Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Yealink T-28 SIP Phones with Avaya Aura® Communication Manager and Avaya Aura® Session Manager - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for the Yealink T-28 SIP phone to interoperate with Avaya Aura® Communication Manager and 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 the steps required to connect Yealink T-28 Handset to a SIP infrastructure consisting of Avaya Aura® Session Manager and Avaya Aura® Communication Manager. The Yealink T-28 Handset is a display handset with 5 line appearances, 4 soft keys and 10 feature buttons. Also described is how Avaya Aura® Communication Manager features can be made available in addition to the standard features supported in the T-28 handset. In this configuration, the Off-PBX Stations (OPS) feature set is extended from Avaya Aura® Communication Manager to the T-28 Handset, providing the T-28 Handset with enhanced calling features.

2. General Test Approach and Test Results

To verify interoperability of Yealink T-28 handset with Communication Manager and Session Manager, calls were made between T-28 handset and Avaya SIP, H.323 and Digital stations using various codec settings and exercising common PBX features. The telephony features were activated and deactivated using pre-programmed buttons. Yealink T-28 handset passed all compliance testing with all scenarios resulting in the expected outcome.

2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- Successful registration of T-28 handset with Session Manager
- Calls between T-28 handset and Avaya SIP, H.323, and digital stations
- G.711 and G729 codec support
- PBX features including Multiple Call Appearances, Hold, Transfer, and Conference
- Proper system recovery after an T-28 handset restart and loss of IP connection
- Correct T-28 handset behavior during Session Manager and Communication Manager simulated network failures.

2.2. Test Results

During testing the Yealink T-28 handset completed all scenarios with results in all cases as expected.

2.3. Support

Technical support from Yealink can be obtained through the following:

Phone: +44 (0)161 763 2060
E-mail: sales@yealink.co.uk.
Web: http://www.yealink.co.uk

3. Reference Configuration

The diagram illustrates an enterprise site with an Avaya SIP-based network, including a Session Manager, S8800 Media Server running Communication Manager with a G650 Media Gateway, and Avaya IP endpoints. The enterprise site also contains one T-28 handset and one T-26 handset used to verify call functionality between Yealink handsets. The SIP handsets are registered with Session Manager and are configured as endpoint users. Communication Manager extends the telephony functionality that is supported by the SIP-based T-28 device through the use of Feature Name Extensions (FNEs).

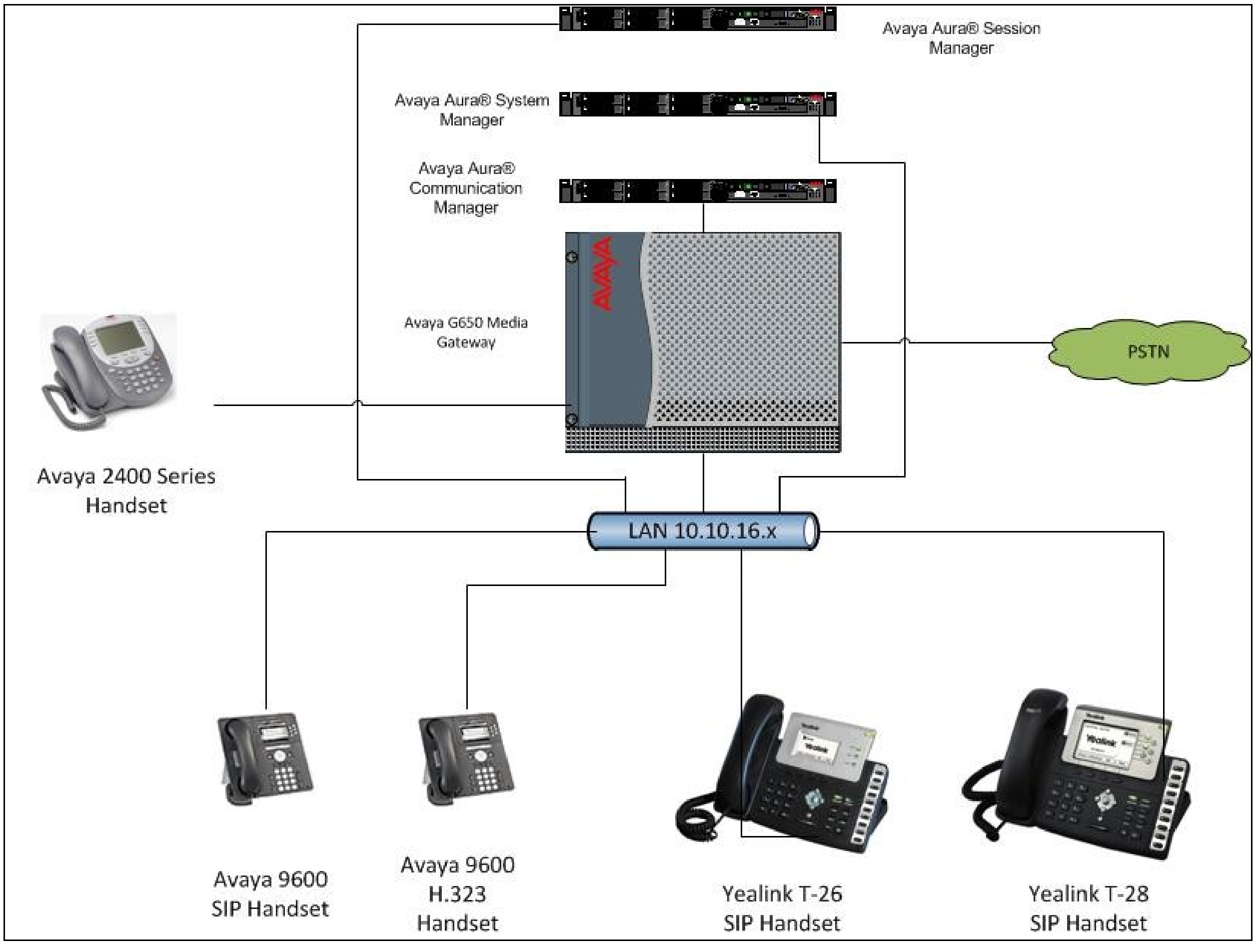


Figure 1: T-28 with Avaya SIP Solution

4. Equipment and Software Validated

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

Equipment	Software
Avaya S8800 Media Server with G650 Media Gateway	Avaya Aura® Communication Manager 6.0.1 (R16x.0.0.345.0-18444)
Avaya S8800 Media Server	Avaya Aura® Session Manager 6.1 (Build 6.1.0.0.610023)
Avaya S8800 Media Server	Avaya Aura® System Manager 6.1 (Build 6.1.0.4.5072-6.1.4.113)
Avaya 9600 Series Handsets	2.6.4.0 (SIP)
Avaya 9600 Series Handsets	3.1 (H.323)
Yealink T-26 Handset	6.60.23.5
Yealink T-28 Handset	2.60.23.5

5. Configure Avaya Aura® Communication Manager

This section describes the steps for configuring the T-28 handset as an Off-PBX Station (OPS) and configuring a SIP trunk between Communication Manager and Session Manager. Use the System Access Terminal (SAT) to configure Communication Manager. Log in with the appropriate credentials. The configuration steps described are also applicable to other Linux-based Avaya Servers and Media Gateways running Avaya Aura® Communication Manager.

5.1. Verify System Capacity

The license file installed on the system controls these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative. Use the **display system-parameters customer-options** command to determine these values. On **Page 1**, verify that the **Maximum Off-PBX Telephones** allowed in the system is sufficient. One OPS station is required per T-28 handset.

```
display system-parameters customer-options                      Page   1 of  10
                                OPTIONAL FEATURES

     G3 Version: V15                              Software Package: Standard
       Location: 2                             RFA System ID (SID): 1
       Platform: 6                             RFA Module ID (MID): 1

                                                              USED
                                Platform Maximum Ports: 48000 282
                                      Maximum Stations: 36000 48
                              Maximum XMOBILE Stations: 0     0
                    Maximum Off-PBX Telephones - EC500: 200   0
                    Maximum Off-PBX Telephones -   OPS: 200   18
                    Maximum Off-PBX Telephones - PBFMC: 0     0
                    Maximum Off-PBX Telephones - PVFMC: 0     0
                    Maximum Off-PBX Telephones - SCCAN: 0     0
```

On **Page 2** of the **System-Parameters Customer-Options** form, verify that the number of **Maximum Administered SIP Trunks** supported by the system is sufficient.

```
display system-parameters customer-options                     Page   2 of  10
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                              USED
                     Maximum Administered H.323 Trunks: 200    0
           Maximum Concurrently Registered IP Stations: 18000 1
             Maximum Administered Remote Office Trunks: 0      0
Maximum Concurrently Registered Remote Office Stations: 0      0
              Maximum Concurrently Registered IP eCons: 0      0
  Max Concur Registered Unauthenticated H.323 Stations: 0      0
                        Maximum Video Capable Stations: 0      0
                   Maximum Video Capable IP Softphones: 0      0
                       Maximum Administered SIP Trunks: 300    138
  Maximum Administered Ad-hoc Video Conferencing Ports: 0      0
   Maximum Number of DS1 Boards with Echo Cancellation: 100    0
                             Maximum TN2501 VAL Boards: 128    0
                     Maximum Media Gateway VAL Sources: 0      0
           Maximum TN2602 Boards with 80 VoIP Channels: 128    0
          Maximum TN2602 Boards with 320 VoIP Channels: 128    0
   Maximum Number of Expanded Meet-me Conference Ports: 0      0

        (NOTE: You must logoff & login to effect the permission changes.)
```

5.2. Define System Features

Use the **change system-parameters features** command to administer system wide features for SIP endpoints. These are all standard Communication Manager features that are also available to OPS stations. On **Page 17** set **Whisper Page Tone Given To: all**

```
change system-parameters features                              Page  17 of  18
                        FEATURE-RELATED SYSTEM PARAMETERS

INTERCEPT TREATMENT PARAMETERS
       Invalid Number Dialed Intercept Treatment: tone
                   Invalid Number Dialed Display:
    Restricted Number Dialed Intercept Treatment: tone
                Restricted Number Dialed Display:
   Intercept Treatment On Failed Trunk Transfers? n

WHISPER PAGE
   Whisper Page Tone Given To: all

6400/8400/2420J LINE APPEARANCE LED SETTINGS
                    Station Putting Call On Hold: green  wink
                     Station When Call is Active: steady
         Other Stations When Call Is Put On Hold: green  wink
              Other Stations When Call Is Active: green
                                         Ringing: green  flash
                                            Idle: steady

                              Pickup On Transfer? y
```

5.3. Define the Dial Plan

Use the **change dialplan analysis** command to define the dial plan used in the system. This includes all telephone extensions, OPS Feature Name Extensions (FNEs), and Feature Access Codes (FACs). A Feature Access Code (FAC) must also be specified for the corresponding feature. In the sample configuration, telephone extensions are four digits long and begin with **1**, FNEs are also four digits beginning with **1**, and the FACs have formats as indicated with a **Call Type** of **fac**.

