



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

---

# **Application Notes for Configuring the ADTRAN NetVanta UC Server with Avaya Aura® Session Manager and Avaya Aura® Communication Manager - Issue 1.0**

### **Abstract**

These Application Notes describe the procedure for configuring the ADTRAN NetVanta UC Server to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager.

Adtran NetVanta UC Server is a software-only package designed for Microsoft Windows platforms that provides capabilities of unified communications.

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 ADTRAN NetVanta UC Server (herein referred to as NetVanta UC Server) to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager.

SIP (Session Initiation Protocol) is a standards-based communications approach designed to provide a common framework to support multimedia communication. RFC 3261 is the primary specification governing this protocol. SIP manages the establishment and termination of connections and the transfer of related information such as the desired codec, calling party identity, etc. Within these Application Notes, SIP is used as the signaling protocol between Avaya Aura® Session Manager and Avaya Aura® Communication Manager.

During the compliance test, the test environment included Communication Manager / Session Manager, and Avaya IP Office. However, in these Application Notes, only Communication Manager / Session Manager and NetVanta UC Server will be discussed. IP Office and NetVanta UC Server scenario will be discussed in other Application Notes.

## 1.1. NetVanta UC Server

NetVanta Unified Communications (UC) Server is a software-only package designed for Microsoft Windows platforms that provides capabilities of unified communications – without the need for a forklift upgrade. It is perfect for organizations that already have one or more PBXs, but want the added benefits of unified communications.

The NetVanta UC Server portfolio includes:

- PBX Integration
- Unified Messaging (UM)
- FAX Server
- Text-to-Speech Engine
- Auto-Attendant and Personal Call Control
- Administration

### Unified Communications Server

NetVanta UC Server is capable of supporting UC on one or more different types of PBXs to provide a centralized UC solution. This feature-rich platform offers advanced UC services like unified messaging, voice mail, integrated messaging, fax server, graphical drag and drop service creation, inbound and outbound IVR services, personal assistants, one number services, call redirection services, notifications, auto-attendants, mobile support and scales from 75 up to 2,000 users on a single server.

### PBX Integration

If you have an existing investment in legacy business communications systems (PBXs and/ or key systems), NetVanta UC Server lets you leverage your existing investment and transition to IP Telephony at your own pace.

### Unified Messaging (UM)

UM is the ability to quickly and effectively retrieve and manage voicemail, faxes, and email messages, all from the familiar interface of your email client or from any telephone. NetVanta UC Server integrates with Microsoft Outlook/Exchange Server, Lotus Notes/Domino, Google Gmail, and a host of other email clients with Internet Message Access Protocol—IMAP4.

#### FAX Server

NetVanta UC Server includes a full fax server. The built-in fax server provides advanced features such as DID fax, and individual “fax on demand” using the multimedia personal call control capabilities. In addition, NetVanta UC Server uses standard TIFF or PDF formats so that you can view faxes on any PC.

#### Text-to-Speech Engine

NetVanta UC Server includes a speech engine to provide text-to-speech conversion. This enables you to listen to e-mail messages from any telephone and speak text from your auto attendants, Interactive Voice Response (IVR) applications, or Personal Assistants.

#### Auto-Attendant and Personal Call Control

NetVanta UC Server provides the ability to create multiple auto-attendants using its award-winning drag-and-drop, database-enabled, graphical service creation environment. These assistants integrate with Microsoft Outlook contacts and internal/external databases, allowing employees to easily configure their own assistants to establish multifaceted business rules for call screening, call routing, find-me/follow-me, and call notifications, all depending on the defined rules like the caller ID, time-of-day/day-of-week, and many others.

#### Administration

NetVanta UC Server can be installed in one of two modes—standalone or within a customer’s Active Directory. When integrated with Active Directory, the Microsoft Active Directory Users and Microsoft Management Console (MMC) Snap-ins can be used to administer and manage users. NetVanta UC Server allows your IT staff to manage your business communications services using the same user accounts and security policies used in your Windows environment, without any programming or special integration.

## **2. General Test Approach and Test Results**

The general test approach was to place calls to NetVanta UC Server, using coverage paths and hunt groups. The main objectives were to verify the following:

- Successfully establish calls to NetVanta UC Server from SIP and H.323 telephones attached to Session Manager or Communication Manager.
- Successfully transfer from NetVanta UC Server to SIP and H.323 telephones attached to Session Manager or Communication Manager.
- MWI was tested and verified.
- Successfully leave messages for subscribers.
- Successfully retrieve messages for subscribers.
- Successfully tested DTMF using the voicemail.
- Successfully tested G.711MU codec.

