Avaya Solution & Interoperability Test Lab

Application Notes for Teo IP Phones with Avaya Aura® Session Manager and Avaya Aura® Communication Manager – Issue 1.0

Abstract

These Application Notes describe a compliance-tested configuration consisting of Avaya Aura® Session Manager, Avaya Aura® Communication Manager and Teo IP Phones.

Teo's product line provides a range of IP telephones, including WiFi handsets, softphones, and mobile device UC clients as well as phones for specialty environments such as the TSG6 IP phone. These endpoints register directly with Avaya Aura® Session Manager.

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 a compliance-tested configuration consisting of Avaya Aura® Session Manager, Avaya Aura® Communication Manager and Teo IP Phones.

Teo IP Phones are available in several models:

- 3100 Series WiFi IP Phone (not tested)
- 4100 Series IP Phone (not tested)
- 7000 Series IP Phone (tested)
  - 7810 (not pictured)
  - 7810 TSG-6 (pictured)

All of these models share core SIP firmware. The primary differences with these phones are either cosmetic, network access (WiFi versus Wired LAN) or secure on-hook applications. These variations are not expected to impact the interoperability between the base station and the Avaya infrastructure, so use of any of these models can be assumed to yield the same results as those observed in the testing described in these Application Notes.

Teo TSG-6 IP phones meet the stringent requirements specified in the CNSS (Committee on National Security Systems) Instruction No. 5000 and 5001, and have been tested for compliance and approved by the National Telecommunications Security Working Group. TSG-6 Class A versions are not dependent on any other equipment for on-hook security, and may be used in standalone applications within a secure area.

2. General Test Approach and Test Results

The compliance test focused on the interoperability between the Teo IP Phones, Avaya Aura® Session Manager and Avaya Aura® Communication Manager including the ability to make and receive calls from PSTN endpoints and Avaya SIP, H.323, Digital and analog phones.

2.1. Interoperability Compliance Testing

Teo phones register with Session Manager and thus are able to use the Communication Manager application sequencing in a similar manner to Avaya SIP endpoints. Testing consisted of typical call scenarios involving internal and external endpoints using a simulated PSTN as well as verification of support for various voice codecs. Additionally, serviceability testing was performed to verify the ability for the phones to recover from loss of network connections.

2.2. Test Results

The objectives described in **Section 2.1** were verified. For serviceability testing, the Teo phones were able to re-register with Session Manager following loss of network connections, and server reboots.

2.3. Support

Information, Documentation and Technical support for Teo phones can be obtained at:

- Phone: (800) 524-0024 or (425) 349-1000
- Web: www.teotech.com
- Email: tech@teotech.com

3. Reference Configuration

The test environment simulated a single site with access to external systems via SIP connections. An existing Avaya Modular Messaging server was used for voicemail for endpoints in the test environment. The voicemail configuration was a standard configuration which was not modified for this test and thus will not be described in these notes aside from some routing steps in Avaya Aura® Session Manager and Avaya Aura® Communication Manager.

Figure 1 illustrates the compliance test configuration consisting of:

- Avaya Aura® System Manager
- Avaya Aura® Session Manager
- Avaya Aura® Communication Manager on S8300 Server
- Avaya Modular Messaging
- Avaya Ethernet Routing Switch 5520-24T-PWR
- Avaya G350 Media Gateway
- Avaya SIP telephones
- Teo IP Phones

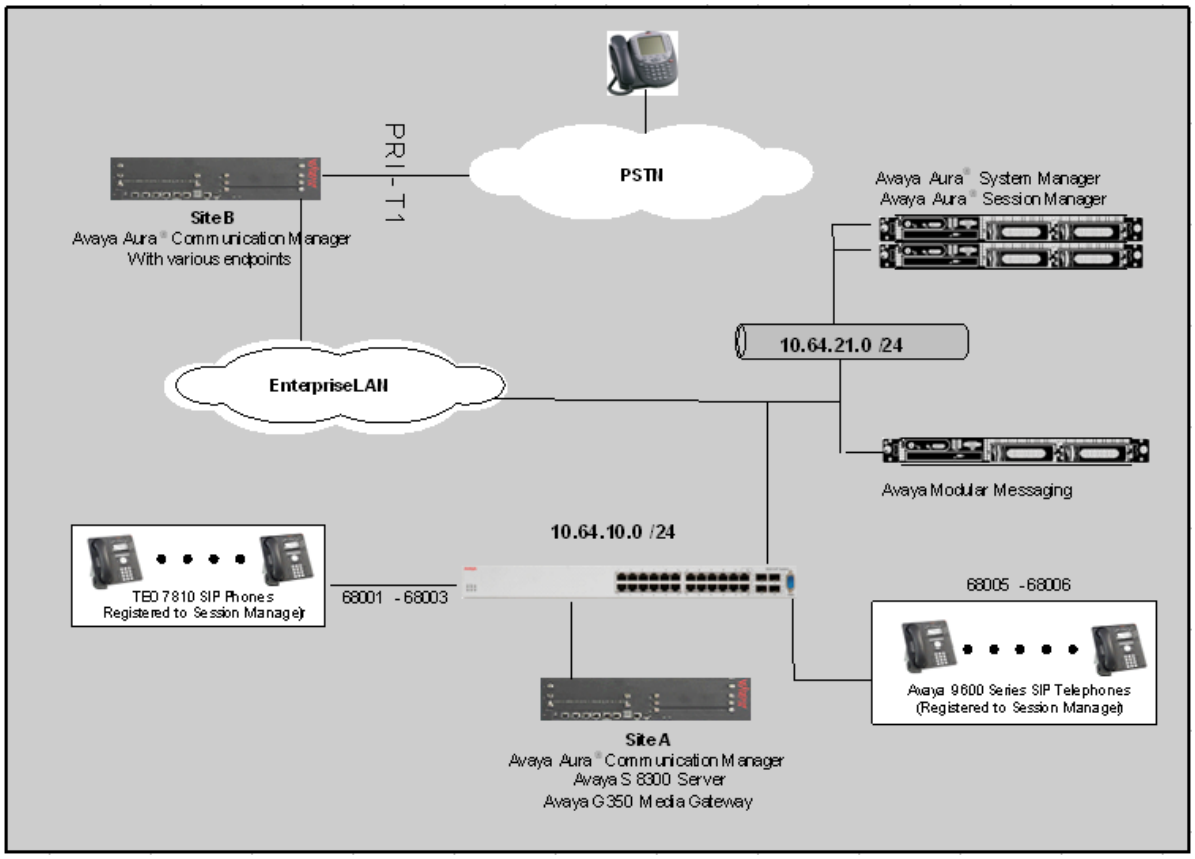


Figure 1 – Teo Phones Configuration

4. Equipment and Software Validated

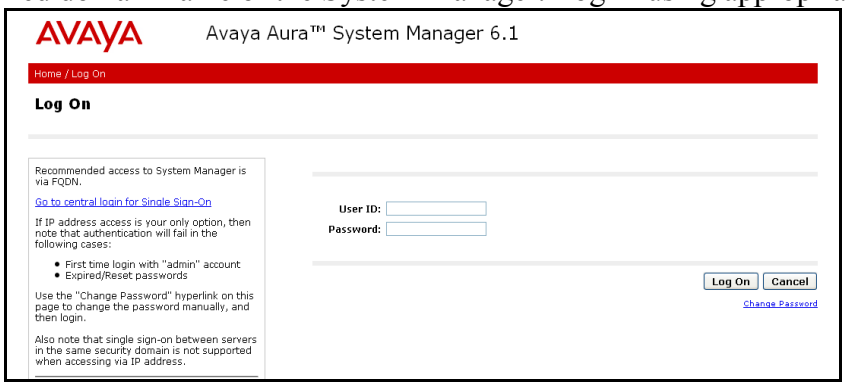
The following equipment and version were used for the sample configuration provided:

Equipment	Version
Avaya Aura® System Manager	6.1.0 (Build No. - 6.1.0.4.5072-6.1.4.11)
Avaya Aura® Session Manager	6.1.0 (Build No. - 6.1.0.0.610023)
Avaya Aura® Communication Manager - Avaya S8300B Server	5.2.1 (R015x.02.1.016.4 -18942)
Avaya Modular Messaging	5.2.1
Avaya G350 Media Gateway	30.18.1
Avaya 9600 Series SIP Phones	Avaya one-X® Deskphone Edition SIP 2.6.3
Teo IP Phones Model 7810 & 7810 TSG-6	05_03_16_71 and 05_80_16_73

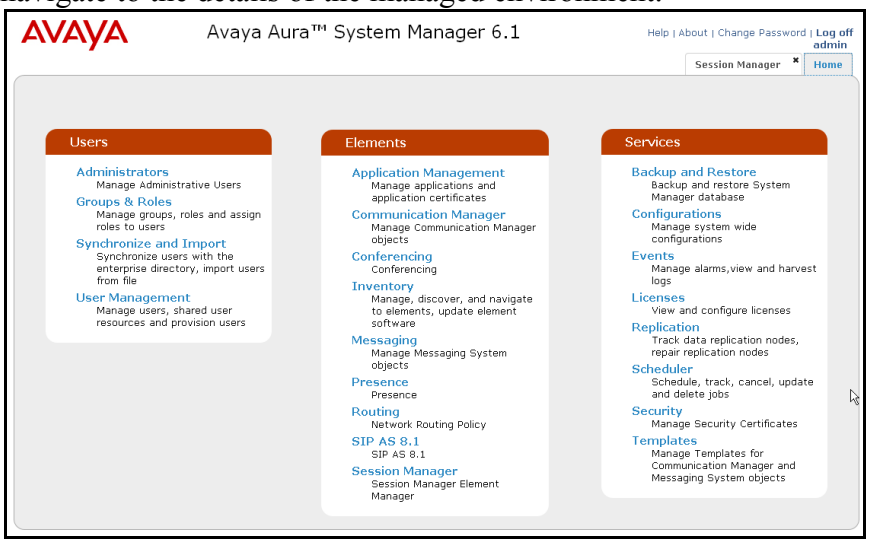
5. Configure Avaya Aura® Session Manager

This section provides the steps for configuring Avaya Aura® Session Manager. For more details, see the administration guide [1].

Session Manager is configured using browser access to System Manager. Enter the URL of System Manager such as https://<hostname>/network-login/SMGR where <hostname> is the ip address or qualified domain name of the System Manager. Log in using appropriate credentials.



The home page is a navigation screen as shown below. Each of these links will open a new tab from which to navigate to the details of the managed environment.

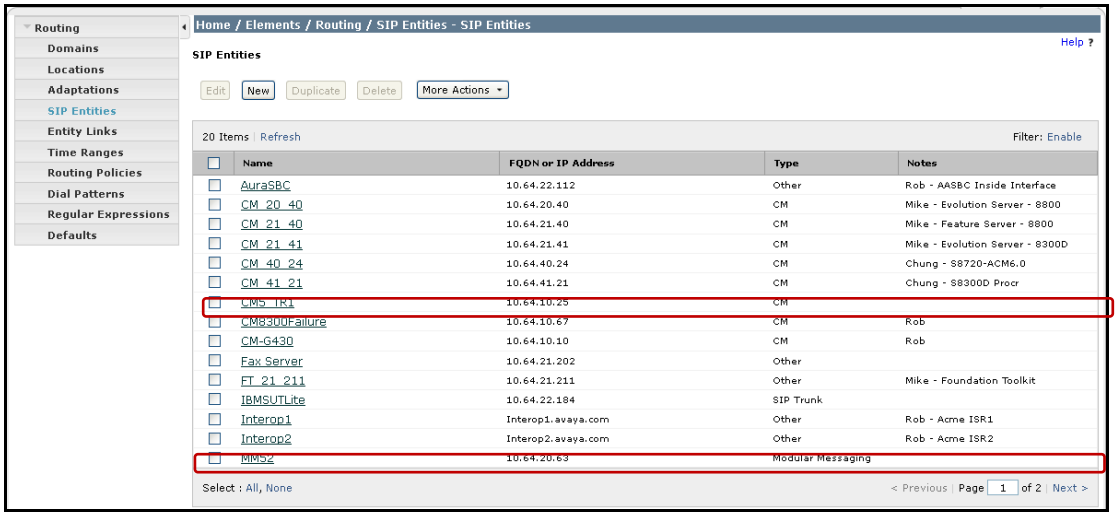
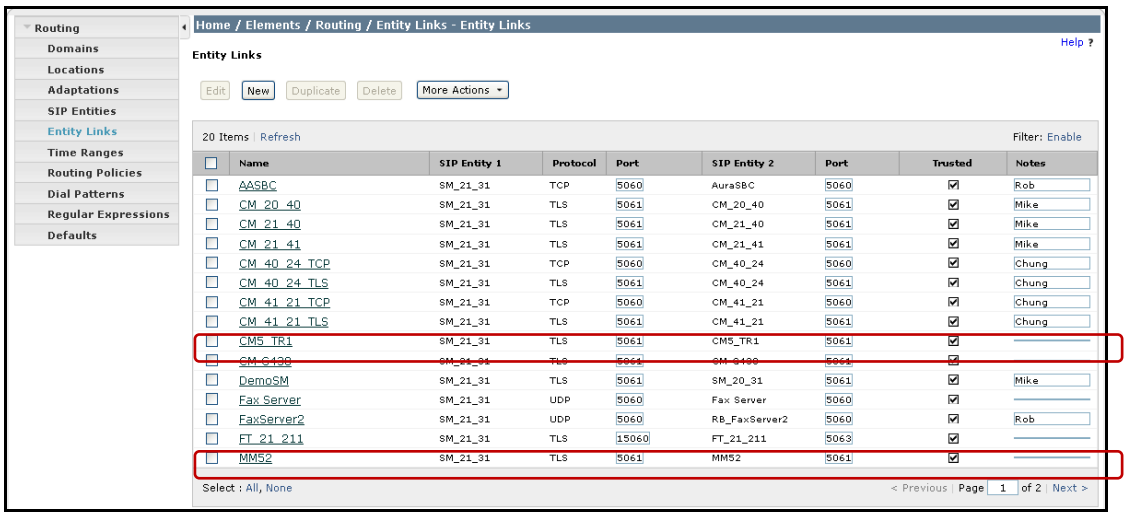


