Avaya Solution & Interoperability Test Lab

Application Notes for configuring the Allworx 6x System with Allworx IP phones to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager via a SIP Trunk – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Allworx 6x with Allworx IP phones to interoperate with Aura® Session Manager and Avaya Aura® Communication Manager via a SIP trunk. The Allworx 6x system is an all-in-one communication system integrating a feature-rich phone system, advanced IP phones, and powerful software features.

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 configuration steps required for the Allworx 6x system with Allworx IP phones to interoperate with Aura® Session Manager and Avaya Aura® Communication Manager via a SIP trunk.

Designed for companies with up to 60 users, the Allworx 6x system is an all-in-one communication system integrating a feature-rich phone system, advanced IP phones, and powerful software features. Key features of the 6x system include:

- Supports VoIP and traditional phone lines
- PBX and/or Key system features
- Built-in nine (9) auto attendants
- Unified messaging
- Unlimited call routes
- Presence management
- One (1) eight (8) seat conference bridge
- Advanced software features support

2. General Test Approach and Test Results

The compliance testing focused on verifying the ability of the Allworx 6x system with Allworx IP phones to interoperate with an Avaya SIP-enabled IP Telephony Environment comprised of Avaya Aura® Session Manager, Avaya Aura® Communication Manager, and Avaya phones (both SIP and H.323).

2.1. Interoperability Compliance Testing

The interoperability compliance test plan included feature and serviceability test cases. The feature testing focused on the following areas:

- Basic calls [verifying proper set up and tear down of the calls, the phones display information (i.e. Caller ID), and the voice paths/quality]
- Audio codec negotiation using G.711 and G.729 codecs
- Direct IP-IP Audio Connections (media shuffling)
- DTMF transmission using RFC 2833
- Voicemail with message waiting indicators (MWI)
- Telephony features such as hold/resume, call coverage, transfers, and conferences.

Serviceability testing focused on verifying the ability of Allworx 6x system and Allworx IP phones to recover from adverse conditions such as network and server (i.e. Allworx 6x, Session Manager, and Communication Manager) outages.

2.2. Test Results

All test cases were executed and passed with the following exceptions/observations noted:

- If an Allworx phone dials an enterprise Avaya phone, and the call is then forwarded back an Allworx phone, the call is established; however, there is no audio on the call.
- The Allworx phones do not update display information for various call scenarios (e.g. call forwarding, transfers, and conferences). Instead of updating the display information to indicate the Allworx phone is now in a conference or connected to a new party (e.g. after the call has been forwarded or transferred), the Allworx phone continues to display the original connected party information.
- Bridging between Allworx phones and Avaya phones is not currently supported.
- For calls from Allworx phones to enterprise Avaya phones, leading digits (e.g. *8) had to be dialed first to indicate that the call would be an enterprise call and should be routed to Session Manager.
- When an Allworx phone receives a call from an enterprise Avaya phone, the Allworx 6x system adds an "outside line" prefix (e.g. 9) to the Avaya phone's extension. For example, if Avaya phone extension 53005 calls an Allworx phone, 953005 will appear on the Allworx phone's display and in the phone's call history log file. The Allworx 6x system does not designate calls it receives from Session Manager as internal enterprise calls. Therefore, if the extension of the caller does not match the Allworx 6x system's own dial plan for the Allworx phones, it assumes the call is from outside the enterprise. As a result, it adds a 9 with the logic that the Allworx phone would have to dial a leading 9 in order to call the caller back. However, using the example above, dialing 953005 from an Allworx phone would not be routed to the Avaya phone. Rather *853005 would need to be dialed, as described in the previous bullet.

2.3. Support

Technical support on the Allworx 6x system and Allworx IP phones can be obtained through the following:

- **Phone:** 1-866-ALLWORX, option 1, option 3
- **Web:** http://www.allworx.com/support/support_overview.aspx
- **Email:** support@allworx.com

3. Reference Configuration

As shown in **Figure 1**, a simulated enterprise site was configured consisting of the following:

- Avaya Aura® Session Manager (configured using Avaya Aura ® System Manager)
- Avaya Aura® Communication Manager with an Avaya G450 Media Gateway
- Avaya SIP and non-SIP phones (extensions 5xxxx)
- Allworx 6x system
- Allworx IP Phones (extensions 7xxx)

The Allworx 6x system's WAN interface was used to establish a SIP trunk to Session Manager. The Allworx 6x system's LAN interface was used to establish network connectivity to the Allworx IP Phones. Note, the Allworx IP Phones registered with the Allworx 6x system, not with Session Manager or Communication Manager.

The enterprise also had connectivity to the PSTN via Communication Manager.

The administration routing and basic connectivity between Communication Manager and Session Manager are not the focus of these Application Notes; however, some details are provided only for reference and completeness.

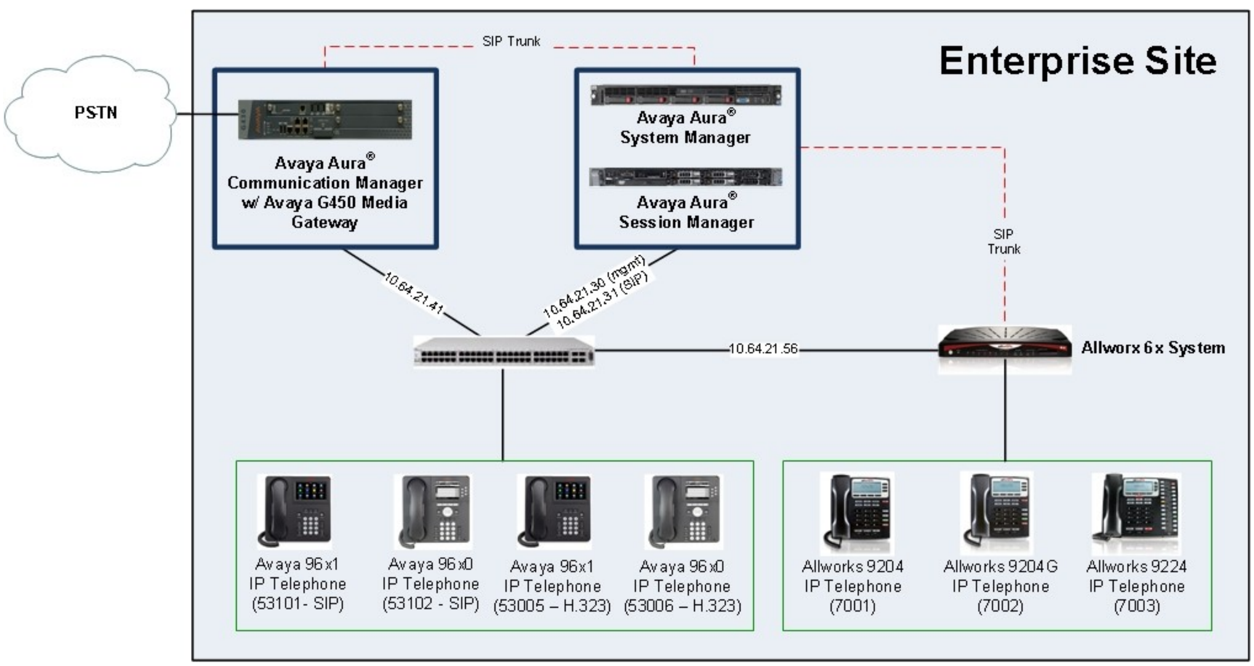


Figure 1: Allworx 6x system with Allworx IP Phones, Session Manager, and Avaya Communication Manager

4. Equipment and Software Validated

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

Equipment	Software
Avaya S8300D Server with an Avaya G450 Media Gateway	Avaya Aura® Communication Manager 6.0.1, R016x.00.1.510.1, Update 19303 (Avaya Aura® System Platform: 6.0.3.4.3)
Dell™ PowerEdge™ R610 Server	Avaya Aura® System Manager: 6.1.0 (Build No. – 6.1.0.0.7345-6.1.5.502), Software Update Revision No : 6.1.9.1.1634 (Avaya Aura® System Platform: 6.0.3.4.3)
HP ProLiant DL360 G7 Server	Avaya Aura® Session Manager 6.1.5.0.615006
Avaya 9600 Series IP Telephones (96x0) • H.323 • SIP	 3.1 Service Pack 2 2.6 Service Pack 5
Avaya 9600 Series IP Telephones (96x1) • H.323 • SIP	 6.0 Service Pack 5 6.0 Service Pack 1
Allworx 6x	7.3.7.2
Allworx IP Phones • 9204 • 9204G • 9224	2.3.2.9

5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager. The procedures include the following areas:

- Verify Communication Manager License
- Administer IP Codec Set
- Administer IP Network Region
- Administer IP Node Names
- Administer SIP Signaling Group
- Administer SIP Trunk Group
- Administer Route Pattern
- Administer Private Numbering
- Administer AAR Analysis

5.1. Verify Avaya Aura® Communication Manager License

Log in to the System Access Terminal (SAT) to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the "display system-parameters customer-options" command. Navigate to **Page 2**, and verify that there is sufficient remaining capacity for SIP trunks by comparing the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column. The license file installed on the system controls the maximum permitted. If there is insufficient capacity, contact an authorized Avaya sales representative to make the appropriate changes.

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

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 12000 32
           Maximum Concurrently Registered IP Stations: 18000 12
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 414   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 18000 0
                   Maximum Video Capable IP Softphones: 18000 1
                       Maximum Administered SIP Trunks: 24000 170
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                             Maximum TN2501 VAL Boards: 128   0
                     Maximum Media Gateway VAL Sources: 250   1
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 300   0

        (NOTE: You must logoff & login to effect the permission changes.)
```

5.2. Administer IP Codec Set

Use the “change ip-codec-set x” command, where “x” is an existing codec set number that will be used for integration with the Allworx 6x system and Allworx IP Phones. Enter the audio codec types ***G.711MU*** and ***G.729A*** in the **Audio Codec** fields. Refer to the Allworx documentation for details on how to configure matching codecs with the Allworx equipment.

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


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

5.3. Administer IP Network Region

Use the "change ip-network-region x" command, where "x" is an existing network region that will be used for integration with the Allworx 6x system and Allworx IP Phones. Enter an **Authoritative Domain** (e.g. ***avaya.com***). For the **Codec Set** field, enter the codec set number from **Section 5.2**. Set **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** to ***yes***.

```
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      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
            Keep-Alive Count: 5
```

5.4. Administer IP Node Names

Use the "change node-names ip" command, and add an entry for the Session Manager signaling interface. In this case, ***SM_21_31*** and ***10.64.21.31*** are entered as **Name** and **IP Address**. Note the ***procr*** / **10.64.21.41** entries, which are the node name / IP address for the processor board. It will be used later to configure the SIP trunk to Session Manager.

```
change node-names ip                                                Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
AES_21_46           10.64.21.46
CM_20_40            10.64.20.40
CM_22_12_CLAN1A     10.64.22.16
CM_22_12_CLAN2A     10.64.22.19
IPO_21_64           10.64.21.64
SM_20_31            10.64.20.31
SM_21_31            10.64.21.31
default             0.0.0.0
msgserver           10.64.21.41
procr               10.64.21.41
procr6              ::
```

5.5. Administer SIP Signaling Group

Administer a SIP signaling group for a new trunk that will be created for the connection between Communication Manager and Session Manager. Use the "add signaling-group x" command, where "x" is an available signaling group number. Enter the following values for the specified fields and the default values may be used for the remaining fields.

- **Group Type:** *sip*
- **IMS Enabled?** *n*
- **Transport Method:** *tls*
- **Peer Detection Enabled?** *y*
- **Peer Server:** *SM* (this field will be automatically populated)
- **Near-end Node Name:** Processor node name from **Section 5.4,** i.e. *procr*
- **Near-end Listen Port:** *5061*
- **Far-end Node Name:** Session Manager node name from **Section 5.4**, i.e. *SM_21_31*
- **Far-end Listen Port:** *5061*
- **Far-end Network Region:** The IP network region number from **Section 5.4**, i.e. *1*
- **DTMF over IP:** *rtp-payload*
- **Direct IP-IP Audio Connections:** *y*

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

 Group Number: 1             Group Type: sip
  IMS Enabled? n       Transport Method: tls
        Q-SIP? n                                            SIP Enabled LSP? n
     IP Video? y          Priority Video? n       Enforce SIPS URI for SRTP? n
  Peer Detection Enabled? y  Peer Server: SM



   Near-end Node Name: procr                  Far-end Node Name: SM_21_31
 Near-end Listen Port: 5061                 Far-end Listen Port: 5061
                                         Far-end Network Region: 1

Far-end Domain:
                                          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? y
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 20
```

5.6. Administer SIP Trunk Group

Administer a SIP trunk group to interface with the Session Manager. Use the "add trunk-group x" command, where "x" is an available trunk group number. Set the **Group Type** to ***sip***, and **Service Type** to ***tie***. Enter a descriptive **Group Name**, and an available trunk access code for the **TAC** field. Set **Member Assignment Method** to ***auto***, **Signaling Group** to the signaling group number from **Section 5.5**, and enter a desired value for number of trunk group members for **Number of Members**.

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

Group Number: 1                  Group Type: sip           CDR Reports: y
  Group Name: to SM_21_31              COR: 1        TN: 1        TAC: 101
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                Night Service:
Queue Length: 0
Service Type: tie                    Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 1
                                                     Number of Members: 50
```

Navigate to **Page 3**, and enter ***unk-pvt*** for the **Numbering Format** field as shown below.

```
change trunk-group 1                                           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. Administer Route Pattern

Create a route pattern to use for the newly created SIP trunk group. Use the "change route-pattern x" command, where "x" is an available route pattern. Enter a descriptive **Pattern Name,** i.e. ***to SM_21_31***. In the **Grp No** field, enter the trunk group number from **Section 5.6**. In the **FRL** field, enter a level that allows access to this trunk.

```
change route-pattern 1                                          Page   1 of   3
                    Pattern Number: 1   Pattern Name: to SM_21_31
                             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: 1    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                              lev0-pvt  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
```

5.8. Administer Private Numbering

Use the "change private-numbering 0" command, to define the calling party number to send to Session Manager. Add an entry for the trunk group defined in **Section 5.6**. In the example shown below, all calls originating from a 5-digit extension beginning with 5 and routed over any trunk group , since the Trk Grp(s) field is blank,will result in a 5-digit calling number. The calling party number will be in the SIP "From" header.

```
change private-numbering 0                                      Page   1 of   2
                           NUMBERING - PRIVATE FORMAT

Ext Ext              Trk        Private           Total
Len Code             Grp(s)     Prefix            Len
 5  2                                             5     Total Administered: 2
 5  5                                             5        Maximum Entries: 540
```

5.9. Administer Automatic Alternate Routing Analysis

This section provides a sample Automatic Alternate Routing (AAR) routing used for routing calls with dialed digits 7xxx to Session Manager. Note that other methods of routing may be used. Use the "change aar analysis "7" command, and add an entry to specify how to route calls to 7xxx. In the example shown below, calls with digits 7xxx will be routed as an AAR call using route pattern "1" from **Section 5.7**. These calls will be routed to Session Manager and then to the Allworx 6x system for delivery to the Allworx IP Phones.

```
change aar analysis 7                                           Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all          Percent Full: 1

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    7                     4    4     1        aar          n
```

6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager as shown in the reference configuration. All provisioning for Session Manager is performed via the System Manager web interface. System Manager delivers a set of shared, secure management services and a common console across multiple products in the Avaya Aura® network, including the central administration of routing policies, and a common format for logs and alarms.

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

The Session Manager server provides the network interface for all inbound and outbound SIP signaling to all provisioned SIP entities. During compliance testing, the IP address assigned to the SIP signaling interface was 10.64.21.31 as specified in **Figure 1**. The Session Manager server also has a separate network interface used for connectivity to System Manager for provisioning Session Manager. The IP address assigned to the Session Manager management interface was 10.64.21.30.

