Application Notes for configuring NEC IP DECT Access Points AP400 and NEC DECT Handsets with Avaya Aura® Communication Manager R7.0 and Avaya Aura® Session Manager R7.0 using TLS/SRTP – Issue 1.0

Abstract

These Application Notes describe the configuration steps for provisioning NEC's IP DECT Access Points and Handsets to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager.

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 NEC's IP DECT Access Point (AP400) and NEC´s DECT handsets to interoperate with Avaya Aura® Communication Manager R7.0 and Avaya Aura® Session Manager R7.0.

An NEC IP DECT solution typically consists of a windows based instance called DAP Controller that runs the IP DECT system software (DAP Configurator and DAP Manager), one or more DECT access points (DAP) AP400, DECT handsets (e.g. G566, I766, G966) and if needed a software based DMLS open interface for messaging and alarming. The DAP´s are connected to the IP network and get the needed power by using POE following 802.3af standard. Multiple NEC DECT access points (DAP) are tied together to build a single DECT system. The handsets are enrolled into that System using Digital Enhanced Cordless Technology (DECT). Each DAP is hosting (responsible for) a particular number of handsets although roaming/handover is possible across all DAPs. The DAPs are configured to register with Session Manager using Session Initiation Protocol (SIP). A single DAP will register multiple times against Session Manager on behalf of the handsets it is responsible for.

Each handset is configured as a SIP user on Avaya Aura® System Manager, using an Avaya 9608 SIP endpoint type on Avaya Aura® Communication Manager. The NEC DECT handsets behave as third-party SIP extensions (non AST device) integrated into the Avaya Aura® Core. They are able to make/receive internal calls, trunk calls, access the voicemail system and can take advantage of the telephony features provided from Communication Manager.

2. General Test Approach and Test Results

The interoperability compliance testing evaluates the ability of NEC DECT handsets to make and receive calls to and from Avaya H.323 and SIP deskphones as well as calls via connected trunks. Avaya Aura® Messaging was used to allow users to leave voicemail messages and to demonstrate Message Waiting Indication (MWI) was working on the NEC handsets.

NEC supports TCP/RTP but also TLS/SRTP. For more information on NEC using TCP/RTP please refer to the Application Notes titled *Application Notes for configuring NEC IP DECT Access Points AP400 and NEC DECT Handsets with Avaya Aura® Communication Manager R7.0 and Avaya Aura® Session Manager R7.0 using TCP/RTP*.

The primary goal of the Transport Layer Security (TLS) protocol is to provide privacy and data integrity between two communicating computer applications. When secured by TLS, connections between a client (e.g., NEC DAP) and a server (e.g., Session Manager) have one or more of the following properties:

- The connection is private because symmetric cryptography is used to encrypt the data transmitted. The keys for this symmetric encryption are generated uniquely for each connection and are based on a shared secret negotiated at the start of the session. The server and client negotiate the details of which encryption algorithm and cryptographic keys to use before the first byte of data is transmitted. The negotiation of a shared secret is both secure and reliable.

- The identity of the communicating parties can be authenticated using public-key cryptography. This authentication can be made optional, but is generally required for at least one of the parties (typically the server).
- The connection is reliable because each message transmitted includes a message integrity check using a message authentication code to prevent undetected loss or alteration of the data during transmission.

The Secure Real-time Transport Protocol (or SRTP) defines a profile of RTP (Real-time Transport Protocol), intended to provide encryption, message authentication and integrity, and replay protection to the RTP data in both unicast and multicast applications. Since RTP is closely related to RTCP (Real Time Control Protocol) which can be used to control the RTP session, SRTP also has a sister protocol, called Secure RTCP (or SRTCP); SRTCP provides the same security-related features to SRTP, as the ones provided by RTCP to RTP. Utilization of SRTP or SRTCP is optional to the utilization of RTP or RTCP; but even if SRTP/SRTCP is used, all provided features (such as encryption and authentication) are optional and can be separately enabled or disabled. The only exception is the message authentication feature which is indispensably required when using SRTCP.

Depending on the number of handsets and DAP´s used in the overall configuration, it might occur that one or more DAP´s are responsible for more than six handsets and need to register against Session Manager. Due to a limit within Session Manager that allows up to six simultaneous registrations from the same IP endpoint, a SIP Entity and an Entity Link are required for each NEC IP DECT Access Point, if more than six registrations are in use.

The setup of a SIP Entity must use the type “Endpoint Concentrator”. This is available starting with Session Manager Release 6.3.9 and above. This Endpoint Concentrator type allows up to 1000 connections from a single IP address against Session Manager.

In addition an Entity Link between the SIP Entity and Session Manager needs to be configured using the new connection policy, “Endpoint Concentrator”. The Endpoint Concentrator policy is an untrusted policy based on the current Default (endpoint) policy. That is, the requests arriving over the SIP entity link with the connection policy Endpoint Concentrator are challenged as for any other endpoint.

Note: SIP Link Monitoring is not available for SIP entities of type Endpoint Concentrator. 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 compliance testing included two particular use cases.

- Using a NEC DECT handset as the only device for one user.
- Using Multi Device Access (MDA) Capabilities of the Avaya Aura® Core to register an Avaya 96x1 SIP deskphone and a NEC DECT handset with the same number at the Aura® Core for one user.

The following features have been tested. Note that when applicable, all tests were performed between NEC DECT handsets and Avaya SIP deskphones, Avaya H.323 deskphones as well as PSTN endpoints.

- Basic Calls
- Calling Line Number / Name Identification
- Hold and Retrieve/Music on Hold
- Attended and Blind Transfer
- Call Forwarding Unconditional, No Reply and Busy
- Enhanced Call Forward
- Send All Calls / Coverage Path
- Call Waiting
- Limit Number of Concurrent Calls (LNCC)
- Call Park/Call Pickup
- Hunt-Group / Hunt-Group busy
- Automatic Callback
- CPN Block
- Priority Calling
- Teaming
- Different Ringtones (Internal, External, Priority, Intercom, Automatic Callback)
- Multi Party Conference (up to 6 parties) hosted via Communication Manager
- Direct IP-IP Media (Shuffling)
- Codec Support (G.711, G.729)
- Trunk-Calls (PSTN)
- COR restricted calls
- DTMF Support
- Message Waiting Indication

2.1.1. NEC DECT handset only

For this use case, there was just the NEC DECT handset registered as a SIP user against Session Manager. The features are either provided from the NEC DECT handset or by using Communication Manager. Communication Manager features are activated / deactivated by using a Feature Access Code (FAC) or by dialling an off-pbx-telephone Feature-Name-Extensions (FNE). The following table shows the tested features.

Feature	result	FAC / FNE	Comments
Incoming Calls	OK		
Outgoing Calls	OK		
Hold / Retrieve	OK		
Attended Transfer	OK		
Blind Transfer	OK		
Call Forwarding Unconditional	OK	FAC	
Call Forwarding No Reply	OK	FAC	
Call Forwarding Busy	OK	FAC	
Enhanced Call Forwarding Unconditional (for Internal, External, All calls)	OK	FAC	
Enhanced Call Forwarding No Reply (for Internal, External, All calls)	OK	FAC	
Enhanced Call Forwarding Busy (for Internal, External, All calls)	OK	FAC	
Send All Calls (SAC)	OK	FAC	
Coverage Path	OK		
Call waiting	OK		waiting call can be answered by pressing “*” on the handset
Limit Number of Concurrent Calls (LNCC)	OK	FAC	
Call Park / Unpark	OK	FAC	
Call Pickup	OK	FAC	
Team Button (passive)	OK		NEC DECT handset can be configured as a Team-Button member at other users. Status-Icon at watcher shows idle, ringing, in a call, active call forward to watcher
Hunt Group	OK		
Hunt Group busy	OK	FAC	
Automatic Callback	OK	FNE	
CPN Block	OK	FAC	
Priority Calling	OK	FAC	
Different Ringtone : Internal Call	OK		User can assign ringtone in handset
Different Ringtone : External Call	OK		User can assign ringtone in handset

Feature	result	FAC / FNE	Comments
Different Ringtone : Priority Call	OK		User can assign ringtone in handset
Different Ringtone : Intercom Call	OK		User can assign ringtone in handset
Different Ringtone : Automatic Callback (as the initiator)	OK		User can assign ringtone in handset
CM multiparty adhoc conference as host (up to 6 parties)	OK		NEC DECT handset supports the CM adhoc conference feature. User needs to press "*" key to add a participant
Music on Hold	OK		provided from Aura® Core
Direct IP-IP Media (Shuffling)	OK		
Codec Support G.711A, G.711M	OK		
Codec Support G.729A, G.729B	OK		NOTE: G.729 is supported between different subnets (e.g. locations) and requires DAP with DSP resources for codec handling
Trunk Calls incoming / outgoing	OK		tested with ISDN and SIP trunk
COR restricted calls	OK		
DTMF support	OK		
MWI support	OK		tested with Avaya Aura® Messaging voicemail system
SM down notification	OK		If SM is not reachable, the user gets a customizable notification on the display of the handset, when trying to make a call e.g. "No Telephonyservice"

2.1.2. Multi Device Access (MDA) using 96x1 SIP and NEC DECT handset

For this use case, there was an Avaya 96x1 SIP deskphone and one NEC DECT handset registered using the same number (SIP handle) against Session Manager. That allows the user to make and receive calls on both devices by using the same number (SIP handle).

In addition to the tested features in **Section 2.1.1**, the following features have been tested.

Feature	**result**	**FAC / FNE**	**Comments**
Incoming Calls	OK		Incoming calls ring on both devices and can be answered on each of them. Depending on the number of configured call-appearances (e.g. three) in CM, the user can have multiple calls. If the user is already active in a call on one device, additional calls can be answered on the second device.
Outgoing Calls	OK		Outgoing calls can be made independently on each of the two devices.
Hold / Retrieve	OK		Hold / Retrieve have been tested. Multiple calls for the same user, can be put on Hold / Retrieve on each device independently. That means Hold / Retrieve on one device, does not impact an active call on the other device.
Transfer Attended / Blind	OK		Call transfer has been tested. Multiple calls for the same user, can be transferred on each device independently. That means call transfer on one device, does not impact an active call on the other device.
Hunt-Group	OK		If the users extension is part of a hunt-group, incoming calls to that hunt-group ring on both devices and the user can answer the call on each of the devices.
Handover NEC DECT handset to Avaya 9600 deskphone	OK		If the user has an active call on the NEC DECT handset, the 9600 deskphone shows the particular call-appearance as active. The user can bridge into that call and continue the call on the deskphone.
Handover	N/A		Handing over a call from the

Feature	**result**	**FAC / FNE**	**Comments**
Avaya 9600 deskphone to NEC DECT handset			deskphone to the NEC DECT handset is currently not possible.
MWI support	OK		When a voicemail message is received for a user, the MWI indicator becomes activated on both devices. If the user listens / deletes the voicemail on one device, the MWI indicator becomes deactivated on both devices.

2.2. Test Results

All test cases passed successfully with the following observations noted during testing.

1. A SIP Entity with “Endpoint Concentrator” assigned was setup for the DAP’s that were present in the solution to register more than 6 devices from the same DAP.
2. When **Initial Direct IP-IP Media** was set to **Y** in the signaling group between Communication Manager and Session Manager, there was an issue observed for Blind Transfer. Party A calls to NEC handset (party B) and NEC handset performs a Blind Transfer to party C, which is a SIP handset or deskphone, when party C goes to pick up the call, the call is disconnected from party C.

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 11** of these Application Notes. Technical support for the NEC IP DECT product can be obtained through NEC global technical support by accessing the website http://www.nec-ipdect.com/Contact-7 or http://businessnet.nec-enterprise.com (which is available only for partners with authorized access).

3. Reference Configuration

Figure 1 shows the network topology during compliance testing. The NEC DECT handsets subscribe to the NEC DECT Access Points (DAP) which is placed on the LAN. The DECT handsets register with Session Manager in order to be able to make/receive calls to and from the Avaya H.323 and SIP deskphones as well as from Trunks (PSTN).

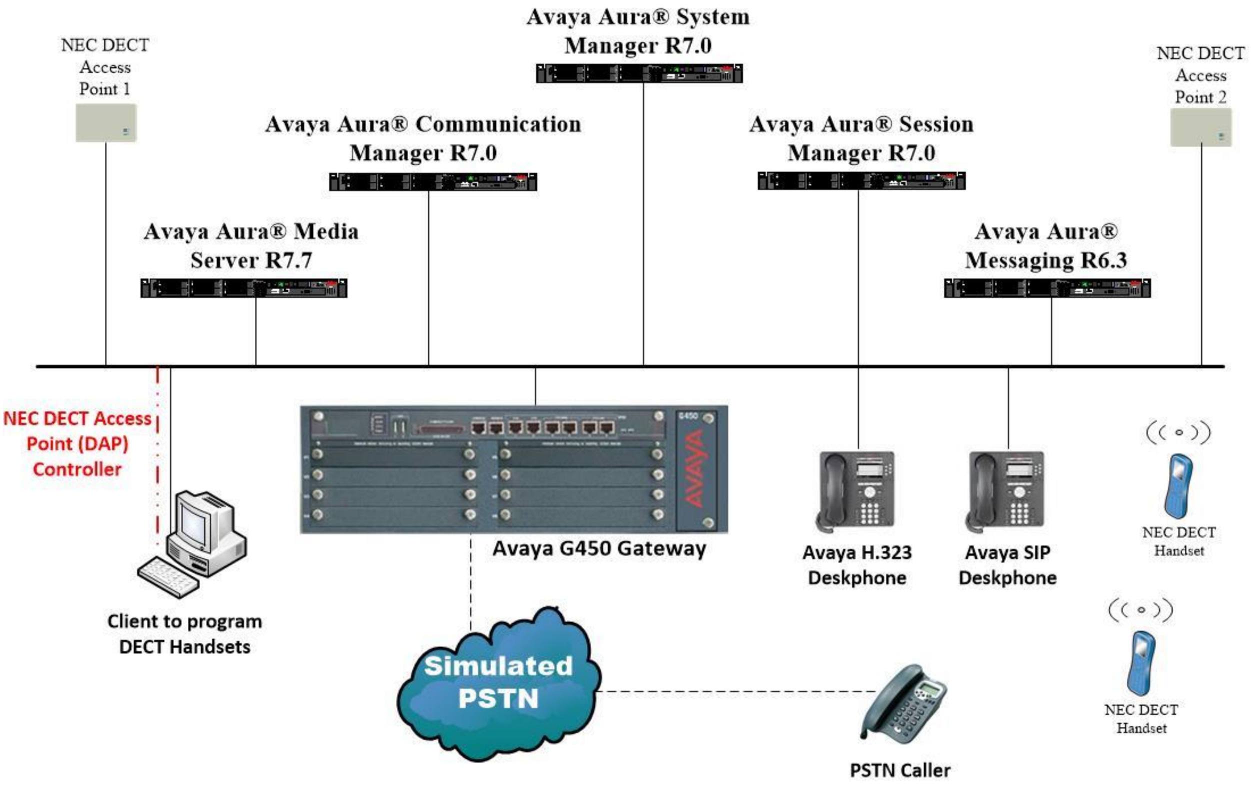

NEC DECT Access Point 1
Avaya Aura® System Manager R7.0
NEC DECT Access Point 2
Avaya Aura® Communication Manager R7.0
Avaya Aura® Session Manager R7.0
Avaya Aura® Media Server R7.7
Avaya Aura® Messaging R6.3
NEC DECT Access Point (DAP) Controller
Avaya G450 Gateway
Avaya H.323 Deskphone
Avaya SIP Deskphone
NEC DECT Handset
Client to program DECT Handsets
Simulated PSTN
NEC DECT Handset
PSTN Caller

Figure 1: Network Solution of NEC DECT Handsets with Avaya Aura® Communication Manager R7.0 and Avaya Aura® Session Manager R7.0

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 server	System Manager 7.0.1.0 Build No. - 7.0.0.0.16266 Software Update Revision No: 7.0.1.0.064859 Feature Pack 1
Avaya Aura® Session Manager running on a virtual server	Session Manager R7.0 SP1 Build No. – 7.0.1.0.701007
Avaya Aura® Communication Manager running on a virtual server	R7.0 R017x.00.0.441.0 00.0.441.0-23012
Avaya Media Server running on a virtual server	Media Server SYSTEM R7.7.0.8 Media Server R7.7.0.200
Avaya G450 Gateway	37.19.0 /1
Avaya Aura® Messaging running on a virtual server	R6.3.3
Avaya 9608 H323 Deskphone	96x1 H323 Release 6.6.028
Avaya 9608 SIP Deskphone	96x1 SIP Release 7.0.0.39
DAP Controller software running on Windows 2012 virtual server	Pre Release of R6.41. Release R6.41 is planned to be GA by the end of September 2016
NEC DECT Access Point	Pre Release of R6.41. Release R6.41 is planned to be GA by the end of September 2016
NEC DECT Handset NEC G566 NEC DECT Handset NEC I766	1.10.00.01 1.10.00.02

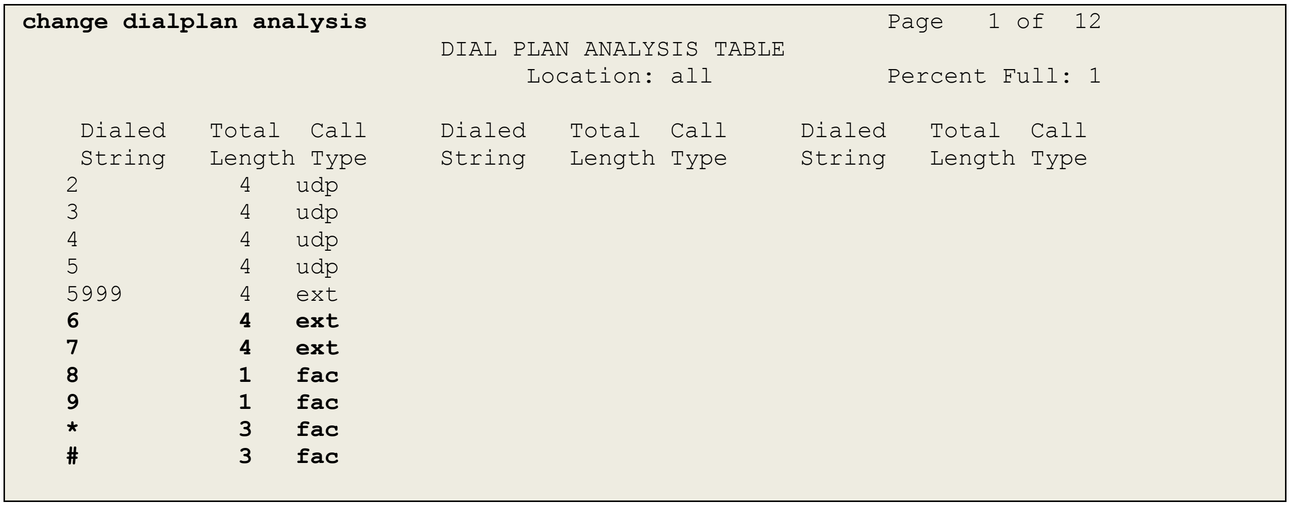
5. Configure Avaya Aura® Communication Manager

It is assumed that a fully functioning Communication Manager is in place with the necessary licensing and with a SIP Trunk in place to Session Manager. For further information on the configuration of Communication Manager please see **Section 11** of these Application Notes. The following sections go through the following.

- Dial Plan Analysis.
- Feature Access Codes (FAC).
- Off-pbx-telephone feature-name-extensions (FNE).
- Class of Service (COS).
- Network Region.
- IP Codec.
- Coverage Path/Hunt Group.

5.1. Configure Dial Plan Analysis

Use the **change dialplan analysis** command to configure the dial plan using the parameters shown below. Extension numbers (**ext**) are those beginning with **6** and **7**. Feature Access Codes (**fac**) use digits **8** and **9** or * and **#**.



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

    Dialed   Total  Call     Dialed   Total  Call     Dialed   Total  Call
    String   Length Type     String   Length Type     String   Length Type
   2           4   udp
   3           4   udp
   4           4   udp
   5           4   udp
   5999        4   ext
   6           4   ext
   7           4   ext
   8           1   fac
   9           1   fac
   *           3   fac
   #           3   fac
```

5.2. Configure Feature Access Codes (FAC)

Use the **change feature-access-codes** command to configure access codes which can be entered from NEC handsets to activate / deactivate Communication Manager telephony features. These access codes must be compatible with the dial plan described in **Section 5.1**. The Feature access codes shown below are what were configured during compliance testing.

```
change feature-access-codes                                  Page   1 of  10
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code: *11
         Abbreviated Dialing List2 Access Code: *12
         Abbreviated Dialing List3 Access Code: *13
Abbreviated Dial - Prgm Group List Access Code: *10
                      Announcement Access Code: *27
                       Answer Back Access Code: #02
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation: *05    Deactivation: #05
Call Forwarding Activation Busy/DA: *03    All: *04    Deactivation: #04
   Call Forwarding Enhanced Status: *73    Act: *74    Deactivation: #74
                         Call Park Access Code: *02
                       Call Pickup Access Code: *09
CAS Remote Hold/Answer Hold-Unhold Access Code:
                  CDR Account Code Access Code: *14
                        Change COR Access Code:
                   Change Coverage Access Code:
            Conditional Call Extend Activation:        Deactivation:
                   Contact Closure   Open Code:          Close Code:
```

```
change feature-access-codes                                  Page   2 of  10
                               FEATURE ACCESS CODE (FAC)
                   Contact Closure  Pulse Code:
        Customer Telephone Activation (#* and):
                  Data Origination Access Code:
                      Data Privacy Access Code:
              Directed Call Pickup Access Code: *29
       Directed Group Call Pickup  Access Code:
     Emergency Access to Attendant Access Code:
        EC500 Self-Administration Access Codes: *61     *62     *63     *64
                     Enhanced EC500 Activation: *60    Deactivation: #60
           Enterprise Mobility User Activation:        Deactivation:
  Extended Call Fwd Activate Busy D/A      All: *06    Deactivation: #06
        Extended Group Call Pickup Access Code: *99
               Facility Test Calls Access Code:
                             Flash Access Code:
             Group Control Restrict Activation:        Deactivation:
                    Hunt Group Busy Activation: *30    Deactivation: #30
                              ISDN Access Code:
                Last Number Dialed Access Code: *08
     Leave Word Calling Message Retrieval Lock: *15
   Leave Word Calling Message Retrieval Unlock: #15
```

```
change feature-access-codes                                  Page   3 of  10
                               FEATURE ACCESS CODE (FAC)
             Leave Word Calling Send A Message: *16
           Leave Word Calling Cancel A Message: #16
   Limit Number of Concurrent Calls Activation: *18    Deactivation: #18
               Malicious Call Trace Activation: *17    Deactivation: #17
         Meet-me Conference Access Code Change:
          Message Sequence Trace (MST) Disable:

 PASTE (Display PBX data on Phone) Access Code: *28
  Personal Station Access (PSA) Associate Code: *20    Dissociate Code: #20
        Per Call CPN Blocking Code Access Code: *24
      Per Call CPN Unblocking Code Access Code: #24
                    Posted Messages Activation:        Deactivation:
                  Priority Calling Access Code: *07
                           Program Access Code: *00

       Refresh Terminal Parameters Access Code: #28
              Remote Send All Calls Activation: #11    Deactivation:
               Self Station Display Activation:
                     Send All Calls Activation: *01    Deactivation: #01
         Station Firmware Download Access Code:
```

5.3. Configure off-pbx-telephone feature-name-extensions (FNE)

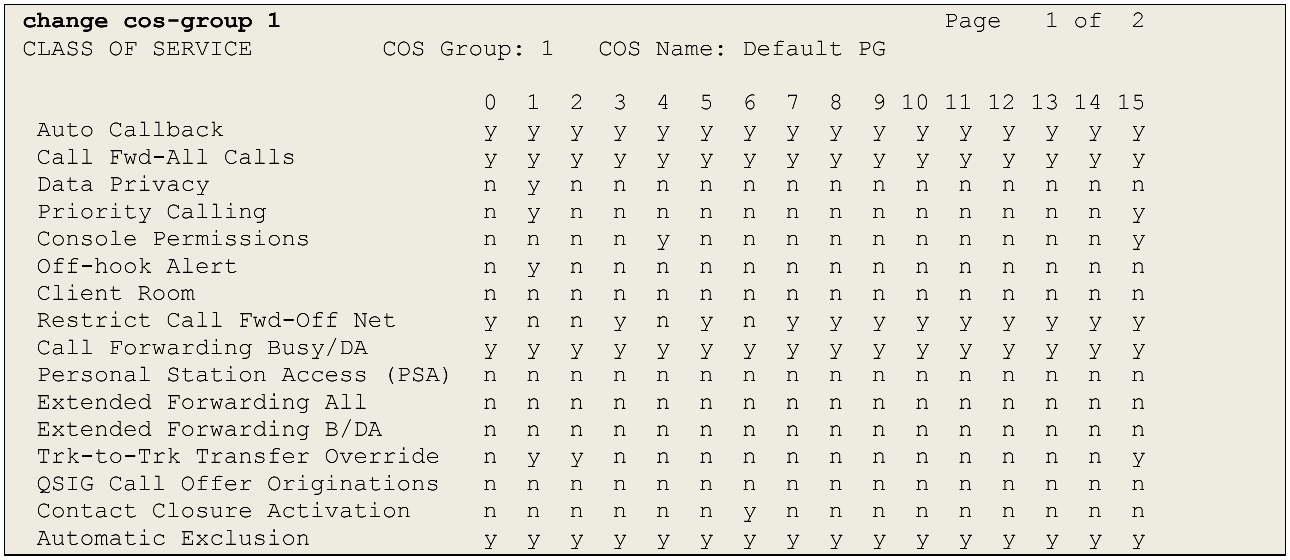
Use the **change off-pbx-telephone feature-name-extensions** command to configure feature-name-extensions (FNE) which can be entered from NEC handsets to activate / deactivate Communication Manager telephony features. These FNE must be compatible with the dial plan described in **Section 5.1**. The FNE shown below are what were configured during compliance testing.

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

        Active Appearance Select:
             Automatic Call Back: 7800
      Automatic Call-Back Cancel:
                Call Forward All:
     Call Forward Busy/No Answer:
             Call Forward Cancel:
                       Call Park: 7888
           Call Park Answer Back: 7999
                    Call Pick-Up: 7998
            Calling Number Block:
          Calling Number Unblock:
  Conditional Call Extend Enable:
 Conditional Call Extend Disable:
             Conference Complete:
            Conference on Answer:
           Directed Call Pick-Up:
           Drop Last Added Party:
```

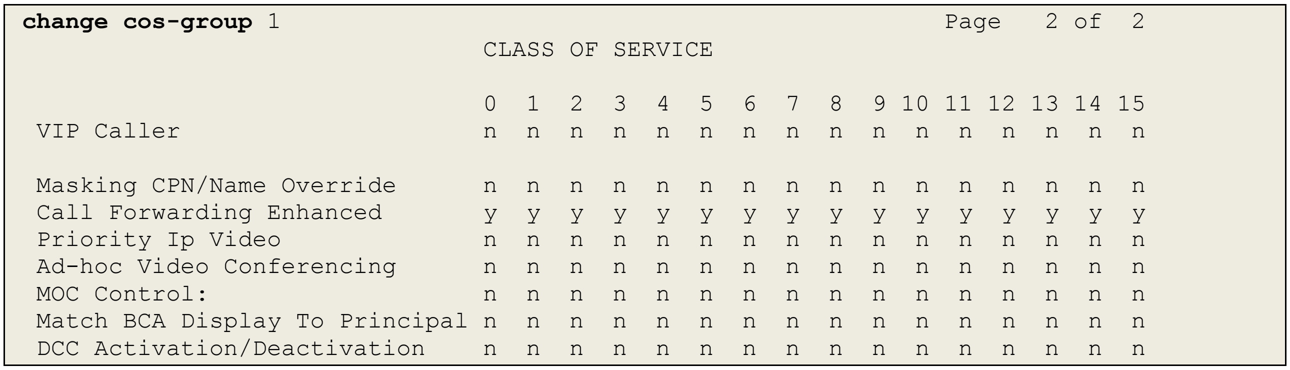
Note: Automatic Call Back feature is only available via FNE to the NEC DECT handset. An “auto-cback” feature-button needs to be assigned to that user (station) to enable the feature.

