Avaya Solution & Interoperability Test Lab

Application Notes for Biamp Tesira SVC-2 with Avaya Aura® Communication Manager and Avaya Aura® Session Manager – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Biamp Tesira SVC-2 which was compliance tested with Avaya Aura® Communication Manager and Avaya Aura® Session Manager.

The overall objective of the interoperability compliance testing is to verify Biamp Tesira SVC-2 functionalities in an environment comprised of Avaya Aura® Communication Manager, Avaya Aura® Session Manager, various Avaya H.323 and SIP IP Deskphones.

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 procedures for configuring Biamp Tesira SVC-2 which was compliance tested with Avaya Aura® Communication Manager and Avaya Aura® Session Manager.

The Tesira SVC-2 is an add-on card to the Tesira Server-IO platform. It enables conferencing over VoIP directly from Tesira SERVER-IO, with two channels of VoIP interface per card. Tesira SVC-2 allows Tesira SERVER-IO to connect directly to IP-based phone systems and eliminate the need for VoIP adapters.

During the compliance test, Tesira SVC-2 was tested as a SIP endpoints solution, thus endpoints registered to Avaya Aura® Session Manager

For further details on Tesira SVC-2 configuration steps not covered in this document, consult **[4]**.

2. General Test Approach and Test Results

All test cases were performed manually. The general approach was to place various types of calls to and from Biamp Tesira SVC-2. Biamp Tesira SVC-2 operations such as inbound calls, outbound calls, hold/resume, DTMF, codecs (G.711Mu, G.729, G.722), media shuffling, TLS registration, SRTP, and Biamp Tesira SVC-2 interactions with Session Manager, Communication Manager, and Avaya SIP and H.323 telephones were verified.

For serviceability testing, failures such as cable pulls and resets were applied.

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.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. The feature testing evaluated the interoperability between Biamp Tesira SVC-2, Session Manager, and Communication Manager. The serviceability testing introduced failure scenarios to see if Biamp Tesira SVC-2 could resume after failure.

2.2. Test Results

All test cases passed. Test included TLS registration and SRTP.

2.3. Support

Technical support for Biamp Tesira SVC-2 solution can be obtained by contacting Biamp at:

- http://www.biamp.com/support/index.aspx
- (800)-826-1457

3. Reference Configuration

Figure 1 illustrates a sample configuration consisting of an Avaya S8300D Server, an Avaya G450 Media Gateway or Avaya Aura® Media Server, a Session Manager Server, and Biamp Tesira SVC-2. The solution described herein is also extensible to other Avaya Servers and Media Gateways. For completeness, Avaya 96x0/96x1 Series H.323 IP Deskphones, and Avaya 96x0/96x1 Series SIP IP Deskphone, are included in Figure 1 to demonstrate calls between the Biamp Tesira SVC-2 and Avaya SIP and H.323.

Note: an assumption was made that a sip trunk between Communication Manager and Session Manager has been already configured prior to testing. For a basic SIP trunk configuration between Communication Manager and Session Manager, refer to [1] and [2].

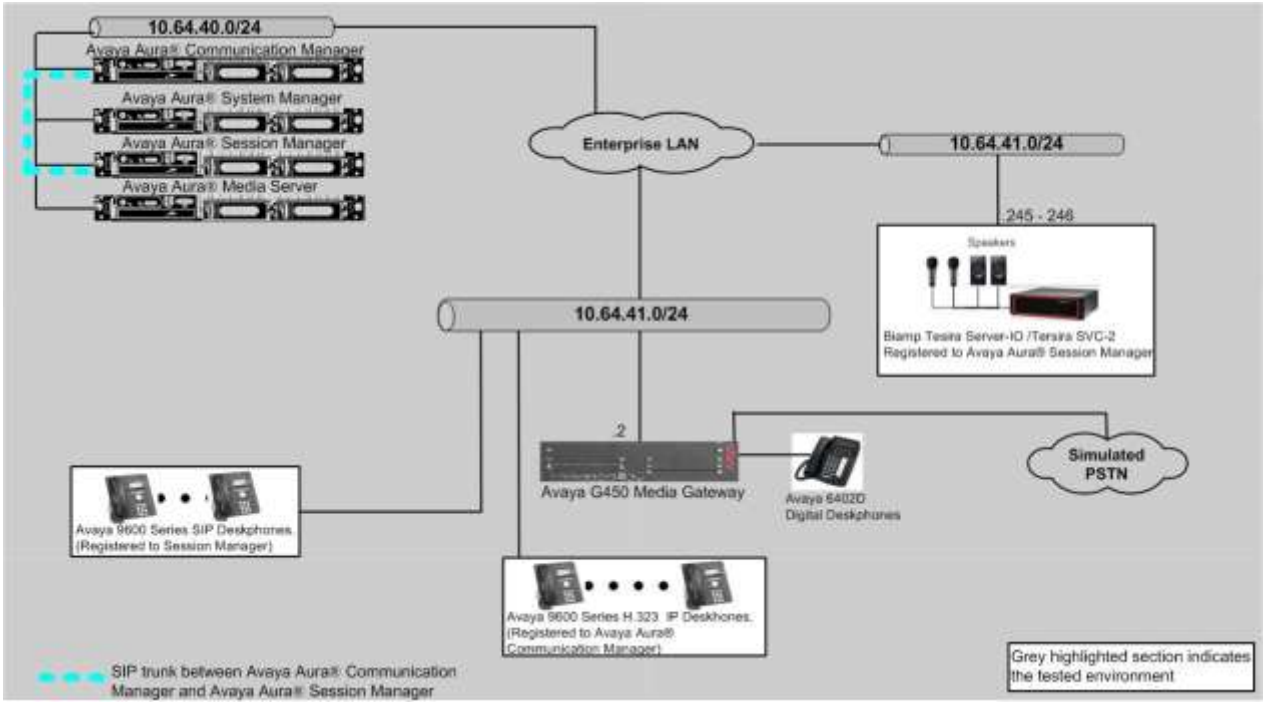


Figure 1: Test Configuration of Biamp Tesira SVC-2

4. Equipment and Software Validated

The following equipment and software were used for the test configuration.

Equipment/Software		Release/Version
Avaya Communication Manager on Virtual Environment Avaya G450 Media Gateway		7.0 (R017x.00.0.441.0) 37.19.0
Avaya Aura® System Manager on Virtual Environment		7.0.0.0.3929
Avaya Aura® Session Manager on Virtual Environment		7.0.0.0.700007
Avaya Aura® Media Server		7.7.0.226
Avaya 96x0 and 96x1 Series IP Deskphones		
	9620 (H.323) 9621G (H.323)	3.25 6.6
Avaya 96x0 and 96x1 Series SIP Deskphones		
	9611G 9650	7.0.0.39 2.6.14
Biamp Tesira Firmware (Tesira Server-IO)		2.4.0.60
Biamp VoIP Software (Tesira SVC-2)		1.3.0.20

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for setting up a SIP trunk between Communication Manager and Session Manager. The steps include setting up an IP codec set, an IP network region, IP node name, a signaling group, a trunk group, and a SIP station. Before a trunk can be configured, it is necessary to verify if there is enough capacity to setup an additional trunk. The highlights in the following screens indicate the values used during the compliance test. Default values may be used for all other fields.

These steps are performed from the Communication Manager System Access Terminal (SAT) interface. Biamp Tesira SVC-2 and other SIP telephones are configured as off-PBX telephones in Communication Manager.