## **2.1. 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 NetVanta UC Server, Session Manager and Communication Manager.

## **2.2. Test Results**

The test objectives were verified. For serviceability testing, NetVanta UC Server operated properly after recovering from failures such as cable disconnects, and resets of NetVanta UC Server and the Session Manager server.

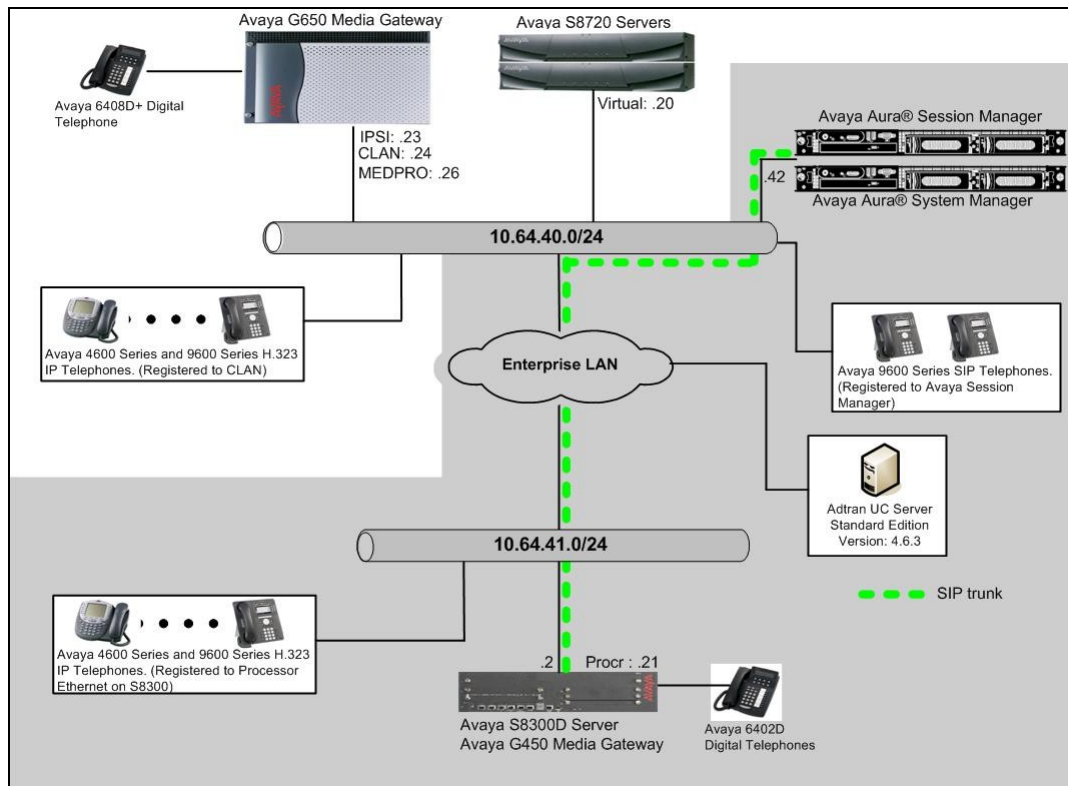
## **2.3. Support**

Technical support for the NetVanta UC Server solution can be obtained by contacting ADTRAN:

- URL – [http://www.adtran.com/web/page/portal/Adtran/wp\\_support\\_postsaletechsupport](http://www.adtran.com/web/page/portal/Adtran/wp_support_postsaletechsupport)
- Phone – 888-4ADTRAN

### 3. 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. The Avaya S8720 Servers with Avaya G650 Media Gateway were included in the test to provide an inter-switch scenario. NetVanta UC Server does not register with Session Manager as an endpoint, but instead, is configured as a trusted SIP entity.



**Figure 1: Test Configuration of NetVanta UC Server**

## 4. Equipment and Software Validated

The following equipment and software/firmware 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 00.0345.0-18246
Avaya Aura® System Manager on S8510		Avaya Aura® System Manager 6.0.0 (6.0.0.0-556-3.0.6.0)
Avaya Aura® Session Manager on S8510		Avaya Aura® Session 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)	2.6.3
	9630 (SIP)	2.6.3
	9650 (SIP)	2.6.3
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		-
ADTRAN NetVanta UC Server		4.6.3

## 5. Configure Avaya Aura® Communication Manager

In the compliance test, Communication Manager was set up as an Evolution Server. 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 NetVanta UC Server, are configured as off-PBX telephones in Communication Manager.

