



## **Application Notes for Configuring Avtec Scout VoIP Console with Avaya Aura® Communication Manager 6.3 and Avaya Aura® Session Manager 6.3 – Issue 1.0**

### **Abstract**

These Application Notes describe the configuration steps required for Avtec Scout VoIP Console to successfully interoperate with Avaya Aura® Communication Manager 6.3 and Avaya Aura® Session Manager 6.3. The Avtec Scout VoIP Console is a SIP-based system that integrates with Avaya Aura® Communication Manager and Avaya Aura® Session Manager as SIP endpoints.

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

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

# 1. Introduction

These Application Notes describe the configuration steps required for the Avtec Scout VoIP Console to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. The Avtec Scout VoIP Console is a SIP-based system that integrates with Avaya Aura® Communication Manager and Avaya Aura® Session Manager as SIP endpoints.

## 2. General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing. The feature testing covered SIP registration, basic calls, simultaneous calls, display verification, media shuffling, audio codec negotiation, transfers and conferencing. The feature test cases were performed manually.

The serviceability testing focused on verifying the ability of the Avtec Scout VoIP Console device to recover from adverse conditions, such as disconnecting and reconnecting the LAN cable to the Avtec Scout VoIP Console. Additionally, the Communication Manager and Session Manager servers were each individually rebooted to verify the Avtec Scout VoIP Console device was able to properly register and function normally after each server recovered.

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 for full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

### 2.1. Interoperability Compliance Testing

The interoperability compliance test plan included feature and serviceability test cases. The feature testing covered SIP registration, basic calls, simultaneous calls, display verification, media shuffling, audio codec negotiation, transfers and conferencing. Various endpoints were configured for the Avtec Scout VoIP Console system to test connectivity to other extensions and out to the PSTN.

The serviceability testing focused on verifying the ability of the Avtec Scout VoIP Console to recover from adverse conditions, such as disconnecting and reconnecting the Ethernet cable to the device, rebooting Communication Manager, and rebooting Session Manager.

## 2.2. Test Results

All feature test cases were executed successfully. The Avtec Scout VoIP Console passed compliance testing with the following observation.

- Silence suppression was required on Communication Manager for Attended transfers by the Avtec Scout Console on calls that originated from the PSTN.

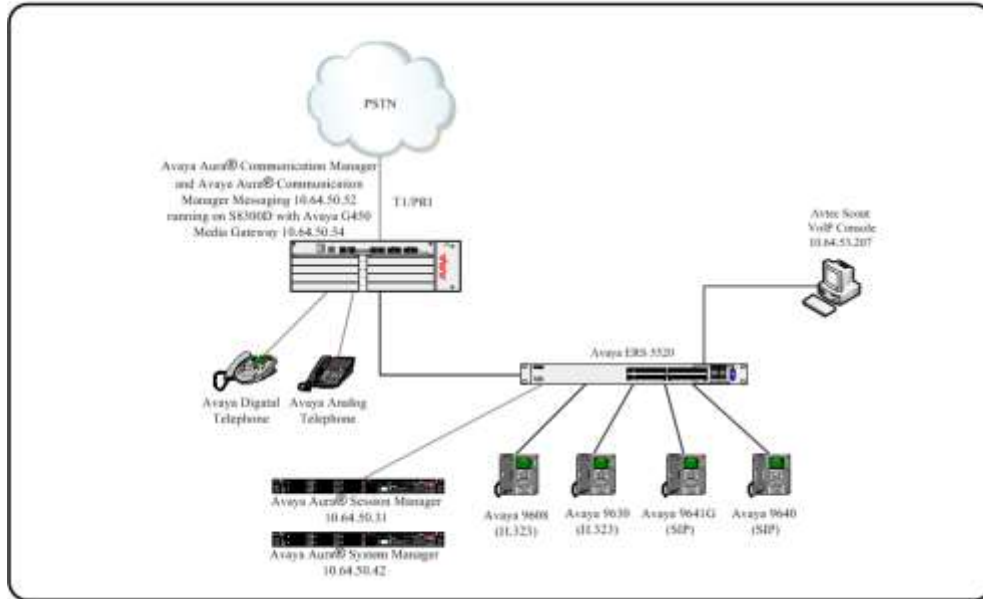
## 2.3. Support

Technical support for Avtec can be obtained through the following:

- **Phone:** 1-800-545-3034
- **Email:** [CustomerSupport@avtecinc.com](mailto:CustomerSupport@avtecinc.com)

### 3. Reference Configuration

The Avtec Scout VoIP Console solution consists of the Avtec Scout VoIP Console and the Avtec VPGate applications running on a Windows PC / Server. It can register multiple SIP endpoints with Session Manager. These endpoints can place and receive calls with various supported features as listed above in **Section 1**. The reference configuration used for the compliance test is shown in **Figure 1** below.



**Figure 1: Avtec Scout VoIP Console Reference Configuration**

## 4. Equipment and Software Validated

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

<b>Equipment/Software</b>	<b>Release/Version</b>
Avaya Aura® Communication Manager running on Avaya S8300D Server	6.3 03.0.124.0-21588
Avaya Aura® Session Manager	6.3.10.0.631008
Avaya Aura® System Manager	6.3.10.7.2656
Avaya 96x0 Deskphone	SIP 2.6.12.1, H.323 3.230A
Avaya 96x1 Deskphone	SIP 6.4.1.25, H.323 6.4014
Avaya 6211 and 6221 Analog Phone	-
Avtec VoIP Console	3.4.14.3
Avtec VPGate	3.4.18.1

## 5. Configure Avaya Aura® Communication Manager

The detailed administration of basic connectivity between Communication Manager and Session Manager is not the focus of these Application Notes and will not be described. For administration of basic connectivity between Communication Manager and Session Manager, refer to the appropriate documentation listed in **Section 10**. This section provides the procedures for the following:

- Verify Communication Manager License
- Silence Suppression

### 5.1. Verify Communication Manager License

Log into the System Access Terminal (SAT) to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the **display system-parameters customer-options** command to verify that there is sufficient capacity for SIP stations by comparing the **Maximum Off-PBX Telephones - OPS** field value with the corresponding value in the **USED** column. The difference between the two values needs to be greater than or equal to the number of SIP extensions required for the Avtec Scout VoIP Console system.

```
display system-parameters customer-options                               Page 1 of 11
                                OPTIONAL FEATURES

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

                                USED
                                Platform Maximum Ports: 6400 116
                                Maximum Stations: 2400 61
                                Maximum XMOBILE Stations: 2400 0
Maximum Off-PBX Telephones - EC500: 9600 0
Maximum Off-PBX Telephones - OPS: 9600 29
Maximum Off-PBX Telephones - PBFMC: 9600 0
Maximum Off-PBX Telephones - PVFMC: 9600 0
Maximum Off-PBX Telephones - SCCAN: 0 0
                                Maximum Survivable Processors: 313 0
```

