Avaya Solution & Interoperability Test Lab

Application Notes for Spectralink Wireless Server 6500/400 with Avaya Aura® Communication Manager and Avaya Aura® Session Manager - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for the Spectralink Wireless Server 6500/400 to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Functionality was validated and compliance testing was conducted in order to verify proper operation.

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

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

1. Introduction

The Spectralink Wireless Server is a wireless Digital Enhanced Cordless Telecommunications (DECT) solution capable of communicating via Session Initiation Protocol (SIP) with Avaya Aura® Session Manager. The Spectralink Wireless Server combines wireless DECT with SIP IP telephony. Each Spectralink Wireless Server can register up to 4,096 wireless DECT phones and handle up to 1,024 simultaneous calls.

2. General Test Approach and Test Results

The compliance testing focused on the ability of the Spectralink Wireless Server and Spectralink DECT handsets to interoperate with Communication Manager and Session Manager and various Avaya telephones, including SIP, H.323, digital and analog. The interoperability compliance test included feature and serviceability testing. The Spectralink Butterfly and 76 Series handsets functioned correctly with good audio quality in both directions. All test cases were executed manually.

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

2.1. Interoperability Compliance Testing

The interoperability compliance test included functionality, failover and serviceability testing. The main objective was to verify Spectralink Wireless Server interoperability with Communication Manager and Session Manager.

Functionality was tested across a range of basic telephony operations including:

- Basic calls to/from Avaya and Spectralink DECT handsets
- Call Hold
- Call Transfer (Blind and Attended)
- Call Forwarding
- Conference Call Participation
- Message Waiting Indicator
- Caller ID
- Call Park
- Multiple Call Appearances
- G.711MU, G.711A, and G.729 Codecs
- Media Shuffling
- Extension to Cellular (EC500)
- Base Station Roaming
- Base Station Failure

Failover testing was performed by disconnecting one of the active base stations. Serviceability tests were performed by resetting and reconnecting the Spectralink DECT handsets, and restarting the Spectralink Wireless Server.

2.2. Test Results

Spectralink successfully achieved the above objectives. All test cases passed.

Testing was completed with the Spectralink Wireless Server 6500. The Spectralink Wireless Server 400 was not used in compliance testing; however, Spectralink has provided the following statement:

"We, Spectralink Corporation, hereby confirm that the following IP-DECT servers
• Spectralink IP DECT Server 400
• Spectralink IP DECT Server 6500
are based on the same platform and therefore:
• Use identical SIP stack
• Use identical XML-RPC API for messaging
• Use the same firmware for support of both platforms"

2.3. Support

For technical support on Spectralink products, contact Spectralink at technicalsupport@spectralink.com , or refer to http://support.spectralink.com.

3. Reference Configuration

Figure 1 illustrates the setup used for compliance testing. The configuration enabled Communication Manager and Session Manager, to interoperate with the Spectralink Wireless Server using SIP. Spectralink DECT handsets register with the Spectralink Wireless Server via the Spectralink Base Stations and the Spectralink Wireless Server functions as a SIP Proxy for the Spectralink DECT handsets.

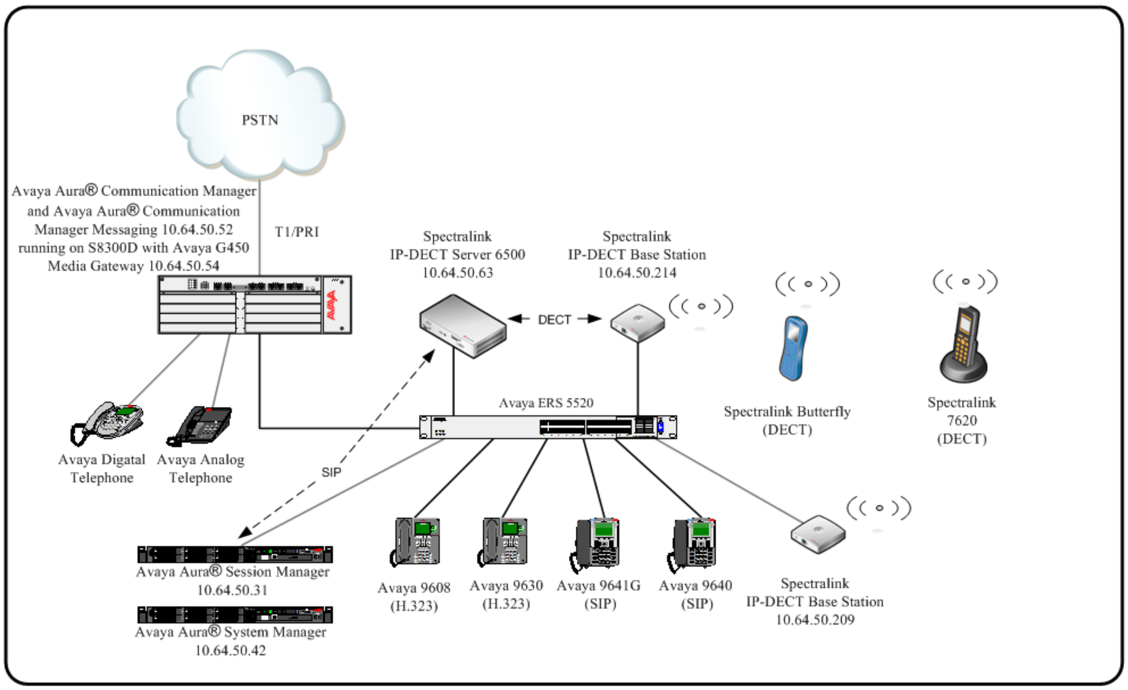


Figure 1: Spectralink Wireless Server Solution

4. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya PBX Products	
Avaya Aura® Communication Manager	6.3 SP6
Avaya Aura® Session Manager	6.3.8
Avaya Messaging (Voice Mail) Products	
Avaya Aura® Communication Manager Messaging	6.3 SP6
Avaya Endpoints	
Avaya 96xx Series IP Deskphone	(H.323 3.2) (SIP 2.6)
Avaya 96x1 Series IP Deskphone	(H.323 6.4) (SIP 6.4)
Avaya Digital Telephone	R39
Avaya Analog Telephone	NA
Spectralink Products	
Spectralink Wireless Server 6500	PCS14B_
Spectralink IP DECT Base Station	PCS14B_
Spectralink 76-Series Handsets	PCS14HB
Spectralink Butterfly Series Handsets	PCS14HB

5. Configure Avaya Aura® Communication Manager

This section describes the steps required for Communication Manager to support the configuration in **Figure 1**. The following pages provide step-by-step instructions on how to administer parameters specific to the Spectralink solution only. The assumption is that the appropriate license and authentication files have been installed on the servers and that login and password credentials are available and that the reader has a basic understanding of the administration of Communication Manager and Session Manager. It is assumed that all other connections, e.g., to PSTN, to LAN, are configured and will not be covered in this document. The reader will need access to the System Administration Terminal screen (SAT). For detailed information on the installation, maintenance, and configuration of Communication Manager, please refer to **Section 10**.

5.1. Configure Node-Names IP

In the **IP NODE NAMES** form, assign the name and IP address of Session Manager. This is used to terminate the SIP Entity Link with Session Manager. The names will be used in the signaling group configuration.
Enter the **change node-names ip** command. Specify node names and security module IP address for Session Manager.

```
change node-names ip                                              Page   1 of   2
                                  IP NODE NAMES
    Name                IP Address
abacus2               10.64.50.64
cms                   10.64.10.85
default               0.0.0.0
iq1                   10.64.50.15
msgserver             10.64.50.52
procr                 10.64.50.52
procr6                ::
sm5031                10.64.50.31
util5022              10.64.50.22









( 9  of 9    administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
```

5.2. IP Codec Set and IP Network Region

Enter the **change ip-codec-set g** command, where "g" is a number between 1 and 7, inclusive, and enter "**G.711MU**" for **Audio Codec**. This IP codec set will be selected later in the IP Network Region form to define which codecs may be used within an IP network region.
Note: *During compliance testing G.711MU, G.711A, and G.729 were used.*

```
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: G.711A           n          2        20
 3: G.729            n          2        20
 4:
 5:
 6:
 7:


     Media Encryption
 1: none
 2:
 3:
```

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is *d4f27.com*. By default, **IP-IP Direct Audio** (shuffling) is enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya G450 Media gateway. The **IP Network Region** form also specifies the **IP Codec Set** to be used for Desk Phone calls. This IP codec set is used when its corresponding network region (i.e., IP Network Region '1') is specified in the SIP signaling groups.

Enter the **change ip-network-region h** command, where "h" is a number between 1 and 250, inclusive. On page 1 of the **ip-network-region** form, set **Codec Set** to the number of the IP codec set configured in previous step. Accept the default values for the other fields.

```
change ip-network-region 1                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: d4f27.com
    Name:                      Stub Network Region: n
MEDIA PARAMETERS               Intra-region IP-IP Direct Audio: yes
      Codec Set: 1             Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                     IP Audio Hairpinning? y
   UDP Port Max: 65535
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
```

5.3. Configure Signaling and Trunk Groups

Add a signaling group for calls that need to be routed to SIP Endpoints registered with Session Manager. Prior to configuring a SIP trunk group for communication with Session Manager, a SIP signaling group must be configured. Configure the Signaling Group form as shown below:

- Set the **Group Type** field to *sip*.
- Specify the Communication Manager (procr) and the Session Manager as the two end-points of the signaling group in the **Near-end Node Name** field and the **Far-end Node Name** field, respectively. These field values were configured in the **IP Node Names** form shown in **Section5.1**.
- Compliance testing used TLS and port value of *5061* in the **Near-end Listen Port** and the **Far-end Listen Port** fields. If the **Far-end Network Region** field is configured, the codec for the call will be selected from the IP codec set assigned to that network region.
- Enter the domain name in the **Far-end Domain** field. In this configuration, the domain name is *d4f27.com*.
- The **DTMF over IP** field is set to the default value of *rtp-payload*. Communication Manager supports DTMF transmission using RFC 2833.
- The default values for the other fields may be used.

```
add signaling-group 2                                          Page   1 of   2
                                SIGNALING GROUP

 Group Number: 2             Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? n                                  Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: Others



   Near-end Node Name: procr                  Far-end Node Name: sm5031
 Near-end Listen Port: 5061                 Far-end Listen Port: 5061
                                         Far-end Network Region: 1

Far-end Domain: d4f27.com
                                              Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                   RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload             Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                       IP Audio Hairpinning? n
         Enable Layer 3 Test? y                    Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n             Alternate Route Timer(sec): 6

ESC-x=Cancel Esc-e=Submit Esc-p=Prev Pg Esc-n=Next Pg Esc-h=Help Esc-r=Refresh
```

Configure the **Trunk Group** form shown below for outgoing calls to be routed to Session Manager.

