



Avaya Solution & Interoperability Test Lab

Application Notes for Avtec Scout VoIP Console 5.3 with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Session Manager 10.1 using SIP Endpoints – 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 provides a customizable interface and supports telephony features, such as inbound and outbound calls, hold, resume, mute, and transfer. It integrates with Avaya Aura® Session Manager via SIP endpoints.

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 provides a customizable interface and supports telephony features, such as inbound and outbound calls, hold, resume, mute, and transfer. Avtec Scout VoIP Console registers with and integrates with Avaya Aura® Session Manager as a SIP endpoints.

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. Additional telephony features, such as call forward, call coverage, call park/unpark, and call pickup were also verified using Communication Manager Feature Access Codes (FACs).

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 subsection 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 these DevConnect Application Notes 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 these Application Notes, 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:

- SIP registration of Scout VoIP Console with Session Manager.
- Calls between Scout VoIP Console and Avaya SIP and H.323 telephones with Direct IP Media (Shuffling) enabled and disabled.
- Calls between the Scout VoIP Console and the PSTN.
- G.711 and G.729 codec support.
- Proper recognition of DTMF tones.
- Basic telephony features, including hold, mute, redial, multiple calls, and blind/attended transfers.
- Extended telephony features using Communication Manager FACs for Call Forward, Call Park/Unpark, and Call Pickup.
- Voicemail coverage, MWI support, and logging into voicemail system to retrieve voice messages.
- Use of programmable buttons on the Scout VoIP Console.
- Proper system recovery after a restart of the Scout VoIP Console and loss of IP connectivity.

2.2. Test Results

All test cases passed with the following observation:

- Incoming call notification is not heard through headset by design, external speakers are required. However, visual indication of incoming calls is provided by the Scout VoIP Console.
- Each SIP line on Scout VoIP Console supports one call at a time. An incoming call to an active line on Scout VoIP Console results in either busy tone or the call covering to the next coverage point, if configured. However, multiple SIP lines may be configured on Scout VoIP Console.
- 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, email, or website.

- **Phone:** +1 (800) 545-3034
+1 (803) 358-3601
- **Email:** customersupport@avtecinc.com
- **Web:** <https://www.avtecinc.com/support>

3. Reference Configuration

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

- Avaya Aura® Communication Manager running in a virtual environment with an Avaya G430/G450 Media Gateway.
- Media resources in the Avaya Media Gateway and Avaya Aura® Media Server.
- Avaya Aura® Session Manager connected to Communication Manager via a SIP trunk and acting as a Registrar/Proxy for SIP telephones.
- Avaya Aura® System Manager used to configure Session Manager.
- Avaya Messaging serving as the voicemail system.
- Avaya 96x1 Series H.323 and SIP Deskphones.
- Avaya J100 Series SIP Telephones.
- Avtec Scout VoIP Console registered to Session Manager via SIP endpoints.
- Avtec Scout VoIP Console was installed on a desktop PC running Microsoft Windows 10 and included the following components: Scout VPGate and Scout Manager. Scout Manager was used to configure the Scout VoIP Console.

Avtec Scout VoIP Console registered with Session Manager as SIP endpoints and configured as Off-PBX Stations (OPS) on Communication Manager.

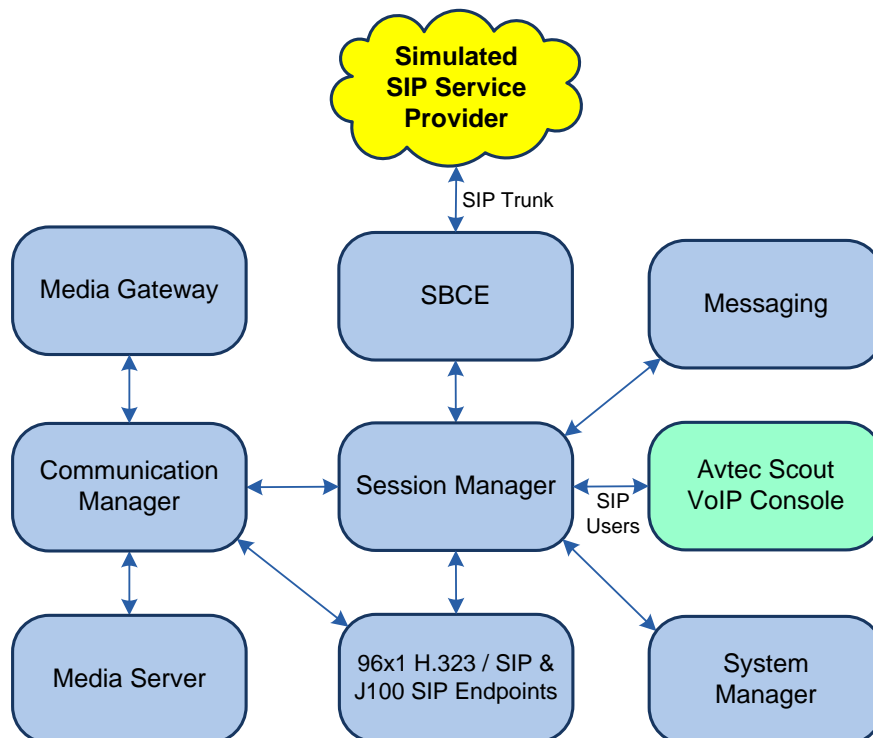


Figure 1: Avaya SIP Network with Avtec Scout VoIP Console

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	10.1.0.1.0-SP1
Avaya G430 Media Gateway	FW 42.4.0
Avaya G450 Media Gateway	FW 42.7.0
Avaya Aura® Media Server	v.10.1.0.77
Avaya Aura® System Manager	10.1.0.1 Build No. – 10.1.0.0.537353 Software Update Revision No: 10.1.0.1.0614394 Service Pack 1
Avaya Aura® Session Manager	10.1.0.1.1010105
Avaya Messaging	11.0.0.3204
Avaya 96x1 Series IP Deskphones	6.8.5.3.2 (H.323) 7.1.13.0.4 (SIP)
Avaya J100 SIP Telephones	4.0.13.0.6
Avtec Scout VoIP Console running on Microsoft Windows 10, including the following components: <ul style="list-style-type: none">Scout ConsoleScout VPGateScout Manager	5.3.0.13 5.3.0.41 5.3.0.13

5. Configure Avaya Aura® Communication Manager

This section provides the steps for configuring Communication Manager using the System Access Terminal (SAT). The procedure includes the following areas:

- Verify Communication Manager license
- Administer IP Node Names
- Administer IP Codec Set
- Administer IP Network Region
- Administer SIP Trunk Group to Session Manager
- Administer AAR Call Routing

Note: It is assumed that basic configuration of the Communication Manager has already been completed, such as the SIP trunk to Session Manager. The SIP station configuration for Scout VoIP Console is configured through Avaya Aura® System Manager in **Section 6.3**.

5.1. Verify License

Using the SAT, verify that the Off-PBX Telephones (OPS) option is enabled on the **system-parameters customer-options** form. The license file installed on the system controls these options. If a required feature is not enabled, contact an authorized Avaya sales representative.

On **Page 1**, verify that the number of OPS stations allowed in the system is sufficient for the number of SIP endpoints that will be deployed.

display system-parameters customer-options		Page	1 of 12
OPTIONAL FEATURES			
G3 Version: V20		Software Package: Enterprise	
Location: 2		System ID (SID): 1	
Platform: 28		Module ID (MID): 1	
		USED	
Platform Maximum Ports:		48000	130
Maximum Stations:		36000	36
Maximum XMOBILE Stations:		36000	0
Maximum Off-PBX Telephones - EC500:		41000	0
Maximum Off-PBX Telephones - OPS:		41000	22
Maximum Off-PBX Telephones - PBFMC:		41000	0
Maximum Off-PBX Telephones - PVFMC:		41000	0
Maximum Off-PBX Telephones - SCCAN:		0	0
Maximum Survivable Processors:		313	0
(NOTE: You must logoff & login to effect the permission changes.)			