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

       Dialed   Total  Call    Dialed   Total  Call     Dialed   Total  Call
       String   Length Type    String   Length Type     String   Length Type
     0            1    ext    7           4    ext
     1            4    ext    88          4    ext
     2            4    udp    89          4    ext
     3005         8    udp    9           1    fac
     3015         9    udp    *           3    fac
     31           4    udp    #           3    fac
```

5.4. Define Feature Access Codes (FACs)

A FAC (feature access code) should be defined for each feature that will be used via the OPS FNEs. Use **change feature-access-codes** to define the required access codes. The FACs used in the sample configuration are shown in bold.

```
change feature-access-codes                                     Page   1 of   9
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code:
                       Answer Back Access Code: *24
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 4
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation: *25    Deactivation: #25
Call Forwarding Activation Busy/DA: *21    All: *20    Deactivation: #20
   Call Forwarding Enhanced Status:        Act:        Deactivation:
                         Call Park Access Code: *26
                       Call Pickup Access Code: *27
CAS Remote Hold/Answer Hold-Unhold Access Code:
                  CDR Account Code Access Code:
                        Change COR Access Code:
                   Change Coverage Access Code:
            Conditional Call Extend Activation:        Deactivation:
                   Contact Closure   Open Code:          Close Code:
```

```
change feature-access-codes                                     Page   2 of   9
                               FEATURE ACCESS CODE (FAC)
                   Contact Closure  Pulse Code:

                  Data Origination Access Code:
                      Data Privacy Access Code:
              Directed Call Pickup Access Code: *28
     Directed Group Call Pickup  Access Code:
   Emergency Access to Attendant Access Code:
        EC500 Self-Administration Access Codes:
                     Enhanced EC500 Activation:        Deactivation:
            Enterprise Mobility User Activation:        Deactivation:
  Extended Call Fwd Activate Busy D/A      All:        Deactivation:
        Extended Group Call Pickup Access Code:
               Facility Test Calls Access Code:
                             Flash Access Code:
             Group Control Restrict Activation:        Deactivation:
                    Hunt Group Busy Activation:        Deactivation:
                              ISDN Access Code:
                Last Number Dialed Access Code: *29
     Leave Word Calling Message Retrieval Lock:
   Leave Word Calling Message Retrieval Unlock:
```

```
change feature-access-codes                                     Page   3 of   9
                               FEATURE ACCESS CODE (FAC)
             Leave Word Calling Send A Message:
           Leave Word Calling Cancel A Message:
   Limit Number of Concurrent Calls Activation:        Deactivation:
               Malicious Call Trace Activation:        Deactivation:
         Meet-me Conference Access Code Change:
          Message Sequence Trace (MST) Disable:

 PASTE (Display PBX data on Phone) Access Code:
  Personal Station Access (PSA) Associate Code:        Dissociate Code:
        Per Call CPN Blocking Code Access Code: *34
      Per Call CPN Unblocking Code Access Code: *35
                    Posted Messages Activation:        Deactivation:
                  Priority Calling Access Code: *30
                           Program Access Code:

      Refresh Terminal Parameters Access Code:
             Remote Send All Calls Activation:        Deactivation:
              Self Station Display Activation:
                   Send All Calls Activation: *31    Deactivation: #31
         Station Firmware Download Access Code:
```

```
change feature-access-codes                                     Page   4 of   9
                               FEATURE ACCESS CODE (FAC)
                             Station Lock Activation:      Deactivation:
            Station Security Code Change Access Code:
                    Station User Admin of FBI Assign:      Remove:
        Station User Button Ring Control Access Code:
                   Terminal Dial-Up Test Access Code:
      Terminal Translation Initialization Merge Code:      Separation Code:
                  Transfer to Voice Mail Access Code: *32
                Trunk Answer Any Station Access Code:
                    User Control Restrict Activation:      Deactivation:
        Voice Coverage Message Retrieval Access Code:
       Voice Principal Message Retrieval Access Code:
                 Whisper Page Activation Access Code: *33

          PIN Checking for Private Calls Access Code:
PIN Checking for Private Calls Using ARS Access Code:
PIN Checking for Private Calls Using AAR Access Code:
```

5.5. Define Feature Name Extensions (FNEs)

The OPS FNEs can be defined using the **change off-pbx-telephone feature-name-extensions set 1** command. The following screens show in bold the FNEs defined for use with the sample configuration.

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

        Active Appearance Select: 1700
             Automatic Call Back: 1701
      Automatic Call-Back Cancel: 1702
                Call Forward All: 1703
     Call Forward Busy/No Answer: 1704
             Call Forward Cancel: 1705
                       Call Park: 1706
           Call Park Answer Back: 1707
                    Call Pick-Up: 1708
            Calling Number Block: 1709
          Calling Number Unblock: 1710
  Conditional Call Extend Enable: 1711
 Conditional Call Extend Disable: 1712
             Conference Complete: 1713
            Conference on Answer: 1714
           Directed Call Pick-Up: 1715
           Drop Last Added Party: 1716
```

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

       Exclusion (Toggle On/Off): 1717
      Extended Group Call Pickup:
          Held Appearance Select: 1718
          Idle Appearance Select: 1719
              Last Number Dialed: 1720
            Malicious Call Trace:
     Malicious Call Trace Cancel:
             Off-Pbx Call Enable:
            Off-Pbx Call Disable:
                   Priority Call: 1725
                          Recall: 1726
                  Send All Calls: 1727
           Send All Calls Cancel: 1728
               Transfer Complete: 1729
             Transfer On Hang-Up: 1730
          Transfer to Voice Mail: 1731
         Whisper Page Activation: 1732
```

5.6. Configure Class of Service (COS)

Use the **change cos** command to set the appropriate service permissions to support OPS features (shown in bold). For the sample configuration a COS of **1** was used.

```
change cos                                                      Page   1 of   2

                                0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15
 Auto Callback                  n  y  y  n  y  n  y  n  y  n  y  y  y  n  y  n
 Call Fwd-All Calls             n  y  n  y  y  n  n  y  y  n  n  y  y  n  n  y
 Data Privacy                   n  n  n  n  n  y  y  y  y  n  n  n  n  y  y  y
 Priority Calling               n  y  n  n  n  n  n  n  n  y  y  y  y  y  y  y
 Console Permissions            n  y  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Off-hook Alert                 n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Client Room                    n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Restrict Call Fwd-Off Net      y  n  y  y  y  y  y  y  y  y  y  n  y  y  y  y
 Call Forwarding Busy/DA        n  y  n  n  n  n  n  n  n  n  n  y  n  n  n  n
 Personal Station Access (PSA)  n  y  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Extended Forwarding All        n  y  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Extended Forwarding B/DA       n  y  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Trk-to-Trk Transfer Override   n  y  n  n  n  n  n  n  n  n  n  y  n  n  n  n
 QSIG Call Offer Originations   n  n  n  n  n  n  n  n  n  n  n  y  n  n  n  n
 Contact Closure Activation     n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
```

5.7. Configure Class of Restriction (COR)

Use the **change cor 1** command to enable applicable calling features. To use the Directed Call Pickup feature, the **Can Be Picked Up By Directed Call Pickup** and **Can Use Directed Call Pickup** fields must be set to **y**. In the sample configuration, the handsets were assigned to COR **1**.

```
change cor 1                                                  Page   1 of  23
                              CLASS OF RESTRICTION

               COR Number: 1
          COR Description: Default

                      FRL: 0                                APLT? y
  Can Be Service Observed? y           Calling Party Restriction: none
Can Be A Service Observer? y            Called Party Restriction: none
 Partitioned Group Number: 1       Forced Entry of Account Codes? n
         Priority Queuing? n                Direct Agent Calling? n
     Restriction Override: all        Facility Access Trunk Test? n
     Restricted Call List? n                 Can Change Coverage? n

            Access to MCT? y            Fully Restricted Service? n
Group II Category For MFC: 7
         Send ANI for MFE? n
            MF ANI Prefix:              Automatic Charge Display? n
Hear System Music on Hold? y   PASTE (Display PBX Data on Phone)? y
                        Can Be Picked Up By Directed Call Pickup? y
                                    Can Use Directed Call Pickup? y
                                    Group Controlled Restriction: inactive
```

5.8. Add Stations

Unlike previous versions of Session Manager the Station Features and button assignments can be added using the Endpoint Editor in System Manager. This method was used in this test configuration and procedure can be found In **Section 6.9**

5.8.1. Verify Off PBX Station Mapping

Following completion of the procedures in **Section 6.9** use the **display off-pbx-telephone station-mapping** command to verify that SIP Endpoints added to Session Manager in **section 6.9** have been administered in Communication Manager. The example below shows that **Station Extension 1318** uses the **Application OPS.**

```
display off-pbx-telephone station-mapping                 Page   1 of   3
                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station       Application Dial   CC  Phone Number    Trunk       Config  Dual
 Extension                 Prefix                     Selection   Set     Mode
 1319             OPS          -      1319            aar        1
```

5.9. Configure SIP Trunk

In the **node-names ip** form, assign an IP address and host name for the C-LAN board in the Avaya G650 Media Gateway and the Session Manager Security module IP address. The host names will be used throughout the other configuration screens of Communication Manager.

