



Application Notes for Configuring the ESNA Telephony Office-LinX with Avaya Aura® Session Manager and Avaya Aura® Communication Manager - Issue 1.0

Abstract

These Application Notes describe the procedure for configuring the ESNA Telephony Office-LinX to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager.

The Telephony Office-LinX Enterprise Edition Unified Communications server is a SIP-based voice processing system that functions with an organization's existing telephone system to enhance its overall telecommunications environment.

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 procedure for configuring ESNA Telephony Office-LinX to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager.

ESNA Telephony Office-LinX is a voice processing system that functions with an organization's existing telephone system to enhance its overall telecommunications environment.

ESNA Telephony Office-LinX acts as a unified messaging solution offering call and voice messaging control over the phone, web, or via client applications from the user's desktop PC or mobile smart device. System Administrative functions may be performed either by using a touchtone telephone or the Windows interface from the Voice Mail server.

Additionally, ESNA Telephony Office-LinX provides unified messaging and integration services between the ESNA Telephony Office-LinX system and other messaging systems. Using a combination of IMAP4, MAPI and Web Services based protocols, the unified messaging system provides an easily manageable and highly scalable system that supports message, calendar and contact synchronization on a broad range of messaging platforms including Microsoft Exchange, Google G-mail, Lotus Domino, Novell Groupwise and others.

1.1. Interoperability Compliance Testing

The interoperability compliance testing included features and serviceability tests. The focus of the compliance testing was primarily on verifying the interoperability between ESNA Telephony Office-LinX, Session Manager, and Communication Manager.

1.2. Support

Technical support for the ESNA Telephony Office-LinX solution can be obtained by contacting ESNA:

- URL – techsupport@esna.com
- Phone – (905) 707-1234

2. Reference Configuration

Figure 1 illustrates the configuration used in these Application Notes. The sample configuration shows an enterprise with a Session Manager and an Avaya S8300D Server with an Avaya G450 Media Gateway. Endpoints include Avaya 9600 Series SIP IP Telephones, Avaya 9600 Series H.323 IP Telephones, and an Avaya 6408D Digital Telephone. Avaya S8720 Servers with Avaya G650 Media Gateway were included in the test to provide an inter-switch scenario.

ESNA Telephony Office-LinX does not register with the Session Manager as an endpoint but instead is configured as a trusted SIP entity.

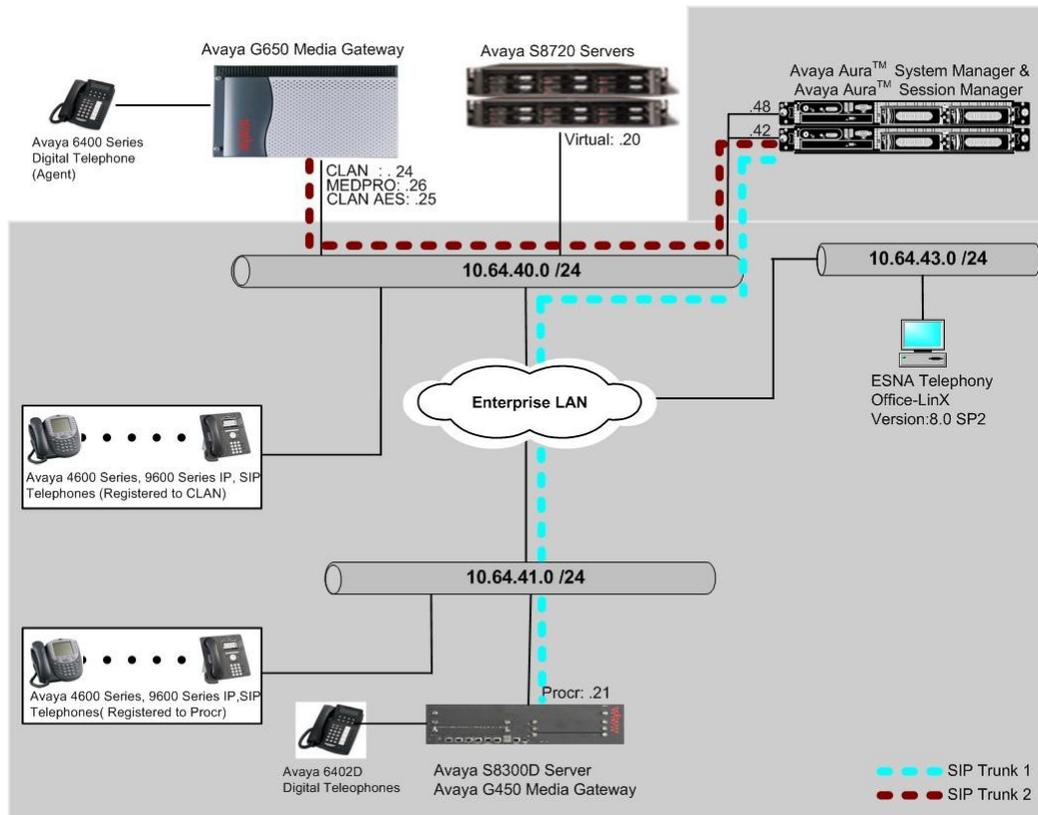


Figure 1: Test Configuration of ESNA Telephony Office-LinX

3. Equipment and Software Validated

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

Equipment		Software/Firmware
Avaya S8300 Media Server with Avaya G450 Media Gateway		Avaya Aura® Communication Manager 6.0 (R016x.00.0.345.0) with Patch 00.0345.0-18246
Avaya Aura® System Manager		Avaya Aura® System Manager 6.0.0 (6.0.0.0-556-3.0.6.0)
Avaya Aura® Session Manager		Avaya Aura® System Manager 6.0.0 (6.0.0.0.600020)
Avaya S8720 Servers with Avaya G650 Media Gateway		Avaya Aura® Communication Manager 5.2 1(R015x.02.0.947.3)
Avaya 4600 and 9600 Series SIP Telephones		
	9620 (SIP)	2.5
	9630 (SIP)	2.5
	9650 (SIP)	2.5
Avaya 4600 and 9600 Series IP Telephones		
	4625 (H.323)	2.9
	9620 (H.323)	3.1
	9630 (H.323)	3.1
	9650 (H.323)	3.1
Avaya 6408D+ Digital Telephone		-
ESNA Telephony Office-LinX		8.0 with SP 2

4. Configure Avaya Aura® Communication Manager

In the compliance test, Communication Manager was set up as an Evolution Server (Full Call Model). This section describes the procedure for setting up a SIP trunk between Communication Manager and Session Manager. The steps include setting up an IP codec set, an IP network region, IP node name, a signaling group, a trunk group, and a SIP station. Before a trunk can be configured, it is necessary to verify if there is enough capacity to setup an additional trunk. The highlights in the following screens indicate the values used during the compliance test. Default values may be used for all other fields.

These steps are performed from the Communication Manager System Access Terminal (SAT) interface. All SIP telephones, except ESNA Telephony Office-LinX, are configured as off-PBX telephones in Communication Manager.

4.1. Capacity Verification

Enter the **display system-parameters customer-options** command. Verify that there are sufficient Maximum Off-PBX Telephones – OPS licenses.

If not, contact an authorized Avaya account representative to obtain additional licenses

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

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

                                                USED
Platform Maximum Ports: 6400 185
Maximum Stations: 500 19
Maximum XMOBILE Stations: 2400 0
Maximum Off-PBX Telephones - EC500: 10 0
Maximum Off-PBX Telephones - OPS: 500 9
Maximum Off-PBX Telephones - PBFMC: 10 0
Maximum Off-PBX Telephones - PVFMC: 10 0
Maximum Off-PBX Telephones - SCCAN: 0 0
Maximum Survivable Processors: 0 0
```

On **Page 2** of the form, verify that the number of SIP trunks supported by the system is sufficient for the number of SIP trunks needed.

If not, contact an authorized Avaya account representative to obtain additional licenses.

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

IP PORT CAPACITIES                                                USED
Maximum Administered H.323 Trunks: 4000 20
Maximum Concurrently Registered IP Stations: 2400 3
Maximum Administered Remote Office Trunks: 4000 0
Maximum Concurrently Registered Remote Office Stations: 2400 0
Maximum Concurrently Registered IP eCons: 68 0
Max Concur Registered Unauthenticated H.323 Stations: 100 0
Maximum Video Capable Stations: 2400 0
Maximum Video Capable IP Softphones: 10 0
Maximum Administered SIP Trunks: 4000 110
Maximum Administered Ad-hoc Video Conferencing Ports: 4000 0
Maximum Number of DS1 Boards with Echo Cancellation: 80 0
Maximum TN2501 VAL Boards: 10 0
Maximum Media Gateway VAL Sources: 50 0
Maximum TN2602 Boards with 80 VoIP Channels: 128 0
Maximum TN2602 Boards with 320 VoIP Channels: 128 0
Maximum Number of Expanded Meet-me Conference Ports: 8 0
```

4.2. IP Codec Set

This section describes the steps for administering a codec set in Communication Manager. This codec set is used in the IP network region for communications between Communication Manager and Session Manager. Enter the **change ip-codec-set <c>** command, where **c** is a number between **1** and **7**, inclusive. IP codec sets are used in **Section 4.3** for configuring IP network region to specify which codec sets may be used within and between network regions.

