Avaya Solution & Interoperability Test Lab

Application Notes for Talkaphone VOIP-200 Series IP Call Stations with Avaya Aura® Communication Manager and Avaya Aura® Session Manager - Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate the Talkaphone VOIP-200 Series IP Call Stations with Avaya Aura ® Communication Manager and Avaya Aura® Session Manager. Talkaphone VOIP-200 Series IP Call Stations registered with Avaya Aura® Session Manager via SIP.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the 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

These Application Notes describe the configuration steps required to integrate the Talkaphone VOIP-200 Series IP Call Stations with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Talkaphone VOIP-200 Series IP Call Stations registered with Session Manager via SIP.

2. General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing. The feature testing focused on establishing calls between Talkaphone VOIP-200 Series IP Call Stations, Avaya H,323, SIP, Digital, Analog telephones, and the PSTN, and exercising basic telephony features, such as hold, mute, transfer, and conference, from the Avaya IP phones. Additional telephony features, such as call forward and call coverage, were also verified.

The serviceability testing focused on verifying that the Talkaphone VOIP-200 Series IP Call Stations come back into service after re-connecting the Ethernet cable or rebooting the IP Call Station.

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.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with this Application Note, the interface between Avaya systems and the Talkaphone VOIP 200 did not include use of any specific encryption features.

Encryption (TLS/SRTP) was used internal to the enterprise between Avaya products.

2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- SIP registration of Talkaphone IP Call Station with Session Manager.
- Inbound and outbound calls between Talkaphone IP Call Station and Avaya SIP and H.323 telephones with Direct IP Media (Shuffling) enabled.
- Inbound and outbound calls between the Talkaphone IP Call Station and the PSTN.
- G.711 and G.729 codec support.
- Proper recognition of DTMF tones.
- Basic telephony features, including hold, mute, redial, transfer, and 3-way conference, initiated from the Avaya IP phone.
- Use of number lists on the Talkaphone IP Call Station.
- Proper system recovery after a restart of the Talkaphone IP Call Station and loss of IP connectivity.

2.2. Test Results

All test cases passed with the following observation(s):

On-hold call that is established between Talkaphone VOIP 200 and Avaya H.323 endpoint gets dropped when Avaya H.323 endpoint resumes the call. The issue only happens with direct media enabled and with Avaya H.323 endpoint. If the destination of the call originated by the Talkaphone VOIP 200 may be an Avaya H.323 endpoint, it is recommended to disable direct media on the Talkaphone VOIP 200 station.

2.3. Support

For technical support and information on Talkaphone VOIP-200 Series IP Call Stations, contact Talkaphone support at:

Address	: 7530 North Natchez Ave.
	Niles, IL 60714
Telephone	: (773) 539-1100
Fax	: (773) 539-1241
Email	: info@talkaphone.com
Web	: www.talkaphone.com

3. Reference Configuration

Figure 1 illustrates a sample configuration with an Avaya SIP-based network that includes the following products:

- Avaya Aura® System Manager, Avaya Aura® Session Manager, Avaya Aura® Communication Manager and Avaya Aura® Media Server running on Virtualized environment.
- Avaya Aura Messaging has SIP trunk connected to Session Manager and used as Voicemail system for the endpoint.
- Avaya G450 Media Gateway registers to Communication Manager and has PRI trunk to simulated PSTN.
- Session Manager has SIP trunk to simulated PSTN
- Avaya 96x1 H323 and SIP Deskphones were used to place and receive call to/from Talkaphone VOIP station.
- Talkaphone VOIP-200 IP Call Stations registered with Avaya Aura® Session Manager.

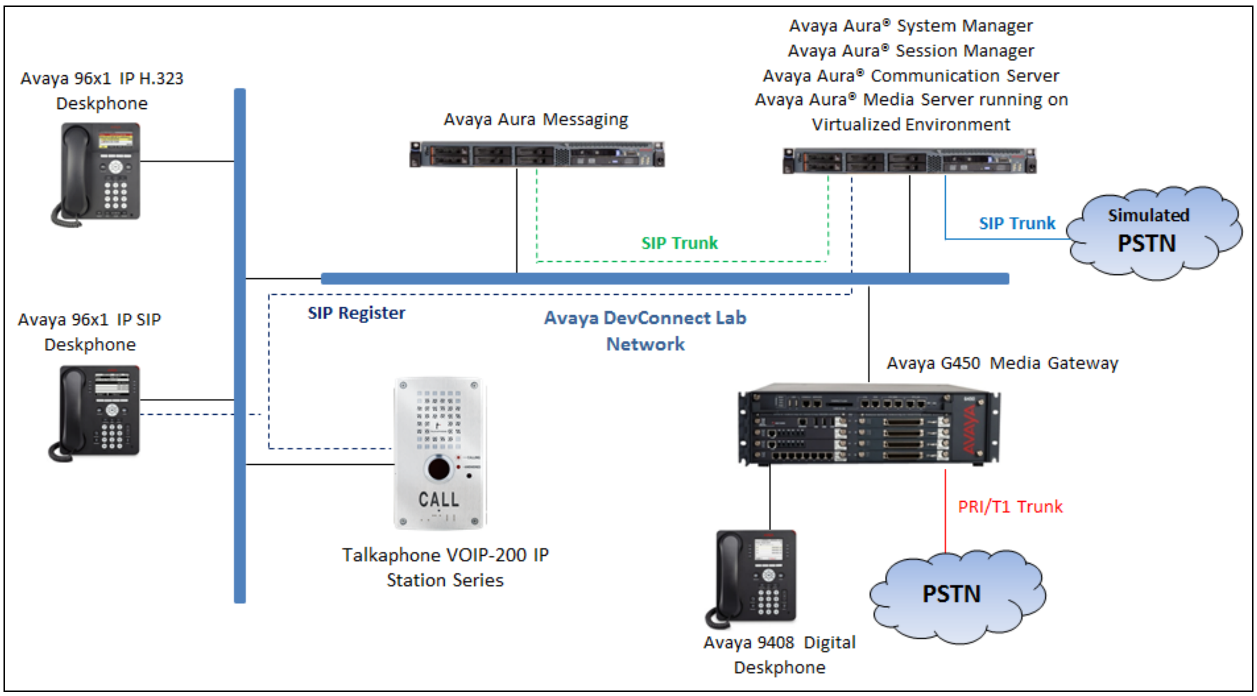


Figure 1: Avaya SIP Network with Talkaphone VOIP-200 Series IP Call Stations

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 Virtualized Environment	R017x.01.0.532.0 7.1.1.0.0.532.23985
Avaya Aura® System Manager running on Virtualized Environment	7.1.1.0.046931
Avaya Aura® Session Manager running on Virtualized Environment	7.1.1.0.711008
Avaya Aura® Media Server running on Virtualized Environment	7.8.0.333
Avaya Aura Messaging	7.0
Avaya G450 Media Gateway	38.20.1
Avaya 96x1 IP Deskphones	6.65 (H323) 7.1.1 (SIP
Talkaphone VOIP-200 Series IP Call Stations	Firmware Version : 2.4.1.40

5. Configure Avaya Aura® Communication Manager

Configuration and verification operations on Communication Manager illustrated in this section were all performed using Avaya Site Administrator Emulation Mode. The information provided in this section describes the configuration of Communication Manager for this solution. It is implied a working system is already in place, including SIP trunks to a Session Manager. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**. The configuration described in this section can be summarized as follows:

- Verify System Capacity
- Administer IP Node Names
- Administer Codecs
- Administer IP Network Region
- Administer Signaling Group
- Administer Trunk Group
- Administer Private Numbering
- Administer Outbound Routing

5.1. Verify System Capacity

The license file installed on the system controls these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative. Use the **display system-parameters customer-options** command to determine these values. On **Page 1**, verify that the **Maximum Off-PBX Telephones** allowed in the system is sufficient. One OPS station is required per SIP device.

```
display system-parameters customer-options                    Page   1 of  10
                                OPTIONAL FEATURES

     G3 Version: V16                                 Software Package: Enterprise
       Location: 2                                    System ID (SID): 1
       Platform: 28                                   Module ID (MID): 1

                                                                  USED
                                Platform Maximum Ports: 65000 290
                                      Maximum Stations: 41000 44
                              Maximum XMOBILE Stations: 41000 0
                    Maximum Off-PBX Telephones - EC500: 41000 0
                    Maximum Off-PBX Telephones -   OPS: 41000 14
                    Maximum Off-PBX Telephones - PBFMC: 41000 0
                    Maximum Off-PBX Telephones - PVFMC: 41000 0
                    Maximum Off-PBX Telephones - SCCAN: 41000 0
                         Maximum Survivable Processors: 313   0

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

On **Page 2** of the **system-parameters customer-options form**, verify that the number of **Maximum Administered SIP Trunks** supported by the system is sufficient.

```
display system-parameters customer-options                          Page    2 of
10
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                              USED
                     Maximum Administered H.323 Trunks: 12000 16
           Maximum Concurrently Registered IP Stations: 18000 2
             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: 41000 1
                   Maximum Video Capable IP Softphones: 18000 4
                       Maximum Administered SIP Trunks: 24000 180
  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   0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 300   0

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

5.2. Administer IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of the server running Communication Manager **(procr**) and for Session Manager (**interopASM**). These node names will be needed for defining the service provider signaling group in **Section 5.5**.

```
change node-names ip                                                Page    1 of    2
                                 IP NODE NAMES
    Name                 IP Address
AMS1                   10.33.1.30
default                0.0.0.0
interopASM             10.33.1.12
procr                  10.33.1.6
```

5.3. Administer Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the local and remote sites. For the compliance test, codec G.711MU and G.729 was configured using ip-codec-set 1. To configure the codecs, enter the codecs in the **Audio Codec** column of the table in the order of preference, the Media Encryption section was configured to use for Avaya endpoints, the VoIP-200 station is not using the Media Encryption. Default values can be used for all other fields.

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

                          IP MEDIA PARAMETERS
    Codec Set: 1

    Audio         Silence      Frames   Packet
    Codec         Suppression  Per Pkt  Size(ms)
 1: G.711MU            n         2        20
 2: G.729              n         2        20
 3:
 4:
 5:
 6:
 7:

     Media Encryption                   Encrypted SRTCP: enforce-unenc-srtcp
 1: none
 2:
 3:
 4:
 5:
```

5.4. Administer IP Network Region

For the compliance test, IP network region 1 was chosen. Use the **change ip-network-region 1** command to configure region 1 with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the local site. In this configuration, the domain name is **bvwdev.com**. This name appears in the “From” header of SIP messages originating from this IP region.
- Enter a descriptive name in the **Name** field. This is optional.
- Enable **IP-IP Direct Audio** (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. Set both **Intra-region** and **Inter-region IP-IP Direct Audio** to **yes.** This is the default setting. Shuffling can be further restricted at the trunk level on the Signaling Group form.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.3**.
- Retain default values for all other fields.

```
change ip-network-region 1                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 1        NR Group: 1
Location: 1        Authoritative Domain: bvwdev.com
    Name: Loc-1                   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? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
```

On **Page 4**, define the IP codec set to be used for traffic between various regions. Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) **1**. Default values may be used for all other fields. In the case of the compliance test, only one IP network region was used, so no inter-region settings were required and therefore only codec set 1 is used.

