



Avaya Solution & Interoperability Test Lab

Application Notes for xMatters enterprise and Avaya Aura® Communication Manager and Avaya Aura® Session Manager – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between xMatters enterprise and an Avaya IP telephony solution. The Avaya solution consists of Avaya Aura® Session Manager, Avaya Aura™ Communication Manager, and various Avaya SIP and H.323 endpoints.

xMatters enterprise is an alert management solution which accelerates decision making, improves operational effectiveness and increases IT service and application availability across the enterprise. The solution transforms complex, monitored event data into meaningful information which is instantly delivered to the appropriate recipient. This information may be acted on by business professionals or used by IT teams to accelerate the incident resolution process, delivering greater application availability.

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 steps to configure Session Initiation Protocol (SIP) trunking between xMatters enterprise and an Avaya IP telephony solution. The Avaya solution consists of Avaya Aura® Session Manager, Avaya Aura® Communication Manager, and various Avaya SIP and H.323 endpoints.

xMatters enterprise is an alert management solution that helps to resolve IT events faster by ensuring incidents are properly assigned and resolution activities are coordinated, escalated and resolved within acceptable service levels. Within xMatters enterprise, users simply subscribe or are assigned to events. In addition, roles, alerts, languages, schedule reports, devices and escalation rules are all self-managed by users. Administrators can assign unlimited user attributes and create dynamic groups at the moment an event takes place – notifying people based on their skills, location, certifications and experience levels or identifying resources with a known ability to resolve an issue.

1.1. Interoperability Compliance Testing

The interoperability compliance test included features and serviceability. The focus of the compliance testing was primarily on verifying the interoperability between xMatters enterprise, Session Manager, and Communication Manager. Basic calls were placed, including inbound calls, outbound calls, and transferred calls.

1.2. Support

Customers with active Technical Support agreements can receive support via email, web, and telephone. Please see <http://www.xmatters.com/services/support-contact> for details.

2. Reference Configuration

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

The specific configuration above was used for the compliance test. Note that this solution will be compatible with other Avaya Server and Media Gateway platforms running similar versions of Communication Manager and Session Manager.

