Avaya Solution & Interoperability Test Lab

# Application Notes for AtlasIED IPX Series with Avaya Aura® Session Manager and Avaya Aura® Communication Manager – Issue 1.0

## Abstract

These Application Notes describe the configuration steps required for AtlasIED IPX Series to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager.

AtlasIED IPX Series is a family of VoIP speakers that can deliver audio and visual notifications with built in microphone and optionable LCD screen. In the compliance testing, AtlasIED IPX IP-SM registered to 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 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 AtlasIED IPX Series (IPX) to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager.

IPX is a family of VoIP speakers that can deliver audio and visual notifications with built in microphone and optionable LCD screen. In the compliance testing, one IPX was used and registered to Session Manager as a SIP endpoint.

The compliance testing focused on the audio integration of IPX with Session Manager. The model of IPX used in the testing was IP-SM, which did not include an LCD screen nor the ability to make outbound call to a pre-configured destination. As such, the test scope did not include display of caller ANI nor origination of outbound call from IPX.

In addition, the visual notification feature for IPX models with LCD screens requires separate integration with a third-party application. As such, visual notification is also outside the scope of this compliance test.

## 2. General Test Approach and Test Results

The feature test cases were performed manually. Inbound calls to IPX were manually originated from PSTN, Avaya SIP, and/or Avaya H.323 endpoints. All call controls such as hold and drop were performed from the originator of the inbound call to IPX.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to IPX.

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

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

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

For the testing associated with these Application Notes, the interface between Session Manager and IPX did not include use of any specific encryption features as requested by AtlasIED.

## 2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing included registration, hold/resume, drop, media shuffling/non-shuffling, G.711, G.722, codec negotiation, transfer, conference, and long duration.

The serviceability testing focused on verifying the ability of IPX to recover from adverse conditions, such as disconnecting and reconnecting the Ethernet connection to IPX.

## 2.2. Test Results

All test cases were executed. The following were observations on IPX from the compliance testing.

- After successful registration with Session Manager, the registration status on the IPX web interface continued to reflect “Not Registered”. This is a known problem with fix to be released in an upcoming release.

- Whenever IP-SM was placed on hold, IP-SM played silence instead of the hold treatment received from Communication Manager. This behavior included scenarios when IP-SM was placed on consultative hold as part of transfer and conference.

## 2.3. Support

Technical support on IPX can be obtained through the following:

- **Phone:** +1 (800) 876-3333, +1 (502) 267-7436
- **Email:** support@atlasied.com
- **Web :** http://atlasied.com/customer_service

# 3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**, with the domain name used in the testing being “dr220.com”.

The configuration of Session Manager is performed via the web interface of System Manager. The detailed administration of basic connectivity between Communication Manager, System Manager, and Session Manager are not the focus of these Application Notes and will not be described.