## 5.2. Configure Silence Suppression

Silence suppression was required on Communication Manager for Attended transfers by the Avtec Scout Console on calls that originated from the PSTN. On the IP Codec Set form, change Silence Suppression to **y** to enable Silence Suppression.

```
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      y          2          20
2: G.729      y          2          20
3:
4:
5:
6:
7:
```

## 6. Configure Avaya Aura® Session Manager

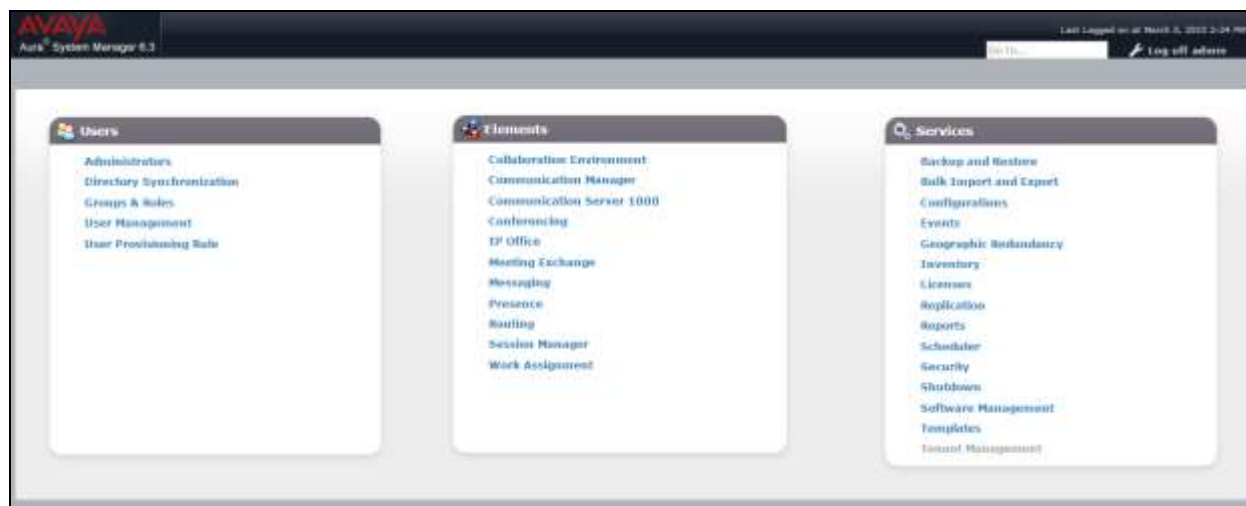
This section provides the procedures for configuring Session Manager. The procedures include the following areas:

- Launch Session Manager administration interface
- Administer users and endpoints

**Note:** During compliance testing Avtec Endpoints were configured to use either TCP or UDP for registering with Session Manager. Typically Avaya endpoints do not register using UDP so it is best practice to confirm that Session Manager is configured to listen for registrations using UDP.

### 6.1. Launch Avaya Aura® System Manager Administration Interface

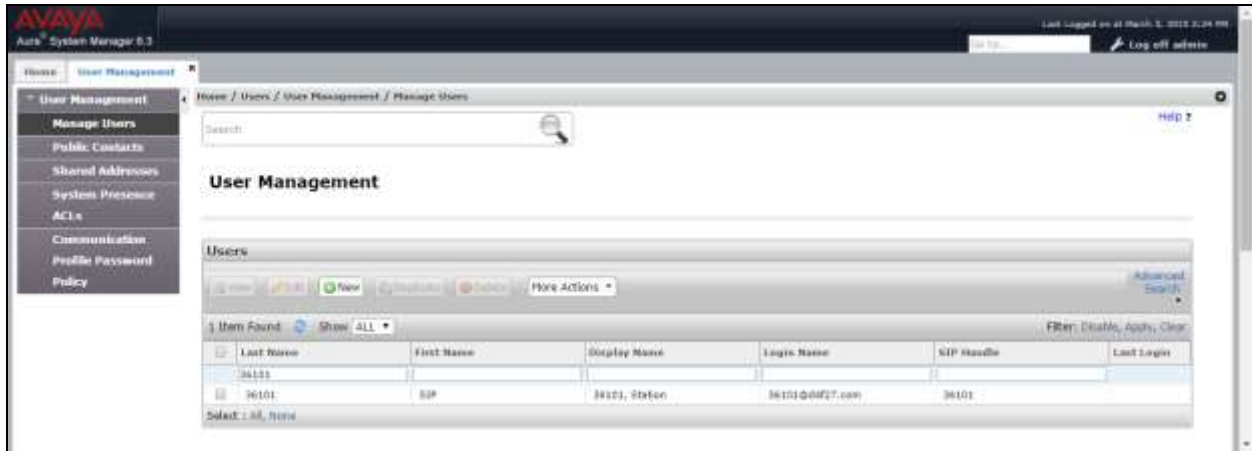
Configuration of Session Manager is accomplished by accessing the browser-based GUI of System Manager, using the URL “https://<ip-address>/SMGR”, where “<ip-address>” is the IP address of System Manager. Log in using the appropriate credentials. The screen shown below is displayed.





## 6.2. Administer Users

Users must be added to Session Manager that corresponds to SIP extensions. From the menu, navigate to **User Management**→**Manage Users** as shown below. Select the **New** button from the right pane.



## 6.2.1. Identity Tab

Enter the following values for the specified fields, all other fields can be left at default values or configured according to customer requirements.

- **Last Name:** Enter a descriptive name.
- **First Name:** Enter a descriptive name.
- **Login Name:** Enter the extension URI including SIP domain.
- **Authentication Type:** Leave this set to the default value of **Basic**.