- Set the **Group Type** field to "**sip**".
- Enter a meaningful name/description for **Group Name.**
- Enter a **Trunk Access Code (TAC)** that is valid under the provisioned dial plan
- Set the **Service Type** field to "**tie**".
- Specify the **Signaling Group** associated with this trunk group.
- Specify the **Number of Members** supported by this SIP trunk group
- The default values for the other fields may be used.

```
add trunk-group 2                                              Page   1 of  21
                                TRUNK GROUP

Group Number: 20                    Group Type: sip           CDR Reports: y
  Group Name: To Session Manager           COR: 1        TN: 1        TAC: *002
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                     Night Service:
Queue Length: 0
Service Type:                        Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 2
                                                     Number of Members: 10
```

5.4. Dial Plan and Access Codes

The dial plan defines what digit strings are defined as extensions and access codes. Feature access codes (fac) can be used to invoke specific PBX features.

Use the **display dialplan analysis** command to display the dial plan. This information will be used in subsequent steps and sections. Extensions beginning with 6 were used for the Avaya and Spectralink Endpoints.

```
display dialplan analysis                                          Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location: all            Percent Full: 2

    Dialed   Total  Call       Dialed   Total  Call       Dialed   Total  Call
    String   Length Type       String   Length Type       String   Length Type
   2           8   ext
   3           5   aar
   4           5   ext
   5           5   udp
   6           5   ext
   7           5   ext
   8           1   fac
   9           1   fac
   *           4   dac
```

Use the "**change feature-access-codes**" command to assign feature access codes for **AAR** and **ARS** (if not already assigned) that is consistent with the existing dial plan.

```
change feature-access-codes                                        Page   1 of  10
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code:
                       Answer Back Access Code:
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: 9      Access Code 2:
                 Automatic Callback Activation:         Deactivation:
Call Forwarding Activation Busy/DA:        All:         Deactivation:
   Call Forwarding Enhanced Status:        Act:         Deactivation:
                         Call Park Access Code:
                       Call Pickup Access Code:
CAS Remote Hold/Answer Hold-Unhold Access Code:
                  CDR Account Code Access Code:
                        Change COR Access Code:
                   Change Coverage Access Code:
            Conditional Call Extend Activation:         Deactivation:
                   Contact Closure   Open Code:           Close Code:
```

5.5. Configure Route Pattern

A route pattern is configured to use the trunk defined in **Section 5.3**. The route pattern can also be configured to perform digit manipulation on outgoing calls if necessary. Calls destined for SIP endpoints registered with Session Manager will be routed using the route pattern defined below.

When configuring a route pattern, use the **change route-pattern x** command, where **x** is an available route pattern number. For the compliance test, route pattern 3 was selected. Set the parameters as shown below.

- For the **Pattern Name**, enter a descriptive name.
- Set the **Grp No** to the trunk group number created in **Section 5.3**.
- Set the **FRL** (Facility Restriction Level) to a value that allows all users access to the trunk that need to use it. The value of **0** is the least restrictive. This is the value used for the compliance test.
- Default values may be used for all other fields.

```
change route-pattern 3                                          Page   1 of   3
                    Pattern Number: 3   Pattern Name: To sm5031
                             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: 2    0                    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
```

5.6. Configure Automatic Alternate Routing

Automatic Alternate Routing (AAR) is used to route calls to SIP Endpoint Registered with Session Manager.

When creating entries in the AAR DIGIT ANALYSIS TABLE, use the **change aar analysis x** command, where **x** is the first digit in the dialed string to be entered. Create an entry to reach the mobile user extensions supported by the configuration in **Figure 1**. The extensions are reached using the aar table entry "**6**". When creating the entries, enter the parameters as defined below.

- For the **Dialed String**, enter the extensions reachable via Session Manager.
- Set the **Total Min** and **Total Max** fields to the number length.
- Set the **Route Pattern** to the route pattern defined in **Section 5.5** that directs calls to the trunk connected to the Avaya Aura® Session Manager.
- Set the **Call Type** to *aar*.

```
change aar analysis 6                                          Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all          Percent Full: 2

          Dialed            Total      Route     Call   Node  ANI
          String           Min  Max  Pattern     Type   Num   Reqd
    61                     5    5     3          aar          n
    69997                  5    5     99         aar          n
    8                      7    7     254        aar          n
    9                      12   12    1          aar          n
```

5.7. Configure EC500

5.7.1. Configure Stations and Off-PBX Station Mapping For Mobile Devices

Each mobile device will be associated with a station extension configured on Communication Manager. The station extension may represent a physical desk phone or an extension with no phone logged in to it. In the case of the compliance test extensions 60002 and 61006 were configured on Communication Manager.

To associate a mobile device to each of these station extensions requires an off-pbx station mapping as shown below.

In general, a mobile device will be associated with an existing desk phone for which the Communication Manager Station extension will already be configured. However, in the case of mobile devices that are not associated with a physical phone then a station must be added.

Use the **change station 61020** command to modify the station for this user. Enter a value of enabled for the **EC500 State:** field.

```
change station 61020                                            Page   2 of   6
                                     STATION
FEATURE OPTIONS
           LWC Reception: spe
          LWC Activation? y                         Coverage Msg Retrieval? y
                                                              Auto Answer: none
             CDR Privacy? n                               Data Restriction? n
                                                Idle Appearance Preference? n
 Per Button Ring Control? n                   Bridged Idle Line Preference? n
   Bridged Call Alerting? n                       Restrict Last Appearance? y
  Active Station Ringing: single

        H.320 Conversion? n         Per Station CPN - Send Calling Number?
                                                         EC500 State: enabled

    MWI Served User Type:
              AUDIX Name:
                                                Coverage After Forwarding? s

 Remote Softphone Emergency Calls: as-on-local Direct IP-IP Audio Connections? y
  Emergency Location Ext: 61020        Always Use? n IP Audio Hairpinning? n
```

To create the mapping between a desktop extension and a mobile device, use the **change off-pbx-telephone station-mapping x** command, where **x** is the desktop extension to be mapped. Multiple station extensions can be added at the same time. Enter the parameters as described below.

- Enter the desktop extension for the **Station Extension**.
- Enter *EC500* for the **Application**.
- Enter the mobile extension for the **Phone Number.**
- Enter *ars* for **Trunk Selection**. This instructs Communication Manager to use the ARS tables to determine how to route this call.
- Enter an off-pbx-telephone configuration set to use with this call. The default values for configuration set 1 were used for compliance testing.

```
change off-pbx-telephone station-mapping 61020              Page   1 of   3
                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station       Application Dial   CC  Phone Number    Trunk       Config  Dual
 Extension                 Prefix                     Selection   Set     Mode
 61020            OPS          -      61020            aar        1
 61020            EC500        -      17205551212      ars        1
```

6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain
- Logical/physical Locations that can be occupied by SIP Entities
- SIP Entities corresponding to Session Manager, and Communication Manager
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Routing Policies, which control call routing between the SIP Entities
- Dial Patterns, which govern to which SIP Entity a call is routed

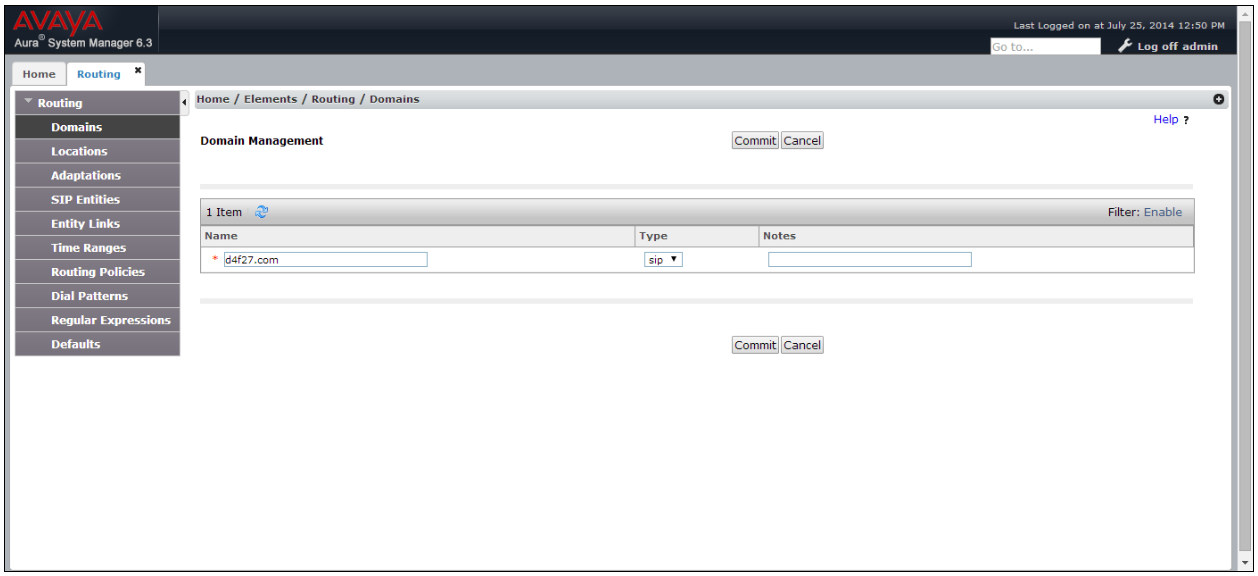
Configuration is accomplished by accessing the browser-based GUI of System Manager using the URL "https://<*ip-address*>/SMGR", where <*ip-address*> is the IP address of System Manager. Log in with the appropriate credentials.

6.1. Specify SIP Domain

Add the SIP domain for which the communications infrastructure will be authoritative. Do this by selecting **Domains** on the left and clicking the **New** button (not shown) on the right. The following screen will then be shown. Provide the following:

- Name: The authoritative domain name (e.g., d4f27.com).
- Type: Select SIP
- Notes: Descriptive text (optional).

Click **Commit**.