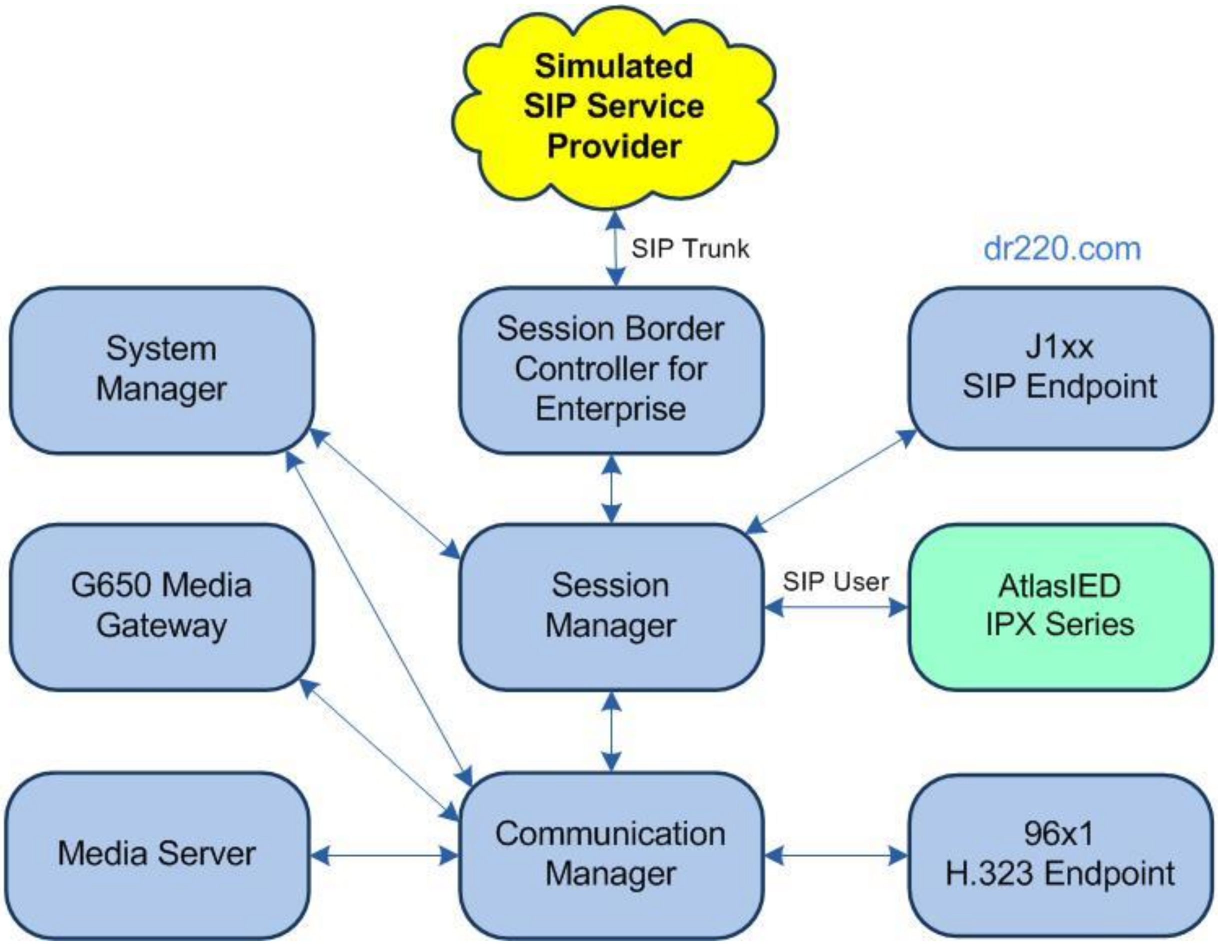


**Figure 1: Compliance Testing Configuration**

## 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 in<br>Virtual Environment | 8.1.1<br>(8.1.0.1.1.890.25763) |
| Avaya G650 Media Gateway | NA |
| Avaya Aura® Media Server in<br>Virtual Environment | 8.0.1.121 |
| Avaya Aura® Session Manager in<br>Virtual Environment | 8.1.1<br>(8.1.1.0.811021) |
| Avaya Aura® System Manager in<br>Virtual Environment | 8.1.1<br>(8.1.1.0.0310912) |
| Avaya 9611G IP Deskphone (H.323) | 6.8202 |
| Avaya J169 IP Deskphone (SIP) | 4.0.2.1.3 |
| AtlasIED IPX Series IP-SM | 1.2.0 |

# 5. Configure Avaya Aura® Communication Manager

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

- Verify license
- Administer IP codec set

## 5.1. Verify License

Log in to the System Access Terminal to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes.

Use the “display system-parameters customer-options” command to verify that there is sufficient license for SIP stations by comparing the **Maximum Off-PBX Telephones – OPS** field value with the corresponding value in the **USED** column.

```
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:  81000    205
                                  Maximum Stations:  41000     20
                          Maximum XMOBILE Stations:  41000      0
                Maximum Off-PBX Telephones - EC500:  41000      0
                Maximum Off-PBX Telephones -   OPS:  41000      2
                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
```

## 5.2. Administer Codec Set

Use the “change ip-codec-set n” command, where “n” is an existing codec set number used for integration with IPX.

For **Audio Codec**, enter the relevant codec, in this case “G.711MU” and “G.722-64K”. For **Media Encryption**, make certain that “none” is included. In the compliance testing, this codec set was used by IPX and by the Avaya endpoints.

```
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: G.722-64K                   2        20
 3:
 4:
 5:
 6:
 7:

     Media Encryption                  Encrypted SRTCP: best-effort
 1: 1-srtp-aescm128-hmac80
 2: aes
 3: none
 4:
```

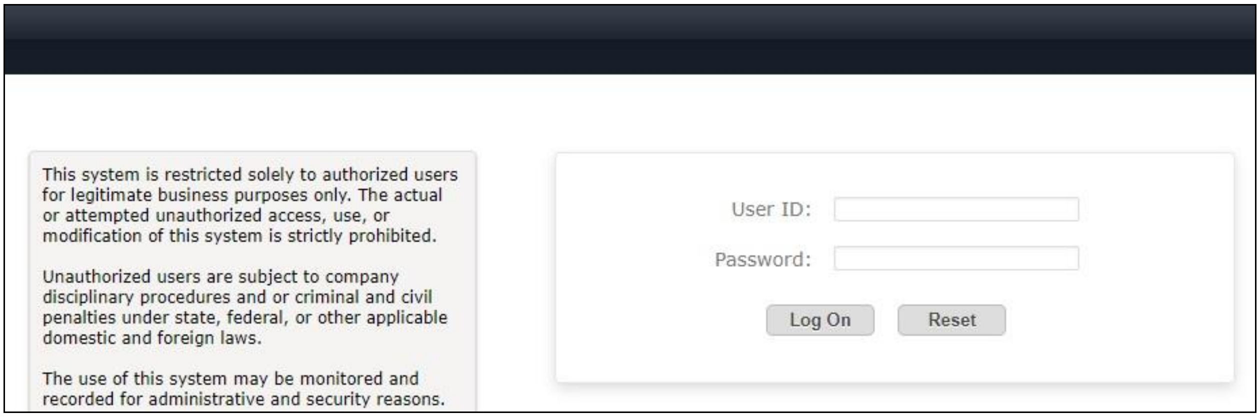
# 6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager, which is performed via the web interface of System Manager. The procedures include the following areas:

- Launch System Manager
- Administer SIP users
- Administer Session Manager entity

## 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 System Manager. Log in using the appropriate credentials.



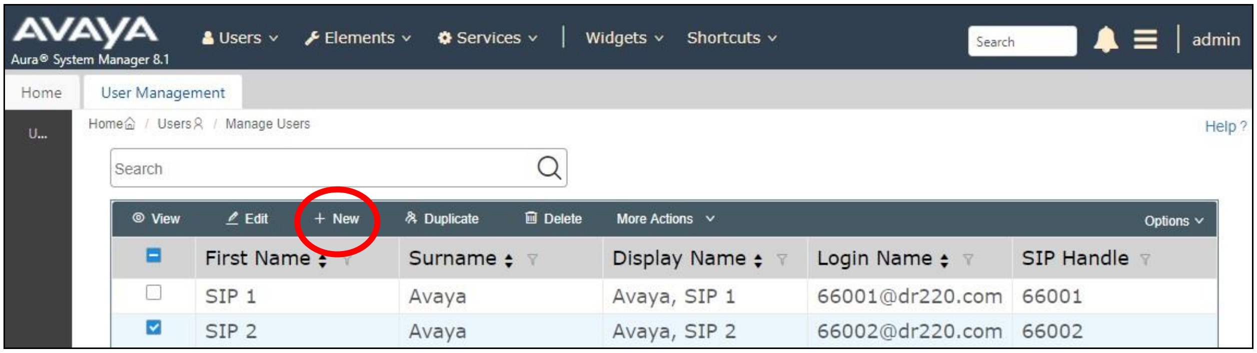
This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

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.

## 6.2. Administer SIP Users

In the subsequent screen, select **Users → User Management → Manage Users** from the top menu to display the **User Management** tab shown below. Click **New** to add a user.

