



Avaya Solution & Interoperability Test Lab

Application Notes for Aiphone IX Series 2 Video Door Station (IX-DBT) with Avaya Aura® Communication Manager and Avaya Aura® Session Manager - Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate Aiphone IX Series 2 Video Door Station (IX-DBT) Version 7.00 with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Session Manager 10.1. Aiphone IX-DBT Video Door Station, which is part of the Aiphone IX Series 2 Video Door Stations, is used for the compliance test. Aiphone IX-DBT Video Door Station is a surface mount, weather resistant Video door station. The Aiphone IX-DBT Video Door Station registers with Avaya Aura® Session Manager as a SIP endpoint.

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 Aiphone IX Series 2 Video Door Station (IX-DBT) Version 7.00 with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Session Manager 10.1. Aiphone IX-DBT Video Door Station, which is part of the Aiphone IX Series 2 Video Door Stations, was used for the compliance test. Aiphone IX-DBT Video Door Station is a surface mount, weather resistant Video door station. Aiphone IX-DBT Video Door Station (IX-DBT) registers with Avaya Aura® Session Manager as a SIP endpoint.

2. General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing. The feature testing focused on establishing audio and video calls between Aiphone IX-DBT Video Door Station, Avaya SIP and H.323 telephones, Avaya Workplace Client for Windows, Avaya Vantage™ K155, and the PSTN, and exercising basic telephony features, such as hold/resume, mute/unmute, transfer, conference, call forwarding, and call coverage from an Avaya IP endpoint. Additional telephony features, such as call forward and call coverage, were also verified.

The serviceability testing focused on verifying that the Aiphone IX-DBT Video Door Station comes back into service after re-connecting the Ethernet cable.

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 Aiphone IX-DBT Video Door Station did not include use of any specific encryption features as requested by Aiphone.

2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- SIP registration of IX-DBT with Session Manager.
- Audio calls between IX-DBT and Avaya SIP and H.323 deskphones with Direct IP Media (Shuffling) enabled and disabled.
- Audio and video calls between IX-DBT, Workplace, and Vantage K155 with Direct IP Media (Shuffling) enabled and disabled. One-way video from IX-DBT to Workplace and Vantage K155 was verified.
- Audio calls between IX-DBT and the PSTN.
- G.711 codec support.
- UDP transport protocol.
- IX-DBT placing, answering, and terminating calls.
- Basic telephony features, including hold/resume, mute/unmute, transfer, and 3-way conference, initiated from an Avaya IP endpoint.
- Proper system recovery after re-establishing IP connectivity to IX-DBT.

2.2. Test Results

All test cases executed passed successfully with the following observations:

- IX-DBT auto answers calls placed to them.
- IX-DBT does not support remote door open via DTMF input of Door Release Authorization Authentication Key
- IX-DBT only supports G.711 codec.
- Video is activated on answer for IX-DBT Station calls to Workplace Client or Vantage when Direct IP Media (shuffling) is enabled.
- Video may not be active on answer for IX-DBT Video Station calls when shuffling is not enabled. If the called station is Vantage or Workplace Client, video from the IX stations can be initiated by Vantage or Workplace Client by starting video manually or cycling block video buttons.

2.3. Support

For technical support of Aiphone IX Series 2 Video Door Stations, contact Aiphone Technical Support via phone or website.

- Phone: +1 (800) 692-0200
- Web: <https://www.aiphone.com/support/technical-support>

3. Reference Configuration

Figure 1 illustrates a sample configuration with an Avaya SIP-based network. Aiphone IX-DBT Video Door Station registered with Session Manager and was configured as an Off-PBX Station (OPS) on Communication Manager.