## 5.1. 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

## 5.2. 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 5.3** for configuring IP network region to specify which codec sets may be used within and between network regions.

**Note:** NetVanta UC Server only supports G.711MU. Thus, G.711MU was utilized 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			

### 5.3. 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. Set to the appropriate domain. During the compliance test, the authoritative domain is set to **avaya.com**.
- **Codec Set** – Set the codec set number as provisioned in **Section 5.2**.

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	
		RSVP Enabled? n	
H.323 Link Bounce Recovery? y			
Idle Traffic Interval (sec): 20			
Keep-Alive Interval (sec): 5			
Keep-Alive Count: 5			

**Note:** In systems with multiple network regions, codec set 1 can be configured as the inter-region codec set for calls between each region and the region of the NetVanta UC Server. The inter-region codec set can be configured using the **Inter Network Region Connection Management** table beginning on **Page 4** of the ip-network-region form.



## 5.4. 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	

## 5.5. 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 as a Feature Server.
- **Transport Method** – Set to **tls** (Transport Layer Security).
- **Near-end Node Name** – Set to **procr** as displayed in **Section 5.4**.
- **Far-end Node Name** – Set to the Session Manager name configured in **Section 5.4**.
- **Far-end Network Region** – Set to the region configured in **Section 5.3**.
- **Far-end Domain** – Set to **avaya.com**. This should match the SIP Domain value in **Section 5.3**.
- **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	
Enable Layer 3 Test? n	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 6	

## 5.6. Configure Trunk Group

To configure the associated 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 configured in the SIGNALING GROUP form.
- **Number of Members** – Allowed value is between 0 and 255. Set to a value large enough to accommodate the number of SIP trunk members required.

```
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
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
                                     UUI Treatment: service-provider
                                     Replace Restricted Numbers? n
                                     Replace Unavailable Numbers? n
                                     Modify Tandem Calling Number: no
Show ANSWERED BY on Display? y
```

## 5.7. Configure Coverage Path

This section describes the steps for administering a coverage path in Communication Manager. Enter the **add coverage path <s>** command, where **s** is a valid coverage path number. The Point1 value of r2 is used to represent the remote coverage 2. 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: r2                Rng:      Point2:
  Point3:                   Point4:
  Point5:                   Point6:
```

Enter the **change coverage remote <s>** command, where **s** is an entry of the remote call coverage. The Point1 value of r2, created on the previous step, is used to represent the remote call coverage 2. The default values for the other fields may be used. When the value **<s>** is set to 1, the table covers r1 through r1000.

