



Application Notes for Valcom V-9972 Universal Paging Interface with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using SIP Endpoint - 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 registered with Avaya Aura® Session Manager as a SIP endpoint. In addition, Valcom V-9972 Universal Paging Interface also registered with Avaya Aura® Session Manager through Avaya Session Border Controller for Enterprise as a remote worker. 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 registered with Avaya Aura® Session Manager as a SIP endpoint. In addition, Valcom V-9972 Universal Paging Interface also registered with Avaya Aura® Session Manager through Avaya Session Border Controller for Enterprise as a remote worker. 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 placed to the Valcom V-9972 Universal Paging Interface using its direct dial SIP extension, 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:

- SIP registration of V-9972 directly with Session Manager as a SIP endpoint.
- SIP registration of V-9972 with Session Manager through Avaya Session Border Controller for Enterprise as a remote worker.
- 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, including the V-9972.
- Avaya Aura® System Manager used to configure Session Manager.
- Avaya Session Border Controller for Enterprise to provide connectivity to a simulated SIP service provider or to register the V-9972 as a remote worker.
- Avaya 96x1 Series H.323 and SIP Deskphones.
- Valcom V-9972 Universal Paging Interface and Valcom VIP-430A IP Wall Speaker.

V-9972 Universal Paging Interface registered with Session Manager as a SIP endpoint and was configured as Off-PBX Stations (OPS) on Communication Manager.

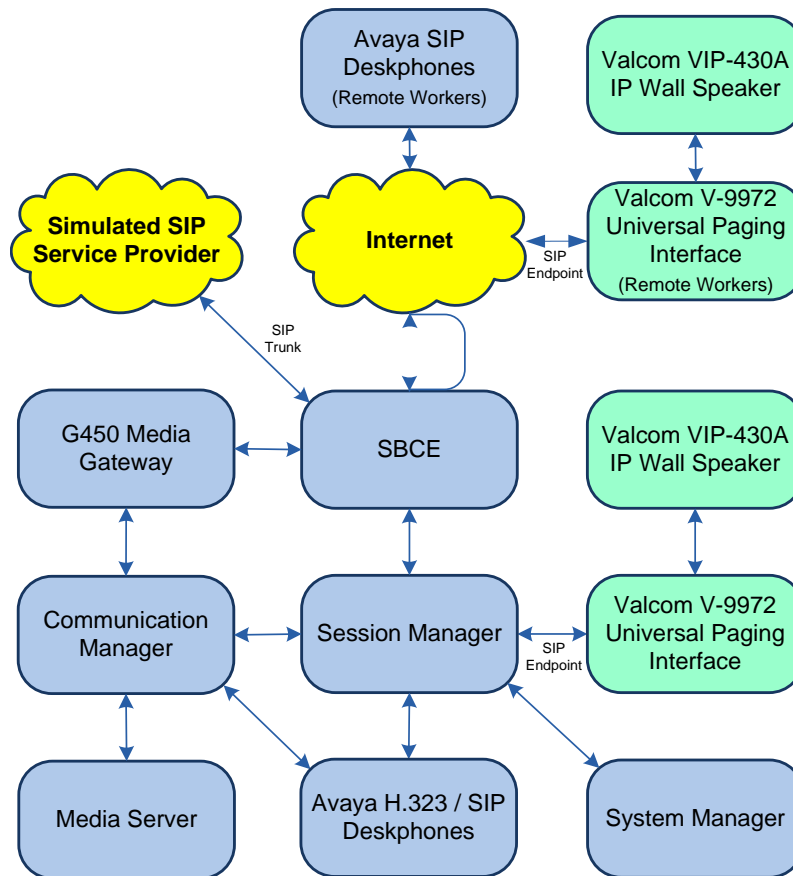


Figure 1: Avaya SIP Network with Valcom V-9972 Universal Paging Interface and Valcom VIP-430A IP Wall Speakers

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:

- Verify Communication Manager license
- 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.

Note: The SIP station configuration for Valcom V-9972 Universal Paging Interface is configured through Avaya Aura® System Manager in **Section 6.3**.

5.1. Verify Communication Manager 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: V18                                     Software Package: Enterprise
Location: 2                                         System ID (SID): 1
Platform: 28                                       Module ID (MID): 1

                                USED
Platform Maximum Ports: 48000 131
Maximum Stations: 36000 37
Maximum XMOBILE Stations: 36000 0
Maximum Off-PBX Telephones - EC500: 41000 0
Maximum Off-PBX Telephones - OPS: 41000 23
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*). 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
```


5.3. Administer IP Network Region

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is *avaya.com*. By default, **IP-IP Direct Audio** (shuffling) is enabled to allow audio RTP traffic to be sent directly between IP endpoints or between Communication Manager and SBCE for remote workers without using media resources in Avaya Aura® Media Servers after the call is established. Note that for remote workers, media is anchored at the SBCE so remote workers will always send/receive audio to/from the SBCE, not directly between each other. 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    Intra-region IP-IP Direct Audio: yes
                   Codec Set: 1           Inter-region IP-IP Direct Audio: yes
                   UDP Port Min: 2048      IP Audio Hairpinning? n
                   UDP Port Max: 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
H.323 IP ENDPOINTS  AUDIO RESOURCE RESERVATION PARAMETERS
                   RSVP Enabled? n
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5
```

5.4. Administer 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                                     Page 1 of 2

                                IP MEDIA PARAMETERS

Codec Set: 1

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

Media Encryption                                Encrypted SRTCP: best-effort
1: 1-srtp-aescm128-hmac80
2: 2-srtp-aescm128-hmac32
3:
4:
5:
```

5.5. 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:

- 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        Clustering? 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/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

```

5.6. 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 String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Reqd
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 Mrk	Hop Lmt	Toll List	No. Del	Inserted Digits	DCS/ QSIG Intw	IXC
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			unk-unk	none
2:	y	y	y	y	y	n	n				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
- Set Network Transport Protocol
- Administer SIP User
- 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 a SIP user for Valcom V-9972 Universal Paging Interface.

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. Set Network Transport Protocol

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 8.1 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The left sidebar shows the 'Routing' menu with 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and contains the following configuration fields:

- Name:** devcon-sm
- IP Address:** 10.64.102.117
- SIP FQDN:** (empty)
- Type:** Session Manager
- Notes:** (empty)
- Location:** Thornton
- Outbound Proxy:** (empty)
- Time Zone:** America/New_York
- Minimum TLS Version:** Use Global Setting
- Credential name:** (empty)
- 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 V-9972 is specified in the list below. For the compliance test, the solution used TLS network transport.

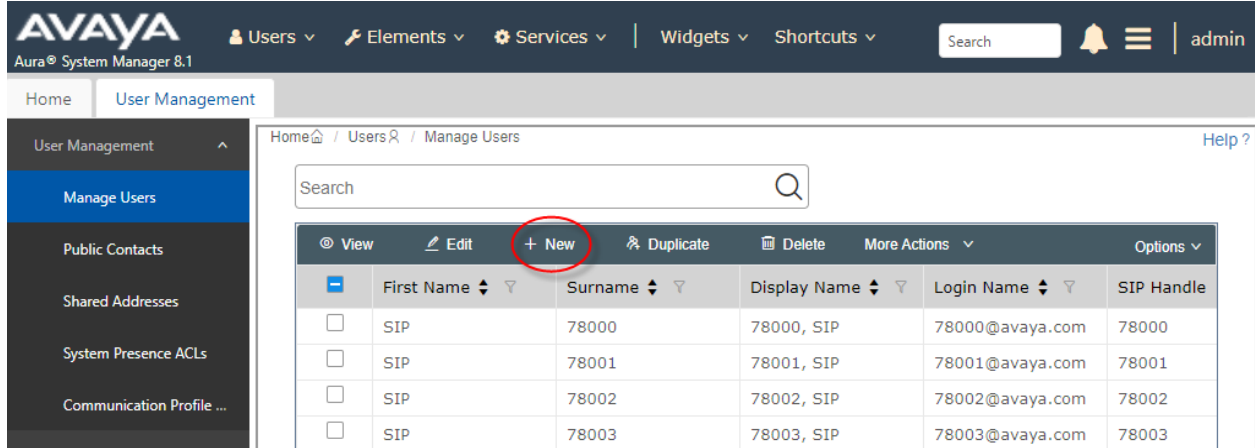
Listen Ports

<input type="checkbox"/>	Listen Ports	Protocol	Default Domain	Endpoint	Notes
<input type="checkbox"/>	5060	TCP	avaya.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	5060	UDP	avaya.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	5061	TLS	avaya.com	<input checked="" type="checkbox"/>	