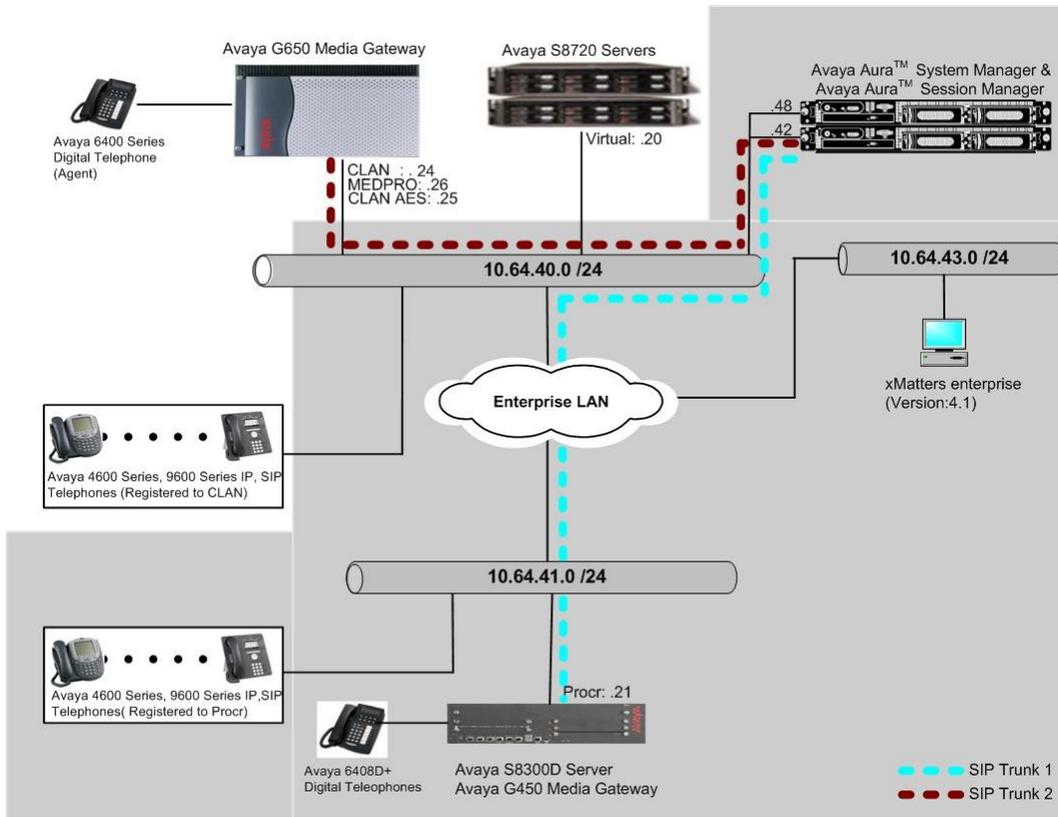


Figure 1: Avaya IP Telephony Network using xMatters enterprise

3. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya S8300D Server with Avaya G450 Media Gateway	Avaya Aura® Communication Manager 6.0 (R016x.00.0.345.0) with Patch 00.0345.0-18567
Avaya S8720 Servers with Avaya G650 Media Gateway	Avaya Aura® Communication Manager 5.2.1 (R015x.02.1.016.4)
Avaya Aura® System Manager S8510	Avaya Aura® System Manager 6.0 (6.0.0.0-556)
Avaya Aura® Session Manager	Avaya Aura® System Manager 6.0 (6.0.0.0.600020)
Avaya 9600 Series IP Telephone (H.323)	Avaya one-X Deskphone Edition (H.323)
9620	3.1
9630	3.1
9650	3.1
Avaya 9620 Series IP Telephone (SIP)	Avaya one-X® Deskphone Edition (SIP)
9620	2.6
9630	2.6
Avaya C363T-PWR Converged Stackable Switch	4.5.14
Extreme Networks Summit 48 Layer III switch	4.1.21
xMatters enterprise	4.1

4. Configure Avaya Aura® Communication Manager

This section describes the steps for configuring Communication Manager for SIP Trunking. SIP trunks are established between Communication Manager and Session Manager. A trunk is created as a part of the initial Session Manager installation and is meant to carry SIP signaling between SIP endpoints within the Session Manager domain.

It is assumed the general installation of Communication Manager, Avaya G450 Media Gateway and Session Manager has been previously completed. In addition, it is also assumed that any initial SIP configuration on Communication Manager that is required to support the Session Manager installation has also been completed.

The Communication Manager configuration was performed using the System Access Terminal (SAT).

4.1. Configure Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunk** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to the service provider. Each Avaya SIP telephone on a 2-party call with the SIP service provider uses two SIP trunk members for the duration of the call. Each non-SIP telephone (e.g., analog, digital, H.323)

on a 2-party call with SIP service provider uses one SIP trunk member. The example shows that 4000 licenses are available and 110 are in use. The license file installed on the system controls the maximum values for these attributes.

If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity.

```
display system-parameters customer-options
```

Page 2 of 11

OPTIONAL FEATURES

IP PORT CAPACITIES	USED
Maximum Administered H.323 Trunks: 4000	30
Maximum Concurrently Registered IP Stations: 2400	5
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: 2400	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	1
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: 300	0

4.2. Configure IP Node Names

The node names defined here will be used in other configuration screens to define a SIP signaling group between Communication Manager and Session Manager. Use the **change node-names ip** command to create a mapping between a logical name and an IP address. In the test environment, node-name *procr* is mapped to IP address **10.64.41.21** (an Avaya S8300D Server processor) and node name *SM-1* is mapped to **10.64.40.42** (the IP address of the Session Manager server).

```
change node-names ip
```

Page 1 of 2

IP NODE NAMES

Name	IP Address
SM-1	10.64.40.42
default	0.0.0.0
procr	10.64.41.21
procr6	::

4.3. Configure IP Network Regions

In the test environment, the Avaya S8300D Server, Avaya G450 Media Gateway, Session Manager server, IP (H.323/SIP) endpoints, and xMatters SIP endpoints are located in a single IP network region. These components are located in the default IP network region 1. The **change**

ip-network-region 1 command was used to configure the region with the parameters described below.

- Set the **Authoritative Domain** field to match the domain name configured on Session Manager. In this configuration, the domain name is **avaya.com**. This name appears in the “From” header of SIP messages originating from this IP region.
- Set the **Codec Set** field to the IP codec set to be used for calls within this IP network region. In this case, IP codec set **1** was selected.
- Default values may be used for all other fields.

```
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 Codecs

Use the **change ip-codec-set 1** command to define the codec(s) contained in this set which is used for calls within the enterprise as defined in the previous section. Which codecs are used and their order of preference is defined by the end customer. The example below uses only G.711MU.

```
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:
```

4.5. Configure Signaling Group

The **add signaling-group** command was used to create a signaling group between Communication Manager and the Session Manager for use by intra-site traffic. For the

compliance test, signaling group 3 was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to *sip*.
- Set the **Transport Method** to the recommended default value of *tls* (Transport Layer Security). As a result, the **Near-end Listen Port** and **Far-end Listen Port** are automatically set to *5061*.
- Set the **Near-end Node Name** to *procr*. This node name maps to the IP address of the processor ethernet in the Avaya S8300 Server that terminates the SIP trunk. Node names are defined using the **change node-names ip** command.
- Set the **Far-end Node Name** to *SM-1*. This node name maps to the IP address of SES as defined using the **change node-names ip** command.
- Set the **Far-end Network Region** to the IP network region defined **Section 4.3**.
- Set the **Far-end Domain** to the domain of the Session Manager.
- Set **Direct IP-IP Audio Connections** to *y*. This field will enable media shuffling on the SIP trunk.
- Set the **DTMF over IP** field to *rtp-payload*. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Default values may be used for all other fields.

```

add signaling-group 92                                     Page 1 of 1
                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
                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): 30

```

4.6. Configure Trunk Group

The **add trunk-group** command was used to create a trunk group for the signaling group created in the previous section. For the compliance test, trunk group 92 was configured using the parameters highlighted below.

- Set the **Group Type** field to *sip*.

- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Service Type** field to *tie*.
- Set the **Signaling Group** to the signaling group shown in the previous step.
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.
- The default values were used for all other fields.