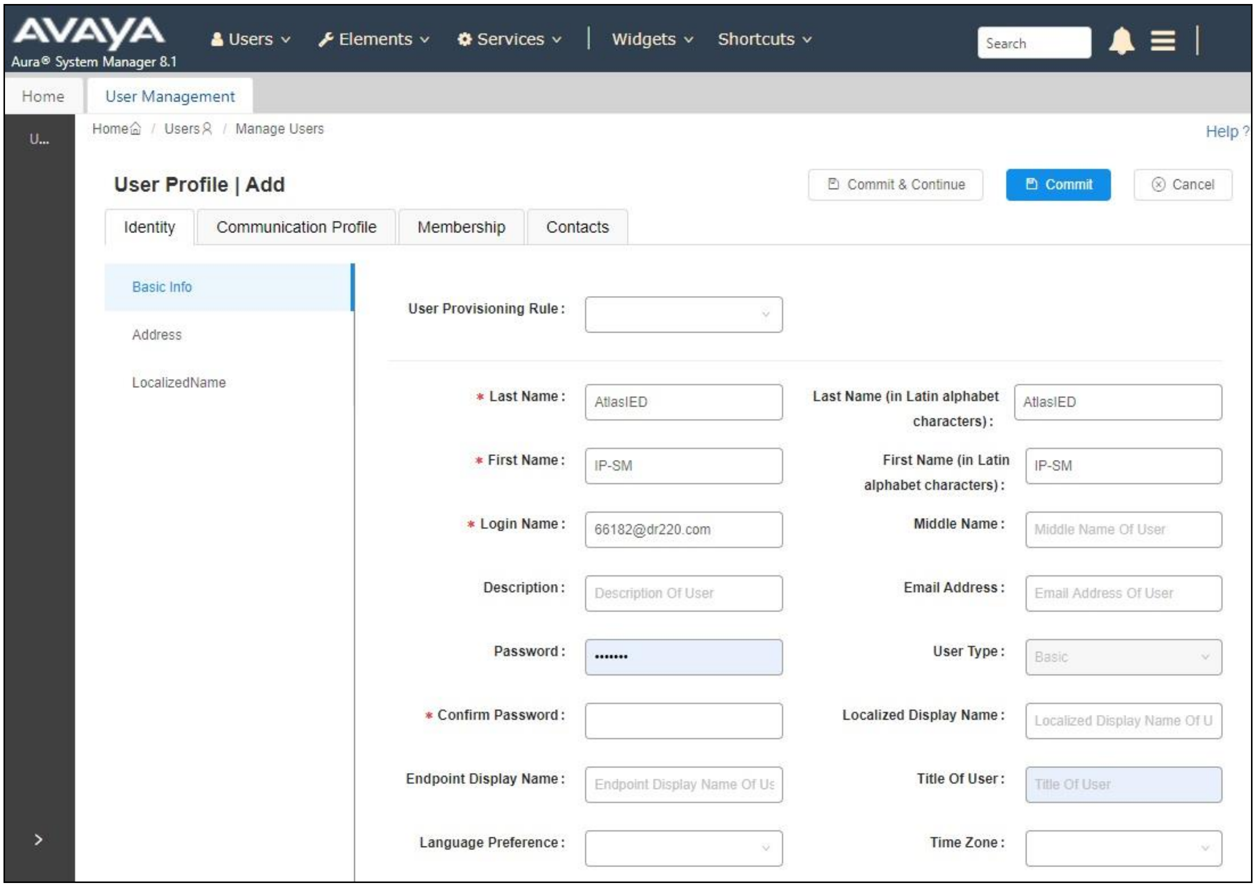


| | First Name | Surname | Display Name | Login Name | SIP Handle |
|---|---|---|---|---|---|
| □ | SIP 1 | Avaya | Avaya, SIP 1 | 66001@dr220.com | 66001 |
| ☑ | SIP 2 | Avaya | Avaya, SIP 2 | 66002@dr220.com | 66002 |

### 6.2.1. Identity

The **User Profile | Add** screen is displayed.  Enter desired **Last Name** and **First Name**.

For **Login Name**, enter “x@y”, where “x” is an available user extension and “y” is the applicable domain name from **Section 3**.  Retain the default values in the remaining fields.



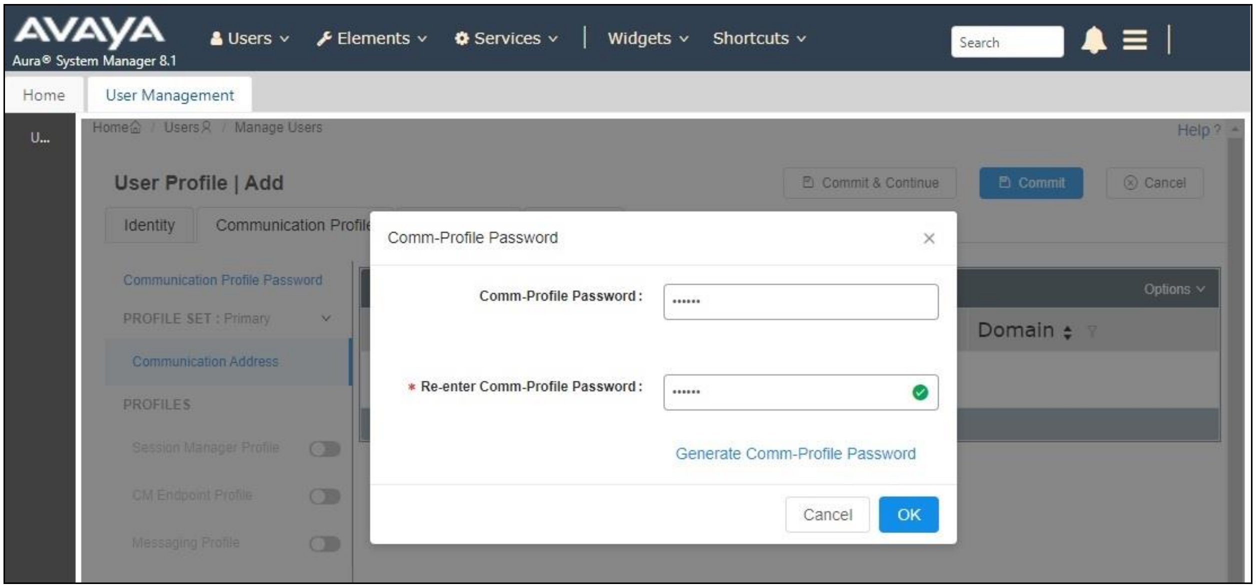
User Profile | Add

| | | | |
|---|---|---|---|
| User Provisioning Rule : | | | |
| * Last Name : | AtlasIED | Last Name (in Latin alphabet characters) : | AtlasIED |
| * First Name : | IP-SM | First Name (in Latin alphabet characters) : | IP-SM |
| * Login Name : | 66182@dr220.com | Middle Name : | Middle Name Of User |
| Description : | Description Of User | Email Address : | Email Address Of User |
| Password : | ••••••• | User Type : | Basic |
| * Confirm Password : | | Localized Display Name : | Localized Display Name Of U |
| Endpoint Display Name : | Endpoint Display Name Of Us | Title Of User : | Title Of User |
| Language Preference : | | Time Zone : | |

### 6.2.2. Communication Profile

Select the **Communication Profile** tab, followed by **Communication Profile Password** to display the **Comm-Profile Password** pop-up box.