Select : All, None

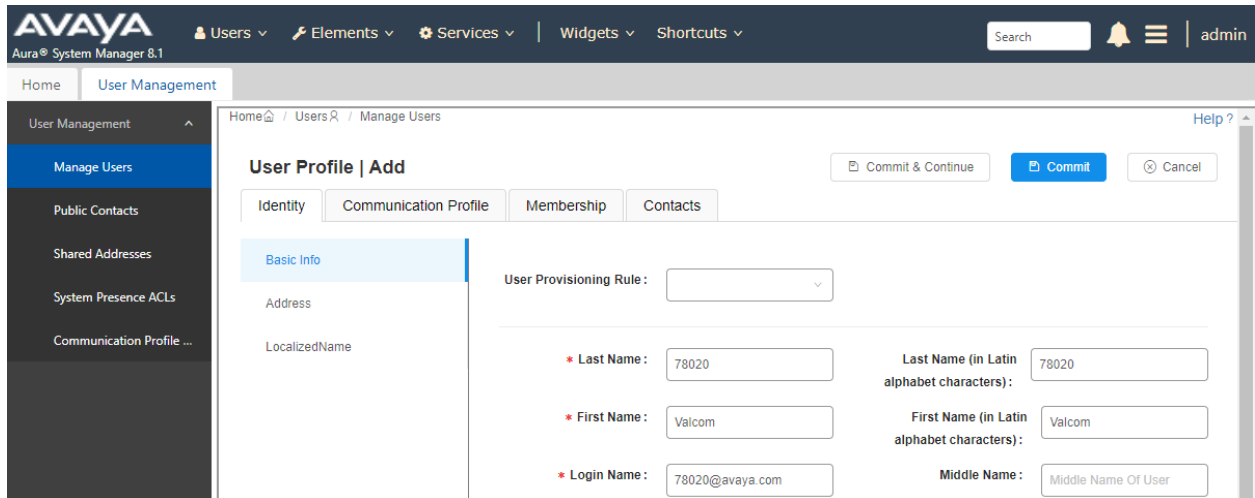
6.3. Administer SIP User

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



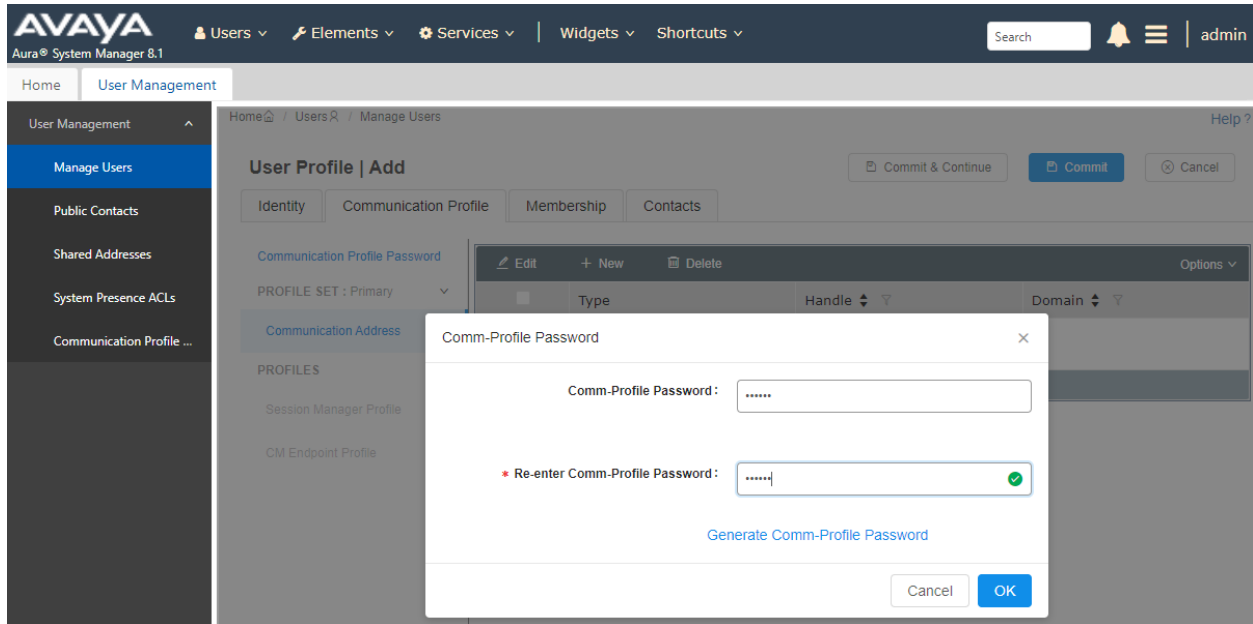
6.3.1. Identity

The **New User Profile** screen is displayed. Enter desired **Last Name** and **First Name**. For **Login Name**, enter “<ext>@<domain>”, where “<ext>” is the desired V-9972 SIP extension and “<domain>” is the applicable SIP domain name from **Section 5.3**. Retain the default values in the remaining fields.



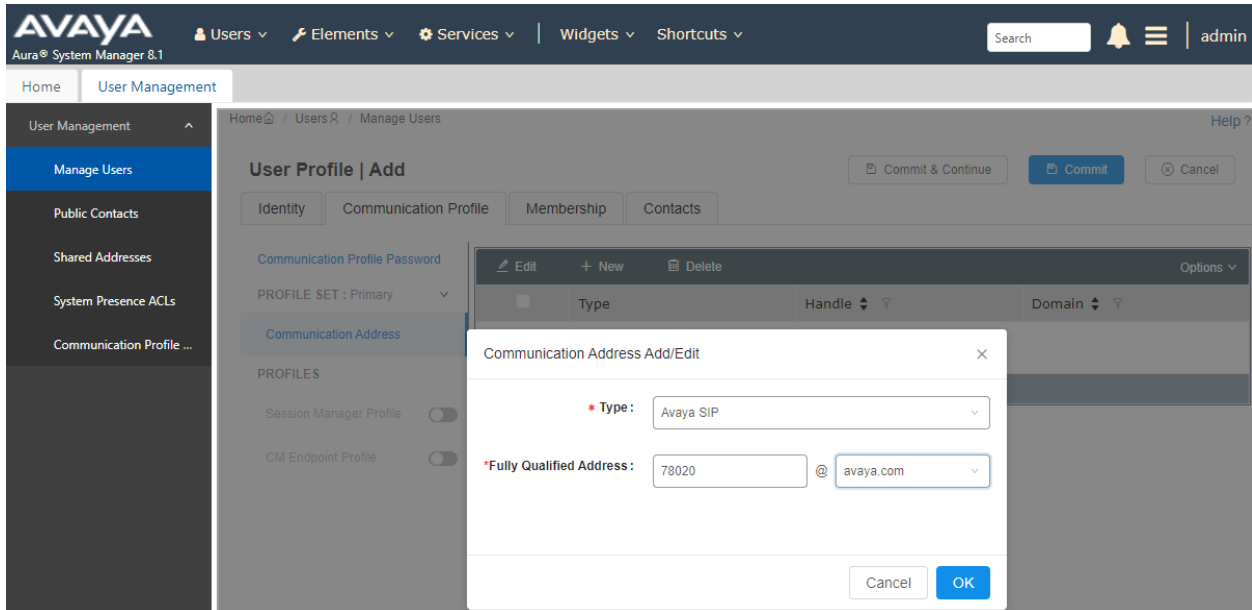
6.3.2. Communication Profile

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**.



