Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Capita Secure Information Solutions DS3000 with Avaya Aura® Session Manager R6.3 and Avaya Aura® Communication Manager R6.3 using SIP Trunks - Issue 1.0

Abstract

These Application Notes describe the configuration steps for provisioning Capita Secure Information Solutions DS3000 to interoperate with Avaya Aura® Session Manager R6.3 and Avaya Aura® Communication Manager R6.3.

Readers should pay particular attention to the scope of testing as outlined in Section 2.1, as well as 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 for provisioning DS3000 from Capita Secure Information Solutions to interoperate with Avaya Aura® Session Manager R6.3 connecting to Avaya Aura® Communication Manager R6.3. The DS3000 is an Integrated Communication Control System that is used by emergency service customers for answering 999/112 calls and then from the same application using radio communication (TETRA digital radio or analogue PMR) to pass details to mobile resources.

As a radio dispatch deployment with basic PTN/PSTN the DS3000 acts as an end Private Branch Exchange (PBX) and performs call prioritisation and distribution to DS3000 operators as defined by the profile in which they have logged in to the DS3000 application. In this type of configuration the DS3000 has one primary connection to the Avaya Solution, a SIP connection to Avaya Aura ® Session Manager. The DS3000 supports basic call control including hold and transfer.

Please note that this setup allows for non-Automatic Call Distributed (ACD) calls only. The configuration setup in an ACD or Contact Center environment is outlined in the Application Notes titled *Application Notes for Configuring Capita Secure Information Solutions DS3000 with Avaya Aura® Contact Center R6.4 and Avaya Communication Server 1000E R7.6 using a Lineside E1 Connection*.

2. General Test Approach and Test Results

The interoperability compliance testing evaluates the ability of the DS3000 application to make and receive calls to and from Communication Manager endpoints. All calls destined for the DS3000 both locally and from the PSTN are routed to the DS3000 over SIP trunks using Session Manager to route the calls.

Note: Both a TCP and a UDP Entity link were required in order to make calls between Communication Manager/Session Manager and Capita.

Communication Manager → Capita uses TCP.
Capita → Communication Manager uses UDP.

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

2.1. Interoperability Compliance Testing

The interoperability compliance testing focuses on various technical testing scenarios to verify the usage of DS3000 with the Avaya solution. In addition, serviceability tests were also performed to assess the reliability and accuracy of the joint solution. The testing focused on the following types of calls:

- **Calls to Communication Manager endpoints** – Ensure that calls can be made to Communication Manager extensions from DS3000.
- **Calls to DS3000 Operators**– Ensure that calls can be made to DS3000 operators from Communication Manager extensions.
- **Calls to PSTN from DS3000 Operators –** Ensure that calls can be made from DS3000 to PSTN across the SIP trunk through Communication Manager.
- **Calls from PSTN into DS3000 Operators** – Ensure that calls can be made to DS3000 from the PSTN by calling into Communication Manager and across the SIP trunk to the DS3000.
- **Hold/transfer and conference functionality**– Verify that calls can be placed on hold and transferred and conferenced.
- **Caller information is preserved on all calls to/from DS3000** – Ensure that the correct CLID information is preserved.
- **Failover testing** – Verify the behaviour of DS3000 application under different simulated LAN failure conditions on the Avaya platform.

Note: All test cases were performed using the following set types:

- Ext 1001 (9630 SIP).
- Ext 2002 (9620 H323).
- Ext 2100 (one-X® Agent (H323)).
- Ext 2500 (Analog set).

Note: All test cases were performed with the following set on the signalling group.

- Direct IP-IP Audio Connections set to N (Shuffling is Off).
- Direct IP-IP Audio Connections set to Y (Shuffling is on) and Initial Direct IP-IP Media set to N.
- Direct IP-IP Audio Connections set to Y (Shuffling is on) and Initial Direct IP-IP Media set to Y.

2.2. Test Results

Most test cases passed except for the following issues observed.

- DTMF does not work with Avaya Aura® Messaging; DS3000 uses in-band DTMF that is not compatible with Aura messaging.

Issues Observed with Direct IP-IP Audio Connections set to Y (Shuffling is on) and Initial Direct IP-IP Media set to N:

1. If Communication Manager phone calls to Operator A and wishes to be transferred to Operator B; Using the “Transfer PABX” function on the DS3000 Operators console , transfer of the call cannot be completed. Using standard “Trans Call” functionality on the DS3000 Operator, the console works perfectly.
2. Call from DS3000 to a Communication Manager SIP phone; the DS3000 initiates a blind transfer to another Communication Manager SIP phone, and this results in the transfer not being completed properly as hold tone is being played to both parties.
3. Call from DS3000 to a Communication Manager SIP phone: the DS3000 initiates a blind transfer to a Communication Manager H323 phone and this results in the transfer not being completed properly as hold tone is being played to both parties.
4. Call from DS3000 to a Communication Manager H323 phone; the DS3000 initiates a blind transfer to another Communication Manager H323 phone and this results in the transfer not being completed properly as hold tone is being played to both parties.
5. Call from a Communication Manager SIP phone to DS3000; the DS30000 initiates a blind transfer to a Communication Manager H.323 phone and this results in the transfer not being completed properly as hold tone is being played to both parties.
6. Call from a Communication Manager H323 phone to DS3000; the DS30000 initiates a blind transfer to another Communication Manager H.323 phone and this results in the transfer not being completed properly as hold tone is being played to both parties.

Issues Observed with Direct IP-IP Audio Connections set to Y (Shuffling is on) and Initial Direct IP-IP Media set to Y:

1. If CM phone calls to Operator A and wishes to be transferred to Operator B; Using the “Transfer PABX” function on the DS3000 Operators console, transfer of the call cannot be completed. Using standard “Trans Call” functionality on the DS3000 Operator console, transfer works perfectly.
2. Call from a Communication Manager SIP phone to DS3000 Operator, the DS3000 initiates a blind transfer to another Communication Manager SIP phone and this results in the transfer not being completed properly as hold tone is being played to both parties. (Intermittent issue).

Note: There are no issues observed with shuffling off (Direct IP-IP Audio Connections set to N).

2.3. Support

Support from Avaya is available by visiting the website http://support.avaya.com and a list of product documentation can be found in **Section 10** of these Application Notes. Technical support for the Capita DS3000 product can be obtained as follows.

- Tel : + 44 (0) 8456 041999
- Email: csis.info@capita.co.uk

3. Reference Configuration

Figure 1 shows the setup for compliance testing Capita's DS3000 with Communication Manager and Session Manager using SIP signalling over SIP trunks to pass callers from Communication Manager to the DS3000 Operators.

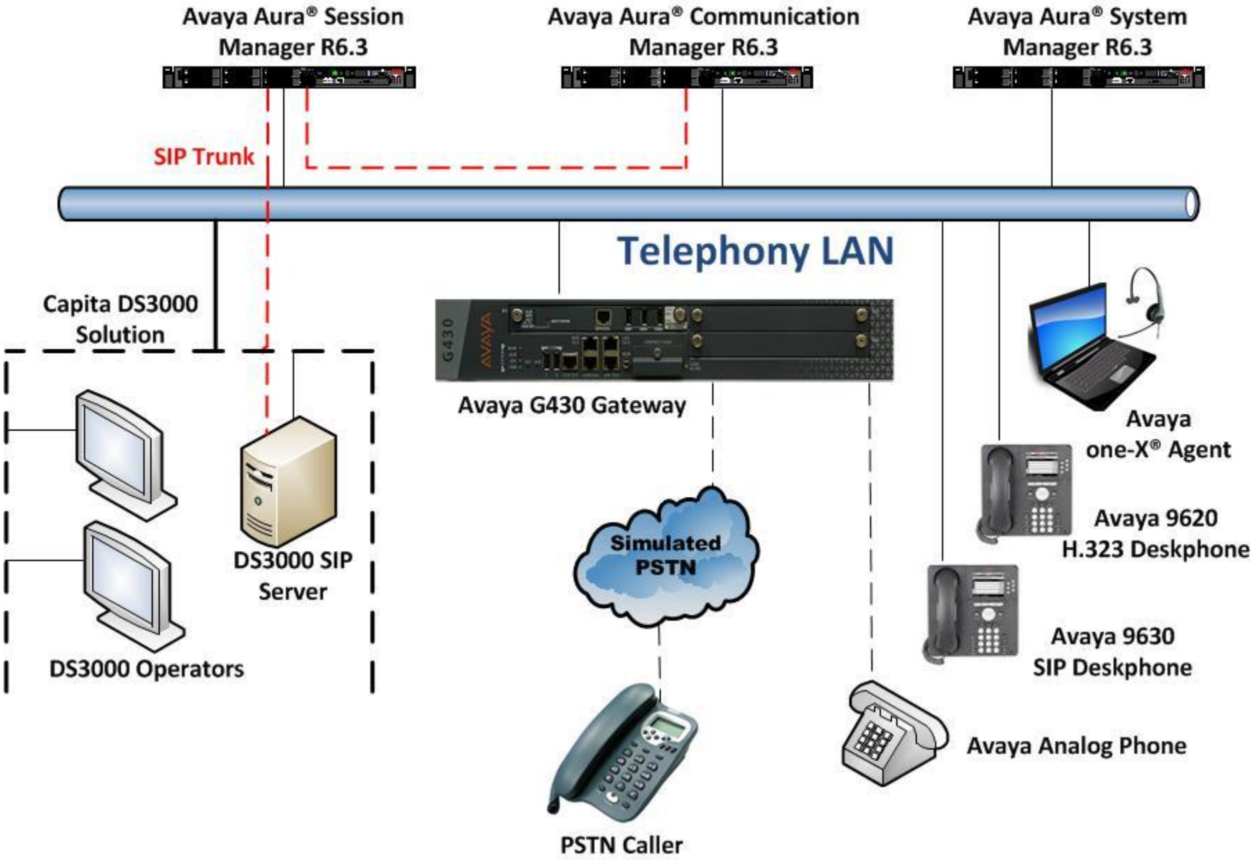


Figure 1: Connection of Capita DS3000 with Avaya Aura® Communication Manager R6.3 and Avaya Aura® Session Manager R6.3

4. Equipment and Software Validated

The following equipment and software was used for the compliance test.

Equipment/Software	Release/Version
Avaya Aura® System Manager running on a Virtual Platform VMWare ESXi 5.1	R6.3.9 [Build 6.3.0.8.5682-6.3.8.4414] [SW Update Rev 6.3.9.1.2482]
Avaya Aura® Session Manager running on a Virtual Platform VMWare ESXi 5.1	R6.3 [Build 6.3.9.0.639011]
Avaya Aura® Communication Manager running on a Virtual Platform VMWare ESXi 5.1	R6.3 SP6 R016x.03.0.124.0
Avaya G430 Gateway	33.12.0 /1
Avaya IP Deskphone H.323 on Avaya 9620 IP Deskphone Avaya IP Deskphone H.323 on Avaya 9608 IP Deskphone	Release s3.186a Release 6.2009
Avaya one-X® Deskphone SIP on Avaya 9641 IP Deskphone Avaya one-X® Deskphone SIP on Avaya 9630 IP Deskphone	Release 6.2.1.26 Release 2.6.8.4
Avaya one-X® Agent running on Windows 7 PC	R2.5
Avaya Analog Phone	N/A
Capita DS3000 Solution Kit (DSX Converged Versions 2013 R1 and later) - Aculab Dual Redundant SIP Server	Release 2x Series V6.5.13

5. Configure Avaya Aura® Communication Manager

It is assumed that a fully functioning Communication Manager is in place with the necessary licensing and with SIP trunks in place, to Session Manager. The configuration and verification operations illustrated in this section were all performed using Communication Manager System Administration Terminal (SAT). The information provided in this section describes the configuration of Communication Manager for this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**.

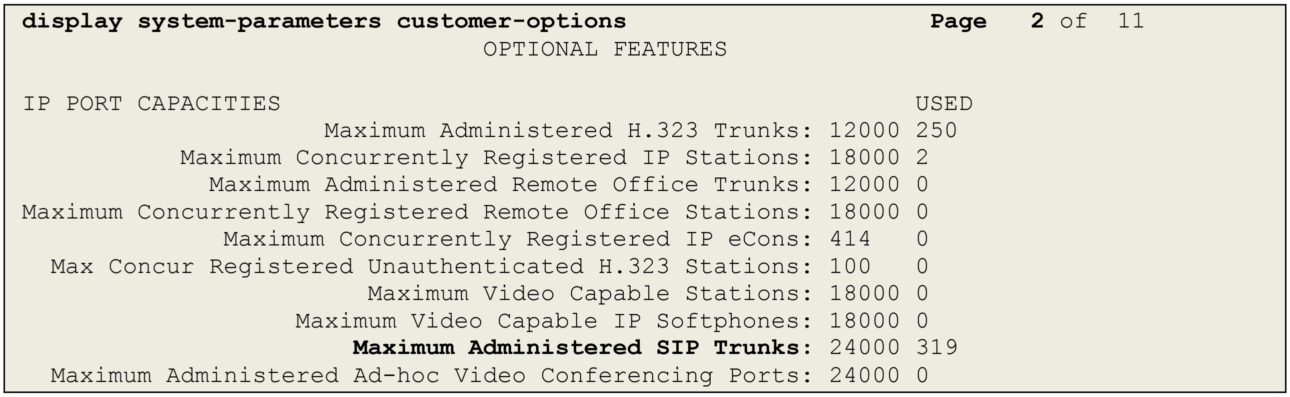
The configuration operations described in this section can be summarized as follows:

- Verify System Parameters Customer Options.
- System Features and Access Codes.
- Administer Dial Plan.
- Administer Route Selection for DS3000 calls.
- Configure SIP Trunk.

Note: The configuration of PSTN trunks and routes are outside the scope of these Application Notes.

5.1. Verify System Parameters Customer Options

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 2**, verify that **Maximum Administered SIP Trunks** has sufficient capacity. Each call that receives IVR treatment from Communications Portal uses a minimum of one SIP trunk. Calls that are routed back to stations commissioned on Communication Manager, or calls that are routed back to Communication Manager to access the PSTN, use 2 SIP trunks.



```
display system-parameters customer-options                    Page   2 of  11
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                           USED
                     Maximum Administered H.323 Trunks: 12000 250
           Maximum Concurrently Registered IP Stations: 18000 2
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 414   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 18000 0
                   Maximum Video Capable IP Softphones: 18000 0
                       Maximum Administered SIP Trunks: 24000 319
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
```

On **Page 3**, ensure that both **ARS** and **ARS/AAR Partitioning** are set to **y**.

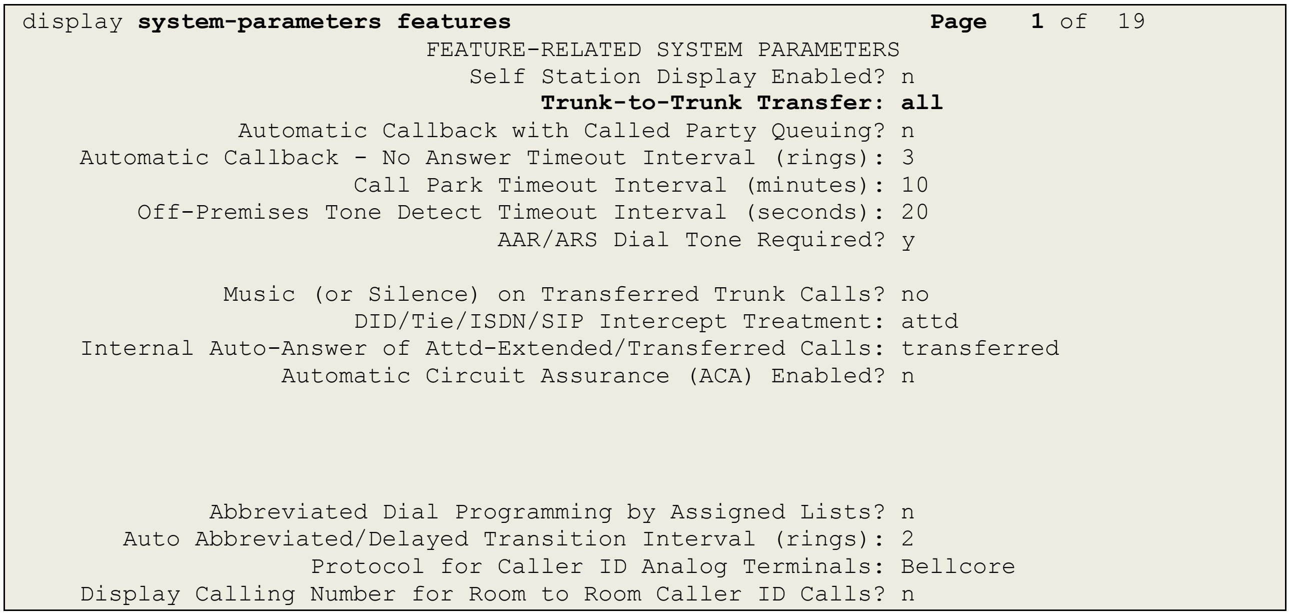
```
display system-parameters customer-options                    Page   3 of  11
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? y           Audible Message Waiting? y
        Access Security Gateway (ASG)? n               Authorization Codes? y
        Analog Trunk Incoming Call ID? y                        CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? y                          CAS Main? n
Answer Supervision by Call Classifier? y                 Change COR by FAC? n
                                  ARS? y  Computer Telephony Adjunct Links? y
                 ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? y                      DCS (Basic)? y
```

On **Page 5**, ensure that **Uniform Dialing Plan** is set to **y**.

```
display system-parameters customer-options                    Page   5 of  11
                                OPTIONAL FEATURES

                Multinational Locations? n             Station and Trunk MSP? y
 Multiple Level Precedence & Preemption? n      Station as Virtual Extension? y
                    Multiple Locations? n
                                            System Management Data Transfer? n
          Personal Station Access (PSA)? y              Tenant Partitioning? y
                        PNC Duplication? n      Terminal Trans. Init. (TTI)? y
                   Port Network Support? y              Time of Day Routing? y
                        Posted Messages? y      TN2501 VAL Maximum Capacity? y
                                                       Uniform Dialing Plan? y
                     Private Networking? y    Usage Allocation Enhancements? y
```

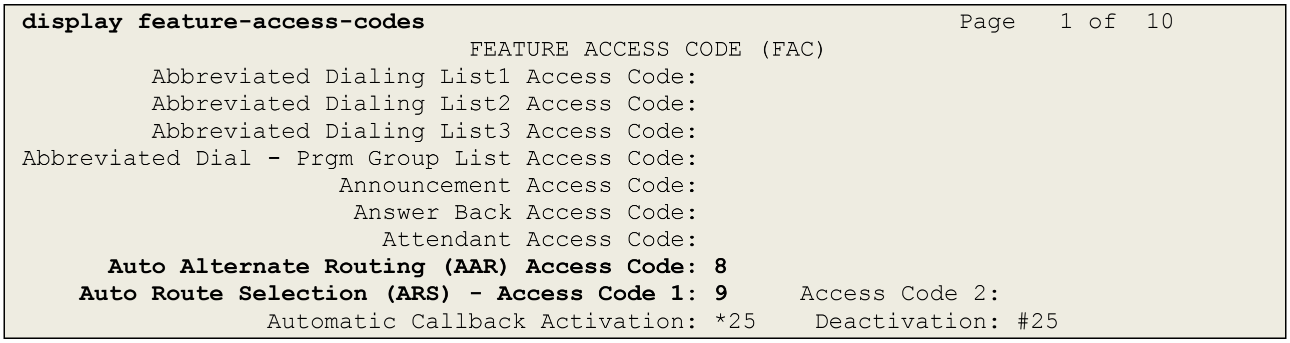
5.2. System Features and Access Codes

For the testing, **Trunk-to Trunk Transfer** was set to **all** on **page 1** of the **system-parameters features** page. This is a system wide setting that allows calls to be routed from one trunk to another and is usually turned off to help prevent toll fraud. An alternative to enabling this feature on a system wide basis is to control it using COR (Class of Restriction). See **Section 10** for supporting documentation.



```
display system-parameters features                             Page   1 of  19
                            FEATURE-RELATED SYSTEM PARAMETERS
                               Self Station Display Enabled? n
                                    Trunk-to-Trunk Transfer: all
               Automatic Callback with Called Party Queuing? n
    Automatic Callback - No Answer Timeout Interval (rings): 3
                       Call Park Timeout Interval (minutes): 10
        Off-Premises Tone Detect Timeout Interval (seconds): 20
                                 AAR/ARS Dial Tone Required? y

              Music (or Silence) on Transferred Trunk Calls? no
                       DID/Tie/ISDN/SIP Intercept Treatment: attd
    Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
                  Automatic Circuit Assurance (ACA) Enabled? n




             Abbreviated Dial Programming by Assigned Lists? n
       Auto Abbreviated/Delayed Transition Interval (rings): 2
                    Protocol for Caller ID Analog Terminals: Bellcore
    Display Calling Number for Room to Room Caller ID Calls? n
```

Use the **display feature-access-codes** command to verify that a FAC (feature access code) has been defined for both AAR and ARS. Note that **8** is used for AAR and **9** for ARS routing.



```
display feature-access-codes                                     Page   1 of  10
                               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:
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation: *25    Deactivation: #25
```

5.3. Administer Dial Plan

It was decided for compliance testing that all calls beginning with 500xx with a total length of 5 digits were to be sent across the SIP trunk to the DS3000 via Session Manager. In order to achieve this automatic alternate routing (aar) would be used to route the calls. The dial plan and aar routing analysis need to be changed to allow this.