```
change coverage remote 1                                Page 1 of 23

                                REMOTE CALL COVERAGE TABLE
                                ENTRIES FROM 1      TO 1000

01:                            16:                            31:
02: 73015                      17:                            32:
03:                            18:                            33:
04:                            19:                            34:
```

## 5.8. Configure SIP Endpoint

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

## 5.9. Configure Route Pattern

For the trunk group created in **Section 5.6**, 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: SIP trunk														
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
2:													n	user
3:													n	user
4:													n	user
5:													n	user
6:													n	user
BCC VALUE			TSC	CA-TSC	ITC BCIE Service/Feature					PARM	No.	Numbering	LAR	
0	1	2	M	4	W	Request					Dgts	Format		
													Subaddress	
1:	y	y	y	y	y	n	n	rest					none	
2:	y	y	y	y	y	n	n	rest					none	
3:	y	y	y	y	y	n	n	rest					none	
4:	y	y	y	y	y	n	n	rest					none	
5:	y	y	y	y	y	n	n	rest					none	
6:	y	y	y	y	y	n	n	rest					none	

## 5.10. Configure AAR Analysis

For the AAR Analysis Table, create the dial string that will map calls to NetVanta UC Server via the route pattern created in **Section 5.9**. 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 NetVanta UC Server system extension, which is configured as x73015. During the configuration of 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	
7301		5	5	92	unku		n	

## 6. 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

## 6.1. Configure SIP Domain

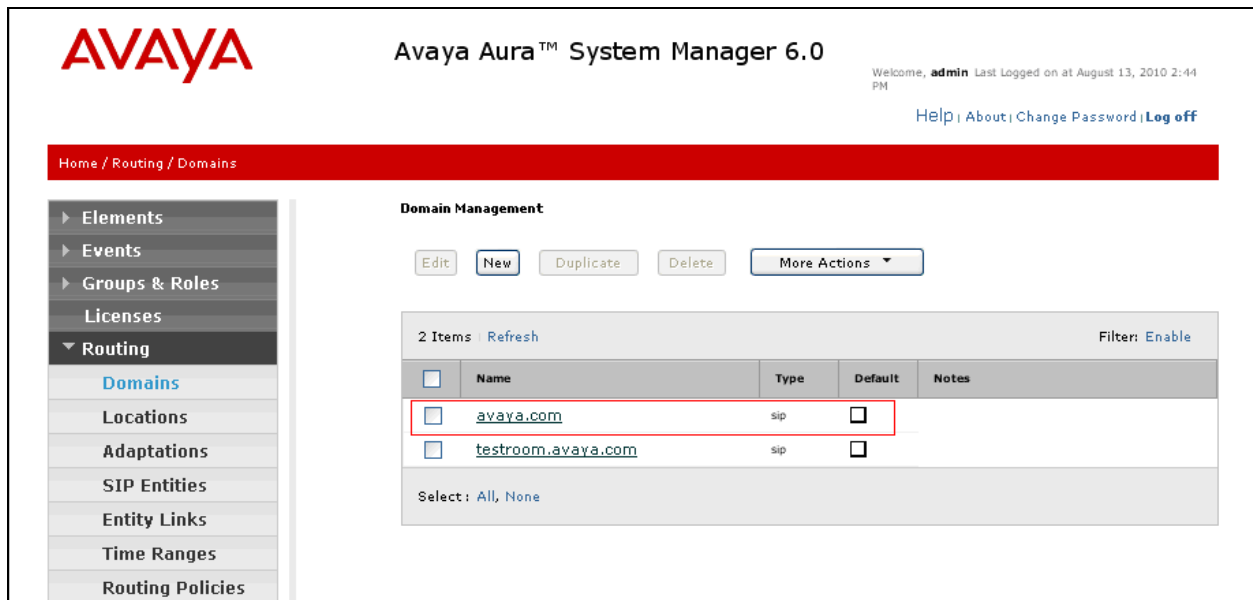
Launch a web browser, enter <http://<IP address of System Manager>/SMGR> in the URL, and log in with the appropriate credentials.

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 5.3**, 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 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 a user status message: 'Welcome, admin Last Logged on at August 13, 2010 2:44 PM'. Below this is a red breadcrumb trail: 'Home / Routing / Domains'. On the left is a sidebar menu with categories like Elements, Events, Groups & Roles, Licenses, Routing (selected), Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, and Routing Policies. The 'Domains' sub-item under Routing is highlighted. The main content area is titled 'Domain Management' and contains buttons for 'Edit', 'New', 'Duplicate', 'Delete', and 'More Actions'. Below these buttons is a table with 2 items. The first item, 'avaya.com', is highlighted with a red box. The table has columns for Name, Type, Default, and Notes. The 'avaya.com' row shows 'sip' for Type and an unchecked checkbox for Default. The second row is 'testroom.avaya.com' with 'sip' for Type and an unchecked checkbox for Default. At the bottom of the table area, it says 'Select: All, None'.

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

## 6.2. 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. **App-10.64.43.0 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** field (e.g. **10.64.43.\***).
- 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.

The following screen shows the SIP Locations list used during the compliance test.