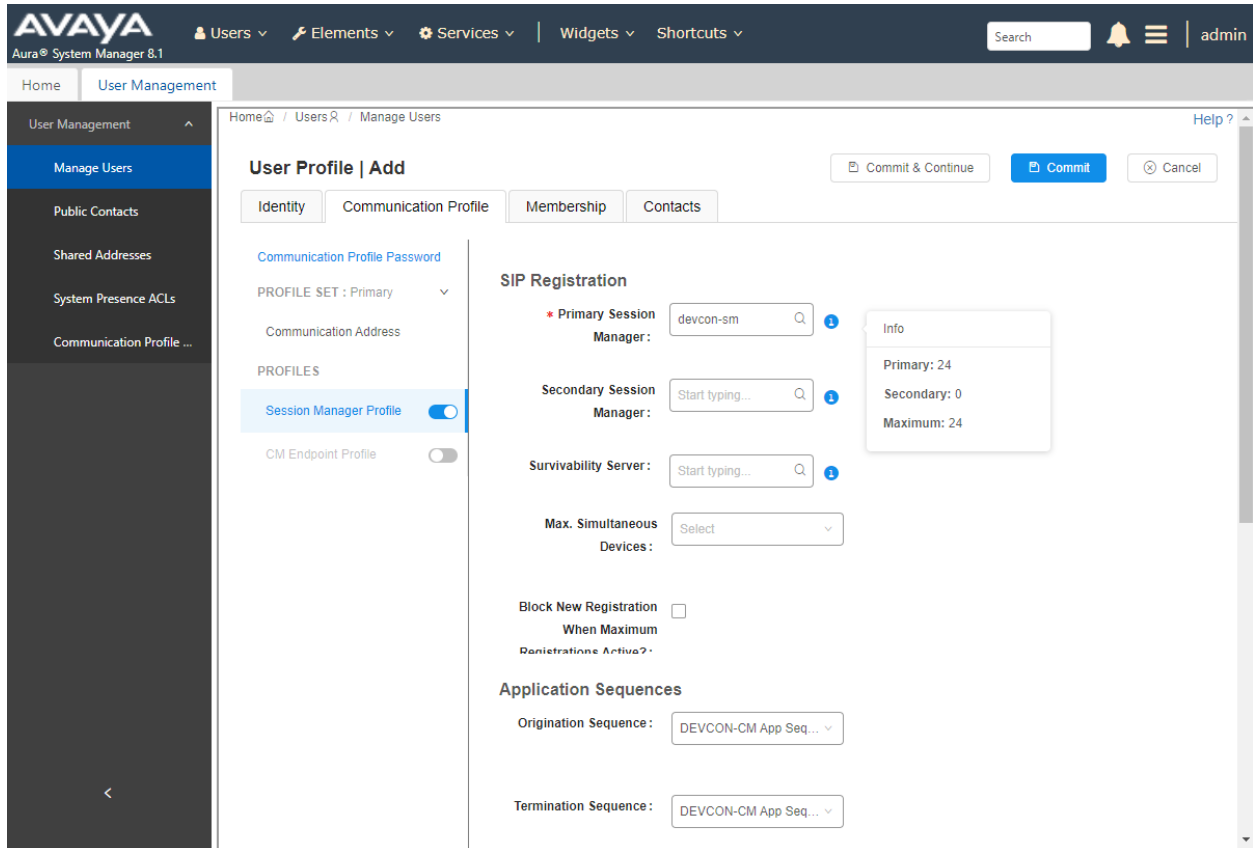
6.3.3. Communication Address

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**, select *Avaya SIP*. For **Fully Qualified Address**, enter the SIP user extension and select the domain name to match the login name from **Section 6.3.1**. Click **OK**.

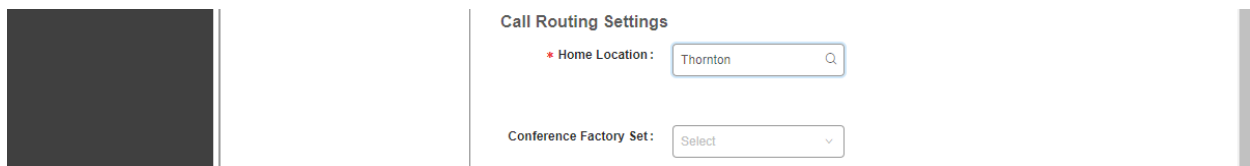


6.3.4. Session Manager Profile

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.



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



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 6.3.1**. For **Template**, select *9641SIP_DEFAULT_CM_8_1*. For **Port**, click and select *IP*. Retain the default values in the remaining fields.

The screenshot displays the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.1', and various menu items like 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. A search bar and user profile 'admin' are also visible. The main content area is titled 'User Profile | Add' and is divided into four tabs: 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. The 'Communication Profile' tab is active. On the left, a sidebar shows 'User Management' with 'Manage Users' selected. The 'Communication Profile' section includes a 'Communication Profile Password' field, 'PROFILE SET : Primary', and 'Communication Address'. Below this, the 'PROFILES' section has two toggle switches: 'Session Manager Profile' (off) and 'CM Endpoint Profile' (on). The main form area contains several fields: 'System' (devcon-cm), 'Profile Type' (Endpoint), 'Extension' (78020), 'Set Type' (9641SIP), 'Template' (9641SIP_DEFAULT_CM_8_1), 'Port' (IP), 'Security Code' (Enter Security Code), 'Voice Mail Number', 'Preferred Handle' (Select), 'Calculate Route Pattern' (off), 'Sip Trunk' (aar), 'SIP URI' (Select), 'Delete on Unassign from User or on Delete User' (checked), and 'Override Endpoint Name and Localized Name' (checked). Buttons for 'Commit & Continue', 'Commit', and 'Cancel' are at the top right.

6.4. 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**.

The screenshot displays the Avaya System Manager 8.1 web interface. The top navigation bar includes the AVAYA logo, 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts' menus, a search bar, and a user profile 'admin'. The left sidebar shows 'Inventory' and 'Manage Elements' options. The main content area has 'Manage Elements' and 'Discovery' tabs, and a 'Help ?' link. The 'Add Trusted Certificate' form is titled 'Add Trusted Certificate' and is part of the 'Manage Elements' section. It features a 'Select Store Type to add trusted certificate' dropdown menu set to 'SECURITY_MODULE_SIP'. Below this, there are four radio button options: 'Import from file' (selected), 'Import as PEM certificate', 'Import from existing certificates', and 'Import using TLS'. A message states '* Please select a file' with a 'Choose File' button and 'No file chosen' text. A 'Retrieve Certificate' button is visible, with a note: 'You must click the Retrieve certificate button and review the certificate details before you can continue.' Below this is a 'Certificate Details' section with various fields: '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), and '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 System Manager 8.1 interface. The main window is titled "Manage Trusted Certificates" and contains a table of 13 items. The table has three columns: "Store Description", "Store Type", and "Subject Name". One row is highlighted with a red border, indicating the certificate that was imported.

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"/>	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 Avaya Session Border Controller

These Application Notes assume that the SBCE is already configured to support remote workers. No additional configuration is required to support V-9972 as a remote worker. However, it would be instructive to show how the **Media Rules** were configured to support SRTP for calls to V-9972 as a remote worker. This media rule is assigned to an **End Point Policy Group**, which in turn is assigned to **Subscriber Flows** and **Server Flows**.

The screenshot shows the Avaya Session Border Controller configuration interface. At the top, there is a navigation bar with the following items: Device: SBCE, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. Below the navigation bar, the page title is "Session Border Controller for Enterprise" and the Avaya logo is visible on the right.

On the left side, there is a navigation menu with the following items: EMS Dashboard, Software Management, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies (Application Rules, Border Rules, **Media Rules**, Security Rules, Signaling Rules, Charging Rules, End Point Policy Groups, Session Policies), TLS Management, Network & Flows, DMZ Services, and Monitoring & Logging.

The main content area is titled "Media Rules: RTP-SRTP". It features an "Add" button and buttons for "Rename", "Clone", and "Delete". Below the title, there is a blue bar with the text "Click here to add a description." and a list of tabs: "Encryption", "Codec Prioritization", "Advanced", and "QoS".