5.1. Session Manager Configuration Details

The steps required to configure the test environment for the Teo IP Phone testing are outlined as follows:

1. Configure Routing for Endpoints and Messaging – Entities and Entity Links
2. Configure Routing for Endpoints and Messaging – Routing Policies and Dial Patterns
3. Add Teo Users

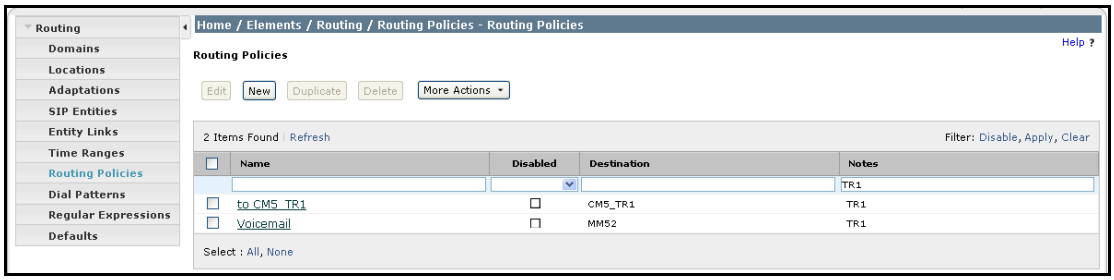
4. Configure the Teo Endpoints
5. Synchronize the System Manager data with Communication Manager

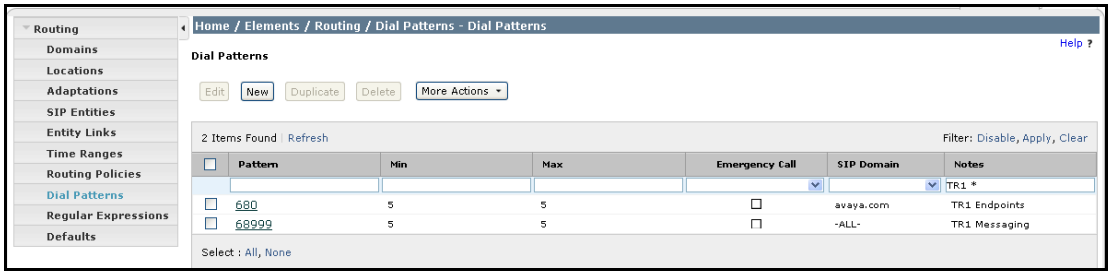
Step	Description
1.	**Configure Routing for Endpoints and Messaging – Entities and Entity Links** Note, the endpoint and messaging routing was in place prior to this test. The following screens are provided for reference to provide a more complete picture of the test environment. Details on configuring these steps can be found in the administration guide [1]. SIP calls to endpoints were routed to the Communication Manager **SIP Entity** "***CM5_TR1***" using the **Entity Link** "***CM5_TR1***". SIP calls for messaging were routed to the Modular Messaging **SIP Entity** "***MM52***" using the **Entity Link** "***MM52***" as shown below.  

2.

Configure Routing for Endpoints and Messaging – Routing Policies and Dial Patterns

The existing **Routing Policy** "***To CM5_TR1***" was used for calls to endpoints using the "***680***" **Dial Pattern**, and the existing **Routing Policy** "***Voicemail***" was used to route calls to the Modular Messaging server using the "***68999***" **Dial Pattern**.

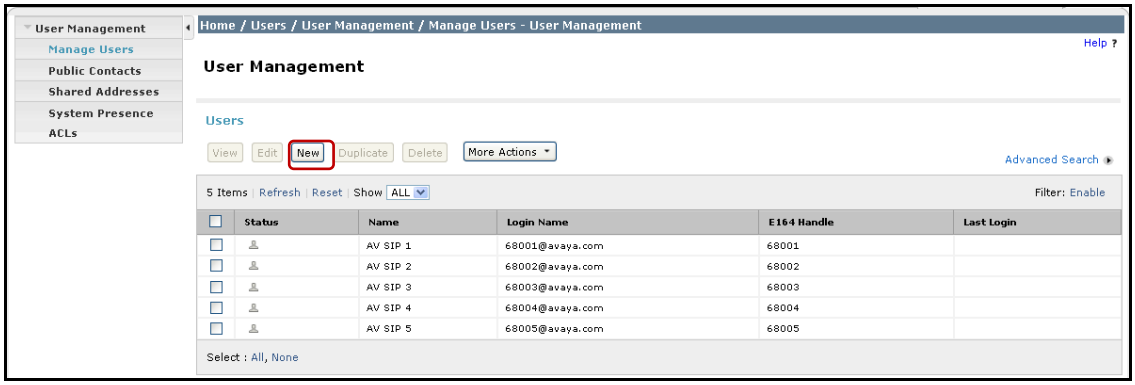




3. **Add Teo Users**

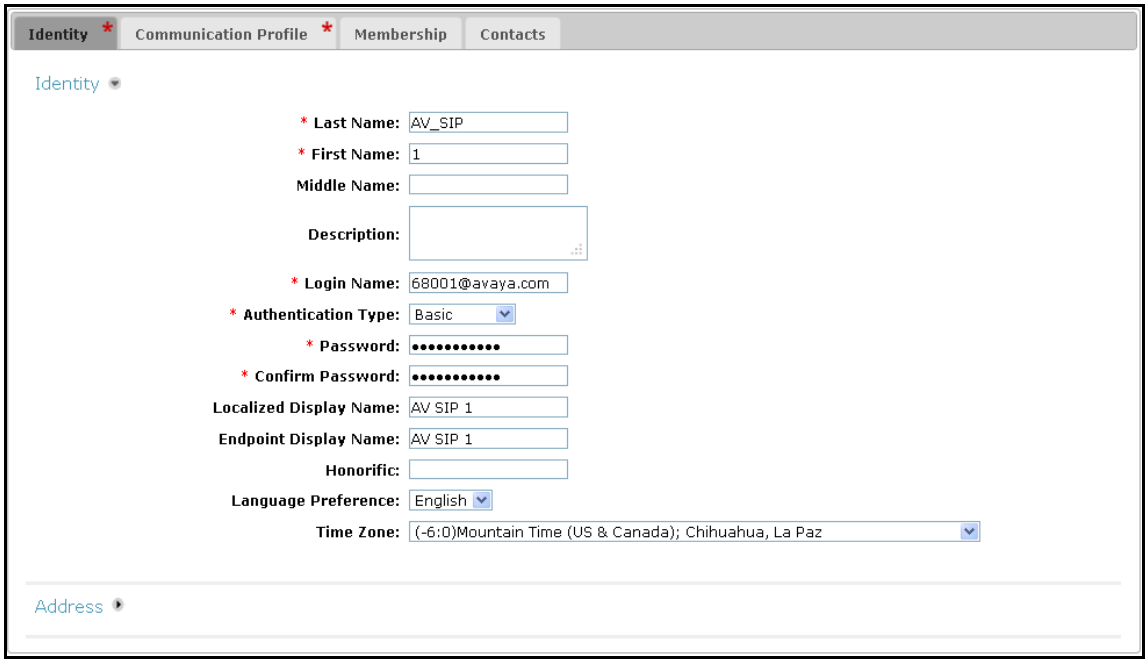
The following steps describe the creation of three Teo user logins. Each user was configured identically, so the steps used for the first user were repeated until all three user accounts were completed. In the screenshot below, the 5 SIP endpoints (2 Avaya, 3 Teo) used in this test environment are listed.