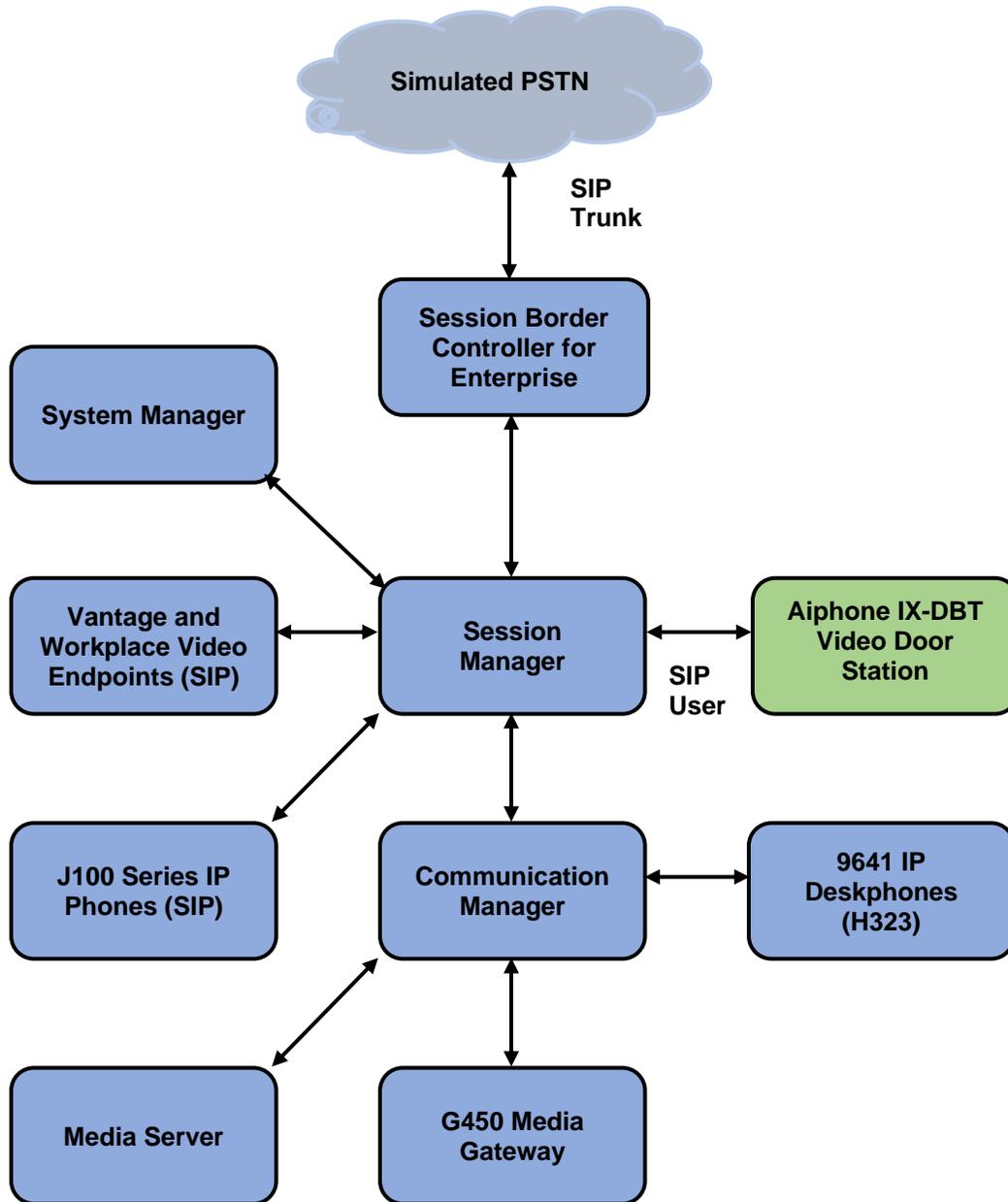


Figure 1: Avaya SIP Telephony Network with Aiphone IX-DBT Video Door Station

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager	10.1.2.0 FP2 01.0.974.0-27783
Avaya G450 Media Gateway	FW 42.18.0
Avaya Aura® Media Server	10.1.0.125
Avaya Aura® System Manager	10.1.2.0 Feature Pack 2 10.1.2.0.0715476
Avaya Aura® Session Manager	10.1.2.0 Feature Pack 2 10.1.0.02.1012016
Avaya Session Border Controller for Enterprise	10.1.0.0-32-21432
Avaya 96x1 Series IP Deskphones	6.8.5.4 (H.323)
Avaya J100 Series IP Phones	4.1.0.0.9
Avaya K155 Vantage Device	3.1.1.2 (bld version 0012)
Avaya Workplace	3.32.0.75
Aiphone IX-DBT Video Door Station	7.00

5. Configure Avaya Aura® Communication Manager

This section describes the configuration of a SIP trunk to Session Manager and routing calls to IX-DBT. Administration of Communication Manager was performed using the System Access Terminal (SAT). The following configuration is covered:

- Verify Communication Manager license.
- Administer IP Node Names.
- Administer IP Codec Set.
- Administer IP Network Region.
- Administer SIP Trunk to Session Manager.
- Configure Private Numbering.

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, including IX-DBT Video Door Stations, that will be deployed.

```
display system-parameters customer-options                               Page 1 of 12
                                OPTIONAL FEATURES

G3 Version: V20                                                         Software Package: Enterprise
Location: 2                                                             System ID (SID): 1
Platform: 28                                                            Module ID (MID): 1

                                USED
Platform Maximum Ports: 48000    108
Maximum Stations: 150            73
Maximum XMOBILE Stations: 36000  0
Maximum Off-PBX Telephones - EC500: 150  0
Maximum Off-PBX Telephones - OPS: 150  42
Maximum Off-PBX Telephones - PBFMC: 150  0
Maximum Off-PBX Telephones - PVFMC: 150  0
Maximum Off-PBX Telephones - SCCAN: 0    0
Maximum Off-PBX Telephones - EMX: 150   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 (*sm10*). The host names will be used in other configuration screens of Communication Manager.

```
change node-names ip                                     Page 1 of 2
                                                    IP NODE NAMES
      Name                IP Address
aes10                    10.64.110.247
ams10                    10.64.110.214
default                  0.0.0.0
procr                   10.64.110.213
procr6                   ::
sm10                   10.64.110.212

( 6 of 6 administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

5.3. Administer IP Codec Set

In the **IP Codec Set** form, select the audio codec type supported for calls routed over the SIP trunk to IX-DBT. The form is accessed via the **change ip-codec-set 1** command. Note the codec set number since it will be used in the IP Network Region covered in the next section. For the compliance test, the G.711MU codec was verified. The following IP codec set is configured with G.711MU.

Media encryption was enabled for Avaya IP endpoints. IX-DBT wasn't configured to support SRTP, so the *none* option was also included under **Media Encryption**.

```
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 SRTP: best-effort
1: 1-srtp-aescm128-hmac80
2: 10-srtp-aescm256-hmac80
3: none
4:
5:
```

On **Page 2**, enable **Allow Direct-IP Multimedia** and set **Maximum Call rate for Direct-IP Multimedia** and **Maximum Call Rate for Priority Direct-IP Multimedia** to *4096 Kbits* as shown below.