The screenshot shows the 'New User Profile' form in the Avaya System Manager 6.3 interface. The 'Identity' tab is selected, and the 'User Provisioning Rule' is set to 'User Provisioning Rule'. The form contains several fields, with two red boxes highlighting specific areas:

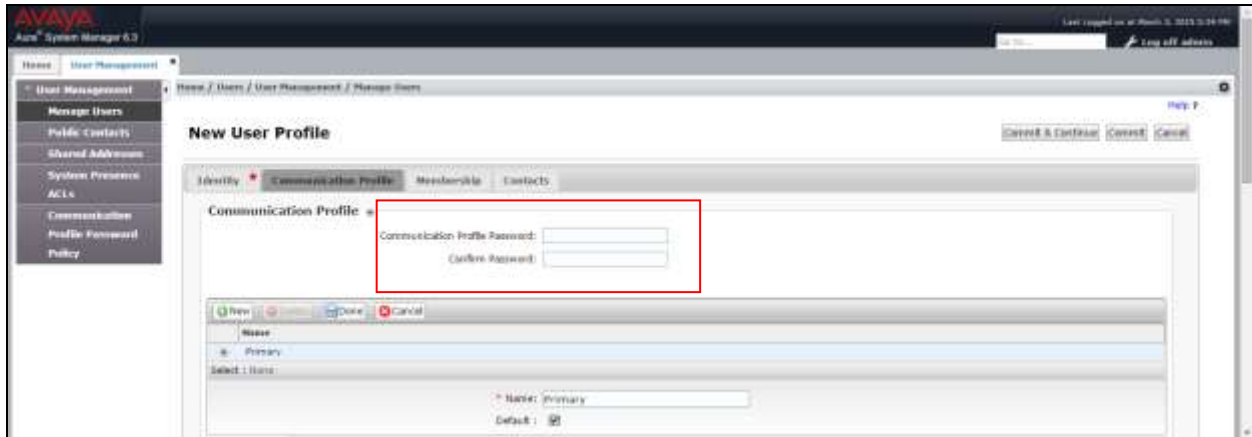
- The first red box highlights the 'Last Name' field (value: 'Line1'), 'Last Name (Latin Translation)' field (value: 'Line1'), 'First Name' field (value: 'Aktec'), and 'First Name (Latin Translation)' field (value: 'Aktec').
- The second red box highlights the 'Login Name' field (value: 's1009@4427.com') and the 'Authentication Type' dropdown menu (value: 'Basic').

Other visible fields include: Middle Name, Description, Password, Confirm Password, Localized Display Name, Endpoint Display Name, Title, Language Reference, Time Zone, Employee ID, Department, and Company. The form also includes 'Address' and 'Localized Names' sections. At the bottom, there are 'Commit & Continue', 'Commit', and 'Cancel' buttons.

## 6.2.2. Communication Profile Tab

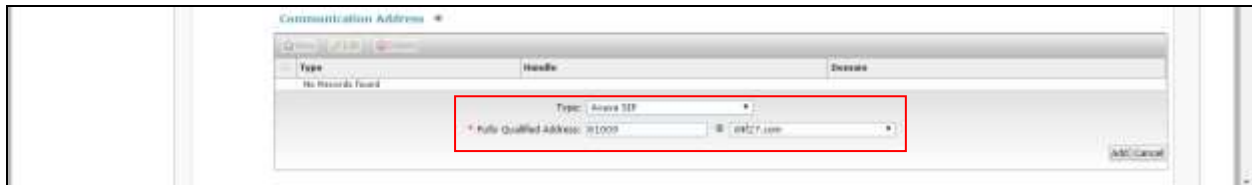
Click on the **Communication Profile** tab at the top. Enter the following values for the specified fields below.

- **Communication Profile Password:** Enter a password that will be the security code for this particular SIP extension.
- **Confirm Password:** Enter the password again to confirm.



Under **Communication Address**, click on **New**. Enter the following values for the specified fields, all other fields can be left at default values or configured according to customer requirements.

- **Type:** Choose **Avaya SIP** from the drop-down menu.
- **Fully Qualified Address:** Enter the SIP extension and choose the appropriate SIP domain from the drop-down menu.



Click the **Add** button when finished.

Expand **Session Manager Profile**. Enter the following values for the specified fields, all other fields can be left at default values or configured according to customer requirements.

- **Primary Session Manager** Select the Session Manager instance that should be used as the home server for the currently displayed Communication Profile.
- **Origination Sequence** Select an Application Sequence that will be invoked when calls are routed *from* this user.
- **Termination Sequence** Select an Application Sequence that will be invoked when calls are routed *to* this user.
- **Home Location** Select the Home Location of this user.

The screenshot shows the configuration page for a Session Manager Profile. The page is divided into several sections: SIP Registration, Application Sequences, Call Routing Settings, and Call History Settings. The following fields are highlighted with red boxes:

- SIP Registration:** Primary Session Manager (set to ser5021). A table below this field shows the status of Primary, Secondary, and Home locations.
- Application Sequences:** Origination Sequence (set to cap5052) and Termination Sequence (set to cap5052).
- Call Routing Settings:** Home Location (set to JMG2\_01).

Primary	Secondary	Home
31	0	31

Expand **CM Endpoint Profile**. The Avtec endpoints were defined using the template for the Avaya 9608 SIP phone during compliance testing. Enter the following values for the specified fields, all other fields can be left at default values or configured according to customer requirements.

- **System** Select the Communication Manager on which the endpoint exists or will be created.
- **Profile Type** Set to **Endpoint**.
- **Use Existing Endpoints** Only check this box to use an endpoint that was previously administered on Communication Manager. When left unchecked, a corresponding endpoint will be created on Communication Manager.
- **Extension** Enter the extension of the endpoint that will be associated with this user.
- **Template** Select an appropriate template. For the compliance test, the Avaya 9608 SIP phone template was used.

The screenshot shows the 'CM Endpoint Profile' configuration page. A red rectangular box highlights the following fields: 'System' (set to 'cm5052'), 'Profile Type' (set to 'Endpoint'), 'Use Existing Endpoints' (unchecked), 'Extension' (set to '01000'), and 'Template' (set to '888SIP\_DEFAULT\_CM\_6\_1'). Below these fields are other configuration options like 'Set Type' (set to 'SIP'), 'Security Code', 'Port SIP', 'Voice Mail Number', 'Preferred Handle' (set to 'Name'), and several checkboxes for advanced features like 'Enhanced Call-Info display for I-fax phones', 'Delete Endpoint on Unassign of Endpoint from User or on Delete User', and 'Override Endpoint Name and Localized Name'.

Click the **Commit** button. Repeat the procedures in this section to add a user for each required endpoint.