```
 change node-names ip
                                  IP NODE NAMES
    Name              IP Address
AES522              10.10.16.25
CLAN                10.10.16.31
CM521               10.10.16.23
Gateway             10.10.16.1
MedPro              10.10.16.32
61sysmgr            10.10.16.56
61sesmgr            10.10.16.54
SM61                10.10.16.201
default             0.0.0.0
procr               10.10.16.47
procr6              ::
( 16 of 16   administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is **avaya.com**. By default, **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** (shuffling) is enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya G650 Media Gateway. The **IP Network Region** form also specifies the **IP Codec Set** to be used. This codec set will be used for calls routed over the SIP trunk to Session Manager as **ip-network region 1** is specified in the SIP signaling group.

```
change ip-network-region 1                                      Page   1 of  19
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: avaya.com
    Name: Default Region
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? y
   UDP Port Max: 8001
DIFFSERV/TOS PARAMETERS                  RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        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
```

In the **IP Codec Set** form, select the audio codec's supported for calls routed over the SIP trunk. The form is accessed via the **change ip-codec-set 1** command. Note that IP codec set 1 was specified in IP Network Region 1 shown above. Multiple codecs may be specified in the **IP Codec Set** form in order of preference; the example below includes **G.711A** (a-law), **G.711MU** (mu-law) and **G.729.**

```
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.711A            n         2        20
 2: G.711MU           n         2        20
 3: G.729             n         2        20
 4:
 5:
 6:
 7:

     Media Encryption
 1: none
 2:
 3:
```

Prior to configuring a SIP trunk group for communication with Session Manager, a SIP signaling group must be configured. Configure the Signaling Group form shown as follows:

- Set the **Group Type** field to **sip**
- Set the **Transport Method** to the desired transport method; **tcp** (transport control protocol) or tls (Transport Layer Security). **Note:** for transparency tcp was used during this compliance test but the recommended method is tls.
- Specify the node names for the C-LAN board in the G650 Media Gateway and the active Session Manager node name as the two ends of the signaling group in the **Near-end Node Name** field and the **Far-end Node Name** field, respectively. These values are taken from the **IP Node Names** form shown above.
- Ensure that the recommended port value of **5060** for tcp is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields **Note**: If tls is used then the recommended port value is **5061.**
- The preferred codec for the call will be selected from the IP codec set assigned to the IP network region specified in the **Far-end Network Region** field.
- Enter the domain name of the Session Manager Security Module in the **Far-end Domain** field. In this configuration, the domain name is **avaya.com**. This domain is specified in the Uniform Resource Identifier (URI) of the **SIP To** Address in the INVITE message. Mis-configuring this field may prevent calls from being successfully established to other SIP endpoints or to the PSTN.
- The **DTMF over IP** field should be set to the default value of **rtp-payload**. Communication Manager supports DTMF transmission using RFC 2833. The default values for the other fields may be used.

```
add signaling-group 6                                              Page   1 of   1
                                SIGNALING GROUP

 Group Number: 6              Group Type: sip
                        Transport Method: tcp
  IMS Enabled? n
     IP Video? n




   Near-end Node Name: CLAN1                  Far-end Node Name: 61sesmgr
 Near-end Listen Port: 5060                 Far-end Listen Port: 5060
                                         Far-end Network Region: 1
Far-end Domain: avaya.com

                                          Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate               RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload         Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                  IP Audio Hairpinning? y
         Enable Layer 3 Test? n                  Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n          Alternate Route Timer(sec): 6
```

Configure the **Trunk Group** form as shown below. This trunk will be used to transport calls between Session Manager and Communication Manager. Enter a descriptive name in the **Group Name** field. Set the **Group Type** field to **sip**. Enter a **TAC** code compatible with the Communication Manager. Set the **Service Type** field to **tie**, specify the signaling group associated with this trunk group in the **Signaling Group** field, and specify the **Number of Members** supported by this SIP trunk group. Accept the default values for the remaining fields.

```
add trunk-group 6                                               Page   1 of  21
                                TRUNK GROUP

Group Number: 6                    Group Type: sip           CDR Reports: y
  Group Name: SES OPS                     COR: 1        TN: 1        TAC: 506
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: tie                    Auth Code? n

                                                     Signaling Group: 6
                                                   Number of Members: 30
```

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

```
add trunk-group 6                                               Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                        Maintenance Tests? y

                     Numbering Format: private
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? y
                                                Replace Unavailable Numbers? y

 Show ANSWERED BY on Display? y
```

Configure the **Private Numbering** form to send the calling party number to the far-end. Add entries so that local stations with a 4-digit extension beginning with **13, 15 and 16** and whose calls are routed over SIP trunk group **6** have the number sent to the far-end for display purposes.

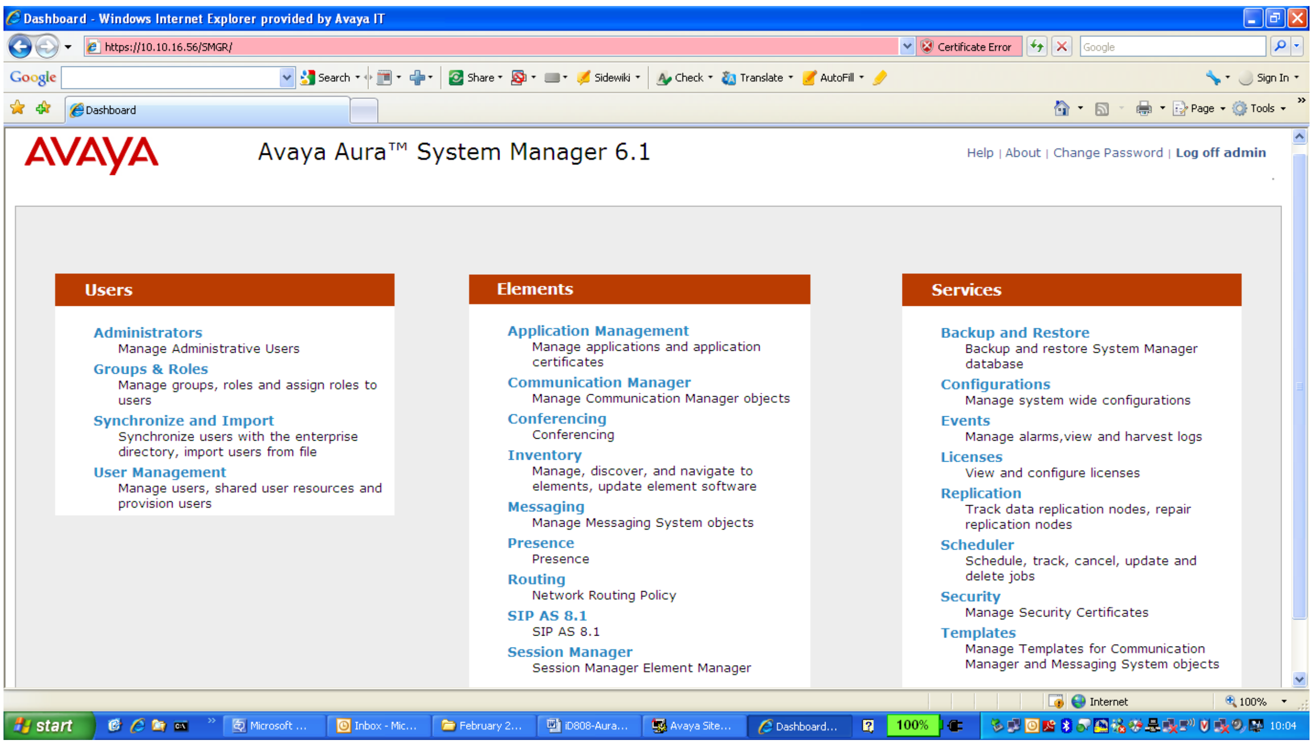
```
change private-numbering 0                                         Page   1 of   2
                           NUMBERING - PRIVATE FORMAT

Ext Ext              Trk        Private           Total
Len Code             Grp(s)     Prefix            Len
 4  13               6                             4     Total Administered: 3
 4  15               6                             4        Maximum Entries: 540
 4  16               6                             4
```

6. Configure Avaya Aura® Session Manager

This section covers the administration of Session Manager. Session Manager is configured via an internet browser using the System Manager web interface. It is assumed that Session Manager software has already been installed. For additional information on installation tasks refer to **[4]**.

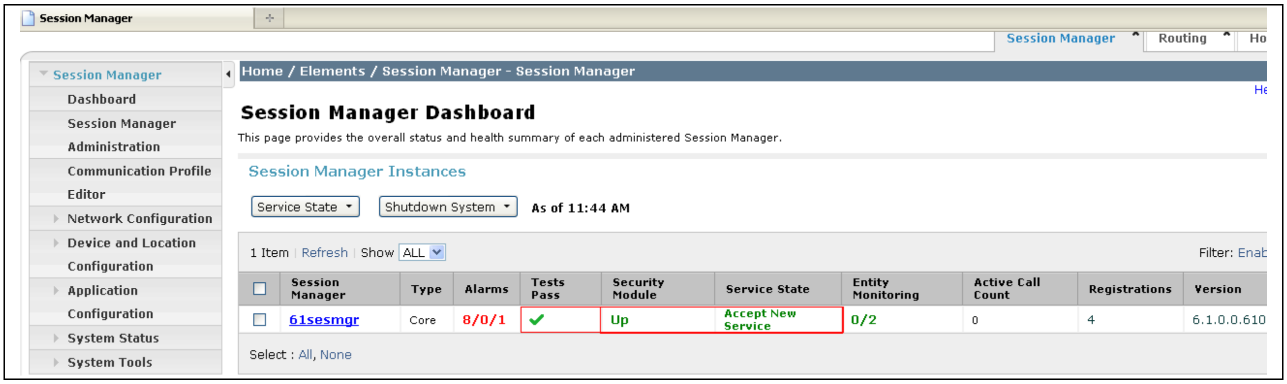
6.1. Logging in to Avaya Aura® System Manager

To access the administration web interface, enter **http://<ip-addr>/SMGR** as the URL in an Internet browser. Where <ip-addr> is the IP address of smgr on System Platform. Log in with the appropriate credentials. The main screen is displayed, as shown below.

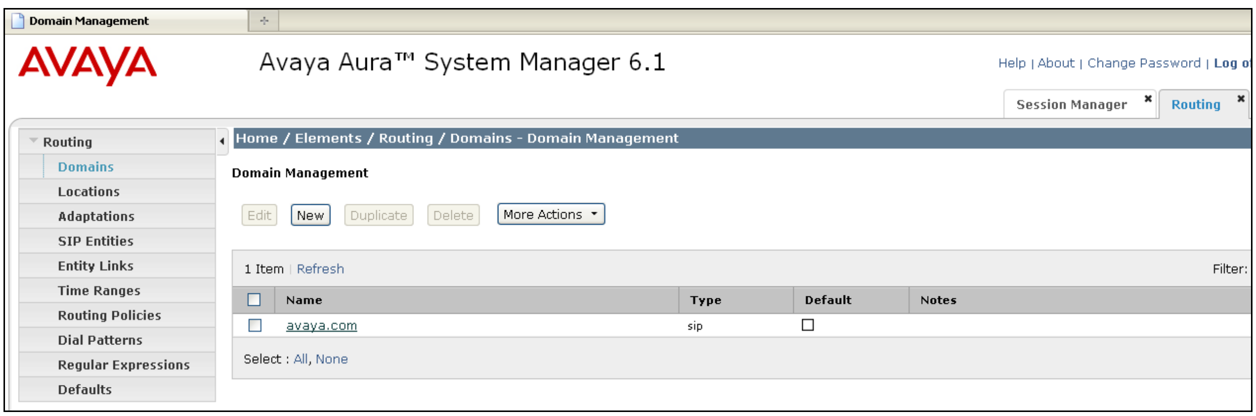


6.2. Verify System Properties

From the main screen of the web interface, choose **Session Manager** from the **Elements** section. Verify that a green tick shows under **Tests Passed**, **Security Module** is **Up** and **Service State** is set to **Accept New Service.**