6.2. Add Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management. To add a location, select **Locations** on the left and click on the **New** button (not shown) on the right. The following screen will then be shown. Provide the following:

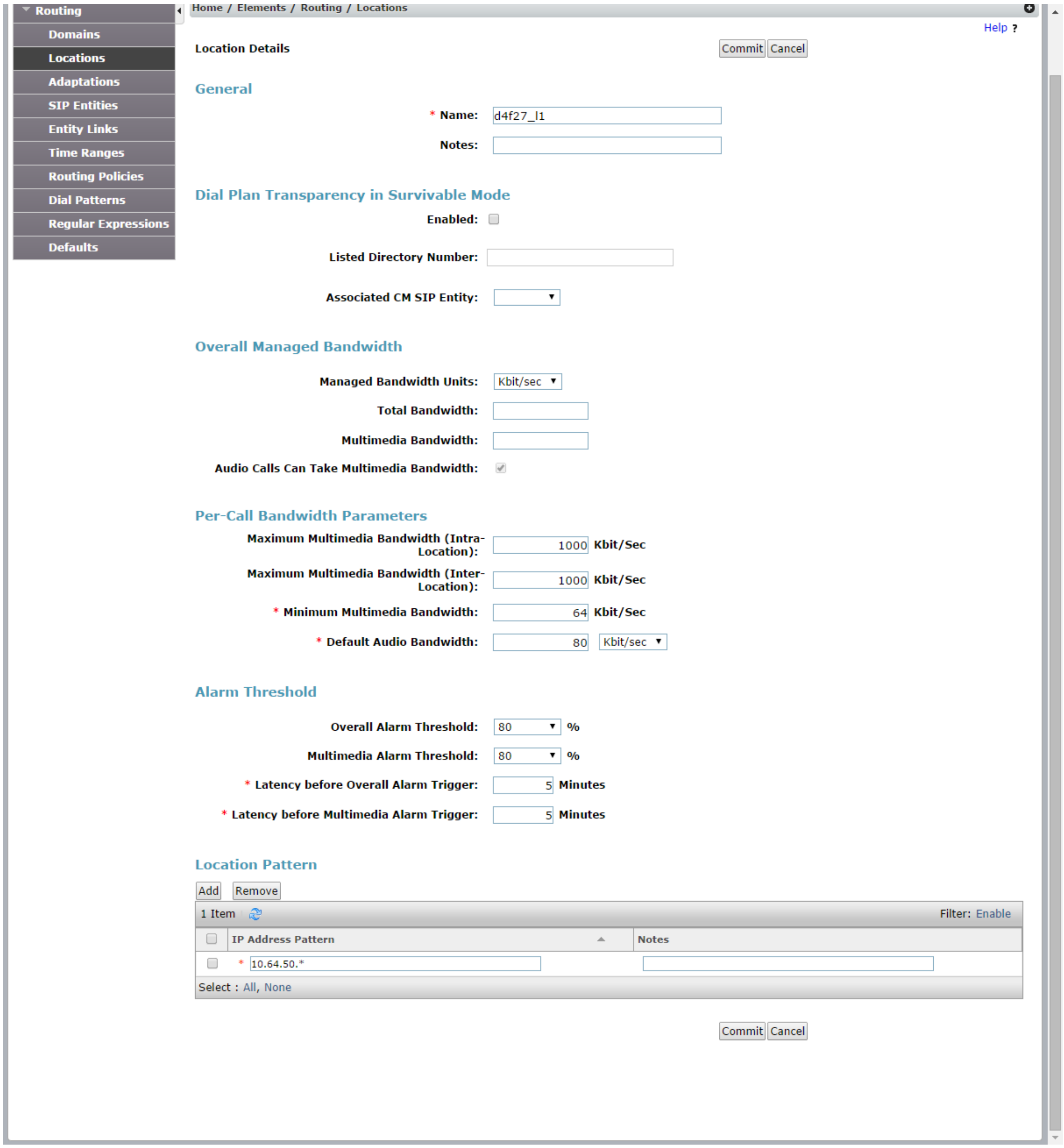
Under *General*:

- Name: A descriptive name.
- Notes: Descriptive text (optional).

Under Location Pattern:

- IP Address Pattern: A pattern used to logically identify the location.
- Notes: Descriptive text (optional).

The location configured below is where Communication Manager and Session Manager reside. Click **Commit** to save the Location definition.


Routing
Domains
Locations
Adaptations
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns
Regular Expressions
Defaults
Home / Elements / Routing / Locations
Help ?
Location Details
Commit Cancel
General
* Name: d4f27_l1
Notes:
Dial Plan Transparency in Survivable Mode
Enabled:
Listed Directory Number:
Associated CM SIP Entity:
Overall Managed Bandwidth
Managed Bandwidth Units: Kbit/sec
Total Bandwidth:
Multimedia Bandwidth:
Audio Calls Can Take Multimedia Bandwidth:
Per-Call Bandwidth Parameters
Maximum Multimedia Bandwidth (Intra-Location): 1000 Kbit/Sec
Maximum Multimedia Bandwidth (Inter-Location): 1000 Kbit/Sec
* Minimum Multimedia Bandwidth: 64 Kbit/Sec
* Default Audio Bandwidth: 80 Kbit/sec
Alarm Threshold
Overall Alarm Threshold: 80 %
Multimedia Alarm Threshold: 80 %
* Latency before Overall Alarm Trigger: 5 Minutes
* Latency before Multimedia Alarm Trigger: 5 Minutes
Location Pattern
Add Remove
1 Item
Filter: Enable
IP Address Pattern
Notes
* 10.64.50.*
Select : All, None
Commit Cancel

6.3. Add SIP Entities

In the sample configuration, a SIP Entity is added for Session Manager, and Communication Manager.

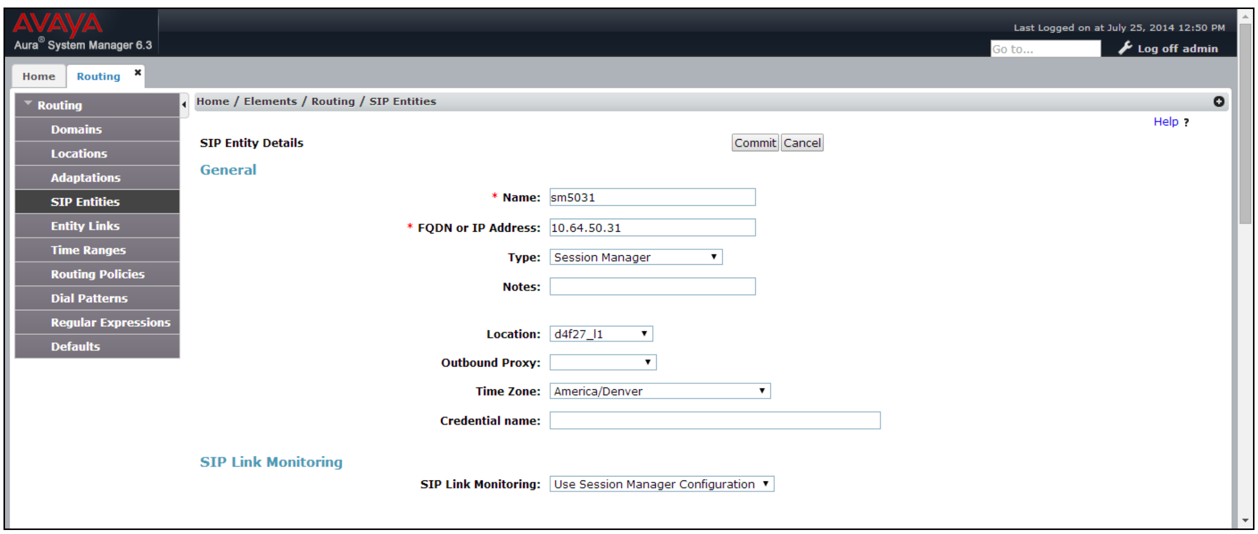
6.3.1. Avaya Aura® Session Manager

A SIP Entity must be added for Session Manager. To add a SIP Entity, select **SIP Entities** on the left and click on the **New** button (not shown) on the right. The following screen is displayed. Provide the following:

Under *General*:

- Name: A descriptive name.
- FQDN or IP Address: IP address of the signaling interface on Session Manager.
- Type: Select Session Manager.
- Location: Select one of the locations defined previously.
- Time Zone: Time zone for this location.

Defaults may be used for the remaining fields. Click **Commit** to save each SIP Entity definition.



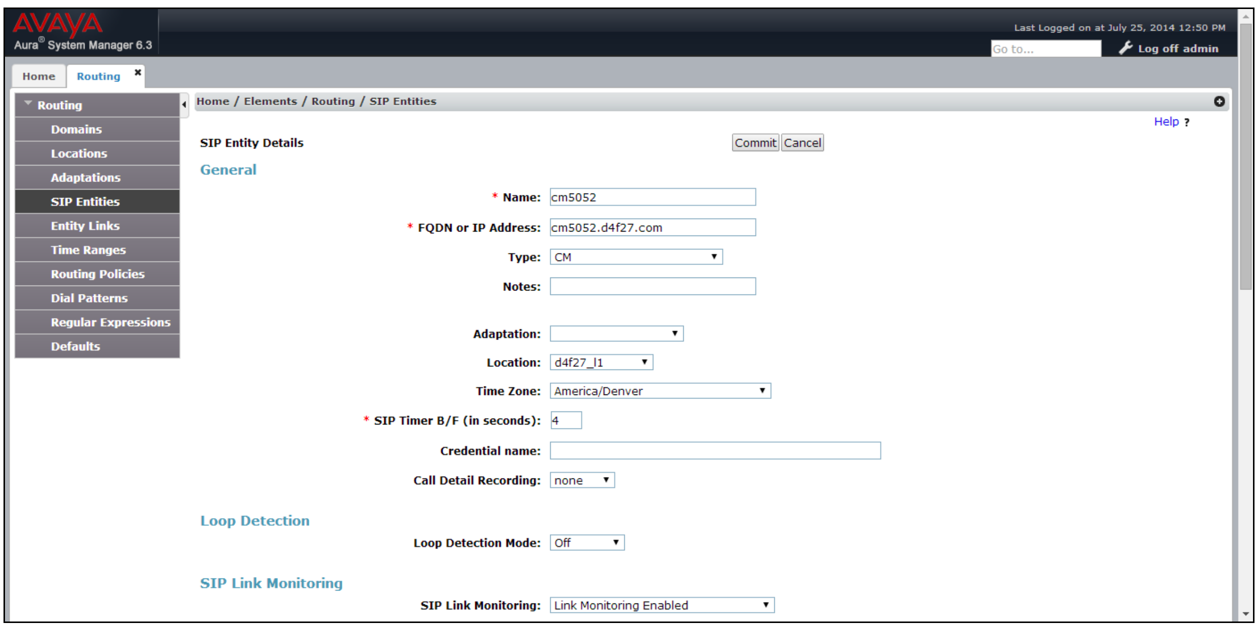
6.3.2. Avaya Aura® Communication Manager

A SIP Entity must be added for Communication Manager. To add a SIP Entity, select **SIP Entities** on the left and click on the **New** button (not shown) on the right. The following screen is displayed. Provide the following:

Under *General*:

- Name: A descriptive name.
- FQDN or IP Address: FQDN or IP address of the signaling interface (e.g.,Procr)
- in the G450 telephony system.
- Type: Select CM.
- Location: Select one of the locations defined previously.
- Time Zone: Time zone for this location.

Defaults may be used for the remaining fields. Click **Commit** to save each SIP Entity definition.