Click on the **New** button on the **Manage Users** > **User Management** page in order to display the **New User Profile** form. This step requires several subtasks which follow on the next few pages.



Add Teo Users (Continued)

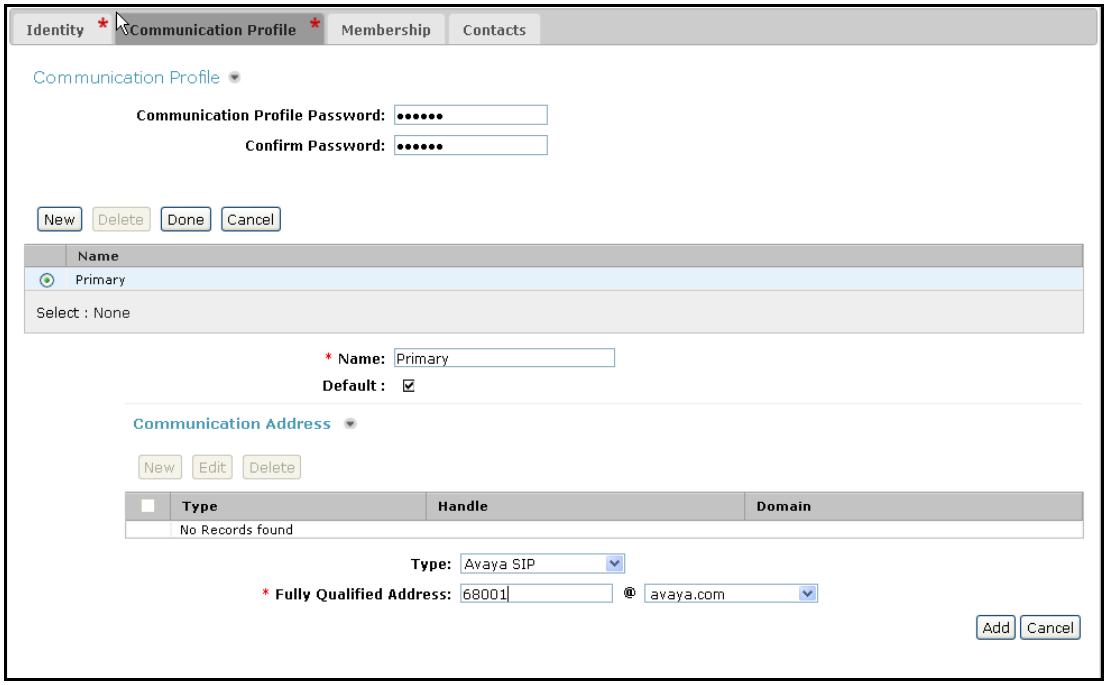
On the **New User Profile** form, enter a meaningful description for the **Last Name** and **First Name** fields, and enter the extension@domain_name in the **Login Name** field ("***68001@avaya.com***" was used in this example). Leave the **Authentication Type** as "***Basic"*** (Default). Provide the System Manager password in the **Password** and **Confirm Password** field for the Administrator user account being used to create the user profile. Enter a preferred display name in the **Localized Display Name** and **Endpoint Display Name** fields. Select the **Language Preference** and **Time Zone** for the endpoint, then select the **Communication Profile** tab to continue configuration for this endpoint.



Add Teo Users (Continued)

On the **Communication Profile** tab of the **New User Profile** form, enter the station login password in the **Communication Profile Password** and **Confirm Password** fields. Leave the default **Name** (***Primary***).

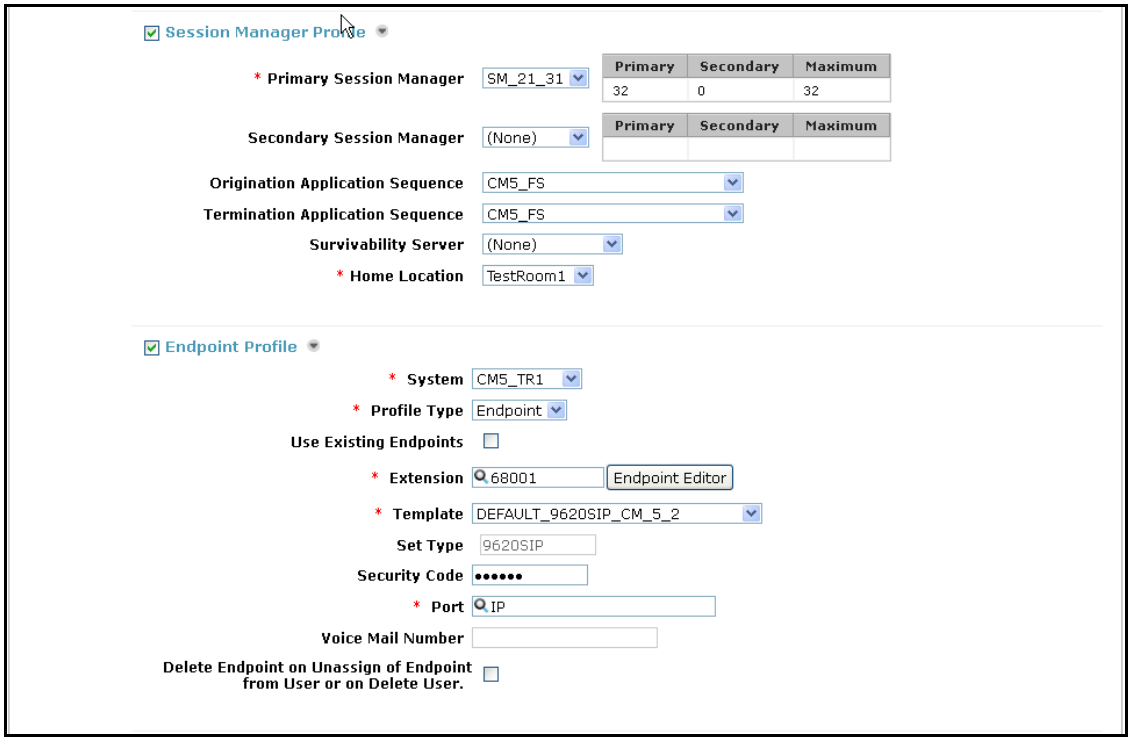
Click **New** to expand the **Communication Address** section to enable entry of the **Fully Qualified Address** "***68001***" as shown. If more than one domain name is being used on the System Manager, select the appropriate domain name and then click on the **Add** button.