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

                IP MEDIA PARAMETERS

                Allow Direct-IP Multimedia? y
                Maximum Call Rate for Direct-IP Multimedia: 4096:Kbits
                Maximum Call Rate for Priority Direct-IP Multimedia: 4096:Kbits

                Mode                               Redun-          Packet
                t.38-standard                       dancy           Size (ms)
                pass-through                          0   ECM: y
                US                                     3
                H.323 Clear-channel y                 0
                SIP 64K Data n                         0               20

Media Connection IP Address Type Preferences
1: IPv4
2:
```

5.4. Administer IP Network Region

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

```
change ip-network-region 1                                     Page 1 of 20
                                                           IP NETWORK REGION
  Region: 1          NR Group: 1
Location: 1        Authoritative Domain: avaya.com
  Name: Main        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: 65535
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
  H.323 Link Bounce Recovery? y
  Idle Traffic Interval (sec): 20
  Keep-Alive Interval (sec): 5
  Keep-Alive Count: 5
                                                           AUDIO RESOURCE RESERVATION PARAMETERS
                                                           RSVP Enabled? n
```

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*.
- Specify the Ethernet processor (*procr*) of Communication Manager and Session Manager (*sm10*) as the two ends of the signaling group in the **Near-end Node Name** field and the **Far-end Node Name** field, respectively. These field values are taken from the **IP Node Names** form in **Section 5.2**.
- Set **IP Video** field to *y*.
- 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*.
- Set **Initial IP-IP Direct Media** field to *y*.

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

```
display signaling-group 1                               Page 1 of 3
                                     SIGNALING GROUP

Group Number: 1                Group Type: sip
  IMS Enabled? n                Transport Method: tls
  Q-SIP? n
  IP Video? y                   Priority Video? n           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: sm10
  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 IX-DBT. Set the **Group Type** field to *sip*, set the **Service Type** field to *tie*, specify the signaling group associated with this trunk group in the **Signaling Group** field, and specify the **Number of Members** supported by this SIP trunk group. Accept the default values for the remaining fields.

```

display trunk-group 1                                     Page 1 of 5
                                     TRUNK GROUP
Group Number: 1                Group Type: sip          CDR Reports: y
  Group Name: SM Trunk 1        COR: 1              TN: 1          TAC: 101
  Direction: two-way          Outgoing Display? n
  Dial Access? n              Night Service:
  Queue Length: 0
Service Type: tie           Auth Code? n
                                     Member Assignment Method: auto
                                     Signaling Group: 1
                                     Number of Members: 10

```

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

```

display trunk-group 1                                     Page 3 of 5
TRUNK FEATURES
  ACA Assignment? n          Measured: both
                                     Maintenance Tests? y

  Suppress # Outpulsing? n  Numbering Format: private
                                     UUI Treatment: shared
                                     Maximum Size of UUI Contents: 128
                                     Replace Restricted Numbers? n
                                     Replace Unavailable Numbers? n

                                     Modify Tandem Calling Number: no
  Send UCID? y

  Show ANSWERED BY on Display? y

  DSN Term? n

```

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

```

display trunk-group 1
                                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. Configure Private Numbering

Configure the **Numbering – Private Format** form to send the calling party number to the far-end. Add an entry so that local stations with a 5-digit extension beginning with ‘7’ whose calls are routed over any trunk group, including SIP trunk group 1, have their extension sent.