```

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
Signalizing Group: 92
Number of Members: 10

```

4.7. Configure SIP Endpoint and Off PBX Telephone Station

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

4.8. Configure AAR Analysis

For the AAR Analysis Table, create the dial string that will map calls to xMatters enterprise via the route pattern created in **Section 4.9**. Enter the **change aar analysis <x>** command, where **x** is a starting digit or partial digits. The dialed string created in the AAR Digit Analysis table should contain a map to the xMatters enterprise extension, which is configured as x72041. 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
7204       5        5        92        unku      n

```

4.9. Configure Route Pattern

For the trunk group created in **Section 4.7**, 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, and the FRL value was set to 0. The default values for the other fields may be used.

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

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.

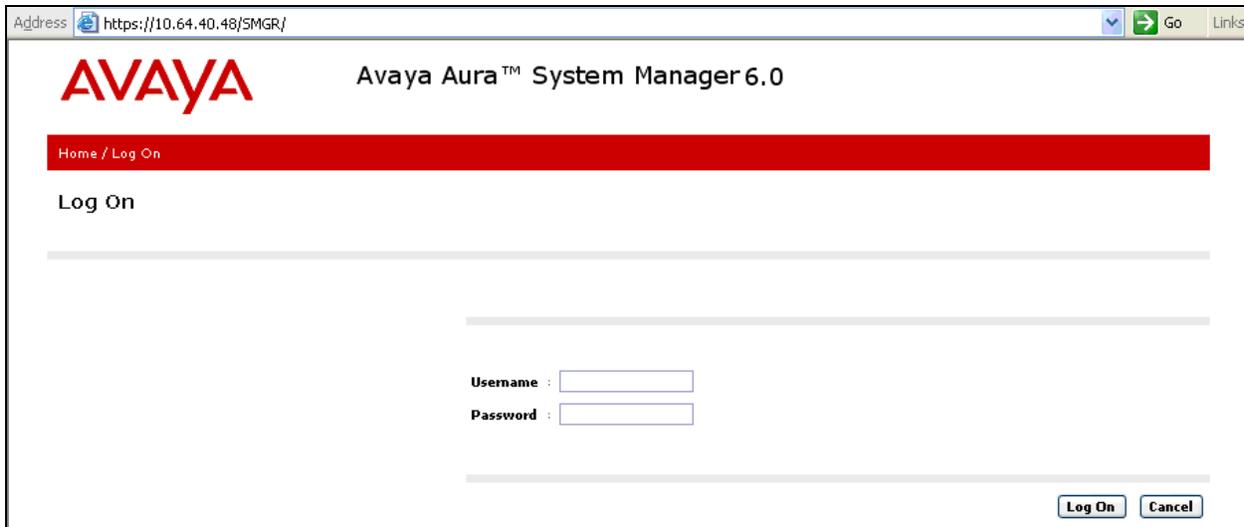
This section assumes that Session Manager and System Manager have been installed, network connectivity exists between the two platforms, and the basic configuration is performed.

In this section the following items will be configured on Session Manager:

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

5.1. Configure SIP Domain

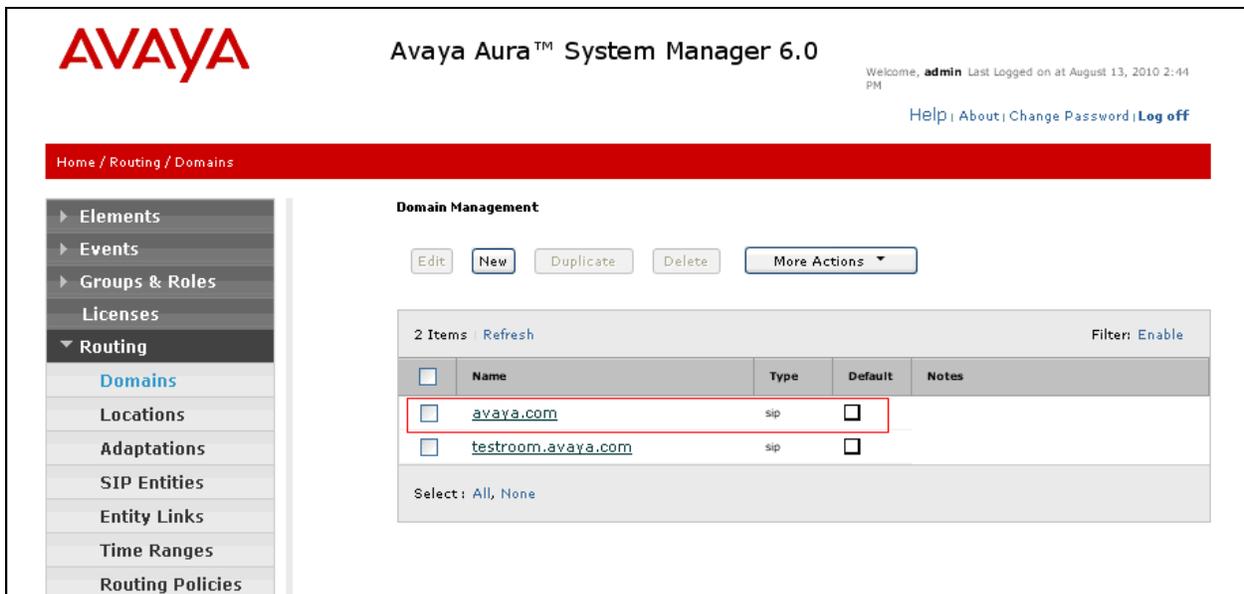
Launch a web browser, enter <https://<IP address of System Manager>/SMGR> in the URL, and log in with the appropriate credentials.