Type **change dialplan analysis** in order to make changes to the dial plan. Ensure that **5** is added with a **Total Length** of **5** and a **Call Type** of **udp**.

```
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           4   ext
   3           4   ext
   4           4   udp
   5           5   udp
   6           4   ext
   9           1   fac
   *           3   fac
   #           3   fac
```

5.4. Administer Route Selection for Communications Portal Calls

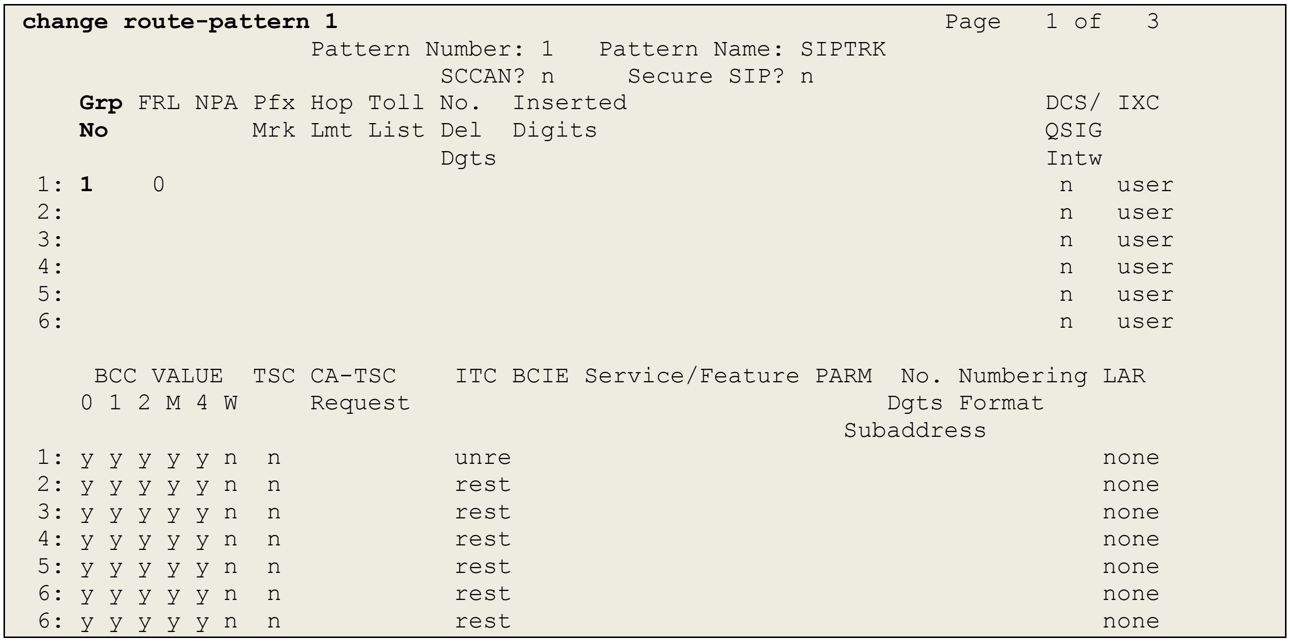
As digits **5** were defined in the dial plan as udp (**Section 5.3**) use the **change uniform-dialplan** command to configure the routing of the dialed digits. In the example below calls to numbers beginning with **500xx** that are **5** digits in length will be matched. No further digits are deleted or inserted. Calls are sent to **aar** for further processing.

```
change uniform-dialplan 5                                      Page   1 of   2
                       UNIFORM DIAL PLAN TABLE
                                                             Percent Full: 0

  Matching                   Insert              Node
  Pattern       Len Del      Digits      Net Conv Num
  500            5   0                   aar  n
                                              n
```

Use the **change aar analysis** x command to further configure the routing of the dialed digits. Calls to Communications Portal begin with **500xx** and are matched with the AAR entry shown below. Calls are sent to **Route Pattern 1**, which contains the outbound SIP Trunk Group.

```
change aar analysis 5                                         Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all           Percent Full: 1

    Dialed                  Total      Route    Call   Node  ANI
    String                 Min  Max   Pattern   Type   Num   Reqd
    500                    5    5      1        unku         n
```

Use the **change route-pattern *n*** command to add the SIP trunk group to the route pattern that AAR selects. In this configuration, **Route Pattern Number 1** is used to route calls to trunk group **(Grp No) 1**, this is the SIP Trunk configured in **Section 5.5**.



```
change route-pattern 1                                          Page   1 of   3
                    Pattern Number: 1   Pattern Name: SIPTRK
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                             DCS/ IXC
    No          Mrk Lmt List Del  Digits                               QSIG
                             Dgts                                      Intw
 1: 1    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  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: y y y y y n  n            unre                                         none
 2: y y y y y n  n            rest                                         none
 3: y y y y y n  n            rest                                         none
 4: y y y y y n  n            rest                                         none
 5: y y y y y n  n            rest                                         none
 6: y y y y y n  n            rest                                         none
 6: y y y y y n  n            rest                                         none
```

5.5. Configure SIP Trunk

In the Node Names IP form, note the IP Address of the **procr** and the Session Manager (**SM63vmpg**). The host names will be used throughout the other configuration screens of Communication Manager and Session Manager. Type **display node-names ip** to show all the necessary node names.

```
display node-names ip                                             Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
AES63VMPG           10.10.40.30
PGDECT              10.10.40.50
SM63vmpg            10.10.40.34
default             0.0.0.0
procr               10.10.40.31
procr6              ::
```

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager in **Section 6.1**. In this configuration, the domain name is **devconnect.local**. 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.

```
display ip-network-region 1                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: devconnect.local
    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? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        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
```

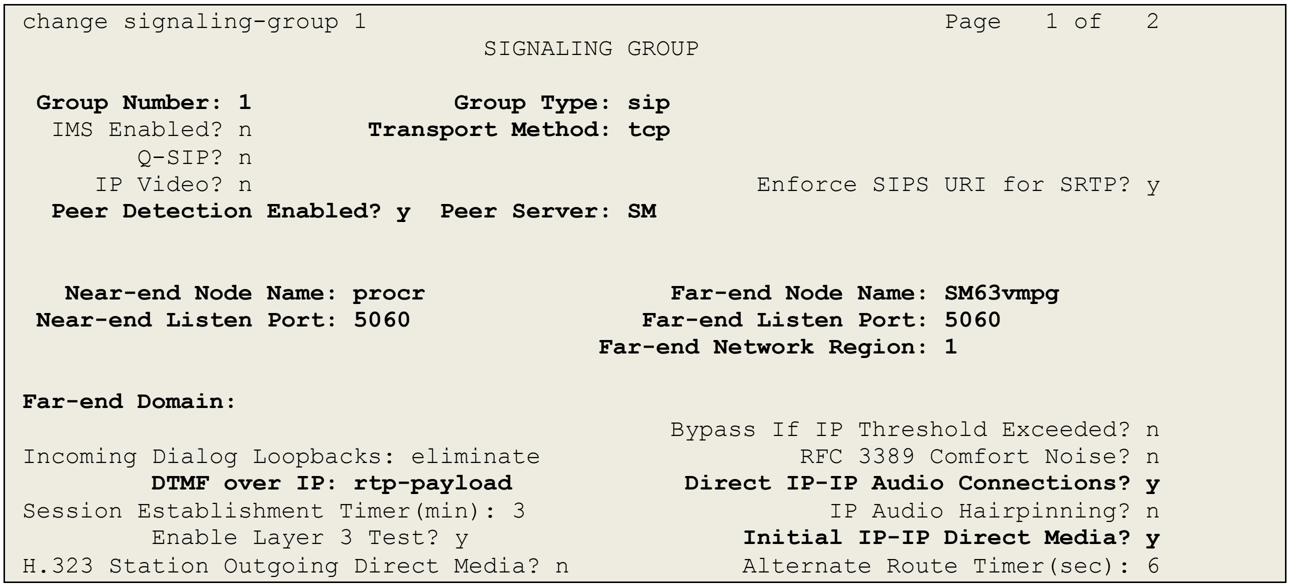
In the **IP Codec Set** form, select the audio codec's supported for calls routed over the SIP trunk to Communications Portal. The form is accessed via the **change ip-codec-set n** command. Note that IP codec set 1 was specified in IP Network Region 1 shown above. Multiple codecs may be specified in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

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

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 below as follows:

- Set the **Group Type** field to **sip**.
- Set the **Transport Method** to the desired transport method, for compliance testing this was set to **tcp**.
- The **Peer Detection Enabled** field should be set to **y** allowing the Communication Manager to automatically detect if the peer server is a Session Manager.
- Specify the node names for the procr and the 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.
- Set the **Near-end Node Name** to **procr**. This value is taken from the **IP Node Names** form shown above.
- Set the **Far-end Node Name** to the node name defined for the Session Manager (node name **SM63vmpg**), as per **Section 5.5**.
- Ensure that the recommended TCP port value of **5060** is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- In the **Far-end Network Region** field, enter the IP Network Region configured above**.** This field logically establishes the **far-end** for calls using this signaling group as network region 1.
- Leave the **Far-end Domain** field blank to allow Communication Manager to accept any domain.
- The **Direct IP-IP Audio Connections** field is set to **y**.
- The **Initial IP-IP Direct Media** field is set to **y**.
- The default values for the other fields may be used.

Note: Compliance testing was carried out with the **Direct IP-IP Audio Connections** field set to both **y** and to **n**. This was to allow testing for shuffling both on and off.



```
change signaling-group 1                                        Page   1 of   2
                                SIGNALING GROUP

 Group Number: 1              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


   Near-end Node Name: procr                  Far-end Node Name: SM63vmpg
 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? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y                   Initial IP-IP Direct Media? y
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 6
```

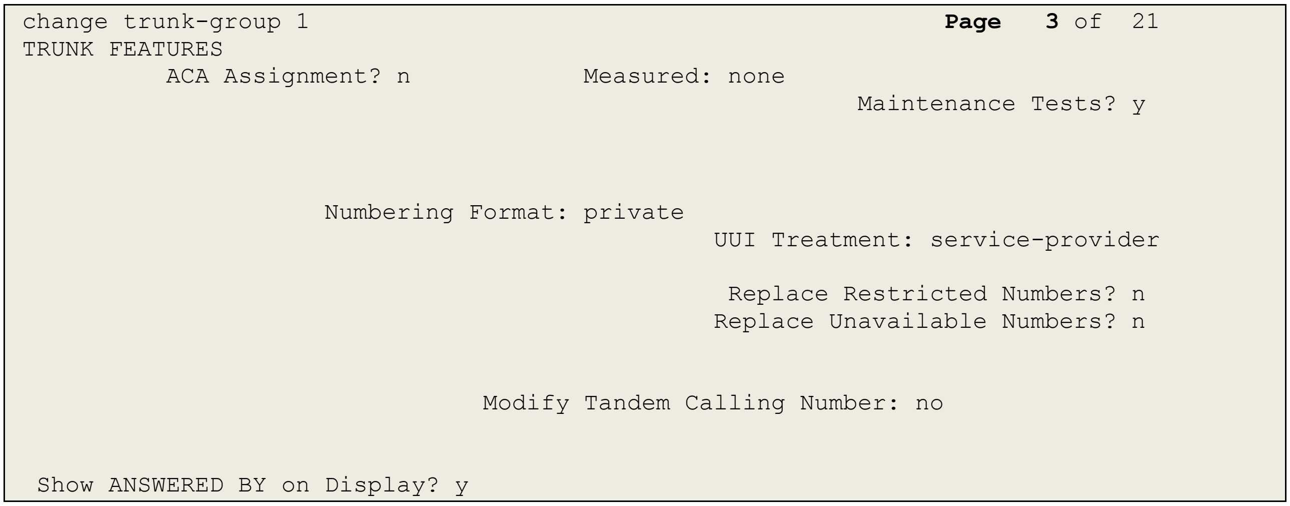
Configure the **Trunk Group** form as shown below. This trunk group is used for calls to and from Communications Portal. Enter a descriptive name in the **Group Name** field. Set the **Group Type** field to **sip**. Enter a **TAC** code compatible with the Communication Manager dial plan. Set the **Service 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.

```
change trunk-group 1                                            Page   1 of  21
                                TRUNK GROUP

Group Number: 1                    Group Type: sip           CDR Reports: y
  Group Name: SIP TRK                     COR: 1        TN: 1        TAC: *11
   Direction: two-way       Outgoing Display? y
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: tie                  Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 1
                                                     Number of Members: 10
```

On **Page 2** of the trunk-group form the **Preferred Minimum Session Refresh Interval (sec)** field should be set to a value mutually agreed with Presence to prevent unnecessary SIP messages during call setup. Session refresh is used throughout the duration of the call, to check the other side has not gone away, for the compliance test a value of **600** was used.

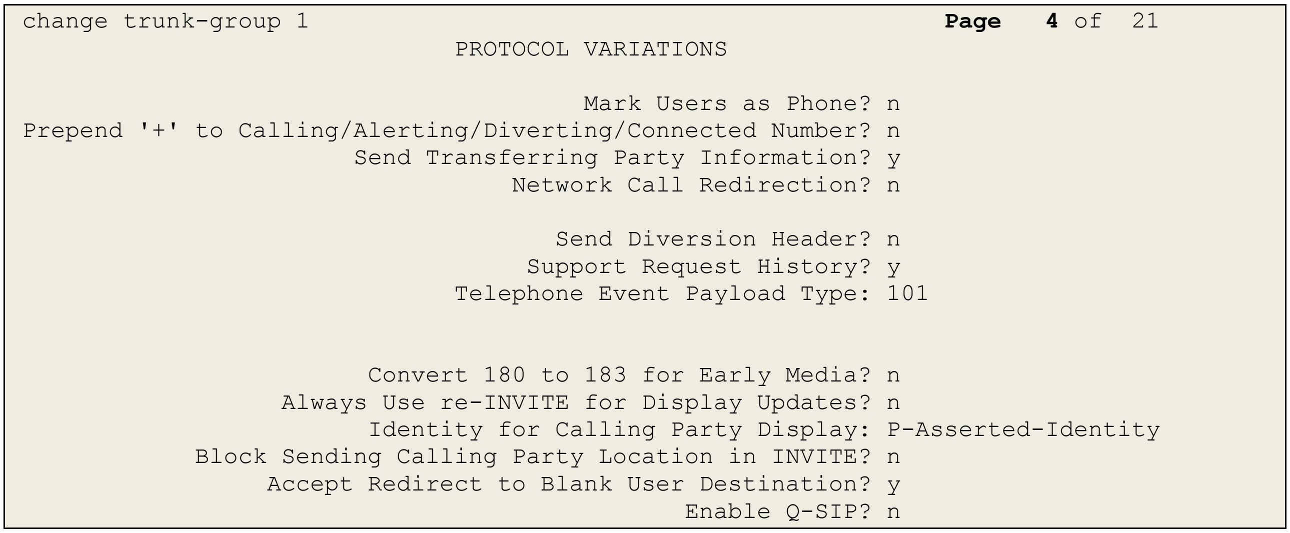
```
change trunk-group 1                                            Page   2 of  21
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name: auto

                                        Redirect On OPTIM Failure: 5000

            SCCAN? n                               Digital Loss Group: 18
                      Preferred Minimum Session Refresh Interval(sec): 600

 Disconnect Supervision - In? y  Out? y


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

Settings on **Page 3** can be left as default.



```
change trunk-group 1                                            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


                                Modify Tandem Calling Number: no


 Show ANSWERED BY on Display? y
```

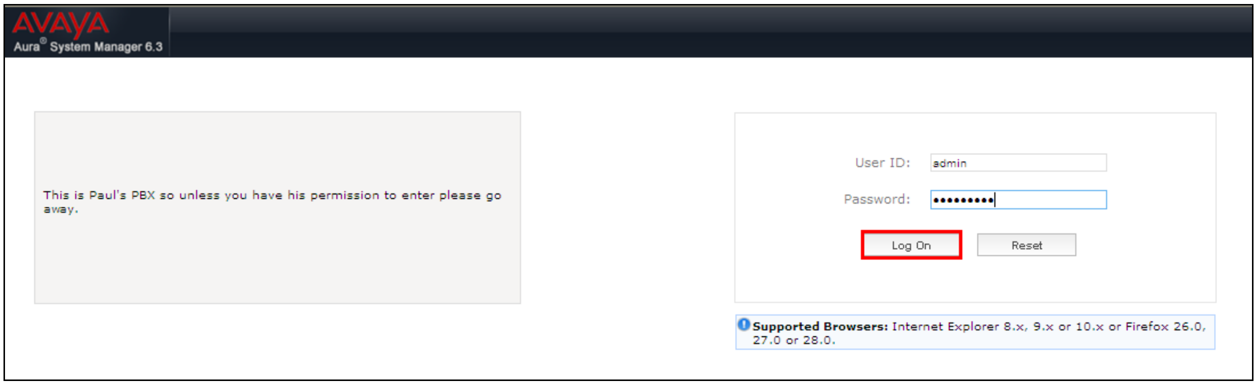
Settings on **Page 4** are as follows.



