



## Avaya Solution & Interoperability Test Lab

---

# Application Notes for Med-Pat XLIP V2 with Avaya Aura® Session Manager R8.1 and Avaya Aura® Communication Manager R8.1 – Issue 1.0

### Abstract

These Application Notes describe the configuration steps required for Med-Pat XLIP V2 to interoperate with Avaya Aura® Session Manager R8.1 and Avaya Aura® Communication Manager R8.1. Med-Pat XLIP V2 is a one-piece SIP hospital phone that can register with Avaya Aura® Session Manager as a SIP endpoint in support of voice communications.

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

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

# 1. Introduction

These Application Notes describe the configuration steps required for Med-Pat XLIP V2 to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager. Med-Pat XLIP V2 is a one-piece SIP telephone that can register with Avaya Aura® Session Manager as a SIP endpoint. Med-Pat XLIP V2 (XLIP) is typically deployed in hospital patient rooms. Med-Pat has noted that the handset does not yet support TLS and media encryption so the tests are limited to the TCP protocol.

## 2. General Test Approach and Test Results

The general test approach was to place calls to and from XLIP and exercise basic telephone operations. The main objectives were to verify the following:

- Registration
- Codecs (G.711, G.722, and G.729)
- Inbound calls
- Outbound calls
- Call termination (origination/destination)
- Avaya Features using FAC (Call Pickup, Call Forward, and Find Me)
- Message Waiting Indicator (MWI)
- Voicemail
- Serviceability

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, XLIP did not include any encryption features as requested by Med-Pat.

## 2.1. Interoperability Compliance Testing

The interoperability compliance test included features and serviceability. The focus of interoperability compliance testing was primarily on verifying call establishment on XLIP. XLIP operations such as inbound calls, outbound calls, hold/resume, transfer, conference, Facility Access Codes, and its interactions with Session Manager, Communication Manager, and other Avaya SIP, and H.323 phones were verified. The serviceability testing introduced failure scenarios to see if XLIP can recover from loss of ethernet connectivity by cable disconnection while a call is active.

## 2.2. Test Results

All test cases were executed. The following observations were noted during compliance testing:

- The following features are not supported by XLIP:
  - Call Mute, Hold, and Resume
  - Call Transfer
  - Conference Call
  - Long Hold Recall Timer
  - Call Park
  - MWI
- When the call is terminated at the far-end, a busy tone is heard on XLIP handset for three to five seconds. As per the signaling, the call terminates properly. Med-Pat indicates this is expected and acceptable.
- XLIP does not indicate a message is waiting via stutter tone. Med-Pat indicates this is not currently enabled and will be added in a future release.
- Using '#' as a leading digit for Feature access codes does not work. The workaround is to use another digit such as '\*'.

