



Avaya Solution & Interoperability Test Lab

Application Notes for Valcom V-9972 Universal Paging Interface with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using SIP Trunk - Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate the Valcom V-9972 Universal Paging Interface with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Valcom V-9972 Universal Paging Interface provides access to paging systems, such as Valcom VIP-430A IP Wall Speakers, which was used in the compliance test. For this compliance test, Valcom V-9972 Universal Paging Interface connected to Avaya Aura® Session Manager via a SIP trunk. The Valcom V-9972 Universal Paging Interface supports two-way audio intercom (talkback) calls and one-way audio group paging calls.

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

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

1. Introduction

These Application Notes describe the configuration steps required to integrate the Valcom V-9972 Universal Paging Interface with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Valcom V-9972 Universal Paging Interface provides access to paging systems, such as Valcom VIP-430A IP Wall Speakers, which was used in the compliance test. For this compliance test, Valcom V-9972 Universal Paging Interface connected to Avaya Aura® Session Manager via a SIP trunk. The Valcom V-9972 Universal Paging Interface supports two-way audio intercom (talkback) calls and one-way audio group paging calls.

When a call is routed to the Valcom V-9972 Universal Paging Interface, the V-9972 plays dial tone back to the caller. The caller can then dial a Valcom speaker Dial Code or Group Code to establish an intercom call (two-way audio) with a single Valcom speaker or a group paging call (one-way audio) to one or more Valcom speakers.

Alternatively, the Valcom VIP-430A IP Wall Speaker can establish intercom calls by pressing its call button. Pressing the call button would place a call to the specified destination in the V-9972 configuration. Pressing the call button during an active call, terminates the call.

All calls to/from the VIP-430A IP Wall Speaker go through the V-9972. Communication between V-9972 and VIP-430A IP Wall Speaker uses unicast for intercom (talkback) calls and multicast for paging calls.

Valcom offers Universal Paging Adapters as different products/models to accommodate different environments. They share the same SIP stack and firmware version, therefore, this testing also applies to those products, as detailed in **Attachment 1. Section 4** of this document shows the actual products/models and SIP Stack and software versions that were tested. For additional details, contact Valcom Support, as noted in **Section 2.3**.

2. General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing. The feature testing focused on establishing calls between the Valcom V-9972 Universal Paging Interface with the Valcom VIP-430A IP Wall Speaker, Avaya SIP / H.323 IP Deskphones, and the PSTN. Two-way audio intercom calls and one-way audio group paging calls were exercised. In addition, basic telephony features were exercised from Avaya SIP / H.323 IP Deskphones, such as hold/resume, call transfer, and conference.

The serviceability testing focused on verifying that the Valcom V-9972 Universal Paging Interface came back into service after reconnecting the network connection or a reboot.

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 Valcom V-9972 Universal Paging Interface used TLS/SRTP encryption features.

2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- Establishing a SIP trunk between V-9972 and Session Manager and verifying the exchange of SIP Options messages.
- Calls between V-9972 and Avaya H.323/SIP endpoints with Direct IP Media (Shuffling) enabled and disabled. Shuffling allows IP endpoints to send audio RTP packets directly to each other without using media resources on Avaya Media Gateway or Avaya Aura® Media Server.
- Establishing two-way audio intercom calls between VIP-430A IP Wall Speaker, via V-9972, Avaya H.323 / SIP Deskphones, and PSTN in both directions.
- Establishing one-way paging calls from Avaya H.323 / SIP Deskphones to VIP-430A IP Wall Speaker via V-9972.
- Verifying that higher priority paging calls take precedence over existing lower priority intercom calls.
- Terminating calls by pressing the call button on the VIP-430A IP Wall Speaker.
- Support of G.711 mu-law codec.
- Support of TLS/SRTP using mutual TLS authentication.
- Since the VIP-430A IP Wall Speaker does not provide a keypad or feature buttons, basic telephony features, such as hold/resume, call transfer, and conference were performed from Avaya H.323/SIP Deskphones.
- Long duration calls and outbound calls from V-9972 that were rejected due to dialing an invalid number or a busy station.
- Proper system recovery after re-establishing network connectivity to the V-9972 or restarting the V-9972.

2.2. Test Results

All test cases passed.

2.3. Support

For technical support and information on Valcom V-9972 Universal Paging Interface, contact Valcom Technical Support at:

- Phone: +1 (800) 825-2661 or +1 (540) 563-2000
- Website: <https://www.valcom.com/Support/techsupport.html>
- Email: support@valcom.com

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 G450 Media Gateway.
- Media resources in Avaya G450 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 endpoints.
- Avaya Aura® System Manager used to configure Session Manager.
- Avaya 96x1 Series H.323 and SIP Deskphones.
- Valcom V-9972 Universal Paging Interface connected to Avaya Aura® Session Manager via a SIP trunk and Valcom VIP-430A IP Wall Speaker.

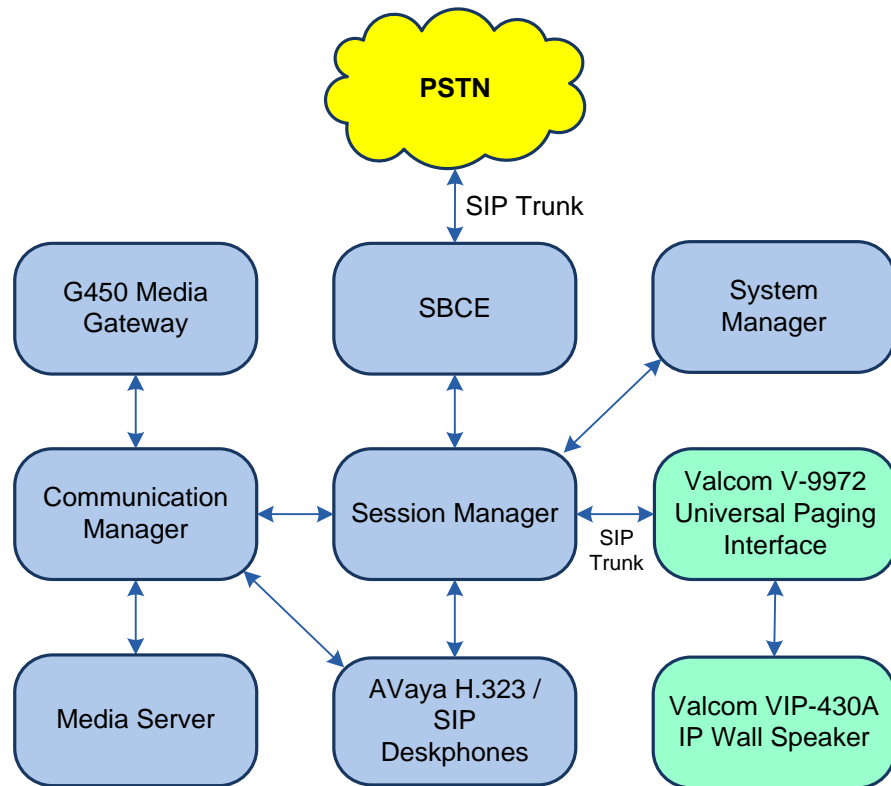


Figure 1: Avaya SIP Network with Valcom V-9972 Universal Paging Interface and Valcom VIP-430A IP Wall Speakers

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	8.1.3.4.0-FP3SP4
Avaya G450 Media Gateway	41.34.4
Avaya Aura® Media Server	8.0.2.138
Avaya Aura® System Manager	8.1.3.4 Build No. – 8.1.0.0.733078 Software Update Revision No: 8.1.3.4-1014185
Avaya Aura® Session Manager	8.1.3.4.813401
Avaya Session Border Controller for Enterprise	8.1.2.0-19794
Avaya 96x1 Series IP Deskphones	6.8511 (H.323)
Avaya J100 Series IP Deskphones	4.0.10.3.2 (SIP)
Valcom V-9972 Universal Paging Interface, including optional L9972-2 feature license	3.00.14
Valcom VIP-430A IP Wall Speaker	3.23.7
Valcom VIP-102B IP Solutions Setup Tool	8.4.0.0

5. Configure Avaya Aura® Communication Manager

This section provides the procedure for configuring Communication Manager. The procedure includes the following areas:

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

Use the System Access Terminal (SAT) to configure Communication Manager and log in with appropriate credentials.

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*). These 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		

5.2. 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 Avaya G450 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. The UDP port range is also specified in this form.

