Avaya Solution & Interoperability Test Lab

Application Notes for Configuring DuVoice DV2000 with Avaya Aura® Session Manager and Avaya Aura® Communication Manager – Draft 0.1

Abstract

These Application Notes contains interoperability instructions for configuring DuVoice DV2000 with Avaya Aura® Session Manager and Avaya Aura® Communication Manager. Compliance testing was conducted to verify the interoperability.

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

This application notes contain instruction for configuring DuVoice DV2000 with Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and various Avaya endpoints. In the compliance testing SIP trunks were used in between the DuVoice DV2000 Voice Messaging System and Avaya Aura® Session Manager.

DuVoice DV2000 is a hospitality application that provides voicemail, automated attendant, and wake-up call features. The compliance testing focused on integrating the DuVoice DV2000 with Avaya Aura® Communication Manager and Aura® Session Manager.

2. General Test Approach and Test Results

The general test approach was to manually place intra-switch calls and inbound trunk calls that were ultimately answered by the DuVoice DV2000. Depending on the type of call, the user then had the option to leave a voicemail message, retrieve a voicemail message, schedule a wake-up call or transfer to another extension. All inbound calls were routed by Communication Manager to the DuVoice DV2000 hunt group via Session Manager, which were answered by the DV2000 with the automated attendant greeting. Internal calls that were unanswered were covered to the DV2000 hunt group. The DV2000 would answer these calls with the voice mailbox greeting of the subscriber extension. Lastly, internal calls placed to the DV2000 directly were answered by the DV2000 with the voicemail menu of the originating extension with an option to retrieve messages. For serviceability testing, the DV2000 and Communication Manager were each restarted separately.

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 testing included feature and serviceability testing.
The feature testing focused on exercising the core features of the DV2000 to validate the integration interface to Session Manager using SIP Trunks. This included the automated attendant, voicemail, wakeup call and performing guest check-in and checkout using the Room Status Monitor functionality. The serviceability testing introduced failure scenarios to verify operation of the DuVoice DV2000 after failure recovery.

2.2. Test Results

All executed test cases were passed.

2.3. Support

3. Reference Configuration

Test configuration used during compliance testing consisted of following:

- Avaya G450 Media Gateway with Avaya 8300D Media Server running Avaya Aura® Communication Manager
- Avaya Aura® Session Manager
- Avaya Aura® System Manager
- DuVoice DV2000 running on a Windows 7 Enterprise

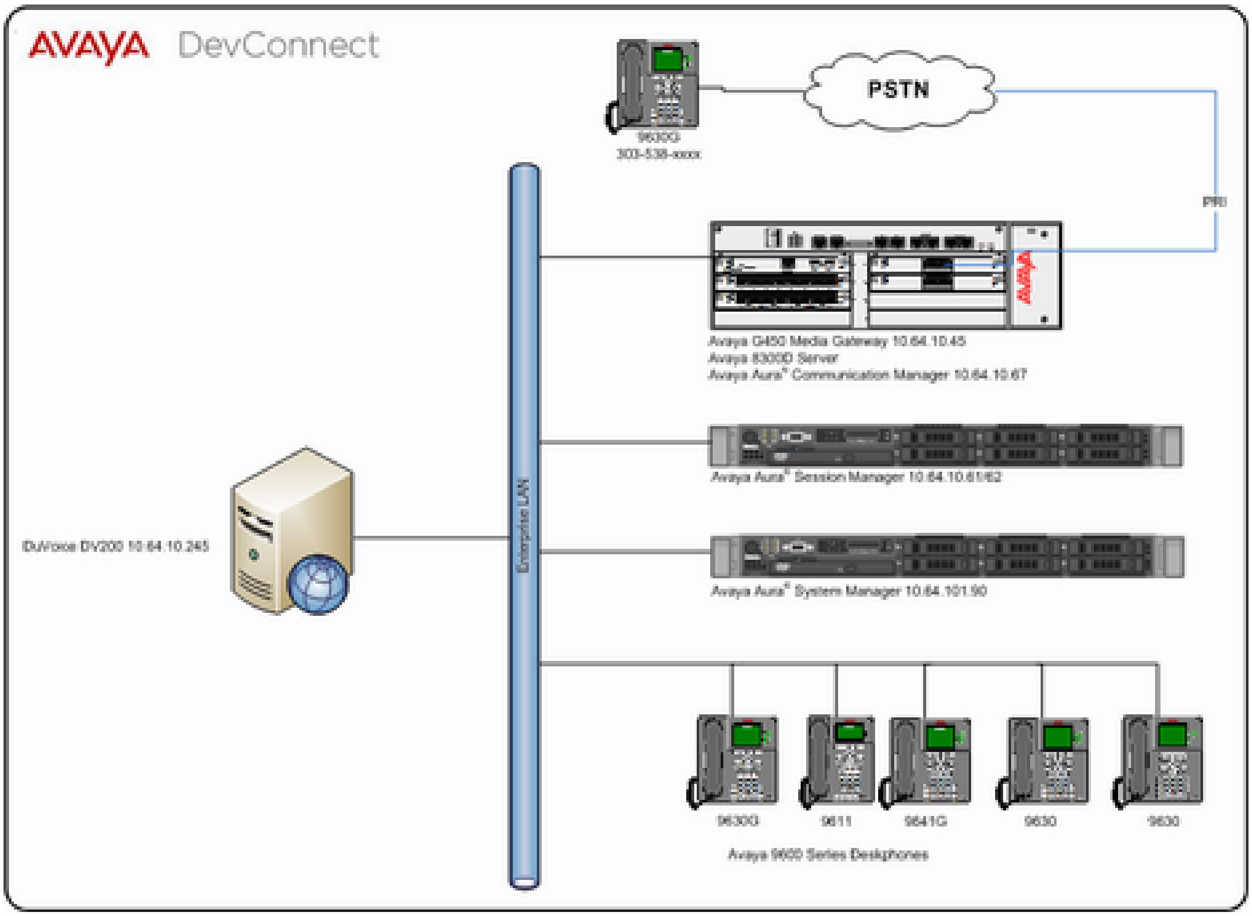


Figure 1: Reference Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on Avaya S8300D Server	6.2 SP5
Avaya Aura® Session Manager	6.3 SP5
Avaya Aura® System Manager	6.3 SP4
DuVoice DV2000 running on Windows Server 2008 R2	?

5. Configure Avaya Aura® Communication Manager

This section provides steps for configuring Communication Manager. All configuration for Communication Manager is done through System Access Terminal (SAT).

5.1. Administer IP Network Region

Use the **change ip-network-region *n*** command to configure a network region, where ***n*** is an existing network region.

Configure this network region as follows:

- Set **Location** to **1**
- Set **Codec Set** to **1**
- Set **Intra-region IP-IP Direct Audio** to **yes**
- Set **Inter-region IP-IP Direct Audio** to **yes**
- Enter and **Authoritative Domain**, e.g. avaya.com

```
change ip-network-region 1                                        Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       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
```

5.2. Administer IP Codec Set

Use the **change ip-codec-set *n*** command to configure IP codec set, where ***n*** is an existing codec set number.

Configure this codec set as follows, on **Page 1**:

- Set **Audio Codec 1** to **G.711MU**

```
change ip-codec-set 1                                          Page   1 of   2

                          IP Codec Set

    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU          n          2        20
 2:
 3:
 4:
 5:
 6:
 7:


     Media Encryption
 1:
 2:
 3:
```

5.3. Administer IP Node Names

Use the **change node-names ip** command to add an entry for Session Manager. For compliance testing, **sm** and **10.64.10.61** entry was added.

```
change node-names ip                                           Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
default             0.0.0.0
msgsrvr             10.64.10.67
procr               10.64.10.67
procr6              ::
sm                  10.64.10.61
```

5.4. Administer SIP Signaling Group

Use the **add signaling-group *n*** command to add a new signaling group, where ***n*** is an available signaling group number.

Configure this signaling group as follows:

- Set **Group Type** to **sip**
- Set **Near-end Node Name** to **procr**
- Set **Far-end Node Name** to the configured Session Manager in **Section 5.4**, i.e. sm
- Set **Far-end Network region** to the configured region in **Section 5.2**, i.e. 1

- Enter a **Far-end Domain,** e.g. avaya.com

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

 Group Number: 1              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: sm
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                        Far-end Network Region: 1

Far-end Domain: avaya.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
```

Note: Signaling Group, Trunk Group and Route Pattern for simulated PSTN calls for inter-site calls over ISDN/PRI and SIP were pre-configured and are not shown in this document.

5.5. Administer SIP Trunk Group

Use the **add trunk-group *n*** command to add a trunk group, where ***n*** is an available trunk group number.

Configure this trunk group as follows, on **Page 1**:

- Set **Group Type** to **sip**
- Enter a **Group Name**, e.g. SM
- Enter a valid **TAC**, e.g. *001
- Set **Service Type** to **tie**
- Enter **Signaling Group** value to the signaling group configured in **Section 5.5**, i.e. 1
- Enter a desired number in **Number of Member** field

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

Group Number: 1                    Group Type: sip          CDR Reports: y
  Group Name: SM                        COR: 1        TN: 1        TAC: *001
   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: 25
```

On **Page 3**:

- Set **Number Format** to private

```
add trunk-group 1                                                  Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                         Maintenance Tests? y



                     Numbering Format: private
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n
```

5.6. Administer Route Pattern

Use the **change route-pattern *n*** command to configure a route pattern, where ***n*** is an available route pattern.

Configure this route pattern as follows:

- Type a name in **Pattern Name** field
- For line 1, set **Grp No** to the trunk group configured in **Section 5.6**, i.e. 1
- For line 1, set **FRL** to **0**

```
change route-pattern 1                                          Page   1 of   3
                    Pattern Number: 1   Pattern Name: Voice
                             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                                                              n   user
 2:                                                                     n   user
```

5.7. Administer Hunt Group

Use the **add hunt-group *n*** command to configure a hunt group, where ***n*** is an available hunt group number.

Configure the hunt group as follows:

- Type a descriptive name in **Group Name** field
- Type in a available extension number for **Group Extension**

```
add hunt-group 6                                                Page   1 of  60
                                  HUNT GROUP

            Group Number: 6                            ACD? n
              Group Name: DuVoice Voicemail          Queue? n
         Group Extension: 25099                     Vector? n
              Group Type: ucd-mia               Coverage Path:
                      TN: 1         Night Service Destination:
                     COR: 1                  MM Early Answer? n
           Security Code:              Local Agent Preference? n
 ISDN/SIP Caller Display:
```

5.8. Administer Coverage Path

Use the **add coverage path *n*** command to add a coverage path, where ***n*** is available coverage path number.

Configure the coverage path as follows:

- Under **COVERAGE POINTS**, for **Point1** type in the hunt group that was configured in previous section. e.g., h6, where h stands for hunt group and 6 is the hunt group number.

```
add coverage path 6                                        Page   1 of   1
                                 COVERAGE PATH

                   Coverage Path Number: 6
     Cvg Enabled for VDN Route-To Party? n        Hunt after Coverage? n
                       Next Path Number:          Linkage

COVERAGE CRITERIA
    Station/Group Status    Inside Call     Outside Call
             Active?             n              n
               Busy?             y              y
         Don't Answer?           y              y        Number of Rings: 2
                All?             n              n
 DND/SAC/Goto Cover?             y              y
   Holiday Coverage?             n              n


COVERAGE POINTS
    Terminate to Coverage Pts. with Bridged Appearances? n
  Point1: h6            Rng:    Point2:
  Point3:                       Point4:
  Point5:                       Point6:
```

5.9. Administer Private Numbering

Use the **change private-numbering 1** command to define the calling party number to send to Session Manager.