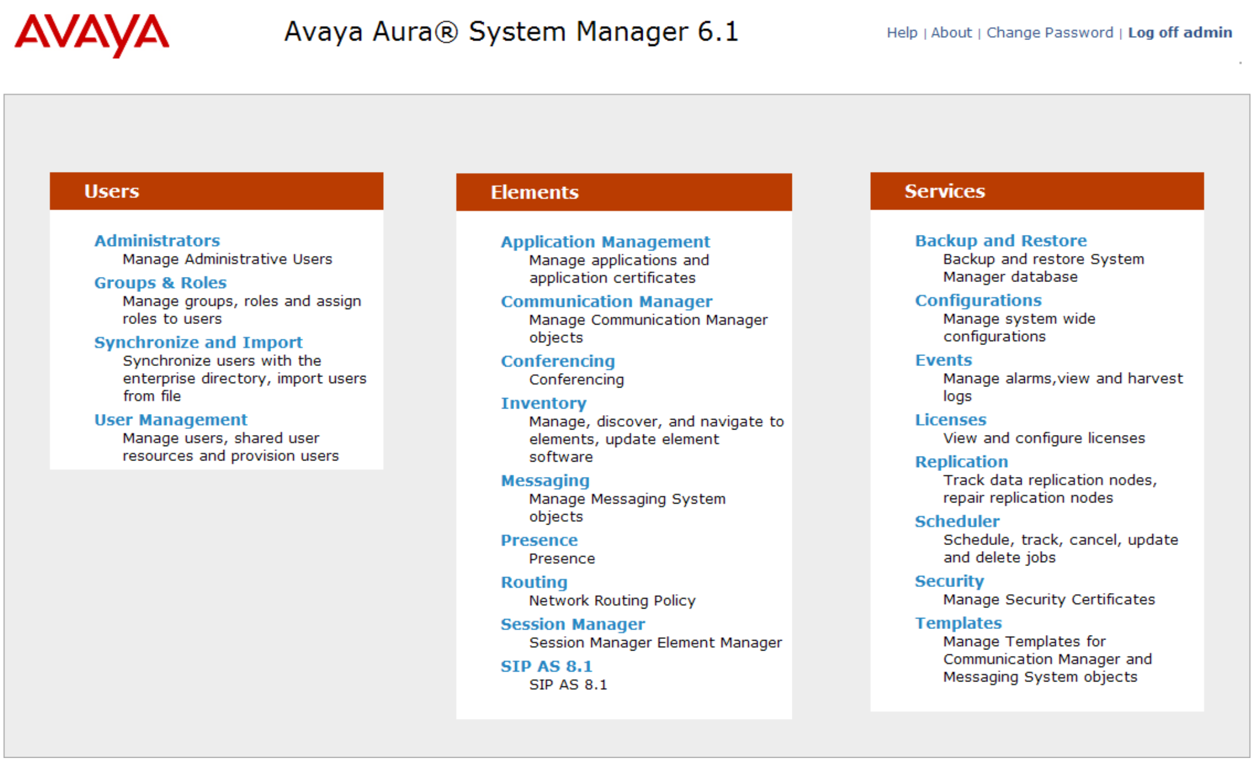
The procedures described in this section include configurations for the following:

- **SIP Domains** – SIP Domains are the domains for which Session Manager is authoritative in routing SIP calls. In other words, for calls to such domains, Session Manager applies Network Routing Policies to route those calls to SIP Entities. For calls to other domains, Session Manager routes those calls to another SIP proxy (either a pre-defined default SIP proxy or one discovered through DNS).
- **Locations** – Locations define the physical and/or logical locations in which SIP Entities reside. Call Admission Control (CAC) / bandwidth management may be administered for each location to limit the number of calls to and from a particular Location.
- **Adaptations –** Adaptations are used to apply any necessary protocol adaptations, e.g., modify SIP headers, and apply any necessary digit conversions for the purpose of inter-working with specific SIP Entities.
- **SIP Entities** – SIP Entities represent SIP network elements such as Session Manager instances, Communication Manager systems, Session Border Controllers, SIP gateways, SIP trunks, and other SIP network devices.
- **Entity Links** – Entity Links define the SIP trunk/link parameters, e.g., ports, protocol (UDP/TCP/TLS), and trust relationship, between Session Manager instances and other SIP Entities.
- **Time Ranges** – Time Ranges specify customizable time periods, e.g., Monday through Friday from 9AM to 5:59PM, Monday through Friday 6PM to 8:59AM, all day Saturday and Sunday, etc. A Network Routing Policy may be associated with one or more Time Ranges during which the Network Routing Policy is in effect.
- **Routing Policies** – Routing Policies are used in conjunction with a Dial Patterns to specify a SIP Entity that a call should be routed to.
- **Dial Patterns** – A Dial Pattern specifies a set of criteria and a set of Network Routing Policies for routing calls that match the criteria. The criteria include the called party number

and SIP domain in the Request-URI, and the Location from which the call originated. For example, if a call arrives at Session Manager and matches a certain Dial Pattern, then Session Manager selects one of the Network Routing Policies specified in the Dial Pattern. The selected Network Routing Policy in turn specifies the SIP Entity to which the call is to be routed.

Access the Session Manager administration web interface by entering **https://*<ip-addr>*/SMGR** as the URL in an Internet browser, where *<ip-addr>* is the IP address of the System Manager server.

Log in using appropriate credentials. The main page for the administrative interface is shown below.

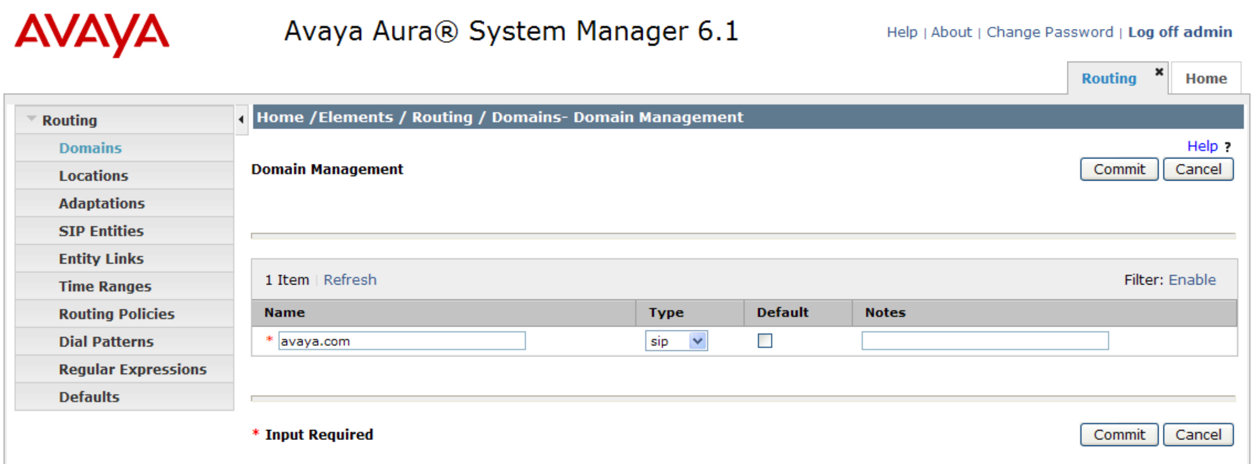


6.1. Specify SIP Domain

Navigate to **Home →Elements →Routing→Domains**, and click the **New** button (not shown) to add the SIP domain with the following:

- **Name**: ***avaya.com*** (as set in **Section 5.3**)
- **Type**: ***sip***
- **Notes**: optional descriptive text

Click **Commit** to save the configuration.



6.2. Add Location

Locations identify logical and/or physical locations where SIP entities reside. Only one Location was configured for compliance testing.

Navigate to **Home → Elements →Routing→Locations** and click the **New** button (not shown) to add the Location. Enter the following information:

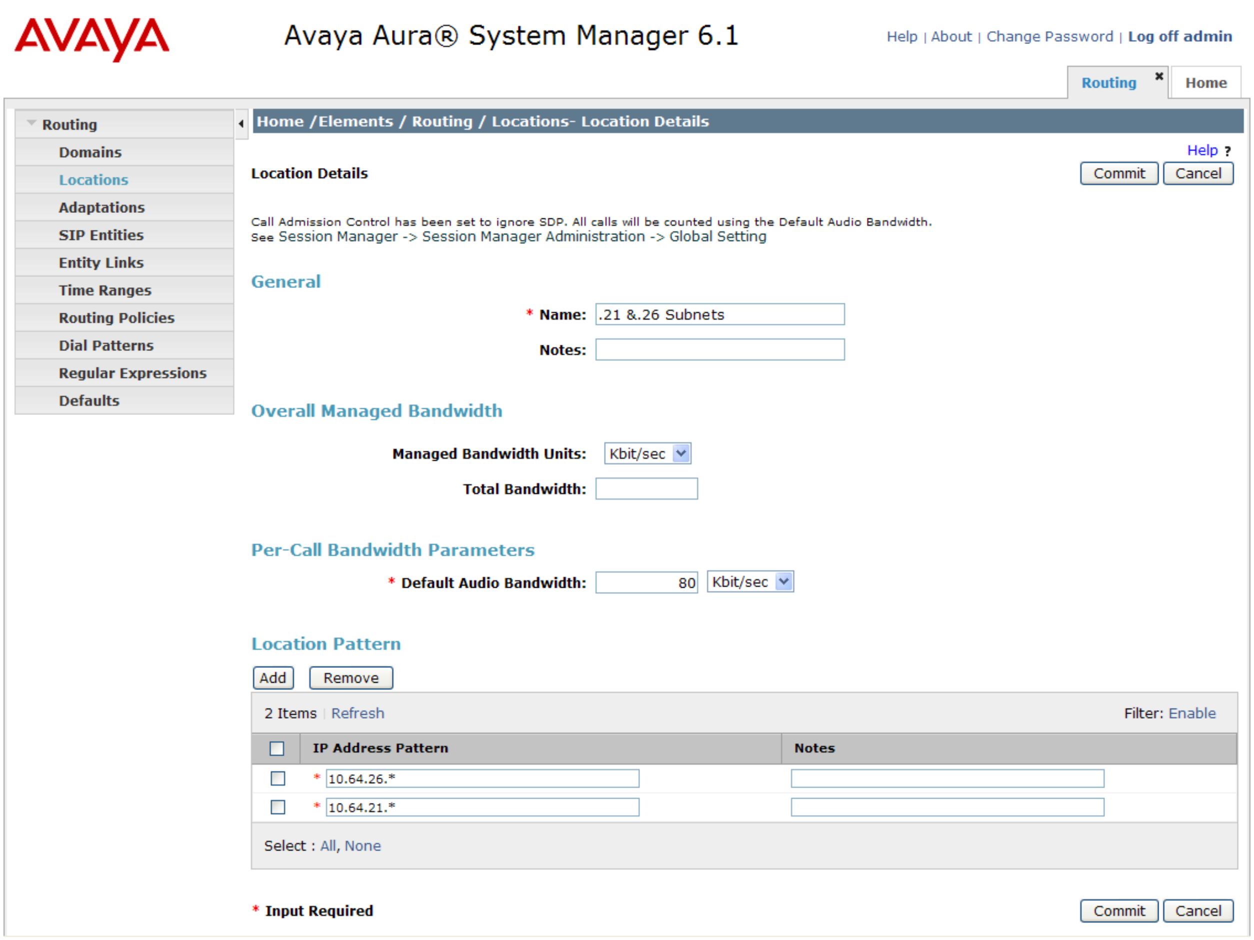
Under **General**:

- **Name**: a descriptive name
- **Notes**: optional descriptive text

Under **Location Pattern**, click the **Add** button to add a new line:

- **IP Address Pattern**: ***10.64.21.****
- **Notes**: optional descriptive text

Click **Commit** to save the configuration.



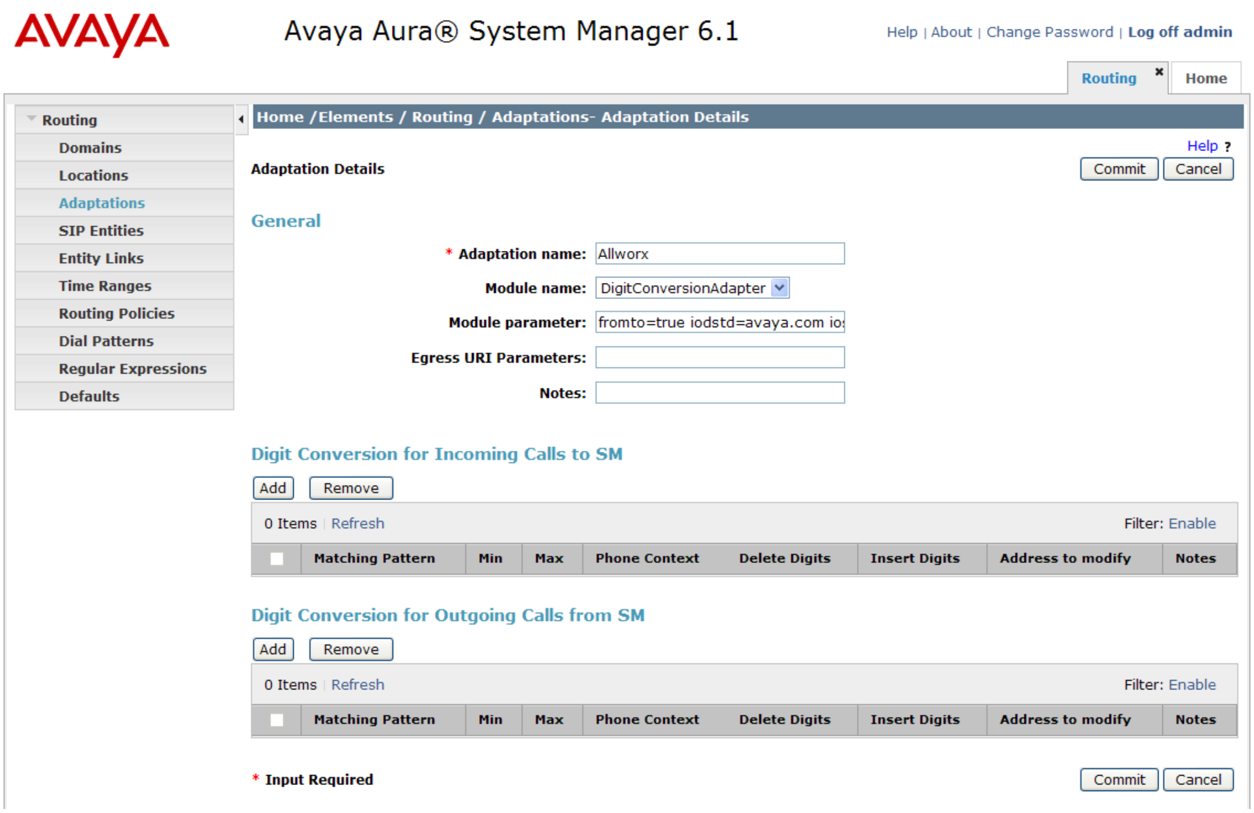
6.3. Add Allworx Adaptation

For calls from an Allworx IP Phone towards Communication Manager, an adaptation was created to change the domain in the *From* header from the Allworx 6x IP address to ***avaya.com***.

To create an adaptation, navigate to **Home → Elements → Routing→Adaptations** and click the **New** button (not shown). Enter the following information:

- **Adaptation name**: a descriptive name
- **Module name**: select from the drop-down menu or enter ***DigitConversionAdapter***
- **Module parameter**: enter ***fromto=true iodstd=avaya.com ioscrd=avaya.com***
- **Notes**: optional descriptive text

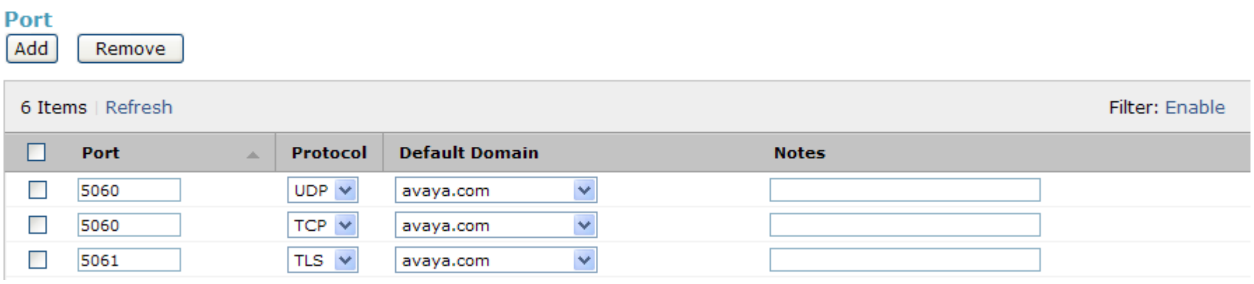
Click the **Commit** button.



6.4. Add SIP Entities

A SIP Entity must be added for Avaya Aura® Session Manager and for each SIP-based telephony system supported by it using SIP trunks. In the sample configuration, a SIP Entity is added for the Session Manager, Communication Manager, and the Allworx 6x system.

Note, the Session Manager SIP Entity is assumed to have already been configured. Navigate to **Home → Elements → Routing→SIP Entities**, check the checkbox for the Session Manager SIP Entity, and click the **Edit** button (not shown). Under the **Ports** section, verify the required Session Manager listening port for communication with Allworx is configured (i.e. **Port *5060*** and **Protocol *UDP***). If necessary, click the **Add** button to add the listening port and then click the **Commit** button when done to save the changes.