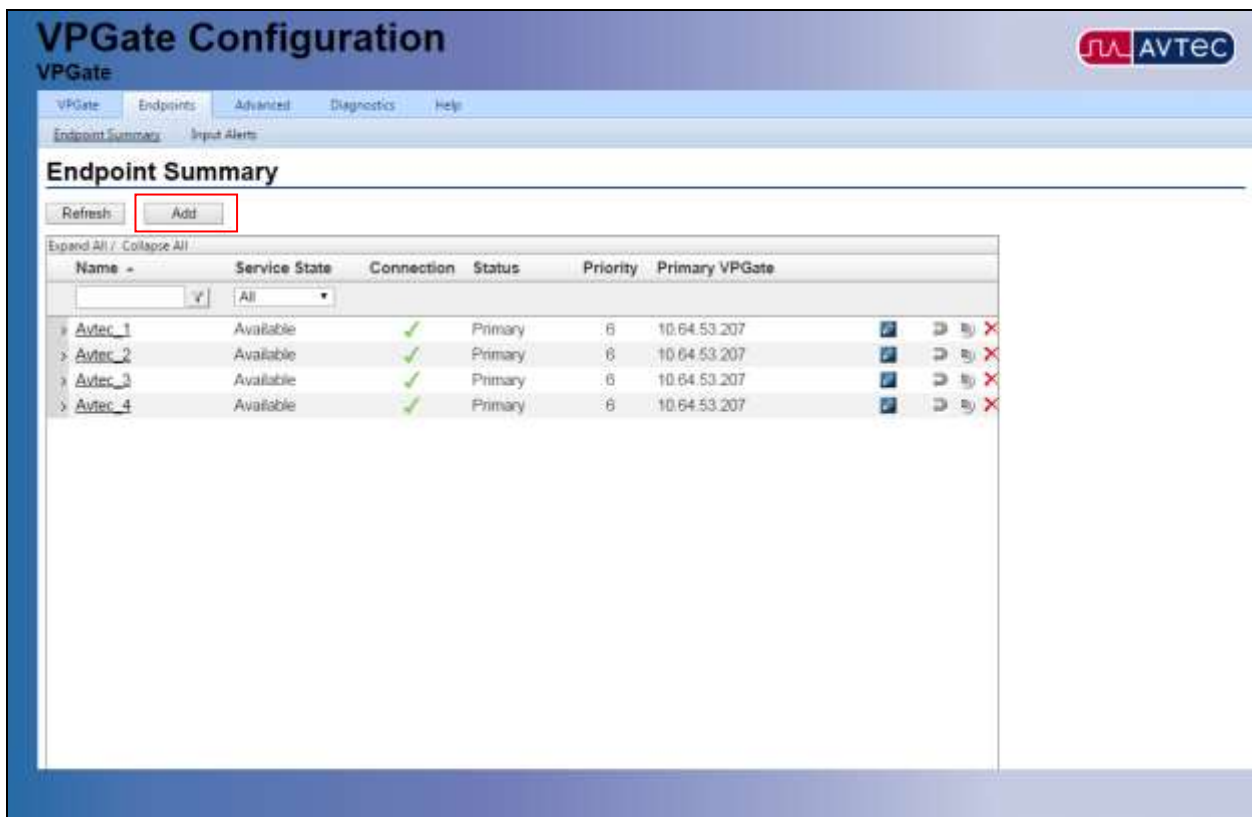
## 7. Configure Avtec Scout VoIP Console

The Avtec Scout VoIP Console solution consists of two main components -- the actual Scout console and the VPGate (VoIP Gateway) back-end component. Each is a separate piece of software that must be installed and configured. This section describes how to create endpoints in the Avtec Scout VoIP Console to connect to Avaya's system. Complete installation and configuration details for the Avtec Scout VoIP Console and VPGate may be found in the Avtec documentation listed in **Section 10**. The procedures include the following areas:

- Configure Endpoints

### 7.1. Configure Avtec Scout VoIP Console Endpoints

To login to VPGate, bring up a web browser and navigate to <http://localhost:3082/>, or connect to it from a different computer, browse to [http://\[computer name or IP\]:3082/](http://[computer name or IP]:3082/), using the name or IP address of the computer that is running the VPGate software (not shown). On the tabs at the top of the page, select **Endpoints**. This will bring up the **Endpoint Summary** page. Press the **Add** button to create the new endpoint as shown below.



The screenshot displays the VPGate Configuration web interface. At the top, there is a navigation bar with tabs for VPGate, Endpoints, Advanced, Diagnostics, and Help. Below this, there are sub-tabs for Endpoint Summary and Input Alerts. The main content area is titled "Endpoint Summary" and features a "Refresh" button and a red-bordered "Add" button. Below the buttons is a table with columns for Name, Service State, Connection, Status, Priority, and Primary VPGate. The table contains four rows of data, each representing an endpoint named Avtec\_1 through Avtec\_4. Each row shows a service state of "Available", a green checkmark in the Connection column, a status of "Primary", a priority of "6", and a primary VPGate IP address of "10.64.53.207".

Name	Service State	Connection	Status	Priority	Primary VPGate
Avtec_1	Available	✓	Primary	6	10.64.53.207
Avtec_2	Available	✓	Primary	6	10.64.53.207
Avtec_3	Available	✓	Primary	6	10.64.53.207
Avtec_4	Available	✓	Primary	6	10.64.53.207

This brings up the **Endpoint Configuration** page. Under **Endpoint Name**, give it a unique identifier. **Note:** This is the name VPGate and Scout use to identify the endpoint. It doesn't have to correspond to anything, just name it something meaningful. Change the next field, **Service State**, to **AVAILABLE**. Under **VoIP Audio Settings**, change the **Receive Audio Mode** to **FULL DUPLEX**. Other fields can be left at their default values for standard use. When finished, press **Add**. It will create the endpoint and return to the **Endpoint Summary** page.

The screenshot shows the VPGate Configuration web interface. The page title is "VPGate Configuration" and the AVTEC logo is in the top right. The navigation menu includes "VPGate", "Endpoints", "Advanced", "Diagnostics", and "Help". The breadcrumb trail is "Endpoint Summary > Endpoint Configuration". The main heading is "Endpoint Configuration".

The configuration form is divided into several sections:

- Endpoint Configuration:** Contains "Endpoint Name" (Avtec\_1) and "Service State" (AVAILABLE).
- Endpoint Connection:** Contains "Endpoint Audio" (VoIP).
- VoIP Audio Settings:** Contains "Receive Audio Mode" (FULL DUPLEX), "Override Receive Audio IP Port" (0), "Override Transmit Audio IP Port" (0), "VoIP Audio Jitter Depth (ms)" (100), "Squelch Tail Time Out" (0), and "Allow Barge-in/Monitor Outbound Audio" (YES).
- Inbound Calls:** Contains "Emergency Only" (NO), "Unanswered Time Out" (0), "Call Clear Time Out" (3600), and "Duplicate Call Supported" (NO).
- Miscellaneous:** Contains "PTT Time Out" (300), "PTT Override Priority" (FIRST CONSOLE), and "PTT Override Immunity Time" (10).