```

change private-numbering 0
                                Page 1 of 2
                                NUMBERING - PRIVATE FORMAT
Ext  Ext      Trk      Private      Total
Len  Code      Grp(s)     Prefix       Len
5   7
                                5   Total Administered: 1
                                Maximum Entries: 540
  
```

6. Configure Avaya Aura® Session Manager

This section covers the procedure for adding a SIP user in Session Manager. The configuration covers:

- Launch System Manager
- Set Network Transport Protocol for IX-DBT
- Administer SIP User

Note: It is assumed that basic configuration of Session Manager has already been performed.

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 System Manager IP address. 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.

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

User ID:

Password:

[Change Password](#)

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

6.2. Set Network Transport Protocol for IX-DBT

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

The screenshot shows the Avaya Aura System Manager 10.1 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The main content area is titled 'SIP Entity Details' and is divided into 'General' and 'Monitoring' sections. The 'General' section contains fields for Name (sm10), IP Address (10.64.110.212), SIP FQDN, Type (Session Manager), Notes, Location (DevConnect), Outbound Proxy, Time Zone (America/Denver), Minimum TLS Version (Use Global Setting), and Credential name. The 'Monitoring' section includes SIP Link Monitoring (Link Monitoring Enabled), Proactive Monitoring Interval (900), Reactive Monitoring Interval (120), and Number of Tries (1). Buttons for 'Commit' and 'Cancel' are visible at the top right of the form.

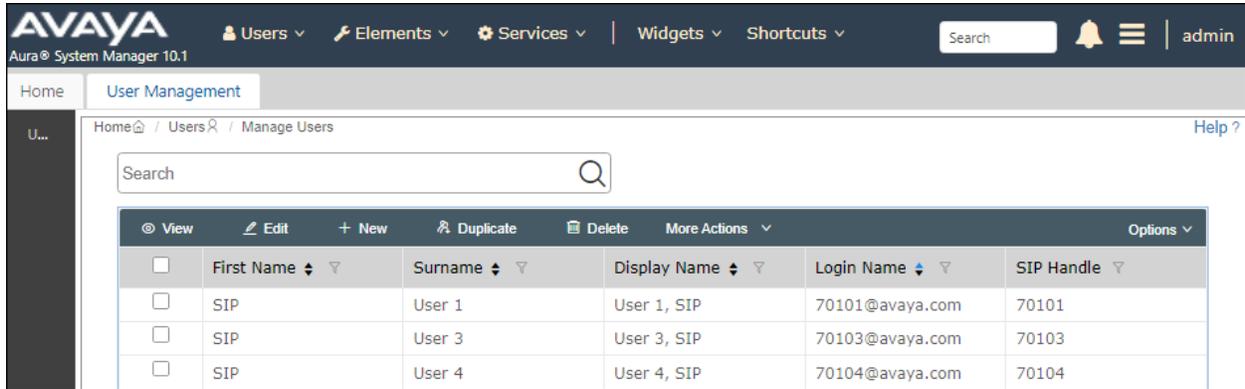
Scroll down to the **Listen Ports** section and verify that the transport network protocol used by IX-DBT is specified in the list below. For the compliance test, the solution used UDP network transport.

The screenshot shows the 'Listen Ports' section of the Avaya Aura System Manager 10.1 interface. It features a table with 3 items, a 'Filter: Enable' button, and a 'Select: All, None' option at the bottom. The table columns are Listen Ports, Protocol, Default Domain, Endpoint, and Notes.

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

6.3. Administer SIP User

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

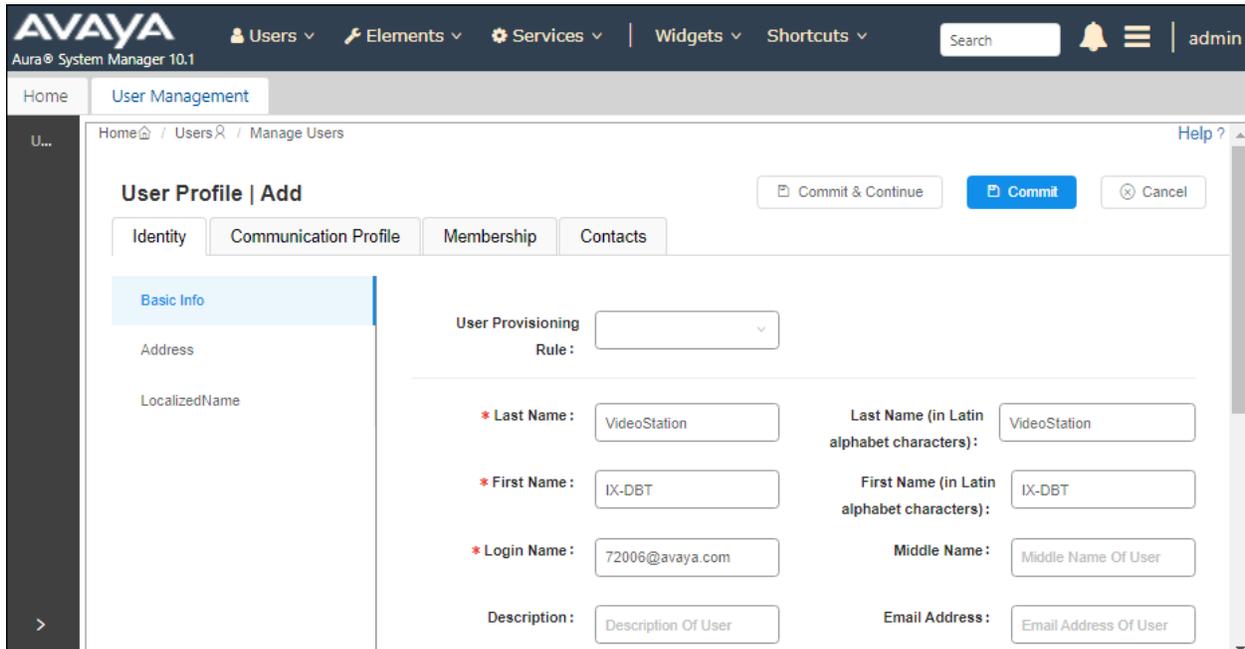


The screenshot shows the Avaya Aura System Manager 10.1 User Management interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. A search bar and a user profile icon are also present. The main content area displays a table of users with the following columns: First Name, Surname, Display Name, Login Name, and SIP Handle. The table contains three rows of user data.

<input type="checkbox"/>	First Name	Surname	Display Name	Login Name	SIP Handle
<input type="checkbox"/>	SIP	User 1	User 1, SIP	70101@avaya.com	70101
<input type="checkbox"/>	SIP	User 3	User 3, SIP	70103@avaya.com	70103
<input type="checkbox"/>	SIP	User 4	User 4, SIP	70104@avaya.com	70104

6.3.1. Identity

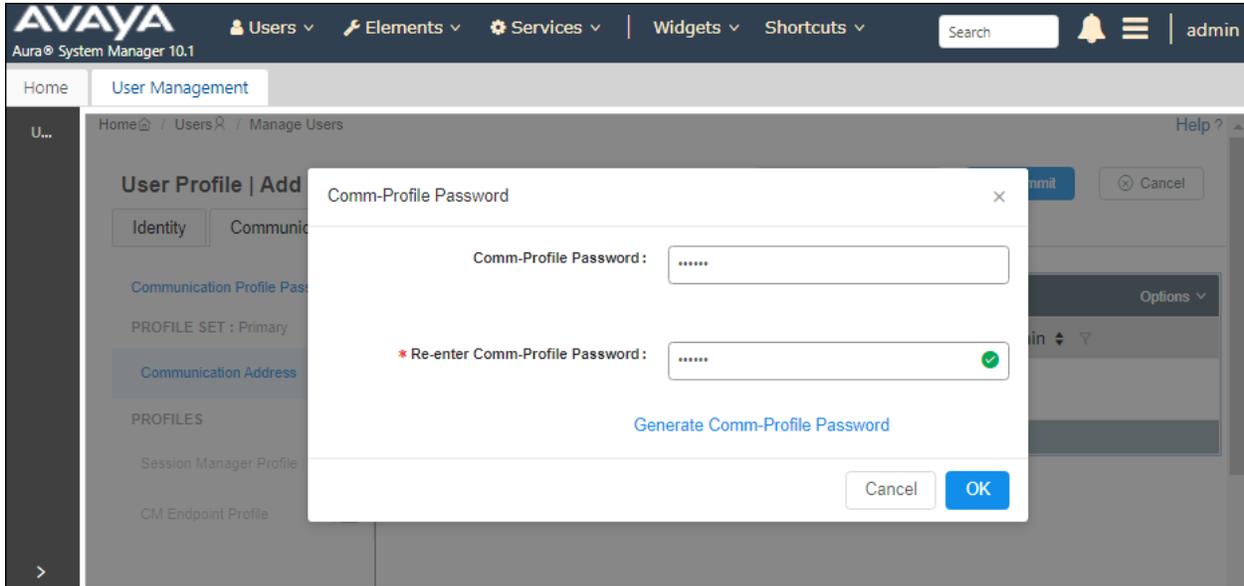
The **New User Profile** screen is displayed. Enter desired **Last Name** and **First Name**. For **Login Name**, enter $\langle extension \rangle @ \langle domain \rangle$, where $\langle extension \rangle$ is the desired IX-DBT SIP extension and $\langle domain \rangle$ is the applicable SIP domain name from **Section 5.4**. Retain the default values in the remaining fields.