```
change trunk-group 1                                            Page   4 of  21
                              PROTOCOL VARIATIONS

                                       Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                       Send Transferring Party Information? y
                                  Network Call Redirection? n

                                     Send Diversion Header? n
                                   Support Request History? y
                              Telephone Event Payload Type: 101


                        Convert 180 to 183 for Early Media? n
                  Always Use re-INVITE for Display Updates? n
                        Identity for Calling Party Display: P-Asserted-Identity
            Block Sending Calling Party Location in INVITE? n
                 Accept Redirect to Blank User Destination? y
                                              Enable Q-SIP? n
```

6. Configure Avaya Aura® Session Manager

In order to make changes in Session Manager, a web session is established to System Manager. Log into System Manager by opening a web browser and navigating to http://<System Manager IP Address>/SMGR. Enter the appropriate credentials for the **User ID** and **Password** and click on **Log On** highlighted below.



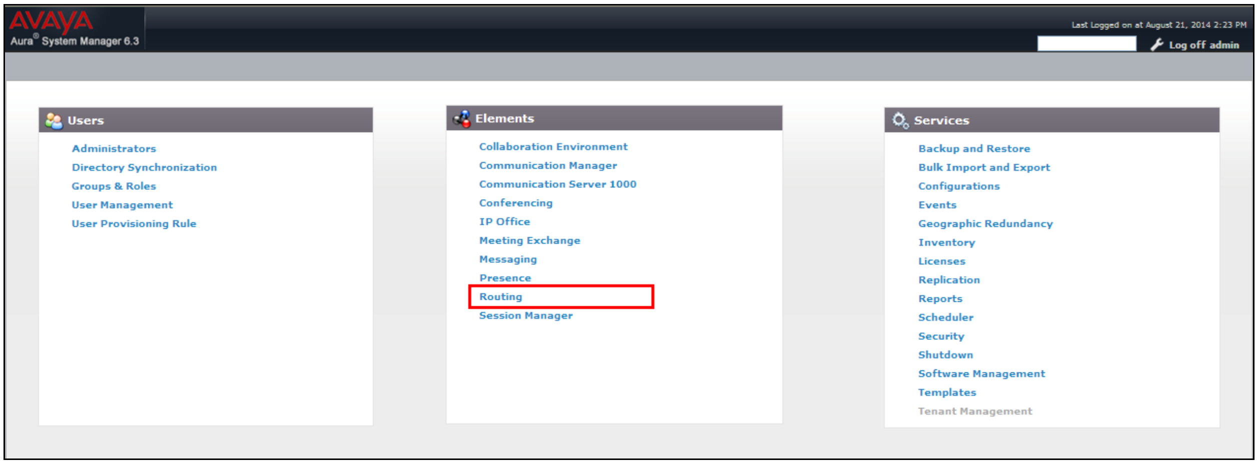
This is Paul's PBX so unless you have his permission to enter please go away.

User ID: admin

Password: •••••••••

Supported Browsers: Internet Explorer 8.x, 9.x or 10.x or Firefox 26.0, 27.0 or 28.0.

Once logged in click on **Routing** as highlighted below.

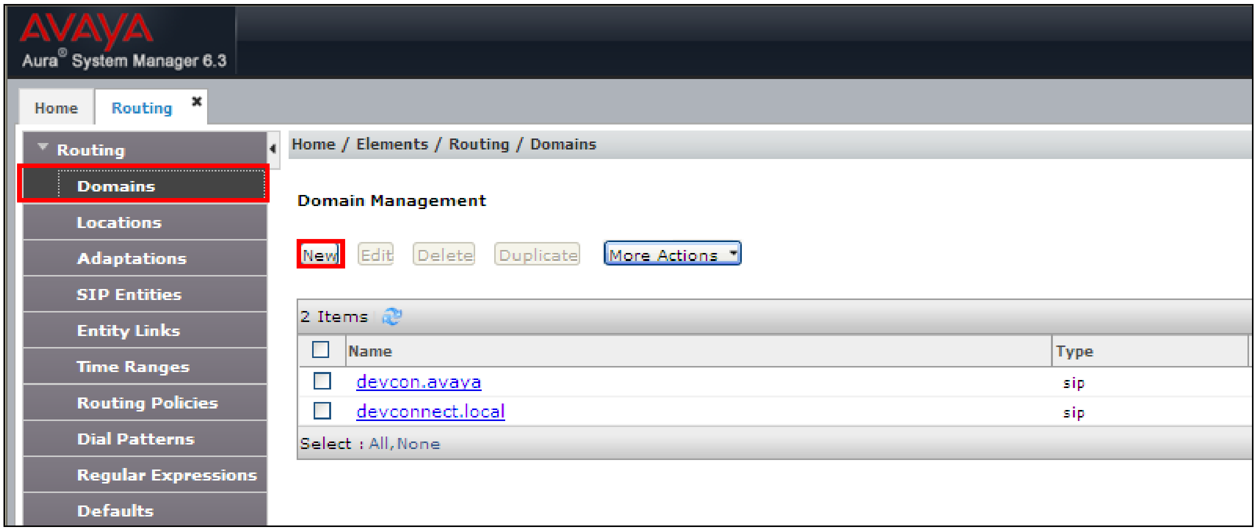


6.1. Domains and Locations

Note: It is assumed that a domain and a location have already been set-up and a SIP trunk already in place to CS1000E. Therefore a quick overview of the domain and location that was used in compliance testing is only provided here.

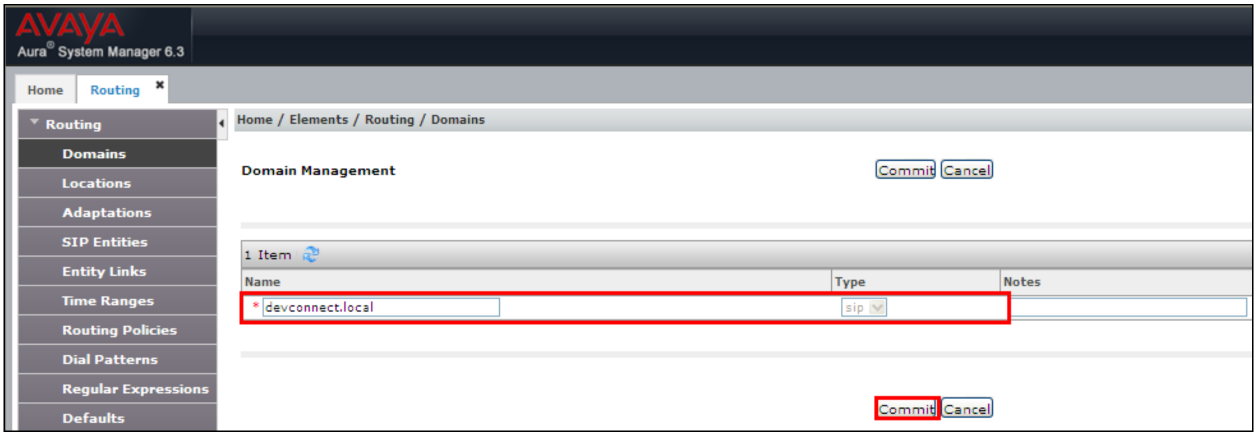
6.1.1. Add a new Domain

If a domain is not already in place then click on **New** as is highlighted below.



	Name	Type
□	devcon.avaya	sip
□	devconnect.local	sip

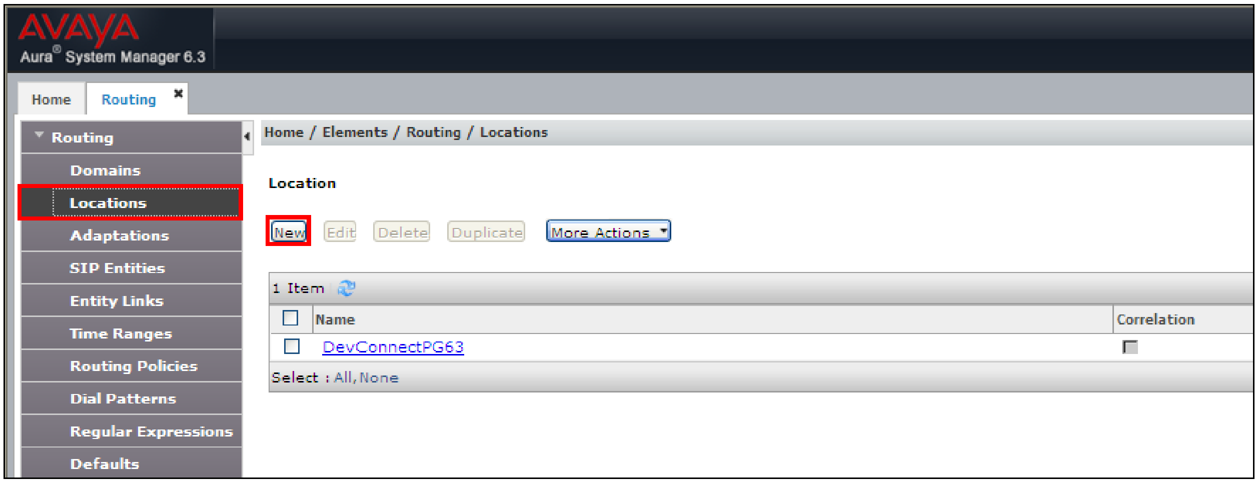
Enter the domain **Name**; note this will be the same as that domain configured in **Section 5.5**, and ensure the **Type** is set to **SIP**. Click on **Commit** once done.



Name	Type	Notes
* devconnect.local	sip	

6.1.2. Add a new Location

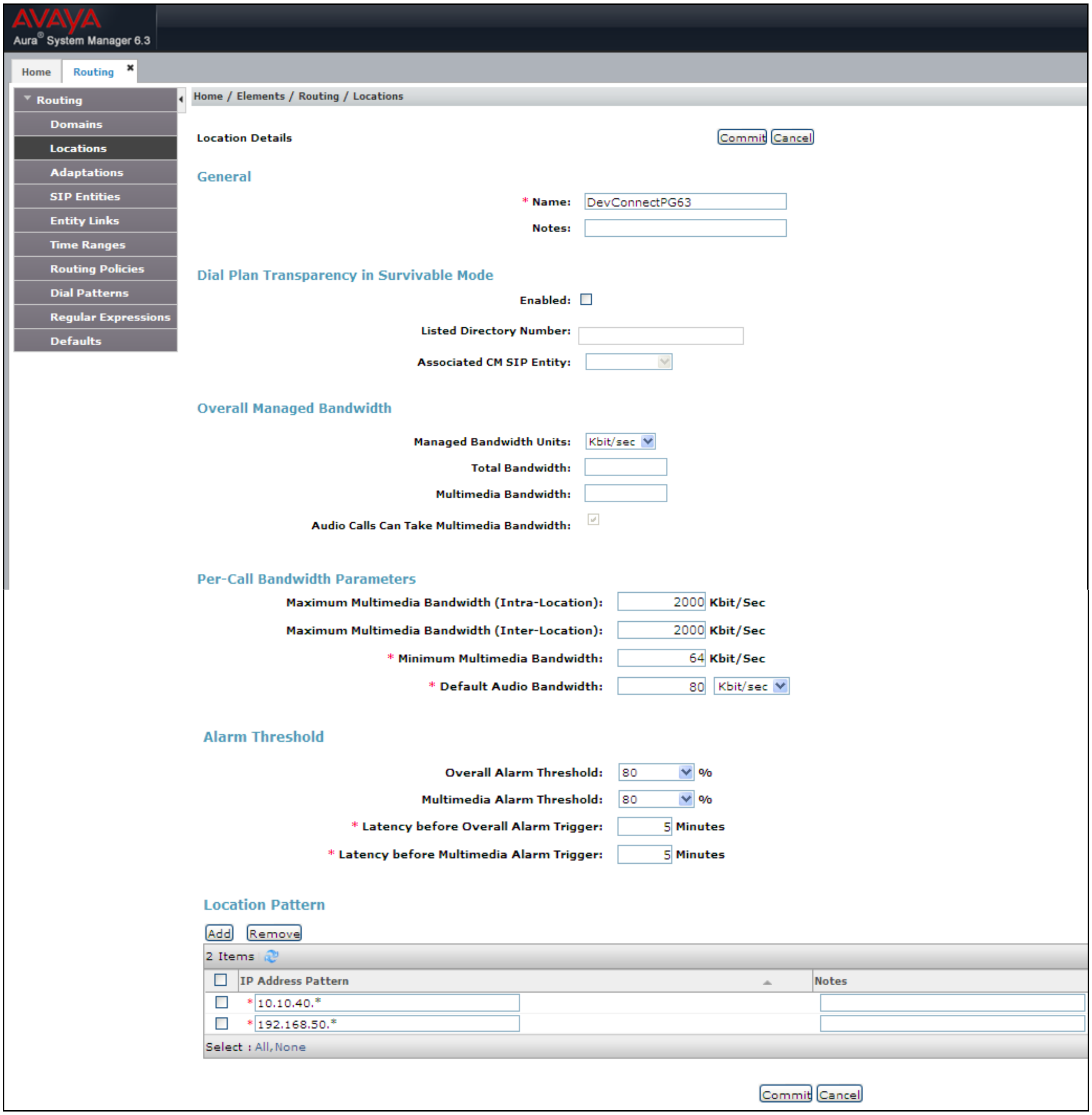
If a location is not already in place then one must be added to include the IP address range of the Avaya solution. Click on **New** as is highlighted below to add a new location.



Location

□	Name	Correlation
□	DevConnectPG63	☐

Enter a suitable **Name** and add the IP address ranges at the bottom of the screen under **Location Pattern** and click on **Commi**t once this is done.



Location Details

General

* Name: DevConnectPG63

Notes:

Dial Plan Transparency in Survivable Mode

Enabled: □

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☑

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): 2000 Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): 2000 Kbit/Sec

* Minimum Multimedia Bandwidth: 64 Kbit/Sec

* Default Audio Bandwidth: 80 Kbit/sec

Alarm Threshold

Overall Alarm Threshold: 80 %

Multimedia Alarm Threshold: 80 %