5.4. Configure Class of Service (COS)

Use the **change cos-group x** (where x is the cos-group to be configured) command to configure the class of service for the users. Via COS you can allow / deny particular features for a group of users. Each user is assigned to one COS. During compliance testing the COS 1 was assigned to the stations.



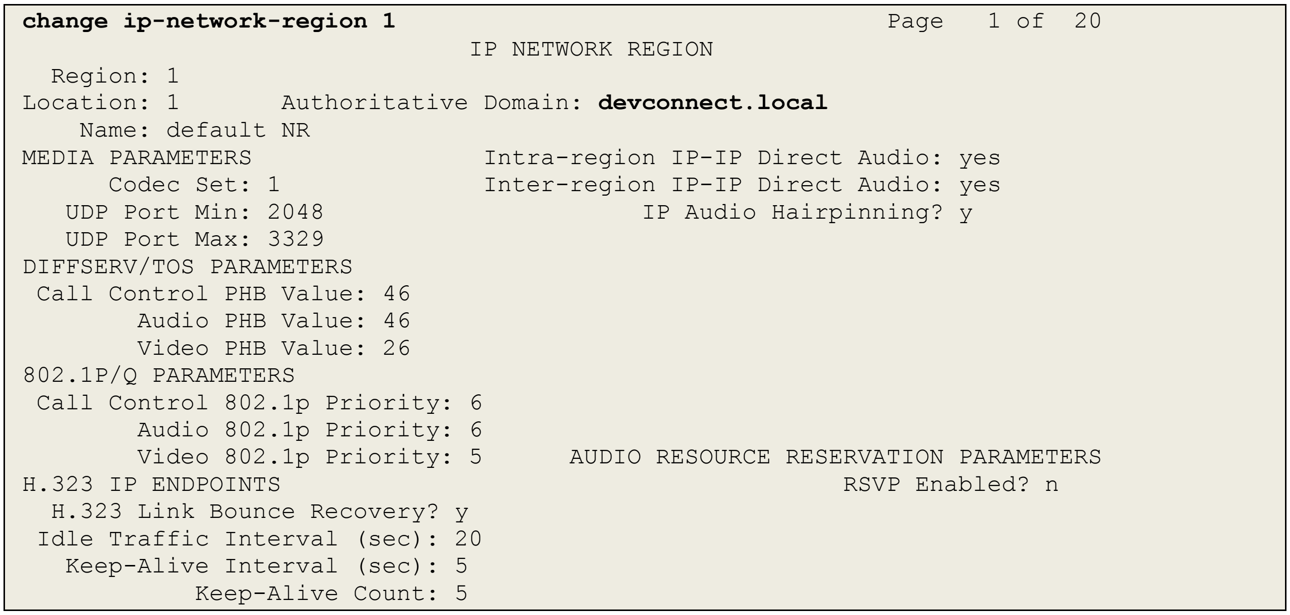
```
change cos-group 1                                              Page   1 of  2
CLASS OF SERVICE         COS Group: 1   COS Name: Default PG

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



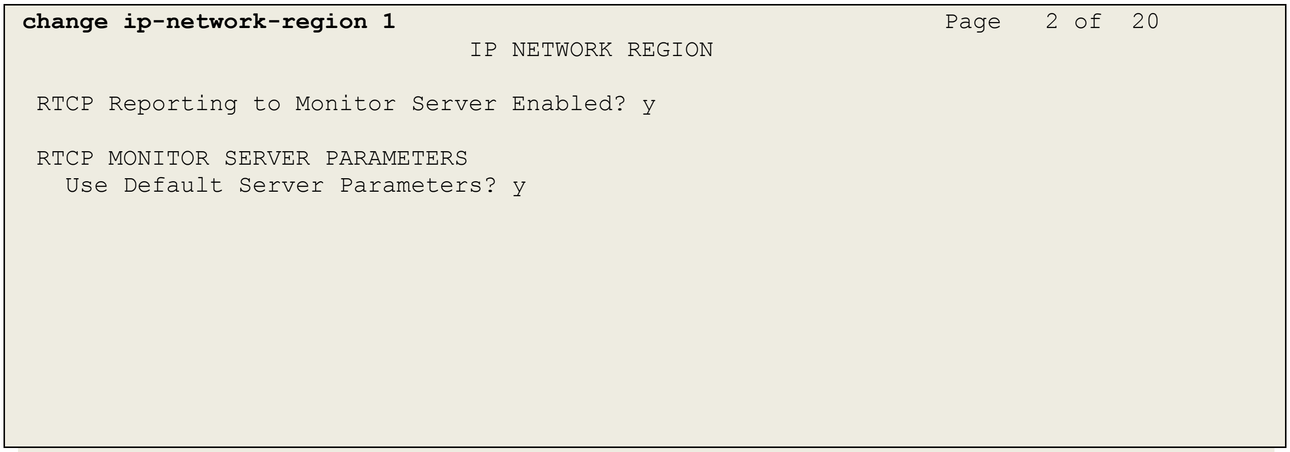
```
change cos-group 1                                              Page   2 of  2
                                CLASS OF SERVICE

                                0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15
 VIP Caller                     n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n

 Masking CPN/Name Override      n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Call Forwarding Enhanced       y  y  y  y  y  y  y  y  y  y  y  y  y  y  y  y
 Priority Ip Video              n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Ad-hoc Video Conferencing      n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 MOC Control:                   n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Match BCA Display To Principal n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 DCC Activation/Deactivation    n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
```

5.5. Configure Network Region

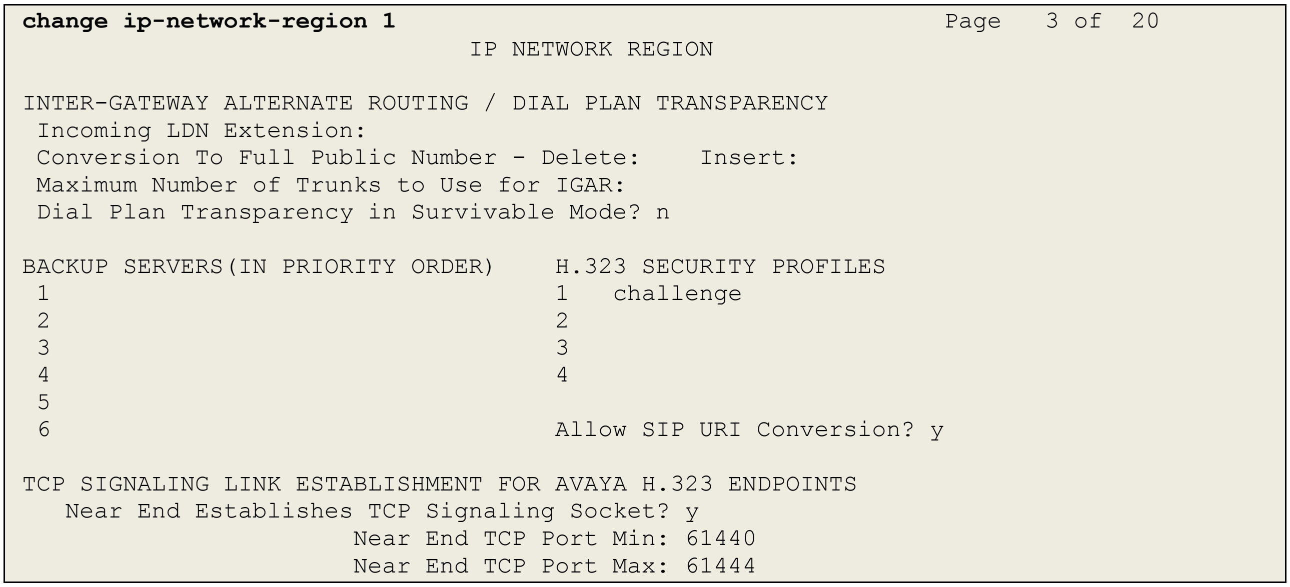
Use the **change ip-network-region x** (where x is the network region to be configured) command to assign an appropriate domain name to be used by Communication Manager, in the example below **devconnect.local** is used. Note this domain is also configured in **Section 6.1** of these Application Notes.



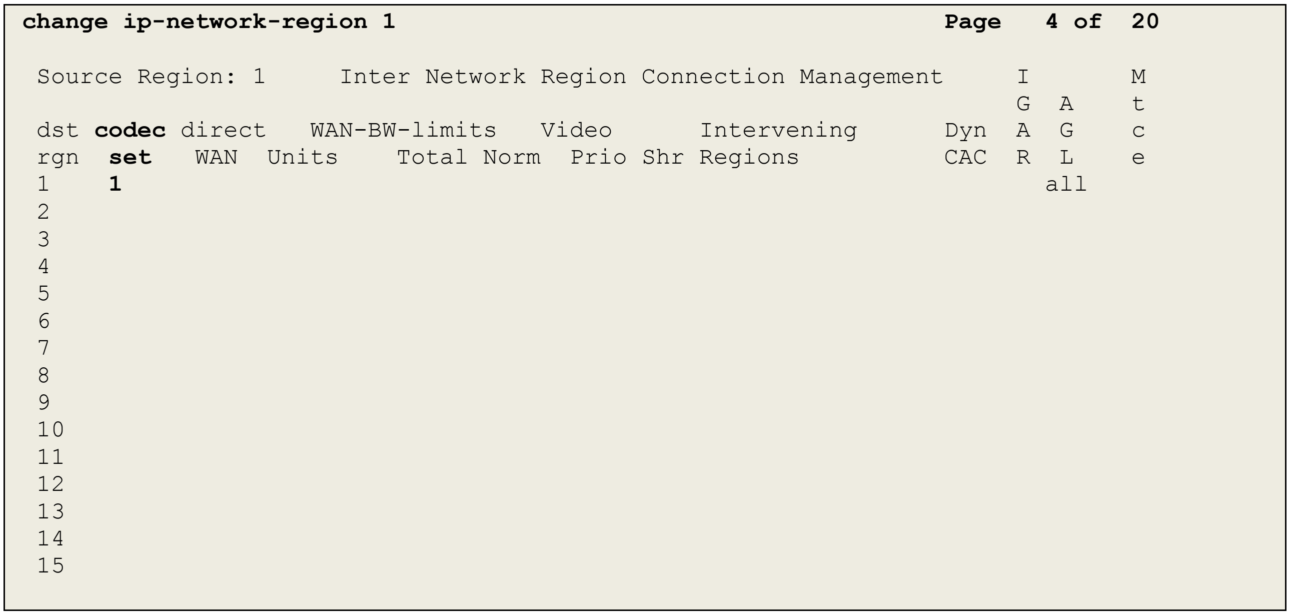
```
change ip-network-region 1                                  Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: devconnect.local
    Name: default NR
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? y
   UDP Port Max: 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
```



```
change ip-network-region 1                                      Page   2 of  20
                               IP NETWORK REGION

 RTCP Reporting to Monitor Server Enabled? y

 RTCP MONITOR SERVER PARAMETERS
   Use Default Server Parameters? y
```



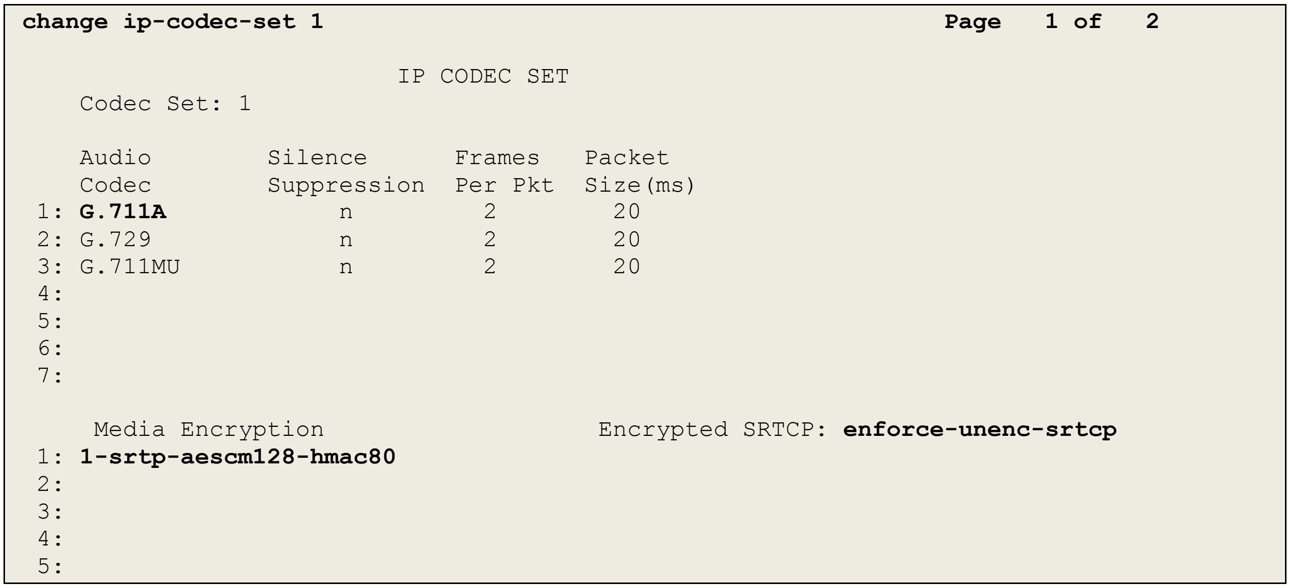
```
change ip-network-region 1                                      Page   3 of  20
                               IP NETWORK REGION

INTER-GATEWAY ALTERNATE ROUTING / DIAL PLAN TRANSPARENCY
 Incoming LDN Extension:
 Conversion To Full Public Number - Delete:    Insert:
 Maximum Number of Trunks to Use for IGAR:
 Dial Plan Transparency in Survivable Mode? n

BACKUP SERVERS(IN PRIORITY ORDER)    H.323 SECURITY PROFILES
 1                                   1   challenge
 2                                   2
 3                                   3
 4                                   4
 5
 6                                   Allow SIP URI Conversion? y

TCP SIGNALING LINK ESTABLISHMENT FOR AVAYA H.323 ENDPOINTS
   Near End Establishes TCP Signaling Socket? y
                       Near End TCP Port Min: 61440
                       Near End TCP Port Max: 61444
```



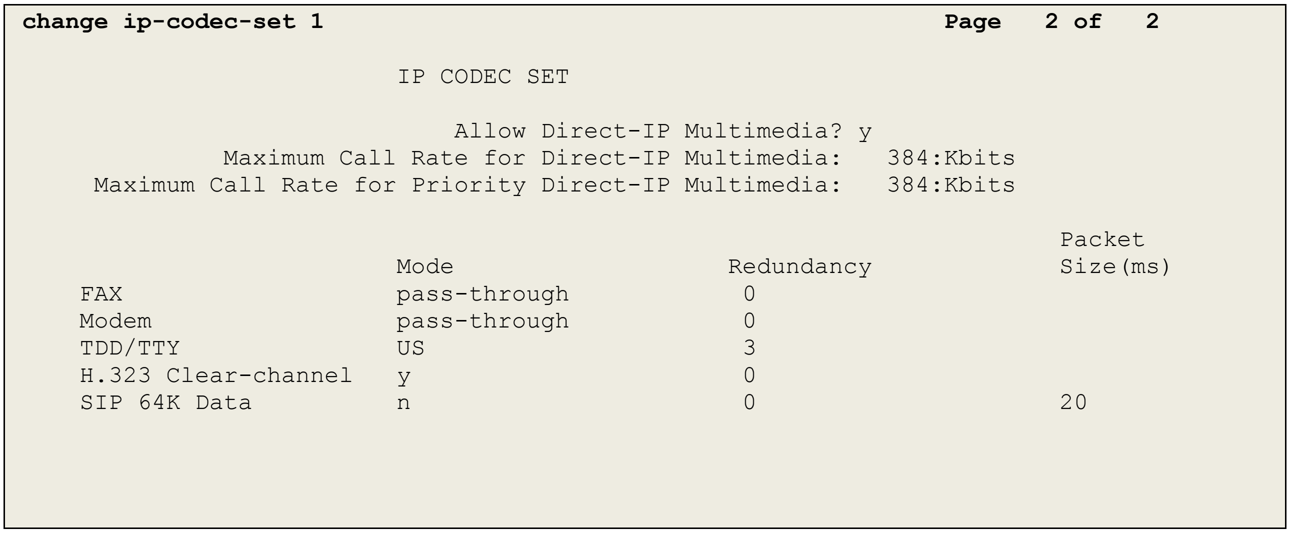
```
change ip-network-region 1                                      Page   4 of  20

 Source Region: 1     Inter Network Region Connection Management     I       M
                                                                     G  A    t
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G    c
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L    e
 1    1                                                                all
 2
 3
 4
 5
 6
 7
 8
 9
 10
 11
 12
 13
 14
 15
```

5.6. Configure IP-Codec

Use the **change ip-codec-set x** (where x is the ip-codec set used) command to designate a codec set compatible with the NEC Handsets, which support both **G.711** and **G.729**. Multiple codecs may be specified in the **IP Codec Set** form in order of preference; the example below includes **G.711A** (a-law), which is supported by NEC.
Note the **Media Encryption** has been set to **1-srtp-aescm128-hmac80**. This is the encryption that is support by NEC and must be set correctly on each side to allow secure RTP (SRTP). In order for SRTP to work properly, **Encrypted SRTCP** needed to be set to **enforce-unenc-srtcp** as shown below.



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

                          IP CODEC SET
    Codec Set: 1

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

     Media Encryption                    Encrypted SRTCP: enforce-unenc-srtcp
 1: 1-srtp-aescm128-hmac80
 2:
 3:
 4:
 5:
```



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

                          IP CODEC SET

                              Allow Direct-IP Multimedia? y
              Maximum Call Rate for Direct-IP Multimedia:   384:Kbits
     Maximum Call Rate for Priority Direct-IP Multimedia:   384:Kbits

                                                                     Packet
                          Mode                   Redundancy          Size(ms)
    FAX                   pass-through            0
    Modem                 pass-through            0
    TDD/TTY               US                      3
    H.323 Clear-channel   y                       0
    SIP 64K Data          n                       0                  20
```

5.7. Configuration of Coverage Path and Hunt Group for voicemail

The coverage path setup used for compliance testing is illustrated below.
Note the following:

Don't' Answer is set to **y**	The coverage path will be used in the event the phone set is not answered.
Number of Rings is set to **4**	The coverage path will be used after 4 rings.
Point 1: is set to **h59**	Hunt Group 59 is utilised by this coverage path.

```
display coverage path 1
                                 COVERAGE PATH

                   Coverage Path Number: 1
     Cvg Enabled for VDN Route-To Party? n        Hunt after Coverage? n
                       Next Path Number:          Linkage
COVERAGE CRITERIA
    Station/Group Status    Inside Call     Outside Call
             Active?             n              n
               Busy?             y              y
       Don't Answer?             y              y         Number of Rings: 4
                All?             n              n
 DND/SAC/Goto Cover?             y              y
   Holiday Coverage?             n              n

COVERAGE POINTS
    Terminate to Coverage Pts. with Bridged Appearances? n
  Point1: h59            Rng:    Point2:
  Point3:                        Point4:
  Point5:                        Point6:
```

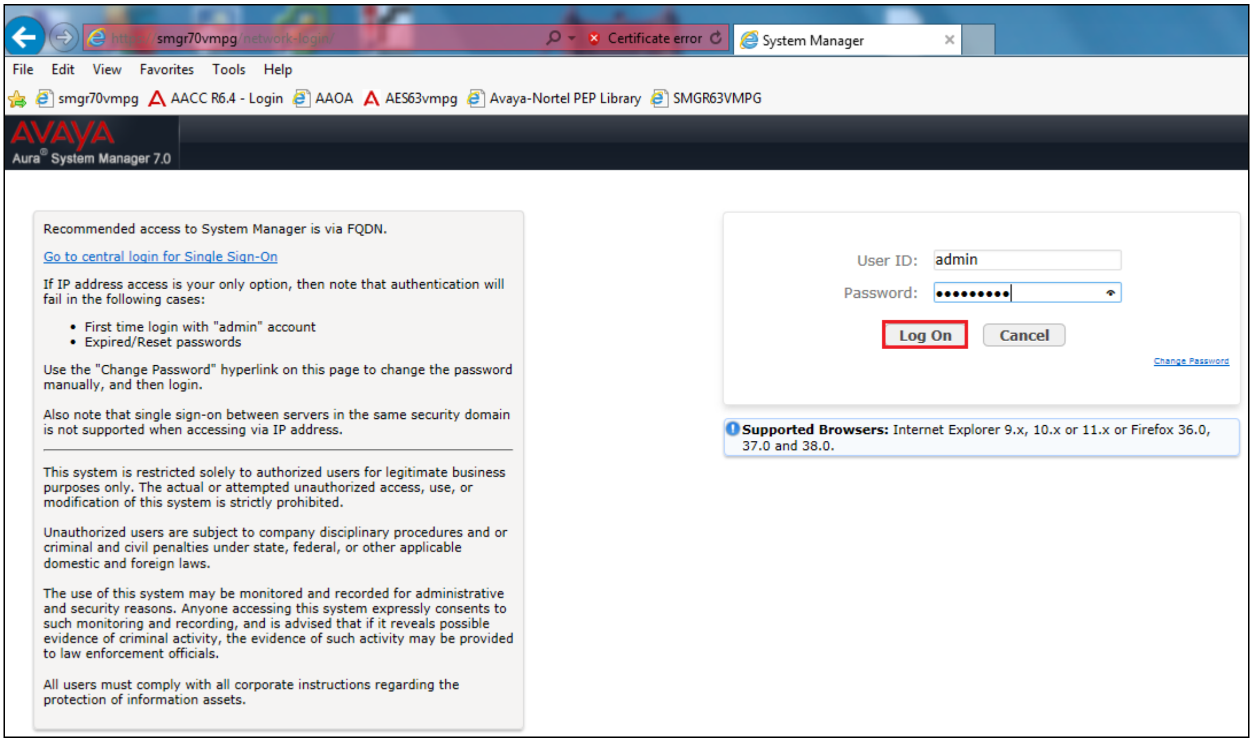
The hunt group used for compliance testing is shown below.
Note on **Page 1** the **Group Extension** is **5999** which is the voicemail number for Messaging and on **Page 2 Message Center** is set to **sip-adjunct**.

