Avaya Solution & Interoperability Test Lab

Application Note for the Polycom KIRK Wireless Server 6000 with Avaya Aura™ Session Manager 6.0 - Issue 1.0

Abstract

This Application Note describes a compliance-tested configuration comprised of Polycom KIRK Wireless Server 6000, KIRK 4040/5040 SIP DECT handsets and Avaya Aura™ Session Manager.

Information in this Application Note 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 a compliance-tested configuration comprised of Polycom KIRK Wireless Server 6000, Polycom KIRK 4040/5040 SIP DECT handsets and Avaya Aura™ Session Manager. For this compliance test, the Polycom KIRK SIP DECT 4040/5040 handsets and Avaya 9600 Series SIP telephones were registered to Avaya Aura™ Session Manager.

The Polycom KIRK Wireless Server 6000 is a wireless Digital Enhanced Cordless Telecommunications (DECT) solution capable of communicating with Avaya Aura™ Session Manager using standard SIP. The Polycom KIRK Wireless Server 6000 combines wireless DECT with SIP IP telephony. Each Polycom KIRK Wireless Server 6000 can register up to 4096 wireless DECT handsets and handle up to 1024 simultaneous calls.

Polycom offers a broad range of DECT handsets that address a broad range of end-user requirements, including the established 40xx series of robust handsets to the latest generation of industry-specific devices: 50xx series for retail/hospitality; 60xx series for manufacturing; 70xx series for healthcare. The testing includes examples for both generations of product to prove compatibility and interoperability for the entire product range.

1.1 Interoperability Compliance Testing

The purpose of the interoperability compliance testing is to verify interoperability of the Polycom KIRK Wireless Server 6000 and the Polycom KIRK 4040/5040 handsets with Avaya Aura™ Session Manager and Avaya SIP telephones. The following objectives for interoperability testing were identified:

1. Demonstrate that Avaya Aura™ Session Manager and the Polycom KIRK 4040/5040 DECT handsets operate as specified and can interoperate in an environment similar to the one that will be encountered at a customer's premises.
2. Demonstrate that Avaya Aura™ Session Manager and the Polycom KIRK 4040/5040 DECT handsets, when used in the tested configurations, meet the serviceability and support standards of the respective organizations.
3. Observe and characterize how the products behave under failure conditions, and provide input for problem isolation procedures.

1.2 Support

Technical support can be obtained for Polycom KIRK products from Polycom. See the support link at http://www.polycom.com/support/index.html for contact information.

2 Reference Configuration

Figure 1 illustrates the test configuration used during compliance testing to verify the KIRK Wireless Server 6000 solution. The configuration was comprised of an Avaya S8510 Server running Communication Manager (configured as an Evolution Server) with an Avaya G650 Media Gateway, an Avaya 8510 Server running System Manager, an Avaya S8510 Server running Session Manager, a KIRK Wireless Server 6000 solution with KIRK 4040/5040 DECT handsets.