* Latency before Overall Alarm Trigger: 5 Minutes

* Latency before Multimedia Alarm Trigger: 5 Minutes

Location Pattern

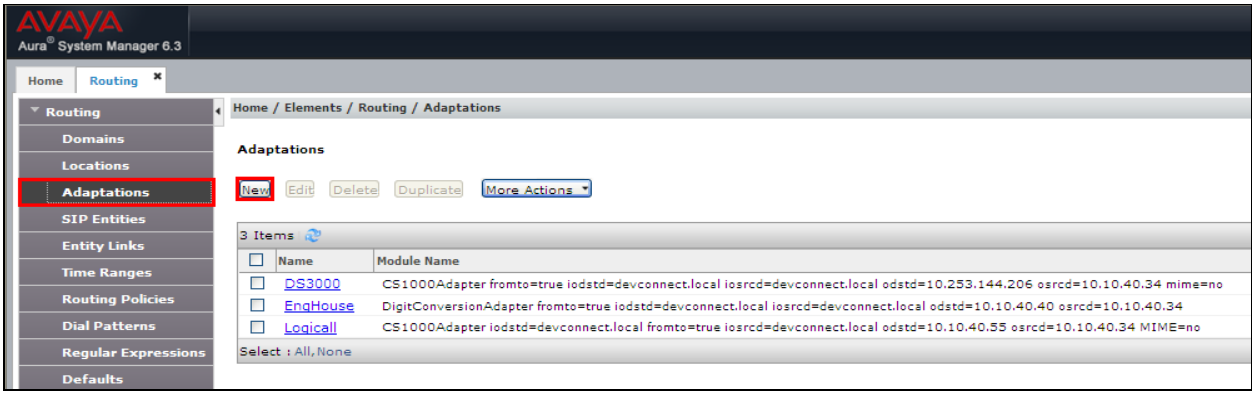
2 Items

□	IP Address Pattern	Notes
□	* 10.10.40.*	
□	* 192.168.50.*	

Select : All, None

6.2. Creating an Adaptation for DS3000

An adaptation can allow the altering of SIP Message. An adaptation is created to convert domain names to IP addresses. Select **Adaptations** from the left window and click on **New** in the main window.



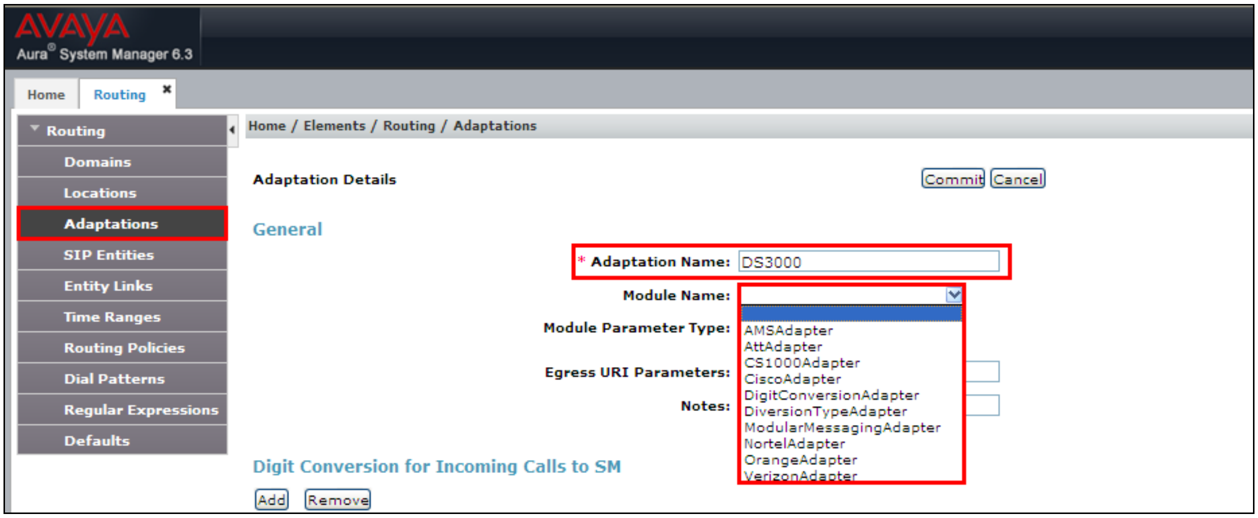
Adaptations

3 Items

□	Name	Module Name
□	DS3000	CS1000Adapter fromto=true iodstd=devconnect.local iosrcd=devconnect.local odstd=10.253.144.206 osrcd=10.10.40.34 mime=no
□	EngHouse	DigitConversionAdapter fromto=true iodstd=devconnect.local iosrcd=devconnect.local odstd=10.10.40.40 osrcd=10.10.40.34
□	Logicall	CS1000Adapter iodstd=devconnect.local fromto=true iosrcd=devconnect.local odstd=10.10.40.55 osrcd=10.10.40.34 MIME=no

Select : All, None

Enter a suitable **Adaptation Name**, select **DigitConversionAdapter** for the **Module Name**.



Adaptation Details

* Adaptation Name: DS3000

Module Name:

Module Parameter Type:

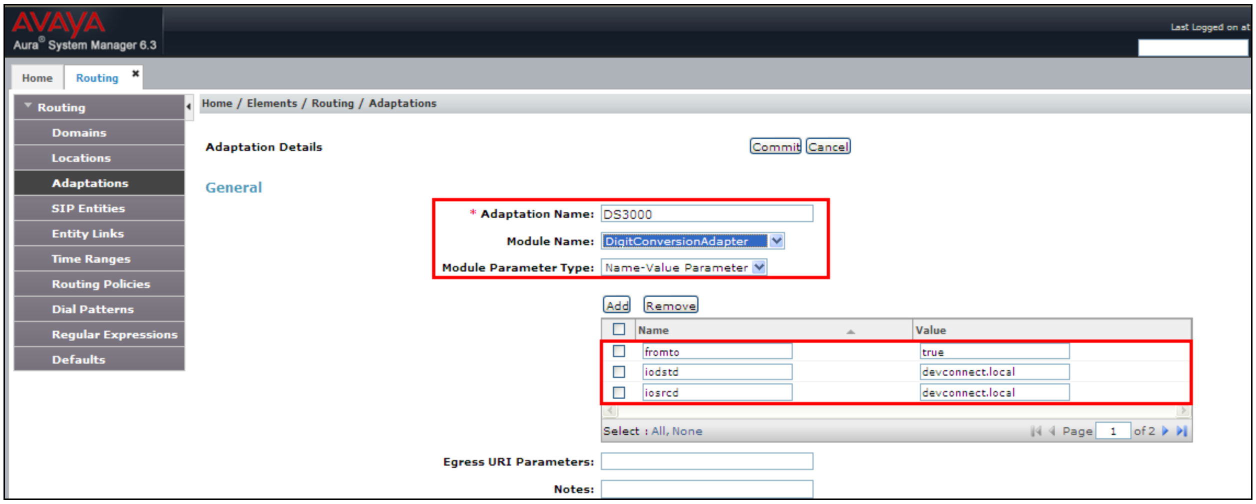
Egress URI Parameters:

Notes:

The **Module Parameter Type** should be set to **Name-Value Parameter**. Add the following module parameters:

- **fromto=true**
- **iodstd=devconnect.local**
- **iosrcd=devconnect.local**
- **odstd=10.253.144.206**
- **osrcd=10.10.40.34**

In this example 10.253.144.206 is the DS3000 SIP Gateway and 10.10.40.34 is the Session Manager SM100 IP Address, these IP addresses may need to be changed to suit accordingly. **devconnect.local** is the domain name as per **Section 6.1**.



Adaptation Details

General

* Adaptation Name: DS3000

Module Name: DigitConversionAdapter

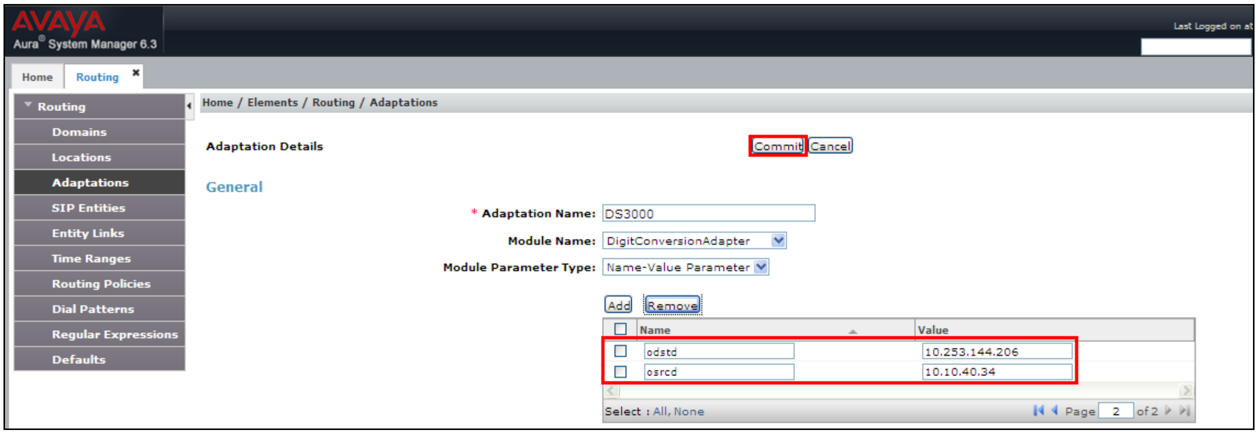
Module Parameter Type: Name-Value Parameter

□	Name	Value
□	fromto	true
□	iodstd	devconnect.local
□	iosrcd	devconnect.local

Egress URI Parameters:

Notes:

Add the remaining module parameters and click on **Commit** once completed.



Adaptation Details

General

* Adaptation Name: DS3000

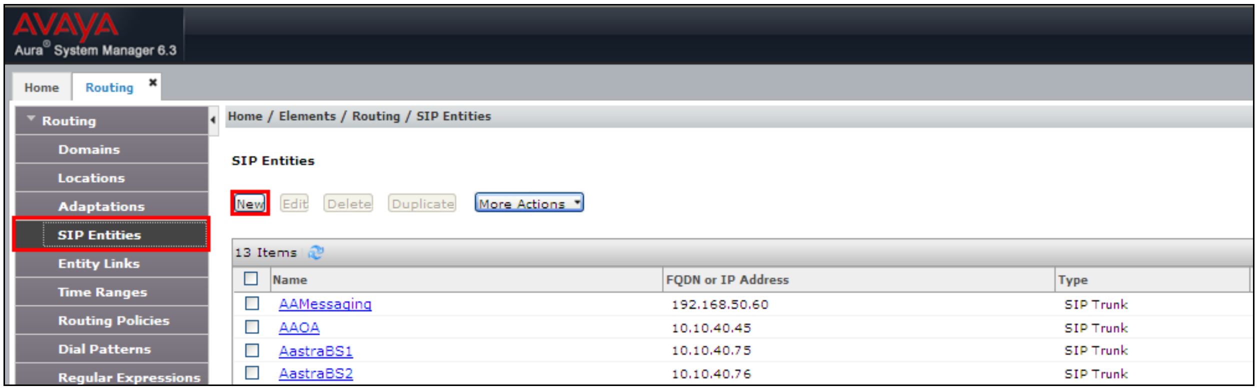
Module Name: DigitConversionAdapter

Module Parameter Type: Name-Value Parameter

□	Name	Value
□	odstd	10.253.144.206
□	osrcd	10.10.40.34

6.3. Adding DS3000 as a SIP Entity

Click on **SIP Entities** in the left column and select **New** in the right window.



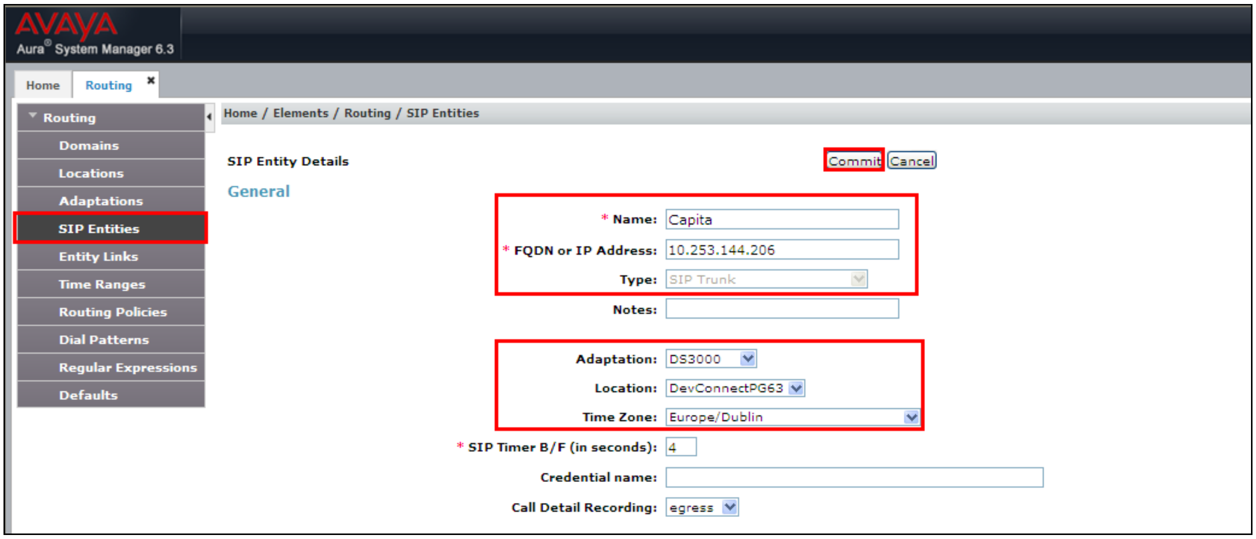
Home / Elements / Routing / SIP Entities

SIP Entities

13 Items

	Name	FQDN or IP Address	Type
□	AAMessaging	192.168.50.60	SIP Trunk
□	AAOA	10.10.40.45	SIP Trunk
□	AastraBS1	10.10.40.75	SIP Trunk
□	AastraBS2	10.10.40.76	SIP Trunk

Enter a suitable **Name** for the new SIP Entity and the **IP Address** of the DS3000, which is the floating IP address of the DS3000 SIP Server. Enter the correct **Time Zone** and **Location** and click on **Commit**.



Home / Elements / Routing / SIP Entities

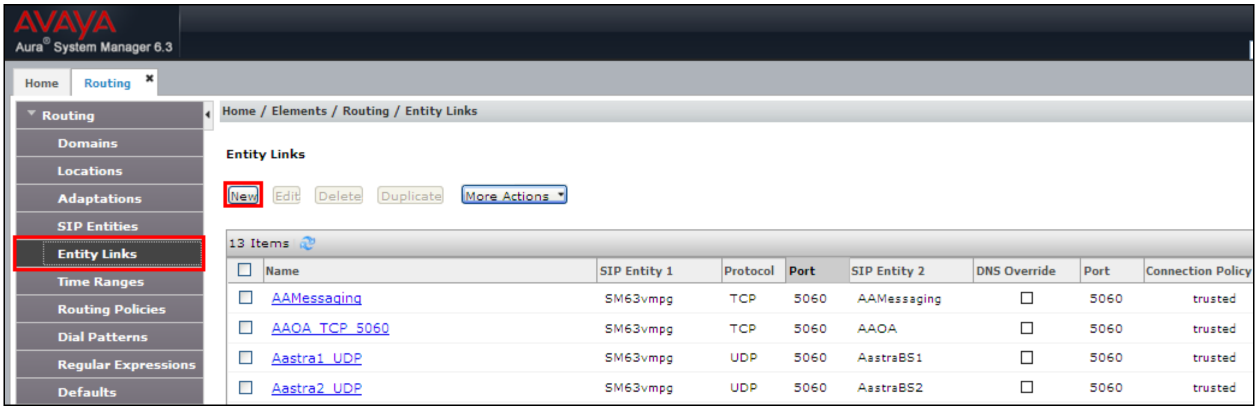
SIP Entity Details

General

* Name:	Capita
* FQDN or IP Address:	10.253.144.206
Type:	SIP Trunk
Notes:	
Adaptation:	DS3000
Location:	DevConnectPG63
Time Zone:	Europe/Dublin
* SIP Timer B/F (in seconds):	4
Credential name:	