```
change ip-network-region 1                                      Page   4 of  20

 Source Region: 1     Inter Network Region Connection Management     I       M
                                                                     G  A    t
 dst codec direct   WAN-BW-limits   Video      Intervening       Dyn A  G    c
 rgn  set   WAN  Units     Total Norm  Prio Shr Regions          CAC R  L    e
 1    1                                                              all
 2    2      y    NoLimit                          n    t
```

5.5. Administer Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and Session Manager for use by SIP trunks. This signaling group is used for inbound and outbound calls between the Communication Manager and Session Manager. For the compliance test, signaling group 1 was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**.
- The compliance test was conducted with the **Transport Method** set to “tls”. The transport method specified here is used between Communication Manager and Session Manager. Whatever protocol is used here, it must also be used on the Session Manager entity link defined in **Section 6.5**.
- Set the **Peer Detection Enabled** field to “y”. The **Peer-Server** field will initially be set to **Others** and cannot be changed via administration. Later, the **Peer-Server** field will automatically change to **SM** once Communication Manager detects its peer as a Session Manager.
- Set the **Near-end Node Name** to “procr”. This node name maps to the IP address of the Communication Manager as defined in **Section 5.4**.
- Set the **Far-end Node Name** to “InteropASM”. This node name maps to the IP address of Session Manager as defined in **Section 5.2**.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to a default well-known port value. (For TCP the well-known port value is 5061).
- Set the **Far-end Network Region** to the IP network region defined for the local site in **Section 5.4**.
- Set the **Far-end Domain** to the domain of the local site.
- Set **Direct IP-IP Audio Connections** to “y”. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the SIP trunk and the enterprise endpoint.
- Set the **DTMF over IP** field to “rtp-payload”. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Retain default values for all other fields.

```
change signaling-group 1                                        Page   1 of   3
                                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? n
  Peer Detection Enabled? n  Peer Server: SM
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr                  Far-end Node Name: interopASM
 Near-end Listen Port: 5061                 Far-end Listen Port: 5061
                                         Far-end Network Region: 1

Far-end Domain: bvwdev.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
```

5.6. Administer Trunk Group

Use the "add trunk-group" command to create a trunk group for the signaling group created in **Section 5.6**. For the compliance test, trunk group 1 was configured using the parameters highlighted below.

- Set the **Group Type** field to "sip".
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Service Type** field to "tie".
- Set **Member Assignment Method** to "auto".
- Set the **Signaling Group** to the signaling group shown in **Section 5.5**.
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.
- Retain default values for all other fields.

```
add trunk-group 1                                              Page   1 of  22
                                TRUNK GROUP

Group Number: 1                  Group Type: sip          CDR Reports: y
  Group Name: Private Trunk             COR: 1        TN: 1        TAC: #01
   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: 14
```

On **Page 3**, set the **Numbering Format** field to **private**. This field specifies the format of the calling party number (CPN) sent to the far-end. The **Numbering Format** was set to "private" and the **Numbering Format** in the route pattern was set to "lev0-pvt" (see **Section 5.8**).

```
add trunk-group 1                                               Page   3 of  22
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y



   Suppress # Outpulsing? n  Numbering Format: private
                                                   UUI Treatment: shared
                                                 Maximum Size of UUI Contents: 128
                                                    Replace Restricted Numbers? y
                                                   Replace Unavailable Numbers? y

                                                     Hold/Unhold Notifications? y
                                Modify Tandem Calling Number: no
               Send UCID? y
```

5.7. Administer Private Numbering

Private numbering defines the calling party number to be sent to the far-end. Use the **change private-numbering** command to create an entry that will be used by the trunk groups defined in **Section 5.6.** In the example shown below, all calls originating from a 4-digit extension beginning with "3" and routed across trunk group 1 are sent with a 4-digit calling number.

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

Ext Ext                Trk        Private          Total
Len Code               Grp(s)     Prefix           Len
 4  3                  1                           4    Total Administered: 5
 4                                                         Maximum Entries: 540
```

5.8. Administer Outbound Routing

In these Application Notes, the Automatic Alternate Routing (AAR) feature is used to route outbound calls via the SIP trunk to the SIP endpoint. In the sample configuration, the dial prefix "34" is used as the Dialed String. This common configuration is illustrated below with little elaboration. Use the "change dialplan analysis" command to define a dialed string beginning with 34 of length 4 as extension (ext).

```
change dialplan analysis                                        Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location: all            Percent Full: 5

    Dialed    Total  Call      Dialed    Total  Call      Dialed    Total  Call
    String    Length Type      String    Length Type      String    Length Type
   34             4  ext
```

The route pattern defines which trunk group will be used for an outgoing call and performs any necessary digit manipulation. Use the “change route-pattern” command to configure the parameters for the local site route pattern in the following manner. The example below shows the values used for route pattern 1 during the compliance test.

- **Pattern Name**: Enter a descriptive name.
- **Grp No**: Enter the outbound trunk group for the SIP trunk. For the compliance test, trunk group **1** was used.
- **FRL**: Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- **Numbering Format**: “lev0-pvt”. All calls using this route pattern will use the private numbering table. See setting of the **Numbering Format** in the trunk group form in **Section 5.6** for full details.
- Retain default values for all other fields.

```
change route-pattern 1                                              Page   1 of   3
                    Pattern Number: 1      Pattern Name: SIP-TLS-To-SM
    SCCAN? n     Secure SIP? n     Used for SIP stations? 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
 3:                                                                         n   user
 4:                                                                         n   user
 5:                                                                         n   user
 6:                                                                         n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM Sub  Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
 1: y y y y y n  n            rest                               lev0-pvt  next
 2: y y y y y n  n            rest                                         none
 3: y y y y y n  n            rest                                         none
```

Use the “change aar analysis” command to create an entry in the AAR Digit Analysis Table for this purpose. The example below shows entries created for the local site “aar analysis 3”. The highlighted entry specifies that 4 digit dial string 3 was to use route pattern 1 to route calls to the SIP endpoint via Session Manager.

```
change aar analysis 3                                               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
    3                    4    4       1         lev0          n
```

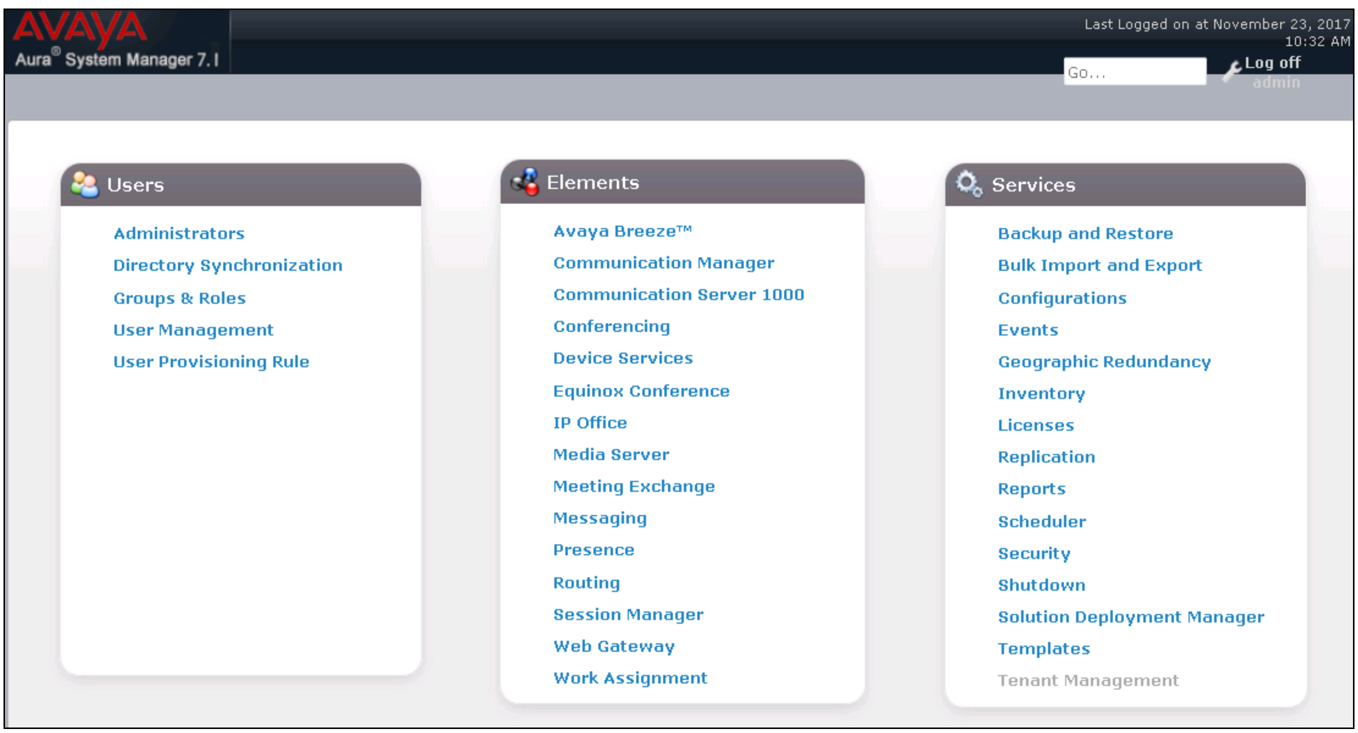
6. Configure Avaya Aura® Session Manager

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

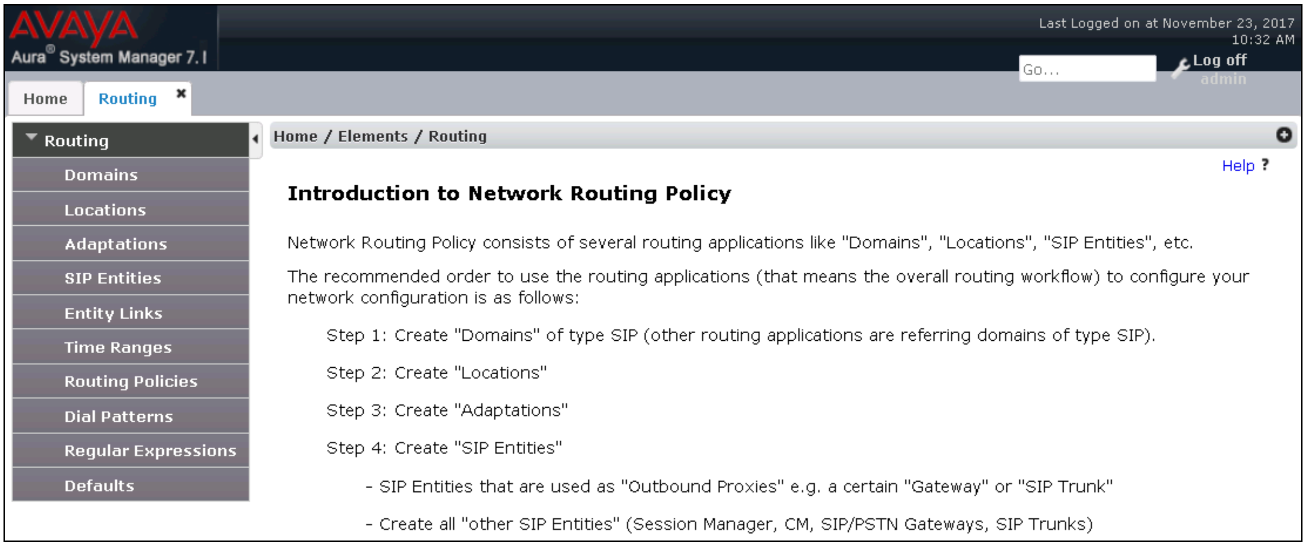
- SIP Domain
- Location
- SIP Entities
- Entity Links
- Routing Policies
- Dial Patterns

For detail configuration details of the Session Manager refer to **Section 10**.

Session Manager 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 and click on **Log on** (not shown). The following page is displayed. The links displayed below will be referenced in subsequent sections to navigate to items requiring configuration.



Clicking the **Elements → Routing** link, displays the **Introduction to Network Routing Policy** page. In the left-hand pane is a navigation tree containing many of the items to be configured in the following sections.