Note: ESNA Telephony Office-LinX supports G.711MU and G.711A. Thus, these two codecs were tested during the compliance test.

```
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
```

4.3. Configure IP Network Region

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

- **Authoritative Domain** – Enter the appropriate name for the Authoritative Domain. During the compliance test, the authoritative domain is set to **avaya.com**. This should match the SIP Domain value on Session Manager, in **Section 5.1**.
- **Codec Set** – Set the codec set number as provisioned in **Section 4.2**.

```
change ip-network-region 1                               Page 1 of 20

                                IP NETWORK REGION

Region: 1
Location:      Authoritative Domain: avaya.com
Name:
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: 3329
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
H.323 IP ENDPOINTS    AUDIO RESOURCE RESERVATION PARAMETERS
H.323 Link Bounce Recovery? y      RSVP Enabled? n
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5
```

4.4. Configure IP Node Name

This section describes the steps for setting IP node name for Session Manager in Communication Manager. Enter the **change node-names ip** command, and add a node name for Session Manager along with its IP address.

```
change node-names ip                                     Page 1 of 2
                                                    IP NODE NAMES
Name          IP Address
CLAN          10.64.40.24
SES           10.64.40.41
SM-1          10.64.40.42
default       0.0.0.0
procr         10.64.41.21
procr6        ::
rdtt          10.64.40.201
s8300-lsp     10.64.42.21
```

4.5. Configure SIP Signaling

Enter the **add signaling-group <s>** command, where **s** is an available signaling group and configure the following:

- **Group Type** – Set to **sip**.
- **IMS Enabled** – Verify that the field is set to **n**. Setting this field to **y** will cause Communication Manager to behave as a Feature Server.
- **Transport Method** – Set to **tls** (Transport Layer Security).
- **Near-end Node Name** – Set to **procr** as displayed in **Section 4.4**.
- **Far-end Node Name** – Set to the Session Manager name configured in **Section 4.4**.
- **Far-end Network Region** – Set to the region configured in **Section 4.3**.
- **Far-end Domain** – Set to **avaya.com**. This should match the SIP Domain value in **Section 4.3**.
- **Direct IP-IP Audio Connections** – Set to **y**, since the shuffling is enabled during the compliance test

```
add signaling-group 92
                                                    SIGNALING GROUP
Group Number: 92
Group Type: sip
IMS Enabled? n
Transport Method: tls
Q-SIP? n
SIP Enabled LSP? n
IP Video? n
Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y Peer Server: SM
Near-end Node Name: procr
Far-end Node Name: SM-1
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
DTMF over IP: rtp-payload
RFC 3389 Comfort Noise? n
Session Establishment Timer(min): 3
Direct IP-IP Audio Connections? y
IP Audio Hairpinning? n
Enable Layer 3 Test? n
Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n
Alternate Route Timer(sec): 6
```

4.6. Configure Trunk Group

To configure the associate trunk group, enter the **add trunk-group <t>** command, where **t** is an available trunk group and configure the following:

- **Group Type** – Set the Group Type field to **sip**.
- **Group Name** – Enter a descriptive name.
- **TAC (Trunk Access Code)** – Set to any available trunk access code.
- **Service Type** – Set the Service Type field to **tie**.
- **Signaling Group** – Set to the Group Number field value for the signalling group configured in **Section 4.5**
- **Number of Members** – Allowed value is between 0 and 255. Set to a value large enough to accommodate the number of SIP telephone extensions being used.

```
add trunk-group 92                                     Page 1 of 21
                                                    TRUNK GROUP
Group Number: 92                                     Group Type: sip                                     CDR Reports: y
Group Name: NO IMS SIP trk                           COR: 1      TN: 1      TAC: 1092
Direction: two-way      Outgoing Display? n
Dial Access? n      Night Service:
Queue Length: 0
Service Type: tie      Auth Code? n
Member Assignment Method: auto
Signaling Group: 92
Number of Members: 20
```

On **Page 3**, set the Numbering Format field to **unk-pvt**.

```
add trunk-group 92                                     Page 3 of 21
TRUNK FEATURES
ACA Assignment? n      Measured: none
Maintenance Tests? y
Numbering Format: unk-pvt
UII Treatment: service-provider
Replace Restricted Numbers? n
Replace Unavailable Numbers? n
Modify Tandem Calling Number: no
Show ANSWERED BY on Display? y
```

4.7. Configure Hunt Group

This section describes the steps for administering a hunt group in Communication Manager. Enter the **add hunt-group <h>** command, where **h** is an available hunt group number. The following fields were configured for the compliance test.

- **Group Name** – Enter a descriptive name
- **Group Extension** – Enter an extension valid in the provisioned dial plan.

```
Add hunt-group 92                                     Page 1 of 60
                                                    HUNT GROUP

Group Number: 92                                     ACD? n
Group Name: ESNA                                     Queue? n
Group Extension: 70000                               Vector? n
Group Type: ucd-mia                                  Coverage Path:
TN: 1                                                 Night Service Destination:
COR: 1                                                MM Early Answer? n
Security Code:                                       Local Agent Preference? n
ISDN/SIP Caller Display:
```

On **Page 2**, provide the following information:

- **Message Center** – Enter **sip-adjunct**, indicating the type of messaging adjunct used for this hunt group. This value will also be used in the Station form.
- **Voice Mail Number** – Enter the Voice Mail Number, which is the extension of ESNA Telephony Office-LinX.
- **Voice Mail Handle** – Enter the Voice Mail Handle which is the extension of ESNA Telephony Office-LinX.
- **Routing Digit (e.g. AAR/ARS Access Code)** – Enter the AAR Access Code as defined in the Feature Access Code form.

```
add hunt-group 92                                     Page 2 of 60
                                                    HUNT GROUP

Message Center: sip-adjunct

Voice Mail Number      Voice Mail Handle      Routing Digits
(e.g., AAR/ARS Access Code)
72031                  72031                  8
```

4.8. Configure Coverage Path

This section describes the steps for administering coverage path in Communication Manager. Enter the **add coverage path <s>** command, where **s** is a valid coverage path number. The Point1 value of **h92** is used to represent the hunt group number 92 created in **Section 4.7**. The default values for the other fields may be used.

```
add coverage path 92                                     Page 1 of 1
                                                    COVERAGE PATH
                                                    Coverage Path Number: 92
Cvg Enabled for VDN Route-To Party? n                Hunt after Coverage? n
                                                    Next Path Number:                Linkage

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

COVERAGE POINTS
    Terminate to Coverage Pts. with Bridged Appearances? n
Point1: h92                Rng:    Point2:
Point3:                    Point4:
Point5:                    Point6:
```

4.9. Configure SIP Endpoint

SIP endpoints and off-pbx-telephone stations will be automatically created in Communication manager when users (SIP endpoints) were created in Session Manager.

4.10. Configure Route Pattern

For the trunk group created in **Section 4.6**, define the route pattern by entering the **change route-pattern <r>** command, where **r** is an unused route pattern number. The route pattern consists of a list of trunk groups that can be used to route a call. The following screen shows route-pattern 92 will utilize the trunk group 92 to route calls. The default values for the other fields may be used.

```
change route-pattern 92                                     Page 1 of 3
                    Pattern Number: 92  Pattern Name: IMS SIP trunk
                    SCCAN? n          Secure SIP? n
  Grp FRL NPA Pfx Hop Toll No.  Inserted
  No   Mrk Lmt List Del  Digits
                    Dgts
1: 92 0
2:
3:
4:
5:
6:
                    DCS/ IXC
                    QSIG
                    Intw
                    n  user
                    n  user
                    n  user
                    n  user
                    n  user

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

4.11. Configure AAR Analysis

For the AAR Analysis Table, create the dial string that will map calls to the Telephony Office-LinX via the route pattern created in **Section 4.10**. Enter the **change aar analysis <x>** command, where **x** is a starting partial digit (or full digit). The dialed string created in the AAR Digit Analysis table should contain a map to the Telephony Office-LinX system extension, which is configured as x72031. During the configuration of the aar table, the Call Type field was set to **unku**.

```
change aar analysis 720                                     Page 1 of 2
                    AAR DIGIT ANALYSIS TABLE
                    Location: all          Percent Full: 3