The screenshot displays the Avaya Aura System Manager 6.0 web interface. The top navigation bar includes the Avaya logo, the product name, and user information (Welcome, admin, Last Logged on at February 24, 2011 1:18 PM). A red breadcrumb trail shows the path: Home / Routing / Locations. On the left, a sidebar menu lists various configuration areas, with 'Routing' expanded to show 'Locations'. The main content area, titled 'Location', contains action buttons (Edit, New, Duplicate, Delete, More Actions, Commit) and a table of 8 items. The table has columns for 'Name' and 'Notes'. The listed locations are: 'App-10.64.43.0 Subnet' (Note: Adtran iVR), 'Denver', 'S8300-Subnet- 10.64.41' (Note: 10.64.41.0 Net), and 'S8720-Subnet-10.64.40' (Note: 10.64.40.0 Net). A 'Filter: Enable' link is present. At the bottom of the table area, it says 'Select : All, None'.

<input type="checkbox"/>	Name	Notes
<input type="checkbox"/>	App-10.64.43.0 Subnet	Adtran iVR
<input type="checkbox"/>	Denver	
<input type="checkbox"/>	S8300-Subnet- 10.64.41	10.64.41.0 Net
<input type="checkbox"/>	S8720-Subnet-10.64.40	10.64.40.0 Net

### 6.3. 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. This entity was created prior to the compliance test.
- Communication Manager. This entity was created prior to the compliance test.
- Adtran

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

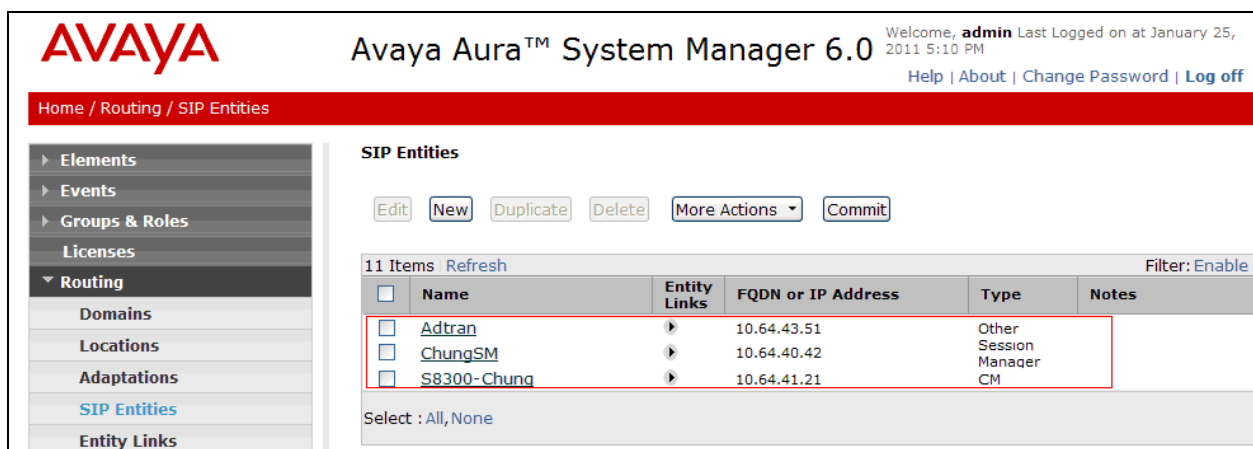
Enter the following values and use default values for remaining fields.

- Enter a descriptive Entity name in the **Name** field.
- Enter IP address for signaling interface on each Communication Manager, virtual SM-100 interface on Session Manager, or 3<sup>rd</sup> party device (in this case, Adtran) in 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 Adtran, select **Other**
- Enter a description in the **Notes** field if desired.
- Select the appropriate time zone.
- Accept the other default values.

#### SIP Link Monitoring section

Select the **Link Monitoring Disabled** using the drop-down list. ADTRAN does not support the SIP OPTIONS message. Thus, during the compliance test, the link monitoring was disabled. Accept all 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 welcome message for the user "admin" last logged on at January 25, 2011 5:10 PM. There are links for "Help", "About", "Change Password", and "Log off". The main content area is titled "SIP Entities" and includes buttons for "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 table contains three rows of data: "Adtran" (Type: Other), "ChungSM" (Type: Session Manager), and "S8300-Chung" (Type: CM). The "Adtran" row is highlighted with a red box. The bottom of the page shows a "Select" dropdown menu with options "All, None".

Name	Entity Links	FQDN or IP Address	Type	Notes
Adtran		10.64.43.51	Other	
ChungSM		10.64.40.42	Session Manager	
S8300-Chung		10.64.41.21	CM	



## 6.4. 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). This entity link was created prior to the compliance test.
- Session Manager ⇔ Adtran

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 shown in **Section 6.3** (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 shown in **Section 6.3**).
- In the **Port** field, enter the port to be used (e.g. **5060** or **5061**). During the compliance test, the port was set to **5080**, since NetVanta UC Server already used 5060 internally.
- Enter a description in the **Notes** field if desired.
- Accept the other default values.

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

Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at January 26, 2011 3:10 PM

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