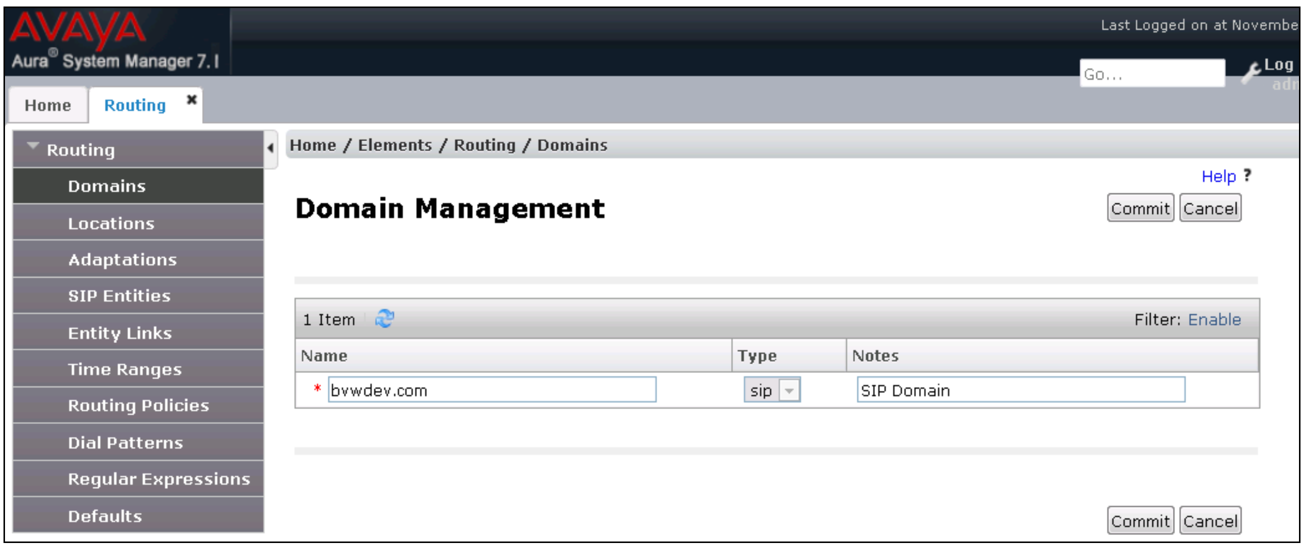


6.1. Specify SIP Domain

Create a SIP Domain for each domain for which Session Manager will need to be aware in order to route calls. For the compliance test, this includes the domain (**bvwdev.com**) as defined in **Section 5.4**. Navigate to **Routing → Domains** in the left-hand navigation pane (**Section 6.1**) and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Name –** Enter the domain name.
- **Type –** Select "sip" from the pull-down menu.
- **Notes –** Add a brief description (optional).

Click **Commit**. The screen below shows the entry for the added domain.



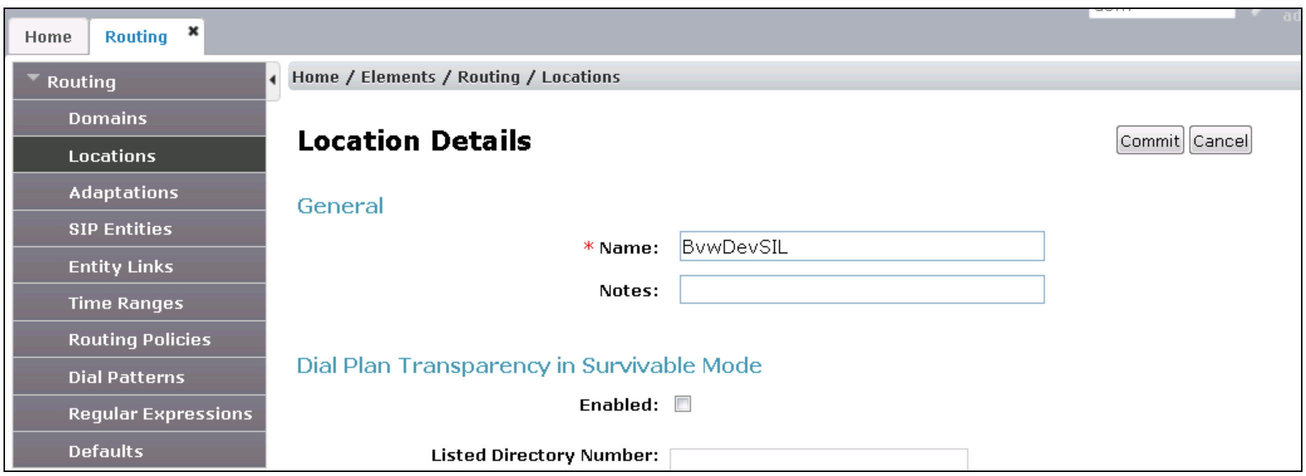
6.2. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. A single Location was defined for the enterprise even though multiple subnets were used. The screens below show the addition of the Location named **BvwDevSIL**, which includes all equipment at the enterprise including Communication Manager, Session Manager and the Dialogic SR140 PC.

To add a Location, navigate to **Routing → Locations** in the left-hand navigation pane (**Section 6.1**) and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

In the **General** section, enter the following values. Use default values for all remaining fields.

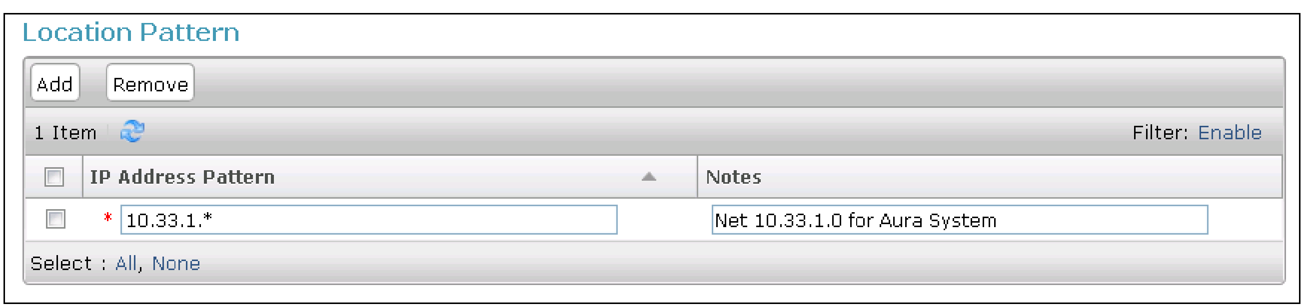
- **Name** – Enter a descriptive name for the Location.
- **Notes** – Add a brief description (optional).



Scroll down to the **Location Pattern** section. Click **Add** and enter the following values.

- **IP Address Pattern** – Add all IP address patterns used to identify the location.
- **Notes** – Add a brief description (optional).

Click **Commit** to save.



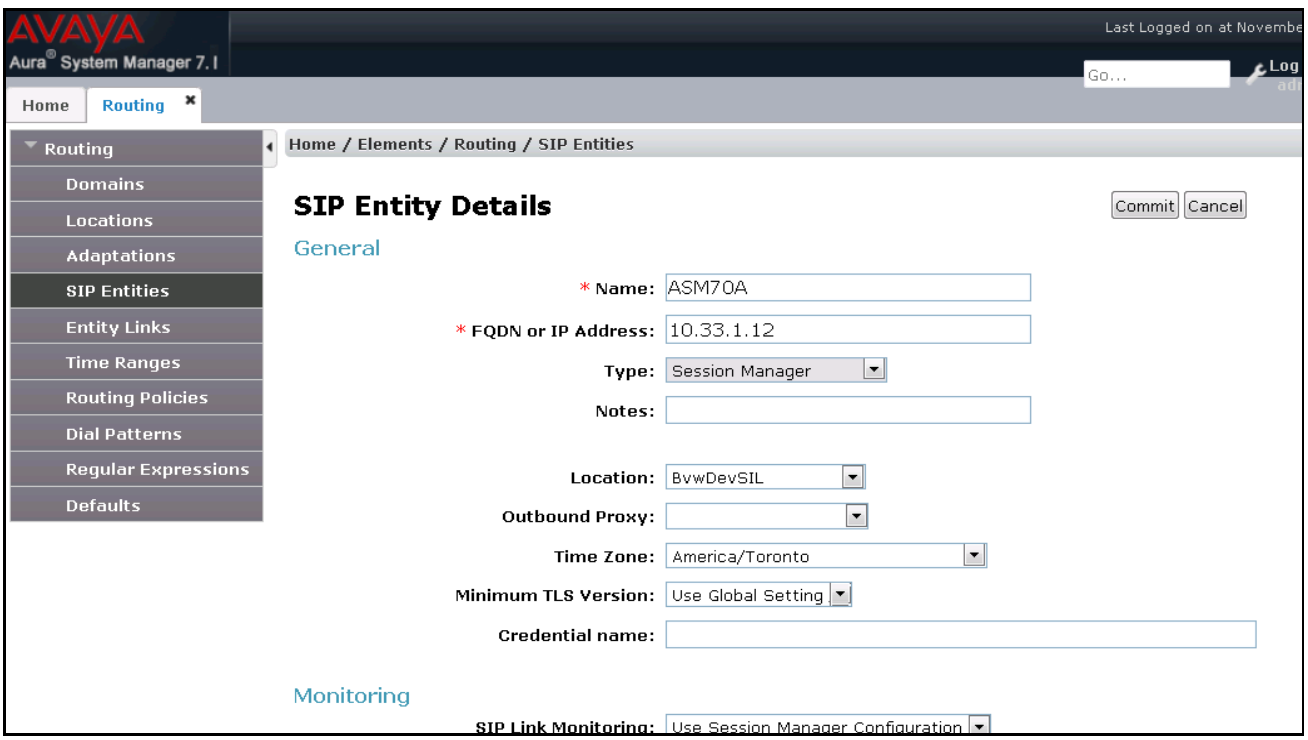
6.3. Add SIP Entity

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to Session Manager which includes Communication Manager. Navigate to **Routing → SIP Entities** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

In the **General** section, enter the following values. Use default values for all remaining fields.

- **Name** – Enter a descriptive name.
- **FQDN or IP Address** – Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type** – Enter "Session Manager" for Session Manager or "CM" for Communication Manager.
- **Adaptation** – This field is only present if Type is not set to Session Manager. If applicable, select the appropriate Adaptation name. During compliance testing no adaptation rule was used.
- **Location** – Select the Location that applies to the SIP Entity being created. For the compliance test, all components were located in Location "BvwDevSIL" created in **Section 6.3**.
- Time Zone – Select the time zone where the server is located.

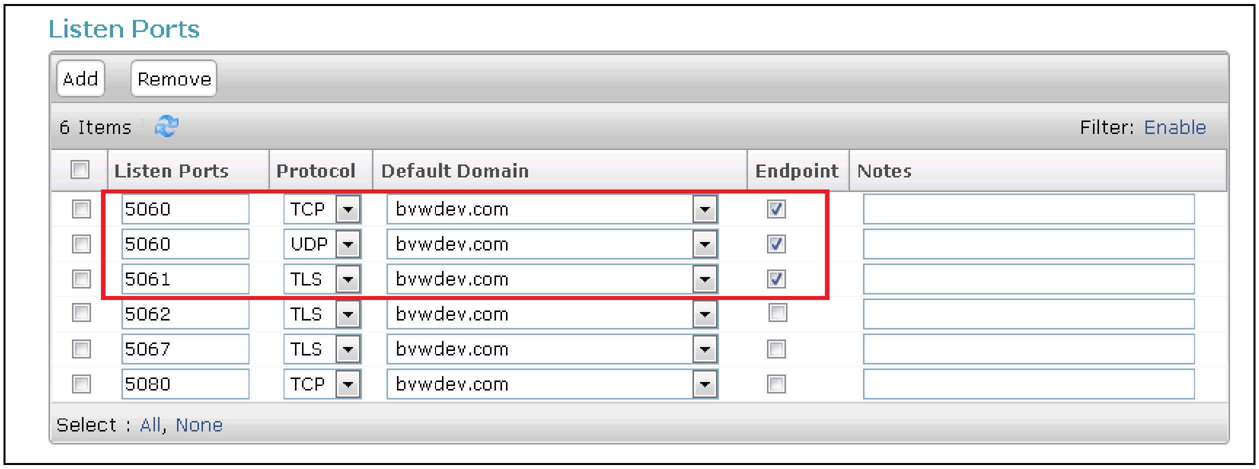
The following screen shows the addition of Session Manager. The IP address of the virtual SM-100 Security Module is entered for **FQDN or IP Address**.