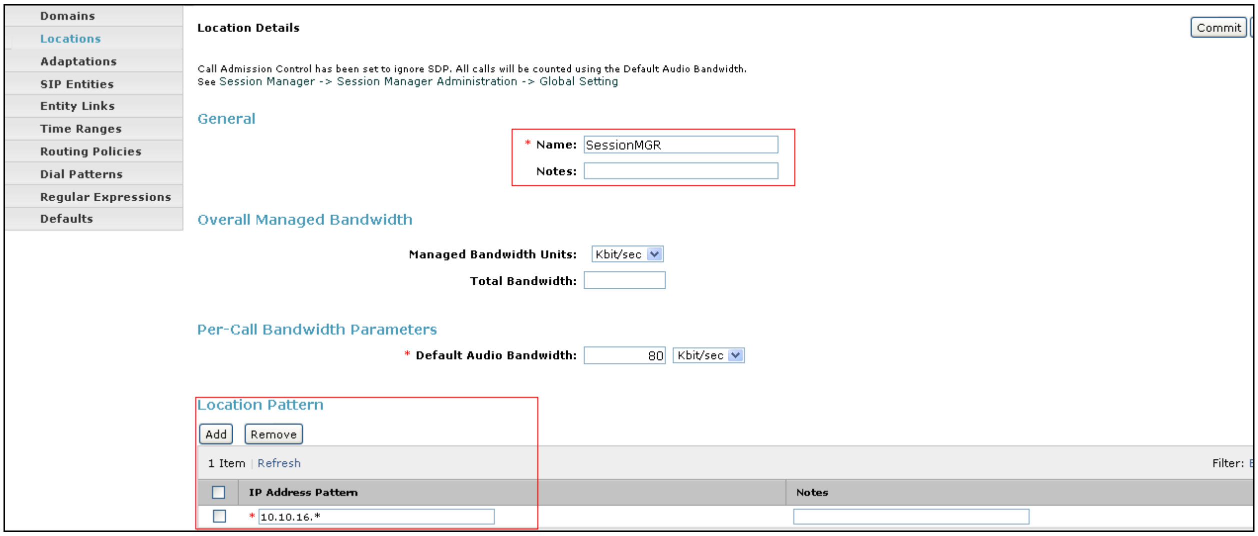


Next go to **Routing** from the **Elements** section of the main screen and select **Domains**. Check the domain administered.



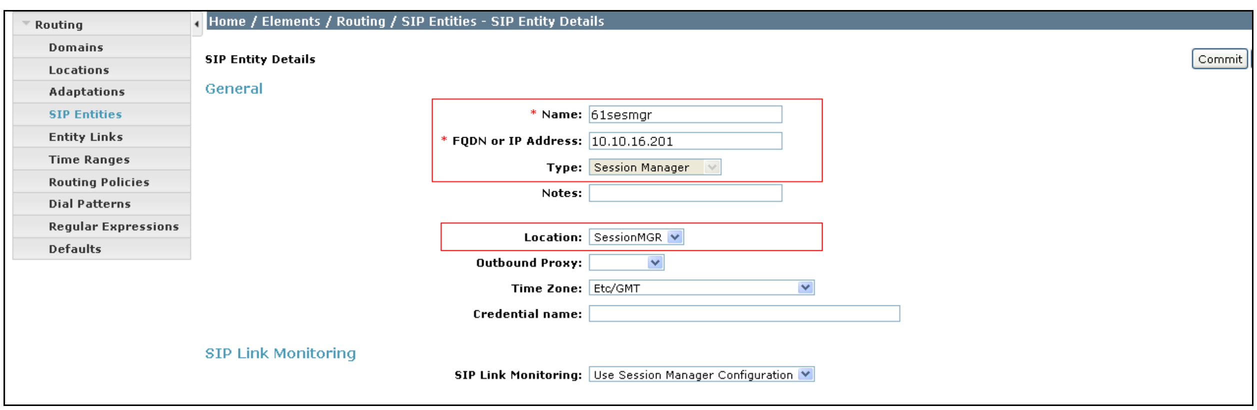
6.3. Add Location

Select **Routing** (not shown) from the **Elements** section of the main screen and chose **Locations.** Click on the new button (not shown) and add a **Name** and **IP Address Pattern** for the Location in the format shown under **Location Patterns**. Click on the **Commit** button to save.

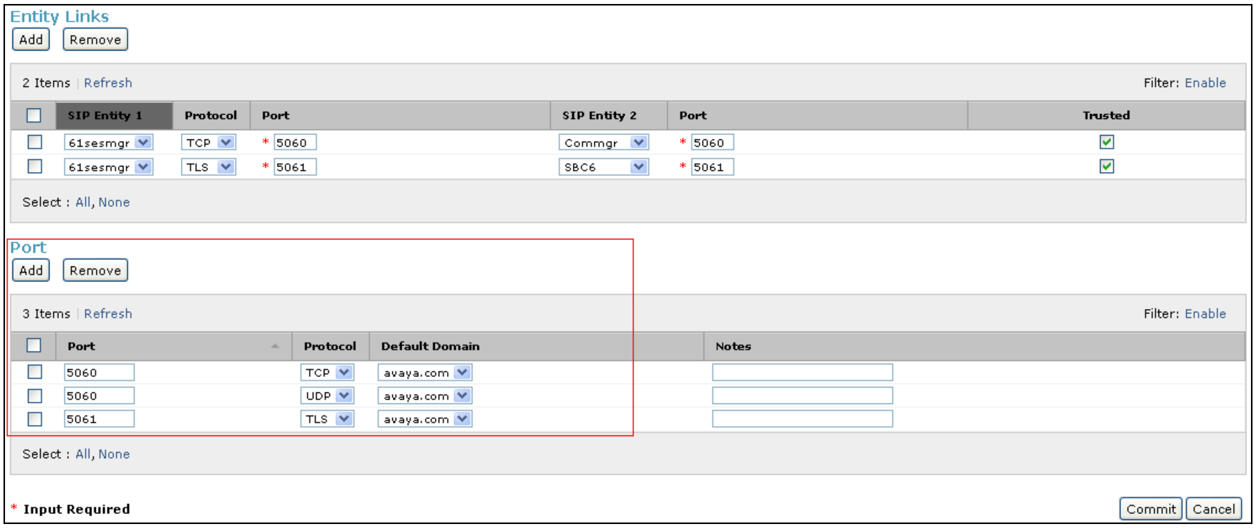


6.4. Create a SIP entity

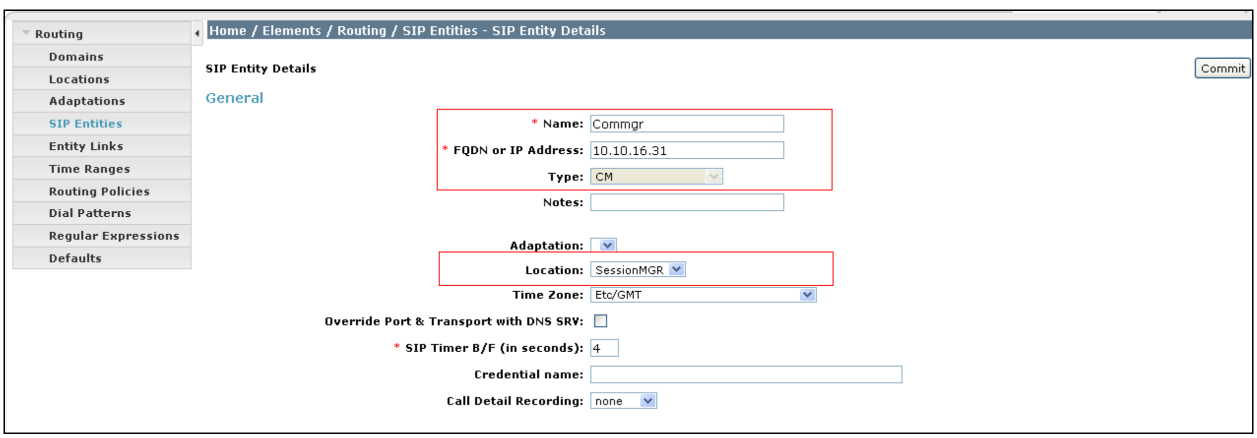
From the **Elements** section of the main screen choose **Routing**. From the left hand side menu choose **SIP Entities**. Click on **New** and enter a **Name** and **FQDN or IP Address** for the Session Manager Security Module. Select **Type** as **Session Manager** and **Location** as the Session Manager Location created in **Section 6.3**.



Add the **Protocol** and **Port** information to the **Port** section of the SIP Entity details screen below. The entity link section will automatically populate after the link is added in **section 6.5.** Click **Commit** to save the changes.

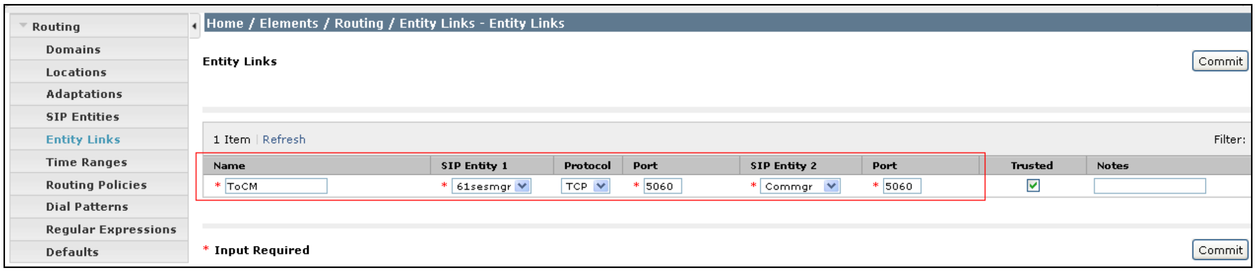


A Communication Manager SIP Entity must be added also with an appropriate **Name** and the **FQDN or IP Address** of the CLAN checked in **Section 5.9 Protocol** and **Port** details are added in the same way as the previous screen.