Red boxes highlight the "Endpoint Name", "Service State", and "Receive Audio Mode" fields.

Click on the endpoint name again to go back to the **Endpoint Configuration** page. At the bottom of the page is a section labeled **Drivers** (not shown). From the drop-down menu, select **SIP** and press **Add driver**. This brings up the **SIP Configuration** page as shown below.

**VPGate Configuration**  
Avtec\_VPGate

VPGate Endpoints Advanced Diagnostics Help

Endpoint Summary Input Alerts

[Endpoint Summary](#) > [Avtec\\_1](#) > SIP

## SIP

### SIP Configuration

Driver Processing Order	<input type="text" value="1"/>	
-------------------------	--------------------------------	--

### Primary Identity

Display Name	<input type="text" value="Private caller"/>	
Username	<input type="text"/>	
SIP Server Address/Domain name	<input type="text"/>	
SIP Server Port	<input type="text" value="0"/>	
Authentication Username	<input type="text"/>	
Authentication Password	<input type="text"/>	
Register with SIP Server?	<input type="text" value="YES"/>	
Register Refresh Time	<input type="text" value="70"/>	
Outbound Proxy Address	<input type="text"/>	
Outbound Proxy Port	<input type="text" value="0"/>	
Force Outbound Proxy	<input type="text" value="NO"/>	

### Secondary Identity

Enable Secondary Identity?	<input type="text" value="NO"/>	
----------------------------	---------------------------------	--

### CODEC Configuration

G.711 uLaw Enabled	<input type="text" value="YES"/>	
G.711 uLaw SDP Payload Type	<input type="text" value="0"/>	
G.711 uLaw SDP Description	<input type="text" value="PCMU"/>	
G.729A Enabled	<input type="text" value="YES"/>	
G.729A SDP Payload Type	<input type="text" value="18"/>	
G.729A SDP Description	<input type="text" value="G729"/>	

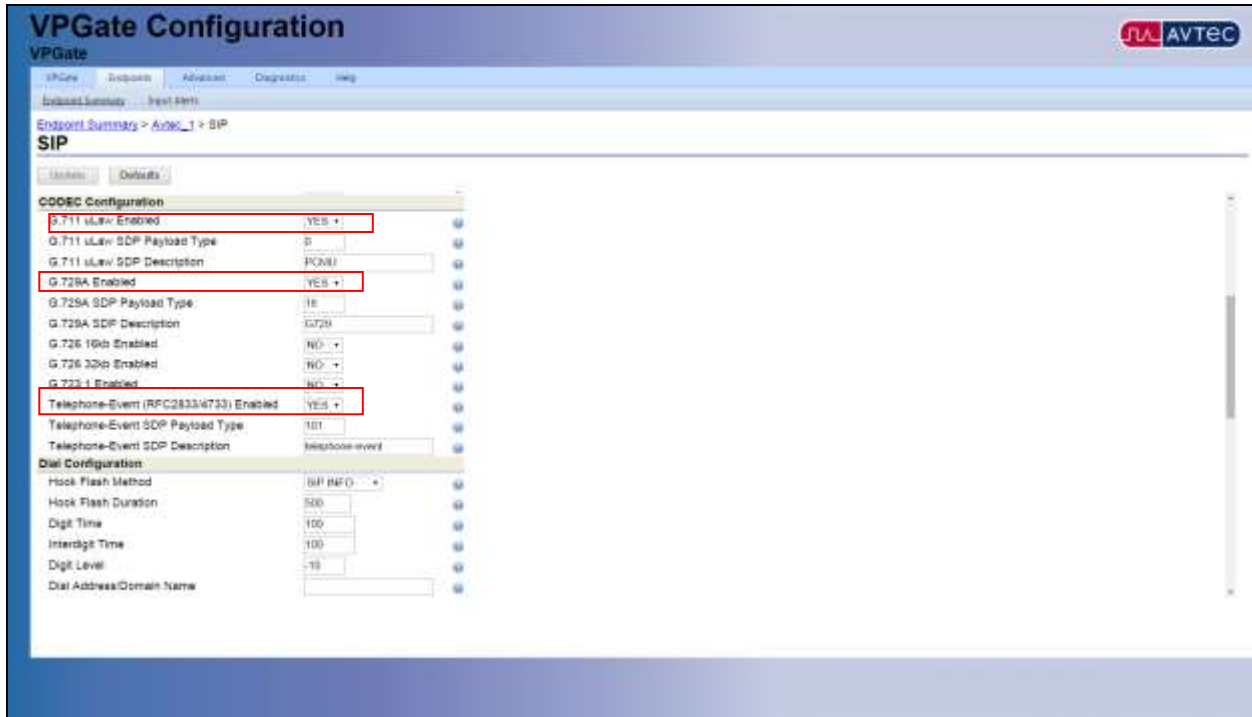


Most of the fields under **Primary Identity** are used to configure the endpoint to register with Session Manager. Under **Display Name**, enter the desired Caller ID to display for this endpoint when calling another endpoint. Under **Username**, enter the extension defined for the new SIP user configured on Session Manager in **Section 6.2**. For **SIP Server Address/Domain name**, enter the IP address of Session Manager, and for **SIP Server Port**, enter the port number the endpoint should use to register with Session Manager. **Authentication Username** and **Authentication Password** should also match the new extension and password configured in **Section 6.2**. **Register Refresh Time** sets how frequently the endpoint will send registrations to the SIP server. This field defaults to 70 seconds. During compliance testing this field was set to 3600 (1 hour) which matches the default maximum value of Session Manager.

The screenshot shows the VPGate Configuration interface for a SIP endpoint. The 'Primary Identity' section is highlighted with a red box, and the 'Register Refresh Time' field is also highlighted with a red box.

