Avaya Solution & Interoperability Test Lab

Application Notes for British Telecom (Unified Trading) IP Trade Platform with Avaya Aura® Session Manager and Avaya Aura® Communication Manager - Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate British Telecom (Unified Trading) IP Trade Platform with Avaya Aura® Session Manager and Avaya Aura® Communication Manager. British Telecom IP Trade Platform is a SIP Endpoint management solution that interoperates with Avaya Aura® Session Manager via a SIP Trunk. It is used to route calls to the British Telecom Trade turrets.

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 configuration steps required to successfully integrate British Telecom(BT) IP Trade Platform with Avaya Aura® Session Manager (Session Manager) and Avaya Aura® Communication Manager (Communication Manager). The BT IP Trade Platform is a SIP Endpoint Management solution that uses Avaya Aura® Session Manager to route calls between Avaya Aura® Communication manager and BT Trade turrets via a SIP Trunk.

2. General Test Approach and Test Results

The general test approach was to configure the BT IP Trade Turrets to communicate with the Session Manager as third party SIP endpoints.

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

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

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

For the testing associated with these Application Notes, the interface between Avaya systems and the BT IP Trade Platform did not include use of any specific encryption features as requested by British Telecom.

2.1. Interoperability Compliance Testing

The interoperability compliance test included both feature functionality and serviceability testing. The feature functionality testing focused on carrying out different call scenarios with good quality audio. The tests included:

- SIP Endpoints are connected and in Service.
- BT Turret can make and receive calls.
- BT Turret can transfer and conference.
- BT Turret can recover from loss of service.

2.2. Test Results

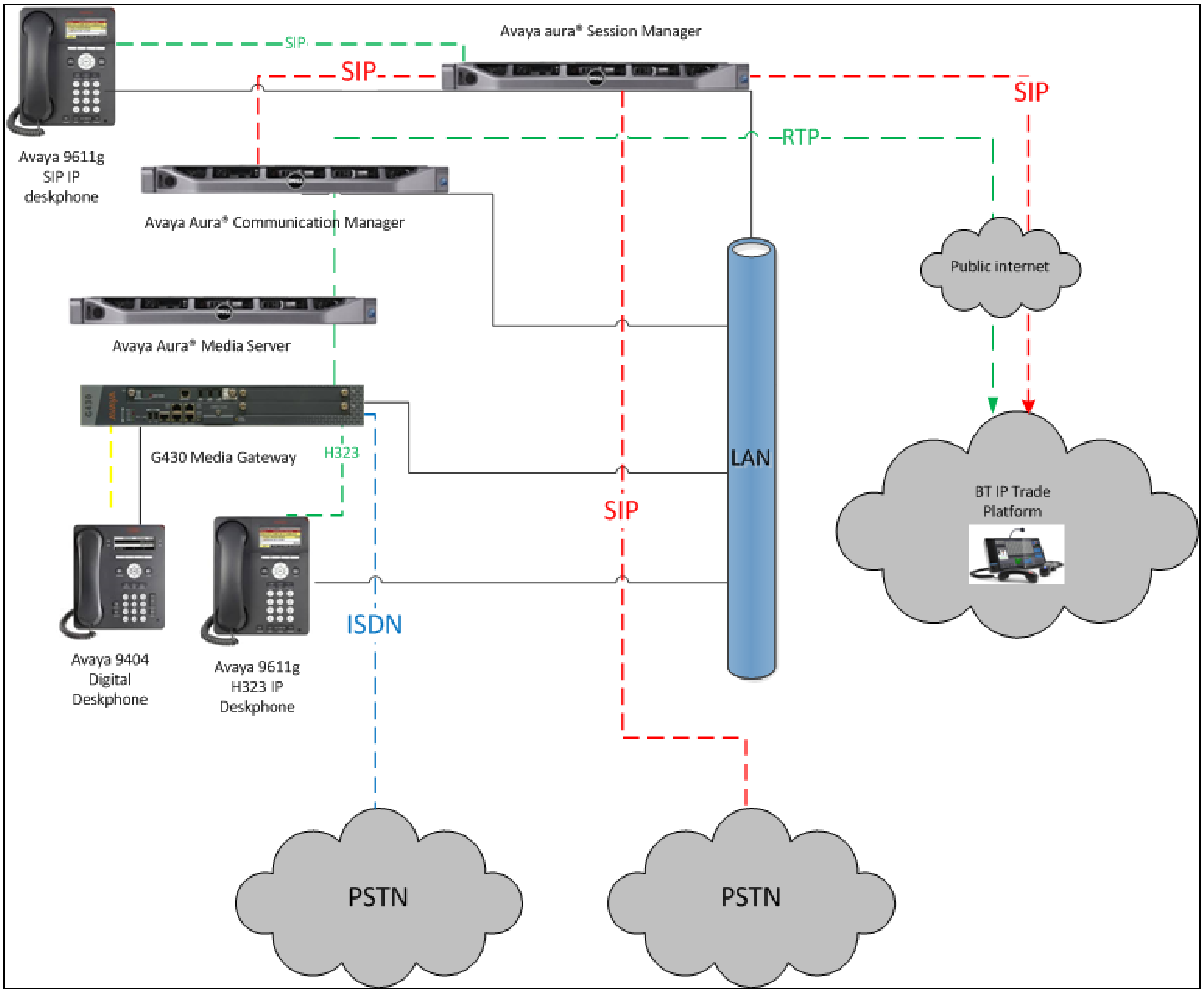
All test cases passed successfully.

2.3. Support

BT Unified Trade Interoperability Team
Email: Unified.Trade.interop.team@bt.com

3. Reference Configuration

The configuration shown in Figure 1 was used during the compliance test of BT IP Trade Platform with Session Manager and Communication Manager. BT IP Trade Platform manages Trade Turrets by registering with Session Manager and allowing communication with Avaya handsets



SIP
SIP
Avaya aura® Session Manager
SIP
RTP
Avaya 9611g SIP IP deskphone
Avaya Aura® Communication Manager
Public internet
Avaya Aura® Media Server
LAN
G430 Media Gateway
H323
BT IP Trade Platform
SIP
ISDN
Avaya 9404 Digital Deskphone
Avaya 9611g H323 IP Deskphone
PSTN
PSTN

Figure 1: Connection of BT IP Trade Platform with Avaya Aura® Session Manager and Avaya Aura® Communication Manager

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager	R7.1.2 FP2 R017x.01.0.532.0 CM 7.1.2.0.0.532.24184 KERNEL-3.10..0-693.e17.AVI PLAT-rhel17.2-0010
Avaya G450 Media Gateway	38.20.1/1
Avaya Aura® Session Manager	R7.1.2.0.712004
Avaya Aura® System Manager	R7.1.2 Build 7.1.0.0.1125193 Update 7.1.2.0.057353 Feature Pack 2
Avaya Aura® Media Server	v.7.8.0.309
Avaya 96x1 Series IP Deskphones H.323	6.6229
Avaya 96x1 Series IP Deskphones SIP	7.1.0.1.1
Avaya 94xx Series Digital Deskphones	R17.0
Turret Support Server(TSS)	9.1.0.41571
TPO	R9.1_0.41588
Turrets, T4 with XMA2	R9.1_0.41580

5. Configure Avaya Aura® Communication Manager

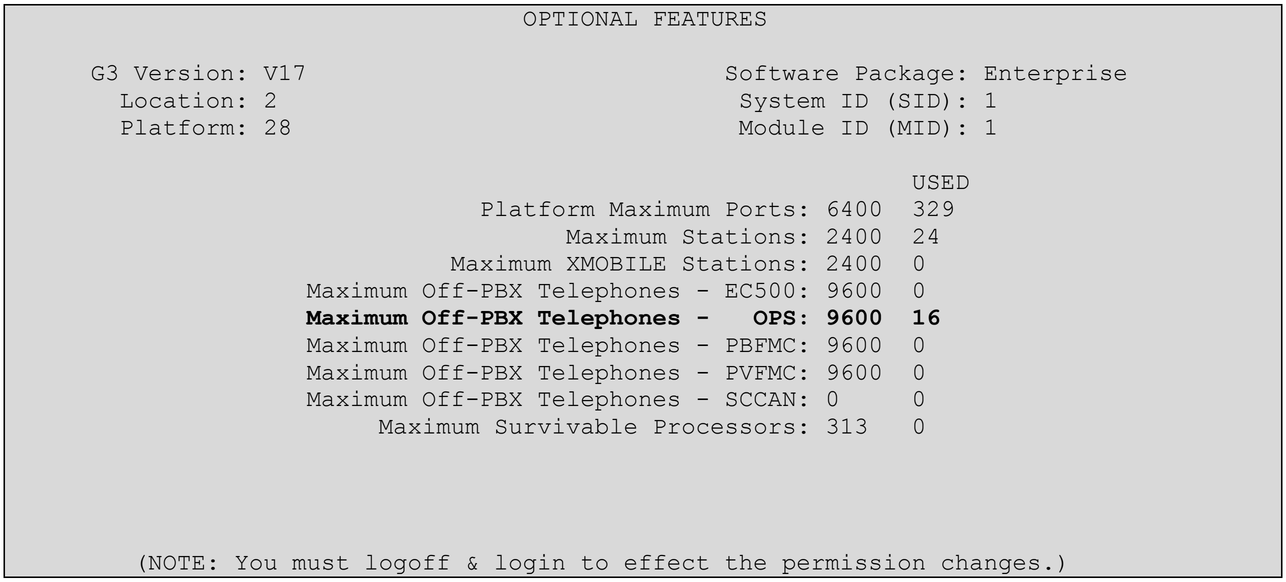
This section describes the steps required to allow Communication Manager to communicate with the IP Trade Platform. Is it assumed that Communication Manager is installed and configured before implementing the configuration steps. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**. The configuration illustrated in this section was performed using Communication Manager System Administration Terminal (SAT).

Configuration steps include:

- Check Off PBX Station Licensing.
- SIP Trunk Administration (to Session Manager).
- Adding Route Pattern.

5.1. Checking Licensing

Using the ***display system-parameters customer-options*** command go to **page 1** and check that the system is sufficiently licensed for **Off-PBX Telephones -   OPS**:.



```
                                    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  329
                                       Maximum Stations: 2400  24
                               Maximum XMOBILE Stations: 2400  0
                     Maximum Off-PBX Telephones - EC500: 9600  0
                     Maximum Off-PBX Telephones -   OPS: 9600  16
                     Maximum Off-PBX Telephones - PBFMC: 9600  0
                     Maximum Off-PBX Telephones - PVFMC: 9600  0
                     Maximum Off-PBX Telephones - SCCAN: 0     0
                          Maximum Survivable Processors: 313   0




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

5.2. Adding a SIP Trunk to Avaya Aura® Session Manager

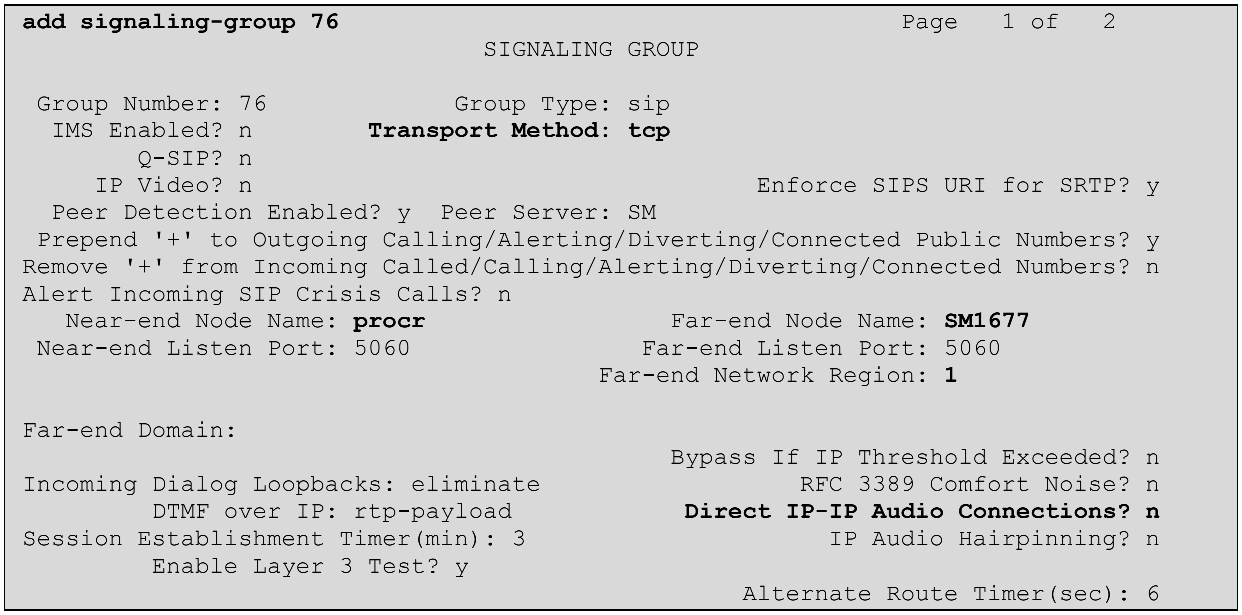
Use the ***change node-names ip*** command to add the Session Manager

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
SM1677              10.10.16.77
default             0.0.0.0
procr               10.10.16.27
procr6              ::-
```

Use ***change dialplan analysis*** to add a **3** digit dial access code(**dac**) for use in the SIP Trunk, a unform dial plan (**udp**) entry for calling out over the SIP Trunk and check that there is an entry for feature access codes(**fac**).

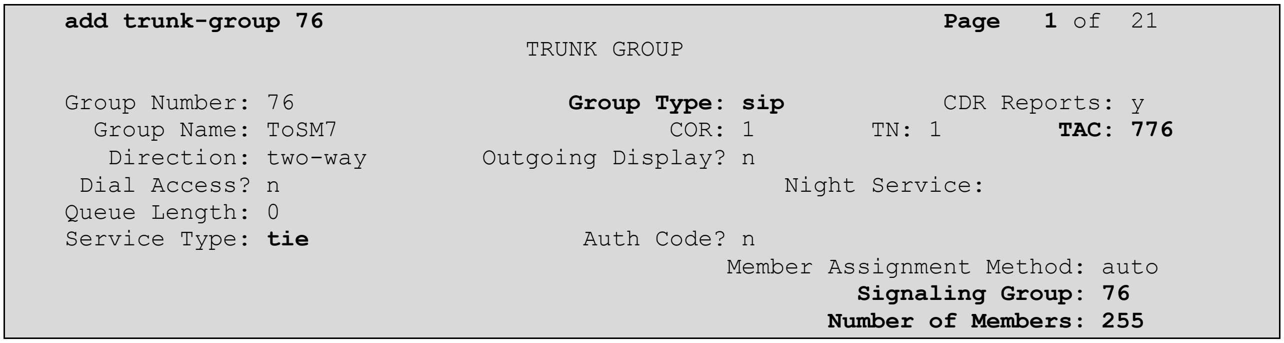
```
change dialplan analysis                                        Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location: all           Percent Full: 2

    Dialed   Total  Call      Dialed   Total  Call      Dialed   Total  Call
    String   Length Type      String   Length Type      String   Length Type
   2           7   udp
   7           3   dac
   8           5   udp
   8           7   udp
   827         7   ext
   9           1   fac
   *           3   fac
   #           3   fac
```

Use ***add-signaling-group x*** where x is the number of the group required. Set **Transport Method** to **tcp, Near-end Node Name** to **procr** and **Far-end Node Name** to the entry added in **node-names**. Set the **Far-end Network Region** to **1** and **Direct IP-IP Audio Connections?** to **n**



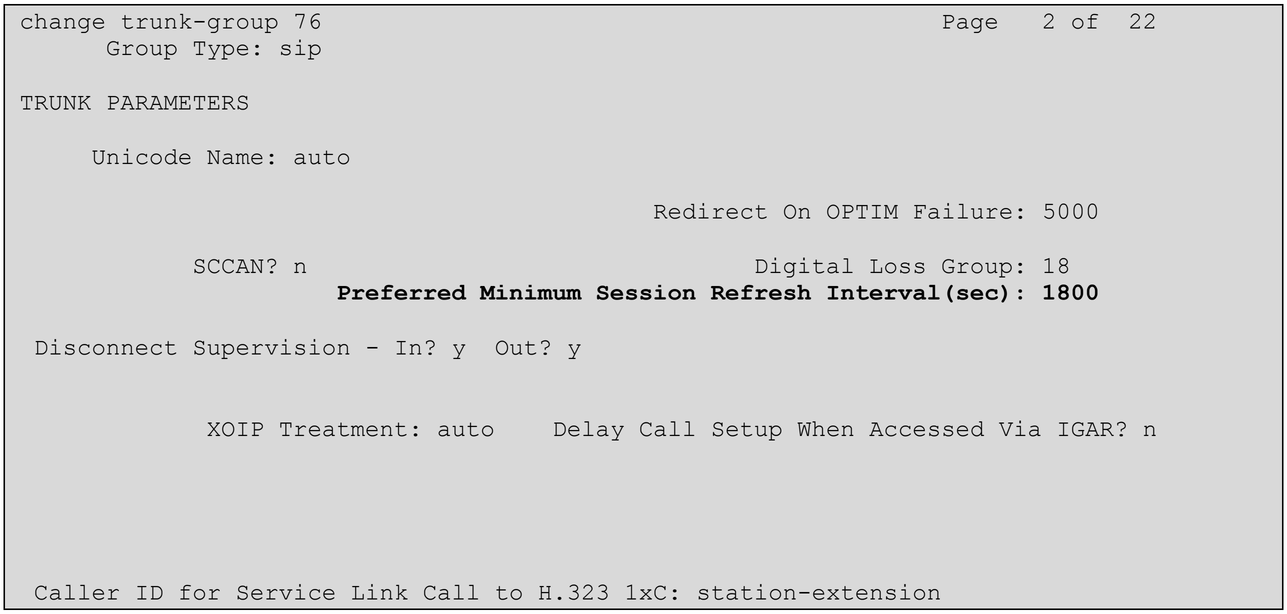
```
add signaling-group 76                                          Page   1 of   2
                                SIGNALING GROUP

 Group Number: 76             Group Type: sip
  IMS Enabled? n        Transport Method: tcp
        Q-SIP? n
     IP Video? n                                  Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr                   Far-end Node Name: SM1677
 Near-end Listen Port: 5060                  Far-end Listen Port: 5060
                                          Far-end Network Region: 1

Far-end Domain:
                                             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? n
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y
                                                  Alternate Route Timer(sec): 6
```

Use ***add trunk-group x*** where x is the number administered for the signaling group. On **Page 1** set the **Group Type** to **sip**. Set the **TAC** to suitable entry based on the dial plan **dac** administered above. Set the **Service Type** to **tie**, **Signaling group** to the one administered above and **Number of Members** to a number satisfactory for call routing required (**255** shown is the max for this type of trunk group).