Home / Routing / Entity Links

**Entity Links** Commit Cancel

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
* ChungSM_Adtran	* ChungSM	UDP	* 5060	* Adtran	* 5080	<input checked="" type="checkbox"/>

\* Input Required Commit Cancel

Repeat the steps to define Entity Link using a different protocol.

## 6.5. Time Ranges

The Time Ranges form allows admission control criteria to be specified for Routing Policies (Section 6.6). 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.

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 / Routing / Time Ranges

Time Ranges Commit Cancel

1 Item Refresh Filter Enable

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

< >

\* Input Required Commit Cancel

## 6.6. Configure Routing Policy

Routing Policies associate destination SIP Entities (**Section 6.3**) with Time of Day admission control parameters (**Section 6.5**) and Dial Patterns (**Section 6.7**). In the reference configuration, Routing Policies are defined for:

- Calls to/from Communication Manager.
- Calls to/from the Adtran

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 Adtran during the compliance test.

**AVAYA** Avaya Aura™ System Manager 6.0 Welcome, **admin** Last Logged on at January 26, 2011 3:10 PM  
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Routing / Routing Policies / Routing Policy Details

**Routing Policy Details** Commit Cancel

**General**

\* Name:

Disabled: ☐

Notes:

**SIP Entity as Destination**

Select

Name	FQDN or IP Address	Type	Notes
Adtran	10.64.43.51	Other	

**Time of Day**

Add Remove View Gaps/Overlaps

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Ranking <sup>1</sup>	Name <sup>2</sup>	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	

## 6.7. 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
- 73015 – NetVanta UC Server

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. **73015**).
- 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 6.6**) that pertain to this Dial Pattern.
  - Originating Location –Check the **Apply The Selected Routing Policies to All Originating Locations** box.
  - Routing Policies **To Adtran**.
  - 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 Adtran during the compliance test.

**Dial Pattern Details** [Commit] [Cancel]

**General**

\* Pattern: 73015

\* Min: 5

\* Max: 5

Emergency Call: ☐

SIP Domain: avaya.com

Notes: Adtran iVR extension

**Originating Locations and Routing Policies**

[Add] [Remove]

1 Item Refresh Filter: Enable

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

## 6.8. 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.
  - **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. It contains four fields: 'Name' with the value 'CM-S8300', 'Type' with a dropdown menu showing 'CM', 'Description' with an empty text area and up/down arrows, and 'Node' with the value '10.64.41.21'. Each field is preceded by a red asterisk indicating it is required.

- 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

Click **Commit** to save the element.

**Attributes** ▼

\* **Login**

**Password**

**Confirm Password**

**Is SSH Connection** ☒

\* **Port**

**Alternate IP Address**

**RSA SSH Fingerprint (Primary IP)**

**RSA SSH Fingerprint (Alternate IP)**

**Is ASG Enabled** ☐


**ASG Key**

**Confirm ASG Key**

**Location**

\* **Required** Commit Cancel

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**
View Edit New Delete More Actions ▼

1 Item | Refresh | Show **ALL** ▼ | Filter: Enable