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.



	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 Entity 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, use all the default values. Click on the **Commit** button.

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

The screenshot displays the Avaya Aura System Manager 6.0 interface. The top navigation bar includes the Avaya logo, the system name, and user information. The breadcrumb trail indicates the current page is 'Home / Routing / Locations'. A sidebar on the left provides navigation options, with 'Routing' selected. The main area shows a 'Location' management page with a list of three locations: 'Denver', 'S8300-Subnet', and 'S8720-Subnet'. The 'S8300-Subnet' entry is highlighted with a red box. Action buttons like 'New', 'Commit', and 'More Actions' are visible at the top of the list.

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
- xMatters enterprise

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 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 xMatters enterprise, 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.

The screenshot displays 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 user information: 'Welcome, admin Last Logged on at December 6, 2010 3:29 PM'. A secondary navigation bar shows 'Home / Routing / SIP Entities'. On the left, a sidebar menu lists various system components, with 'Routing' expanded to show 'SIP Entities'. The main content area is titled 'SIP Entities' and contains action buttons: 'Edit', 'New', 'Duplicate', 'Delete', 'More Actions', and 'Commit'. Below these buttons is a table with 11 items. The table has columns for 'Name', 'Entity Links', 'FQDN or IP Address', 'Type', and 'Notes'. The 'AlarmPoint' row is highlighted with a red border. The table also includes a 'Filter: Enable' option and a 'Select: All, None' dropdown.

<input type="checkbox"/>	Name	Entity Links	FQDN or IP Address	Type	Notes
<input type="checkbox"/>	AlarmPoint	▶	10.64.43.111	Other	AlarmPoint App location
<input type="checkbox"/>	ChungSM	▶	10.64.40.42	Session Manager	
<input type="checkbox"/>	S8300-Chung	▶	10.64.41.21	CM	

5.4. Configure Entity Links

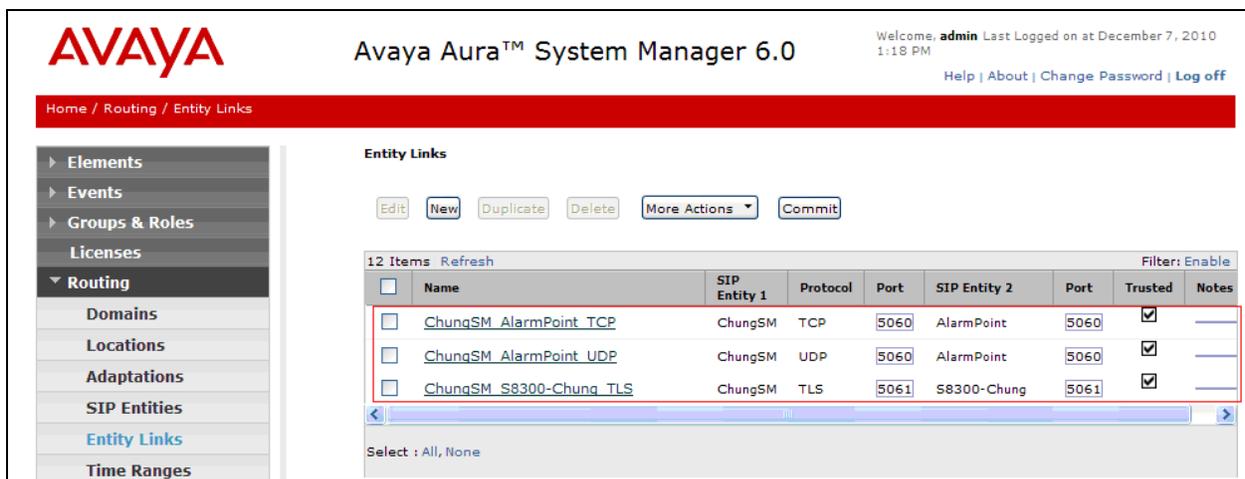
Entity Links define the connections between the SIP Entities and Session Manager. In the compliance test, the following entity links are defined from Session Manager.

- Session Manager ↔ Communication Manager
- Session Manager ↔ xMatters enterprise

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 one of the two entities in the bullet list above (which were created in **Section 5.3**). In the compliance test **S8300-Chung** was selected.
- 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 Communication Manager) 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 system name "Avaya Aura™ System Manager 6.0", and user information: "Welcome, admin Last Logged on at December 7, 2010 1:18 PM". There are links for "Help | About | Change Password | Log off". The breadcrumb trail is "Home / Routing / Entity Links".

The main content area is titled "Entity Links" and contains several action buttons: "Edit", "New", "Duplicate", "Delete", "More Actions", and "Commit". Below the buttons is a table with 12 items. The table has columns for "Name", "SIP Entity 1", "Protocol", "Port", "SIP Entity 2", "Port", "Trusted", and "Notes". The table contains three rows of data:

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
<input type="checkbox"/>	ChungSM AlarmPoint TCP	ChungSM	TCP	5060	AlarmPoint	5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	ChungSM AlarmPoint UDP	ChungSM	UDP	5060	AlarmPoint	5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	ChungSM S8300-Chung TLS	ChungSM	TLS	5061	S8300-Chung	5061	<input checked="" type="checkbox"/>	

Below the table, there is a "Select : All, None" option and a "Filter: Enable" dropdown menu.