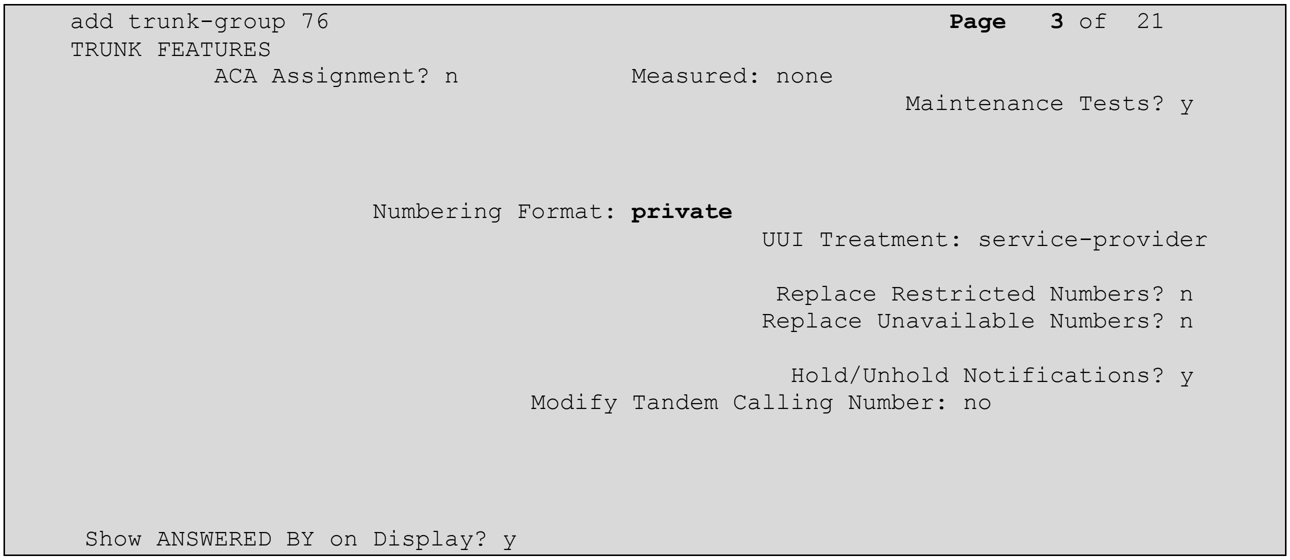
```
add trunk-group 76                                              Page   1 of  21
                                TRUNK GROUP

Group Number: 76                   Group Type: sip          CDR Reports: y
  Group Name: ToSM7                       COR: 1        TN: 1        TAC: 776
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: tie                  Auth Code? n
                                            Member Assignment Method: auto
                                                     Signaling Group: 76
                                                   Number of Members: 255
```

On **Page 2** set the **Preferred Minimum Session refresh Interval(sec): to 1800** as this is a time greater than the BT Session Manager refresh interval.



```
change trunk-group 76                                           Page   2 of  22
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name: auto

                                            Redirect On OPTIM Failure: 5000

            SCCAN? n                                   Digital Loss Group: 18
                      Preferred Minimum Session Refresh Interval(sec): 1800

 Disconnect Supervision - In? y  Out? y


             XOIP Treatment: auto    Delay Call Setup When Accessed Via IGAR? n




 Caller ID for Service Link Call to H.323 1xC: station-extension
```

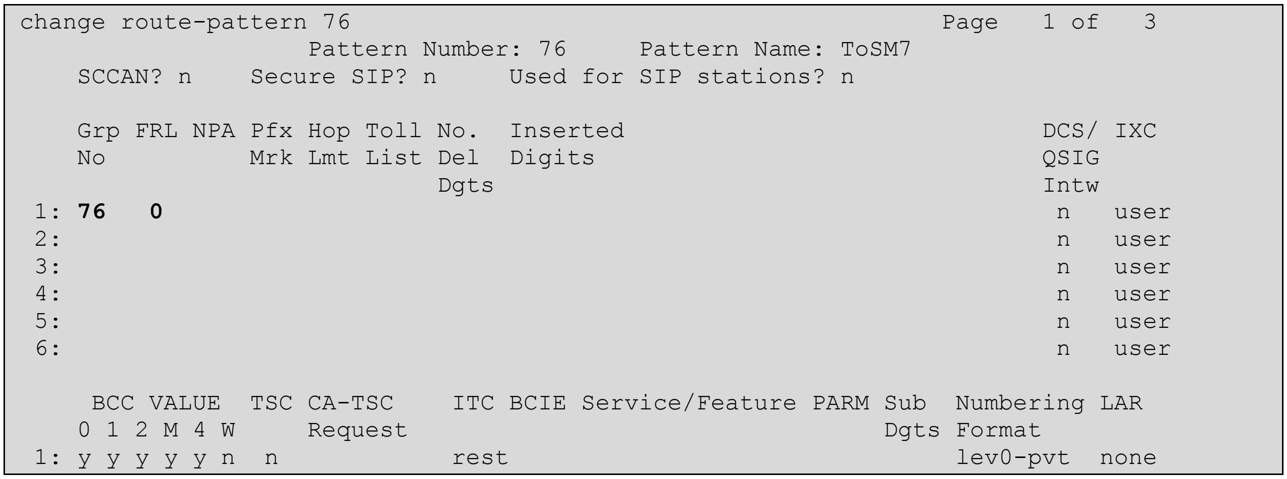
On P**age 3** set the **Numbering Format**. For this test the **private** numbering table was used to set the calling party number format.



```
   add trunk-group 76                                           Page   3 of  21
   TRUNK FEATURES
             ACA Assignment? n            Measured: none
                                                             Maintenance Tests? y



                        Numbering Format: private
                                                   UUI Treatment: service-provider

                                                    Replace Restricted Numbers? n
                                                   Replace Unavailable Numbers? n

                                                     Hold/Unhold Notifications? y
                                   Modify Tandem Calling Number: no




    Show ANSWERED BY on Display? y
```

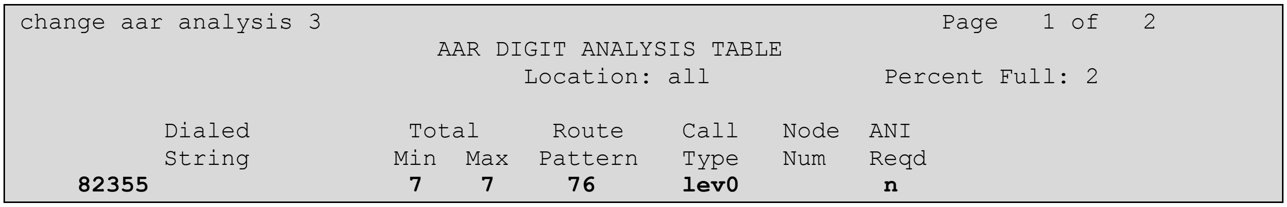
5.3. Adding a Route Pattern

A route pattern needs to be added so that call can be routed out of Communication Manager to Session Manager. Use ***change route-pattern x*** where x is the number of the SIP trunk created. Enter the Trunk group created above beside the first **Grp No,** an **FRL** of **0**.



```
change route-pattern 76                                         Page   1 of   3
                    Pattern Number: 76     Pattern Name: ToSM7
    SCCAN? n    Secure SIP? n     Used for SIP stations? n

    Grp FRL NPA Pfx Hop Toll No.  Inserted                             DCS/ IXC
    No          Mrk Lmt List Del  Digits                               QSIG
                             Dgts                                      Intw
 1: 76   0                                                              n   user
 2:                                                                     n   user
 3:                                                                     n   user
 4:                                                                     n   user
 5:                                                                     n   user
 6:                                                                     n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM Sub  Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
 1: y y y y y n  n            rest                               lev0-pvt  none
```

An Alternate Route Selection (ars) entry must be made for dialing the external numbers that are to be routed via the BT IP Trade Platform. Use ***change aar analysis x*** where x is the first number in the dialed string. Set **Dialed String** to **x**, **Total Min/Max** to the length of the number to be dialed, **Route Pattern** to the one administered above and **Call Type** to **lev0.**



```
change aar analysis 3                                           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
    82355                  7    7     76      lev0          n
```

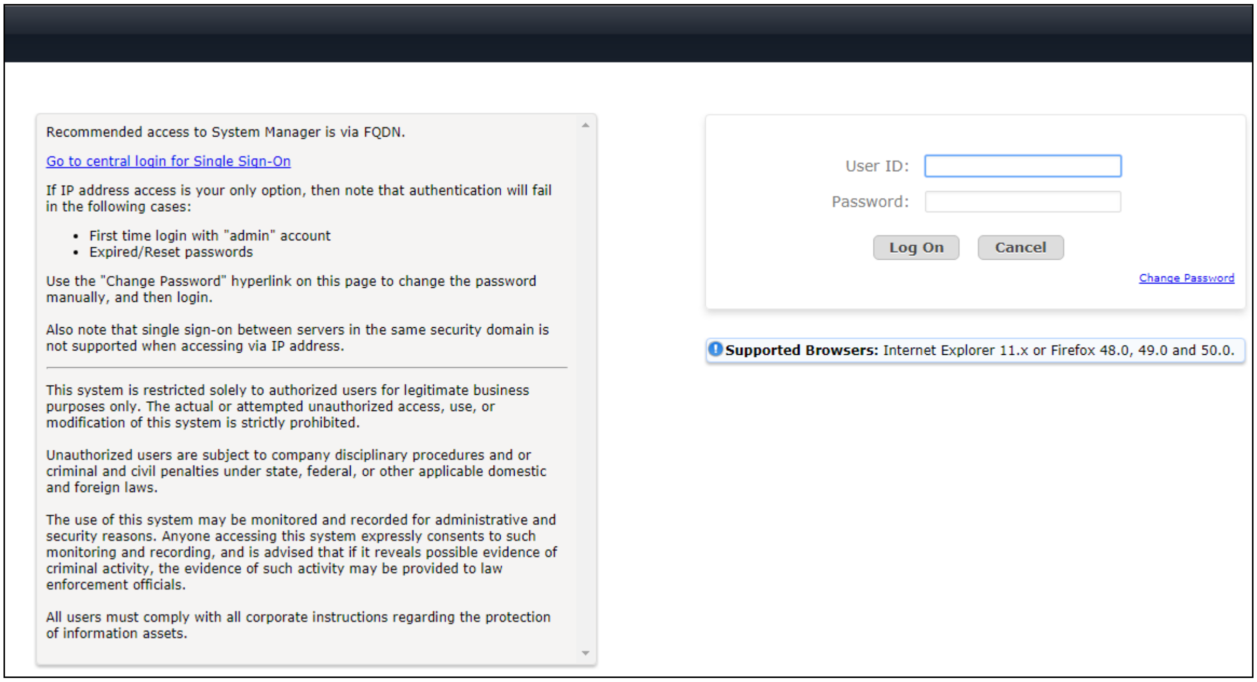
6. Configure Avaya Aura® Session Manager

In this section the configuration steps required to connect BT IP Trade Platform to Session Manager as a SIP Endpoint is described. It is assumed that an existing Session manager instance has already been installed and configured as this is out of the scope of this document. All Configuration steps were carried out using Avaya Aura® System Manager. Configuration steps will include:

- Adding a BT IP Trade Turrets as SIP Users.

6.1. Configure SIP User

A SIP user must be added for each BT IP Trade Turret required. Navigate to the System Manager web interface, in this case **https://<IP Address>/SMGR** and login with the relevant credentials.



Recommended access to System Manager is via FQDN.

Go to central login for Single Sign-On

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

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

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

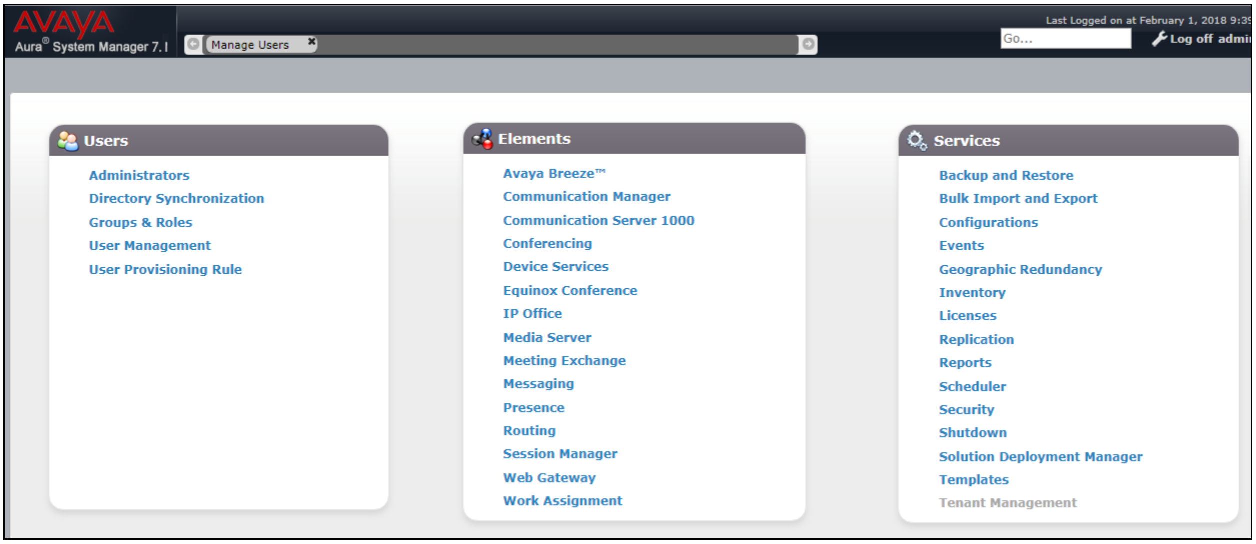
All users must comply with all corporate instructions regarding the protection of information assets.

User ID:

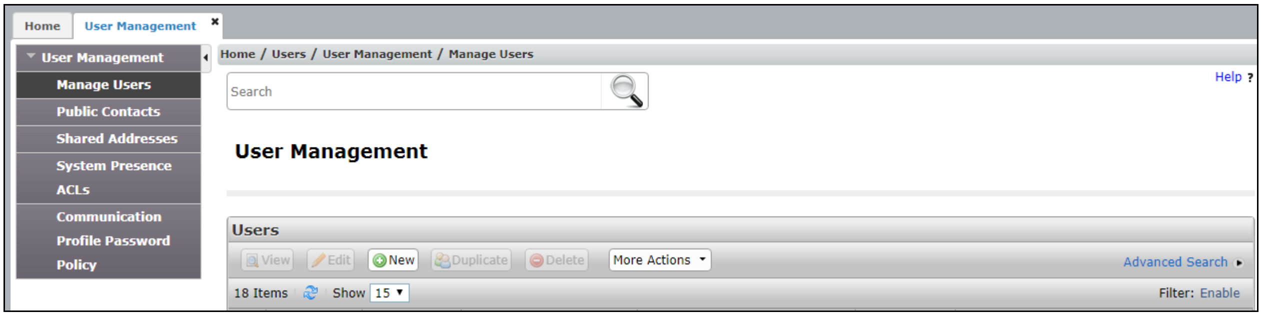
Password:

Supported Browsers: Internet Explorer 11.x or Firefox 48.0, 49.0 and 50.0.

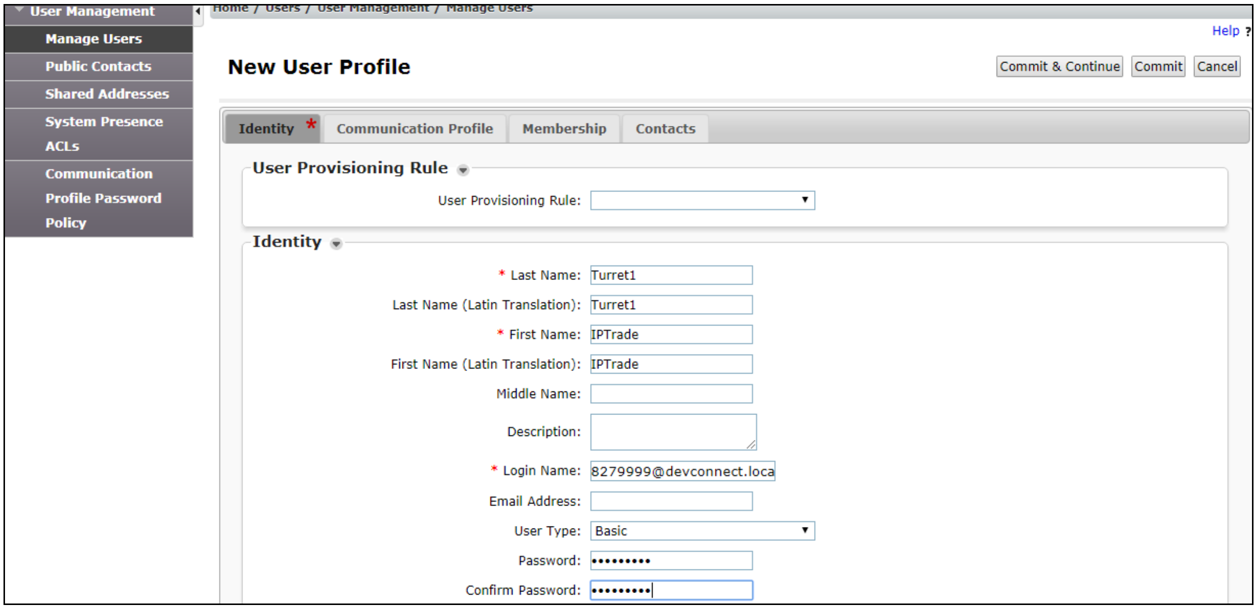
From the Dashboard select **Users → User Management**



Select **Manage Users → New**



On the Identity tab enter an identifying **Last Name** and **First Name**, enter an appropriate **Login Name**, set **Authentication Type** to **Basic** and administer a password in the **Password** and **Confirm Password** fields.



New User Profile

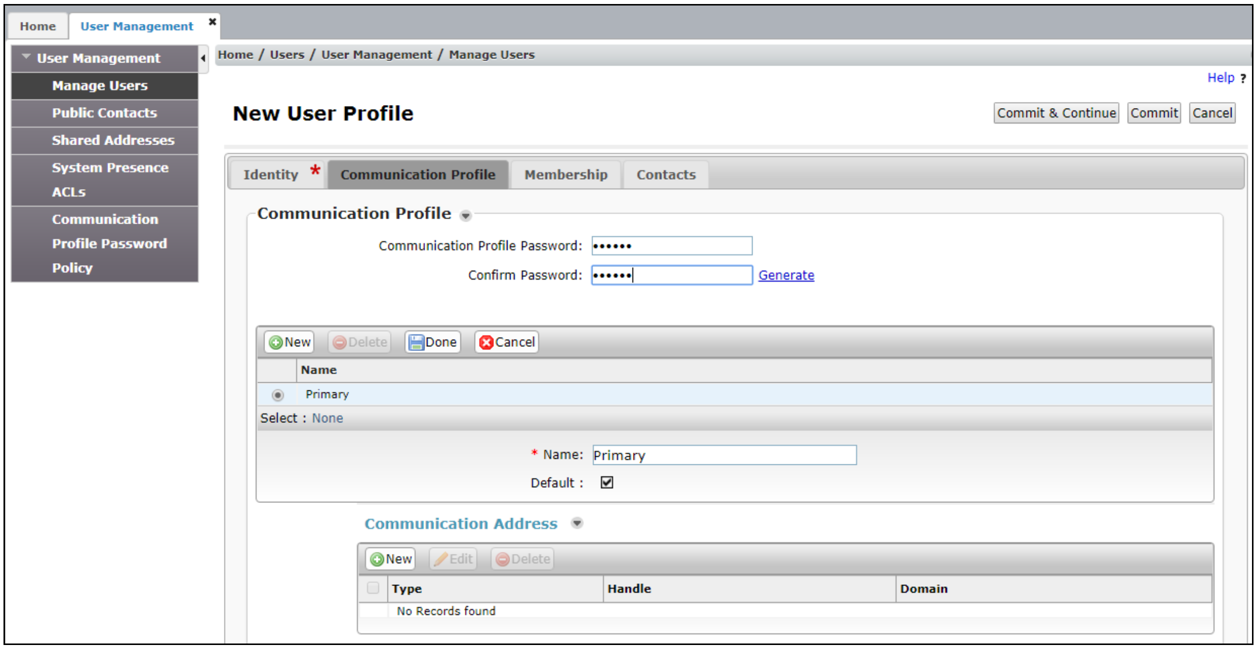
User Provisioning Rule

User Provisioning Rule:

Identity

* Last Name: Turret1
Last Name (Latin Translation): Turret1
* First Name: IPTrade
First Name (Latin Translation): IPTrade
Middle Name:
Description:
* Login Name: 8279999@devconnect.loca
Email Address:
User Type: Basic
Password: •••••••••
Confirm Password: •••••••••

Click on the **Communication Profile** tab and enter and confirm a **Communication Profile Password**, this is used when logging in the SIP endpoint. Under **Communication Address** click **New**.