5.1. Capacity Verification

Enter the **display system-parameters customer-options** command. Verify that there are sufficient **Maximum Off-PBX Telephones – OPS** licenses. If not, contact an authorized Avaya account representative to obtain additional licenses

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

     G3 Version: V17                            Software Package: Enterprise
       Location: 2                               System ID (SID): 1
       Platform: 28                              Module ID (MID): 1

                                                          USED
                                Platform Maximum Ports: 6400  193
                                     Maximum Stations: 2400  45
                                Maximum XMOBILE Stations: 2400  0
                    Maximum Off-PBX Telephones - EC500: 9600  1
                    Maximum Off-PBX Telephones -   OPS: 9600  20
```

On **Page 2** of the form, verify that the number of SIP trunks supported by the system is sufficient for the number of SIP trunks needed. If not, contact an authorized Avaya account representative to obtain additional licenses.

```
display system-parameters customer-options                      Page   2 of  12
                              OPTIONAL FEATURES

IP PORT CAPACITIES                                            USED
                      Maximum Administered H.323 Trunks: 4000  17
           Maximum Concurrently Registered IP Stations: 2400  2
             Maximum Administered Remote Office Trunks: 4000  0
Maximum Concurrently Registered Remote Office Stations: 2400  0
              Maximum Concurrently Registered IP eCons: 68    0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                       Maximum Video Capable Stations: 2400  0
                   Maximum Video Capable IP Softphones: 2400  1
                       Maximum Administered SIP Trunks: 4000  15
  Maximum Administered Ad-hoc Video Conferencing Ports: 4000  0
   Maximum Number of DS1 Boards with Echo Cancellation: 80    0
```

On **Page 5** of the form, verify that the **Media Encryption over IP** field is set to **y**. This is needed to enable the media encryption. When the field is enabled, the media encryption section in the ip-codec-set form is displayed. If the field is not enabled, please contact an authorized Avaya account representative to enable the feature.

```
change system-parameters customer-options                      Page   5 of  12
                              OPTIONAL FEATURES

   Emergency Access to Attendant? y                               IP Stations? y
            Enable 'dadmin' Login? y
            Enhanced Conferencing? y                         ISDN Feature Plus? n
                  Enhanced EC500? y          ISDN/SIP Network Call Redirection? y
    Enterprise Survivable Server? n                            ISDN-BRI Trunks? y
       Enterprise Wide Licensing? n                                  ISDN-PRI? y
              ESS Administration? y                 Local Survivable Processor? n
          Extended Cvg/Fwd Admin? y                       Malicious Call Trace? y
     External Device Alarm Admin? y                   Media Encryption Over IP? y
  Five Port Networks Max Per MCC? n       Mode Code for Centralized Voice Mail? n
                Flexible Billing? n
   Forced Entry of Account Codes? y                   Multifrequency Signaling? y
      Global Call Classification? y           Multimedia Call Handling (Basic)? y
             Hospitality (Basic)? y        Multimedia Call Handling (Enhanced)? y
 Hospitality (G3V3 Enhancements)? y                  Multimedia IP SIP Trunking? y
                       IP Trunks? y

           IP Attendant Consoles? y
```

5.2. IP Codec Set

This section describes the steps for administering a codec set in Communication Manager. This codec set is used in the IP network region for communications between Communication Manager and Session Manager. Enter the **change ip-codec-set <c>** command, where **c** is a number between **1** and **7**, inclusive. IP codec sets are used in **Section 5.3** when configuring an IP network region to specify which codec sets may be used within and between network regions. Under the **Media Encryption** section, two encryption methods were selected. One of these encryption methods has to be implemented by Biamp to communicate between Tesira SVC-2 and Avaya endpoints.

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

                         IP CODEC SET
   Codec Set: 1

   Audio         Silence      Frames   Packet
   Codec         Suppression  Per Pkt  Size(ms)
 1: G.711MU           n         2        20
 2: G.729             n         2        20
 3:
 4:
 5:
 6:
 7:

    Media Encryption                  Encrypted SRTCP: best-effort
 1: 1-srtp-aescm128-hmac80
 2: 2-srtp-aescm128-hmac32
 3: none
```

6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. Session Manager is comprised of two functional components: The Session Manager server and the System Manager server. All SIP call provisioning for Session Manager is performed through the System Manager Web interface and is then downloaded into Session Manager.

This section assumes that Session Manager and System Manager have been installed, and network connectivity exists between the two platforms.

The following steps describe for configuring Session Manager.

- Launch System Manager
- User Management
- TLS certificate between 3rd party endpoint and Session Manager

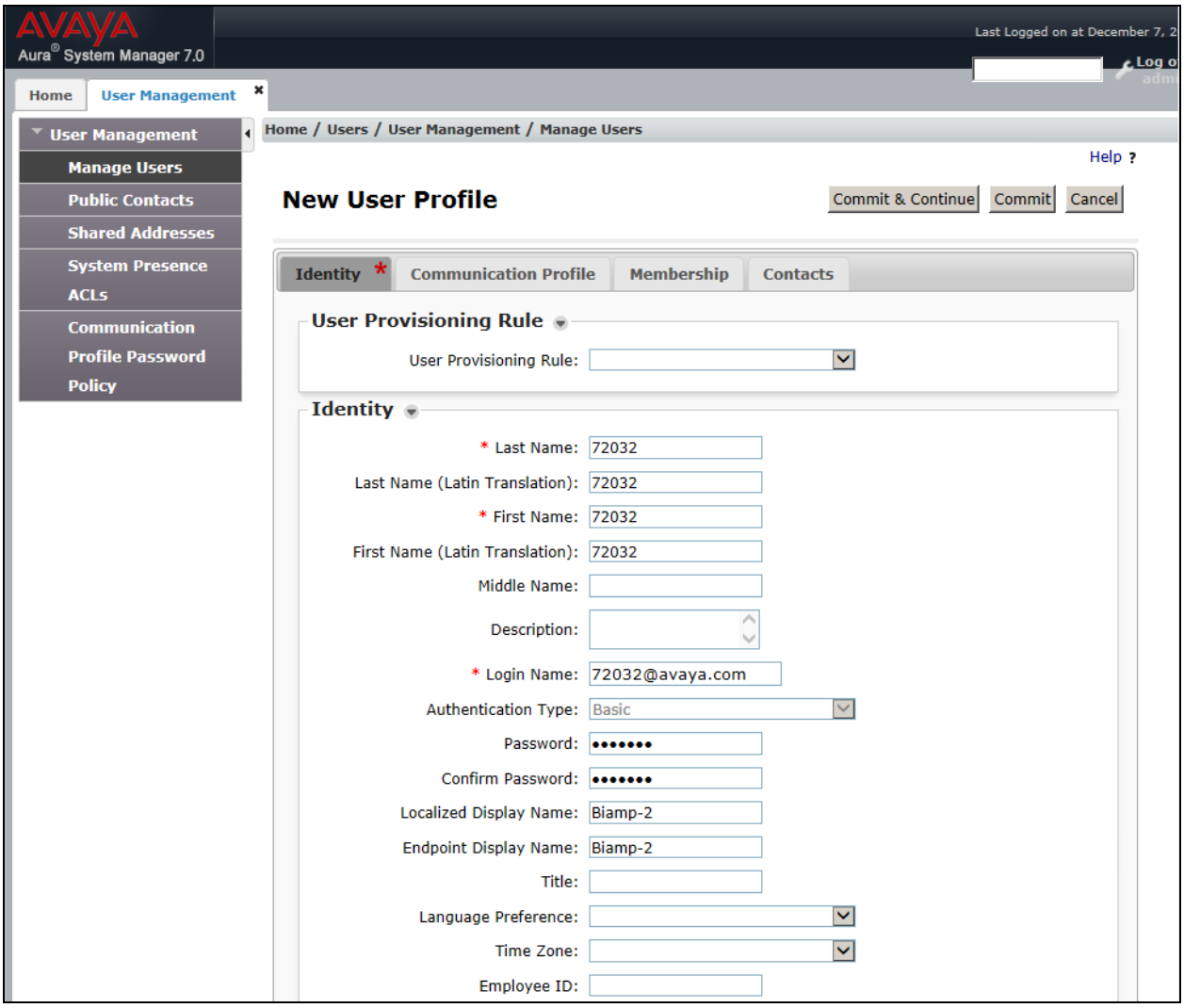
6.1. Launch System Manager

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.