The "Encryption" tab is active, showing the following configuration options:

Audio Encryption	
Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80 RTP
Encrypted RTCP	<input checked="" type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime	Any
Interworking	<input checked="" type="checkbox"/>
Symmetric Context Reset	<input checked="" type="checkbox"/>
Key Change in New Offer	<input type="checkbox"/>

Video Encryption	
Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime	Any
Interworking	<input checked="" type="checkbox"/>
Symmetric Context Reset	<input checked="" type="checkbox"/>
Key Change in New Offer	<input type="checkbox"/>

Miscellaneous	
Capability Negotiation	<input type="checkbox"/>

8. Configure Valcom V-9972 Universal Paging Interface

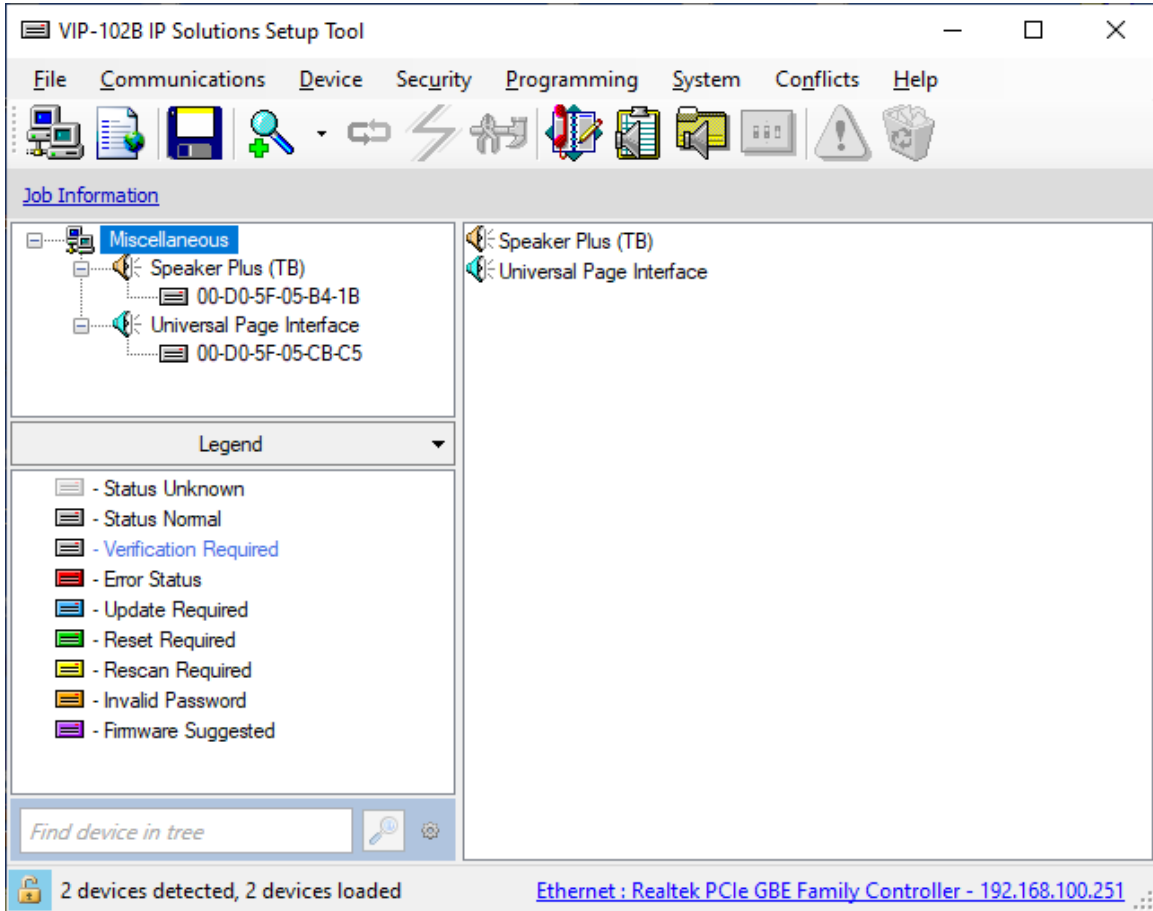
This section covers the configuration of Valcom V-9972 Universal Paging Interface using the Valcom VIP-102B IP Solutions Setup Tool. The configuration covers the following areas:

- 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.

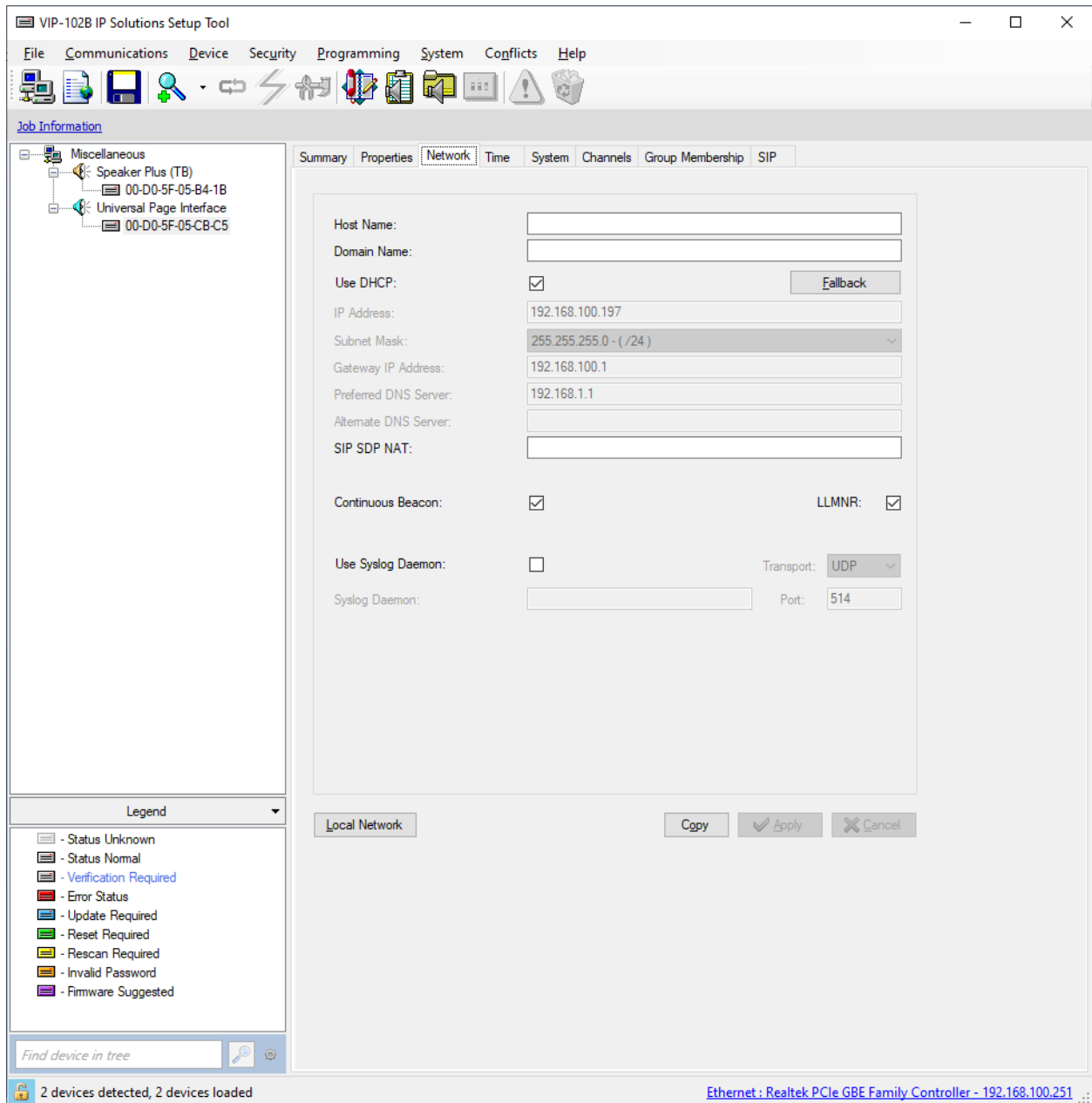
8.1. Launch Valcom VIP-102B IP Solutions Setup Tool