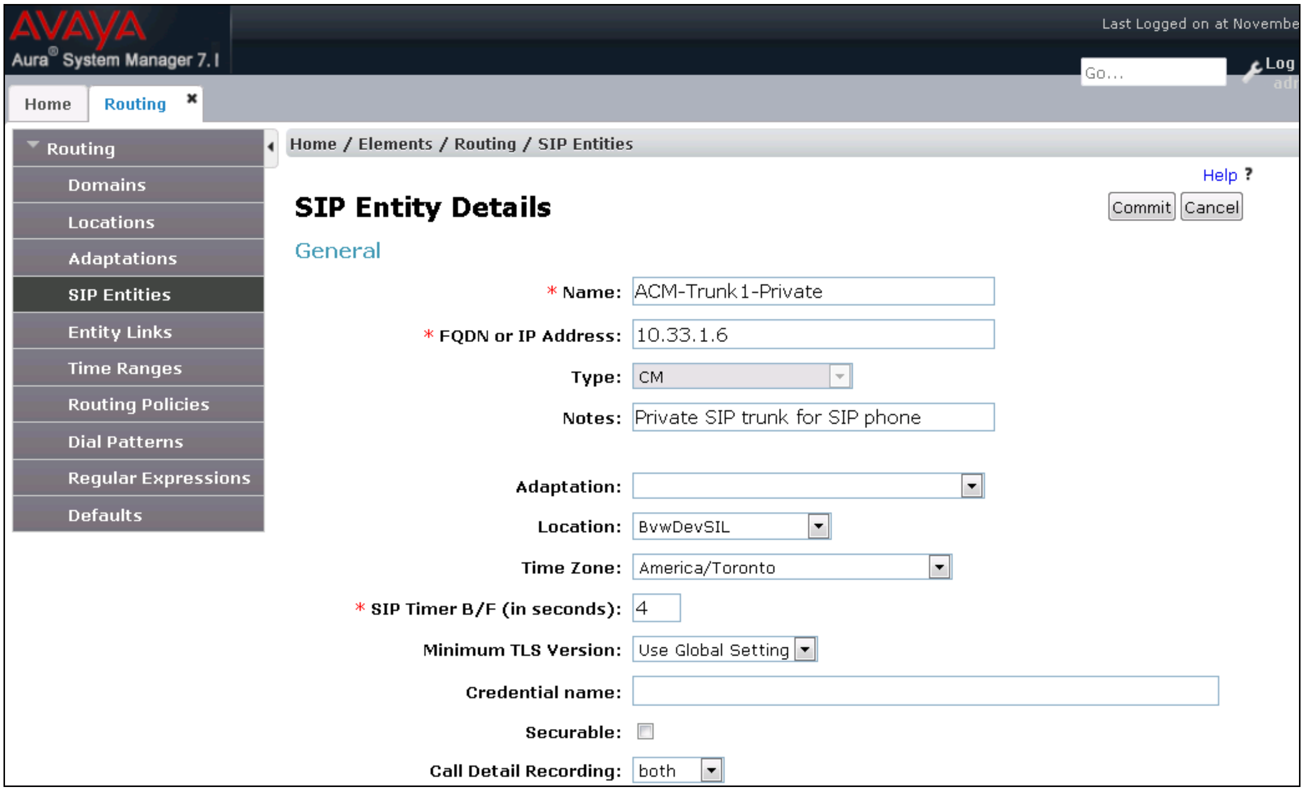
To define the ports used by Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for **Session Manager** SIP Entities.

In the **Port** section, click **Add** and enter the following values. Use default values for all remaining fields:

- **Port** – Port number on which Session Manager can listen for SIP requests.
- **Protocol** – Transport protocol to be used with this port.
- **Default Domain** – The default domain associated with this port.
- **Endpoint** – Checked the checkbox to indicate the specific ports used for SIP endpoint.



The following screen shows the addition of Communication Manager. In order for Session Manager to send SIP service provider traffic on a separate entity link to Communication Manager; this requires the creation of a SIP Entity for Communication Manager for use with all other SIP traffic. The **FQDN or IP Address** field is set to the IP address of Communication Manager. The **Location** field is set to **BewDevSIL** which is the Location defined for the subnet where Communication Manager resides. See **Section 6.3**.

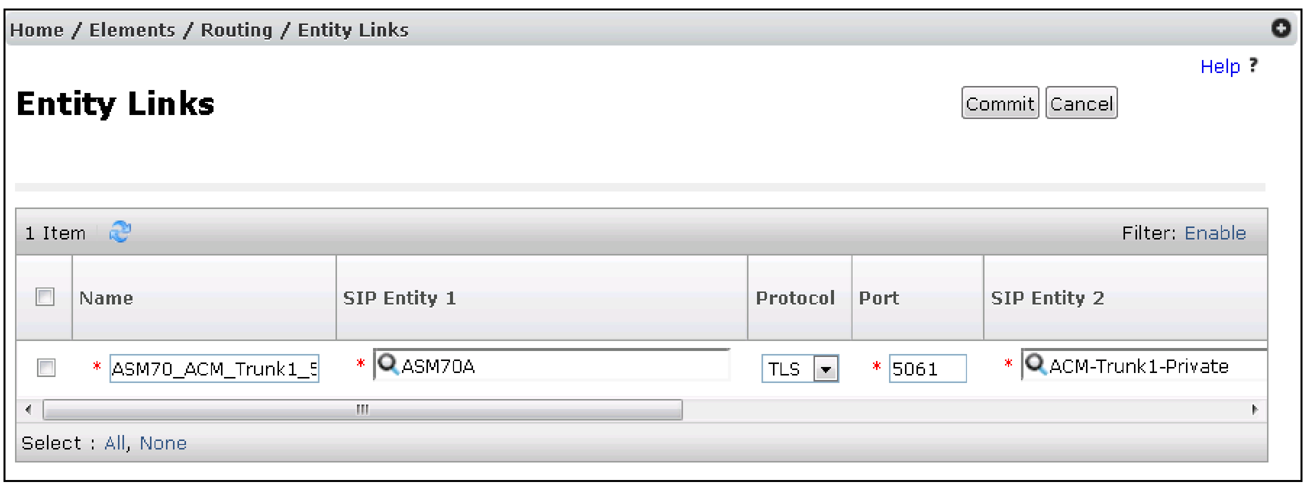


6.4. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. The Entity Link was created to Communication Manager, to add an Entity Link, navigate to **Routing → Entity Links** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Name** – Enter a descriptive name.
- **SIP Entity 1** – Select the Session Manager SIP Entity.
- **Protocol** – Select the transport protocol used for this link. This must match the protocol used in the Communication Manager signaling group in Section 5.5.
- **Port** – Port number on which Session Manager will receive SIP requests from the far-end. For the Communication Manager Entity Link, this must match the one defined on the Communication Manager signaling group in Section 5.5.
- **SIP Entity 2** – Select the name of the other system. For the Communication Manager Entity Link, select the Communication Manager SIP Entity defined in Section 6.4.
- **Port** – Port number on which the other system receives SIP requests from Session Manager. For the Communication Manager Entity Link, this must match the one defined on the Communication Manager signaling group in Section 5.5.
- **Connection Policy** – Select trusted from pull-down menu.

Click **Commit** to save. The following screen illustrates the Entity Link to Communication Manager. The protocol and ports defined here must match the values used on the Communication Manager signaling group configuration in **Section 5.5**.



6.5. Add Routing Policies

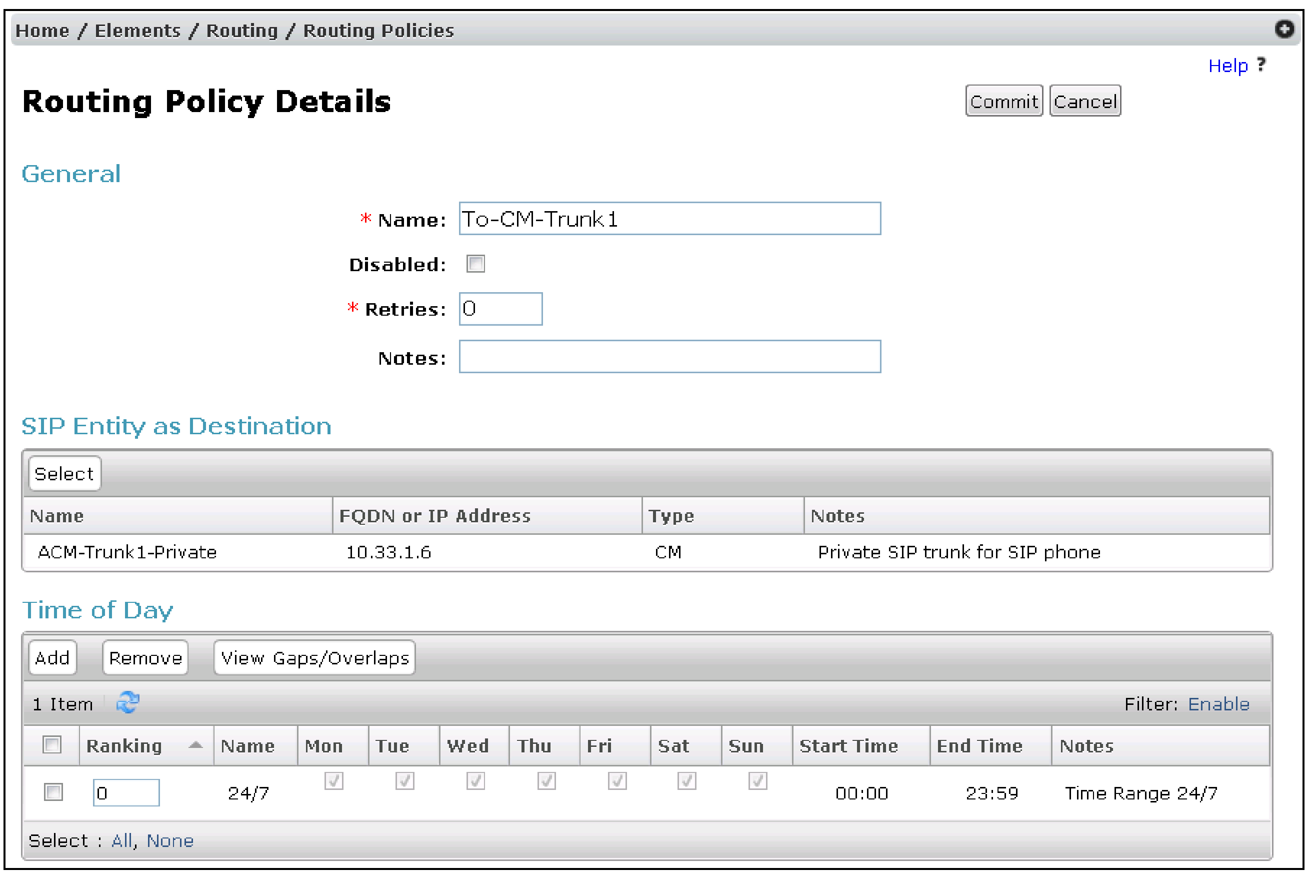
Routing Policy describes the conditions under which calls will be routed to the SIP Entities specified in **Section 6.4**. Routing Policy must be added for Communication Manager. To add a Routing Policy, navigate to **Routing → Routing Policies** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

In the **General** section, enter the following values. Use default values for all remaining fields.

- Name – Enter a descriptive name.
- Notes – Add a brief description (optional).

In the **SIP Entity as Destination** section, click **Select.** The **SIP Entity List** page opens (not shown). Select the appropriate SIP Entity to which this Routing Policy applies and click **Select**. The selected SIP Entity displays on the **Routing Policy Details** page as shown below. Use default values for remaining fields. Click **Commit** to save.

The following screen shows the Routing Policy for Communication Manager.