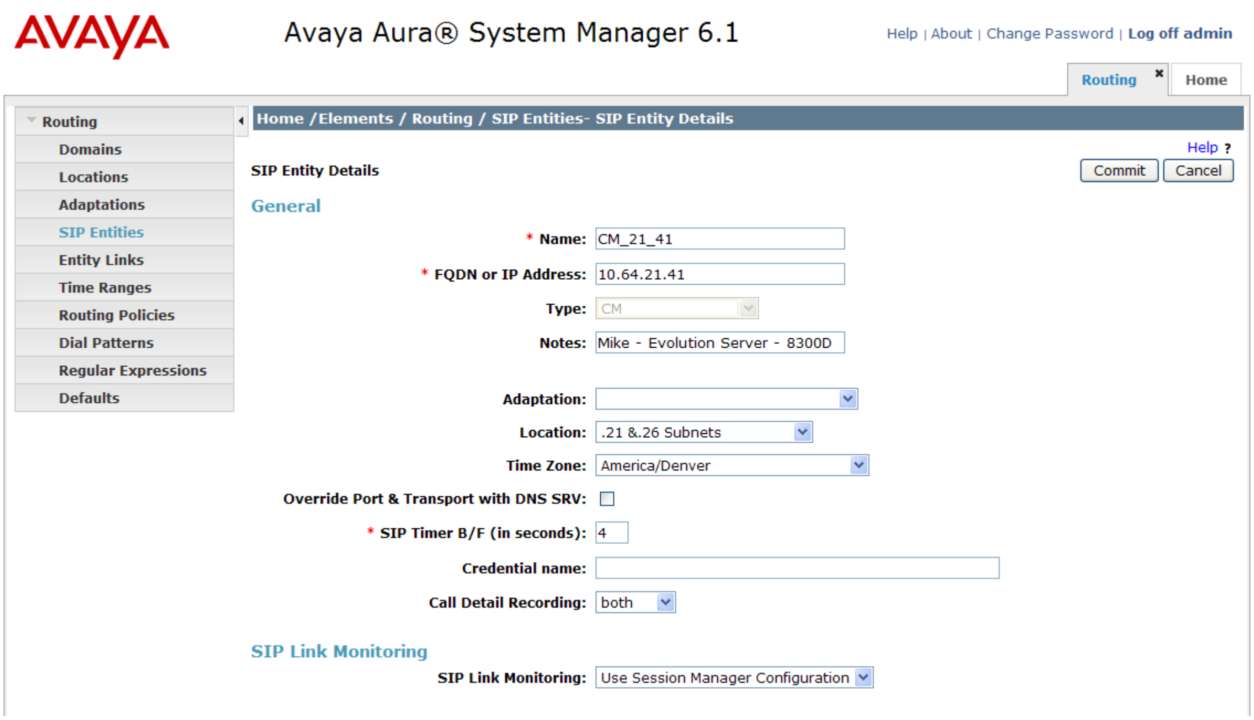
To add a SIP Entity, navigate to **Home → Elements → Routing→SIP Entities** and click the **New** button (not shown).

The configuration details for the SIP Entity defined for the Communication Manager are below:

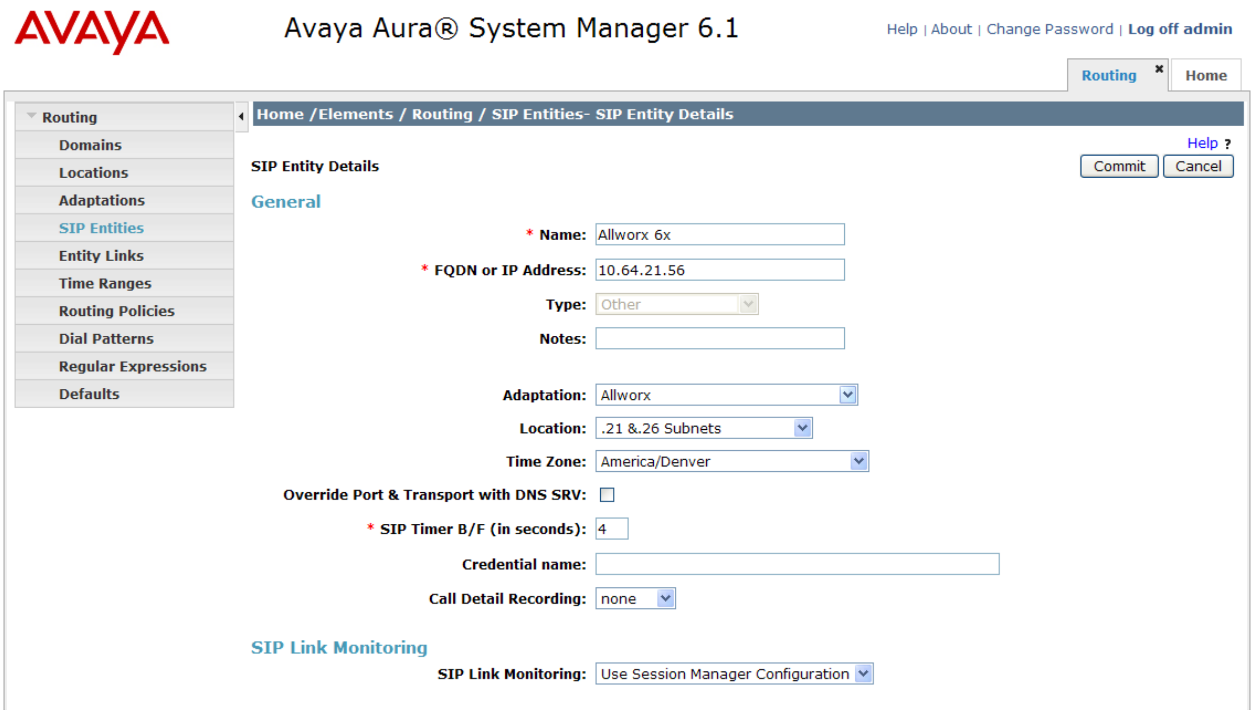
Under **General**:

- **Name**: a descriptive name
- **FQDN or IP Address**: ***10.64.21.41*** as specified in **Figure 1**
- **Type**: select ***CM***
- **Location**: select the location configured in **Section 6.2**

Default settings can be used for the remaining fields. Click **Commit** to save the SIP Entity definition.



The following screen shows addition of the Allworx 6x SIP Entity. Note the selection of ***Other*** for **Type**.



6.5. Add Entity Links

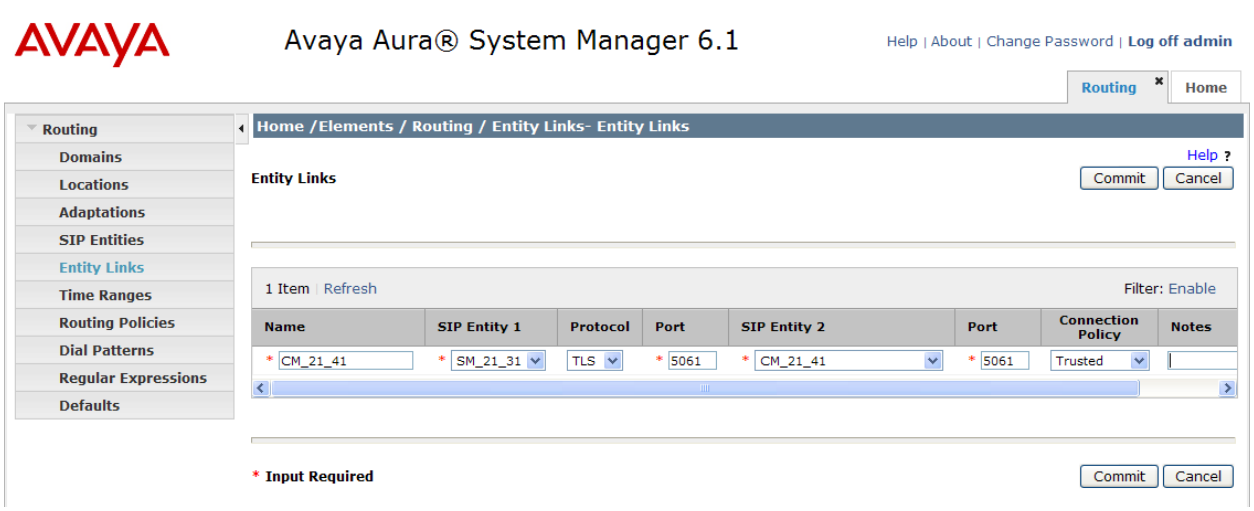
A SIP trunk between Session Manager and a telephony system is described by an Entity link. Two Entity Links were created:

- Session Manager ←→ Communication Manger
- Session Manager ←→ Allworx 6x

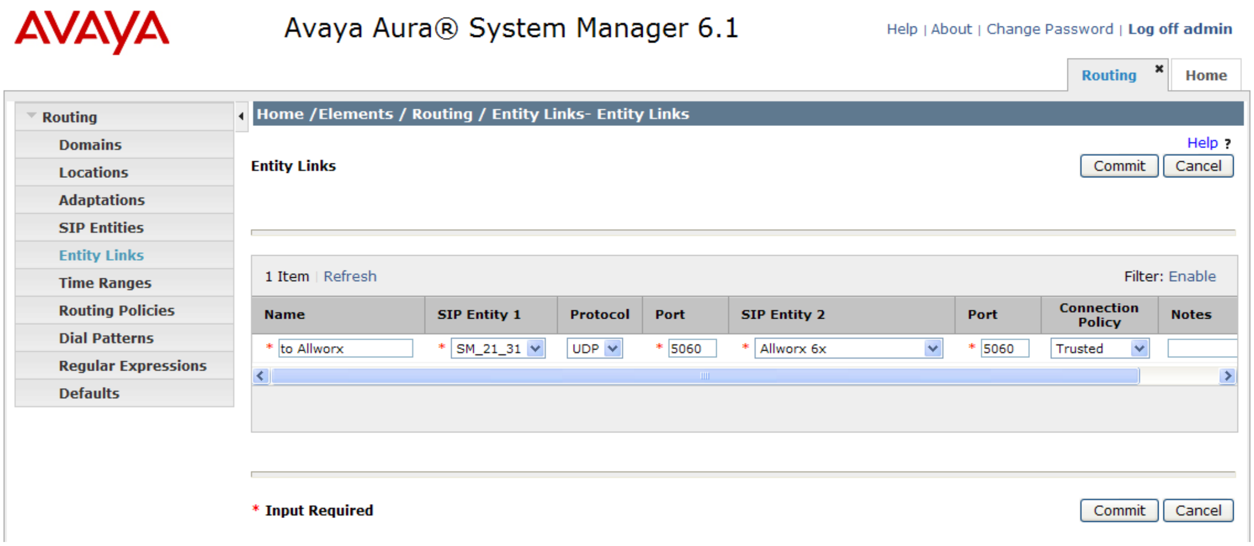
Navigate to **Home → Elements → Routing→Entity Links**, and click the **New** button (not shown) to add a new Entity Link. The screen below shows the configuration details for the Entity Link connecting Session Manager with Communication Manager.

- **Name**: a descriptive name
- **SIP Entity 1**: select the Session Manager SIP Entity.
- **Protocol**: select ***TLS*** as the transport protocol
- **Port**: ***5061***. This is the port number to which the other system sends SIP requests
- **SIP Entity 2**: select the Communication Manager SIP Entity
- **Port**: ***5061***. This is the port number on which the other system receives SIP requests
- **Connection Policy**: select ***Trusted***
- **Notes**: optional descriptive text

Click **Commit** to save the configuration.



The Entity Link for connecting Session Manager with Allworx 6x was similarly defined as shown in the screen below. Note the use of ***UDP*** and port ***5060***.



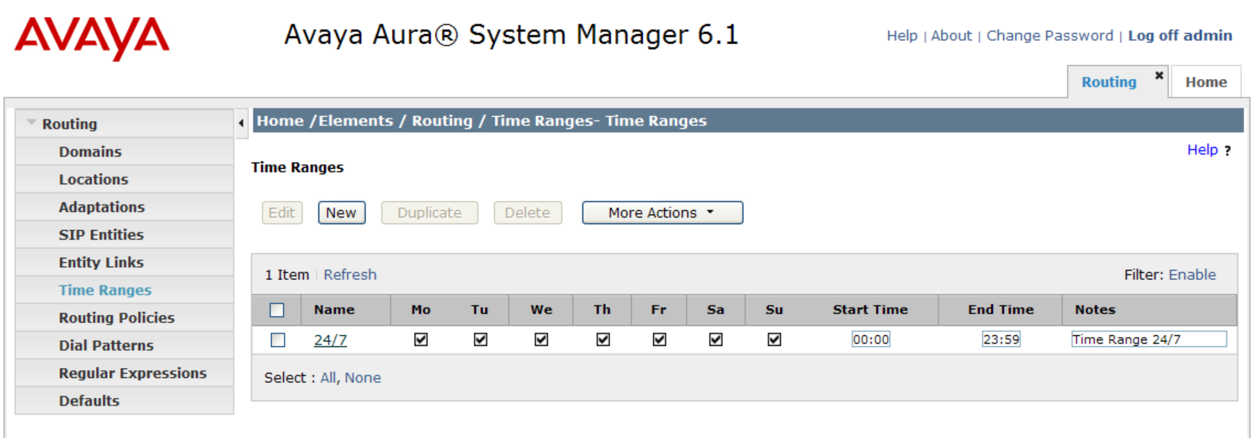
6.6. Add Time Ranges

Before adding routing policies (configured in next step), time ranges must be defined during which the routing policies will be active. One time range was defined that would allow routing to occur at any time.

Navigate to **Elements → Routing→Time Ranges**, and click the **New** button to add a new Time Range. Enter the following information:

- **Name**: a descriptive name
- **Mo** through **Su**: check the box under each of these headings
- **Start Time**: enter ***00:00***
- **End Time**: enter ***23:59***
- **Notes**: optional descriptive text

Click **Commit** to save this time range. The screen below shows the configured Time Range.



6.7. Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities connected to the Session Manager. One routing policy must be added for routing calls to Communication Manager and one for routing calls to the Allworx 6x system.

Navigate to **Home → Elements → Routing→Routing Policies**, and click the **New** button (not shown) to add a new Routing Policy. Enter the following information:

Under **General**:

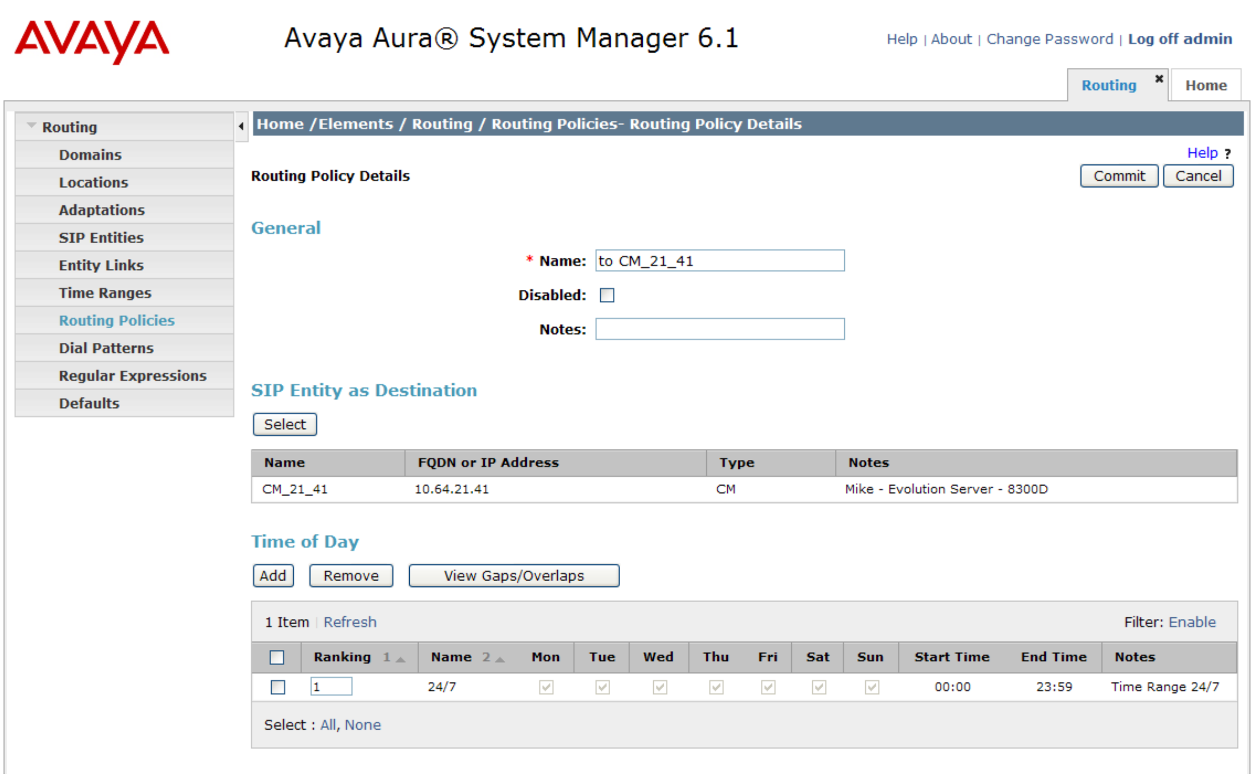
- **Name**: a descriptive name
- **Notes**: optional descriptive text

Under **SIP Entity as Destination**
Click **Select** to select the appropriate SIP Entity to which the routing policy applies (not shown).