Call Detail Recording:	egress

6.4. Adding the DS3000 Entity Link

Two Entity links are added for the DS3000 as it can use both UDP and TCP to transport SIP messaging. Click on **Entity Links** in the left column and select **New** in the main window.



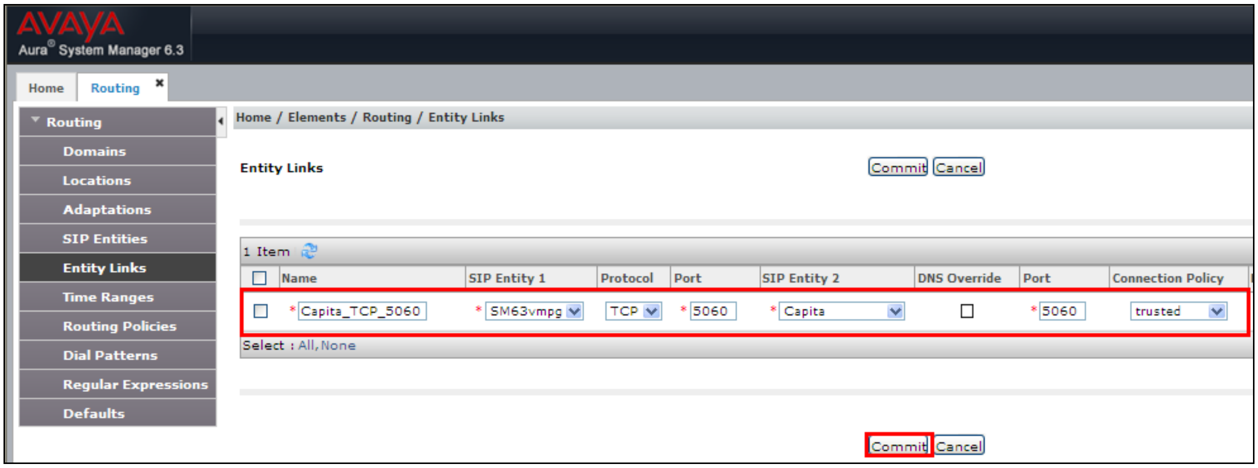
Home / Elements / Routing / Entity Links

Entity Links

13 Items

□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy
□	AAMessaging	SM63vmpg	TCP	5060	AAMessaging	□	5060	trusted
□	AAOA_TCP_5060	SM63vmpg	TCP	5060	AAOA	□	5060	trusted
□	Aastra1_UDP	SM63vmpg	UDP	5060	AastraBS1	□	5060	trusted
□	Aastra2_UDP	SM63vmpg	UDP	5060	AastraBS2	□	5060	trusted

Enter a suitable **Name** for the Entity Link and select the **Session Manager** SIP Entity for **SIP Entity 1** and the newly created **DS3000** Entity for **SIP Entity 2**. Ensure that **TCP** is selected for the **Protocol** and that **Port 5060** is used. Click on **Commit** once finished to save the new Entity Link.



Home / Elements / Routing / Entity Links

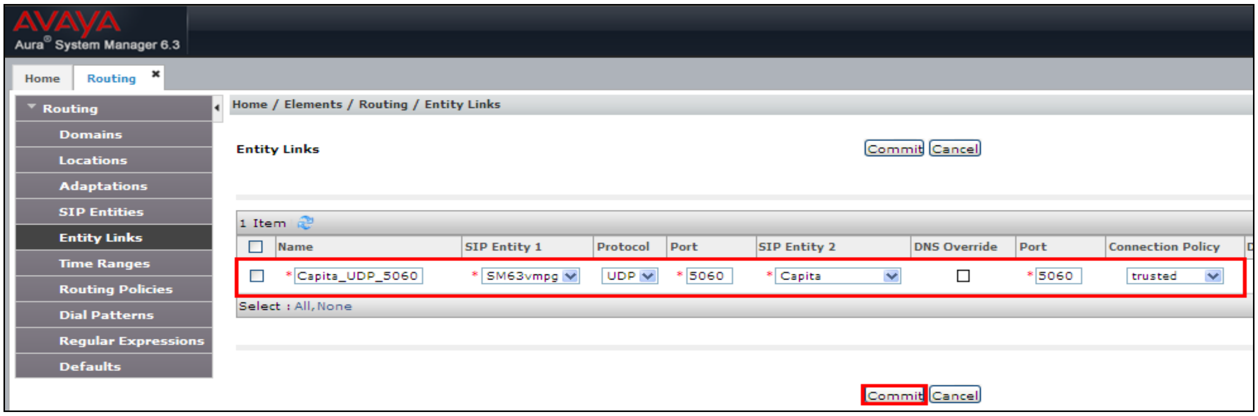
Entity Links

1 Item

□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy
□	* Capita_TCP_5060	* SM63vmpg	TCP	* 5060	* Capita	□	* 5060	trusted

Select : All, None

A second Entity Link is added for UDP, enter a suitable **Name** for the Entity Link and select the **Session Manager** SIP Entity for **SIP Entity 1** and the newly created **DS3000** Entity for **SIP Entity 2**. Ensure that **UDP** is selected for the **Protocol** and that **Port 5060** is used. Click on **Commit** once finished to save the new Entity Link.



Home / Elements / Routing / Entity Links

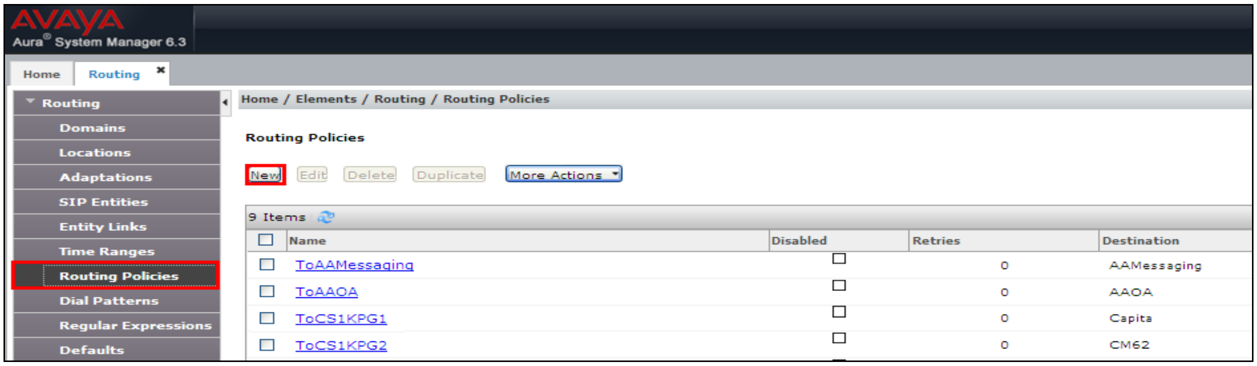
Entity Links

1 Item

□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy
□	* Capita_UDP_5060	* SM63vmpg	UDP	* 5060	* Capita	□	* 5060	trusted

6.5. Adding the DS3000 Routing Policy

Click on **Routing Policies** in the left window and select **New** in the main window.



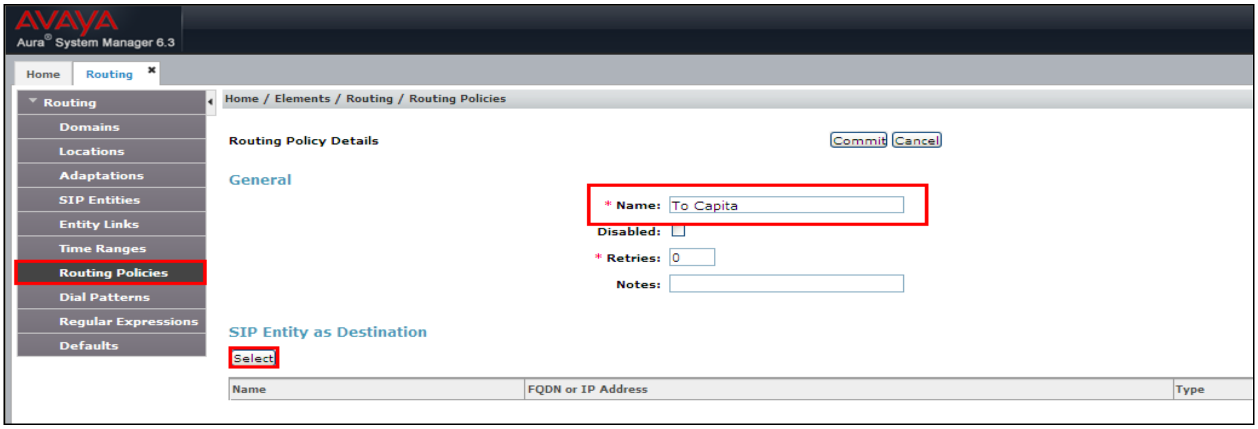
Home / Elements / Routing / Routing Policies

Routing Policies

9 Items

□	Name	Disabled	Retries	Destination
□	ToAAMessaging	□	0	AAMessaging
□	ToAAOA	□	0	AAOA
□	ToCS1KPG1	□	0	Capita
□	ToCS1KPG2	□	0	CM62

Enter a suitable **Name** for the Routing Policy and click on **Select** under **SIP Entity as Destination**, highlighted below.



Home / Elements / Routing / Routing Policies

Routing Policy Details

General

* Name: To Capita

Disabled: □

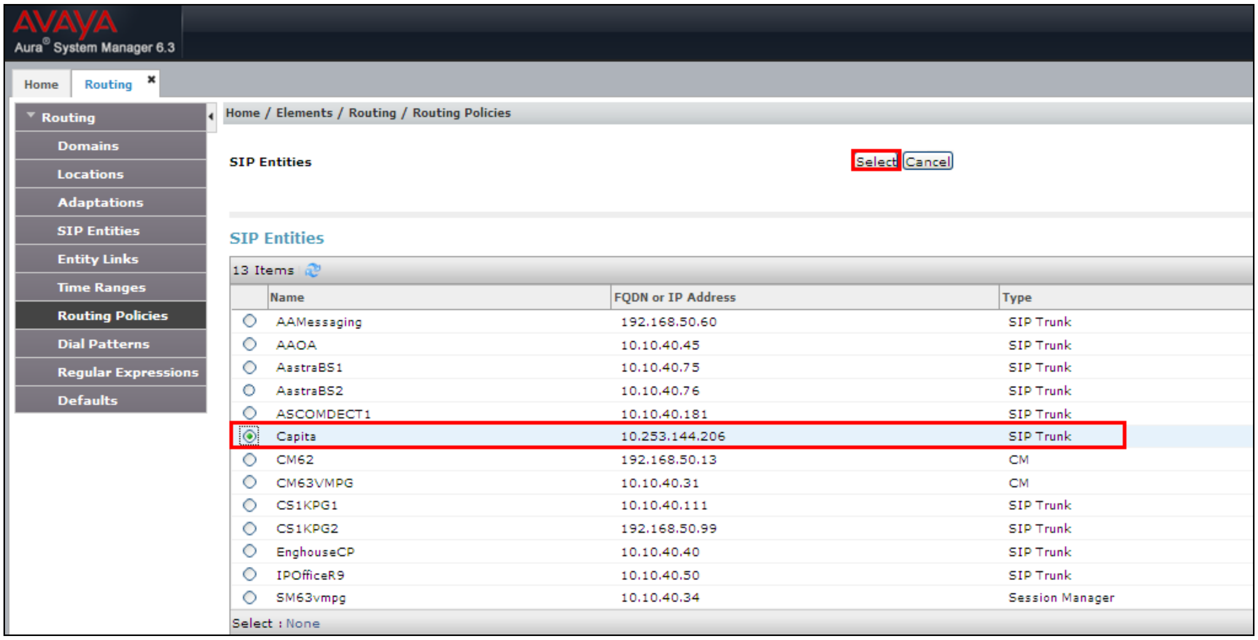
* Retries: 0

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type

Select the **Capita** SIP Entity as shown below and click on **Select**.



Home / Elements / Routing / Routing Policies

SIP Entities

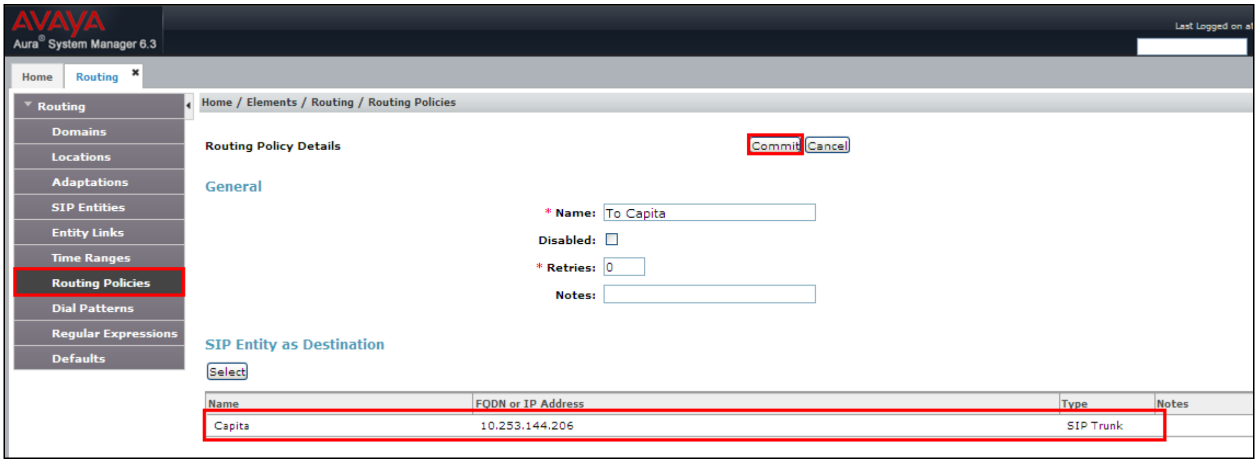
SIP Entities

13 Items

	Name	FQDN or IP Address	Type
○	AAMessaging	192.168.50.60	SIP Trunk
○	AAOA	10.10.40.45	SIP Trunk
○	AastraBS1	10.10.40.75	SIP Trunk
○	AastraBS2	10.10.40.76	SIP Trunk
○	ASCOMDECT1	10.10.40.181	SIP Trunk
●	Capita	10.253.144.206	SIP Trunk
○	CM62	192.168.50.13	CM
○	CM63VMPG	10.10.40.31	CM
○	CS1KPG1	10.10.40.111	SIP Trunk
○	CS1KPG2	192.168.50.99	SIP Trunk
○	EnghouseCP	10.10.40.40	SIP Trunk
○	IPOfficeR9	10.10.40.50	SIP Trunk
○	SM63vmpg	10.10.40.34	Session Manager

Select : None

The selected destination is now shown, click on **Commit** to save this.