  Dialed          Total      Route      Call      Node      ANI
  String          Min Max  Pattern  Type      Num      Reqd
7202             5   5    92      unku      n
7203             5   5    92      unku      n
```

5. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager as provisioned in the reference configuration. Session Manager is comprised of two functional components: the Session Manager server and the System Manager server. All SIP call provisioning for Session Manager is performed through the System Manager Web interface and is then downloaded into Session Manager.

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

In this section, the following topics are discussed:

- SIP Domains
- Locations
- SIP Entities
- Entity Links
- Time Ranges
- Routing Policy
- Dial Patterns
- Manage Element
- Applications
- Application Sequence
- User Management
- Synchronization

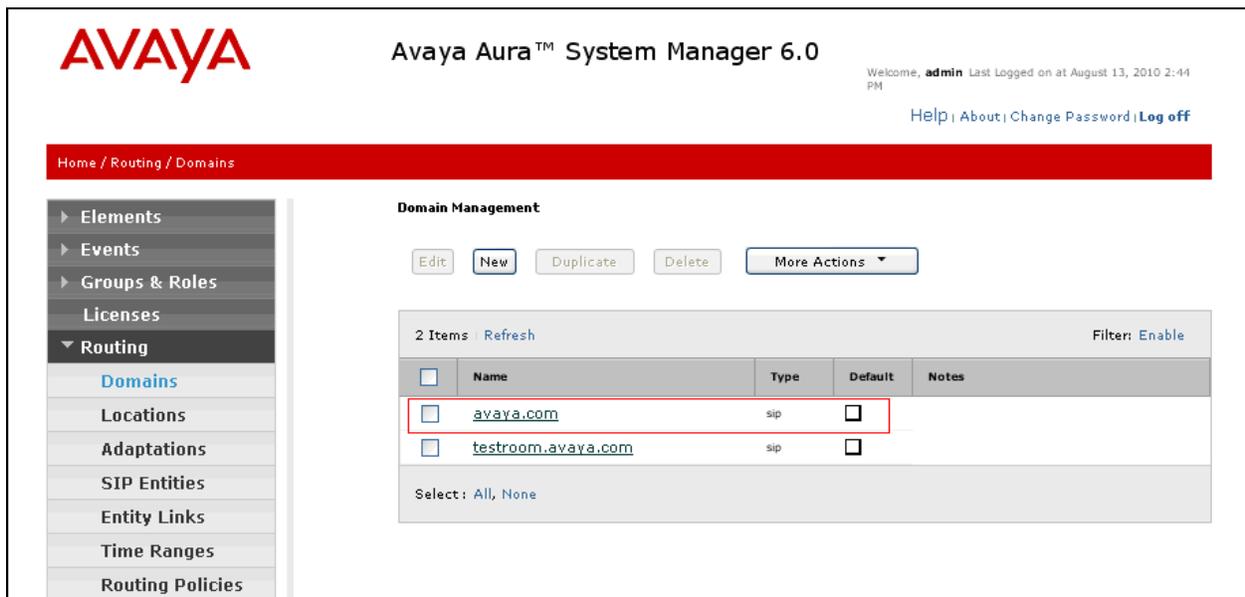
5.1. Configure SIP Domain

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

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

- **Name** – Enter the Authoritative Domain Name specified in **Section 4.3**, which is **avaya.com**.
- **Type** – Select **SIP**

Click **Commit** to save. The following screen shows the Domains page used during the compliance test.



The screenshot shows the Avaya Aura System Manager 6.0 interface. The top navigation bar includes the Avaya logo, the product name, and user information. The left sidebar shows a menu with 'Routing' expanded to 'Domains'. The main content area is titled 'Domain Management' and contains a table of domains. The table has columns for Name, Type, Default, and Notes. Two domains are listed: 'avaya.com' and 'testroom.avaya.com', both with a type of 'sip'. The 'avaya.com' row is highlighted with a red box. Below the table, there is a 'Select' dropdown menu set to 'All, None'.

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

5.2. Configure Locations

Locations are used to identify logical and/or physical locations where SIP Entities reside, for purposes of bandwidth management or location-based routing.

Navigate to **Routing** → **Locations**, and click on the **New** button (not shown) to create a new SIP endpoint location.

General section

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

- Enter a descriptive Location name in the Name field (e.g. **S8300-Subnet**).
- Enter a description in the **Notes** field if desired.

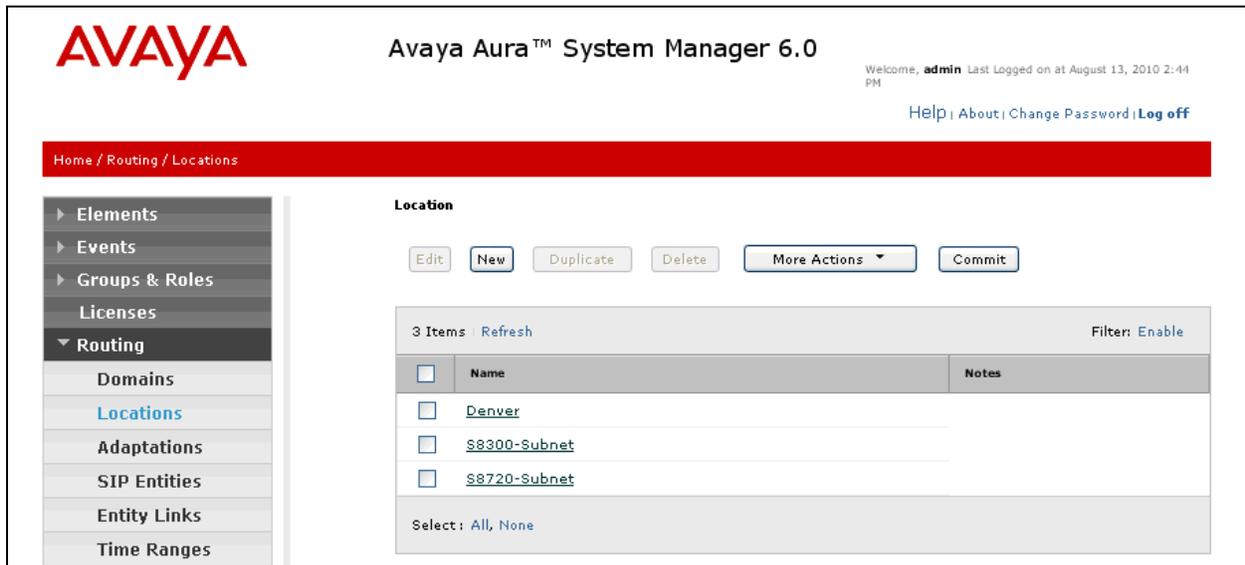
Location Pattern section

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

- Enter the IP address information for the IP address Pattern (e.g. **10.64.41.***)
- Enter a description in the **Notes** field if desired.

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

Repeat all the steps for each new Location. The following screen shows the Locations page used during the compliance test.



The screenshot shows the Avaya Aura System Manager 6.0 interface. The top left features the Avaya logo. The top right displays the user name 'admin' and the last login time 'August 13, 2010 2:44 PM'. Below this, there are links for 'Help', 'About', 'Change Password', and 'Log off'. A red breadcrumb trail indicates the current path: 'Home / Routing / Locations'. On the left side, a navigation menu is visible with categories like 'Elements', 'Events', 'Groups & Roles', 'Licenses', and 'Routing'. Under 'Routing', 'Locations' is highlighted. The main content area is titled 'Location' and contains several action buttons: 'Edit', 'New', 'Duplicate', 'Delete', 'More Actions', and 'Commit'. Below these buttons is a table with 3 items, a 'Refresh' button, and a 'Filter: Enable' option. The table has columns for 'Name' and 'Notes'. The items listed are 'Denver', 'S8300-Subnet', and 'S8720-Subnet'. At the bottom of the table, there is a 'Select: All, None' option.

5.3. Configure SIP Entities

A SIP Entity must be added for Session Manager and for each network component that has a SIP trunk provisioned to Session Manager. During the compliance test, the following SIP Entities were configured:

- Session Manager itself.
- Communication Manager
- ESNA-iVR

Navigate to **Routing → SIP Entities**, and click on the **New** button (not shown) to create a new SIP entity. Provide the following information:

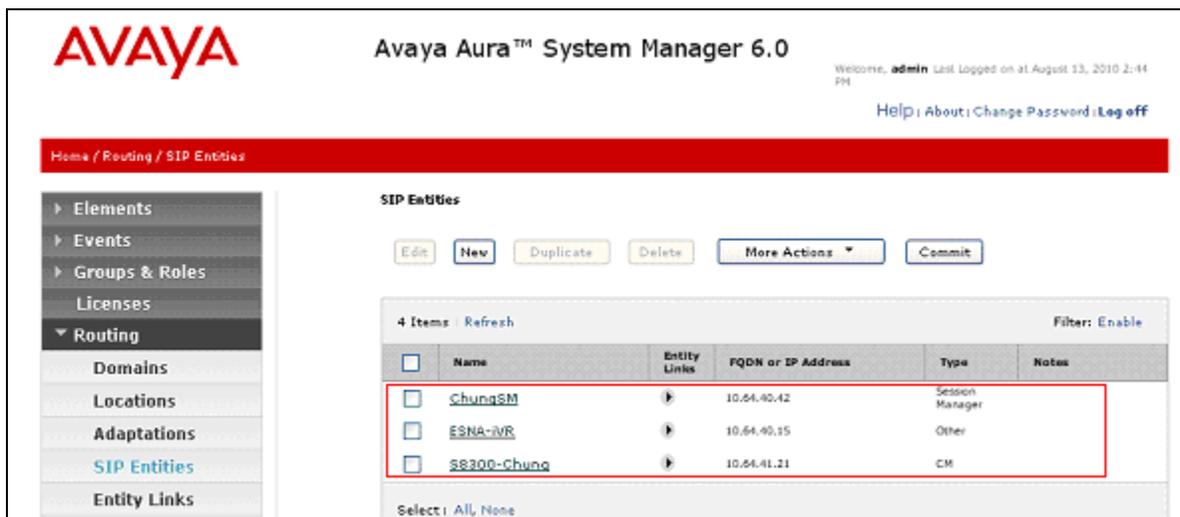
General section

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

- Enter a descriptive Location name in the Name field.
- Enter IP address for signaling interface on each Communication Manager, virtual SM-100 interface on Session Manager, or 3rd party device on the FQDN or IP Address field
- From the **Type** drop down menu select a type that best matches the SIP Entity.
 - For Communication Manager, select CM
 - For Session Manager, select Session Manager
 - For ESNA, select **Other**
- Enter a description in the **Notes** field if desired.
- Select the appropriate time zone.
- Accept the other default values.

Click on the **Commit** button to save each SIP entity. The following screen shows the SIP Entities page used during the compliance test.

Repeat all the steps for each new entity.



The screenshot shows the Avaya Aura System Manager 6.0 interface. The top navigation bar includes the Avaya logo, the product name "Avaya Aura™ System Manager 6.0", and a user status "Welcome, admin Last Logged on at August 13, 2010 2:44 PM". Below the navigation bar is a breadcrumb trail "Home / Routing / SIP Entities". The main content area is titled "SIP Entities" and contains a table with 4 items. The table has columns for Name, Entity Links, FQDN or IP Address, Type, and Notes. The table is highlighted with a red border. The table contains the following data:

<input type="checkbox"/>	Name	Entity Links	FQDN or IP Address	Type	Notes
<input type="checkbox"/>	ChungSM	▶	10.64.40.42	Session Manager	
<input type="checkbox"/>	ESNA-iVR	▶	10.64.40.15	Other	
<input type="checkbox"/>	SS300-Chung	▶	10.64.41.21	CM	

5.4. Configure Entity Links

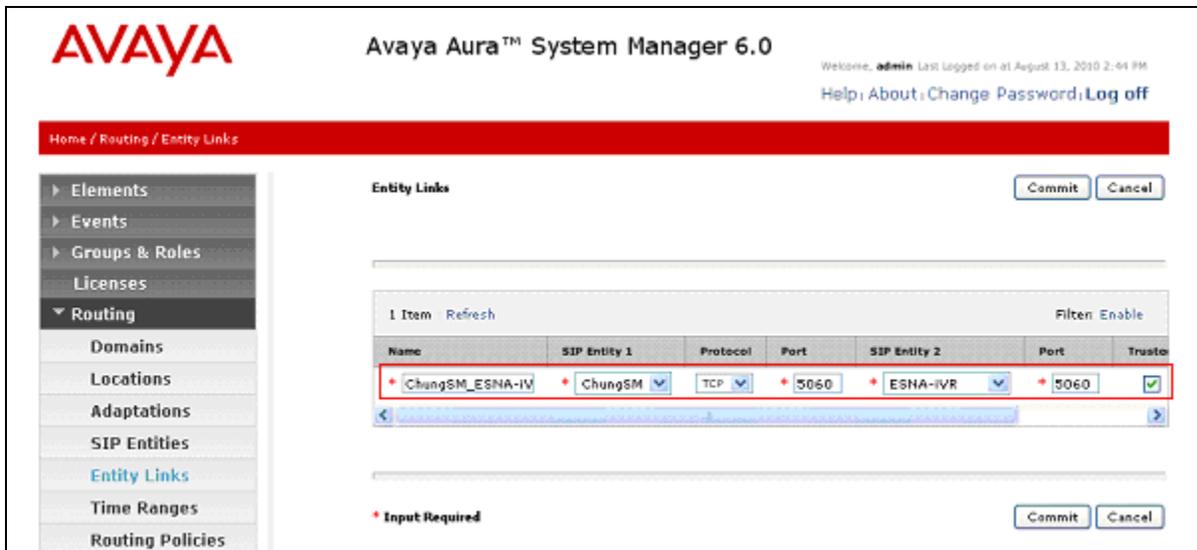
Entity Links define the connections between the SIP Entities and Session Manager. In the compliance test, the following entity links are defined from Session Manager.

- Session Manager ↔ Communication Manager (Avaya S8300D Server)
- Session Manager ↔ ESNA-iVR

Navigate to **Routing** → **Entity Links**, and click on the **New** button (not shown) to create a new entity link. Provide the following information:

- Enter a descriptive name in the **Name** field.
- In the **SIP Entity 1** drop down menu, select the Session Manager SIP Entity created in **Section 5.3** (e.g. **ChungSM**).
- In the **Protocol** drop down menu, select the protocol to be used.
- In the **Port** field, enter the port to be used (e.g. **5060** or **5061**).
 - TLS – 5061
 - UDP or TCP – 5060
- In the **SIP Entity 2** drop down menu, select an entity created in **Section 5.3**.
- In the **Port** field, enter the port to be used (e.g. **5060** or **5061**).
- Check the **Trusted** box.
- Enter a description in the **Notes** field if desired.

Click on the **Commit** button to save each Entity Link definition. The following screen shows an Entity Links page (between Session Manager and ESNA-iVR) used during the compliance test.



The screenshot shows the Avaya Aura System Manager 6.0 interface. The breadcrumb trail is Home / Routing / Entity Links. The left sidebar shows the navigation menu with 'Entity Links' selected. The main content area is titled 'Entity Links' and contains a table with one item. The table has columns for Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, and Trusted. The row shows 'ChungSM_ESNA-IV' with 'ChungSM' as SIP Entity 1, 'TCP' as Protocol, '5060' as Port, 'ESNA-iVR' as SIP Entity 2, '5060' as Port, and the 'Trusted' checkbox checked. There are 'Commit' and 'Cancel' buttons at the top right and bottom right of the table area.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
* ChungSM_ESNA-IV	* ChungSM	TCP	* 5060	* ESNA-iVR	* 5060	<input checked="" type="checkbox"/>

Repeat the steps to define Entity Links between Session Manager and Communication Manager.

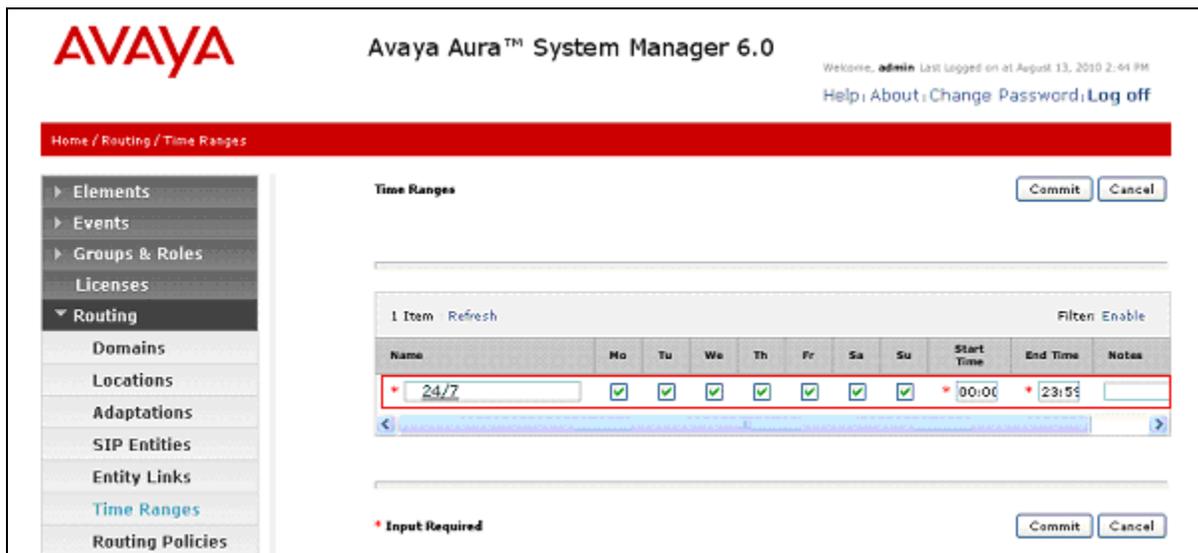
5.5. Time Ranges

The Time Ranges form allows admission control criteria to be specified for Routing Policies (**Section 5.6**). In the reference configuration, no restrictions were used.

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

- Enter a descriptive Location name in the **Name** field (e.g. **24/7**).
- Check each day of the week.
- In the **Start Time** field, enter **00:00**.
- In the **End Time** field, enter **23:59**.
- Enter a description in the **Notes** field if desired.

Click the **Commit** button. The following screen shows the Time Range page used during the compliance test.



5.6. Configure Routing Policy

Routing Policies associate destination SIP Entities ([Section 5.3](#)) with Time of Day admission control parameters ([Section 5.5](#)) and Dial Patterns ([Section 5.7](#)). In the reference configuration, Routing Policies are defined for:

- Inbound calls to Communication Manager.
- Outbound calls to the ESNA-iVR

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

General section

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

SIP Entity as Destination section

- Click the **Select** button.
- Select the SIP Entity that will be the destination for this call (not shown).
- Click the **Select** button and return to the Routing Policy Details form.

Time of Day section

- Leave default values.

Click **Commit** to save Routing Policy definition. The following screen shows the Routing Policy used for ESNA-iVR during the compliance test.

The screenshot displays the Avaya Aura System Manager 6.0 interface. The breadcrumb trail is 'Home / Routing / Routing Policies / Routing Policy Details'. The left sidebar shows a navigation menu with 'Routing Policies' selected. The main content area is titled 'Routing Policy Details' and contains three sections: 'General', 'SIP Entity as Destination', and 'Time of Day'. In the 'General' section, the 'Name' field is set to 'to ESNA-iVR'. In the 'SIP Entity as Destination' section, a 'Select' button is present, and a table lists the selected entity 'ESNA-iVR' with FQDN '10.61.40.15' and Type 'Other'. In the 'Time of Day' section, a table shows a single time range with a ranking of 0, name '24/7', and start/end times of 00:00 and 23:59 respectively. The 'Filter: Enable' checkbox is checked.

Name	FQDN or IP Address	Type	Notes
ESNA-iVR	10.61.40.15	Other	

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
0	24/7	✓	✓	✓	✓	✓	✓	✓	00:00	23:59	

Repeat the steps to define a routing policy to Communication Manager.

5.7. Dial Patterns

Dial Patterns define digit strings to be matched for inbound and outbound calls. In addition, the domain in the request URI is also examined. In the compliance test, the following dial patterns are defined from Session Manager.

- 7202x – SIP endpoints in Avaya S8300D Server
- 72031 – ESNA iVR SIP endpoint