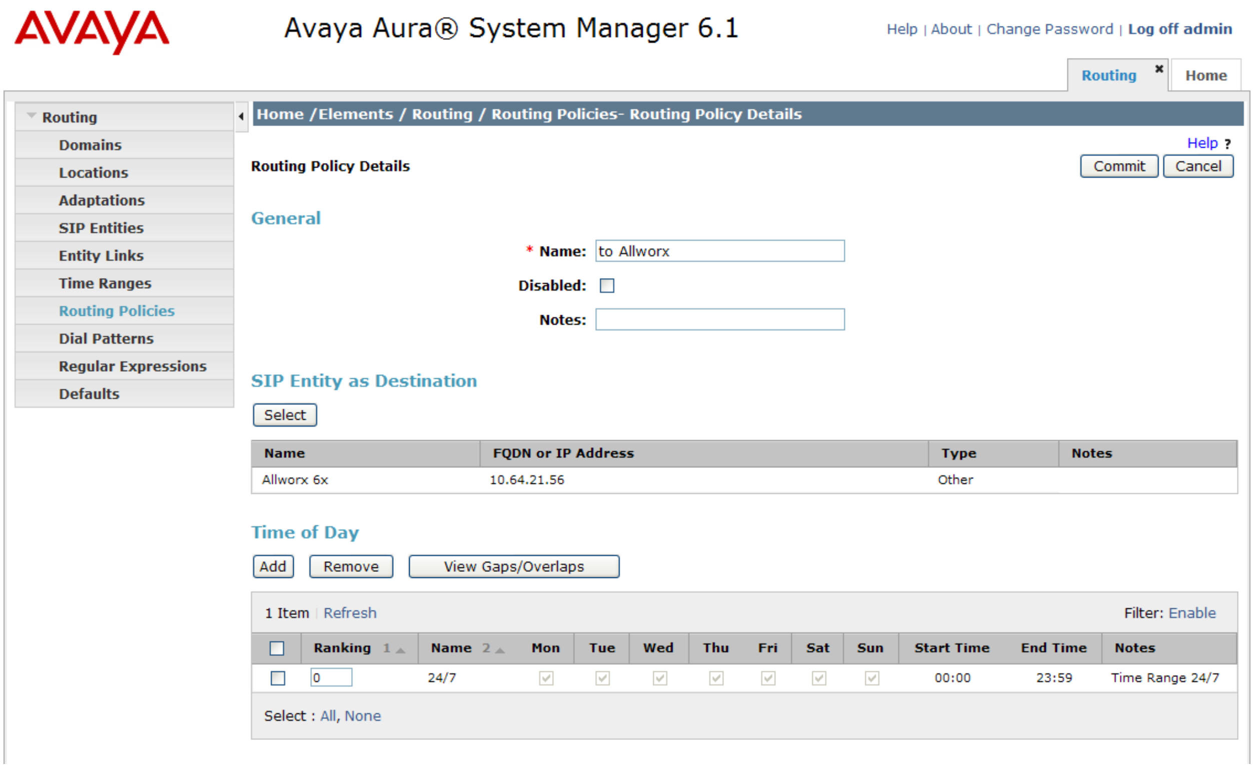
Under **Time of Day**
Click **Add** to select the Time Range configured in the previous step (not shown).

Default settings can be used for the remaining fields. Click **Commit** to save the configuration.

The following screen shows the Routing Policy for routing calls to Communication Manager.



The following screen shows the Routing Policy for routing calls to the Allworx 6x system.



6.8. Add Dial Patterns

Define dial patterns to direct calls to the appropriate SIP Entity.

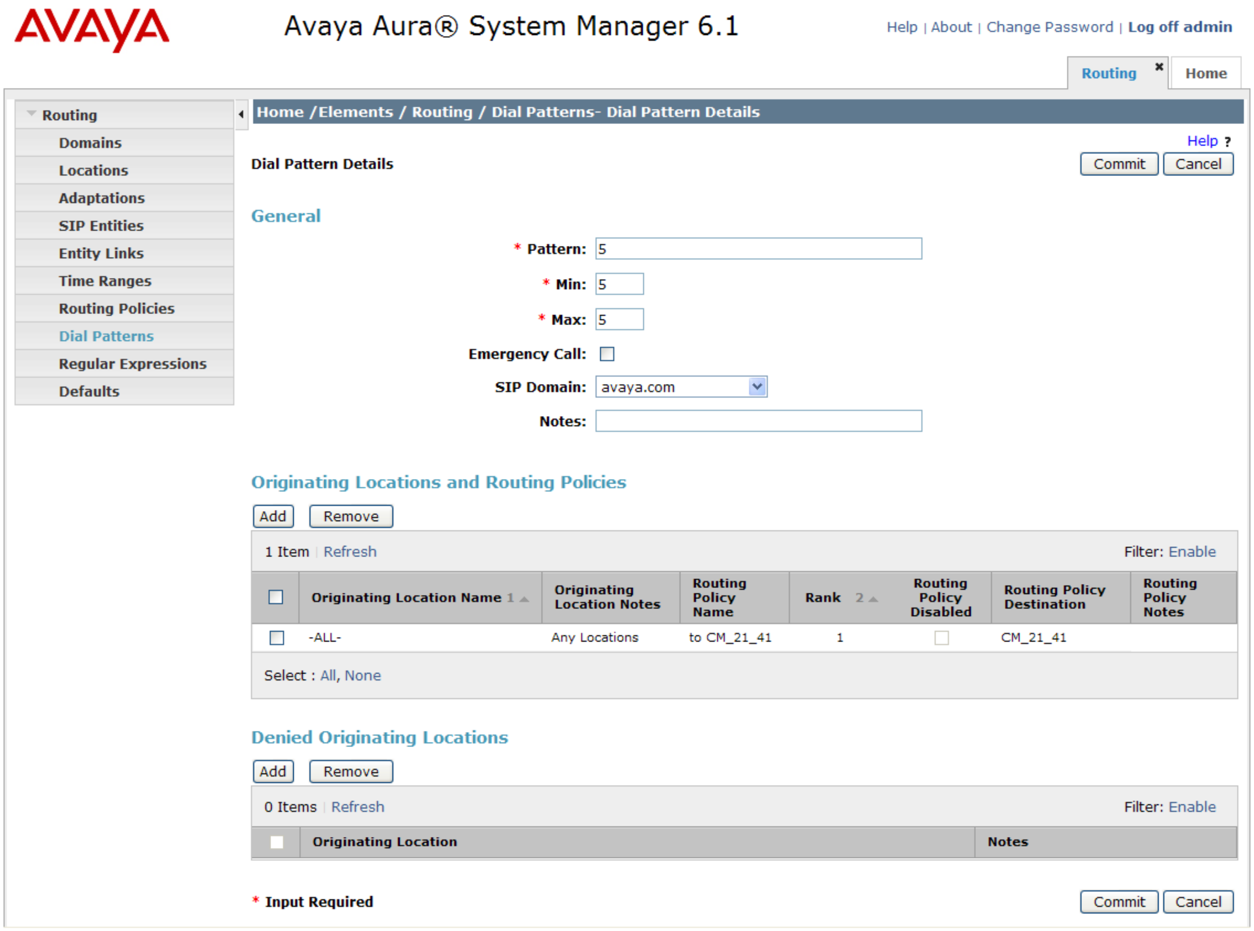
Navigate to **Home → Elements → Routing→Dial Patterns**, and click the **New** button (not shown) to add a new Dial Pattern. Enter the following information to route calls that match the pattern ***5xxxx*** to Communication Manager.

Under **General**:

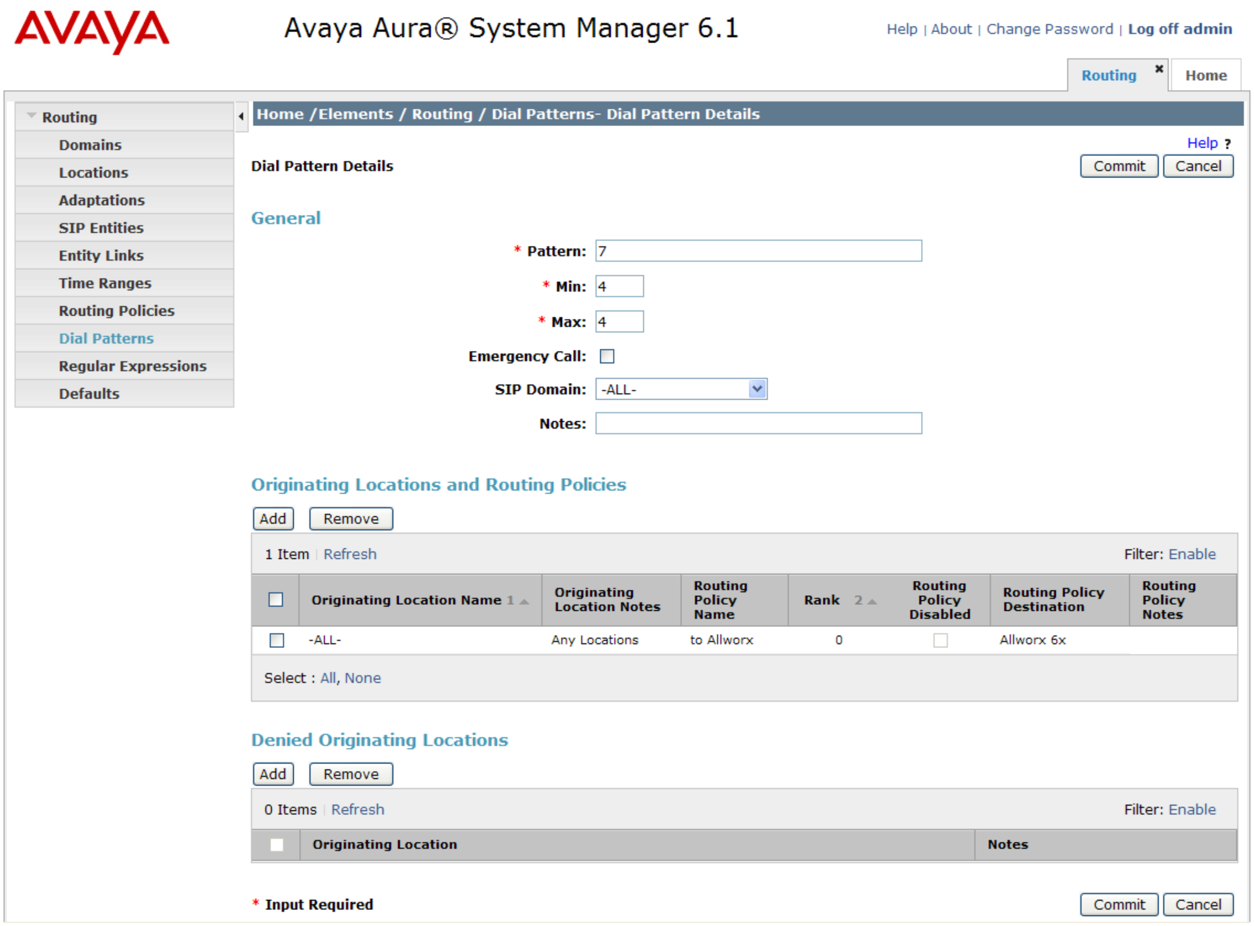
- **Pattern**: dialed number or prefix
- **Min**: minimum length of dialed number
- **Max**: maximum length of dialed number
- **SIP Domain**: select the SIP Domain created in **Section 6.1** (or select **–ALL–** to be less restrictive)
- **Notes**: optional descriptive text

Under **Originating Locations and Routing Policies**
Click **Add** to select the appropriate originating Location and Routing Policy from the list (not shown).

Default settings can be used for the remaining fields. Click **Commit** to save the configuration.


AVAYA
Avaya Aura® System Manager 6.1
Help | About | Change Password | Log off admin
Routing
Home
Routing
Domains
Locations
Adaptations
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns
Regular Expressions
Defaults
Home /Elements / Routing / Dial Patterns- Dial Pattern Details
Help ?
Dial Pattern Details
Commit
Cancel
General
* Pattern: 5
* Min: 5
* Max: 5
Emergency Call:
SIP Domain: avaya.com
Notes:
Originating Locations and Routing Policies
Add
Remove
1 Item | Refresh
Filter: Enable
Originating Location Name
Originating Location Notes
Routing Policy Name
Rank
Routing Policy Disabled
Routing Policy Destination
Routing Policy Notes
-ALL-
Any Locations
to CM_21_41
1
CM_21_41
Select : All, None
Denied Originating Locations
Add
Remove
0 Items | Refresh
Filter: Enable
Originating Location
Notes
* Input Required
Commit
Cancel

Enter the following information to route calls that match the pattern ***7xxx*** to the Allworx 6x system. The Allworx 6x system will then route the calls to the Allworx IP Phones.



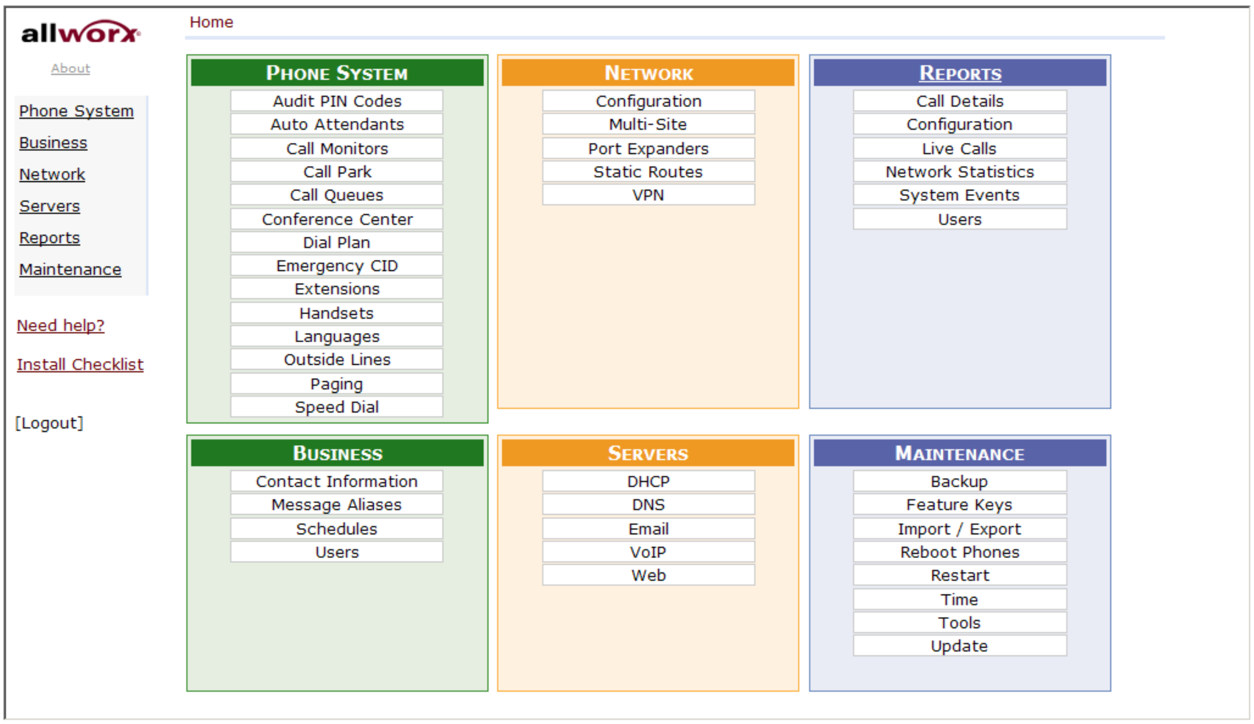
7. Configure Allworx 6x System and Allworx IP Phones

This section provides the procedures for configuring the Allworx 6x system and Allworx IP Phones as shown in the reference configuration.

7.1. Access Allworx Administration Web Pages

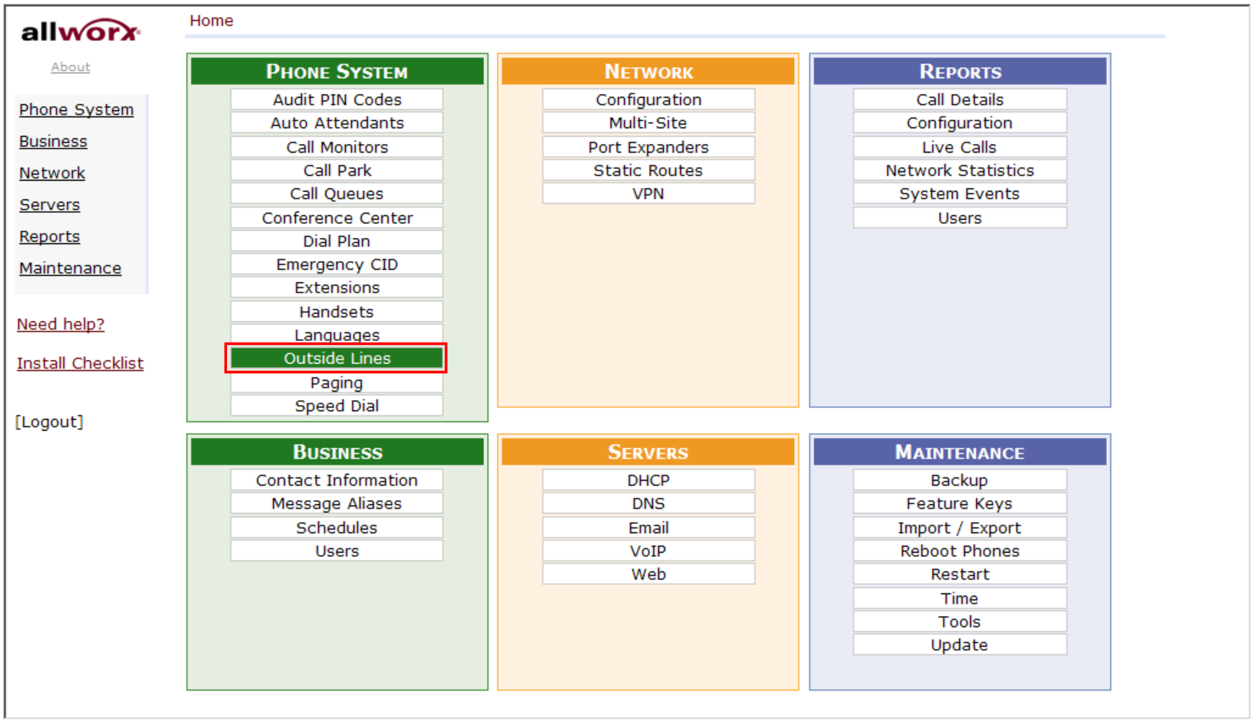
Access the Allworx 6x administration web interface by entering **http://<*ip-addr*>** as the URL in an Internet browser, where <*ip-addr*> is the IP address of the Allworx 6x system. Log in using appropriate credentials.