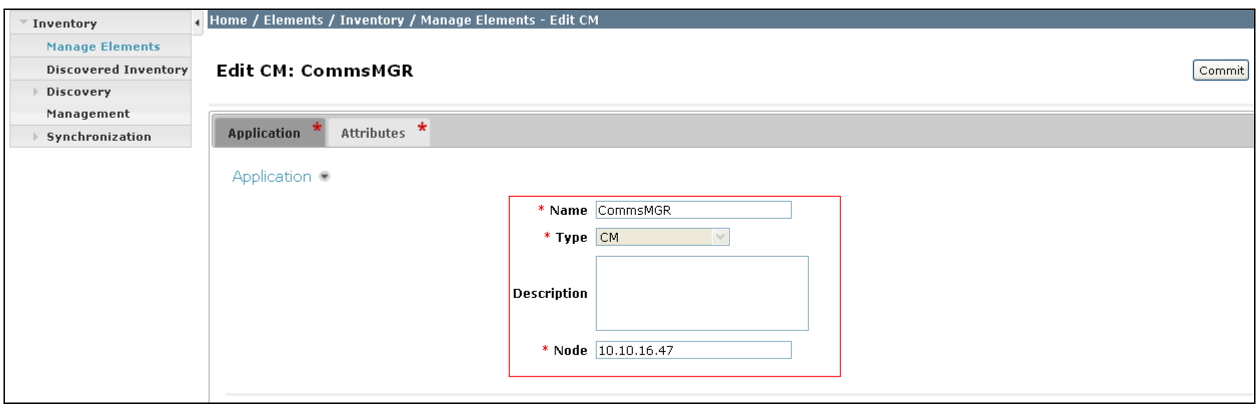
6.5. Add an Entity link

From the **Routing** menu choose **Entity Links**, choose an appropriate **Name** and then choose the entities added in **section 6.4,** the **Protocol** used (TCP used in this example) and the **Port** the protocol communicates on. Click on the **Commit** button to save.



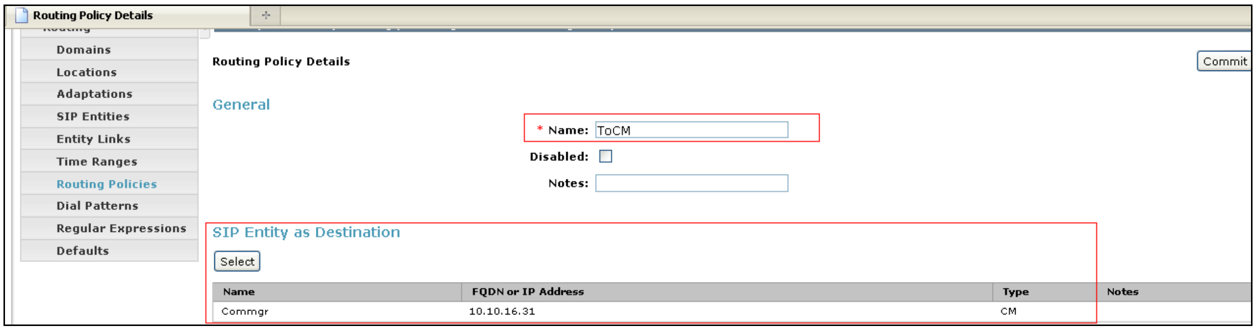
6.6. Add Avaya Aura® Communication Manager Managed Element

From the **Elements** section of the main screen chose **Inventory** and then **Manage Elements**. Click the **New** (not shown) button and enter a valid **Name**, **Type** as **CM** and the SAT IP address in the **Node** field. Click on **Commit** to save.

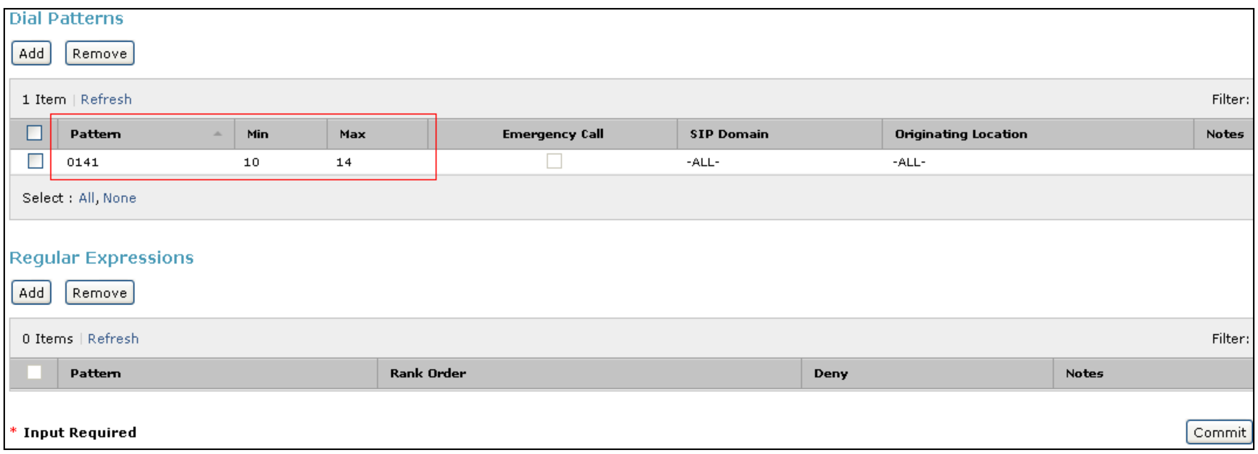


6.7. Add Routing Policy

From the **Elements** section of the main screen chose **Routing** and then **Routing Policies**. Click on the **New** button and add a **Name** for the policy. Select the Communication Manager entity as a Destination under **SIP Entity as Destination**.

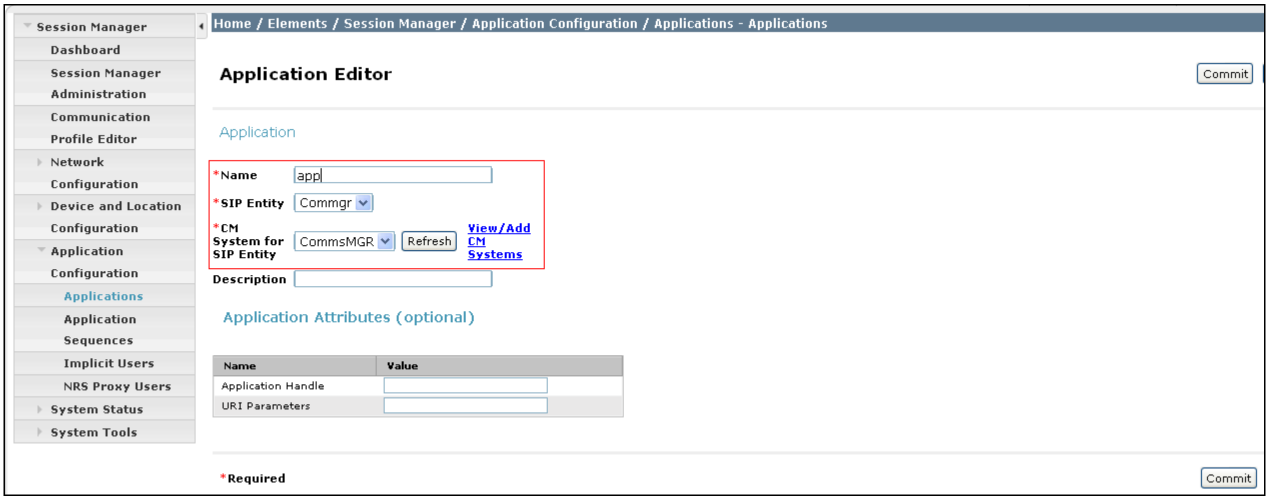


Add the **Dial Patterns** for non SIP stations and PSTN routing. A **Pattern** to be dialed and **Min**, **Max** digits are entered. Click on the **Commit** button to save.

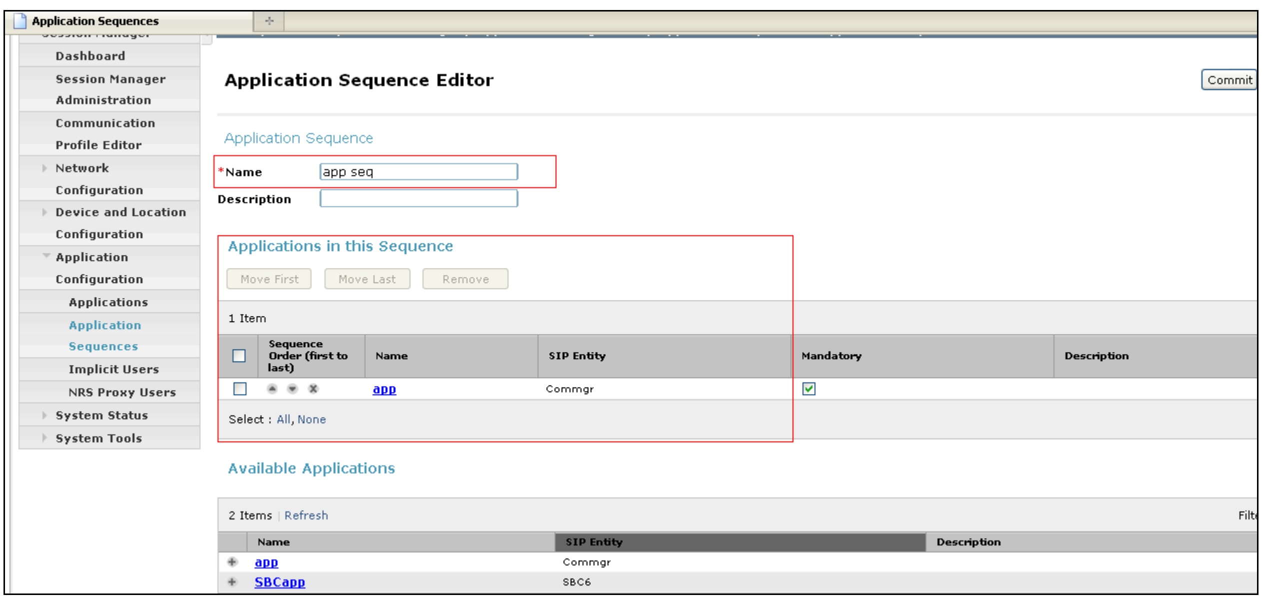


6.8. Add Application and Application Sequence

Select **Session Manager** from the **Elements** section of the main screen and choose **Application Configuration → Application.** Click on the **New** button (not shown) and enter an appropriate **Name**, Select the CM **SIP Entity** added in **Section 6.4** and the Communication Manager Managed Element added in **Section 6.6** as **CM System for SIP Entity**. Click on the **Commit** button to save.

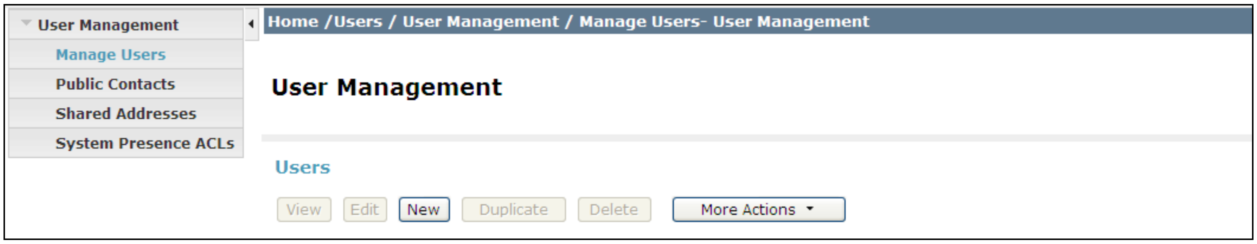


Next, choose **Application Sequences** and click the **New** button (not shown). Add a **Name** and select the Application added above to interact with the Communication Manager Entity.