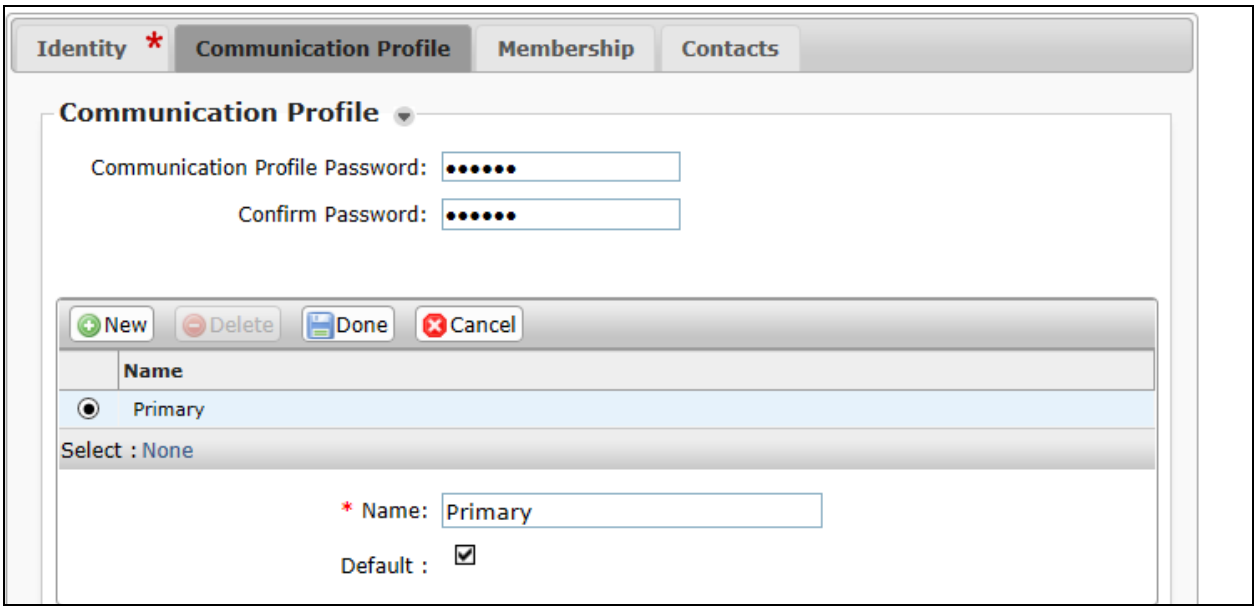
6.2. Configure User

To add new SIP users, navigate to **Home → Users → User Management → Manage Users**. Click **New** and provide the following information:

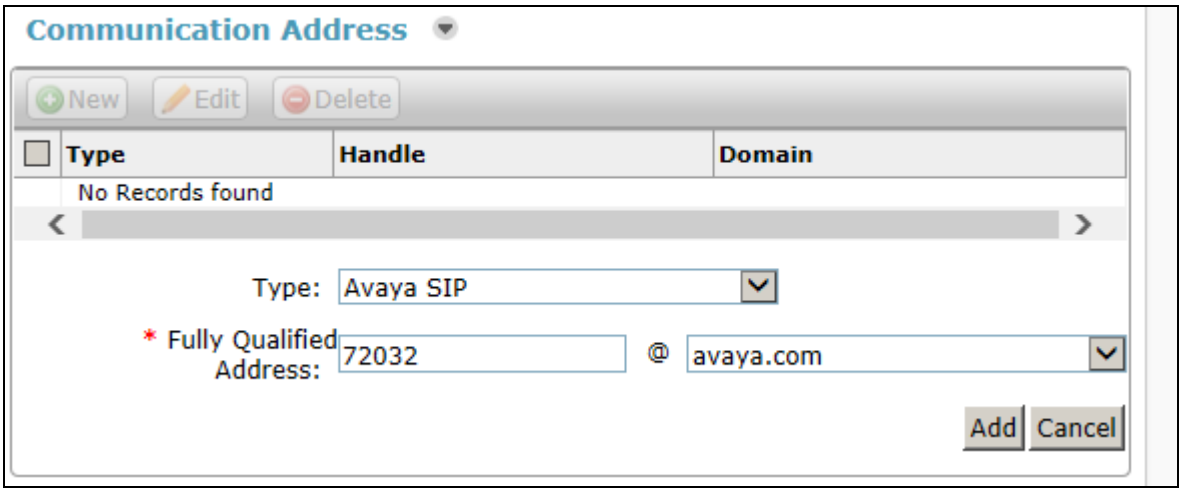
- Identity section
  - **Last Name –** Enter last name of user.
  - **First Name –** Enter first name of user.
  - **Login Name –** Enter extension number@sip domain. The sip domain is defined as authoritative domain in **Section 5.3**.
  - **Password –** Enter password to be used to log into System Manager.
  - **Confirm Password –** Repeat value entered above.



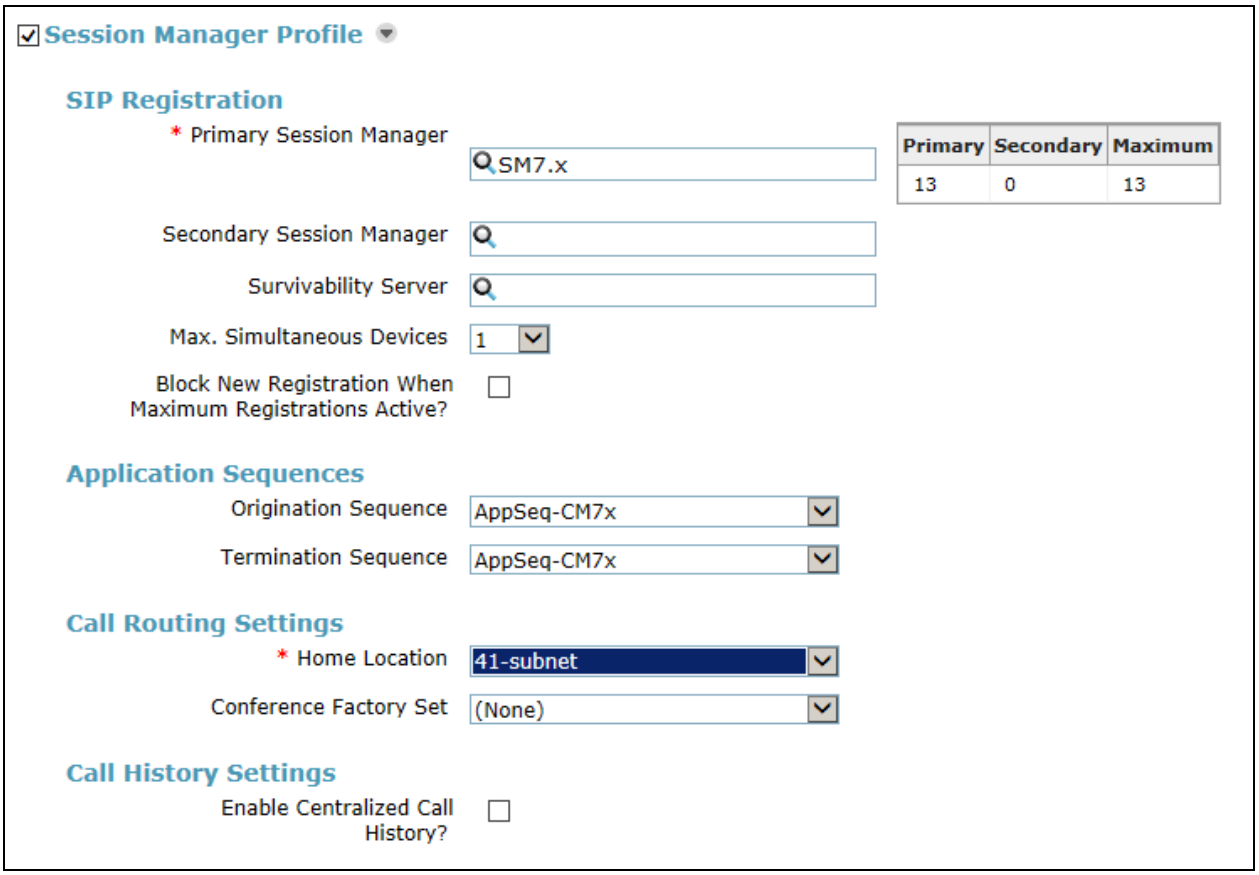
- Communication Profile section
  - **Communication Profile Password –** Type communication profile password in this field
  - **Confirm Password –** Repeat value entered above.