After logging in, the following **Home** screen is displayed.

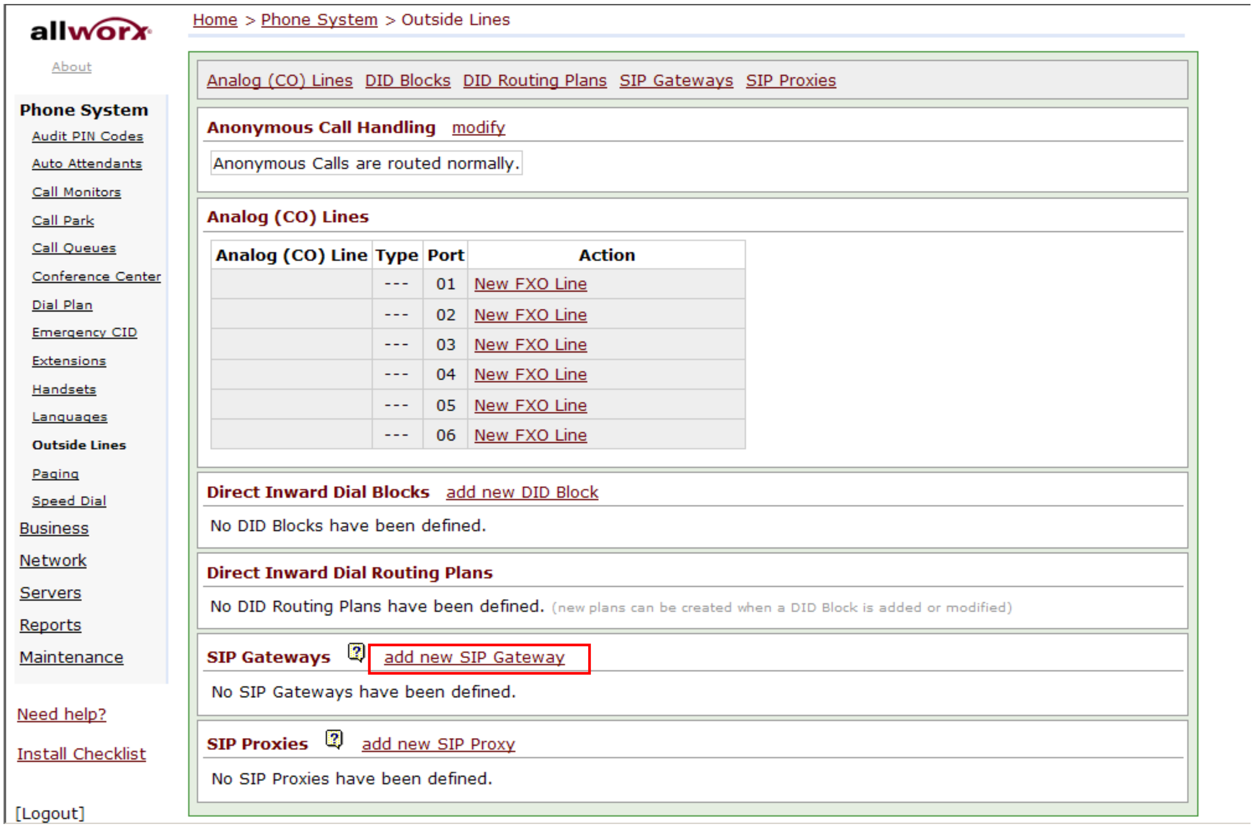


7.2. Configure SIP Gateway

From the Home page, navigate to **Phone System → Outside Lines**.


allworx
About
Home
Phone System
Business
Network
Servers
Reports
Maintenance
Need help?
Install Checklist
[Logout]
Phone System
Audit PIN Codes
Auto Attendants
Call Monitors
Call Park
Call Queues
Conference Center
Dial Plan
Emergency CID
Extensions
Handsets
Languages
Outside Lines
Paging
Speed Dial
Network
Configuration
Multi-Site
Port Expanders
Static Routes
VPN
Reports
Call Details
Configuration
Live Calls
Network Statistics
System Events
Users
Business
Contact Information
Message Aliases
Schedules
Users
Servers
DHCP
DNS
Email
VoIP
Web
Maintenance
Backup
Feature Keys
Import / Export
Reboot Phones
Restart
Time
Tools
Update

The **Outside Lines** page is displayed as shown below. In the **SIP Gateways** section, click the **add new SIP Gateway** link.



Enter the following information:

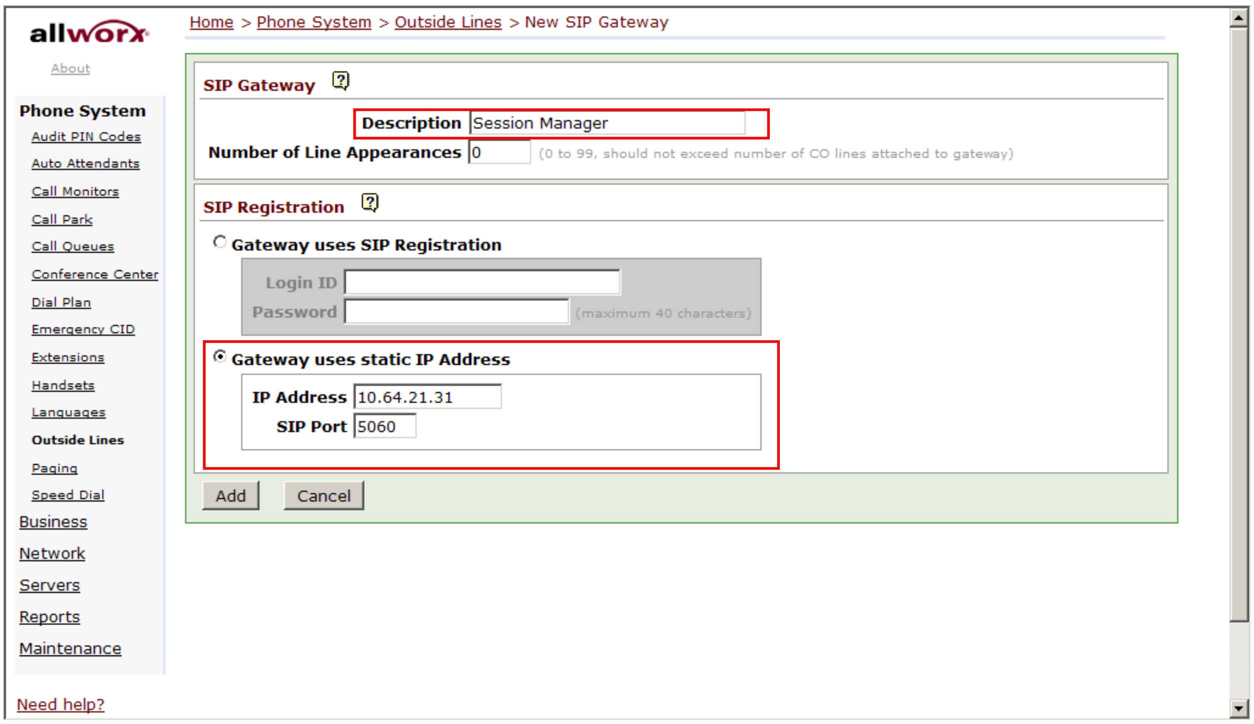
Under **SIP Gateway**:

- **Description**: enter descriptive text

Under **SIP Registration**:

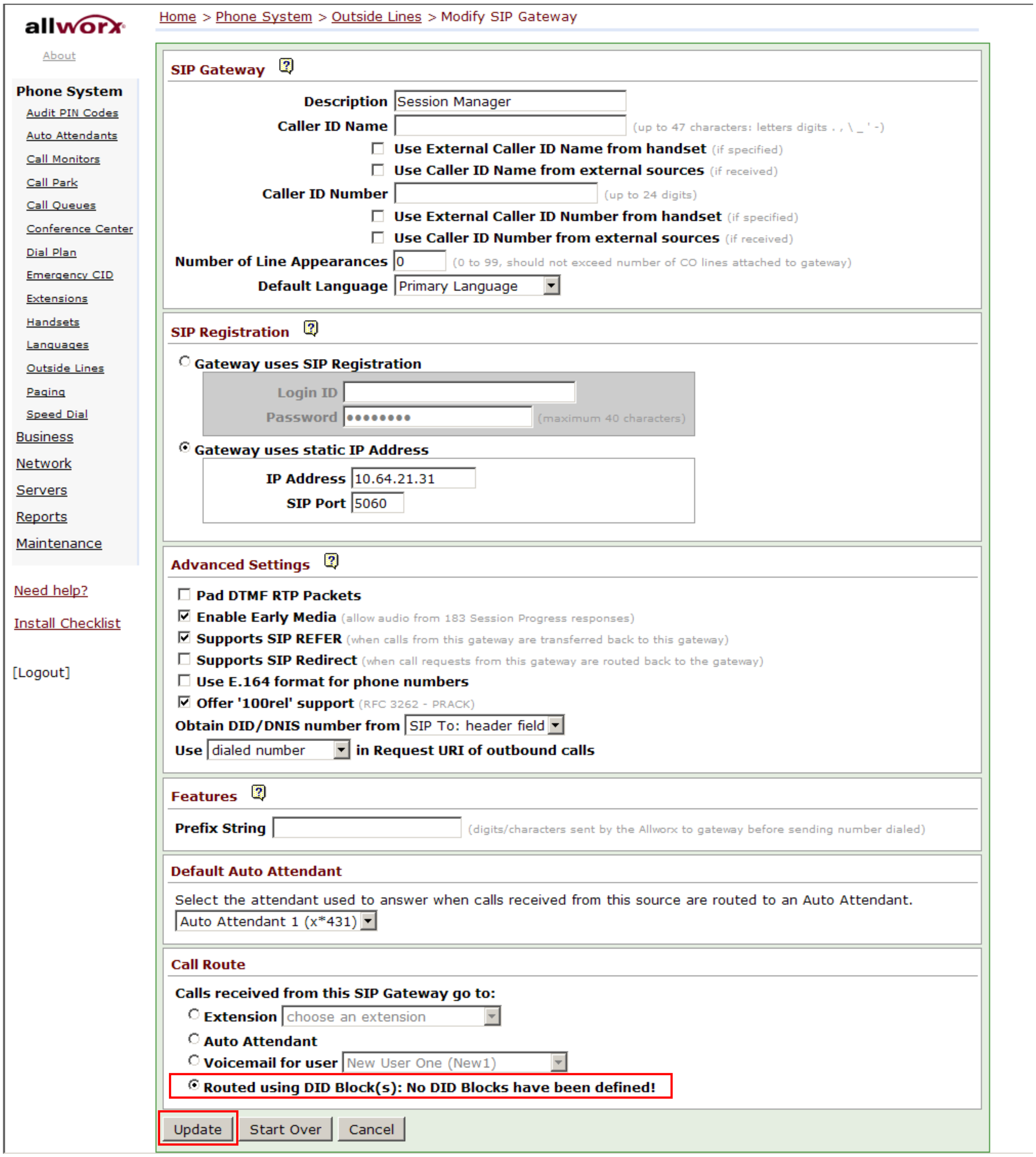
- Check the radio button for **Gateway uses static IP Address**:
  - **IP Address**: enter the SIP signaling IP address of Session Manager
  - **SIP Port**: enter the SIP signaling port used by Session Manager

Click the **Add** button.



On the **Outside Lines** page, click the **Modify** link (not shown) for the SIP Gateway just added.

Under the **Call Route** section at the bottom of the screen, click the radio box for **Routed using DID Block(s)** and click the **Update** button.



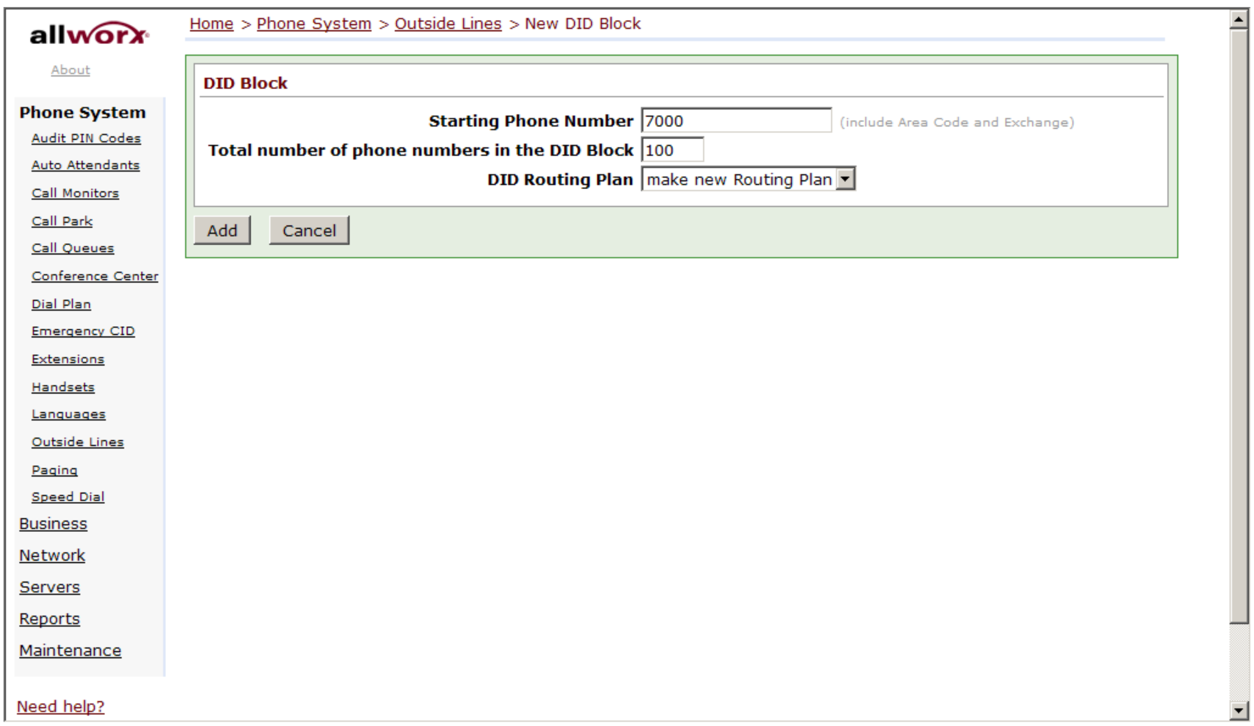
7.3. Configure DID Block

In the **Direct Inward Dial Blocks** section of the **Outside Lines** page shown in **Section 7.2**, click the **add new DID block** link.

Enter the following:

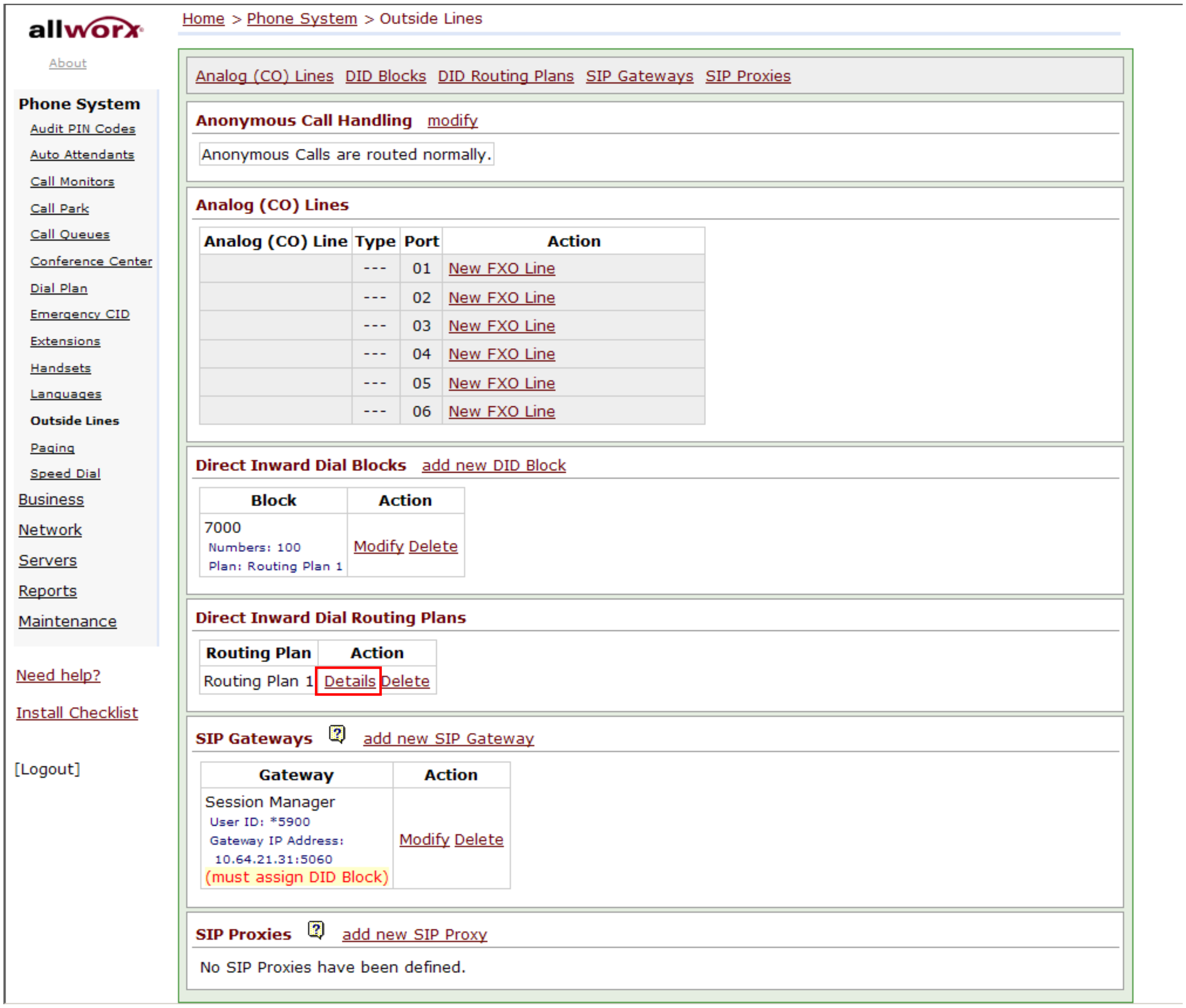
- **Starting Phone Number**: enter the starting/first phone number of the Allworx IP Phones. Note, these are the phone numbers/extensions that will be used by Communication Manager and Session Manager to route calls to the Allworx IP phones.
- **Total number of phone number in the DID Block**: enter the number of phone numbers desired
- **DID Routing Plan**: select ***make new Routing Plan*** from the drop-down menu.