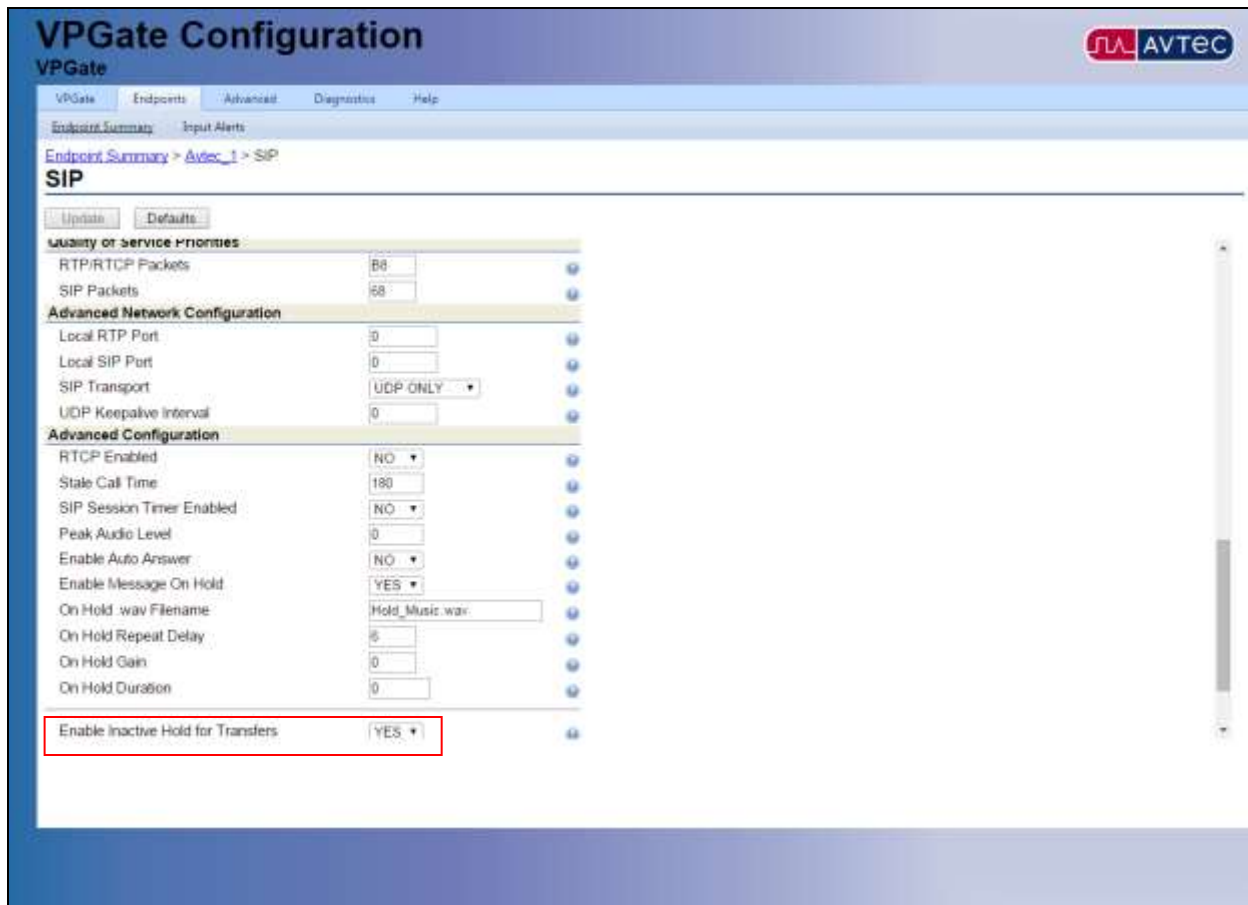
SIP Configuration	
Driver Processing Order	2
Primary Identity	
Display Name	x61009
Username	61009
SIP Server Address/Domain name	10.64.50.31
SIP Server Port	5060
Authentication Username	61009
Authentication Password	123456
Register with SIP Server?	YES
Register Refresh Time	3600
Outbound Proxy Address	
Outbound Proxy Port	0
Force Outbound Proxy	NO
Secondary Identity	
Enable Secondary Identity?	NO
CODEC Configuration	
G.711 uLaw Enabled	YES
G.711 uLaw SDP Payload Type	0
G.711 uLaw SDP Description	PCMU
G.711A Enabled	NO

In the **Codec Configuration** section, set the desired CODEC(s) to **YES**. Both G.711 $\mu$  and G.729A were used during compliance testing. Also set **Telephone-Event (RFC2833/4733)** to **Enabled**. This setting causes DTMF be sent in the RTP Payload and was required for interoperation with Messaging.



Under **Advanced Configuration**, **Enable Inactive Hold for Transfers** should be set to **YES**. Other fields can be left at their default values.