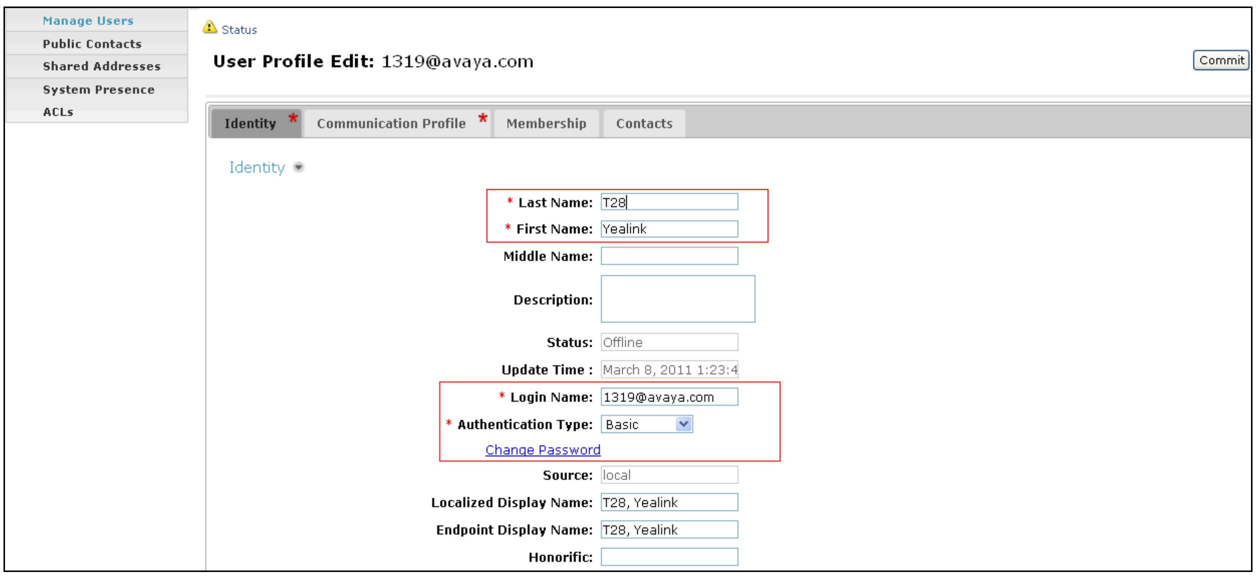


6.9. Add User

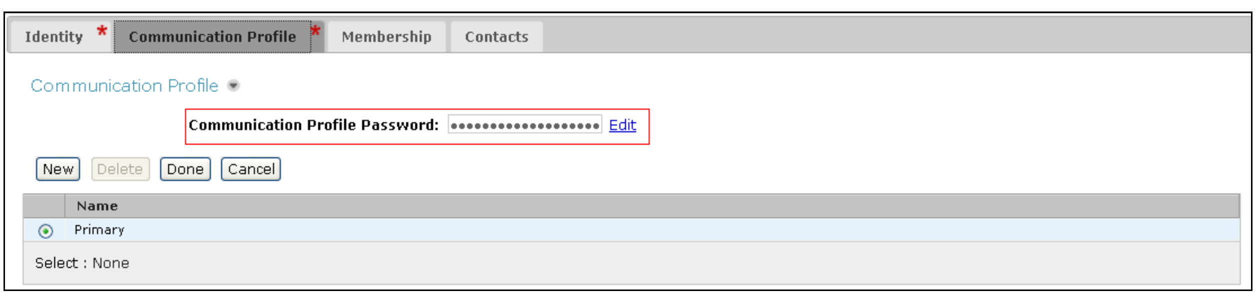
From the **User** section of the **Main Screen** choose **User Management** and then choose **Manage Users** from the menu. Click **New** to add a user.



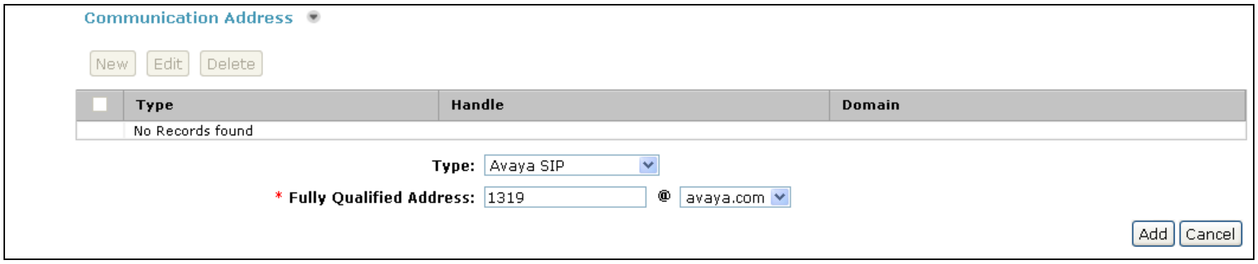
Under the **Identity** tab fill in the required information. The **Login Name** field contains the fully qualified name in the form <user>@<sip domain>. The **Password** in this section is purely for user log in and is not the passcode used to log in the phone.



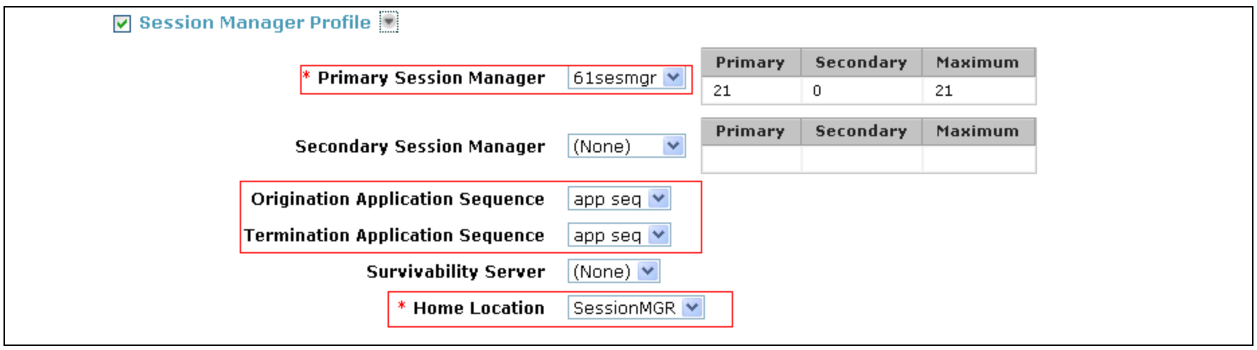
Under the **Communication Profile** tab enter the **Communication Profile Password** as the passcode used to log in the handset.



Still on the **Communication Profile** tab move down to **Communication Address** and click on the **New** button. Enter the **Type** as **Avaya SIP** and the **Fully Qualified Address** the same as on the Identity tab.

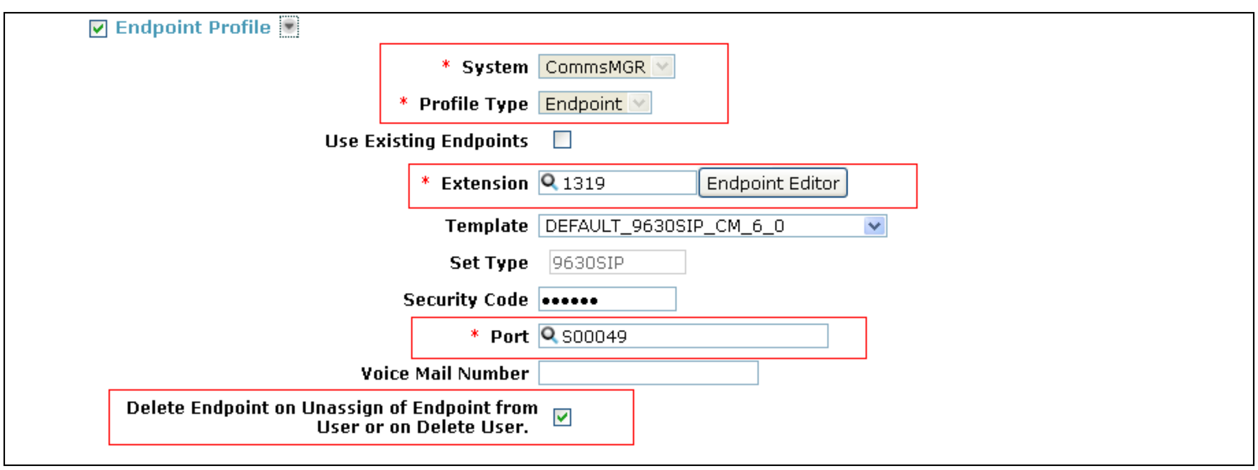


Move down and select **Session Manager Profile.** Fill in the details with the **Primary Session Manager** as the SIP entity added in **Section 6.4.** Fill in the **Application Sequences** as the Application Sequence added in **Section 6.8**. Fill in the **Home Location** as the Location added in **Section 6.3**



Move down and select **Endpoint Profile**. Fill in the **System** as the Communication Manager Managed Element added in **Section 6.6**. Add the **Extension** and **Port** as required and tick the **Delete Endpoint on Unassign of Endpont from User or on Delete User**.

Note: Endpoint editor can be used to administer features and buttons but this was not required in this instance.