Configure private numbering as follows:

- Add entries for trunk group configured in **Section 5.6**

Note: For compliance testing, 5-digit hunt group extension 25099 routed over trunk groups 1 resulted in a 5-digit calling party number.

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

Ext Ext              Trk        Private          Total
Len Code             Grp(s)     Prefix           Len
 5  25099            1                           5     Total Administered: 1
                                                          Maximum Entries: 540
```

5.10. Administer AAR Analysis

Use the **change aar analysis *n*** command to configure routing for hunt group extension number ***n***. For compliance testing, hunt group extension 25099 was used for routing calls to DV2000.

- Set **Dialed String** to hunt group extension, e.g. 25099
- Set **Min** and **Max** to 5 for 5 digit extensions
- Set **Route Pattern** to pattern configured in **Section 5.7**, i.e. 1
- Set **Call Type** to **aar**

Note: An entry to dial plan will need to be added for extension range used in this step.

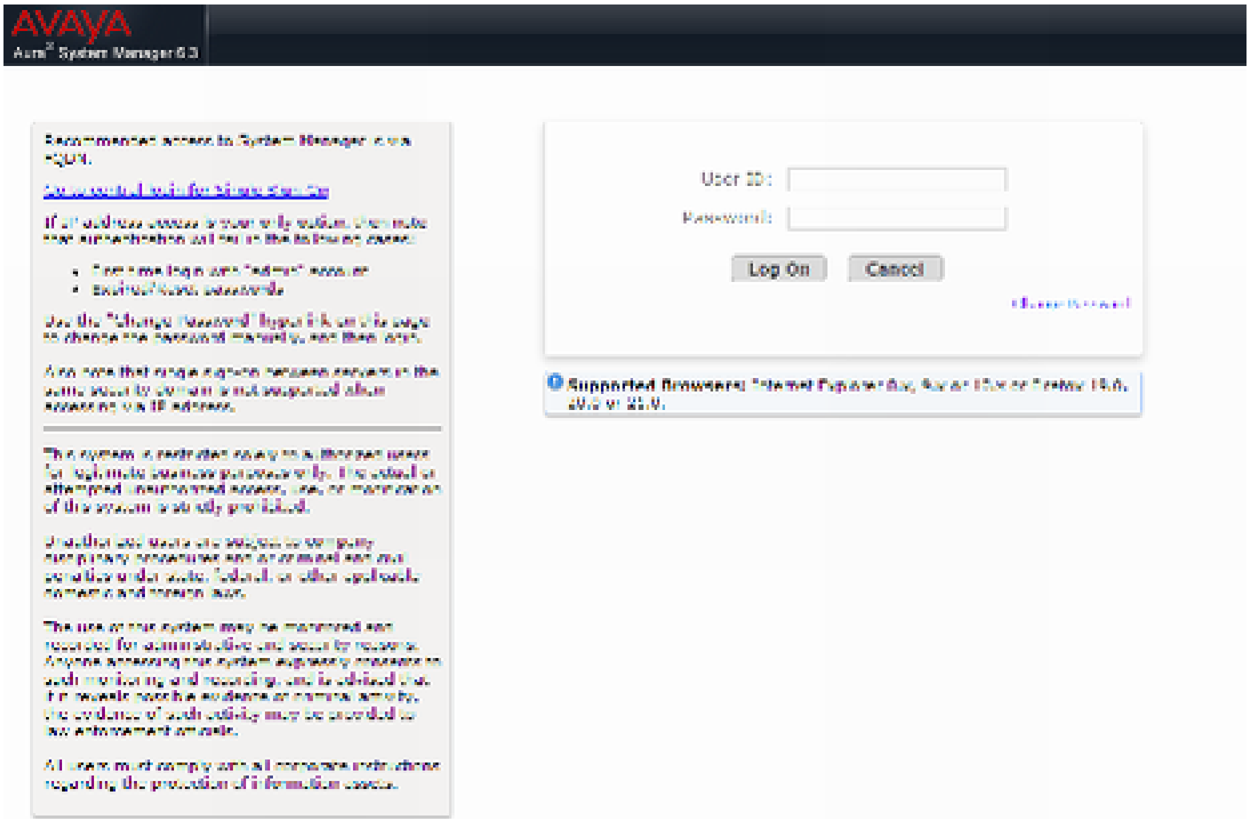
```
change aar analysis 25099                                      Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all           Percent Full: 2