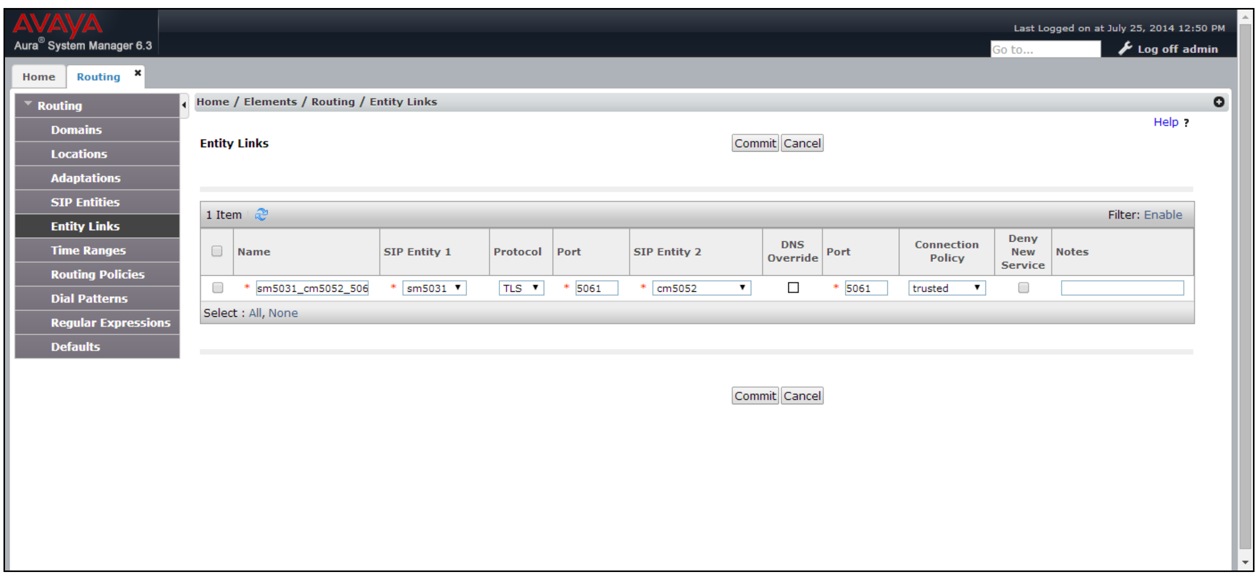


6.4. Add Entity Links

The SIP trunk from Session Manager to Communication Manager are described by Entity Links. To add an Entity Link, select **Entity Links** on the left and click on the **New** button (not shown) on the right. Fill in the following fields in the new row that is displayed:

- Name: A descriptive name.
- SIP Entity 1: Select the Session Manager.
- Protocol: Select TLS as the transport protocol.
- Port: Port number to which the other system sends SIP
- Requests (e.g., 5061 for TLS).
- SIP Entity 2: Select the Communication Manager.
- Port: Port number to which the other system sends SIP
- Requests (e.g., 5061 for TLS).
- Connection Policy: Select Trusted.

The following screens display the configuration of the entity link is for the connection between Session Manager and Communication Manager.



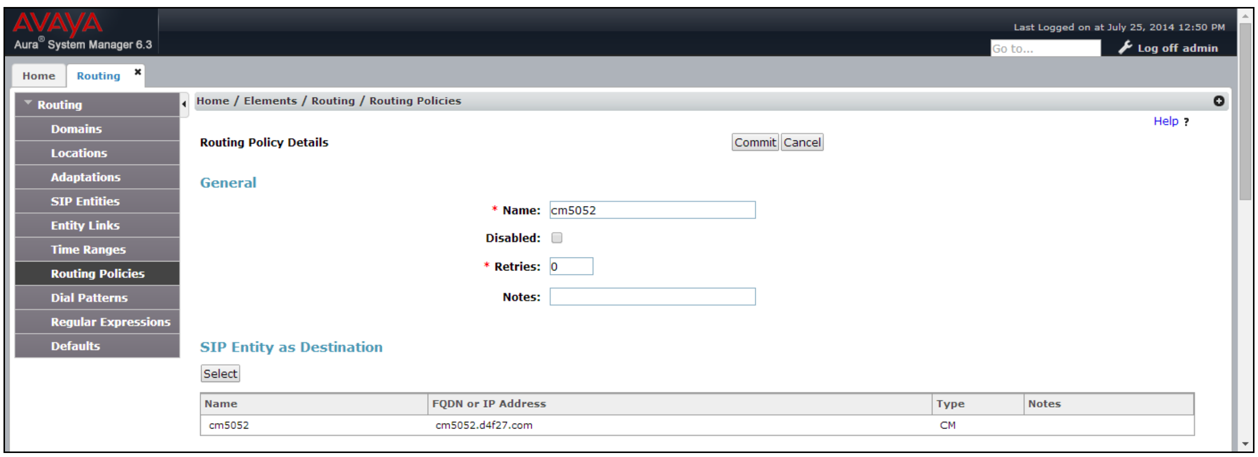
6.5. Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.3**. One routing policy was added for Communication Manager. To add a routing policy, select **Routing Policies** on the left and click on the **New** button (not shown) on the right. The following screen is displayed. Fill in the following:

Under *General*:
Enter a descriptive name in **Name**.

Under *SIP Entity as Destination*:
Click **Select**, and then select the appropriate SIP entity to which this routing policy applies.

Defaults can be used for the remaining fields. Click **Commit** to save each Routing Policy definition. The following screen shows the Routing Policy for Communication Manager.



6.6. Add Dial Patterns

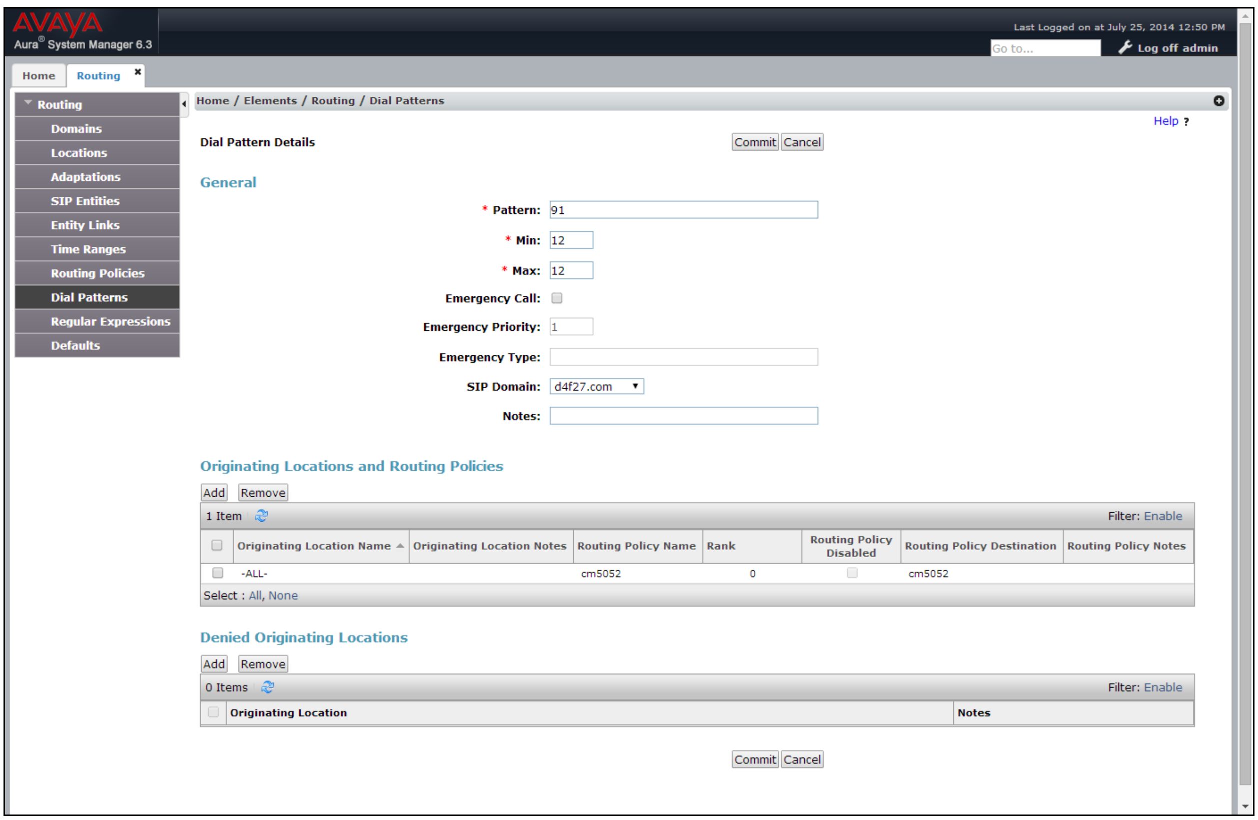
Dial patterns must be defined that will direct calls to the appropriate SIP Entity. In the sample configuration, 12-digit numbers beginning with "91" will be routed to Communication Manager. To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button (not shown) on the right. Provide the following:

Under *General*:

- Pattern: Dialed number or prefix.
- Min Minimum length of dialed number.
- Max Maximum length of dialed number.
- SIP Domain SIP domain of dial pattern.
- Notes Comment on purpose of dial pattern.

Under *Originating Locations and Routing Policies*:
Click **Add**, and then select the appropriate location and routing policy from the list.

Default values can be used for the remaining fields. Click **Commit** to save this dial pattern.