For **Comm-Profile Password** and **Re-enter Comm-Profile Password**, enter the desired password for the SIP user to use for registration.



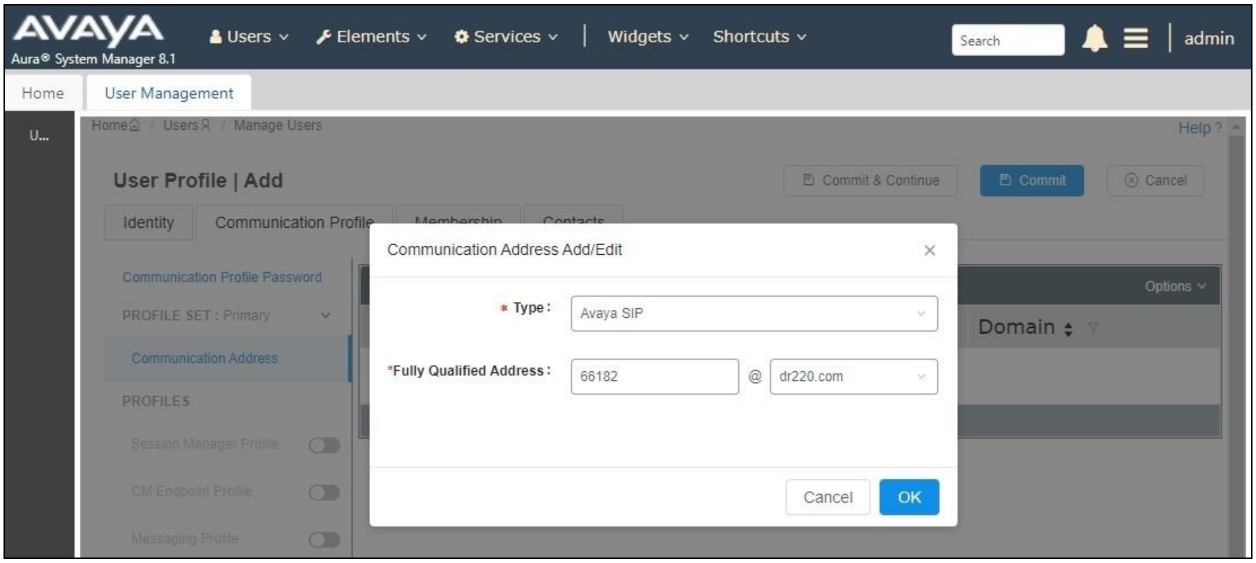
Comm-Profile Password

Comm-Profile Password : ••••••

* Re-enter Comm-Profile Password : ••••••

Select **Communication Address** from the left, followed by **New** to display the **Communication Address Add/Edit** pop-up box.

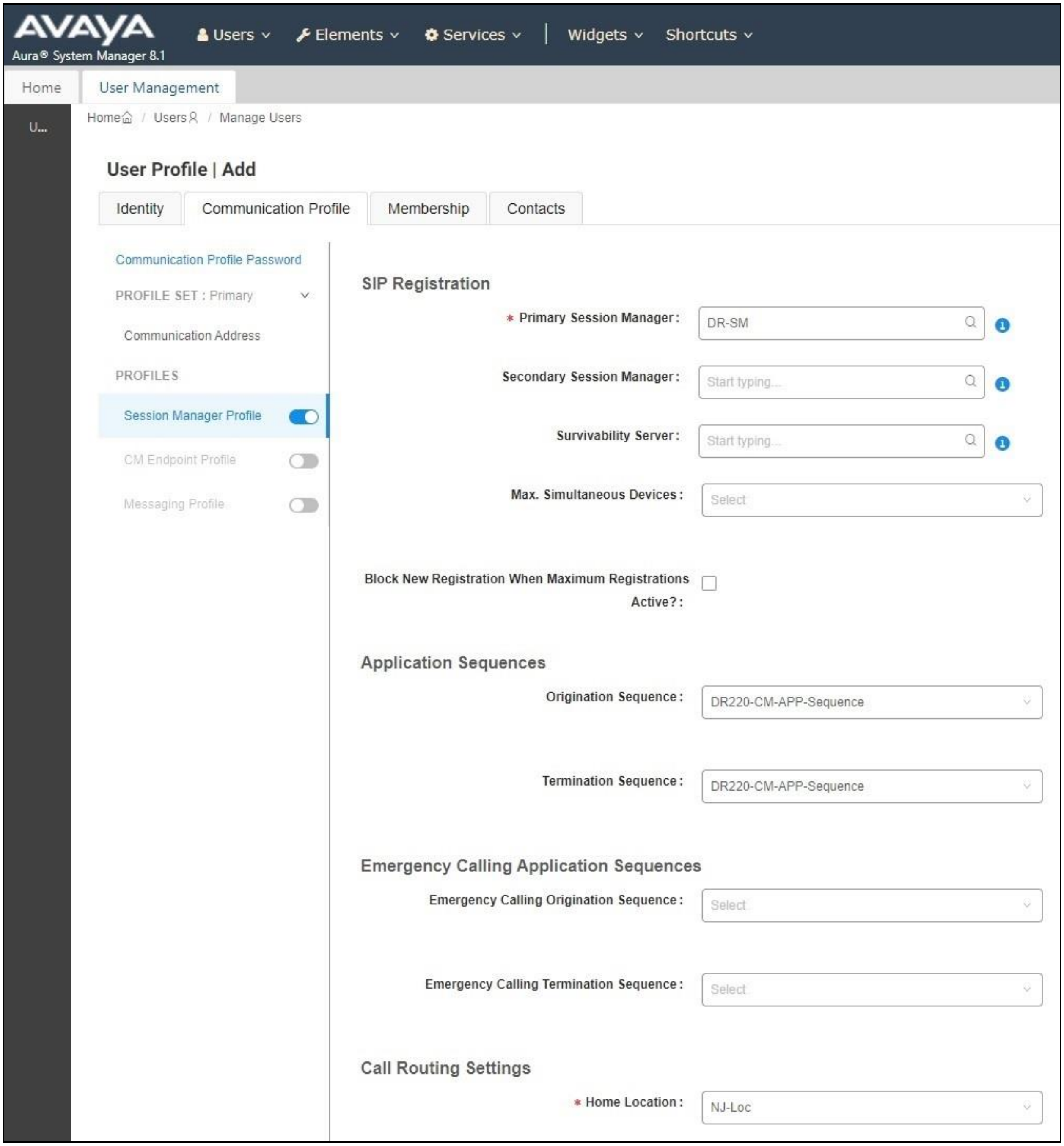
For **Type**, select "Avaya SIP". For **Fully Qualified Address**, enter and select the SIP user extension and domain name to match the login name from **Section 6.2.1**.