          Dialed          Total     Route    Call   Node  ANI
          String         Min  Max  Pattern   Type   Num   Reqd
    25099                 5    5     1       aar          n
    252                   5    5     2       aar          n
    257                   5    5     10      aar          n
    258                   5    5     10      aar          n
    25990                 5    5     13      aar          n
    25999                 5    5     98      aar          n
    26                    5    5     10      aar          n
    27                    5    5     21      aar          n
    275                   5    5     10      aar          n
```

5.11. Administer Stations

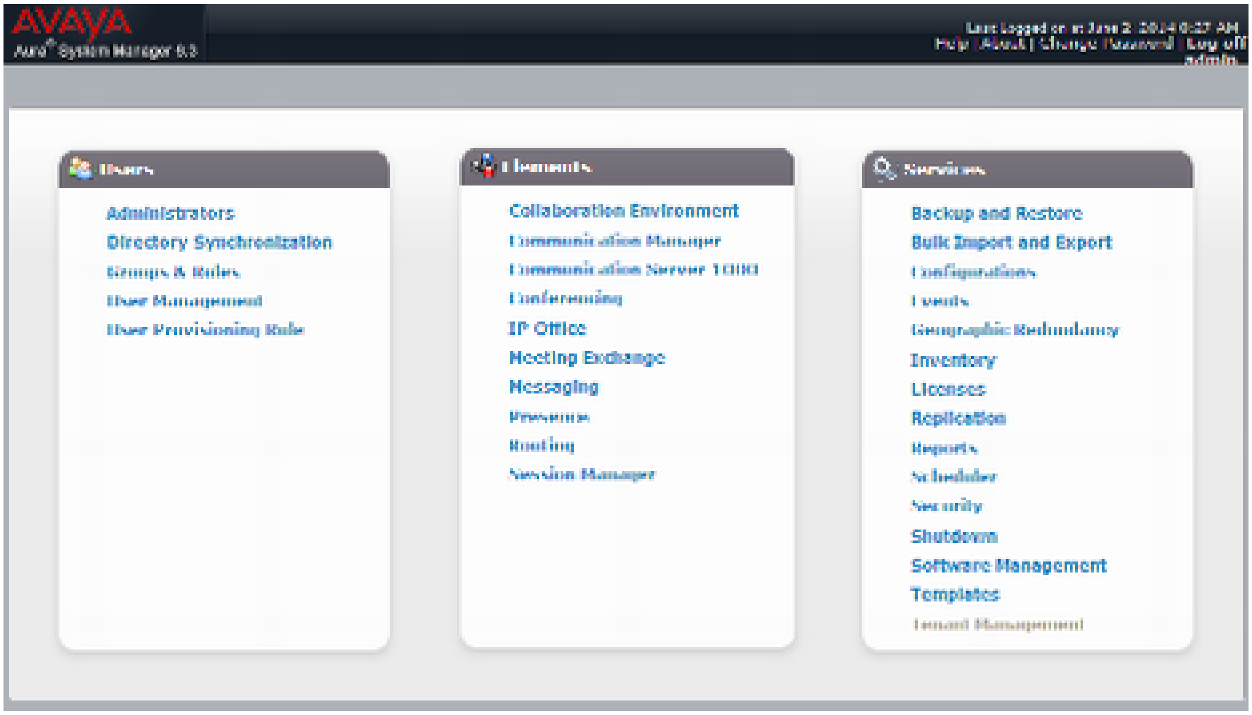
Administration of Avaya Stations/Extensions in Communication Manager and Session Manager is not shown in this document. Please refer to document [1] and/or [2] in reference section of this document.

6. Configure Avaya Aura® Session Manager

Configuration of Avaya Aura® Session Manager is performed via Avaya Aura® System Manager. Access the System Manager Administration web interface by entering https://<ip-address>/SMGR URL in a web browser, where <ip-address> is the IP address of System Manager.



Log in using appropriate credentials.

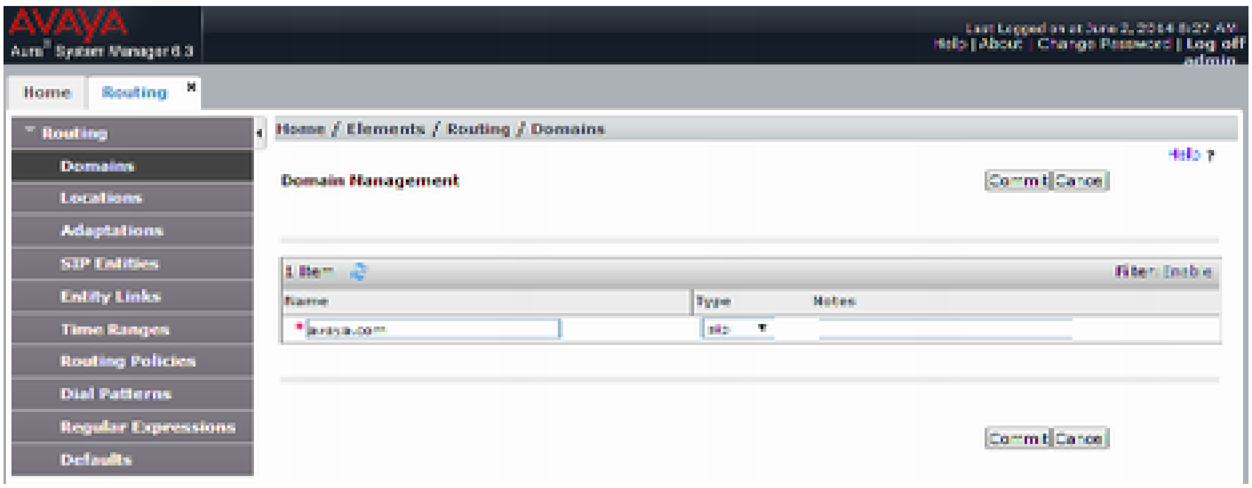


6.1. Add SIP Domain

Navigate to **Home → Elements → Routing → Domains**, click on **New** button (not shown) and configure as follows:

- In **Name** field type in a domain (authoritative domain used in **Section 5**) i.e. avaya.com
- Set **Type** to **sip**

Click **Commit** to save changes.



6.2. Add Location

Navigate to **Home → Elements → Routing → Location**, click on **New** button (not shown) and configure as follows:

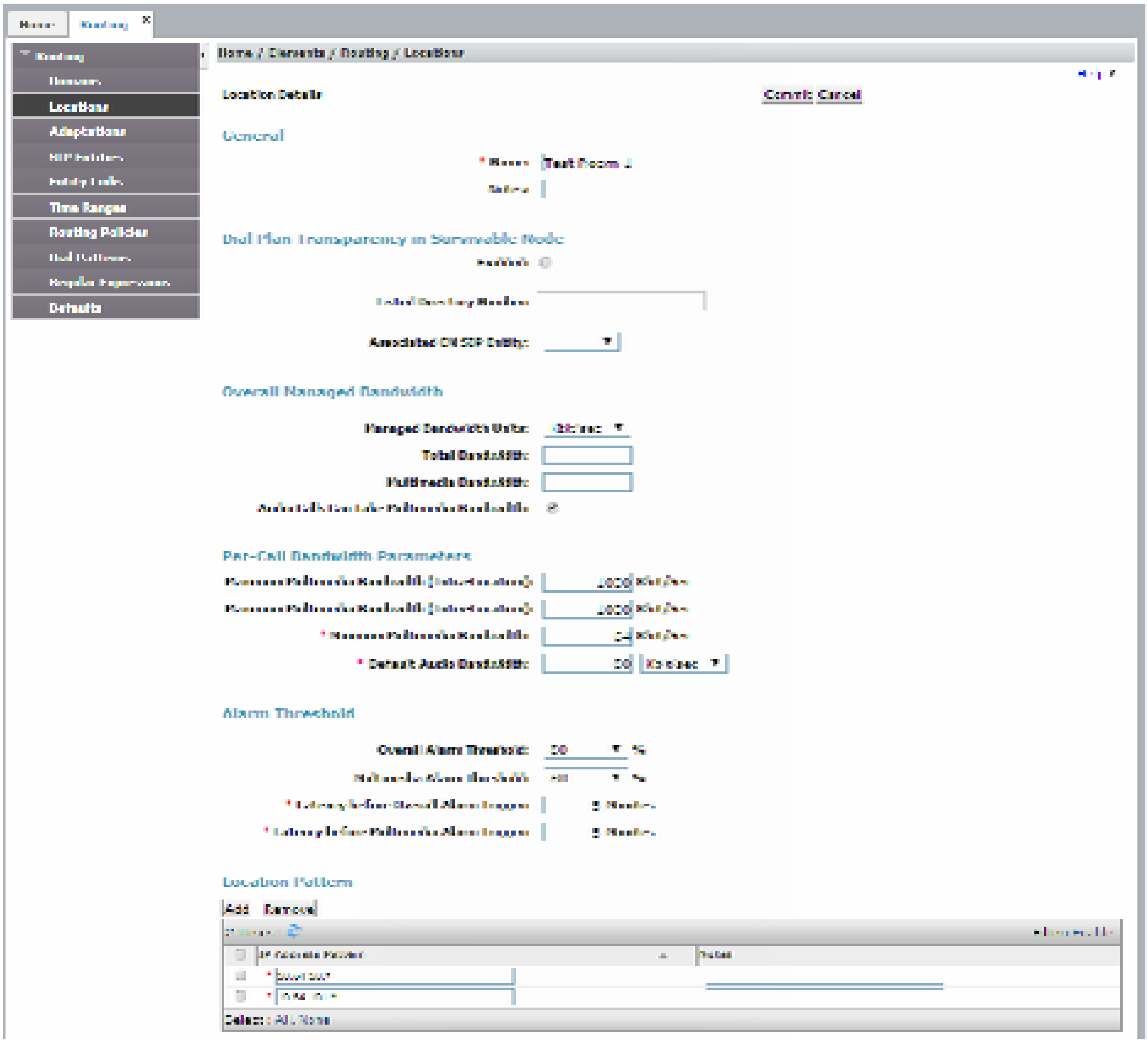
Under **General**:

- Type in a descriptive **Name**

Under **Location Pattern** click on **New** (not shown):

- Type in an **IP Address Pattern**, e.g.10.64.10.*

Click **Commit** to save changes. Screen shot shown on next page.


Home / Elements / Routing / Locations
Locations
Adaptations
Time Ranges
Routing Policies
Defaults
Location Details
Commit Cancel
General
Dial Plan Transparency in Survivable Mode
Associated CM SIP Entity:
Overall Managed Bandwidth
Managed Bandwidth Units:
Total Bandwidth:
Multimedia Bandwidth:
Per-Call Bandwidth Parameters
Default Audio Bandwidth:
Alarm Threshold
Overall Alarm Threshold:
Location Pattern
Add
Remove
Select : All, None

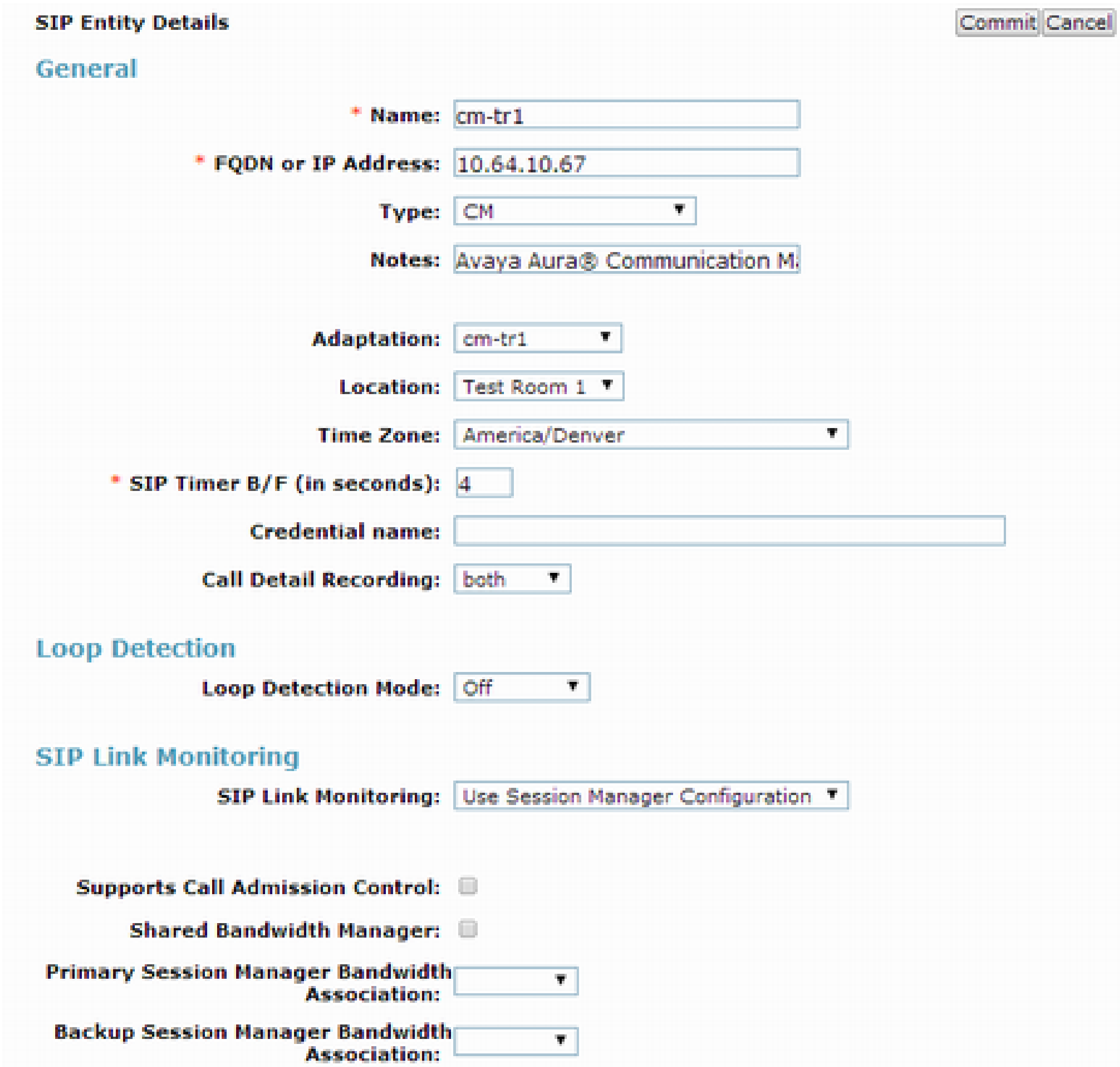
6.3. Add SIP Entity – Communication Manager

Add Communication Manager as a SIP Entity. Navigate to **Home → Elements → Routing → SIP Entities,** click on **New** (no shown) and configure as follows:

- Type in a descriptive name in **Name** field
- Type in the IP address or FQDN of Communication Manager in **FQDN or IP Address** field.
- Set **Type** to **CM**
- Set **Location** to the location configured in **Section 6.2**

Click **Commit** to save changes.

Note: It is assumed that SIP Entity for Session Manager has been already configured.

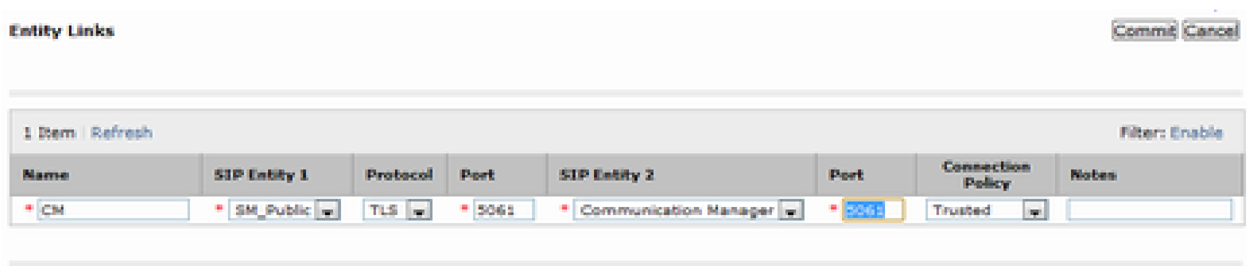

SIP Entity Details
Commit
Cancel
General
* Name: cm-tr1
* FQDN or IP Address: 10.64.10.67
Type: CM
Notes: Avaya Aura® Communication M
Adaptation: cm-tr1
Location: Test Room 1
Time Zone: America/Denver
* SIP Timer B/F (in seconds): 4
Credential name:
Call Detail Recording: both
Loop Detection
Loop Detection Mode: Off
SIP Link Monitoring
SIP Link Monitoring: Use Session Manager Configuration
Supports Call Admission Control:
Shared Bandwidth Manager:
Primary Session Manager Bandwidth Association:
Backup Session Manager Bandwidth Association:

6.4. Add Entity Link – Communication Manager

Navigate to **Home → Elements → Routing → Entity Links**, click on **New** (not shown) and configure as follows:

- Type in a descriptive name in **Name** field
- Set **SIP Entity 1** to the name of Session Manager SIP Entity
- Set **SIP Entity 2** to Communication Manager SIP Entity configured in **Section 6.3**

Click **Commit** to save changes.



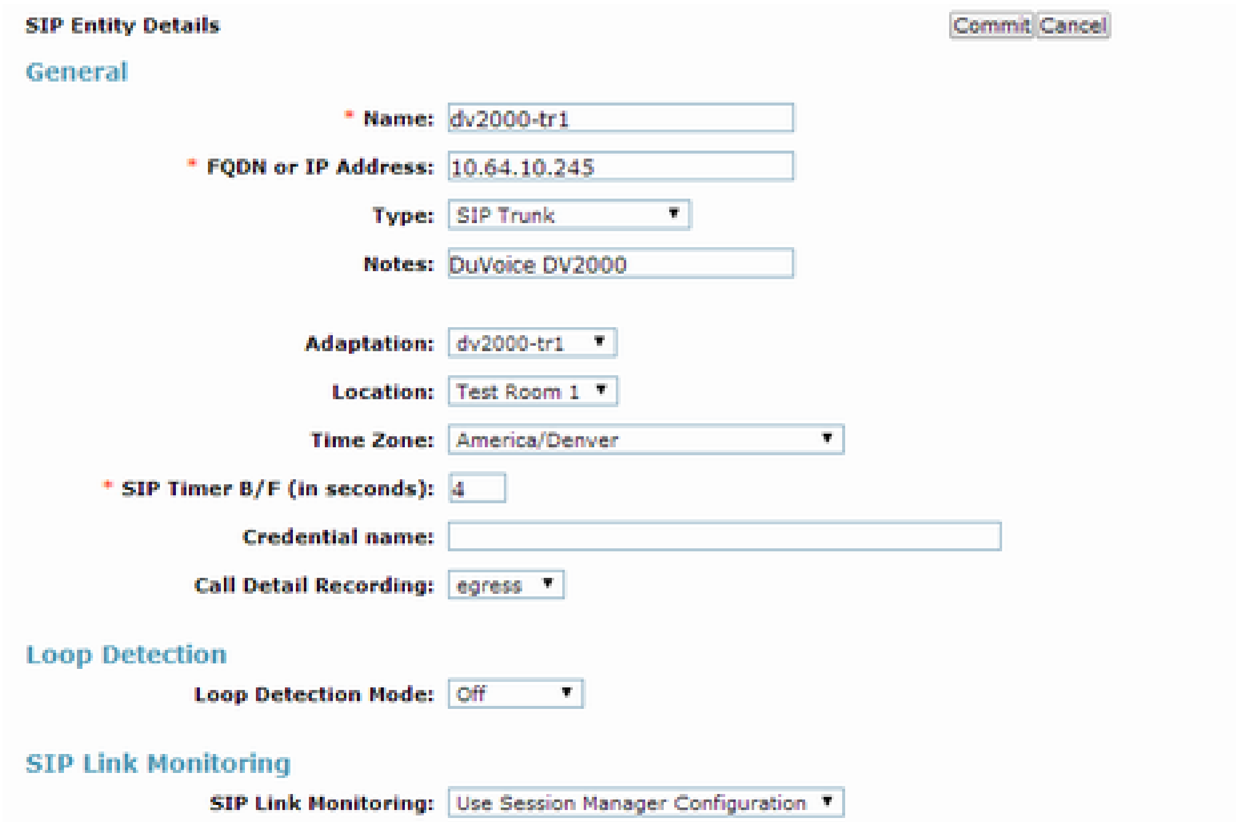
6.5. Add SIP Entity – DuVoice

Add Communication Manager as a SIP Entity. Navigate to **Home → Elements → Routing → SIP Entities,** click on **New** (no shown) and configure as follows:

- Type in a descriptive name in **Name** field
- Type in the IP address or FQDN of DuVoice DV2000 in **FQDN or IP Address** field.
- Set **Type** to **SIP Trunk**
- Set **Location** to the location configured in **Section 6.2**

Click **Commit** to save changes.

Note: It is assumed that SIP Entity for Session Manager has been already configured.

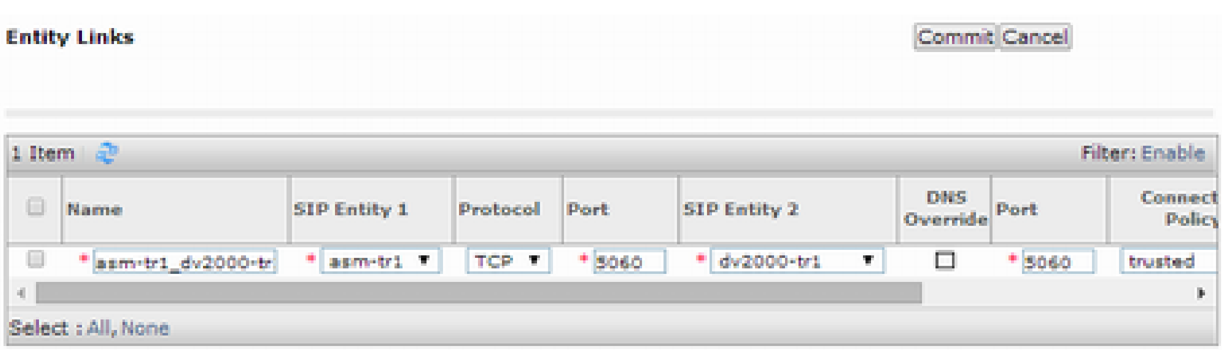


6.6. Add Entity Link – DuVoice

Navigate to **Home → Elements → Routing → Entity Links**, click on **New** (not shown) and configure as follows:

- Type in a descriptive name in **Name** field
- Set **SIP Entity 1** to the name of Session Manager SIP Entity
- Set **SIP Entity 2** to DuVoice DV2000 SIP Entity configured in **Section 6.5**
- Set **Protocol** to **UDP**

Click **Commit** to save changes.

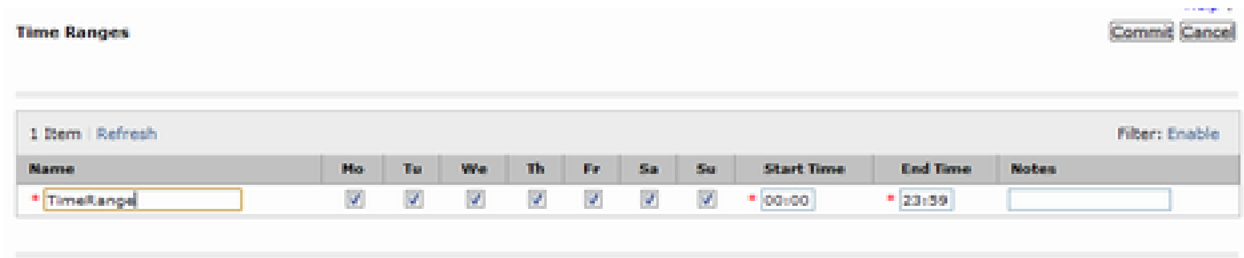


6.7. Add Time Ranges

Navigate to **Home → Elements → Routing → Time Ranges**, click on **New** (now shown) and configure as follows:

- Type in a descriptive name in **Name** field