To add a Dial Pattern, select **Routing** → **Dial Patterns**, and click on the **New** button (not shown) on the right. During the compliance test, 5 digit dial plan was utilized. Provide the following information:

General section

- Enter a unique pattern in the **Pattern** field (e.g. **72031**).
- In the **Min** field enter the minimum number of digits (e.g. **5**).
- In the **Max** field enter the maximum number of digits (e.g. **5**).
- In the **SIP Domain** field drop down menu select the domain that will be contained in the Request URI *received* by Session Manager from Communication Manager.
- Enter a description in the **Notes** field if desired.

Originating Locations and Routing Policies section

- Click on the **Add** button and a window will open (not shown).
- Click on the boxes for the appropriate Originating Locations (see **Section 5.2**), and Routing Policies (see **Section 5.6**) that pertain to this Dial Pattern.
 - Location **10.64.41.0**.
 - Routing Policies **To ESNA-iVR**.
 - Click on the **Select** button and return to the Dial Pattern window.

Click the **Commit** button to save the new definition. The following screen shows the dial pattern used for ESNA-iVR during the compliance test.

Dial Pattern Details [Commit] [Cancel]

General

* Pattern: 72031

* Min: 5

* Max: 5

Emergency Call:

SIP Domain: avaya.com

Notes: ESNA iVR extension

Originating Locations and Routing Policies

[Add] [Remove]

1 Item Refresh Filter: Enable

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

5.8. Configure Managed Elements

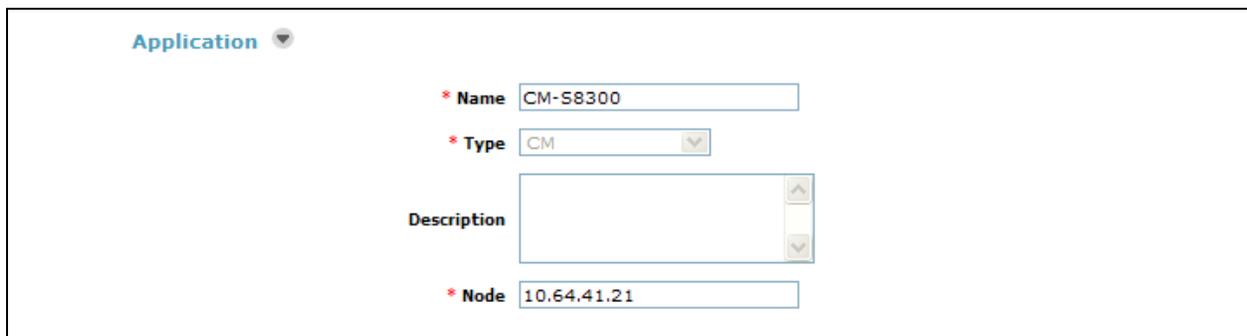
To define a new Managed Element, navigate to **Elements** → **Inventory** → **Manage Elements**. Click on the **New** button (not shown) to open the **New Entities Instance** page.

In the **New Entities Instance** Page

- In the **Type** field, select **CM** using the drop-down menu, and the **New CM Instance** page opens (not shown).

In the New CM Instance Page, provide the following information:

- Application section
 - **Name** – Enter name for Communication Manager Evolution Server.
 - **Description** - Enter description if desired.
 - **Node** – Enter IP address of the administration interface. During the compliance test, the procr IP address (10.64.41.21) was utilized.



The screenshot shows a web form titled "Application" with a dropdown arrow. Below the title are four fields:

- * Name**: A text input field containing "CM-58300".
- * Type**: A dropdown menu with "CM" selected.
- Description**: A text area with up and down arrows on the right side, currently empty.
- * Node**: A text input field containing "10.64.41.21".

- Leave the fields in the Port and Access Point sections blank. In the SNMP Attributes section, verify the default value of **None** is selected for the Version field.

- Attributes section.

System Manager uses the information entered in this section to log into Communication Manager using its administration interface. Enter the following values and use default values for remaining fields.

- **Login** – Enter login used for administration access
- **Password** – Enter password used for administration access
- **Confirm Password** – Repeat value entered in above field.
- **Is SSH Connection** – Check the check box.
- **Port** – Verify **5022** has been entered as default value

The screenshot shows the 'Attributes' configuration page. The fields are as follows:

- * Login:** init
- Password:** masked with dots
- Confirm Password:** masked with dots
- Is SSH Connection:** checked
- * Port:** 5022
- Alternate IP Address:** empty
- RSA SSH Fingerprint (Primary IP):** empty
- RSA SSH Fingerprint (Alternate IP):** empty
- Is ASG Enabled:** unchecked
- ASG Key:** empty
- Confirm ASG Key:** empty
- Location:** empty

Click **Commit** to save the element. The following screen shows the element created, CM-S8300, during the compliance test.

The screenshot shows the 'Manage Elements' page in Avaya Aura System Manager 6.0. The page title is 'Avaya Aura™ System Manager 6.0'. The user is 'admin' and last logged on at August 13, 2010 2:44 PM. The breadcrumb is 'Home / Elements / Application Management / Applications'. The left navigation menu includes 'Elements', 'Conferencing', 'Presence', 'Application Management', 'Endpoints', 'SIP AS 8.1', 'Feature Management', and 'Inventory'. The main content area shows 'Manage Elements' with a table of entities.

Entities

View Edit New Delete More Actions

1 Item Refresh Show ALL Filter: Enable

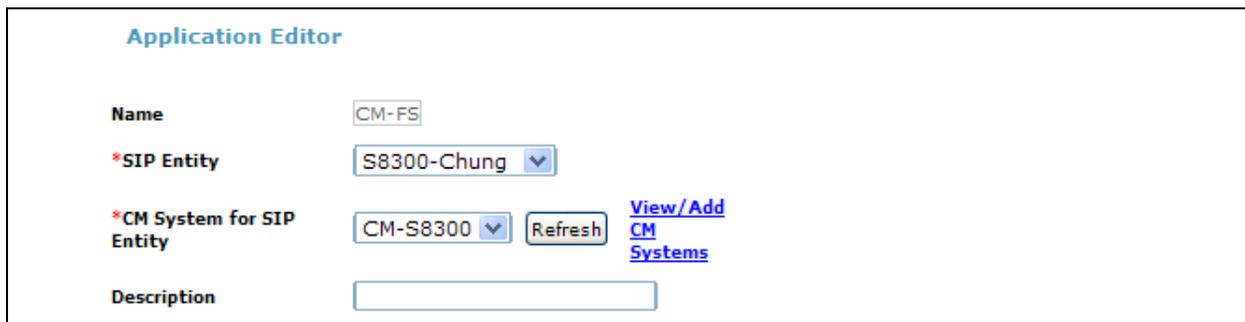
	Name	Node	Type	Version	Description
<input type="checkbox"/>	CM-S8300	10.64.41.21	CM		

Select: All, None

5.9. Configure Applications

To define a new Application, navigate to **Elements → Session Manager → Application Configuration → Applications**. Click **New** (not shown) to open the Applications Editor page, and provide the following information:

- Application Editor section
 - **Name** – Enter name for the application.
 - **SIP Entity** - Select SIP Entity for Communication Manager Evolution Server defined in **Section 5.3**
 - **CM System for SIP Entity** – Select name of Managed Element defined for Communication Manager in **Section 5.8**
 - **Description** – Enter description if desired.



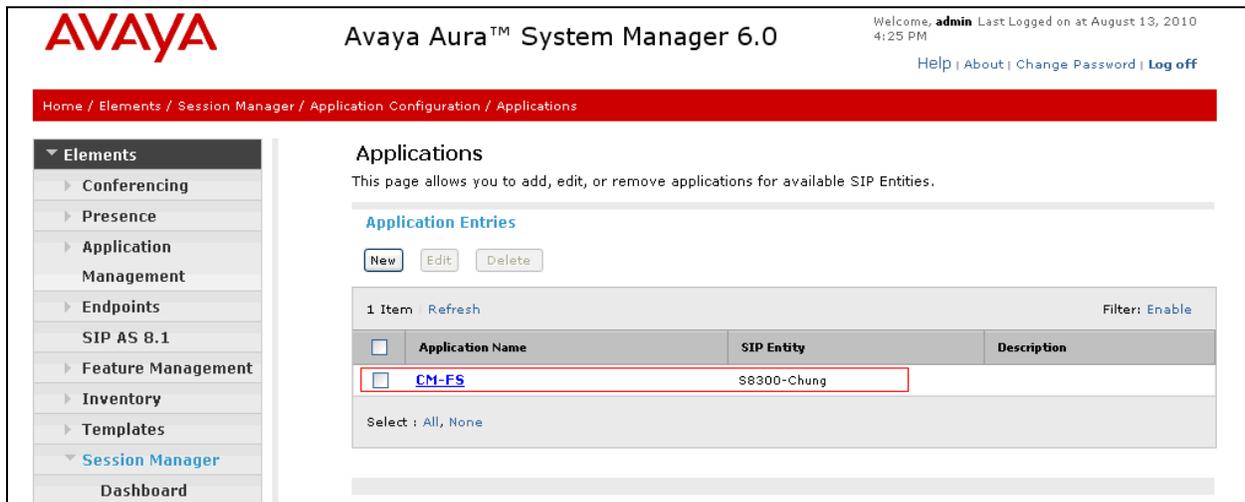
The screenshot shows the 'Application Editor' form with the following fields and values:

- Name:** CM-FS
- *SIP Entity:** S8300-Chung
- *CM System for SIP Entity:** CM-S8300
- Description:** (empty)