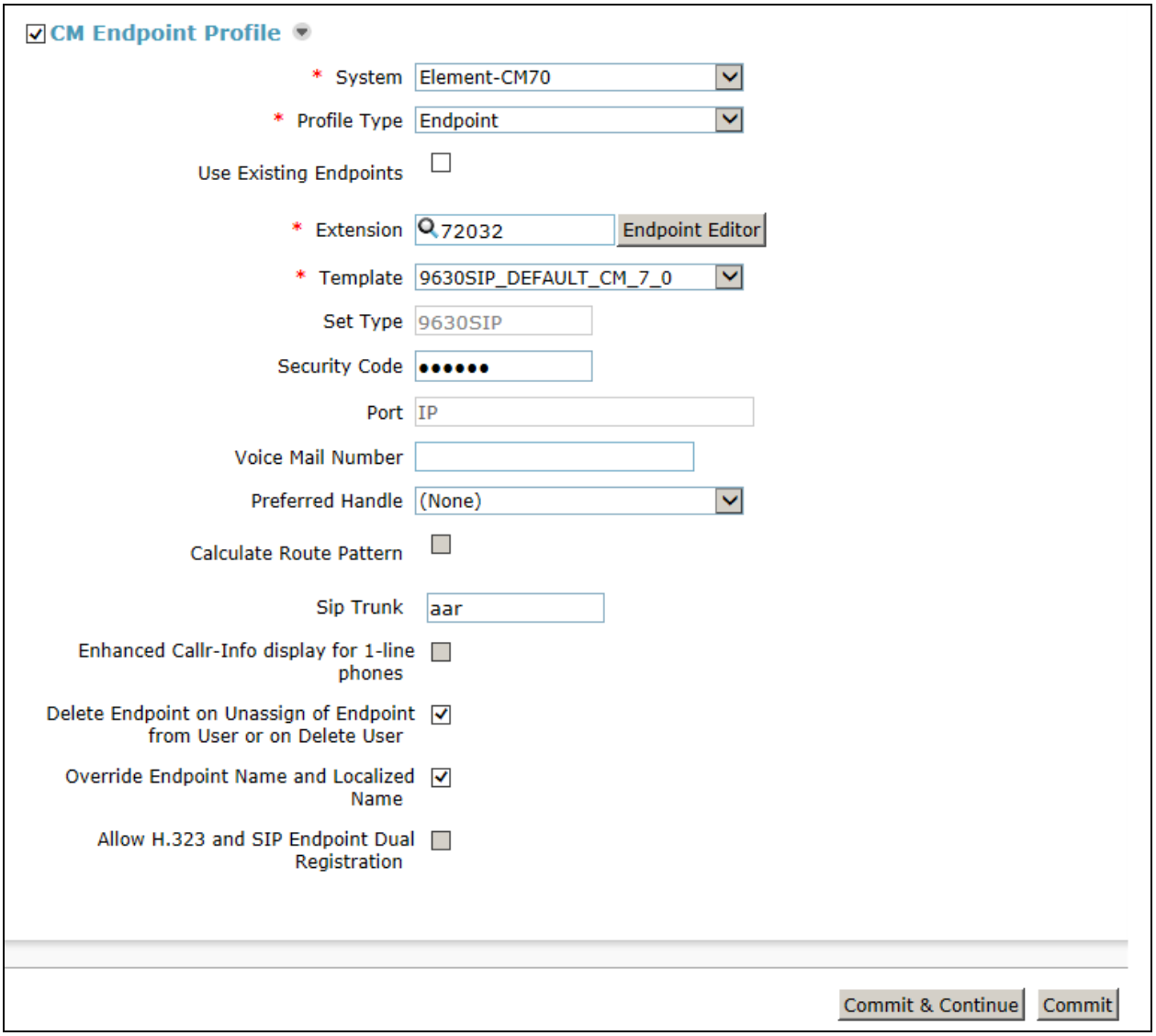
- Communication Address sub-section
  - **Fully Qualified Address –** Enter the extension of the user and select a domain name.
  - Click **Add** button



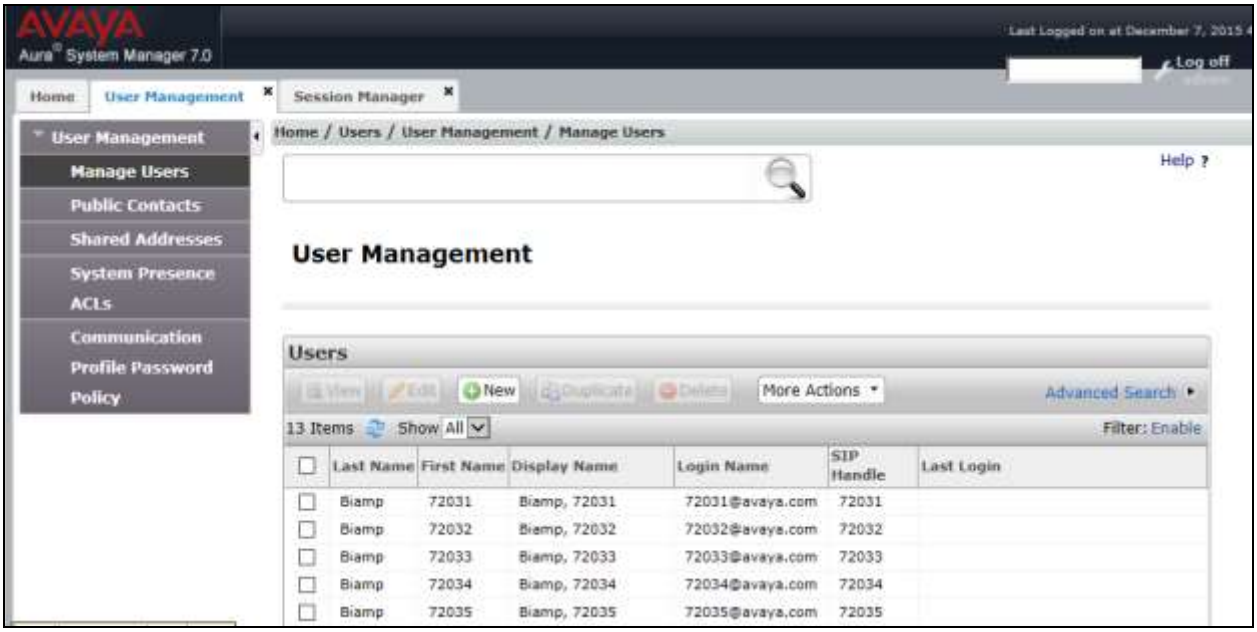
- Session Manager Profile sub-section
  - **Primary Session Manager** – Select the pertinent Session Manager.
  - **Origination Sequence –** Select the application sequence defined for Communication Manager.
  - **Termination Sequence** – Select application sequence for Communication Manager.
  - **Home Location** – Select the applicable location.