New User Profile

Communication Profile

Communication Profile Password: ••••••
Confirm Password: ••••••

	Name
●	Primary

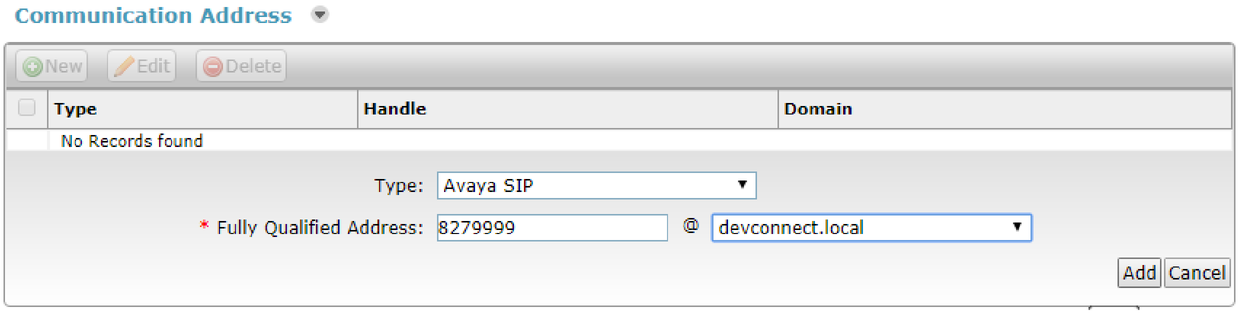
Select : None

* Name: Primary
Default : ☑

Communication Address

□	Type	Handle	Domain
	No Records found		

Select **Avaya SIP** from the **Type** drop down box and enter the **Fully Qualified Address** of the new SIP user. Click **Add** when done.

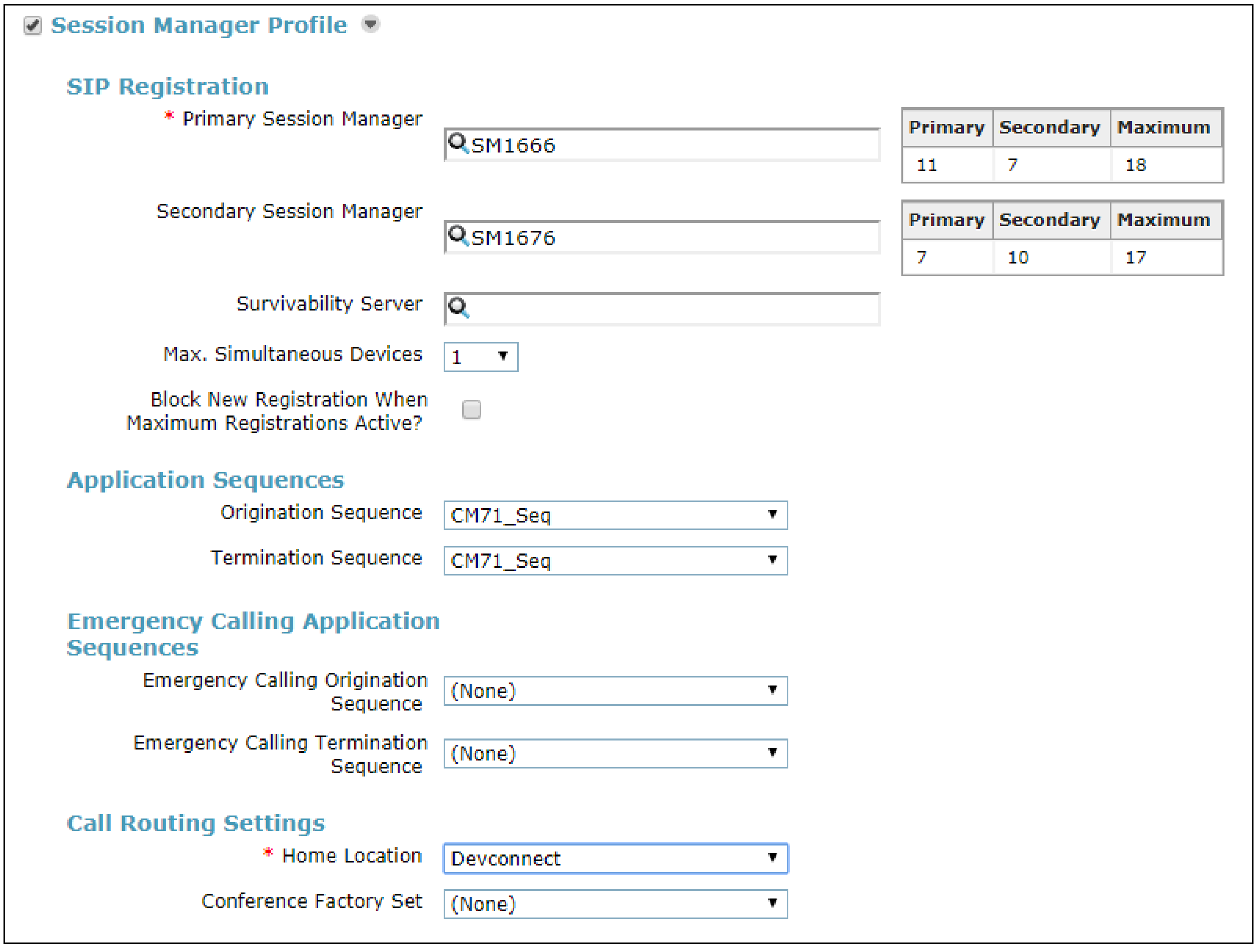


☐	Type	Handle	Domain
	No Records found		

Type: Avaya SIP

* Fully Qualified Address: 8279999 @ devconnect.local

Continue to scroll down on the same page. Select Session Manager Profile and enter the **Primary Session Manager, Origination Application Sequence, Termination Application Sequence** and **Home Location** relevant to the implementation.


☑ Session Manager Profile

SIP Registration

* Primary Session Manager: SM1666

Primary	Secondary	Maximum
11	7	18

Secondary Session Manager: SM1676

Primary	Secondary	Maximum
7	10	17

Survivability Server:

Max. Simultaneous Devices: 1

Block New Registration When Maximum Registrations Active? ☐

Application Sequences

Origination Sequence: CM71_Seq

Termination Sequence: CM71_Seq

Emergency Calling Application Sequences

Emergency Calling Origination Sequence: (None)

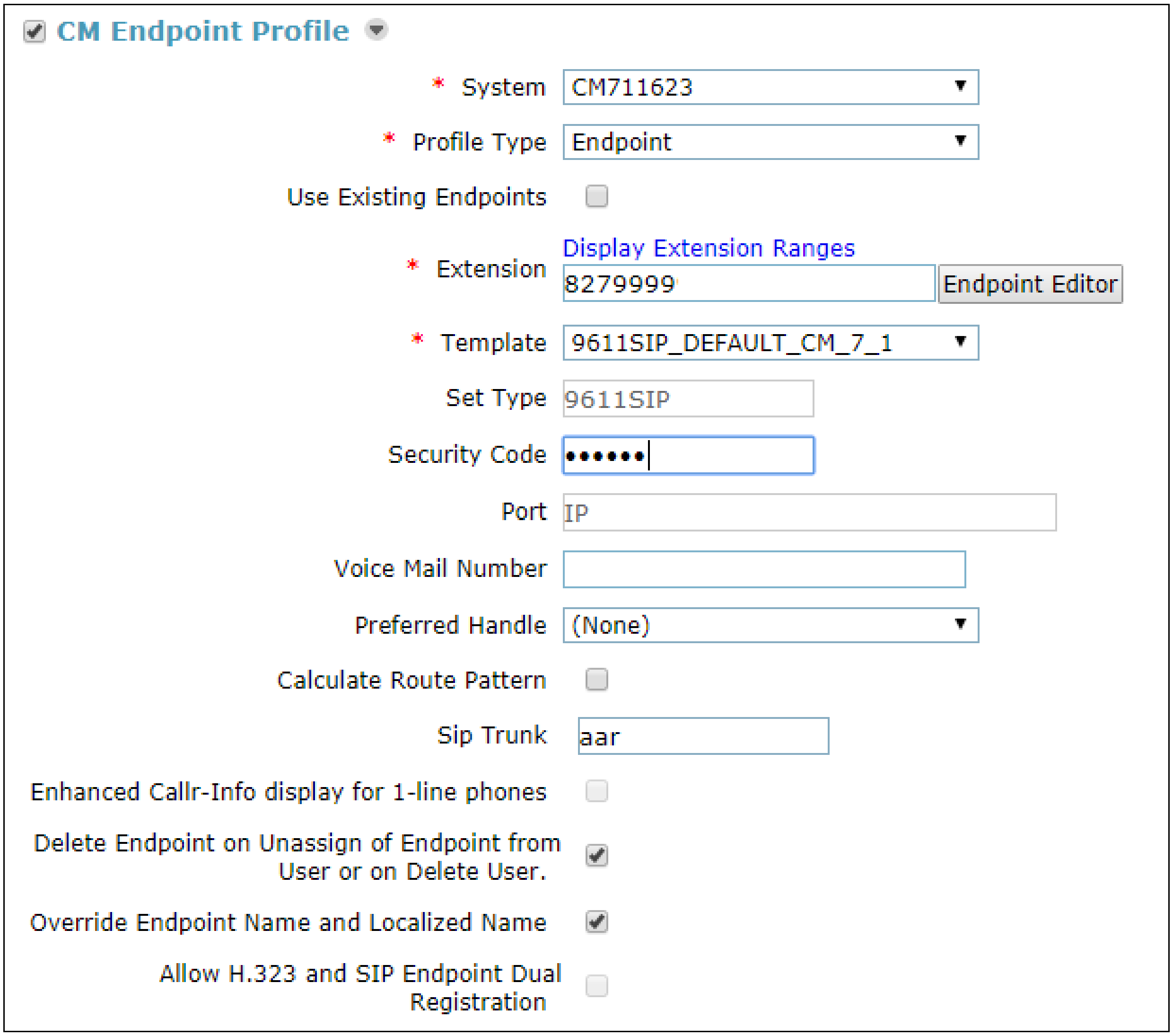
Emergency Calling Termination Sequence: (None)

Call Routing Settings

* Home Location: Devconnect

Conference Factory Set: (None)

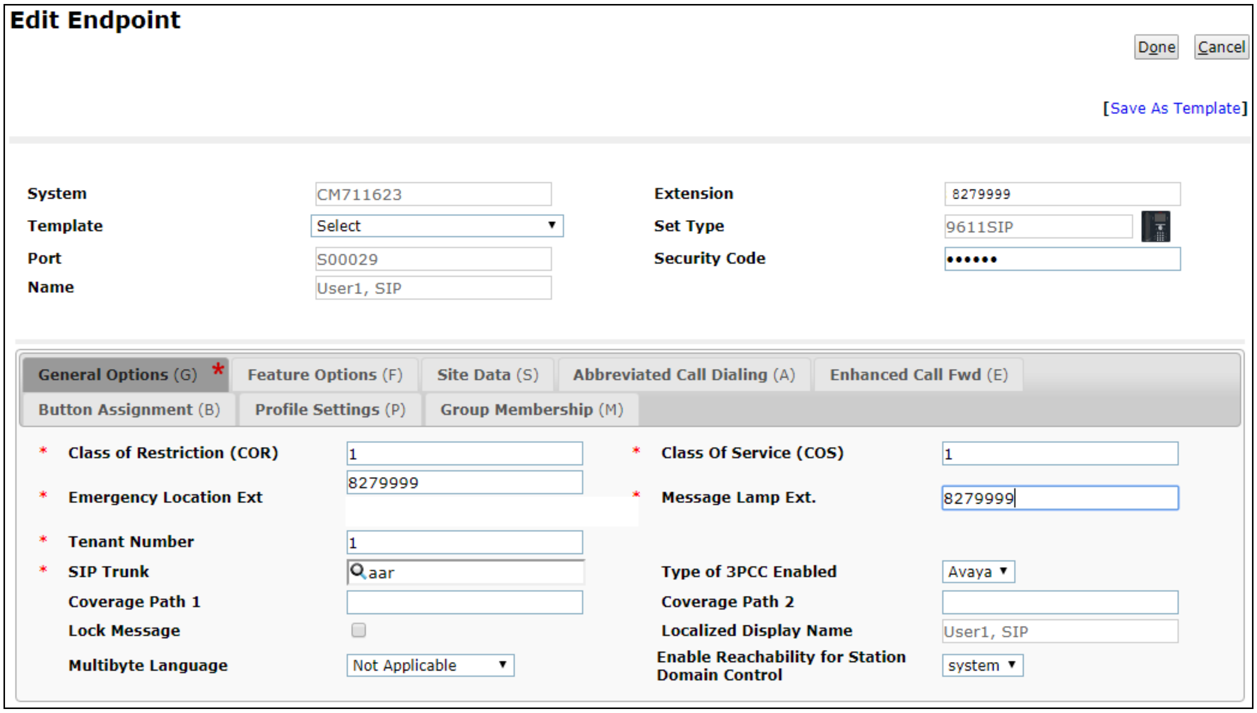
Scroll down the page and select **CM Endpoint Profile** section. Select the Communication Manager system from the **System** drop down box, select **Endpoint** as the **Profile Type**, enter the **Extension** number you wish to use, select **9611SIP_DEFAULT_CM_7_1** as the **Template** and ensure **IP** is configured as the **Port**, click Commit & Coninue (not shown) when finished.



☑ CM Endpoint Profile

* System	CM711623
* Profile Type	Endpoint
Use Existing Endpoints	□
* Extension	Display Extension Ranges 8279999 [Endpoint Editor]
* Template	9611SIP_DEFAULT_CM_7_1
Set Type	9611SIP
Security Code	••••••
Port	IP
Voice Mail Number	
Preferred Handle	(None)
Calculate Route Pattern	□
Sip Trunk	aar
Enhanced Callr-Info display for 1-line phones	□
Delete Endpoint on Unassign of Endpoint from User or on Delete User.	☑
Override Endpoint Name and Localized Name	☑
Allow H.323 and SIP Endpoint Dual Registration	□

Click on **Endpoint Editor** in the **CM Endpoint Profile** and on the General options tab set **Type of 3PCC Enabled** as **Avaya**. Click on **Done** to save changes and go back to the User Communication Profile screen.

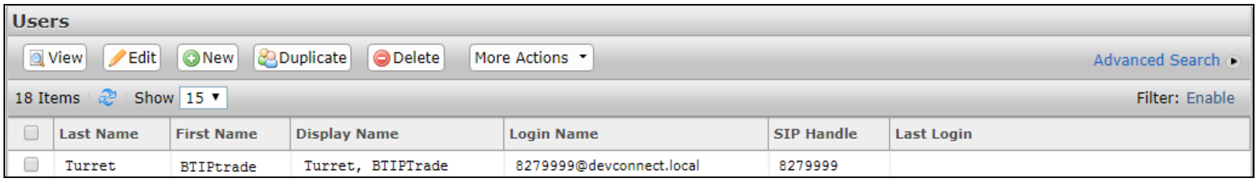


Edit Endpoint

System	CM711623	Extension	8279999
Template	Select	Set Type	9611SIP
Port	S00029	Security Code	••••••
Name	User1, SIP		

* Class of Restriction (COR)	1	* Class Of Service (COS)	1
* Emergency Location Ext	8279999	* Message Lamp Ext.	8279999
* Tenant Number	1		
* SIP Trunk	aar	Type of 3PCC Enabled	Avaya
Coverage Path 1		Coverage Path 2	
Lock Message	□	Localized Display Name	User1, SIP
Multibyte Language	Not Applicable	Enable Reachability for Station Domain Control	system

Click on Commit to save the user. The user is now listed



Users

	Last Name	First Name	Display Name	Login Name	SIP Handle	Last Login
□	Turret	BTIPtrade	Turret, BTIPTrade	8279999@devconnect.local	8279999	

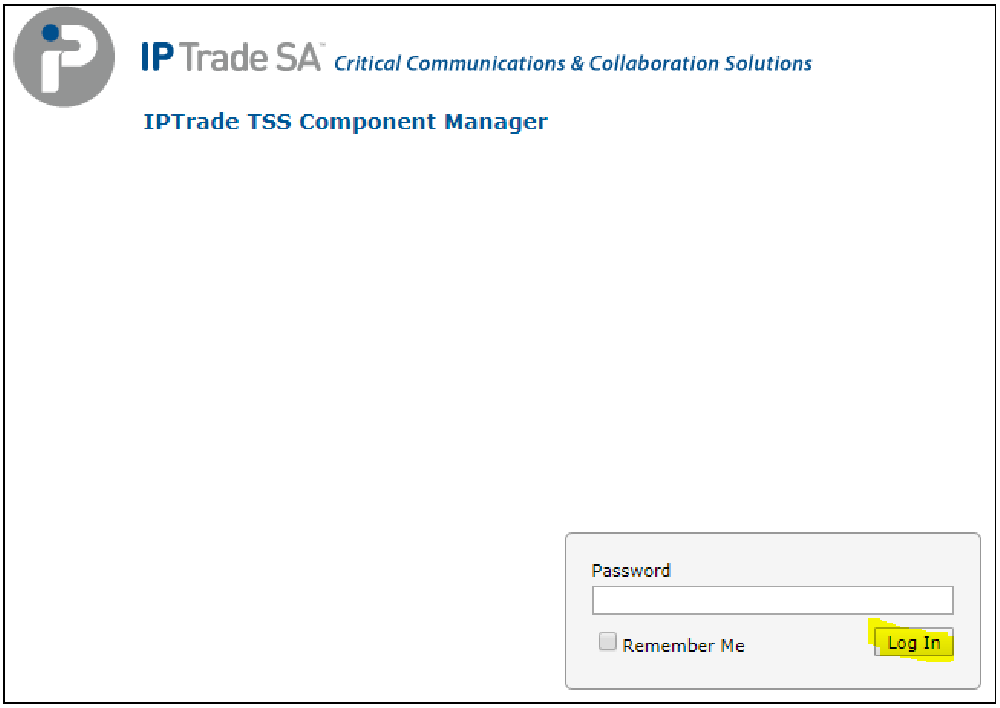
7. Configure the IP Trade System.

This section addresses the administrative steps to be performed on the IP Trade solution. The installation of the IP Trade solution software, as well as the initial configuration of the turrets and servers, is beyond the scope of this document.

7.1. Configure the IP Trade Turret Support Server.

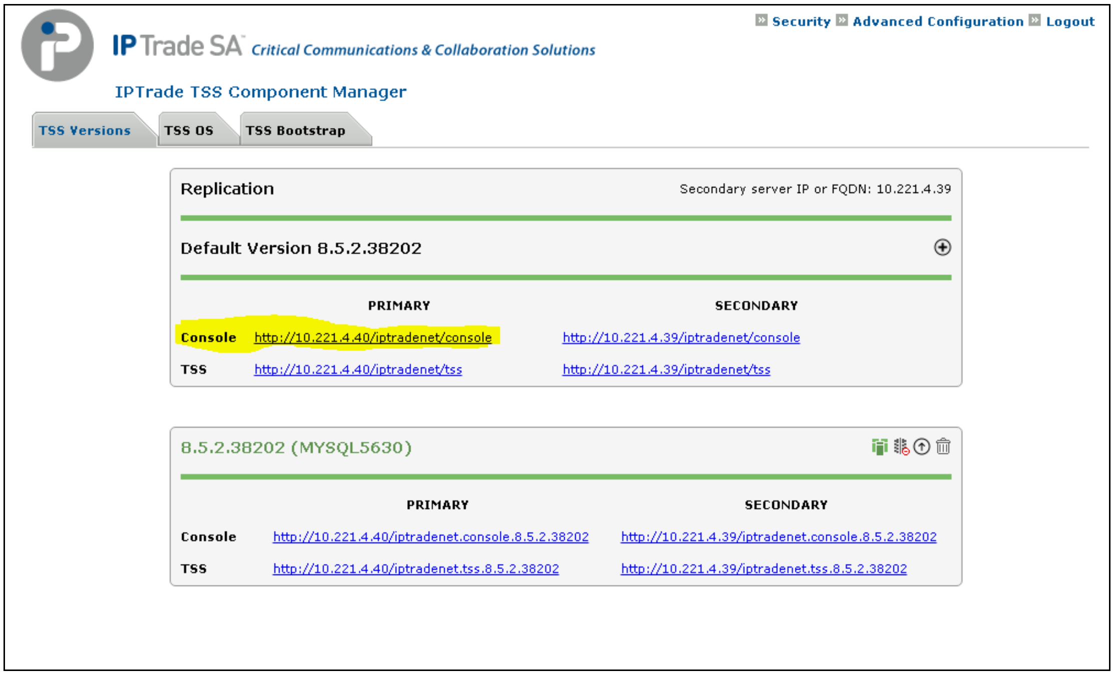
This section describes the procedure for configuring the IP Trade Turret Support Server (TSS). This procedure assumes that the TSS has already been configured with an anonymous profile and that a TFTP server (typically co-resident with the TSS) is being used for downloading certain configuration parameters to the turrets.

From a Web browser, navigate to the IP Address of the TSS. Enter the correct password and click on **Log In**.