Additional controls include a 'Refresh' button and a link 'View/Add CM Systems'.

- Leave fields in the Application Attributes (optional) section blank.

Click the **Commit** button (not shown) to save the Application. The screen below shows the Application, CM-FS, defined for Communication Manager.



The screenshot shows the Avaya Aura™ System Manager 6.0 interface. The page title is 'Avaya Aura™ System Manager 6.0'. The user is 'admin' and last logged on at August 13, 2010 4:25 PM. The breadcrumb trail is 'Home / Elements / Session Manager / Application Configuration / Applications'. The left sidebar shows a tree view with 'Session Manager' selected. The main content area is titled 'Applications' and contains the following information:

- Applications**
This page allows you to add, edit, or remove applications for available SIP Entities.
- Application Entries**
Buttons: New, Edit, Delete
- 1 Item Refresh Filter: Enable

<input type="checkbox"/>	Application Name	SIP Entity	Description
<input type="checkbox"/>	CM-FS	S8300-Chung	

- Select : All, None

5.10. Define Application Sequence

Navigate to **Elements** → **Session Manager** → **Application Configuration** → **Application Sequences**. Click **New** (not shown) and provide the following information:

- Sequence Name section
 - **Name** – Enter name for the application
 - **Description** – Enter description, if desired.

Sequence Name

Name

Description

- Available Applications section
 - Click **+** icon associated with the Application for Communication Manager defined in **Section 5.9** to select this application.
 - Verify a new entry is added to the Applications in this Sequence table as shown below.

Click the **Commit** button (not shown) to save the new Application Sequence.

Applications in this Sequence

1 Item

<input type="checkbox"/>	Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
<input type="checkbox"/>	▲ ▼ ✕	CM-FS	S8300-Chung	<input checked="" type="checkbox"/>	

Select : All, None

Available Applications

1 Item Refresh Filter: Enable

	Name	SIP Entity	Description
<input type="checkbox"/>	CM-FS	S8300-Chung	

The screen below shows the Application Sequence, CM-FS, defined during the compliance test.

The screenshot shows the Avaya Aura System Manager 6.0 interface. At the top left is the AVAYA logo. The page title is "Avaya Aura™ System Manager 6.0". On the top right, it says "Welcome, admin Last Logged on at August 13, 2010 4:25 PM" and provides links for "Help | About | Change Password | Log off". A red breadcrumb trail reads "Home / Elements / Session Manager / Application Configuration / Application Sequences". On the left is a navigation menu under "Elements" with options: Conferencing, Presence, Application Management, Endpoints, SIP AS 8.1, Feature Management, Inventory, Templates, Session Manager, and Dashboard. The main content area is titled "Application Sequences" and includes the text "This page allows you to add, edit, or remove sequences of applications." Below this are "New", "Edit", and "Delete" buttons. A summary bar shows "1 Item" and "Refresh" with a "Filter: Enable" option. A table lists the application sequence:

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	CM-FS	

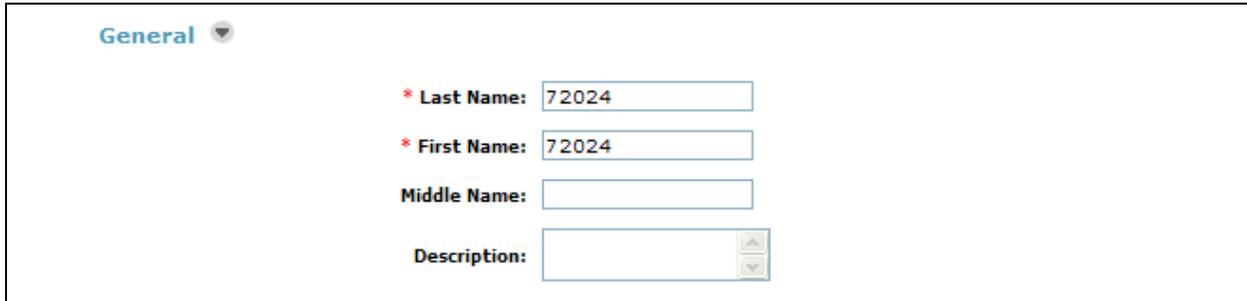
At the bottom of the table, it says "Select : All, None".

Repeat steps if multiple applications are needed as part of the Application Sequence.

5.11. Configure SIP Users

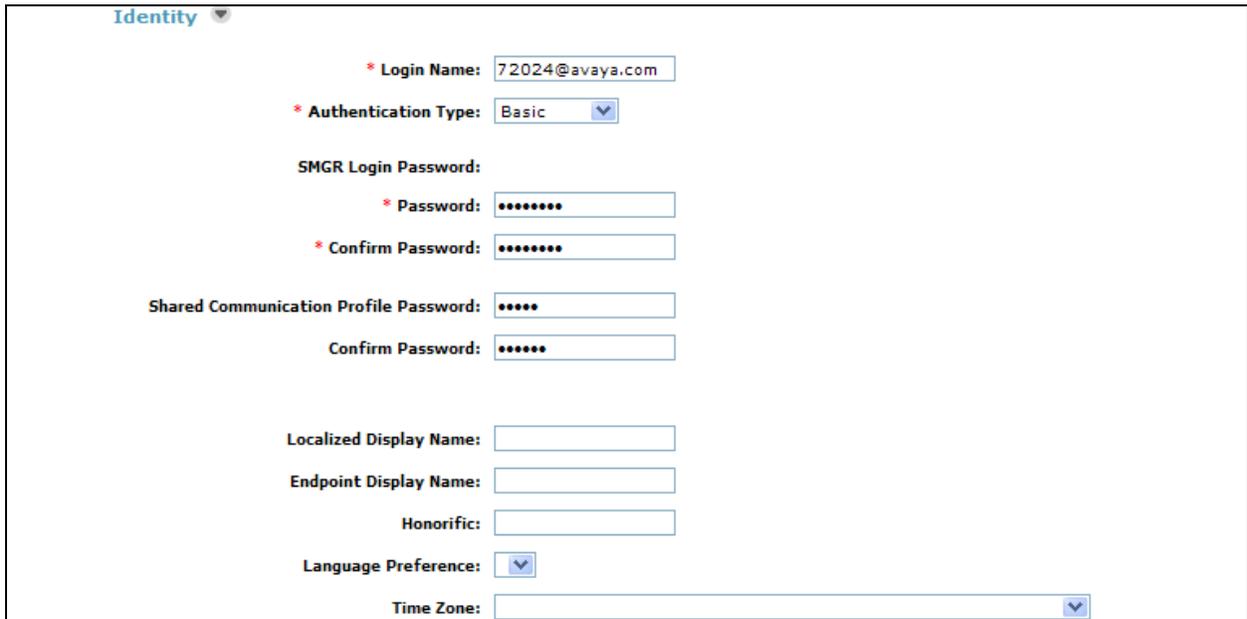
To add new SIP users, Navigate to **Users** → **Manage Users**. Click **New** (not shown) and provide the following information:

- General section
 - **Last Name** – Enter last name of user.
 - **First Name** – Enter first name of user.



The screenshot shows the 'General' section of a configuration form. It includes a dropdown menu labeled 'General' with a downward arrow. Below it are four input fields: 'Last Name' with a red asterisk and the value '72024', 'First Name' with a red asterisk and the value '72024', 'Middle Name' which is empty, and 'Description' which is empty and has a small up/down arrow icon to its right.

- Identity section
 - **Login Name** – Enter extension number@sip domain. The sip domain is defined in Section 4.3.
 - **Authentication Type** – Verify **Basic** is selected.
 - **SMGR Login Password** – Enter password to be used to log into System Manager.
 - **Confirm Password** – Repeat value entered above.
 - **Shared Communication Profile Password** – Enter a numeric value used to logon to SIP telephone.
 - **Confirm Password** – Repeat numeric password



The screenshot shows the 'Identity' section of a configuration form. It includes a dropdown menu labeled 'Identity' with a downward arrow. Below it are several input fields and dropdown menus: 'Login Name' with a red asterisk and the value '72024@avaya.com', 'Authentication Type' with a red asterisk and a dropdown menu showing 'Basic', 'SMGR Login Password' with a red asterisk and a password field containing seven dots, 'Confirm Password' with a red asterisk and a password field containing seven dots, 'Shared Communication Profile Password' with a password field containing four dots, 'Confirm Password' with a password field containing four dots, 'Localized Display Name' which is empty, 'Endpoint Display Name' which is empty, 'Honorific' which is empty, 'Language Preference' with a dropdown menu showing a blue downward arrow, and 'Time Zone' with a dropdown menu showing a blue downward arrow.

- Communication Profile section