5.2. 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-aes	10.64.102.119	
devcon-ams	10.64.102.118	
devcon-sm	10.64.102.117	
procr	10.64.102.115	
procr6	::	

(6 of 6 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

5.3. 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. Although media encryption was configured, Scout VoIP Console did not use SRTP. Media encryption option of *none* must be specified as shown below. The Scout VoIP Console was tested using G.711 and G.729 codecs.

change ip-codec-set 2		Page 1 of 2
IP MEDIA PARAMETERS		
Codec Set: 2		
Audio Codec	Silence Suppression	Frames Per Pkt
1: G.711MU	n	2
2: G.729	n	2
3:		
4:		
5:		
6:		
7:		

Media Encryption	Encrypted SRTP: best-effort
1: 1-srtp-aescm128-hmac80	
2: 2-srtp-aescm128-hmac32	
3: none	
4:	
5:	

5.4. 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 IP endpoints without using media resources in the Avaya Media Gateway or Avaya Aura® 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.

change ip-network-region 1		Page 1 of 20
IP NETWORK REGION		
Region: 1	NR Group: 1	
Location: 1	Authoritative Domain: avaya.com	
Name: SIP Enterprise	Stub Network Region: n	
MEDIA PARAMETERS		
Codec Set: 1	Intra-region IP-IP Direct Audio: yes	
	Inter-region IP-IP Direct Audio: yes	
UDP Port Min: 2048	IP Audio Hairpinning? n	
UDP Port Max: 50999		
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		

5.5. 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:

- **Group Type** was set to *sip*.
- **IMS Enabled** was set to *n*.
- **Transport Method** was set to *tls*.
- **Enforce SIPS URI for SRTP** was set to *n*.
- Specify Communication Manager (*procr*) and the 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.
- Set the TLS port value (e.g., *5061*) 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*.
- **Direct IP-IP Audio Connections** was enabled on this form.
- **Initial IP-IP Direct Media** was enabled.
- **DTMF over IP** was left at 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? y	Enforce SIPS URI for SRTP? n		
Peer Detection Enabled? y	Peer Server: SM	Clustered? n	
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			
Incoming Dialog Loopbacks: eliminate		Bypass If IP Threshold Exceeded? n	
		RFC 3389 Comfort Noise? n	
DTMF over IP: rtp-payload		Direct IP-IP Audio Connections? y	
Session Establishment Timer(min): 3		IP Audio Hairpinning? n	
Enable Layer 3 Test? y		Initial IP-IP Direct Media? y	
H.323 Station Outgoing Direct Media? n		Alternate Route Timer(sec): 6	

Configure the **Trunk Group** form as shown below. This trunk group is used for SIP calls to Scout VoIP Console, Avaya SIP deskphones, and Avaya Messaging. 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. Configure the other fields in bold and accept the default values for the remaining fields.

```

add trunk-group 10                                     Page 1 of 22

                                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
  
```

5.6. AAR Call Routing

SIP calls to Session Manager are routed over a SIP trunk via AAR call routing. Configure the AAR analysis form and enter add an entry that routes digits beginning with “78” to route pattern 10 as shown below.

```

change aar analysis 78                                     Page 1 of 2

                                AAR DIGIT ANALYSIS TABLE
                                Location: all                Percent Full: 1

Dialed      Total      Route      Call      Node      ANI
String      Min  Max    Pattern    Type      Num      Req'd
78          5   5     10         lev0      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
                                Intw
1: 10  0
2:
3:
4:
5:
6:

                                DCS/ IXC
                                QSIG
                                Intw
n    user
n    user
n    user
n    user
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
  
```

6. Configure Avaya Aura® Session Manager

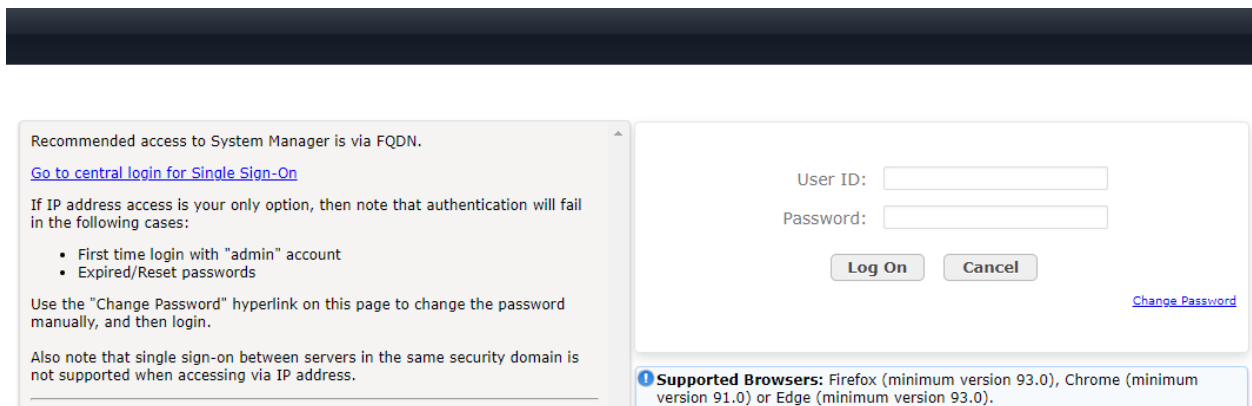
This section provides the procedure for configuring Session Manager. The procedures include the following areas:

- Launch System Manager
- Set Network Transport Protocol for Scout VoIP Console
- Administer SIP User

Note: It is assumed that basic configuration of Session Manager has already been performed. This section will focus on the configuration of a SIP user for the Scout VoIP Console.

6.1. Launch System Manager

Access the System Manager Web interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of the System Manager server. Log in using the appropriate credentials.



Recommended access to System Manager is via FQDN.
[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

User ID:

Password:

[Change Password](#)

Supported Browsers: Firefox (minimum version 93.0), Chrome (minimum version 91.0) or Edge (minimum version 93.0).

6.2. Set Network Transport Protocol for Scout VoIP Console

From the System Manager **Home** screen, select **Elements** → **Routing** → **SIP Entities** and edit the SIP Entity for Session Manager shown below.

The screenshot shows the Avaya Aura System Manager 10.1 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', 'Shortcuts', a search bar, and a user profile 'admin'. The left sidebar shows a tree view with 'Routing' selected, and 'SIP Entities' highlighted. The main content area is titled 'SIP Entity Details' and contains two sections: 'General' and 'Monitoring'. In the 'General' section, the 'Name' is 'devcon-sm', 'IP Address' is '10.64.102.117', 'SIP FQDN' is empty, 'Type' is 'Session Manager', 'Notes' is empty, 'Location' is 'Thornton', 'Outbound Proxy' is empty, 'Time Zone' is 'America/New_York', 'Minimum TLS Version' is 'Use Global Setting', and 'Credential name' is empty. In the 'Monitoring' section, 'SIP Link Monitoring' and 'CRLF Keep Alive Monitoring' are both set to 'Use Session Manager Configuration'. 'Commit' and 'Cancel' buttons are at the top right.

General	
* Name:	devcon-sm
* IP Address:	10.64.102.117
SIP FQDN:	
Type:	Session Manager
Notes:	
Location:	Thornton
Outbound Proxy:	
Time Zone:	America/New_York
Minimum TLS Version:	Use Global Setting
Credential name:	

Monitoring	
SIP Link Monitoring:	Use Session Manager Configuration
CRLF Keep Alive Monitoring:	Use Session Manager Configuration

Scroll down to the **Listen Ports** section and verify that the transport network protocol used by Scout VoIP Console is specified in the list below. For the compliance test, the solution used UDP network transport.

Listen Ports

<div>Add Remove</div>					
3 Items Filter: Enable					
<input type="checkbox"/>	Listen Ports	Protocol	Default Domain	Endpoint	Notes
<input type="checkbox"/>	5060	TCP	avaya.com	<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/>	5060	UDP	avaya.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	5061	TLS	avaya.com	<input checked="" type="checkbox"/>	
Select : All, None					

6.3. Administer SIP User

In the subsequent screen (not shown), select **Users** → **User Management** → **Manage Users** to display the **User Management** screen below. Click **New** to add a user.

	First Name	Surname	Display Name	Login Name	SIP Handle
<input type="checkbox"/>	SIP	78000	78000, SIP	78000@avaya.com	78000
<input type="checkbox"/>	SIP	78001	78001, SIP	78001@avaya.com	78001
<input type="checkbox"/>	SIP	78002	78002, SIP	78002@avaya.com	78002
<input type="checkbox"/>	SIP	78003	78003, SIP	78003@avaya.com	78003

6.3.1. Identity

The **New User Profile** screen is displayed. Enter the desired **Last Name** and **First Name**. For **Login Name**, enter “<ext>@<domain>”, where “<ext>” is the desired Scout VoIP Console SIP extension and “<domain>” is the applicable SIP domain name from **Section 5.3**. Retain the default values in the remaining fields.