IP Trade SA Critical Communications & Collaboration Solutions
IPTrade TSS Component Manager
Password
□ Remember Me
Log In

Upon selecting Log In, the following screen will be presented.

From the TSS Versions tab select the **Console** Link as shown below.


Security
Advanced Configuration
Logout
IP Trade SA Critical Communications & Collaboration Solutions
IPTrade TSS Component Manager
TSS Versions
TSS OS
TSS Bootstrap

Replication — Secondary server IP or FQDN: 10.221.4.39

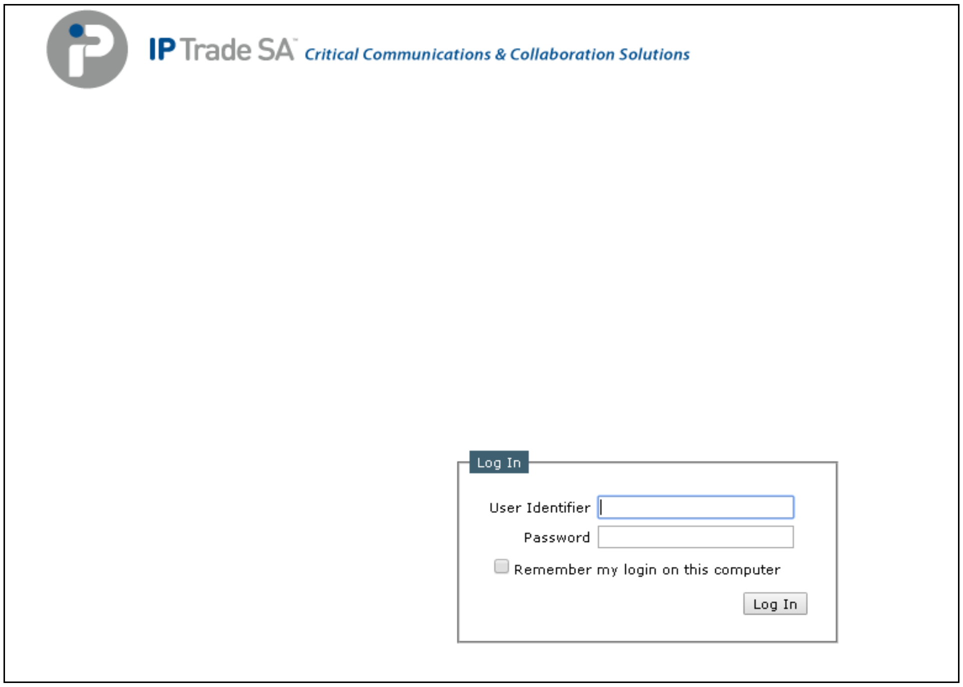
Default Version 8.5.2.38202

	PRIMARY	SECONDARY
Console	http://10.221.4.40/iptradenet/console	http://10.221.4.39/iptradenet/console
TSS	http://10.221.4.40/iptradenet/tss	http://10.221.4.39/iptradenet/tss

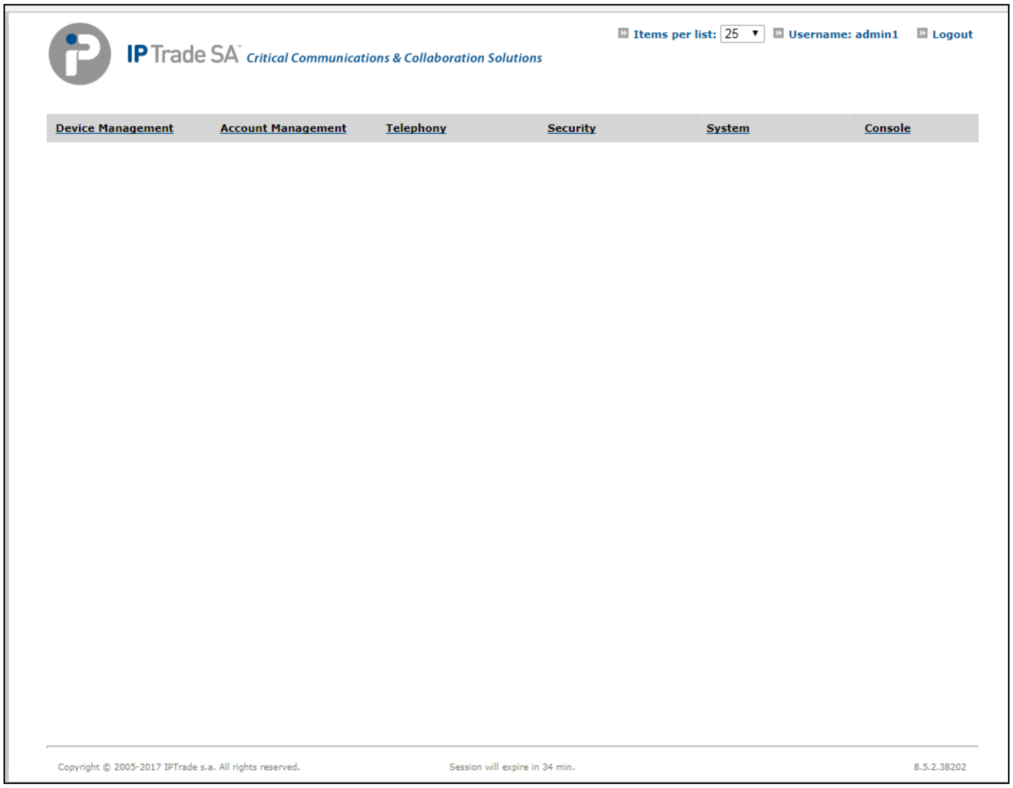
8.5.2.38202 (MYSQL5630)

	PRIMARY	SECONDARY
Console	http://10.221.4.40/iptradenet.console.8.5.2.38202	http://10.221.4.39/iptradenet.console.8.5.2.38202
TSS	http://10.221.4.40/iptradenet.tss.8.5.2.38202	http://10.221.4.39/iptradenet.tss.8.5.2.38202

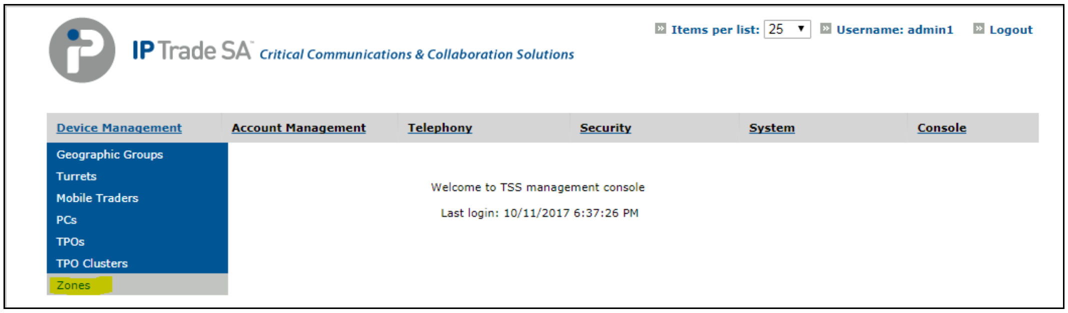
Enter the **User Identifier** and **Password** for the IP Trade system and select **Log In**.


IP Trade SA Critical Communications & Collaboration Solutions
Log In
User Identifier
Password
□ Remember my login on this computer
Log In

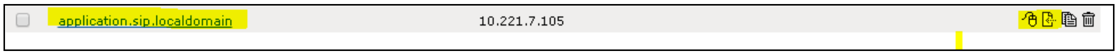
Upon successful login, the following screen will be presented.


IP Trade SA Critical Communications & Collaboration Solutions
Items per list: 25
Username: admin1
Logout
Device Management
Account Management
Telephony
Security
System
Console
Copyright © 2005-2017 IPTrade s.a. All rights reserved.
Session will expire in 34 min.
8.5.2.38202

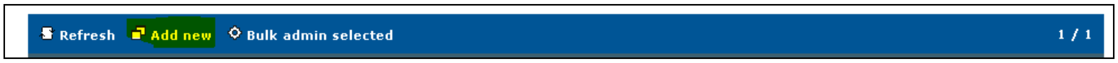
Select **Device Management** from the top menu bar and then **Zones** from the resulting drop down box.



NOTE: If any of the below advanced parameters are already configured, you just need to edit them rather than add. This can be done by either clicking the advanced parameter or by selecting either of the two symbols as shown in the picture below.



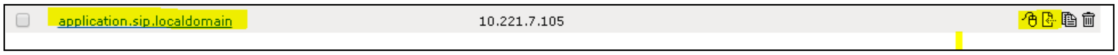
Select **Add new** from the menu bar.



Enter a name for the new zone and accept all other defaults on the first page then select **Update** (not shown).

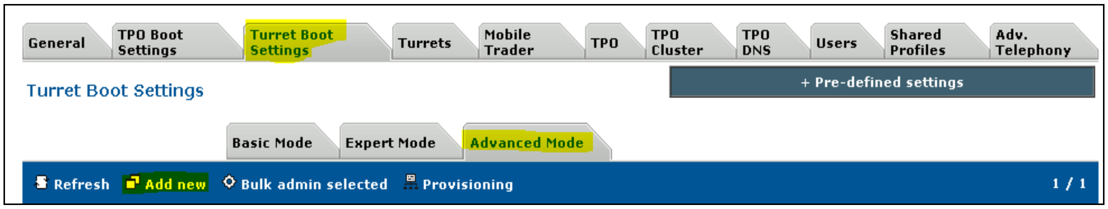
Navigate to the **Turret Boot Settings** Tab and then select **the Advanced Mode** tab.

NOTE: If any of the below advanced parameters are already configured, you just need to edit them rather than add. This can be done by either clicking the advanced parameter or by selecting either of the two symbols as shown in the picture below.

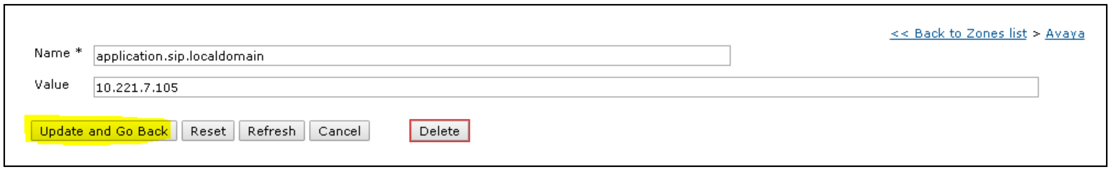


application.sip.localdomain 10.221.7.105

If the advanced parameter is not present, select **Add new**.



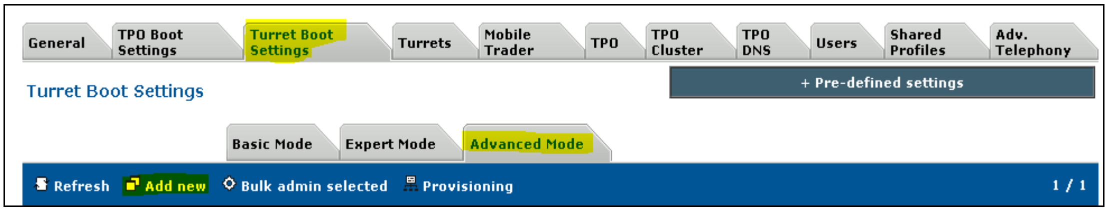
Now enter the statement below beside **Name:** The IP Address should mirror the Session Manager. In this example the IP Address is 10.221.7.105. When complete, select **Update and Go Back.**



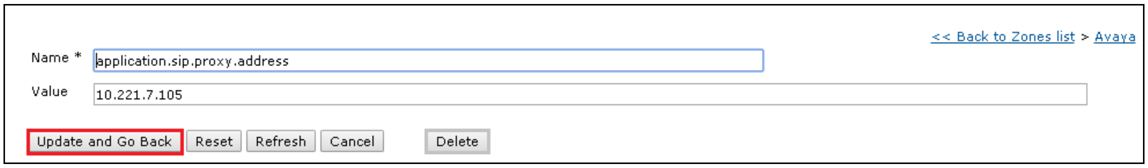
Name * application.sip.localdomain

Value 10.221.7.105

Select **Add new**.



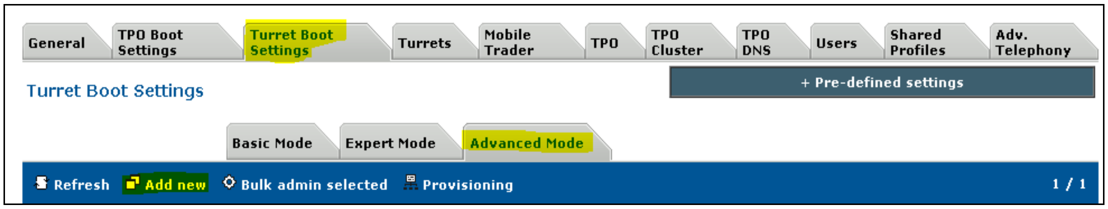
Again, enter the name exactly as it is above and specify the Session Manager. When complete, select **Update and Go Back.**



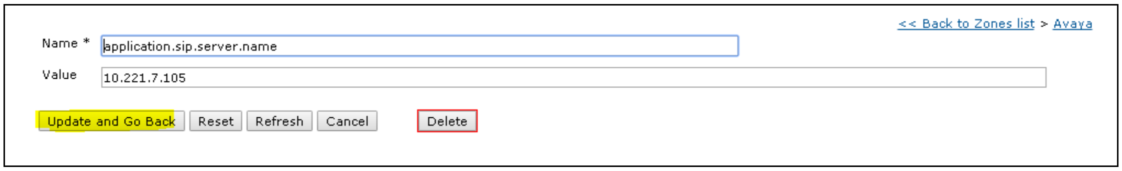
Name * application.sip.proxy.address

Value 10.221.7.105

Select **Add new**.



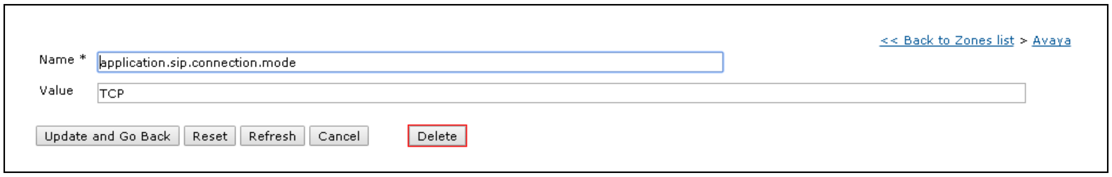
Again, enter the name exactly as it is above and specify the Avaya Session Manager. When complete, select **Update and Go Back.**



Name * application.sip.server.name

Value 10.221.7.105

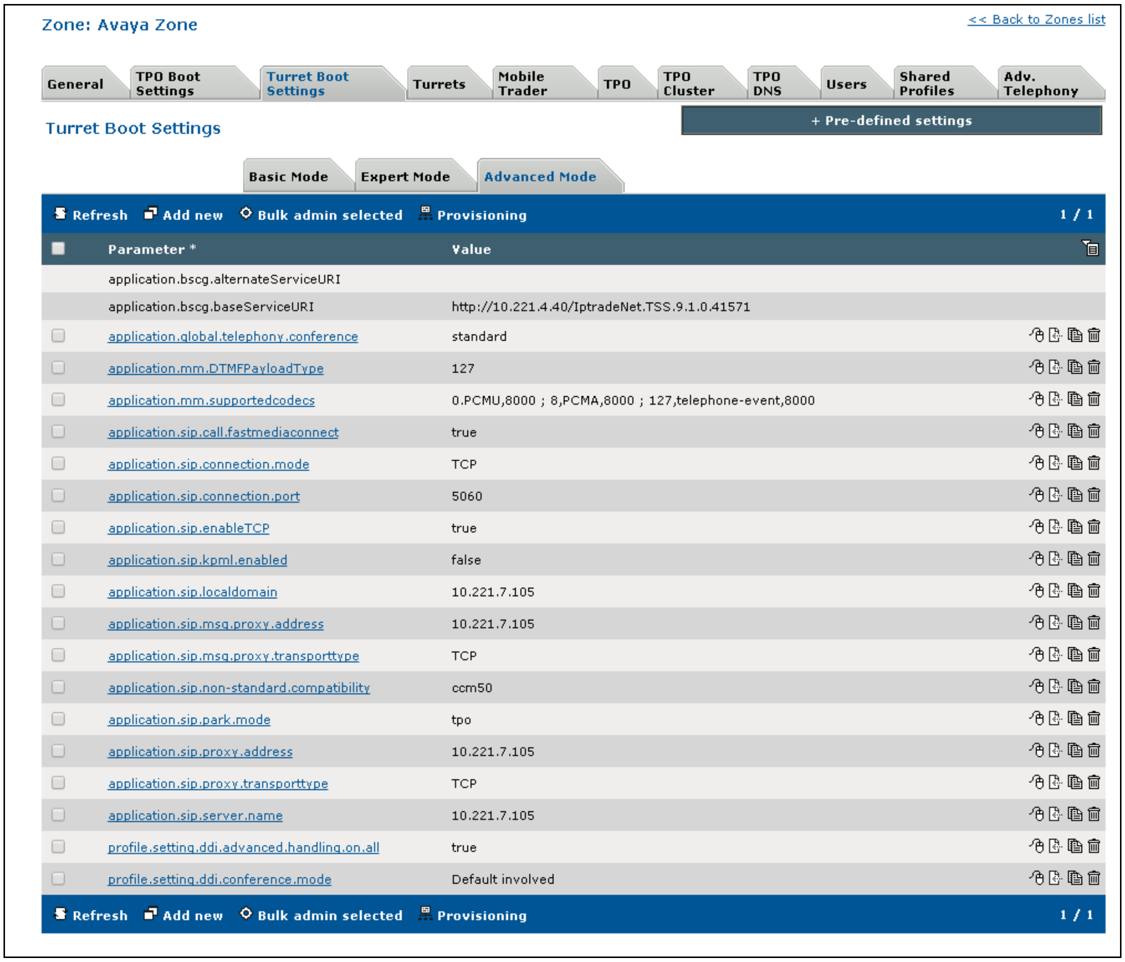
Lastly, select the advanced parameter, application.sip.connection.mode and change the transport type from UDP to TCP



Name * application.sip.connection.mode

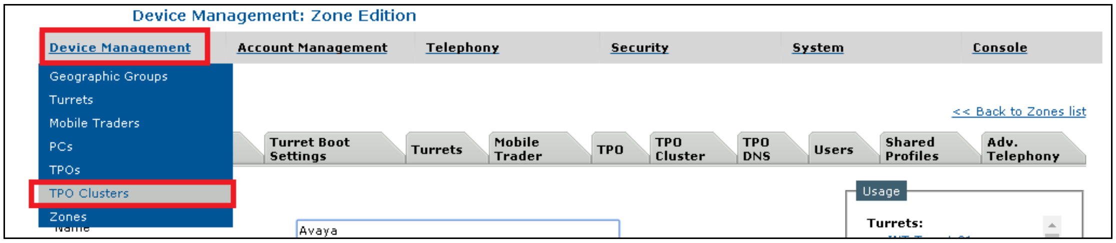
Value TCP

Finally, please ensure that all other advanced parameters are configured as shown below. Add any that are missing by using the same process as above or by using the individual menus..