**Note:** The default **SIP Transport** is “UDP ONLY”. Both UDP and TCP were verified during compliance testing.

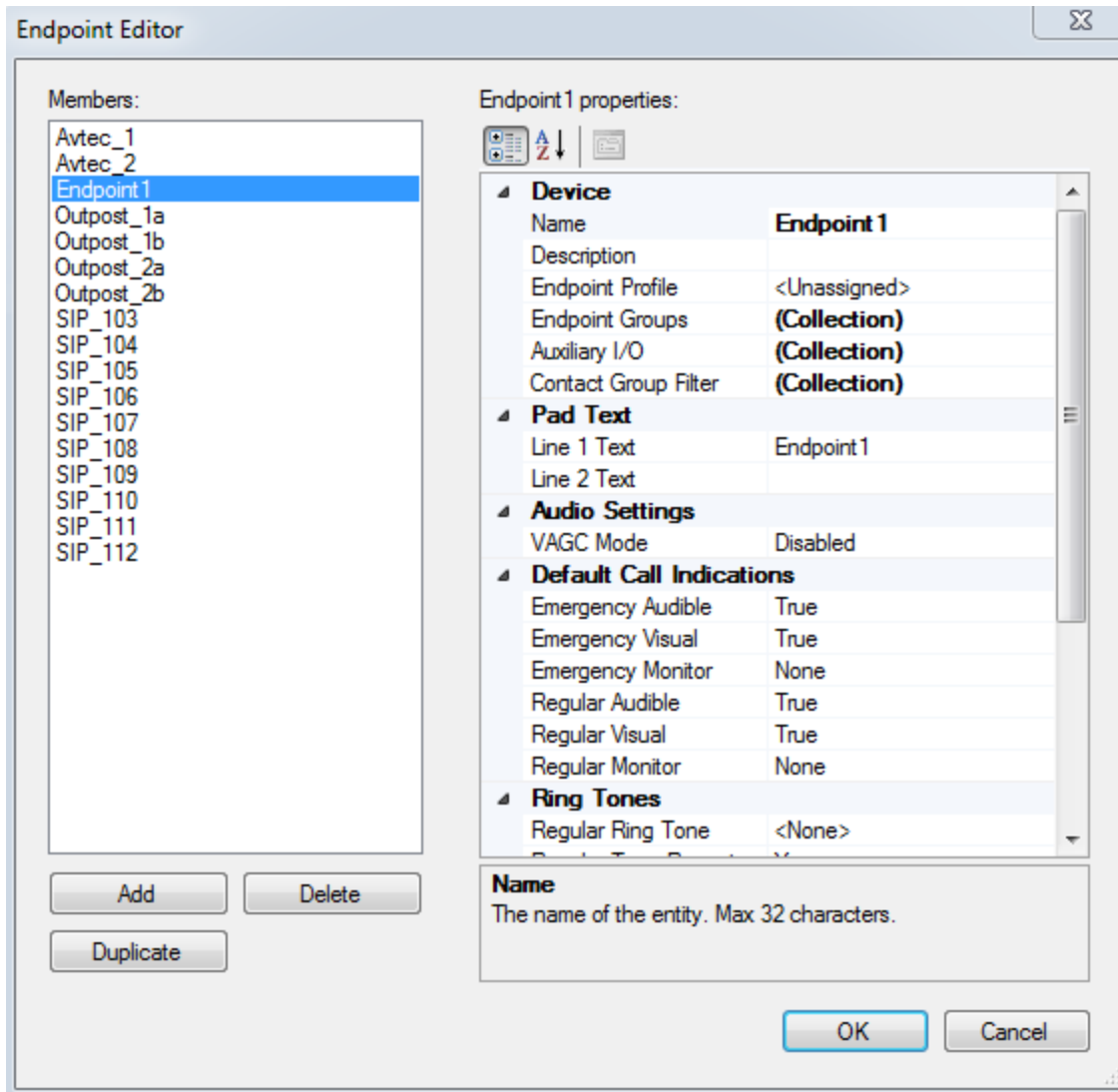


When finished with the endpoint configuration, press **Add** (as was shown above) or **Update** when editing an existing endpoint.

Follow the same procedure above, making sure to use a unique identifier in the **Endpoint Name** field, for every endpoint that needs to be configured.

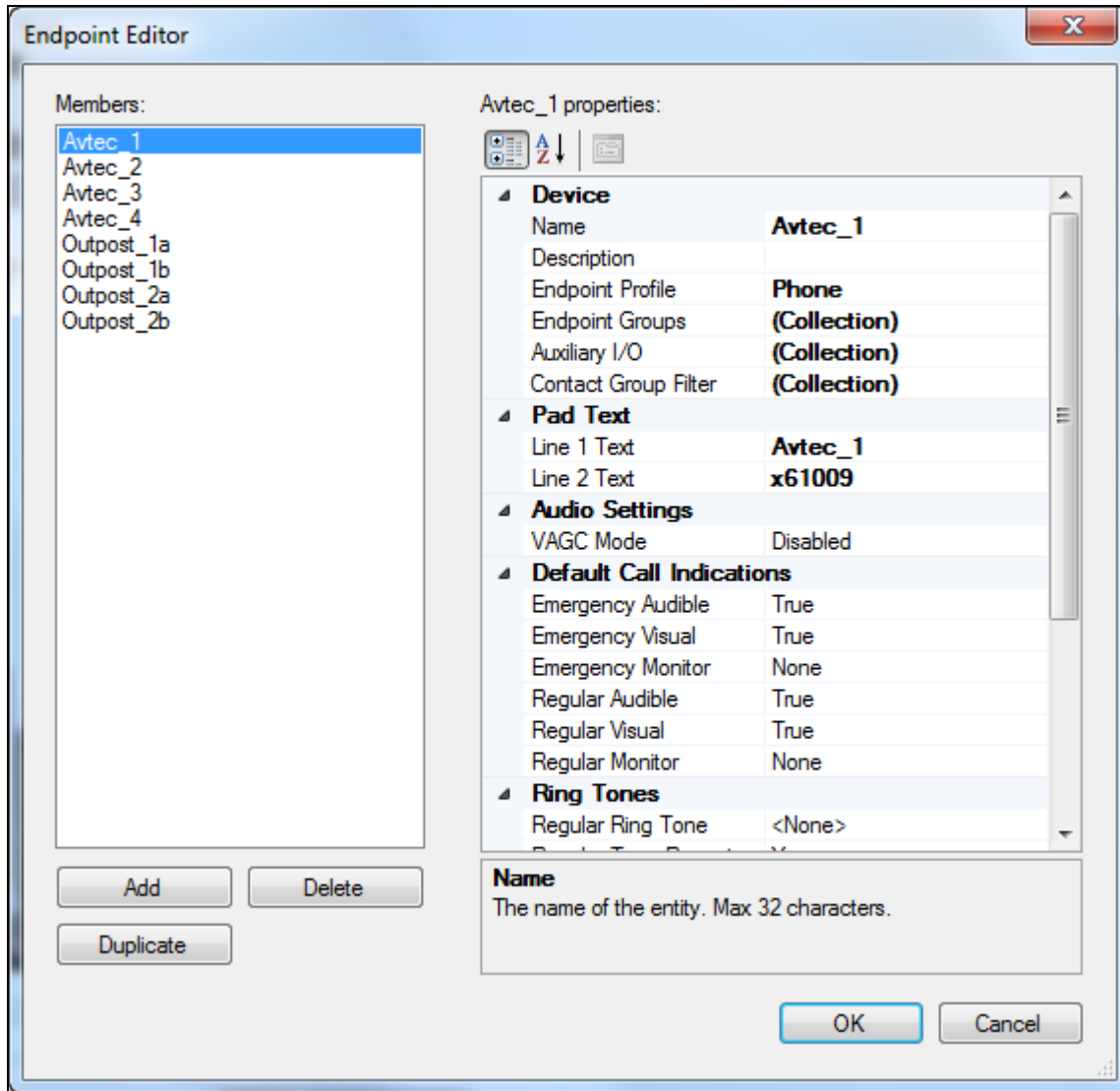
Now that the endpoint is configured, it will be necessary to add a "line pad" to the Avtec Scout VoIP Console so it can be used. First, start up the **Project Manager** software. **Note:** This was installed alongside the Avtec Scout VoIP Console software. The Avtec Scout VoIP Console installation and help files describe in detail how to create a new project and new screens. These next steps assume there is a basic project defined and that new endpoints simply need to be added.

In **Project Manager**, in the **Project Explorer** tree on the left-hand side, right-click the **Endpoints** folder and choose **Add New**→**Endpoint** (not shown). This creates a new endpoint with the generic name, **Endpoint1**, under the **Endpoints** folder. Double-click that endpoint to bring up the **Endpoint Editor** window as shown below.



In the **Properties** window on the right side, change the **Name** field to match the name entered for the endpoint in VPGate. Under **Endpoint Profile**, select the preferred profile to use with this endpoint.

