Uncheck All](#) [Check All Extensions /](#) [Uncheck All Extensions](#)

With selected: [Delete Handset\(s\)](#) [Register Handset\(s\)](#) [Deregister Handset\(s\)](#) [Start SIP Registration\(s\)](#) [SIP Delete Extension\(s\)](#)

- Establish a call between M65 handset and an Avaya SIP deskphone. The **status trunk** command may be used to view the active call status. The trunk that is being monitored here is the trunk to Session Manager. This command should specify the trunk group and trunk member used for the call. On **Page 2**, **Audio Connection Type** will set to *ip-direct* if the call is shuffled. The **Codec Type** is also displayed.

```

status trunk 10/1                                     Page 2 of 3
CALL CONTROL SIGNALING

Near-end Signaling Loc: PROCR
  Signaling IP Address      Port
  Near-end: 10.64.102.115   : 5061
  Far-end: 10.64.102.117   : 5061
H.245 Near:
H.245 Far:
H.245 Signaling Loc:           H.245 Tunneled in Q.931? no

Audio Connection Type: ip-direct      Authentication Type: None
Near-end Audio Loc:                   Codec Type: G.711MU
  Audio IP Address      Port
  Near-end: 192.168.100.59 : 5004
  Far-end: 192.168.100.191 : 50010

Video Near:
Video Far:
Video Port:
Video Near-end Codec:
Video Far-end Codec:

```

**Page 3** will indicate if SRTP is enabled for the call as shown below.

```
status trunk 10/1                                     Page 3 of 3
                SRC PORT TO DEST PORT TALKPATH
src port: T000001
T000001:TX:192.168.100.191:50010/g711u/20ms/1-srtp-aescm128-hmac80
T000010:RX:192.168.100.59:5004/g711u/20ms/1-srtp-aescm128-hmac80
dst port: T000010
```

7. While the call is active, basic telephony features can be exercised to verify proper operation.

## 11. Conclusion

These Application Notes describe the configuration steps required to integrate Snom M900 Multicell DECT Phones with Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and Avaya Session Border Controller for Enterprise. The Snom M900 Multicell DECT Phones registered directly to Session Manager or to Session Manager through SBCE as remote workers. Calls were then established to H.323 / SIP deskphones and the PSTN with TLS/SRTP. In addition, basic telephony features were verified. All feature and serviceability test cases were completed successfully with observations noted in **Section 2.2**.

## 12. References

This section references the Avaya and Snom documentation relevant to these Application Notes. The Avaya product documentation is available at <http://support.avaya.com>. The Snom product documentation is available at <https://service.snom.com/display/wiki/M900>.

- [1] *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 12, July 2021.
- [2] *Administering Avaya Aura® System Manager for Release 8.1.x*, Release 8.1.x, Issue 15, October 2021.
- [3] *Administering Avaya Aura® Session Manager*, Release 8.1.x, Issue 10, September 2021.
- [4] *Administering Avaya Session Border Controller for Enterprise*, Release 8.1.x, Issue 5, August 2021.
- [5] *Snom M900 and M900 Outdoor Base Station Admin and Installation Guide v1.03*.

---

**©2021 Avaya Inc. All Rights Reserved.**

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

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



VTech Technologies Canada Ltd.

Date: November 15, 2021

## Declaration of Conformance

We, VTech Technologies Canada LTD., declare under sole responsibility that product series DECT M-Series handsets all share the same firmware version. Therefore; the products are expected to behave in the same manner. The differences between the different models in the series are detailed in the table below.

Model	Description
M25	DECT Office Handset, color display, and 3.5 mm headset jack
M65	DECT Professional Handset, Wideband speakerphone
M70	DECT Ruggedized Office Handset, HD Audio, Color LCD, Bluetooth, Alarm
M80	DECT M80 Ruggedized Handset, IP65 Rating, Bluetooth, Alarm
M85	DECT Industrial Handset, IP65 Rating, Bluetooth, Alarm
M90	Antibacterial DECT Handset, JIS-Z 2801 tested, MIL-STD-810g 516.6 tested, IP65 Rating, Bluetooth, Alarm

Please do not hesitate to contact should you require further information.

Thank you,

Ralph Tischler  
Director of Engineering  
Vtech Technologies Canada Ltd  
604-233-5203