User Profile | Add

Commit & Continue | Commit | Cancel

Identity | Communication Profile | Membership | Contacts

Basic Info

Address

LocalizedName

User Provisioning Rule: [v]

* Last Name: 78010 Last Name (in Latin alphabet characters): 78010

* First Name: Avtec First Name (in Latin alphabet characters): Avtec

* Login Name: 78010@avaya.com Middle Name: Middle Name Of User

6.3.2. Communication Profile

Select the **Communication Profile** tab. Next, click on **Communication Profile Password**. For **Comm-Profile Password** and **Re-enter Comm-Profile Password**, enter the desired password for the SIP user to use for registration. Click **OK**.

The screenshot shows the Avaya Aura System Manager 10.1 interface. The 'User Management' sidebar is on the left, and the 'User Profile | Add' form is in the center. The 'Communication Profile' tab is selected. A dialog box titled 'Comm-Profile Password' is open, showing two password fields: 'Comm-Profile Password' and 'Re-enter Comm-Profile Password'. The 'Re-enter' field has a green checkmark, indicating the passwords match. There is a 'Generate Comm-Profile Password' link and 'Cancel' and 'OK' buttons at the bottom of the dialog.

6.3.3. Communication Address

Click on **Communication Address** and then click **New** to add a new entry. The **Communication Address Add/Edit** dialog box is displayed as shown below. For **Type**, retain *Avaya SIP*. For **Fully Qualified Address**, enter and select the SIP user extension and domain name to match the login name from **Section 6.3.1**. Click **OK**.

The screenshot shows the Avaya Aura System Manager 10.1 interface. The 'User Management' sidebar is on the left, and the 'User Profile | Add' form is in the center. The 'Communication Profile' tab is selected. A dialog box titled 'Communication Address Add/Edit' is open, showing two fields: 'Type' (set to 'Avaya SIP') and 'Fully Qualified Address' (set to '78010 @ avaya.com'). There are 'Cancel' and 'OK' buttons at the bottom of the dialog.

6.3.4. Session Manager Profile

Click on toggle button by **Session Manager Profile**. For **Primary Session Manager**, **Origination Application Sequence**, **Termination Application Sequence**, and **Home Location**, select the values corresponding to the applicable Session Manager and Communication Manager. Retain the default values in the remaining fields.

The screenshot displays the 'User Profile | Add' form in the Avaya Aura System Manager 10.1 interface. The left sidebar shows the 'User Management' menu with 'Manage Users' selected. The main content area has tabs for 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. The 'Communication Profile' tab is active, showing a 'Communication Profile Password' field and a 'PROFILES' section with a 'Session Manager Profile' toggle turned on. The 'SIP Registration' section contains fields for 'Primary Session Manager' (devcon-sm), 'Secondary Session Manager' (Start typing...), and 'Survivability Server' (Start typing...). The 'Application Sequences' section shows 'Origination Sequence' and 'Termination Sequence' both set to 'DEVCON-CM App S...'. The 'Call Routing Settings' section is partially visible at the bottom, showing 'Home Location' set to 'Thornton' and 'Conference Factory Set' set to 'Select'.

Scroll down to the **Call Routing Settings** section to configure the **Home Location**.

The screenshot shows the 'Call Routing Settings' section of the form. It includes a 'Home Location' field set to 'Thornton' and a 'Conference Factory Set' dropdown menu set to 'Select'.

6.3.5. CM Endpoint Profile

Click on the toggle button by **CM Endpoint Profile**. For **System**, select the value corresponding to the applicable Communication Manager. For **Extension**, enter the SIP user extension from **Section 6.3.3**. For **Template**, select *9641SIP_DEFAULT_CM_8_1*. For **Port**, click and select *IP*. Retain the default values in the remaining fields. Click on the Endpoint Editor (i.e., Edit icon in Extension field) to set the **Coverage Path** to voicemail.

The screenshot displays the Avaya Aura System Manager 10.1 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 10.1', and various menu items: Users, Elements, Services, Widgets, and Shortcuts. A search bar and user profile (admin) are also present. The left sidebar shows the 'User Management' section with options like 'Manage Users', 'Public Contacts', 'Shared Addresses', 'System Presence ACLs', and 'Communication Profile ...'. The main content area is titled 'User Profile | Add' and features tabs for 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. The 'Communication Profile' tab is active, showing a form for adding a new profile. The form includes fields for 'System' (devcon-cm), 'Profile Type' (Endpoint), 'Extension' (78010), 'Template' (9641SIP_DEFAULT_CM_8_1), 'Set Type' (9641SIP), 'Security Code' (Enter Security Code), 'Port' (IP), 'Voice Mail Number', 'Preferred Handle' (Select), 'Sip Trunk' (aar), 'Calculate Route Pattern' (Calculate Route Pattern), 'SIP URI' (Select), 'Delete on Unassign from User or on Delete' (checked), 'Override Endpoint Name and Localized Name' (checked), and 'Allow H.323 and SIP Endpoint Dual Registration' (unchecked). The 'CM Endpoint Profile' toggle is turned on.

Navigate to the **General Options** tab and set the **Coverage Path 1** field to the voicemail coverage path. This provides voicemail coverage for the SIP user. In this example, coverage path *15* was used.

New Endpoint

Help ?

Done

[Save As Template]

* System

devcon-cm

* Template

9641SIP_DEFAULT_CM_8_1

* Port

IP

Name

* Extension

78010

Set Type

9641SIP

Security Code

Display Extension Ranges

General Options (G) *

Feature Options (F)

Site Data (S)

Abbreviated Call Dialing (A)

Enhanced Call Fwd (E)

Button Assignment (B)

Profile Settings (P)

Group Membership (M)

* Class of Restriction (COR)

1

* Emergency Location Ext

78010

* Tenant Number

1

* SIP Trunk

Qaar

Coverage Path 1

15

Lock Message

☐

Multibyte Language

Not Applicable

* Class Of Service (COS)

1

* Message Lamp Ext.

78010

Type of 3PCC Enabled

None

Coverage Path 2

Localized Display Name

Enable Reachability for Station Domain Control

system

7. Configure Avtec Scout VoIP Console

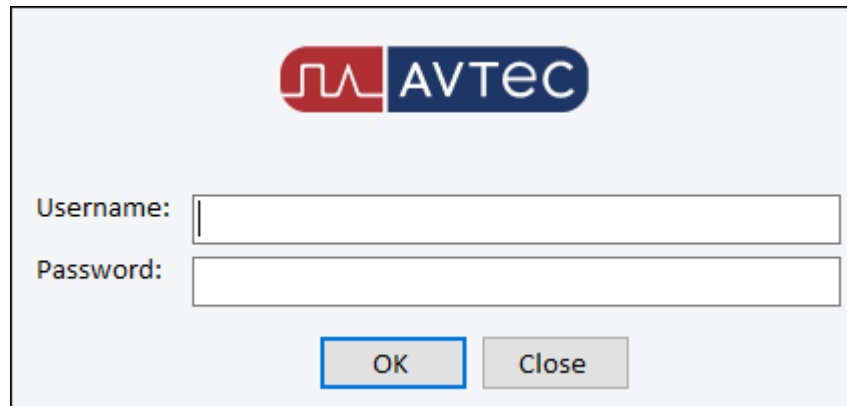
This section covers the configuration of Scout VoIP Console using the **Scout Manager** application. This section assumes that the Scout VoIP Console software has already been installed successfully. In the **Scout Manager** application, the following procedures are performed:

- Launch Scout Manager
- Add Endpoints
- Modify SIP Line Label and Set Endpoint Profile
- Add Voicemail/MWI Button
- Deploy the Configuration