Click the **Add** button.

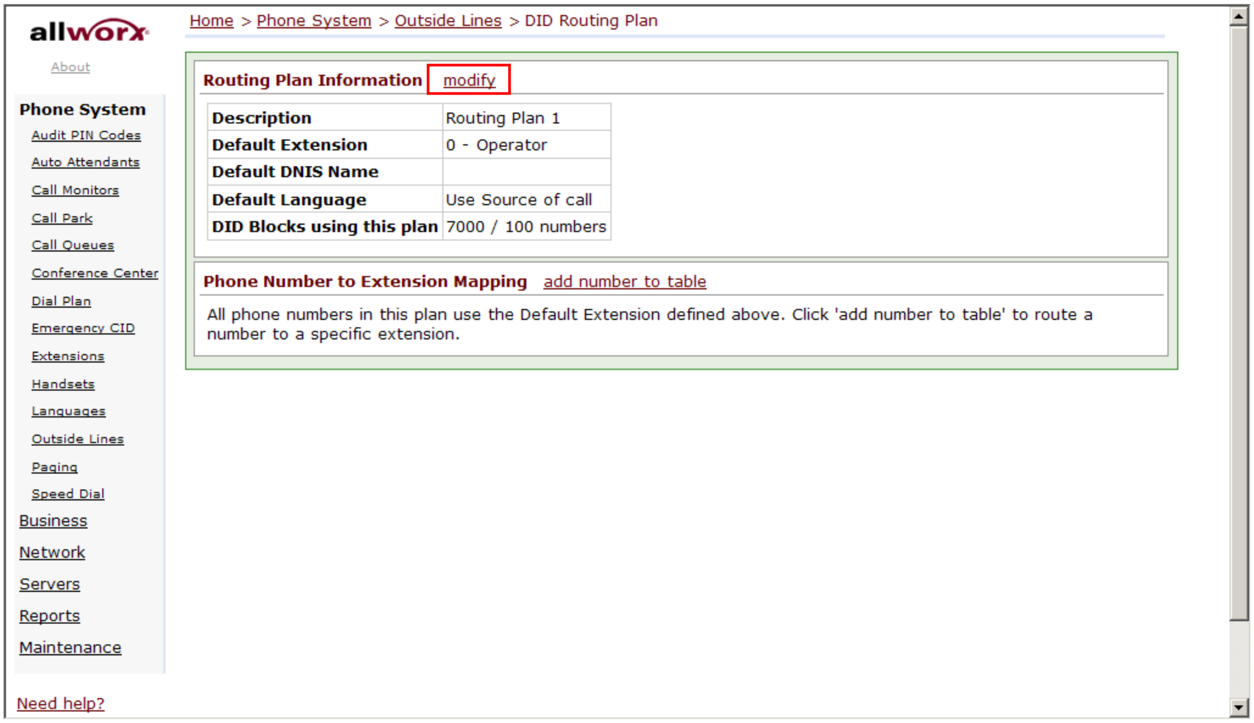


7.4. Configure DID Routing Plan

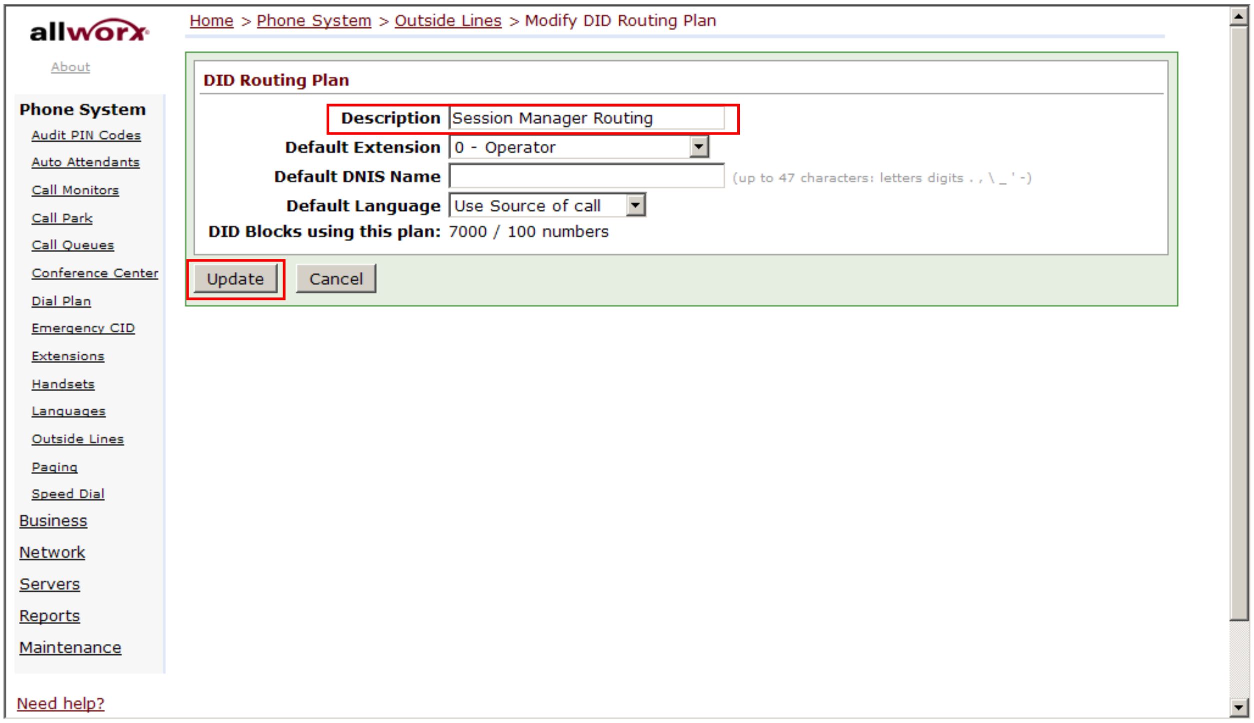
On the **Outside Lines** page, click the **Details** link under the **Direct Inward Dialing Routing Plans** section.



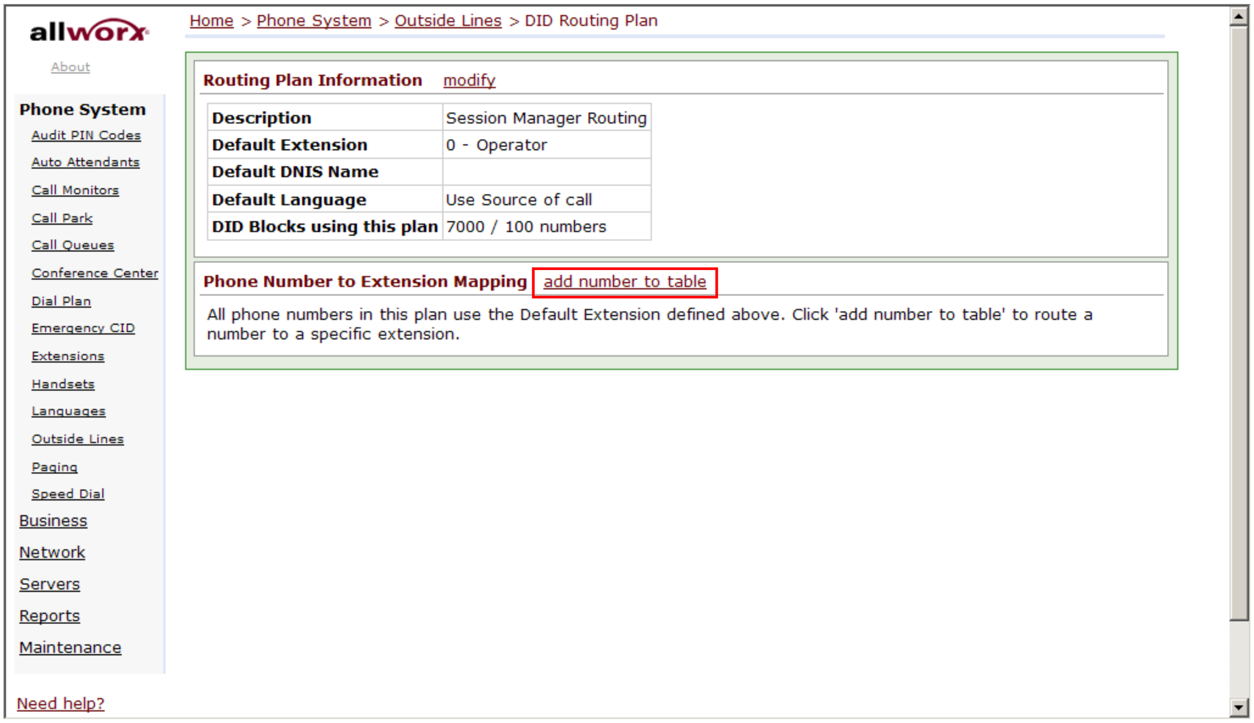
Click the **modify** link next to **Routing Plan Information**.



Enter descriptive text for **Description** and click the **Update** button.

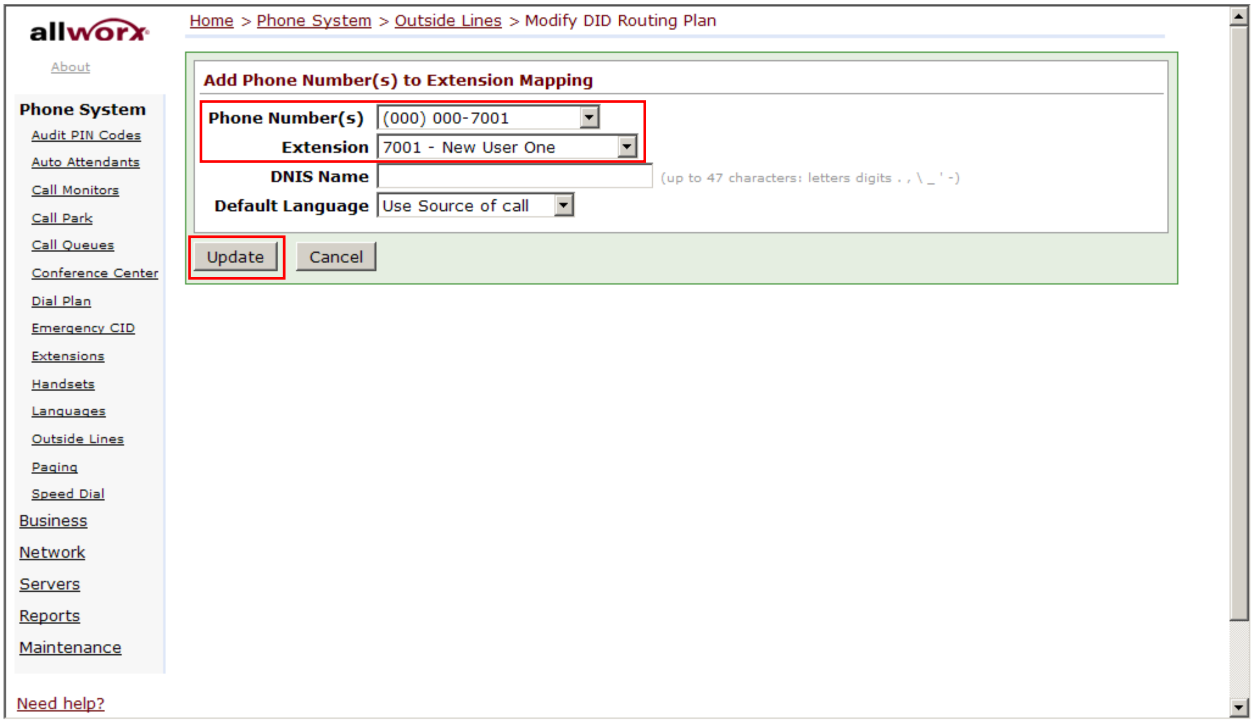


Click the **add number to table** link next to **Phone Number to Extension Mapping**.



Select a **Phone Number(s)** and **Extension** from the drop-down menus to map the select phone number to the selected extension.

Click the **Update** button.

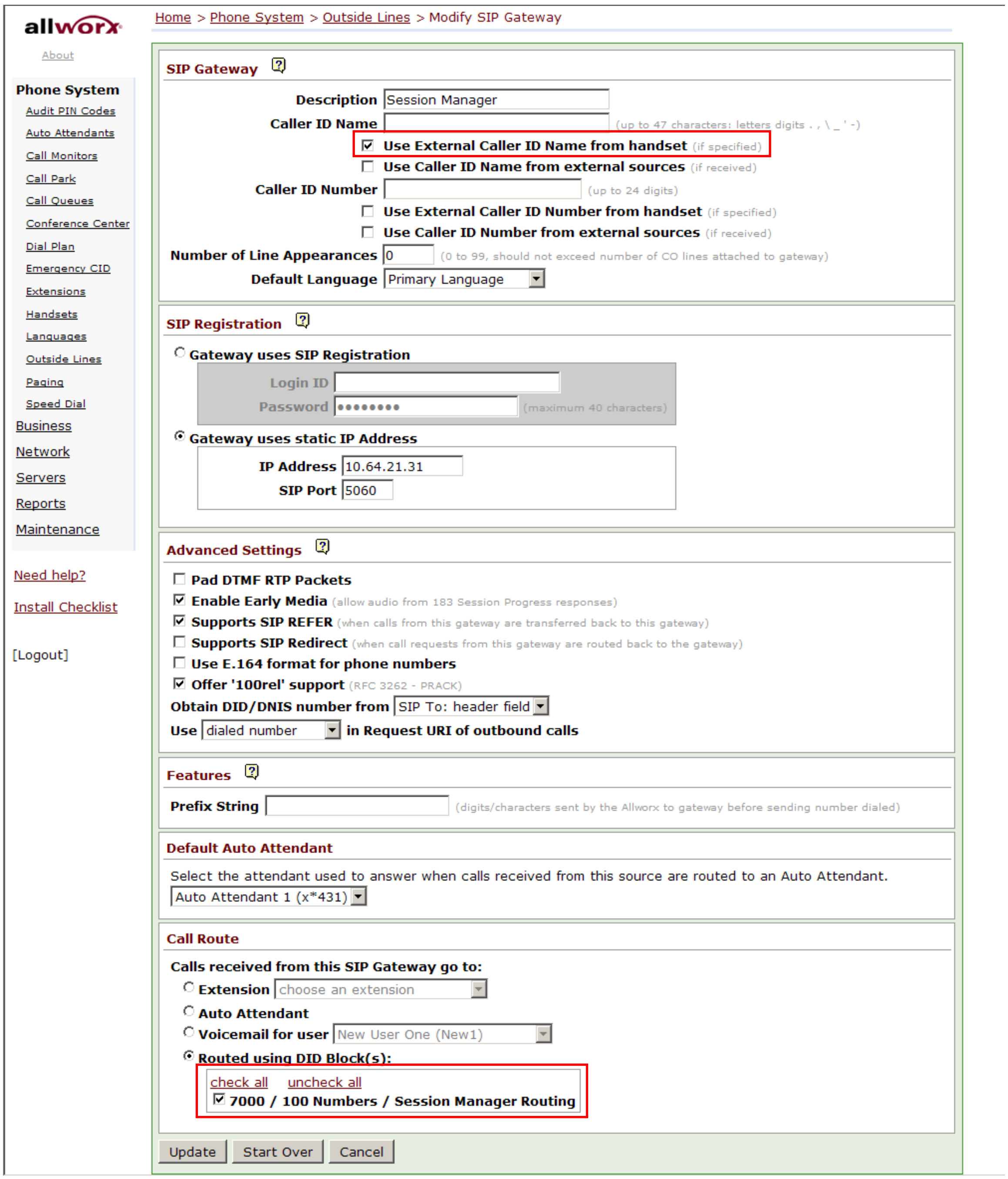


Repeat the previous step for each phone number / extension mapping.