- CM Endpoint Profile sub-section
  - **System** – Select managed element defined in System Manager.
  - **Profile Type** – Select **Endpoint**.
  - **Extension** - Enter same extension number used in this section.
  - **Template** – Select template for type of SIP telephone.
  - **Security Code** – Enter numeric value used to logon to SIP telephone. (**Note:** this field must match the value entered for the Communication Profile Password field.
  - Click **Commit**.

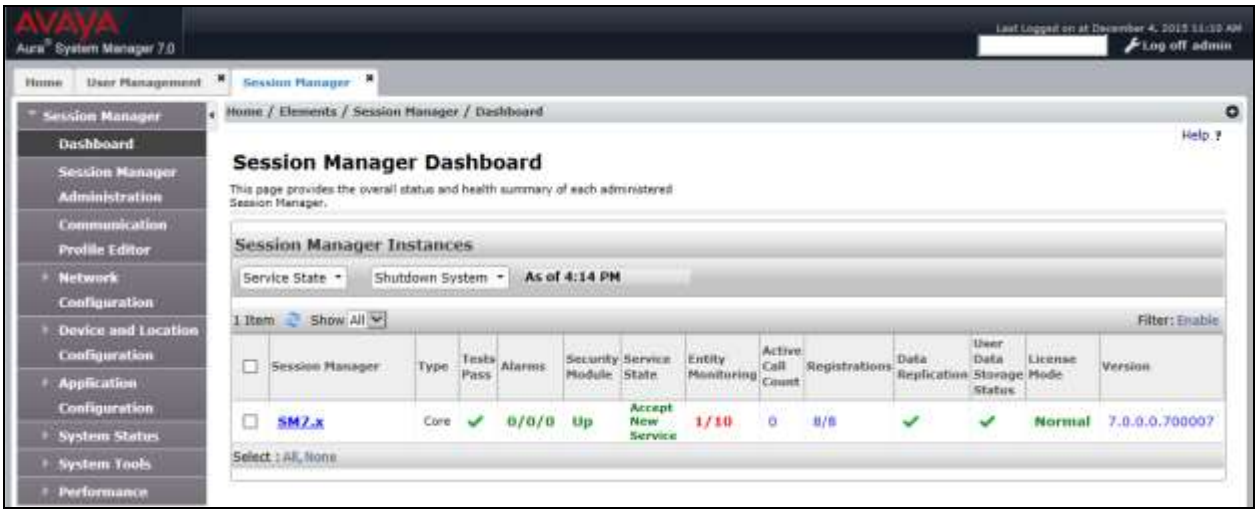


The following page shows the Biamp Tesira users created during the test.

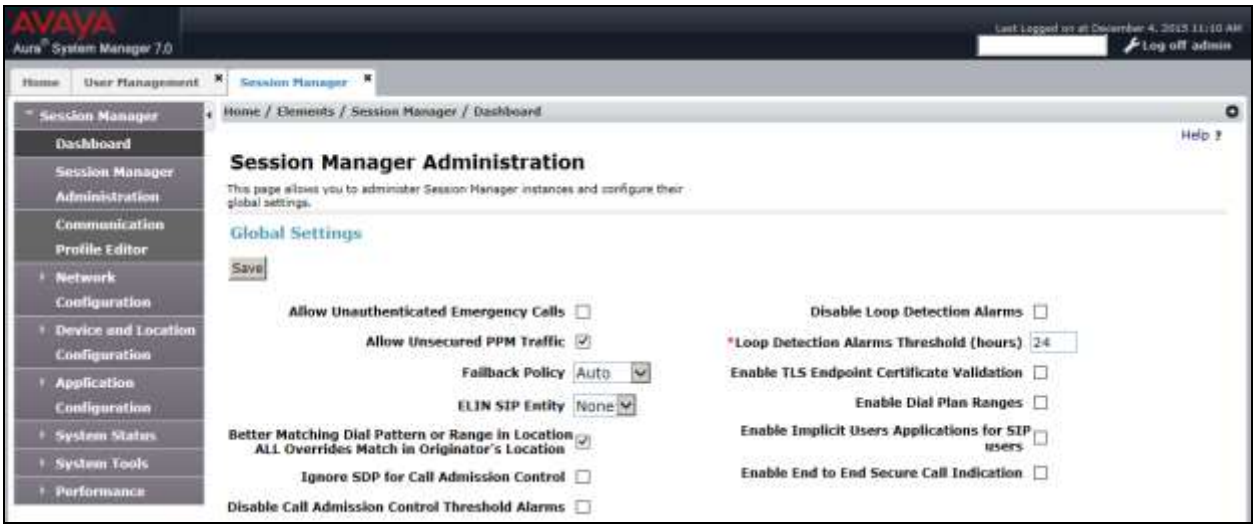


6.3. Configure Biamp Users for TLS

In System Manager, navigate to **Home →Elements → Session Manager → Dashboard**. Select the pertinent **Session Manager**.

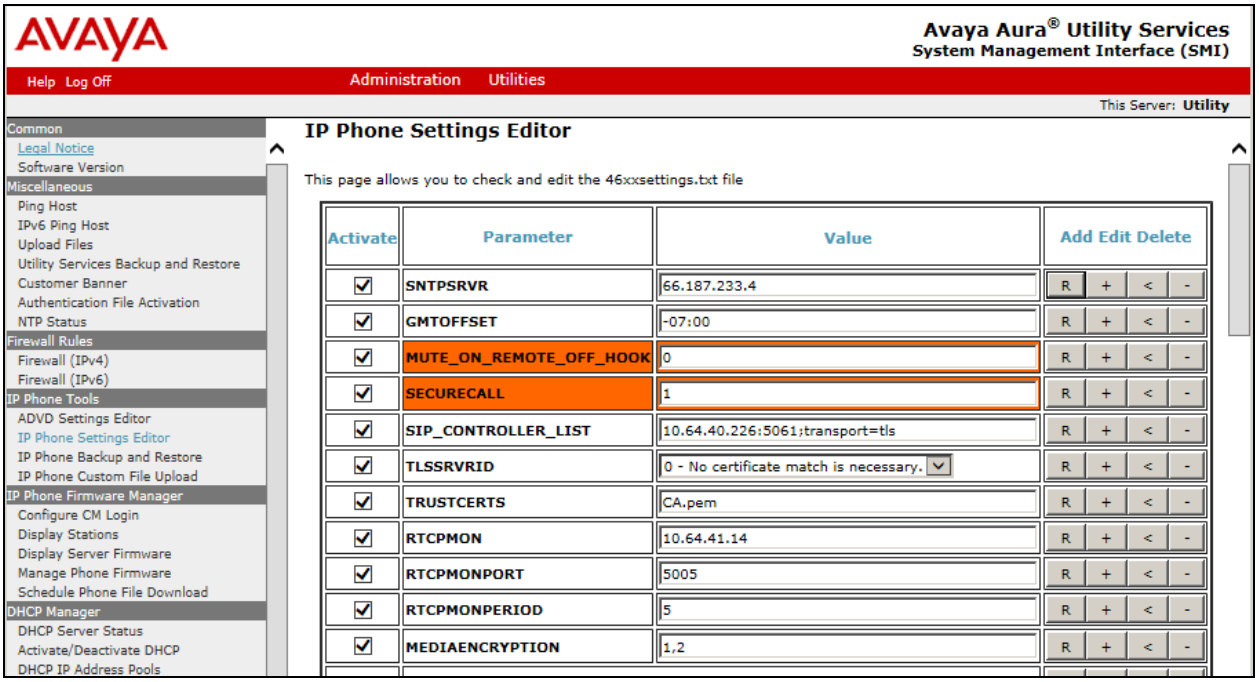


- From the **Session Manager Administration** page, verify that the **Enable TLS Endpoint Certificate Validation** field is not checked. By not checking Session Manager does not request a certificate from the 3rd party endpoint.