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		
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		

5.3. Administer IP Codec Set

In the **IP Codec Set** form, the audio codec type supported for calls routed over the SIP trunk to V-9972 is specified. The form is accessed via the **change ip-codec-set 1** command. Note that IP codec set 1 was specified in IP Network Region 1 shown above. The default settings of the **IP Codec Set** form are shown below. V-9972 supports G.711 codecs with the VIP-430A IP Wall Speaker.

To enable SRTP, **Media Encryption** was set to *1-srtp-aescm128-hmac80* and **Encrypted SRTCP** was left at the default value of *best-effort*. Note that RTP, which would be indicated by *none* under **Media Encryption**, must not be included.

change ip-codec-set 1

Page1 of 2

IP MEDIA PARAMETERS

Codec Set: 1

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

Media Encryption

Encrypted SRTCP: best-effort

1: 1-srtp-aescm128-hmac80

2: 2-srtp-aescm128-hmac32

3:

4:

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*.
- Set the **Enforce SIPS URI for SRTP** field 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.
- 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*.
- Enable **Initial IP-IP Direct Media**.

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
DTMF over IP: rtp-payload		RFC 3389 Comfort Noise? n
Session Establishment Timer(min): 3		Direct IP-IP Audio Connections? y
Enable Layer 3 Test? y		IP Audio Hairpinning? n
H.323 Station Outgoing Direct Media? n		Initial IP-IP Direct Media? y
		Alternate Route Timer(sec): 6

Configure the **Trunk Group** form as shown below. This trunk group is used for SIP calls to/from V-9972, Avaya SIP Deskphones, and the PSTN. Set the **Group Type** field to *sip*, set the **Service Type** field to *tie* or *public-ntwrk*, 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: public-ntwrk	Auth Code? n		
	Member Assignment Method: auto		
	Signaling Group: 10		
	Number of Members: 10		

Page 5 of the SIP trunk group was configured as follows.

add trunk-group 10		Page 5 of 5	
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: 101			
Convert 180 to 183 for Early Media? n			
Always Use re-INVITE for Display Updates? n			
Resend Display UPDATE Once on Receipt of 481 Response? 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. 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 String	Total Min	Max	Route Pattern	Call Type	Node Num	ANI 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 No	FRL	NPA	Pfx	Hop	Toll	No.	Inserted			DCS/ IXC	
			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

6. Configure Avaya Aura® Session Manager

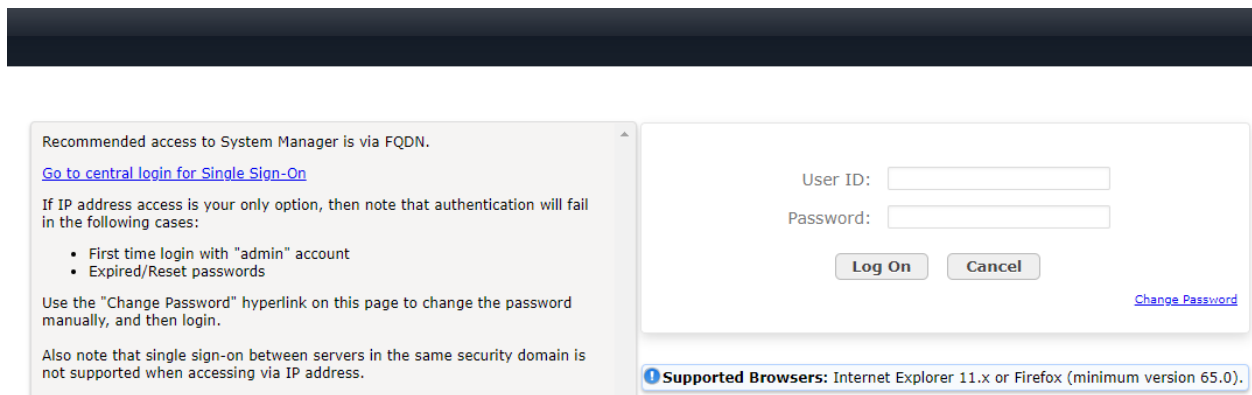
This section provides the procedure for configuring Session Manager, which is required whether V-9972 registers directly with Session Manager or through SBCE as a remote worker. The procedures include the following areas:

- Launch System Manager
- Administer SIP Entities for Session Manager and V-9972
- Administer Entity Link between Session Manager and V-9972
- Add Routing Policy
- Add Dial Pattern
- Enable Monitoring on Session Manager
- Install Valcom V-9972 Universal Paging Interface TLS Certificate

Note: It is assumed that basic configuration of Session Manager has already been performed. This section will focus on the configuration of the SIP trunk to Valcom V-9972 Universal Paging Interface and routing calls to it.

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: Internet Explorer 11.x or Firefox (minimum version 65.0).

6.2. Administer SIP Entities

This section covers the configuration of SIP Entities for Session Manager and V-9972.

6.2.1. Avaya Aura® Session Manager

From the System Manager **Home** screen, navigate to **Elements → Routing → SIP Entities** and click on the **New** button (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 signaling interface on Session Manager.
- **Type:** Select *Session Manager*.
- **Location:** Select one of the locations defined previously.
- **Time Zone:** Time zone for this location.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, a search bar, and user information (admin). The left sidebar shows the navigation menu with 'Routing' selected. The main content area displays the 'SIP Entity Details' configuration page. The 'General' tab is active, showing fields for 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), and Credential name. The 'Monitoring' tab is also visible, showing SIP Link Monitoring and CRLF Keep Alive Monitoring, both set to 'Use Session Manager Configuration'.

6.2.2. Valcom V-9972 Universal Paging Interface

A SIP Entity must be added for V-9972. To add a SIP Entity, navigate to **Elements** → **Routing** → **SIP Entities** and click on the **New** button (not shown). The following screen is displayed. Fill in the following:

Under *General*:

- **Name:** A descriptive name.
- **FQDN or IP Address:** V-9972 IP address.
- **Type:** Select *SIP Trunk*.
- **Location:** Select one of the locations previously defined.
- **Time Zone:** Time zone for this location.

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

The screenshot displays the Avaya Aura System Manager 8.1 web interface. The top navigation bar includes the Avaya logo, a search bar, and links for Users, Elements, Services, Widgets, and Shortcuts. The left sidebar shows a menu with options like Routing, Domains, Locations, Conditions, Adaptations, SIP Entities (highlighted), Entity Links, Time Ranges, Routing Policies, and Dial Patterns. The main content area is titled 'SIP Entity Details' and features a 'General' tab. The form contains the following fields: Name (Valcom V-9972), FQDN or IP Address (192.168.100.197), Type (SIP Trunk), Notes, Adaptation, Location (Thornton), Time Zone (America/New_York), SIP Timer B/F (in seconds) (4), Minimum TLS Version (Use Global Setting), Credential name, and a Securable checkbox.

Field	Value
Name	Valcom V-9972
FQDN or IP Address	192.168.100.197
Type	SIP Trunk
Notes	
Adaptation	
Location	Thornton
Time Zone	America/New_York
SIP Timer B/F (in seconds)	4
Minimum TLS Version	Use Global Setting
Credential name	
Securable	<input type="checkbox"/>

6.3. Administer Entity Link between Session Manager and V-9972

The SIP trunk between Session Manager and V-9972 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., *Valcom V-9972 Link*).
- **SIP Entity 1:** Select the Session Manager.
- **Protocol:** Select TLS transport protocol.
- **Port:** Port number to which the other system sends SIP requests.
- **SIP Entity 2:** Select the *Valcom V-9972* SIP entity.
- **Port:** Port number on which the other system receives SIP requests.
- **Connection Policy:** Select *Trusted*. *Note: If the link is not trusted, calls from the associated SIP Entity specified in Section 6.2 will be denied.*

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

The screenshot shows the Avaya Aura System Manager 8.1 interface. The left sidebar contains a navigation menu with the following items: Home, Routing, Domains, Locations, Conditions, Adaptations, SIP Entities, Entity Links (selected), Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Entity Links' and features a table with 11 items. The table has the following columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, DNS Override, Connection Policy, Deny New Service, and Notes. The 'Valcom V-9972 Link' is highlighted with a red border. The table data is as follows:

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service	Notes
devcon-aam Link	devcon-sm	TLS	5061	devcon-aam	5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
devcon-cm Link	devcon-sm	TLS	5061	devcon-cm	5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
devcon-cm SBC Trk Link	devcon-sm	TLS	5062	devcon-cm SBC Trk	5062	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
devcon-ipose Link	devcon-sm	TLS	5061	devcon-ipose	5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
devcon-ixm Link	devcon-sm	TLS	5061	devcon-ixm	5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
devcon-mpp Link	devcon-sm	TLS	5061	devcon-mpp	5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
devcon-sbce Link	devcon-sm	TLS	5061	devcon-sbce	5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>	
Valcom V-9972 Link	devcon-sm	TLS	5061	Valcom V-9972	5061	<input type="checkbox"/>	trusted	<input type="checkbox"/>	

6.4. Add Routing Policy

A routing policy describes the conditions under which calls will be routed to the V-9972 SIP entity. To add a routing policy, navigate to **Elements → Routing → Routing Policies** and click on the **New** button (not shown). 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.

