Avaya Solution & Interoperability Test Lab

Application Notes for Avtec Scout VoIP Console with Avaya Aura® Communication Manager and Avaya Aura® Session Manager – Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate Avtec Scout VoIP Console with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Avtec Scout VoIP Console is a SIP-based system that supports inbound and outbound calls, hold, resume, mute, and transfer, and integrates with Avaya Aura® Session Manager via a SIP trunk.

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 Avtec Scout VoIP Console with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Avtec Scout VoIP Console is a SIP-based system that supports inbound and outbound calls, hold, resume, mute, and transfer, and integrates with Avaya Aura® Session Manager via a SIP trunk.

2 General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing. The feature testing focused on establishing calls between Avtec Scout VoIP Console, Avaya SIP and H.323 IP Deskphones, and the PSTN, and exercising basic telephony features, such as hold, mute, and transfer.

The serviceability testing focused on verifying that Avtec Scout VoIP Console came back into service after re-connecting the Ethernet cable and rebooting the system. The following sub-section covers the features and functionality that were covered in more detail.

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 Avtec Scout VoIP Console did not include use of any specific encryption features as requested by Avtec.

2.1 Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- Establishing a SIP trunk between Scout VoIP Console and Session Manager. This includes verifying that Scout VoIP Console successfully responds to SIP OPTIONS messages.
- Calls between Scout VoIP Console and Avaya SIP/H.323 IP Deskphones with Direct IP Media (Shuffling) enabled and disabled.

- Calls between Scout VoIP Console and the PSTN.
- G.711 and G.729 codec support.
- Proper recognition of DTMF tones from Scout VoIP Console.
- Basic telephony features, including hold, mute, redial, multiple calls, and blind/attended transfers.
- Proper system recovery after a reboot of Scout VoIP Console and loss of IP connectivity.

2.2 Test Results

All test cases passed with the following observations.

- Scout VoIP Console does not currently support conferencing.
- SIP TLS transport and SRTP is currently not supported by Scout VoIP Console.

2.3 Support

Avtec Technical Support for Scout VoIP Console can be obtained via phone, website, or email.

- **Phone:** 1 (800) 545-3034
  1 (803) 358-3600 x1201
- **Web:** http://www.avtecinc.com/support
- **Email:** customersupport@avtecinc.com

3 Reference Configuration

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

- Communication Manager running in a virtual environment with a G450 Media Gateway.
- Session Manager connected to Communication Manager and Scout VoIP Console via SIP trunks. Session Manager was configured using Avaya Aura ® System Manager.
- Avaya Aura® Media Server running in a virtual environment (not shown).
- Avaya H.323 and SIP telephones.
- Scout VoIP Console connected to Session Manager via a SIP trunk.

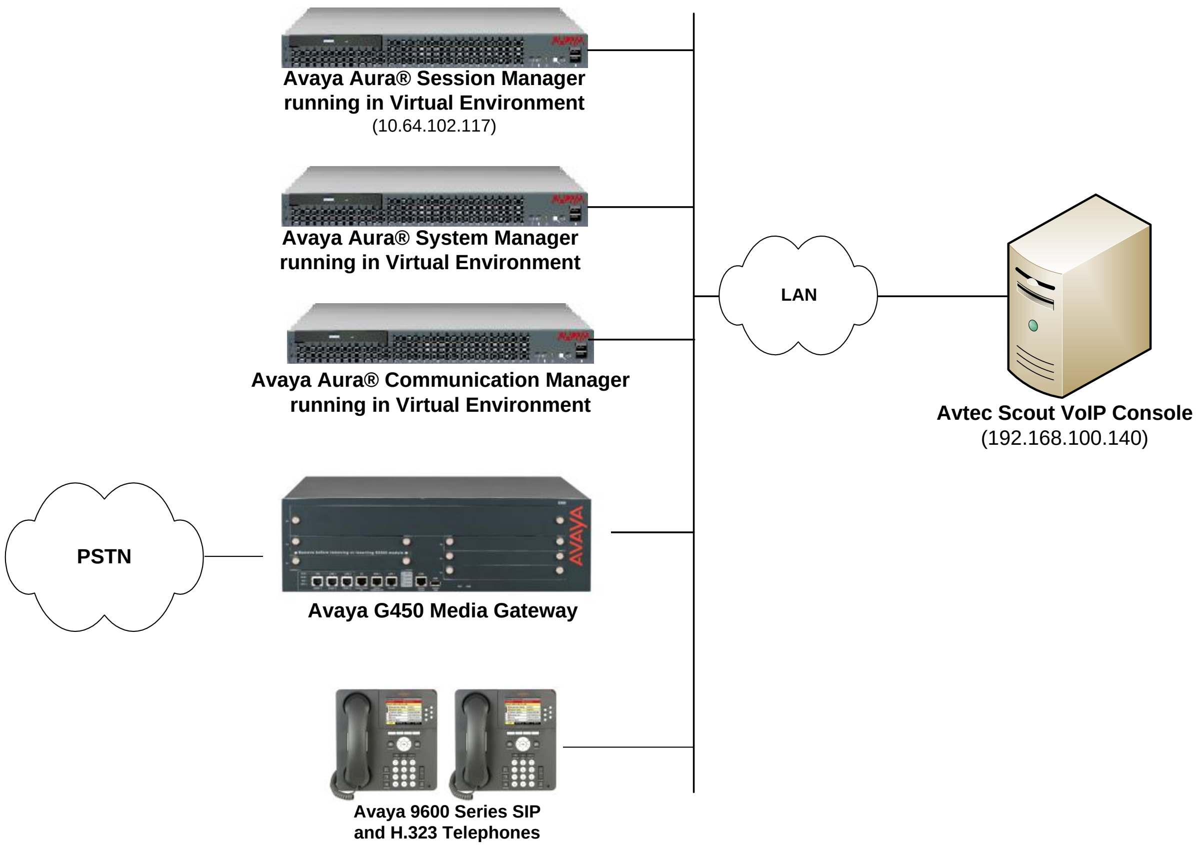


Figure 1: Avaya SIP Telephony Network with Avtec Scout VoIP Console

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 in a Virtual Environment with an Avaya G450 Media Gateway	7.0.1.2 SP 2 (R017x.00.0.441.0 with Patch 23523)
Avaya Aura® Media Server running in a Virtual Environment	7.7.0.375
Avaya Aura® System Manager running in a Virtual Environment	7.0.1.2 (Build No. 7.0.0.016266 Software Update Revision No: 7.0.1.0.086224 Service Pack 2)
Avaya Aura® Session Manager running in a Virtual Environment	7.0.1 SP 2 (7.0.1.2.701230)
Avaya Aura® Messaging	6.3.2 SP 2 Patch 3
Avaya 96x1 Series IP Deskphones	6.6401U (H.323) 7.0.1.4.6 (SIP)
Avtec Scout VoIP Console running on Microsoft Windows 7, including the following components: ▪ Scout Console ▪ Scout VPGate ▪ Scout SIP Proxy	 4.3.13.5 4.3.13.5 4.3.13.5

5 Configure Avaya Aura® Communication Manager

This section describes the steps for configuring a SIP trunk to Session Manager and routing calls to Scout. Administration of Communication Manager was performed using the System Access Terminal (SAT).

This section covers the following configuration:

- **IP Node Names** to associate names with IP addresses.
- **IP Codec Set** to specify the codec type used for calls to Scout VoIP Console.
- **IP Network Region** to specify the domain name and the IP codec set, to enable IP-IP direct audio (i.e., Shuffling), and to specify the UDP port range.
- **SIP trunk** for calls towards Session Manager and Scout.
- **Private Numbering** to allow the caller's extension to be sent to Scout VoIP Console.
- **Call Routing** to route calls to Scout VoIP Console using AAR.

5.1 Administer IP Node Names

In the **IP Node Names** form, assign an IP address and host name for Communication Manager (*procr*) and Session Manager (*devcon-sm*). The host names will be used in other configuration screens of Communication Manager.

```
change node-names ip                                              Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
default             0.0.0.0
devcon-ams          10.64.102.118
devcon-sm           10.64.102.117
procr               10.64.102.115
procr6              ::

( 5  of 5    administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

5.2 Administer IP Codec Set

In the **IP Codec Set** form, select the audio codec type supported for calls routed over the SIP trunk to Scout VoIP Console. The form is accessed via the **change ip-codec-set 1** command. Note the codec set number since it will be used in the IP Network Region covered in the next section. For the compliance test, G.711MU and G.729 codecs were used.

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

                          IP CODEC SET
    Codec Set: 1

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

5.3 Administer IP Network Region

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is *avaya.com*. By default, **IP-IP Direct Audio** (shuffling) is enabled to allow audio traffic to be sent directly between Scout VoIP Console and IP endpoints without using media resources in the Avaya G450 Media Gateway or Avaya Media Server. The **IP Network Region** form also specifies the **IP Codec Set** to be used for calls routed over the SIP trunk to Session Manager. This codec set is used when its corresponding network region (i.e., IP Network Region 1) is specified in the SIP signaling group.

```
change ip-network-region 1                                    Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: avaya.com
    Name:                      Stub Network Region: n
MEDIA PARAMETERS               Intra-region IP-IP Direct Audio: yes
      Codec Set: 1             Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                     IP Audio Hairpinning? 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 SIP Trunk to Session Manager

Prior to configuring a SIP trunk group for communication with Session Manager, a SIP signaling group must be configured. Configure the **Signaling Group** form as follows:

- Set the **Group Type** field to *sip*.
- Set the **IMS Enabled** field to *n*.
- The **Transport Method** field was set to *tls*.
- Specify the Ethernet processor (*procr*) of Communication Manager and Session Manager as the two ends of the signaling group in the **Near-end Node Name** field and the **Far-end Node Name** field, respectively. These field values are taken from the **IP Node Names** form in **Section 5.1**.
- Ensure that the TLS port value of *5061* is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- The preferred codec for the call will be selected from the IP codec set assigned to the IP network region specified in the **Far-end Network Region** field.
- Enter the domain name of Session Manager in the **Far-end Domain** field. In this configuration, the domain name is *avaya.com*.
- The **Direct IP-IP Audio Connections** field was enabled on this form.
- The **DTMF over IP** field should be set to the default value of *rtp-payload*.