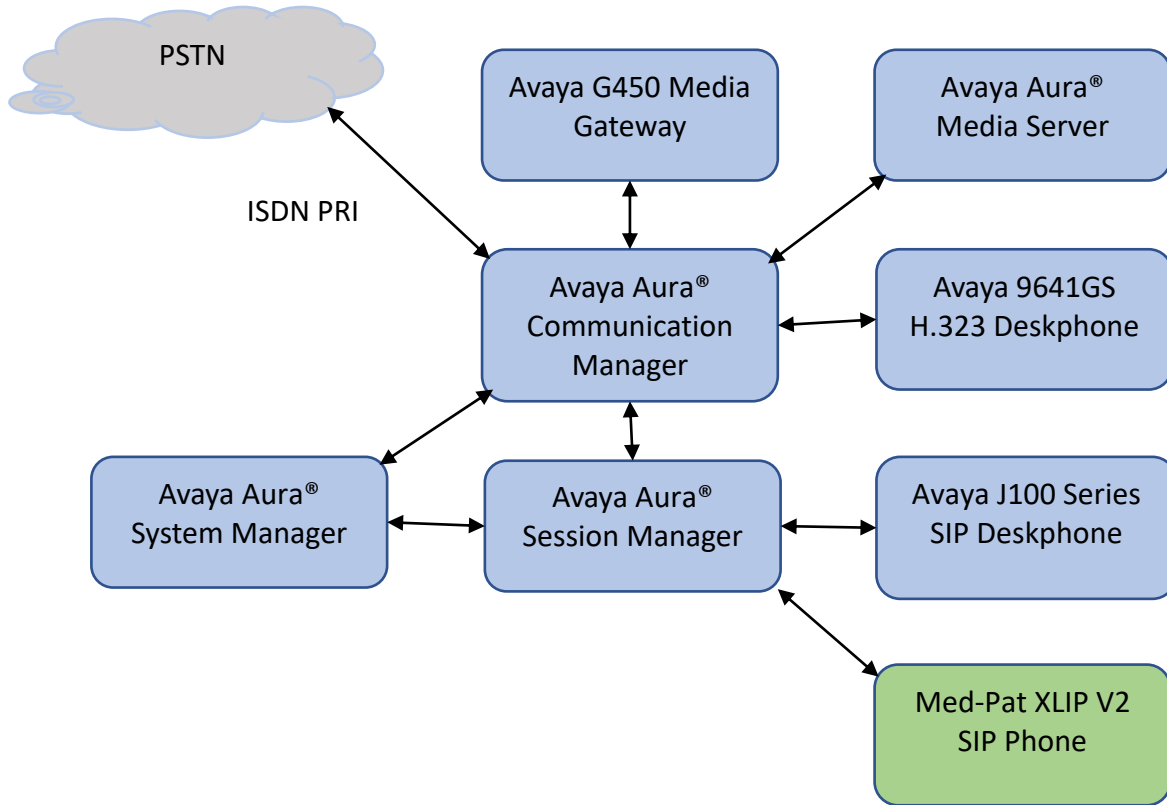
## 2.3. Support

For Technical Support:

- Med-Pat XLIP V2 please visit <http://www.med-pat.com>
- Telephone: 800 626-0410

### 3. Reference Configuration

Once XLIP registers as a SIP endpoint with Session Manager, it can place and receive voice calls with various supported features as listed above in **Section 2.1**. The reference configuration used for the compliance test is shown in **Figure 1** below.



**Figure 1: Med-Pat XLIP V2 with Avaya Aura® Session Manager and Avaya Aura® Communication Manager**

## 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 running on a virtual server	8.1.3.0.1.890.26685
Avaya Aura® System Manager running on a virtual Machine	8.1.3.0.813014
Avaya Aura® Session Manager running on a virtual server	8.1.3.0.813014
Avaya Aura® Media Server running on a virtual server	8.0.0 169
Avaya G450 Media Gateway	41.34.1
Avaya 9641GS Deskphone (H.323)	R6_8_5_11-050321
Avaya J100 Series Deskphone (SIP)	R4_0_9_0-040821
Med-Pat XLIP V2	V0.0.23

## 5. Configure Avaya Aura® Communication Manager

This section describes the steps for configuring Communication Manager. The procedures include the following areas:

- Verify the Communication Manager OPS (Off-PBX station) Licensed Capacity
- Administer IP Network Region
- Administer IP Codec Set

Use the System Access Terminal (SAT) to configure Communication Manager and log in with the appropriate credentials. The configuration steps illustrate field values changed for this reference configuration. Default values were used for all other fields.

**Note:** It is assumed that basic configuration of the Communication Manager has already been completed, such as the SIP trunk to Session Manager. The SIP station configuration for XLIP is configured through System Manager in **Section 6.2**.