7. Configure Spectralink Wireless Server

This section focuses only on the configuration of the Spectralink Wireless Server solution. The values configured in this section were used during the compliance tests. The procedures include the following areas:

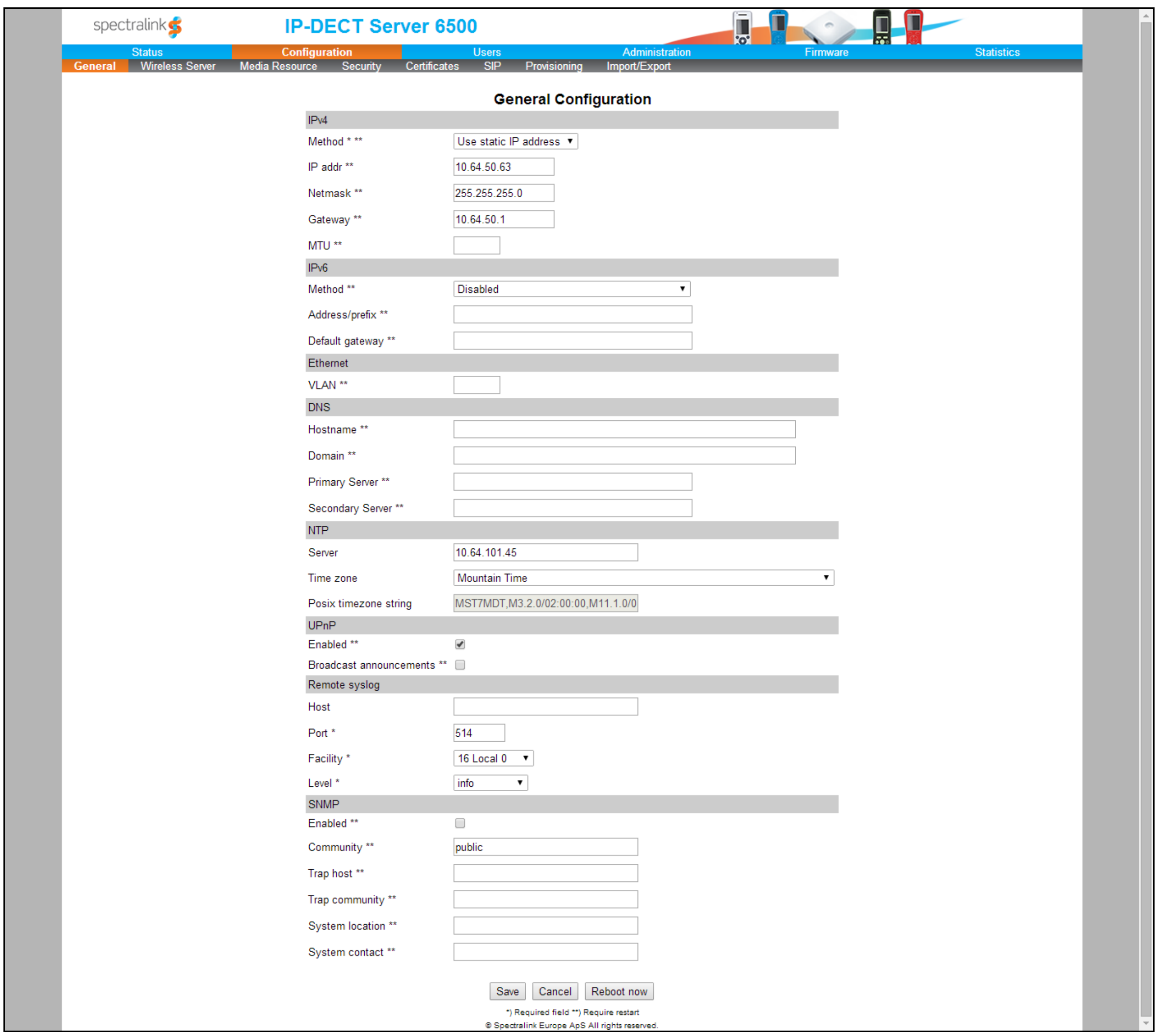
- Administer Spectralink Wireless Server IP address
- Administer DECT handset subscription
- Enable Call Forward feature code
- Administer SIP configuration
- Administer DECT users
- Administer Spectralink Base Station IP address
- Administer Wireless Sever host

7.1. Administer Spectralink Wireless Server IP address

The default IP address of a Spectralink Wireless Server is 192.168.0.1. Connect a PC directly to the Spectralink Wireless Server 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:

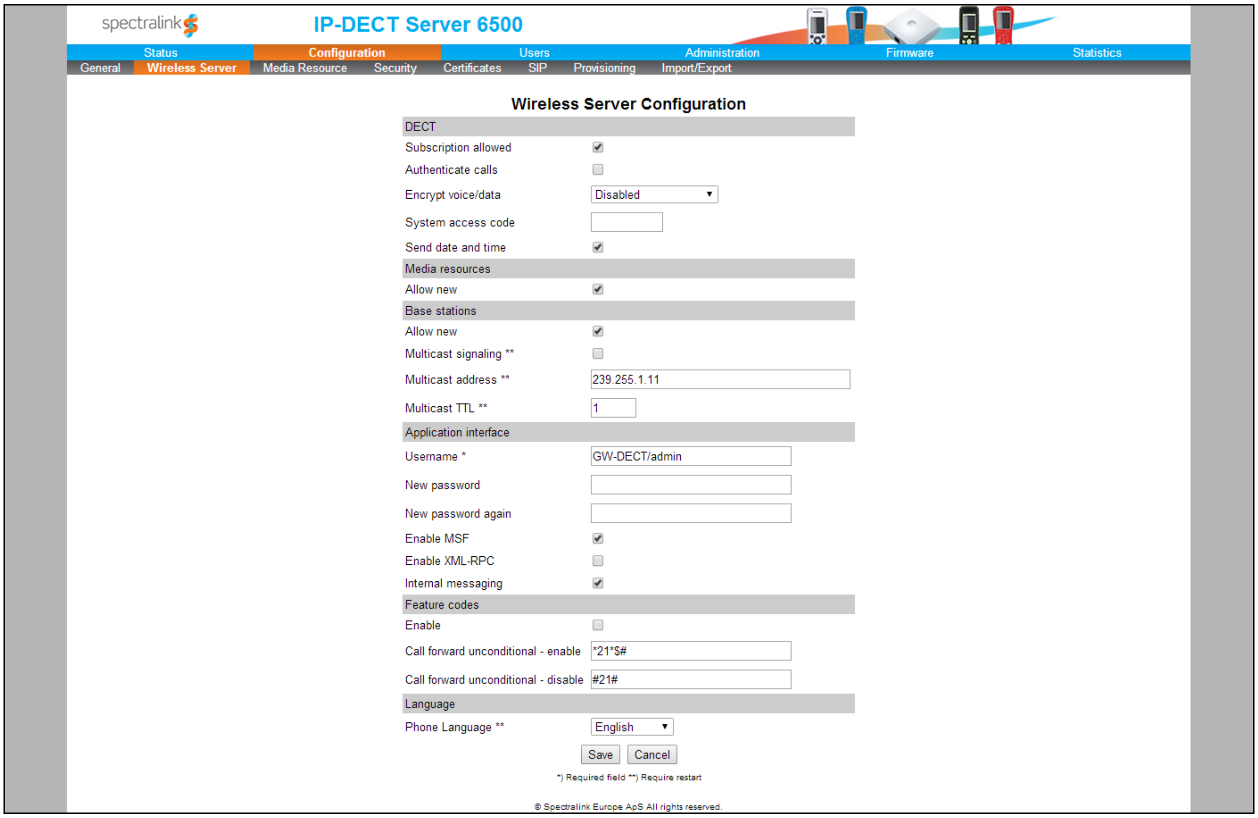
- Method — Select "Use Static IP address"
- IP addr — Enter IP address
- Netmask — Enter subnet mask address
- Gateway — Enter default gateway address
- DNS primary Server — Enter DNS IP address (Optional)
- NTP Server — Enter NTP Server IP Address (Optional)
- Time Zone — Select Time Zone (Optional)

Click **Save** to save changes.



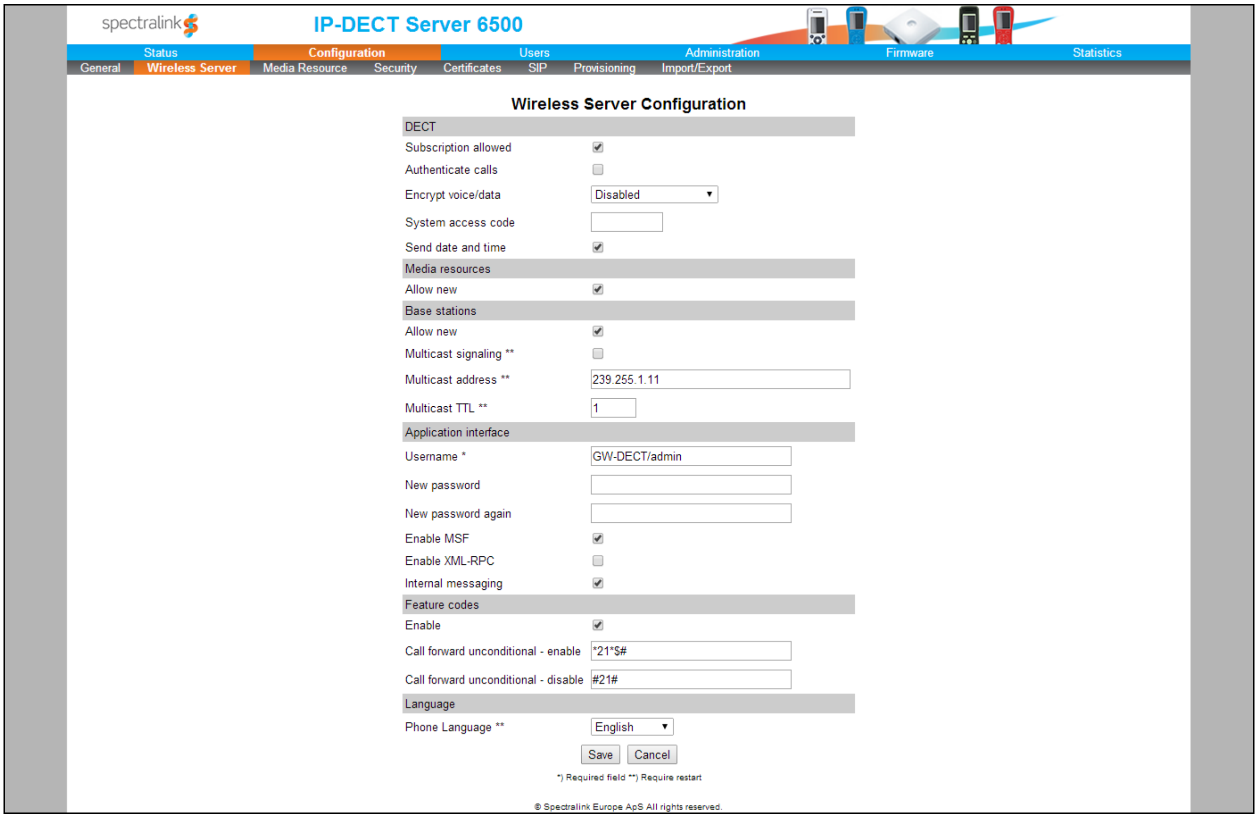
7.2. Administer DECT handset subscription