Communication Manager supports DTMF transmission using RFC 2833. The default values for the other fields may be used.

```
add signaling-group 10                                       Page   1 of   2
                                SIGNALING GROUP

 Group Number: 10              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: 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: devcon-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
```

Configure the **Trunk Group** form as shown below. This trunk group is used for SIP calls to Scout VoIP Console. Set the **Group Type** field to *sip*, set the **Service Type** field to *tie*, specify the signaling group associated with this trunk group in the **Signaling Group** field, and specify the **Number of Members** supported by this SIP trunk group. Accept the default values for the remaining fields.

```
add trunk-group 10                                          Page   1 of  21
                                TRUNK GROUP

Group Number: 10                   Group Type: sip          CDR Reports: y
  Group Name: To devcon-sm                COR: 1        TN: 1        TAC: 1010
   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: 10
                                                    Number of Members: 10
```

On **Page 3** of the trunk group form, set the **Numbering Format** field to *private*. This field specifies the format of the calling party number sent to the far-end.

```
add trunk-group 10                                          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

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

 Show ANSWERED BY on Display? y
```

On **Page 4** of the trunk group form, the default settings were used as shown below.

```
add trunk-group 10                                          Page   4 of  21
                              PROTOCOL VARIATIONS

                                       Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                       Send Transferring Party Information? n
                                  Network Call Redirection? n

                                     Send Diversion Header? n
                                   Support Request History? y
                              Telephone Event Payload Type:

                        Convert 180 to 183 for Early Media? n
                  Always Use re-INVITE for Display Updates? n
                        Identity for Calling Party Display: P-Asserted-Identity
            Block Sending Calling Party Location in INVITE? n
                 Accept Redirect to Blank User Destination? n
                                              Enable Q-SIP? n
          Interworking of ISDN Clearing with In-Band Tones: keep-channel-active
                                Request URI Contents: may-have-extra-digits
```

5.5 Configure Private Numbering

Configure the **Numbering – Private Format** form to send the calling party number to the far-end. Add an entry so that local stations with a 5-digit extension beginning with '7' whose calls are routed over any trunk group, including SIP trunk group 10, have the extension sent to Scout VoIP Console.

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

Ext Ext              Trk        Private           Total
Len Code             Grp(s)     Prefix            Len
 5  7                                             5     Total Administered: 1
                                                           Maximum Entries: 540
```

The **Numbering – Public/Unknown Format** form was also configured as shown below.

```
change public-unknown-numbering 0                               Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                         Total
Ext Ext             Trk       CPN             CPN
Len Code            Grp(s)    Prefix          Len
                                                    Total Administered: 1
 5  7                                         5        Maximum Entries: 240

                                                    Note: If an entry applies to
                                                    a SIP connection to Avaya
                                                    Aura(R) Session Manager,
                                                    the resulting number must
                                                    be a complete E.164 number.

                                                    Communication Manager
                                                    automatically inserts
                                                    a '+' digit in this case.
```

5.6 AAR Call Routing

Configure the uniform dial plan table to route calls using AAR for dialed digits that are 5-digits long and begin with '78'. This would cover call routing to the Scout VoIP Console extensions (i.e., 78800 – 78803). For the compliance test, four Scout VoIP Console lines were configured as shown in **Section 7.3**.

```
change uniform-dialplan 7                                       Page   1 of   2
                       UNIFORM DIAL PLAN TABLE
                                                              Percent Full: 0

  Matching                   Insert              Node
  Pattern       Len Del      Digits      Net Conv Num
 78              5   0                   aar  n
```

SIP calls to Session Manager are routed over a SIP trunk via AAR call routing. Configure the AAR analysis form and add an entry that routes digits beginning with "78" to route pattern 10 as shown below. Note that the **Call Type** was set to *lev0*. This routes calls to SIP stations and to Scout VoIP Console.

```
change aar analysis 7                                           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
    7                     7    7      254       aar          n
    78                    5    5      10        lev0         n
    8                     7    7      254       aar          n
    9                     7    7      254       aar          n
                                                             n
                                                             n
```

Configure a preference in **Route Pattern** 10 to route calls over SIP trunk group 10 as shown below.