Add Teo Users (Continued)

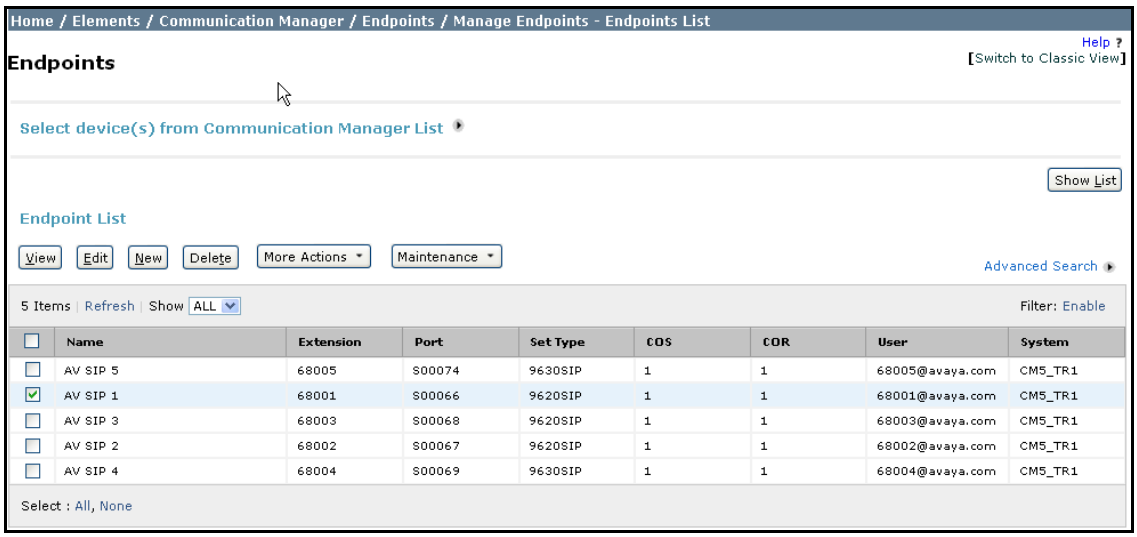
Click the arrow next to the **Session Manager Profile** header to enable selection of the **Primary Session Manager** ("***SM_21_31***" in this example), **Originating** and **Terminating Application Sequences** ("***CM5_FS***" in this example), and **Home Location** ("***TestRoom1***" in this example).

Click the arrow next to the **Endpoint Profile** header to enable selection of the remaining settings for the user profile. For **System**, select the Communication Manager the endpoint will be associated with ("***CM5_TR1***" was used in this example), and leave the **Profile Type** as "***Endpoint"*** (default). Enter the **Extension** to be associated with the endpoint ("***68001***" was used in this example), select an appropriate **Template** ("***Default_9620SIP_CM_5_2***" was used in this example). Provide the station login password ("***123456***" which is the same as **Communication Profile Password** on the previous page) in the **Security Code** field. Select "***IP***" for the **Port** type. Press the **Commit** button (not shown) to save the settings.

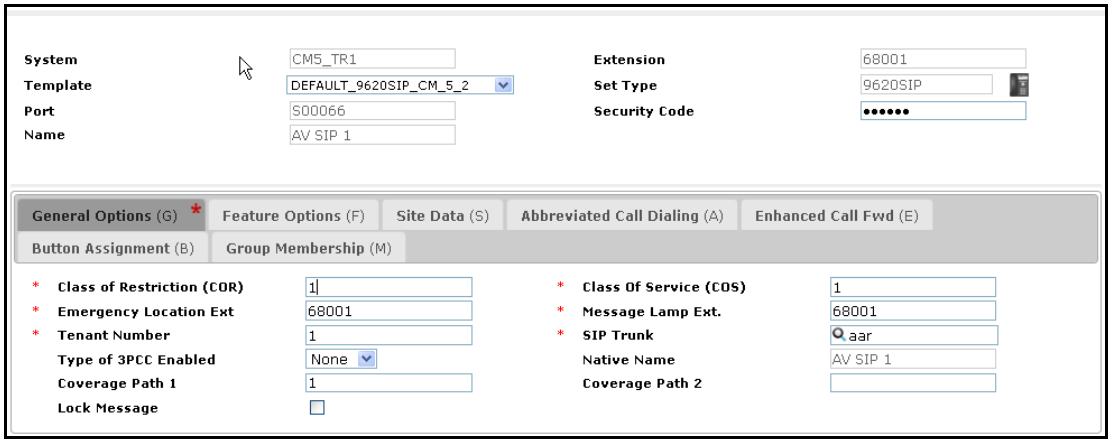


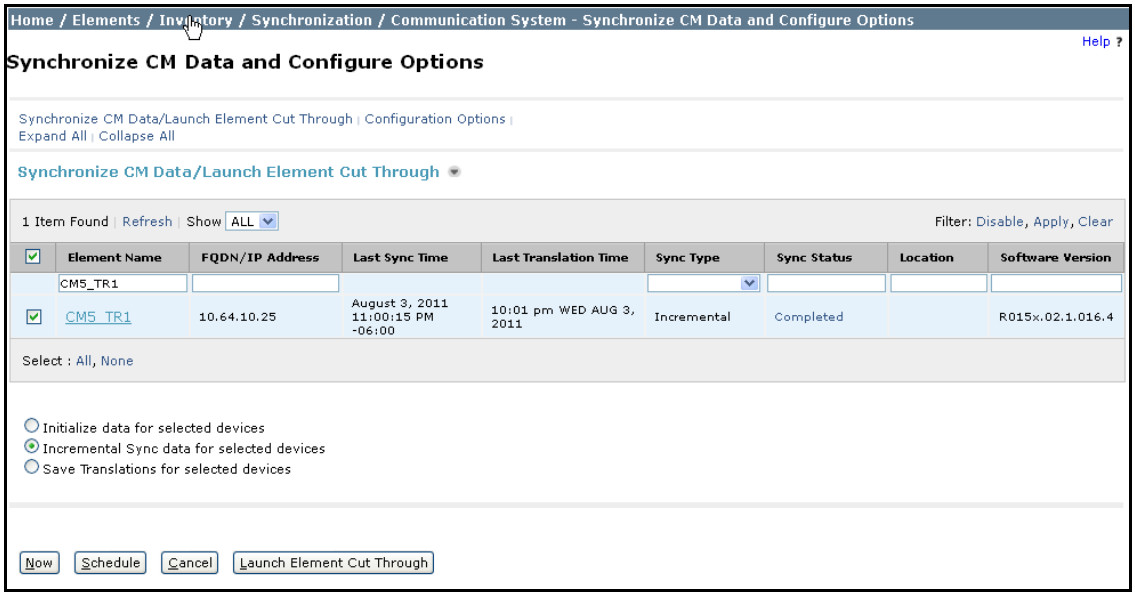
4. **Configure the Teo Endpoints**

Navigate to the **Elements>Communication Manager>Endpoints>Manage Endpoints** form and select the device created in **Step 3** above, and click the **Edit** button.



On the **Edit Endpoint** form, enter the Coverage Path that will route calls to Modular Messaging in the **Coverage Path 1** field. In this example, Coverage Path "***1***" was used; further details can be seen in the Communication Manager configuration in **Section 6, Step 2**.



5.	**Synchronize the System Manager data with Communication Manager** Navigate to **Inventory > Synchronization > Communication System** and select the Communication Manager to synch the new user and endpoint data with. Use the **Incremental Synch data for selected devices** option and choose the appropriate timing (**Now** or **Schedule**). 

6. Configure Avaya Aura® Communication Manager

Communication Manager used an existing configuration with SIP trunks to connect to Avaya Aura® Session Manager. Configuration of this aspect of the integration was standard and not directly relevant to the interoperability of Teo IP Phones. These Application Notes will not cover the full details of this aspect of the configuration, however some overview will be covered for Application Note completeness.