6.6. Add Dial Patterns

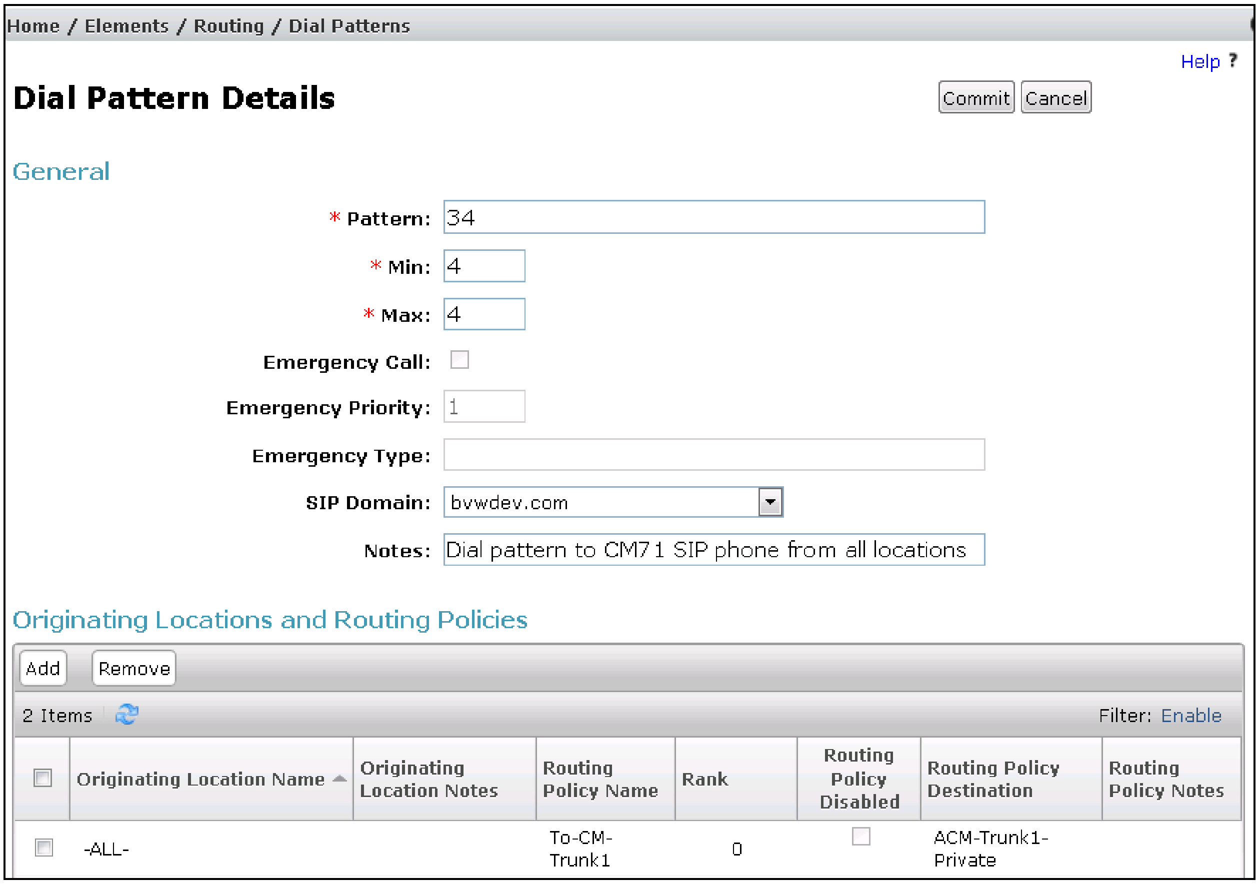
Dial Patterns are needed to route calls through Session Manager. For the compliance test, Dial Patterns were needed to route calls from Communication Manager to the SIP endpoint and vice versa. Dial Patterns define which Route Policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a Dial Pattern, navigate to **Routing → Dial Patterns** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

In the **General** section, enter the following values. Use default values for all remaining fields.

- **Pattern** – Enter a dial string that will be matched against the Request-URI of the call.
- **Min** – Enter a minimum length used in the match criteria.
- **Max** – Enter a maximum length used in the match criteria.
- **SIP Domain** – Enter the destination domain used in the match criteria.
- **Notes** – Add a brief description (optional).

In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating location for use in the match criteria. Lastly, select the Routing Policy from the list that will be used to route all calls that match the specified criteria. Click **Select**. Default values can be used for the remaining fields. Click **Commit** to save.

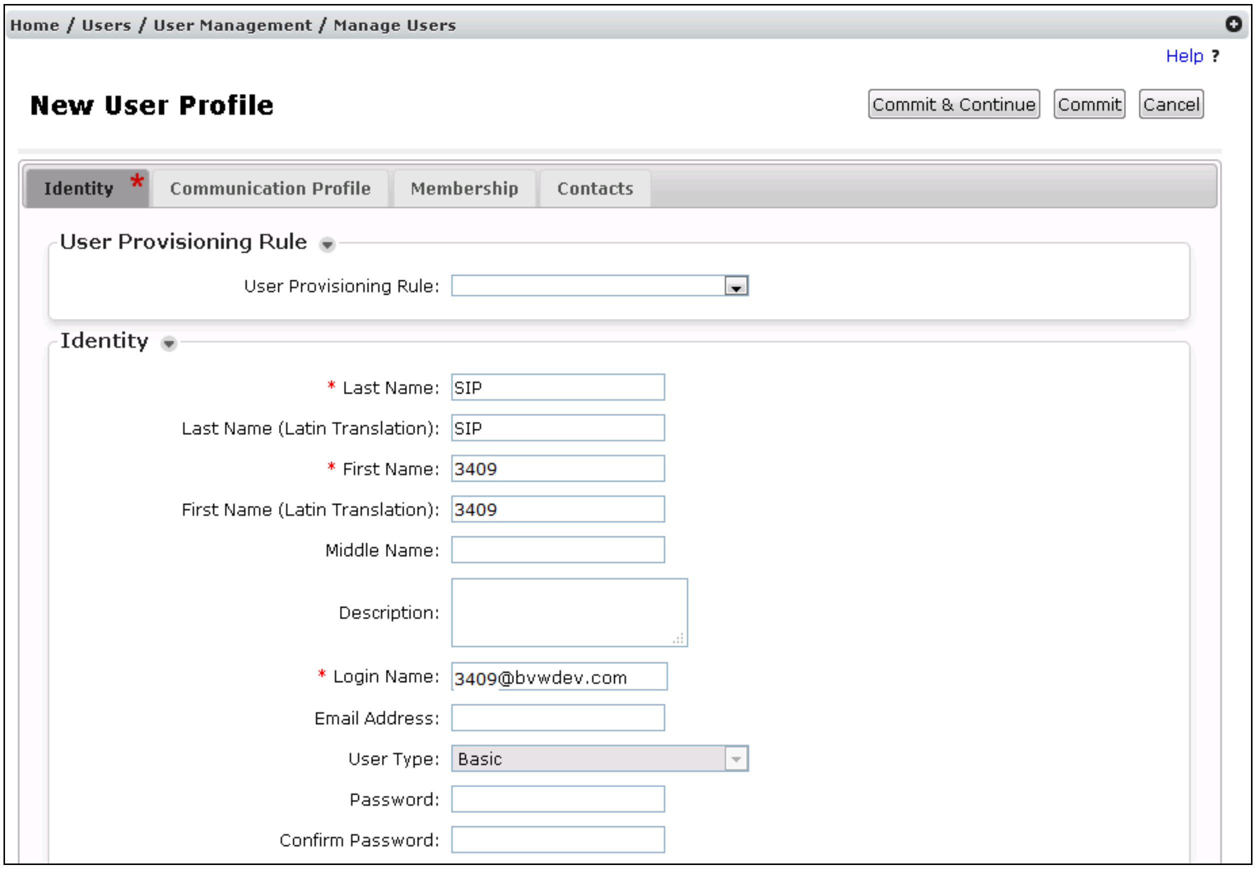
The first example shows the pattern (4 digits) that begins with “34” and has a destination domain of “bvwdev.com” from “All” location use route policy “ACM-Trunk1-Private”.


Home / Elements / Routing / Dial Patterns
Help ?
Dial Pattern Details
Commit
Cancel
General
* Pattern: 34
* Min: 4
* Max: 4
Emergency Call:
Emergency Priority: 1
Emergency Type:
SIP Domain: bvwdev.com
Notes: Dial pattern to CM71 SIP phone from all locations
Originating Locations and Routing Policies
Add
Remove
2 Items
Filter: Enable
Originating Location Name
Originating Location Notes
Routing Policy Name
Rank
Routing Policy Disabled
Routing Policy Destination
Routing Policy Notes
-ALL-
To-CM-Trunk1
0
ACM-Trunk1-Private

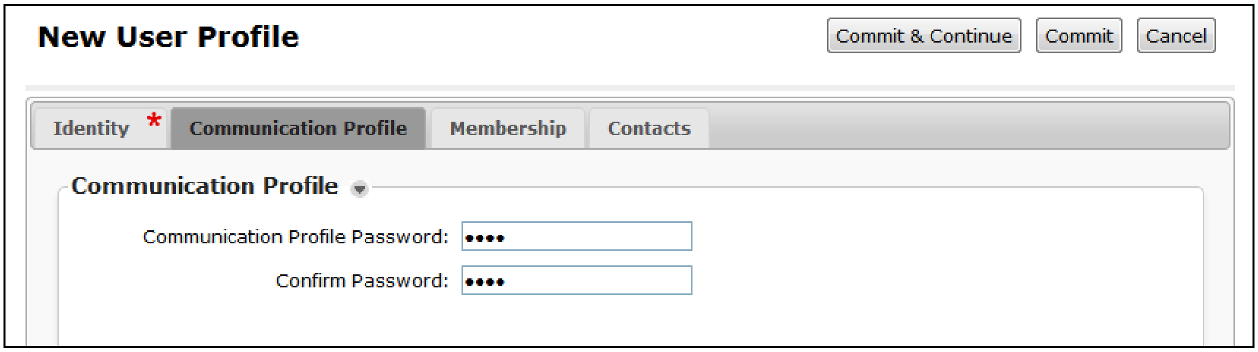
6.7. Add a SIP User

A SIP user must be added for Talkaphone VoIP station. Click **User Management → Manage Users → New** (not shown) and configure the following in the **Identity** tab.

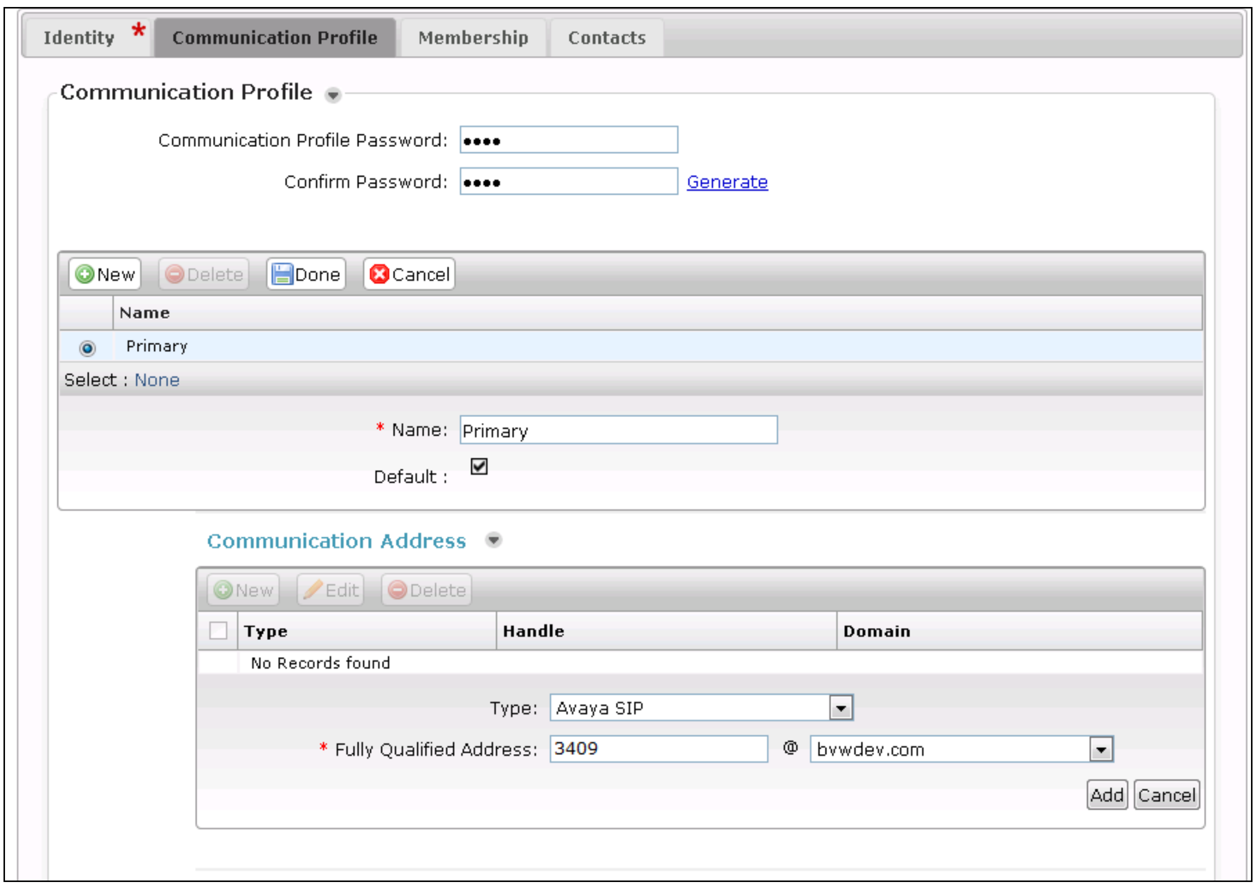
- **First Name** – Enter an identifying name
- **Last Name** – Enter an identifying name
- **Login Name** – Enter the extension number followed by the domain, in this case "3409@bvwdev.com"