```
change route-pattern 10                                         Page   1 of   3
                    Pattern Number: 10      Pattern Name: To devcon-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: 10   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                               unk-unk   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
```

6 Configure Avaya Aura® Session Manager

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

- Adaptation
- SIP Entity for Scout VoIP Console
- Entity Link, which defines the SIP trunk parameters used by Session Manager when routing calls to/from Scout VoIP Console
- Routing Policies and Dial Patterns
- Session Manager, corresponding to the Avaya Aura® Session Manager Server to be managed by Avaya Aura® System Manager

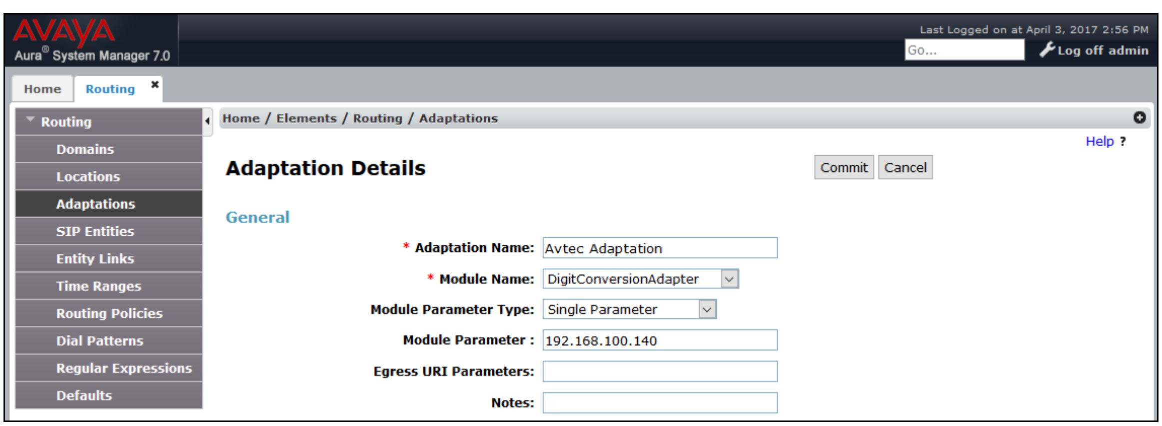
Configuration is accomplished by accessing the browser-based GUI of Avaya Aura® System Manager using the URL "https://<*ip-address*>/SMGR", where <*ip-address*> is the IP address of Avaya Aura® System Manager. Log in with the appropriate credentials.

Note: It is assumed that basic configuration of Session Manager has already been performed. *This section will focus on the configuration of the adaptation, SIP entity, entity link, and call routing for Avtec Scout VoIP Console only*.

6.1 Add Adaptation

Session Manager can be configured with Adaptations that can modify SIP messages before or after routing decisions have been made; for example, replacing a domain name with an IP address as shown in this section. To create an **Adaptation** that will be applied to the Scout VoIP Console SIP entity in **Section 6.2**, navigate to **Elements → Routing → Adaptations** and click on the **New** button (not shown). In the **General** section, enter the following values. Use default values for all remaining fields.

- **Adaptation Name:** Enter a descriptive name for the Adaptation (e.g., *Avtec Adaptation*).
- **Module Name:** Select **DigitConversionAdapter**.
- **Module Parameter Type:** Select **Single Parameter**.
- **Module Parameter:** Enter the Scout VoIP Console IP address.



6.2 Add SIP Entity for Avtec Scout VoIP Console

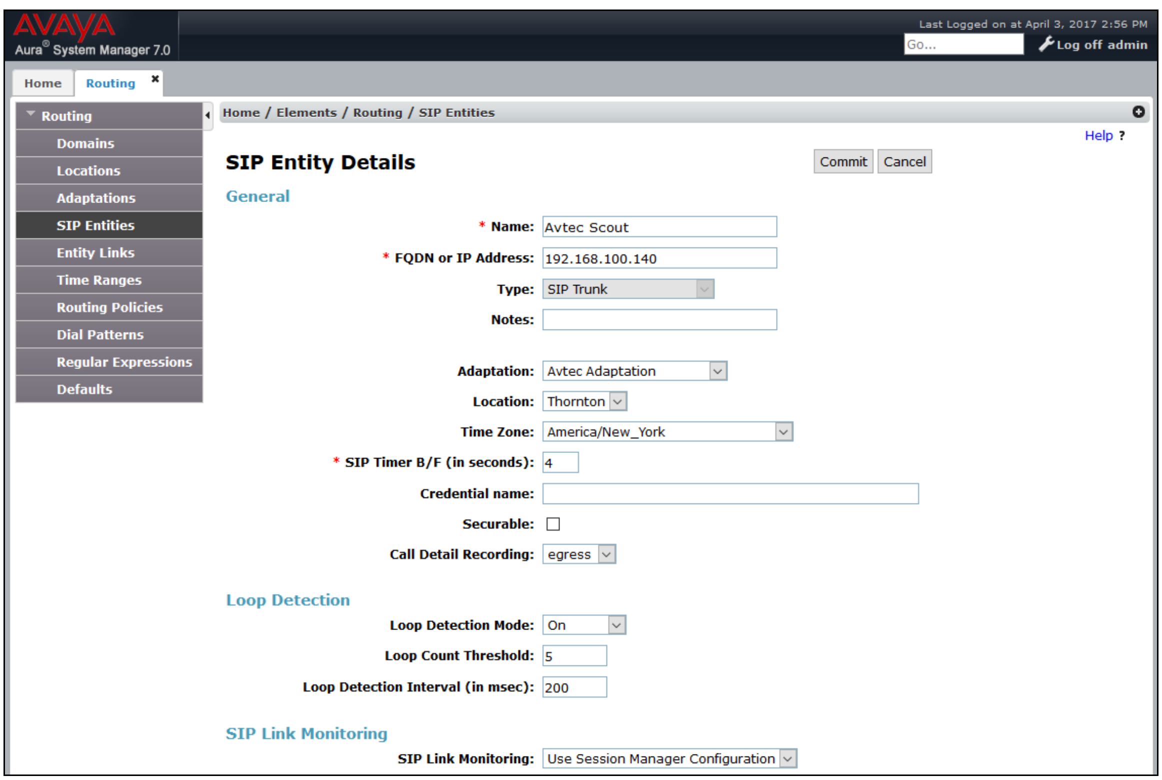
In the sample configuration, one SIP trunk was configured for Scout VoIP Console, which provided four lines with four different extensions for this compliance test. These SIP extensions registered with the internal Scout VoIP Console SIP registrar/proxy, not with Session Manager.