Tasks associated with configuring SIP endpoints were done on System Manager and were covered in **Section 5** above.

The configuration steps in Communication Manager that were specific to this test plan were:

- Configure Dial Plan and AAR
- Configure Coverage Path for Voicemail
- Configure Feature Access Code (FAC) and Feature Name Extensions (FNE)
- Note the Codecs in use

1. **Configure Dial Plan and AAR**

Routing rules were configured in order to route calls to 5 digit extensions matching the pattern ***68x*** (SIP endpoints) and ***68999*** (Modular Messaging) to Session Manager over a SIP Trunk.

First, the **change dialplan analysis** command was used to define these patterns. In addition, the 3 digit ***0xx*** pattern was defined as a ***fac*** (Feature Access Code) pattern, and the 4 digit ***5xxx*** pattern was defined as ***ext*** (Extension) for the Feature Name Extensions (FNE) described in **step 3** below.

Note: SIP endpoints are managed as Off Premise Stations, **aar** is used to define route patterns for OPS stations.

```
change dialplan analysis                                        Page   1 of  12
                            DIAL PLAN ANALYSIS TABLE
                                 Location:  all           Percent Full:    2

      Dialed   Total  Call    Dialed   Total  Call     Dialed   Total  Call
      String   Length Type    String   Length Type     String   Length Type
    0           3    fac
    1           3    fac
    2           5    ext
    5           4    ext
    6           4    aar
    68          5    ext
    8           1    fac
    9           1    fac
    *           2    fac
    *           3    fac
    *           4    dac
    #           2    fac
    #           3    fac
```

The **change aar analysis 6** command was used to specify that calls to 4 digit dialed numbers ***(6xxx)*** and 5 digit ***(68xxx)*** would use route pattern ***1*** to reach Session Manager. The 4 digit 6xxx extensions were on a tandem Communication Manager with H.323, DCP and Analog sets).

```
change aar analysis 6                                           Page   1 of   2
                            AAR DIGIT ANALYSIS TABLE
                                 Location:  all           Percent Full:    2

         Dialed           Total     Route    Call   Node  ANI
         String         Min  Max  Pattern   Type   Num   Reqd
    6                   4    4    1         aar           n
    6                   5    5    1         aar           n
```

Trunk Group 1 and Signaling Group 1 were already in place as SIP facilities connecting to Session Manager. Route Pattern 1 was also in place and defined Trunk Group 1 as the facility to use. Details on configuring these items are described in [2].

2. **Configure Coverage Path for Voicemail**

Coverage Path 1 was defined, and assigned to all extensions in order to route calls to Communication Manager Messaging. The **change coverage path 1** command was used to define Coverage Criteria rules for **Busy, Don't Answer, Do Not Disturb (DND), Send all Calls (SAC),** and **Goto Cover** by setting the flag for internal and external calls to "***y***" as shown below. Additionally, **Rng:** was set to "***4***" to define that after 4 rings, the call should go to the Coverage Point "***h1***".

```
change coverage path 1                                          Page   1 of   1
                                COVERAGE PATH

                 Coverage Path Number: 1
    Cvg Enabled for VDN Route-To Party? n        Hunt after Coverage? n
                      Next Path Number:          Linkage

COVERAGE CRITERIA
    Station/Group Status    Inside Call     Outside Call
             Active?            n               n
               Busy?            y               y
       Don't Answer?            y               y         Number of Rings: 4
                All?            n               n
 DND/SAC/Goto Cover?            y               y
   Holiday Coverage?            n               n

COVERAGE POINTS
    Terminate to Coverage Pts. with Bridged Appearances? n
  Point1: h1             Rng: 4  Point2:
  Point3:                        Point4:
  Point5:                        Point6:
```

Coverage Point h1 defined above means that calls will be routed to Hunt Group 1. The **change hunt-group 1** command was used to configure the hunt group. The **Group Extension** "***68999***" was used to assign a valid extension to the hunt group for routing rules defined above in **Step 1**. The hunt group was defined as associated with **Coverage Path** "***1***". A meaningful **Group Name** "***VM***" was used, and the **Group Type** was set to "***ucd-mia***".

```
change hunt-group 1                                             Page   1 of  60
                                HUNT GROUP

           Group Number: 1                                 ACD? n
             Group Name: VM                              Queue? n
        Group Extension: 68999                           Vector? n
             Group Type: ucd-mia                 Coverage Path:
                     TN: 1          Night Service Destination:
                    COR: 1                    MM Early Answer? n
          Security Code:               Local Agent Preference? n
 ISDN/SIP Caller Display:
```

3. **Configure Feature Access Code (FAC) and Feature Name Extensions (FNE)**

Third Party SIP phones generally are not able to define buttons to be associated with Communication Manager features. The equivalent functionality is accomplished by defining an FAC and FNE to invoke the features. In the test, the primary line was taken off hook and the FAC or FNE was dialed. This approach did not require routing rules for the dialed digits as the gateway interpreted the DTMF.

Speed dials can be programmed on the phones to simplify user interactions. Use of speed dials would require additional routing configuration in both Communication Manager and Session Manager in order to properly route based on the dialed digit patterns. This method was not used in the test and is therefore not described in these Application Notes but would generally follow the routing steps described above for voicemail and SIP phones.

The **change feature-access-codes** command was used to define the following (list edited for brevity, not all features were tested):

```
change feature-access-codes                                    Page   1 of   8
                              FEATURE ACCESS CODE (FAC)
     Auto Alternate Routing (AAR) Access Code: 8
   Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                Automatic Callback Activation: 001    Deactivation: 002
Call Forwarding Activation Busy/DA: 003    All: 004    Deactivation: 005
                       Call Park Access Code: 006
                     Call Pickup Access Code: 007
CAS Remote Hold/Answer Hold-Unhold Access Code: 008
              Directed Call Pickup Access Code: 009
                Last Number Dialed Access Code: 010
    Leave Word Calling Message Retrieval Lock: 011
  Leave Word Calling Message Retrieval Unlock: 012
                    Send All Calls Activation: 013    Deactivation: 014
```

In addition, the change **off-pbx-telephone feature-name-extensions set 1** command was used to define FNEs (list edited for brevity, not all features were tested):

```
change off-pbx-telephone feature-name-extensions set 1          Page   1 of   2
     EXTENSIONS TO CALL WHICH ACTIVATE FEATURES BY NAME
                    Set Name: SIP Phones

            Automatic Call Back: 5000
     Automatic Call-Back Cancel: 5001
               Call Forward All: 5002
    Call Forward Busy/No Answer: 5003
            Call Forward Cancel: 5004
                      Call Park: 5005
           Call Park Answer Back: 5006
                  Call Pick-Up: 5007
          Conference on Answer: 5008
          Drop Last Added Party: 5009
         Idle Appearance Select: 5013
             Last Number Dialed: 5010
                 Send All Calls: 5011
          Send All Calls Cancel: 5012
```

4.	**Note the Codecs in use** All endpoints and gateways used the Codec Set 1. The codecs shown below were active in the system, these were changed at times during the testing to ensure the Teo phones properly negotiated codecs with the gateway.

```
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.722.1-32K                 1        20
 2: G.711MU           n         2        20
 3: G.729             n         2        20
 4:
```

7. Configure Avaya Modular Messaging

Avaya Modular Messaging was configured prior to the testing, details of the configuration are beyond the scope necessary to enable Teo phones to interoperate with Session Manager and Communication Manager. Details on how to configure this messaging solution can be found in [3].