```
display hunt-group 59                                        Page   1 of  60
                                  HUNT GROUP
            Group Number: 59                               ACD? n
              Group Name: Voicemail                      Queue? n
         Group Extension: 5999                          Vector? n
              Group Type: ucd-mia                Coverage Path:
                      TN: 1         Night Service Destination:
                     COR: 1                MM Early Answer? n
           Security Code:             Local Agent Preference? n
 ISDN/SIP Caller Display: mbr-name

```

```
display hunt-group 59                                        Page   2 of  60
                                  HUNT GROUP
                      Message Center: sip-adjunct

     Voice Mail Number        Voice Mail Handle         Routing Digits
                                                 (e.g., AAR/ARS Access Code)
     5999                    5999                       8
```

6. Configure Avaya Aura® Session Manager

The NEC DECT handsets are added to Session Manager as SIP Users. In order to make changes in Session Manager, a web session to System Manager is opened. Navigate to http://<System Manager IP Address>/SMGR, enter the appropriate credentials and click on **Log On** as shown below.



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.

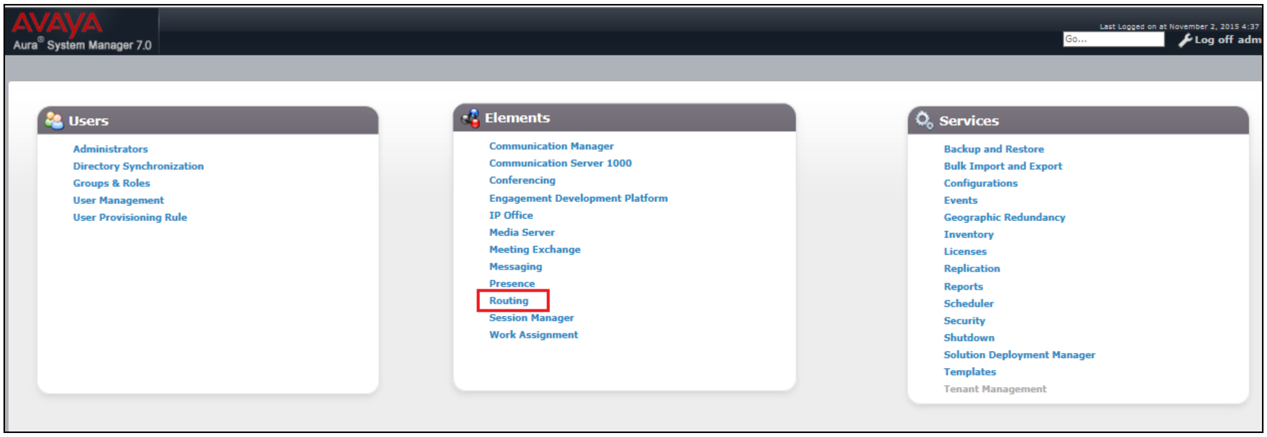
User ID: admin

Password: •••••••••

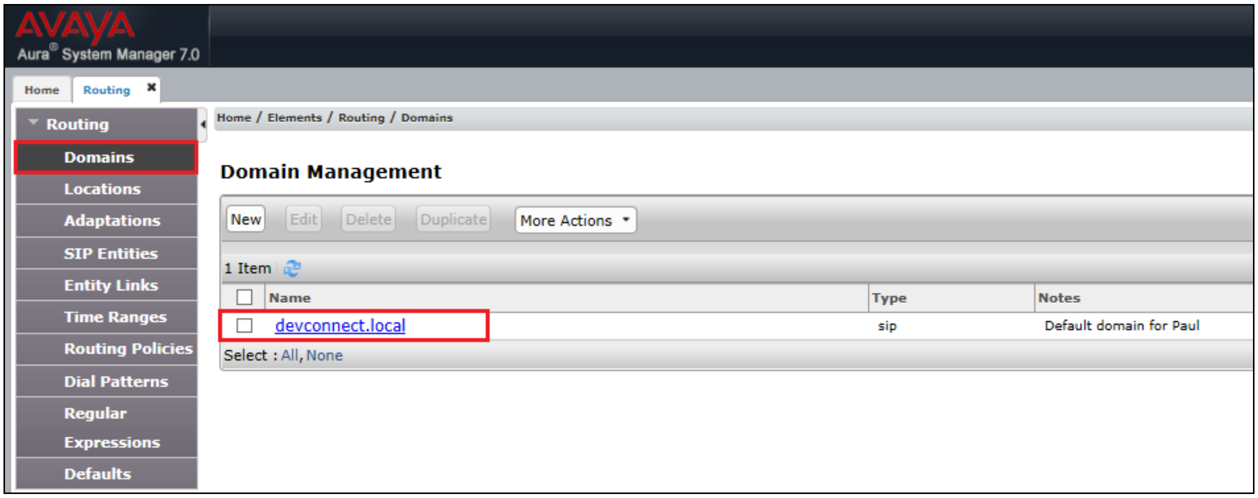
Supported Browsers: Internet Explorer 9.x, 10.x or 11.x or Firefox 36.0, 37.0 and 38.0.

6.1. Configuration of a Domain

Click on **Routing** highlighted below.

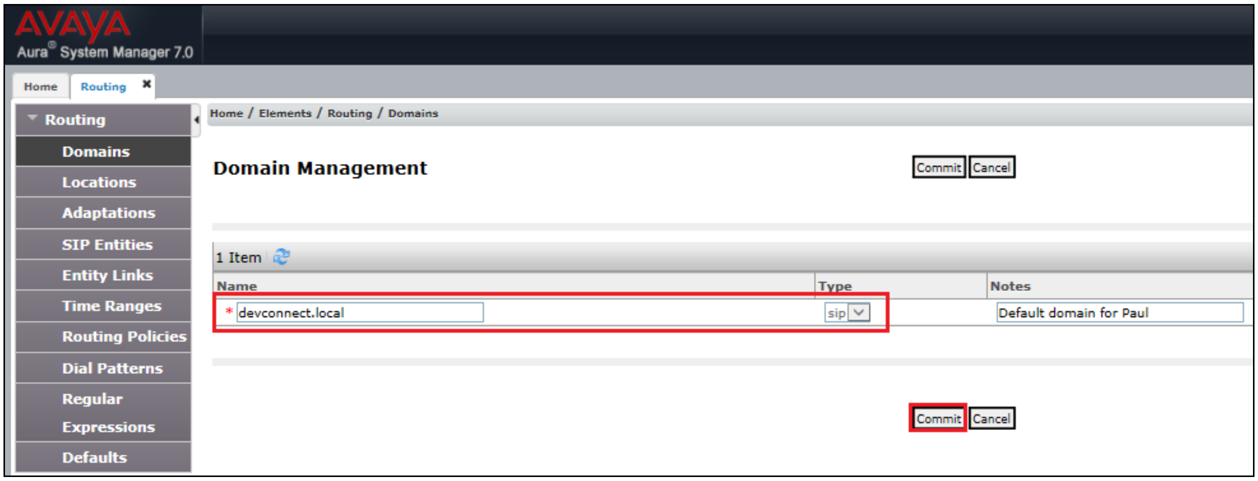


Click on **Domains** in the left window. If there is not a domain already configured click on **New**. In the example below there exists a domain called devconnect.local which has been already configured.



□	Name	Type	Notes
□	devconnect.local	sip	Default domain for Paul

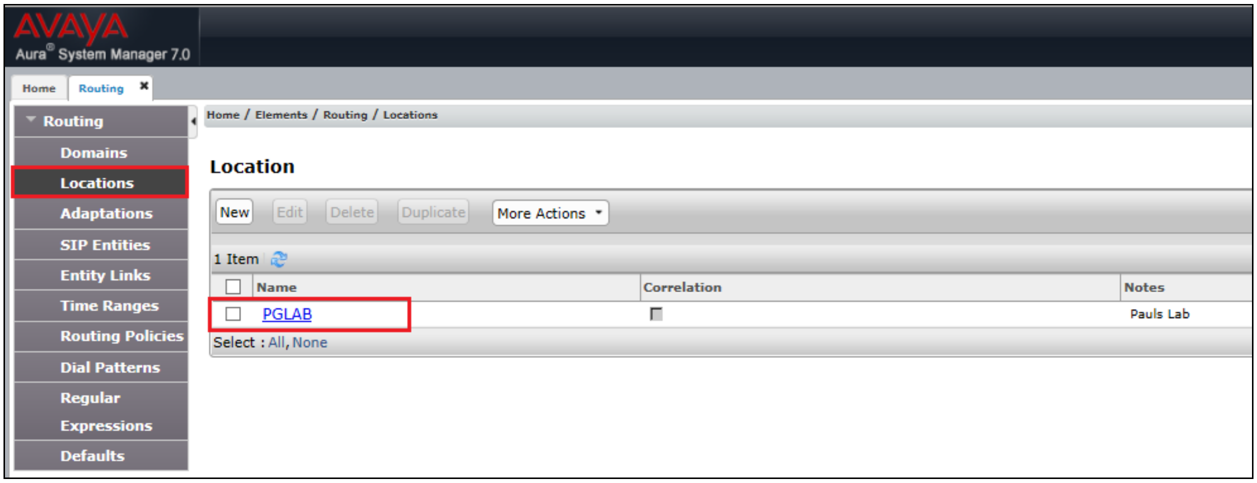
Clicking on the domain name above will open the following window; this is simply to show an example of such a domain. When entering a new domain the following should be entered, once the domain name is entered click on **Commit** to save this.



Name	Type	Notes
* devconnect.local	sip	Default domain for Paul

6.2. Configuration of a Location

Click on **Locations** in the left window and if there is no Location already configured then click on **New**, however in the screen below a location called **PGLAB** is already setup and configured and clicking into this will show its contents.



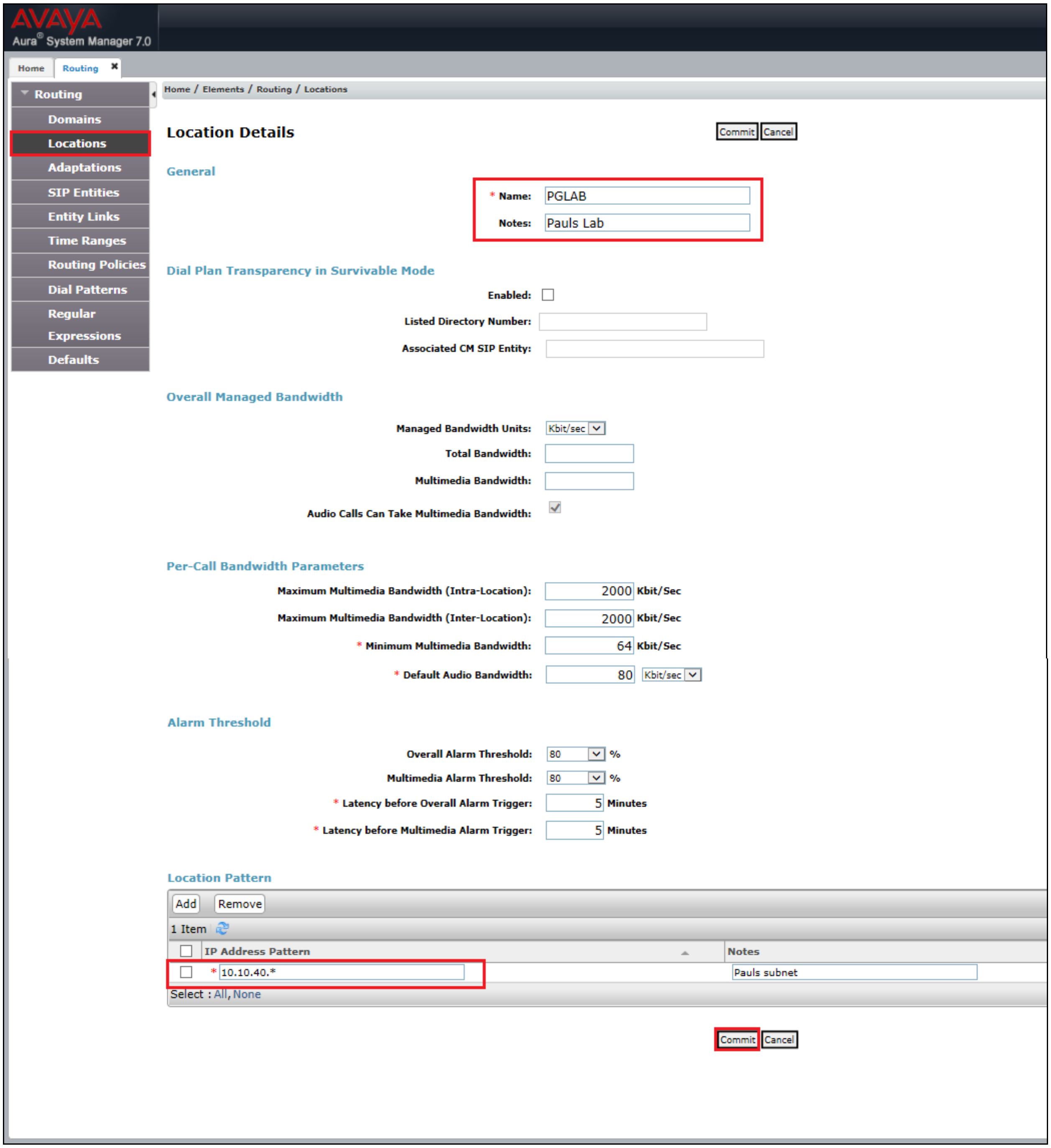
Location

1 Item

☐	Name	Correlation	Notes
☐	PGLAB	☐	Pauls Lab

Select : All, None

The Location below shows a suitable **Name** with a **Location Pattern** of **10.10.40.***. Once this is configured, click on **Commit**.



Location Details

General

* Name: PGLAB

Notes: Pauls Lab

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

1 Item

□	IP Address Pattern	Notes
□	* 10.10.40.*	Pauls subnet

Select : All, None

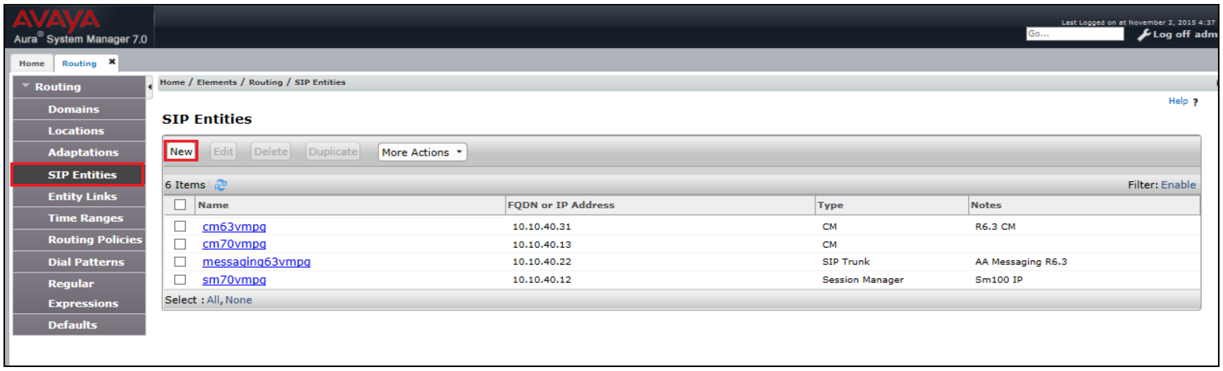
6.3. Configuration of SIP Entities

Clicking on **SIP Entities** in the left window shows what SIP Entities have been added to the system and allows the addition of any new SIP Entity that may be required. Please note the SIP Entities already present for the Compliance Testing of NEC DECT handsets.

- Communication Manager SIP Entity (cm70vmpg)
- Session Manager SIP Entity (sm70vmpg)
- Messaging SIP Entity (messaging63vmpg)

For the NEC IP DECT solution a SIP entity is only required, when more than six handsets would register through one DAP. This basically depends on the ratio between the number of DAP´s and NEC DECT handsets used in the overall system.

If needed, for each DAP a SIP Entity will be added as type “Endpoint Concentrator”. This Endpoint Concentrator type, allows up to 1000 connections from a single IP address. The single IP address can be shared by multiple Windows instances running on a Virtualized server or multiple DECT handsets sharing the same Access Point IP address.



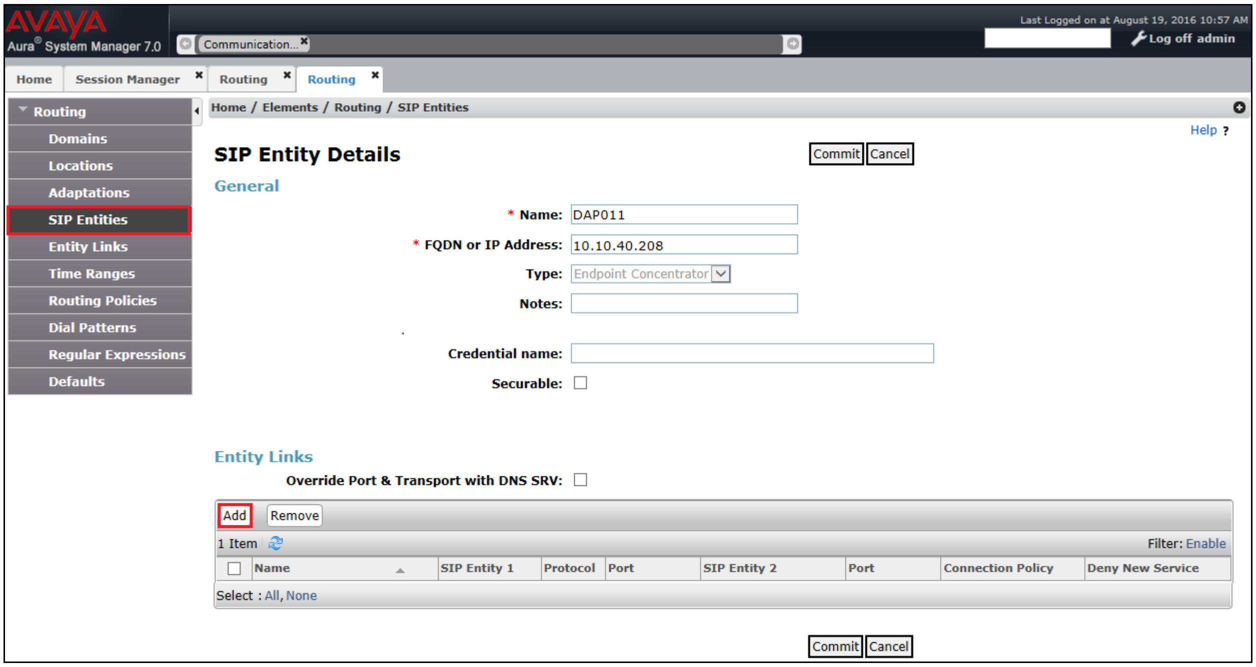
SIP Entities

6 Items

□	Name	FQDN or IP Address	Type	Notes
□	cm63vmpg	10.10.40.31	CM	R6.3 CM
□	cm70vmpg	10.10.40.13	CM	
□	messaging63vmpg	10.10.40.22	SIP Trunk	AA Messaging R6.3
□	sm70vmpg	10.10.40.12	Session Manager	Sm100 IP

Select : All, None

To add a SIP entity, click on “New” (not shown) and enter a suitable **Name** as well as the **IP Address** of the DECT Access Point. Select **Endpoint Concentrator** as the **Type**. Click on **Commit** once completed.



Home / Elements / Routing / SIP Entities

SIP Entity Details

General

* Name: DAP011
* FQDN or IP Address: 10.10.40.208
Type: Endpoint Concentrator
Notes:
Credential name:
Securable: □

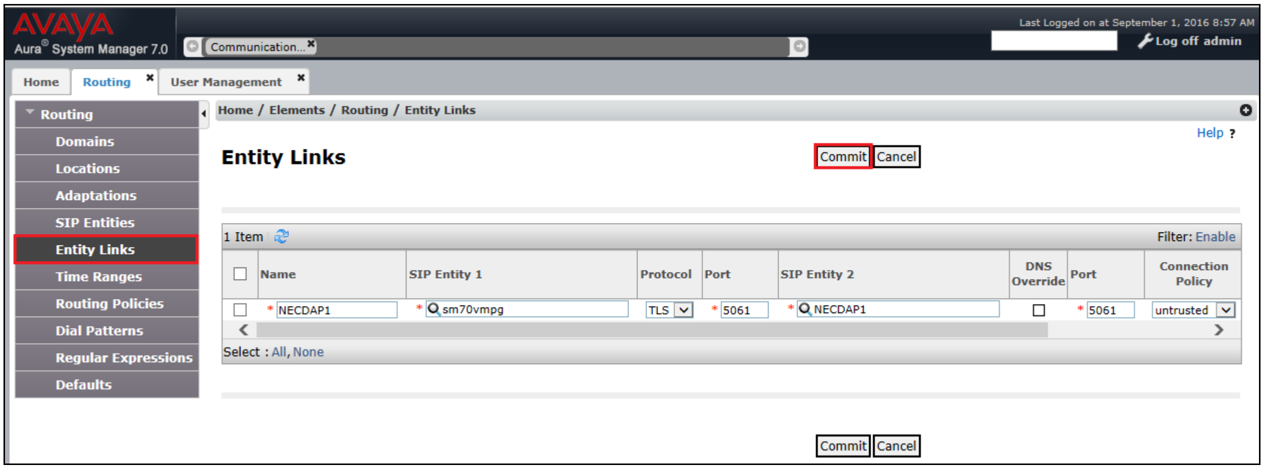
Entity Links

Override Port & Transport with DNS SRV: □

1 Item

□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service