Defaults can be used for the remaining fields. Click **Commit** to save each Routing Policy definition. The following screen shows the Routing Policy for V-9972.

The screenshot displays the 'Routing Policy Details' page in the Avaya Aura System Manager 8.1. The left sidebar shows the navigation menu with 'Routing Policies' selected. The main content area is divided into three sections: 'General', 'SIP Entity as Destination', and 'Time of Day'.

General Section:

- Name:** Valcom Policy
- Disabled:** ☐
- Retries:** 0
- Notes:** (empty text box)

SIP Entity as Destination Section:

A 'Select' button is present above a table listing available SIP entities.

Name	FQDN or IP Address	Type	Notes
Valcom V-9972	192.168.100.197	SIP Trunk	

Time of Day Section:

Buttons: Add, Remove, View Gaps/Overlaps. Filter: Enable

1 Item

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

6.5. Add Dial Pattern

Dial patterns must be defined to direct calls to the appropriate SIP Entity. In the sample configuration, 78570 is routed to V-9972. To add a dial pattern, navigate to **Elements** → **Routing** → **Dial Patterns** and click on the **New** button (not shown). 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.

Default values can be used for the remaining fields. Click **Commit** to save this dial pattern. The following screen shows the dial pattern definition for V-9972.

AVAYA Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾

Search 🔍 🔔 ☰ admin

Home Routing

Dial Pattern Details Commit Cancel Help ?

General

* **Pattern:** 78570

* **Min:** 5

* **Max:** 5

Emergency Call: ☐

SIP Domain: -ALL- ▾

Notes: Valcom V-9972

Originating Locations and Routing Policies

Add Remove

1 Item 🔍

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Thornton		Valcom Policy	0	<input type="checkbox"/>	Valcom V-9972	

Select : All, None

Denied Originating Locations

Add Remove

0 Items 🔍

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

Commit Cancel

6.6. Enable Monitoring on Avaya Aura® Session Manager

Verify that monitoring is enabled for Session Manager. Navigate to **Elements** → **Session Manager** → **Session Manager Administration**, select the appropriate Session Manager and click **Edit** (not shown). This assumes that Session Manager has already been configured System Manager.

Next, scroll down to the **Monitoring** section, which determines how frequently Session Manager sends SIP Options messages to V-9972. Ensure that monitoring is enabled and 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 60 secs. If there is no response, Session Manager will send a SIP Options message every 120 secs.

AVAYA Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ Widgets ▾ Shortcuts ▾

Search 🔍 | admin

Home Routing Session Manager

Session Manager Administration

Edit Session Manager [Commit] [Cancel]

General | Security Module | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server | Logging | Expand All | Collapse All

General

SIP Entity Name: devcon-sm

Description:

*Management Access Point Host Name/IP: 10.64.102.116

*Direct Routing to Endpoints: Enable ▾

Data Center: None ▾

Avaya Aura Device Services Server Pairing: None ▾

Maintenance Mode: ☐

Security Module

SIP Entity IP Address: 10.64.102.117

*Network Mask: 255.255.255.0

*Default Gateway: 10.64.102.1

*Call Control PHB: 46

*SIP Firewall Configuration: SM 6.3.8.0 ▾

Monitoring

Enable SIP Monitoring: ☒

*Proactive cycle time (secs): 60

*Reactive cycle time (secs): 120

*Number of Tries: 1

*Number of Successes: 1

6.7. Install Valcom V-9972 Universal Paging Interface TLS Certificate

To support mutual TLS authentication, the V-9972 TLS certificate must be installed on Session Manager. From System Manager Web interface, navigate to **Services → Inventory → Manage Elements** and select checkbox for the Session Manager. From the **More Actions** drop-down box, select **Manage Trusted Certificate** (not shown). In **Manage Trusted Certificates**, click **Add**. In Add Trusted Certificate, select *SECURITY_MODULE_SIP* in the **Select Store Type to add trusted certificate** field. Click the **Import from file** radio button and select the certificate file (e.g., *technicalsupportca.crt*). Next, click on **Retrieve Certificate** and then **Commit**.

AVAYA
Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ Widgets ▾ Shortcuts ▾ Search 🔍 admin

Home Inventory

Inventory ▾
Manage Elements
Create Profiles and Disc...
Element Type Access
Subnet Configuration
Manage Serviceabilit... ▾
Synchronization ▾
Connection Pooling ▾

Manage Elements Discovery

Add Trusted Certificate [Help ?](#) [Commit](#) [Cancel](#)

Select Store Type to add trusted certificate: **SECURITY_MODULE_SIP** ▾

☒ Import from file
☐ Import as PEM certificate
☐ Import from existing certificates
☐ Import using TLS

* Please select a file [Choose File](#) No file chosen

You must click the Retrieve certificate button and review the certificate details before you can continue. [Retrieve Certificate](#)

Certificate Details

Subject Details	CN=TechSupportCA	
Valid From	Tue Jan 05 16:59:41 EST 2021	Valid To Fri Jan 03 16:59:41 EST 2031
Key Size	2048	
Issuer Name	CN=TechSupportCA	
Certificate Fingerprint	7d5c7721a43df335d5b32df9fc66640c50209ddc6a8333f	
CA Certificate	Yes	
Serial Number:	E7C727BDF565B57E	
Basic Constraints:	CA Certificate	
Key Usage Extension:	Key Cert Sign, CRL Sign	

After the certificate has been imported, it should be listed in **Manage Trusted Certificates** as shown below.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The left sidebar contains navigation options: Home, Inventory, Manage Elements, Create Profiles and Disc..., Element Type Access, Subnet Configuration, Manage Serviceabilit..., Synchronization, and Connection Pooling. The main content area is titled 'Manage Trusted Certificates' and contains a table with 13 items. The table has columns for 'Store Description', 'Store Type', and 'Subject Name'. The row for 'Used for validating TLS server identity certificates' with 'Store Type' 'SYSLOG' and 'Subject Name' 'O=AVAYA, OU=MGMT, CN=System Manager CA' is highlighted with a red box.

Store Description	Store Type	Subject Name
<input type="checkbox"/> Used for validating TLS client identity certificates	SECURITY_MODULE_HTTP	CN=devcon-epm.avaya.com, OU=EPM CA 1620852383797, O=Avaya
<input type="checkbox"/> Used for validating TLS client identity certificates	SECURITY_MODULE_HTTP	O=AVAYA, OU=MGMT, CN=System Manager CA
<input type="checkbox"/> Used for validating TLS client identity certificates	SAL_AGENT	O=AVAYA, OU=MGMT, CN=System Manager CA
<input type="checkbox"/> Used for validating TLS client identity certificates	POSTGRES	O=AVAYA, OU=MGMT, CN=System Manager CA
<input type="checkbox"/> Used for validating TLS client identity certificates	WEBSPPHERE	O=AVAYA, OU=MGMT, CN=System Manager CA
<input type="checkbox"/> Used for validating TLS server identity certificates	SYSLOG	O=AVAYA, OU=MGMT, CN=System Manager CA
<input type="checkbox"/> Used for validating TLS client identity certificates	SECURITY_MODULE_SIP	CN=TechSupportCA
<input type="checkbox"/> Used for validating TLS client identity certificates	SECURITY_MODULE_SIP	C=US, O=AVAYA, OU=SDP, CN=devcon-ixm
<input type="checkbox"/> Used for validating TLS client identity certificates	SECURITY_MODULE_SIP	CN=Avaya Product Root CA, OU=Avaya Product PKI, O=Avaya Inc., C=US
<input type="checkbox"/> Used for validating TLS client identity certificates	SECURITY_MODULE_SIP	CN=Avaya Call Server, OU=Media Server, O=Avaya Inc., C=US
<input type="checkbox"/> Used for validating TLS client identity certificates	SECURITY_MODULE_SIP	O=AVAYA, OU=MGMT, CN=System Manager CA
<input type="checkbox"/> Used for validating TLS client identity certificates	SECURITY_MODULE_SIP	C=US, O=AVAYA, OU=SDP, CN=devcon-ixm
<input type="checkbox"/> Used for validating TLS client identity certificates	MGMT_JBOSS	O=AVAYA, OU=MGMT, CN=System Manager CA