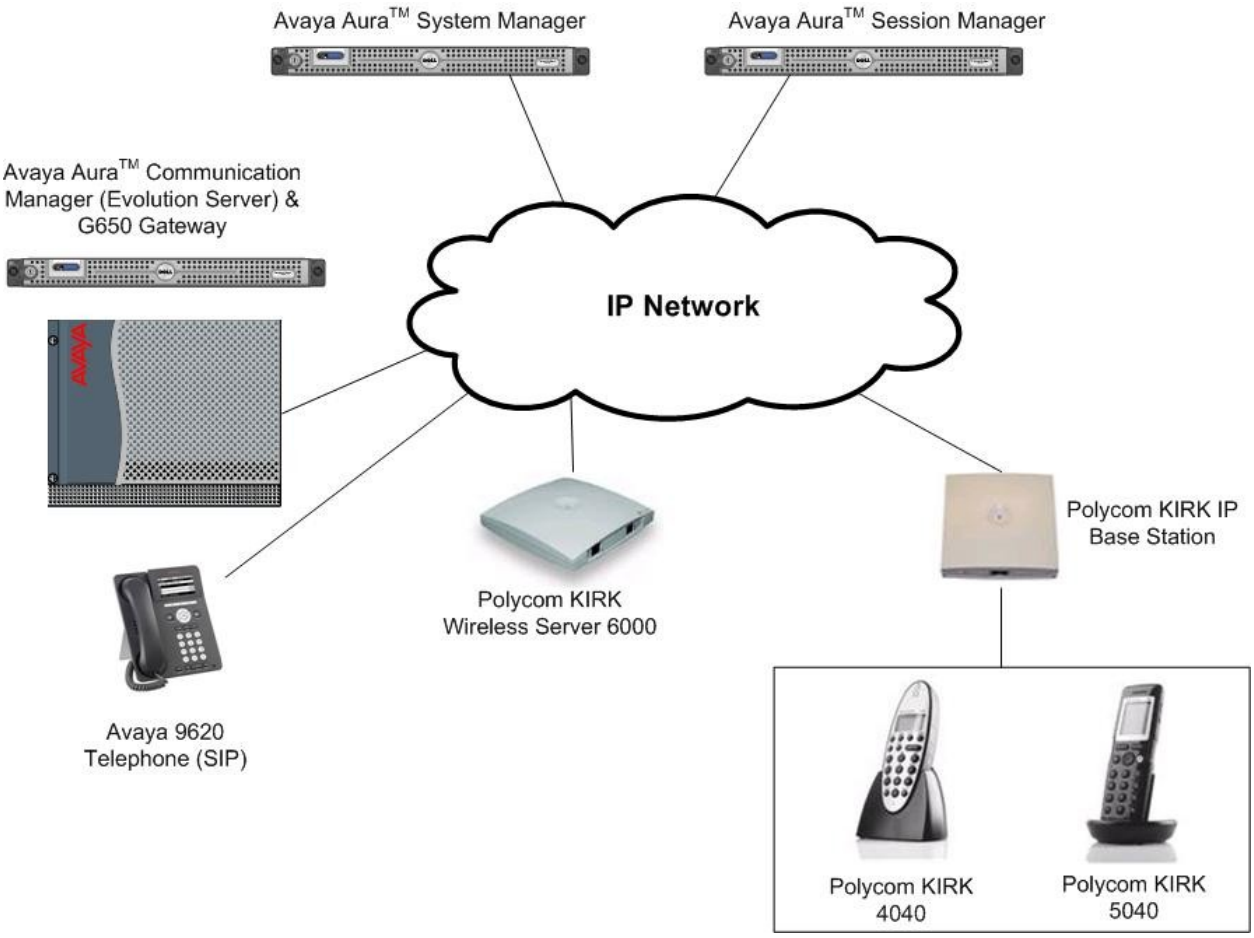


Figure 1: Network Topology

3 Equipment and Software Validated

All the hardware and associated software used in the compliance testing is listed below.

Equipment	Software/Firmware
Avaya S8510 Server	Avaya Aura™ Communication Manager 6.0 SP1
Avaya G650 Media Gateway • TN799DP C-LAN Circuit Pack • TN2312BP IP Server Interface • TN2602AP IP Media Pro	 HW16 FW038 HW15 FW051 HW08 FW055
Avaya S8510 Server	Avaya Aura™ Session Manager 6.0
Avaya S8510 Server	Avaya Aura™ System Manager 6.0
Avaya 9620 IP Telephone (SIP)	2.6.2
Polycom KIRK KWS6000	PCS06A_
Polycom KIRK IP Base Station	PCS06A_
Polycom KIRK 4040 DECT handset	PCS06Uc
Polycom KIRK 5040 DECT handset	PCS08Eb

Table 1: Hardware and Software Version Numbers

4 Configuration of Avaya Aura™ Session Manager

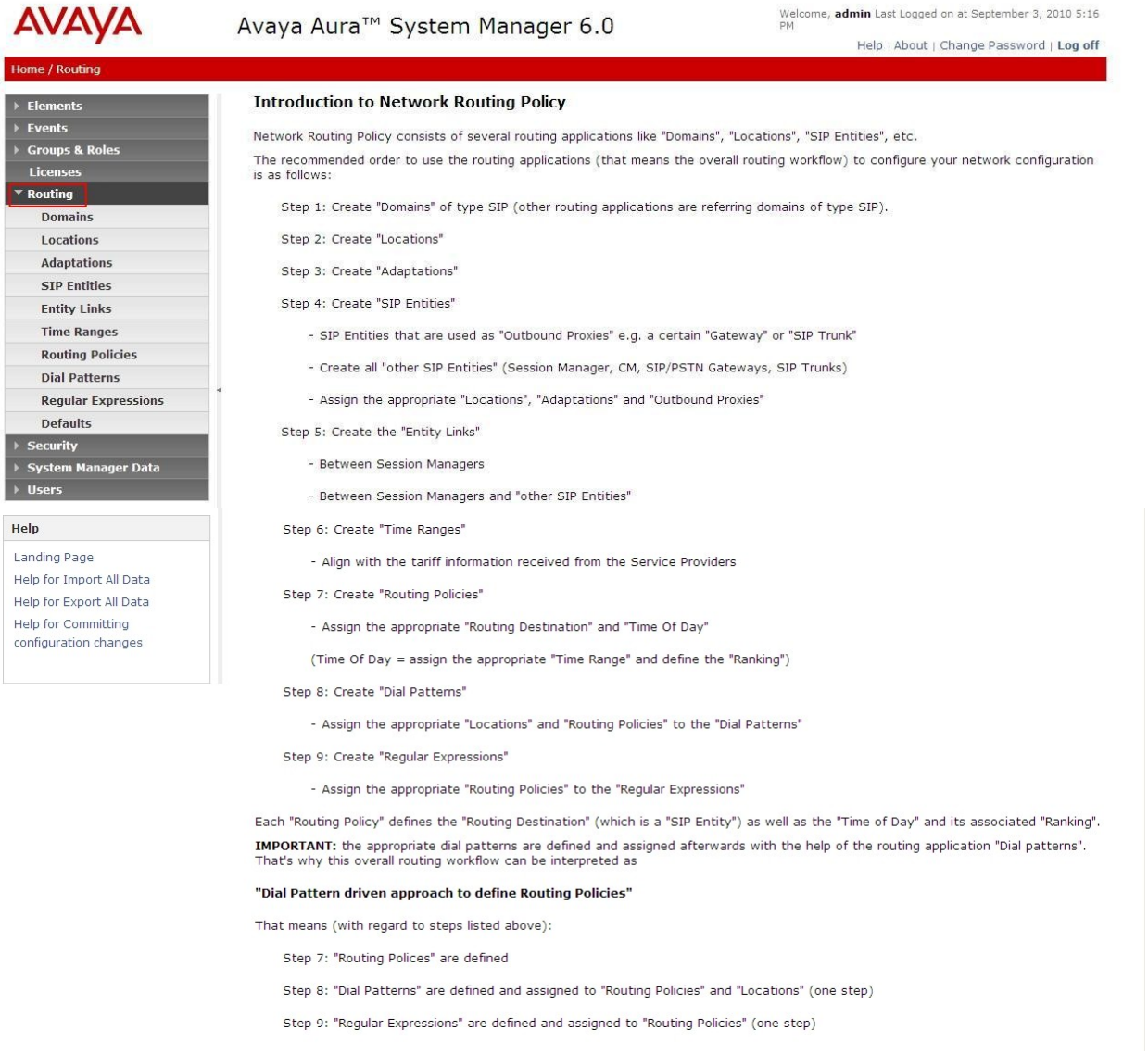
These Application Notes assume that Session Manager and Communication Manager (Evolution Server) are configured and operational. This section focuses only on the configuration of the connection to the KIRK Wireless Server 6000 and the DECT users. The values configured in this section were used during the compliance test with default values being used for other fields not configured in these Application Notes. The procedures include the following areas:

- Log into Avaya Aura™ Session Manager
- Administer SIP Entity
- Administer Entity Link
- Add Users for DECT Phones

4.1 Log into Avaya Aura™ Session Manager

Access the System Manager using a Web Browser and entering ***http://<ip-address>/SMGR***, where <ip-address> is the IP address of System Manager. Log in using appropriate credentials and accept the subsequent Copyright Legal Notice.

By selecting **Routing** from the left panel menu, a short procedure for configuring Network Routing Policy is shown on the right panel.



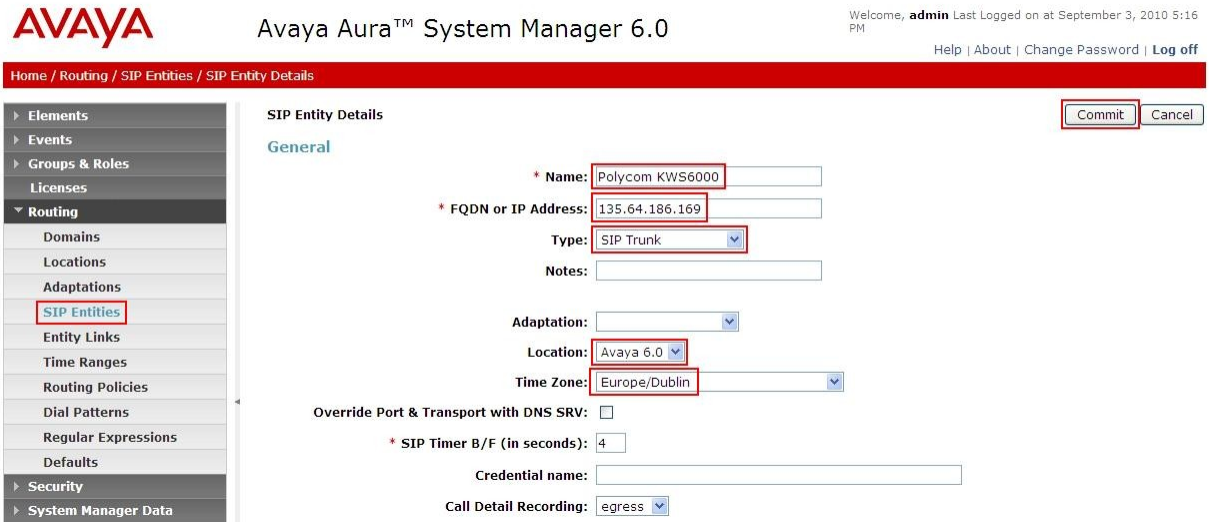
4.2 Administer SIP Entity

A SIP Entity must be added for the KIRK Wireless Server 6000. To add a SIP Entity, select **SIP Entities** from the left panel menu and then click on the **New** button (not shown). Enter the following for the SIP Entity:

Under **General:**

- **Name** An informative name (e.g., **Polycom KWS6000**)
- **FQDN or IP Address** IP address of the signaling interface on the KWS6000
- **Type** **SIP Trunk**
- **Location** A predefined location
- **Time Zone** Time zone for this location

Click **Commit** to save changes.