An Entity-Link between the DAP and SM is required. Click on **Add** (this can be done from the **SIP Entity** page above or by clicking on Entity Links in the left column and then on **New**, which is not shown here) and ensure that **TLS** is selected for the **Protocol** and **5061** for the **Port**. The **Connection Policy** must be setup as **untrusted** as shown below. Click on **Commit** once completed.



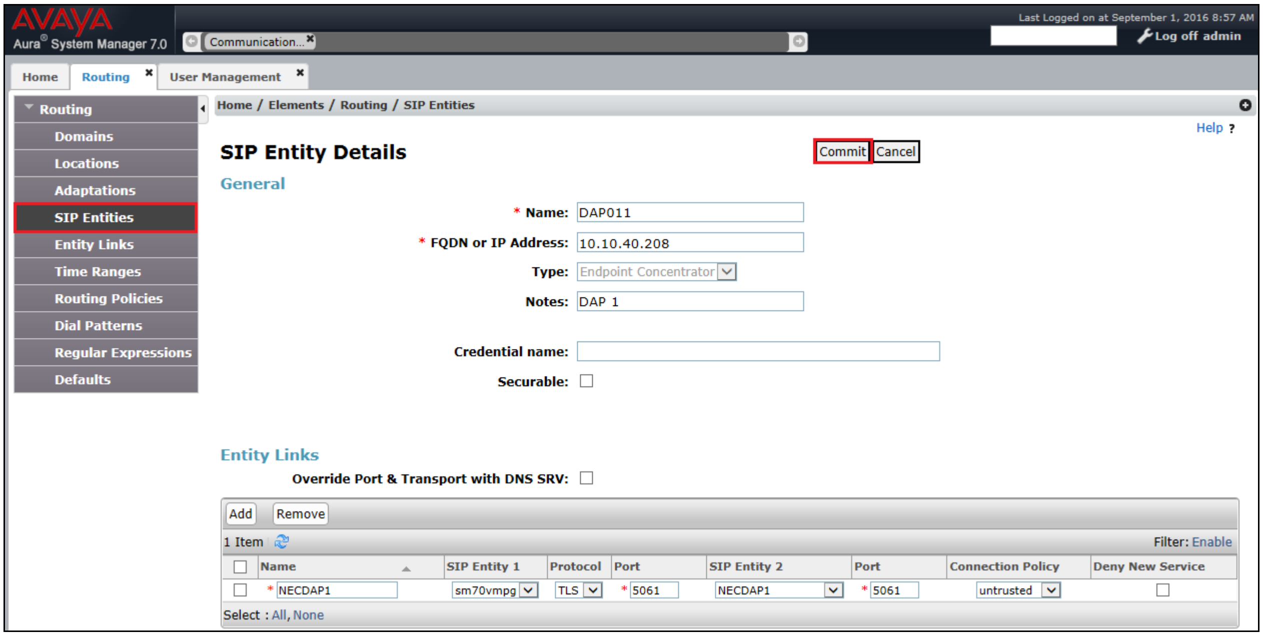
Home / Elements / Routing / Entity Links

Entity Links

1 Item

□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy
□	* NECDAP1	* sm70vmpg	TLS	* 5061	* NECDAP1	□	* 5061	untrusted

Click on **Commit** in the SIP Entity page to complete.



SIP Entity Details

General

* Name: DAP011

* FQDN or IP Address: 10.10.40.208

Type: Endpoint Concentrator

Notes: DAP 1

Credential name:

Securable: □

Entity Links

Override Port & Transport with DNS SRV: □

Add Remove

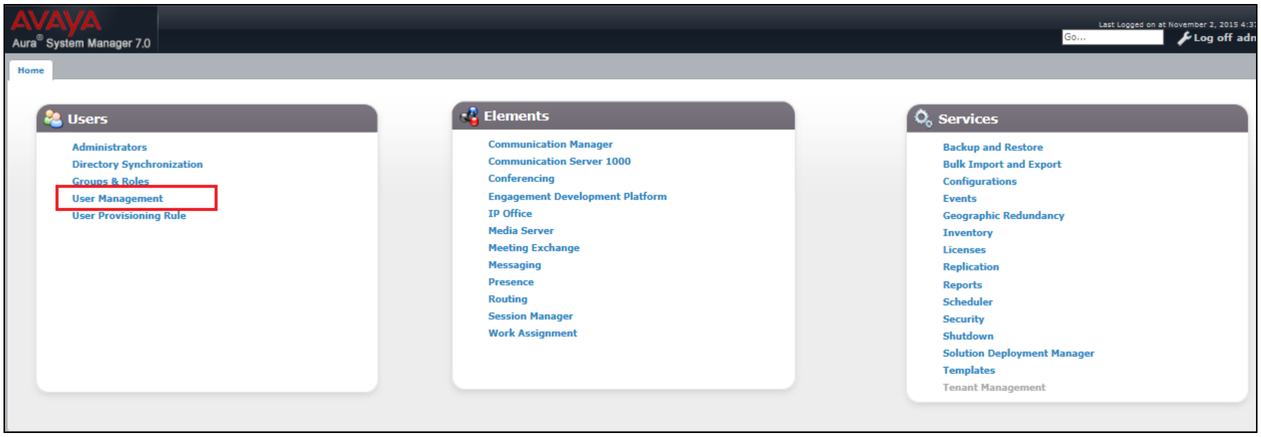
1 Item Filter: Enable

□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
□	* NECDAP1	sm70vmpg	TLS	* 5061	NECDAP1	* 5061	untrusted	□

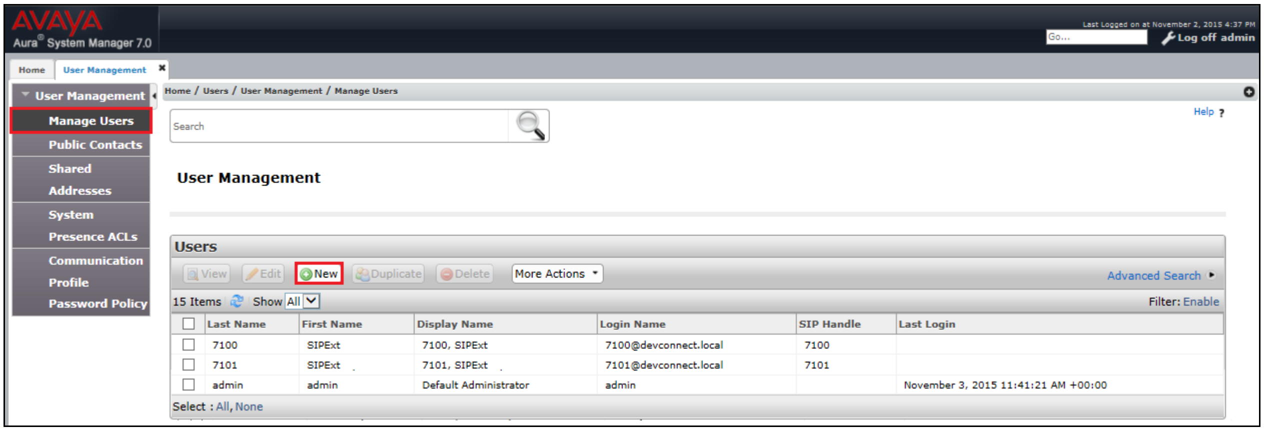
Select : All, None

6.4. Adding NEC SIP Users

From the home page click on **User Management** highlighted below.



Click on **New** highlighted to add a new SIP user.



User Management

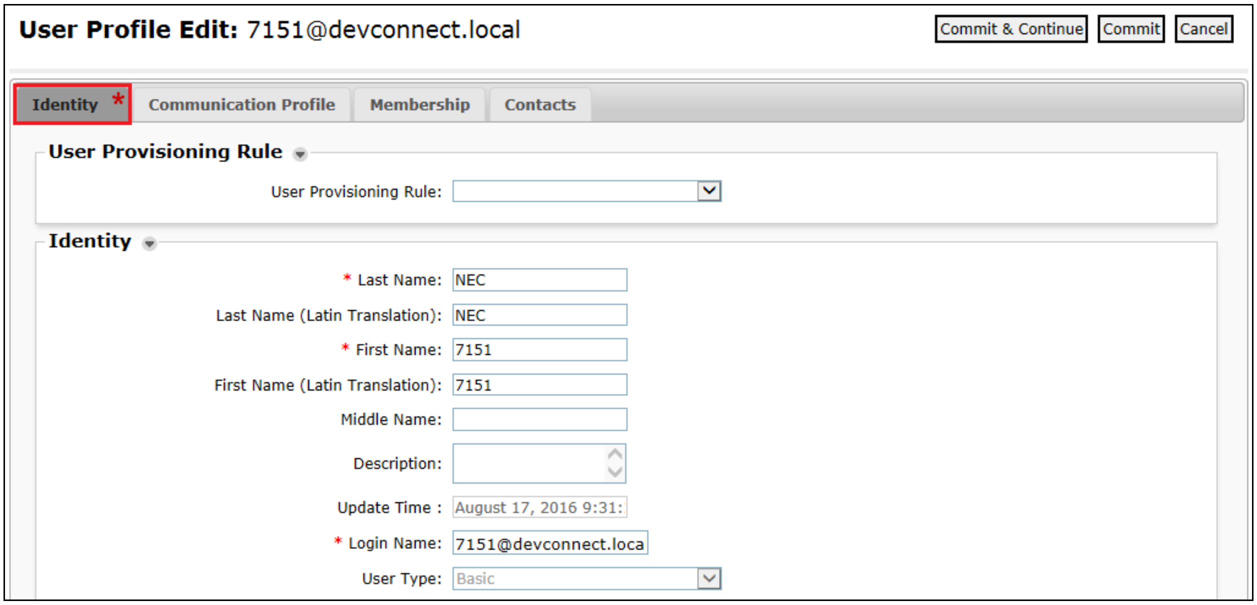
Users

15 Items Show All

□	Last Name	First Name	Display Name	Login Name	SIP Handle	Last Login
□	7100	SIPExt	7100, SIPExt	7100@devconnect.local	7100	
□	7101	SIPExt	7101, SIPExt	7101@devconnect.local	7101	
□	admin	admin	Default Administrator	admin		November 3, 2015 11:41:21 AM +00:00

Select : All, None

Under the **Identity** tab fill in the user's **Last Name** and **First Name** as shown below. Enter a **Login Name**. The remaining fields can be left as default.



User Profile Edit: 7151@devconnect.local

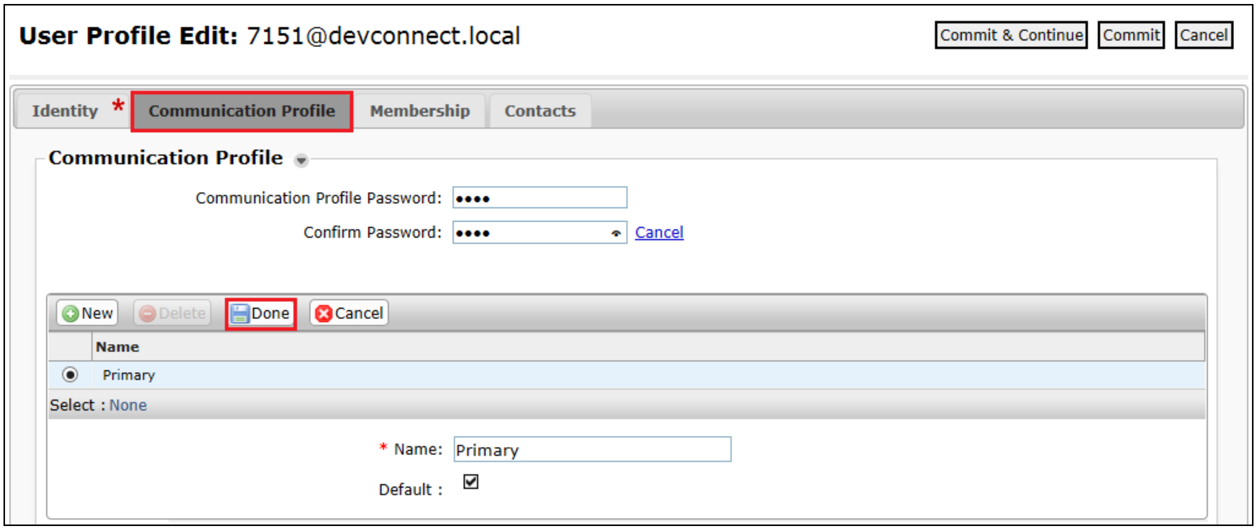
User Provisioning Rule

User Provisioning Rule:

Identity

* Last Name:	NEC
Last Name (Latin Translation):	NEC
* First Name:	7151
First Name (Latin Translation):	7151
Middle Name:	
Description:	
Update Time :	August 17, 2016 9:31:
* Login Name:	7151@devconnect.loca
User Type:	Basic

Under the **Communication Profile** tab enter a suitable **Communication Profile Password** (which is the login password for the SIP communication) and click on **Done** when added. Note that this password is required when configuring the NEC handset in **Section 8.4**.



User Profile Edit: 7151@devconnect.local

Communication Profile

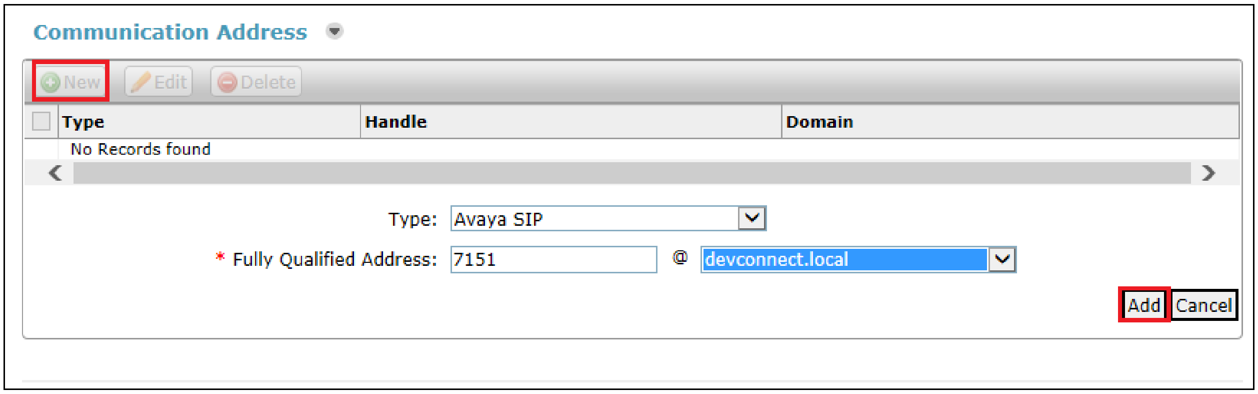
Communication Profile Password:	••••
Confirm Password:	••••

	Name
●	Primary

Select : None

* Name:	Primary
Default :	☑

Click on **New** to add a new **Communication Address**. Enter the extension number and the domain for the **Fully Qualified Address** and click on **Add** once finished.

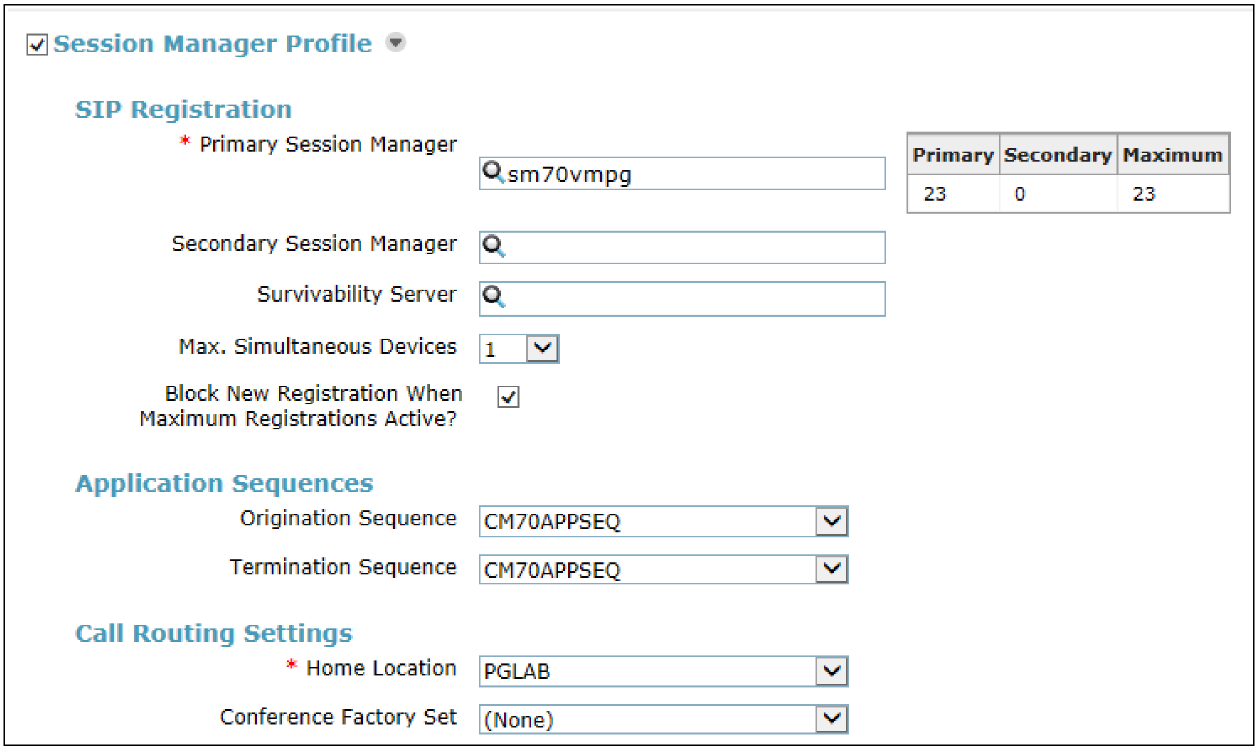


☐ Type	Handle	Domain
No Records found		

Type: Avaya SIP

* Fully Qualified Address: 7151 @ devconnect.local

Ensure **Session Manager Profile** is checked and enter the **Primary Session Manager** details, enter the **Origination Application Sequence** and the **Termination Application Sequence** and the **Home Location** as shown below.



☑ Session Manager Profile

SIP Registration

* Primary Session Manager: sm70vmpg

Primary	Secondary	Maximum
23	0	23

Secondary Session Manager:

Survivability Server:

Max. Simultaneous Devices: 1

Block New Registration When Maximum Registrations Active? ☑

Application Sequences

Origination Sequence: CM70APPSEQ

Termination Sequence: CM70APPSEQ

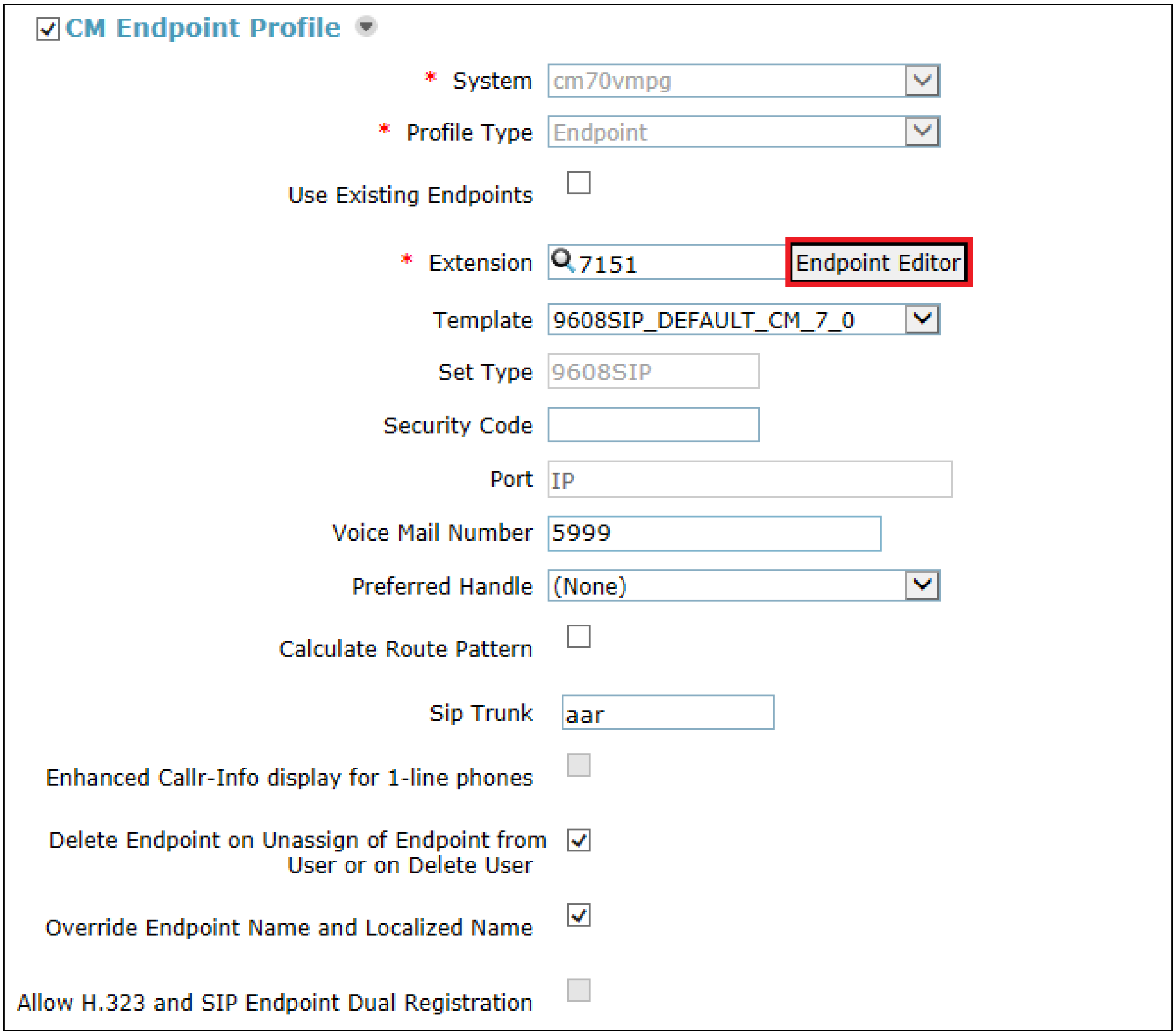
Call Routing Settings

* Home Location: PGLAB

Conference Factory Set: (None)

Note: If a Multi Device Access (MDA) is to be used and a single user would have an Avaya 96x1 deskphone along with a NEC DECT handset, then the **Max. Simultaneous Devices** needs to be set to two (2) to allow both devices can register at the same time.

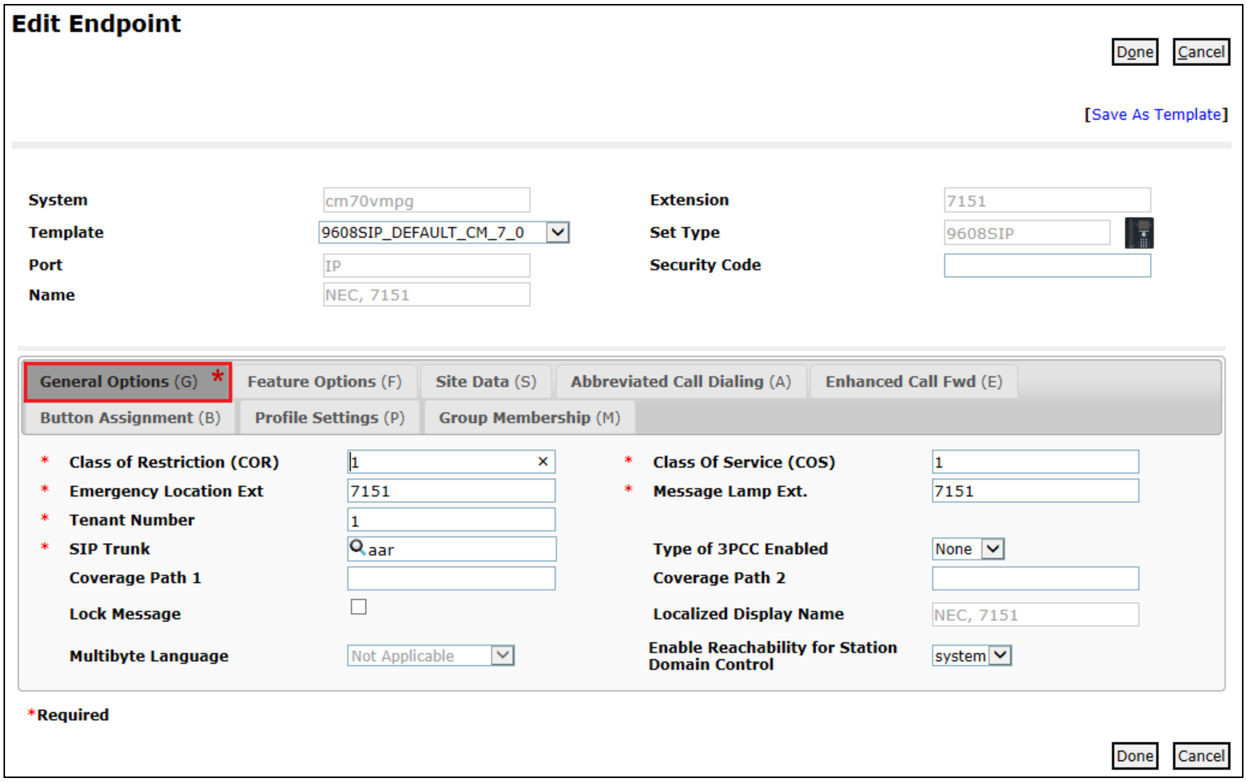
Ensure that **CM Endpoint Profile** is selected and choose the **9608SIP_DEFAULT_CM_7_0** as the **Template**. Enter the correct voicemail number, the rest of the fields can be left as default or set as shown below. Click on **Endpoint Editor** to configure the buttons and features for that handset on Communication Manager.



☑ CM Endpoint Profile

* System	cm70vmpg
* Profile Type	Endpoint
Use Existing Endpoints	□
* Extension	7151 [Endpoint Editor]
Template	9608SIP_DEFAULT_CM_7_0
Set Type	9608SIP
Security Code	
Port	IP
Voice Mail Number	5999
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 the **General Options** tab, if voicemail is being used ensure that **Coverage Path 1** is set to that configured in **Section 5.7**. Also ensure that **Message Lamp Ext.** is showing the correct extension number.



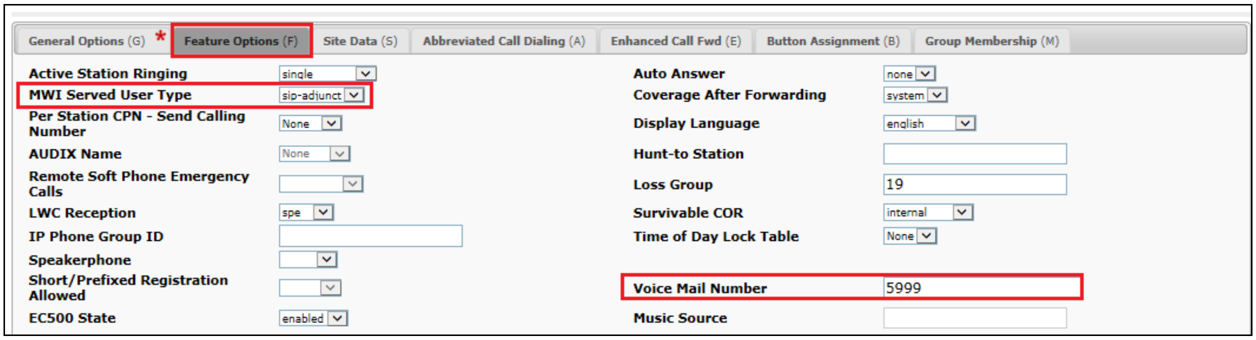
Edit Endpoint

System	cm70vmpg	Extension	7151
Template	9608SIP_DEFAULT_CM_7_0	Set Type	9608SIP