7. Configure Valcom V-9972 Universal Paging Interface

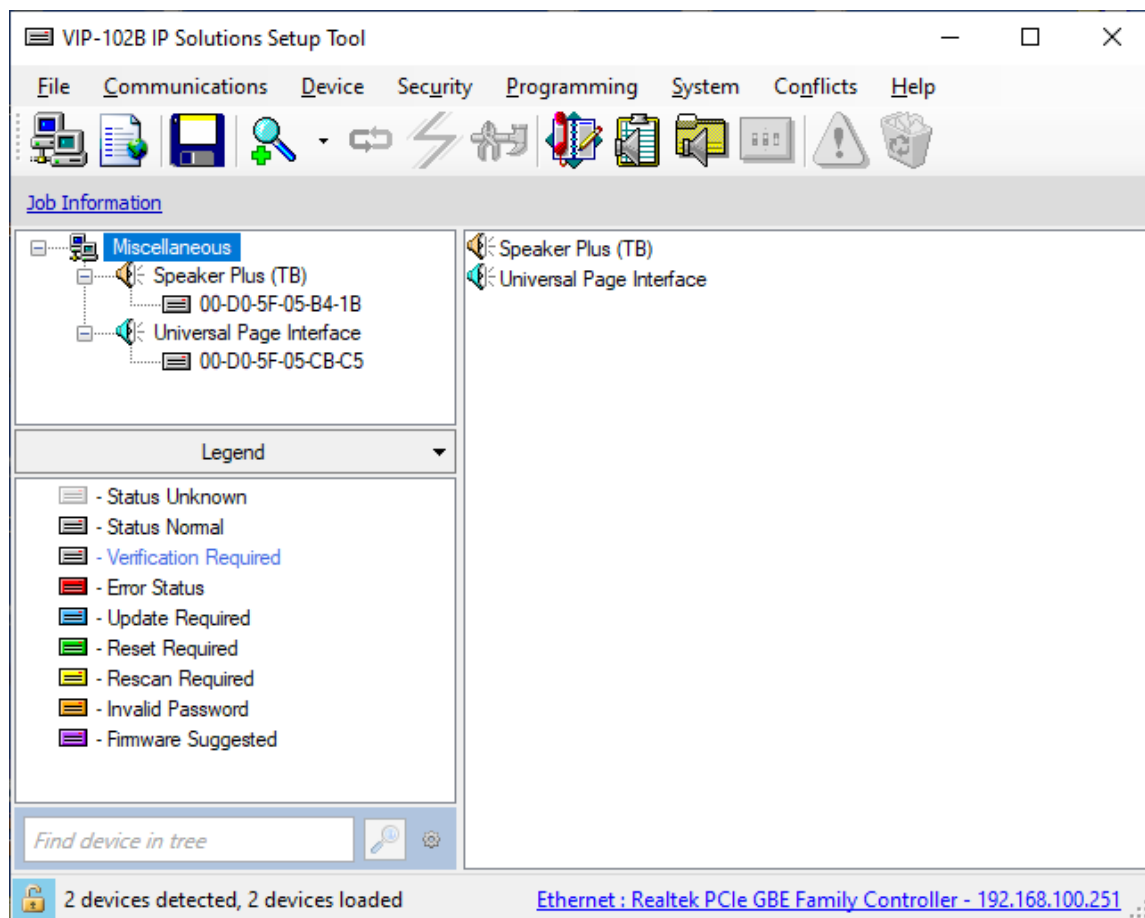
This section covers the configuration of Valcom V-9972 Universal Paging Interface using the Valcom VIP-102B IP Solutions Setup Tool. The configuration covers the following areas:

- Launch the Valcom VIP-102B IP Solutions Setup Tool
- Configure the Network Settings
- Configure Time
- Install System Manager CA TLS Certificate
- Configure SIP Parameters
- Verify Codec Settings
- Update Universal Paging Interface with the New Configuration

Note: These Application Notes do not cover the configuration of the Valcom VIP-430A IP Wall Speakers, Audio Groups, or the assignment of Dial Codes to Valcom speakers. Refer to [5] and [6] for details.

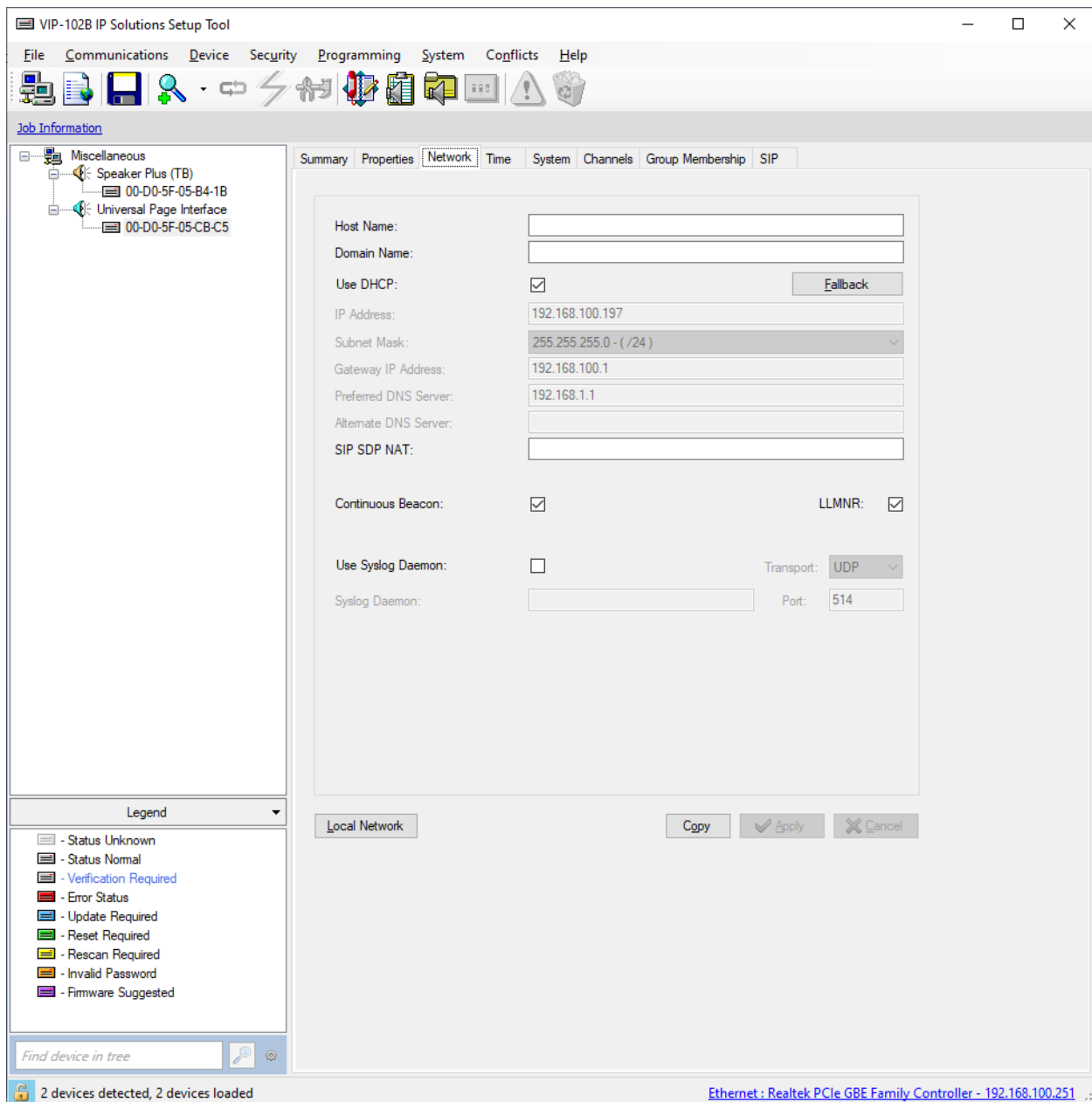
7.1. Launch Valcom VIP-102B IP Solutions Setup Tool

Launch the **VIP-102B IP Solutions Setup Tool** and follow the prompts. The main window is displayed as shown below.