The screenshot shows the Avaya Aura System Manager 10.1 User Profile | Add screen. The interface includes a navigation bar with 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The main content area displays the 'User Profile | Add' form with tabs for 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. The 'Basic Info' tab is selected, showing fields for 'User Provisioning Rule', 'Last Name', 'First Name', 'Login Name', 'Description', 'Last Name (in Latin alphabet characters)', 'First Name (in Latin alphabet characters)', 'Middle Name', and 'Email Address'. The 'Last Name' field is populated with 'VideoStation', 'First Name' with 'IX-DBT', and 'Login Name' with '72006@avaya.com'.

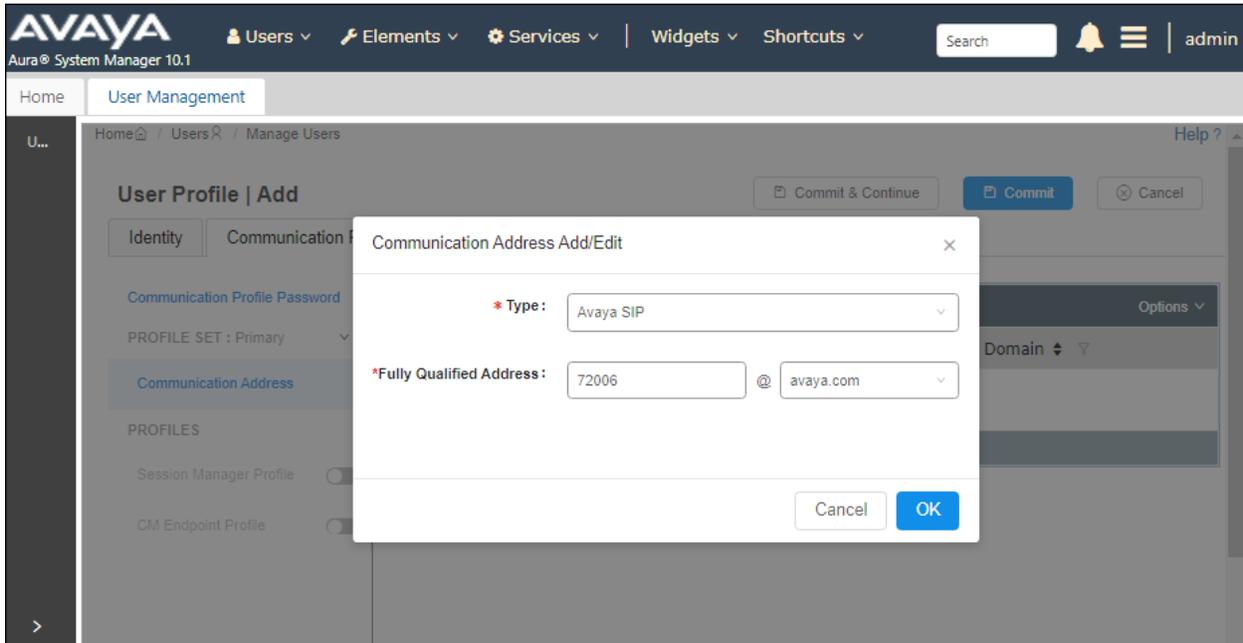
6.3.2. Communication Profile Password

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**, retain *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 Sequence** and **Termination Sequence** (Application Sequences), and **Home Location**, select the values corresponding to the applicable Session Manager and Communication Manager. Retain the default values in the remaining fields.

The screenshot shows the 'User Profile | Add' form in the Avaya Aura System Manager 10.1 interface. The 'Communication Profile Password' section is active, showing 'PROFILE SET : Primary' and 'Communication Address'. The 'SIP Registration' section includes fields for 'Primary Session Manager' (sm10), 'Secondary Session Manager' (Start typing...), 'Survivability Server' (Start typing...), 'Max. Simultaneous Devices' (Select), and 'Block New Registration When Maximum Registrations Active?' (checkbox). The 'Application Sequences' section shows 'Origination Sequence' and 'Termination Sequence' both set to 'cm10 App Seq'.

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

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

6.3.5. CM Endpoint Profile

Click on the toggle button by **CM Endpoint Profile**. For **System**, select the value corresponding to the applicable Communication Manager. For **Extension**, enter the SIP user extension from **Section 6.3.1**. For **Template**, select *9641SIP_DEFAULT_CM_10_1*. Retain the default values in the remaining fields. Click on **Endpoint Editor** (i.e., the Edit icon in the Extension field) to configure **IP Video**.

The screenshot shows the Avaya Aura System Manager 10.1 interface for adding a new user profile. The 'Communication Profile' tab is active, showing various configuration fields. The 'CM Endpoint Profile' toggle is turned on. The form includes fields for System (cm10), Profile Type (Endpoint), Extension (72006), Template (9641SIP_DEFAULT_CM_10_1), Set Type (9641SIP), Security Code (Enter Security Code), Port (IP), Voice Mail Number, Preferred Handle (Select), Calculate Route Pattern, SIP URI (Select), Sip Trunk (aar), and checkboxes for 'Override Endpoint Name and Localized Name' (checked) and 'Delete on Unassign from User or on Delete User' (checked). There is also an unchecked checkbox for 'Allow H.323 and SIP Endpoint Dual'. Action buttons for 'Commit & Continue', 'Commit', and 'Cancel' are visible at the top right of the form area.

In the **Endpoint Editor**, navigate to the **Feature Options** tab and enable **IP Video** under **Features** as shown below.

General Options (G) *		Feature Options (F)		Site Data (S)	Abbreviated Call Dialing (A)	Enhanced Call Fwd (E)
Button Assignment (B)		Profile Settings (P)		Group Membership (M)		
Active Station Ringing	single ▼	Auto Answer	none ▼			
MWI Served User Type	None ▼	Coverage After Forwarding	system ▼			
Per Station CPN - Send Calling Number	None ▼	Display Language	english ▼			