A SIP Entity must be added for Scout VoIP Console. This SIP entity will have an adaption rule to convert the domain name in the SIP URL of INVITE message to the Scout VoIP Console IP address and vice versa. To add a SIP Entity, select **SIP Entities** on the left and click on the **New** button on the right (not shown). The following screen is displayed. Fill in the following:

Under *General*:

- **Name:** A descriptive name.
- **FQDN or IP Address:** IP address of the Scout VoIP Console.
- **Type:** Select *SIP trunk*.
- **Adaptation :** Specify the adaptation configured in **Section 6.1**.
- **Location:** Select the location defined previously (not shown).
- **Time Zone:** Time zone for this location.

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



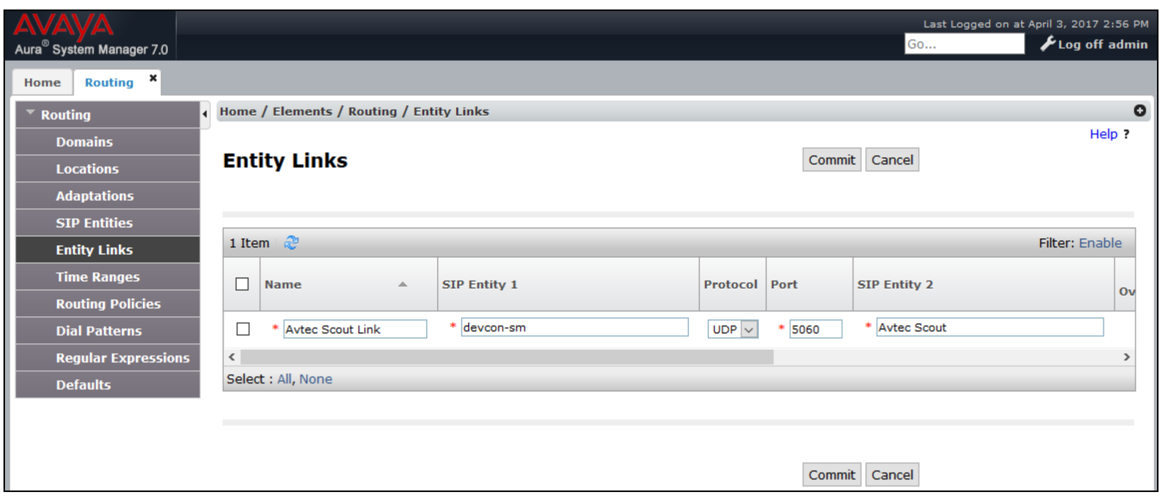
6.3 Add Entity Link for Avtec Scout VoIP Console

This section covers the configuration of an Entity Link for Scout VoIP Console. This entity link will specify that SIP entity configured in **Section 6.2.**

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

- **Name:** A descriptive name (e.g., *Avtec Scout Link*).
- **SIP Entity 1:** Select Session Manager.
- **Protocol:** Select the appropriate protocol (e.g., *UDP*).
- **Port:** Port number to which the other system sends SIP requests.
- **SIP Entity 2:** Select the Scout SIP entity configure in **Section 6.2**.
- **Port:** Port number on which the other system receives SIP requests.
- **Connection Policy:** Select *Trusted*. *Note: If Trusted is not selected, calls from the associated SIP Entity specified in* ***Section 6.3*** *will be denied.*

Click **Commit** to save the Entity Link definition.



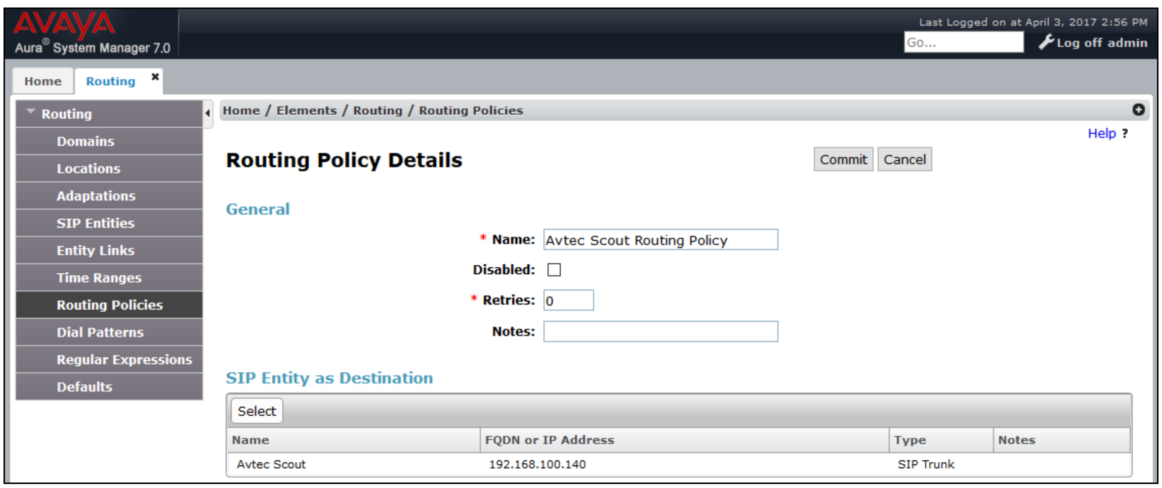
6.4 Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the Scout VoIP Console SIP Entity specified in **Section 6.2.** To add a routing policy, select **Routing Policies** on the left and click on the **New** button (not shown) on the right. The following screen is displayed. Fill in the following:

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

Under *SIP Entity as Destination*:
Click **Select** and then select the appropriate SIP entity to which this routing policy applies. In this case, the Scout VoIP Console SIP entity is selected.

Defaults can be used for the remaining fields. Click **Commit** to save the Routing Policy definition. The following screen shows the Routing Policy for Scout VoIP Console.



6.5 Add Dial Patterns

Dial patterns must be defined to direct calls to the appropriate SIP Entity. In the sample configuration, a 5-digit number beginning with '788' will be routed to lines on Scout VoIP Console.

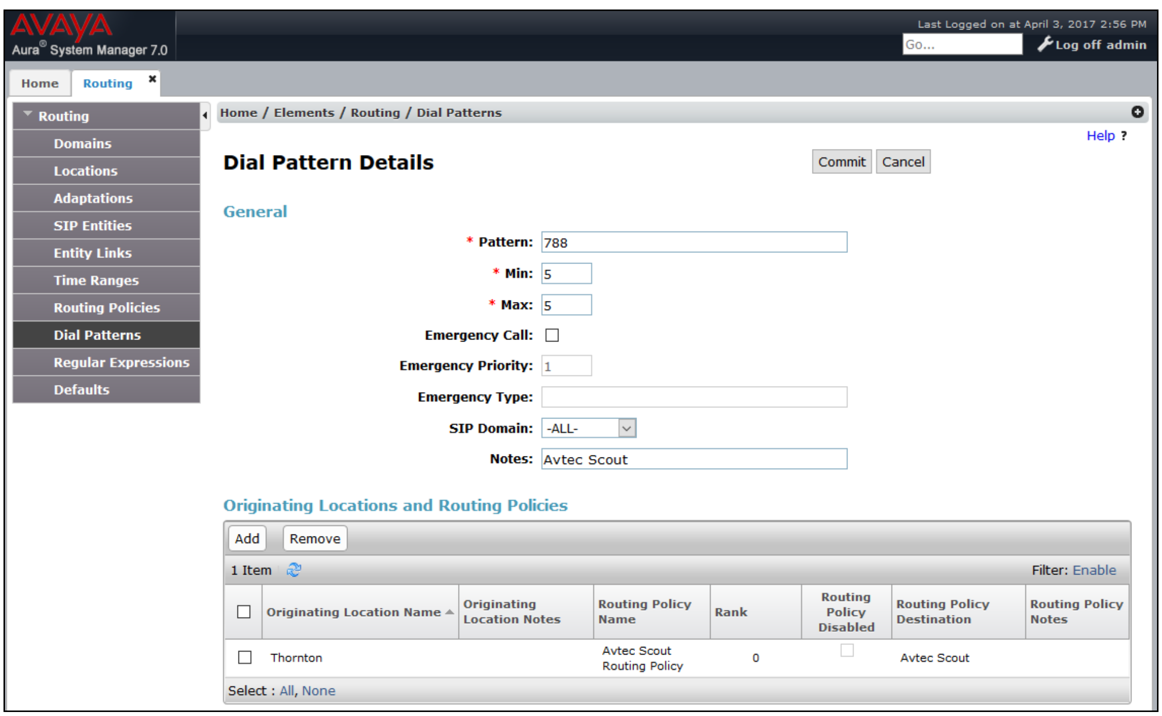