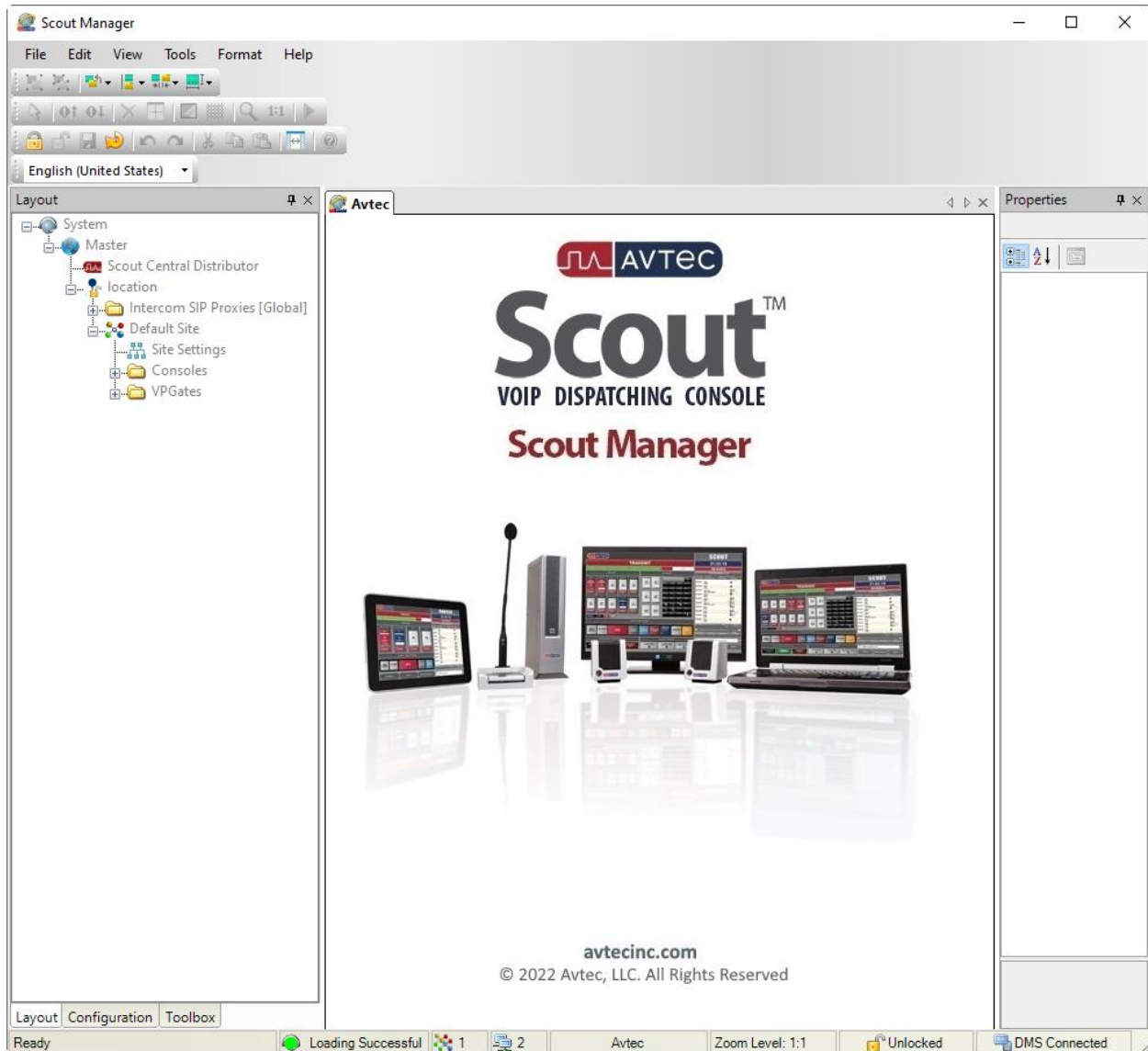
7.1. Launch Scout Manager



Launch the **Scout Manager** application by clicking on the appropriate icon. The following screen is displayed. Log in with the appropriate credentials.

A login dialog box for the Avtec Scout Manager application. It features the Avtec logo at the top, which consists of a red square with a white waveform and the word 'AVTEC' in white on a blue background. Below the logo are two input fields: 'Username:' and 'Password:'. At the bottom are two buttons: 'OK' and 'Close'.

Once logged in, the **Scout Manager** screen appears as shown below. Click on the **Lock** icon to allow configuration.



7.2. Add Endpoints

Endpoints are created under VPGate configuration. 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., 78010).
- **Service State:** Set to *Available*.

Under **Endpoint Connection**:

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

Under **VoIP Audio Settings**:

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

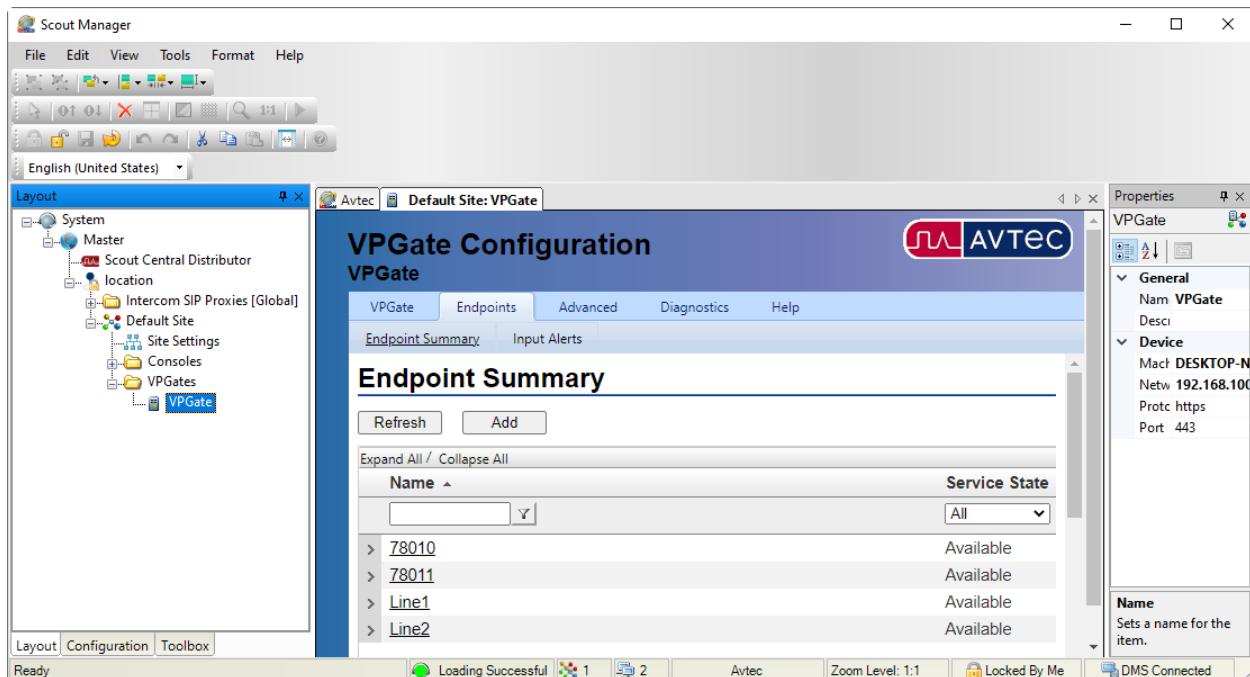
Use the default settings for the remaining fields. Click the **Add** button.

The screenshot displays the Avtec Scout Manager VPGate Configuration interface. The main window is titled "VPGate Configuration" and features a navigation pane on the left with a tree view showing the system hierarchy: System > Master > Location > Intercom SIP Proxies [Global] > Default Site > Site Settings > VPGates. The main content area is divided into tabs: VPGate, Endpoints, Advanced, Diagnostics, and Help. The "Endpoints" tab is active, showing the "Endpoint Summary" and "Input Alerts" sections. The "Endpoint Configuration" page is displayed, featuring a "Add" button and several configuration sections:

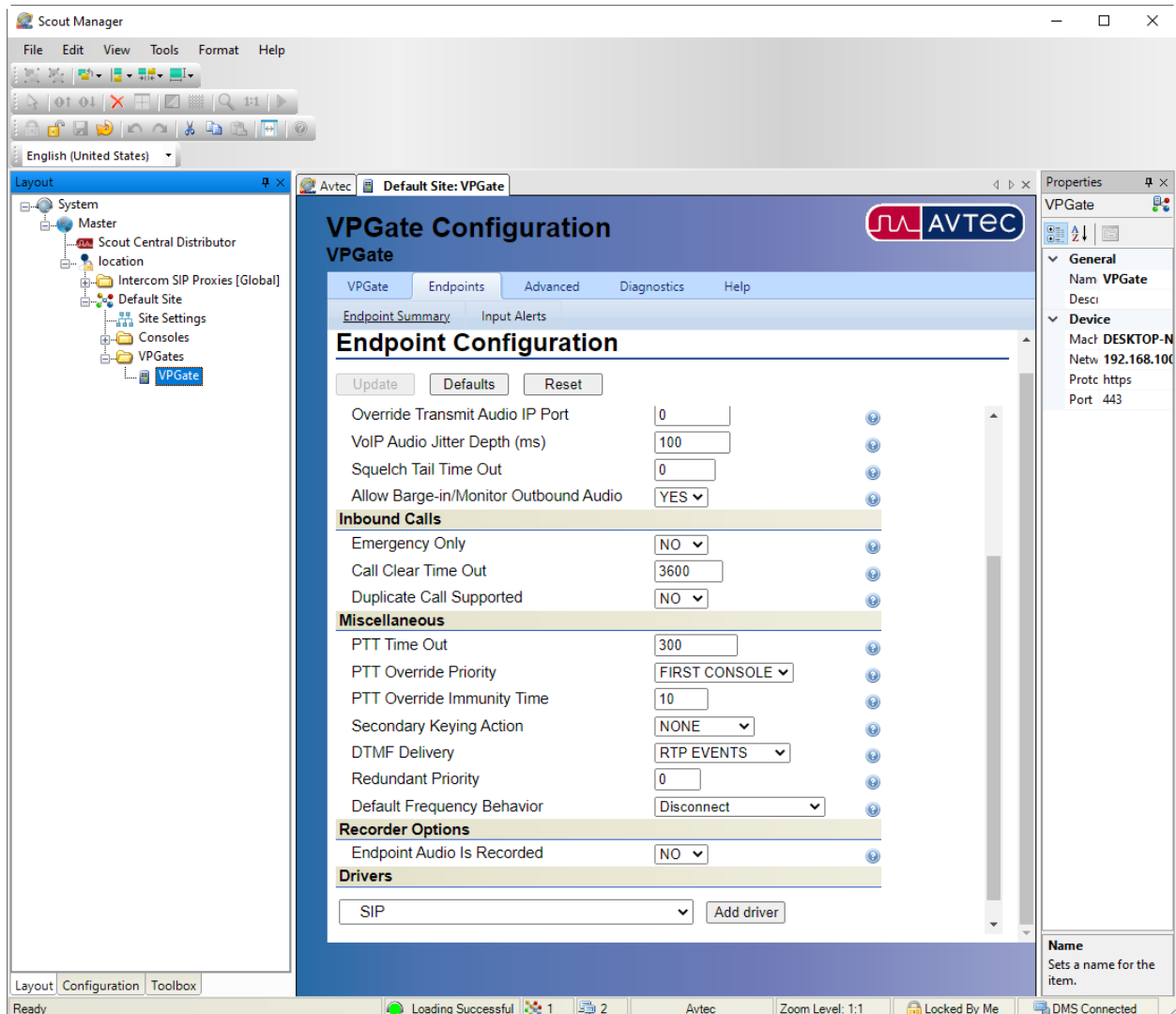
- Endpoint Configuration:**
 - Endpoint Name: 78010
 - Service State: AVAILABLE
- Endpoint Connection:**
 - Endpoint Audio: VoIP
- VoIP Audio Settings:**
 - Receive Audio Mode: FULL DUPLEX
 - Override Receive Audio IP Port: 0
 - Override Transmit Audio IP Port: 0
 - VoIP Audio Jitter Depth (ms): 100
 - Squelch Tail Time Out: 0
 - Allow Barge-in/Monitor Outbound Audio: YES
- Inbound Calls:**
 - Emergency Only: NO
 - Call Clear Time Out: 3600
 - Duplicate Call Supported: NO
- Miscellaneous:**

The right-hand side of the interface shows a "Properties" pane for the selected VPGate, displaying details such as Name (VPGate), Description, Device (Mac Desktop-N), Network (192.168.100), Protocol (https), and Port (443). The bottom status bar indicates "Ready", "Loading Successful", and "DMS Connected".

The **Endpoint** previously added is now displayed in the **Endpoint Summary** page shown below. Click on the endpoint that was previously added (i.e., *78010*) to open the configuration again.

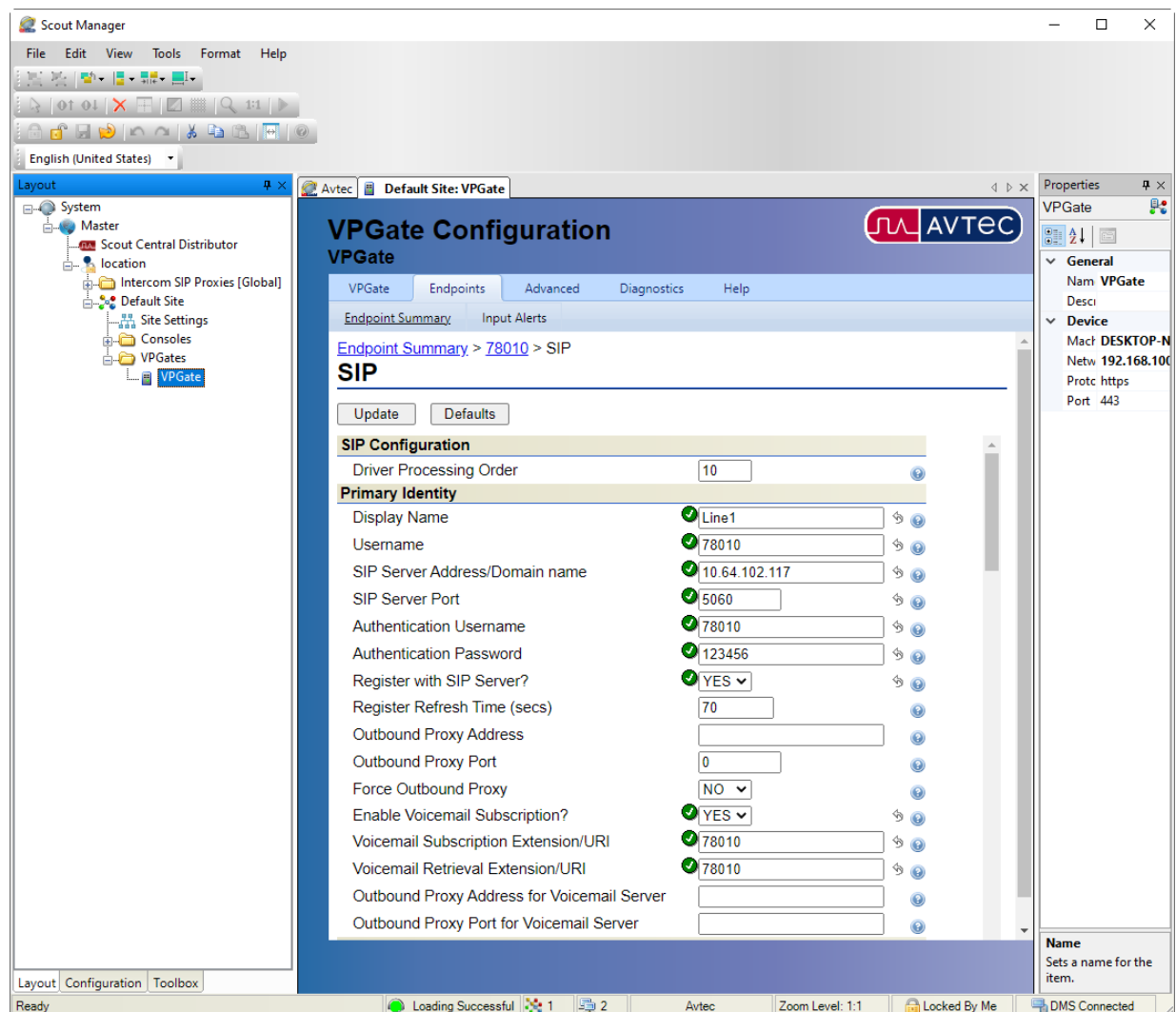


The **Endpoint Configuration** page is displayed. Scroll to the bottom of the page to the **Drivers** section as shown below. Select *SIP* from the drop-down field and click **Add driver**.



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., *78010*).
- **SIP Server Address/Domain name:** Specify the signaling IP address of Session Manager.
- **SIP Server Port:** Specify port *5060*.
- **Authentication Username:** Specify the SIP extension (e.g., *78010*).
- **Authentication Password:** Specify the password used for SIP registration as configured in **Section 6.3.2**.
- **Register with SIP Server:** Enable this option.
- **Enable Voicemail Subscription:** Enable this option.
- **Voicemail Subscription Extension/URL:** Specify the SIP extension (e.g., *78010*).
- **Voicemail Retrieval Extension/URL:** Specify the voicemail number.