6.4. Configure SRTP on Session Manager

Biamp Tesira SVC-2 is registered to Session Manager. Avaya Aura® Utility Services server was used for IP Phone settings. To configure or add an encryption method that used during the SRTP telephone call, navigate to **IP Phone Settings Editor** in Avaya Aura® Utility Services. The following displays the **IP Phone Settings Editor** page. In the page, the **SECURECALL** field is set to "1", and **MEDIAENCRYPTION** is set to "**1,2**" which indicates **1-srtp-aescm128-hmac80** and **2-aescm128-hmac32** . One of these values has to match with the ip-codec-set form in Communication Manager and Biamp settings.



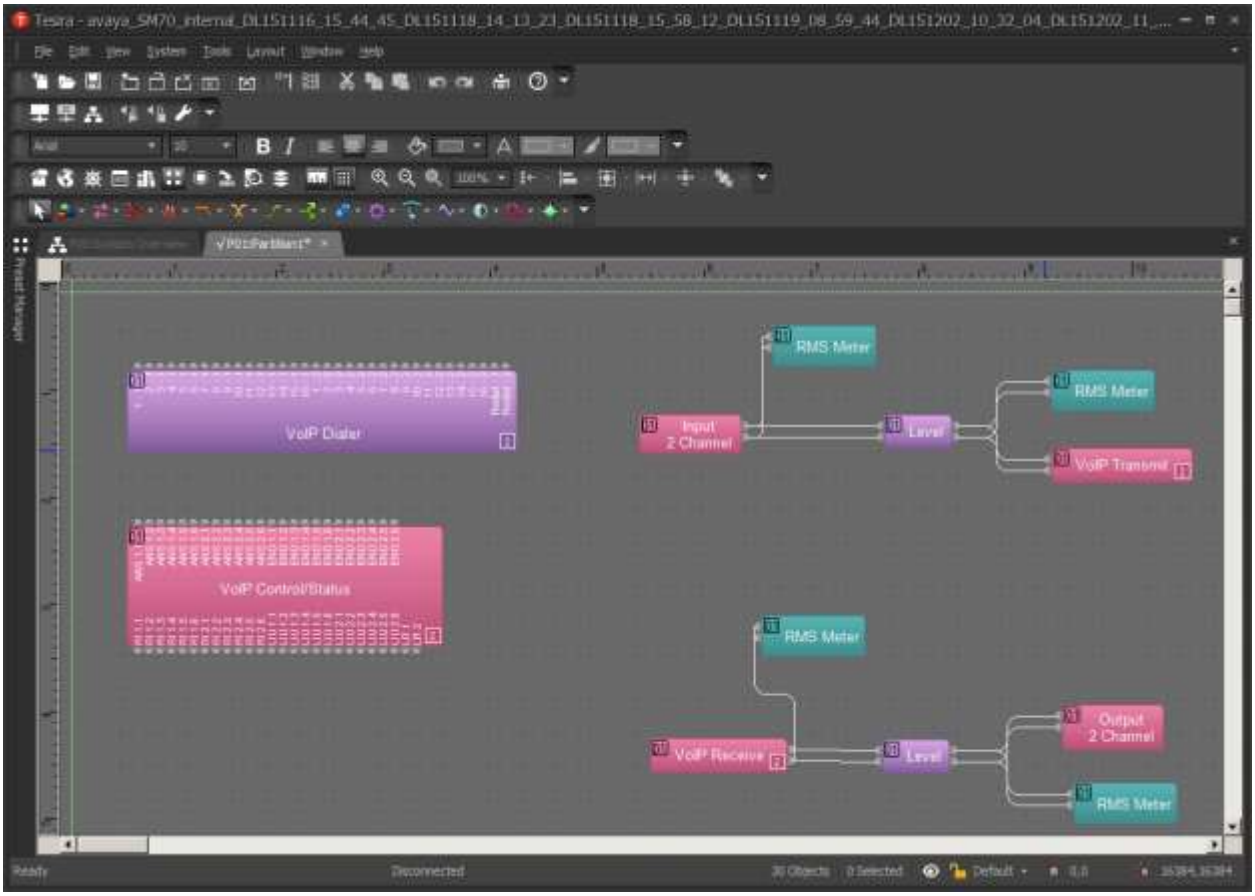
7. Configure Biamp Tesira SVC-2

Biamp installs, configures, and customizes the Tesira SVC-2 card for their end customers. This section only provides steps to configure Biamp Tesira SVC-2 to interface with Session Manager.

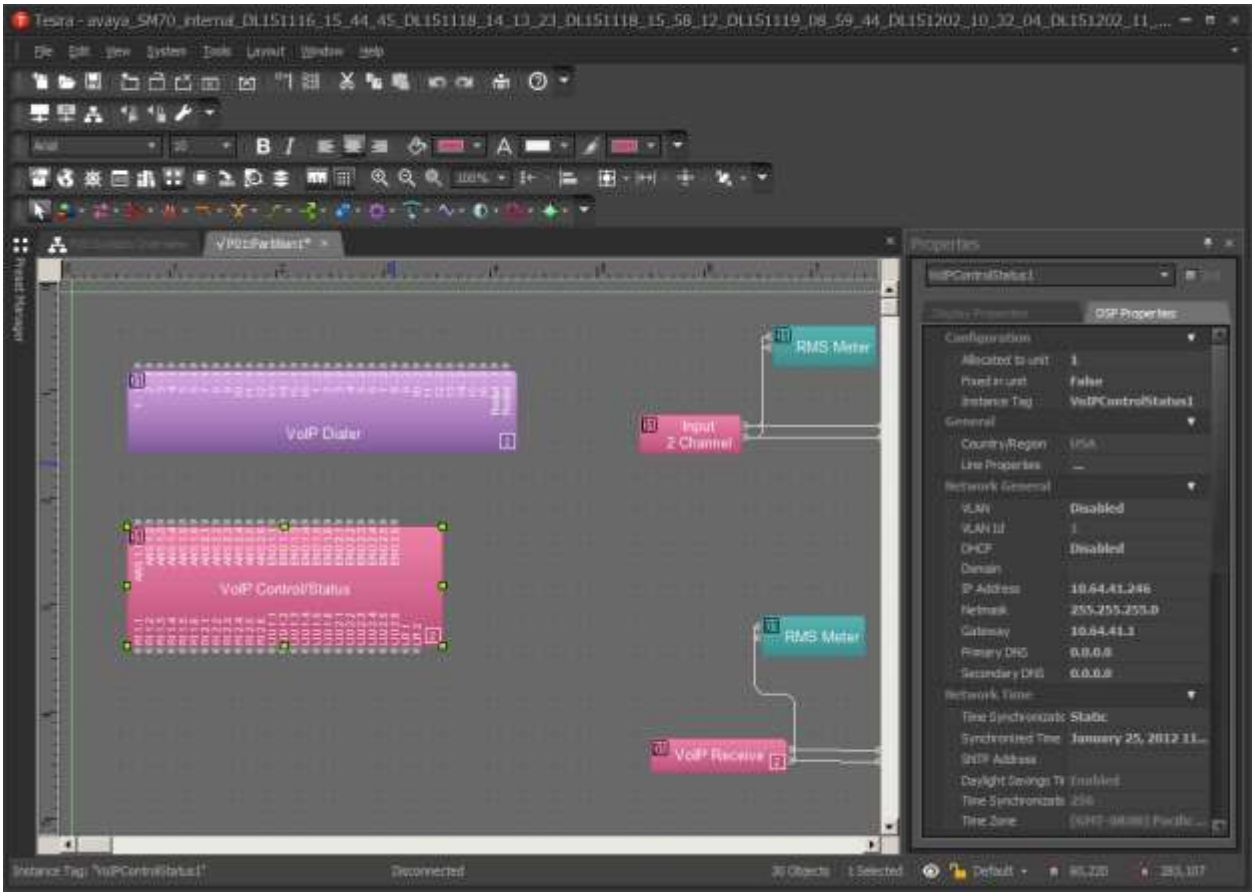
Select the Tesira icon, 

, from the PC that installed Tesira software to start the VoIP system. How to install/configure a Tesira system is out of the scope of these Application Notes.