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 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.

The screenshot displays 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 user information: 'Welcome, admin. Last logged on at August 13, 2010 2:44 PM'. There are links for 'Help', 'About', 'Change Password', and 'Log off'. The breadcrumb trail is 'Home / Routing / Time Ranges'. A left-hand menu shows 'Routing' expanded with sub-items: Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges (highlighted), and Routing Policies. The main content area is titled 'Time Ranges' and contains a table with the following data:

Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
* 24/7	<input checked="" type="checkbox"/>	* 00:00	* 23:59							

Below the table, there is a red asterisk and the text 'Input Required'. At the bottom right of the form area, there are 'Commit' and 'Cancel' buttons.

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:

- Calls to Communication Manager.
- Calls to xMatters enterprise

To add a Routing Policy, navigate to **Routing → Routing Policies**, 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 Communication Manager 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 "Avaya Aura™ System Manager 6.0", and user information: "Welcome, admin Last Logged on at December 7, 2010 1:18 PM". There are links for "Help | About | Change Password | Log off". The breadcrumb trail is "Home / Routing / Routing Policies".

The left sidebar contains a menu with the following items: Elements, Events, Groups & Roles, Licenses, Routing (expanded), Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, and Routing Policies (highlighted).

The main content area is titled "Routing Policies" and features several action buttons: Edit, New, Duplicate, Delete, More Actions (dropdown), and Commit. Below the buttons, there is a table with 10 items, a Refresh button, and a Filter: Enable option. The table has columns for Name, Disabled, Destination, and Notes. Two rows are visible and highlighted with a red border:

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input type="checkbox"/>	To AlarmPoint	<input type="checkbox"/>	AlarmPoint	
<input type="checkbox"/>	to_S8300	<input type="checkbox"/>	S8300-Chung	

Below the table, there is a "Select : All, None" option.

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

General section

- Enter a unique pattern in the **Pattern** field (e.g. **7202**).
- 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, and Routing Policies (see **Section 5.6**) that pertain to this Dial Pattern.
 - Select the Originating Location to **Apply The Selected Routing Policies to All Originating Location**.
 - Select Routing Policies to **S8300**
 - 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 7202X during the compliance test.

The screenshot displays the Avaya Aura System Manager 6.0 interface. The top navigation bar includes the Avaya logo, the title "Avaya Aura™ System Manager 6.0", and user information: "Welcome, admin Last Logged on at August 31, 2010 12:41 PM" with links for "Help | About | Change Password | Log off". The breadcrumb trail is "Home / Routing / Dial Patterns / Dial Pattern Details".

The left sidebar shows a tree view with "Routing" expanded, listing "Domains", "Locations", "Adaptations", "SIP Entities", "Entity Links", "Time Ranges", "Routing Policies", "Dial Patterns", "Regular Expressions", and "Defaults".

The main content area is titled "Dial Pattern Details" and includes "Commit" and "Cancel" buttons. Under the "General" section, the following fields are visible:

- * Pattern: 7202
- * Min: 5
- * Max: 5
- Emergency Call:
- SIP Domain: avaya.com
- Notes: (empty text box)

Under the "Originating Locations and Routing Policies" section, there are "Add" and "Remove" buttons. Below is a table with 1 item:

<input type="checkbox"/>	Originating Location Name ¹	Originating Location Notes	Routing Policy Name	Rank ²	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	to S8300	0	<input type="checkbox"/>	S8300-Chung	

Repeat steps for the remaining Dial Patterns.

5.8. Configure Managed Elements

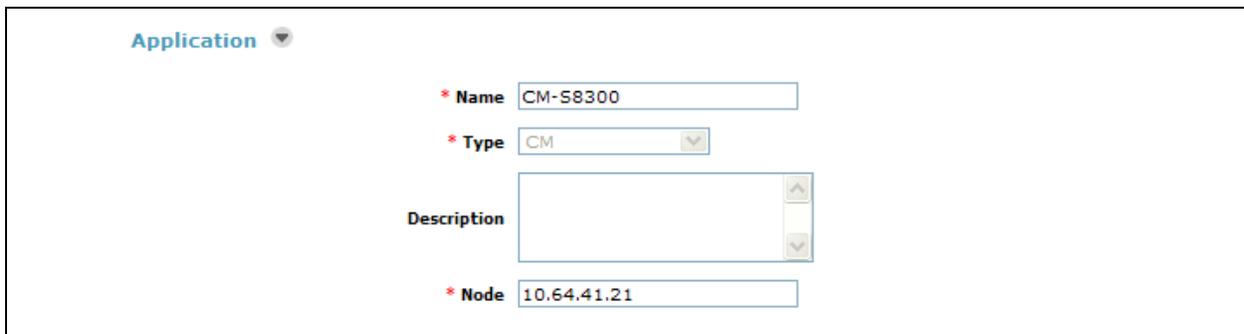
To define a new Managed Element, navigate to **Elements → Inventory → Manage Elements**. Click on the **New** button (not shown) to open the **New Entities Instance** page.