* Type : Avaya SIP

*Fully Qualified Address : 66182 @ dr220.com

Select **Session Manager Profile** from the left. For **Primary Session Manager**, **Origination Sequence**, **Termination Sequence**, and **Home Location**, select values that correspond to the applicable Session Manager and Communication Manager as shown below. Retain the default values in the remaining fields.



User Profile | Add

SIP Registration

* Primary Session Manager : DR-SM

Secondary Session Manager : Start typing...

Survivability Server : Start typing...

Max. Simultaneous Devices : Select

Block New Registration When Maximum Registrations Active? : □

Application Sequences

Origination Sequence : DR220-CM-APP-Sequence

Termination Sequence : DR220-CM-APP-Sequence

Emergency Calling Application Sequences

Emergency Calling Origination Sequence : Select

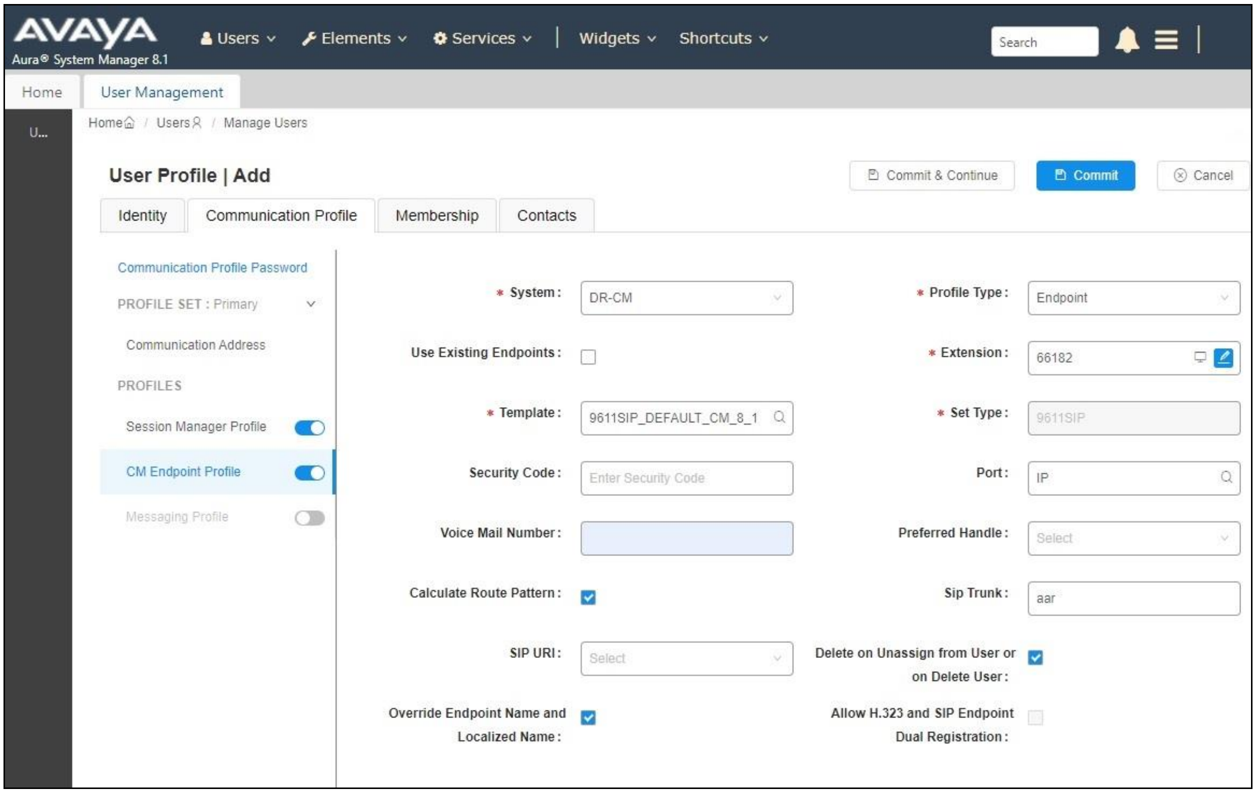
Emergency Calling Termination Sequence : Select

Call Routing Settings

* Home Location : NJ-Loc

Select **CM Endpoint Profile** from the left. For **System**, select value that corresponds to the applicable Communication Manager. For **Template**, select “9611SIP_DEFAULT_CM_8_1”. For **Extension**, enter the SIP user extension from **Section 6.2.1**. Retain the default values in the remaining fields.

Repeat **Section 6.2** as necessary to add a SIP user for each IPX. In the compliance testing, one SIP user with extension “66182” was created.