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

Select: All, None

## 6.9. 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 shown in **Section 6.3**
  - **CM System for SIP Entity** – Select name of Managed Element defined for Communication Manager in **Section 6.8**
  - **Description** – Enter description if desired.

The screenshot shows the 'Application Editor' form. It has the following fields and controls:

- Name:** A text input field containing 'CM-FS'.
- \*SIP Entity:** A dropdown menu with 'S8300-Chung' selected.
- \*CM System for SIP Entity:** A dropdown menu with 'CM-S8300' selected, followed by a 'Refresh' button.
- Description:** An empty text input field.
- On the right side, there are two links: '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 top navigation bar includes the Avaya logo, the title 'Avaya Aura™ System Manager 6.0', and a welcome message for 'admin' last logged on at August 13, 2010, 4:25 PM. Below the navigation bar is a red breadcrumb trail: 'Home / Elements / Session Manager / Application Configuration / Applications'.

The left sidebar shows a tree view with 'Elements' expanded, containing 'Conferencing', 'Presence', 'Application Management', 'Endpoints', 'SIP AS 8.1', 'Feature Management', 'Inventory', 'Templates', 'Session Manager', and 'Dashboard'.

The main content area is titled 'Applications' and contains the text: 'This page allows you to add, edit, or remove applications for available SIP Entities.' Below this is a section titled 'Application Entries' with 'New', 'Edit', and 'Delete' buttons. A table shows one item:

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

Below the table, it says 'Select : All, None'. At the top right of the table area, it says '1 Item' and 'Refresh'. At the bottom right, it says 'Filter: Enable'.

## 6.10. 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

CM-FS

Description

- Available Applications section
  - Click  icon associated with the Application for Communication Manager defined in **Section 6.9** 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

Move First

Move Last

Remove

1 Item					
<input type="checkbox"/>	Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
<input type="checkbox"/>		<a href="#">CM-FS</a>	S8300-Chung	<input checked="" type="checkbox"/>	

Select : All, None

### Available Applications

1 Item Refresh Filter: Enable

	Name	SIP Entity	Description
	<a href="#">CM-FS</a>	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

▼ Session Manager

Dashboard

### Application Sequences

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

#### Application Sequences

New

Edit

Delete

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

Select : All, None

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

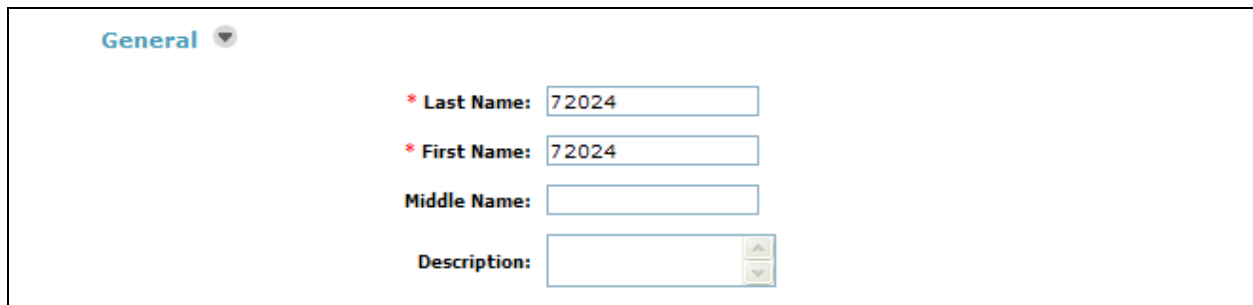


## 6.11. Configure SIP Users

During the compliance test, no special users were created for this solution. All users were created prior to the compliance test. However, the steps to configure a user are included. Add new SIP users for each 9600 Series SIP station. 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 the 'General' section of a user configuration form. It includes 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. Each field has a small up/down arrow icon to its right. The 'General' tab is selected and highlighted in blue.

- Identity section
  - **Login Name** – Enter extension number@sip domain name. This domain name is also configured in **Section 5.3** and **Section 6.1**.