Port	IP	Security Code	
Name	NEC, 7151		

* Class of Restriction (COR)	1	* Class Of Service (COS)	1
* Emergency Location Ext	7151	* Message Lamp Ext.	7151
* Tenant Number	1		
* SIP Trunk	aar	Type of 3PCC Enabled	None
Coverage Path 1		Coverage Path 2	
Lock Message	□	Localized Display Name	NEC, 7151
Multibyte Language	Not Applicable	Enable Reachability for Station Domain Control	system

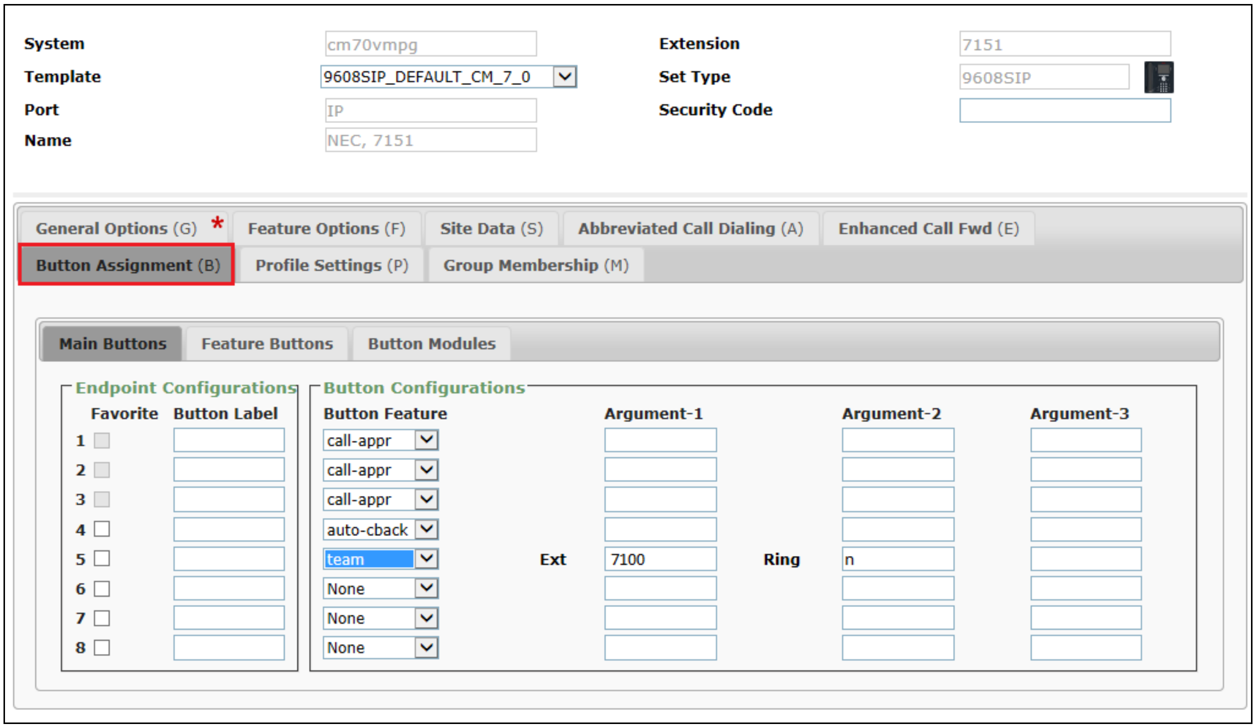
*Required

Under the tab **Feature Options** ensure that **MWI Served User Type** is set to **sip-adjunct**. Ensure the **Voice Mail Number** is set to that configured in **Section 5.7**.



Active Station Ringing	single	Auto Answer	none
MWI Served User Type	sip-adjunct	Coverage After Forwarding	system
Per Station CPN - Send Calling Number	None	Display Language	english
AUDIX Name	None	Hunt-to Station	
Remote Soft Phone Emergency Calls		Loss Group	19
LWC Reception	spe	Survivable COR	internal
IP Phone Group ID		Time of Day Lock Table	None
Speakerphone			
Short/Prefixed Registration Allowed		Voice Mail Number	5999
EC500 State	enabled	Music Source	

Feature buttons can be added here, this will be different for every site. Once the **Button Assignment** is completed, click on **Done** to finish (not shown).

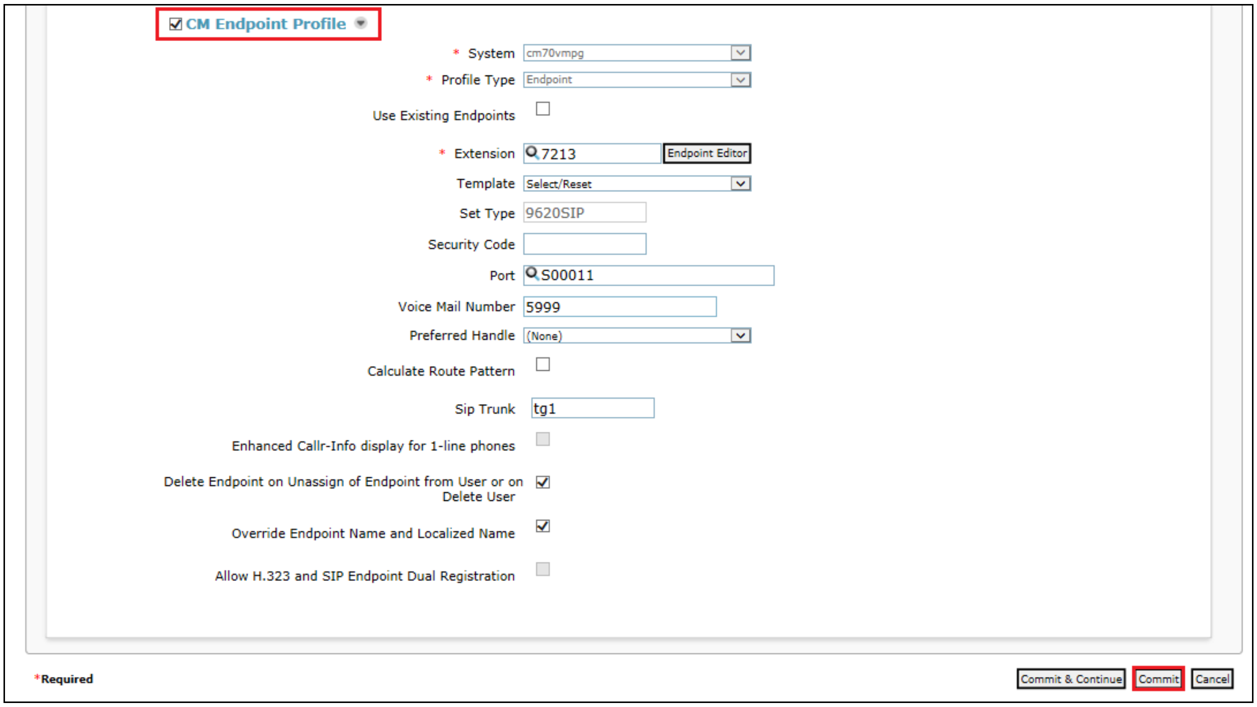


System	cm70vmpg	Extension	7151
Template	9608SIP_DEFAULT_CM_7_0	Set Type	9608SIP
Port	IP	Security Code	
Name	NEC, 7151		

Endpoint Configurations / Button Configurations

	Favorite	Button Label	Button Feature		Argument-1		Argument-2	Argument-3
1	□		call-appr					
2	□		call-appr					
3	□		call-appr					
4	□		auto-cback					
5	□		team	Ext	7100	Ring	n	
6	□		None					
7	□		None					
8	□		None					

Once the **CM Endpoint Profile** is completed correctly, click on **Commit** to save the new user.



☑ CM Endpoint Profile

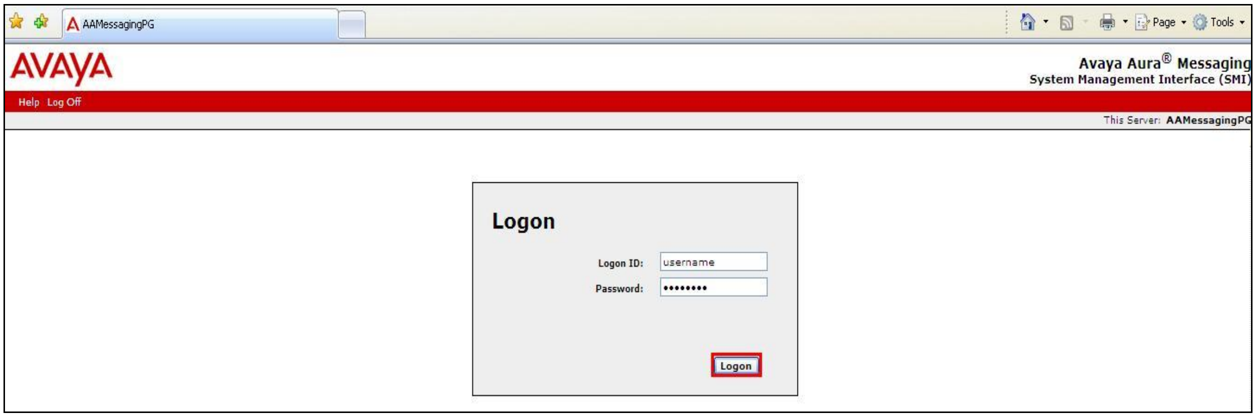
* System	cm70vmpg
* Profile Type	Endpoint
Use Existing Endpoints	□
* Extension	7213
Template	Select/Reset
Set Type	9620SIP
Security Code	
Port	S00011
Voice Mail Number	5999
Preferred Handle	(None)
Calculate Route Pattern	□
Sip Trunk	tg1
Enhanced Callr-Info display for 1-line phones	□
Delete Endpoint on Unassign of Endpoint from User or on Delete User	☑
Override Endpoint Name and Localized Name	☑
Allow H.323 and SIP Endpoint Dual Registration	□

*Required

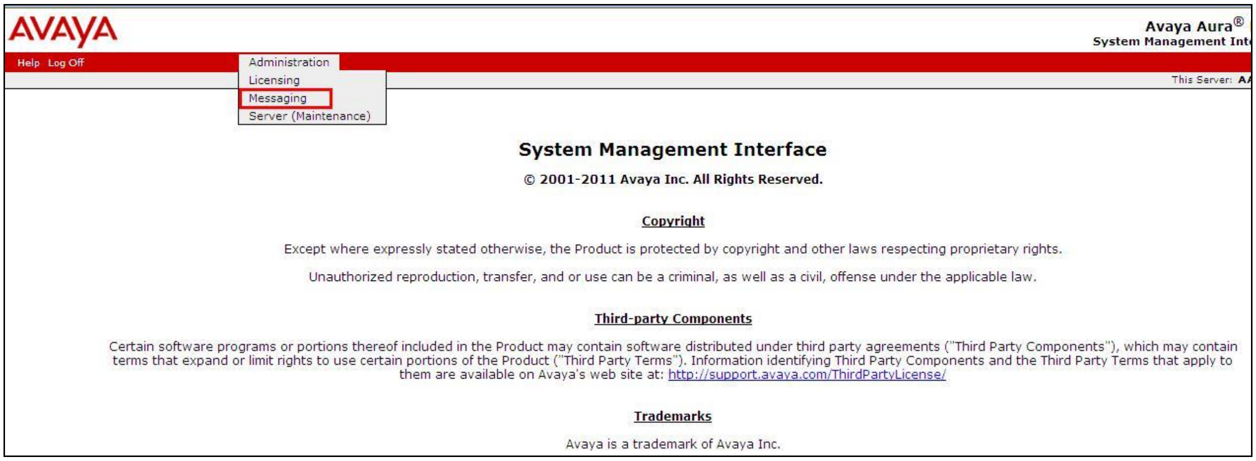
7. Configure Avaya Aura® Messaging

It is assumed that a fully working messaging system is in place and the necessary configuration for Communication Manager and Session Manager has already been done. For further information on the installation and configuration of Messaging please refer to **Section 11** of these Application Notes.

Navigate to http://<Messaging IP Address>. Enter the appropriate credentials and click on **Logon** highlighted below.



Once logged on select **Messaging** under **Administration** as shown below.



System Management Interface

© 2001-2011 Avaya Inc. All Rights Reserved.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights.

Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

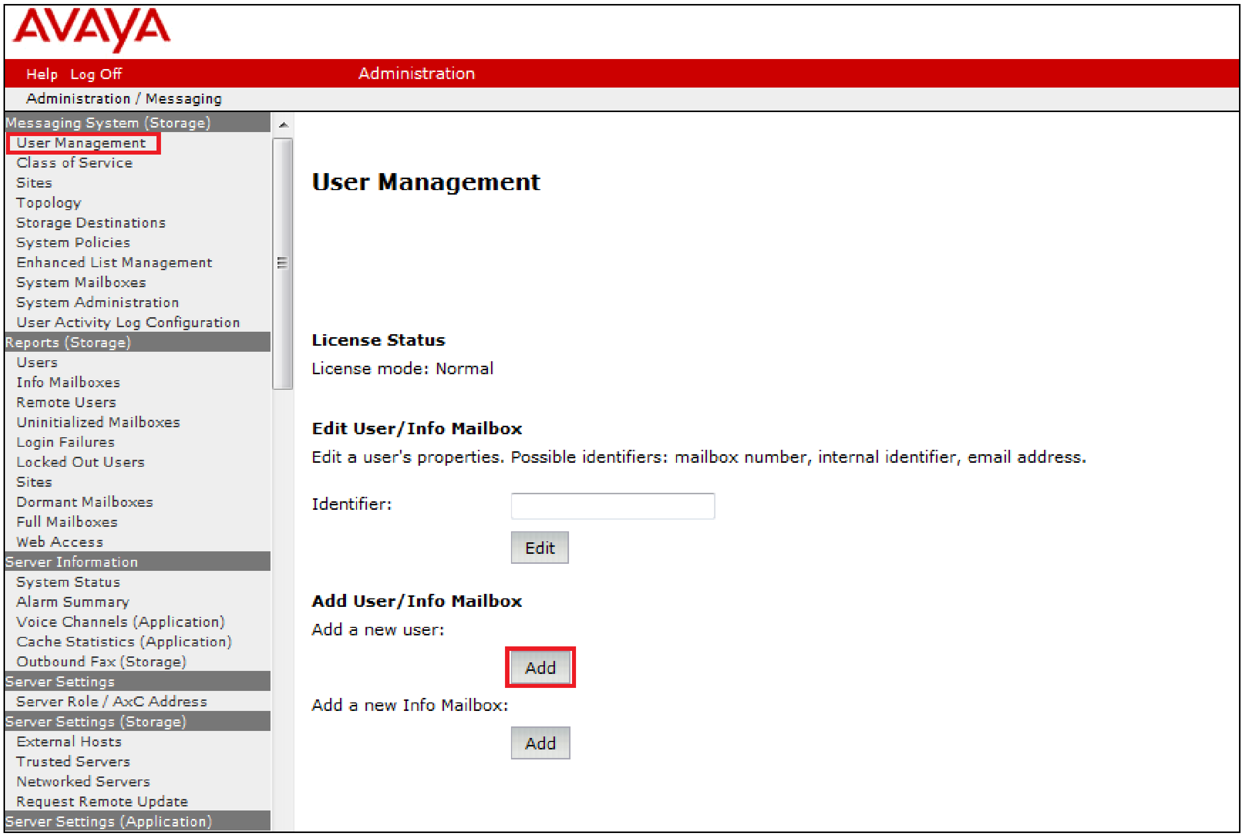
Third-party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them are available on Avaya's web site at: http://support.avaya.com/ThirdPartyLicense/

Trademarks

Avaya is a trademark of Avaya Inc.

Click on **User Management** in the left hand column and click on **Add** under **Add User/Info Mailbox** as highlighted below.



User Management

License Status

License mode: Normal

Edit User/Info Mailbox

Edit a user's properties. Possible identifiers: mailbox number, internal identifier, email address.

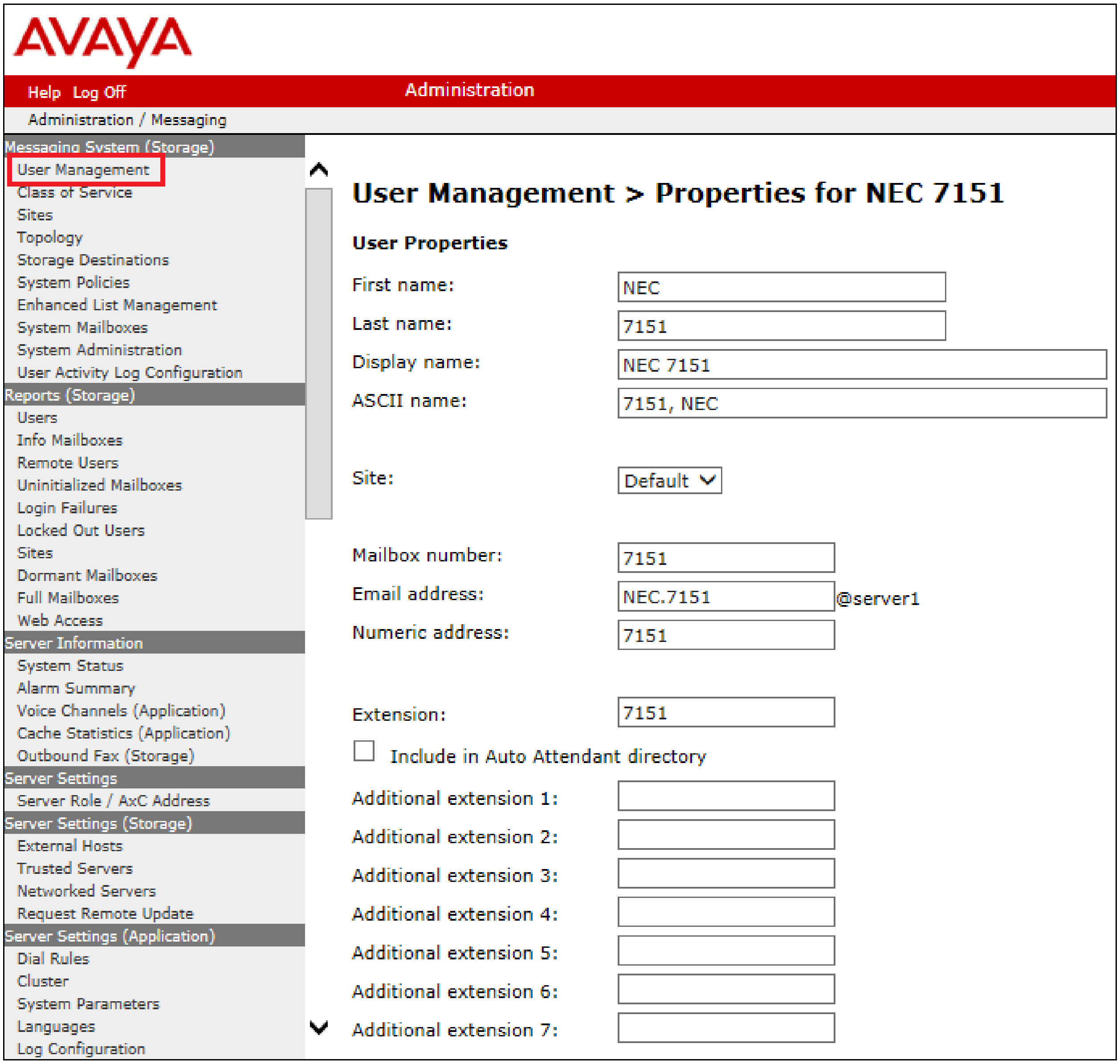
Identifier:

Add User/Info Mailbox

Add a new user:

Add a new Info Mailbox:

Enter a suitable **First Name** and **Last Name**. Select the appropriate **Site** from the drop down box. Enter the correct **Mailbox number** and **Extension**.



User Management > Properties for NEC 7151

User Properties

First name: NEC

Last name: 7151

Display name: NEC 7151

ASCII name: 7151, NEC

Site: Default

Mailbox number: 7151

Email address: NEC.7151 @server1

Numeric address: 7151

Extension: 7151

□ Include in Auto Attendant directory

Additional extension 1:

Additional extension 2:

Additional extension 3:

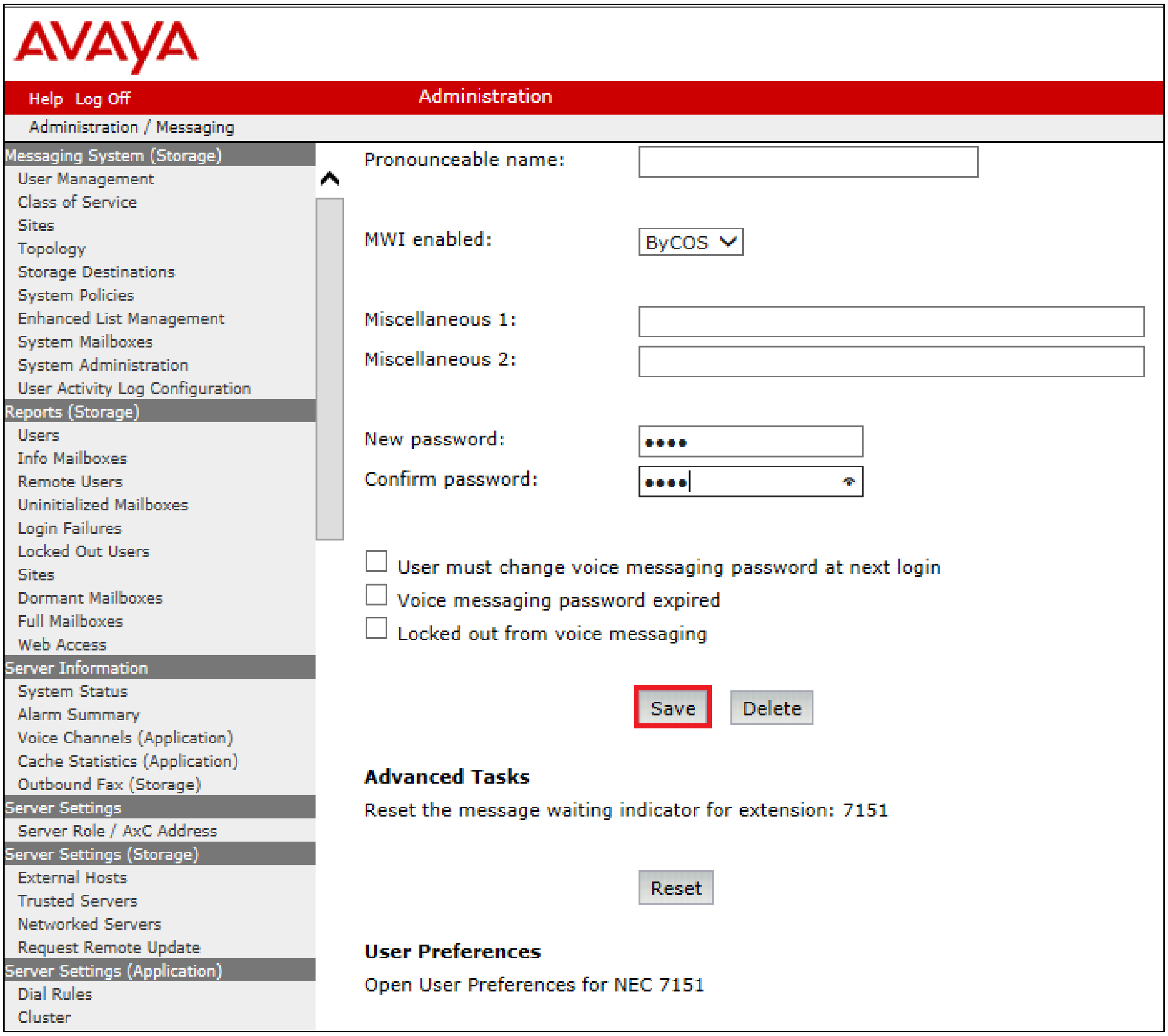
Additional extension 4:

Additional extension 5:

Additional extension 6:

Additional extension 7:

Ensure that **MWI Enabled** is set to **ByCOS**. Enter a suitable voicemail **password** (PIN) and click on **Save** once finished.



Pronounceable name:

MWI enabled: ByCOS

Miscellaneous 1:

Miscellaneous 2:

New password: ••••

Confirm password: ••••

□ User must change voice messaging password at next login
□ Voice messaging password expired
□ Locked out from voice messaging

Advanced Tasks

Reset the message waiting indicator for extension: 7151

User Preferences

Open User Preferences for NEC 7151

8. Configure NEC DECT Access Points and Handsets