7.5. Modify SIP Gateway

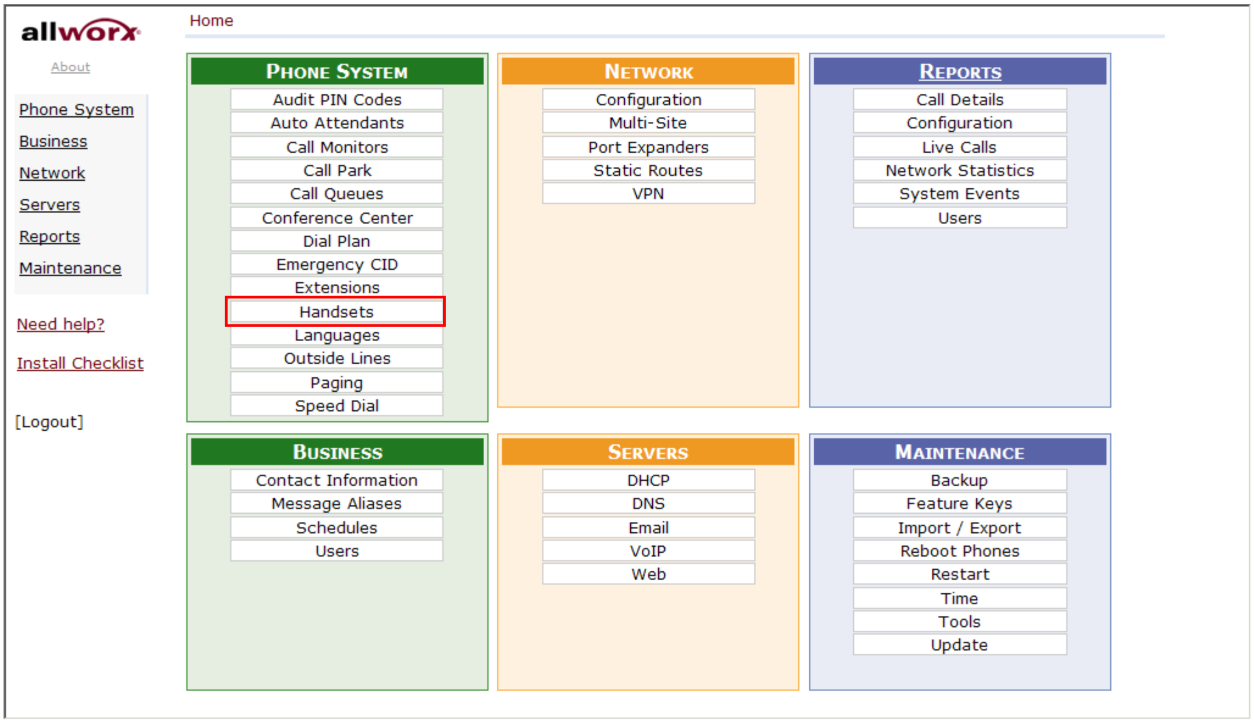
On the **Outside Lines** page, click the **Modify** link (not shown) next to the SIP Gateway shown in **Section 7.2**. Under the **SIP Gateway** section at the top of the screen, check the **Use External Caller ID Name from handset** checkbox. Under the **Call Route** section at the bottom of the screen, check the checkbox for the DID block created in **Section 7.3**.

Click the **Update** button.

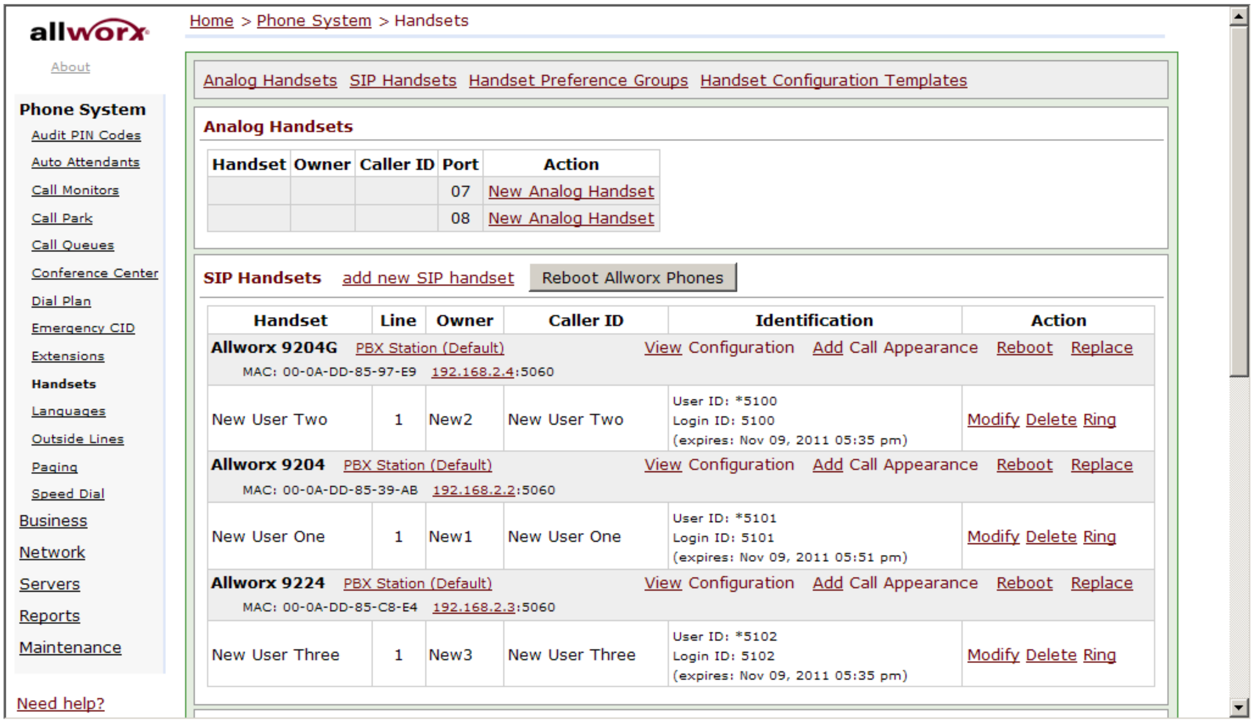


7.6. Modify Handsets

Navigate back to the **Home** page shown below and click the **Handsets** link under **Phone System**.

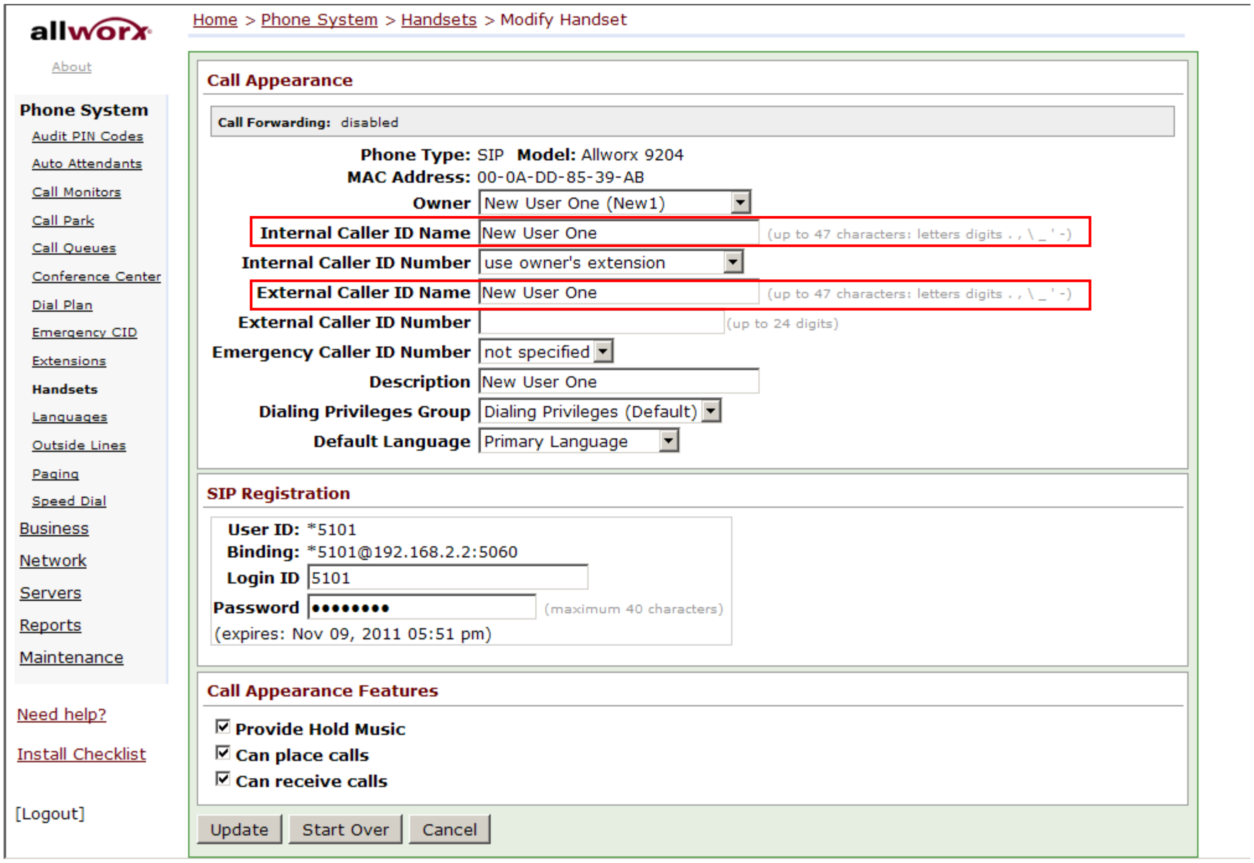


The following screen is displayed. Click the **Modify** link for one of the Handsets.

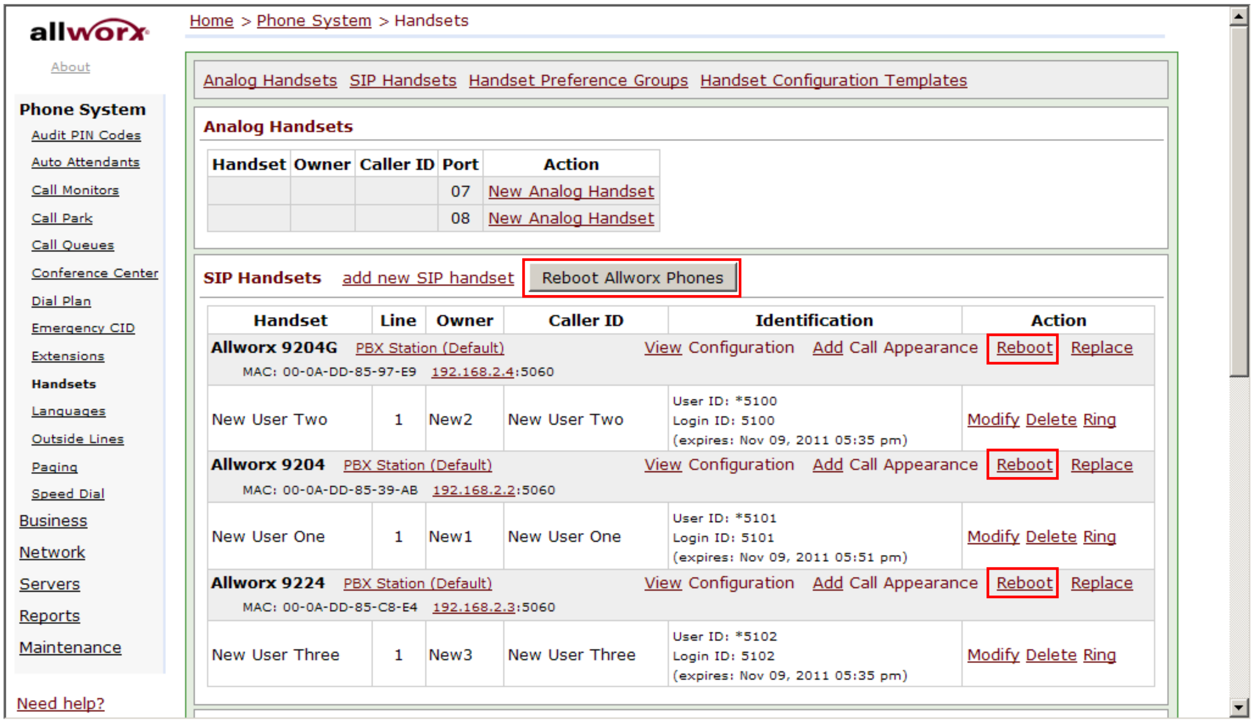


Enter text in the **External Caller ID Name** field to match the text shown in the **Internal Caller ID Name** field. Repeat this procedure for each of the handsets.

Click the **Update** button.

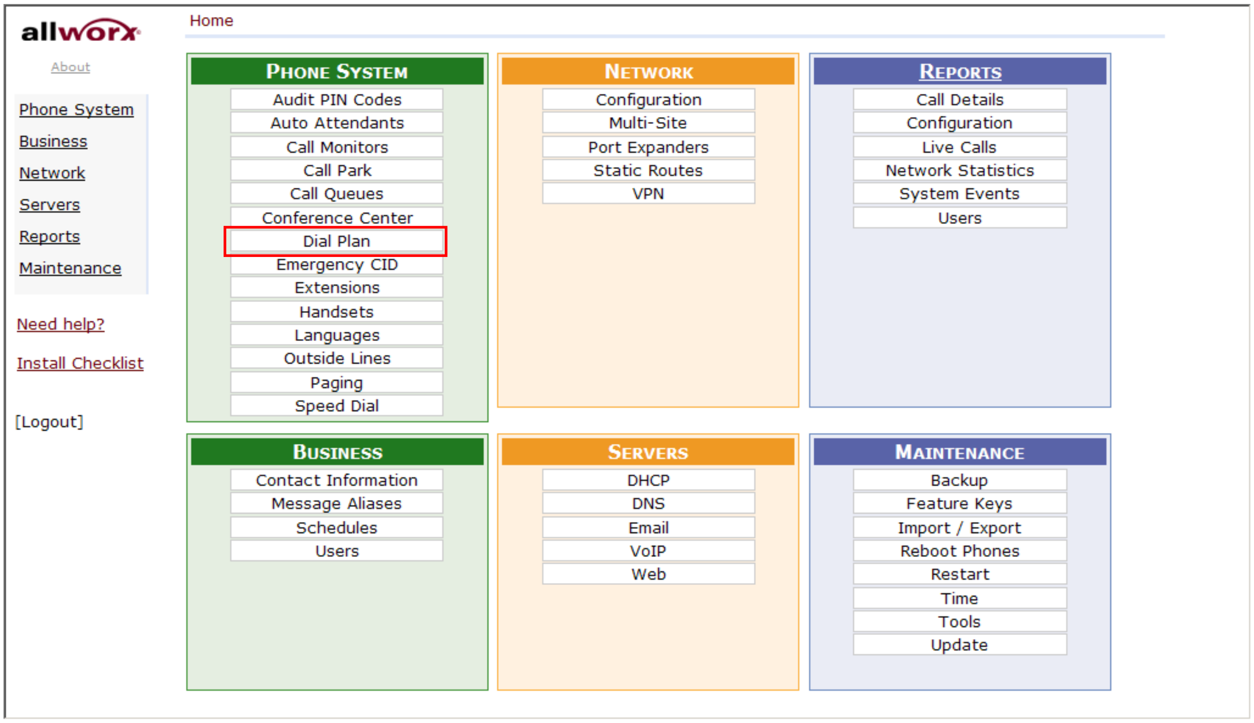


After modifying the handsets, click the **Reboot Allworx Phones** button to reboot all the handsets, or click each of the individual **Reboot** links for each modified handset.