### 5.1. Verify Communication Manager OPS Licensed Capacity

Using the SAT, verify that the Off-PBX Stations (OPS) and SIP Trunks features are 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    111
Maximum Stations: 36000         86
Maximum XMOBILE Stations: 36000    0
Maximum Off-PBX Telephones - EC500: 41000    0
Maximum Off-PBX Telephones - OPS: 41000    51
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 Network Region

This IP network region is for the signaling group associated with the SIP trunk between Session Manager and Communication Manager. This form also specifies the **IP Codec Set** to be used for calls routed over the SIP trunk to Session Manager. Verify the following values:

- **Authoritative Domain:** The applicable domain (e.g., **avaya.com**)
- **Codec Set:** The codec set number from **Section 5.3**

By default, **IP-IP Direct Audio** (shuffling) is enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in Avaya G450 Media Gateway or Avaya Media Server.

```
change ip-network-region 1                                     Page 1 of 20
                                                           IP NETWORK REGION
  Region: 1
Location: 1          Authoritative Domain: avaya.com
  Name: Main
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: 3329
DIFFSERV/TOS PARAMETERS
  Call Control PHB Value: 46
  Audio PHB Value: 46
  Video PHB Value: 26
802.1P/Q PARAMETERS
  Call Control 802.1p Priority: 6
  Audio 802.1p Priority: 6
  Video 802.1p Priority: 5          AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS          RSVP Enabled? n
  H.323 Link Bounce Recovery? y
  Idle Traffic Interval (sec): 20
  Keep-Alive Interval (sec): 5
  Keep-Alive Count: 5
```

### 5.3. Administer IP Codec Set

In the **IP Codec Set** form, select the audio codec type supported for calls routed over the SIP trunk to XLIP. The form is accessed via the **change ip-codec-set 1** command. Note that IP codec set **1** is specified in **IP Network Region 1** shown above. The form shows the list of codecs tested. Enter values for the following:

- **Audio Codec:** The audio codec tested
- **Media Encryption:** **none** as an option to assure TCP and no encryption is available.

```
display 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: G.711A      n              2              20
3: G.722       n              2              20
4: G.729       n              2              20
5:
6:
7:
Media Encryption          Encrypted SRTCP: best-effort
1:1-srtp-aescm128-hmac80
2:2-srtp-aescm128-hmac32
3:none
4:
5:
```



## 6. Configure Avaya Aura® Session Manager

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

- Launch System Manager
- Administer SIP Users

**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 XLIP.

### 6.1. Launch System Manager

Access Session Manager Administration web interface by entering **http://<ip-address>/SMGR** in a web browser, where <ip-address> is the IP address of System Manager. 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:** Internet Explorer 11.x or Firefox 65.0, 66.0 and 67.0.

## 6.2. Administer SIP Users

XLIP is administered as a SIP user on Session Manager by the following steps. This configuration is automatically synchronized with Communication Manager. In Session Manager, select **Users** → **User Management** → **Manage Users** to display the **User Management** screen (not shown). Click + **New** to add a user.

### 6.2.1. Identity

Enter values for the following required attributes for a new SIP user in the **New User Profile** screen:

- **Last Name:** Enter the last name of the user, e.g., **MedPat**
- **First Name:** Enter the first name of the user, e.g., **XLIP**
- **Login Name:** Enter <extension>@<sip domain> of the user (e.g., **70128@avaya.com**)
- **Password:** Enter an appropriate password
- **Confirm Password:** Re-enter the password from above

The screenshot displays the 'User Profile | Add' form in the Avaya Aura System Manager 8.1 interface. The form is organized into several sections:

- User Provisioning Rule:** A dropdown menu.
- Basic Info:** A section containing several input fields:
  - Last Name:** MedPat
  - First Name:** XLIP
  - Login Name:** 70128@avaya.com
  - Description:** Description Of User
  - Password:** Masked with dots
  - Confirm Password:** Empty field
  - Last Name (in Latin alphabet characters):** MedPat
  - First Name (in Latin alphabet characters):** XLIP
  - Middle Name:** Middle Name Of User
  - Email Address:** Email Address Of User
  - User Type:** Basic
  - Localized Display Name:** Localized Display Name Of