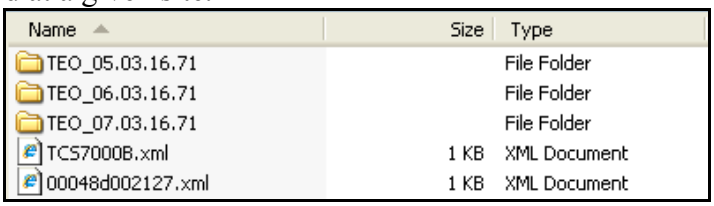
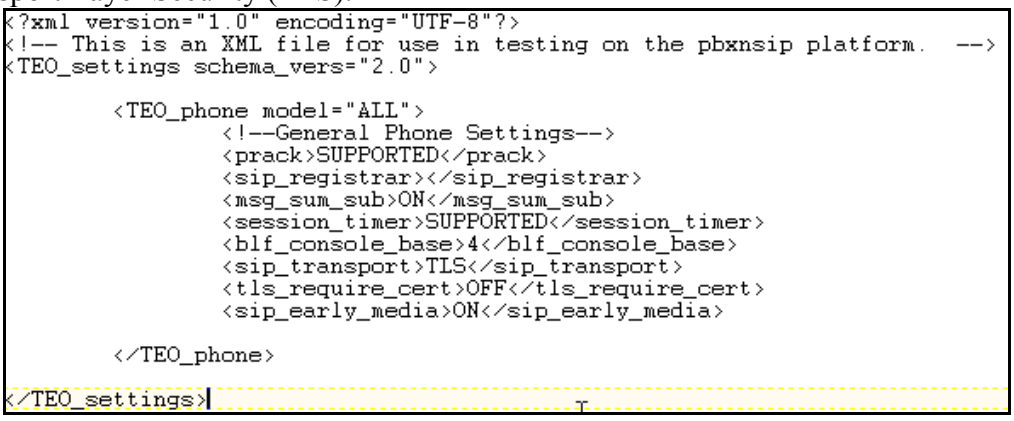
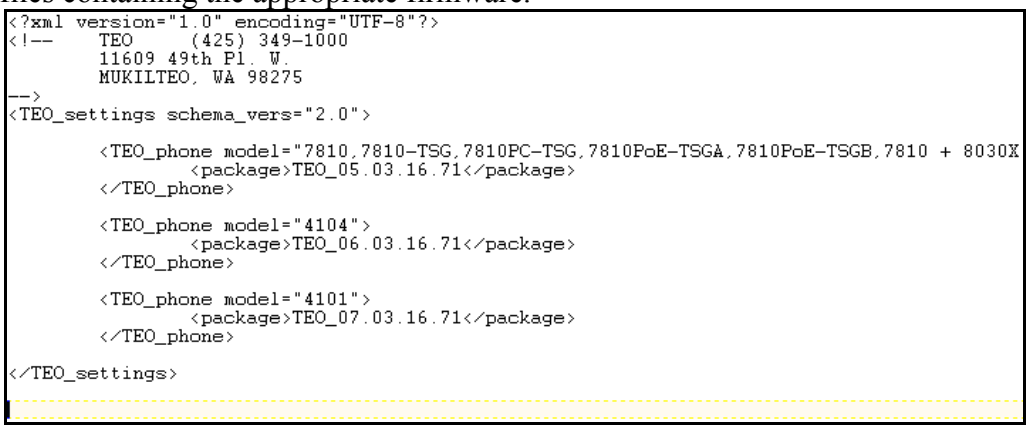
8. Configure Teo Phones

Teo IP Phones are configured using a combination of XML tags in a settings file stored on an FTP, TFTP or HTTP server, and manual configuration settings performed directly on the phones. The phones use DHCP by default and are powered over their Ethernet port. In the tested configuration, the phones were connected to the LAN via an Avaya BayStack 5520-PWR network switch on a segment with a DHCP server.

8.1. Teo Configuration Details

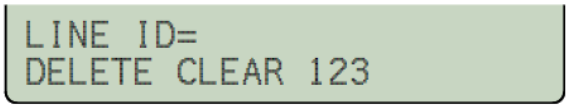
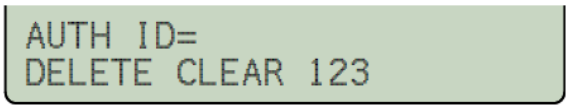
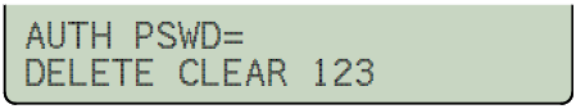
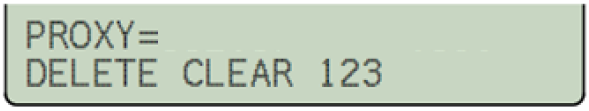
In general, the steps were as follows:

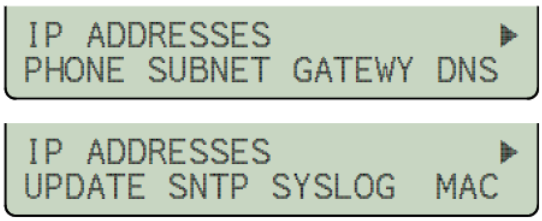
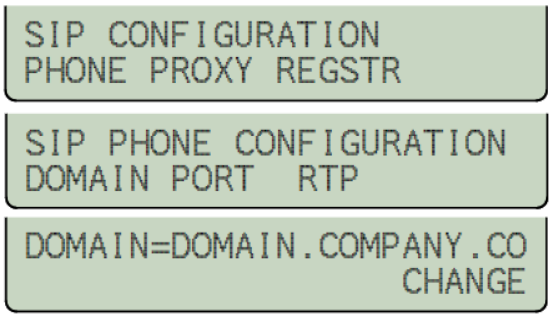
- Copy the phone firmware, settings and upgrade files to the TFTP Server
- Provide initial phone configuration parameters
- Modify any settings as necessary on the phone