The following section shows the setup used during compliance testing for the NEC DECT solution, both the configuration of the DECT Access Points and the addition and subscription of the NEC DECT handsets are clearly outlined. The installation of the NEC DECT solution is outside the scope of these Application Notes for more information on this please refer to Section 11.

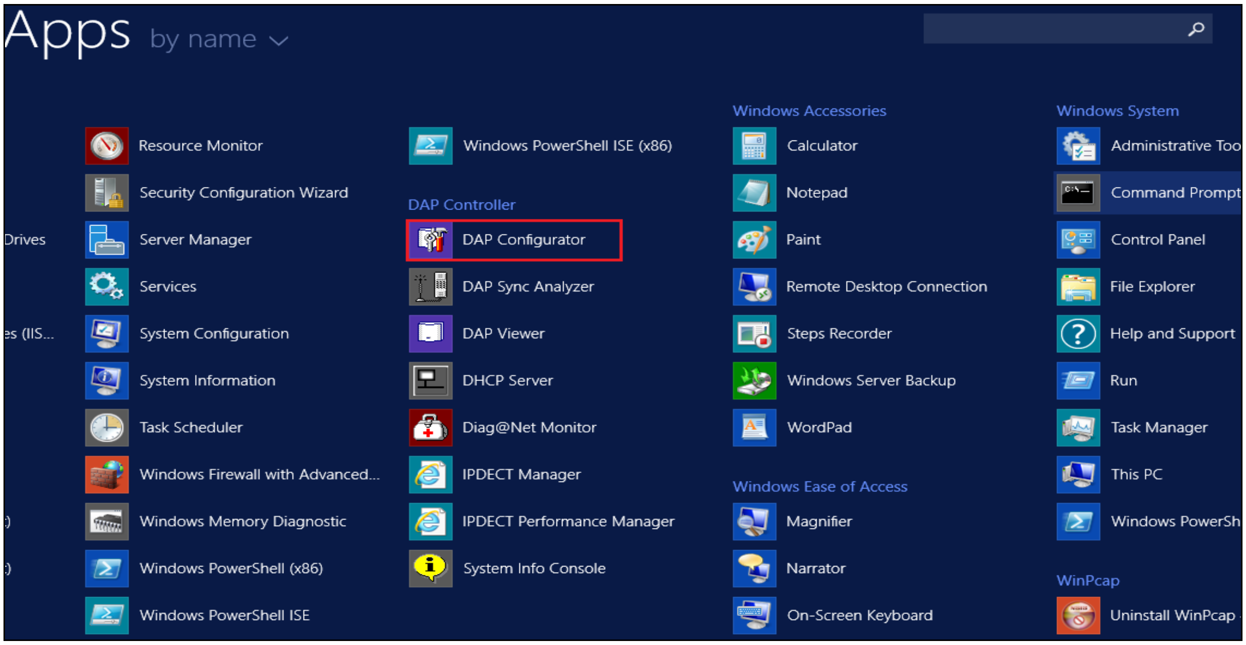
Note: The NEC IP DECT solution relies on DHCP (Option 66, 67), NTP and TFTP as network-services. DHCP and TFTP services can be provided from the DAP controller instance. In addition a Multi-Cast IP address is also required for the DAP´s to synch.

8.1. DAP Configurator - Configure DECT Access Point (DAP)

The configuration of the DECT Access Point uses the DAP Configurator which creates a configuration file that is this pushed to each DAP on the network. Click on DAP Configurator as shown below.

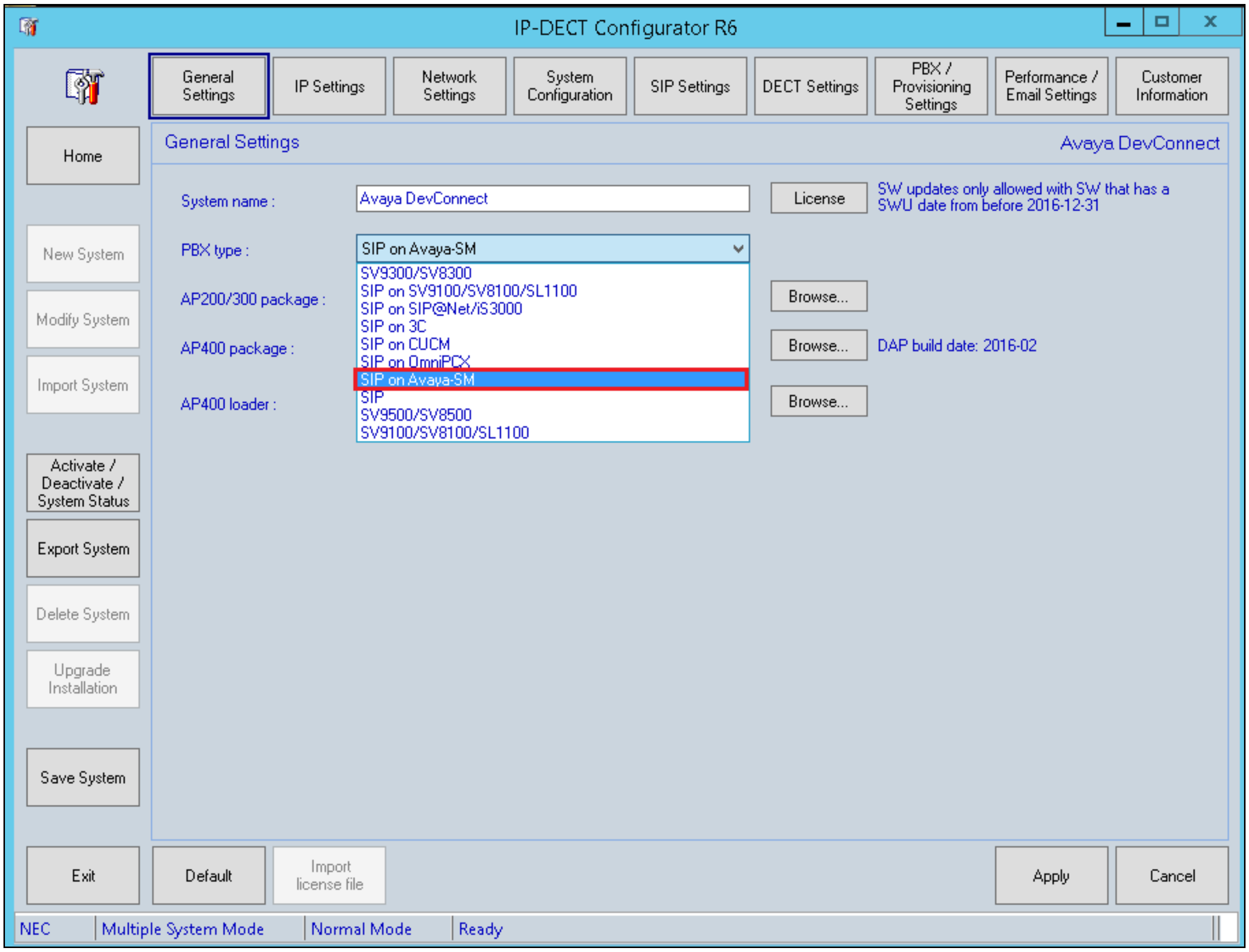
Note: An NEC IP DECT solution typically consists of a windows based instance called DAP Controller which includes "DAP Configurator" and "DAP Manager".

Note: The DAP Controller Package must be installed in the DAP Controller server. This package is only available from NEC.



Click on the **General Settings** tab and enter the information on the main window. Enter a suitable **System Name** and ensure the **PBX type** is set to **SIP on Avaya-SM**.

Note: Typically a license file is ordered and contains the licenses (number of access points (DAP's) and other features) for the new IP DECT Release 6.41 system. This license file also contains the PARI, which must be unique for each DECT System. When the license file is loaded here the PARI will be filled in automatically.



General Settings — Avaya DevConnect

System name : Avaya DevConnect

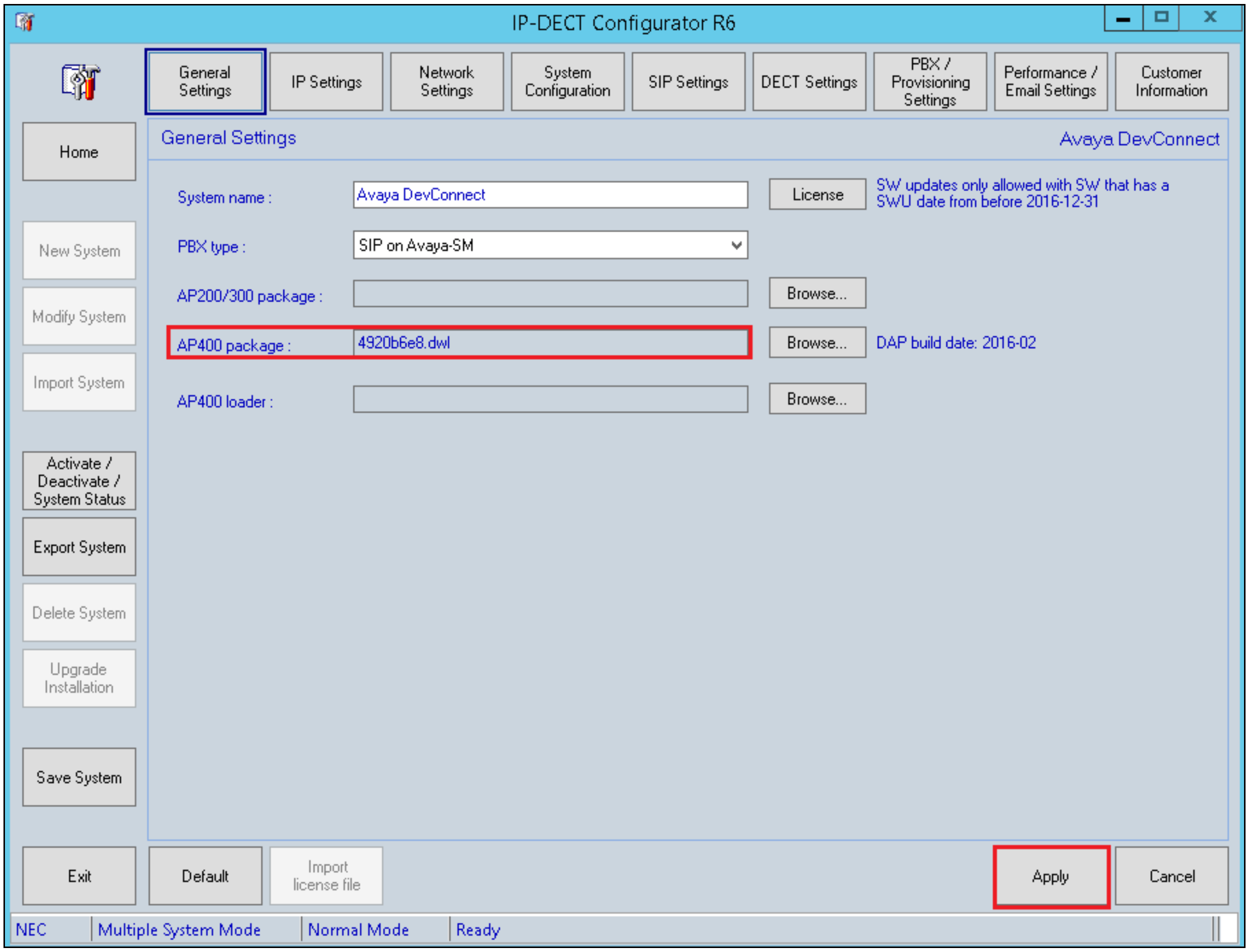
PBX type : SIP on Avaya-SM

SW updates only allowed with SW that has a SWU date from before 2016-12-31

DAP build date: 2016-02

NEC | Multiple System Mode | Normal Mode | Ready

Ensure the correct AP400 package file from NEC is available on the machine with the DAP configurator. Click on **Browse** for the **AP400 package** and select the proper file (<filename>.dwl). Click on **Apply** at the bottom of the screen.



General Settings — Avaya DevConnect

System name : Avaya DevConnect

SW updates only allowed with SW that has a SWU date from before 2016-12-31

PBX type : SIP on Avaya-SM

AP200/300 package :

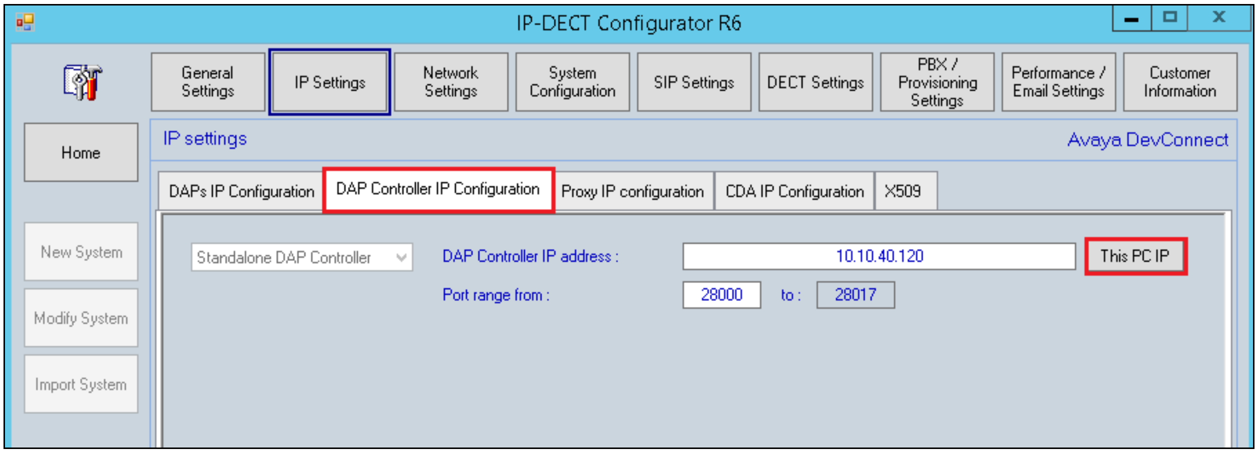
AP400 package : 4920b6e8.dwl

DAP build date: 2016-02

AP400 loader :

NEC | Multiple System Mode | Normal Mode | Ready

Click on the **IP Settings** tab at the top of the screen and on the **DAP Controller IP Configuration** tab in the main window. Enter the IP address of the DAP Controller server. In this case just pressing **This PC IP** will fill in the required information.



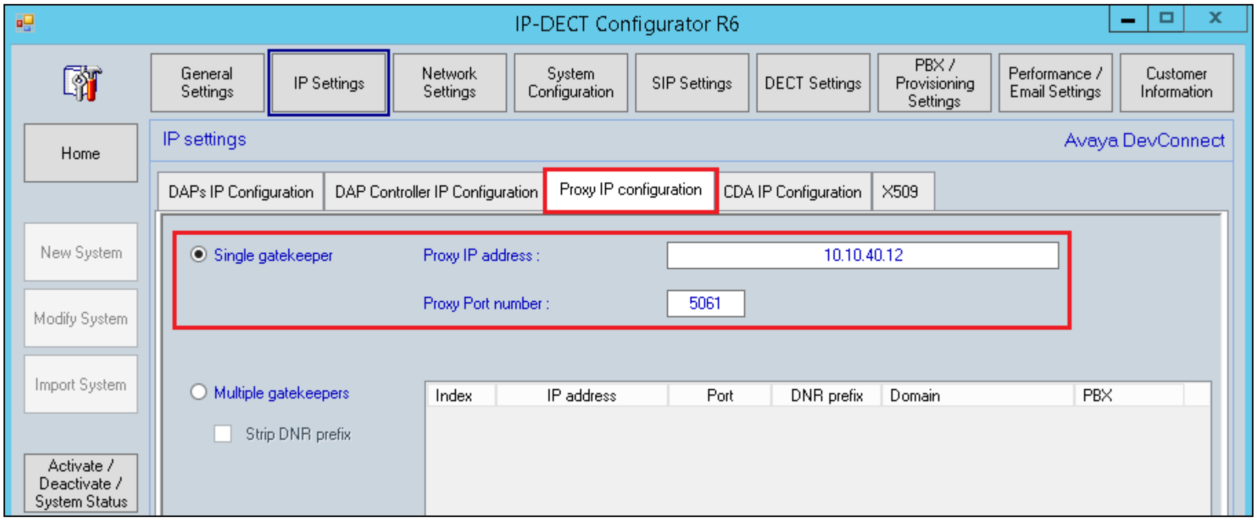
Standalone DAP Controller

DAP Controller IP address : 10.10.40.120

Port range from : 28000 to : 28017

Click on the **Proxy IP configuration** tab and click on **Single gatekeeper** in the main window. Enter the Session Manager IP address as the **Proxy IP address** and **5061** as the **Proxy Port number** as this is the port number used for TLS. This port will be the same as configured in Session Manager.

Note: For redundant systems multiple gatekeepers can be selected.



● Single gatekeeper

Proxy IP address : 10.10.40.12

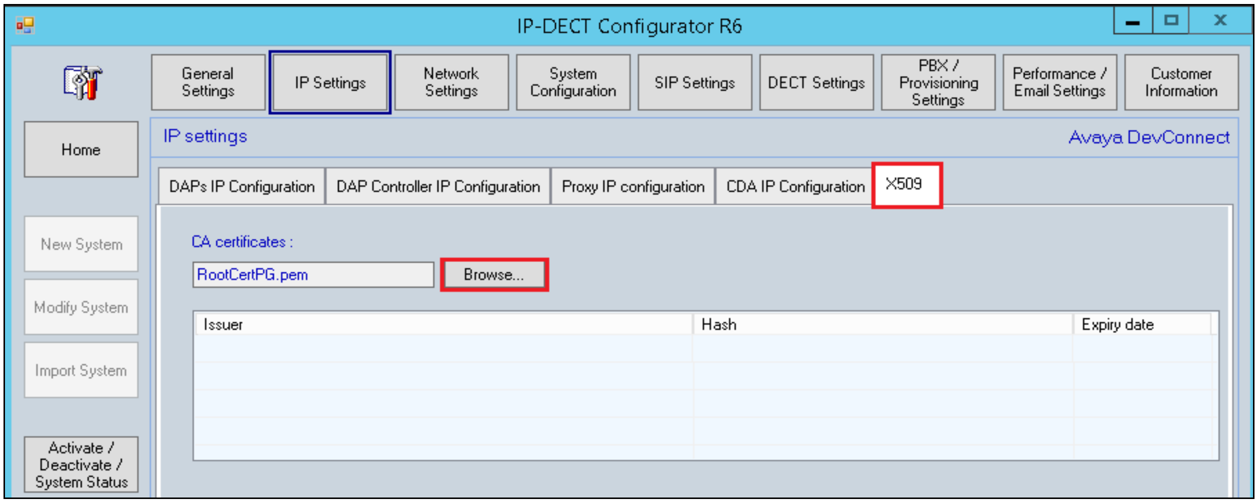
Proxy Port number : 5061

○ Multiple gatekeepers

□ Strip DNR prefix

Index	IP address	Port	DNR prefix	Domain	PBX

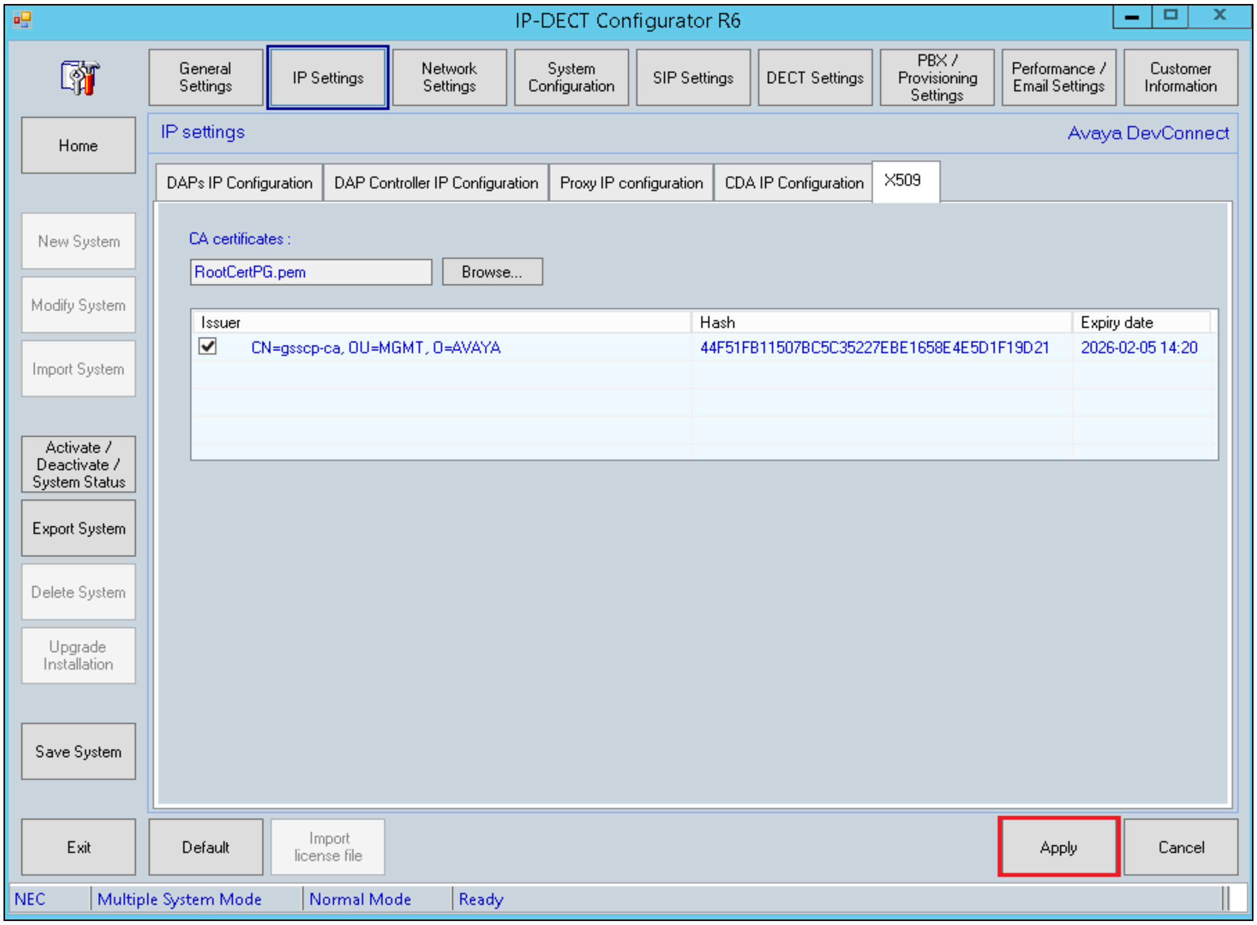
Click on the **X509** tab and import the Root Cert into the DAP Controller. This will be the same root cert that is being used on Session Manager so as when the DAP sends the cert to Session Manager it is the correct cert that is being sent.



CA certificates : RootCertPG.pem

Issuer	Hash	Expiry date

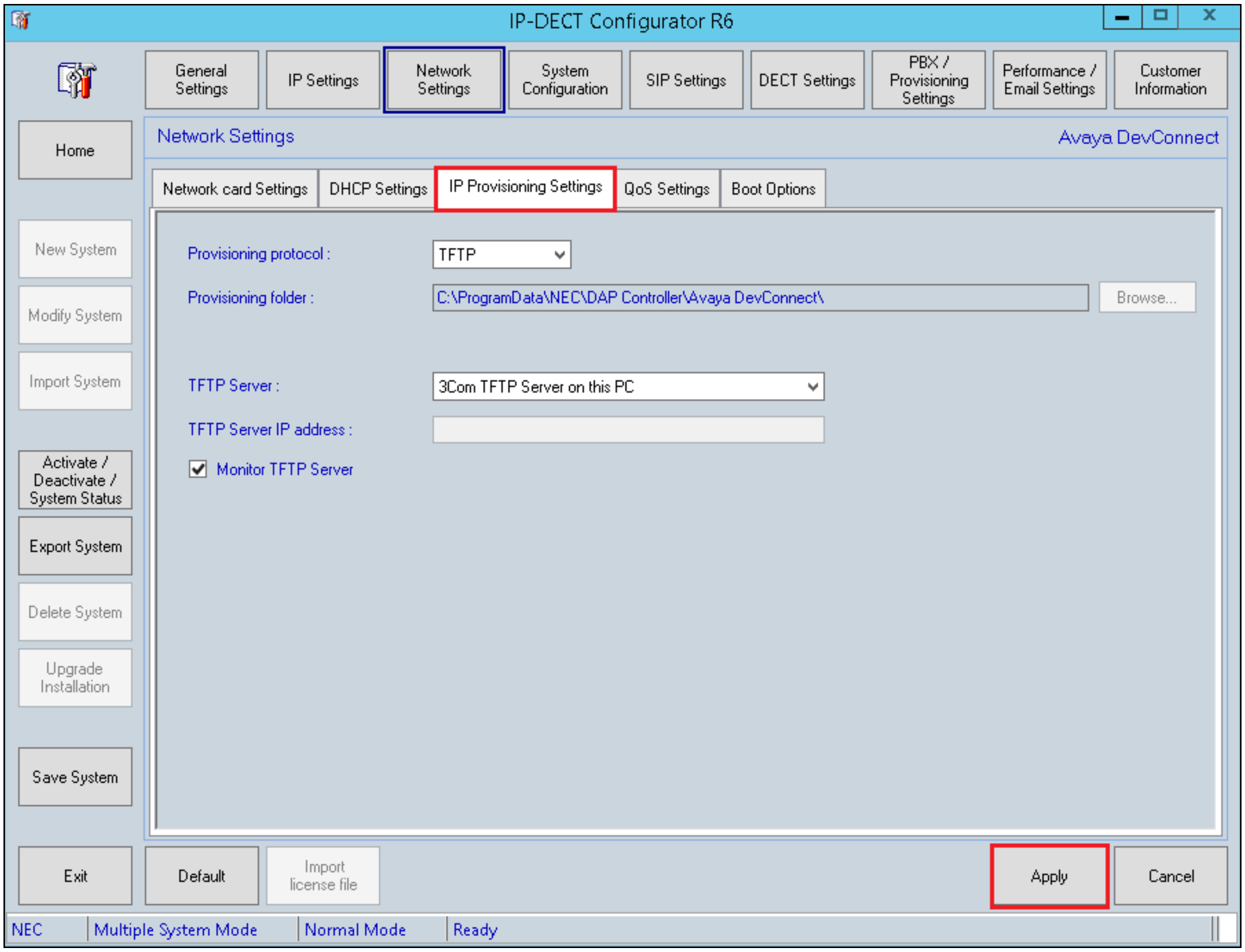
The following shows the imported cert information, click on **Apply** once done.



CA certificates : RootCertPG.pem

Issuer	Hash	Expiry date
☑ CN=gsscp-ca, OU=MGMT, O=AVAYA	44F51FB11507BC5C35227EBE1658E4E5D1F19D21	2026-02-05 14:20

Click on **Network Settings** at the top of the page and within this tab select the **IP Provisioning Settings** tab to check the **TFTP** details. The NEC DAP Controller sever can be setup as a TFTP server which will send any and all details to each DAP using TFTP. This information should be filled in automatically but the screen shot below shows the setup implemented for compliance testing. Once the information here is correctly filled in, click on **Apply** at the bottom of the page to continue.



Provisioning protocol : TFTP

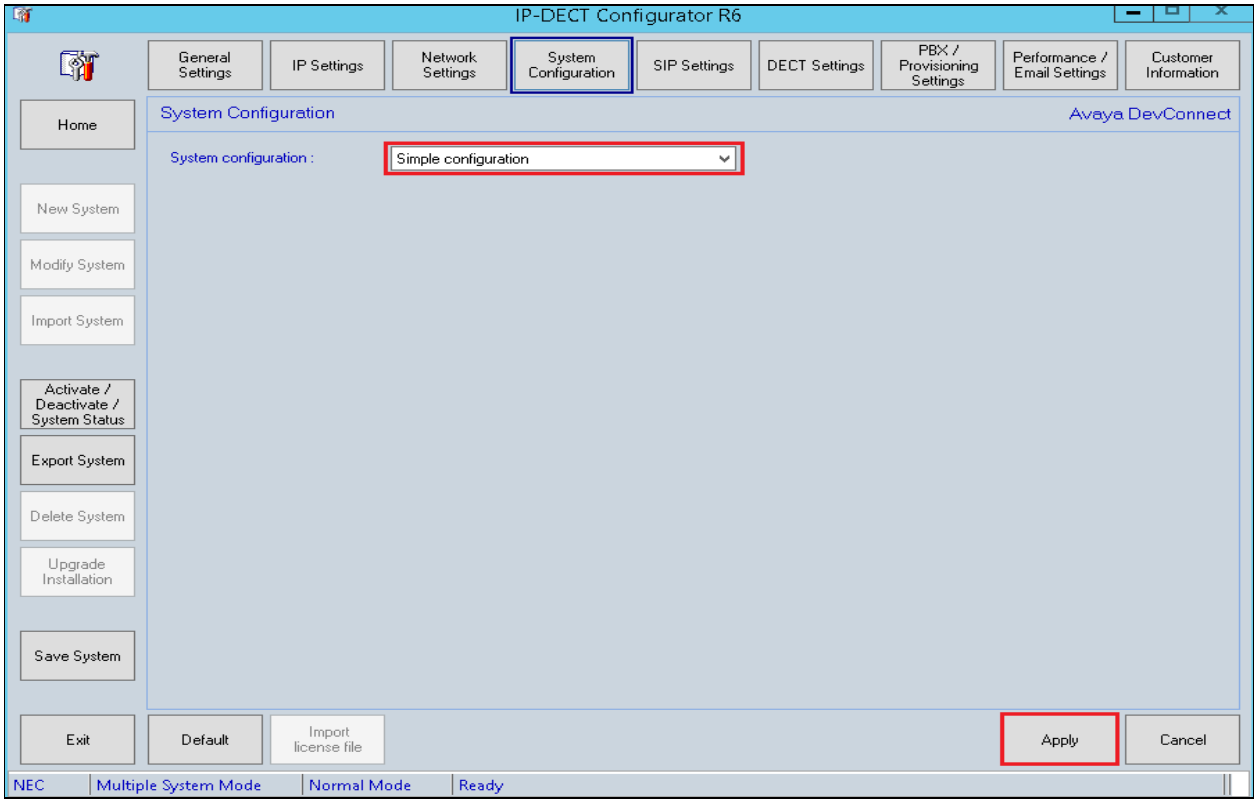
Provisioning folder : C:\ProgramData\NEC\DAP Controller\Avaya DevConnect\

TFTP Server : 3Com TFTP Server on this PC

TFTP Server IP address :

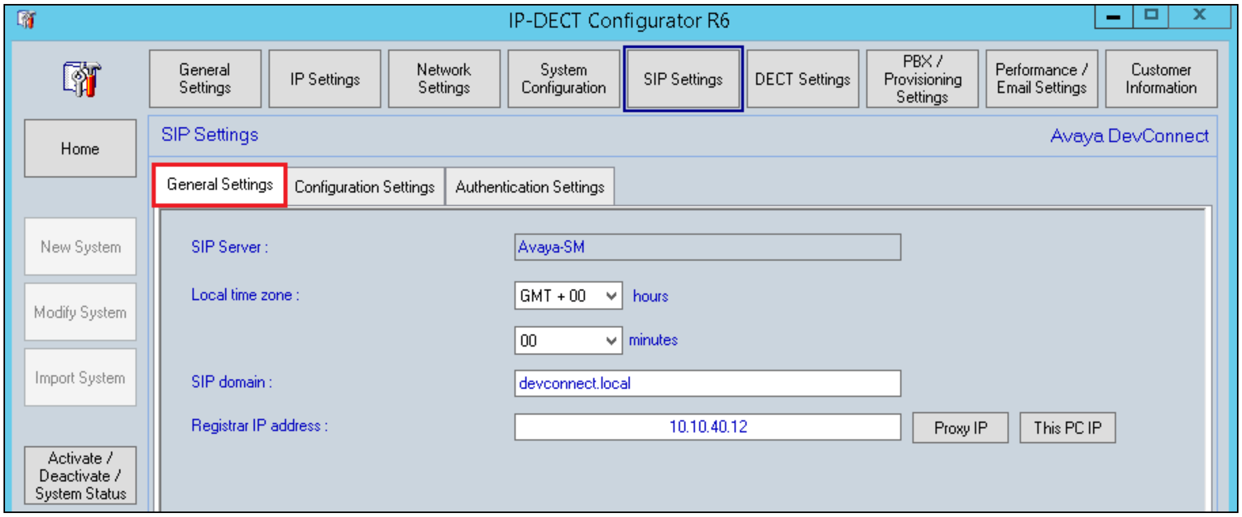