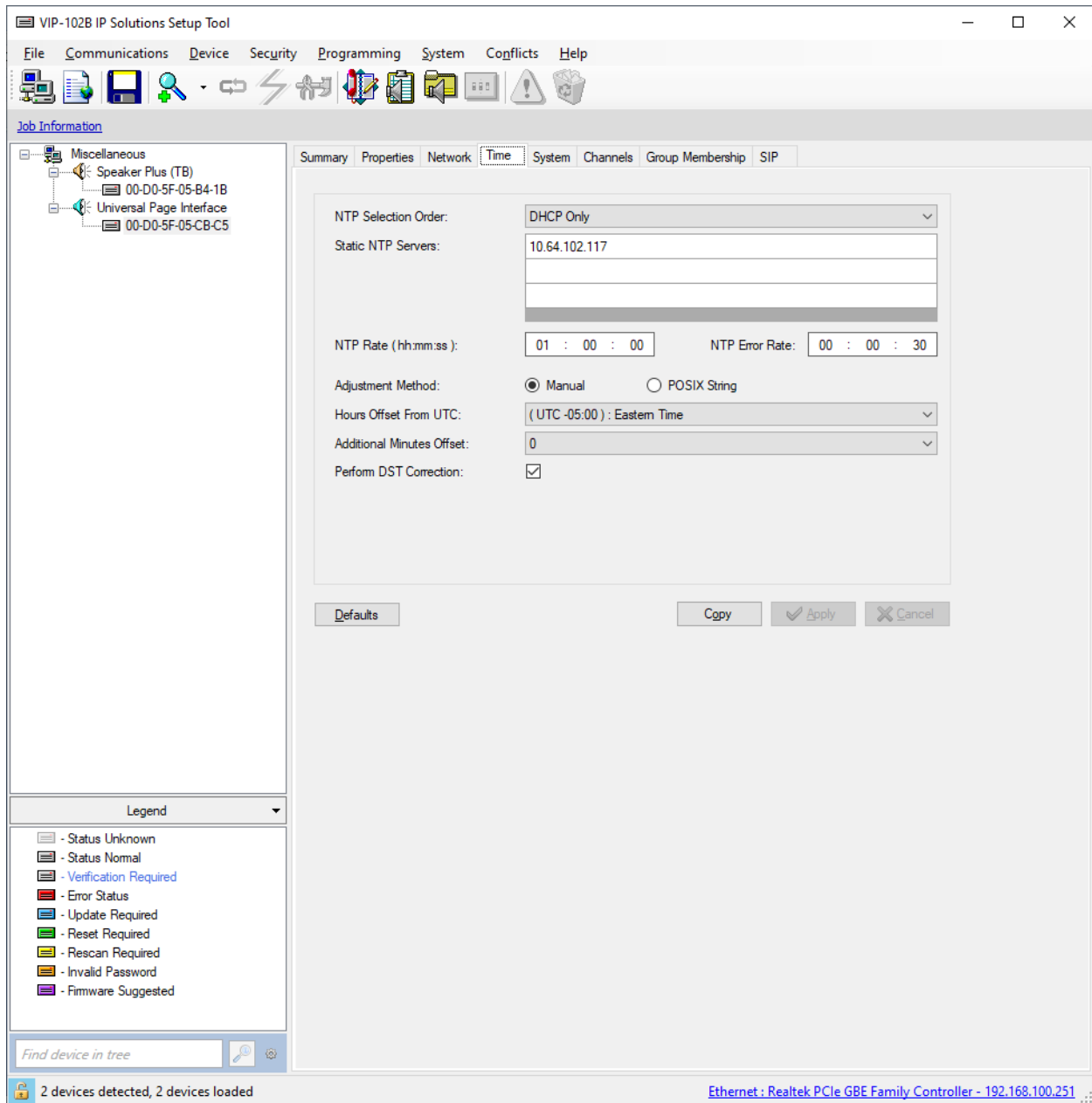
7.2. Configure the Network Settings

Click the MAC/hardware address under Universal Page Interface in the left pane and select the **Network** tab. V-9972 must first acquire IP network settings before proceeding with provisioning. These network settings were automatically obtained from a DHCP server as shown below. Alternatively, V-9972 could be configured with static IP addresses, but for the compliance test, DHCP was used.



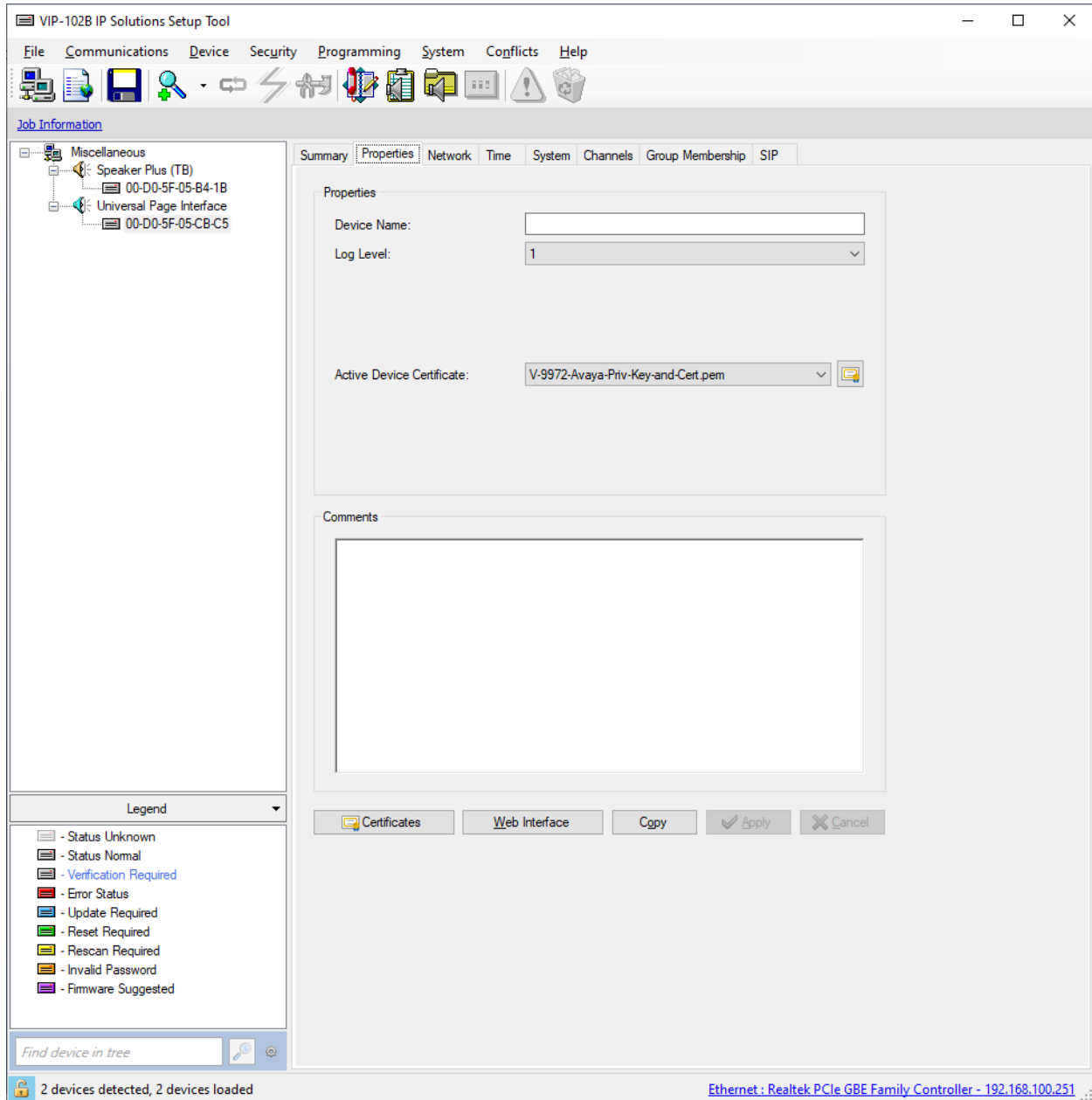
7.3. Configure the Time

Navigate to the **Time** tab and set the Static NTP Servers to ensure the proper date/time on the device.