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

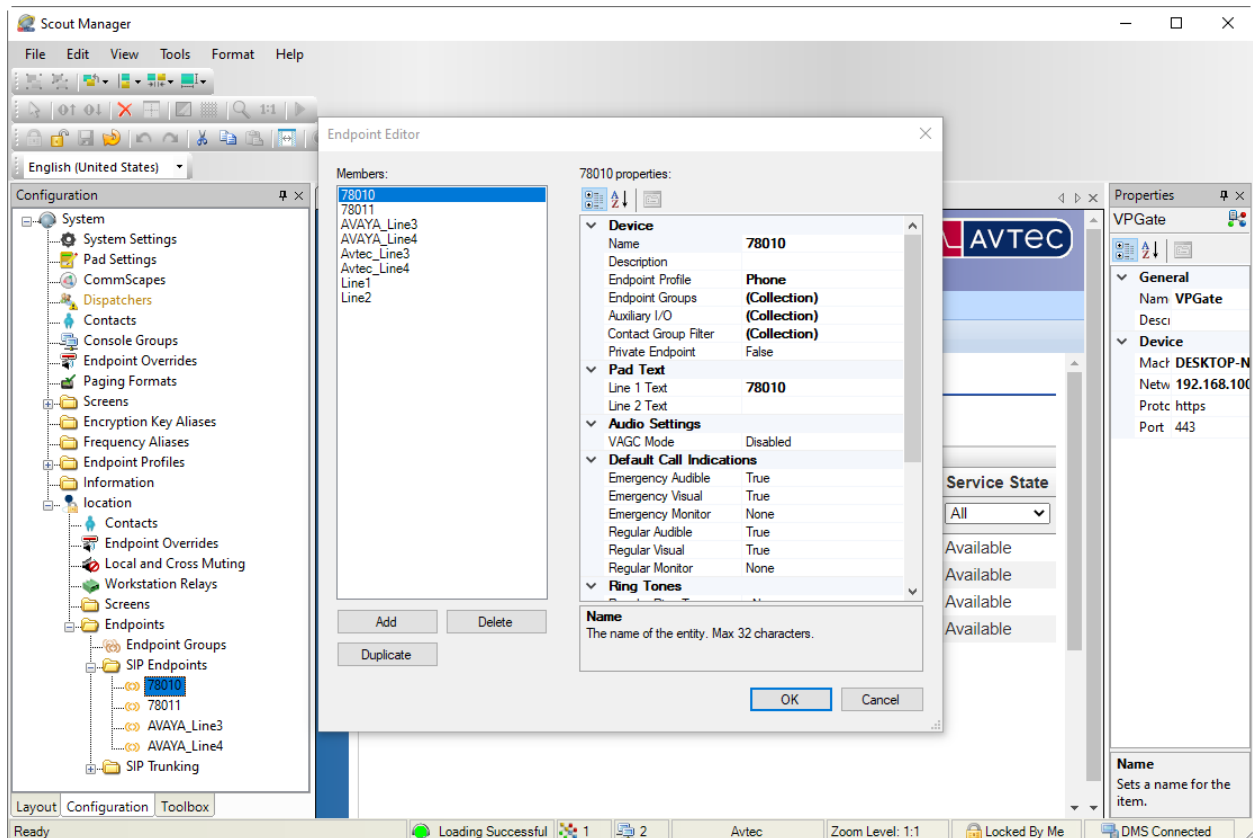
The screenshot displays the Scout Manager interface with the VPGate Configuration window open. The left sidebar shows a tree view with 'VPGate' selected under 'VPGates'. The main window has tabs for 'VPGate', 'Endpoints', 'Advanced', 'Diagnostics', and 'Help'. The 'VPGate' tab is active, showing the 'Endpoint Summary' and 'Input Alerts' sections. Below these, the 'SIP' section is expanded, and the 'CODEC Configuration' table is visible.

CODEC Configuration	
G.711 uLaw Enabled	YES
G.711 uLaw SDP Payload Type	0
G.711 uLaw SDP Description	PCMU
G.729A Enabled	YES
G.729A SDP Payload Type	18
G.729A SDP Description	G729
G.726 16kb Enabled	YES
G.726 16kb SDP Payload Type	97
G.726 16kb SDP Description	G726-16
G.726 32kb Enabled	YES
G.726 32kb SDP Payload Type	96
G.726 32kb SDP Description	G726-32
G.723.1 Enabled	NO
Telephone-Event (RFC2833/4733) Enabled	YES
Telephone-Event SDP Payload Type	101
Telephone-Event SDP Description	telephone-event

The right sidebar shows the 'Properties' panel for the selected VPGate, displaying 'General' and 'Device' information. The 'Device' section shows 'Mac: DESKTOP-N', 'Netw: 192.168.100', 'Prot: https', and 'Port: 443'.

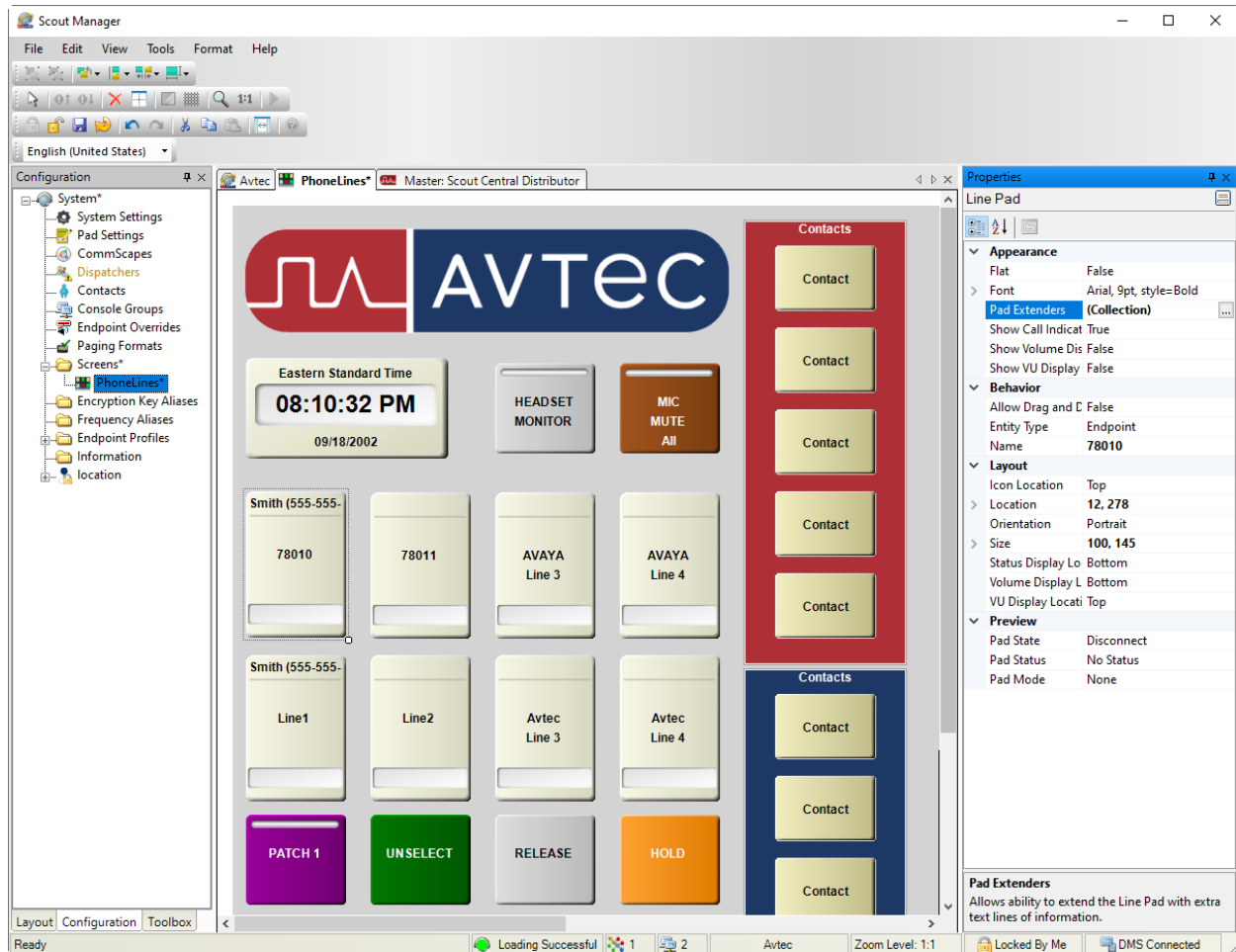
7.3. Modify SIP Line Label and Set Endpoint Profile

To modify the label of the SIP line button on Scout VoIP Console and set the endpoint profile, select the **Configuration** tab in the left pane, double-click on the SIP endpoint added above. In the **Endpoint Editor**, change **Name** and **Line 1 Text** to the SIP extension (e.g., 78010). Set **Endpoint Profile** to *Phone* so that dial tone and ringback (or other audio feedback, such as busy tone) is heard when Scout Console goes off-hook and places an outbound call.