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 the 'Application' section of a web form. It contains four fields: a text input for 'Name' with the value 'CM-58300', a dropdown menu for 'Type' with 'CM' selected, a text area for 'Description' which is currently empty, and a text input for 'Node' with the value '10.64.41.21'. Each field is preceded by a red asterisk indicating it is a required field.

- 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

Attributes ▾

Login

Password

Is SSH Connection

Port

Alternate IP Address

RSA SSH Fingerprint (Primary IP)

RSA SSH Fingerprint (Alternate IP)

Is ASG Enabled

ASG Key

Location

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



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](#) / [Application Management](#) / [Applications](#)

▾ **Elements**

- Conferencing
- Presence
- Application Management
- Endpoints
- SIP AS 8.1
- Feature Management
- ▾ **Inventory**
- [Manage Elements](#)

Manage Elements

Entities

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 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.

Application Editor

Name:

*SIP Entity:

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

Description:

- 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.

AVAYA Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at August 13, 2010 4:25 PM

[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Elements / Session Manager / Application Configuration / Applications

Applications

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

Application Entries

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	
+	CM-FS	S8300-Chung		

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

Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at August 13, 2010 4:25 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

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

Elements

- ▶ Conferencing
- ▶ Presence
- ▶ Application Management
- ▶ Endpoints
- SIP AS 8.1
- ▶ Feature Management
- ▶ Inventory
- ▶ Templates

Application Sequences

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

Application Sequences

1 Item Refresh			Filter: Enable
<input type="checkbox"/>	Name	Description	
<input type="checkbox"/>	CM-FS		

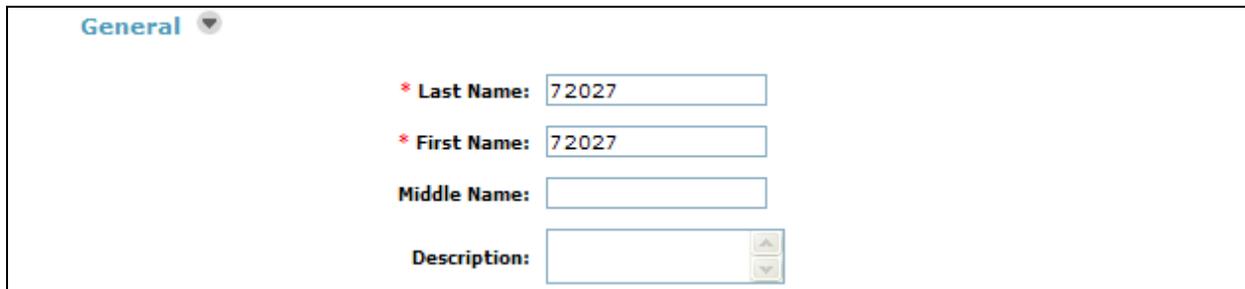
Select : All, None

5.11. Configure SIP Users

Add new SIP users for each 9600 Series SIP station defined in **Section 4.7**. Alternatively, use the option to automatically generate the SIP station after adding a new SIP user.

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 a web form titled "General" with a dropdown arrow. It contains four input fields: "Last Name" with a red asterisk and the value "72027", "First Name" with a red asterisk and the value "72027", "Middle Name" which is empty, and "Description" which is empty and has a small icon to its right.

- Identity section
 - **Login Name** – Enter extension number@sip domain 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. (**Note:** this field must match the Security Code field on the STATION form defined in **Section 4.7**)
 - **Confirm Password** – Repeat numeric password
 - Set the **Localized Display Name** to **Default Company**. During the compliance test, xMatters enterprise is configured, so that it only accepts calling party name with **Default Company**.
 - Set the **Endpoint Display Name** to **Default Company**. During the compliance test, xMatters enterprise is configured, so that it only accepts calling party name with **Default Company**.

Identity ▼

* Login Name: 72027@avaya.com

* Authentication Type: Basic ▼

SMGR Login Password:

* Password: ●●●●●●

* Confirm Password: ●●●●●●

Shared Communication Profile Password: ●●●●●

Confirm Password: ●●●●●

Localized Display Name: Default Company

Endpoint Display Name: Default Company

Honorific:

Language Preference: ▼

Time Zone: ▼

- 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 ▼

Name
<input checked="" type="radio"/> 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.
 - **Full 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: 72027 @ 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 ChungSM

Primary	Secondary	Maximum
9	0	9

Secondary Session Manager (None)

Primary	Secondary	Maximum

Origination Application Sequence CM-FS

Termination Application Sequence CM-FS

Survivability Server (None)

* Home Location S8300-Subnet

- Endpoint Profile section
 - **System** – Select Managed Element defined in **Section 5.8** for Communication Manager
 - **Use Existing Endpoints** - Leave unchecked to automatically create new endpoint when new user is created. Otherwise check the box if endpoint is already defined in Communication Manager. When unchecked, the station will be automatically created 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.
- **Delete Station on Unassign of Endpoint** – Check the box to automatically delete station when Endpoint Profile is un-assigned from user.