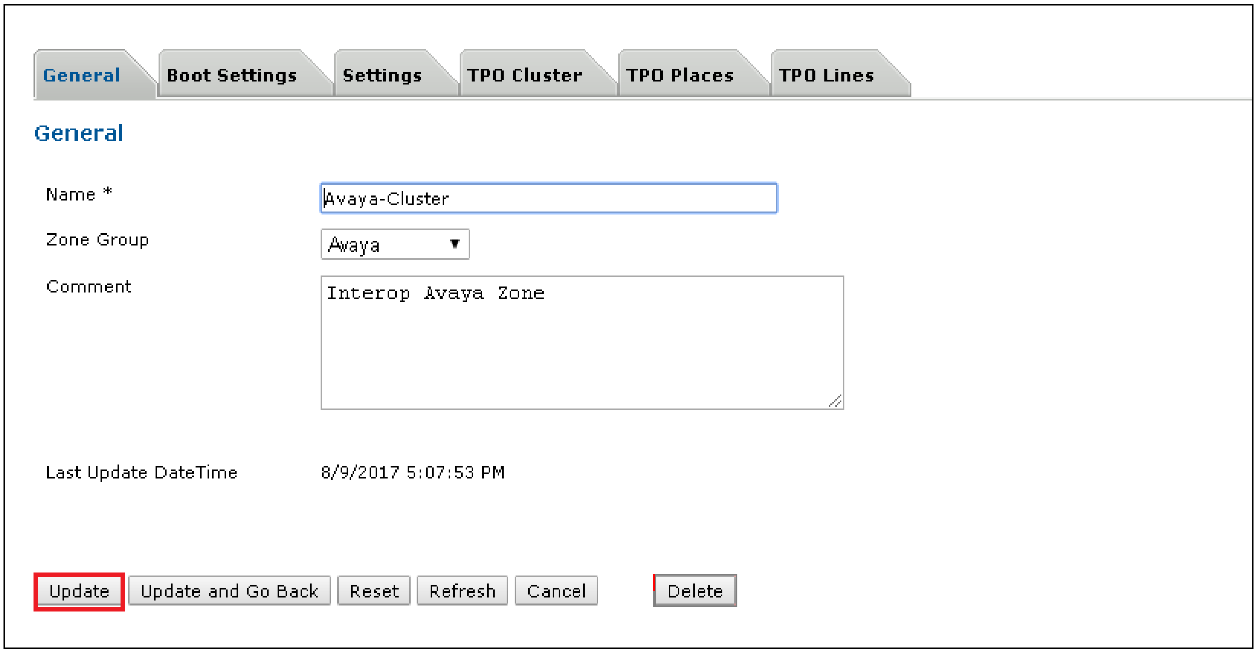
Parameter *	Value
application.bscg.alternateServiceURI	
application.bscg.baseServiceURI	http://10.221.4.40/IptradeNet.TSS.9.1.0.41571
application.global.telephony.conference	standard
application.mm.DTMFPayloadType	127
application.mm.supportedcodecs	0.PCMU,8000 ; 8,PCMA,8000 ; 127,telephone-event,8000
application.sip.call.fastmediaconnect	true
application.sip.connection.mode	TCP
application.sip.connection.port	5060
application.sip.enableTCP	true
application.sip.kpml.enabled	false
application.sip.localdomain	10.221.7.105
application.sip.msg.proxy.address	10.221.7.105
application.sip.msg.proxy.transporttype	TCP
application.sip.non-standard.compatibility	ccm50
application.sip.park.mode	tpo
application.sip.proxy.address	10.221.7.105
application.sip.proxy.transporttype	TCP
application.sip.server.name	10.221.7.105
profile.setting.ddi.advanced.handling.on.all	true
profile.setting.ddi.conference.mode	Default involved

From the Top menu, select **Device Management** and then **TPO Clusters.**



Select **Add new**.

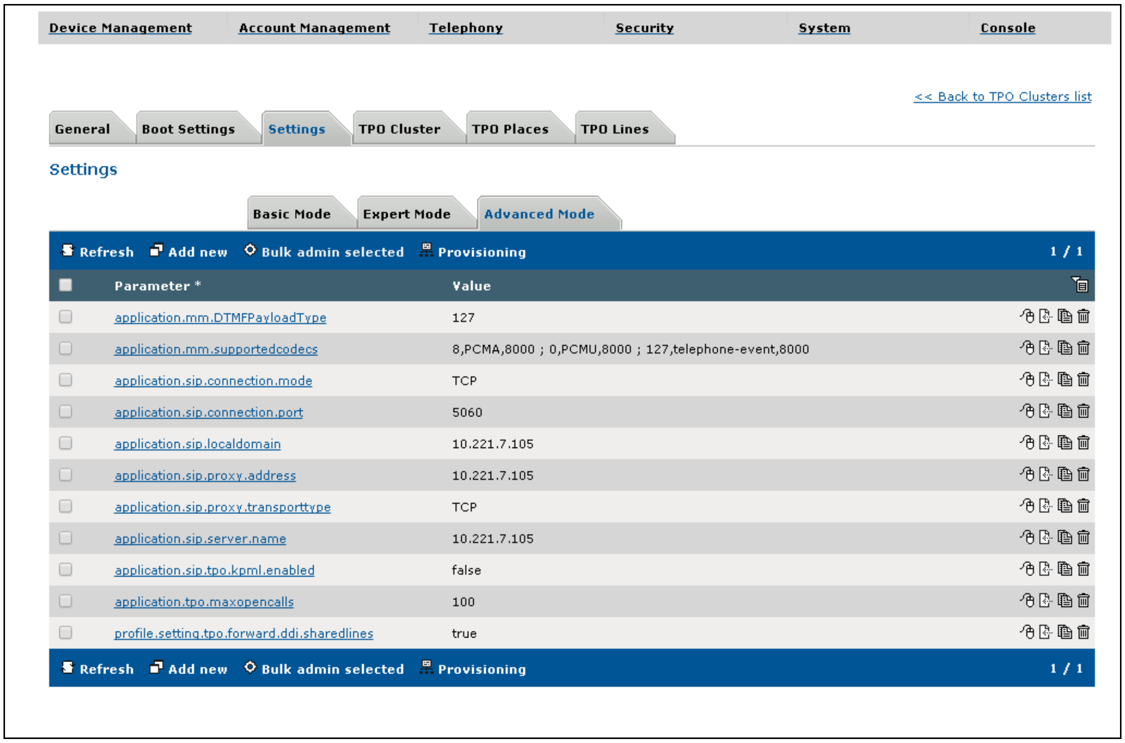
Enter a meaningful name and **select the Zone** just created from the Zone Group drop down box. Select **Update**.



General

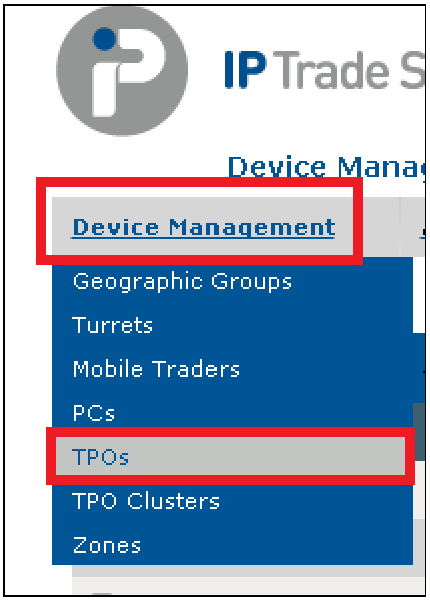
Name *	Avaya-Cluster
Zone Group	Avaya
Comment	Interop Avaya Zone
Last Update DateTime	8/9/2017 5:07:53 PM

Select the **Settings** tab and then **Advanced Mode**, ensure that the configuration matches the screen below but with the Session Manager details.

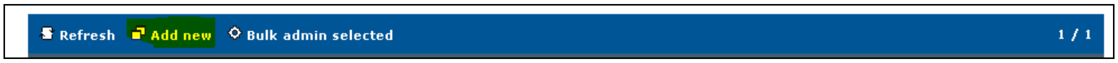


Parameter *	Value
application.mm.DTMFPayloadType	127
application.mm.supportedcodecs	8,PCMA,8000 ; 0,PCMU,8000 ; 127,telephone-event,8000
application.sip.connection.mode	TCP
application.sip.connection.port	5060
application.sip.localdomain	10.221.7.105
application.sip.proxy.address	10.221.7.105
application.sip.proxy.transporttype	TCP
application.sip.server.name	10.221.7.105
application.sip.tpo.kpml.enabled	false
application.tpo.maxopencalls	100
profile.setting.tpo.forward.ddi.sharedlines	true

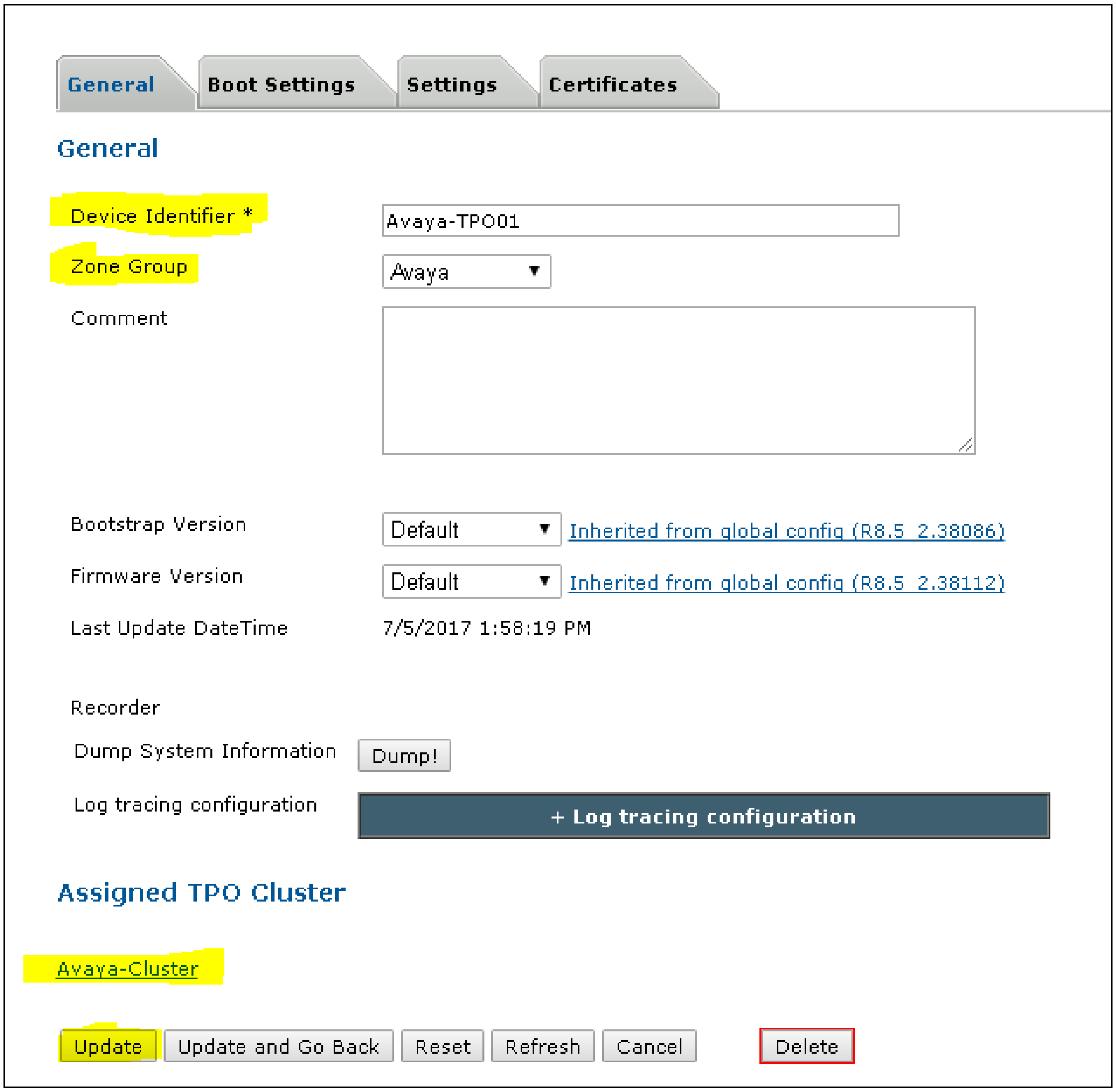
Select Device Management and then TPOs.



Select **Add new** from the menu bar.



Enter **Device Identifier** of the previously provisioned TPO, select the **Zone Group** created and ensure that the TPO Cluster assigned is the TPO Cluster that has been configured in the previous step. Then select **Update.**



Device Identifier * Avaya-TPO01

Zone Group Avaya

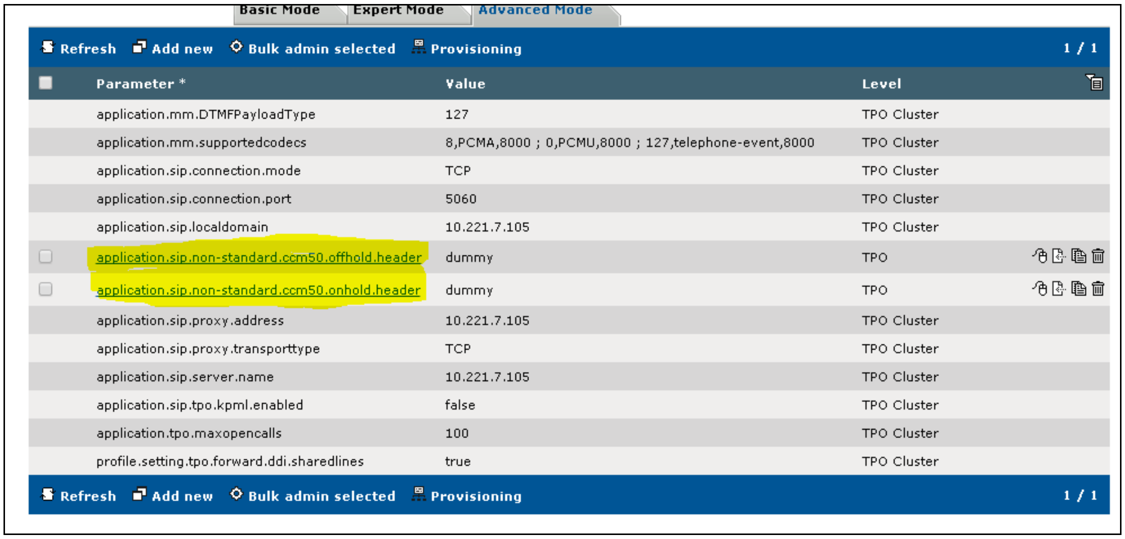
Comment

Bootstrap Version Default Inherited from global config (R8.5_2.38086)

Firmware Version Default Inherited from global config (R8.5_2.38112)

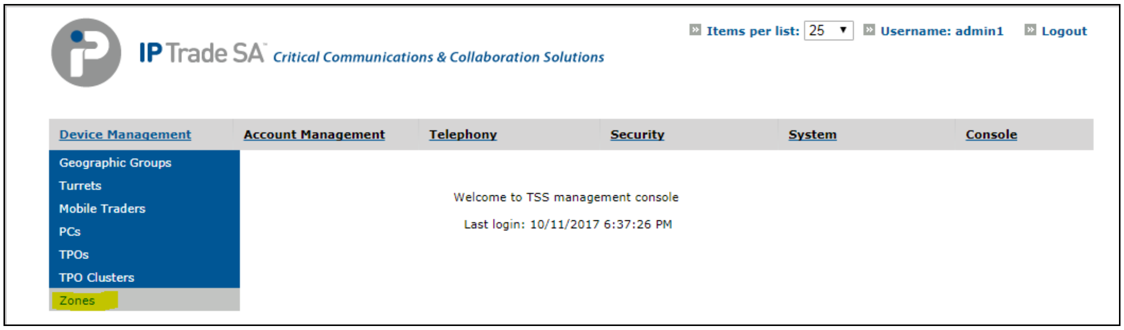
Last Update DateTime 7/5/2017 1:58:19 PM

Select the **Settings** tab and then **Advanced Mode**, ensure that the configuration matches the screen below but with the Session Manager details. Please note the two Avaya specific settings which are highlighted.



Parameter *	Value	Level
application.mm.DTMFPayloadType	127	TPO Cluster
application.mm.supportedcodecs	8,PCMA,8000 ; 0,PCMU,8000 ; 127,telephone-event,8000	TPO Cluster
application.sip.connection.mode	TCP	TPO Cluster
application.sip.connection.port	5060	TPO Cluster
application.sip.localdomain	10.221.7.105	TPO Cluster
application.sip.non-standard.ccm50.offhold.header	dummy	TPO
application.sip.non-standard.ccm50.onhold.header	dummy	TPO
application.sip.proxy.address	10.221.7.105	TPO Cluster
application.sip.proxy.transporttype	TCP	TPO Cluster
application.sip.server.name	10.221.7.105	TPO Cluster
application.sip.tpo.kpml.enabled	false	TPO Cluster
application.tpo.maxopencalls	100	TPO Cluster
profile.setting.tpo.forward.ddi.sharedlines	true	TPO Cluster

Select Device Management and then Zones.

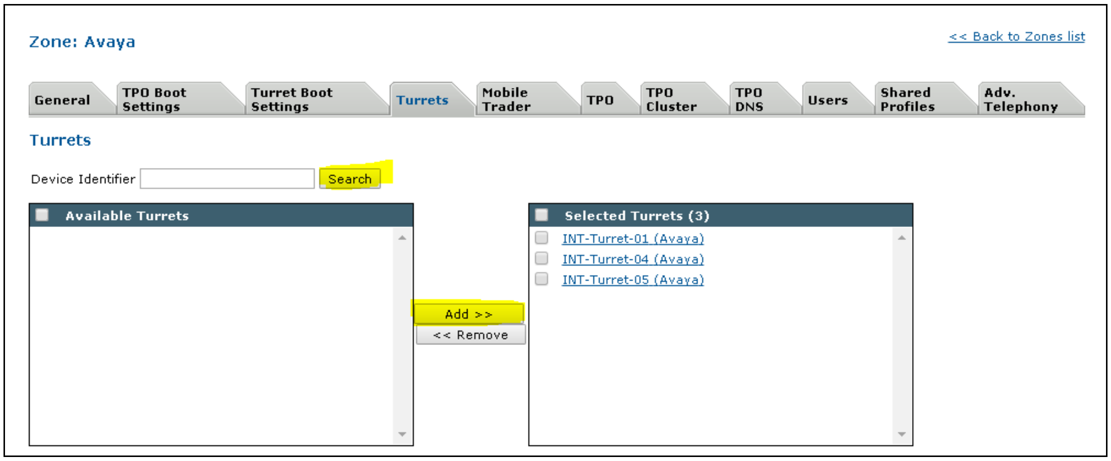


Welcome to TSS management console

Last login: 10/11/2017 6:37:26 PM

Select the **Turrets** tab, click **Search** as shown in the screen below and look for the turrets needing to be added into the newly created Zone.

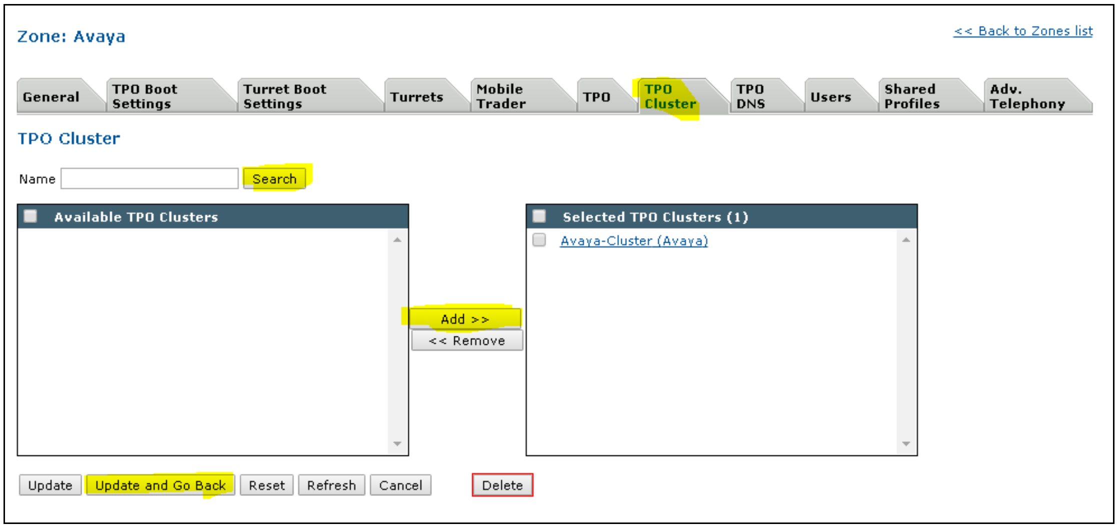
Select the Turrets from the left hand window and select **Add** to move the Turrets into the Zone. Select **Update**.