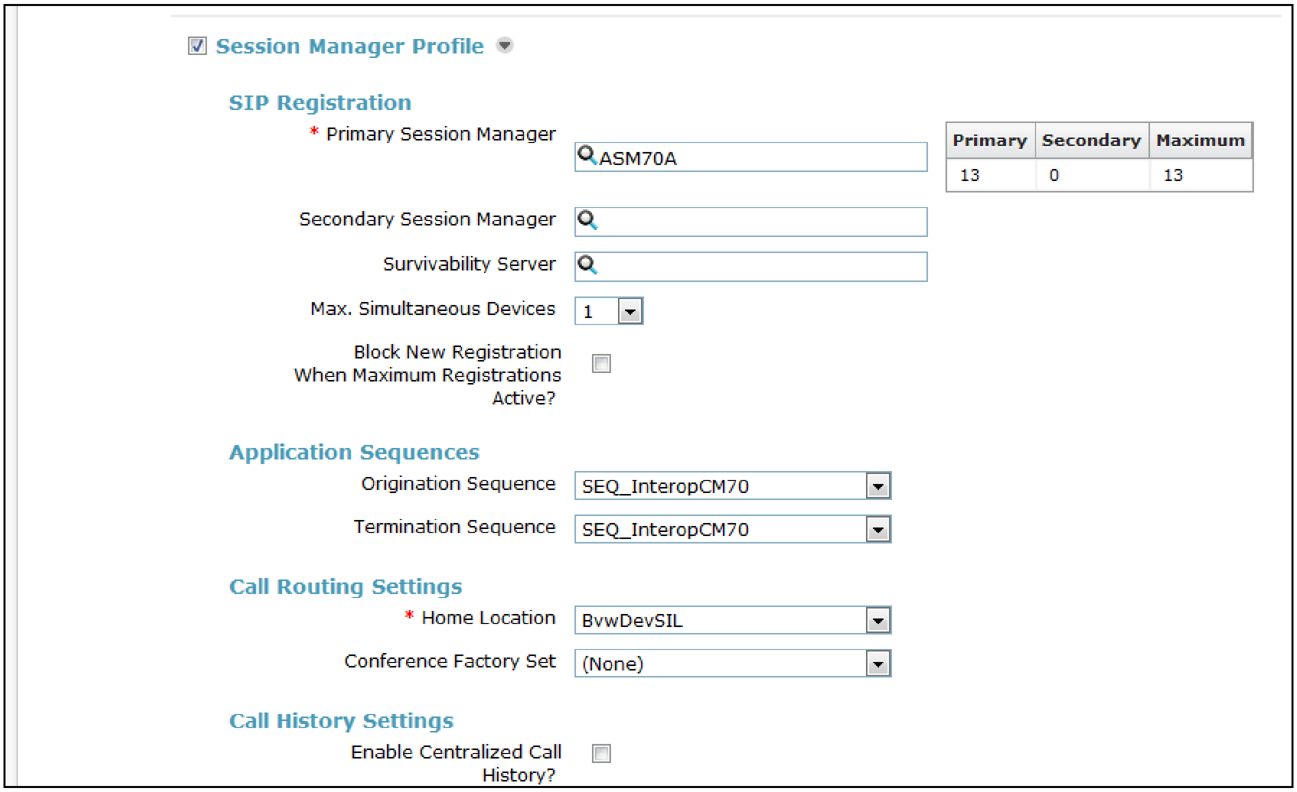
Click the **Communication Profile** tab and in the **Communication Profile Password** and **Confirm Password** fields, enter a numeric password. This will be used to register the Talkaphone VoIP station.



In the **Communication Address** section select **New**; for **Type** select **Avaya SIP** from the drop down list. In the **Fully Qualified Address** field enter the extension number and select the appropriate Domain from the drop down list, in this case the SIP domain is "bvwdev.com". Click **Add** when done.

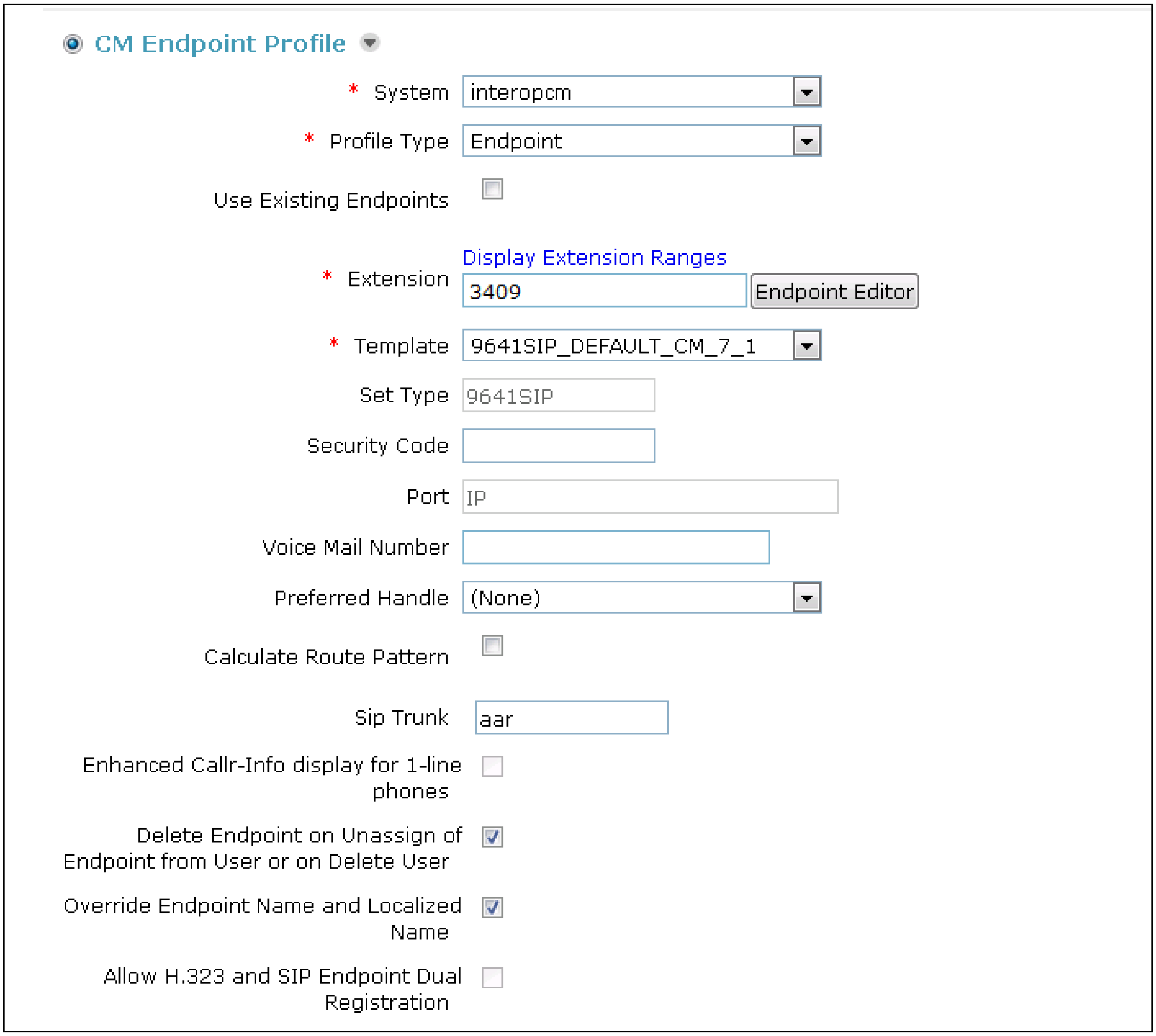


Select the check box for **Session Manager Profile** and configure the **Primary Session Manager, Origination Sequence, Termination Sequence** and **Home Location,** from the respective drop down lists.

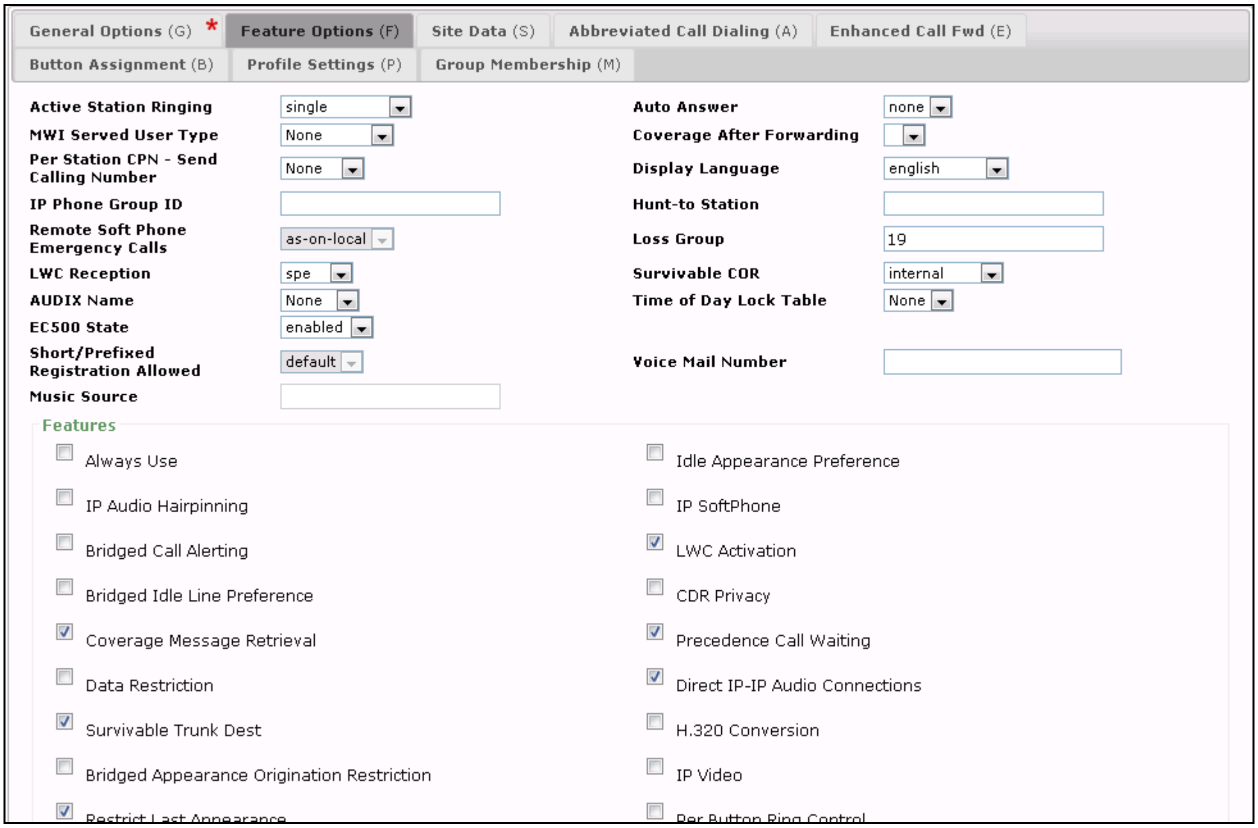


Select the check box for **CM Endpoint Profile** and configure as follows:

- **System** – Select the relevant Communication Manager Element from the drop down list
- **Profile Type** – Select "Endpoint" from the drop down list
- **Extension** – Enter the required extension number, in this case "3409"
- **Template** – Select "9641SIP_DEFAULT_CM_7_1" from the drop down list
- **Port** – The "IP" is auto filled out by the system



Continuing from above, click on **Endpoint Editor**. Click on the **Feature Options** tab, the screen shot below shows the Feature options that were used during compliance testing.