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



7.3. Enable Call Forward Feature Code

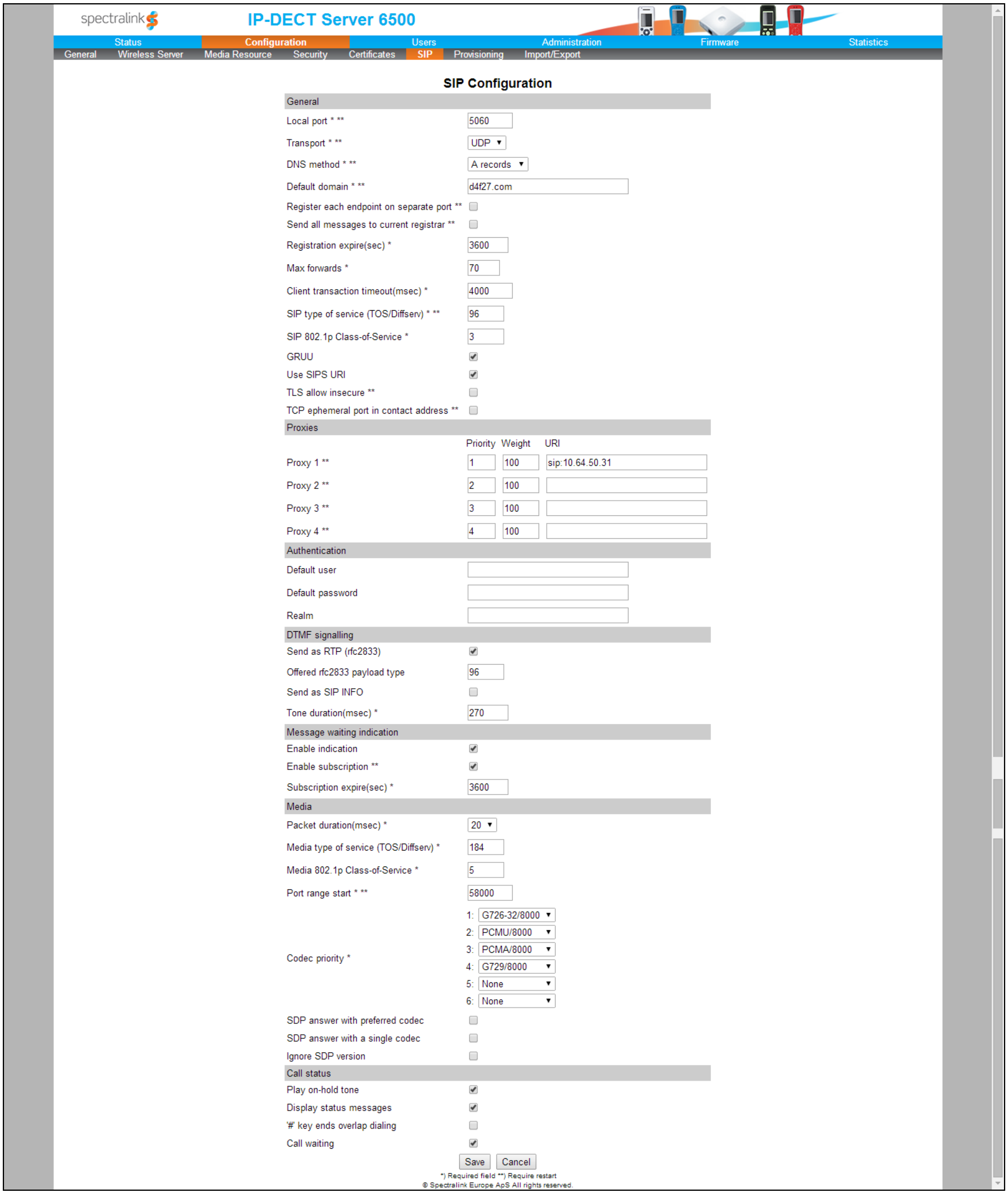
From the menu, click on **Configuration → Wireless Server**. Under the **Feature Codes** section, check the box next to **Enable.**
Click **Save** to save changes.



7.4. Administer SIP Configuration

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

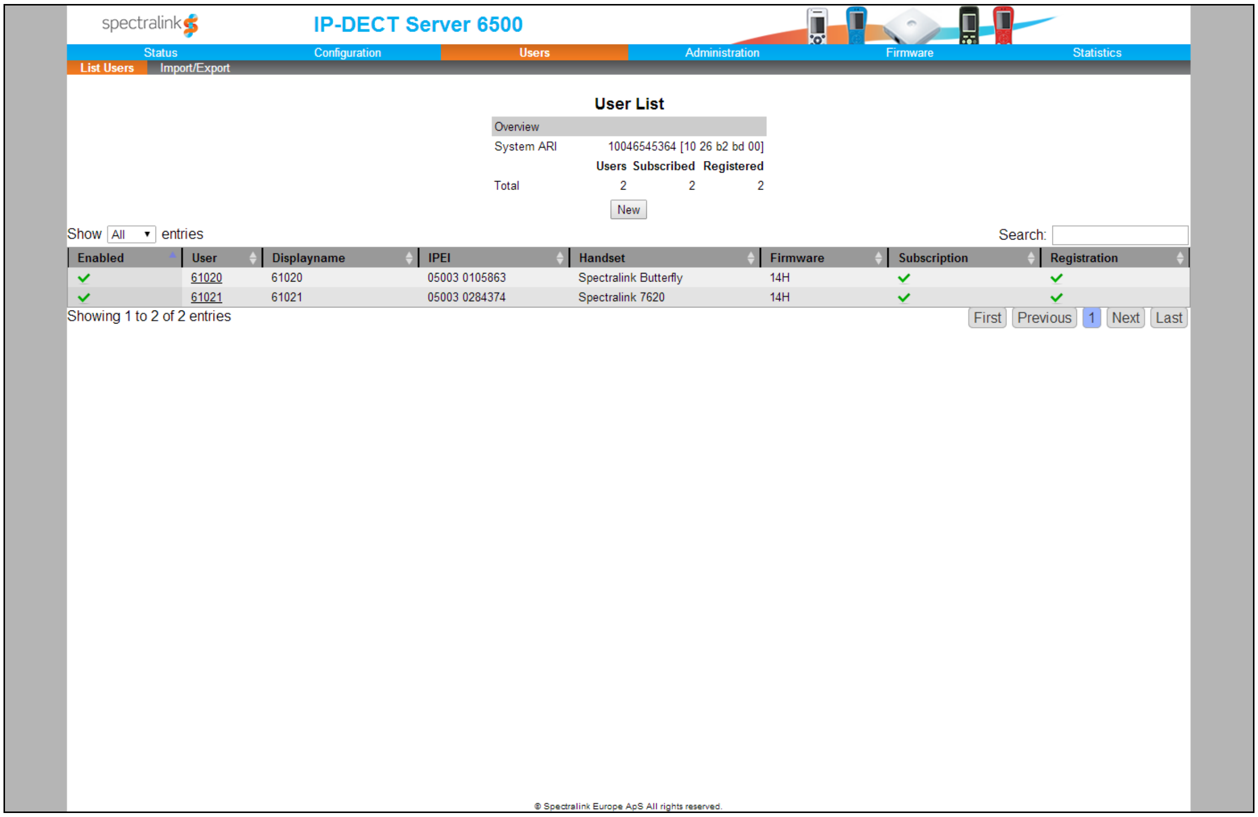
- General Section:
  - Local Port: **5060**
  - Transport: **UDP**
  - Default Domain: Enter domain name (e.g. **d4f27.com**)
- Proxies Section:
  - Proxy 1: **Enter sip:<IP Address of Session Manager> for the sip URI.**
- Message waiting indication Section:
  - Enable indication: Check the checkbox
  - Enable subscription: Check the checkbox
- Under Media Section, Select preferred codecs and priority



- Click on **Save** to save changes.

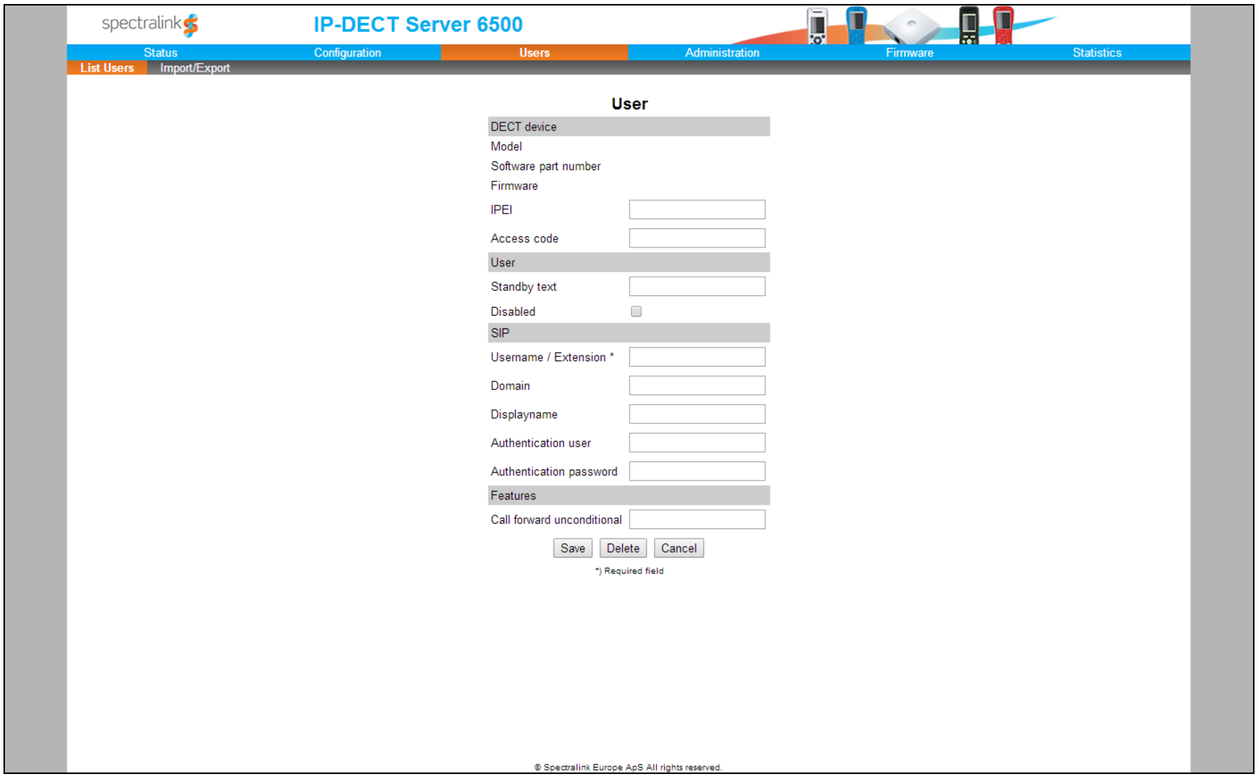
7.5. Administer DECT users

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 used to register with Session Manager
- Domain Enter the SIP domain name used in **Section 6.1**
- Displayname Enter a desired display name (Optional)
- Authentication User Enter the user defined for Session Manager
- Authentication Password Enter password for user.