Selected Turrets (3)

- INT-Turret-01 (Avaya)
- INT-Turret-04 (Avaya)
- INT-Turret-05 (Avaya)

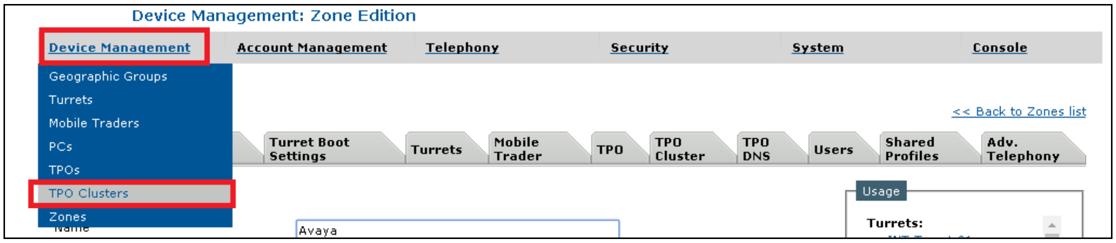
Select the **TPO Clusters** tab and select **Search**, select the TPO Cluster created from the left hand window and select the **Add** button.
Select **Update and Go Back.**



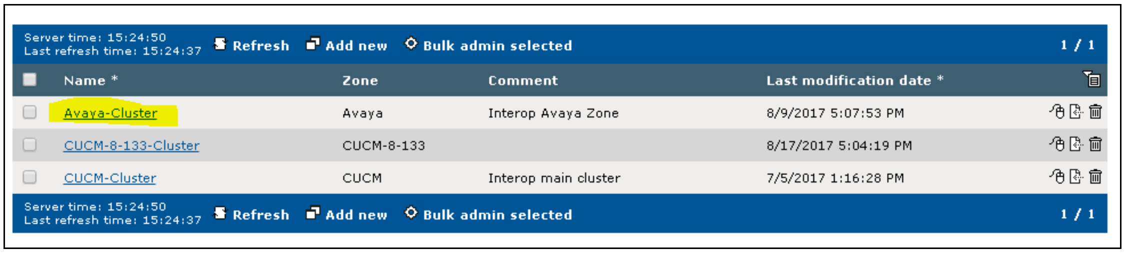
Selected TPO Clusters (1)

- Avaya-Cluster (Avaya)

Select **Device Management** and the **TPO** Clusters.

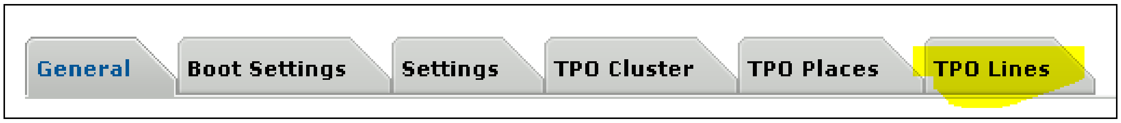


Select the **TPO Cluster** previously configured.

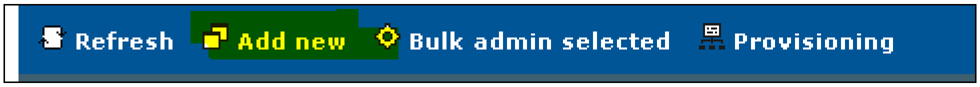


Name *	Zone	Comment	Last modification date *
Avaya-Cluster	Avaya	Interop Avaya Zone	8/9/2017 5:07:53 PM
CUCM-8-133-Cluster	CUCM-8-133		8/17/2017 5:04:19 PM
CUCM-Cluster	CUCM	Interop main cluster	7/5/2017 1:16:28 PM

Select the **TPO Lines** tab.

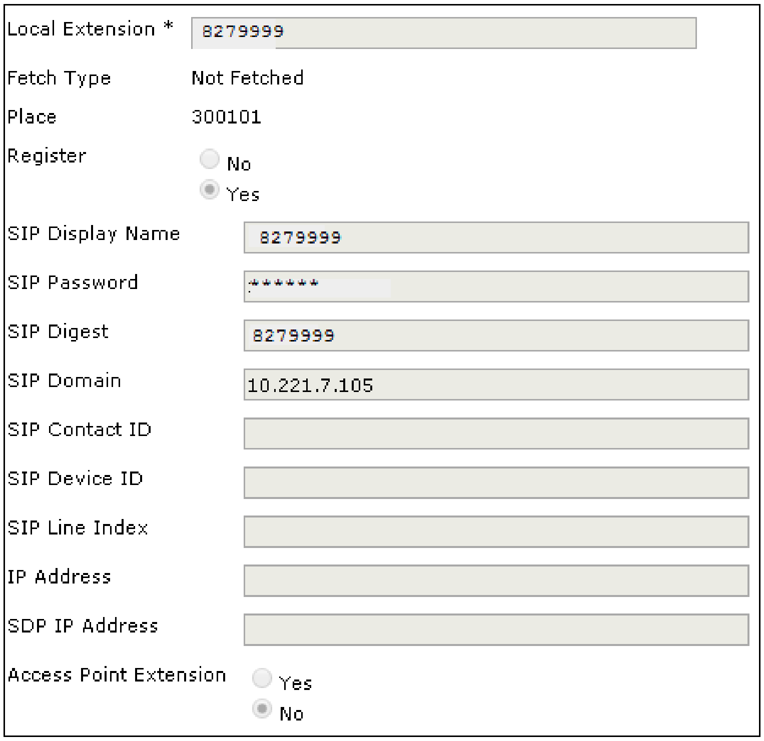


Select Add new.



Enter the data below.

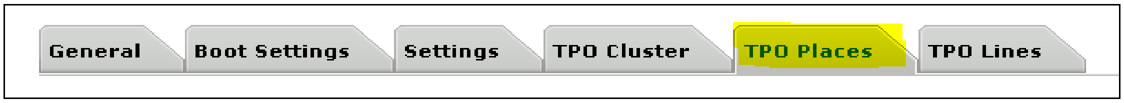
Extension: The Avaya Number defined in **Section 6.1**.
Register: Select the Yes radio button.
SIP Display Name: Define the Avaya Number again.
SIP Password: The Communication Profile Password that you set on the Session Manager.
SIP Digest: Define the Avaya Number again.
SIP Domain: Define the IP Address of the Session Manager.
Access Point Extension: Set the radio button to No.



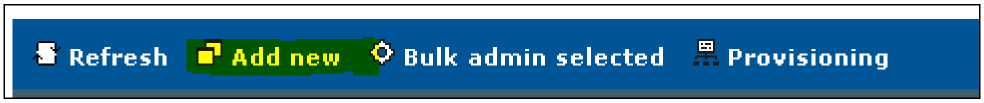
Local Extension *	8279999
Fetch Type	Not Fetched
Place	300101
Register	○ No ● Yes
SIP Display Name	8279999
SIP Password	******
SIP Digest	8279999
SIP Domain	10.221.7.105
SIP Contact ID	
SIP Device ID	
SIP Line Index	
IP Address	
SDP IP Address	
Access Point Extension	○ Yes ● No

Once complete, select **Save and Go Back**(not shown)**.**

Select **TPO Places.**

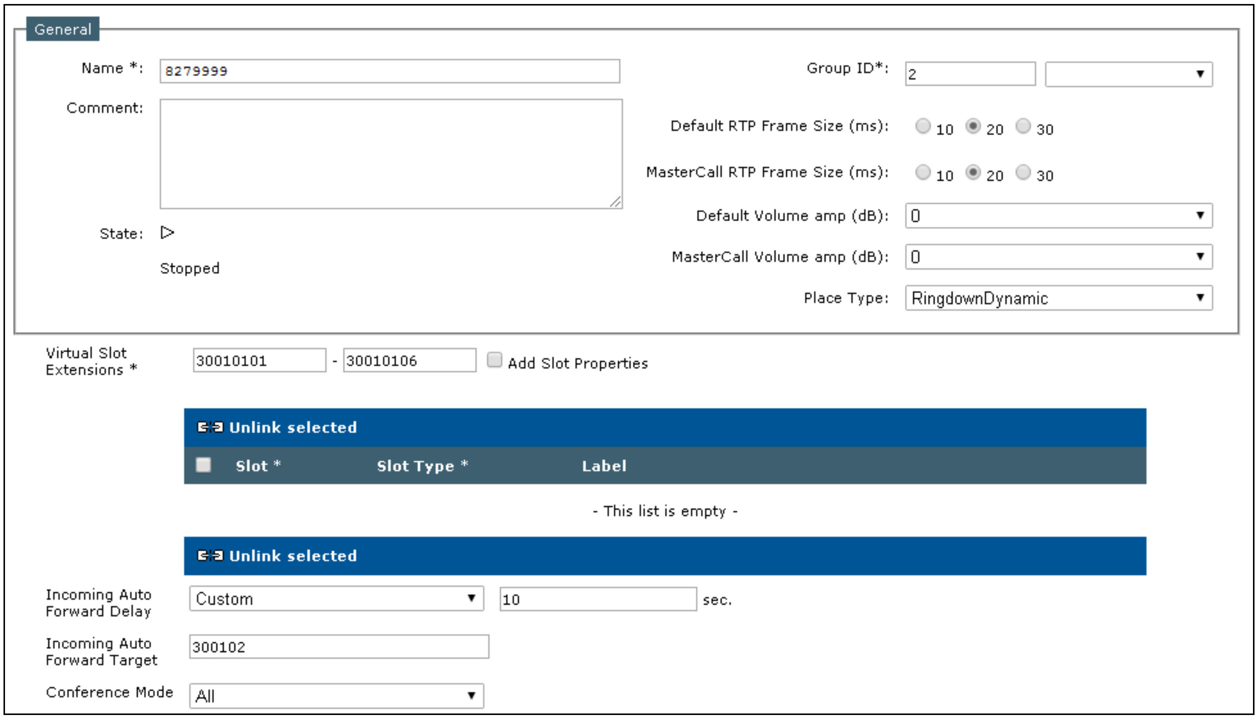


Select **Add new**.



In the first instance, create a **Name**. Select the **Group ID** used. Ensure **RingdownDynamic** is selected as the **Place Type**.

In the **Virtual Slot Extensions**, 30010101 to 30010106 are specified. This is creating six appearances for the 8279999 which are associated with Avaya, 300101**01** is Slot 1, 300101**02** is Slot 2 etc.



General

Name *: 8279999

Comment:

State: ▷ Stopped

Group ID*: 2

Default RTP Frame Size (ms): ○ 10 ● 20 ○ 30

MasterCall RTP Frame Size (ms): ○ 10 ● 20 ○ 30

Default Volume amp (dB): 0

MasterCall Volume amp (dB): 0

Place Type: RingdownDynamic

Virtual Slot Extensions *: 30010101 - 30010106 □ Add Slot Properties

□	Slot *	Slot Type *	Label

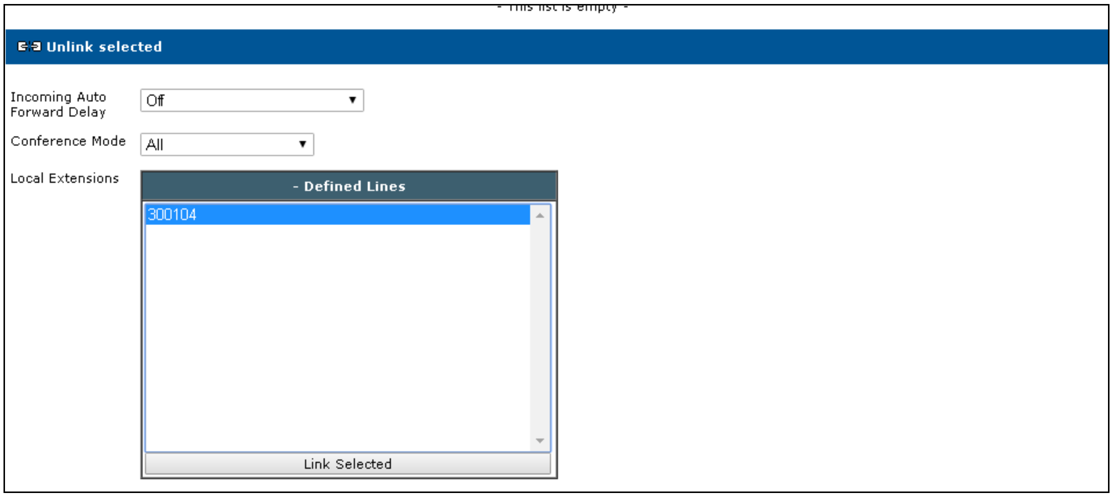
- This list is empty -

Incoming Auto Forward Delay: Custom 10 sec.

Incoming Auto Forward Target: 300102

Conference Mode: All

Link the Line to the TPO Place by selecting the grey **Defined Lines** box.
Select **Link Selected**.



- This list is empty -

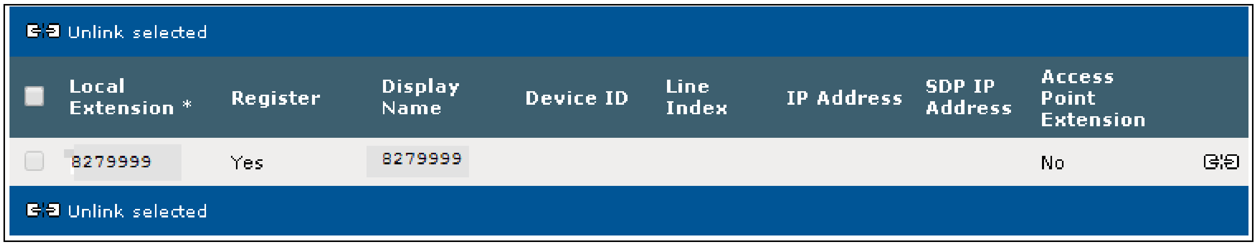
Incoming Auto Forward Delay: Off

Conference Mode: All

Local Extensions

300104

Ensure that the extension has linked correctly by looking at the linked extensions below.

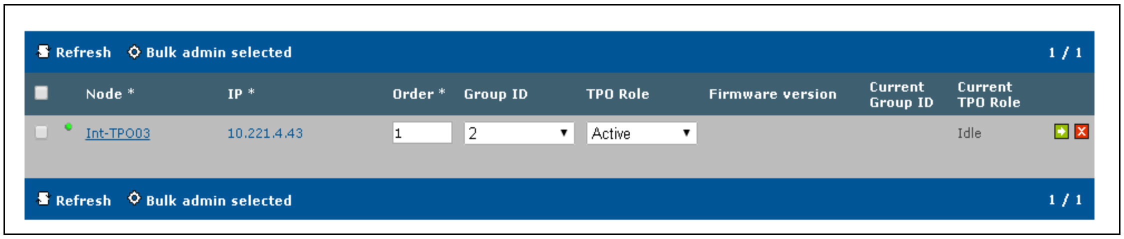


□	Local Extension *	Register	Display Name	Device ID	Line Index	IP Address	SDP IP Address	Access Point Extension
□	8279999	Yes	8279999					No

Select Save and Go Back.

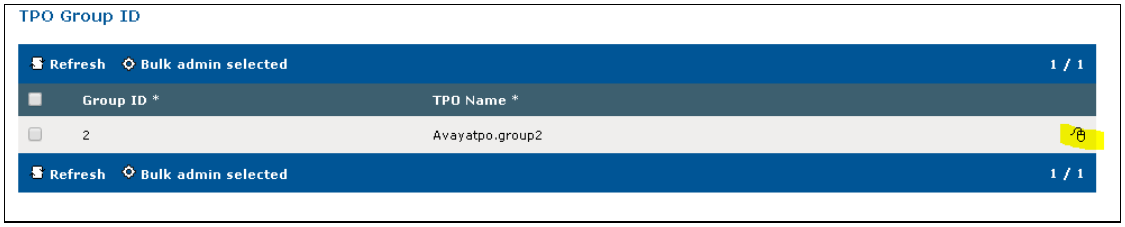
Next, navigate to the **TPO Cluster** Tab. Click the Cluster Mouse button to edit (not shown).

Add the **Order** of preference (if more than two TPO's are in a TPO Cluster). For the **Group ID** that Lines were added to, select **Active** from the **TPO Role** drop down. Select the green arrow to the right to save the changes.



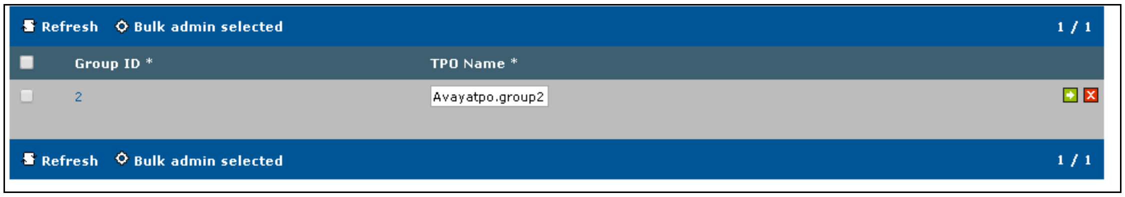
□	Node *	IP *	Order *	Group ID	TPO Role	Firmware version	Current Group ID	Current TPO Role	
□	Int-TPO03	10.221.4.43	1	2 ▼	Active ▼			Idle	🟩 🟥

Next edit the **TPO Group ID** by clicking the Mouse Button.


TPO Group ID

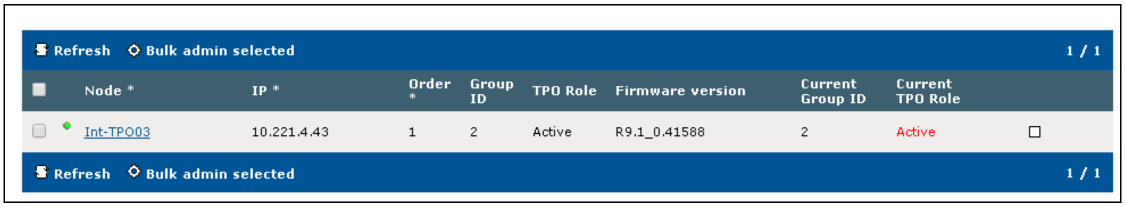
□	Group ID *	TPO Name *
□	2	Avayatpo.group2

Add the **TPO Name** in a format which has a dot in it, in this example Avayatpo.group2 is used. This name is registered on the DNS. Again, select the green arrow to commit the changes.



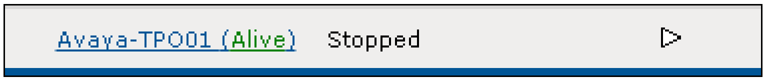
□	Group ID *	TPO Name *	
□	2	Avayatpo.group2	🟩 🟥

After a couple of minutes, the TPO becomes active as shown below.



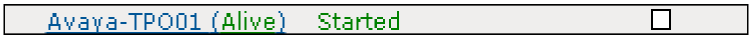
□	Node *	IP *	Order *	Group ID	TPO Role	Firmware version	Current Group ID	Current TPO Role	
□	Int-TPO03	10.221.4.43	1	2	Active	R9.1_0.41588	2	Active	□

Now select the **TPO Places** tab (not shown), the lines show that the TPO is Active but the lines are in a Stopped state.



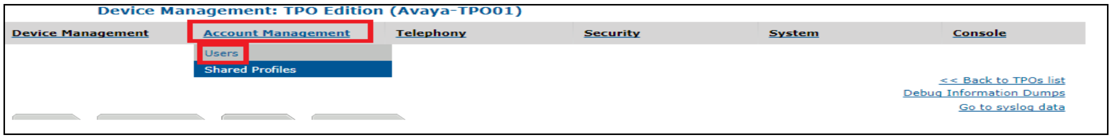
Avaya-TPO01 (Alive) Stopped ▷

Select the Play button and wait for the line to register. Once the line registers, it will display a status as below.