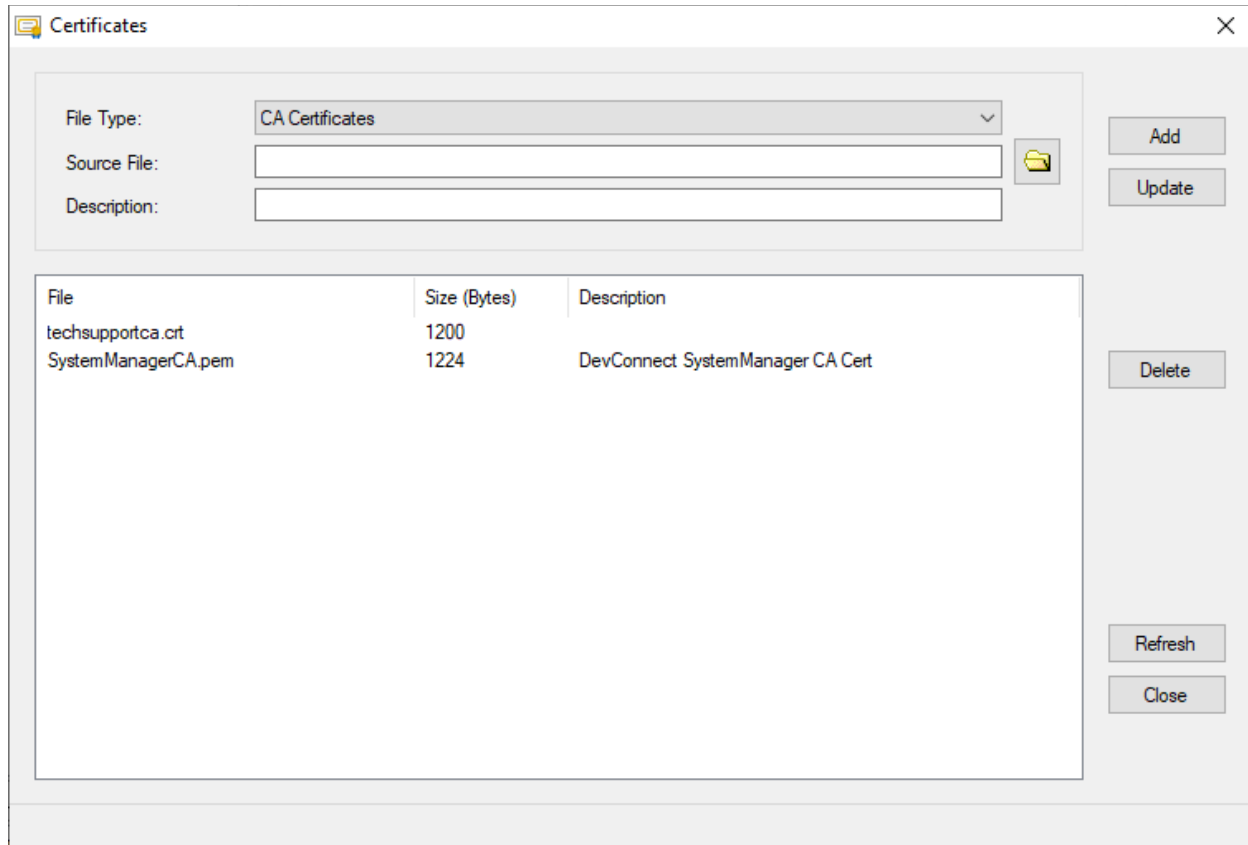


7.4. Install the System Manager CA TLS Certificate

Navigate to the **Properties** tab to install the System Manager CA certificate. Note that the V-9972 has a device certificate (*V-9972-Avaya-Priv-Key-and-Cert.pem*) signed by a different CA other than the System Manager. Click on **Certificates**.



In the **Certificate** dialog box, add the System Manager CA TLS certificate. Note that the certificate has already been imported as shown below. In addition, the V-9972 root certificate (*techsupportca.crt*) is also installed. This certificate must be installed on Session Manager to support mutual TLS authentication.



7.5. Configure SIP Parameters

From the **VIP-102B IP Solutions Setup Tool**, navigate to the **SIP** tab of the Universal Page Interface and configure the parameters as follows.

- **Transport:** Set to *Accept: TLS, Originate: TLS*.
- **Phone Number:** Set to number that will be routed to V-9972 (e.g., 78570).
- **Description:** Provide optional description.
- **Authentication Name:** Leave blank.
- **Secret:** Leave blank.
- **Realm:** Set to SIP domain (e.g., *avaya.com*).
- **Validate Remote Certificate:** Enable this option so that V-9972 validates the remote TLS certificate installed in **Section 7.4**.
- **Primary Server:** Set to Session Manager IP address (i.e., *10.64.102.117*).
- **Port:** Set to TLS port (e.g., *5061*).
- **Register:** Disable this option.
- **Max Calls:** Specify maximum number of calls (e.g., *4*). For example, V-9972 could establish an intercom call to the IP speaker and then a higher priority paging call to the same IP speaker. In addition, V-9972 could establish up to four calls to four different IP speakers (not tested).
- **SRTP:** Enable SRTP and then select *Media Encryption Mandatory*.
- **Auto Destination:** Set to the number that should be dialed when the call button on the VIP-430A IP Wall Speaker is pressed.

Accept the values in the remaining fields and click **Apply**.

VIP-102B IP Solutions Setup Tool

File Communications Device Security Programming System Conflicts Help

Job Information

Miscellaneous

- Speaker Plus (TB)
- 00-D0-5F-05-B4-1B
- Universal Page Interface
- 00-D0-5F-05-CB-C5

Legend

- Status Unknown
- Status Normal
- Verification Required
- Error Status
- Update Required
- Reset Required
- Rescan Required
- Invalid Password
- Firmware Suggested

Find device in tree

2 devices detected, 2 devices loaded

Summary Properties Network Time System Channels Group Membership SIP

Transport: Accept: TLS, Originate: TLS

1 2 3 4

Phone Number: 78570

Description: VIP-430A

Authentication Name:

Secret:

Realm: avaya.com Validate Remote Certificate: ☒

SIP Servers:

	Server	Port
Primary	10.64.102.117	5061
Backup 1		5061
Backup 2		5061
Backup 3		5061

Register: ☐

DNS SRV: ☐

Max Calls: 4 SRTP: ☒ Media Encryption Mandatory: ☐

Busy Message:

Call Fwd Busy (302): Ring Timeout (secs): None

Outbound Proxy: Outbound Port: 5061

Keep Alive Timer (secs): 600 Options Timer (secs): 40

SIP Port: 5061 Idle Timeout (secs): 0

RTP Port: 20000 Max Call Timer (secs): 0

Night Ring: ☐ Night Ring Group:

CID Number: 78570

CID Name: VIP-430A

Auto Destination: 78002

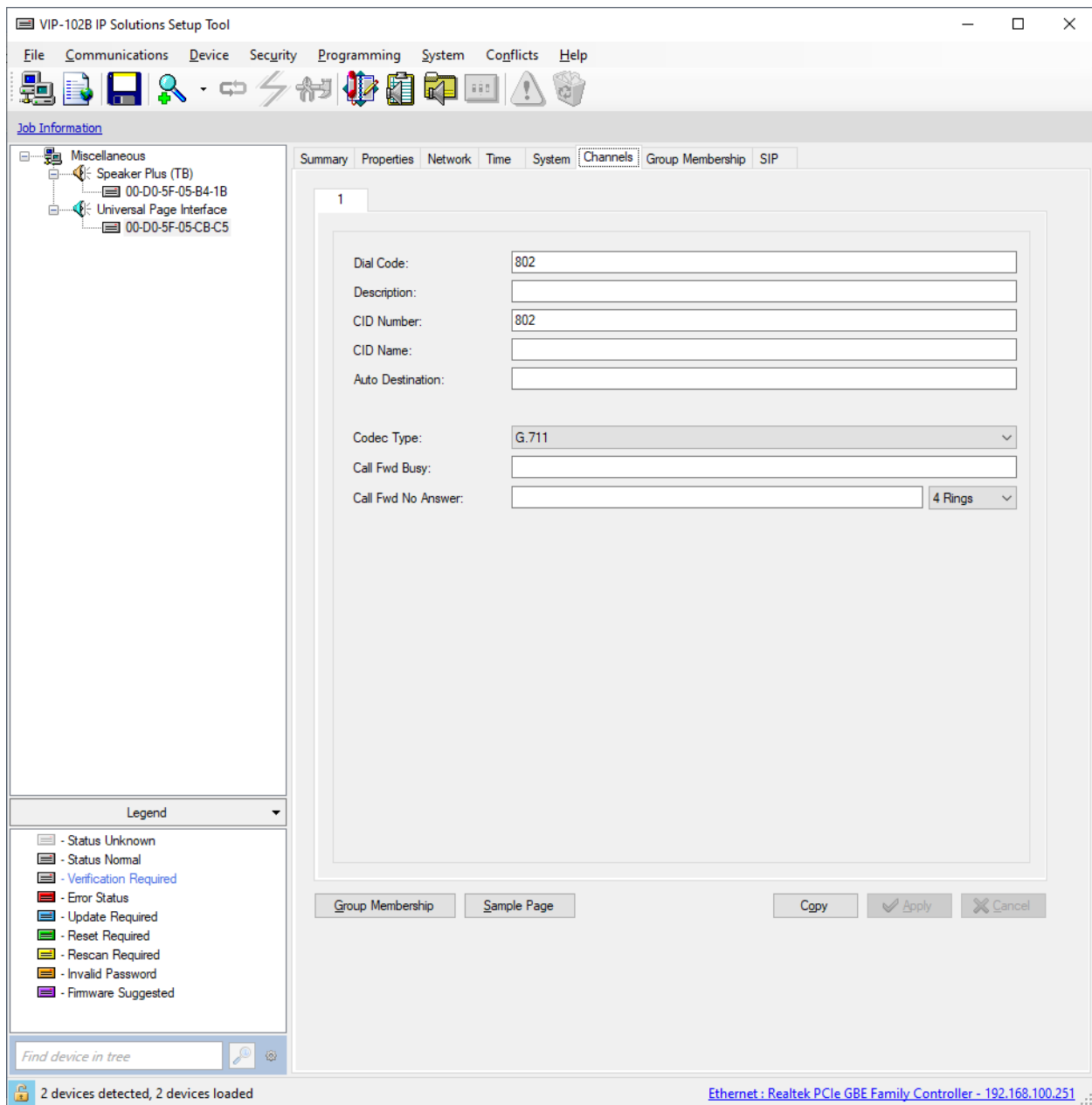
Channel Priority: Medium

Defaults Status Copy Apply Cancel

Ethernet : Realtek PCIe GBE Family Controller - 192.168.100.251

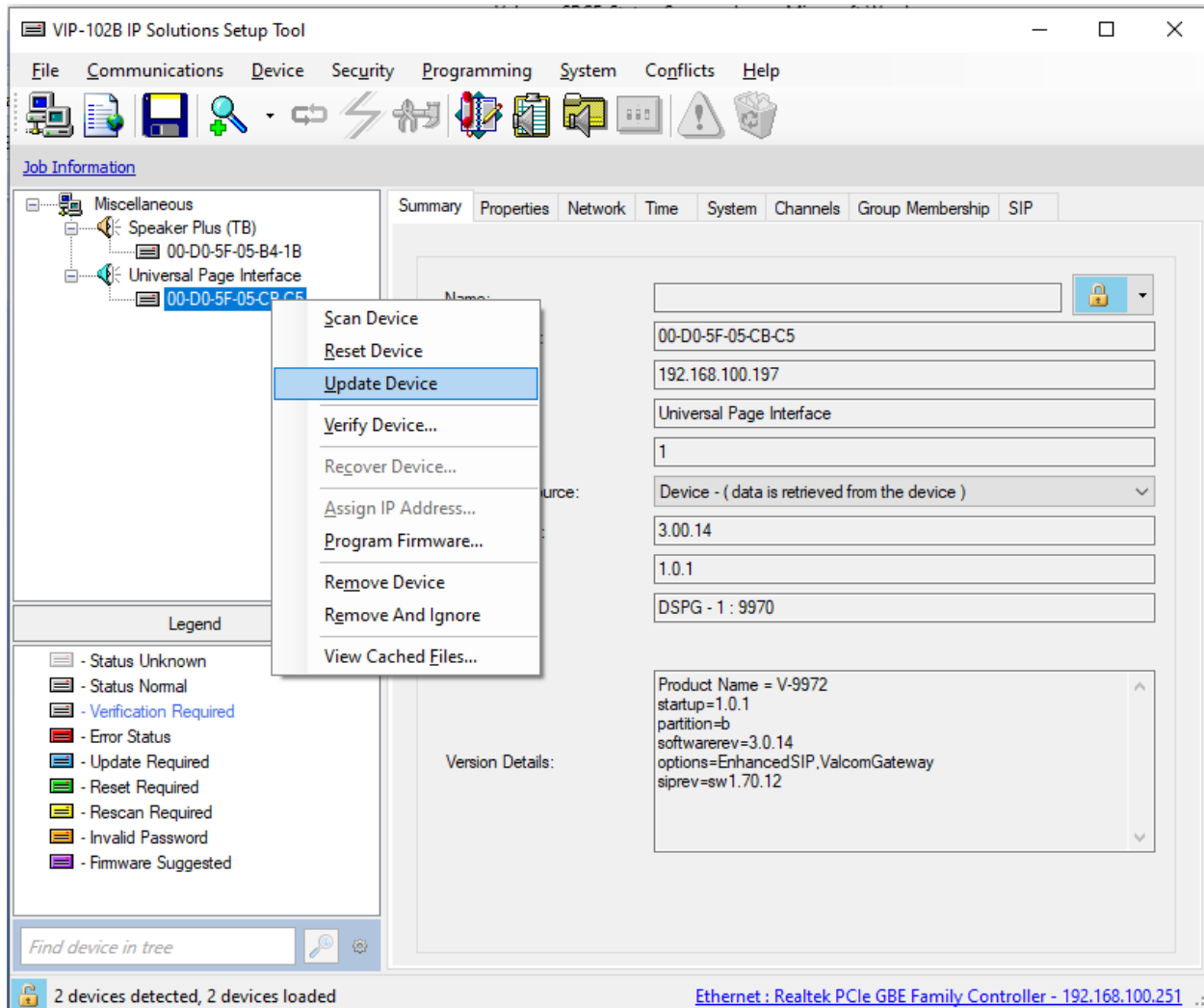
7.6. Verify Codec Settings

Navigate to the **Channels** tab shown below. The Codec Type should be set G.711, currently the only option supported with VIP-430A IP Wall Speaker.

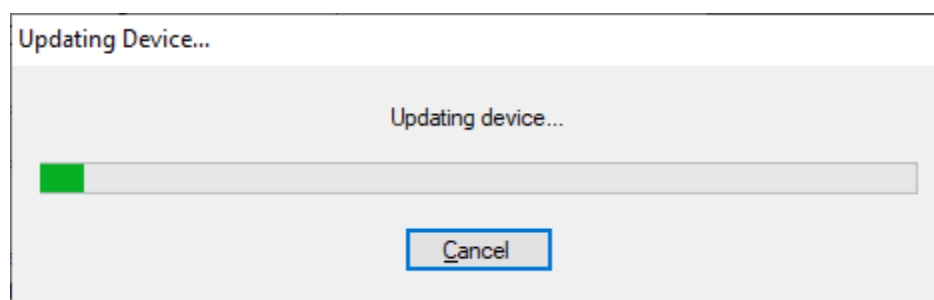


7.7. Update Universal Page Interface with the New Configuration

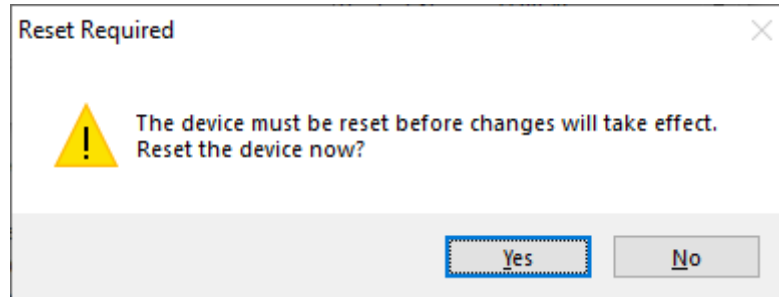
From the **VIP-102B IP Solutions Setup Tool**, right-mouse click on the MAC/hardware address of the Universal Page Interface and select **Update Device** from the pop-up menu as shown below.