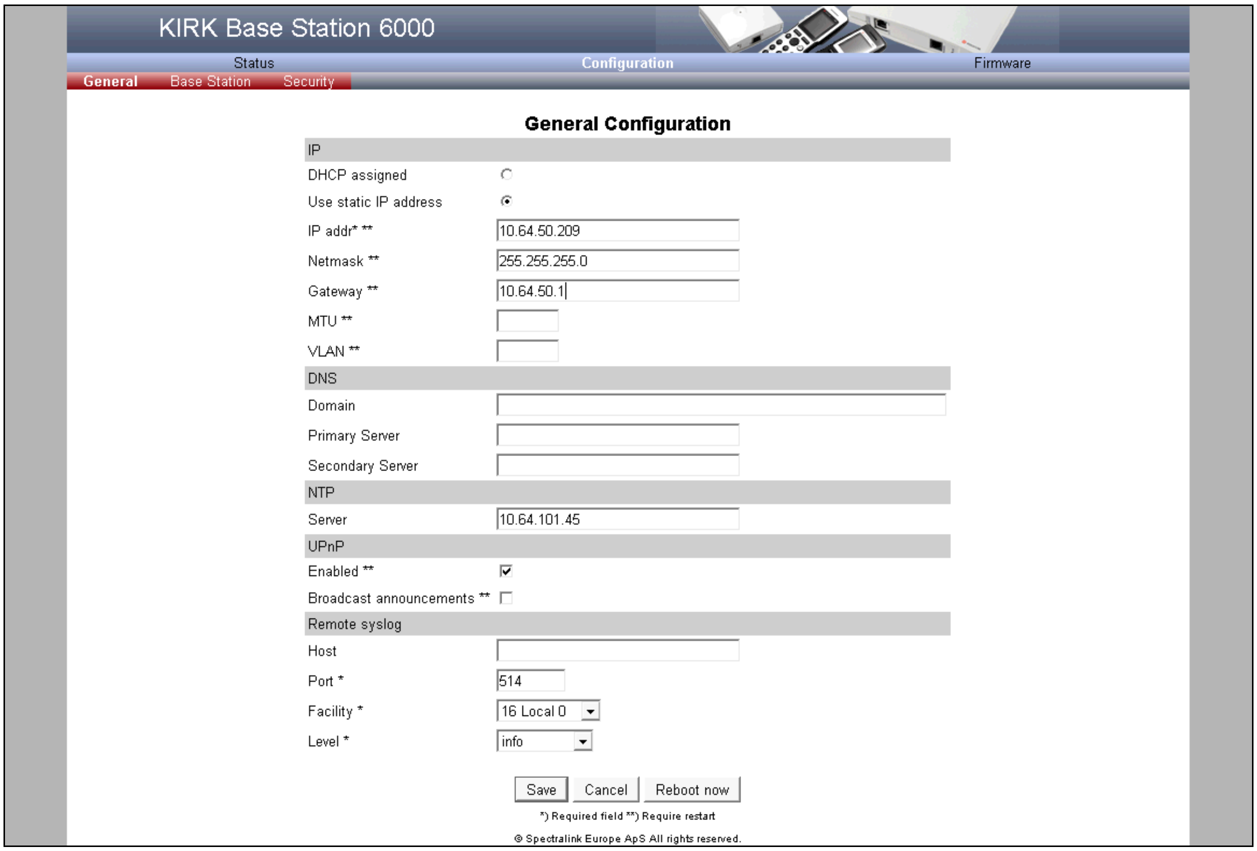
Click on **Save** to save changes.

7.6. Administer Spectralink Base Station IP address

The default IP address of a Spectralink 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:

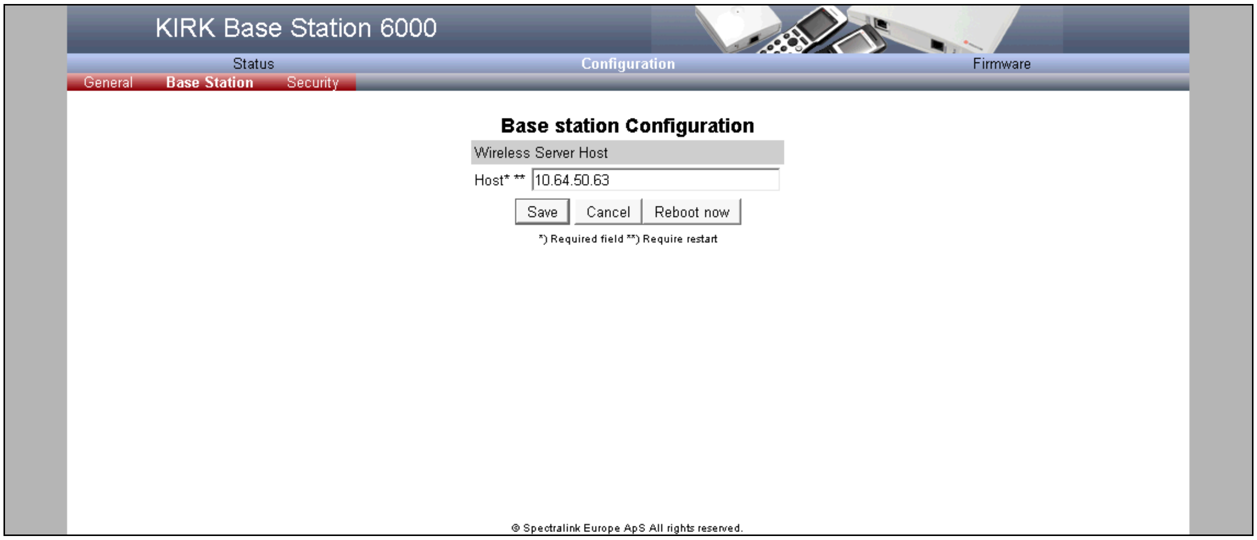
- Use Static IP address	Click the button to select
- IP addr	Enter IP address
- Netmask	Enter subnet mask
- Gateway	Enter default gateway IP address
- NTP Server	Enter NTP Server IP Address (Optional)

Click **Save** to save changes.



7.7. Administer Wireless Sever host

From the menu, go to **Configuration → Base Station** and for **Host** enter the ip address of the Spectralink Wireless Server 6500 configured in **Section 6.1**.
Click **Save** to save changes.



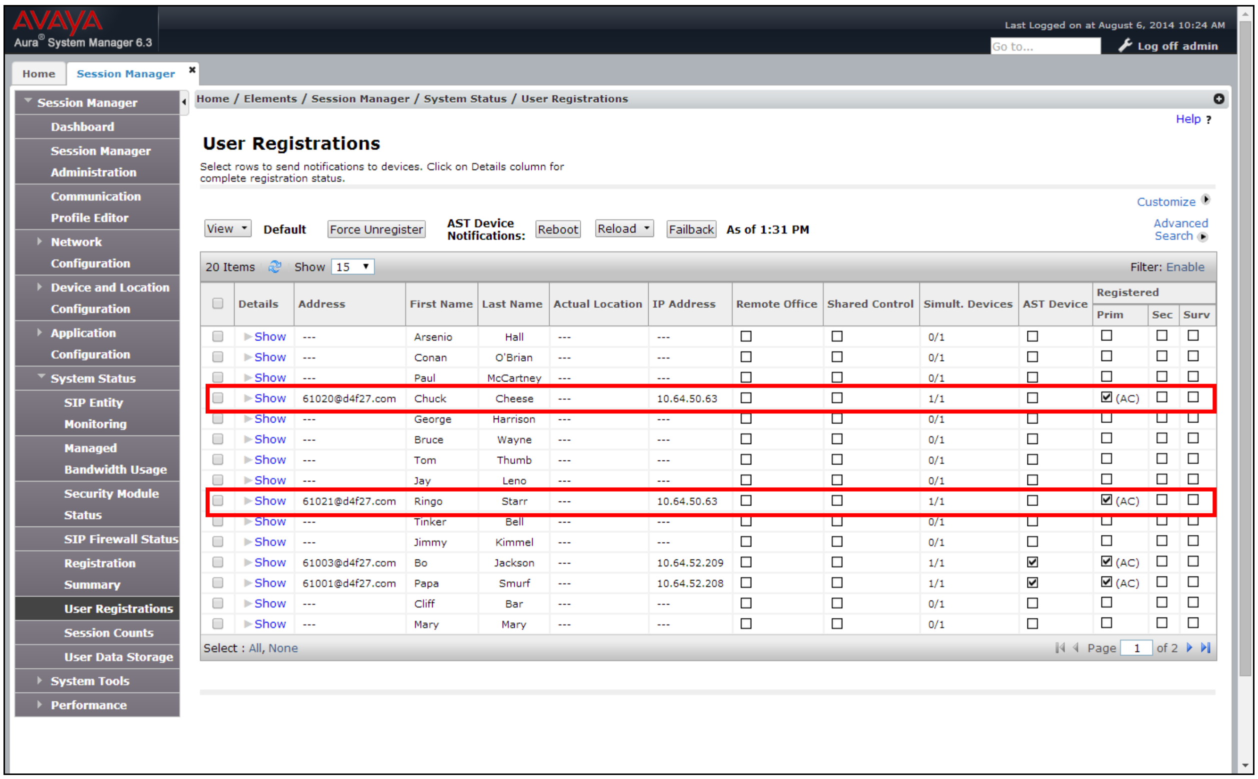
8. Verification Steps

The following steps may be used to verify the configuration:

8.1. Verify Registered spectralink Endpoints on Avaya Aura® Session Manager

From the System Manager GUI select **Elements → Session Manager →** (Not Shown). From the left pane select **System Status → User Registrations.** Find and verify that the spectralink endpoints are registered.

Note: *The spectralink endpoints will use the IP address of the spectralink Wireless Server.*



8.2. Verify Active Call on Avaya Aura® Communication Manager

From the SAT interface use the status trunk command to determine which port(s) are carrying an active call.

```
status trunk 2

                             TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy

0002/001 T00036   in-service/active  no   T00044
0002/002 T00037   in-service/idle    no
0002/003 T00038   in-service/idle    no
0002/004 T00039   in-service/idle    no
0002/005 T00040   in-service/idle    no
0002/006 T00041   in-service/idle    no
0002/007 T00042   in-service/idle    no
0002/008 T00043   in-service/idle    no
0002/009 T00044   in-service/active  no   T00036
0002/010 T00045   in-service/idle    no
```

The screen shot below displays a g711mu call between an Avaya Deskphone with IP address 10.64.52.209 and the spectralink Wireless Server at IP address 10.64.50.63.