7. Configure Yealink T-28 Handset

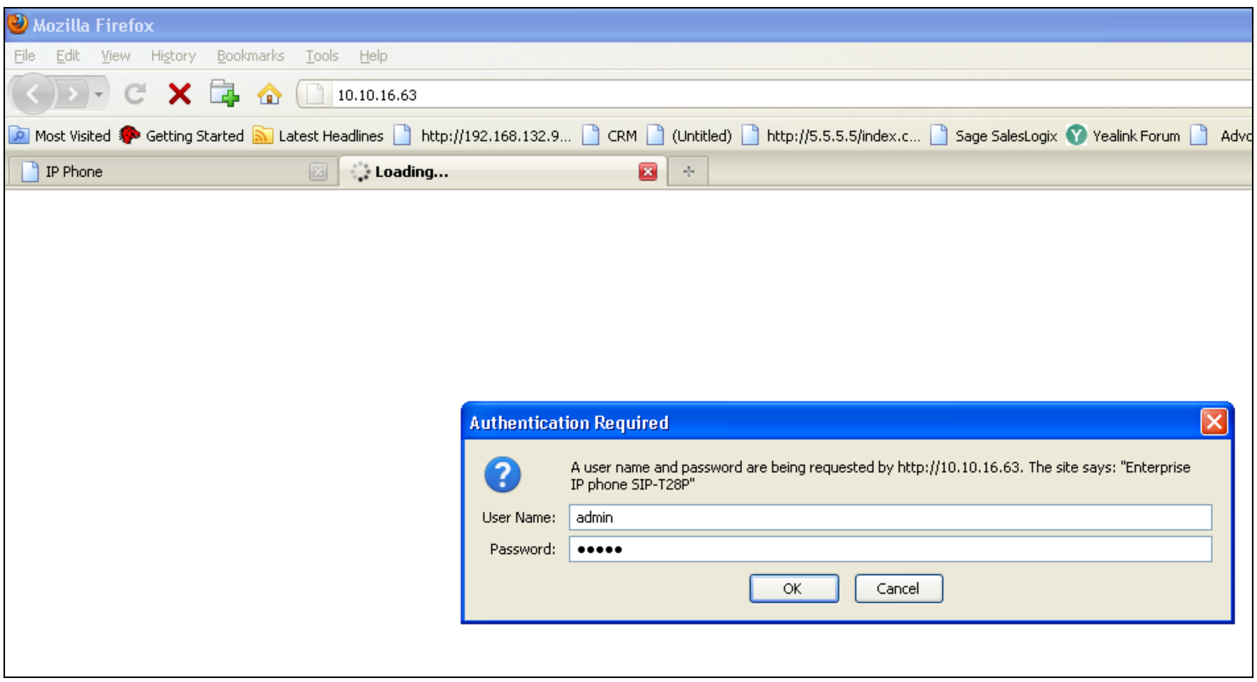
This section covers the administration of the Yealink T-28 Handset device. The Yealink T-28 is configured via an Internet browser using the integral web interface. To access the web interface the IP Address of the device is entered into the browser command line. The Yealink T-28 by default is set to obtain an IP Address by DHCP.

7.1. Determining device IP Address

Press OK button on the keypad of the phone to enter the status page and find out the IP address of IP phone. Enter it (for example http://10.10.16.63) into the address bar of web browser. The default administrator's login name and password are **admin/admin**.

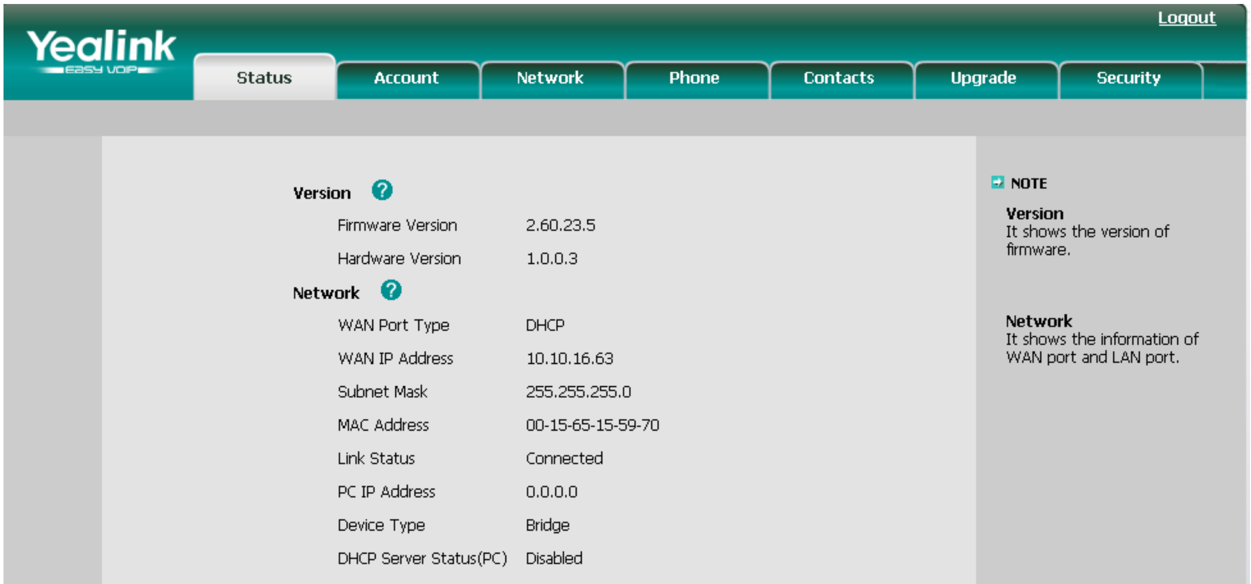
7.2. Configuring via the Web Browser

Enter the Yealink T-28 IP Address (for example http://10.10.16.63) into the address bar of web browser. The default login name and password are both **admin**.



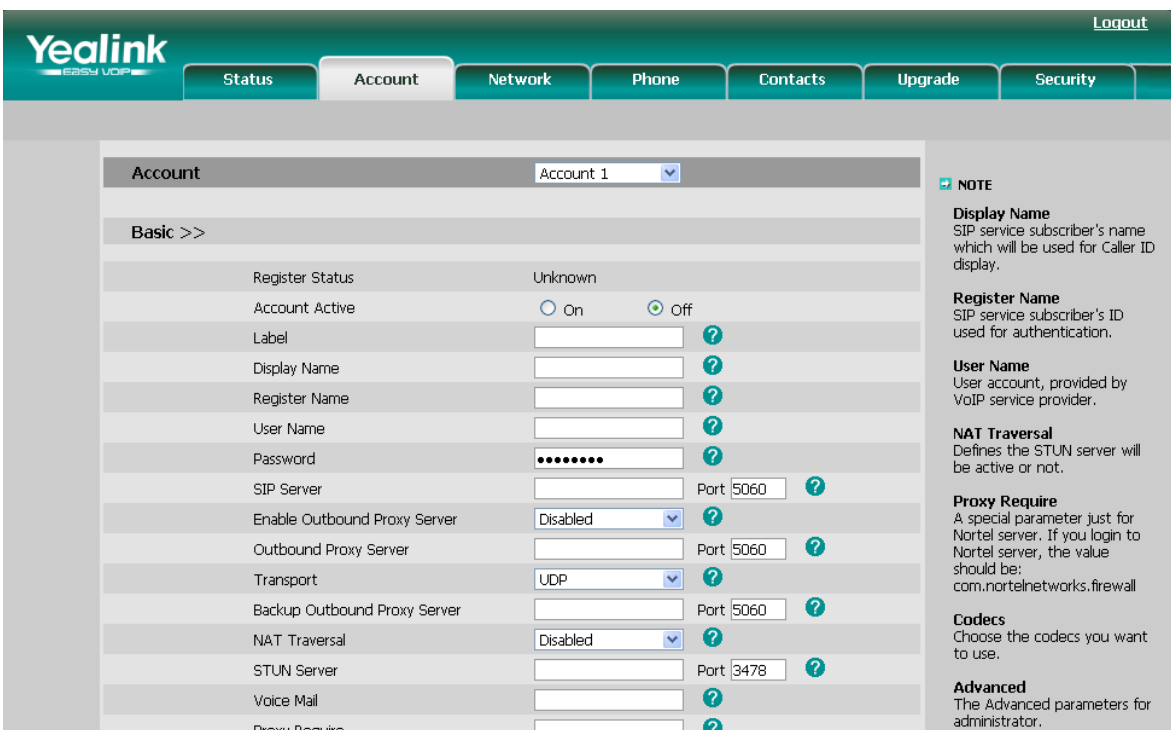
7.3. Status Screen

After log in credentials are successfully entered the **Status** Screen is displayed.