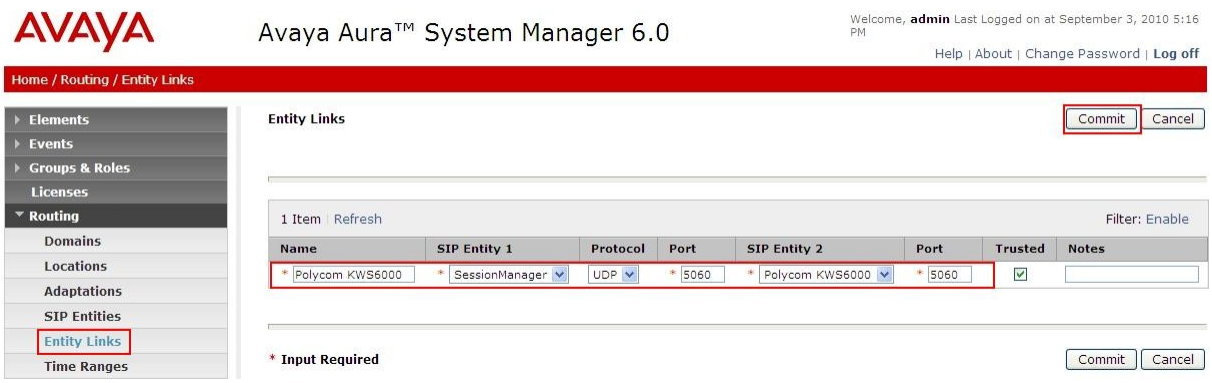


4.3 Administer Entity Link

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. To add an Entity Link, select **Entity Links** from the left panel menu and click on the **New** button (not shown). Fill in the following fields in the new row that is displayed.

- **Name** An informative name
- **SIP Entity 1** Select **SessionManager** (previously configured)
- **Port** Port number to which the other system sends its SIP requests
- **SIP Entity 2** The KWS6000 SIP Entity created in **Section 4.2**
- **Port** Port number to which the other system expects to receive SIP requests
- **Trusted** Whether to trust the other system (i.e., SIP Entity 2)
- **Protocol** Transport protocol to be used to send SIP requests

Click **Commit** to save changes.

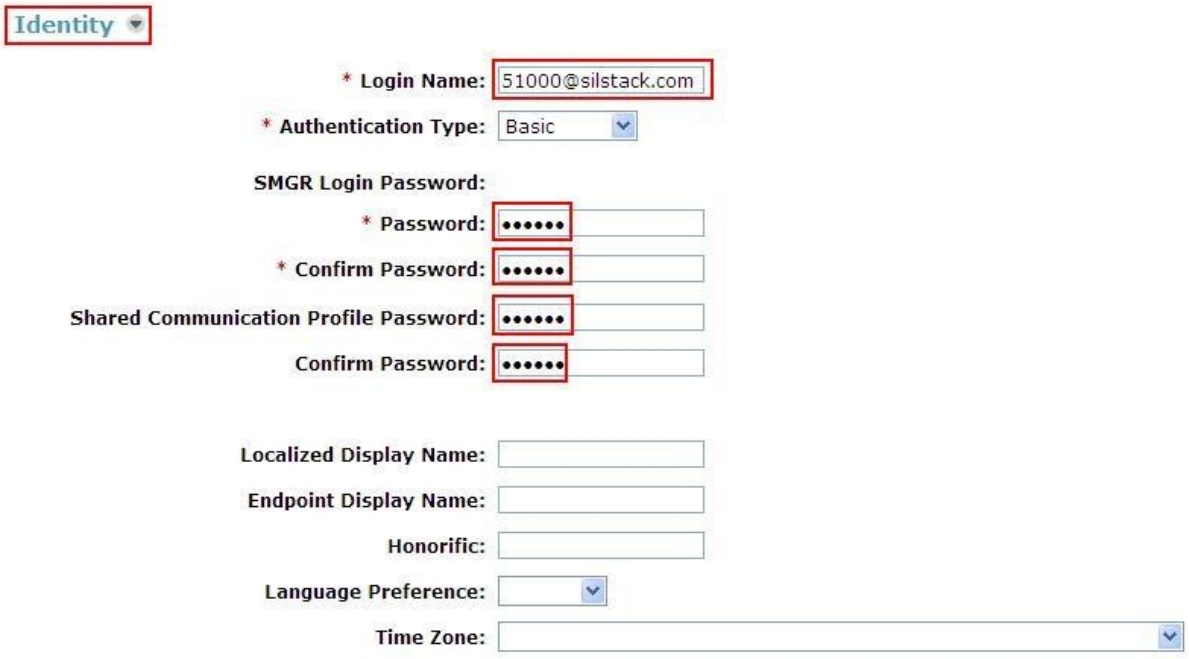


4.4 Add Users for DECT Phones

Users must be added via Session Manager and the details will be updated on Communication Manager. Select **Users → Manage Users** on the left. Click on **New** (not shown). Enter a **First Name** and **Last Name**.

Navigate to the **Identity** section and enter the following and use defaults for other fields:

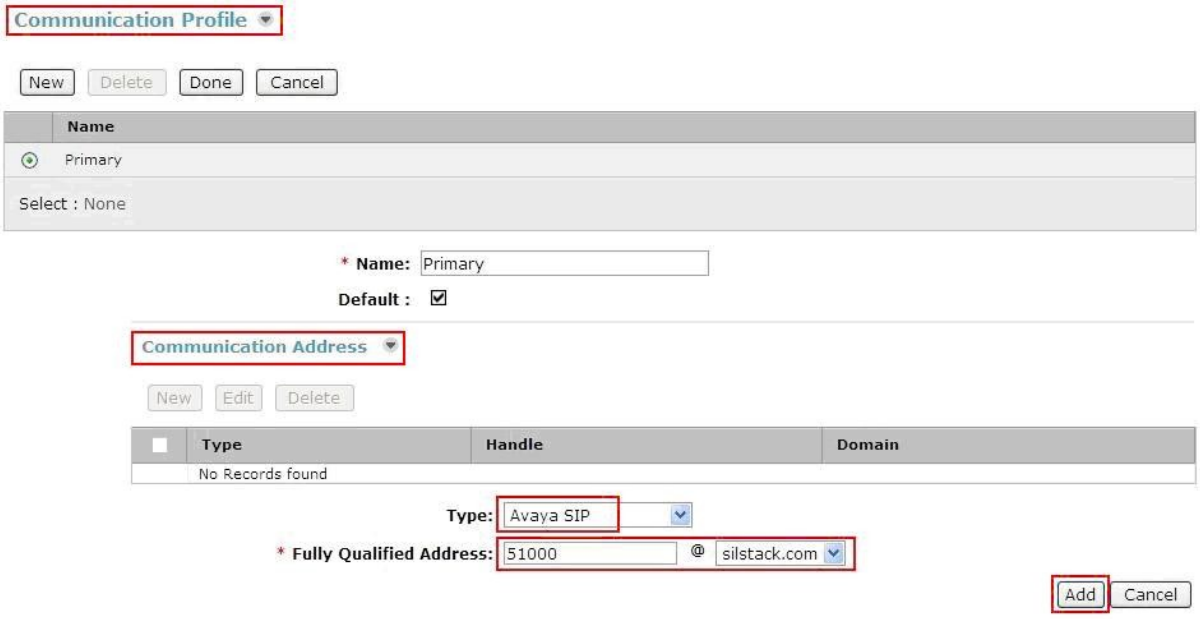
- **Login Name** The desired phone extension *number@domain name*
- **Password** Password for user to log into System Manager
- **Shared Communication Profile Password**
  Password to be entered by the user when registering with Session Manager



Navigate to and click on **Communication Profile** section to expand. Click on **Communication Address** to expand that section. Enter the following and defaults for the remaining fields:

- **Type** Select **Avaya SIP**
- **Fully Qualified Address** Enter the extension number

Click on **Add**.



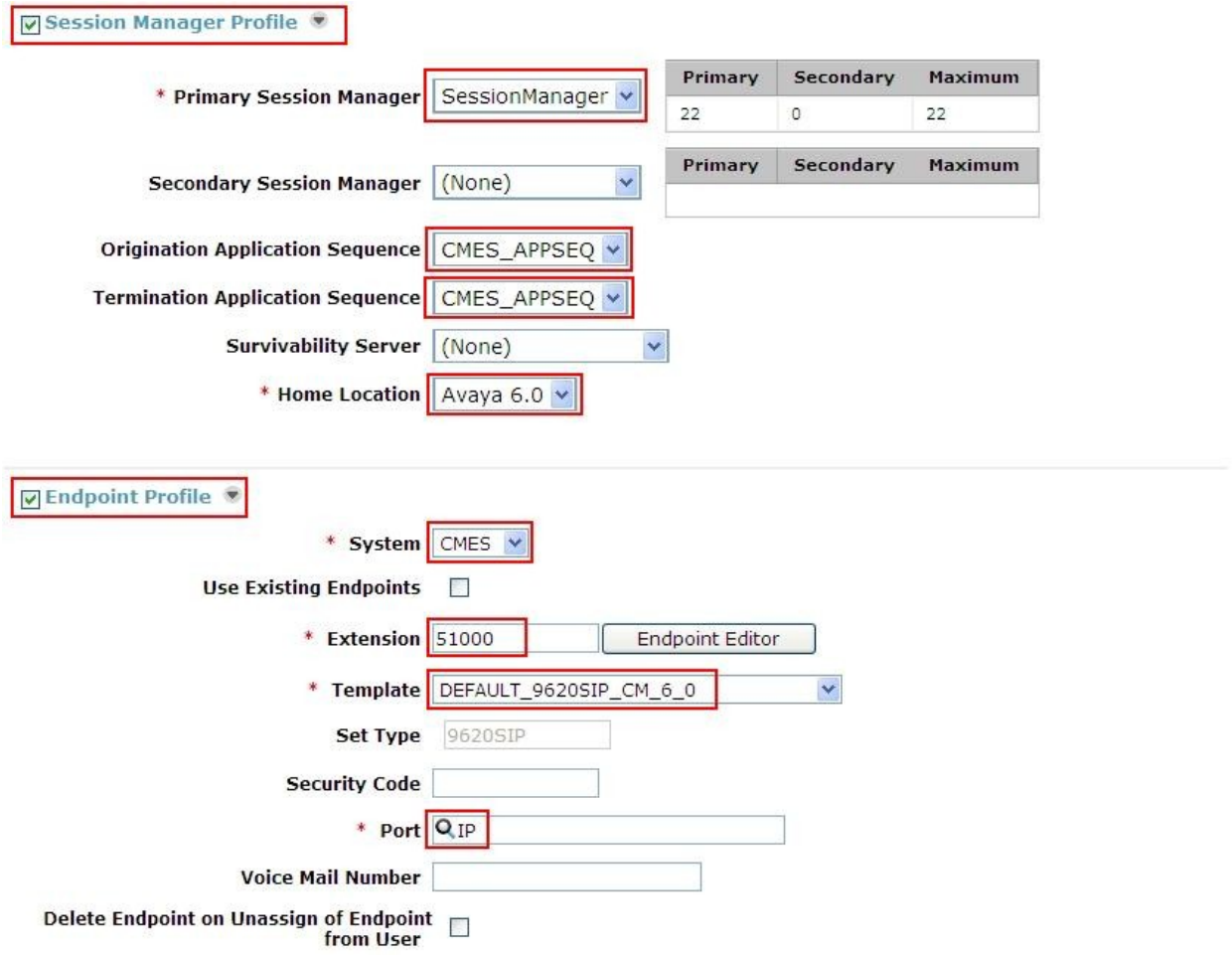
Navigate to and click on **Session Manager Profile** to expand that section. Enter the following fields and use defaults for the remaining fields:

- **Primary Session Manager** Select a Session Manager
- **Origination Application Sequence** Select a CM originating application sequence
- **Termination Application Sequence** Select a CM terminating application sequence
- **Home Location** Select a home location

Click on **Endpoint Profile** to expand that section. Enter the following fields and use defaults for the remaining fields:

- **System** Select the CM Entity
- **Extension** Enter a desired extension number
- **Template** Select a telephone type template
- **Port** Select **IP**

Click on **Commit** to save (not shown).



5 Configure KIRK Wireless Server 6000 Solution

This section focuses only on the configuration of the KIRK Wireless Server 6000 solution. The values configured in this section were used during the compliance tests with default values being used for other fields not configured in these Application Notes. The procedures include the following areas:

- Administer KIRK Wireless Server IP address
- Administer DECT handset subscription
- Enable Call Forward feature code
- Administer SIP configuration
- Administer DECT users
- Administer KIRK Base Station IP address
- Administer Wireless Sever host

5.1 Administer KIRK Wireless Server IP address

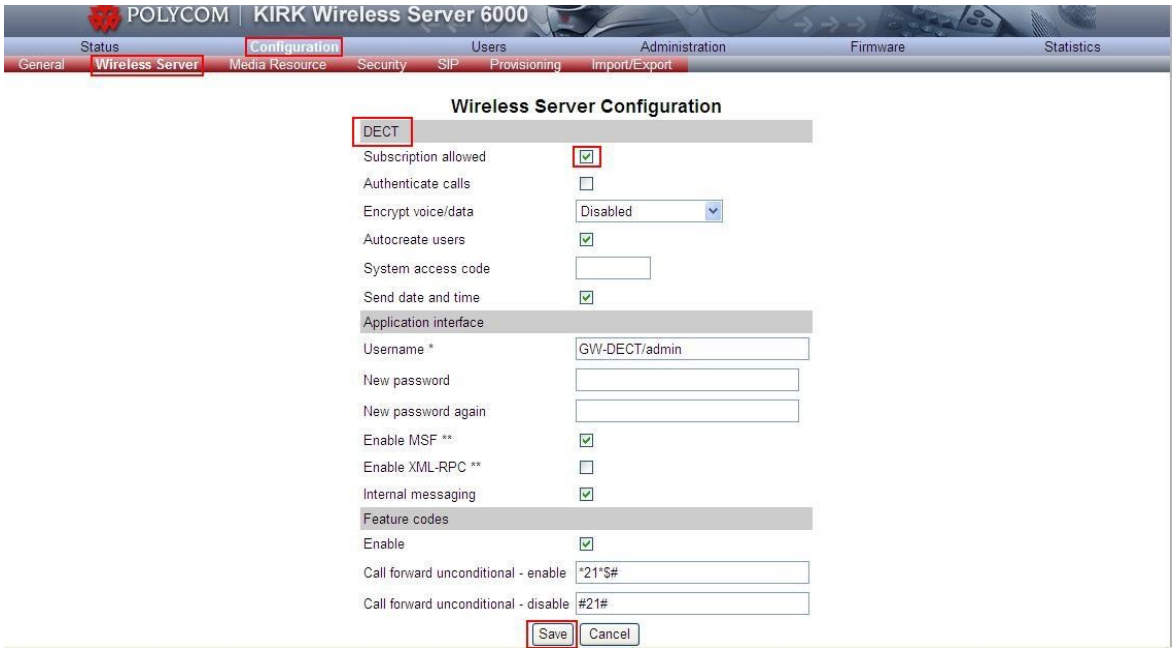
The default IP address of a KWS6000 is 192.168.0.1. Connect a PC directly to the KWS6000 with an Ethernet crossover cable. Open up an Internet browser and type in the following URL: ***http://192.168.0.1.*** From the menu, click on **Configuration → General** and enter the following:

- **Use Static IP address** Click button to select
- **IP addr** Enter IP address
- **Netmask** Enter subnet mask address
- **Gateway** Enter default gateway address

Click **Save** (not shown) to save changes.