Home / Elements / Routing / Routing Policies

Routing Policy Details

General

* Name: To Capita

Disabled: □

* Retries: 0

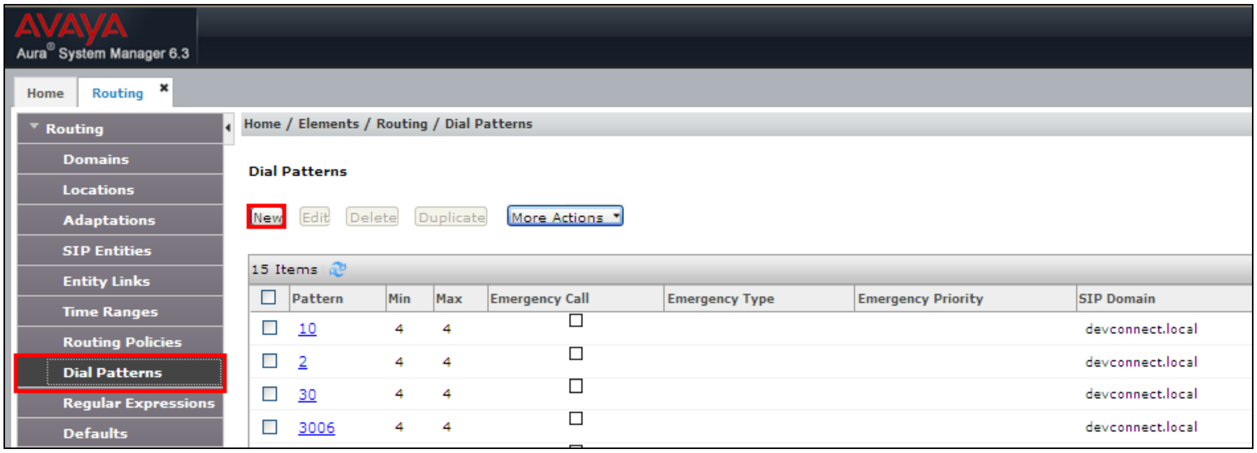
Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
Capita	10.253.144.206	SIP Trunk	

6.6. Adding a Dial Pattern for DS3000

Select **Dial Patterns** in the left window and select **New** in the main window.

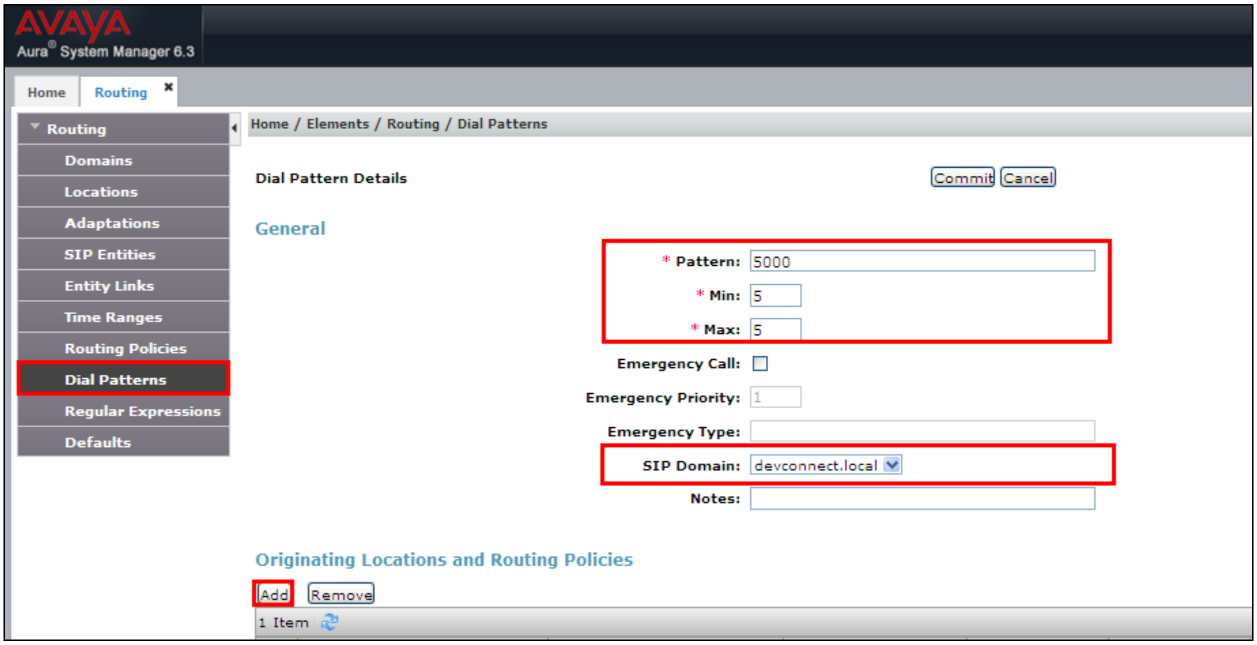


Dial Patterns

15 Items

□	Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Domain
□	10	4	4	□			devconnect.local
□	2	4	4	□			devconnect.local
□	30	4	4	□			devconnect.local
□	3006	4	4	□			devconnect.local

Enter the required digits for the Pattern, in the example below 5000x is used, which means that 50000 – 50009 will use the Routing Policy that will be selected. **5000** is entered as the **Pattern** and the **Min** and **Max** digit length of **5** is used thus giving 5000x. Ensure that the correct domain is entered for **SIP Domain** in this example the domain created in **Section 6.1** is added. Click on **Add** under **Originating Locations and Routing Policies** in order to select this Routing Policy.



Dial Pattern Details

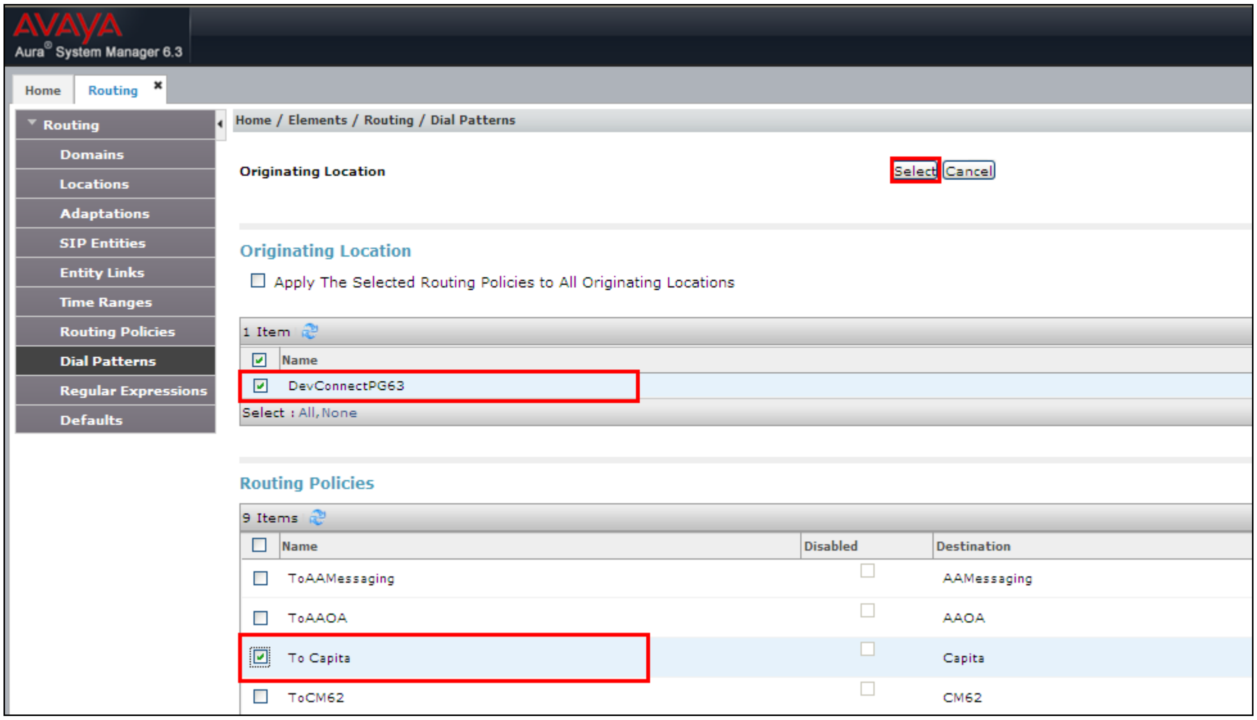
General

* Pattern:	5000
* Min:	5
* Max:	5
Emergency Call:	□
Emergency Priority:	1
Emergency Type:	
SIP Domain:	devconnect.local
Notes:	

Originating Locations and Routing Policies

1 Item

Select the Originating Location, this will be the location added in **Section 6.1** select the newly created routing policy for the DS3000 created in **Section 6.5** for **Routing Policies**.



Home / Elements / Routing / Dial Patterns

Originating Location

Originating Location

□ Apply The Selected Routing Policies to All Originating Locations

1 Item

☑	Name
☑	DevConnectPG63

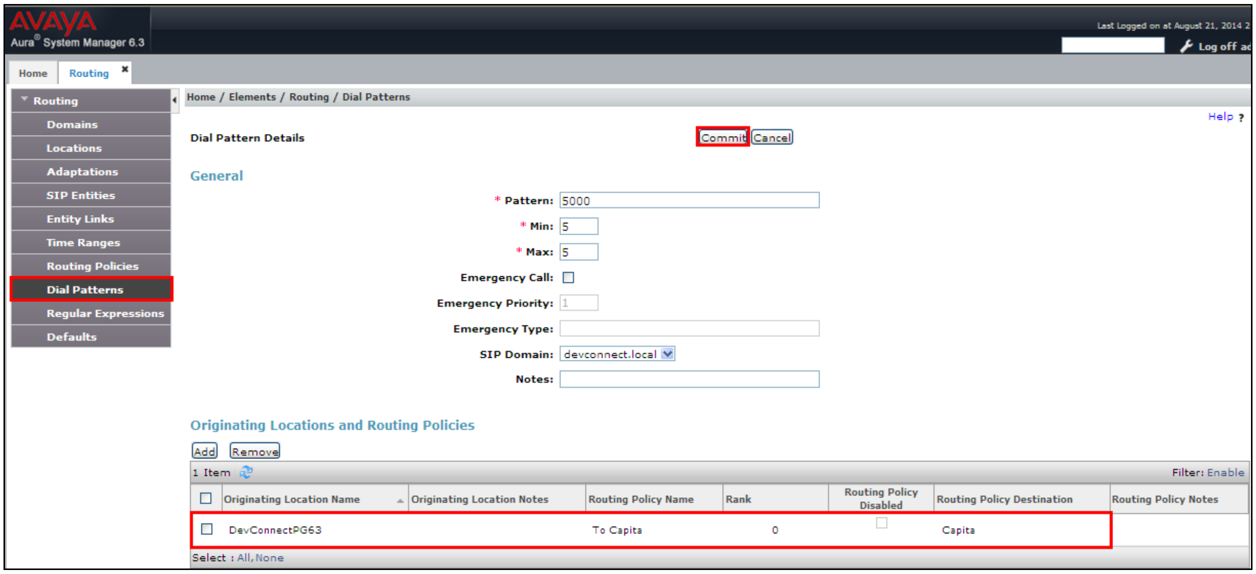
Select : All, None

Routing Policies

9 Items

□	Name	Disabled	Destination
□	ToAAMessaging	□	AAMessaging
□	ToAAOA	□	AAOA
☑	To Capita	□	Capita
□	ToCM62	□	CM62

With the Routing Policy selected click on **Commit** to finish adding the **Dial Pattern**.



Home / Elements / Routing / Dial Patterns

Dial Pattern Details

General

* Pattern:	5000
* Min:	5
* Max:	5
Emergency Call:	□
Emergency Priority:	1
Emergency Type:	
SIP Domain:	devconnect.local
Notes:	

Originating Locations and Routing Policies

1 Item — Filter: Enable

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	DevConnectPG63		To Capita	0	□	Capita	

Select : All, None

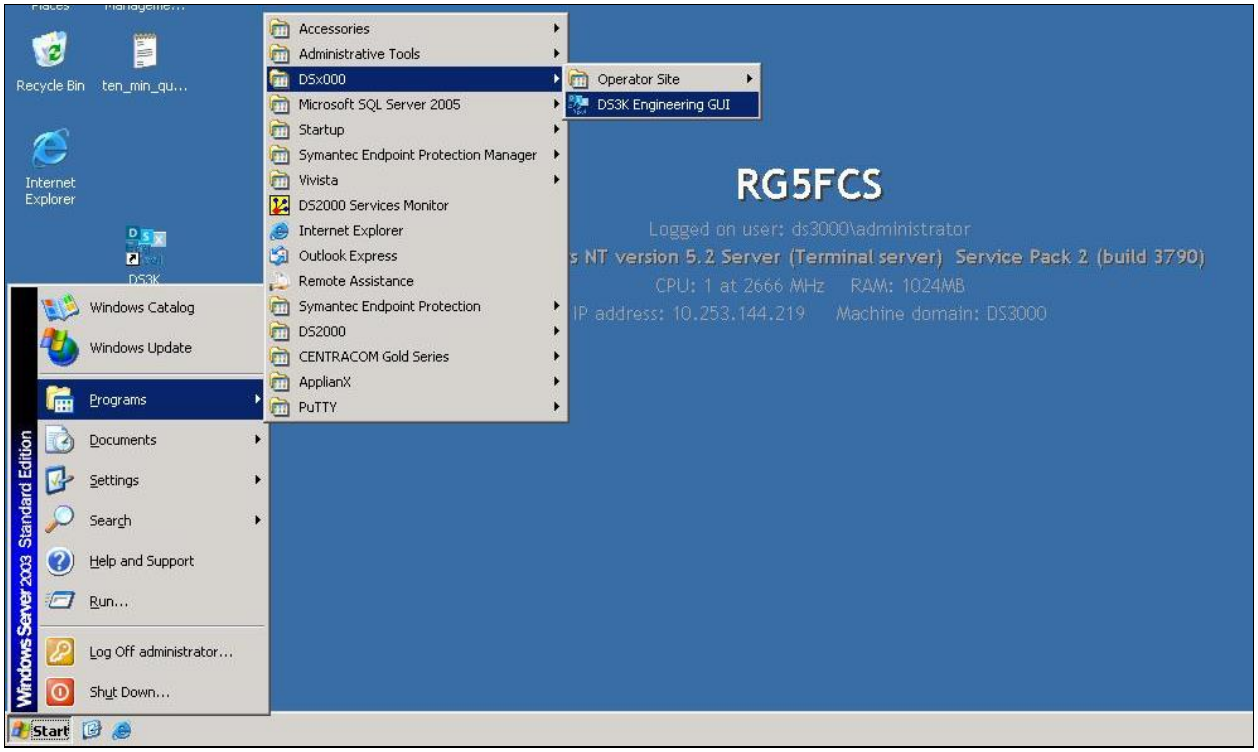
7. Configure Capita DS3000 Application

The following sections describe the steps required to configure the DS3000 application in order to connect successfully with Session Manager using SIP trunks.

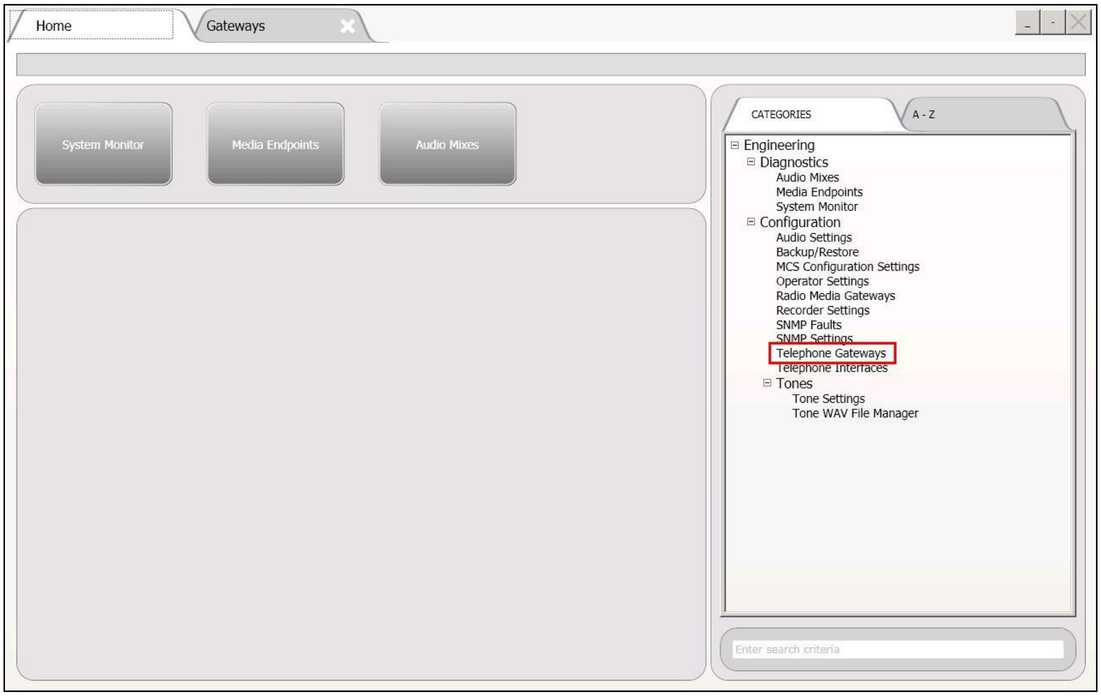
7.1. Configure DS3000 connection to Session Manager

The configuration for the connection to Session Manager is performed on the DS3000 SIP Server called RG5FCS.

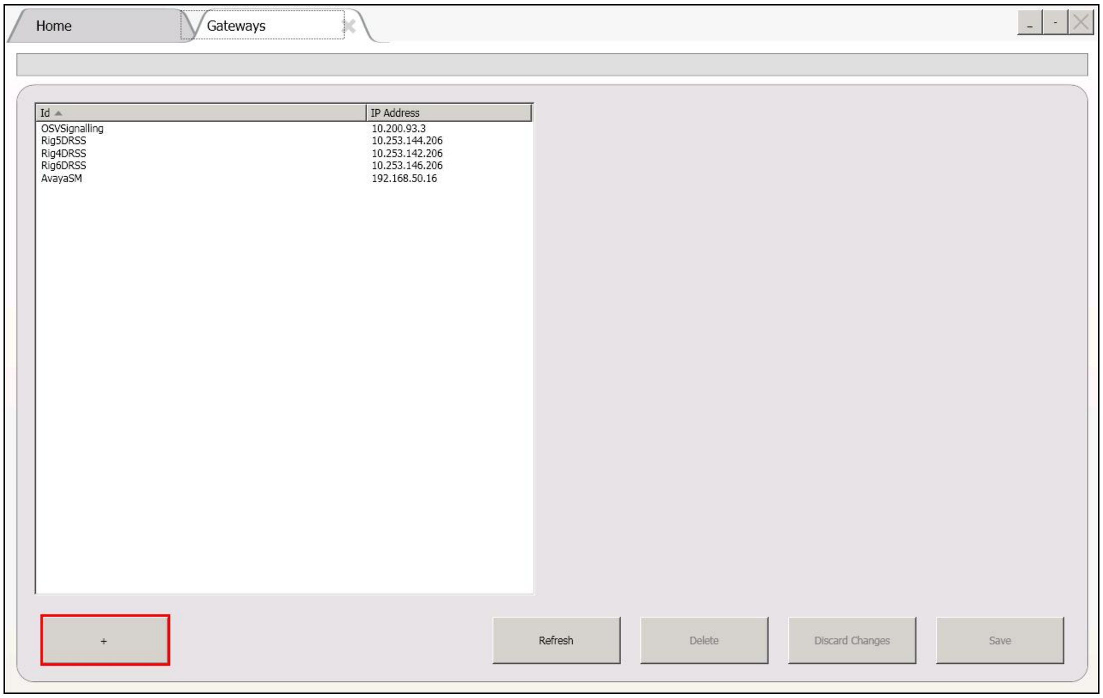
Log into **DS3K Engineering GUI** as shown below on the DS3000 SIP Server.



Once logged in the following screen appears. Select **Telephone Gateways** in the right column, highlighted below.

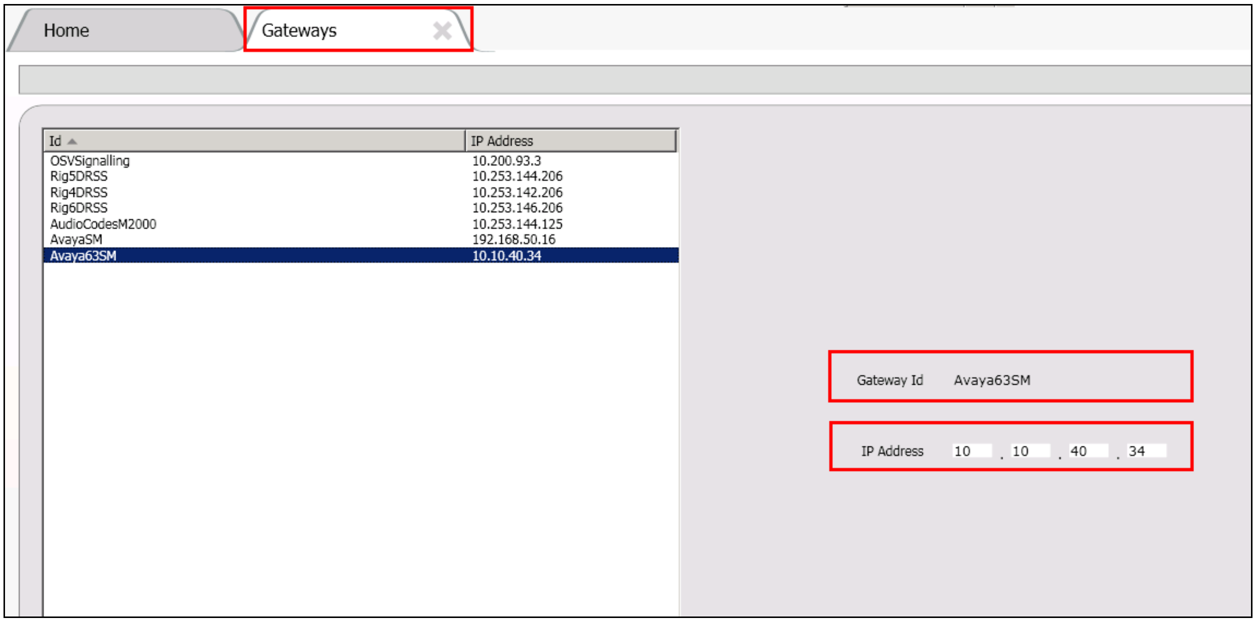


The **Gateways** tab is opened. Select the **+** icon at the bottom left of the screen.