Click **Commit** to save changes.

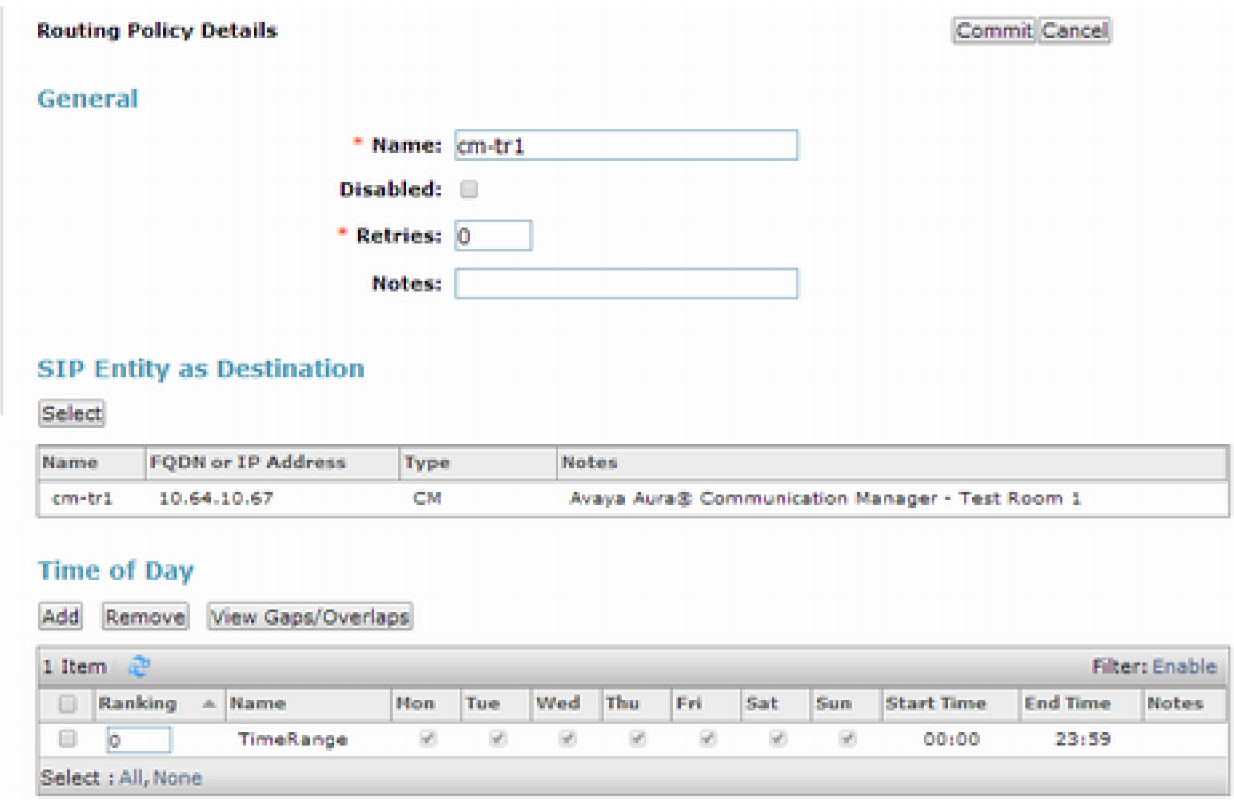


6.8. Add Routing Policy – Communication Manager

Navigate to **Home → Elements → Routing → Routing Policies**, click on **New** (not shown) and configure as follows:

- Type in a descriptive name in **Name** field
- Under **SIP Entity as Destination**, click on **Select** (not shown):
    - Select Communication Manager SIP entity added in **Section 6.3**
- Under **Time of Day**, click on **Add** (not shown):
    - Select time range added in previous step

Click **Commit** to save changes.

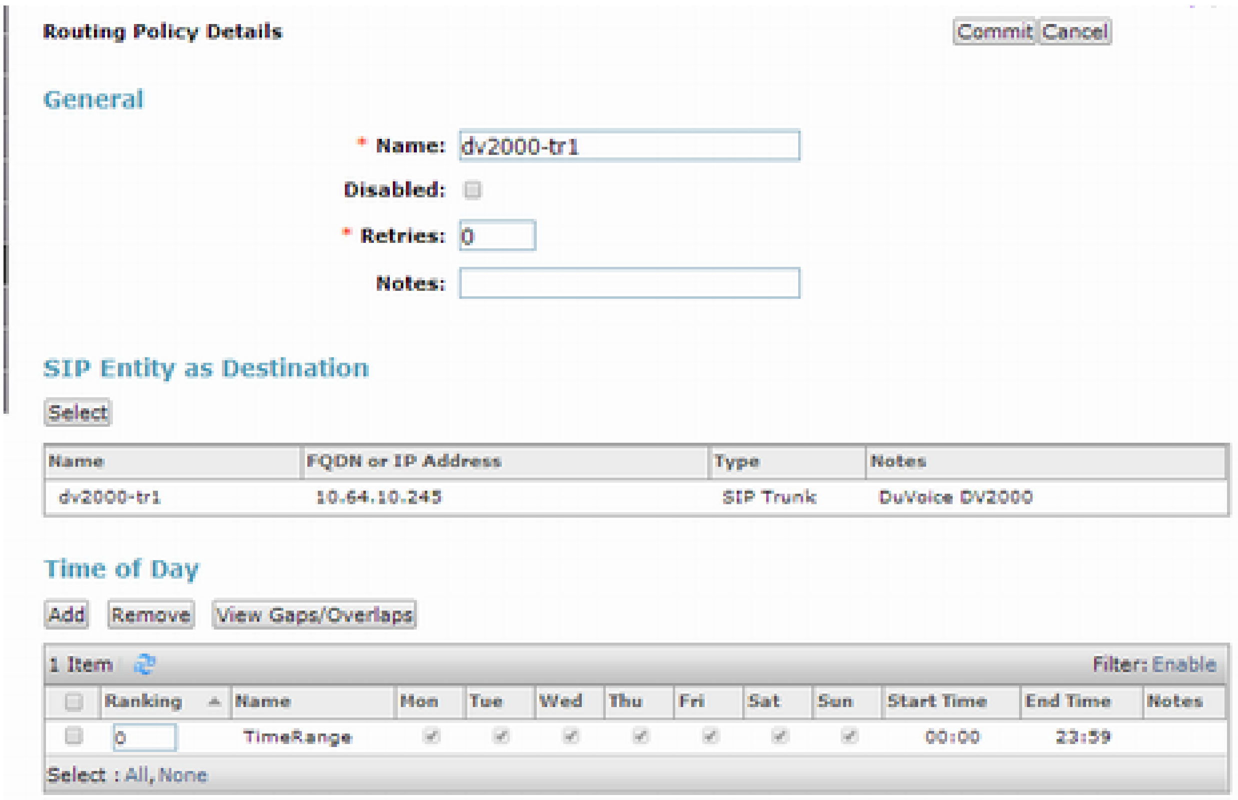


6.9. Add Routing Policy – DuVoice

Navigate to **Home → Elements → Routing → Routing Policies**, click on **New** (not shown) and configure as follows:

- Type in a descriptive name in **Name** field
- Under **SIP Entity as Destination**, click on **Select** (not shown):
    - Select DuVoice DV2000 SIP entity added in **Section 6.5**
- Under **Time of Day**, click on **Add** (not shown):
    - Select time range added in previous step

Click **Commit** to save changes.



6.10. Add Dial Patterns – Communication Manager

Navigate to **Home → Elements → Routing → Dial Patterns**, click on **New** (not shown) and configure as follows:

Under **General:**

- Set **Pattern** to prefix of dialed number
- Set **Min** to minimum length of dialed number
- Set **Max** to maximum length of dialed number
- Set **Domain** to domain configured on **Section 6.1**

Under **Originating Locations and Routing Policies:**

- Click **Add** and select originating location and Communication Manager routing policy as configured in **Section 6.8**

Click **Commit** to save changes.

Note: For Compliance testing, dialed number of 25xxx were used to route calls to Communication Manager. Thus, pattern, min and max values were all set to 5.