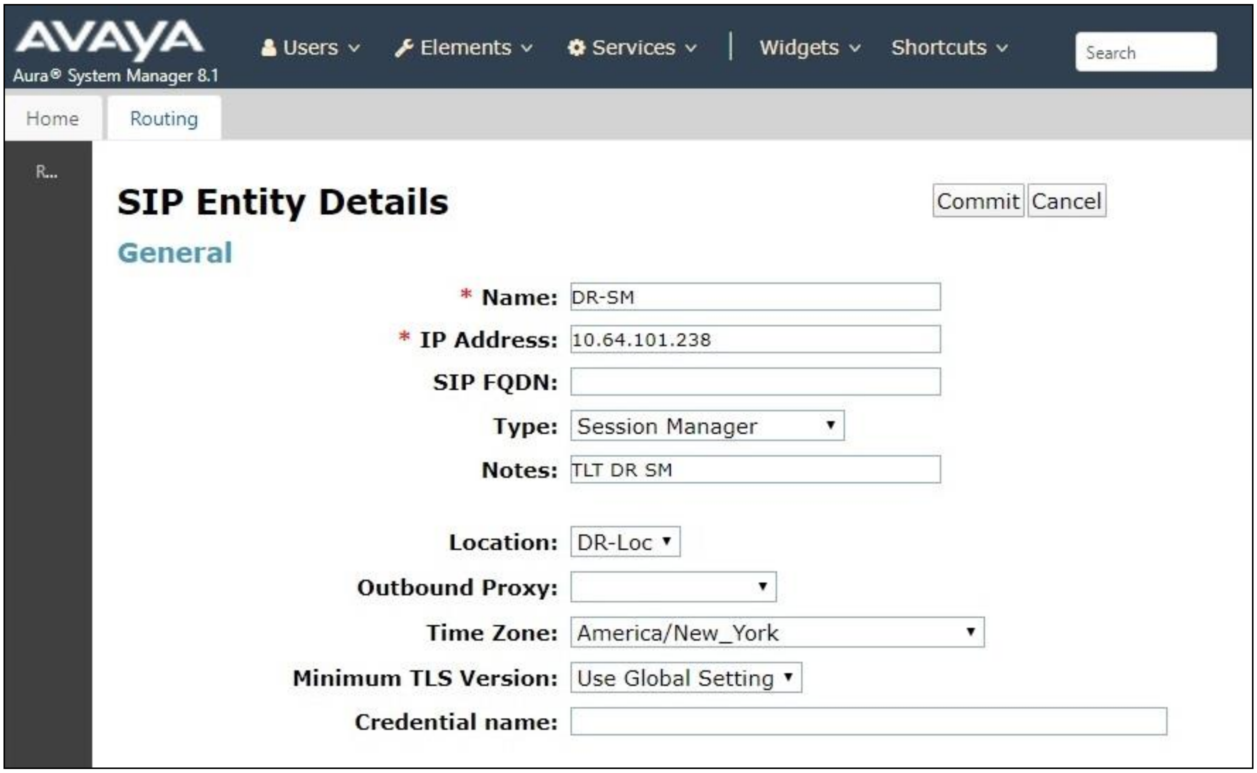


User Profile | Add

| | | | |
|---|---|---|---|
| * System : | DR-CM | * Profile Type : | Endpoint |
| Use Existing Endpoints : | □ | * Extension : | 66182 |
| * Template : | 9611SIP_DEFAULT_CM_8_1 | * Set Type : | 9611SIP |
| Security Code : | Enter Security Code | Port : | IP |
| Voice Mail Number : | | Preferred Handle : | Select |
| Calculate Route Pattern : | ☑ | Sip Trunk : | aar |
| SIP URI : | Select | Delete on Unassign from User or on Delete User : | ☑ |
| Override Endpoint Name and Localized Name : | ☑ | Allow H.323 and SIP Endpoint Dual Registration : | □ |

## 6.3. Administer Session Manager Entity

Select **Elements → Routing → SIP Entities** from the top menu to display the **Routing** tab, followed by the applicable SIP entity for Session Manager from the left pane (not shown), in this case “DR-SM7”.  The **SIP Entity Details** screen is displayed.

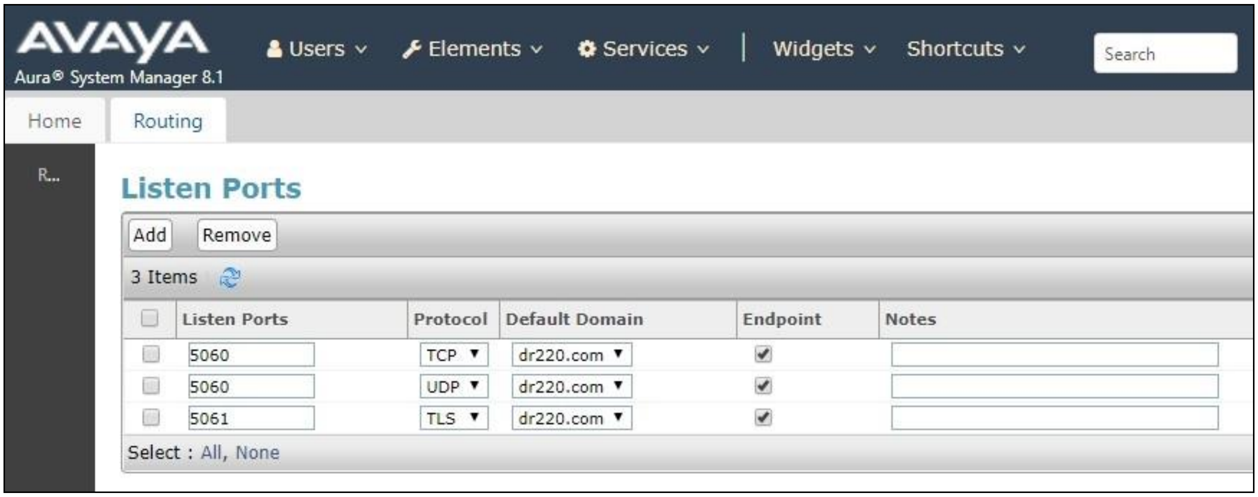


SIP Entity Details

General

| | |
|---|---|
| * Name: | DR-SM |
| * IP Address: | 10.64.101.238 |
| SIP FQDN: | |
| Type: | Session Manager |
| Notes: | TLT DR SM |
| Location: | DR-Loc |
| Outbound Proxy: | |
| Time Zone: | America/New_York |
| Minimum TLS Version: | Use Global Setting |
| Credential name: | |

Scroll down to **Listen Ports** and verify that the transport protocol used by IPX is specified in the list, in thise case “UDP” as shown below.