  - **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

**Identity** ▼

\* Login Name: 72024@avaya.com

\* Authentication Type: Basic ▼

SMGR Login Password:

\* Password: ••••••

\* Confirm Password: ••••••

Shared Communication Profile Password: •••••

Confirm Password: •••••

Localized Display Name:

Endpoint Display Name:

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.
- **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 6.10** for Communication Manager.
  - **Termination Application Sequence** – Select Application Sequence defined in **Section 6.10** for Communication Manager.
  - **Survivability Server** – Select **(None)** from drop-down menu.
  - **Home Location** – Select Location defined in **Section 6.2**.

✓ 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 6.8** for Communication Manager.
  - **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 new user. The following screen shows the created users 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 / Users / Manage Users

Elements
Events
Groups & Roles
Licenses
Routing
Security
System Manager
Data
Users
Manage Users
Public Contact
Lists
Shared Addresses
System Presence
ACLs
Help

### User Management

Users

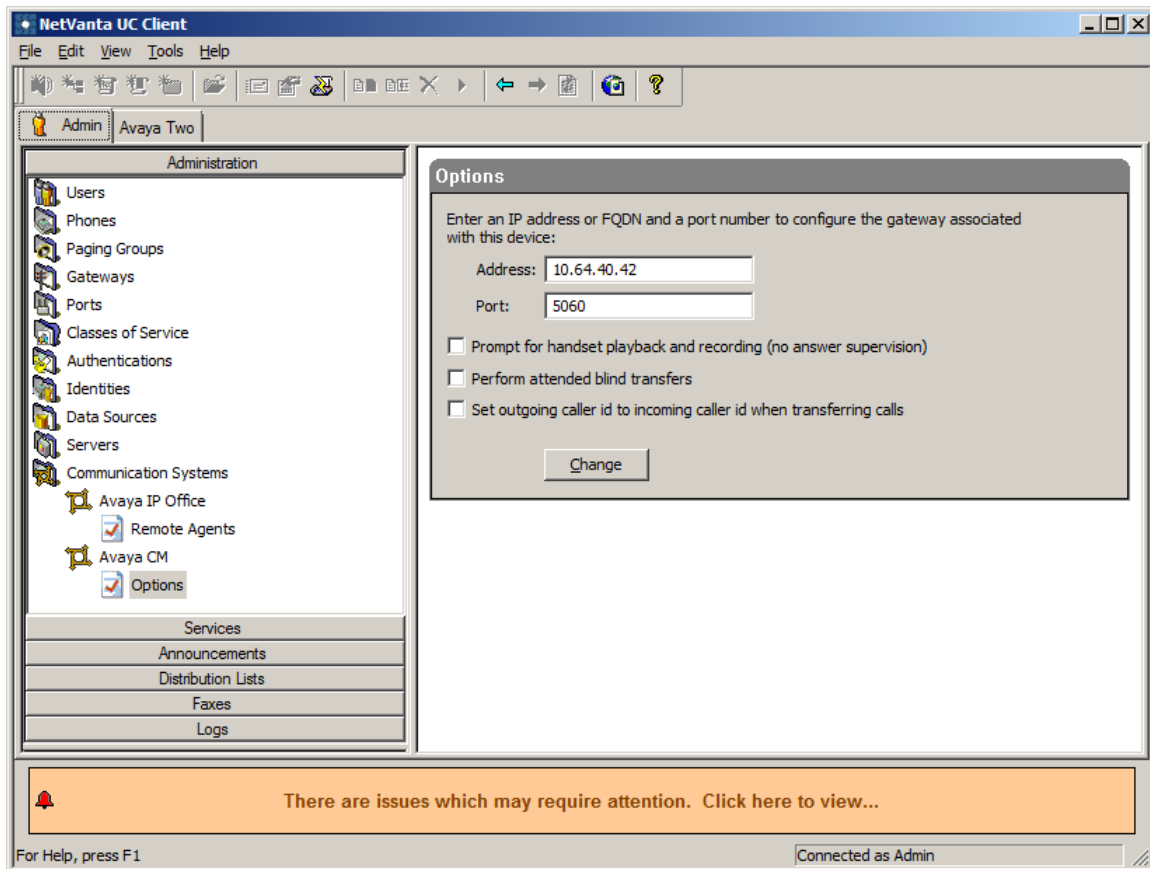
8 Items Refresh Show ALL Filter: Enable

<input type="checkbox"/>	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		

## 7. Configure the ADTRAN UC Server

ADTRAN installs, configures, and customizes the NetVanta UC Server application for their end customers. Thus, this section only describes the interface configuration, so that NetVanta UC Server can talk to Session Manager and Communication Manager. To configure NetVanta UC Server, click on the NetVanta UC Server Client icon on the DeskTop. The NetVanta UC Server Client should be displayed. Navigate to Communications Systems and right click on that icon. Create a Communication System and name it Avaya CM. Now navigate to **Communication Systems → Avaya CM → Options** and enter the Session Manager IP address in the **Address** field.

Click the **Change** button to submit the change.



Select **Ports** from the left pane. Double click the Avaya CM port.  
The Port-Avaya CM window should appear.


Provide the following information:

- **Port number:** Enter **5080**. During the compliance test, the port 5080 was utilized on the NetVanta UC Server.
- **Protocol:** Select TCP/UDP, using the drop down menu.

Click the **OK** button.

**Port - Avaya CM**

General information

 **Name:** Avaya CM

**Identity:** 73015

☒ **Enable use of port for:**


☒ **Handset call** ☒ **Fax transmission**

☒ **Pager notification** ☐ **Port audit**

☒ **Message delivery** ☒ **Outbound dialing**

☐ **Message waiting indicator changes**


Device options

 **Communication System:** Avaya CM

**Device:** Built-in SIP Port

**Information:**  
SIP (5080/TCP/UDP)

SIP options

 **Port number:** 5080

**Protocol:** TCP/UDP

OK Cancel Help

## 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 NetVanta UC Server, and transfer and conference can be accomplished.
- 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 ADTRAN UC Server to interoperate with Session Manager and Communication Manager. ADTRAN UC Server 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™ Session Manager*, August 2010, Release 6.0, Document Number 03-603324.
- [3] *Administering Avaya™ System Manager*, June 2010, Release 6.0.

---

**©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](mailto:devconnect@avaya.com).