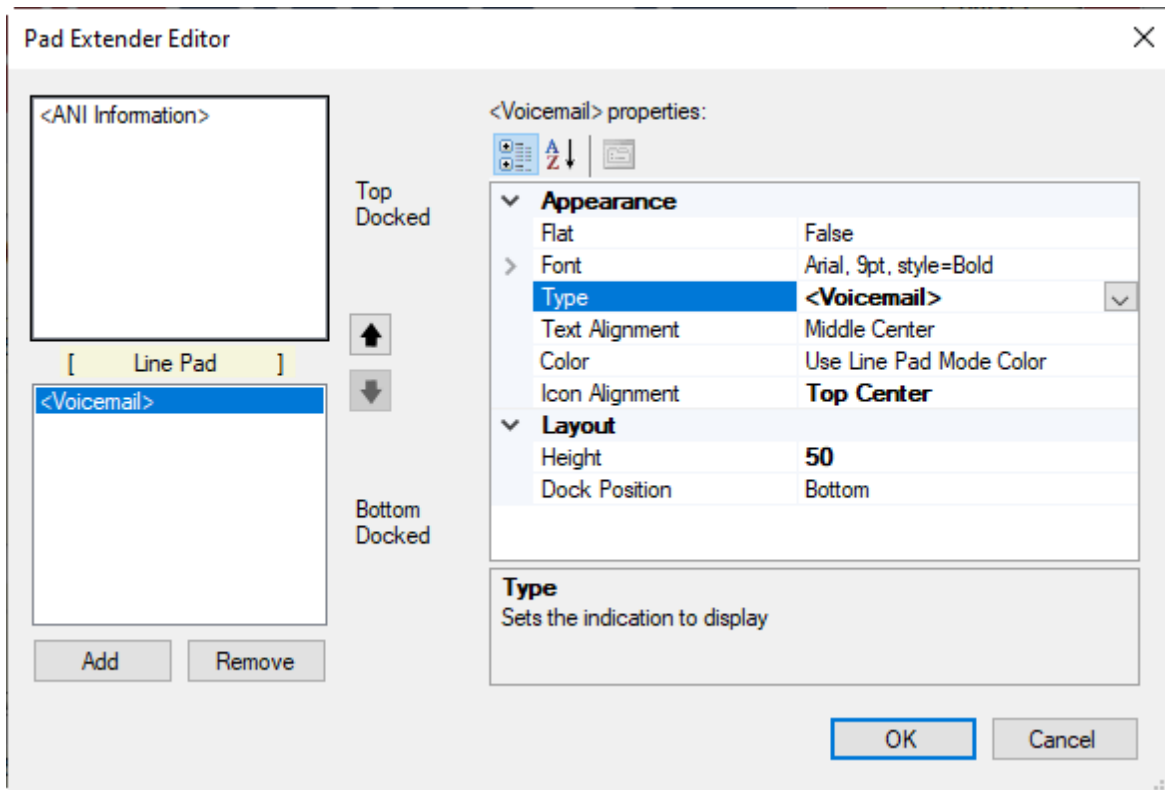


7.4. Add Voicemail/MWI Button

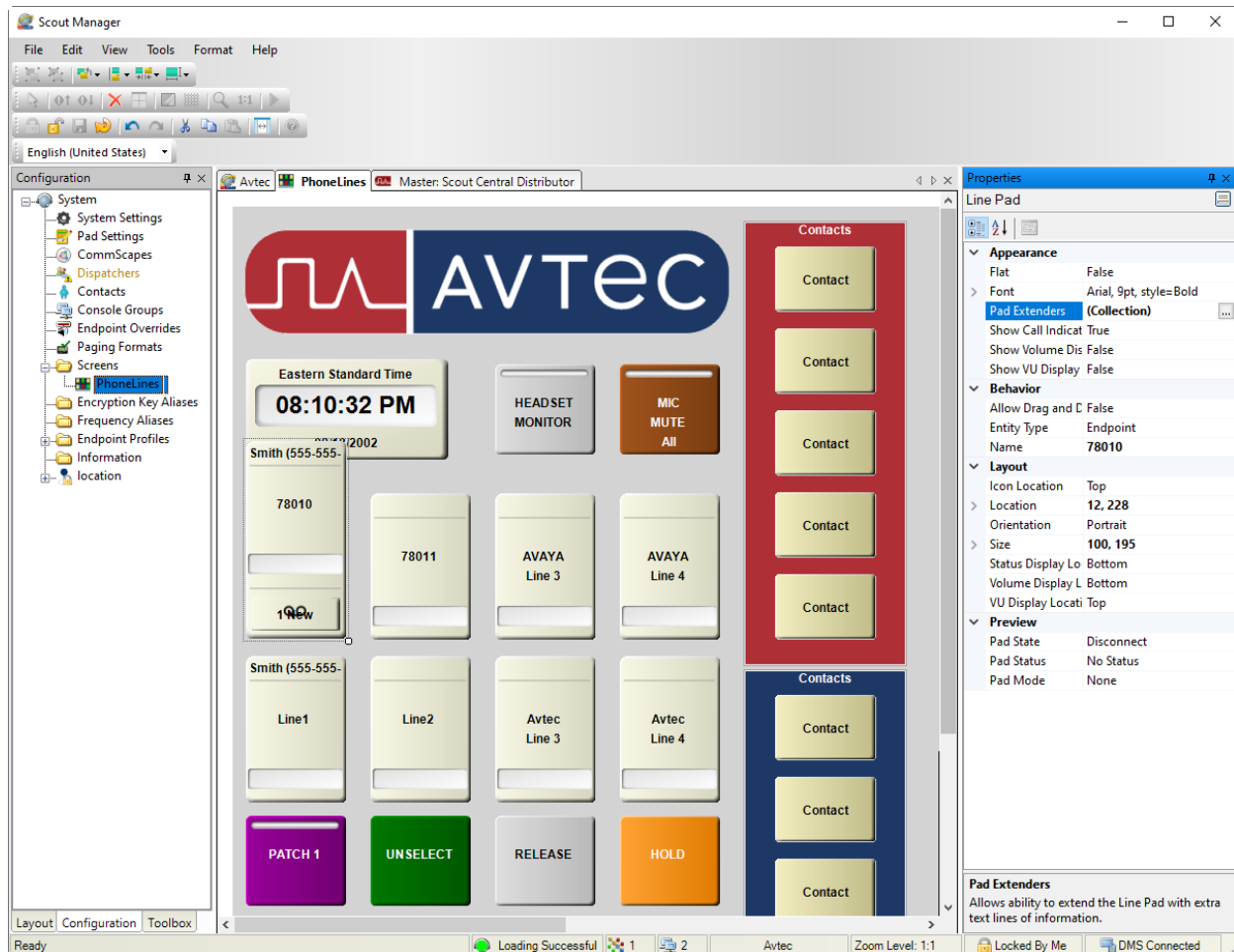
A voicemail/MWI button calls the voicemail system when pressed and provides an indication of any new voicemail messages. To add a voicemail/MWI button associated with a SIP line, select the **Configuration** tab in the left pane and open the **PhoneLines** screen shown below. Next, click on the SIP line button (e.g., 78010) that will be configured with a voicemail/MWI button. In the **Line Pad** section, click on the ellipses (...) button by **Pad Extender** to display the **Pad Extender Editor** window.



The **Pad Extender Editor** window is displayed below. Click the **Add** button. In the properties section to the right, set the **Type** field to *Voicemail*. Select the **Dock Position** for the button. In this example, the button was docked at the *Bottom*. Click **OK**.