To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button (not shown) on the right. Fill in the following:

Under *General*:

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

Under *Originating Locations and Routing Policies*:
Click **Add** and then select the appropriate location and routing policy from the list. In this case, the Scout VoIP Console routing policy is selected.

Default values can be used for the remaining fields. Click **Commit** to save this dial pattern. The following screen shows the dial pattern definitions for extensions on Scout VoIP Console.



6.6 Add Session Manager

Adding the Session Manager will provide the linkage between System Manager and Session Manager. Expand the **Session Manager** menu on the left and select **Session Manager Administration**. Then click **Add** (not shown), and fill in the fields as described below and shown in the following screen:

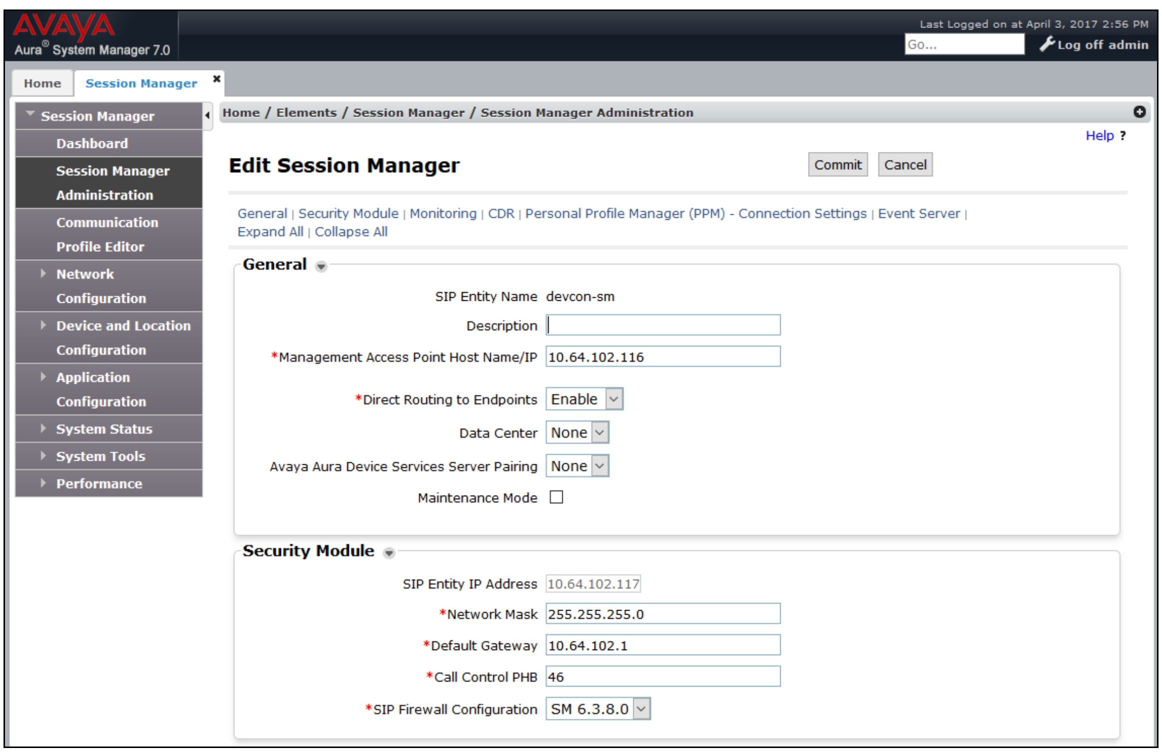
Under *General*:

- **SIP Entity Name:** Select the name of the SIP Entity added for Session Manager
- **Description:** Descriptive comment (optional)
- **Management Access Point Host Name/IP:** Enter the IP address of the Session Manager management interface.

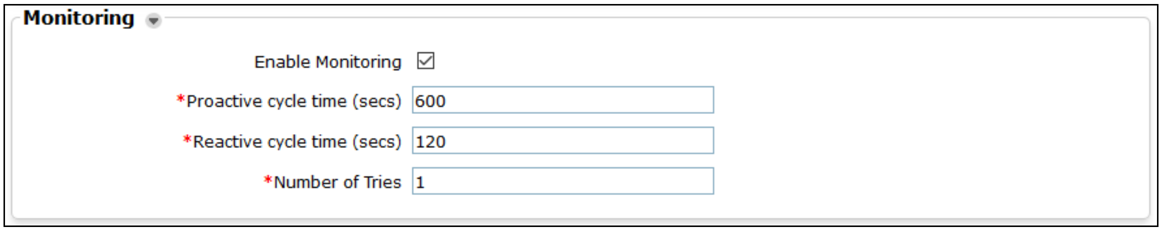
Under *Security Module*:

- **Network Mask:** Enter the network mask corresponding to the IP address of Session Manager
- **Default Gateway**: Enter the IP address of the default gateway for Session Manager

Use default values for the remaining fields. Click **Commit** to add this Session Manager.



The following screen shows the **Monitoring** section, which determines how frequently Session Manager sends SIP Options messages to Scout VoIP Console. Use default values for the remaining fields. Click **Commit** to add this Session Manager. In the following configuration, Session Manager sends a SIP Options message every 600 secs. If there is no response, Session Manager will send a SIP Options message every 120 secs.



7 Configure Avtec Scout VoIP Console

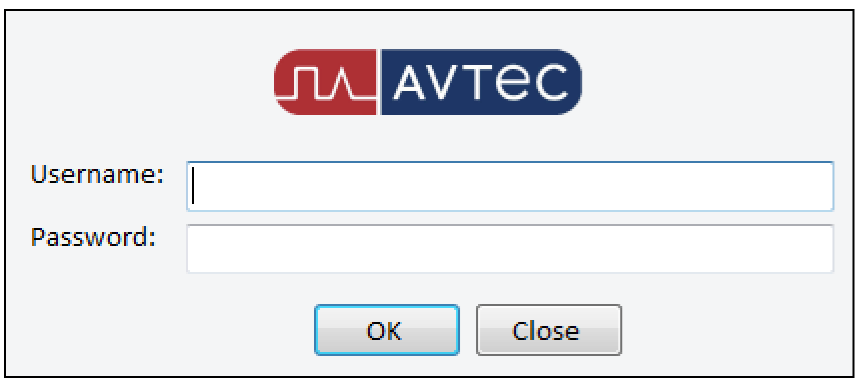
This section covers the configuration of Scout VoIP Console using the **Scout Manager** application. This section assumes that the Scout VoIP Console software has already been installed successfully. In the **Scout Manager** application, the following procedures are performed:

- Launch Scout Manager
- Add Local Domain
- Add SIP Users
- Add Access Control List (ACLs) – Trusted Endpoints
- Add Routes
- Add Endpoints

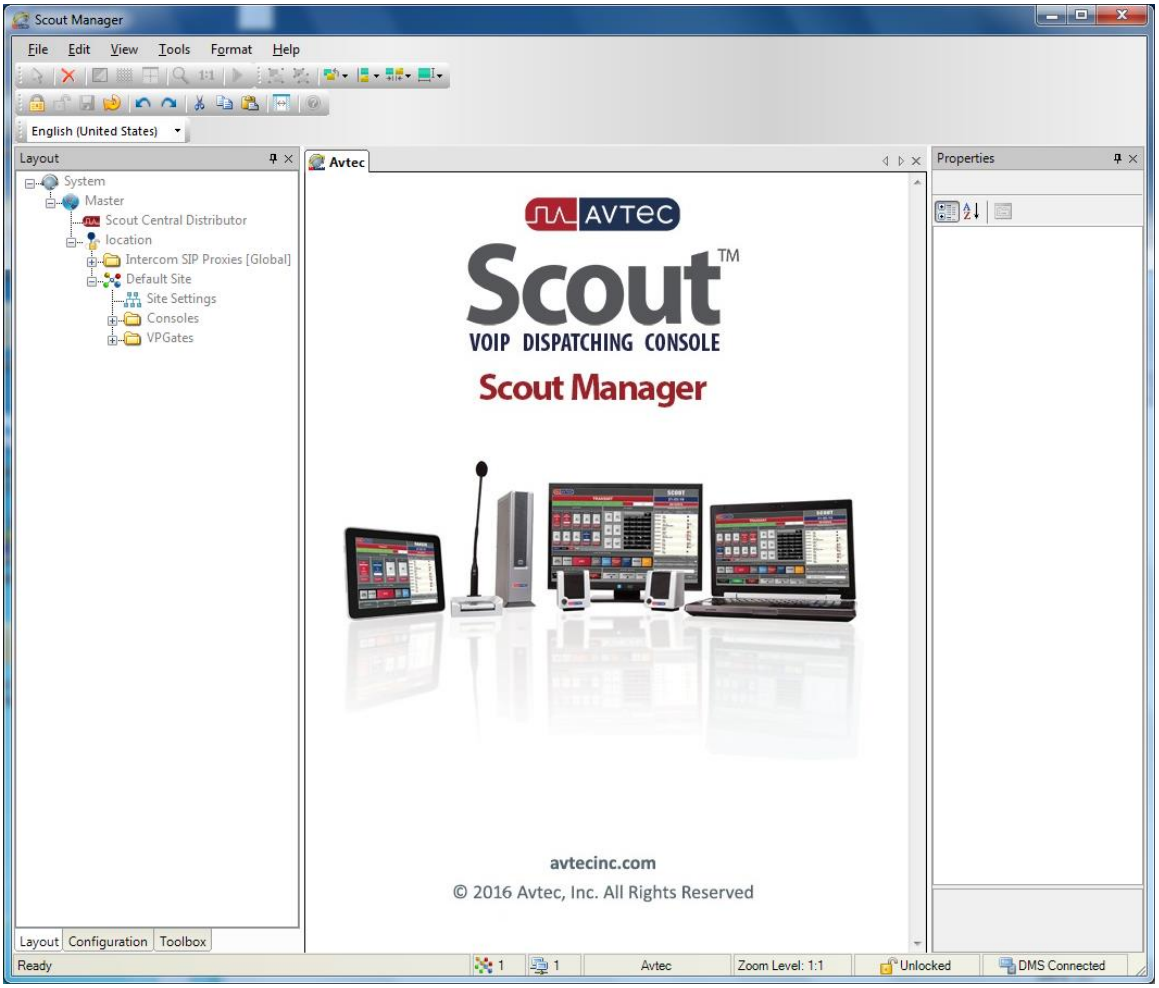
7.1 Launch Scout Manager

Log into the **Scout Manager** application by clicking on the appropriate 