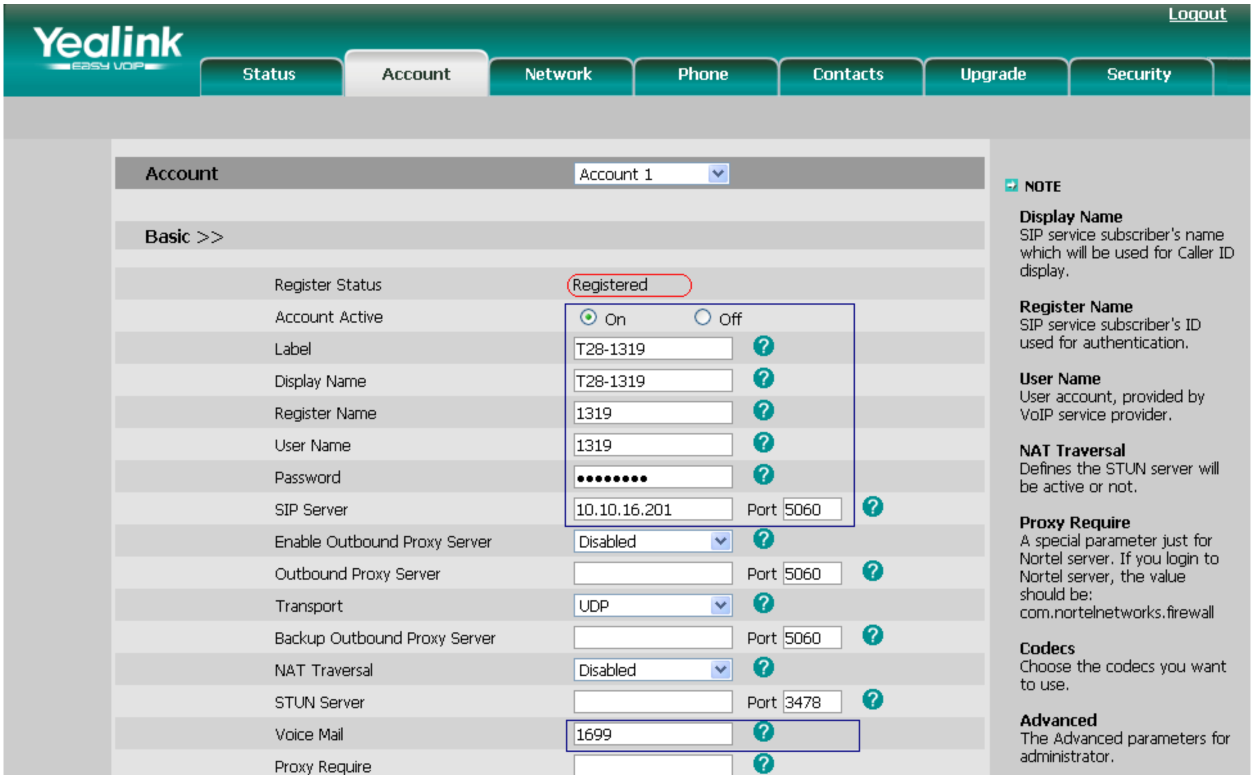
7.4. Account Configuration

Click on the tab labeled **Account**

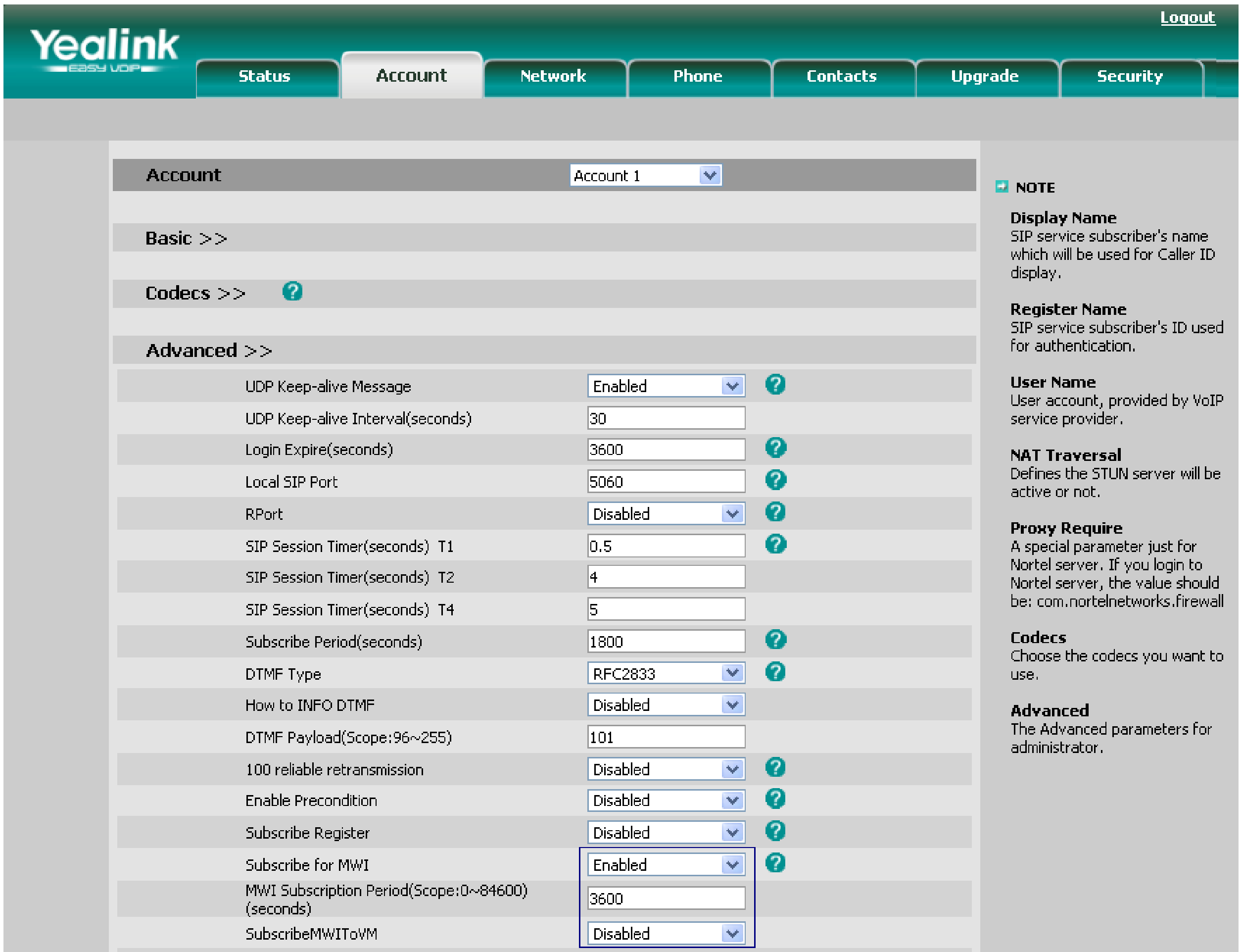


7.4.1. Enter the Account details

Enter the account details as highlighted in blue in the image below to match the settings in the Session Manager added in **Section 6.9**. Press the **Confirm** button (not shown) at the bottom of the page to save the changes and if the details have been entered correctly the **Register Status** will be **Registered** as highlighted in Red in the image below.

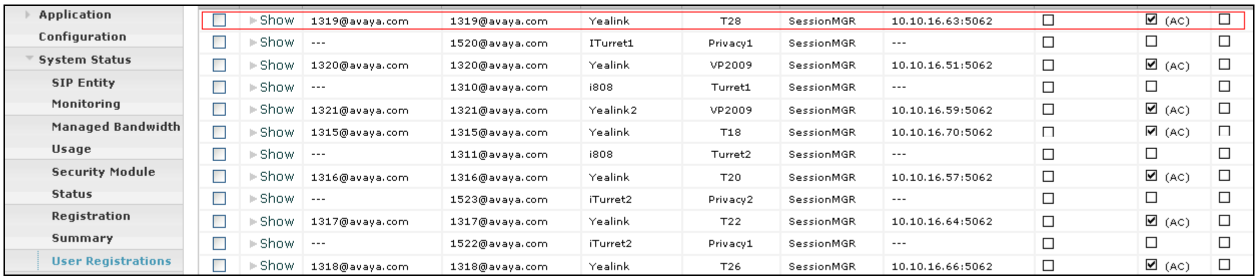


Click the **Advanced** option under the **Account** tab and enter the voicemail message waiting settings as highlighted in blue in the image below. If Voicemail is to be used as part of the Yealink T-28 setup the setting: **SubscribeMWIToVM** must be set to **Disabled** to enable the device to register to the voicemail system as the Account Number.



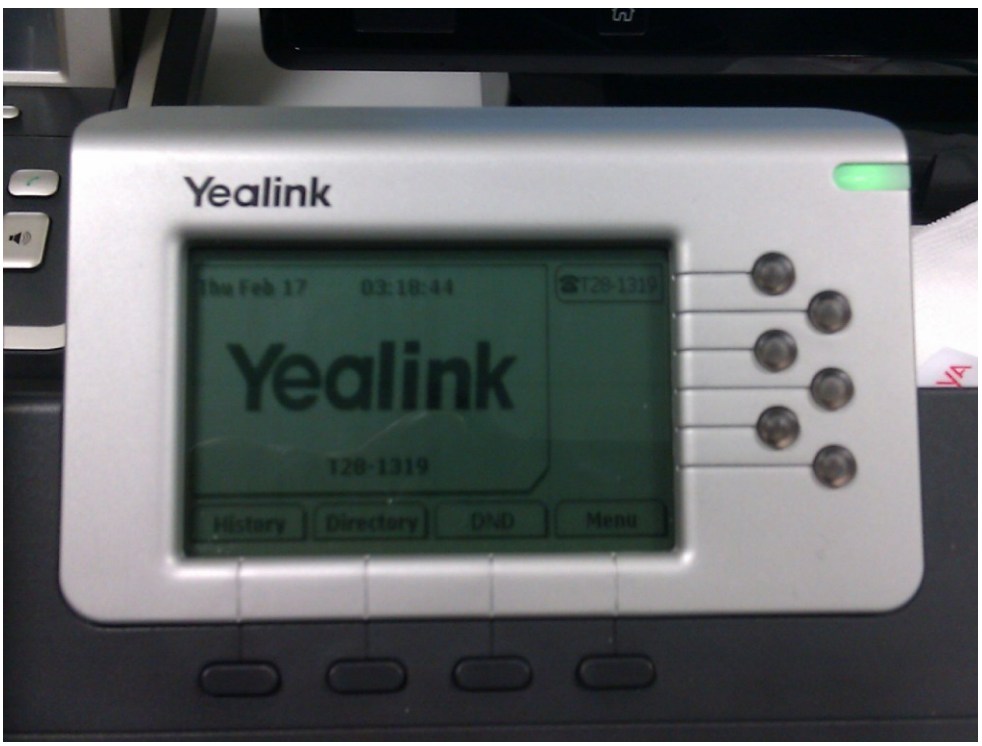
8. Verification Steps

All features were tested using the sample configuration. The following steps can be used to verify and/or troubleshoot installations in the field. Verify that the T-28 handset has successfully registered with Session Manager, from the main screen select **Session Manager** from the **Elements** section and choose **System Status → User Registrations** this will display a list of registered user's on Session Manager as shown below. The **Address** and **IP Address** fields are populated when the handset has successfully registered.



☐	Show	1319@avaya.com	1319@avaya.com	Yealink	T28	SessionMGR	10.10.16.63:5062	☐	☑ (AC)	☐
☐	Show	---	1520@avaya.com	ITurret1	Privacy1	SessionMGR	---	☐	☐	☐
☐	Show	1320@avaya.com	1320@avaya.com	Yealink	VP2009	SessionMGR	10.10.16.51:5062	☐	☑ (AC)	☐
☐	Show	---	1310@avaya.com	i808	Turret1	SessionMGR	---	☐	☐	☐
☐	Show	1321@avaya.com	1321@avaya.com	Yealink2	VP2009	SessionMGR	10.10.16.59:5062	☐	☑ (AC)	☐
☐	Show	1315@avaya.com	1315@avaya.com	Yealink	T18	SessionMGR	10.10.16.70:5062	☐	☑ (AC)	☐
☐	Show	---	1311@avaya.com	i808	Turret2	SessionMGR	---	☐	☐	☐
☐	Show	1316@avaya.com	1316@avaya.com	Yealink	T20	SessionMGR	10.10.16.57:5062	☐	☑ (AC)	☐
☐	Show	---	1523@avaya.com	iTurret2	Privacy2	SessionMGR	---	☐	☐	☐
☐	Show	1317@avaya.com	1317@avaya.com	Yealink	T22	SessionMGR	10.10.16.64:5062	☐	☑ (AC)	☐
☐	Show	---	1522@avaya.com	iTurret2	Privacy1	SessionMGR	---	☐	☐	☐
☐	Show	1318@avaya.com	1318@avaya.com	Yealink	T26	SessionMGR	10.10.16.66:5062	☐	☑ (AC)	☐

The picture below shows that the T-28 Handset is registered with Session Manager. The handset name is shown on the display. When the handset fails to register the display shows **No Service**.



9. Conclusion

These Application Notes have described the administration steps required to use Yealink T-28 handsets with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Both basic and extended feature sets were covered in the interoperability testing.

10. Additional References

This section references the Avaya documentation relevant to these Application Notes. The following Avaya product documentation is available at http://support.avaya.com.

[1] *Administering Avaya Aura® Communication Manager, 9th august 2010, Document Number 03-300509*.
[2] *Avaya Extension to Cellular User Guide Avaya Aura® Communication Manager, Nov 2009*
[3] *SIP Support in Avaya Aura® Communication Manager Running on the Avaya S8xxx Servers, May 2009, Issue 9, Document Number 555-245-206.*
[4] *Installing and configuring Avaya Aura® Session Manager, 5th January 2011, Document Number 03-603473.*
[5] *Session Initiation Protocol Service Examples draft-ietf-sipping-service-examples-15*, Internet-Draft, 11th July 2008, available at http://tools.ietf.org/html/draft-ietf-sipping-service-examples-15

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.