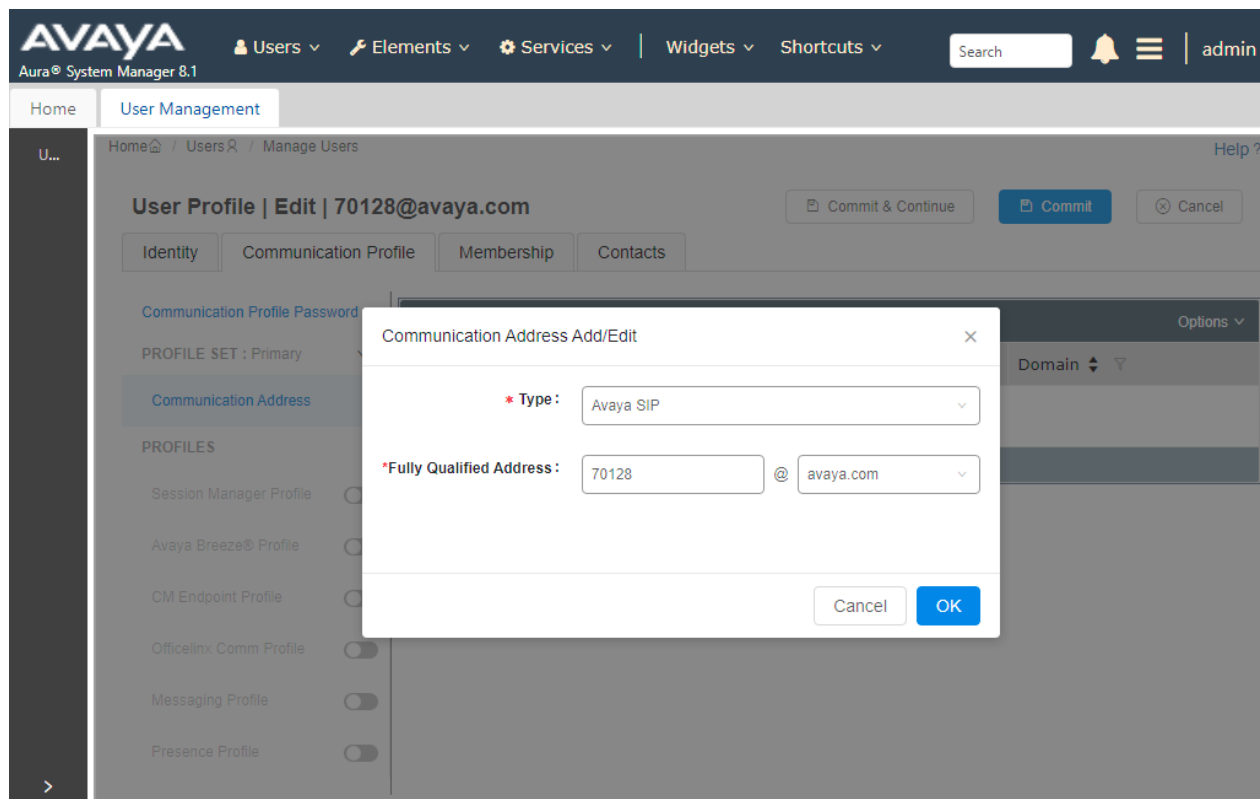
Press **Commit & Continue** after making entries or selections.

## 6.2.2. Communication Address

Select **Communication Address** in the left list and click + **New** (not shown).