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



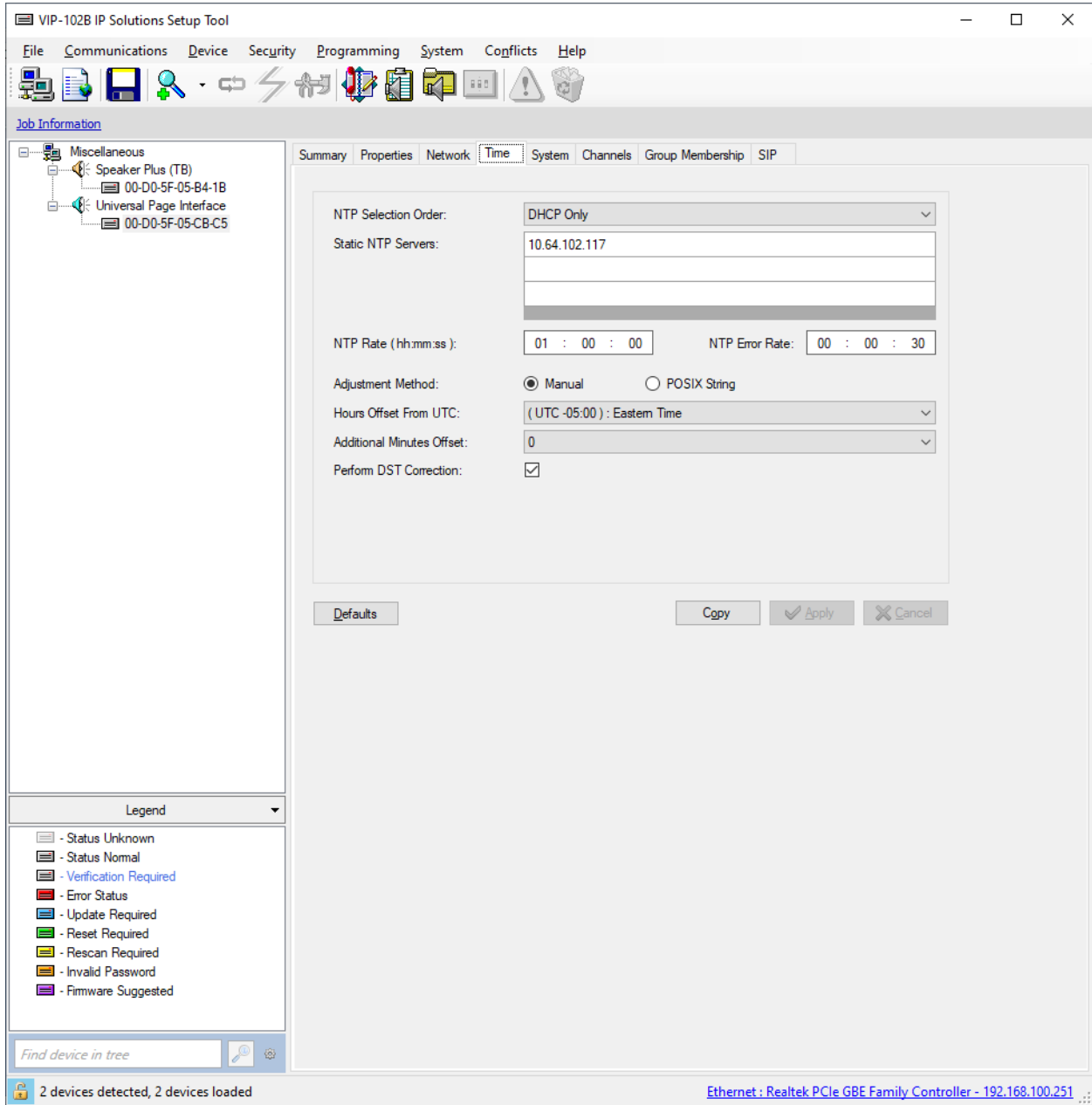
8.2. Configure the Network Settings

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.