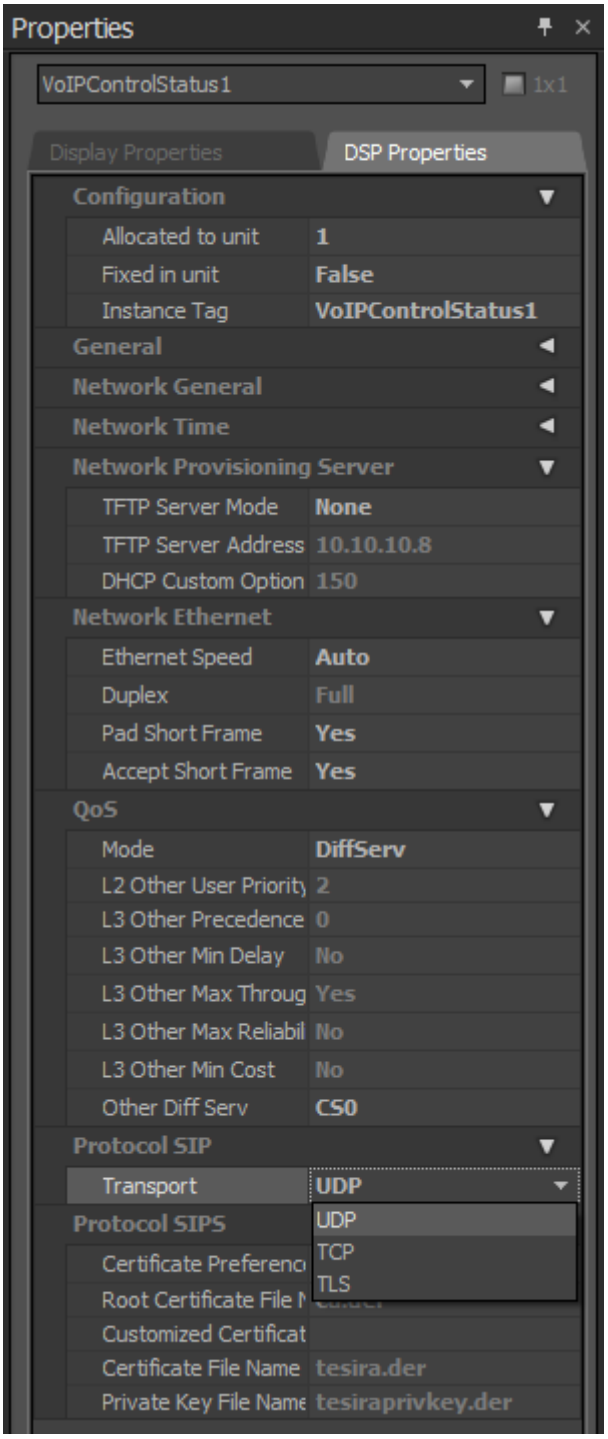
- Highlight the **VoIPControl/Status** block, as shown below.



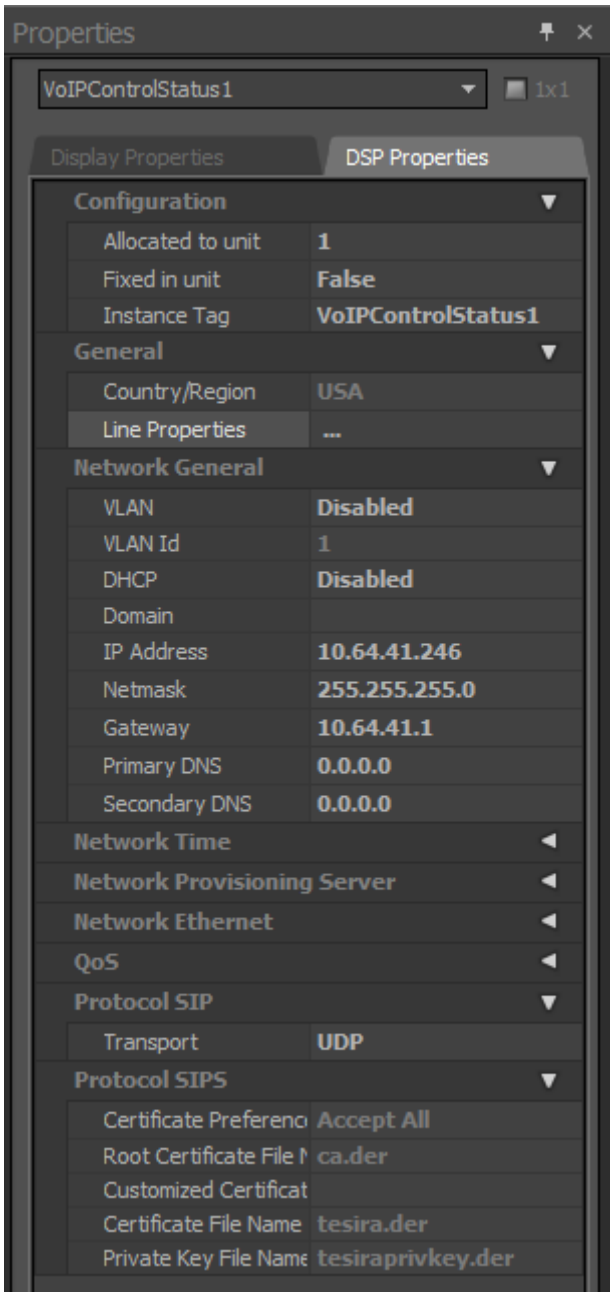
- Click right mouse button and select **Properties**, and the **Properties** menu will display on the right.



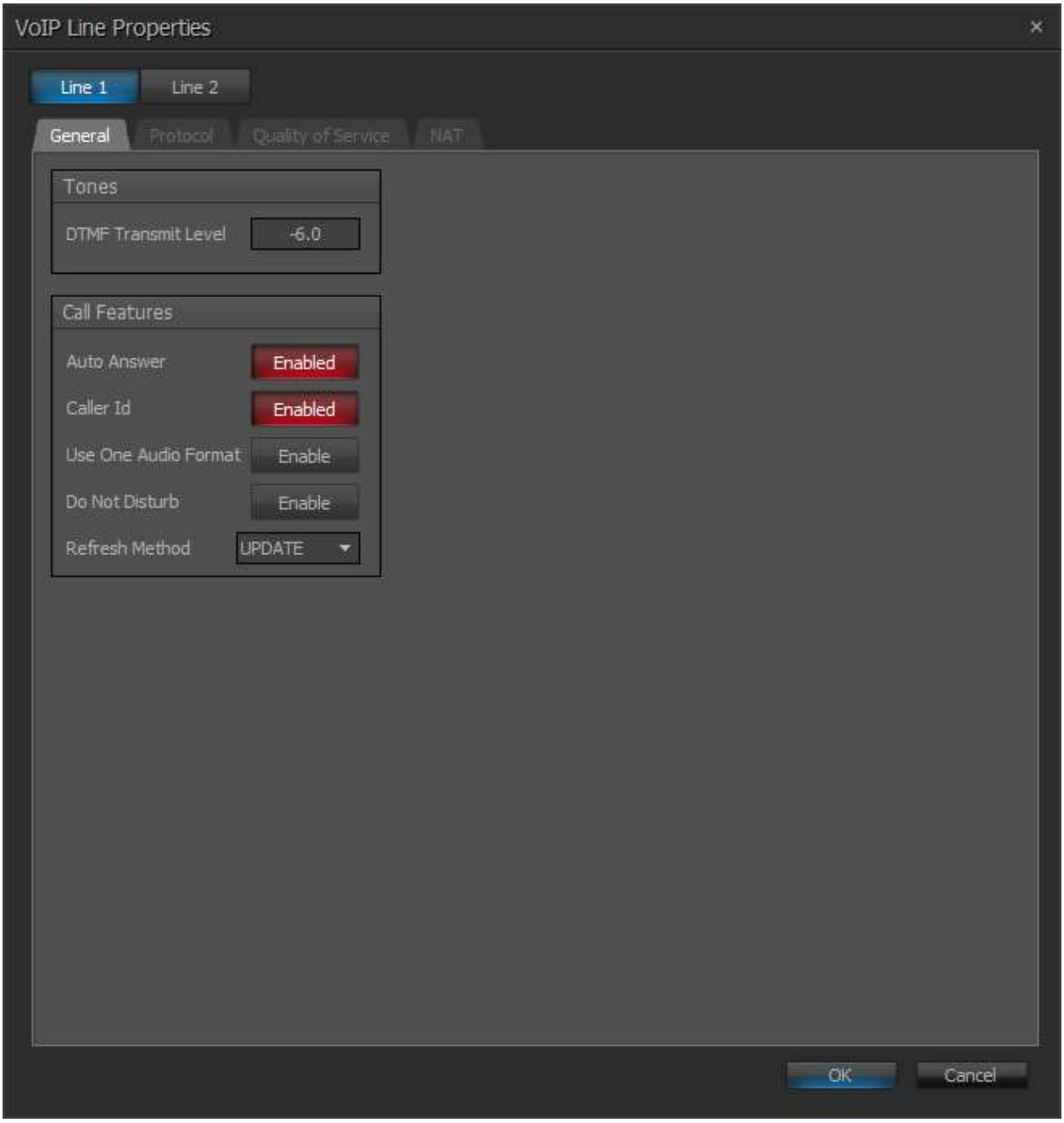
- Navigate the **Protocol SIP→Transport** to configure transport to be used. The default is UDP. When TLS is selected, please refer to Tesira Operational Manual for additional configuration. All three transport methods (UDP/TCP/TLS) were tested.