7. Configure Talkaphone VOIP-200 Series IP Call Stations

This section covers the configuration of the Talkaphone VOIP-200 Series IP Call Stations. The following procedures are covered:

1. Launching the Web Administration Interface
2. Network Configuration
3. SIP Configuration
4. Configure Audio Settings
5. Configure Call Parameters
6. Configure Buttons

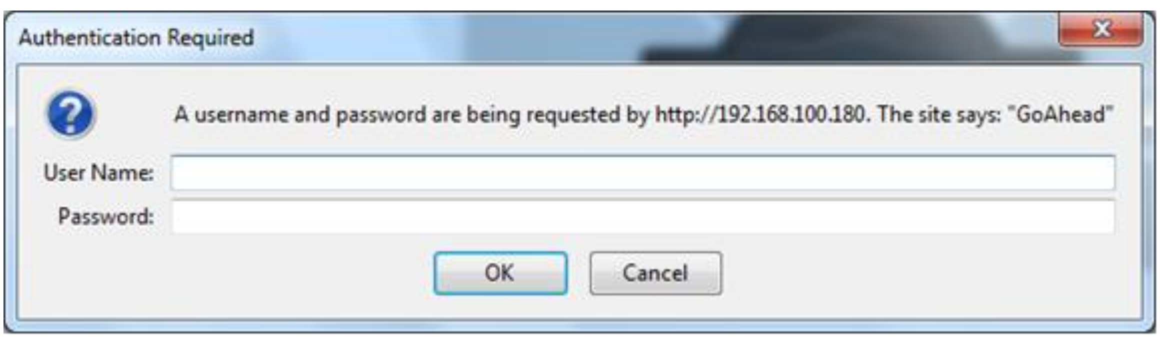
For more information on configuring other features of the Talkaphone IP Call Stations, refer to **[10].**

7.1. Launching the Web Administration Interface

The Talkaphone IP Call Stations are pre-configured with the following default values:

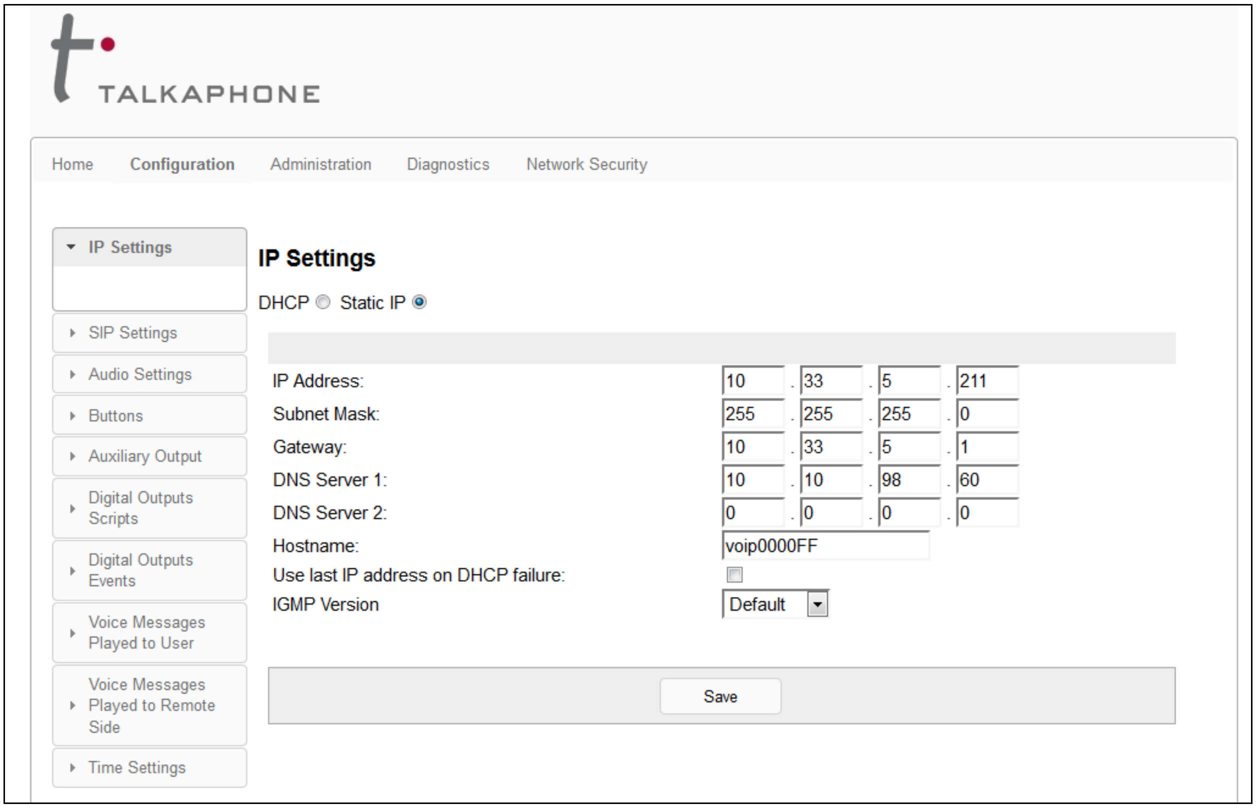
- **IP Address:** 192.168.1.10
- **Username:** admin
- **Password:** admin@123

Ensure that the administration PC and Talkaphone IP Call Station are connected to the LAN. Open a web browser and enter the IP address of the Talkaphone IP Call Station in the URL field. The browser prompts for authentication. Log in with the appropriate credentials above.



7.2. Network Configuration

To modify the IP network configuration of the Talkaphone IP Call Station, navigate to the **Configuration → IP Settings** page. Configure the IP settings so that it conforms to the customer network requirements. Click **Save** when done.



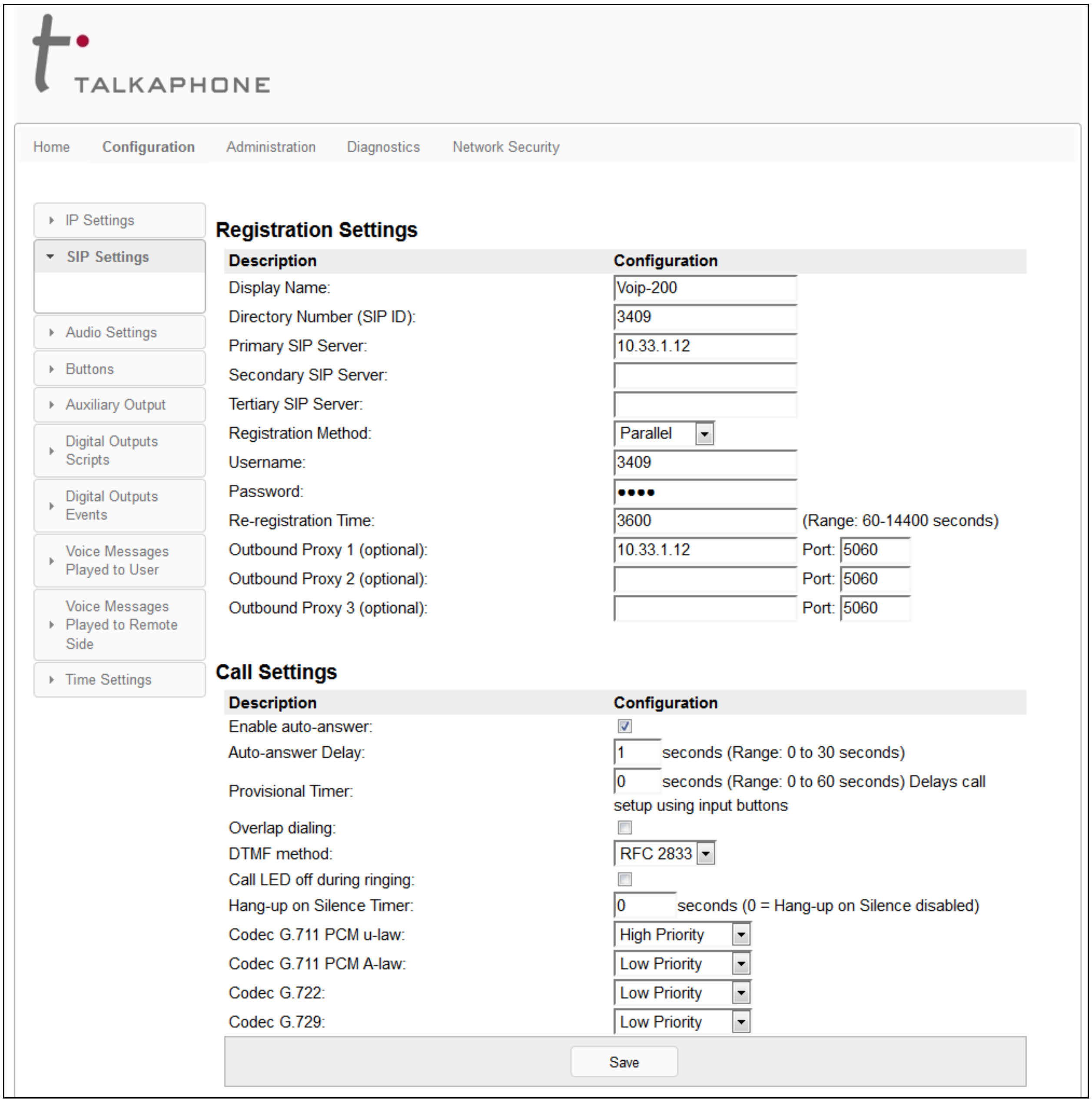
7.3. SIP Configuration

Navigate to **Configration → SIP Settings** to configure the SIP setting of the Talkaphone IP Call Station. Configure the following parameters.