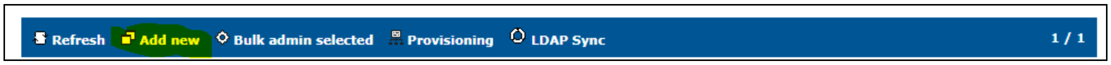


Avaya-TPO01 (Alive) Started □

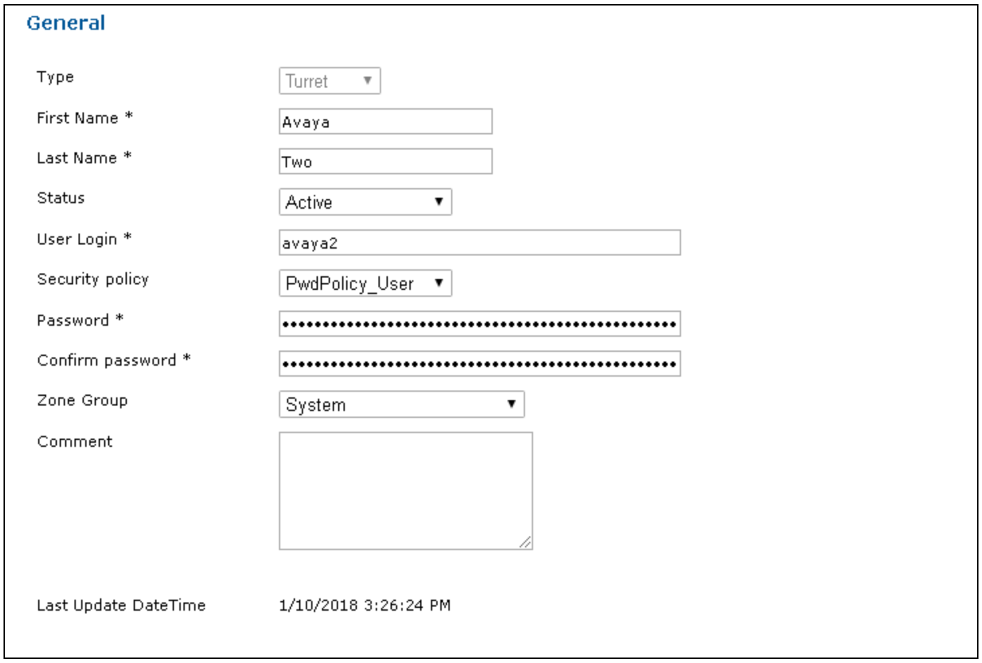
The next task is to add a user, use the top menu and select **User Management**, and then **Users.**



Select **Add new**.



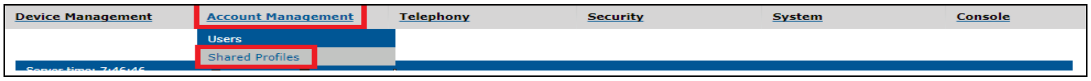
Enter the information regarding the user below. For this example, the username of Avaya2 was created.



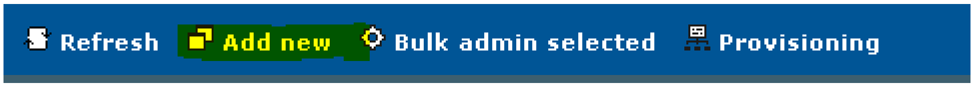
General

Type	Turret
First Name *	Avaya
Last Name *	Two
Status	Active
User Login *	avaya2
Security policy	PwdPolicy_User
Password *	••
Confirm password *	••
Zone Group	System
Comment	
Last Update DateTime	1/10/2018 3:26:24 PM

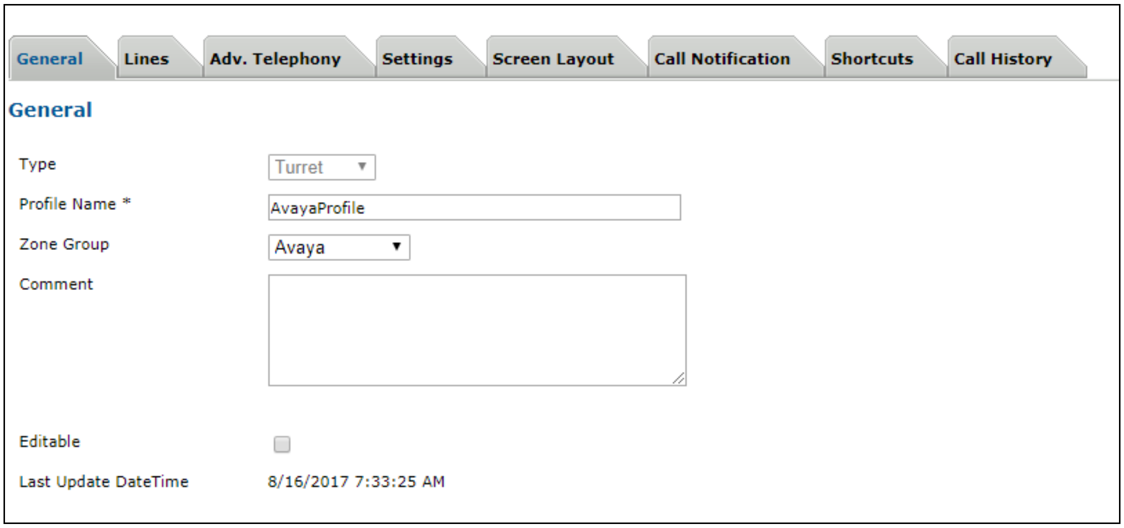
Now create a shared profile, select **Account Management** and then **Shared Profiles.**



Select **Add new**.



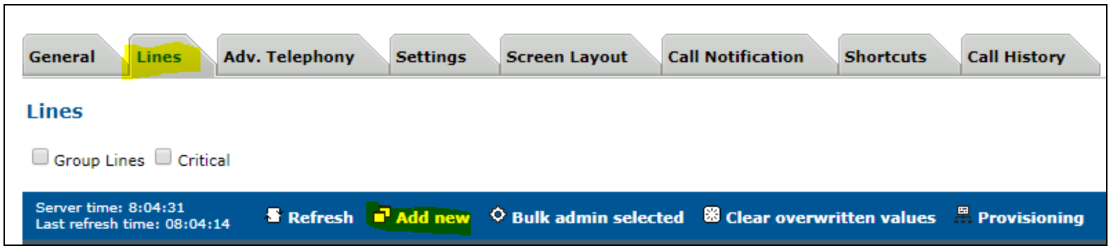
Enter the data as below. Select **Update** (not shown).



General

Type	Turret
Profile Name *	AvayaProfile
Zone Group	Avaya
Comment	
Editable	□
Last Update DateTime	8/16/2017 7:33:25 AM

Select the Lines tab, then select **Add new**.

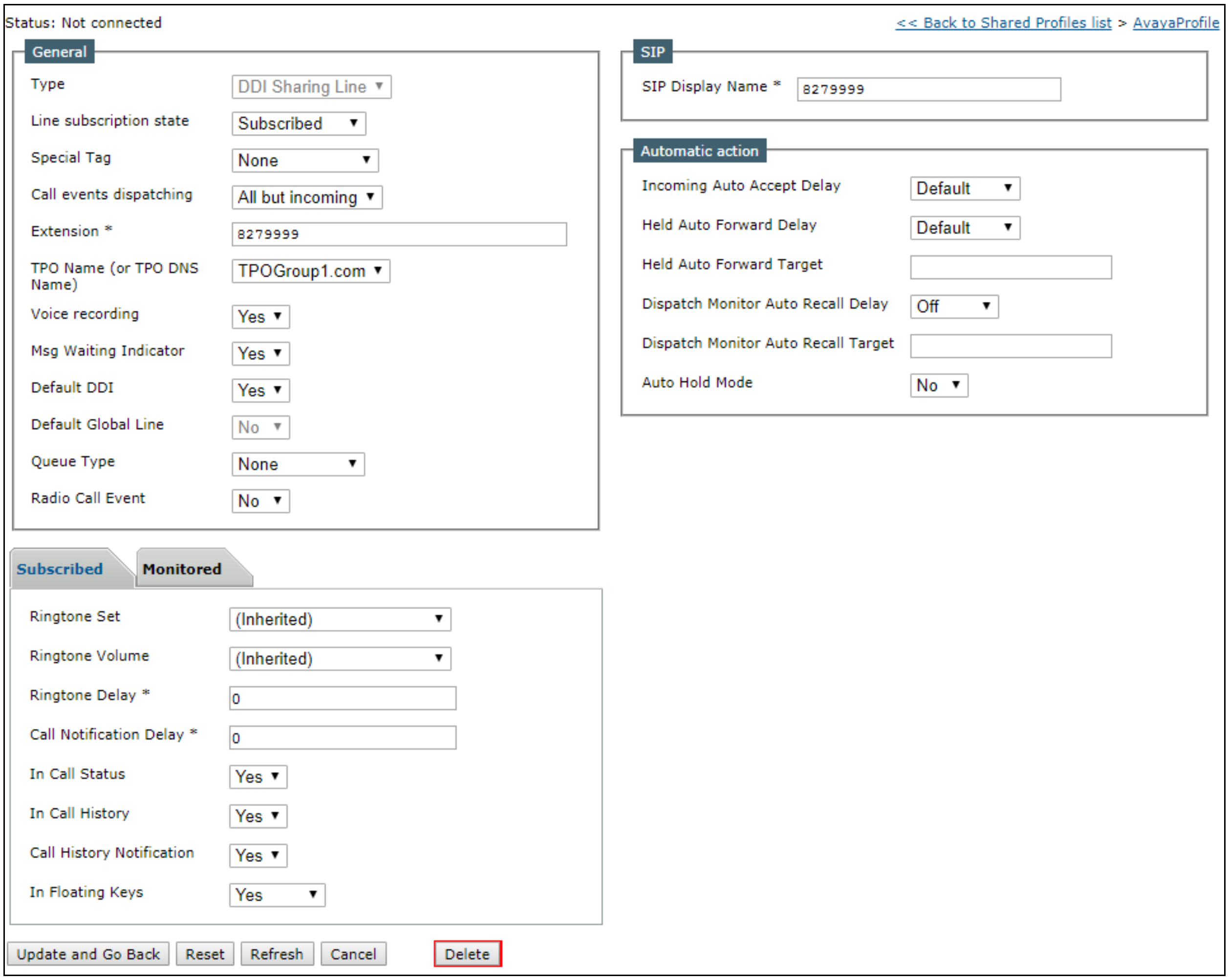


Lines

□ Group Lines □ Critical

Server time: 8:04:31
Last refresh time: 08:04:14

Enter all the Lines associated with the Avaya profile by entering the following information. In this example the shared appearance 8279999 is added.



Status: Not connected

<< Back to Shared Profiles list > AvayaProfile

General

Type	DDI Sharing Line
Line subscription state	Subscribed
Special Tag	None
Call events dispatching	All but incoming
Extension *	8279999
TPO Name (or TPO DNS Name)	TPOGroup1.com
Voice recording	Yes
Msg Waiting Indicator	Yes
Default DDI	Yes
Default Global Line	No
Queue Type	None
Radio Call Event	No

Subscribed | Monitored

Ringtone Set	(Inherited)
Ringtone Volume	(Inherited)
Ringtone Delay *	0
Call Notification Delay *	0
In Call Status	Yes
In Call History	Yes
Call History Notification	Yes
In Floating Keys	Yes

SIP

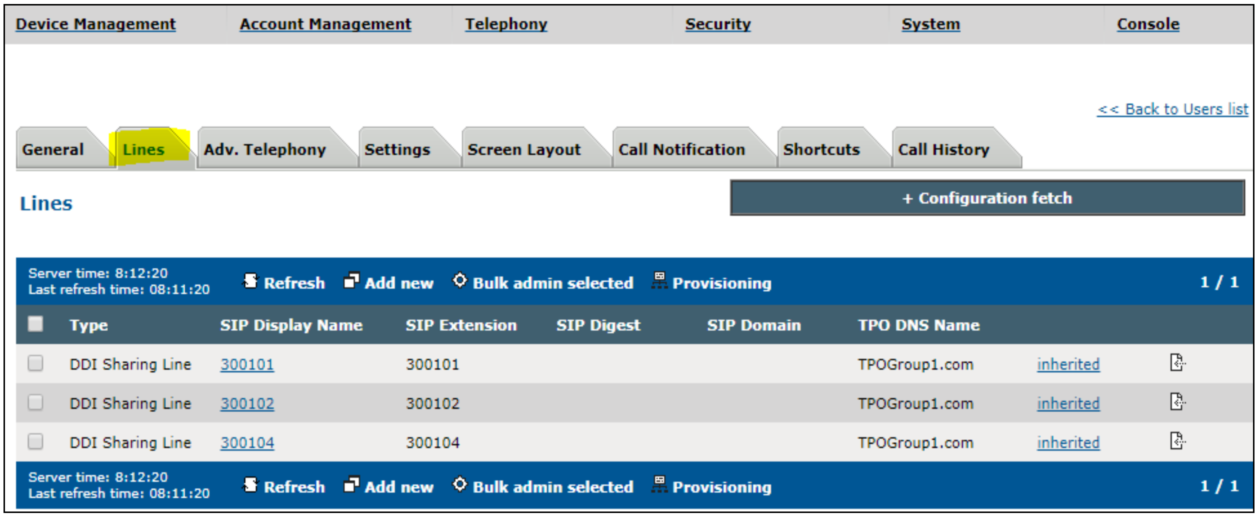
SIP Display Name *	8279999

Automatic action

Incoming Auto Accept Delay	Default
Held Auto Forward Delay	Default
Held Auto Forward Target	
Dispatch Monitor Auto Recall Delay	Off
Dispatch Monitor Auto Recall Target	
Auto Hold Mode	No

Select **Update and Go Back** when completed.

Ensure all of the Lines are present via the shared profile by selecting the **Lines** tab.



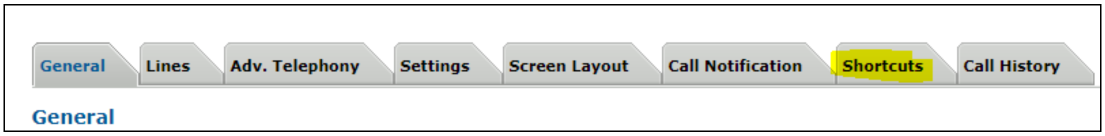
Server time: 8:12:20
Last refresh time: 08:11:20

□	Type	SIP Display Name	SIP Extension	SIP Digest	SIP Domain	TPO DNS Name		
□	DDI Sharing Line	300101	300101			TPOGroup1.com	inherited	
□	DDI Sharing Line	300102	300102			TPOGroup1.com	inherited	
□	DDI Sharing Line	300104	300104			TPOGroup1.com	inherited	

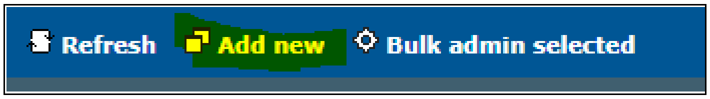
Server time: 8:12:20
Last refresh time: 08:11:20

Now that the lines are added, they need to be inserted onto a Keypage. Navigate **to Account Management** and then **Shared Profiles**(not shown).

Select the Shared Profile and select the **Shortcuts** tab from the Menu bar.

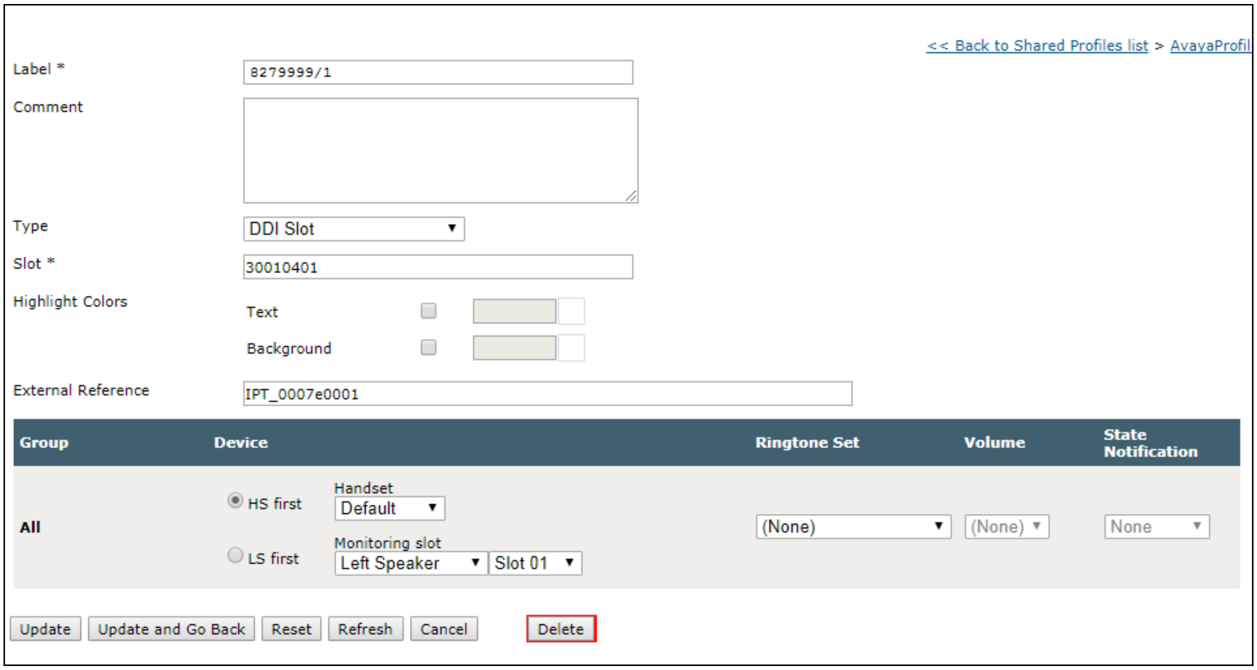


Select **Add new**.



Add each field as the example shows below, in this example the first slot (/1) is configured for Shared Appearance 8279999.

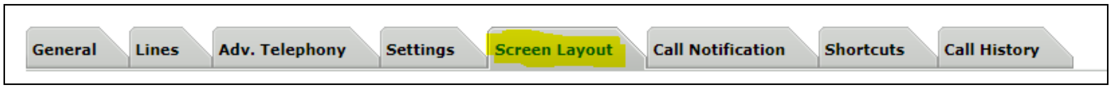
Label: The Shared Appearance followed by the slot number.
Type: Select **DDI Slot**.
Slot: The full Shared Appearance.



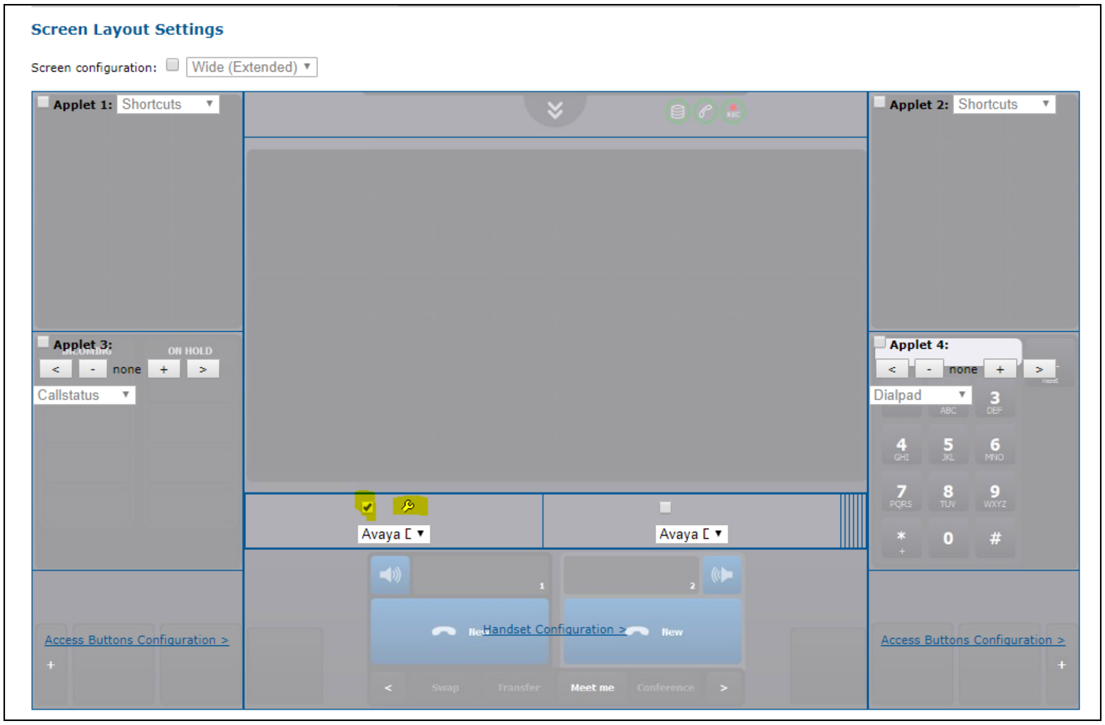
Label *	8279999/1
Comment	
Type	DDI Slot
Slot *	30010401
Highlight Colors	Text □ Background □
External Reference	IPT_0007e0001

Group	Device		Ringtone Set	Volume	State Notification
All	● HS first ○ LS first	Handset: Default Monitoring slot: Left Speaker, Slot 01	(None)	(None)	None

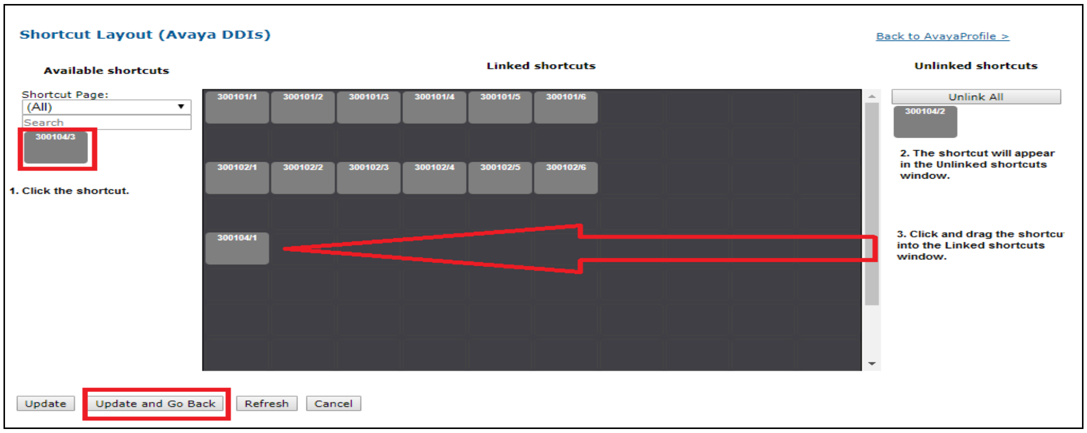
Once complete, select **Update and Go Back**. Next, select the Screen Layout tab from the top menu bar.