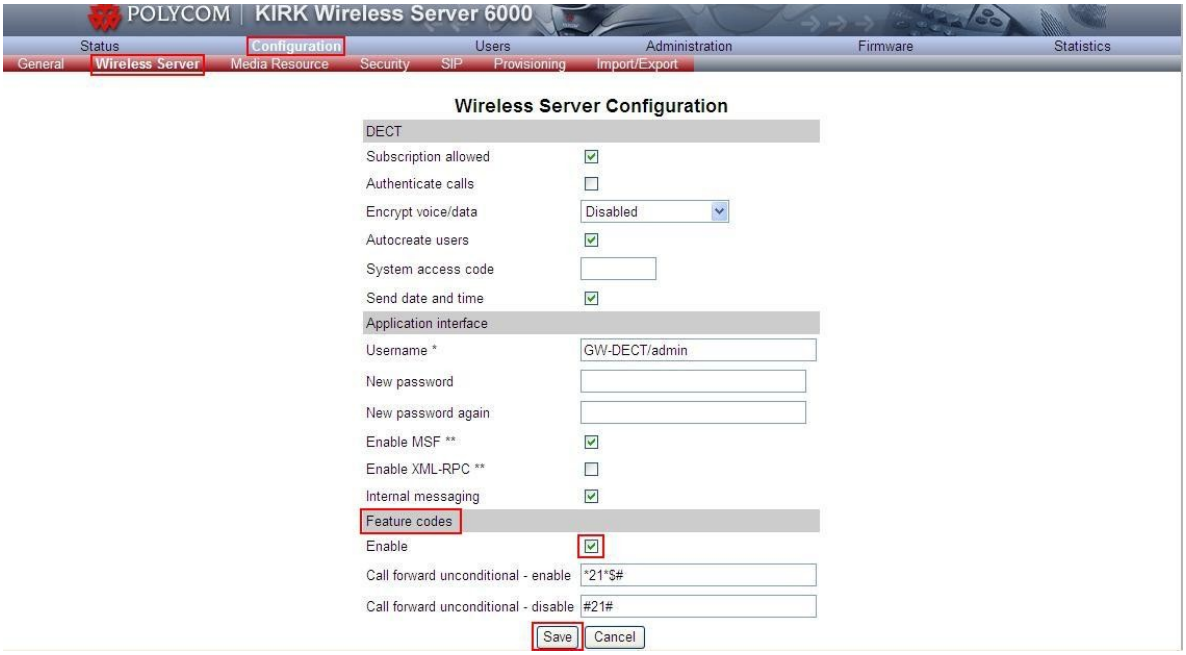
5.2 Administer DECT handset subscription

From the menu, click on **Configuration → Wireless Server.** Navigate to the **DECT** section and check the box next to **Subscription Allowed.** Click **Save** to save changes.



5.3 Enable Call Forward Feature Code

From the menu, click on **Configuration → Wireless Server**. Navigate to the **Feature Codes** section and check the box next to **Enable.** Click **Save** to save changes.



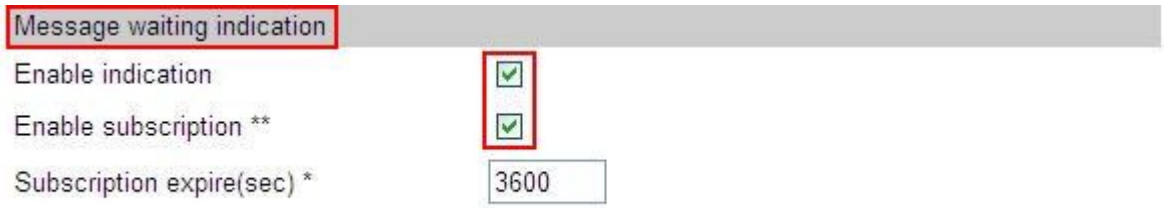
5.4 Administer SIP Configuration

This section details the settings needed to create the SIP connection from the KWS6000 to the Session Manager. Preferred audio codecs and message waiting indications are also set. From the menu, go to **Configuration → SIP** and enter the following:

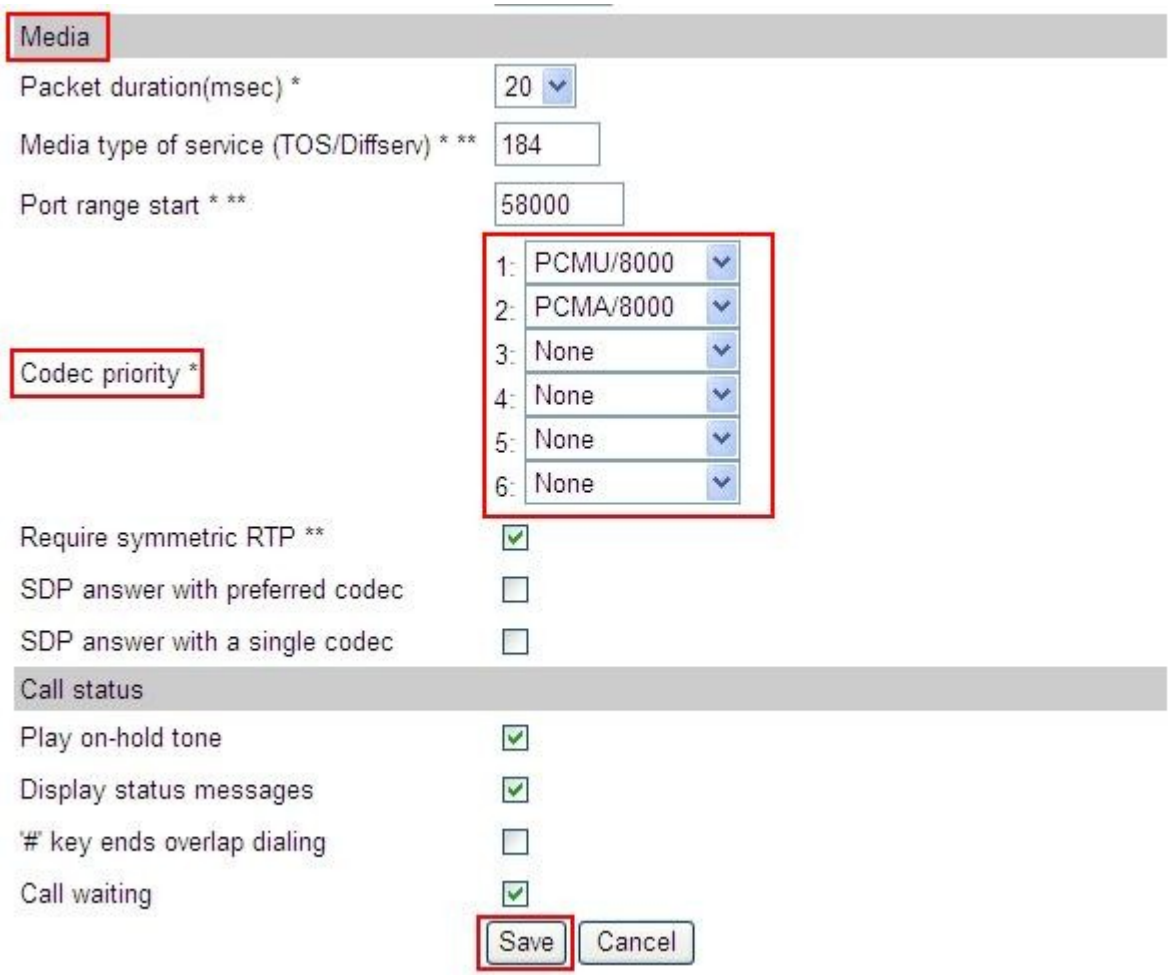
- **Local Port** **5060**
- **Transport** **UDP only**
- **Default Domain** Enter domain name (e.g. **silstack.com)**