Id	IP Address
OSVSignalling	10.200.93.3
Rig5DRSS	10.253.144.206
Rig4DRSS	10.253.142.206
Rig6DRSS	10.253.146.206
AvayaSM	192.168.50.16

Fill in the **Gateway Id** and **IP Address** information. This will be the IP address of the Session Manager.

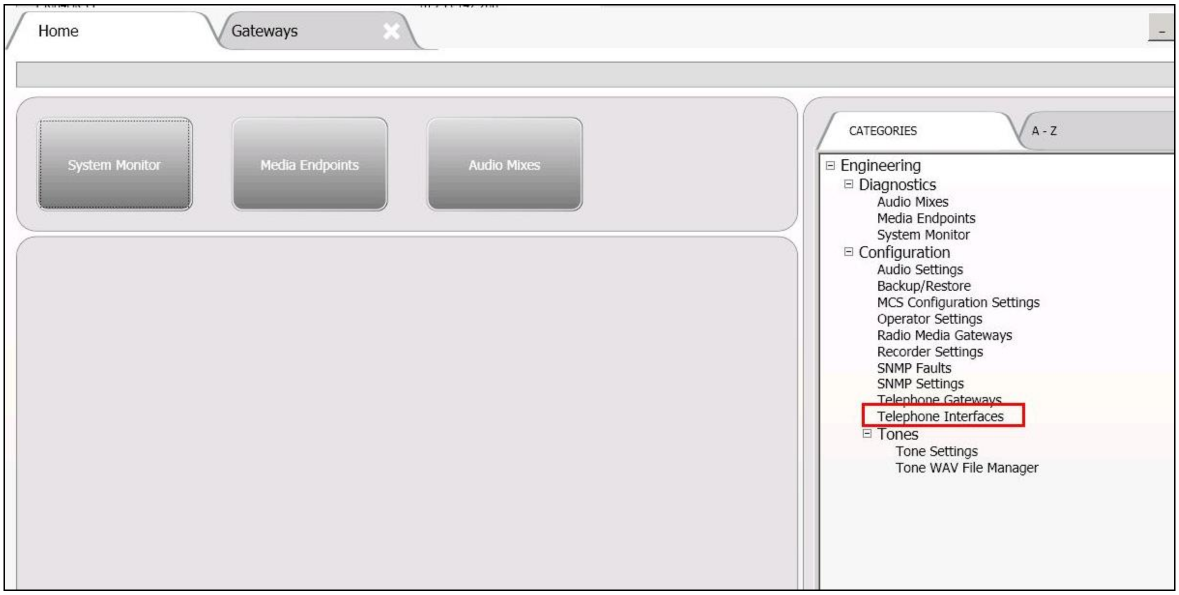


Id	IP Address
OSVSignalling	10.200.93.3
Rig5DRSS	10.253.144.206
Rig4DRSS	10.253.142.206
Rig6DRSS	10.253.146.206
AudioCodesM2000	10.253.144.125
AvayaSM	192.168.50.16
Avaya63SM	10.10.40.34

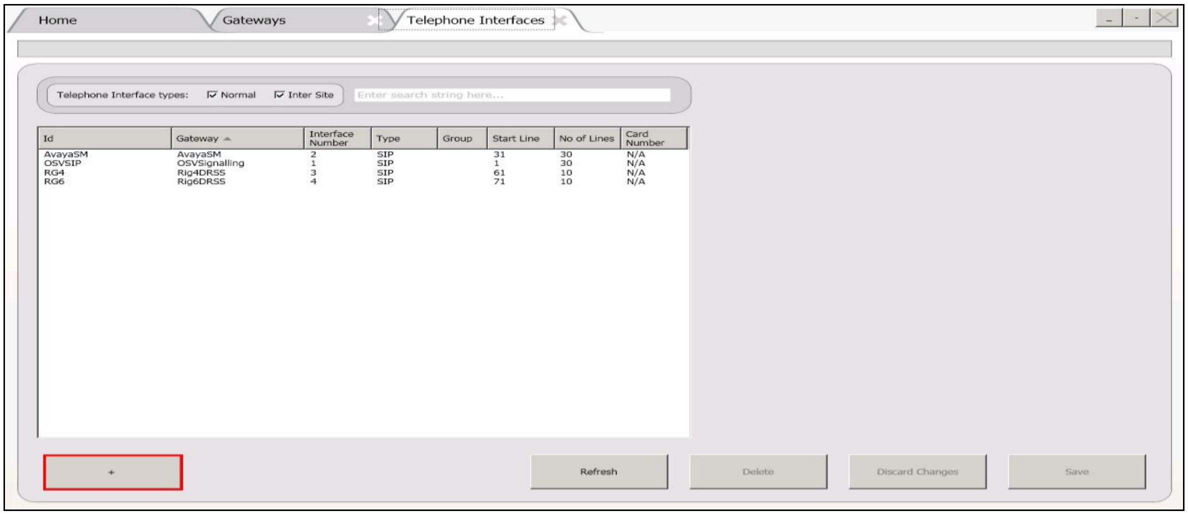
Gateway Id Avaya63SM

IP Address 10 . 10 . 40 . 34

Click on the **Home** tab and select **Telephone Interfaces** in the right column as highlighted below.



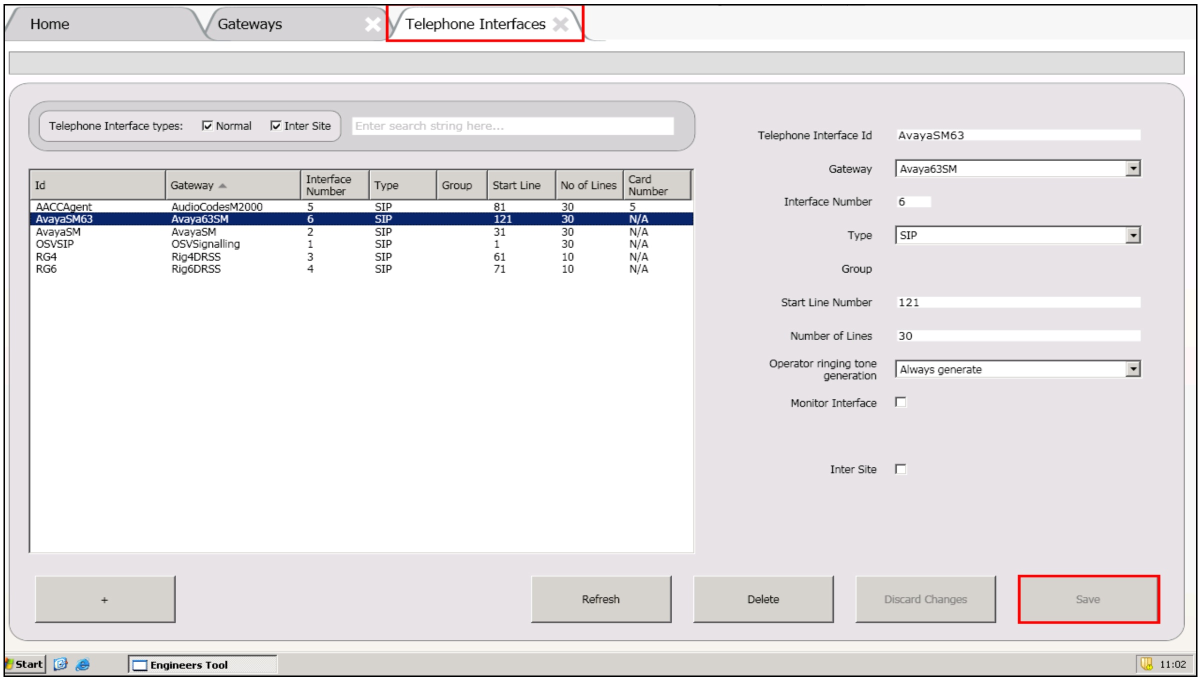
The **Telephone Interfaces** tab is opened. Select the **+** icon at the bottom left of the screen to add a new Telephone interface.



Telephone Interface types: ☑ Normal ☑ Inter Site

Id	Gateway	Interface Number	Type	Group	Start Line	No of Lines	Card Number
AvayaSM	AvayaSM	2	SIP		31	30	N/A
OSVSIP	OSVSignalling	1	SIP		1	30	N/A
RG4	Rig4DRSS	3	SIP		61	10	N/A
RG6	Rig6DRSS	4	SIP		71	10	N/A

All the information in the right column must be filled in. The screen below shows the information that was used during compliance testing. Click on **Save** at the bottom right of the screen once all the information has been entered correctly. Note, set the **Operator ringing tone generation** to **Always generate** only when there is no "early media" set on the PBX.



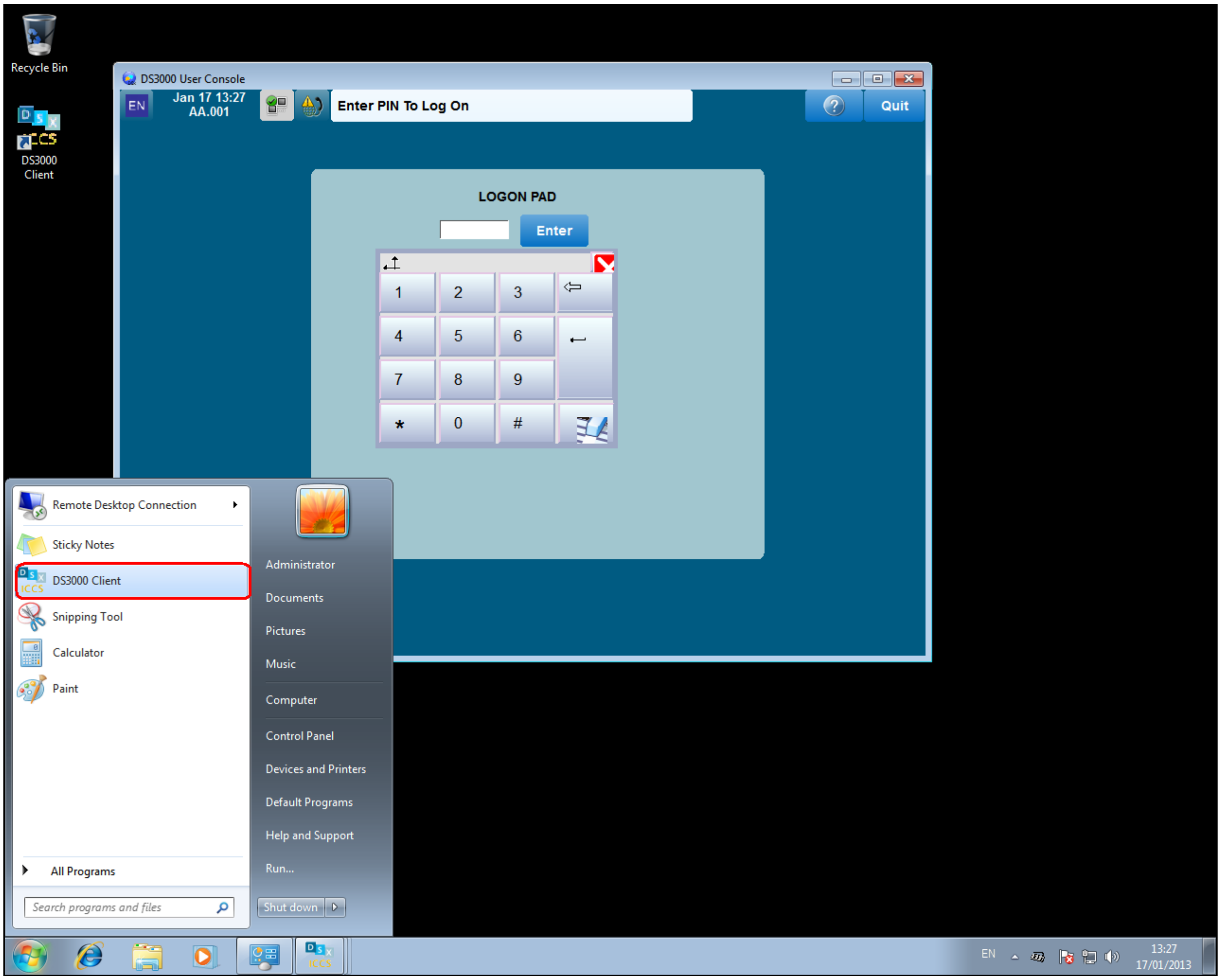
Telephone Interface types: ☑ Normal ☑ Inter Site

Id	Gateway	Interface Number	Type	Group	Start Line	No of Lines	Card Number
AACCAgent	AudioCodesM2000	5	SIP		81	30	5
AvayaSM63	Avaya63SM	6	SIP		121	30	N/A
AvayaSM	AvayaSM	2	SIP		31	30	N/A
OSVSIP	OSVSignalling	1	SIP		1	30	N/A
RG4	Rig4DRSS	3	SIP		61	10	N/A
RG6	Rig6DRSS	4	SIP		71	10	N/A

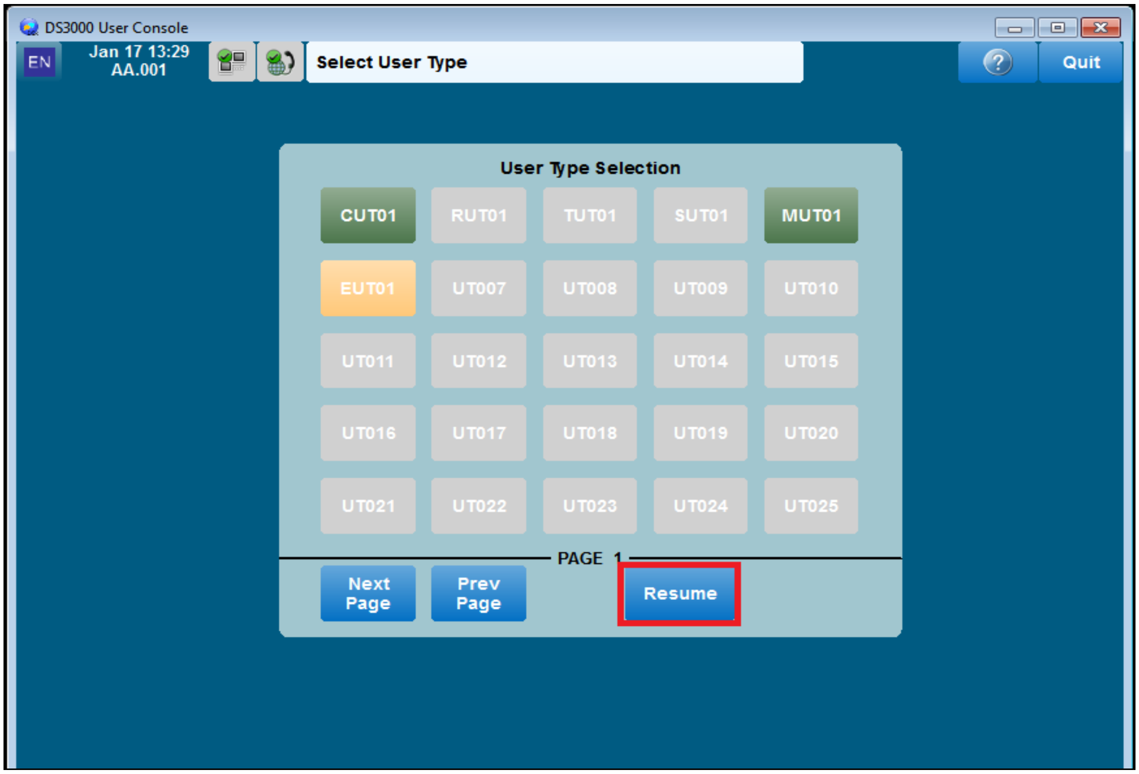
Telephone Interface Id: AvayaSM63
Gateway: Avaya63SM
Interface Number: 6
Type: SIP
Group:
Start Line Number: 121
Number of Lines: 30
Operator ringing tone generation: Always generate
Monitor Interface: □
Inter Site: □

7.2. Configure DS3000 extension numbers

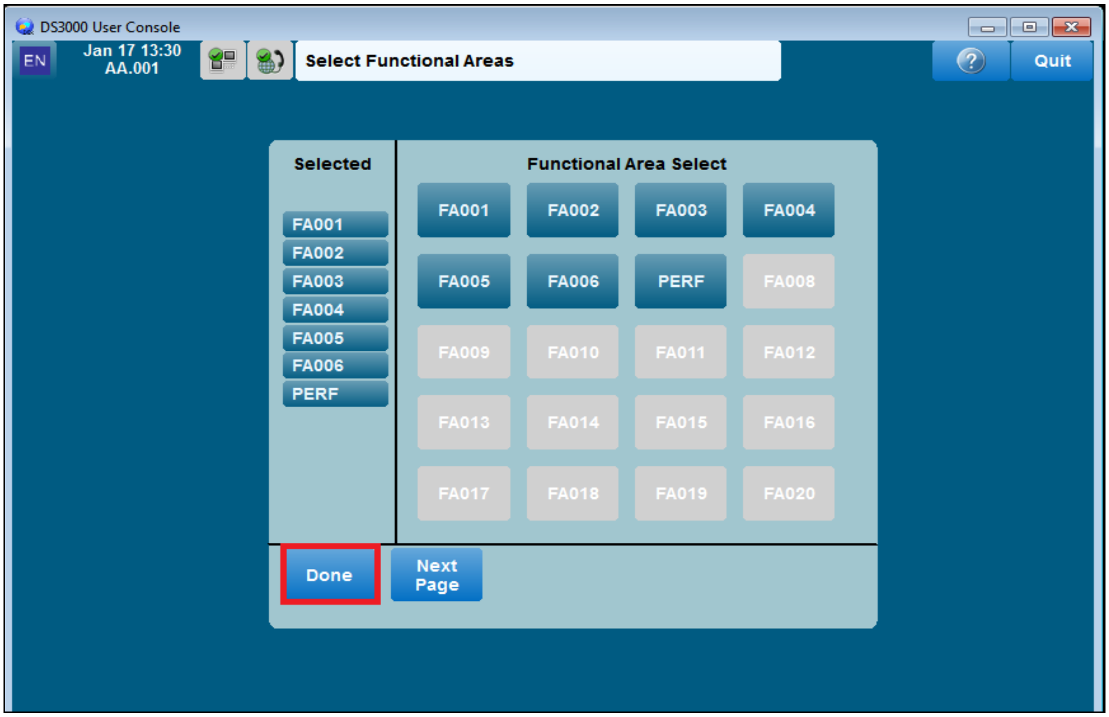
Open the **DS3000 Client** on the DS3000 Client machine. Enter the correct credentials on the **LOGON PAD**.



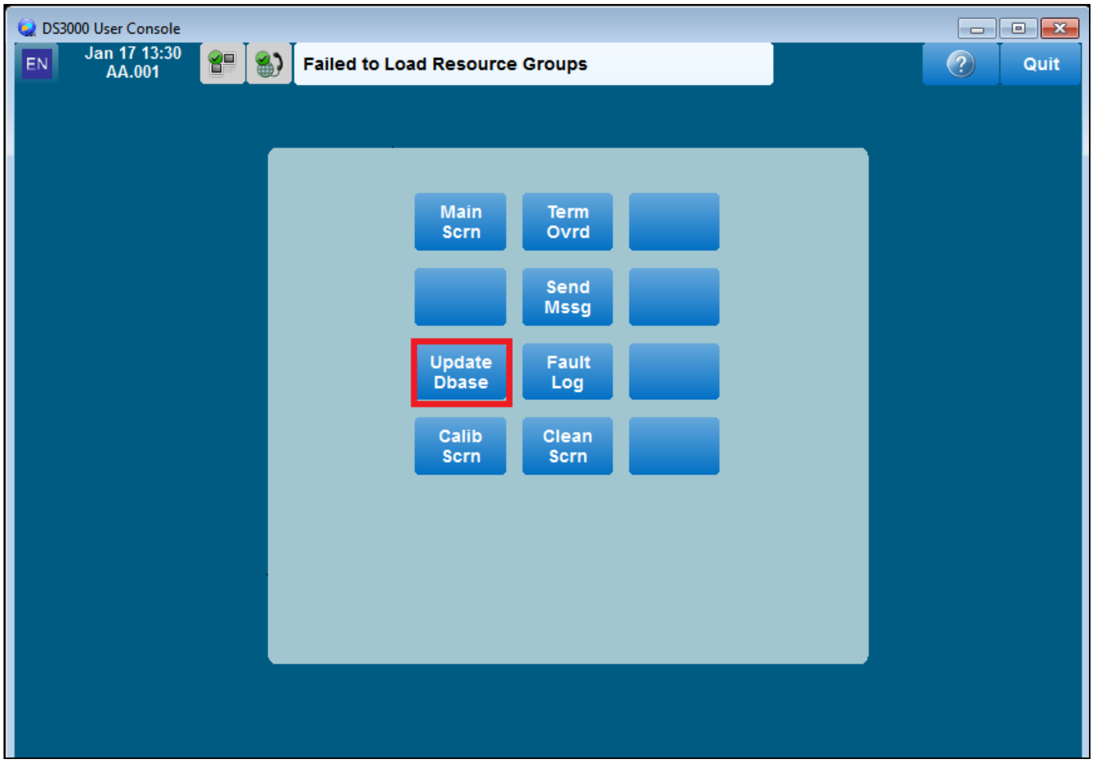
Click on **Resume** at the bottom of the screen as highlighted.



Select **Done** at the bottom of the screen as highlighted.

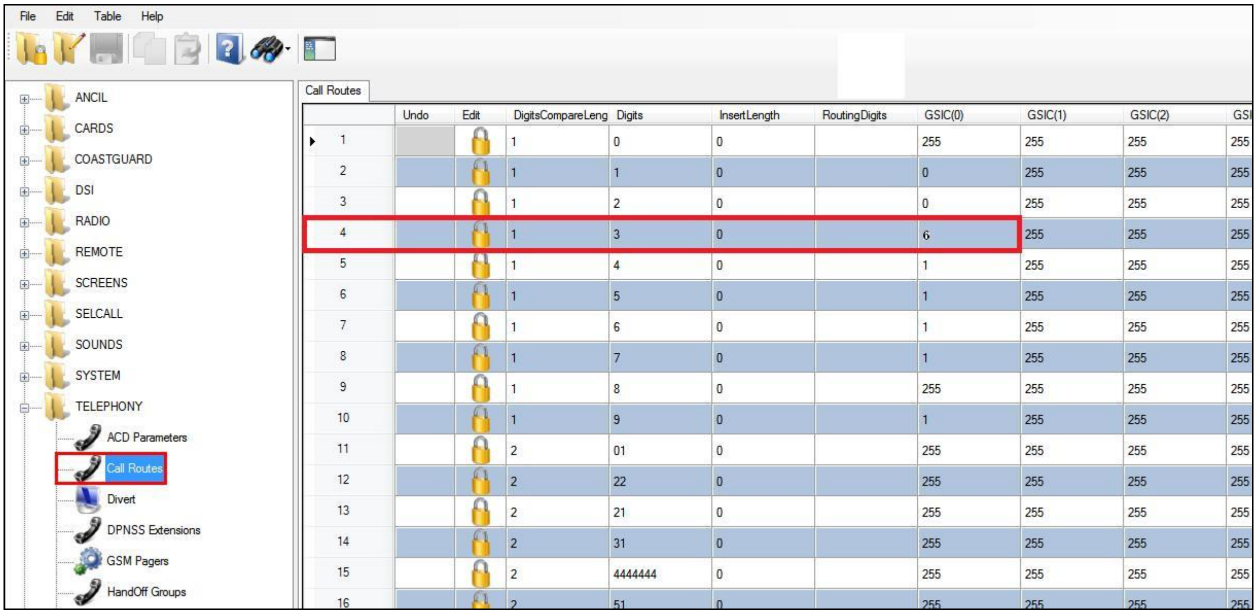


Click on the **UpdateDbase** button highlighted.



Failed to Load Resource Groups

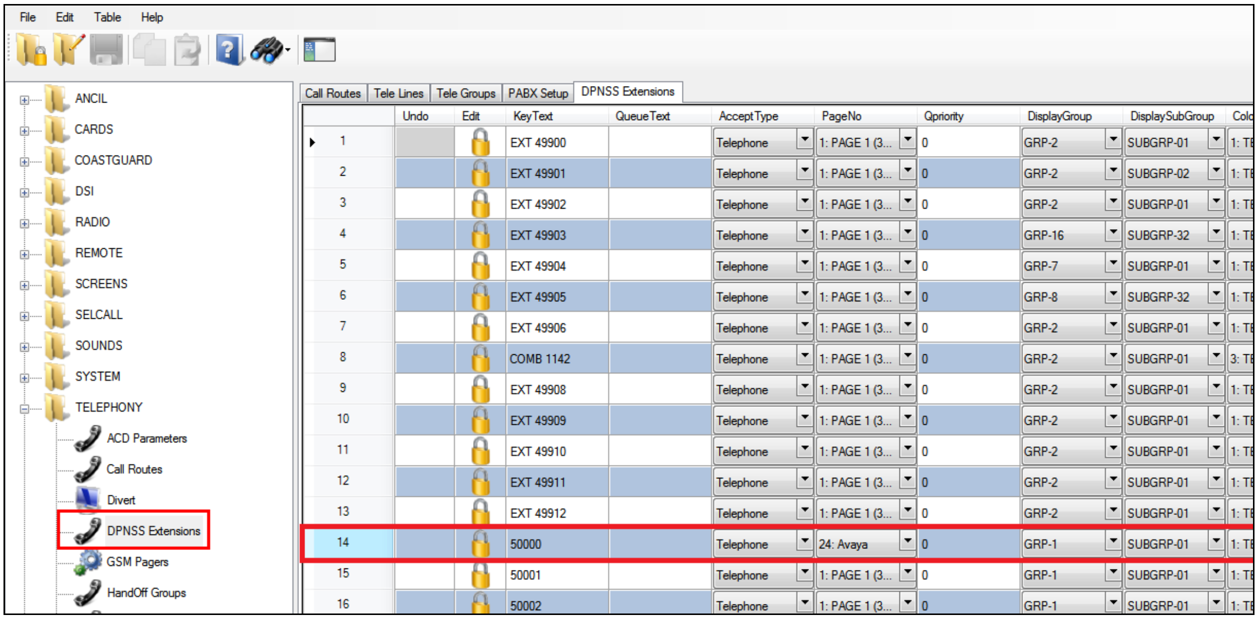
Click on the **Call Routes** icon highlighted in the left window. The highlighted row in the right window shows that when 3xxx is dialled, Interface 2 is used. Note: The interface numbers are as defined by the configuration entered in **Section 7.1**.



Call Routes

	Undo	Edit	DigitsCompareLeng	Digits	InsertLength	RoutingDigits	GSIC(0)	GSIC(1)	GSIC(2)	GSI
1		🔒	1	0	0		255	255	255	255
2		🔒	1	1	0		0	255	255	255
3		🔒	1	2	0		0	255	255	255
4		🔒	1	3	0		6	255	255	255
5		🔒	1	4	0		1	255	255	255
6		🔒	1	5	0		1	255	255	255
7		🔒	1	6	0		1	255	255	255
8		🔒	1	7	0		1	255	255	255
9		🔒	1	8	0		255	255	255	255
10		🔒	1	9	0		1	255	255	255