Select the Key page to place the shared appearances by checking the tick box and then selecting the spanner symbol next to it as shown in the screen below.



You will see the shortcuts you just created as Available The shortcuts are on the left hand side of the screen. Click on each shortcut which will automatically place the shortcut into the Unlinked shortcuts window. Click and drag the shortcut into the Linked shortcuts window.



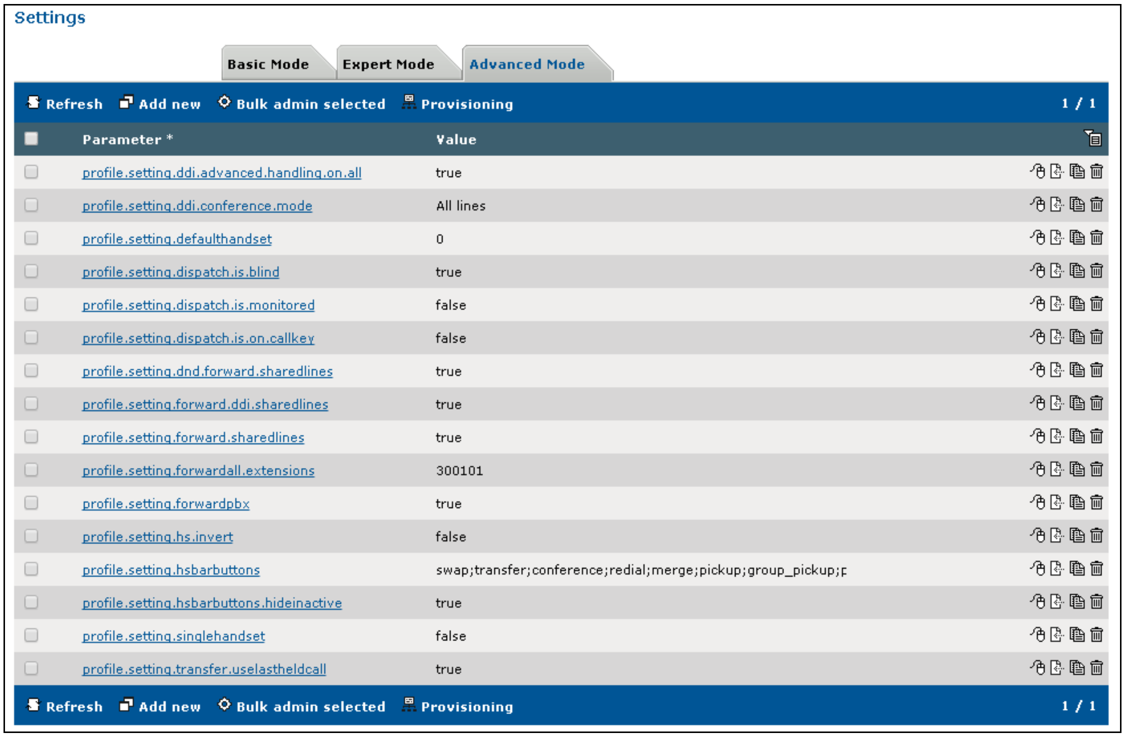
1. Click the shortcut.

2. The shortcut will appear in the Unlinked shortcuts window.

3. Click and drag the shortcu into the Linked shortcuts window.

Select Update and Go Back.

Within the Settings Tab in Shared Profile, ensure that all of the advanced settings are present as per the screen below. Please refer to earlier in this document for adding new parameters.



Settings

Basic Mode | Expert Mode | Advanced Mode

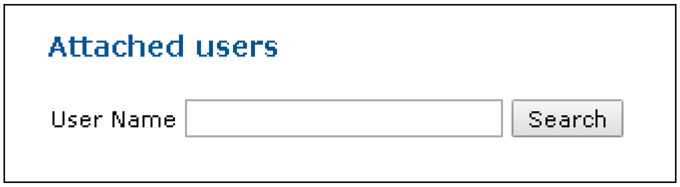
Refresh · Add new · Bulk admin selected · Provisioning · 1 / 1

□	Parameter *	Value
□	profile.setting.ddi.advanced.handling.on.all	true
□	profile.setting.ddi.conference.mode	All lines
□	profile.setting.defaulthandset	0
□	profile.setting.dispatch.is.blind	true
□	profile.setting.dispatch.is.monitored	false
□	profile.setting.dispatch.is.on.callkey	false
□	profile.setting.dnd.forward.sharedlines	true
□	profile.setting.forward.ddi.sharedlines	true
□	profile.setting.forward.sharedlines	true
□	profile.setting.forwardall.extensions	300101
□	profile.setting.forwardpbx	true
□	profile.setting.hs.invert	false
□	profile.setting.hsbarbuttons	swap;transfer;conference;redial;merge;pickup;group_pickup;p
□	profile.setting.hsbarbuttons.hideinactive	true
□	profile.setting.singlehandset	false
□	profile.setting.transfer.uselastheldcall	true

Refresh · Add new · Bulk admin selected · Provisioning · 1 / 1

Now that the Shared Profile has been configured, the users need to be added into it.

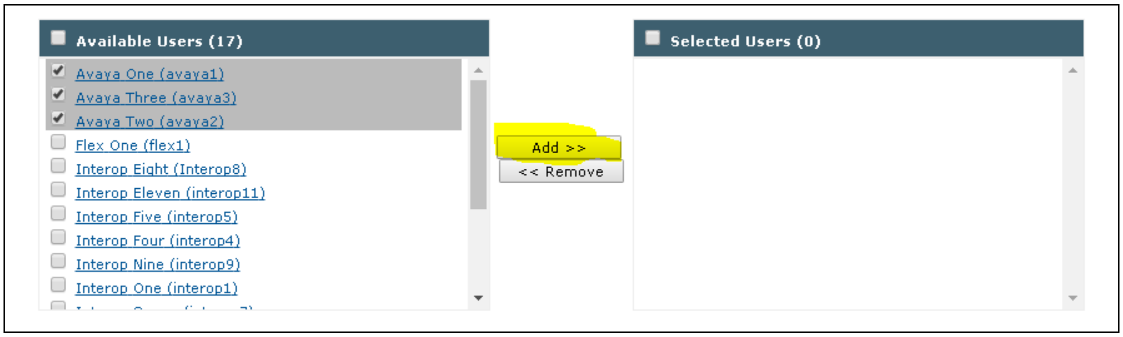
Select the **General** Tab (not shown) and halfway down the page there is a search box as shown in the screen below. Select **Search**.



Attached users

User Name [ ] Search

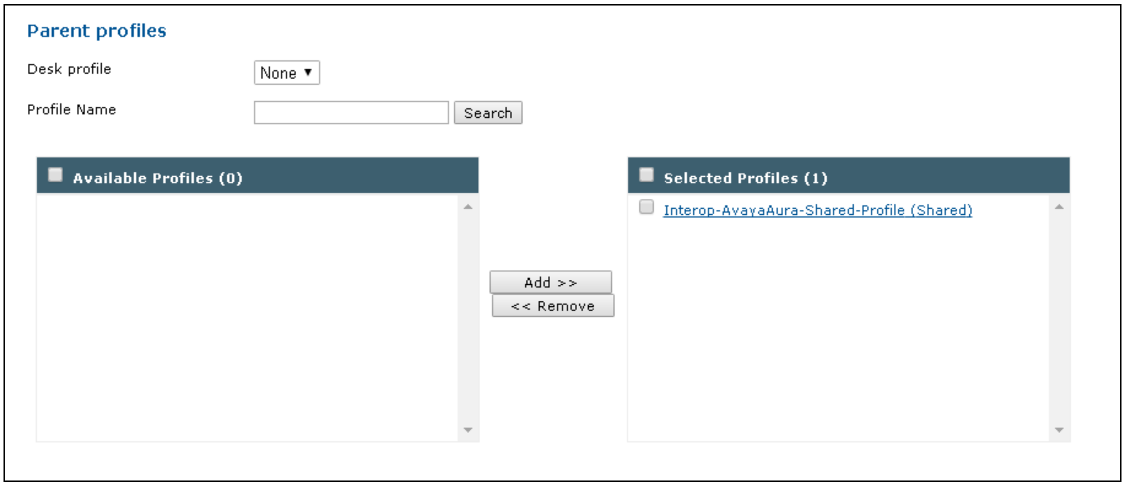
All Users configured on the system will appear, select the ones you want to add into this Shared Profile and select **Add.**


☐ Available Users (17)

- ☑ Avaya One (avaya1)
- ☑ Avaya Three (avaya3)
- ☑ Avaya Two (avaya2)
- ☐ Flex One (flex1)
- ☐ Interop Eight (Interop8)
- ☐ Interop Eleven (interop11)
- ☐ Interop Five (interop5)
- ☐ Interop Four (interop4)
- ☐ Interop Nine (interop9)
- ☐ Interop One (interop1)

☐ Selected Users (0)

The users have been added into the right hand window. Select **Update and Go Back.** To confirm, select the User and check that the user is showing as added into the Shared Profile.


Parent profiles

Desk profile: None

Profile Name:

☐ Available Profiles (0)

☐ Selected Profiles (1)

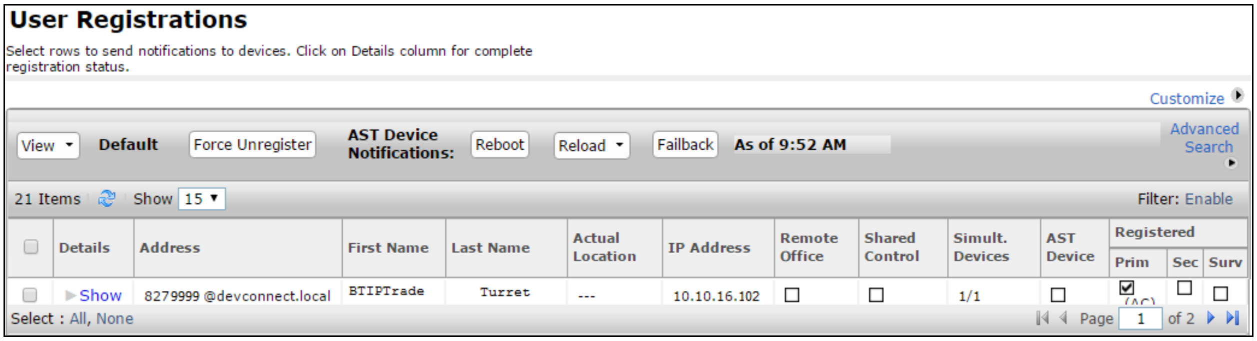
- ☐ Interop-AvayaAura-Shared-Profile (Shared)

8. Verification Steps

This section describes the checks that can be carried out to verify the connection between BT IP Trade Platform with Avaya Aura® Communication Manager and Avaya Aura® Session Manager

8.1. Avaya Aura® Session Manager Verification

From the main System Manager dashboard select Session Manager from the Elements section (not shown). Select **System Status → User Registrations** from the left hand menu (not shown). The BT IP Trade Turret user is listed and will show a tick in the **Prim** box under **Registered**.



User Registrations

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

As of 9:52 AM

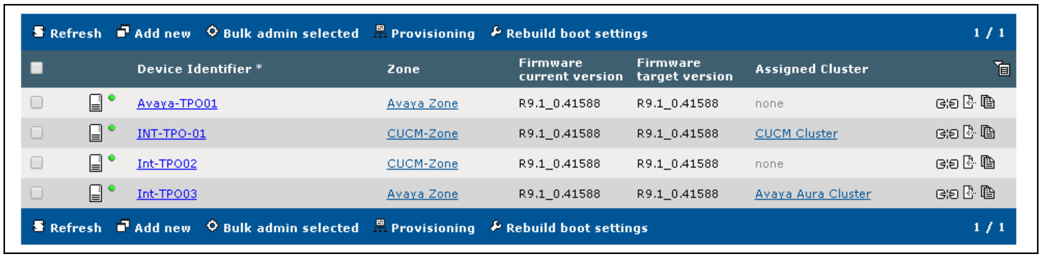
21 Items Show 15 Filter: Enable

□	Details	Address	First Name	Last Name	Actual Location	IP Address	Remote Office	Shared Control	Simult. Devices	AST Device	Registered		
											Prim	Sec	Surv
□	▶ Show	8279999 @devconnect.local	BTIPTrade	Turret	---	10.10.16.102	□	□	1/1	□	☑ (AC)	□	□

Select : All, None Page 1 of 2

8.2. BT IP Trade Platform Verification

In Device Management/TPOs, ensure that the TPO is reachable. This is indicated by a Green Status as shown by below.

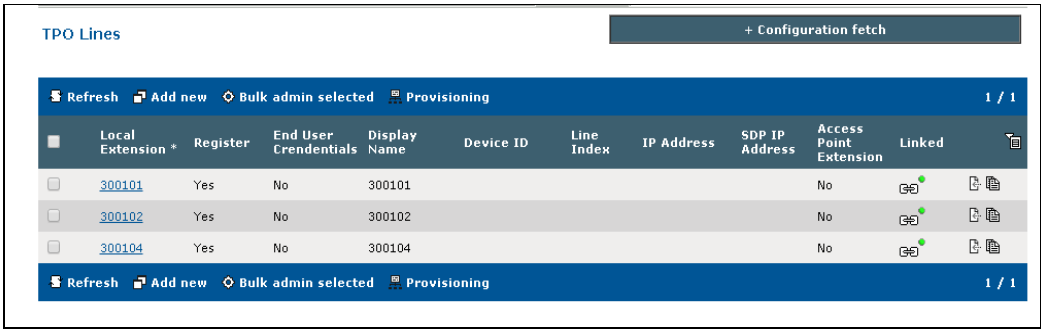


Refresh Add new Bulk admin selected Provisioning Rebuild boot settings 1 / 1

□		Device Identifier *	Zone	Firmware current version	Firmware target version	Assigned Cluster
□	●	Avaya-TPO01	Avaya Zone	R9.1_0.41588	R9.1_0.41588	none
□	●	INT-TPO-01	CUCM-Zone	R9.1_0.41588	R9.1_0.41588	CUCM Cluster
□	●	Int-TPO02	CUCM-Zone	R9.1_0.41588	R9.1_0.41588	none
□	●	Int-TPO03	Avaya Zone	R9.1_0.41588	R9.1_0.41588	Avaya Aura Cluster

Refresh Add new Bulk admin selected Provisioning Rebuild boot settings 1 / 1

In Device Management/TPO Clusters/Your TPO Cluster, navigate to the **TPO Lines** Tab. The Lines must be linked to a TPO Place. This is indicated by the **Linked** column. Green status indicates that the TPO is up and the TPO Place is started.



TPO Lines

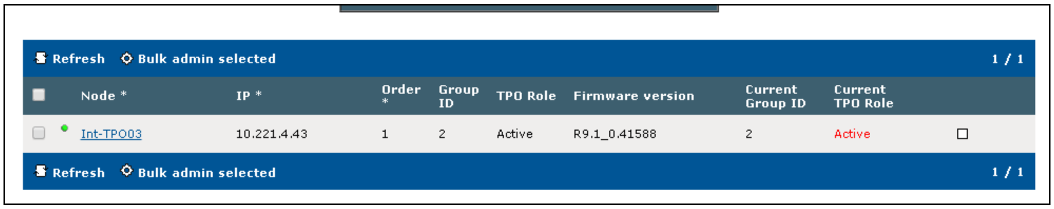
+ Configuration fetch

Refresh Add new Bulk admin selected Provisioning 1 / 1

□	Local Extension *	Register	End User Crendentials	Display Name	Device ID	Line Index	IP Address	SDP IP Address	Access Point Extension	Linked
□	300101	Yes	No	300101					No	●
□	300102	Yes	No	300102					No	●
□	300104	Yes	No	300104					No	●

Refresh Add new Bulk admin selected Provisioning 1 / 1

In the same area, on the TPO Cluster Tab, the TPO must show a green status and as Active.

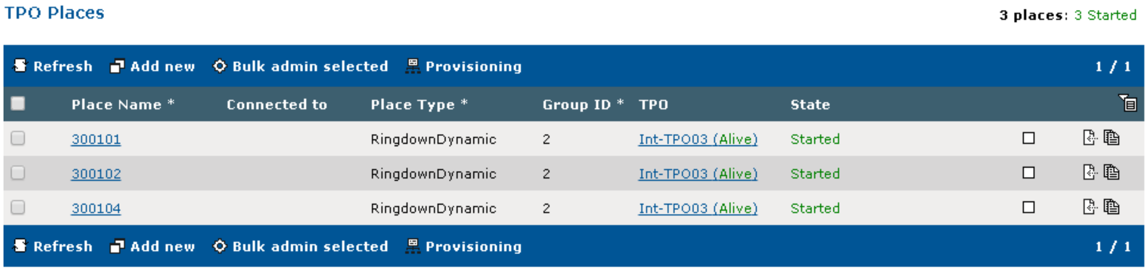


Refresh Bulk admin selected 1 / 1

□	Node *	IP *	Order *	Group ID	TPO Role	Firmware version	Current Group ID	Current TPO Role	
□	● Int-TPO03	10.221.4.43	1	2	Active	R9.1_0.41588	2	Active	□

Refresh Bulk admin selected 1 / 1

Lastly select the TPO Places Tab (not shown). All lines show a status of **Started**, this indicates that the TPO has registered the line to the Session Manager.



TPO Places

3 places: 3 Started

□	Place Name *	Connected to	Place Type *	Group ID *	TPO	State		
□	300101		RingdownDynamic	2	Int-TPO03 (Alive)	Started	□	
□	300102		RingdownDynamic	2	Int-TPO03 (Alive)	Started	□	
□	300104		RingdownDynamic	2	Int-TPO03 (Alive)	Started	□	

9. Conclusion

These Application Notes describe the configuration steps required for BT (Unified Trading) IP Trade Platform to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager. All feature functionality and serviceability test cases were completed successfully as outlined in **Section 2.2**.

10. Additional References

This section references the Avaya and BT product documentation that are relevant to these Application Notes.
Product documentation for Avaya products may be found at http://support.avaya.com.

[1] *Administering Avaya Aura® Communication Manager*, Document ID 03-300509
[2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Document ID 555-245-205
[3] *Administering Avaya Aura® Session Manager*, Release 7.0, 03-603324
[4] *Quick Start Guide to Using the Avaya Aura® Media Server with Avaya Aura® Communication Manager*, August 2015

Information regarding Product documentation for BT Netrix Trade Turret can be obtained by contacting the Support email in **Section 2.3**

The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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