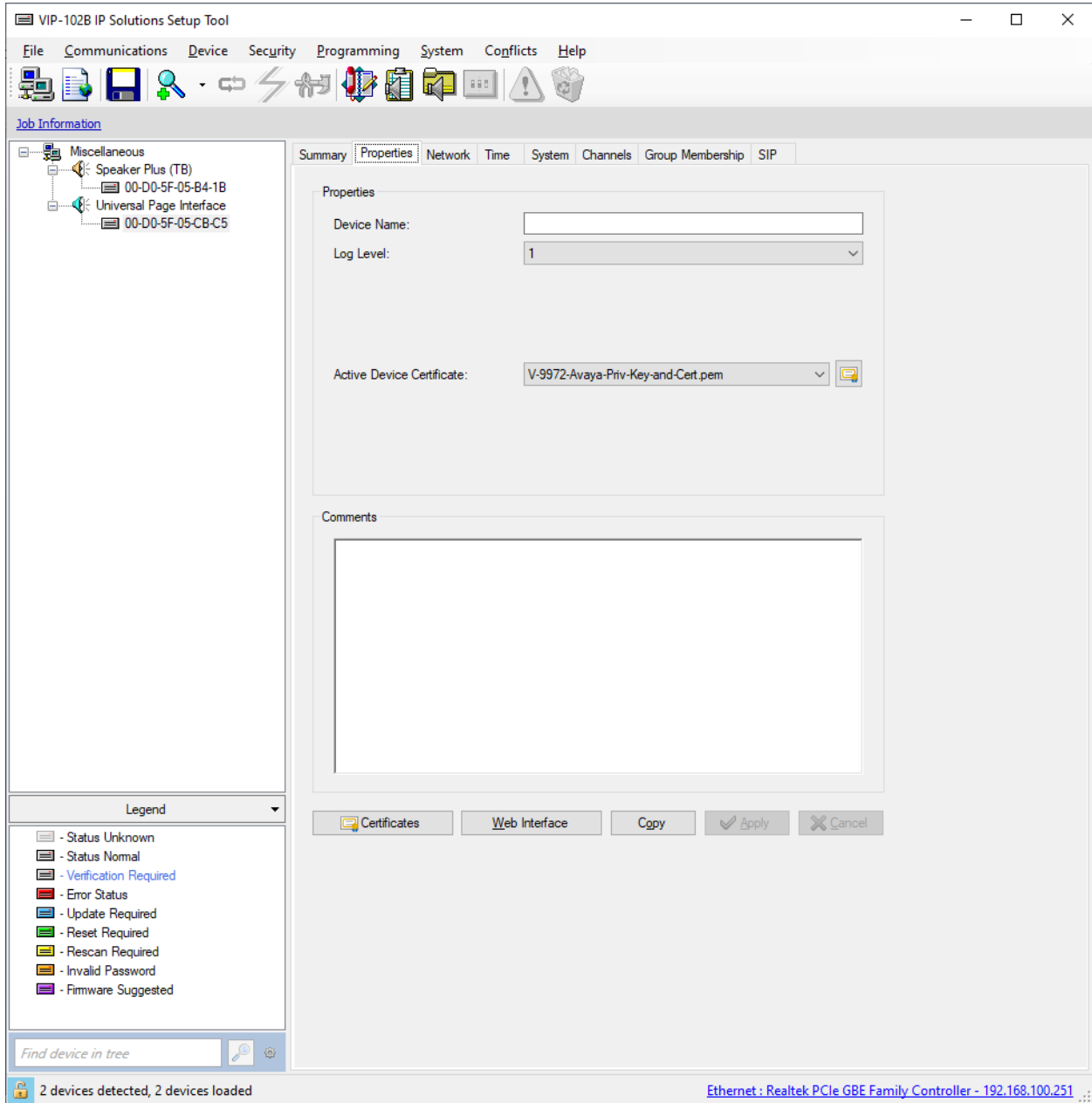
8.3. Configure the Time

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

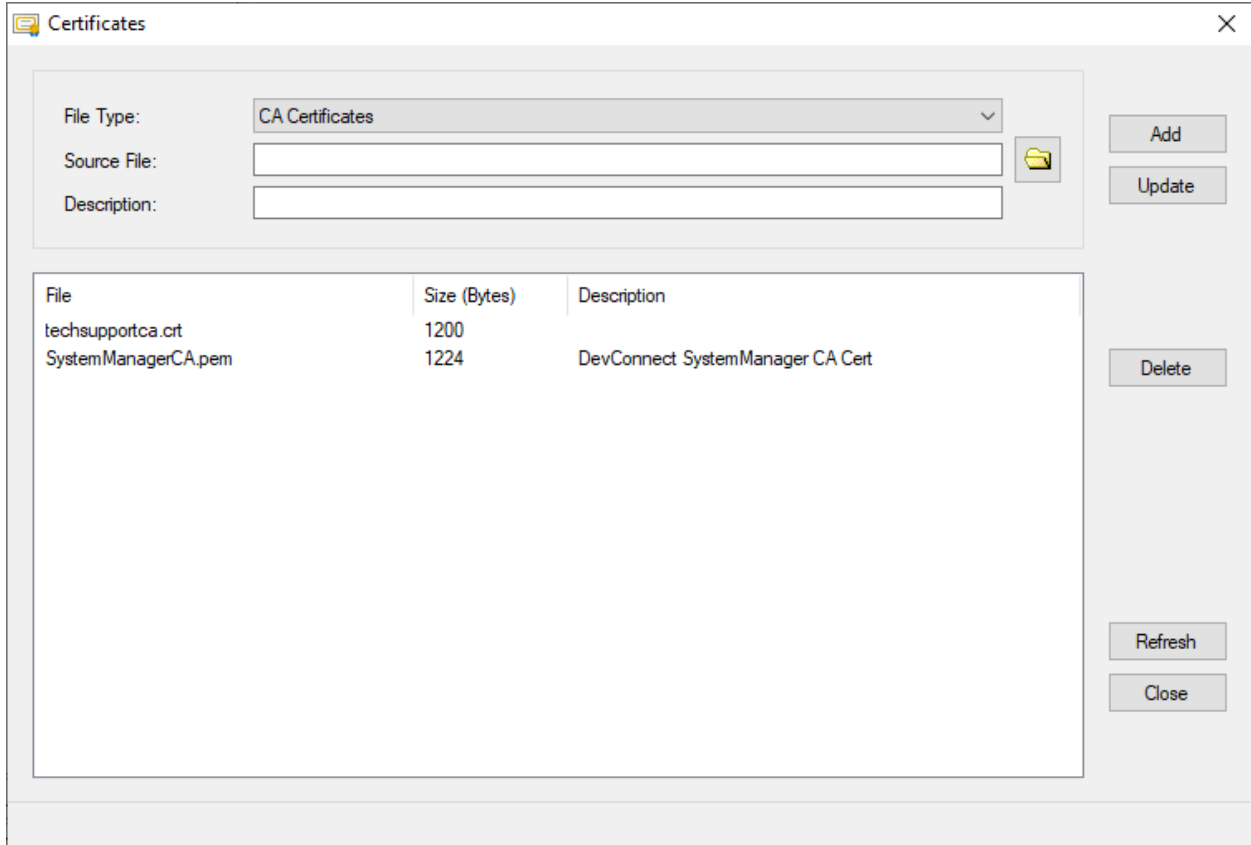


8.4. Install the System Manager CA TLS Certificate

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.

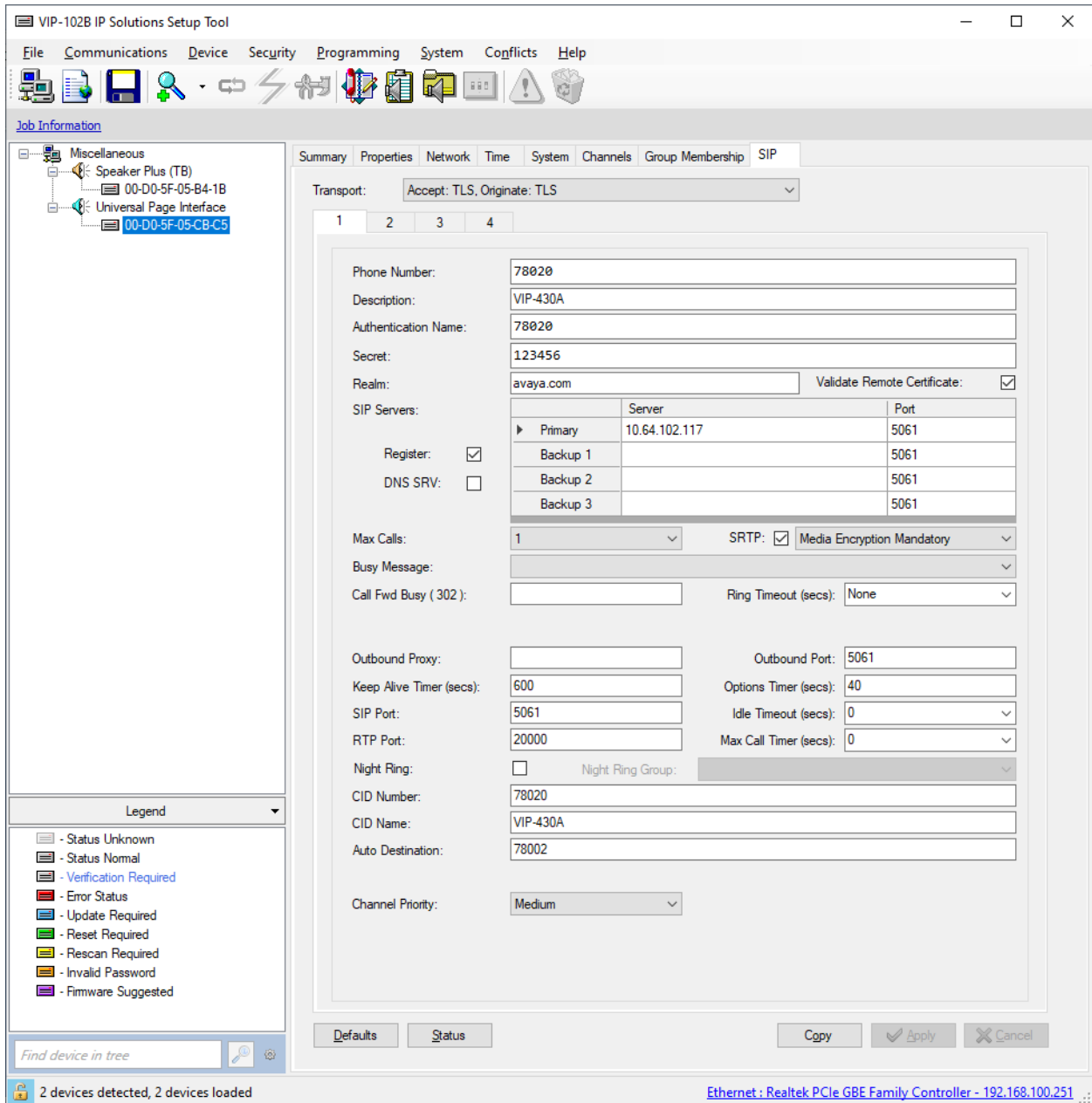


8.5. Configure SIP Parameters

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

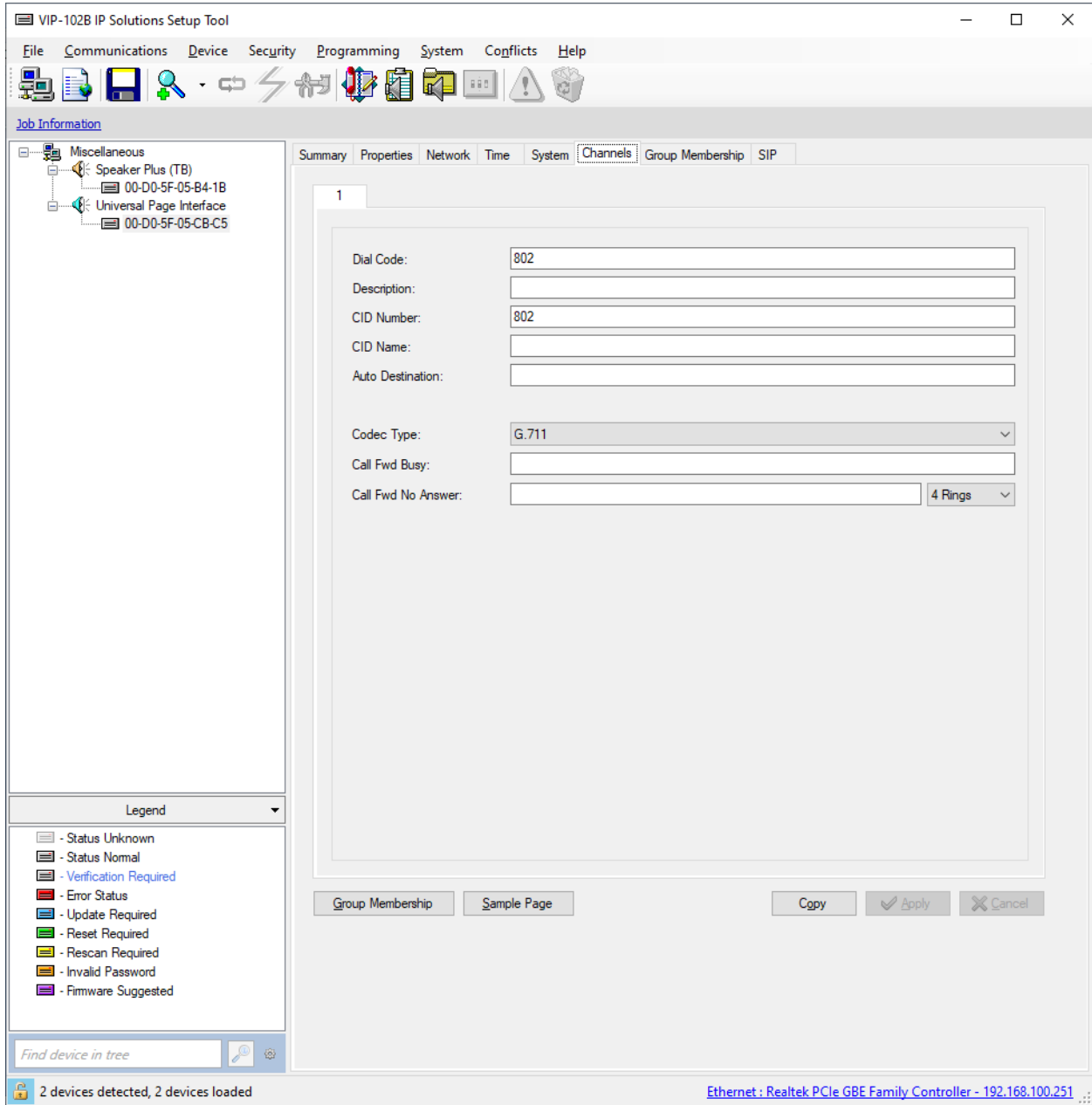
- **Transport:** Set to *Accept: TLS, Originate: TLS*.
- **Phone Number:** Set to SIP extension (e.g., 78020).
- **Description:** Provide optional description.
- **Authentication Name:** Set to SIP extension configured in Session Manager in **Section 6.3**.
- **Secret:** Set to SIP password configured in **Section 6.3.2**.
- **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 8.4**.
- **Primary Server:** Set to Session Manager IP address (i.e., *10.64.102.117*), if V-9972 will register directly to Session Manager, or set to the IP address of the SBCE public interface, if V-9972 will register to Session Manager through SBCE as a remote worker.
- **Port:** Set to TLS port (e.g., *5061*).
- **Register:** Enable this option to allow V-9972 to register as a SIP endpoint.
- **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**.