11		🔒	2	01	0		255	255	255	255
12		🔒	2	22	0		255	255	255	255
13		🔒	2	21	0		255	255	255	255
14		🔒	2	31	0		255	255	255	255
15		🔒	2	4444444	0		255	255	255	255
16		🔒	2	51	0		255	255	255	255

Select **DPNSS Extensions** in the left column highlighted. Note the entry highlighted is for DS3000 Extension **50000**. Ensure **Accept Type** is set to **Telephone.**



	Undo	Edit	KeyText	QueueText	AcceptType	PageNo	Qpriority	DisplayGroup	DisplaySubGroup	Colo
► 1		🔒	EXT 49900		Telephone	1: PAGE 1 (3...	0	GRP-2	SUBGRP-01	1: TE
2		🔒	EXT 49901		Telephone	1: PAGE 1 (3...	0	GRP-2	SUBGRP-02	1: TE
3		🔒	EXT 49902		Telephone	1: PAGE 1 (3...	0	GRP-2	SUBGRP-01	1: TE
4		🔒	EXT 49903		Telephone	1: PAGE 1 (3...	0	GRP-16	SUBGRP-32	1: TE
5		🔒	EXT 49904		Telephone	1: PAGE 1 (3...	0	GRP-7	SUBGRP-01	1: TE
6		🔒	EXT 49905		Telephone	1: PAGE 1 (3...	0	GRP-8	SUBGRP-32	1: TE
7		🔒	EXT 49906		Telephone	1: PAGE 1 (3...	0	GRP-2	SUBGRP-01	1: TE
8		🔒	COMB 1142		Telephone	1: PAGE 1 (3...	0	GRP-2	SUBGRP-01	3: TE
9		🔒	EXT 49908		Telephone	1: PAGE 1 (3...	0	GRP-2	SUBGRP-01	1: TE
10		🔒	EXT 49909		Telephone	1: PAGE 1 (3...	0	GRP-2	SUBGRP-01	1: TE
11		🔒	EXT 49910		Telephone	1: PAGE 1 (3...	0	GRP-2	SUBGRP-01	1: TE
12		🔒	EXT 49911		Telephone	1: PAGE 1 (3...	0	GRP-2	SUBGRP-01	1: TE
13		🔒	EXT 49912		Telephone	1: PAGE 1 (3...	0	GRP-2	SUBGRP-01	1: TE
14		🔒	50000		Telephone	24: Avaya	0	GRP-1	SUBGRP-01	1: TE
15		🔒	50001		Telephone	1: PAGE 1 (3...	0	GRP-1	SUBGRP-01	1: TE
16		🔒	50002		Telephone	1: PAGE 1 (3...	0	GRP-1	SUBGRP-01	1: TE

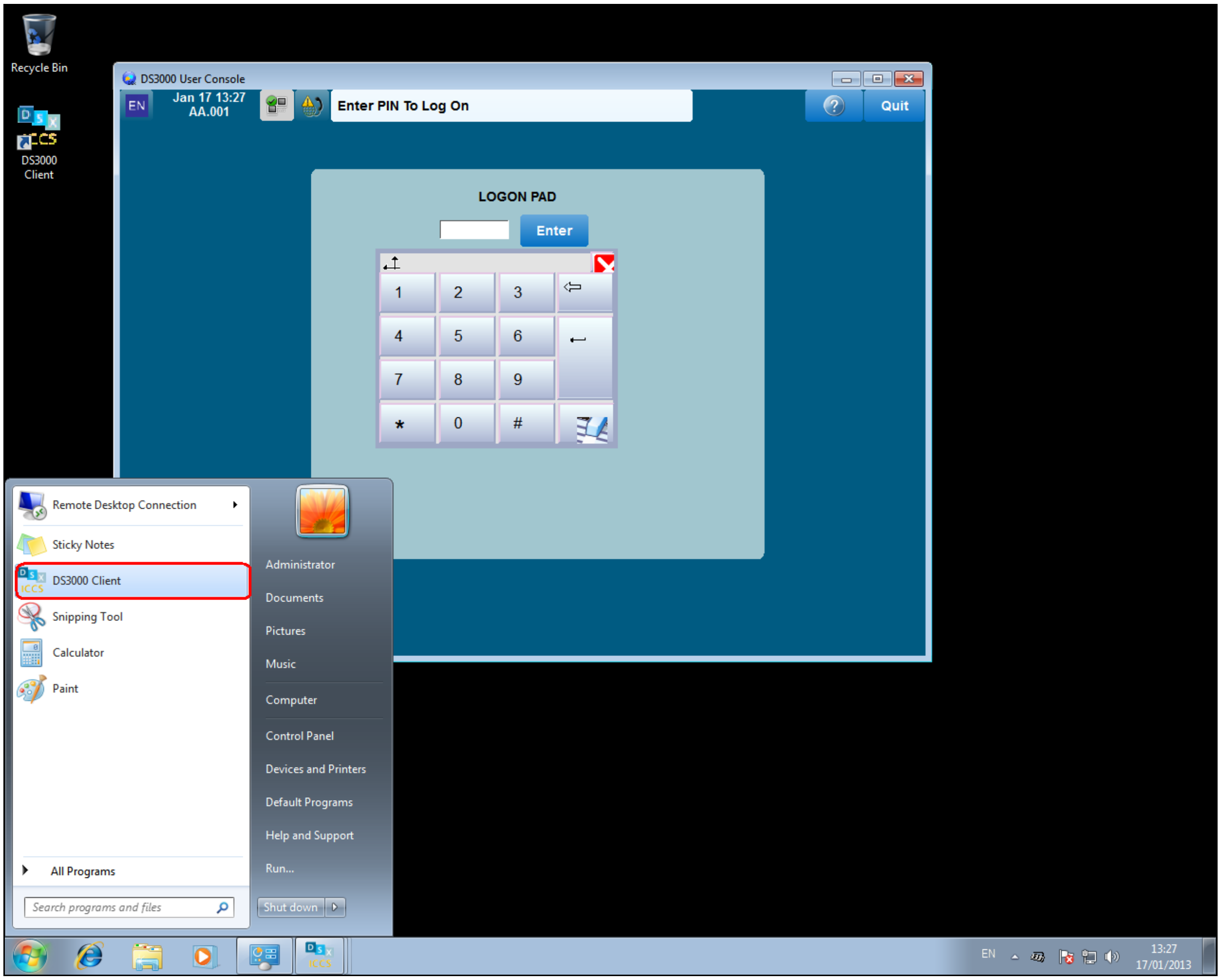
8. Verification Steps

The following steps can be taken to ensure that all connections between Capita's DS3000 Solution and the Avaya Solution is configured correctly.

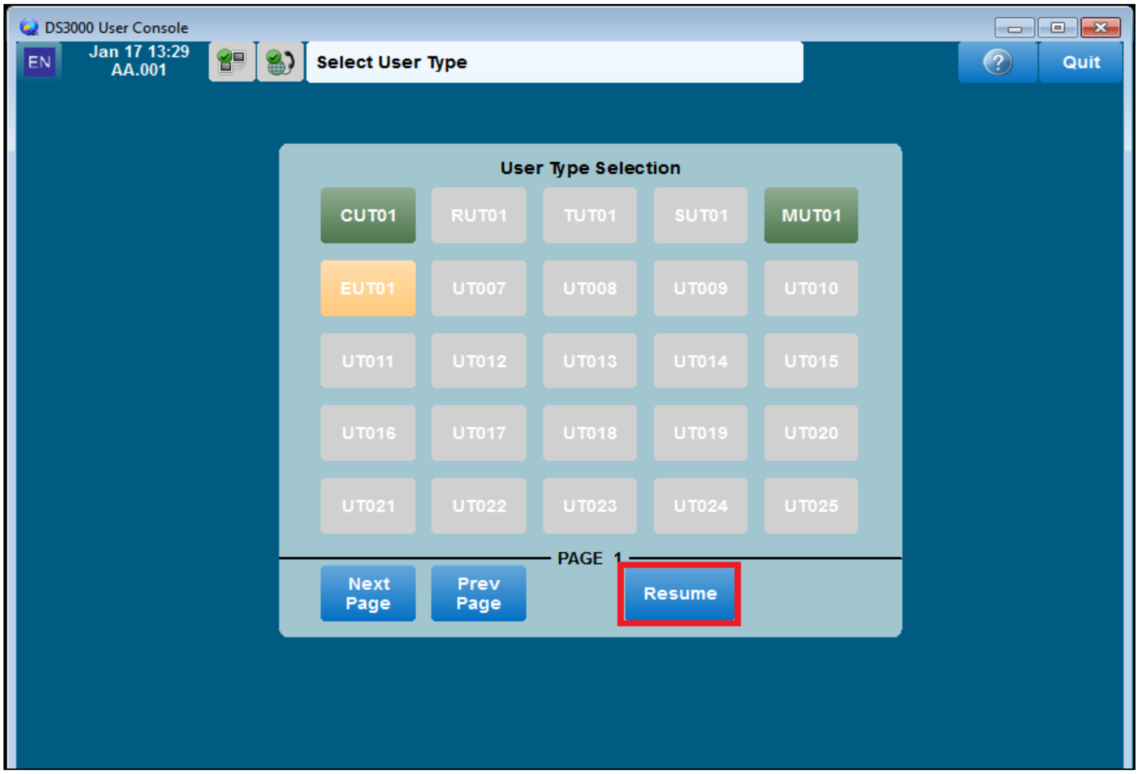
- Make a call to and from DS3000 and verify that the caller can be heard.

8.1. Verify that calls can be made to DS3000

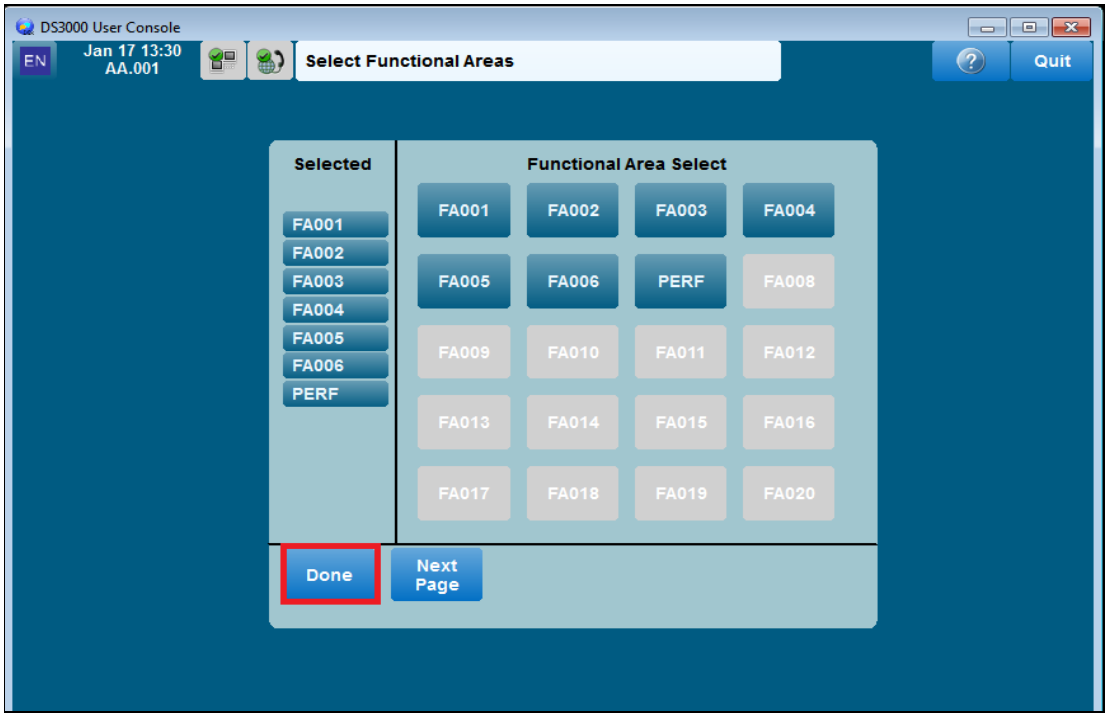
Open the **DS3000 Client** on the DS3000 Client machine. Enter the correct credentials on the **LOGON PAD**.



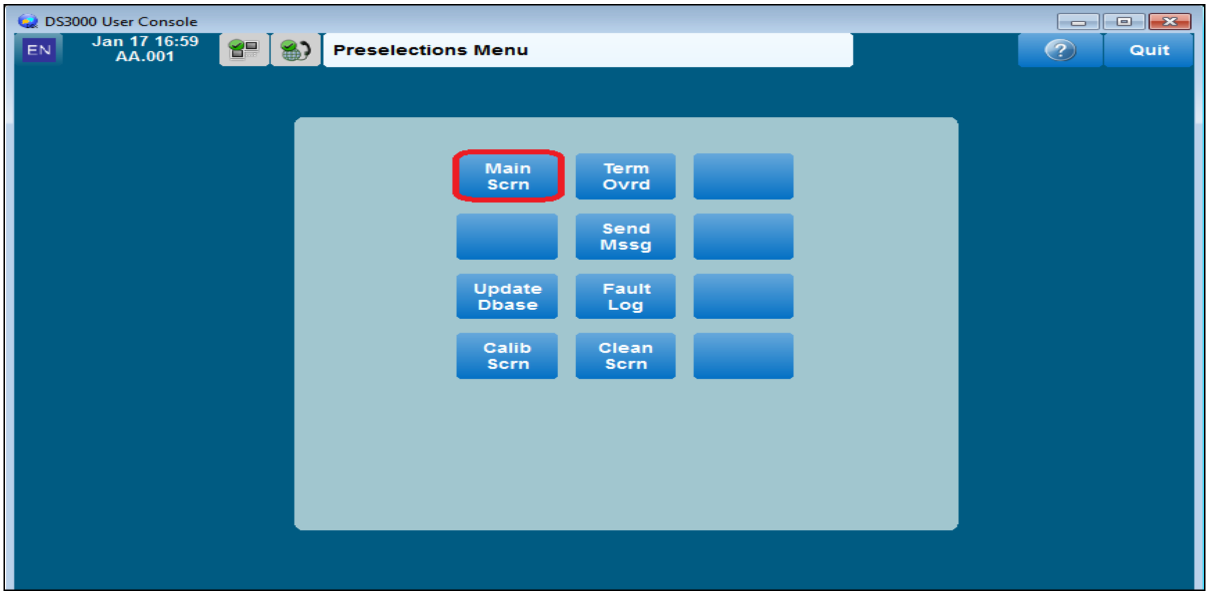
Click on **Resume** at the bottom of the screen as highlight.



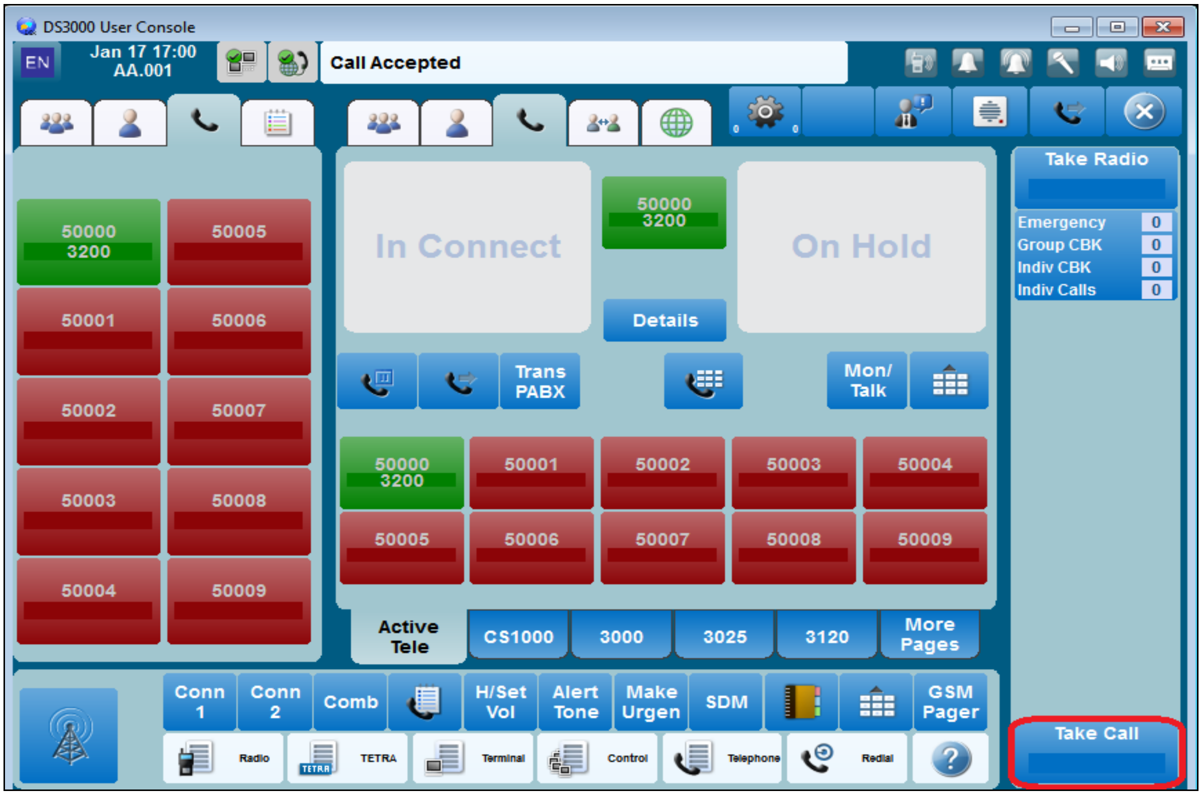
Select **Done** at the bottom of the screen as highlighted.



Click on the **Main Scrn** button highlighted below.



Once a call is presented to DS3000, the following screen should appear. Click on the **Take Call** button on the bottom right of the screen to take the call.



9. Conclusion

These Application Notes describe the configuration steps required for DS3000 from Capita Secure Information Solutions to successfully interoperate with Avaya Aura® Communication Manager R6.3 and Avaya Aura® Session Manager R6.3. Please refer to **Section 2.2** for test results and observations.

10. Additional References

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

[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 6.3, 03-603324

[4] *Application Notes for Configuring Capita Secure Information Solutions DS3000 with Avaya Aura® Session Manager R6.3 and Avaya Communication Server 1000E R7.5 using SIP Trunks*

Product documentation for DS3000 can be requested from Capita or may be downloaded from *http://www.capitasecureinformationsolutions.co.uk*

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.