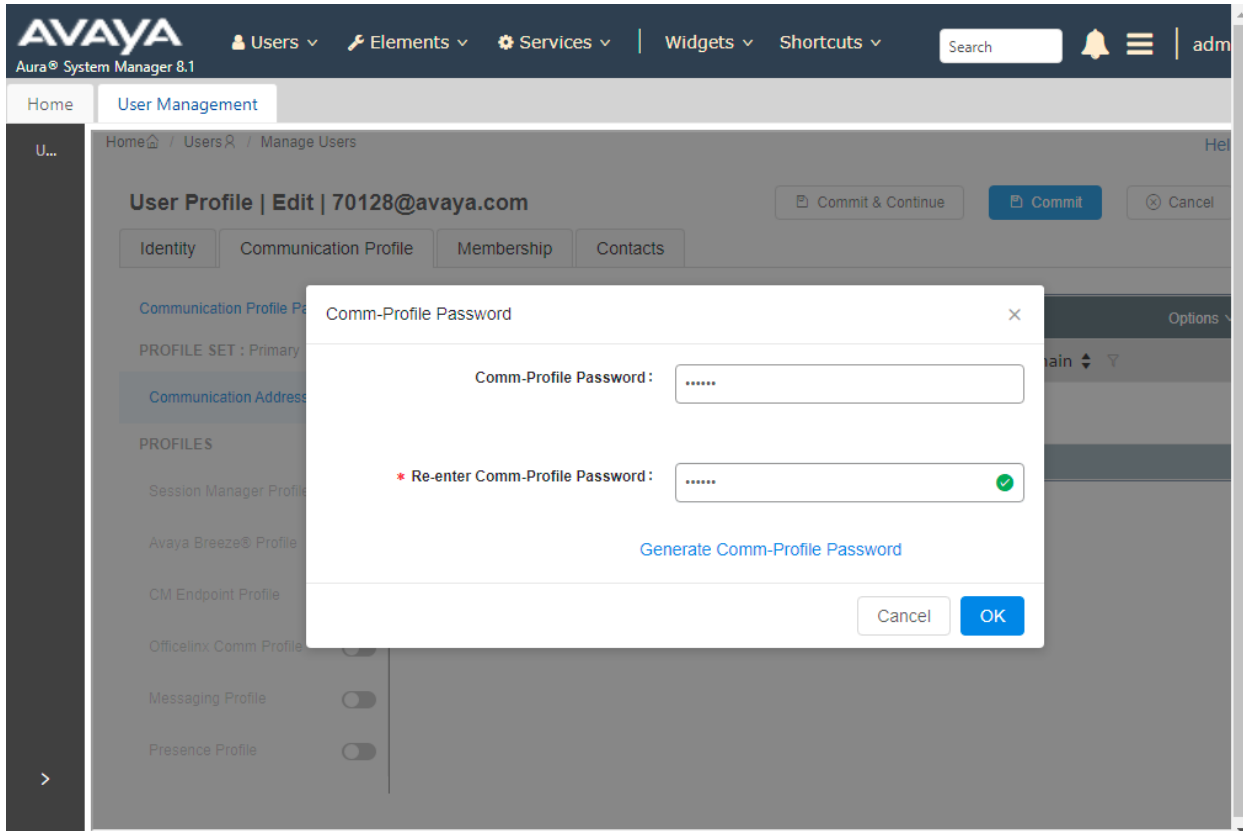
Enter the following attributes for the **Communication Address**:

- **Type:** Select **Avaya SIP** from the drop-down list
- **Fully Qualified Address:** Enter the extension number (e.g., **70128**)
- **Domain:** Enter the domain (e.g., **avaya.com**)



### 6.2.3. Communication Profile

Click the **Communication Profile** tab and in the **Comm-Profile Password** and **Re-enter Comm-Profile Password** fields, enter a numeric password. This will be used to register the device during login. Click **OK**.



## 6.2.4. Session Manager Profile

Click on the **Session Manager Profile** slide button. For **Primary Session Manager**, **Origination Sequence**, **Termination Sequence**, and **Home Location** (not shown), select the values corresponding to the applicable Session Manager and Communication Manager. 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, a search bar, and user information (admin). The main content area is titled "User Management" and shows the "Session Manager Profile" configuration page. The left sidebar lists various profiles, with "Session Manager Profile" selected and its toggle switch turned on. The main configuration area is divided into two sections: "SIP Registration" and "Application Sequences".