Listen Ports

| □ | Listen Ports | Protocol | Default Domain | Endpoint | Notes |
|---|---|---|---|---|---|
| □ | 5060 | TCP | dr220.com | ☑ | |
| □ | 5060 | UDP | dr220.com | ☑ | |
| □ | 5061 | TLS | dr220.com | ☑ | |

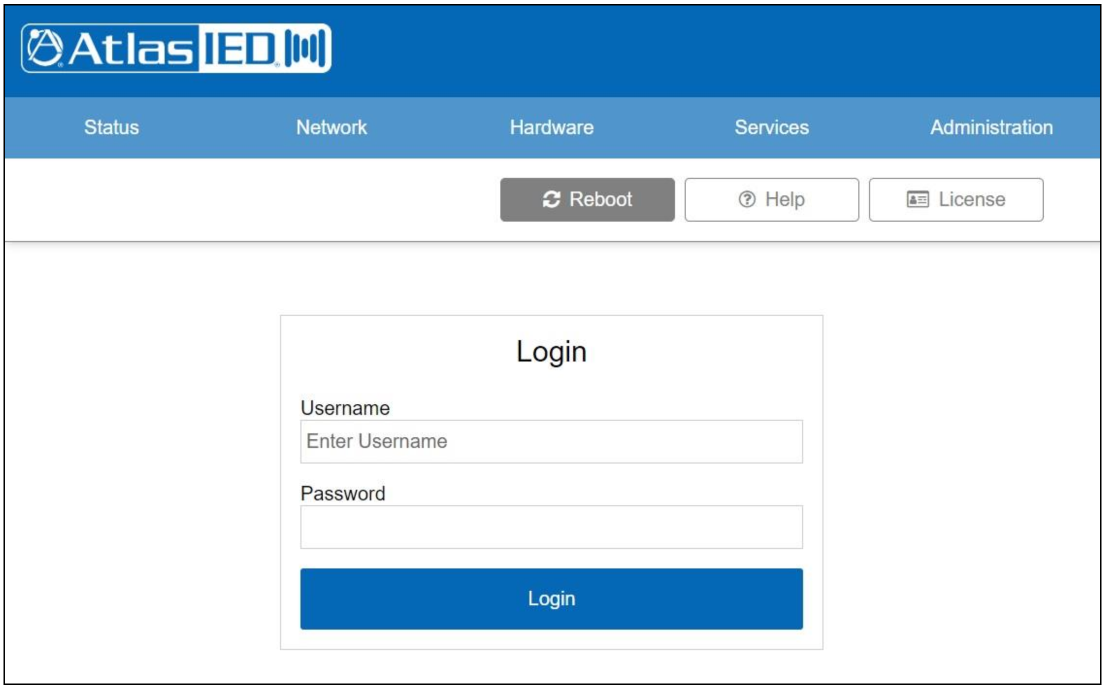
# 7. Configure AtlasIED IPX Series

This section provides the procedures for configuring each IPX. The procedures include the following areas:

- Launch web interface
- Administer SIP service

## 7.1. Launch Web Interface

Access the IPX web-based interface by using the URL "http://ip-address" in an Internet browser window, where "ip-address" is the IP address of the IPX speaker. Log in using the appropriate credentials.