icon. The following screen is displayed. Log in with the appropriate credentials.

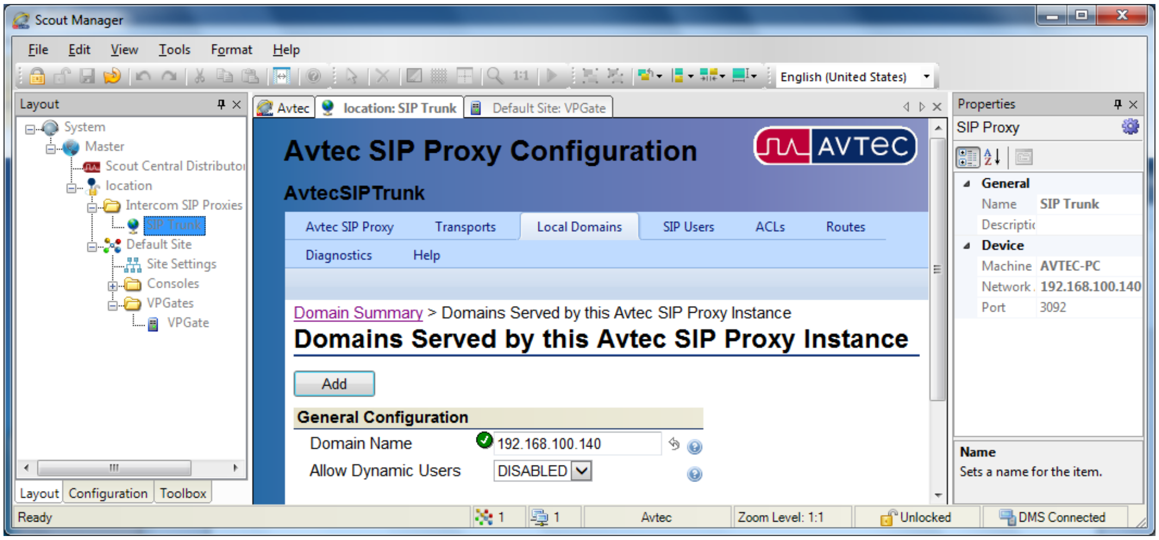


Once logged in, the **Scout Manager** screen appears as shown below.



7.2 Add Local Domain

Create an Avtec SIP Proxy domain. Navigate to **SIP Trunk → Local Domains** and click the **Add** button (not shown). The **Domains Served by this Avtec SIP Proxy Instance** page is displayed as shown below. For the **Domain Name**, enter the IP address of the Scout VoIP Console. Click the **Add** button.



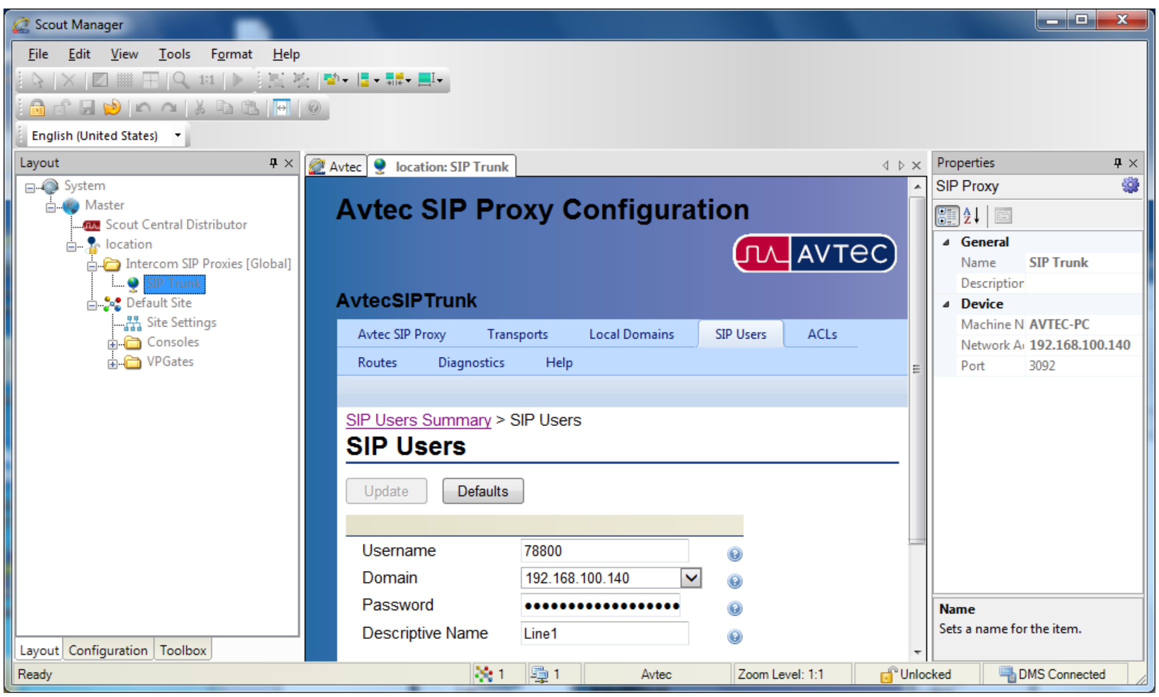
7.3 Add SIP Users

Add SIP users for the Scout VoIP Console. These SIP users register with the Avtec SIP Proxy, not Session Manager. Calls destined for these SIP users are routed over the SIP trunk between Session Manager and the Scout VoIP Console. Incoming calls are then routed to a SIP user based on the SIP URI. Outgoing calls from a SIP user is routed over the SIP trunk to Session Manager, which will in turn route the call to Communication Manager.

To add a SIP user, navigate to **SIP Trunk → SIP Users** and click the **Add** button (not shown). The SIP Users page is displayed as shown below. Configure the following parameters:

- **Username:** Specify the SIP extension (e.g., *78800*).
- **Domain:** Specify the local domain configured in **Section 7.2**.
- **Password:** Specify the password specified in **Section 7.6**.
- **Descriptive Name:** Specify a descriptive name for the line.

Click the **Add** button. Repeat for each line required by Scout VoIP Console. For the compliance test, four SIP users were created with extensions 78800-78803).



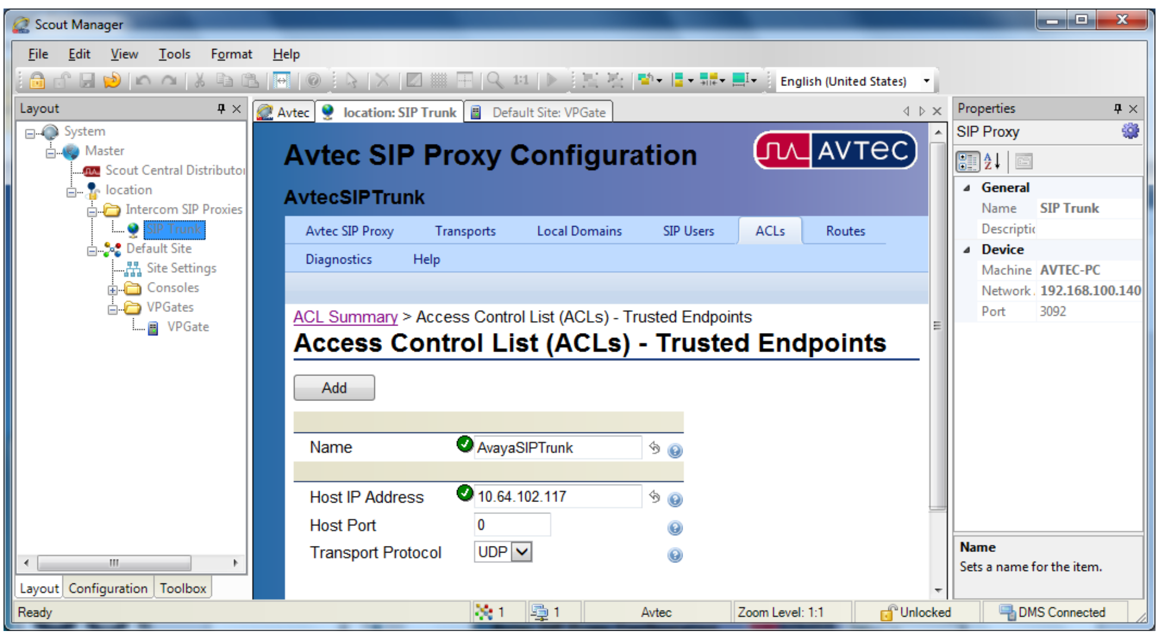
7.4 Add Access Control List (ACLs) – Trusted Endpoint

Configure an access control list (ACL) for SIP trunking. An ACL is added to trust calls from Session Manager. Navigate to **SIP Trunk → ACLs** and click the **Add** button as shown below (not shown).

The **Access Control List (ACL) – Trusted Endpoints** page is displayed as shown below. Configure the following parameters as follows:

- **Name:** Provide a descriptive name (e.g., *AvayaSIPTrunk*).
- **Host IP Address:** Specify the SIP signaling interface of Session Manager (i.e., *10.64.102.117*).
- **Host Port:** Enter '0' to trust traffic coming from any port.
- **Transport Protocol:** Specify the transport protocol (i.e., *UDP*).

Click the **Add** button.

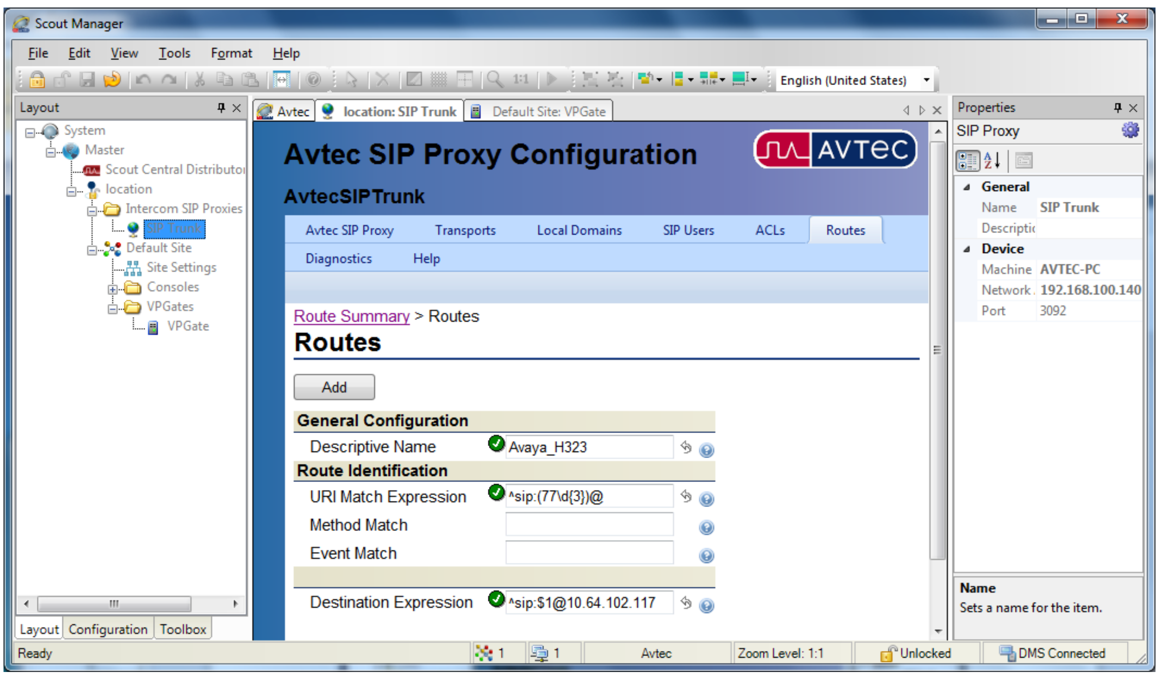


7.5 Add Routes

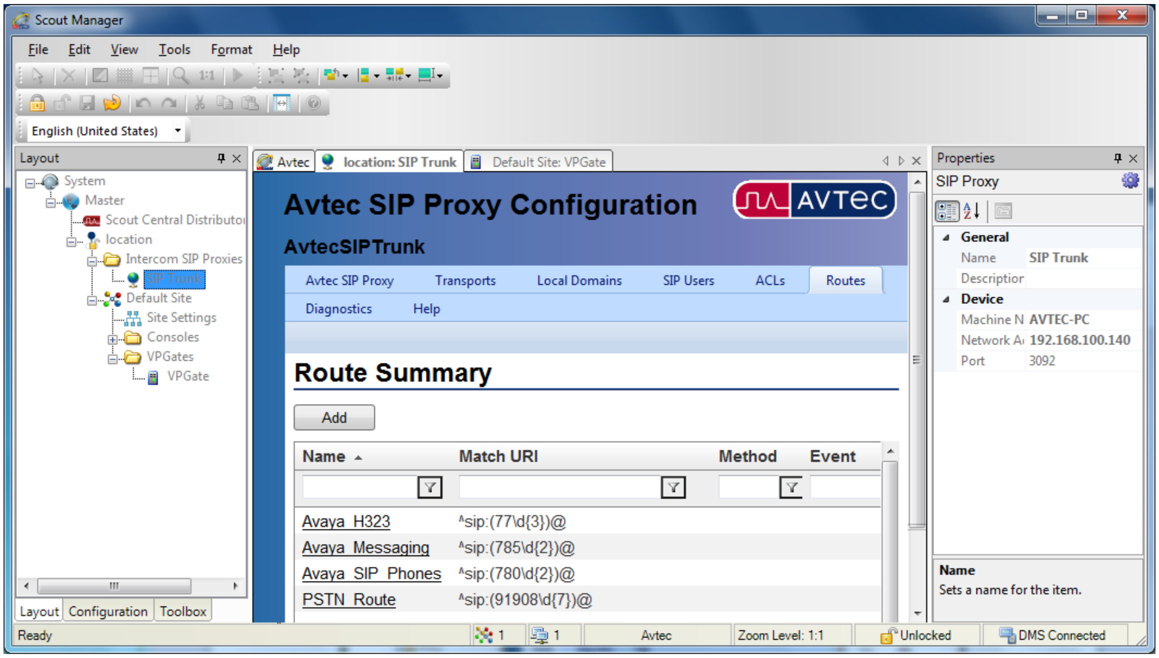