**SIP Registration**

- Primary Session Manager:** sm81
- Secondary Session Manager:** Start typing...
- Survivability Server:** Start typing...
- Max. Simultaneous Devices:** 3
- Block New Registration When Maximum Registrations Active?**

**Application Sequences**

- Origination Sequence:** cm81
- Termination Sequence:** cm81

## 6.2.5. CM Endpoint Profile

Click on the **CM Endpoint Profile** slide button. Fill in the following fields:

- **System:** Select the relevant Communication Manager SIP Entity (e.g., **cm81**)
- **Profile Type:** Select **Endpoint**
- **Template:** Select **9641\_DEFAULT\_CM\_8\_1** for **XLIP**
- **Extension:** Enter the extension number (e.g., **70128**)

Click on **Endpoint Editor** in the Extension field to edit Communication Manager settings if desired. Click **Commit**.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The main content area is titled 'User Profile | Edit | 70128@avaya.com'. The 'Communication Profile' tab is selected, and the 'CM Endpoint Profile' is turned on. The form contains the following fields and values:

- System:** cm81
- Profile Type:** Endpoint
- Extension:** 70128
- Template:** 9641\_DEFAULT\_CM\_8\_1
- Security Code:** Enter Security Code
- Voice Mail Number:** (empty)
- Calculate Route Pattern:**
- SIP URI:** Select
- Set Type:** 9641
- Port:** IP
- Preferred Handle:** Select
- Sip Trunk:** (empty)
- Enhanced Callr-Info Display for 1-line phones:**
- Delete on Unassign from User or on Delete User:**
- Override Endpoint Name and Localized Name:**

Buttons at the top right include 'Commit & Continue', 'Commit', and 'Cancel'.

## 7. Configure Med-Pat XLIP

This section provides the steps for configuring XLIP. The steps to configure XLIP to integrate with Communication manager are as follows:

- Configure IP Address of XLIP
- Launch Web Interface
- Configure SIP account
- Modify Codec Settings

### 7.1. Configure IP Address of XLIP

XLIP is configured for DHCP as a factory default. The following steps provide network connectivity and determine the phone IP address for use in launching administration detailed in **Section 7.2**:

- Connect the WAN port of XLIP to a Power over Ethernet (PoE) switch
- Determine the assigned IP address using an IP scanner or a keycode that is input to XLIP. In this case, enter the code **47\*#** (e.g., '**IP\*#**') to get the IP address read out

**Note:** Additional keycodes that may be useful during setup are:

- **47\*#** IP address
- **48\*#** Firmware Version
- **49\*#** Factory Reset
- **50\*#** VLAN Tag On/Off (Only on or off)
- **51\*#** DHCP/Static IP Mode
- **52\*#** Last 4 Octets of MAC Readback

### 7.2. Launch Web Interface

- Invoke the web interface using the IP address from **Section 7.1** using the URL **http://<IP address>**.
- In the login dialog, enter an appropriate password



The screenshot shows the web interface for Med-Pat XLIP. At the top, there is a logo with a caduceus and the text 'MED PAT'. Below the logo, the word 'Password' is displayed next to a text input field. To the right of the input field is a 'Login' button. At the bottom of the page, there is a copyright notice: 'Copyright © 2012 - 2021 Vogtec Inc. All Rights Reserved.'

### 7.3. Configure SIP Account

The SIP account used to register with Session Manager is configured here. From the Web Interface, Select **Accounts** from left pane. Click on the **Enable Account** checkbox. The account settings become visible. Input the following values:

- **Register Server:** The Session Manager domain (e.g., **avaya.com**)
- **Account Name:** Any appropriate descriptive string (e.g., **70128**)
- **Proxy Server Address:** Session Manager IP address
- **Authorization Name:** SIP user ID as created in **Section 6.2.1** (e.g., **70128**)
- **Password:** SIP user password used in **Section 6.2.3**
- **User ID:** User extension used for SIP user created in **Section 6.2** (e.g., **70128**)
- **Display Name:** Any appropriate descriptive string (e.g., **70128**)

Click **Apply**.