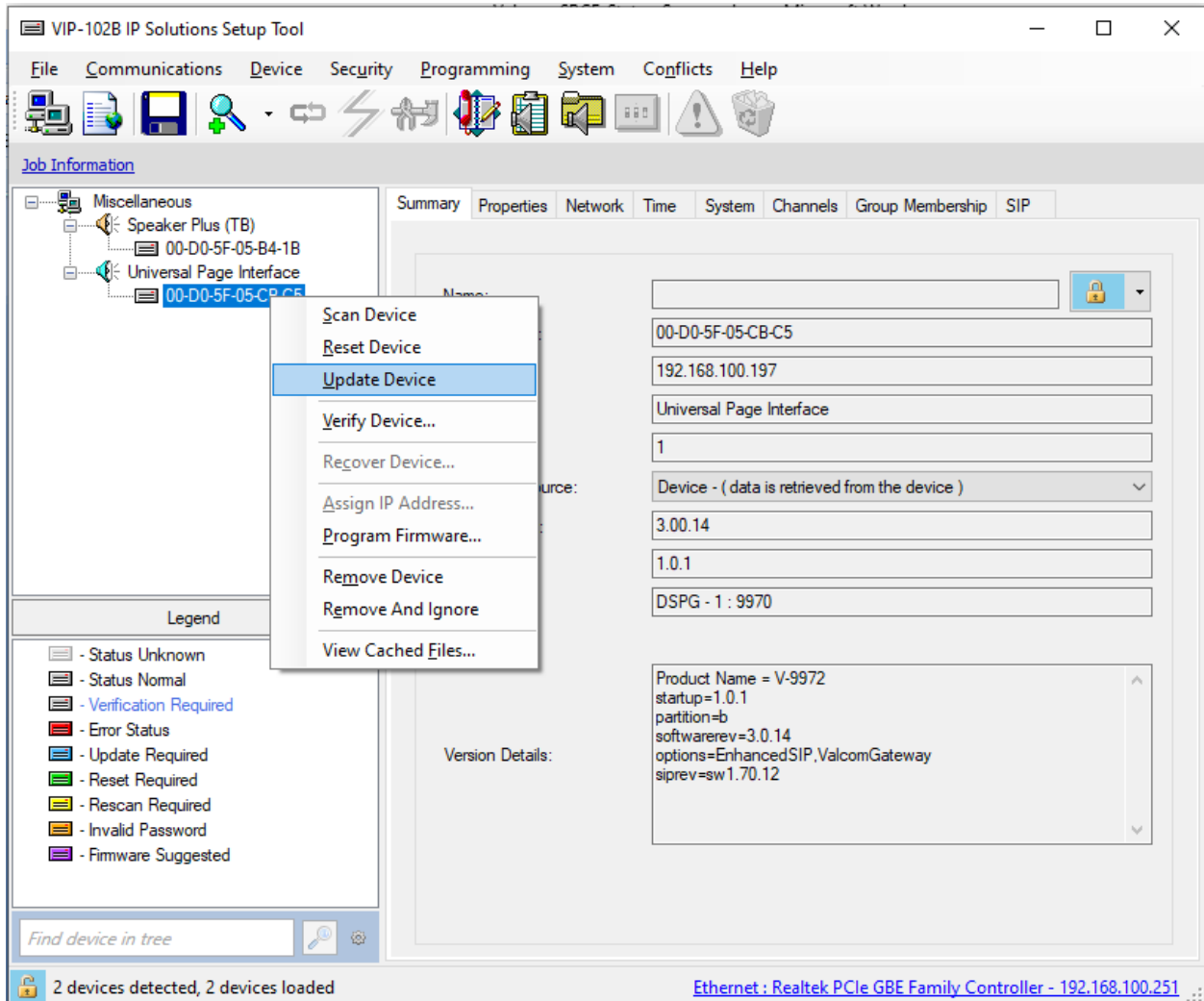
8.6. Verify Codec Settings

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.

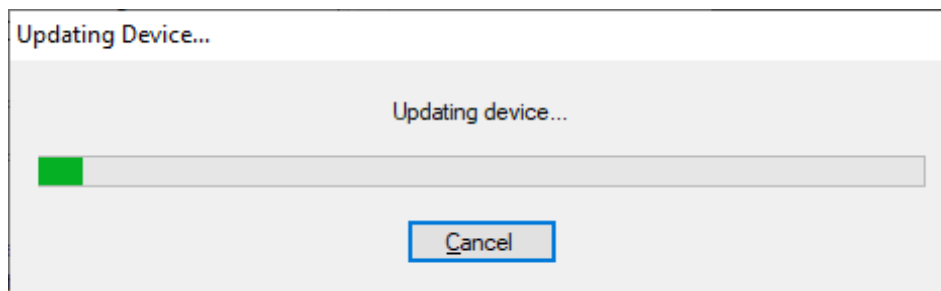


8.7. Update Universal Page Interface with the New Configuration

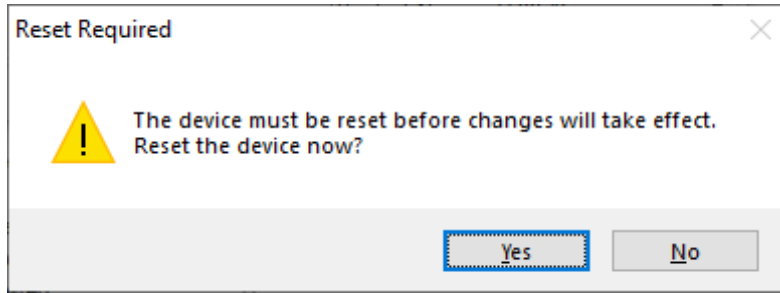
From the **VIP-102B IP Solutions Setup Tool**, right-mouse click on the MAC/hardware address of the Universal Page Interface and select **Update Device** from the pop-up menu as shown below.