IP Phone Group ID	<input type="text"/>	Hunt-to Station	<input type="text"/>			
Remote Soft Phone Emergency Calls	as-on-local ▼	Loss Group	19			
LWC Reception	spe ▼	Survivable COR	internal ▼			
AUDIX Name	None ▼	Time of Day Lock Table	None ▼			
EC500 State	enabled ▼	Voice Mail Number	<input type="text"/>			
Short/Prefixed Registration Allowed	default ▼	Bridging Tone for This Extension	None ▼			
Music Source	<input type="text"/>					
Features						
<input type="checkbox"/> Always Use	<input type="checkbox"/> Idle Appearance Preference					
<input type="checkbox"/> IP Audio Hairpinning	<input type="checkbox"/> IP SoftPhone					
<input type="checkbox"/> Bridged Call Alerting	<input checked="" type="checkbox"/> LWC Activation					
<input type="checkbox"/> Bridged Idle Line Preference	<input type="checkbox"/> CDR Privacy					
<input checked="" type="checkbox"/> Coverage Message Retrieval	<input checked="" type="checkbox"/> Precedence Call Waiting					
<input type="checkbox"/> Data Restriction	<input checked="" type="checkbox"/> Direct IP-IP Audio Connections					
<input checked="" type="checkbox"/> Survivable Trunk Dest	<input type="checkbox"/> H.320 Conversion					
<input type="checkbox"/> Bridged Appearance Origination Restriction	<input checked="" type="checkbox"/> IP Video					
<input checked="" type="checkbox"/> Restrict Last Appearance	<input type="checkbox"/> Per Button Ring Control					
<input type="checkbox"/> Turn on mute for remote off-hook attempt						
<input type="checkbox"/> IP Hoteling						

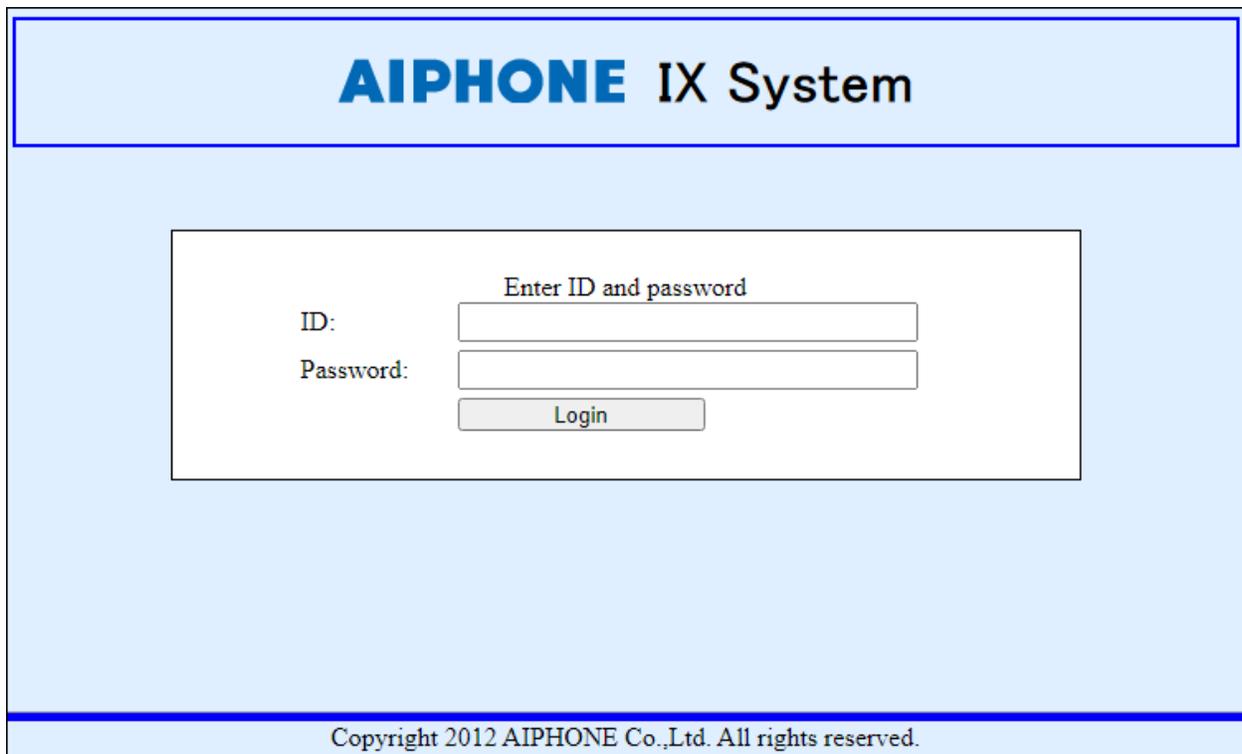
7. Configure Aiphone IX-DBT Video Door Station

This section provides the procedure for configuring IX-DBT to provide SIP connectivity to Session Manager. Configuration of IX-DBT is performed via Aiphone IX System web interface. The following configuration is covered:

- Log into Aiphone IX System Web Interface
- Administer Station Information
- Administer SIP Parameters
- Administer Video SIP Channel
- Administer Audio Settings
- Administer Call Settings

7.1. Log into Aiphone IX System Web Interface

Access the Aiphone IX System Web Interface by using the URL <https://<ip-address>/webset.cgi?login> in an Internet browser, where <ip-address> is the IX-DBT IP address. Select language (not shown) and log in using the appropriate credentials.



AIPHONE IX System

Enter ID and password

ID:

Password:

Login

Copyright 2012 AIPHONE Co.,Ltd. All rights reserved.

7.2. Administer Station Information

Navigate to **Station Information** → **Identification** and set the **Number** to the IX-DBT SIP extension (e.g., 72006). Input an appropriate **Name**.

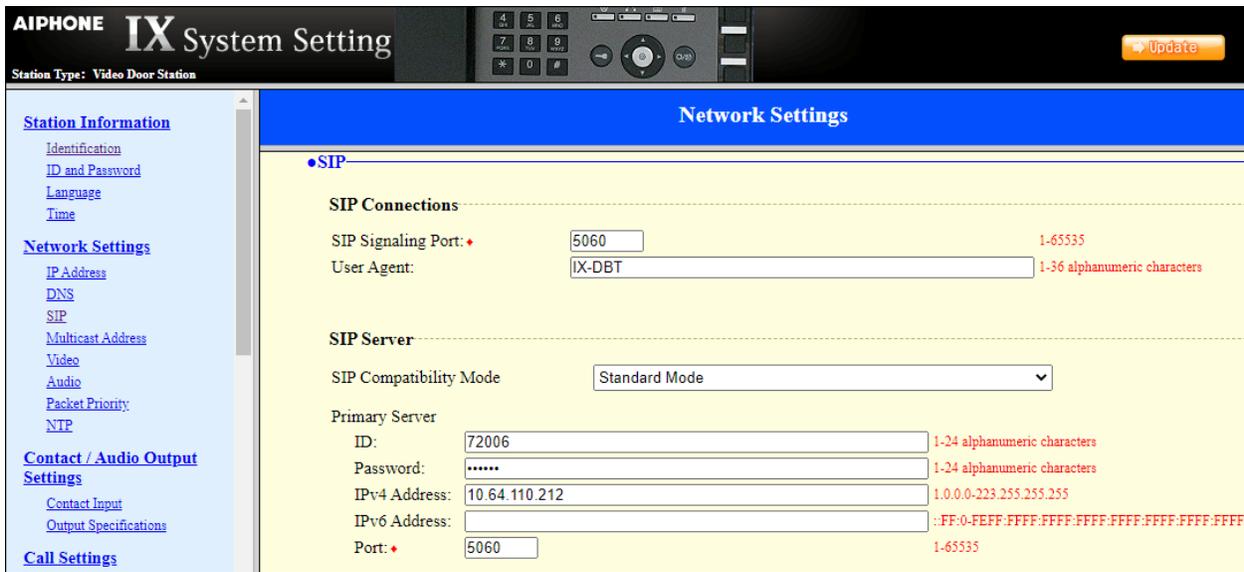
The screenshot shows the AIPHONE IX System Setting web interface for a Video Door Station. The interface is divided into a sidebar on the left and a main content area on the right. The sidebar contains a list of settings: Station Information (selected), ID and Password, Language, Time, Network Settings, IP Address, DNS, and SIP. The main content area is titled 'Station Information' and has a sub-section for 'Identification'. This section contains three input fields: 'Number' (set to 72006, with a red note '3-5 digits'), 'Name' (set to IX-DBT, with a red note '1-24 alphanumeric characters'), and 'Location' (empty, with a red note '1-24 alphanumeric characters'). An 'Update' button is located in the top right corner of the interface.

7.3. Administer SIP Parameters

Navigate to **Network Settings** → **SIP** from the left pane and configure the following parameters:

- **SIP Signaling Port:** Set to *5060*.