The screenshot shows the Avaya Session Manager Web Interface. The top navigation bar includes the MED-PAT logo and a LOGOUT button. Below the navigation bar, there are tabs for SIP 1 and SIP 2. The left sidebar contains a menu with options: Status, Accounts (selected), Phone, Network, Maintenance, and Directory. The main content area displays the configuration for the selected SIP account (SIP 2). The 'Enable Account' checkbox is checked. The 'General Settings' section includes the following fields:

Field	Value	Field	Value
Status	registered	Enable Register	<input checked="" type="checkbox"/>
Register Server	avaya.com	Account Name	70128
Server Port	5060	Proxy Server Address	10.64.110.212
Authorization Name	70128	Proxy Server Port	5060
Password	*****	Backup Proxy Server Address	
User ID	70128	Backup Proxy Server Port	5060
Display Name	70128	DHCP Option 120	<input type="checkbox"/>

Below the General Settings, there are sections for 'Codecs Settings>>', 'Call settings>>', and 'Advanced Settings>>'. An 'Apply' button is located at the bottom right of the configuration area.



## 7.4. Modify Codec Settings

Continuing from the **Accounts** pane, select **Codecs Settings>>**. Modify the priority order and codecs as desired and click **Apply**.

SIP 1			
Enable Account <input checked="" type="checkbox"/>			
General Settings>>			
Codecs Settings>>			
Choice 1	PCMU	Choice 2	PCMA
Choice 3	G.722	Choice 4	G.729
Choice 5	G.723	Choice 6	G.726
DTMF Type	RFC2833	G722 Timestamps	G722.1(160/20)
G723 Bit Rate	6.3kb/s	G729AB Packaging Time	20ms
Call settings>>			
Advanced Settings>>			
<input type="button" value="Apply"/>			

## 8. Verification Steps

The proper configuration of XLIP with Avaya Session Manager and Avaya Communication Manager is verified by the following.

### 8.1. View Session Manager Status

Verify XLIP has successfully registered with Session Manager. In System Manager, navigate to **Elements** → **Session Manager** → **System Status** → **User Registrations** to check the registration status.

- Verify that XLIP (here **70128**) is registered with Session Manager by noting the registered users include **70128**.

The screenshot displays the Avaya Aura System Manager 8.1 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The main content area is titled 'User Registrations' and shows a table of 44 items. The table has columns for 'Details', 'Address', 'First Name', 'Last Name', 'Actual Location', 'IP Address', 'Remote Office', 'Shared Control', 'Simult. Devices', 'AST Device', and 'Registered'. The 'Registered' column is further divided into 'Prim', 'Sec', 'Surv', and 'Visiting'. The user '70128@avaya.com' is listed with IP address '192.168.5.6' and is registered as 'Prim'.

	Details	Address	First Name	Last Name	Actual Location	IP Address	Remote Office	Shared Control	Simult. Devices	AST Device	Registered			
											Prim	Sec	Surv	Visiting
<input type="checkbox"/>	<a href="#">Show</a>	70128@avaya.com	XLIP	MedPat	---	192.168.5.6	<input type="checkbox"/>	<input type="checkbox"/>	1/3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### 8.2. Call Verification

Verify that basic calls can be made from and to XLIP and another telephone registered to Session Manager.

## 9. Conclusion

These Application Notes describe the configuration steps required for Med-Pat XLIP V2 SIP one-piece telephone to successfully interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

## 10. Additional References

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

Product documentation for Avaya products may be found at <http://support.avaya.com>.

1. *Administering Avaya Aura<sup>®</sup> Communication Manager*, Issue 10, Release 8.1.x, March 2021.
2. *Administering Avaya Aura<sup>®</sup> Session Manager*, Issue 8, Release 8.1.x, February 2021.
3. *Administering Avaya Aura<sup>®</sup> System Manager*, Issue 11, Release 8.1.x, April 2021.

Product documentation for Med-Pat products may be found at <http://www.med-pat.com>.

4. *VOIP Phone Model XL-IP User Manual*.

**©2021 Avaya Inc. All Rights Reserved.**

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

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