**Note:** The preinstalled **Phone** profile should work fine. Profiles define basic things like default ring and call-progress tones, whether the endpoint can be put on hold, etc. Other fields can be customized, but these are the required fields that are needed to make the endpoint function properly.



Next, it will be necessary to add the endpoint to a screen (assuming a screen for the endpoint has already been created.) There are several different ways to do that. The simplest way is to click on the endpoint name in the **Project Explorer** window and drag it over to the screen. This can also be done through the **Toolbox** window. In the left-hand window of **Project Manager**, click on the **Toolbox** tab. Find the **Line Pad** icon. Click and drag the icon from the Toolbox to the screen. Then in the **Properties** window on the right-hand side, under **Behavior**, select the drop-down next to the **Name** field and choose the endpoint that was just created. If a line pad is already defined on the screen and it needs to be reassigned, select the line pad and change the **Name** field in the **Properties** window.



Save the project and send it. To do this, press the **Send Project** button on the toolbar at the top, assuming the **Project Manager** is configured to send projects either locally or to a centralized project server.



Now the endpoint(s) should be usable.

## 8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Session Manager, and the Avtec Scout VoIP Console.

### 8.1. Verify User Registrations

On Session Manager, verify the registration status of the Avtec Scout VoIP Console device by navigating to **Session Manager → System Status → User Registrations**. Verify that all the users administered in **Section 6.2** are listed as registered users.

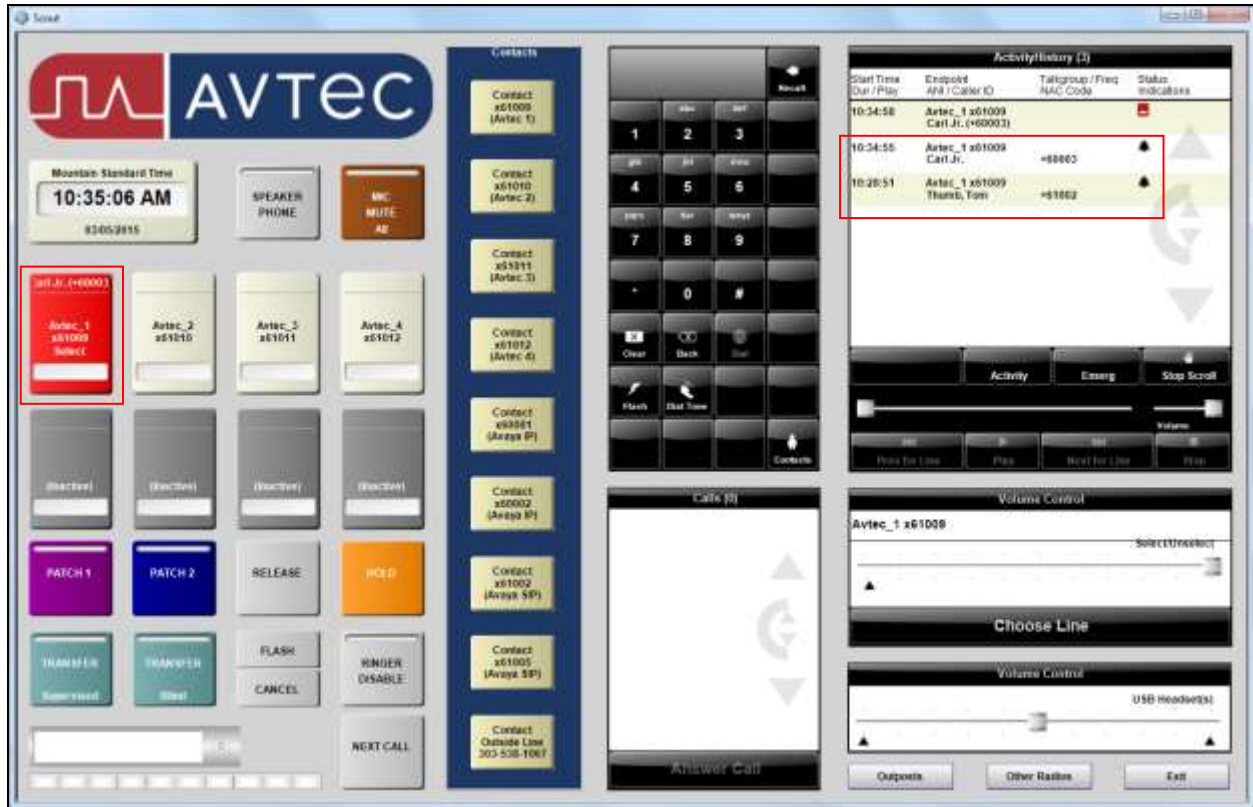
The screenshot displays the Avaya System Manager 6.3 interface. The left sidebar contains a navigation menu with categories like System Manager, Device and Location, Application, System Status, and User Registrations. The main content area is titled "User Registrations" and includes a table of user registrations. The table has the following columns: Details, Address, First Name, Last Name, Actual Location, IP Address, Service (SIP), Shared (Foot), Shared Device, and AST Device. A single user is listed with the following details: Details: [checkbox], Address: 6180464427.com, First Name: Avtec, Last Name: sip1, Actual Location: 4W27\_1, IP Address: 10.64.13.207. The IP address field is highlighted with a red box. The table also includes checkboxes for "Service (SIP)", "Shared (Foot)", "Shared Device", and "AST Device".

Details	Address	First Name	Last Name	Actual Location	IP Address	Service (SIP)	Shared (Foot)	Shared Device	AST Device	Registered
<input type="checkbox"/>	6180464427.com	Avtec	sip1	4W27_1	10.64.13.207	<input type="checkbox"/>	<input type="checkbox"/>	L/L	<input type="checkbox"/>	<input checked="" type="checkbox"/>



## 8.2. Verify Avtec Scout VoIP Console

Make a call to one of the extensions or DIDs for the Avtec Scout VoIP Console endpoint(s). Verify that the call has ring back tone, two-way audio for at least 30 seconds, and that the call properly disconnects. Additionally the Avtec Scout VoIP Console should display the active call as shown below.



## 9. Conclusion

These Application Notes describe the configuration steps required for Avtec Scout VoIP Console to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager.

All feature and serviceability test cases were completed with observations listed in **Section 2.2**.

## 10. Additional References

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

Avaya documentation referenced below can be found at <http://support.avaya.com>

- [1] Administering Avaya Aura® Communication Manager, Document 03-300509
- [2] Administering Avaya Aura® Session Manager, Document 03-603324

Avtec documentation can be found at <https://portal.avtecinc.com>

---

**©2015 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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](mailto:devconnect@avaya.com).