Navigate to the **Proxies** section and on the **Proxy 1** row enter the sip **URI** for the Session Manager SM100 IP address.

Navigate to the **Message waiting indication** section, check the boxes next to **Enable indication** and **Enable subscription**.



Navigate to the **Media** section and select preferred codecs and priority. Click on **Save** to save changes.



5.5 Administer DECT users

From the menu, go to **Users → List Users** and click on the **New** button to add a new user.

Enter the following in the new **User** window:

- **IPEI** Enter the handset IPEI
- **Access Code** Enter a desired access code (Optional)
- **Standby Text** Enter desired standby text (Optional)
- **Username / Extension** Enter the extension number defined in **Section 4.4**
- **Domain** Enter the domain name used in **Section 4.4**
- **Displayname** Enter a desired display name (Optional)
- **Authentication User** Enter the user defined in **Section 4.4**
- **Authentication Password** Enter the **Shared communication profile password** defined in **Section 4.4**

Click on **Save** to save changes.

5.6 Administer KIRK Base Station IP address

The default IP address of a KIRK Base Station is 192.168.0.1. Connect a PC directly to the Base Station with an Ethernet crossover cable. Open up an Internet browser and type in the following URL: ***http://192.168.0.1.*** From the menu, click on **Configuration → General** and enter the following:

- **Use Static IP address** Click button to select
- **IP addr** Enter IP address
- **Netmask** Enter subnet mask address
- **Gateway** Enter default gateway address

Click **Save** (not shown) to save changes.

5.7 Administer Wireless Sever host

From the menu, go to **Configuration → Base Station** and for **Host** enter the ip address of the KIRK Wireless Server 6000 configured in **Section 5.1**. Click **Save** to save changes.

6 General Test Approach and Test Results

The compliance testing focused on the ability of the KIRK Wireless Server 6000 and KIRK DECT handsets to interoperate with the Session Manager and Avaya 9600 Series IP telephones. The interoperability compliance test included feature and serviceability testing. The KIRK 4040 and 5040 handsets functioned correctly with good audio quality in both directions. Functionality was tested across a range of basic telephony operations such as:

- Basic calls to/from Avaya and KIRK DECT handsets
- Call Hold
- Call Transfer (Blind and Supervised)
- Call Diversion/Forwarding
- Conference Calls
- Message Waiting
- Caller ID
- Handset messaging

The serviceability tests were performed by resetting and reconnecting the KIRK DECT handsets, restarting the Session Manager and resetting the KIRK Wireless Server 6000.

7 Verification Steps

To verify that the KIRK Wireless Sever 6000 is operating properly, go to the KWS6000 web admin tool. From the menu bar, go to **Users → List Users** and verify that each user has subscribed and registered successfully.

8 Conclusion

These Application Notes describe the configuration steps required for the Polycom KIRK Wireless Server 6000 solution to successfully interoperate with Avaya Aura™ Session Manager and Avaya Aura™ Communication Manager. All feature functionality and serviceability test cases were completed successfully.

9 Additional References

This section references the Avaya and Polycom KIRK product documentation that are relevant to these Application Notes.

Product documentation for Avaya products may be found at http://support.avaya.com

[1] *Administering Avaya Aura™ Session Manager*, Doc # 03-603324, Issue 3
[2] *Administering Avaya Aura™ Communication Manager*, Doc # 03-300509, Issue 6.0

Product documentation for Polycom KIRK Wireless Solution 6000 may be found at:
http://www.polycom.com/support/voice/dect/dect_ws_6000.html

[1] *KIRK Wireless Server 6000 Installation and Configuration Guide*, Version 2

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.