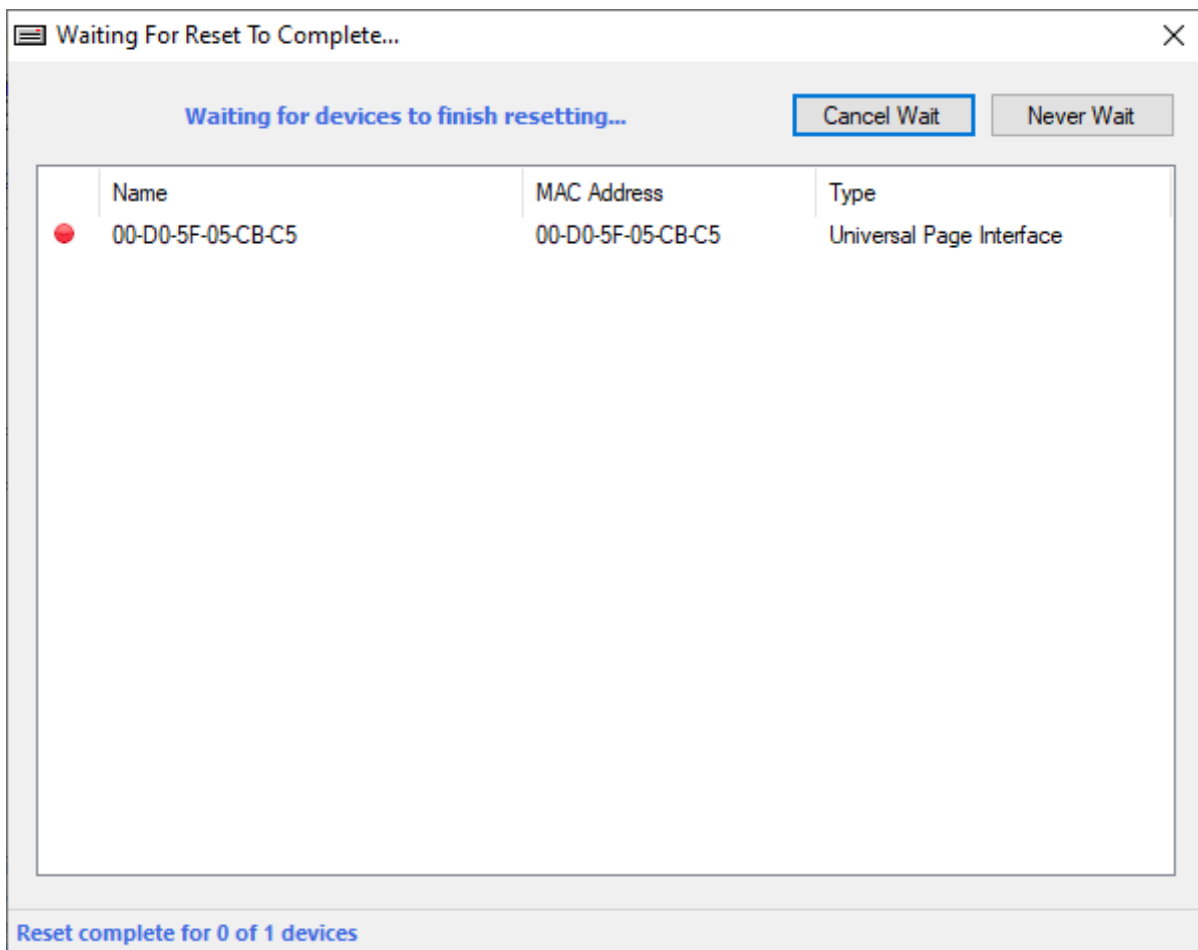
The following window is displayed indicating that the device is being updated.



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.



9. Verification Steps

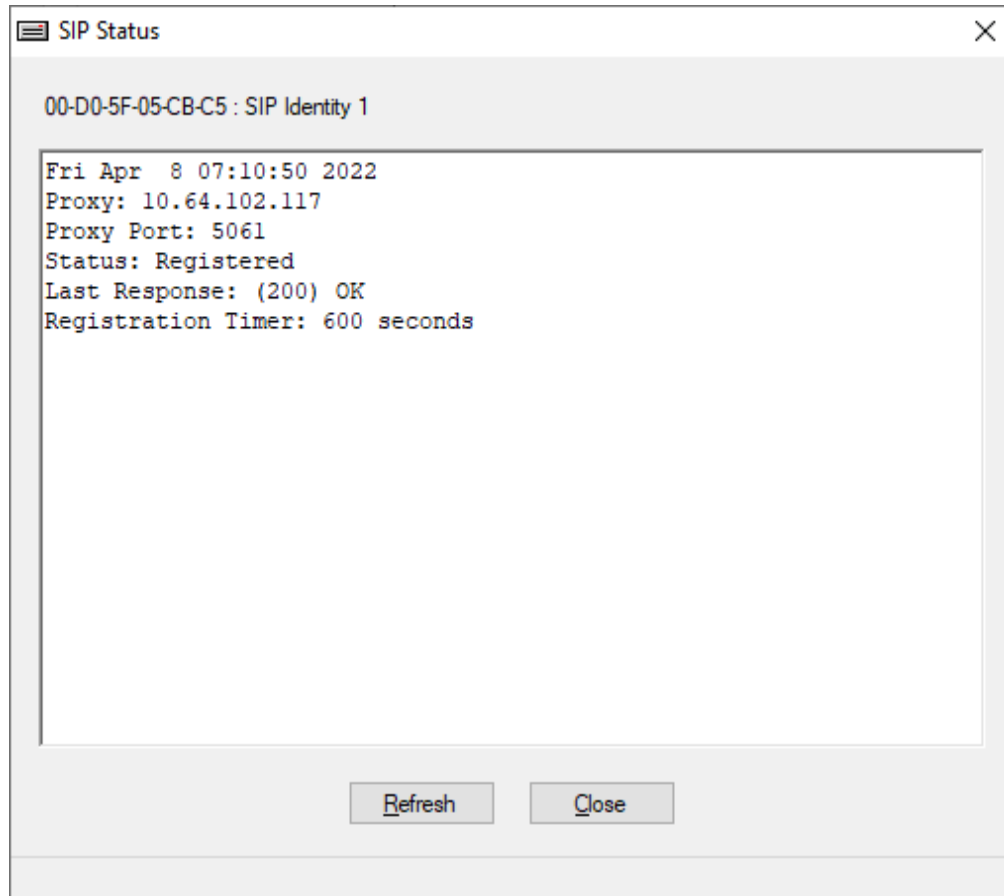
This section provides the tests that may be performed to verify proper configuration of Valcom V-9972 Universal Paging Interface with Avaya Aura® Session Manager, Avaya Aura® Communication Manager, and Avaya Session Border Controller for Enterprise.

1. Verify that V-9972 has successfully registered with Session Manager. In System Manager, navigate to **Elements** → **Session Manager** → **System Status** → **User Registrations** to check the registration status. Note that when V-9972 is registered as a remote worker, the **Remote Office** checkbox would be selected.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The main content area is titled "User Registrations" and displays a table of user registrations. The table has the following columns: Details, Address, First Name, Last Name, Actual Location, IP Address, Remote Office, Shared Control, Simult. Devices, AST Device, and Registered (Prim, Sec, Surv, Visiting). The row for the user 78020@avaya.com is highlighted in red, indicating it is the focus of the verification step. This row shows the user is registered as a Remote Office worker, with the Remote Office checkbox checked.

Details	Address	First Name	Last Name	Actual Location	IP Address	Remote Office	Shared Control	Simult. Devices	AST Device	Registered			
										Prim	Sec	Surv	Visiting
Show	---	█	78301	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Show	---	█	78011	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Show	---	SIP	78001	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Show	---	SIP	78000	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Show	---	Remote	78801	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Show	78002@avaya.com	SIP	78002	---	192.168.100.59	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Show	---	█	78010	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Show	78020@avaya.com	Valcom	78020	Thornton	192.168.100.197	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- Alternatively, the registration state may be verified the Valcom VIP-102B IP Solutions Setup Tool. Navigate to the **SIP** tab of the Universal Page Interface and click **Status** button. The **Status** should be *Registered*. Note that the **Proxy** would be the Session Manager IP address, if V-9972 is registered directly to Session Manager. The **Proxy** would be the IP address of the SBCE public interface if V-9972 is registered through SBCE as a remote worker.



- If the V-9972 is registered as a remote worker, the SBCE would also provide a registration status by navigating to **Status** → **User Registrations**.

User Registrations - Avaya Session Border Controller for Enterprise - Google Chrome
10.64.102.105/sbc/list

Device: SBCE ▾ Help

User Registrations

AVAYA

Displaying entries 1 to 2 of 2.

AOR	SIP Instance	SBC Device	SM Address	Registration State
78004@avaya.com	ab4d83147fe5	SBCE	10.64.102.117(PRIMARY)	REGISTERED(ACTIVE)
78020@avaya.com	00D05F05CBC5	SBCE	10.64.102.117(PRIMARY)	REGISTERED

1

4. 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.
5. 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.
6. Place an intercom call by pressing the call button on the IP speaker. Verify two-way audio to the call destination. Terminate the call.

10. Conclusion

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

11. 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