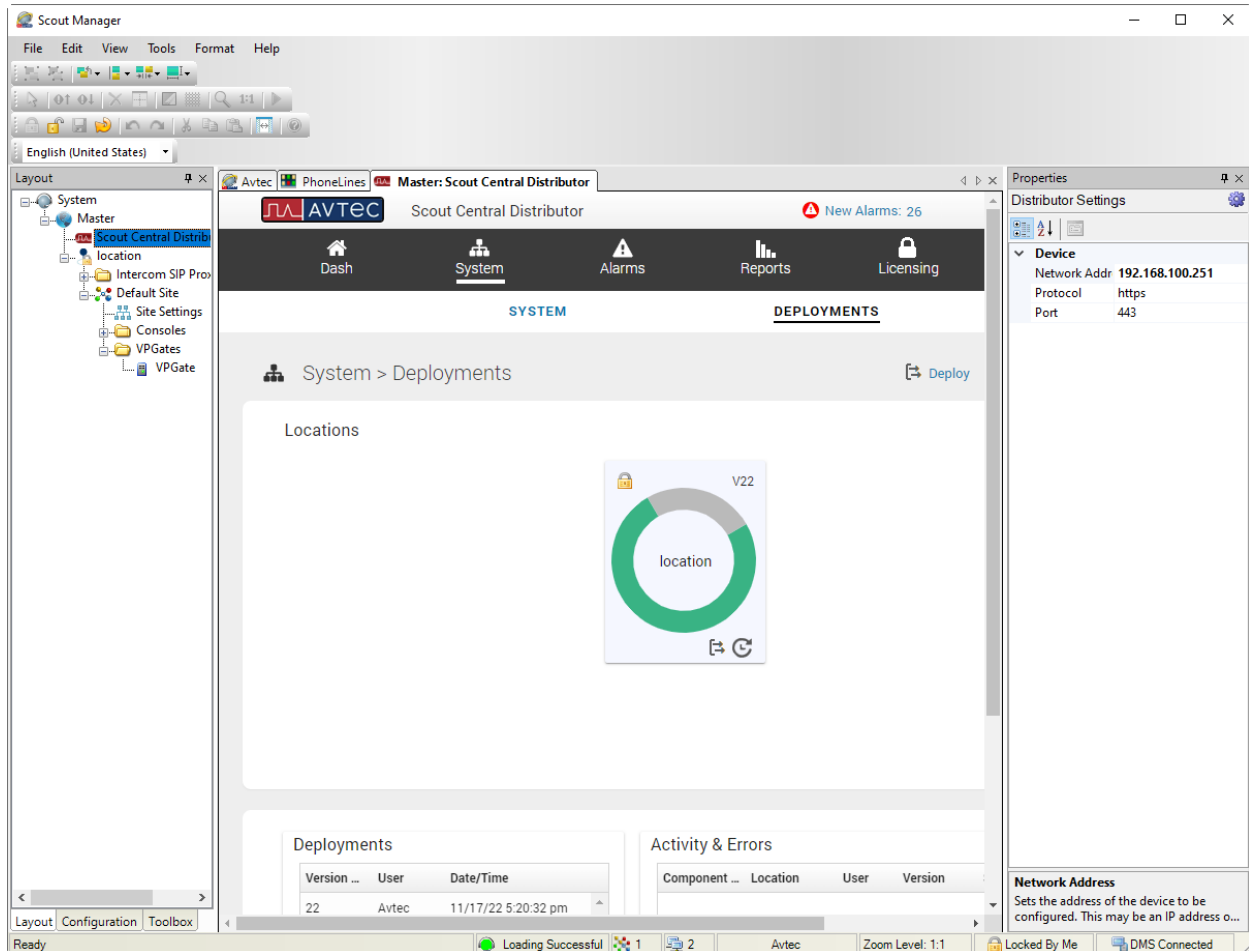


The voicemail/MWI button appears with the SIP line button as shown below. Click **Save**.



7.5. Deploy the Configuration

Lastly, deploy the changes to the **Scout VoIP Console**. Select the **Layout** tab in the left pane and then open the **Scout Central Distributor** screen as shown below. Navigate to **System** → **Deployment** to display the following screen. Click on the **Deploy** hyperlink.



In the **Select Deployment Locations** screen shown below, click the **Deploy** button to deploy the changes to the **Scout VoIP Console**.

Select Deployment Locations

Select deployment location(s) and then click **Deploy**.

☒ [Select All](#) [Missing Locations?](#)

Location Name	
<input checked="" type="checkbox"/>	location

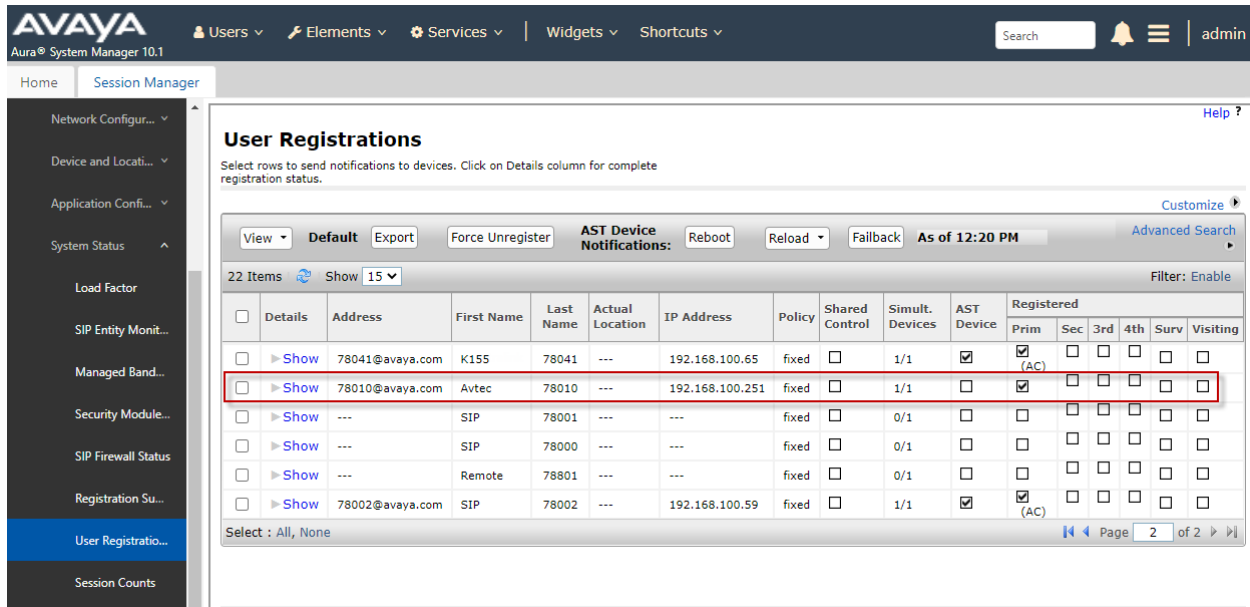
The **Scout VoIP Console** below displays the voicemail/MWI button associated with the appropriate SIP line (e.g., 78010). Note that the label on the SIP line is the SIP extension (78010) , which was changed in **Section 7.3**.



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. Verify that the Scout VoIP Console has successfully registered with Session Manager. In System Manager, navigate to **Elements → Session Manager → System Status → User Registrations** to check the registration status as shown below.



The screenshot displays the Avaya Aura System Manager 10.1 interface. The top navigation bar includes the Avaya logo, a search bar, and a user profile (admin). The left sidebar shows the navigation menu with options like Network Configur..., Device and Locati..., Application Confi..., System Status, Load Factor, SIP Entity Monit..., Managed Band..., Security Module..., SIP Firewall Status, Registration Su..., User Registratio..., and Session Counts. The main content area is titled "User Registrations" and includes a sub-header "Select rows to send notifications to devices. Click on Details column for complete registration status." Below this, there are buttons for View, Default, Export, Force Unregister, AST Device Notifications, Reboot, Reload, and Fallback. A table of 22 items is shown, with 15 items displayed. The table has columns for Details, Address, First Name, Last Name, Actual Location, IP Address, Policy, Shared Control, Simult. Devices, AST Device, and Registered. The row for user 78010@avaya.com is highlighted with a red box, showing a successful registration status.

Details	Address	First Name	Last Name	Actual Location	IP Address	Policy	Shared Control	Simult. Devices	AST Device	Registered
<input type="checkbox"/> Show	78041@avaya.com	K155	78041	---	192.168.100.65	fixed	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)
<input type="checkbox"/> Show	78010@avaya.com	Avtec	78010	---	192.168.100.251	fixed	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)
<input type="checkbox"/> Show	---	SIP	78001	---	---	fixed	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Show	---	SIP	78000	---	---	fixed	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Show	---	Remote	78801	---	---	fixed	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Show	78002@avaya.com	SIP	78002	---	192.168.100.59	fixed	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)

2. Launch the Avtec Scout VoIP Console. The Scout VoIP Console will be displayed as shown below. If the SIP line is down, the line buttons will display *Unavailable*. The line buttons shown below indicate that the SIP lines for extensions 78010 and 78011 are in-service.



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 or PSTN and answer the call. Verify two-way audio is provided.
6. Verify basic telephony features by establishing calls between Scout VoIP Console and another phone.

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. Avtec Scout VoIP Console was successfully registered with Session Manager as a SIP endpoint and basic and supplementary telephony features were verified. All test cases passed with observations noted in **Section 2.2**.

10. Additional References

This section references the Avaya documentation relevant to these Application Notes. The following Avaya product documentation is available at support.avaya.com. Avtec Scout VoIP Console documentation is available through the application via online help.

- [1] *Administering Avaya Aura® Communication Manager*, Release 10.1.x, Issue 1, December 2021, available at <http://support.avaya.com>.
- [2] *Administering Avaya Aura® System Manager*, Release 10.1.x, Issue 6, June 2022, available at <http://support.avaya.com>.
- [3] *Administering Avaya Aura® Session Manager*, Release 10.1.x, Issue 3, April 2022, available at <http://support.avaya.com>.
- [4] *Administering Avaya Session Border Controller for Enterprise*, Release 10.1.x, Issue 1, December 2021, available at <http://support.avaya.com>.

©2023 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.