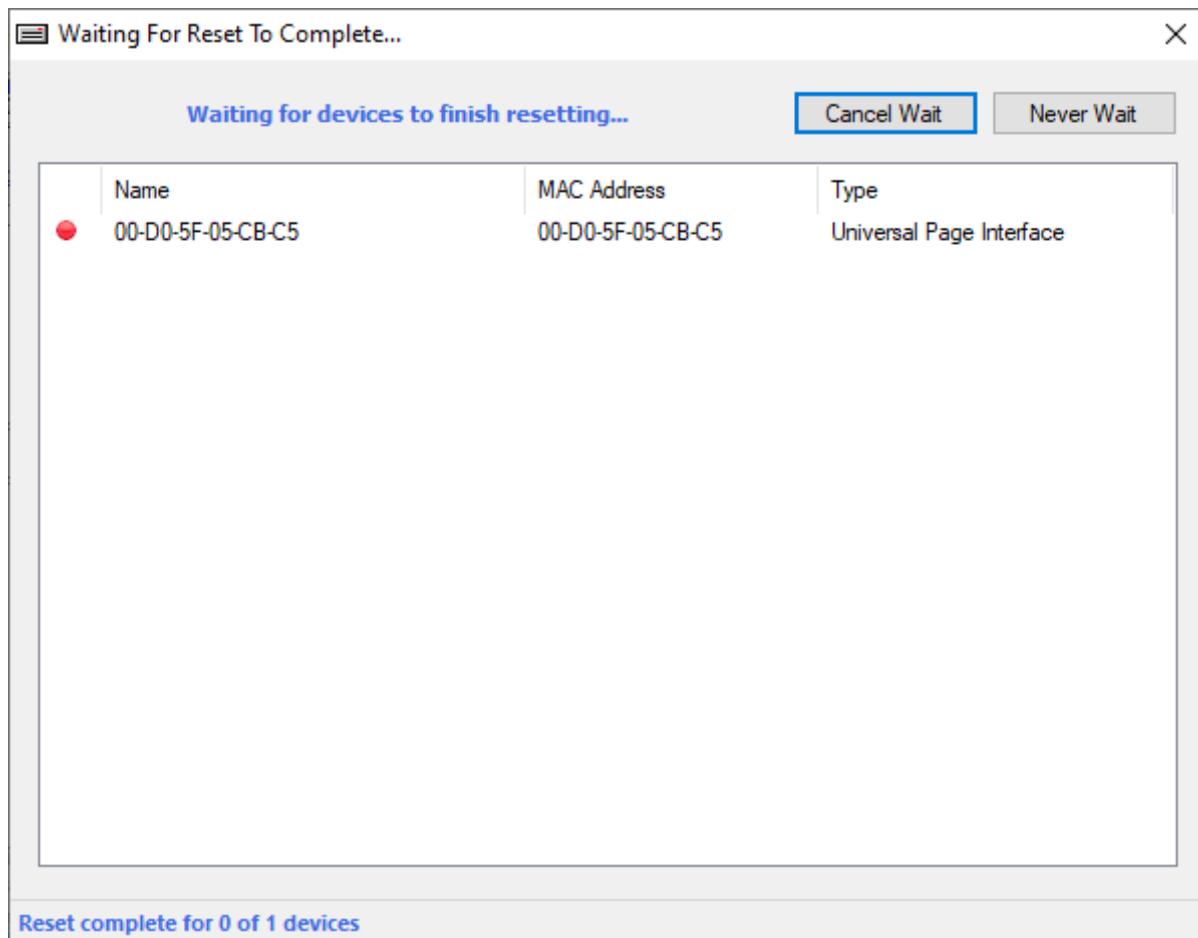
The following window is displayed indicating that the device is being updated.



A device reset is required so respond with **Yes** when prompted.



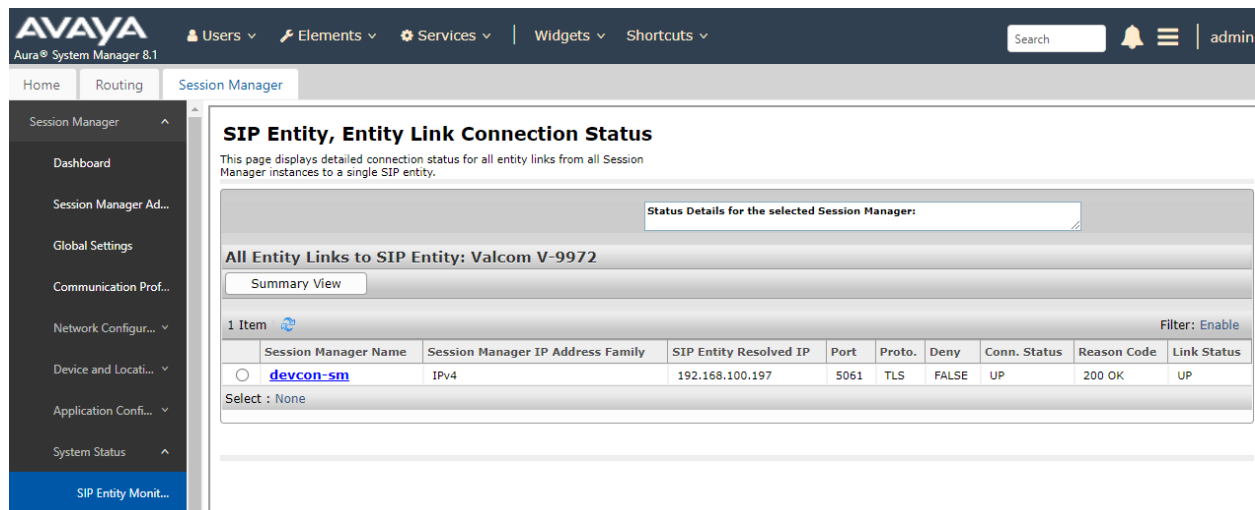
The following window will be displayed while the device is being reset. When the reset is completed, the window will disappear.



8. Verification Steps

This section provides the tests that may be performed to verify proper configuration of Valcom V-9972 Universal Paging Interface with Avaya Aura® Session Manager, Avaya Aura® Communication Manager.

1. Verify that the SIP trunk between V-9972 and Session Manager has been established successfully. In System Manager, navigate to **Elements → Session Manager → System Status → SIP Entity Monitoring**, and then click on the Valcom V-9972 SIP entity (not shown) to check the Entity Link connection status.



The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The left sidebar shows the 'Session Manager' menu with options like 'Dashboard', 'Session Manager Ad...', 'Global Settings', 'Communication Prof...', 'Network Configur...', 'Device and Locati...', 'Application Confi...', 'System Status', and 'SIP Entity Monit...'. The main content area is titled 'SIP Entity, Entity Link Connection Status' and includes a sub-header 'All Entity Links to SIP Entity: Valcom V-9972'. Below this, there is a 'Summary View' button and a table with one item. The table has columns for Session Manager Name, Session Manager IP Address Family, SIP Entity Resolved IP, Port, Proto, Deny, Conn. Status, Reason Code, and Link Status. The single row shows 'devcon-sm' with IP address 192.168.100.197, port 5061, TLS protocol, and a status of 'UP'.

Session Manager Name	Session Manager IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
devcon-sm	IPv4	192.168.100.197	5061	TLS	FALSE	UP	200 OK	UP

2. Place a call to the V-9972 and at the dial tone, enter the dial code for the IP speaker to establish an intercom call from an Avaya IP deskphone to a Valcom speaker. Verify two-way audio. Terminate the call from the Avaya IP deskphone or by pressing the call button on the IP speaker.
3. Place a call to the V-9972 and at the dial tone, enter the dial code a group page code to establish a one-way paging call from an Avaya IP deskphone to IP speaker(s). Verify one-way audio. Terminate the call from the Avaya IP deskphone.
4. Place an intercom call by pressing the call button on the IP speaker. Verify two-way audio to the call destination. Terminate the call.

9. Conclusion

These Application Notes described the configuration steps required to integrate Valcom V-9972 Universal Paging Interface with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Intercom and group paging calls were established with Valcom V-9972 Universal Paging Interface, Valcom VIP-430A IP Wall Speakers, Avaya H.323 / SIP Deskphones, and the PSTN. All feature and serviceability test cases were completed successfully.

10. References

This section references the Avaya and Valcom documentation relevant to these Application Notes.

- [1] *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 12, July 2021, available at <http://support.avaya.com>.
- [2] *Administering Avaya Aura® System Manager for Release 8.1.x*, Release 8.1.x, Issue 19, April 2022, available at <http://support.avaya.com>.
- [3] *Administering Avaya Aura® Session Manager*, Release 8.1.x, Issue 11, March 2022, available at <http://support.avaya.com>.
- [4] *Administering Avaya Session Border Controller for Enterprise*, Release 8.1.x, Issue 5, August 2021, available at <http://support.avaya.com>.
- [5] *Valcom VIP-102B IP Solutions Setup Tool Version 8.4.0.0 Reference Manual*, Revision 17 – 3/16/22, available at <https://www.valcom.com/resources/documents-manuals>.
- [6] *Valcom V-9972 Universal Page Interface Configuration Guide*, Rev. 3.1, available at <https://www.valcom.com/resources/documents-manuals>.

©2022 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.



Declaration of Conformance

May 20, 2022

Jeff Gartner
Senior Manager
DevConnect Program
Avaya

Dear Jeff Gartner:

We, Valcom Inc, declare under sole responsibility that product series named Universal Paging Adapter, including product models V-9972, V-9972-2 or VRCPA share the same hardware circuitry, software, SIP stack and firmware version. Therefore, the products are expected to behave in the same manner. The differences between the different models in each series are generally cosmetic in nature, such as enclosure shape or color, mounting arrangement, etc.

Sincerely,

/s/ David Ellison

David Ellison
Technical Support Manager
Valcom Inc
dellison@valcom.com