Endpoint Profile

* System CM-S8300

Use Existing Endpoints

* Extension 72027 Endpoint Editor

Template DEFAULT_9630SIP_CM_6_0

Set Type 9630SIP

Security Code ●●●●●●

* Port ip

Voice Mail Number 72027

Delete Endpoint on Unassign of Endpoint from User

Click **Commit** to save definition of new user. The following screen shows the created users during the compliance test. The highlight shows users created for endpoints to call xMatters enterprise during the compliance test.

AVAYA Avaya Aura™ System Manager 6.0 Welcome, admin Last Logged on at December 7, 2010 1:18 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Users / Manage Users

User Management

Users

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

24 Items Refresh Show 15 Filter: Enable

<input type="checkbox"/>	Status	Name	Login Name	E164 Handle	Last Login
<input type="checkbox"/>		73011, 73011	73011@avaya.com	73011	
<input type="checkbox"/>		73012, 73012	73012@avaya.com	73012	
<input type="checkbox"/>		73013, 73013	73013@avaya.com	73013	
<input type="checkbox"/>		Default Administrator	admin		December 7, 2010 2:11:22 PM -07:00
<input type="checkbox"/>		Default Company	72024@avaya.com	72024	
<input type="checkbox"/>		Default Company	72025@avaya.com	72025	
<input type="checkbox"/>		Default Company	72027@avaya.com	72027	
<input type="checkbox"/>		Default Company	72041@avaya.com	72041	
<input type="checkbox"/>		System User	system		

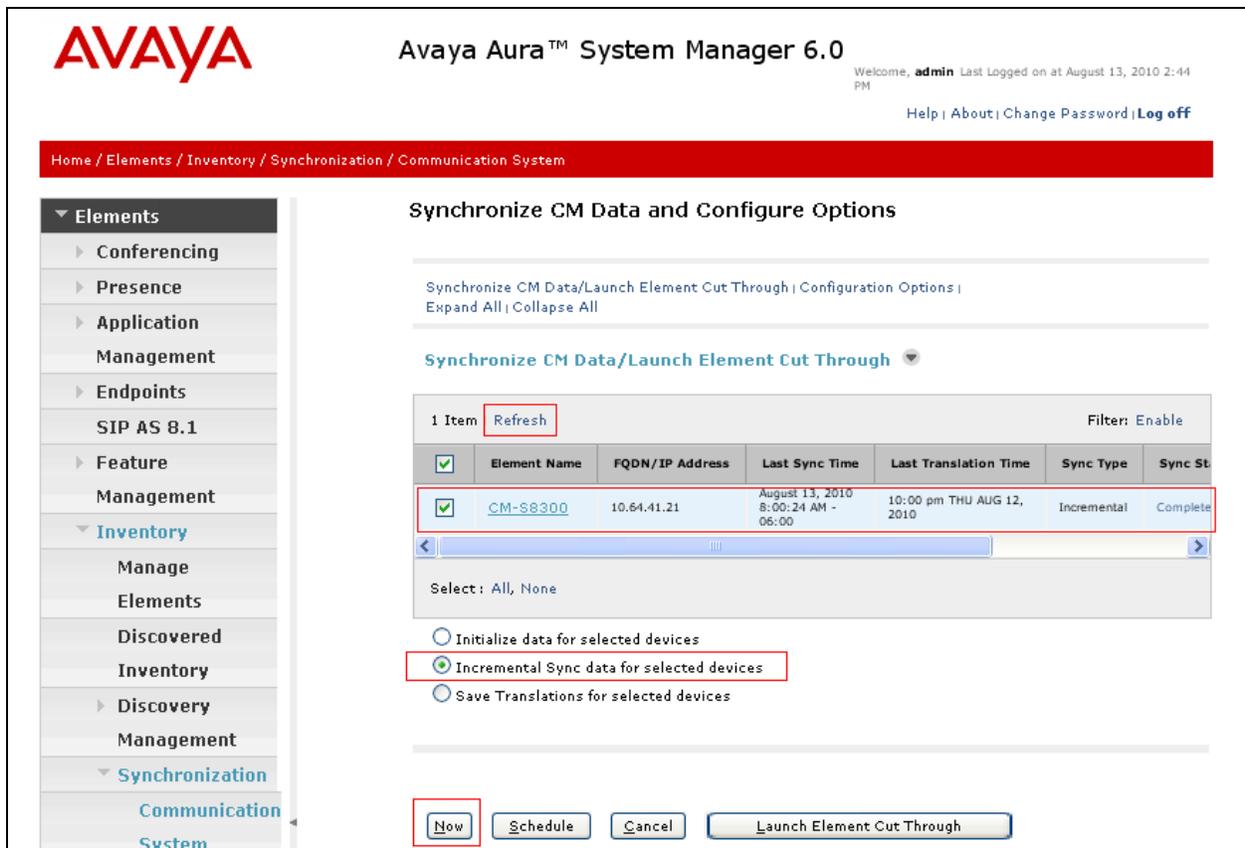
Select : All, None < Previous Page 2 of 2 Next >

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

6. xMatters Configuration

This section describes how to configure an xMatters SIP-based notification service. The SIP notification capability is configured by accessing the xMatters Web User interface with a web browser. The following sections assume that xMatters is properly installed and licensed.

6.1. Configure SIP Device Engine

The xMatters (*alarmpoint*) *engine installation and administration guide* provides configuration details for the SIP Engine. During compliance testing, the configuration settings described in the following sections were used.