☑ Monitor TFTP Server

Click on **System Configuration** at the top of the page, the **System configuration** in the main window should display **Simple configuration** as shown below, click on **Apply** to continue.



System configuration : Simple configuration

Click on **SIP Settings** at the top of the page and the **General Settings** tab in the main window. The SIP Server details will be automatically filled in. Set the time zone and the **SIP domain**, note this is the same SIP domain featured in **Section 6.1**. Enter the Session Manager IP address for the **Registrar IP address**; typically this will be automatically filled in from the Proxy information (see Proxy IP Configuration setting from page 39).



SIP Server : Avaya-SM

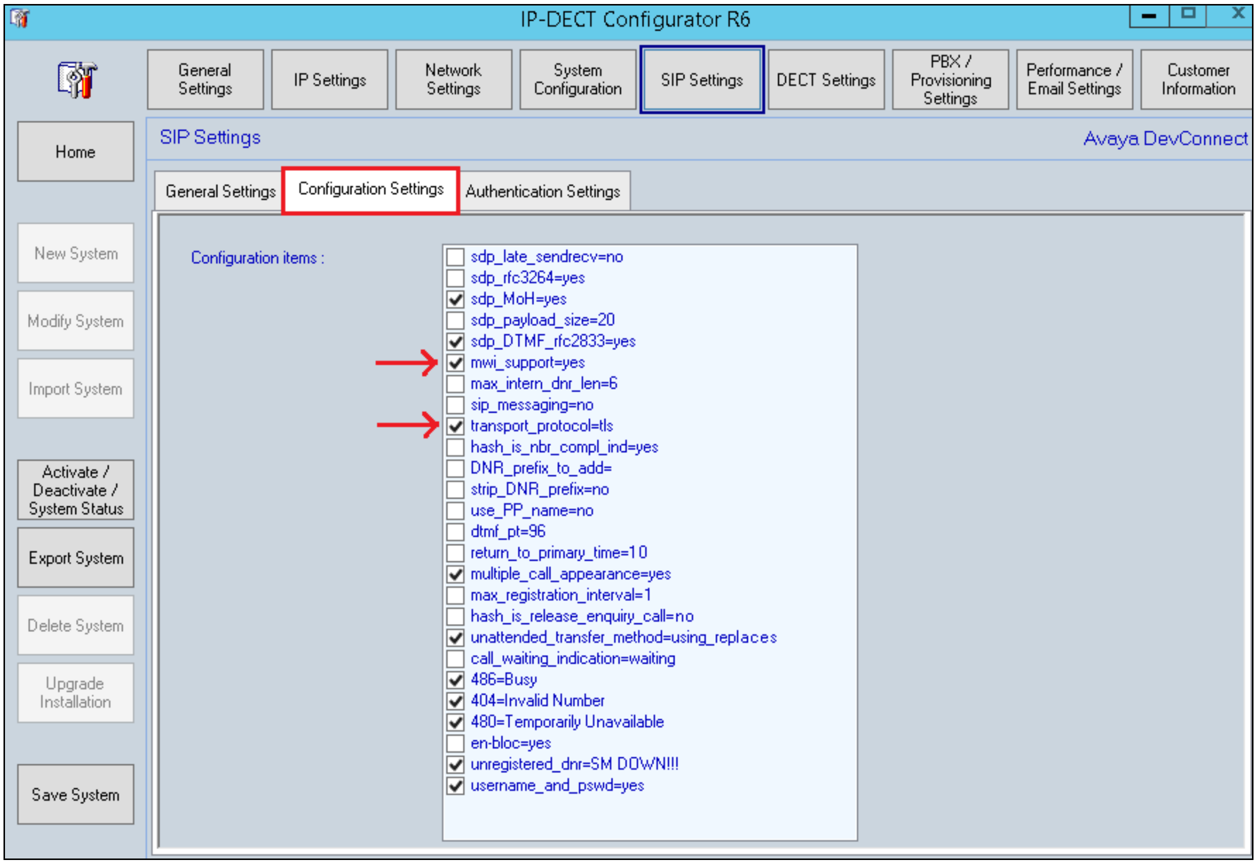
Local time zone : GMT + 00 hours

00 minutes

SIP domain : devconnect.local

Registrar IP address : 10.10.40.12

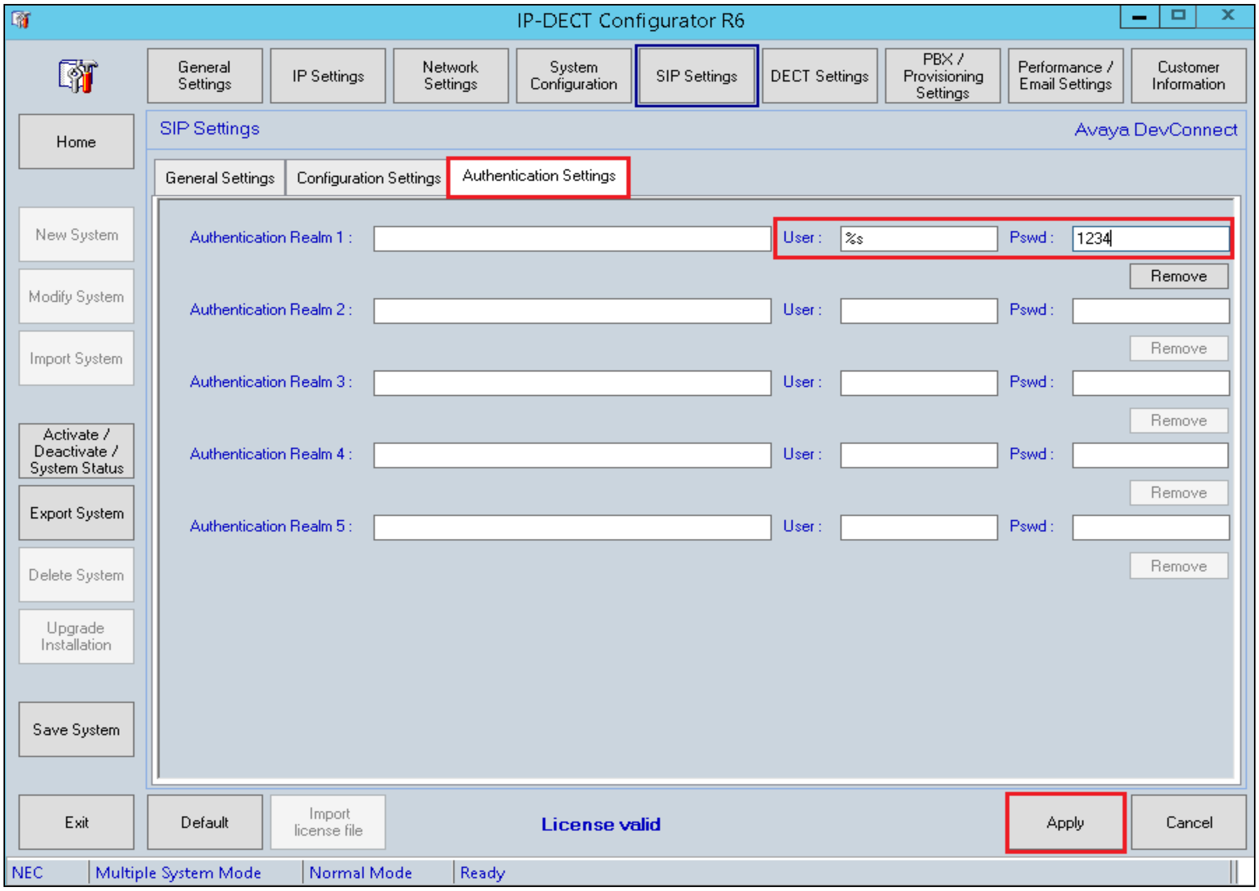
Click on **Configuration Settings** tab, the information will be automatically filled in but the screen shot below shows the settings used during compliance testing. The **transport_protocol** shows that **TLS** is being used and the **mwi_support=yes**. These settings can be changed here.



Configuration items :

☐ sdp_late_sendrecv=no
☐ sdp_rfc3264=yes
☑ sdp_MoH=yes
☐ sdp_payload_size=20
☑ sdp_DTMF_rfc2833=yes
☑ mwi_support=yes
☐ max_intern_dnr_len=6
☐ sip_messaging=no
☑ transport_protocol=tls
☐ hash_is_nbr_compl_ind=yes
☐ DNR_prefix_to_add=
☐ strip_DNR_prefix=no
☐ use_PP_name=no
☐ dtmf_pt=96
☐ return_to_primary_time=10
☑ multiple_call_appearance=yes
☐ max_registration_interval=1
☐ hash_is_release_enquiry_call=no
☑ unattended_transfer_method=using_replaces
☐ call_waiting_indication=waiting
☑ 486=Busy
☑ 404=Invalid Number
☑ 480=Temporarily Unavailable
☐ en-bloc=yes
☑ unregistered_dnr=SM DOWN!!!
☑ username_and_pswd=yes

Click on **Authentication Settings** tab and enter **%s** as the user (means the DNR will be used as the SIP extension) and **1234** as the password, note that this is the same password set in **Section 6.4**.



Authentication Realm 1 : User : %s Pswd : 1234

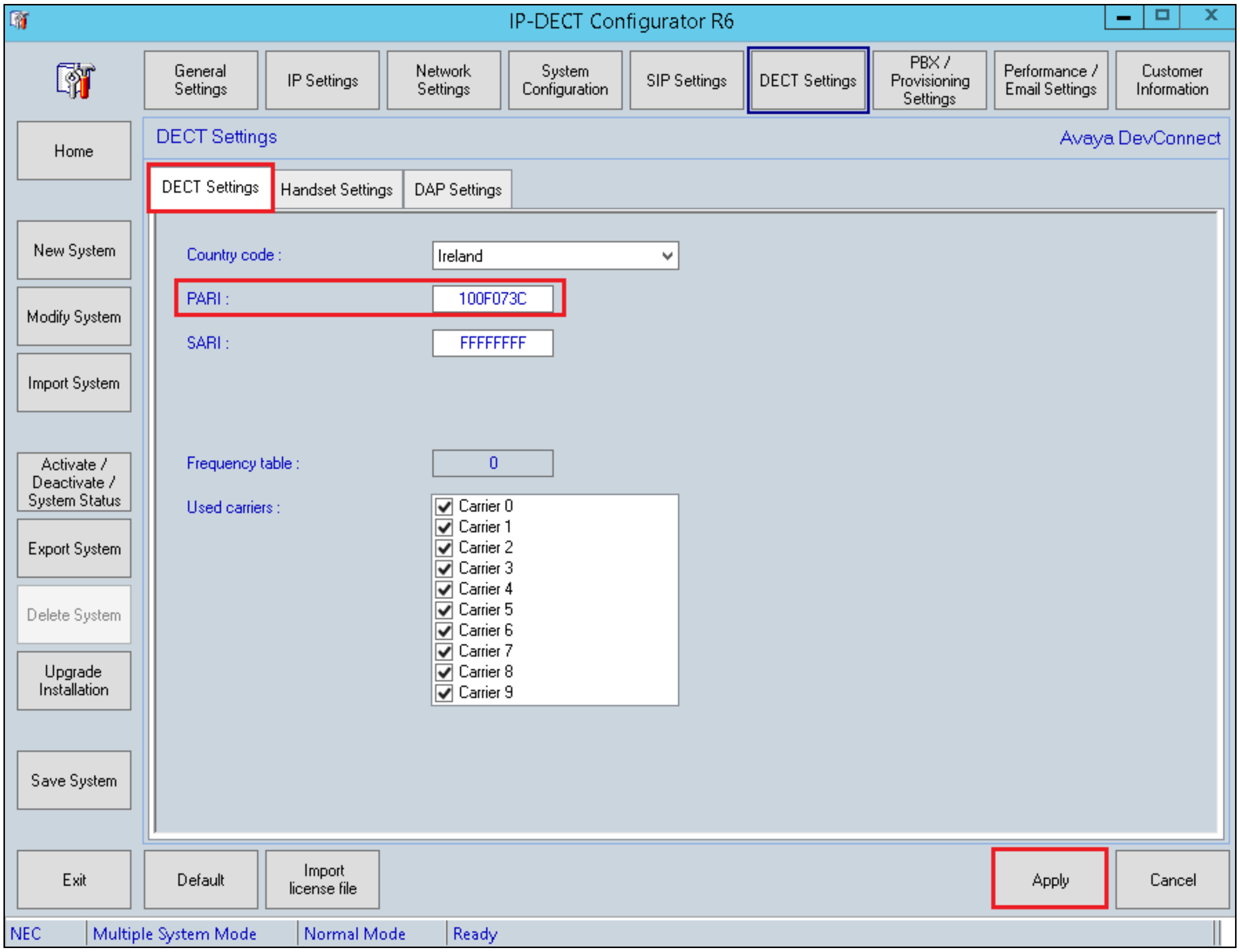
Authentication Realm 2 : User : Pswd :

Authentication Realm 3 : User : Pswd :

Authentication Realm 4 : User : Pswd :

Authentication Realm 5 : User : Pswd :

Click on **DECT Settings** at the top of the page and the **DECT Settings** tab in the main window. The **PARI** should be already filled in from the information provided by the license file. The **Country code** can be changed to suite and click on **Apply** once this information has been entered as the other tabs do not need to be changed.



Country code : Ireland

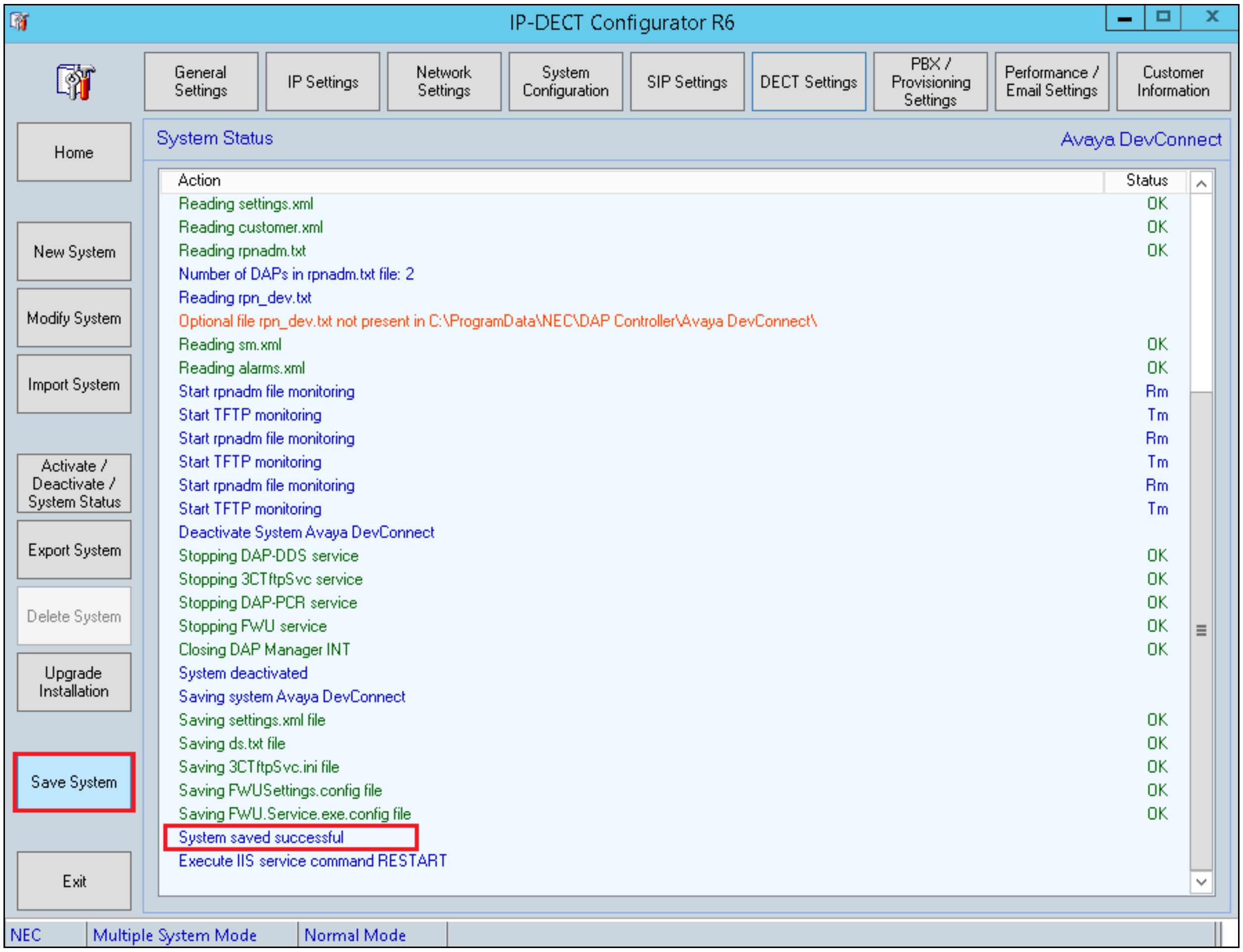
PARI : 100F073C

SARI : FFFFFFFF

Frequency table : 0

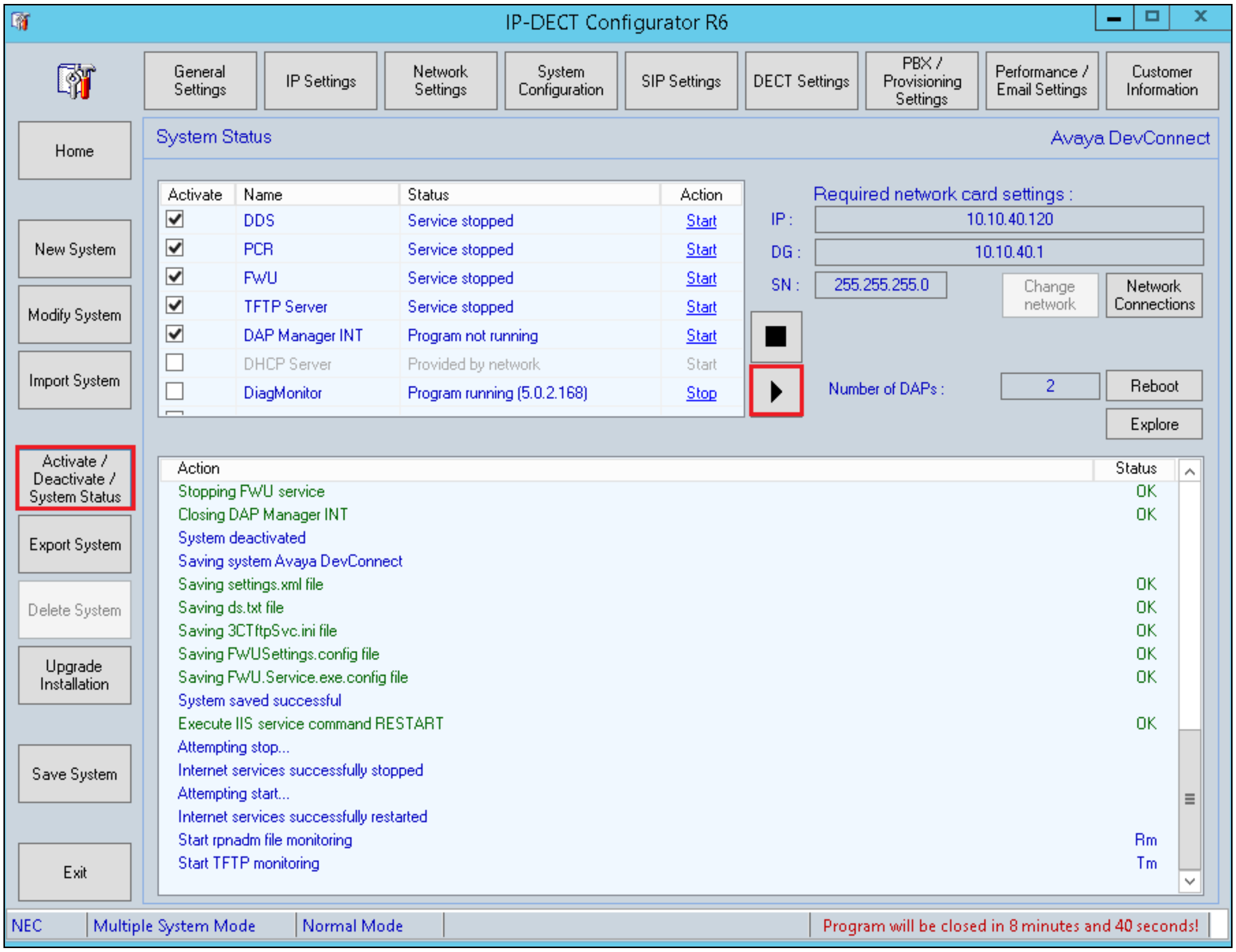
Used carriers :
☑ Carrier 0
☑ Carrier 1
☑ Carrier 2
☑ Carrier 3
☑ Carrier 4
☑ Carrier 5
☑ Carrier 6
☑ Carrier 7
☑ Carrier 8
☑ Carrier 9

Once **Save System** has been pressed at the bottom right of the screen the following will be displayed showing that the system has **saved successfully**.



Action	Status
Reading settings.xml	OK
Reading customer.xml	OK
Reading rpnadm.txt	OK
Number of DAPs in rpnadm.txt file: 2	
Reading rpn_dev.txt	
Optional file rpn_dev.txt not present in C:\ProgramData\NEC\DAP Controller\Avaya DevConnect\	
Reading sm.xml	OK
Reading alarms.xml	OK
Start rpnadm file monitoring	Rm
Start TFTP monitoring	Tm
Start rpnadm file monitoring	Rm
Start TFTP monitoring	Tm
Start rpnadm file monitoring	Rm
Start TFTP monitoring	Tm
Deactivate System Avaya DevConnect	
Stopping DAP-DDS service	OK
Stopping 3CTftpSvc service	OK
Stopping DAP-PCR service	OK
Stopping FWU service	OK
Closing DAP Manager INT	OK
System deactivated	
Saving system Avaya DevConnect	
Saving settings.xml file	OK
Saving ds.txt file	OK
Saving 3CTftpSvc.ini file	OK
Saving FWUSettings.config file	OK
Saving FWU.Service.exe.config file	OK
System saved successful	
Execute IIS service command RESTART	

Clicking on **Activate/Deactivate System Status** on the left side of the screen will bring a page on which a restart can be done by clicking the start icon (> button). The DAPs remain fully operational and making and receiving calls is still possible. The DAP controller is only necessary for Management actions regarding the handsets. Clicking on the start icon highlighted in the main screen will restart the system again after Activate/Deactivate System Status has been pressed.



System Status — Avaya DevConnect

Activate	Name	Status	Action
☑	DDS	Service stopped	Start
☑	PCR	Service stopped	Start
☑	FWU	Service stopped	Start
☑	TFTP Server	Service stopped	Start
☑	DAP Manager INT	Program not running	Start
☐	DHCP Server	Provided by network	Start
☐	DiagMonitor	Program running (5.0.2.168)	Stop

Required network card settings :

IP : 10.10.40.120

DG : 10.10.40.1

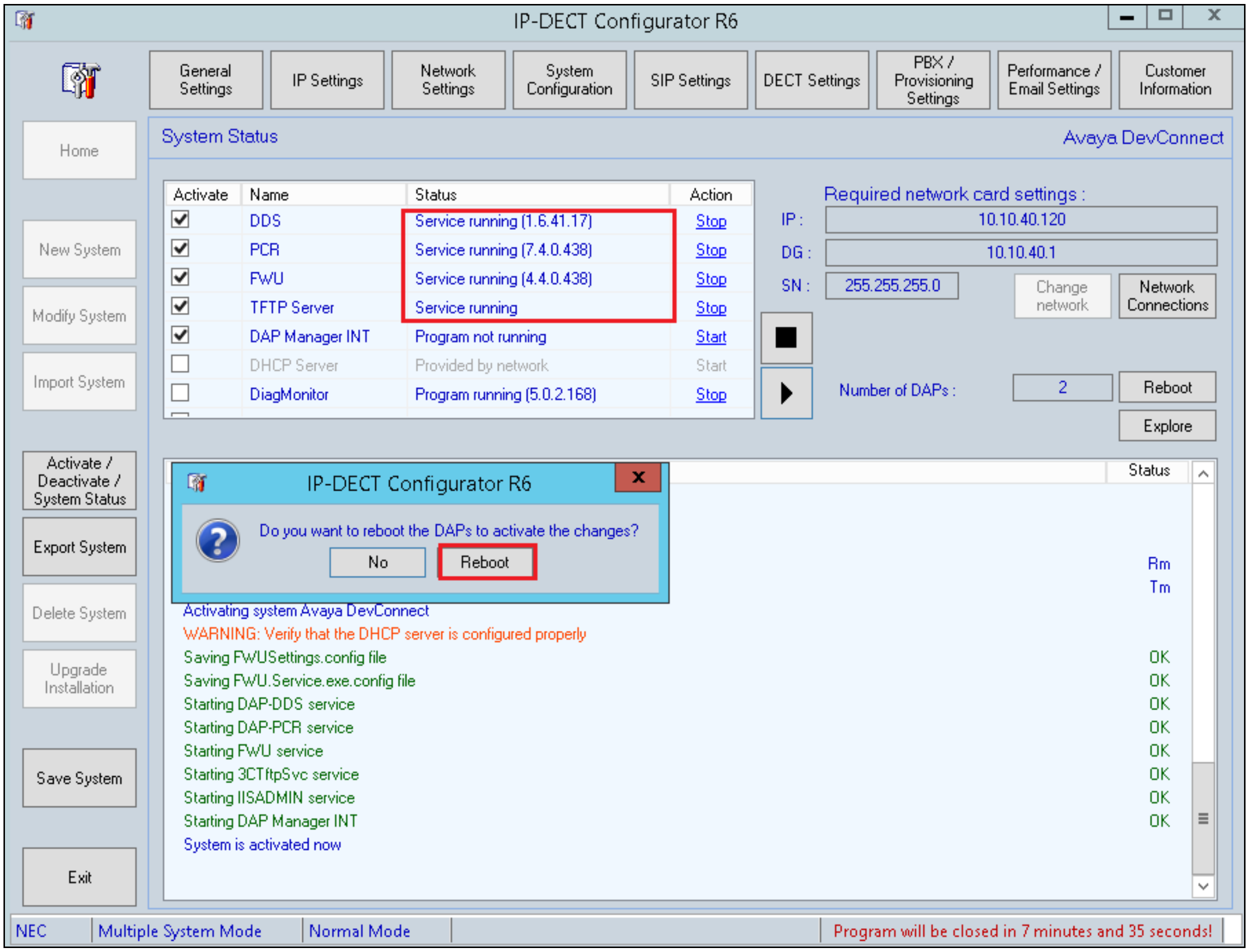
SN : 255.255.255.0

Number of DAPs : 2