- Select **Line Properties** under the **General** section to display the **VoIP Line Properties** page.

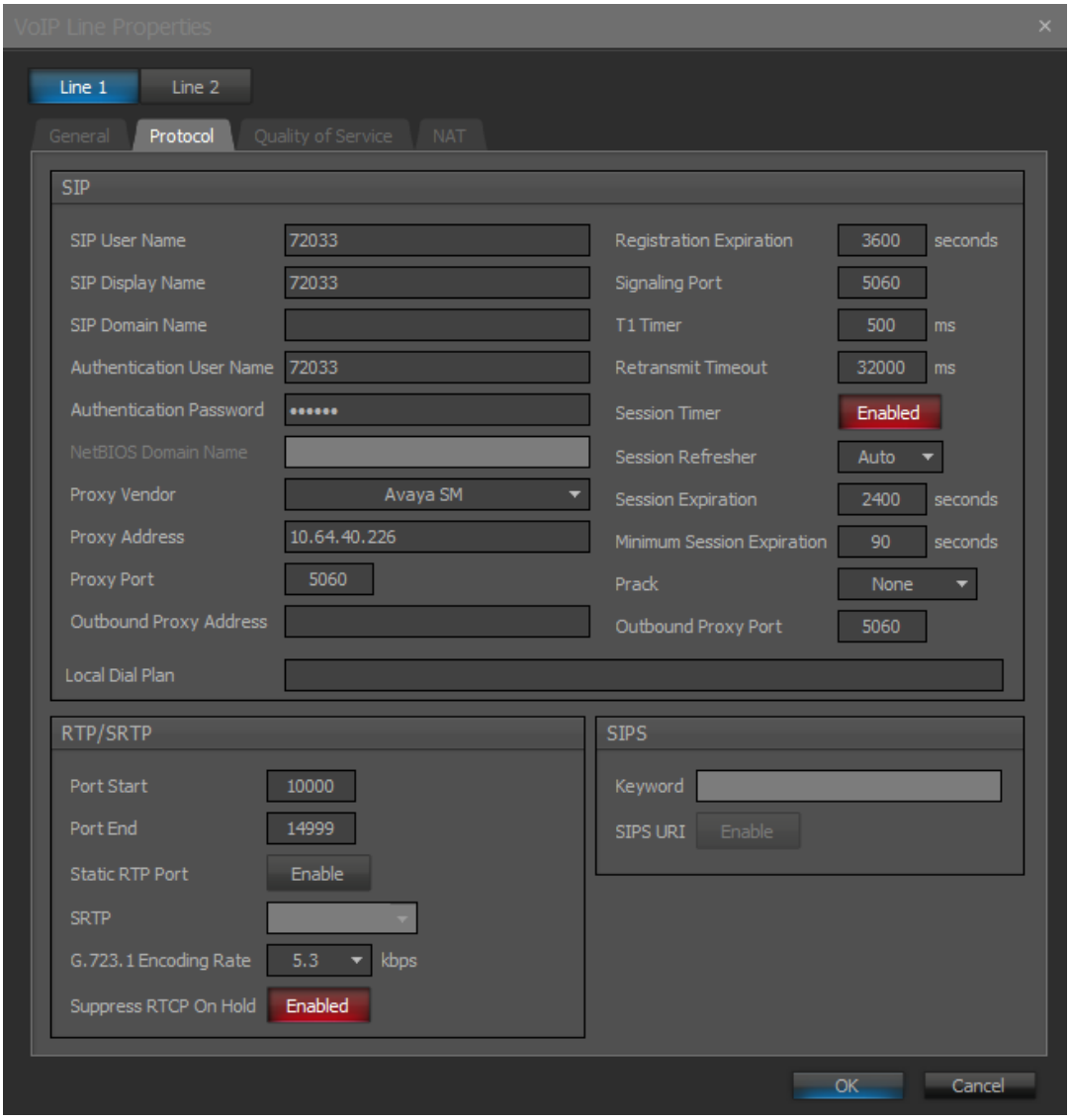


- From the **VoIP Line Properties** page, click the **Protocol** tab.



- From the **Protocol** page, provide the following information:
  - **SIP User Name** – Enter a user created in **Section 6.1**.
  - **Authentication User Name** – Enter a user created in **Section 6.1**.
  - **Authentication Password** – Enter the password for the user in **Section 6.1**.
  - **Proxy Vendor** – Select **Avaya SM**.
  - **Proxy Address** – Enter the IP address of Session Manager.
  - **Proxy Port** – Enter either 5060 (for TCP/UDP) or 5061 (for TLS).
  - Click on the **OK** button. Default values may be used for all other fields.

Note: *The Biamp Tesira SVC-2 card can provide two extensions (L1 and L2). In the testing, one card was used and both lines (extensions) were configured.*



8. Verification Steps

The following steps may be used to verify the configuration:

- Verify that Biamp Tesira SVC-2 successfully registers with the Session Manager server by following the **Home → Elements → Session Manager → System Status → User Registrations** in the System Manager
- Place calls to and from Biamp Tesira SVC-2 and verify that the calls are successfully established with two-way talk path.

9. Conclusion

Biamp Tesira SVC-2 was compliance tested with Communication Manager and Session Manager. Biamp Tesira SVC-2 functioned properly for feature and serviceability. During compliance testing, Biamp Tesira SVC-2 successfully registered with Session Manager (TLS and SRTP), placed and received calls to and from SIP and non-SIP telephones.

10. Additional References

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

[1] *Administering Avaya Aura® Communication Manager*, Release 7.0, August 2015, Issue 1,Document Number 03-300509
[2] *Administering Avaya Aura® Session Manager*, Release 7.0, August2015, Issue 1
[3] *Administering Avaya Aura® System Manager for Release 7.0*, Release 7.0, December 2015, Issue 1

The following document was provided by Biamp. To obtain a copy, contact Biamp Support in **Section 2.3**.

[4] *Tesira Operation Manual*, Document.

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.