6.11. Add Dial Patterns – DuVoice

Navigate to **Home → Elements → Routing → Dial Patterns**, click on **New** (not shown) and configure as follows:

Under **General:**

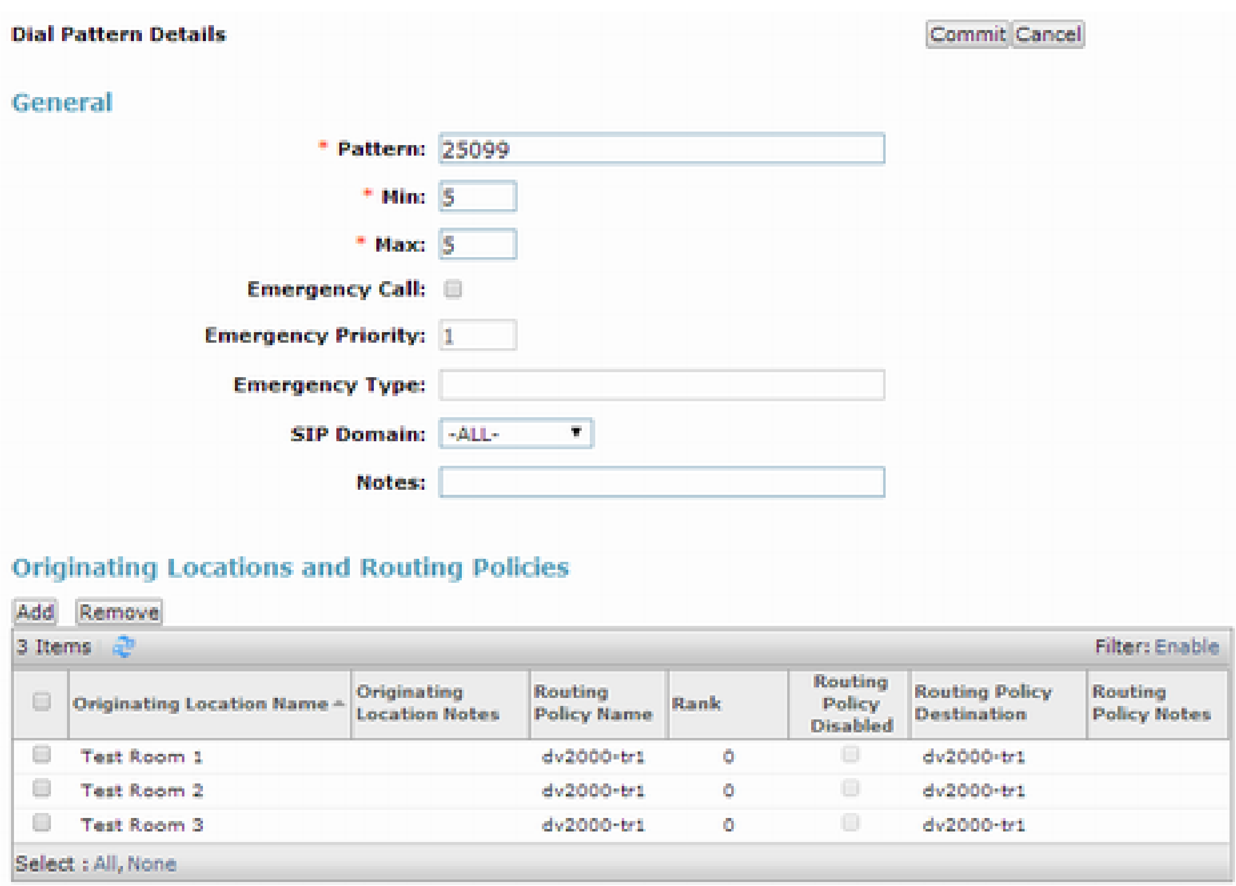
- Set **Pattern** to prefix of dialed number
- Set **Min** to minimum length of dialed number
- Set **Max** to maximum length of dialed number
- Set **Domain** to **–All-**

Under **Originating Locations and Routing Policies:**

- Click **Add** and select originating location and DuVoice DV2000 routing policy as configured in **Section 6.9**

Click **Commit** to save changes.

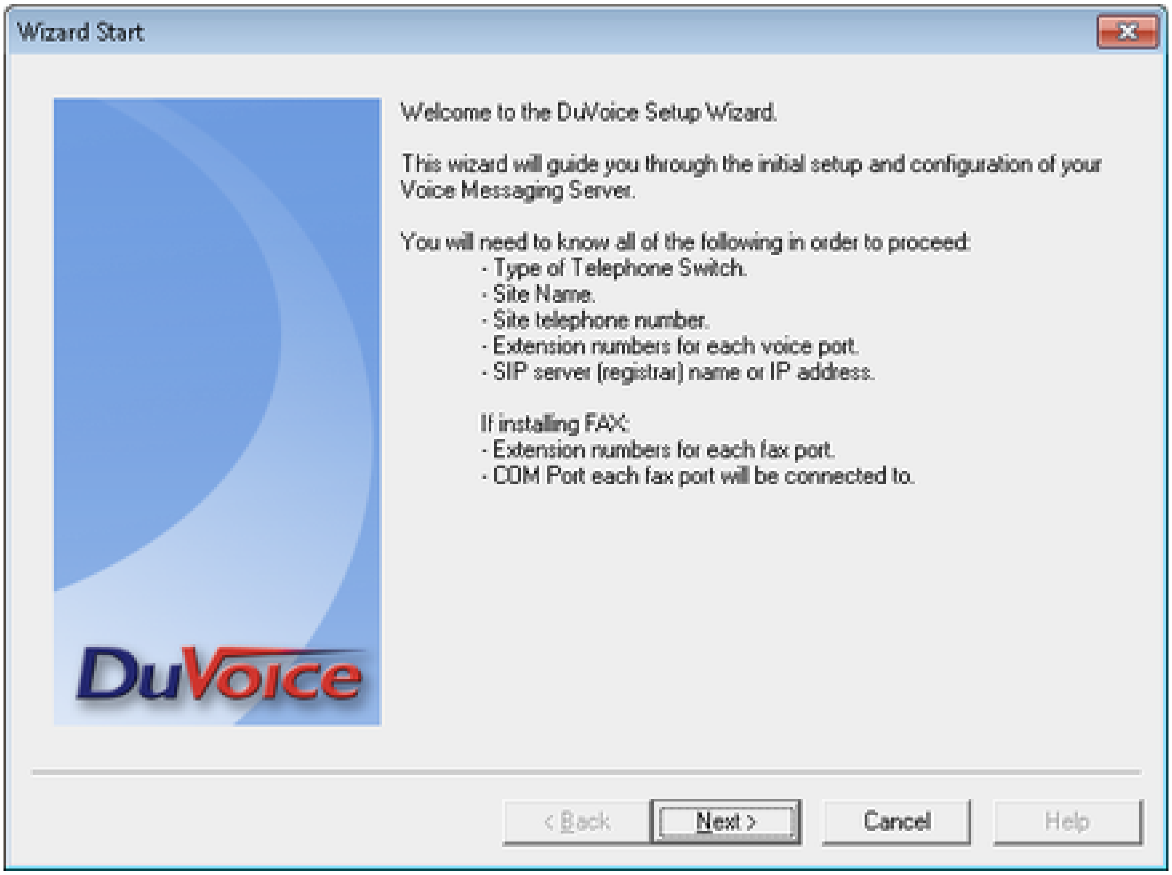
Note: For Compliance testing, dialed number of 25099 were used to route calls to DuVoice. Thus, pattern, min and max values were all set to 5.



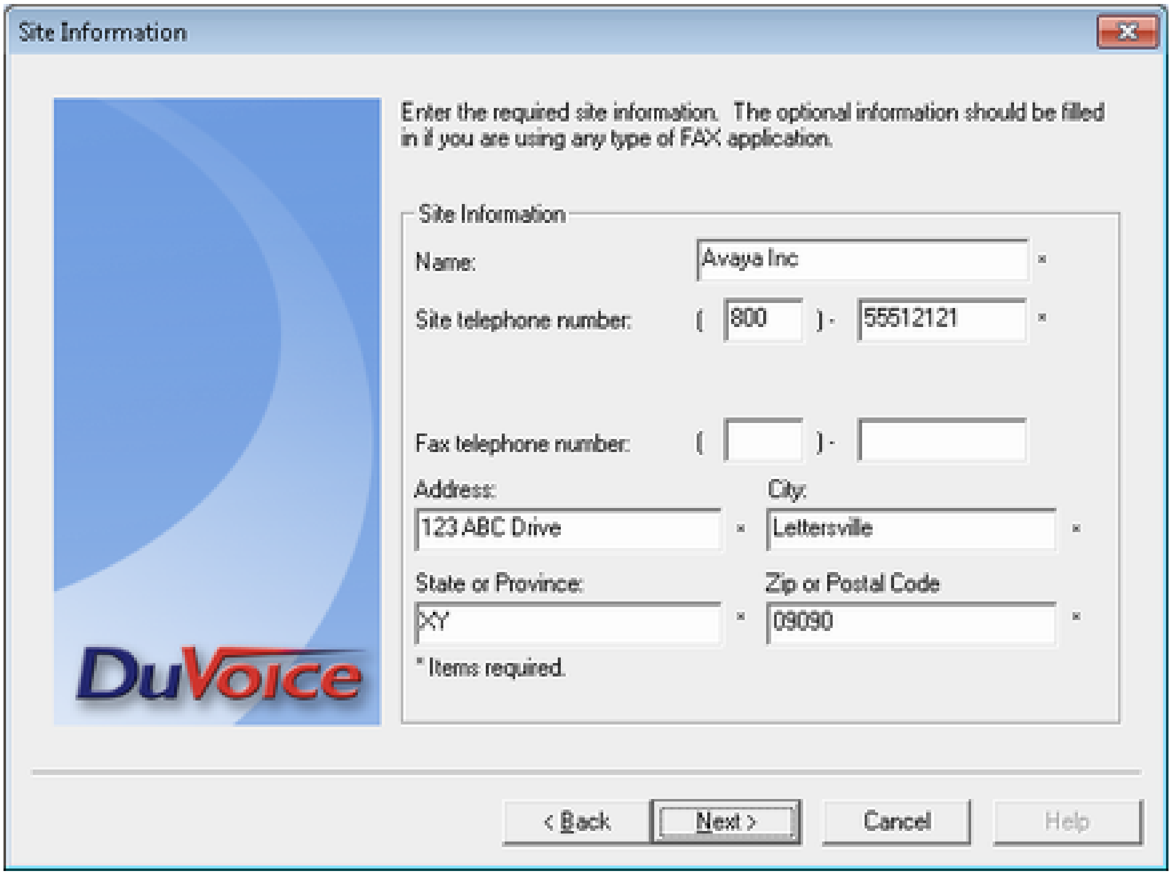
7. Configure DuVoice

To configure SIP connectivity to Session Manager, locate the SETUP.exe file for DuVoice DV2000 and open it.

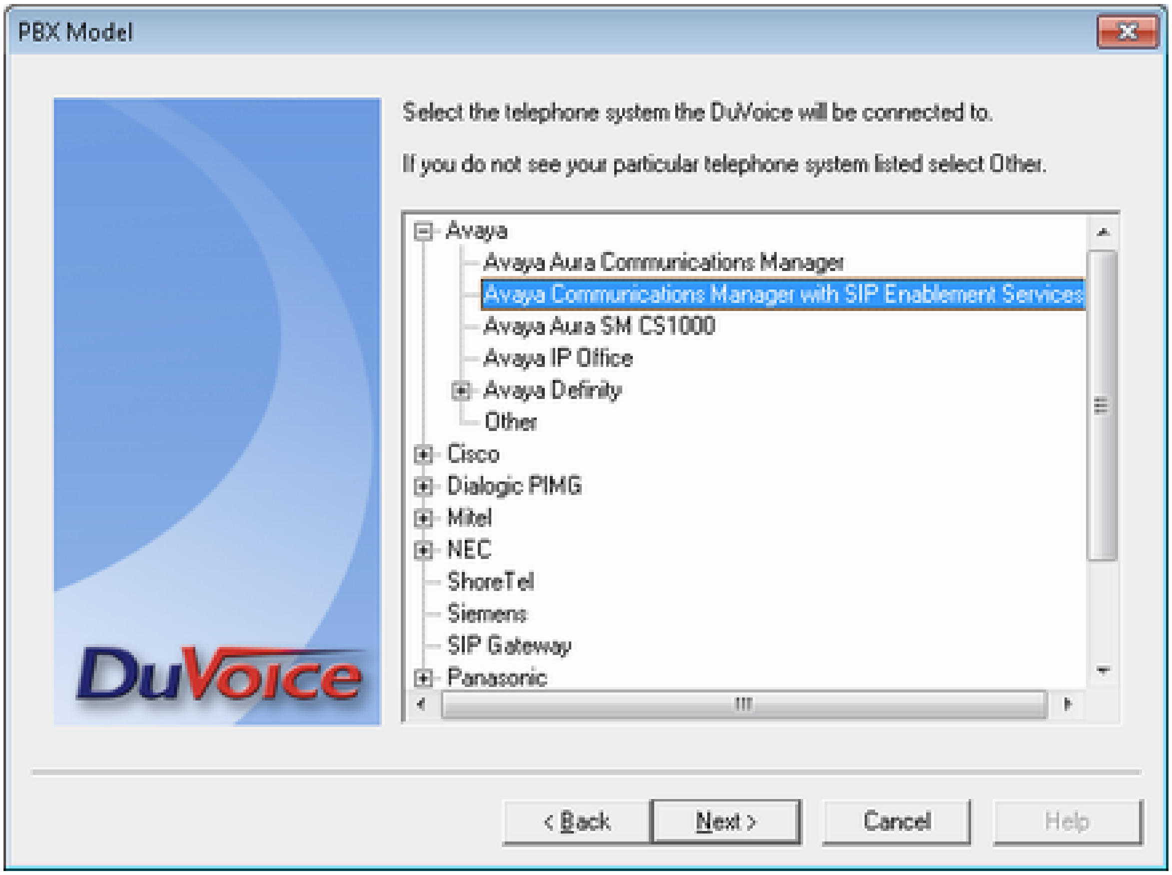
On the **Wizart Start** window select **Next**



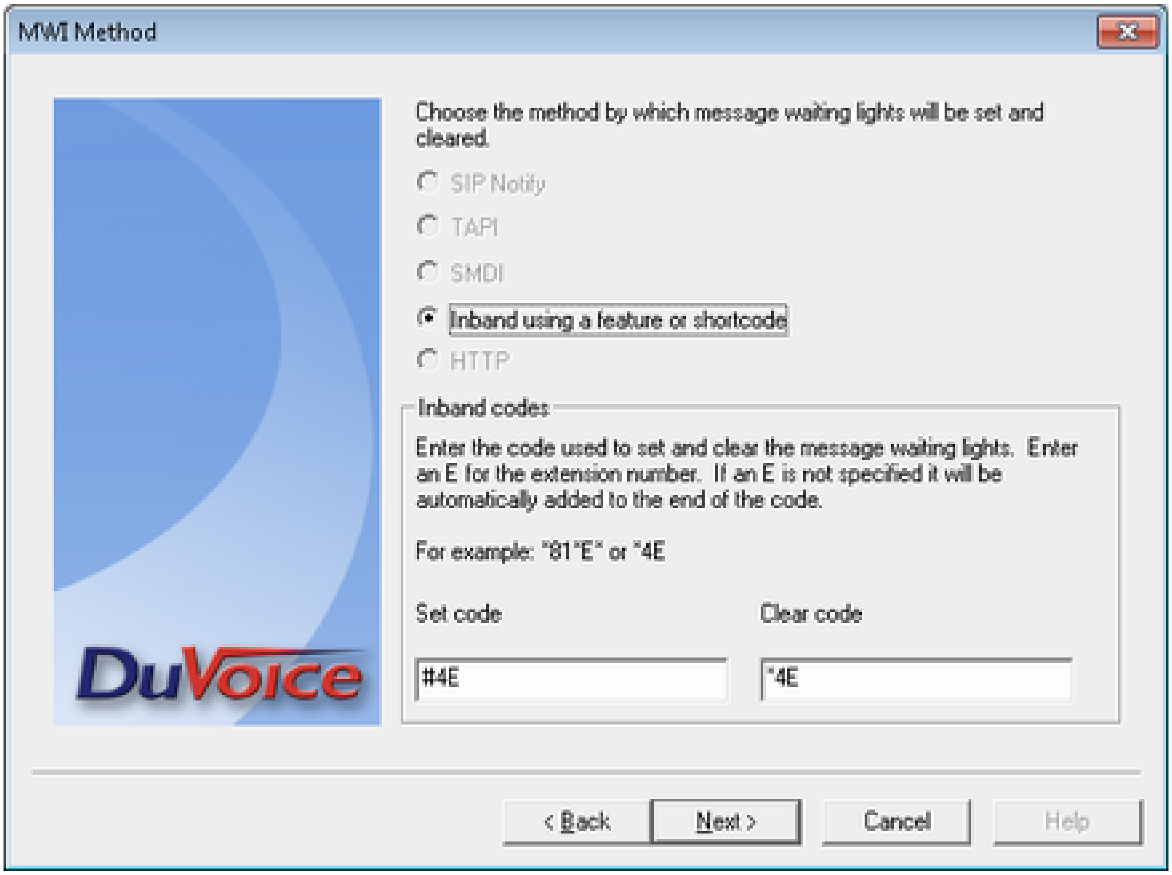
On the **Site Information** window, fill in the fields marked with * and click **Next**.



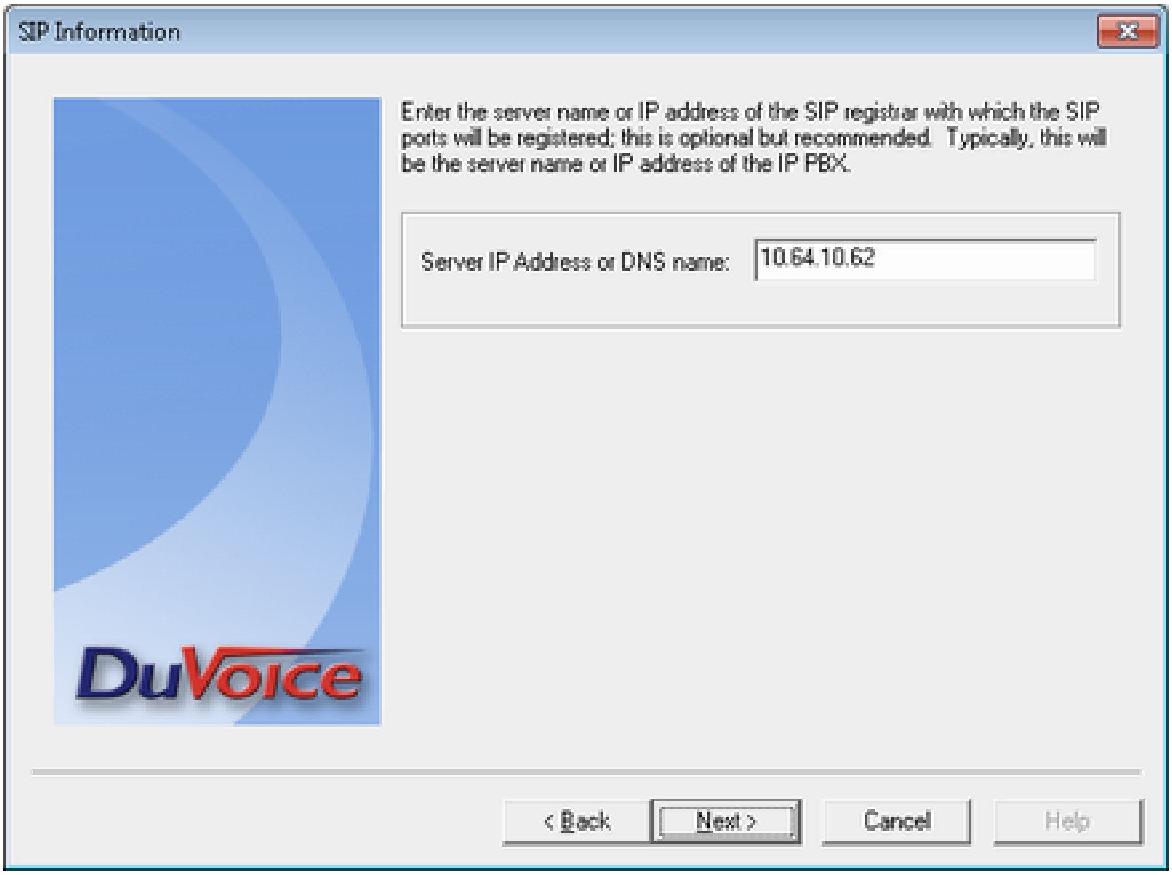
On the **PBX Model** window, select **Avaya → Avaya Communication Manager with SIP Enablement Services** and click **Next**.



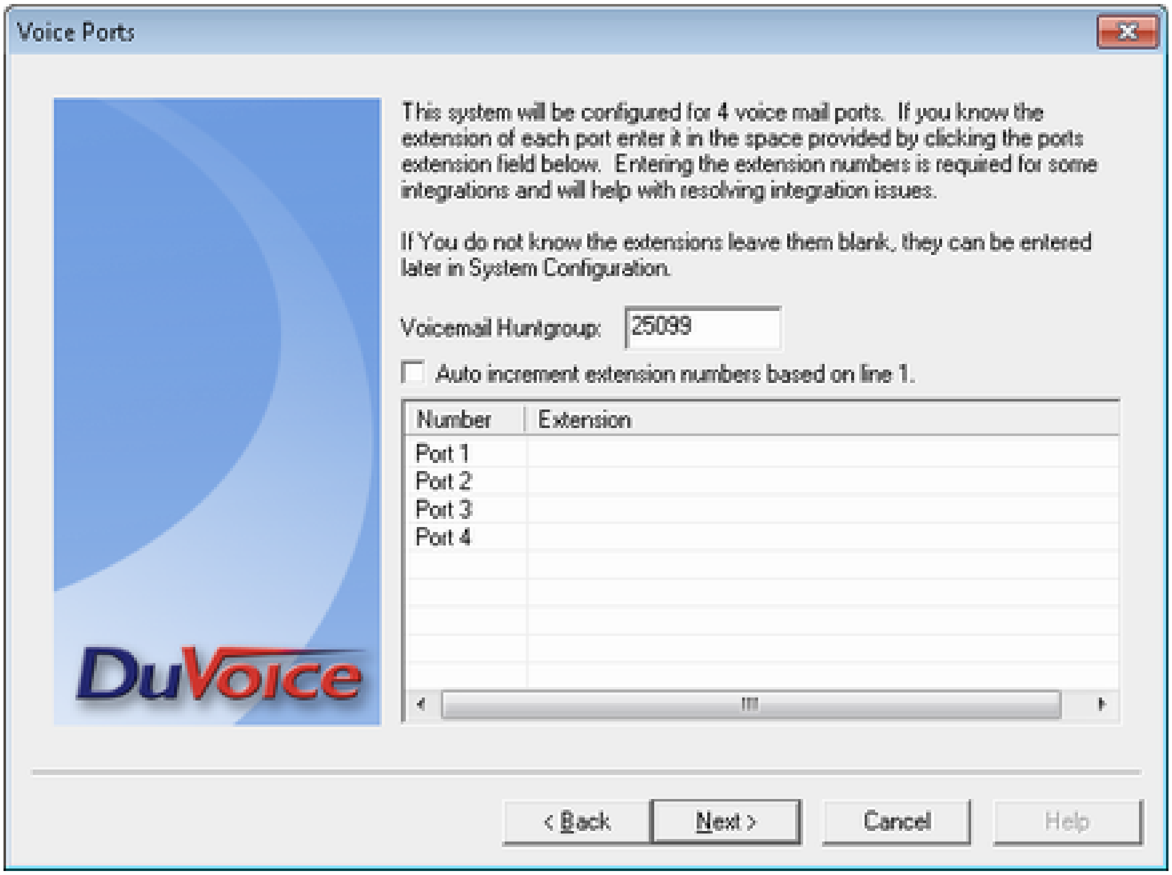
On the **MWI Method** window, accept the default values and click **Next**. Please note that MWI method will be changed to SIP in a later section.



On the **SIP Information** window, type in the Session Manager IP Address in **Server IP Address or DNS Name** field and click **Next.**



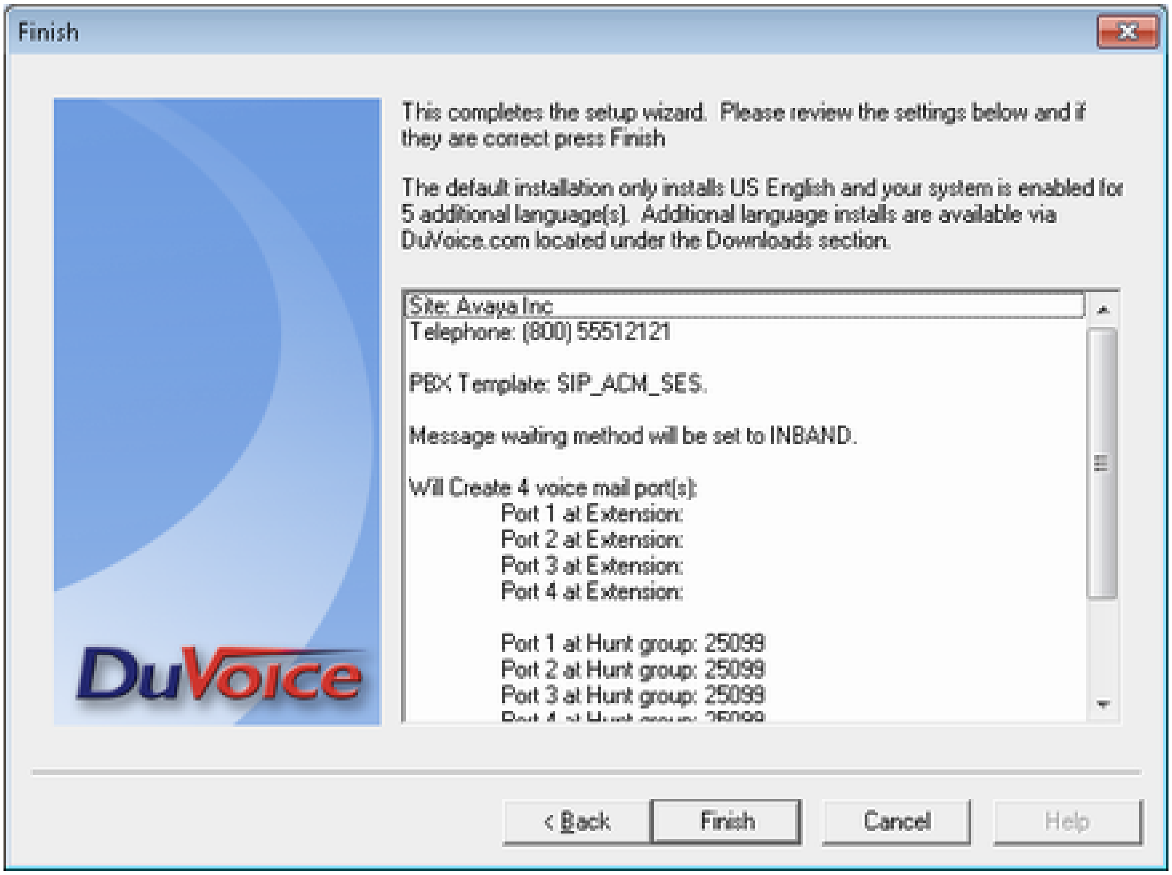