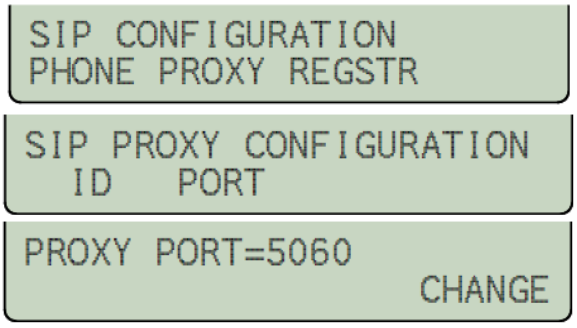
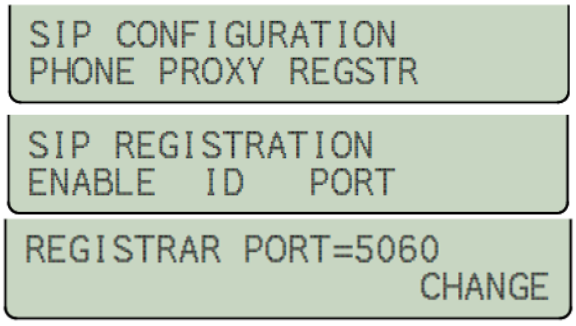
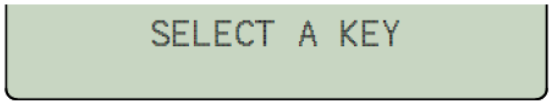
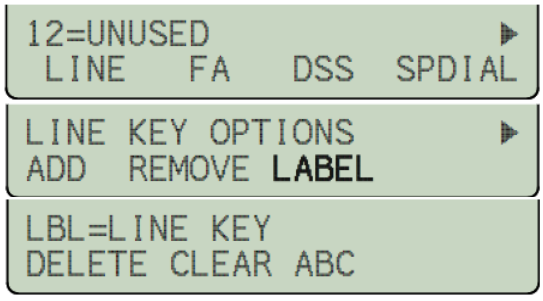
Step	Description
1.	**Copy the phone firmware, settings and upgrade files to the TFTP Server** An existing Windows 2003 Server running a TFTP service was used in this step. The Teo IP Phone firmware, upgrade settings file, and phone settings file were copied to the root FTP folder on the TFTP server. This process will vary based on the FTP, TFTP or HTTP server used at a given site.  For each phone, a copy of a phone settings file was placed in the root folder and re-named to match the phone's hardware MAC address. Any unique settings that were used for the phone were specified by adding XML tags to the file. Below is a look at the settings for one of the phones. Note that this phone was successfully tested using Transport Layer Security (TLS).  A firmware upgrade settings file like the one below will point the phone to the folder and files containing the appropriate firmware. 


```
<?xml version="1.0" encoding="UTF-8"?>
<!-- This is an XML file for use in testing on the pbxnsip platform.  -->
<TEO_settings schema_vers="2.0">

        <TEO_phone model="ALL">
                <!--General Phone Settings-->
                <prack>SUPPORTED</prack>
                <sip_registrar></sip_registrar>
                <msg_sum_sub>ON</msg_sum_sub>
                <session_timer>SUPPORTED</session_timer>
                <blf_console_base>4</blf_console_base>
                <sip_transport>TLS</sip_transport>
                <tls_require_cert>OFF</tls_require_cert>
                <sip_early_media>ON</sip_early_media>

        </TEO_phone>

</TEO_settings>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<!--    TEO     (425) 349-1000
        11609 49th Pl. W.
        MUKILTEO, WA 98275
-->
<TEO_settings schema_vers="2.0">

        <TEO_phone model="7810,7810-TSG,7810PC-TSG,7810PoE-TSGA,7810PoE-TSGB,7810 + 8030X
                <package>TEO_05.03.16.71</package>
        </TEO_phone>

        <TEO_phone model="4104">
                <package>TEO_06.03.16.71</package>
        </TEO_phone>

        <TEO_phone model="4101">
                <package>TEO_07.03.16.71</package>
        </TEO_phone>

</TEO_settings>
```

Step	Description
2.	**Provide initial phone configuration parameters** Connect the Teo IP Phone to the network and power. As the phone is initializing, the display will prompt for the following entries for each phone: **LINE ID** is the Extension (**68001** for example) entered in **Section 5.1, Step 3** above. This is the extension in Communication Manager, and the User ID in Session Manager. Press the **OK** key on the phone when entry is complete.  **AUTH ID** is the same as the **LINE ID.** Press the **OK** key when entry is complete.  **AUTH PSWD** is the Password entered in **Section 5.1, Step 3** above for the phone **Security Code** and **Communication Profile Password**. Press the **OK** key when entry is complete.  **PROXY** is the IP Address of the Session Manager. Press the **OK** key when entry is complete.  At this point, the phone will register with the Session Manager. Upon successful registry, the LEDs for Lines 1 through 3 will illuminate momentarily and the idle display indicating date and time will be shown.

Step	Description
3.	**Modify any settings as necessary on the phone** The display on the Teo phones contains context sensitive menus. Most programming is initiated by pressing the dedicated **SETUP** button on the phone, then the corresponding button under each menu option, and finally **OK** or **SETUP** again to write the changes to the phone's configuration. In the following instructions, **SETUP>INSTL>IP** would indicate to press the dedicated **SETUP** button, then the context sensitive **INSTL** button and so on. If the ▶ symbol appears in the string, this indicates to press the right arrow key to scroll right to see more menu options. Common settings that need to be made for interoperability with the Avaya environment include: • **UPDATE** server (TFTP/FTP or HTTP as described in **Step 1** above) • **SIP** Configuration (Domain Name, Proxy/port (if other than UDP), Registrar (if different than the Proxy set in **Step 2**). • **Key** Labels (the phone's extension on the first three line buttons). To set the **UPDATE** server, click **SETUP> INSTL> IP>** ▶ **>UPDATE** and enter the IP Address of the FTP/TFTP or HTTP server where updated firmware files can be found. Press the **OK** key when entry is complete.  To set the SIP domain and update the Proxy and Registrar settings (for TLS ports for example), press **SETUP>INSTL>SIP>PHONE>DOMAIN** to enter the domain (avaya.com was used in the test). Press the **OK** key when entry is complete. 

Step	Description
	Modify any settings as necessary on the phone (Continued) To modify the Registrar and Proxy ports (5060 is default for UDP signaling, and 5061 would need to be set when using TLS), press **SETUP>INSTL>SIP>PROXY>PORT** to set the Proxy port. Press the **OK** key when entry is complete.  Press **SETUP>INSTL>SIP>REGSTR>PORT** to set the Registrar port. Press the **OK** key when entry is complete.  To label the Line Keys, press **SETUP>INSTL>KEYS** and select the key you want to label.  Select **LINE>LABEL>CLEAR** then enter the extension number and press the **OK** key when entry is complete.  From the above, one can see that there are many more options such as Speed Dial that can be set. These Application Notes do not cover every option. See the product guides [4 – 6] for more information.

9. Verification Steps

Calls were placed to and from the Teo and Avaya SIP phones manually. Confirmation of functionality was generally observed by listening for audio on connected calls. Tracing was used on Avaya Aura® Session Manager, and using Wireshark from a locally connected PC to review SIP messages to and from the phones.

10. Conclusion

The Teo IP Phones successfully interoperated with the Avaya SIP environment as described in these notes.

11. Additional References

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

[1] *Administering Avaya Aura™ Session Manager*, Document ID 03-603324, Issue 1, Release 6.1, November, 2010.
[2] *Administering Avaya Aura™ Communication Manager,* Document ID 03-300509, Issue 5.0, Release 5.2, May, 2009.
[3] *Modular Messaging - Messaging Application Server (MAS) Administration Guide,* November 2009

Product documentation for Teo products may be found at www.teotech.com.

[4] *IP Telephone Network Administration Guide*, Document ID 13-280132 Rev. D March 2011
[5] *IP Phone 7810 TSG Series Installation Instructions*, Document ID 13-280138 Rev. B March 2011
[6] *IP Phone 7810 TSG Series User Guide,* Document ID 14-280211 Rev. B March 2011

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.