Verify there is a default entry identified as the **Primary** profile for the new SIP user. If an entry does not exist, select **New** and enter values for the following required attributes:

- **Name** – Enter **Primary**.
- **Default** – Enter

Communication Profile

New Delete Done Cancel

Name
Primary

Select: None

* Name: Primary

Default:

- Communication Address sub-section

Select **New** to define a **Communication Address** for the new SIP user, and provide the following information.

- **Type** – Select **Avaya SIP** using drop-down menu.
- **Fully Qualified Address** – Enter same extension number and domain used for Login Name, created previously.

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

Communication Address

New Edit Delete

Type	Handle	Domain
No Records found		

Type: Avaya SIP

* Fully Qualified Address: 72024 @ avaya.com

Add Cancel

- Session Manager Profile section

- **Primary Session Manager** – Select one of the Session Managers.
- **Secondary Session Manager** – Select **(None)** from drop-down menu.
- **Origination Application Sequence** – Select Application Sequence defined in **Section 5.10** for Communication Manager.
- **Termination Application Sequence** – Select Application Sequence defined in **Section 5.10** for Communication Manager.
- **Survivability Server** – Select **(None)** from drop-down menu.
- **Home Location** – Select Location defined in **Section 5.2**.

Session Manager Profile

* Primary Session Manager

Primary	Secondary	Maximum
9	0	9

Secondary Session Manager

Primary	Secondary	Maximum

Origination Application Sequence

Termination Application Sequence

Survivability Server

* Home Location

- Endpoint Profile section
 - **System** – Select Managed Element defined in **Section 5.8** for Communication Manager Feature Server.
 - **Use Existing Endpoints** - Leave unchecked to automatically create new endpoint when new user is created. Or else, check the box if endpoint is already defined in Communication Manager.
 - **Extension** - Enter same extension number used in this section.
 - **Template** – Select template for type of SIP phone
 - **Security Code** – Enter numeric value used to logon to SIP telephone. (**Note:** this field must match the value entered for the Shared Communication Profile Password field.
 - **Port** – Select **IP** from drop down menu
 - **Voice Mail Number** – Enter **Pilot Number** for Avaya Modular Messaging if installed. Or else, leave field blank. This feature is not used during the compliance test.
 - **Delete Station on Unassign of Endpoint** – Check the box to automatically delete station when Endpoint Profile is un-assigned from user.

Endpoint Profile

* System

Use Existing Endpoints

* Extension

Template

Set Type

Security Code

* Port

Voice Mail Number

Delete Endpoint on Unassign of Endpoint from User

Click **Commit** to save definition of the new user. The following screen shows the created users during the compliance test.

The screenshot displays the Avaya Aura System Manager 6.0 interface. The top navigation bar includes the Avaya logo, the product name, and a user status message: "Welcome, admin Last Logged on at August 13, 2010 2:44 PM". Below this is a breadcrumb trail: "Home / Users / Manage Users".

The left sidebar contains a menu with the following items: Elements, Events, Groups & Roles, Licenses, Routing, Security, System Manager, Data, Users (expanded), Manage Users (highlighted), Public Contact, Lists, Shared Addresses, System Presence, ACLs, and Help.

The main content area is titled "User Management" and shows a "Users" section. It includes action buttons: View, Edit, New, Duplicate, Delete, and More Actions. There is also an "Advanced Search" link. Below the buttons, it indicates "8 Items" and a "Filter: Enable" option.

The user list is displayed in a table with the following columns: Status, Name, Login Name, E164 Handle, and Last Login. The first three rows of the table are highlighted with a red border, indicating newly created users:

Status	Name	Login Name	E164 Handle	Last Login
<input type="checkbox"/>	72024, 72024	72024@avaya.com	72024	
<input type="checkbox"/>	72025, 72025	72025@avaya.com	72025	
<input type="checkbox"/>	72026, 72026	72026@avaya.com	72026	
<input type="checkbox"/>	72027, 72027	72027@avaya.com	72027	
<input type="checkbox"/>	72028, 72028	72028@avaya.com	72028	
<input type="checkbox"/>	72029, 72029	72029@avaya.com	72029	
<input type="checkbox"/>	Default Administrator	admin		August 13, 2010 2:46:57 PM -06:00
<input type="checkbox"/>	System User	system		

5.12. Synchronization Changes with Avaya Aura® Communication Manager

After completing these changes in System Manager, perform an on demand synchronization. Navigate to **Elements** → **Inventory** → **Synchronization** → **Communication System**.

On the Synchronize CM Data and Configure Options page, expand the Synchronize CM Data/Launch Element Cut Through table

- Click to select **Incremental Sync data for selected devices** option. Click **Now** to start the synchronization.
- Use the **Refresh** button in the table header to verify status of the synchronization.
- Verify synchronization successfully completes by verifying the status in the Sync Status column shows **Completed**.

AVAYA Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at August 13, 2010 2:44 PM

Help | About | Change Password | **Log off**

Home / Elements / Inventory / Synchronization / Communication System

Synchronize CM Data and Configure Options