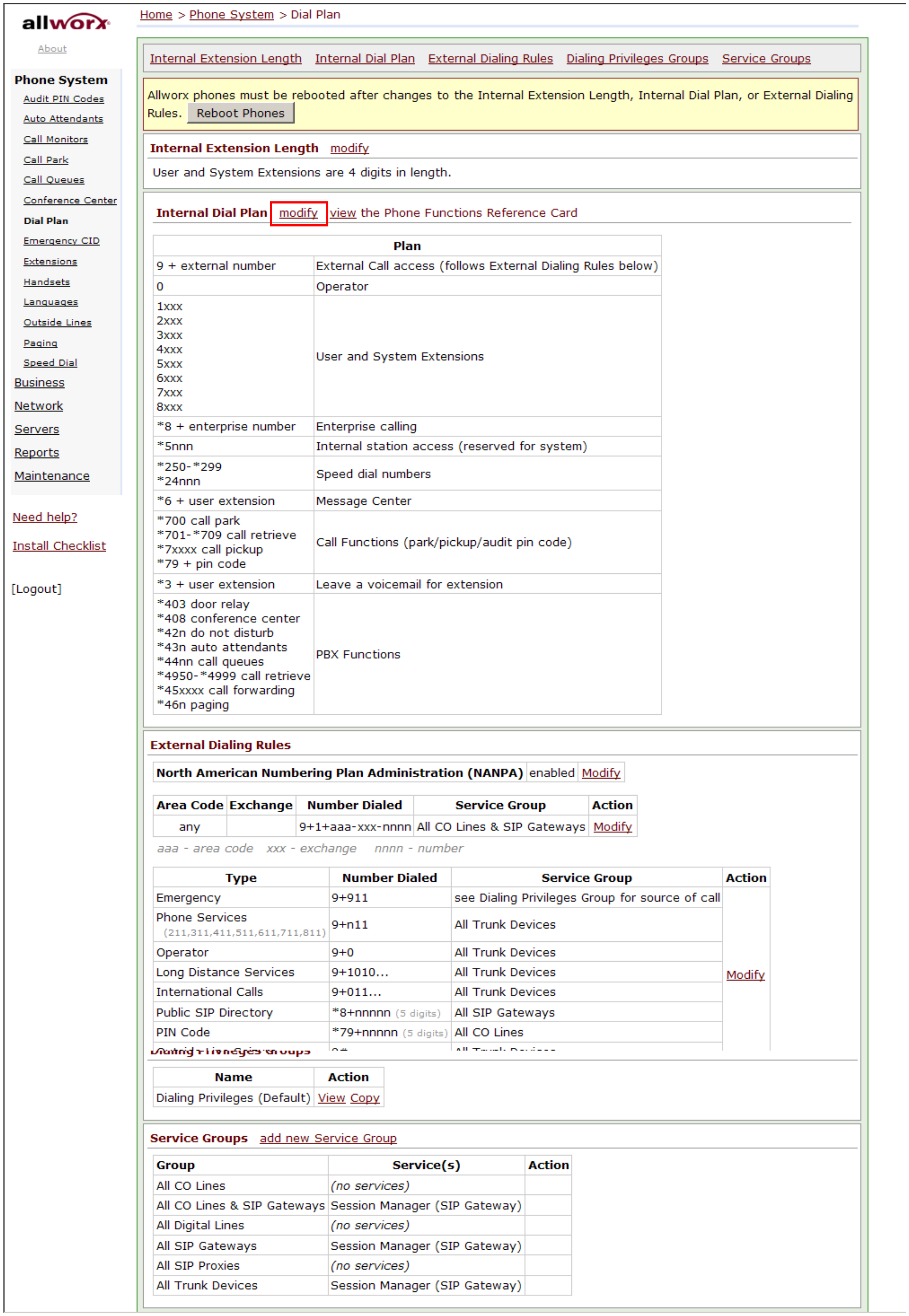


7.7. Modify Dial Plan

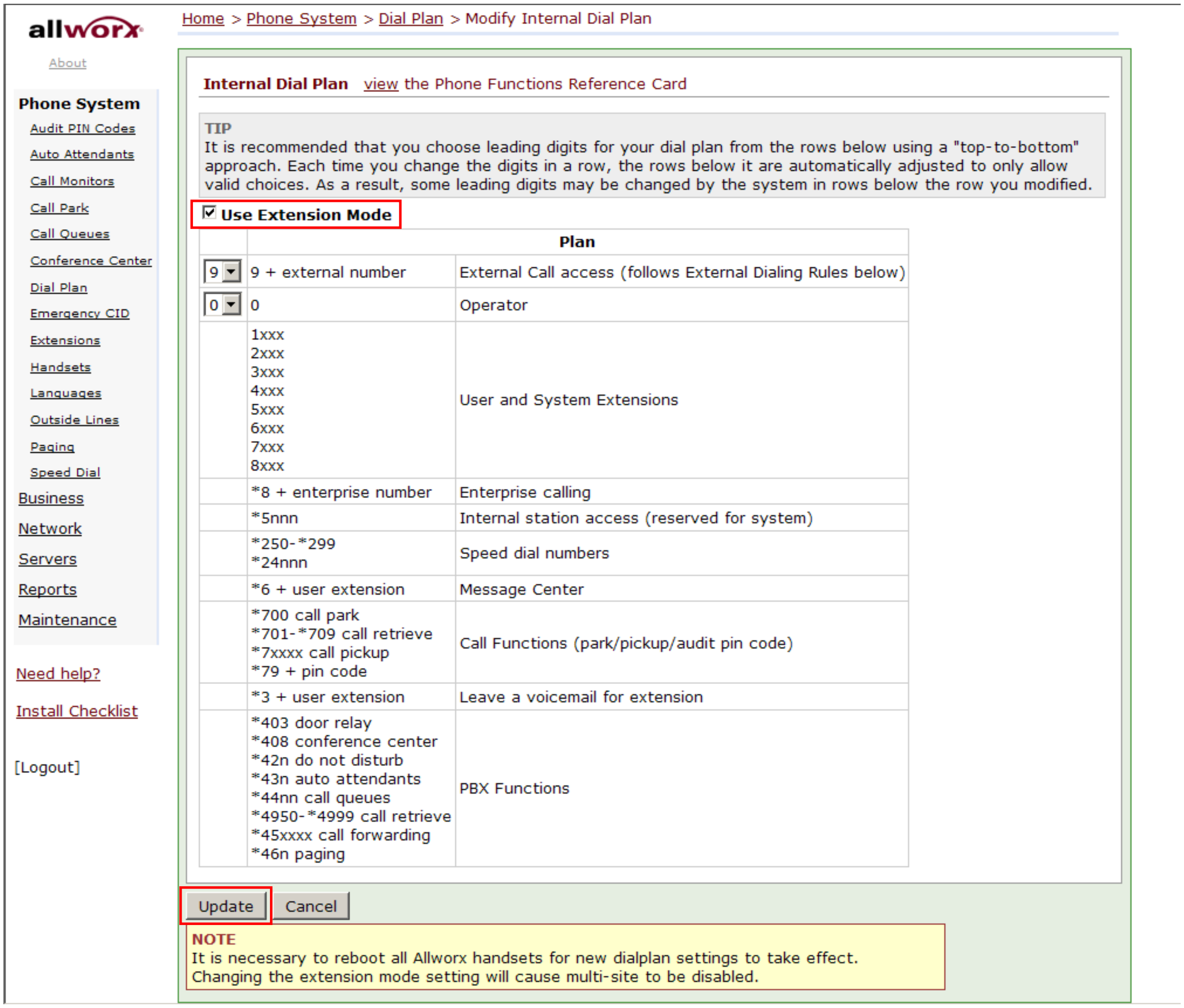
Navigate back to the **Home** page shown below and click the **Dial Plan** link under **Phone System**.



The following **Dial Plan** screen is displayed. Click the **modify** link next to **Internal Dial Plan**.



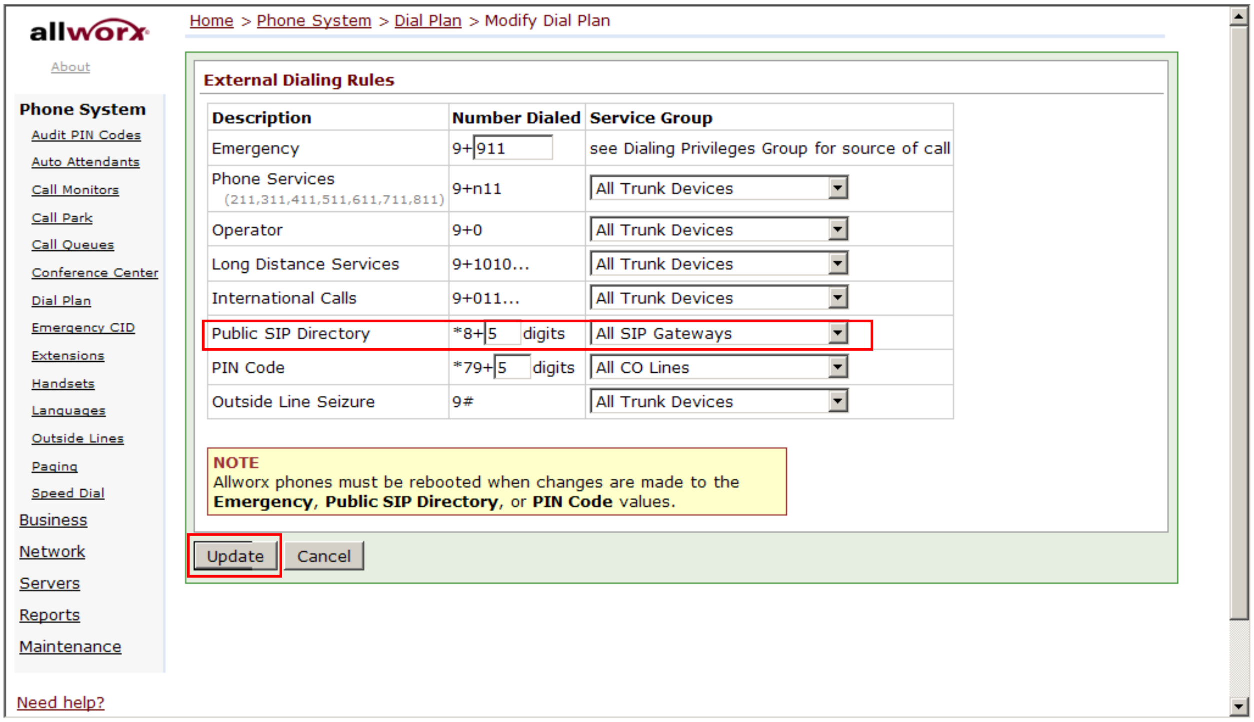
Verify the **Use Extension Mode** checkbox is checked. If it isn't, check it and click the **Update** button.



Back on the **Dial Plan** screen, under **External Dialing Rules**, click the **modify** link to edit the **Public SIP Directory**.

For the **Public SIP Directory** row, enter the number of digits (e.g. ***5***) in the **Number Dialed** column that will be used to dial enterprise Avaya phones. Select **All SIP Gateways** from the **Service Group** drop-down menu. Note, this row indicates that ****8*** followed by a ***5*** digit extension will be used to route calls from the Allworx IP Phones to the SIP Gateway (Session Manager).

Click the **Update** button.



8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Session Manager, the Allworx 6x system and Allworx IP Phones.

8.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify the status of the SIP signaling group by using the "status signaling-group n" command, where "n" is the signaling group number administered in **Section 5.5**. Verify that the signaling group is ***in-service*** as indicated in the **Group State** field shown below.

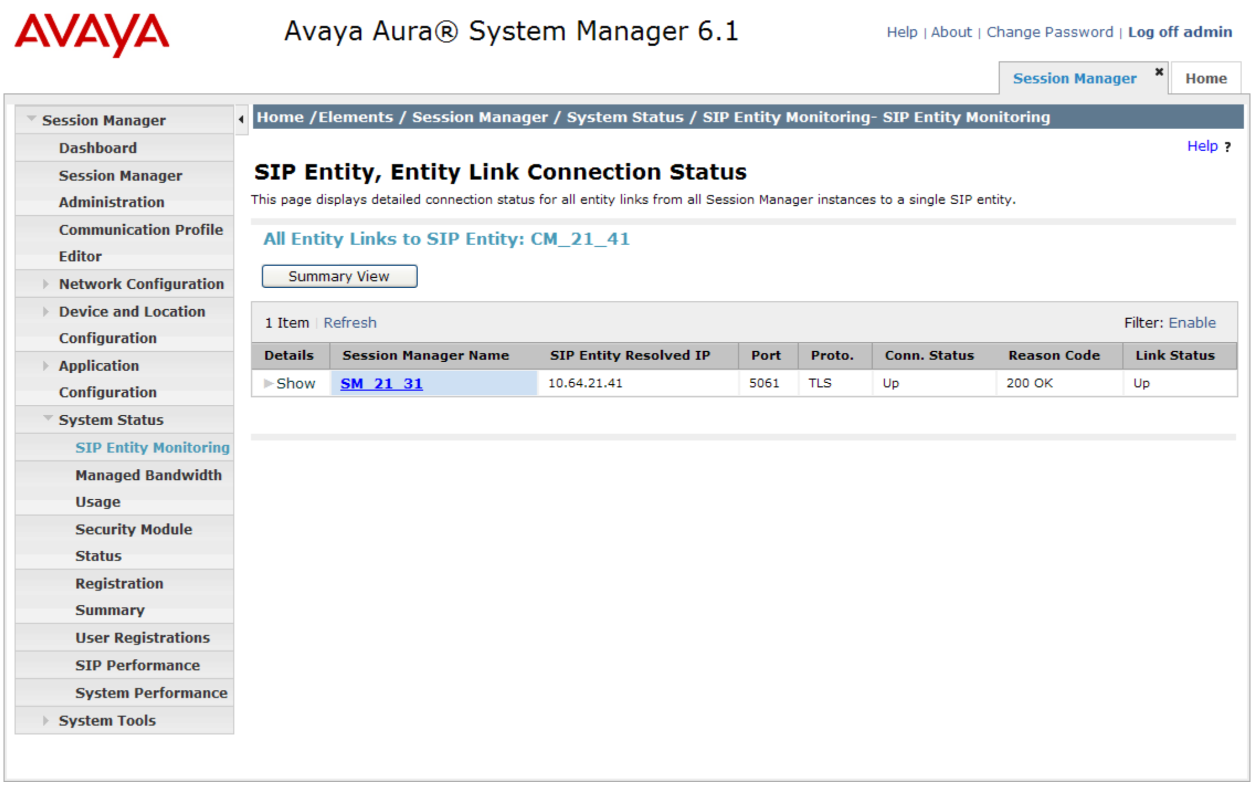
```
status signaling-group 1
                         STATUS SIGNALING GROUP

        Group ID: 1
      Group Type: sip

     Group State: in-service
```

Verify the status of the local SIP trunk group by using the "status trunk n" command, where "n" is the trunk group number administered in **Section 5.6**. Verify that all trunks are in the ***in-service/idle*** state as shown below.

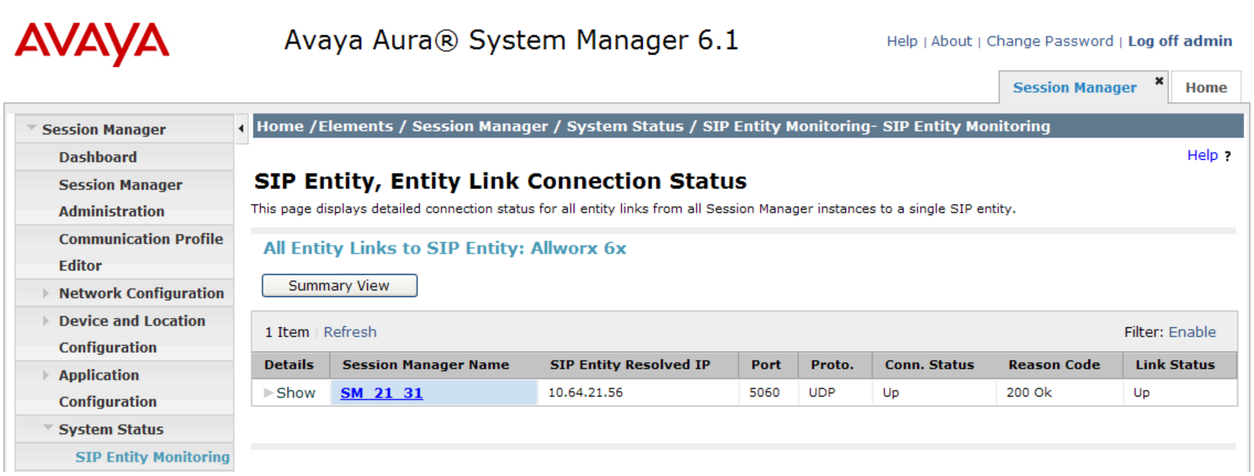
```
status trunk 1

                             TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy

0001/001 T00001   in-service/idle    no
0001/002 T00002   in-service/idle    no
0001/003 T00003   in-service/idle    no
0001/004 T00004   in-service/idle    no
0001/005 T00005   in-service/idle    no
0001/006 T00006   in-service/idle    no
0001/007 T00007   in-service/idle    no
0001/008 T00008   in-service/idle    no
0001/009 T00009   in-service/idle    no
0001/010 T00010   in-service/idle    no
```

8.2. Verify Avaya Aura® Session Manager

Navigate to **Home → Elements → Session Manager → System Status → SIP Entity Monitoring** and select the Communication Manager SIP Entity (not shown). Verify the **Conn. Status** and **Link Status** are ***Up***.



Repeat the procedure above selecting the Allworx 6x SIP Entity, and verify the **Conn. Status** and **Link Status** are ***Up***.



8.3. Verify Allworx 6x System and Allworx IP Phones

Make the following calls and verify the calls are set up properly, there is two-way audio with good audio quality, and the calls are torn down properly after completing the calls.

- Place a call from an Allworx IP Phone to an enterprise Avaya phone
- Place a call from an enterprise Avaya phone to an Allworx IP phone
- Place a call from an Allworx IP Phone to the PSTN
- Place a call from the PSTN to an Allworx IP Phone

9. Conclusion

These Application Notes describe the configuration steps required for the Allworx 6x system with Allworx IP phones to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager via a SIP trunk. All feature and serviceability test cases were completed and passed with the exceptions/observations noted in **Section 2.2**.

10. Additional References

This section references the product documentation relevant to these Application Notes.

1. *Administering Avaya Aura® Communication Manager*, Document 03-300509, Issue 6.0, Release 6.0, August 2010, available at http://support.avaya.com.
2. *Administering Avaya Aura® Session Manager*, Document 03-603324, Issue 1.1, Release 6.1, October 2011, available at http://support.avaya.com

Allworx documentation is available at http://www.allworx.com/support/resources.aspx.

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.