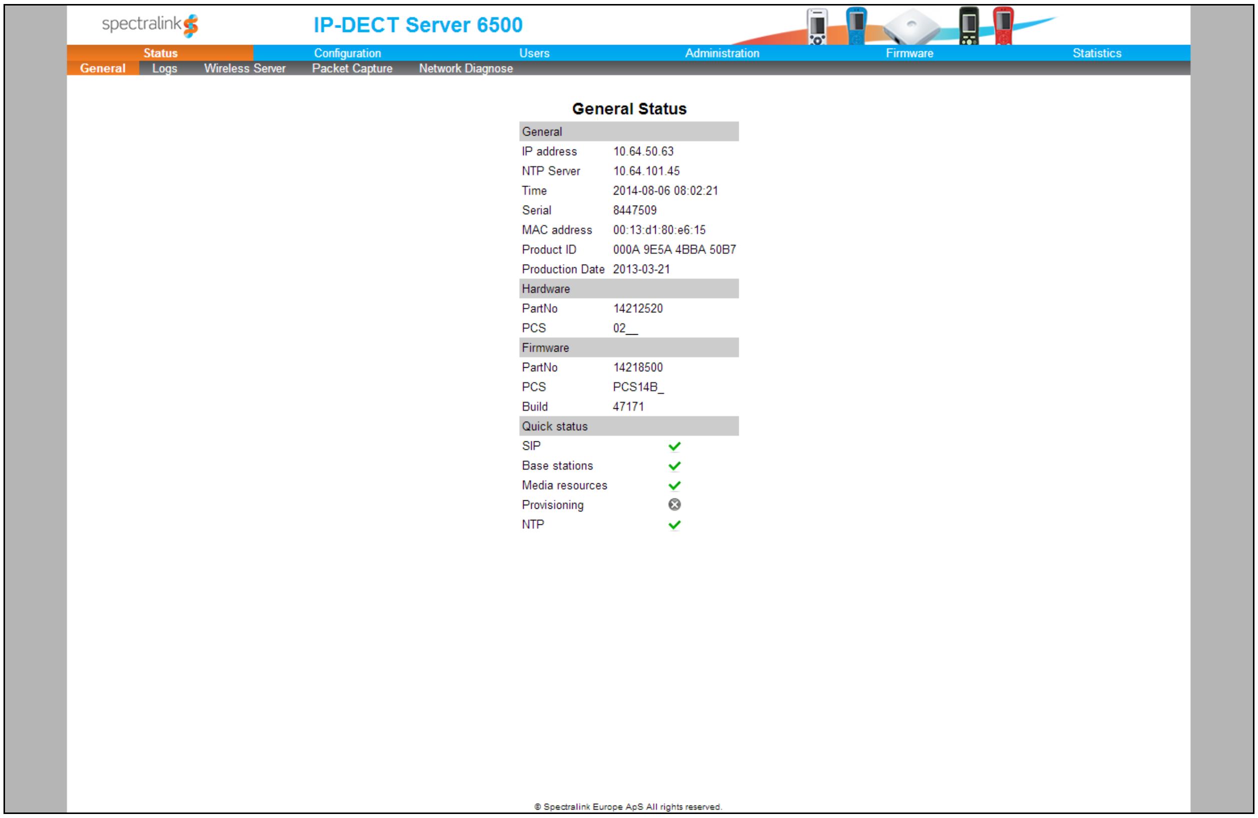
Note: *The specteralink Wireless Server proxies for the DECT phone.*

```
status trunk 2/001                                             Page   3 of   3
                       SRC PORT TO DEST PORT TALKPATH
src port: T00036
T00036:TX:10.64.52.209:5004/g711u/20ms
T00044:RX:10.64.50.63:58364/g711u/20ms















dst port: T00044
```

8.3. Verify Spectralink Wireless Server Status

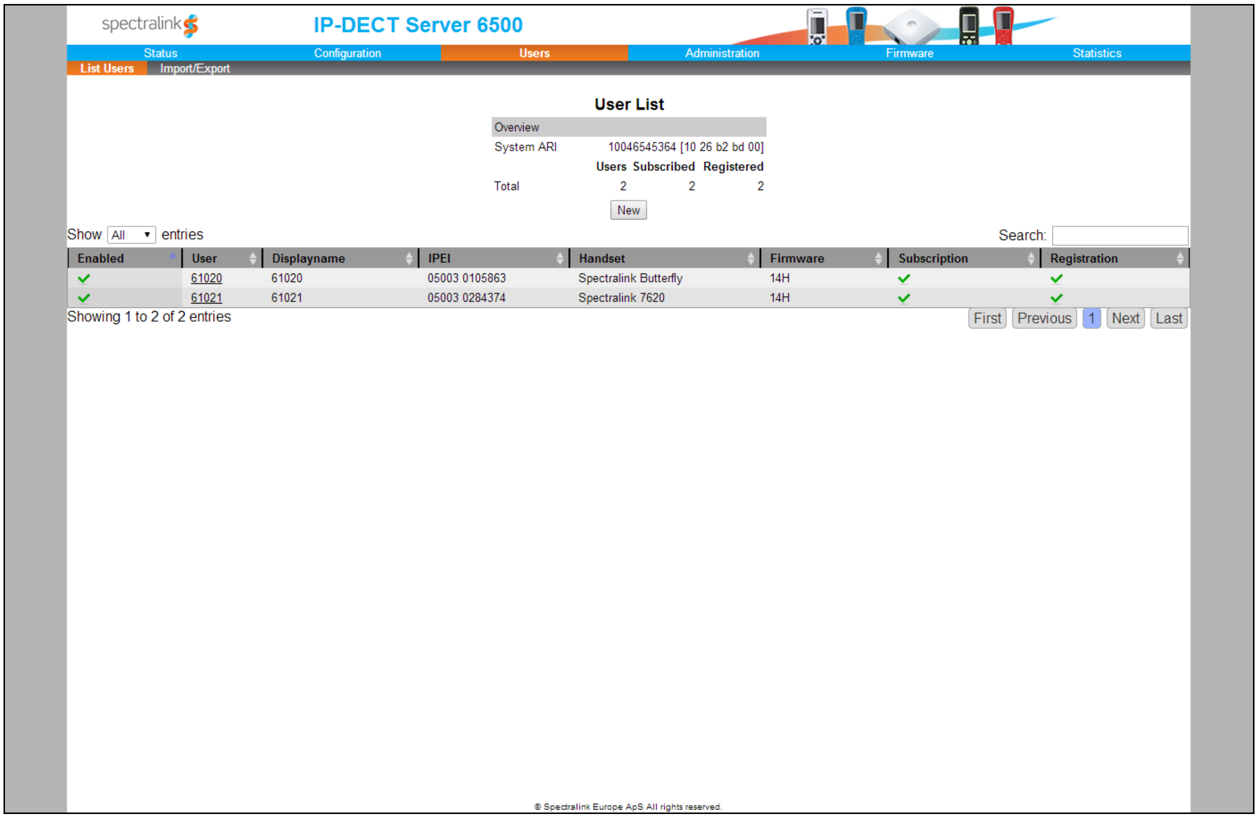
8.3.1. Quick Status

From the menu, go to **Status → General** and verify **Quick Status** green checks indicate proper functionality. Mouse over indicator for a status explanation.



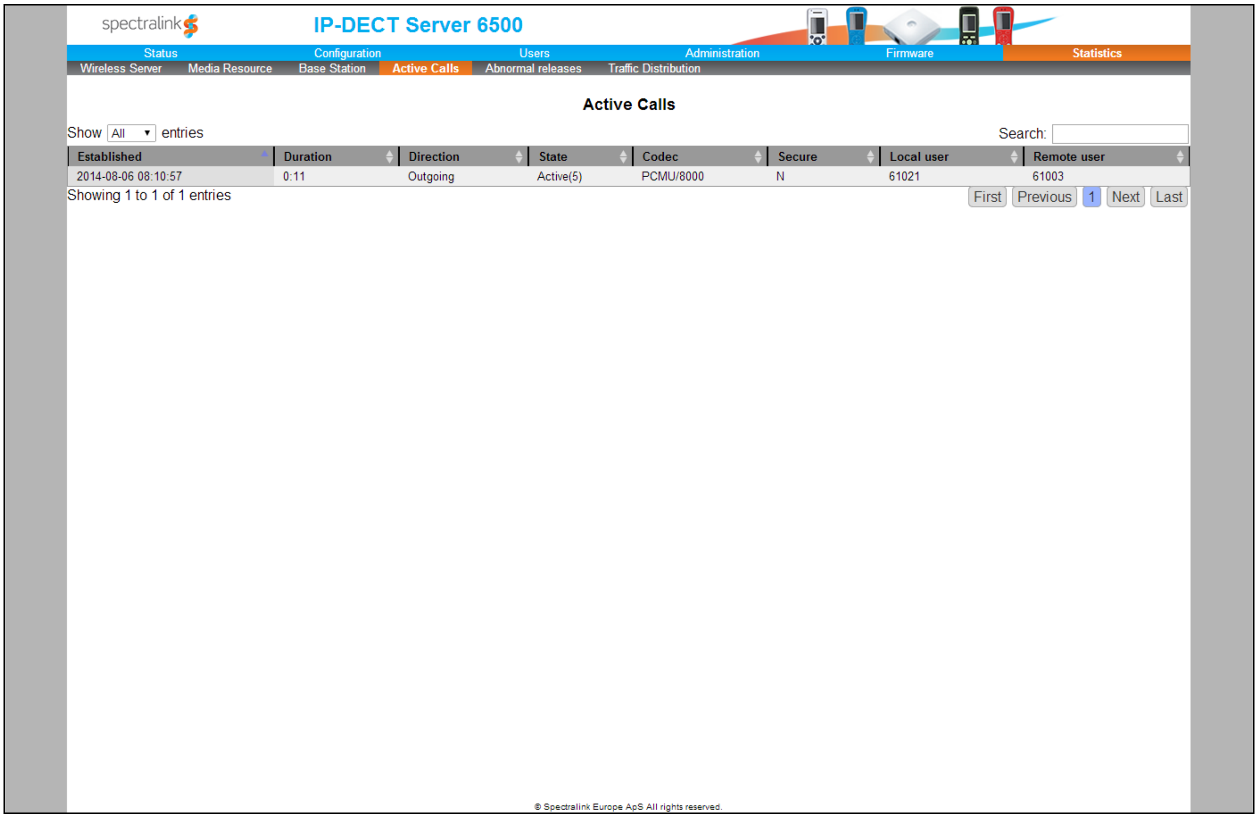
8.3.2. List Users

From the menu, go to **Users → List Users** and verify that each user has subscribed and registered successfully.



8.3.3. Active Call

From the menu, go to **Statistics** → **Active Calls** to display active call details.



9. Conclusion

These Application Notes describe the configuration steps required for the Spectralink Wireless Server 6500/400 solution to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. All feature functionality and serviceability test cases were completed successfully.

10. Additional References

The documents referenced below were used for additional support and configuration information.

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

[1] *Administering Avaya Aura® Session Manager*, Release 6.3 Issue 5 June 2014

[2] *Avaya Aura® Communication ManagerFeature Description and Implementation*, Release 6.3 Issue 12 June 2014

Product documentation for Spectralink Wireless Solution may be found at:
http://www.spectralink.com/product-information/dect

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.