```
Action                                              Status
Stopping FWU service                                OK
Closing DAP Manager INT                             OK
System deactivated
Saving system Avaya DevConnect
Saving settings.xml file                            OK
Saving ds.txt file                                  OK
Saving 3CTftpSvc.ini file                           OK
Saving FWUSettings.config file                      OK
Saving FWU.Service.exe.config file                  OK
System saved successful
Execute IIS service command RESTART                 OK
Attempting stop...
Internet services successfully stopped
Attempting start...
Internet services successfully restarted
Start rpnadm file monitoring                        Rm
Start TFTP monitoring                               Tm
```

NEC | Multiple System Mode | Normal Mode | Program will be closed in 8 minutes and 40 seconds!

With the system up and running again a window should automatically appear asking to reboot the DAP’s. Click on **Reboot** to complete the setup.



Activate	Name	Status	Action
☑	DDS	Service running (1.6.41.17)	Stop
☑	PCR	Service running (7.4.0.438)	Stop
☑	FWU	Service running (4.4.0.438)	Stop
☑	TFTP Server	Service running	Stop
☑	DAP Manager INT	Program not running	Start
□	DHCP Server	Provided by network	Start
□	DiagMonitor	Program running (5.0.2.168)	Stop

Required network card settings :

IP : 10.10.40.120

DG : 10.10.40.1

SN : 255.255.255.0

Number of DAPs : 2

IP-DECT Configurator R6

Do you want to reboot the DAPs to activate the changes?

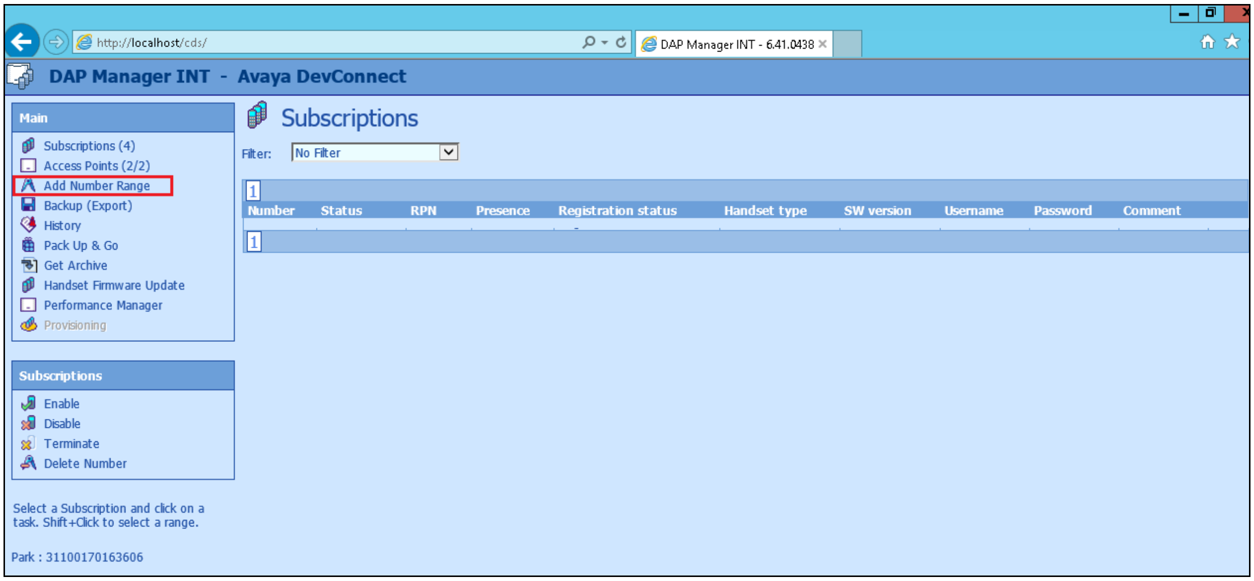
```
                                                        Rm
                                                        Tm
Activating system Avaya DevConnect
WARNING: Verify that the DHCP server is configured properly
Saving FWUSettings.config file                          OK
Saving FWU.Service.exe.config file                      OK
Starting DAP-DDS service                                OK
Starting DAP-PCR service                                OK
Starting FWU service                                    OK
Starting 3CTftpSvc service                              OK
Starting IISADMIN service                               OK
Starting DAP Manager INT                                OK
System is activated now
```

NEC | Multiple System Mode | Normal Mode | Program will be closed in 7 minutes and 35 seconds!

8.2. DAP Manager – Managing DECT users and handsets

Once the DAP configurator has been fully configured, the following window of the DAP manager is automatically popped. The DAP manager can also be reached by typing the following URL http://<IP-of-DAP-manager>/cds/. The DAP manager is used to manage the extensions (DNR) on the DECT system and also to subscribe the DECT handsets.

Click on **Add Number Range** in the left window.

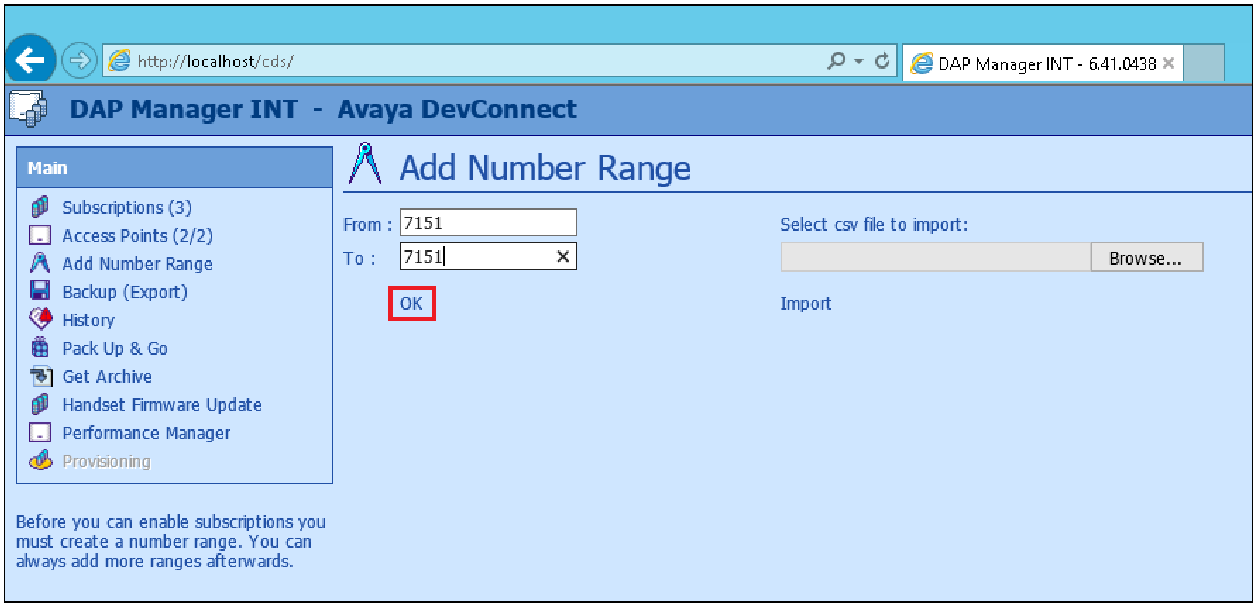


Filter: No Filter

Select a Subscription and click on a task. Shift+Click to select a range.

Park : 31100170163606

Enter the number range or the number of the extension(s) to be added and click on **OK**.

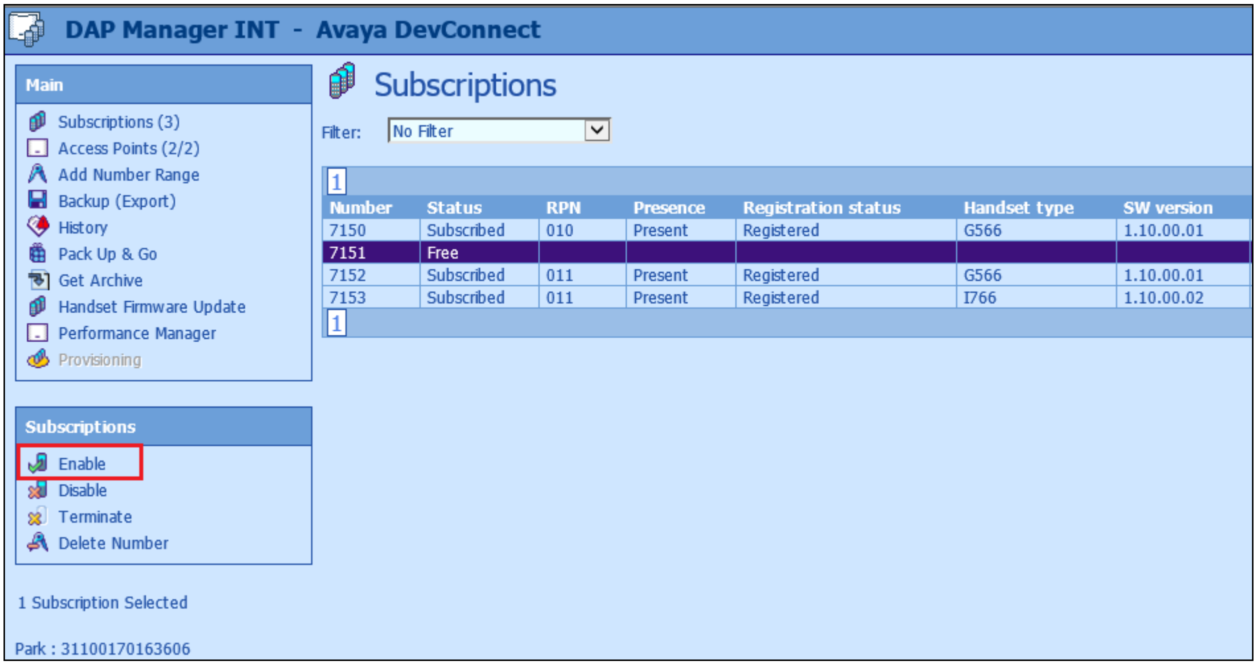


From : 7151

To : 7151

Before you can enable subscriptions you must create a number range. You can always add more ranges afterwards.

Highlight the new extension added in the main window and click on **Enable** in the left window.



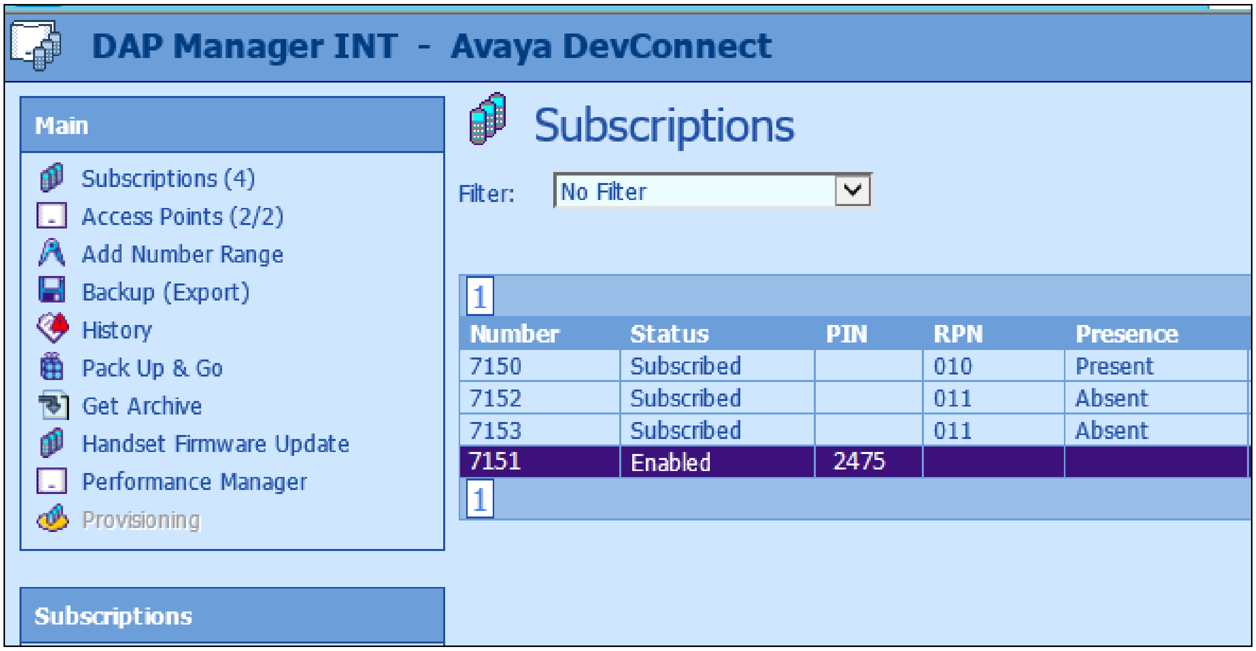
Filter: No Filter

Number	Status	RPN	Presence	Registration status	Handset type	SW version
7150	Subscribed	010	Present	Registered	G566	1.10.00.01
7151	Free					
7152	Subscribed	011	Present	Registered	G566	1.10.00.01
7153	Subscribed	011	Present	Registered	I766	1.10.00.02

1 Subscription Selected

Park : 31100170163606

Note the **PIN** number which will be used to subscribe the handset in the next section.

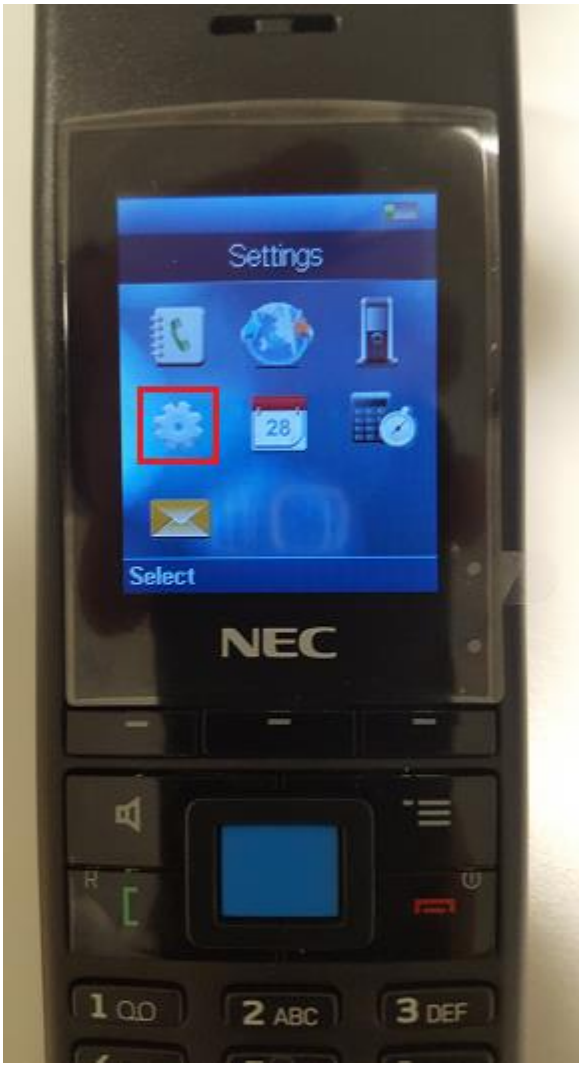


Filter: No Filter

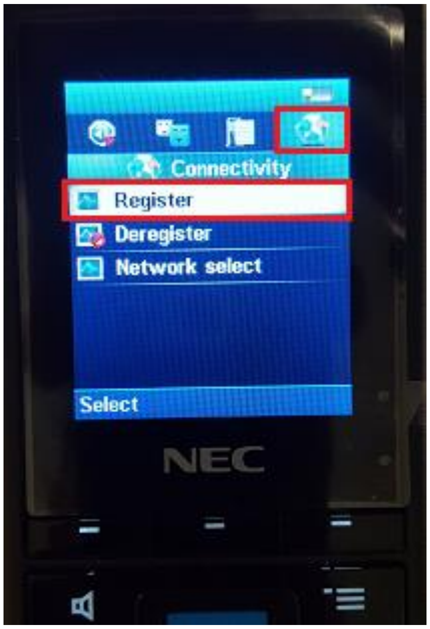
Number	Status	PIN	RPN	Presence
7150	Subscribed		010	Present
7152	Subscribed		011	Absent
7153	Subscribed		011	Absent
7151	Enabled	2475		

8.3. How to Subscribe the DECT Handset

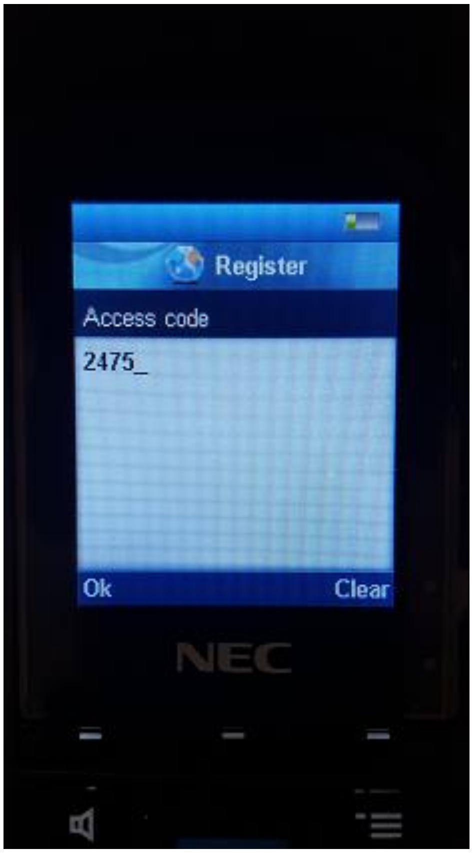
From the DECT handset click on the menu button (on top of the power button) and select **Settings** as highlighted below.



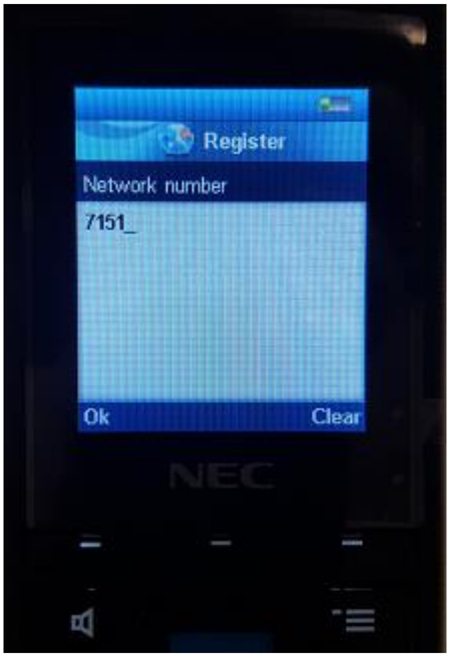
Scroll right to **Connectivity** and select **Register** as shown below.



There will be a number of slots labelled **Empty** (not shown) choose one and continue pressing Ok until the Access Code is asked for. Enter the **Access code** as per **Section 8.2**.



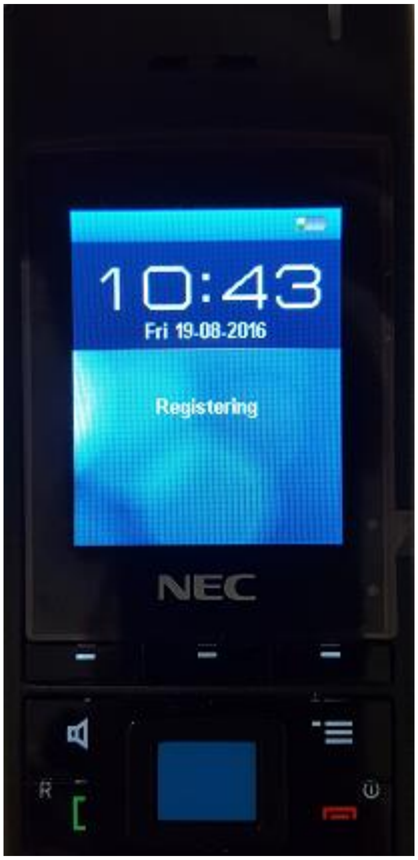
Enter the extension number for the **Network number** as shown below for extension **7151**.


Register

Network number

7151_

Once this are all entered the phoneset display should show **Registering**, as shown below.


10:43

Fri 19-08-2016

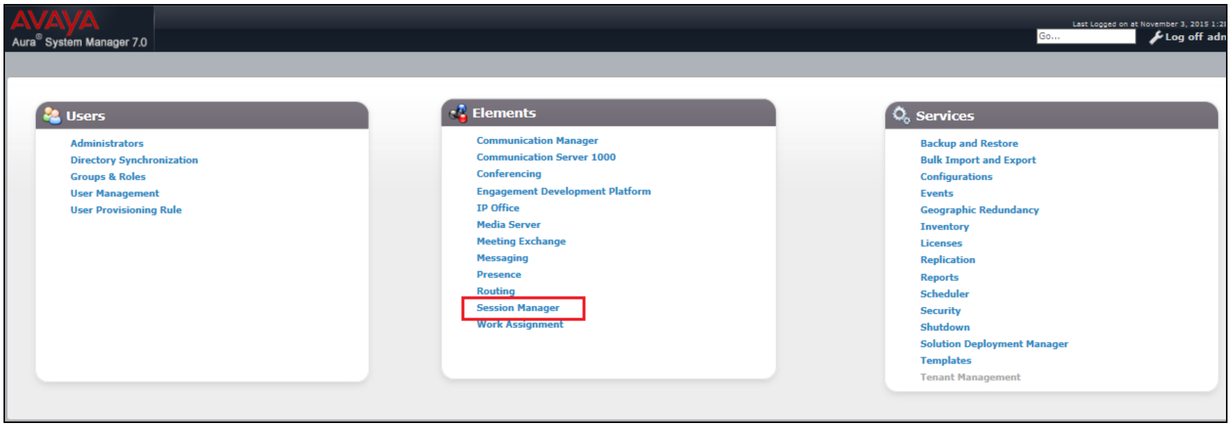
Registering

9. Verification Steps

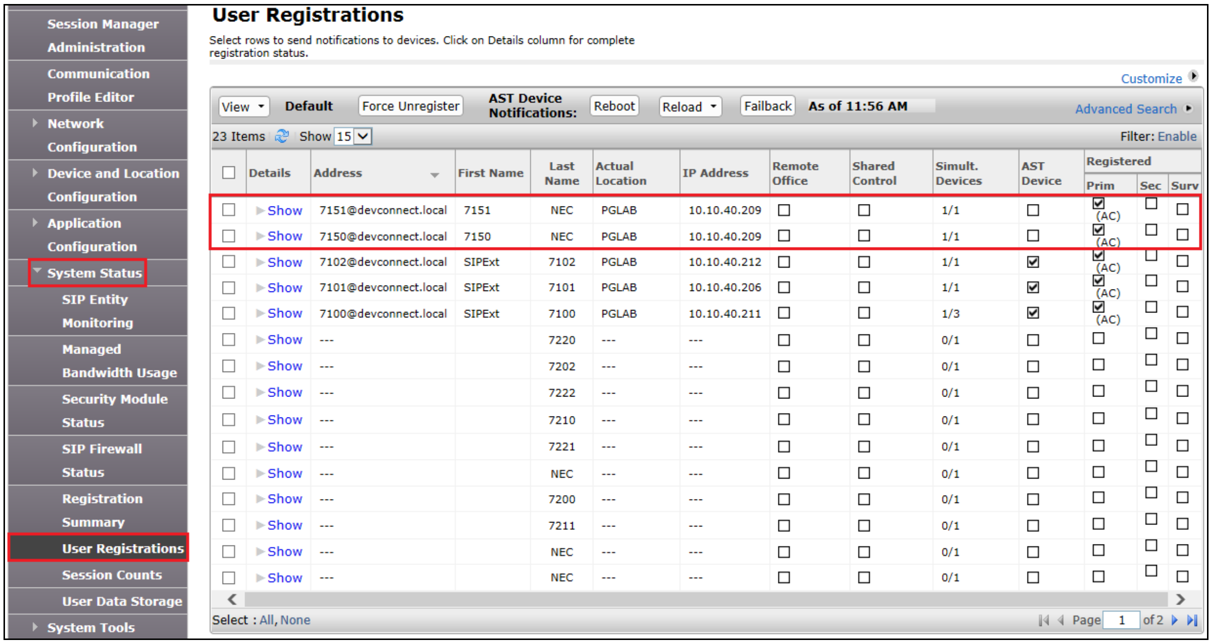
The ultimate test is to make and receive calls between the NEC DECT handsets and to and from the Avaya phones. This will verify that the NEC DECT handsets are connected correctly with the Avaya solution. The following steps can be taken to ensure that connections between NEC DECT handsets and Session Manager and Communication Manager are up.

9.1. Session Manager Registration

Log into System Manager as done previously in **Section 6.1**, select **Session Manager** as highlighted below.



Under **System Status** in the left window, select **User Registrations** to display all the SIP users that are currently registered with Session Manager. The NEC DECT users should show as being registered as highlighted.



User Registrations

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

As of 11:56 AM

23 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	7151@devconnect.local	7151	NEC	PGLAB	10.10.40.209	□	□	1/1	□	☑ (AC)	□	□
□	Show	7150@devconnect.local	7150	NEC	PGLAB	10.10.40.209	□	□	1/1	□	☑ (AC)	□	□
□	Show	7102@devconnect.local	SIPExt	7102	PGLAB	10.10.40.212	□	□	1/1	☑	☑ (AC)	□	□
□	Show	7101@devconnect.local	SIPExt	7101	PGLAB	10.10.40.206	□	□	1/1	☑	☑ (AC)	□	□
□	Show	7100@devconnect.local	SIPExt	7100	PGLAB	10.10.40.211	□	□	1/3	☑	☑ (AC)	□	□
□	Show	---		7220	---	---	□	□	0/1	□	□	□	□
□	Show	---		7202	---	---	□	□	0/1	□	□	□	□
□	Show	---		7222	---	---	□	□	0/1	□	□	□	□
□	Show	---		7210	---	---	□	□	0/1	□	□	□	□
□	Show	---		7221	---	---	□	□	0/1	□	□	□	□
□	Show	---		NEC	---	---	□	□	0/1	□	□	□	□
□	Show	---		7200	---	---	□	□	0/1	□	□	□	□
□	Show	---		7211	---	---	□	□	0/1	□	□	□	□
□	Show	---		NEC	---	---	□	□	0/1	□	□	□	□
□	Show	---		NEC	---	---	□	□	0/1	□	□	□	□

Select : All, None

Page 1 of 2

10. Conclusion

These Application Notes describe the configuration steps required for NEC's IP DECT Access Point (DAP) and DECT handsets to successfully interoperate with Avaya Aura® Communication Manager R7.0 and Avaya Aura® Session Manager R7.0 by registering the NEC Handsets with Session Manager as third-party SIP phones. Please refer to **Section 2.1 and 2.2** for test results and observations.

11. 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] *Implementing Avaya Aura® Session Manager* Document ID 03-603473

[4] *Administering Avaya Aura® Session Manager*, Doc ID 03-603324

NEC's technical documentation is available from NEC or from http://businessnet.nec-enterprise.com.

[5] *NEC, 2016, Business Mobility IP DECT CE Manual for SIP Connectivity, R6.41*, available at http://businessnet.nec-enterprise.com

[6] *NEC, 2016, IP DECT Administrator Guide, R6.41*, available at http://businessnet.nec-enterprise.com

Appendix

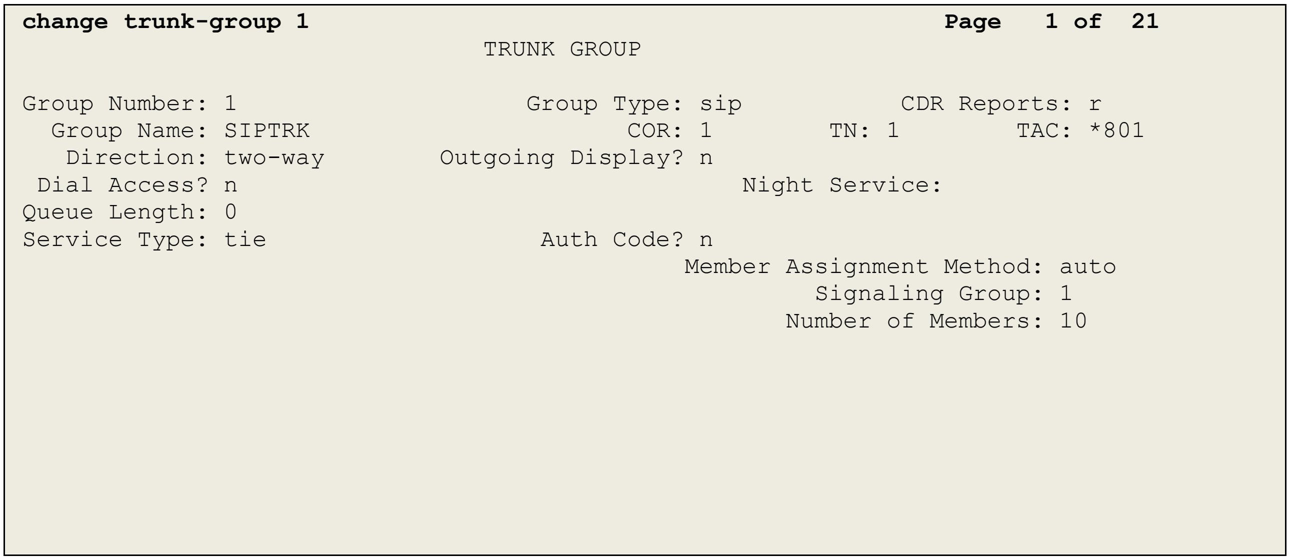
Configure SIP Trunk between Session Manager and Communication Manager

The following shows the SIP Signalling Group and SIP trunk that was used during compliance testing.

- Set the **Group Type** field to **sip**.
- For compliance testing **Transport Method** was set to **tls**.
- 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.
- Set the **Near-end Node Name** to **procr**. Set the **Far-end Node Name** to the node name defined for the Session Manager (node name **sm70vmpg**), as per **Section 5.5**.
- Ensure that the recommended TLS port value of **5061** 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 in **Section 5.** This field logically establishes the **far-end** for calls using this signaling group as network region 1.
- **Far-end Domain** was set to the domain used during compliance testing.
- The **DTMF over IP** field should remain set to the default value of **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- The **Direct IP-IP Audio Connections** field is set to **y**.
- **Initial IP-IP Direct Media** was set to **N** for compliance testing.
- The default values for the other fields may be used.

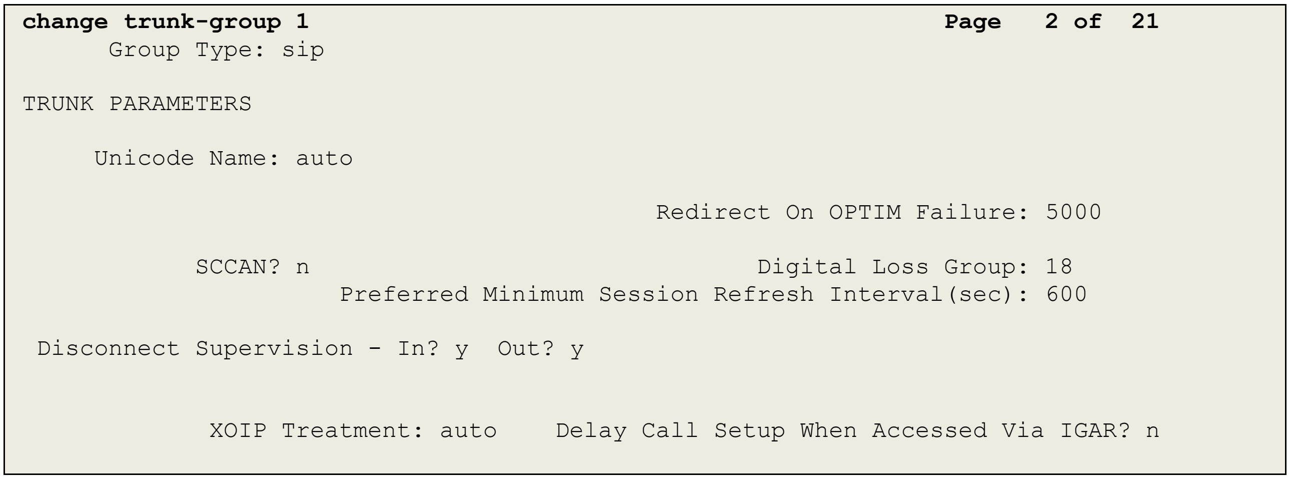
```
change signaling-group 1                                       Page   1 of   2
                                SIGNALING GROUP

 Group Number: 1              Group Type: sip
   IMS Enabled? n       Transport Method: tls
        Q-SIP? n
     IP Video? n                                   Enforce SIPS URI for SRTP? n
  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: sm70vmpg
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                        Far-end Network Region: 1

Far-end Domain: devconnect.local
                                             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? n
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: r
  Group Name: SIPTRK                      COR: 1        TN: 1        TAC: *801
   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: 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 NEC 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. However the **Numbering Format** in the example below is set to **private**.

```
change trunk-group 1                                            Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y



   Suppress # Outpulsing? n  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
```

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

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

                                       Mark Users as Phone? y
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                       Send Transferring Party Information? y
                                  Network Call Redirection? y
          Build Refer-To URI of REFER From Contact For NCR? n
                                     Send Diversion Header? n
                                   Support Request History? y
                              Telephone Event Payload Type: 120


                        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? n
                                              Enable Q-SIP? n

          Interworking of ISDN Clearing with In-Band Tones: keep-channel-active
                                Request URI Contents: may-have-extra-digits
```

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.