Protocol Specific Details

- Set the **Number of Line Appearances** to **9**.

Note: This represents the total lines available for outgoing and incoming SIP calls. The number of lines available for outgoing calls is the total number of line appearances less those reserved for incoming calls.

Note: When using multiple registrations (as defined in the Registration List below) the number of line appearances should be set to a multiple of the number of registrations to fully utilize all line appearances.



The screenshot shows a web interface with a header "Protocol Specific Details". Below the header, there is a label "Number of Line Appearances:" followed by a text input field containing the number "9". A small asterisk "*" is located to the right of the input field.

Inbound Details

- Initially select **Codec List** set to **Ulaw**.
- Ensure that **Call-in Script Name** is set to **Default Company-callin**.

Note: xMatters supports Ulaw and Alaw and during compliance testing both of these codecs were tested.

Note: Avaya **must** be configured to support the codec selected here.



The screenshot shows a web interface with a header "Inbound Details". Below the header, there are two configuration items: "Codec List:" with a dropdown menu set to "Ulaw" and "Default Call-in Script:" with a dropdown menu set to "Default Company-callin". Both dropdown menus have a small asterisk "*" to their right.

Inbound SIP Registration List

During compliance testing, both a single Inbound SIP Registration (Registration1 below) and three registrations were used. The following table shows the registrations used (non-default values are highlighted in red text):

Parameter	Registration 1	Registration 2	Registration 3
SIP Server Address	10.64.40.42	10.64.40.42	10.64.40.42
SIP Server Port	5060	5060	5060
SIP Local Port	5060	5061	5062
SIP Local Address	10.64.43.111	10.64.43.111	10.64.43.111
SIP Domain			
SIP Outbound Proxy Address			
SIP Outbound Proxy Port	5060	5060	5060
RTP Port (min)	60000	60200	60300
RTP Port (max)	60199	60299	60399
DTMF Payload ID	101	101	101
Registration Attempts	1	1	1
Registration Timeout	60	60	60
Session Timeout	3600	3600	3600
User Name	2392	2393	2394
Password	*****	*****	*****
Display Name	x2392	x2393	x2394

Notes:

- The **SIP Server Address** is the IP address of Session Manager.
- The **SIP Local Address** is the IP address of the xMatters Notification server.
- **SIP Local Port** must be unique per registration.
- The span of values defined between **RPT Port (min)** and **(max)** must be unique and cannot overlap with the values for any other registration.
- Avaya supplied the **User Names** and **Passwords**.

6.2. Configure SIP Protocol Provider

The xMatters (*alarmpoint*) engine installation and administration guide provides configuration details for SIP Protocol Providers. During compliance testing, the configuration settings described in the following sections were used.

General Details

- Set **Maximum Retries** to **0**.
Note: The number of retries was set to 0 to avoid retries during testing.

SIP Details

- Ensure that **Use Device Engine Settings** is selected.
- Ensure that the **Call-out Script** default is **callout**.

General Details	
Name:	<input type="text" value="SIP Provider"/> *
Description:	<input type="text"/>
Maximum retries:	<input type="text" value="3"/> *
Retry Interval:	<input type="text" value="10"/> *(sec)
SIP Details	
Use Device Engine Settings	<input checked="" type="checkbox"/>
Call-out Script:	<input type="text" value="callout"/> *

7. General Test Approach and Test Results

This section describes the interoperability compliance testing used to verify interoperability between the xMatters enterprise and an Avaya IP Telephony Solution.

Inbound scenario: A call to xMatters enterprise

Outbound scenario: A call from xMatters enterprise

The compliance test included the following:

- xMatters enterprise successfully registers with Session Manager.
- Establish calls between xMatters enterprise and Avaya SIP and H.323 IP telephones attached to Session Manager or Communication Manager.
- Inbound blind transfer
- Inbound consult transfer
- Outbound blind transfer
- Outbound consult transfer
- Multiple Inbound calls (three) and consult transfer to a simulated conference bridge, using Avaya 9630 H.323 telephone
- Multiple outbound calls (three) and consult transfer to a simulated conference bridge, using Avaya 9630 H.323 telephone
- With Multiple outbound calls, dropping a call and adding a call
- Direct IP-to-IP media (also known as “shuffling”) with SIP and H.323 telephones. This allows IP endpoints to send audio (RTP) packets directly to each other without using media resources on the Avaya Media Gateway.

8. Verification Steps

This section provides verification steps that may be performed in the field to verify that xMatters enterprise can place outbound and receive inbound PSTN, H.323 and SIP calls.

1. Verify that SIP endpoints were able to register with Session Manager.
2. Verify the test cases in **Section 7** using the **traceSM** command in the Session Manager server.
3. Verify that xMatters enterprise can make outbound call, and DTMF works.
4. Verify that xMatters enterprise can receive inbound call, and DTMF works.

9. Conclusion

These Application Notes describe the configuration steps necessary to connect Communication Manager and Session Manager to xMatters enterprise. The xMatters enterprise is a SIP-based endpoint solution. During the compliance test, all test cases passed.

10. References

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

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

Product information for xMatters products may be found at <http://connect.xmatters.com>. The following xMatters enterprise document was provided by xMatters, inc.

- [4] *xMatters (alarmpoint) Engine Installation and Administration Guide*, version 4.0, January 2010.

©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.