Synchronize CM Data/Launch Element Cut Through | Configuration Options |
Expand All | Collapse All

Synchronize CM Data/Launch Element Cut Through

1 Item		Refresh		Filter: Enable		
<input checked="" type="checkbox"/>	Element Name	FQDN/IP Address	Last Sync Time	Last Translation Time	Sync Type	Sync St
<input checked="" type="checkbox"/>	CM-S8300	10.64.41.21	August 13, 2010 8:00:24 AM - 06:00	10:00 pm THU AUG 12, 2010	Incremental	Complete

Select: All, None

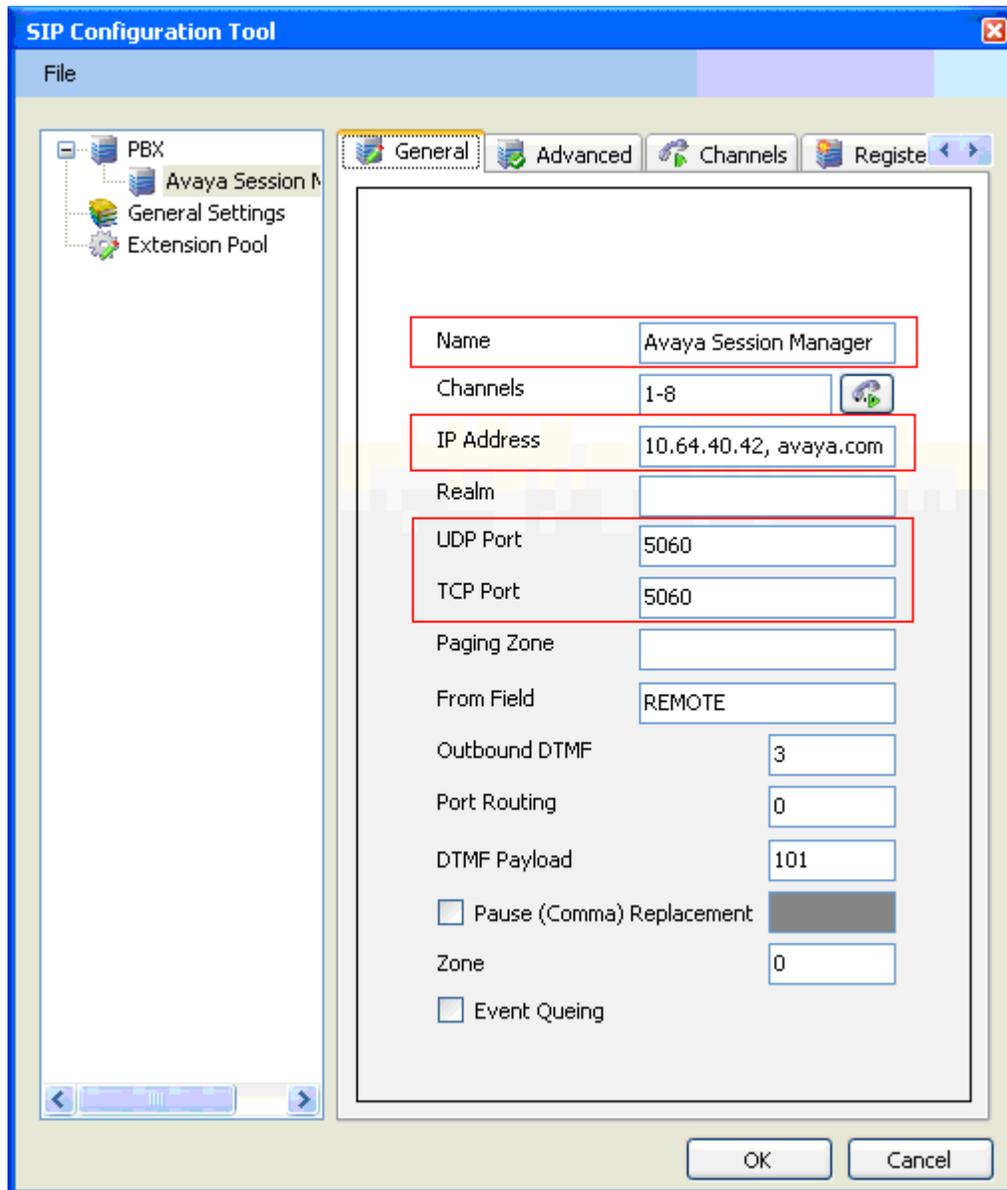
Initialize data for selected devices
 Incremental Sync data for selected devices
 Save Translations for selected devices

Now | Schedule | Cancel | Launch Element Cut Through

6. Configure the ESNA Telephony Office-LinX

ESNA installs, configures, and customizes the Telephony Office-LinX application for their customers. Thus, this section only describes the interface configuration, so that the Telephony Office-LinX can talk to Session Manager and Communication Manager. To configure ESNA Telephony Office-LinX, navigate to **Start → All program → Telephony Office LinX Enterprise Edition → SIP Configurator**. Select **Avaya Session Manager** under PBX in the left pane. Provide the following information:

- **IP Address** – Enter **IP address** and **Domain** in the field
- **UDP Port** – Enter **5060**
- **TCP Port** – Enter **5060**



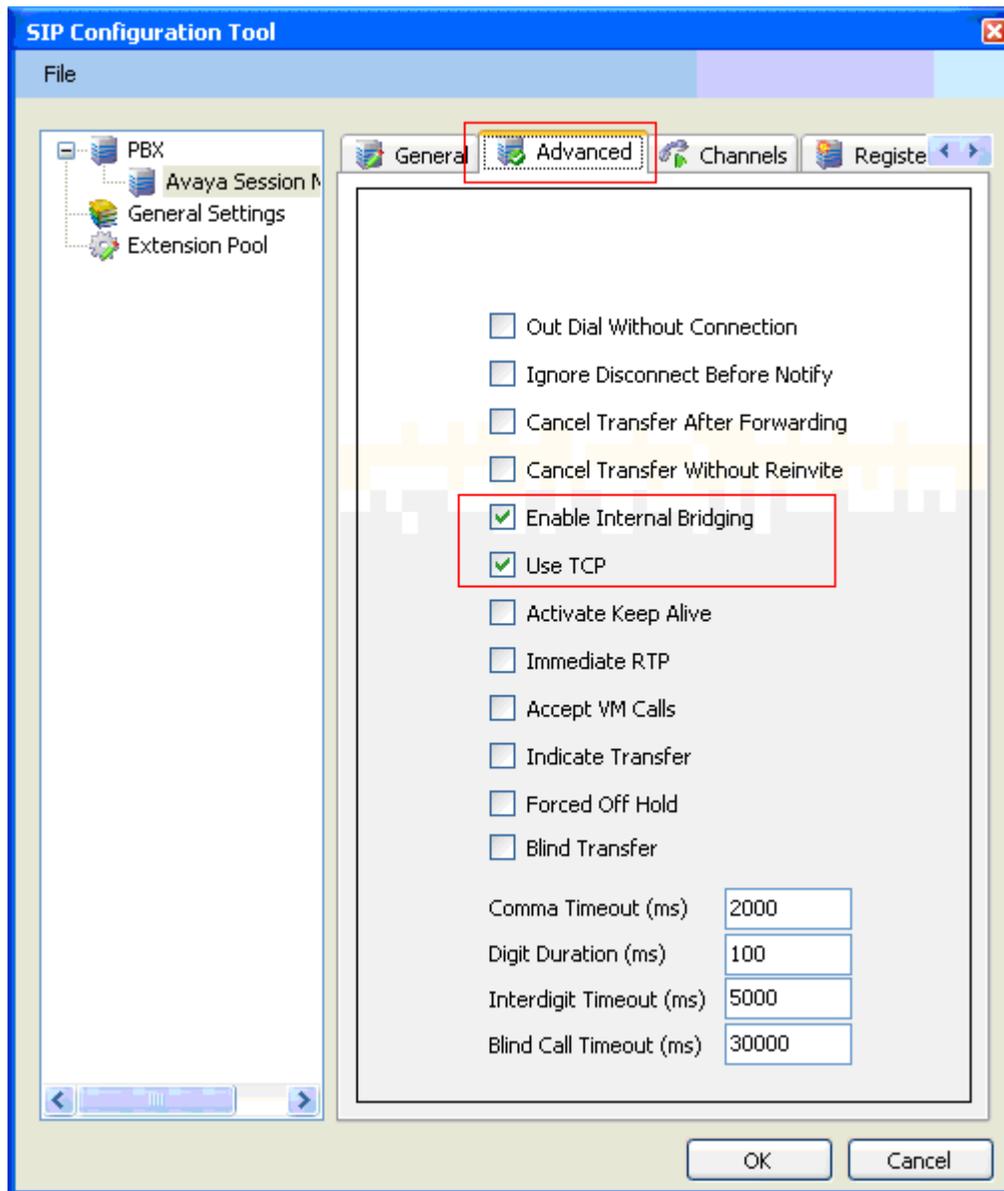
The screenshot displays the 'SIP Configuration Tool' window. The left-hand pane shows a tree view with 'PBX' expanded, containing 'Avaya Session Manager', 'General Settings', and 'Extension Pool'. The main area is titled 'General' and contains the following configuration fields:

Name	Avaya Session Manager
Channels	1-8
IP Address	10.64.40.42, avaya.com
Realm	
UDP Port	5060
TCP Port	5060
Paging Zone	
From Field	REMOTE
Outbound DTMF	3
Port Routing	0
DTMF Payload	101
<input type="checkbox"/> Pause (Comma) Replacement	
Zone	0
<input type="checkbox"/> Event Queing	

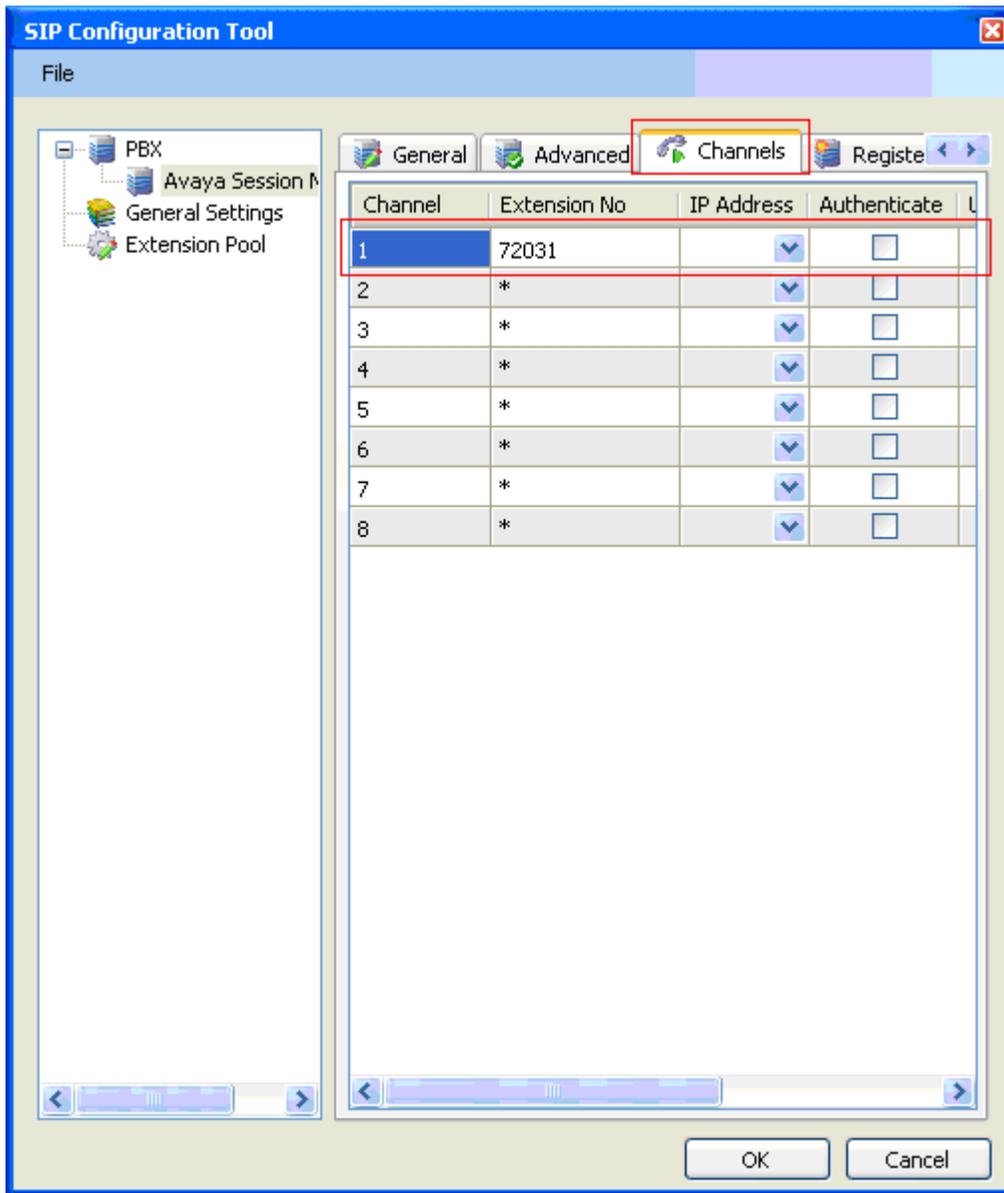
At the bottom of the window are 'OK' and 'Cancel' buttons.

Click the **Advanced** tab in the right pane, and check the following check boxes:

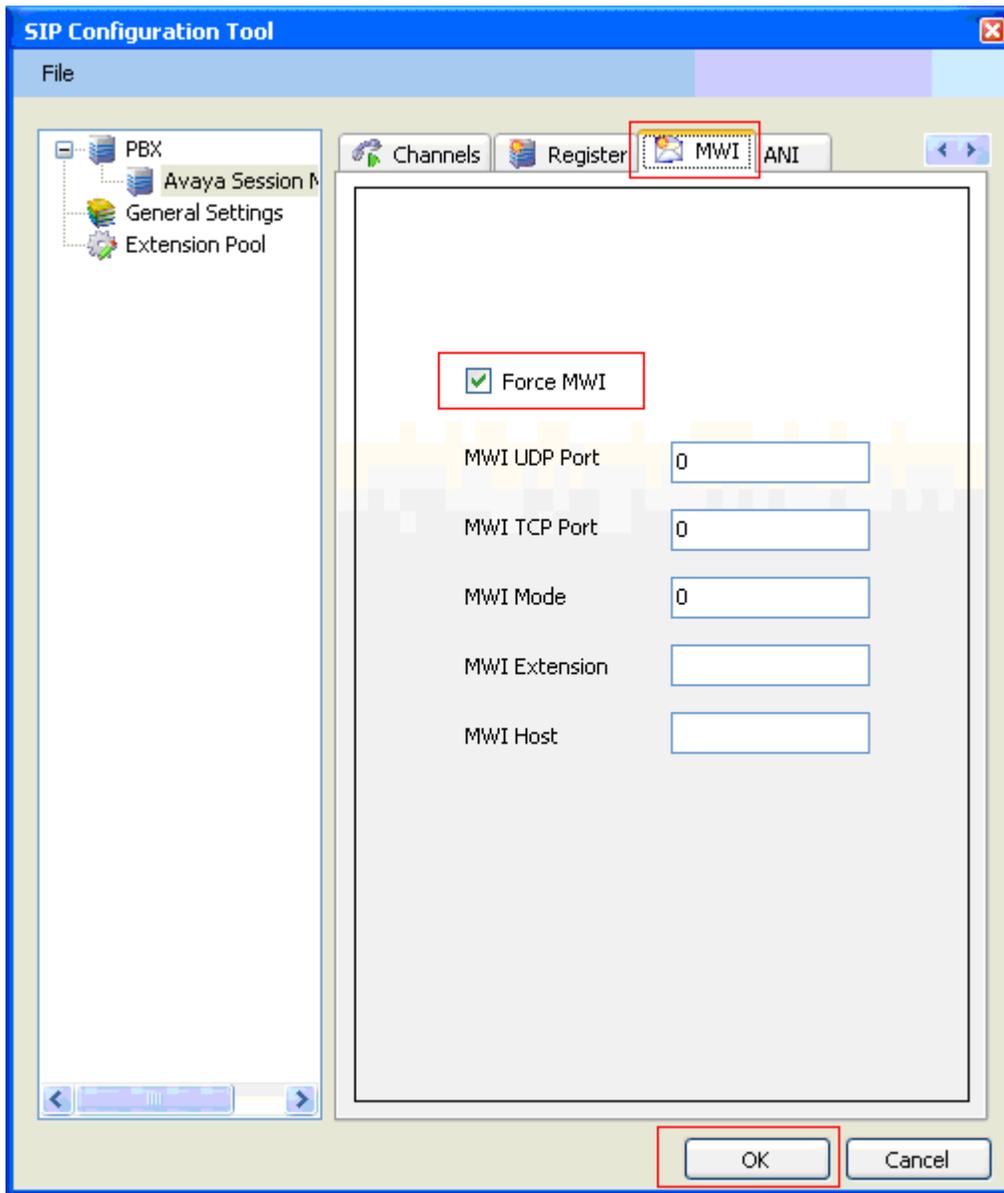
- Enable Internal Bridging
- Use TCP



Click the **Channels** tab, and provide the Telephony Office-LinX extension. During the compliance test, extension 72031 was utilized for the Telephony Office-LinX extension.



Click the **MWI** tab, and check the Force MWI check box.
Click on the **OK** button.



The following line must be added to the SIP Configuration file (ETSIPService.ini, found under C:\Windows\) manually under the [PBX#] heading:

Subscription State for MWI = 0

This provides a subscription state line in the message body indicating a subscription state is active, this is required even for unsolicited Notify messages for MWI with Session Manager.

7. General Test Approach and Test Results

The general test approach was to place calls to ESNA Telephony Office-LinX, using coverage path and hunt group. The main objectives were to verify the following:

- Successfully establish calls to ESNA Telephony Office-LinX from SIP and H.323 telephones attached to Session Manager or Communication Manager.
- Successfully transfer from ESNA Telephony Office-LinX to SIP and H.323 telephones attached to Session Manager or Communication Manager.
- Successfully leave messages for subscribers.
- Successfully retrieve messages for subscribers.
- MWI was tested and verified
- Successfully tested DTMF using the voicemail.
- Successfully tested G.711MU and G.711A codecs.

The test objectives were verified. For serviceability testing, ESNA Telephony Office-LinX operated properly after recovering from failures such as cable disconnects, and resets of ESNA Telephony Office-LinX and the Session Manager server.

8. Verification Steps

The following steps may be used to verify the configuration:

- From the Communication Manager SAT, use the **status signaling-group** command to verify that the SIP signaling group is **in-service**.
- From the Communication Manager SAT, use the **status trunk-group** command to verify that the SIP trunk group is **in-service**.
- Verify that calls can be placed to the Telephony Office-LinX and that call recording can be enabled and disabled.
- Verify with the **list trace tac** command that calls are using the correct trunk, coverage.

9. Conclusion

These Application Notes describe the procedures required to configure the ESNA Telephony Office-LinX to interoperate with Session Manager, and Communication Manager. The ESNA Telephony Office-LinX successfully passed compliance testing.

10. Additional References

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

- [1] *Administering Avaya Aura® Communication Manager*, June 2010, Release 6.0, Document Number 03-300509.
- [2] *Administering Avaya Aura® Session Manager*, August 2010, Release 6.0, Document Number 03-603324.
- [3] *Administering Avaya Aura® System Manager*, June 2010, Release 6.0.

The following document was provided by ESNA.

- [4] *Telephony Office-LinX 7.1+ Integration with Avaya Communication Manager, April 2009, Document Version 7.0.2.0*
- [5] *Server Configuration Guide*, January 2011, Document Version 8.0.3
- [6] *Server Installation Guide*, November 2010, Document Version 8.0.4.
- [7] *TECHNICAL OPERATING GUIDELINES*, November 2010, Document Version 8.0.4.

©2011 Avaya Inc. All Rights Reserved.

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

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