On the **Voice Ports** window, type in the Hunt Group that was configured in Communication Manager in **Voicemail Huntgroup** field.



Update:
Enter the huntgroup number in the extension field for each line.

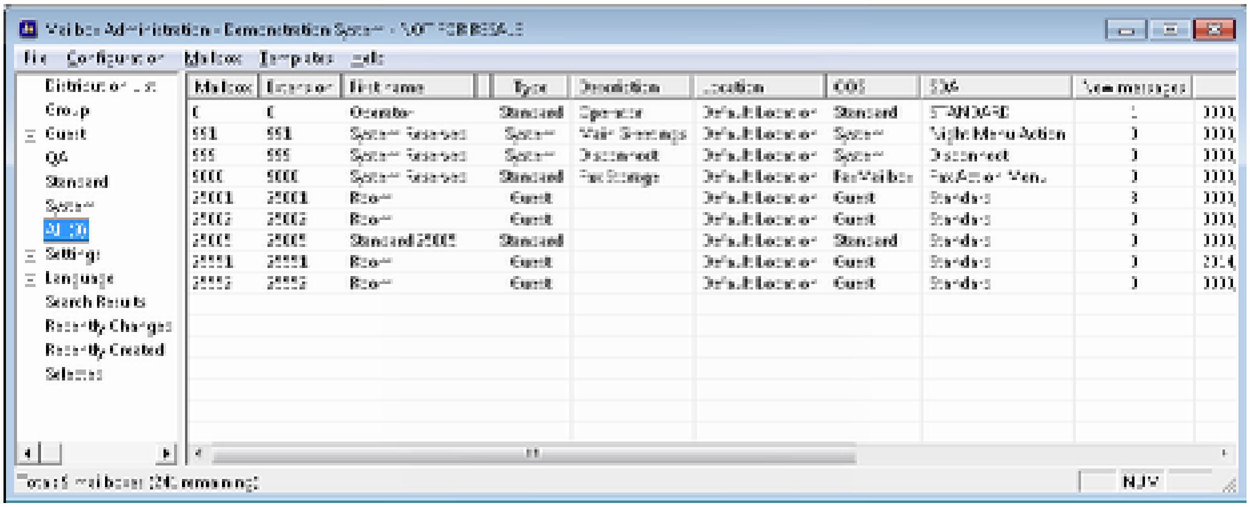
If this is not done, on some systems the PBX will give an error about the identity being wrong when callouts are attempted.

The final screen shows the configuration, click **Finish.**

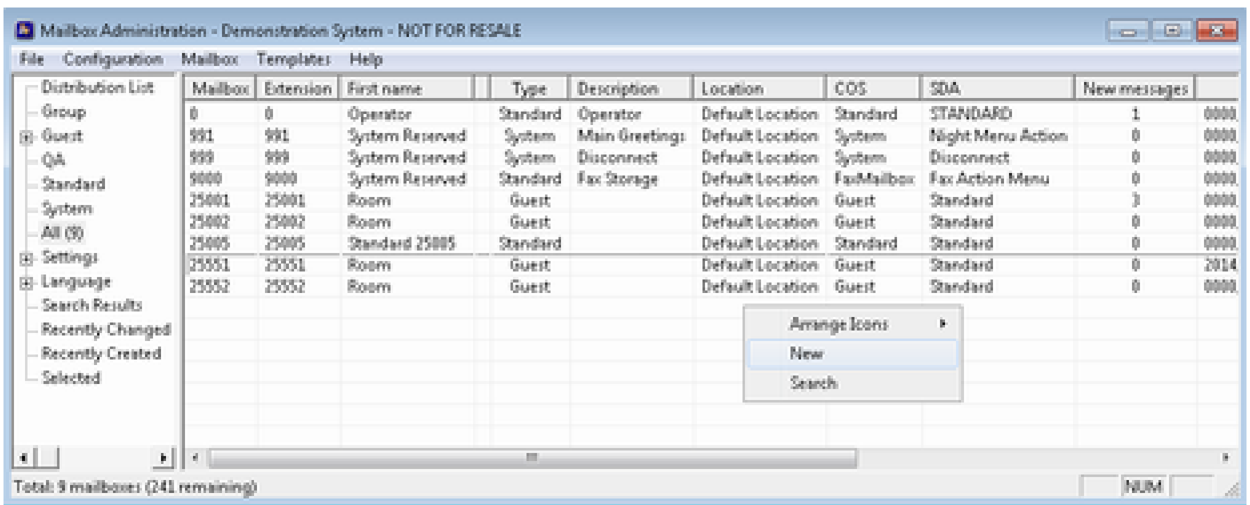


7.1. Configure MailBox

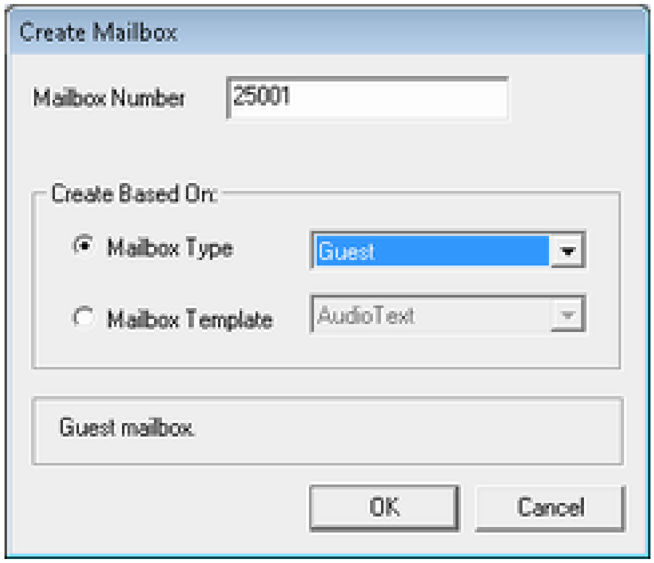
To configure mail boxes for guests, open Mailbox Administration, and select **All** in the left pane.



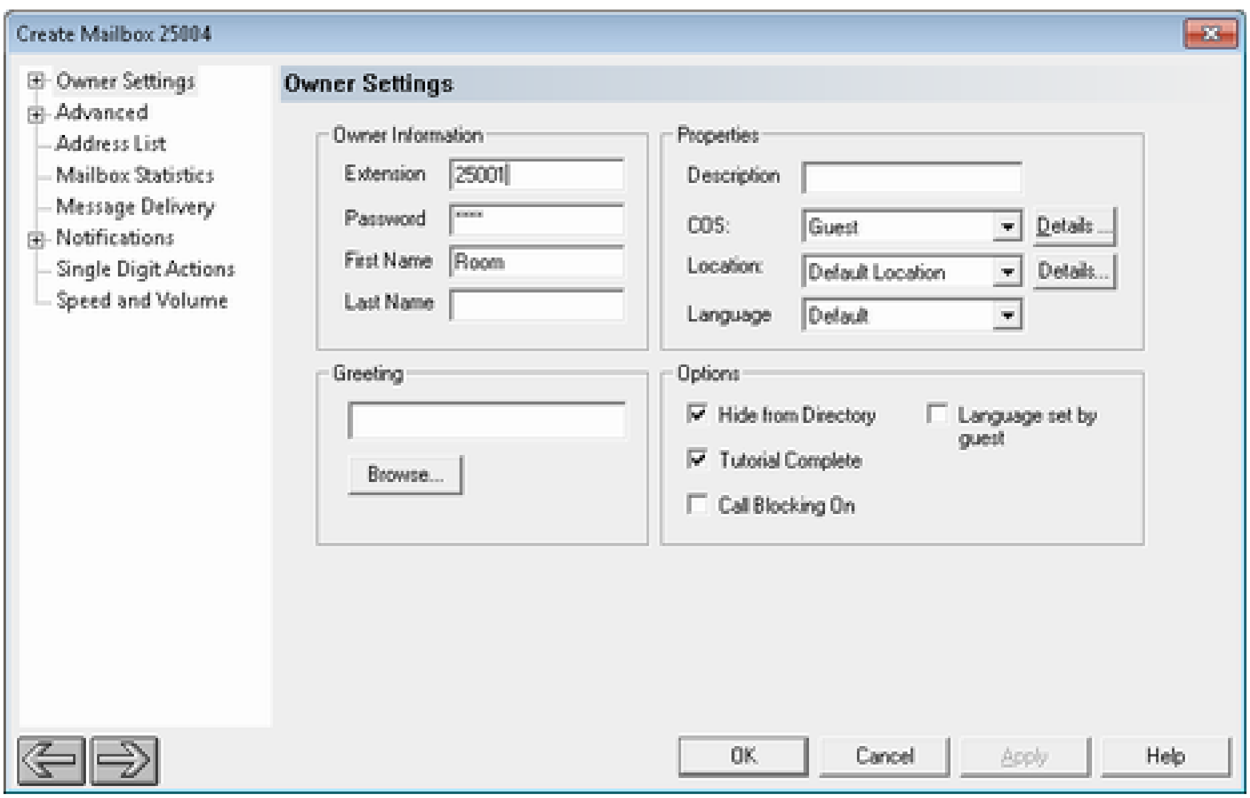
To add a mail box, right click on the right pane and select **New.**



On the **Create Mailbox** window, the in the station extension and select **Guest** for **Mailbox Type**, click **OK.**



One the next window, accept default values and click **OK.**



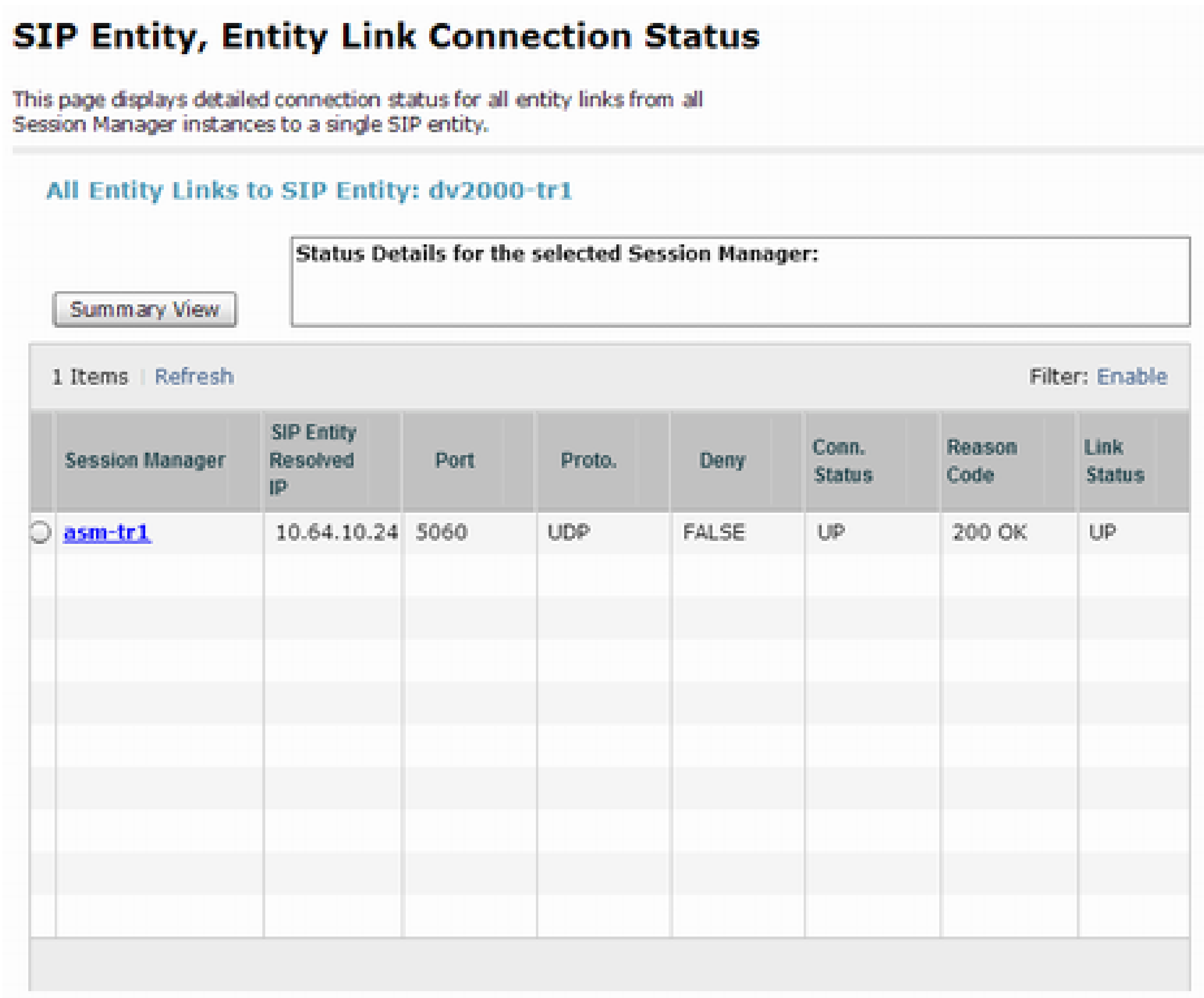
8. Verification Steps

This section describes verification steps that may be used to verify SIP connectivity between DuVoice DV2000 and Session Manager.

8.1. Avaya Aura® Session Manager

On the System Manager, navigate to **Home → Element → Session Manager → System Station → SIP Entity Monitoring**.

Verify the **Conn. Status** and **Reason Code** are **Up** and **200 OK**.



9. Conclusion

DuVoice DV2000 passed compliance testing. These Application Notes describe the procedures required to configure DuVoice DV2000 to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager to support the network shown in **Figure 1**.

10. Additional References

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

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.