- **User Agent:** Enter desired value (e.g., *IX-DBT*).
- **ID:** Set to SIP extension (e.g., *72006*) from **Section 6.3.1**.
- **Password:** Enter SIP password from **Section 6.3.2**.
- **IPv4 Address:** Set to signaling IP address of Session Manager (e.g., *10.64.110.212*).
- **Port:** Set to *5060*.

Click **Update** to save changes.



7.4. Administer Video SIP Channel

Navigate to **Network Settings** → **Video** in the left pane and configure the video settings as shown below.

The screenshot displays the AIPHONE IX System Setting web interface. At the top, it shows 'Station Type: Video Door Station' and an 'Update' button. The left sidebar contains a navigation menu with sections: Station Information (Identification, ID and Password, Language, Time), Network Settings (IP Address, DNS, SIP, Multicast Address, Video, Audio, Packet Priority, NTP), Contact / Audio Output Settings (Contact Input, Output Specifications), and Call Settings. The main content area is titled 'Network Settings' and features a 'Video' section. This section includes a warning: 'Items marked [H.264 / AVC] or [Motion-JPEG] apply only to their respective Coding System. The 'SIP Channel' RTP End Port should be greater than 90 digits from the RTP Start Port. The 'ONVIF Transmit Channel' RTP End Port should be greater than 10 digits from the RTP Start Port.' Below the warning, the 'SIP Channel' configuration is shown with the following settings:

Parameter	Value	Range
Coding System:	H.264 / AVC	
Resolution:	320x240 (QVGA)	
Frame Rate [fps]:	15	
Select Profile [H.264 / AVC]:	High	
I-picture interval [H.264 / AVC]: ♦	15	1-100
Bit rate [kbps] [H.264 / AVC]:	1024	
Select Quality [Motion-JPEG]:	6	
RTP Start Port: ♦	30000	1-65534
RTP End Port: ♦	31000	1-65535

7.5. Administer Audio Settings

Navigate to **Network Settings** → **Audio** in the left pane and set **Audio Codec** to select *G.711 (u-law)*.

The screenshot displays the 'AIPHONE IX System Setting' web interface. The top navigation bar includes a keypad and an 'Update' button. The left sidebar contains a tree view with categories: Station Information, Network Settings, Contact / Audio Output Settings, Call Settings, and Function Settings. The 'Network Settings' section is expanded, and the 'Audio' sub-section is selected. The main content area shows the following settings:

- Audio CODEC:** G.711(μ-law) G.711(A-law)
- Audio RTP Transmission Interval [msec]:** 20 (Note: This setting is ignored when transmitting to multiple stations (paging, etc.))
- RTP Idle Detection Time [sec]:** 10 (Range: 10-180sec)
- SIP Channel:**
 - RTP Start Port:** 20000 (Range: 1-65534)
 - RTP End Port:** 21000 (Range: 1-65535)
- ONVIF Transmit Channel:**
 - RTP Start Port:** 22000 (Range: 1-65534)
 - RTP End Port:** 23000 (Range: 1-65535)
- Audio Buffer:**
 - Packets Buffered at Audio Start:** 1
 - Maximum Packets Buffered:** 3 (Note: Maximum Packet Buffer must be larger than Audio Start Buffer.)

7.6. Administer Call Settings

Navigate to **Call Settings** → **Called Stations** in the left pane. In the **Called Stations** section, add an entry that specifies the number that should be dialed when the call button is pressed. Set the **Station Number** to the called number (e.g., 70103), set the **IPv4 Address** to the signaling IP address of Session Manager (e.g., 10.64.110.212), and set **Protocol** to *U*.

The screenshot shows the 'AIPHONE IX System Setting' interface. The left sidebar contains navigation links for Station Information, Network Settings, Contact / Audio Output Settings, and Call Settings. The 'Call Settings' section is active, showing a 'Called Stations' table. The table has columns for Number, IPv4 Address, IPv6 Address, and Protocol. The first row is filled with the example values: Number 70103, IPv4 Address 10.64.110.212, and Protocol U.