Configure routes for calls destined to local H.323 and SIP stations, voicemail system, and PSTN, as necessary. Navigate to **SIP Trunk → Routes** and click the **Add** button (not shown). The **Routes** page is displayed. For example, to route calls to local H.323 stations, the following parameters were configured:

- **Descriptive Name:** Provide a descriptive route name.
- **URI Match Expression:** Enter an expression that identifies a route for calls with a 5-digit dial number starting with '77', such as ^*sip:(77\d{3})@*
- **Destination Expression:** Enter the destination URI that routes calls to Session Manager. In this case, the expression used was ^*sip:$1@10.64.102.117*.

Click the **Add** button.



Add additional Routes as necessary. For the compliance test, the following Routes were configured.



7.6 Add Endpoints

Endpoints are created under VPGate configuration. One endpoint was created per SIP user or line. Navigate to **VPGate → Endpoints** and click the **Add** button in the Endpoint Summary page (not shown). The **Endpoint Configuration** page is displayed as shown below.

Under **Endpoint Configuration**:

- **Endpoint Name:** Specify a descriptive name (e.g., *Line1*).
- **Service State:** Set to *Available*.

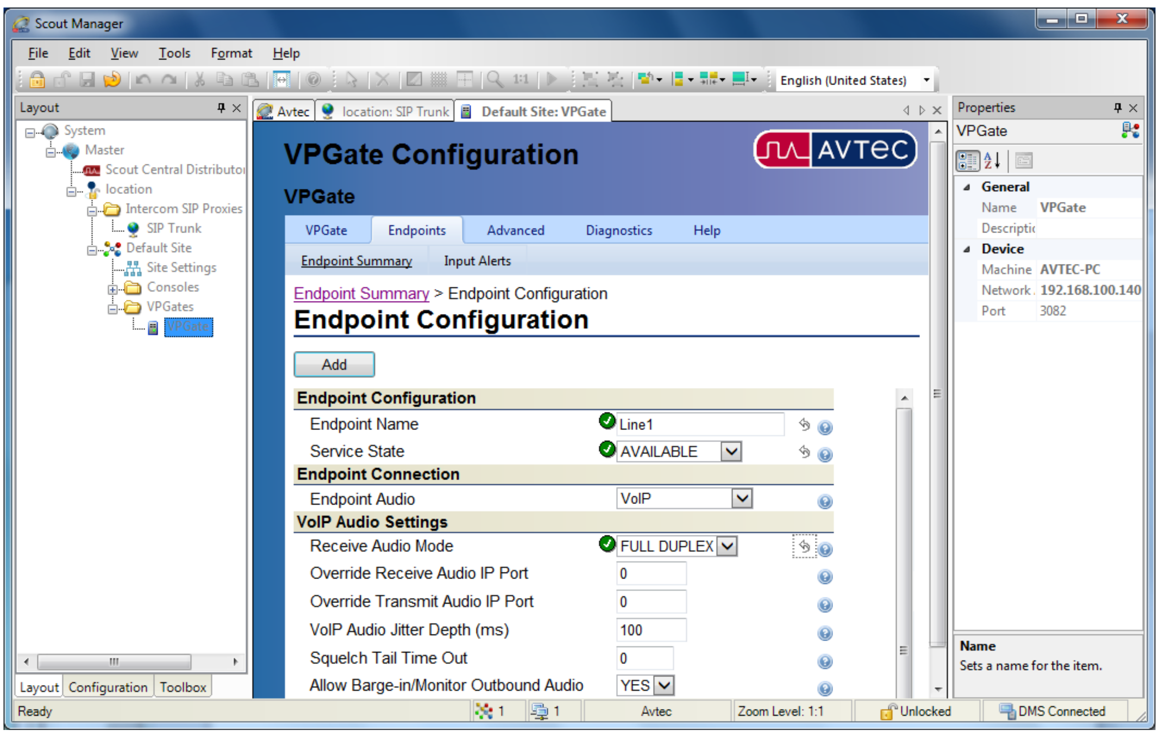
Under **Endpoint Connection**:

- **Endpoint Audio:** Set to *VoIP*.

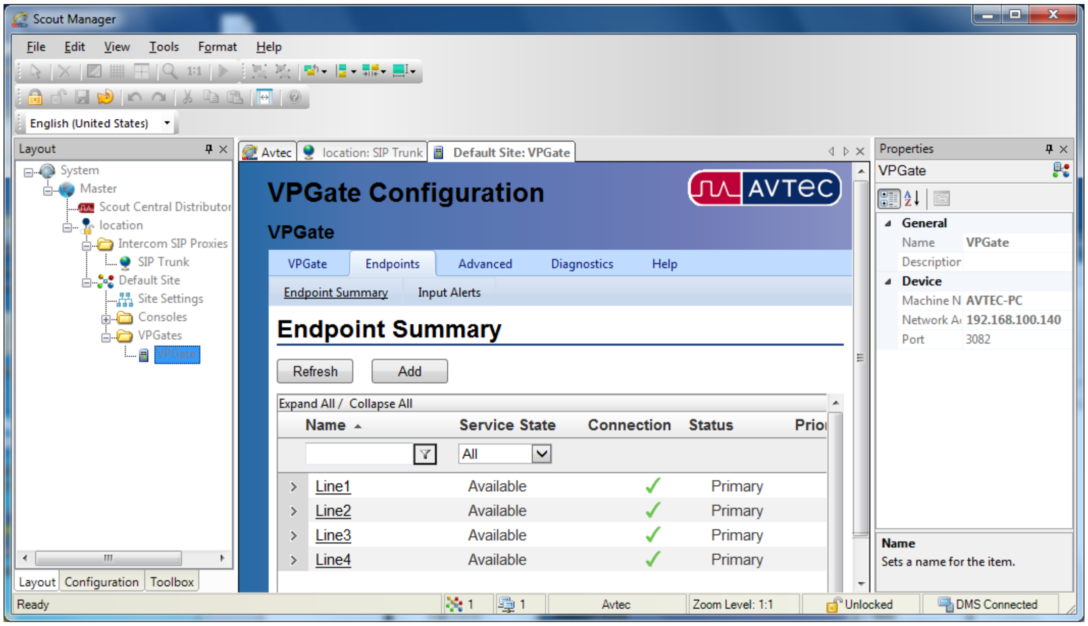
Under **VoIP Audio Settings**:

- **Receive Audio Mode**: Set to *FULL DUPLEX*.

Use the default settings for the remaining fields. Click the **Add** button.

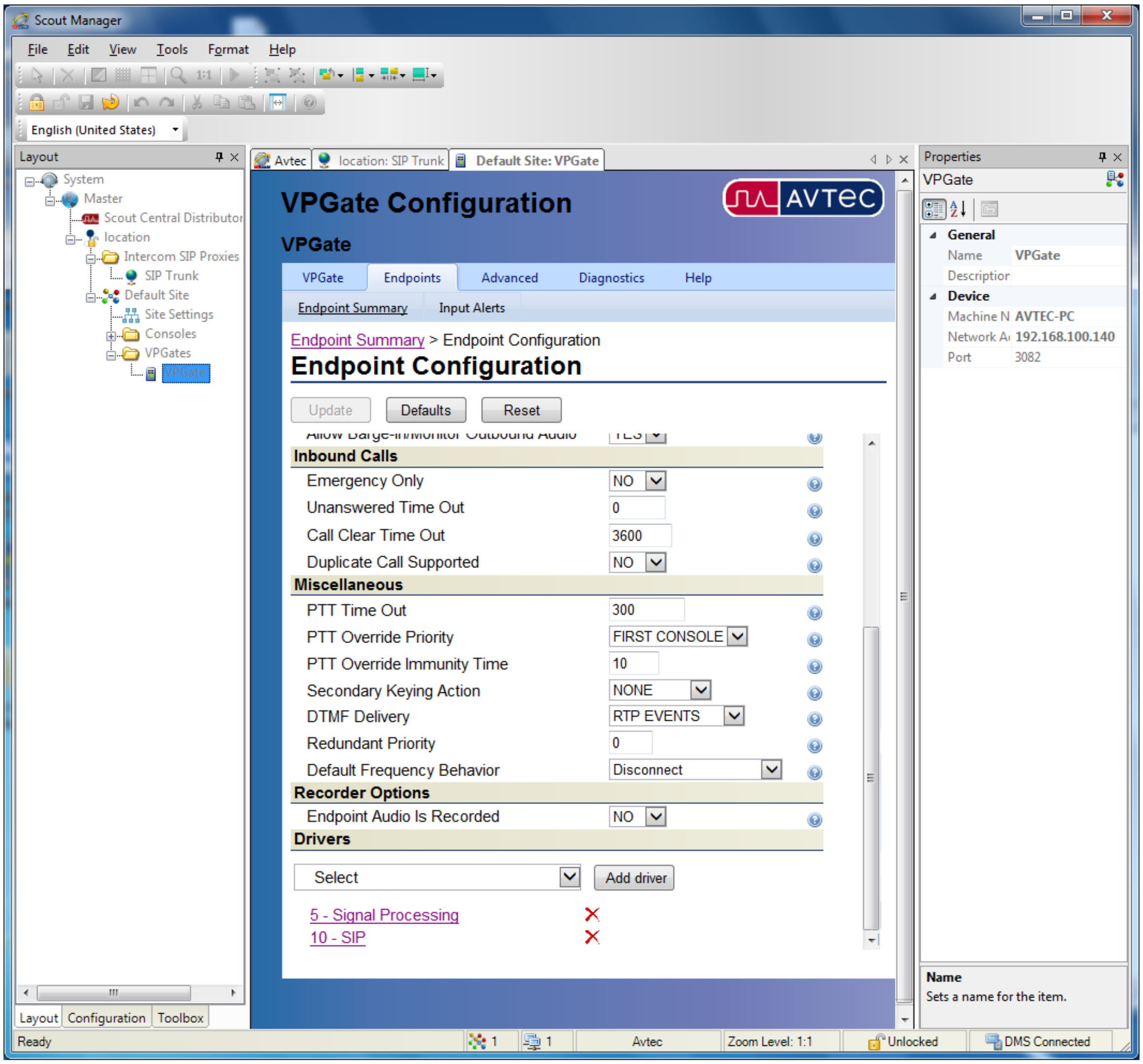


The **Endpoint** previously added is now displayed in the **Endpoint Summary** page shown below. Click on the endpoint that was previously added (i.e., *Line1*) to open the configuration again.



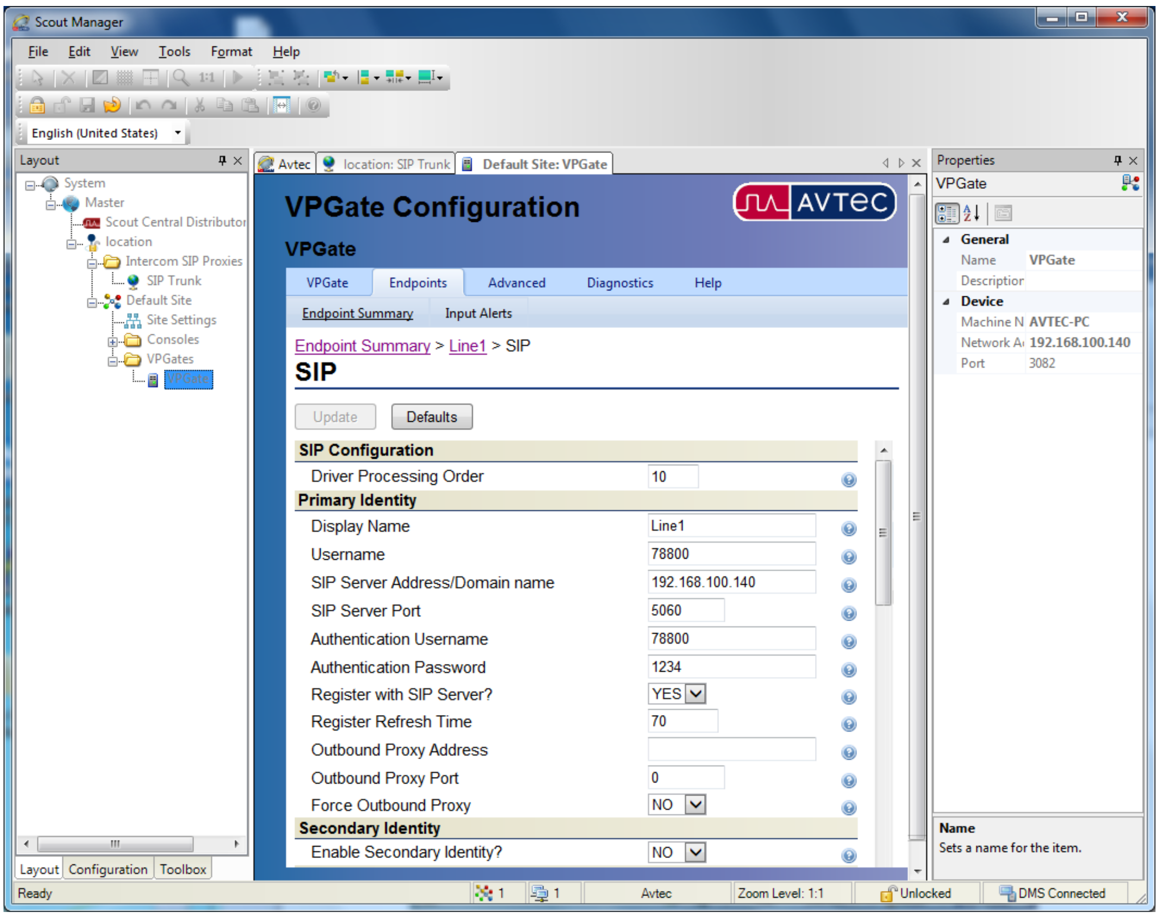
The **Endpoint Configuration** page is displayed. Scroll to the bottom of the page to the **Drivers** section as shown below. Select *10 – SIP* from the drop-down field and click **Add driver**.

Note: If Auto Answer with a music is going to be enabled for this endpoint, then the *5 – Signal Processing* driver will have to be added too as shown below.

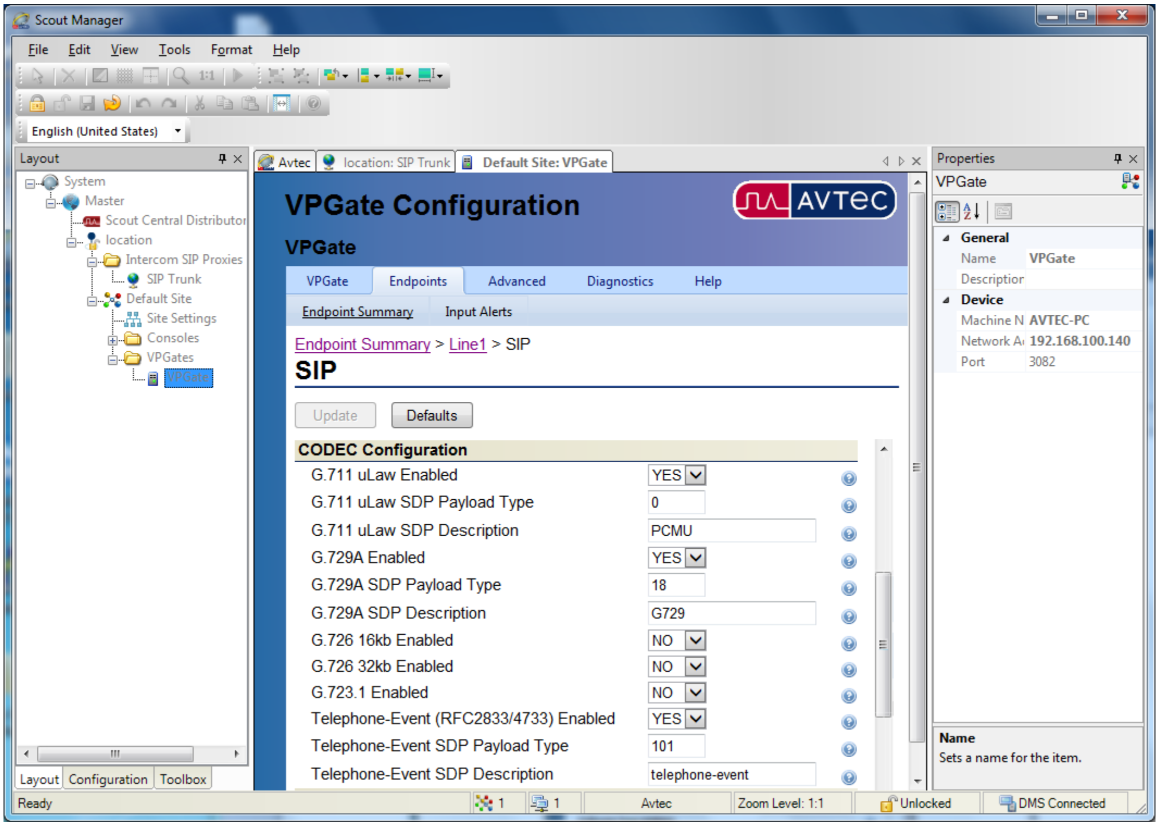


The **SIP** page is displayed as shown below. Under **Primary Identity**, configure the following fields:

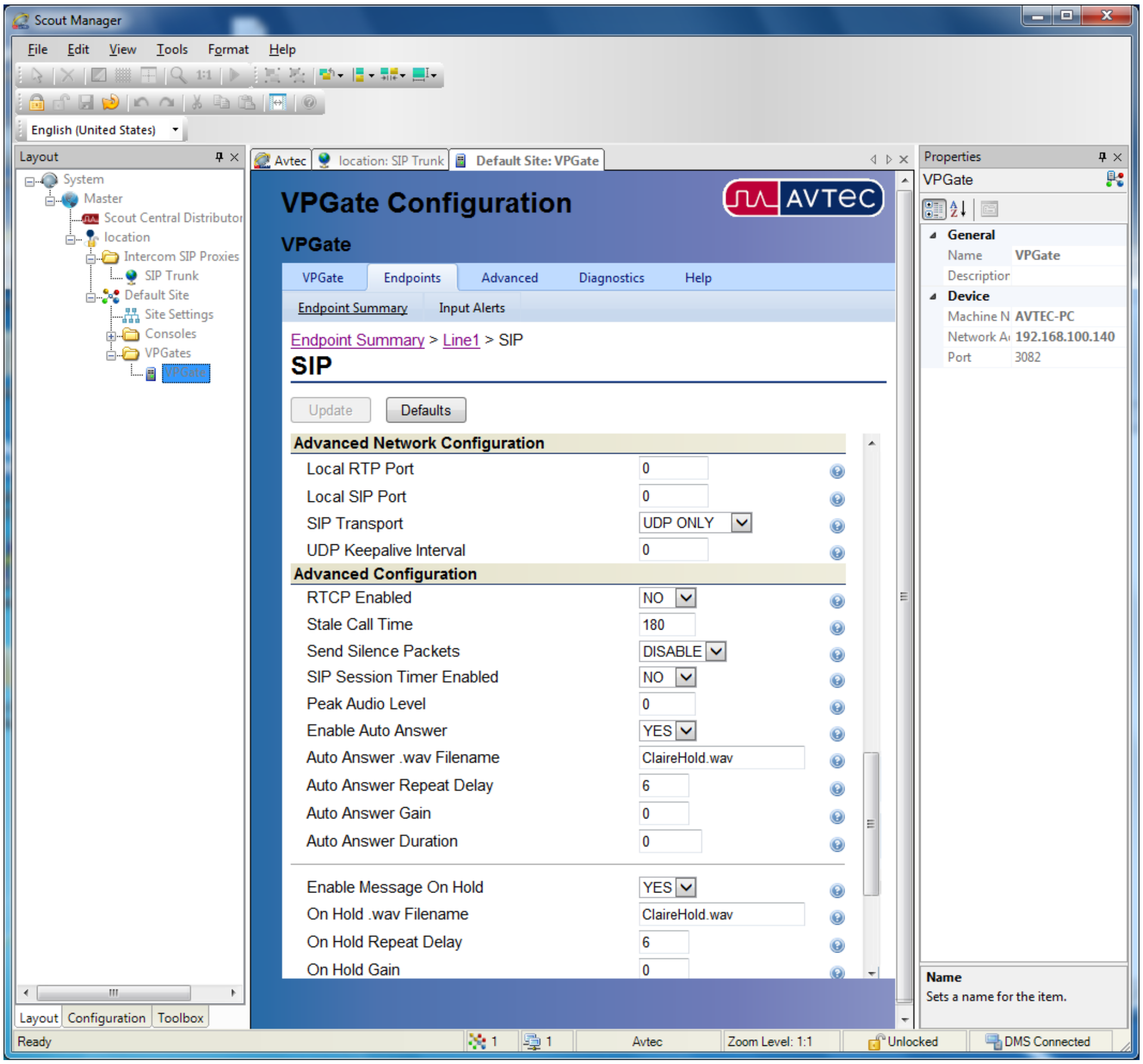
- **Display Name:** Specify a descriptive name (e.g., *Line1*).
- **Username:** Specify a descriptive name (e.g., *78800*).
- **SIP Server Address/Domain name:** Specify the IP address of Scout VoIP Console, which is also the local domain.
- **SIP Server Port:** Specify port *5060*.
- **Authentication Username:** Specify the SIP extension (e.g., *78800*).