- **Description**
  - **Display Name** – enter a descriptive name, e.g. VoIP-200
  - **Directory Number (SIP ID)** – enter the username "3409" as configured in **Section 6.7**
  - **Primary SIP Server** – enter the SIP signaling IP address of Session Manager
  - **Username** – enter the username "3409" as configured in **Section 6.7**
  - **Password** – enter the password of the SIP user "3409". This is the 'Communication Profile Password' as configured in Section 6.7.
  - **Re-registration time** – leave at the default value
  - **Outbound Proxy 1** – enter the SIP signaling IP address of Session Manager as configured in **Section 6.4**

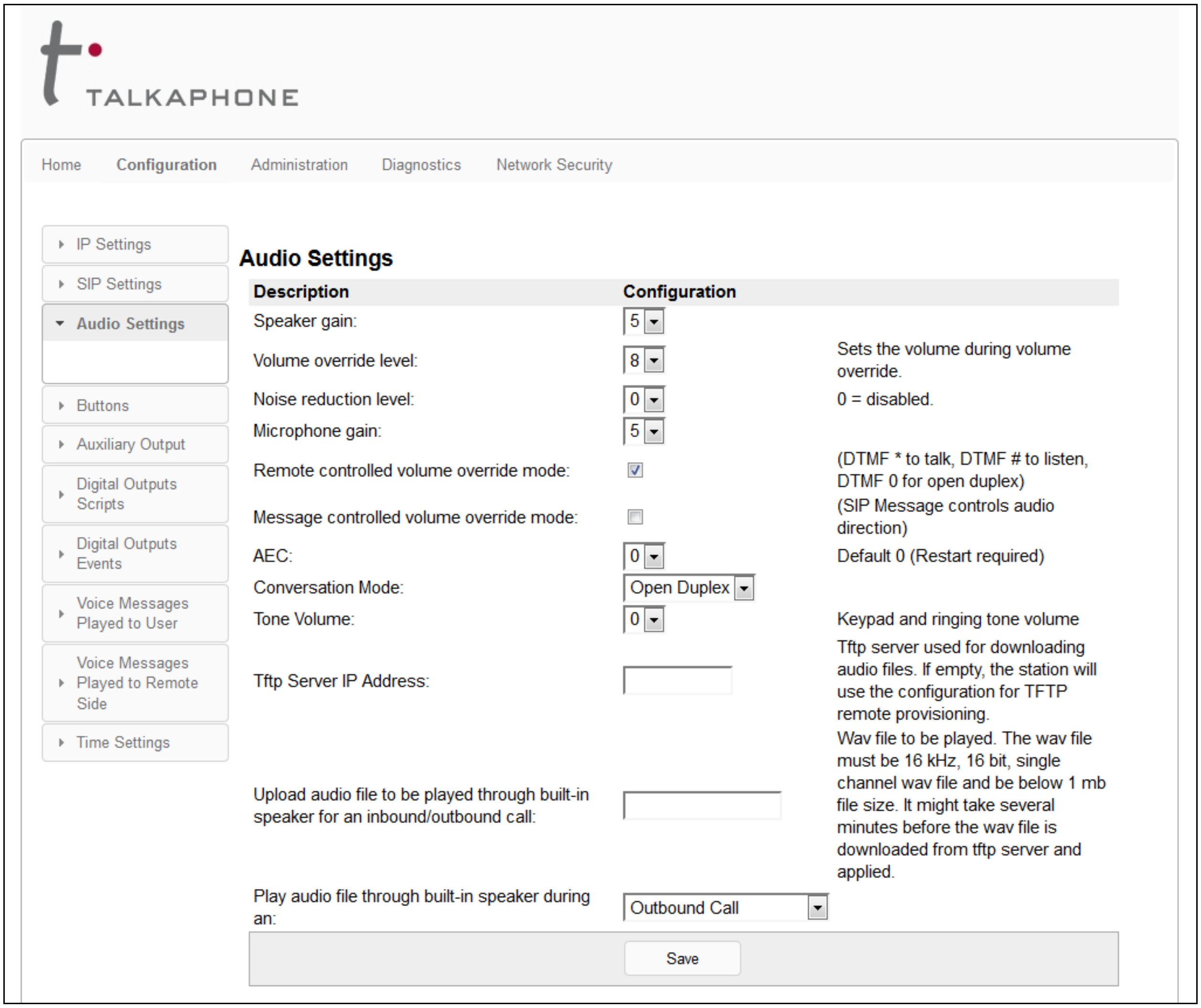
- **Call Settings**
  - **Enable auto-answer** – the VoIP-200 IP station will auto answer an incoming call if this feature enabled
  - **Auto-answer Delay** – enter time in second for the auto-answer delay
  - **Codec G.711 PCM u-law** – select "High Priority" in the drop-down menu

Leave other settings at default and click on **Save** button.



7.4. Configure Audio Settings

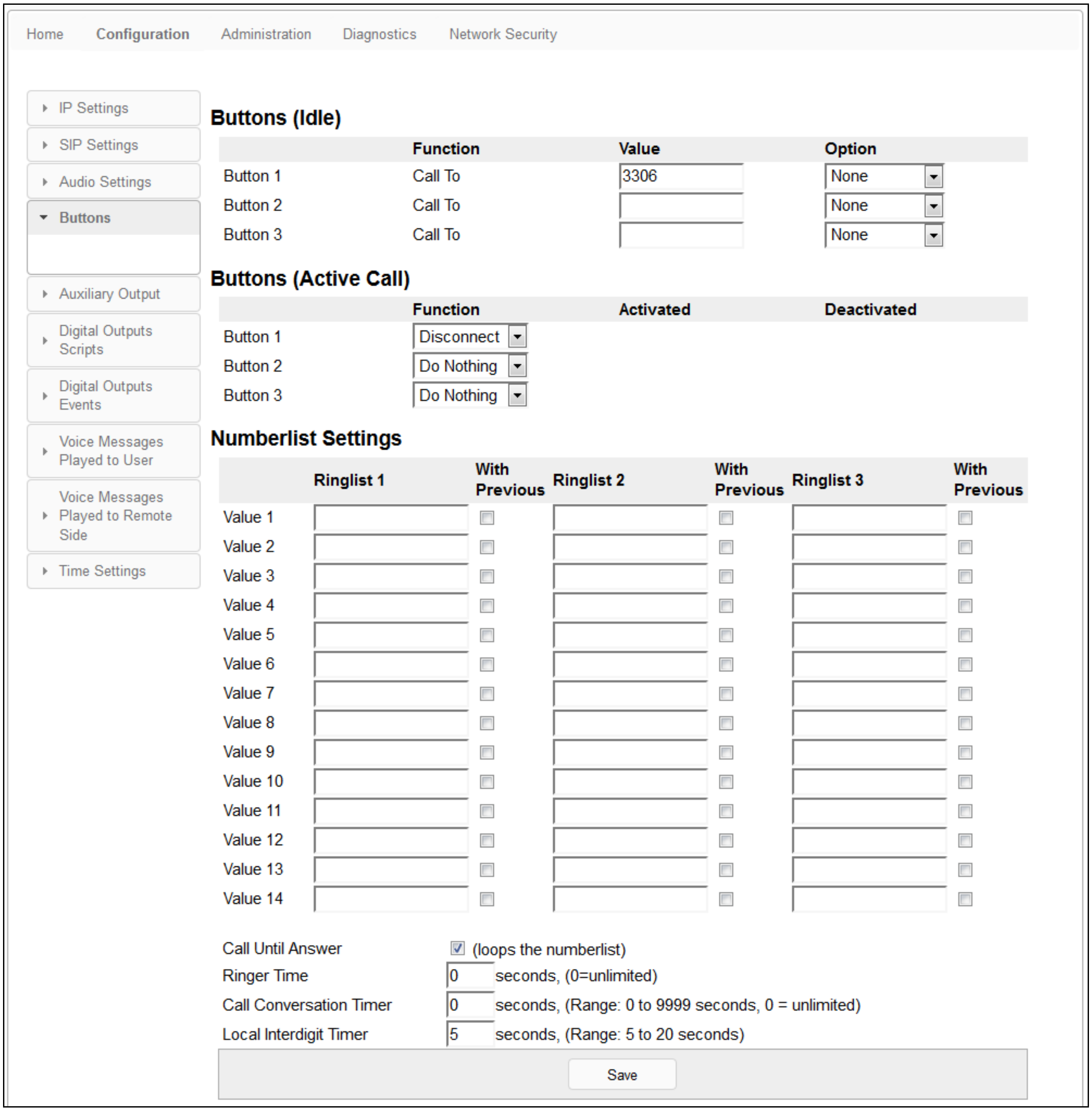
Navigate to **Configuration → Audio Settings** to configure Speaker gain, Volume override level, Noise reduction level. All fields were left at the default values. Click **Apply** when done.



7.5. Configure Buttons

Navigate to **Configuration → Buttons** to verify the appropriate settings. For the compliance test, the **Button 1** was configured as shown below. Note that the VoIP-200 only has one button.

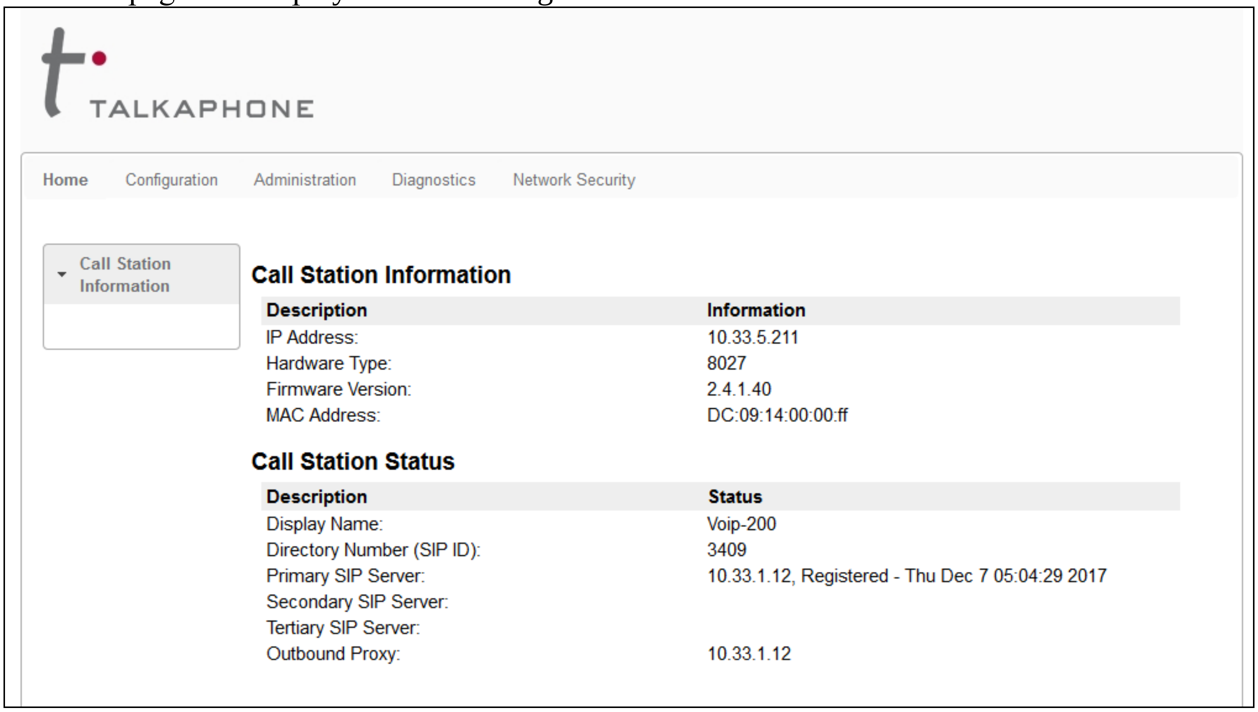
- **Buttons (Idle)** – Button 1: enter a phone number in **Value** field to make outbound call
- **Buttons (Active Call)** – Button 1: select "Disconnect" in the dropdown menu **Function** to enable the VoIP-200 ability to disconnect the call.



8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of the Talkaphone VOIP-200 Series IP Call Stations with Session Manager.

The ‘Home’ page will display the current Registration status.



From the Talkaphone IP station makes an outbound call to a local endpoint and verifies 2-way audio and proper call termination.

9. Conclusion

These Application Notes have described the administration steps required to integrate the Talkaphone VOIP-200 Series IP Call Stations with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Talkaphone IP Call Stations successfully registered with Avaya Aura® Session Manager and basic telephony features were verified. All test cases passed with observations noted in **Section 2.2**.

10. Additional References

This section references the Avaya and Talkaphone documentation relevant to these Application Notes. The following Avaya product documentation is available at support.avaya.com.

[1] Administering Avaya Aura® Communication Manager, Release 7.1, August 2017, Document Number 03-300509, Issue 1.

[2] Avaya Aura® Communication Manager Feature Description and Implementation, Release 7.1, August 2017, Document Number 555-245-205, Issue 1.

[3] Administering Avaya Aura® Session Manager, Release 7.1, Issue 1 August 2017

[4] Administering Avaya Aura® System Manager, Release 7.1, Issue 1, August, 2017

The following Talkaphone documentation may be found at www.talkaphone.com.

[5] *Talkaphone VOIP-200 Series Phone Configuration and Operation Manual v3.0.2*, Rev 7/31/2012.

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.