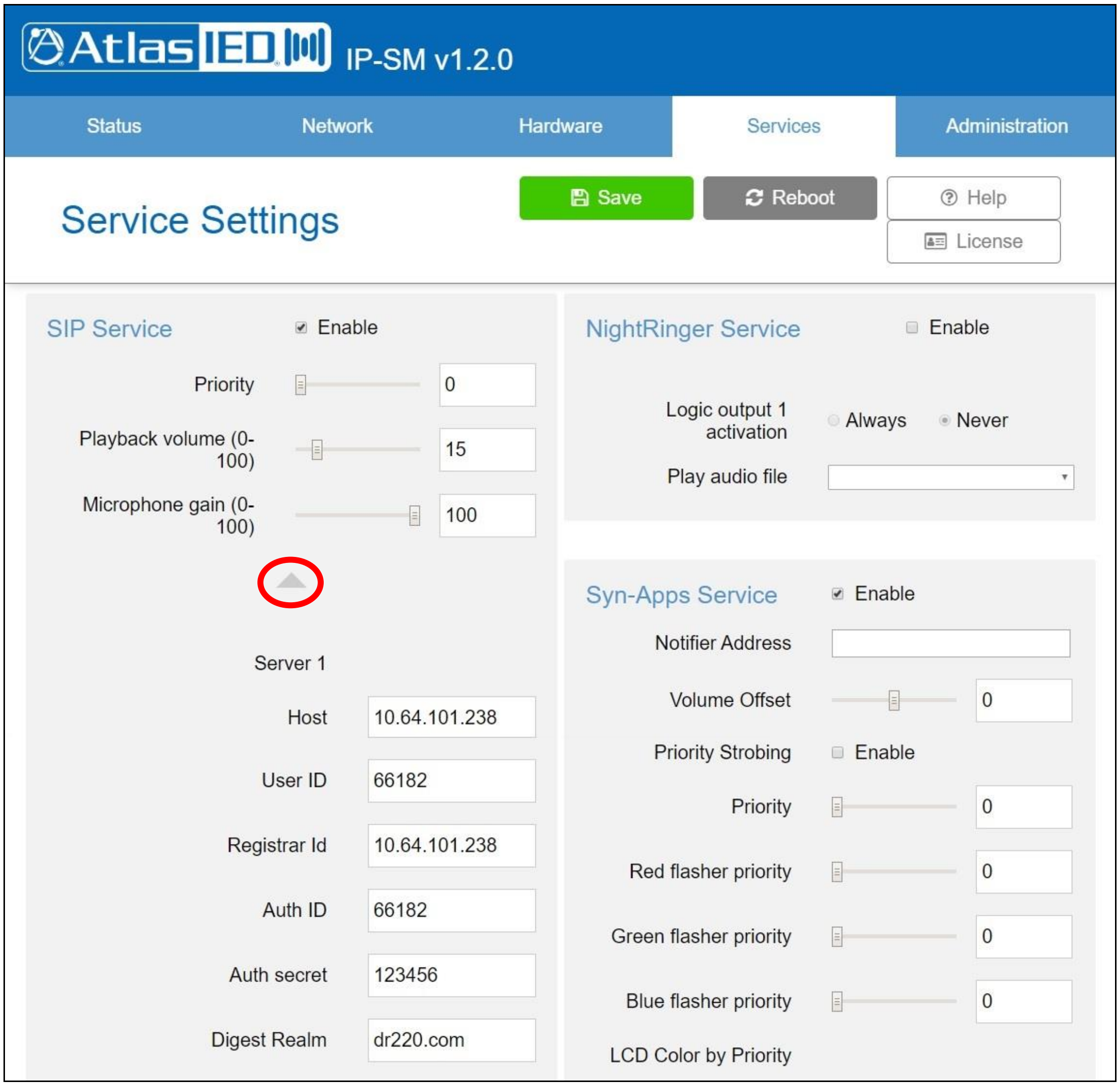


## 7.2. Administer SIP Service

The **AtlasIED** screen is displayed. Select **Services** from the top menu to display the **Service Settings** screen. In the **SIP Service** sub-section, check **Enable** and click on the icon highlighted below to display additional parameters.

Under **Server 1**, enter the following values for the specified fields and retain the default values for the remaining fields. Select **Save** followed by **Reboot**.

- **Host:** IP address of the Session Manager signaling interface.
- **User ID:** The SIP user extension from **Section 6.2.1**.
- **Registrar Id:** IP address of the Session Manager signaling interface.
- **Auth ID:** The SIP user extension from **Section 6.2.1**.
- **Auth secret:** The SIP user password from **Section 6.2.2**.
- **Digest Realm:** The domain name from **Section 3**.



SIP Service ☑ Enable

Priority 0

Playback volume (0-100) 15

Microphone gain (0-100) 100

Server 1

Host 10.64.101.238

User ID 66182

Registrar Id 10.64.101.238

Auth ID 66182

Auth secret 123456

Digest Realm dr220.com

NightRinger Service □ Enable

Logic output 1 activation ○ Always ● Never

Play audio file

Syn-Apps Service ☑ Enable

Notifier Address

Volume Offset 0

Priority Strobing □ Enable

Priority 0

Red flasher priority 0

Green flasher priority 0

Blue flasher priority 0

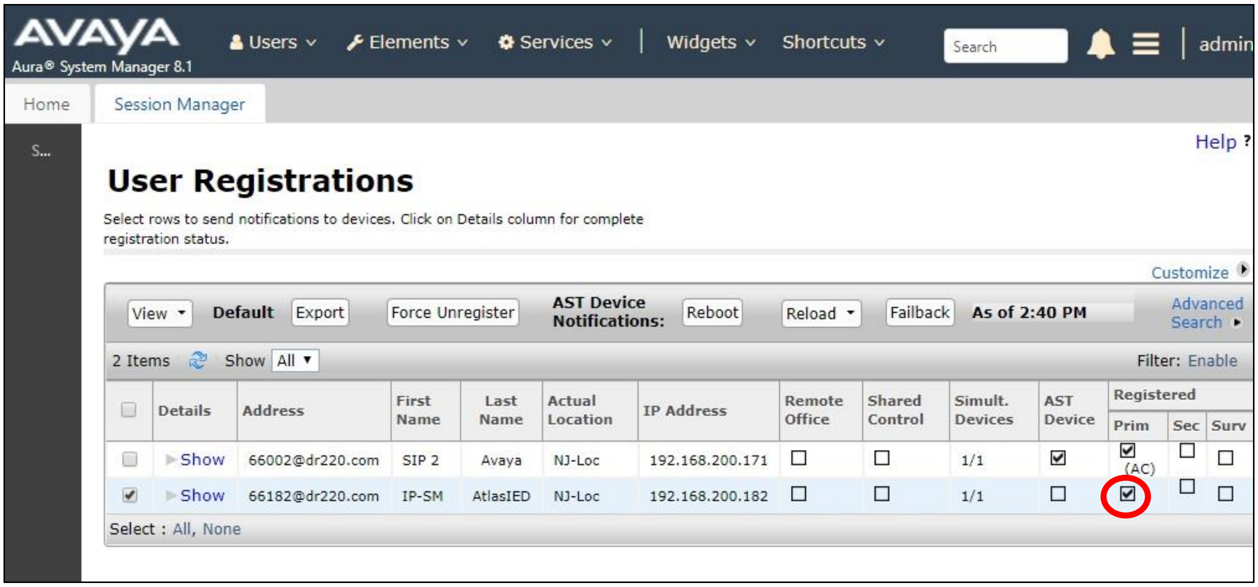
LCD Color by Priority

# 8. Verification Steps

This section provides the test that can be performed to verify proper configuration of Communication Manager, Session Manager, and IPX.

From the System Manager web-based interface, select **Elements → Session Manager → System Status → User Registrations** from the top menu to display the **User Registrations** screen.

Verify that the SIP user from **Section 6.2** is registered, as shown below with a check in the **Registered Prim** column.



## User Registrations

Select rows to send notifications to devices. Click on Details column for complete registration status.

| ☐ | Details | Address | First Name | Last Name | Actual Location | IP Address | Remote Office | Shared Control | Simult. Devices | AST Device | Registered | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | Prim | Sec | Surv |
| ☐ | ▶ Show | 66002@dr220.com | SIP 2 | Avaya | NJ-Loc | 192.168.200.171 | ☐ | ☐ | 1/1 | ☑ | ☑ (AC) | ☐ | ☐ |
| ☑ | ▶ Show | 66182@dr220.com | IP-SM | AtlasIED | NJ-Loc | 192.168.200.182 | ☐ | ☐ | 1/1 | ☐ | ☑ | ☐ | ☐ |

## 9. Conclusion

These Application Notes describe the configuration steps required for AtlasIED IPX Series to 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.

1. *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 3, August 2019, available at http://support.avaya.com.

2. *Administering Avaya Aura® Session Manager*, Release 8.1, Issue 1, June 2019, available at http://support.avaya.com.

3. *AtlasIED IP Endpoint Speakers Install Sheet*, available from https://www.atlasied.com/speakers-horns-voip-speakers

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.