- **Authentication Password:** Specify the password used for SIP registration.
- **Register with SIP Server:** Enable this option.



Scroll down to the **Codec Configuration** section and specify the codecs to be supported. In this example, G.711 uLaw and G.729a were enabled.



Lastly, scroll down to the **Advanced Configuration** section and enable auto answer, if desired. An audio file may be specified, which is what the caller will hear until the Scout VoIP Console answers the call. If this option is enabled, add the Signaling Processing driver as mentioned earlier. Use the default values for the remaining fields and click the **Update** button.

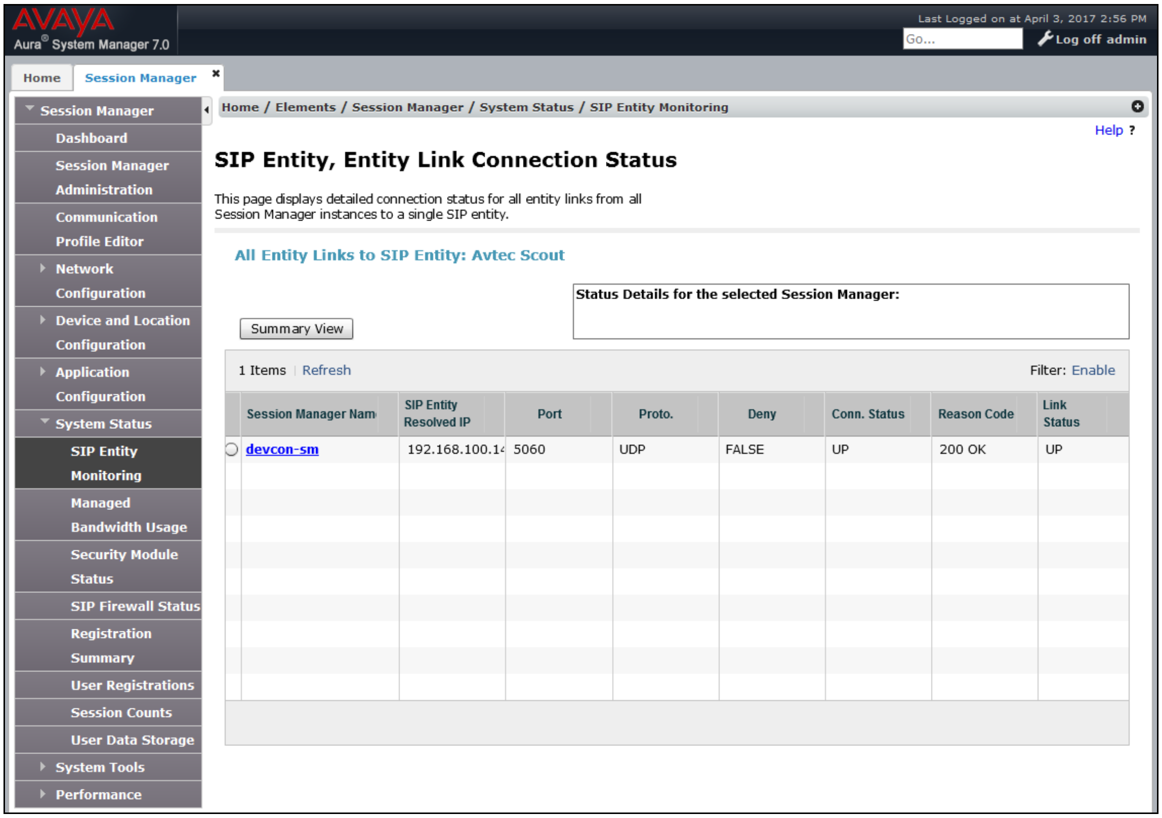


8 Verification Steps

This section provides the tests that can be performed to verify proper configuration of the Avtec Scout VoIP Console with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. The following steps can be used to verify installations in the field.

1. Launch the Avtec Scout VoIP Console. The Scout VoIP Console will be displayed as shown below. If the SIP trunk is down, the line buttons will display *Unavailable*. The line buttons shown below indicate that the SIP trunk is in-service.

2. Verify that the SIP trunk between Session Manager and Scout VoIP Console is up by navigating to **Home→Elements→Session Manager→System Status→SIP Entity Monitoring** on System Manager. Below is the status of the SIP trunk to Scout VoIP Console.



3. Verify that the SIP trunk between Communication Manager and Session Manager is in-service using the **status trunk** command on Communication Manager.

4. Place an incoming call to Scout VoIP Console and answer the call. Verify two-way audio is provided.

5. Place an outgoing call from Scout VoIP Console to an Avaya local station on PSTN and answer the call. Verify two-way audio is provided.

9 Conclusion

These Application Notes describe the configuration steps required to integrate Avtec Scout VoIP Console with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. A SIP trunk was established between Avtec Scout VoIP Console and Avaya Aura® Session Manager and basic telephony features were verified. All feature and serviceability test cases were completed successfully with observations noted in **Section 2.2**.

10 References

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

[1] *Administering Avaya Aura® Communication Manager*, Release 7.0.1, Issue 2, May 2016, Document Number 03-300509.

[2] *Administering Avaya Aura® Session Manager*, Release 7.0.1, Issue 2, May 2016.

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.