	Number 3-32 digits	IPv4 Address 1.0.0.0-255.255.255.255	IPv6 Address 2000::0- 3FFF:FFFF:FFFF:FFFF:FFFF:FFFF or FD00::0- FDFE:FFFF:FFFF:FFFF:FFFF:FFFF	Protocol
1	70103	10 64 110 212		U
2				▼
3				▼
4				▼
5				▼
6				▼
7				▼
8				▼

8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Session Manager, and Aiphone IX-DBT Video Door Station.

1. Verify that IX-DBT has successfully registered with Session Manager. In System Manager, navigate to **Elements** → **Session Manager** → **System Status** → **User Registrations** to check the registration status as shown below.

The screenshot shows the Avaya Aura System Manager 10.1 interface. The top navigation bar includes the Avaya logo, user information (Users), and various menu items (Elements, Services, Widgets, Shortcuts). The main content area is titled "User Registrations" and contains a table of registered devices. The table has columns for Address, First Name, Last Name, Actual Location, IP Address, Policy, Shared Control, Simult. Devices, AST Device, and Registered status (Prim, Sec, 3rd, 4th, Surv, Visiting). The table shows five rows of registered devices, including IX-MV7-HBT, IX-EAT, IX-DVT, IX-DBT, and IX-DB.

	Details	Address	First Name	Last Name	Actual Location	IP Address	Policy	Shared Control	Simult. Devices	AST Device	Registered					
											Prim	Sec	3rd	4th	Surv	Visiting
<input type="checkbox"/>	Show	72009@avaya.com	IX-MV7-HBT	MasterStation	---	10.64.10.83	fixed	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>				
<input type="checkbox"/>	Show	72008@avaya.com	IX-EAT	VideoStation	---	10.64.10.82	fixed	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>				
<input type="checkbox"/>	Show	72007@avaya.com	IX-DVT	VideoStation	---	10.64.10.81	fixed	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>				
<input type="checkbox"/>	Show	72006@avaya.com	IX-DBT	VideoStation	---	10.64.10.80	fixed	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>				
<input type="checkbox"/>	Show	72005@avaya.com	IX-DB	VideoStation	---	10.64.10.79	fixed	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>				

2. Establish inbound and outbound video calls to IX-DBT with Avaya Workplace and/or Vantage endpoints and verify two-way audio and one-way video.

9. Conclusion

These Application Notes describe the administration steps required to integrate Aiphone IX Series 2 Video Door Stations (IX-DBT) with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. The Aiphone IX-DBT Video Door Station successfully registered with Avaya Aura® Session Manager as a SIP endpoint and audio and video calls were verified. All test cases executed passed with observations as noted in **Section 2.2**.

10. References

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

- [1] *Administering Avaya Aura® Communication Manager*, Release 10.1.x, Issue 5, March 2023, available at <http://support.avaya.com>.
- [2] *Administering Avaya Aura® System Manager*, Release 10.1.x, Issue 8, February 2023, available at <http://support.avaya.com>.
- [3] *Administering Avaya Aura® Session Manager*, Release 10.1.x, Issue 5, February 2023, available at <http://support.avaya.com>.
- [4] *Aiphone IX Door Stations Web Setting Manual*, Software version 6.00 or later, available from Aiphone.

©2023 Avaya Inc. All Rights Reserved.

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

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.