Sipgate configuration settings used on a BCM phone system to provide a new SIP account

Here are a few screen shots taken showing the settings that I used to set it up. I registered for free via the Sipgate residential basic service at www.sipgate.co.uk and all they require from you is a valid email address. You can from anywhere in the world select a free United Kingdom telephone number and this can also be a geographical or non-geographical number.

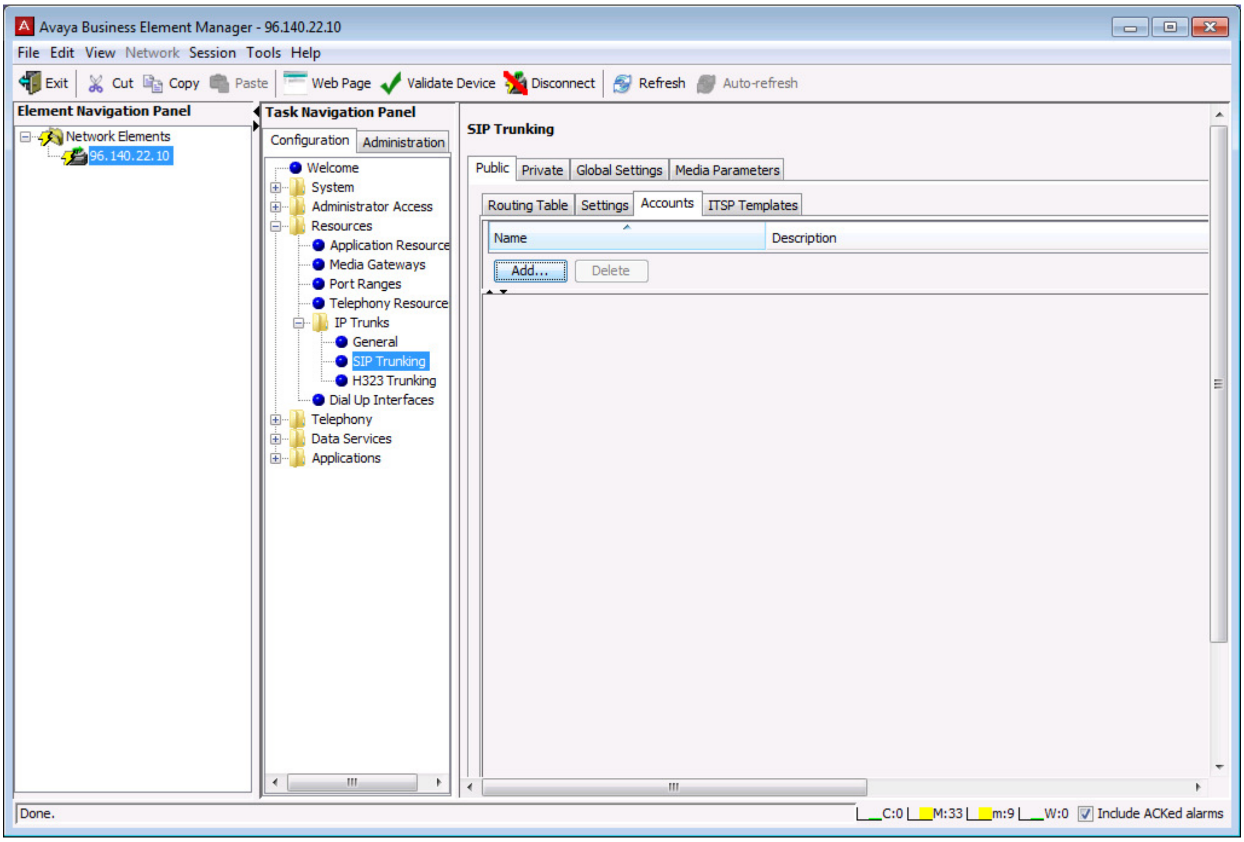
All UK geographical numbers start with 01, 02 or 03 and the non-geographical numbers are generally 08. The phone number will usually be 11 digits long and the good thing about this is that it will receive CLID and send CLID. There aren't any restrictions and of course the good thing here is that Sipgate to Sipgate calls are free. This means that I can make and receive calls from anyone else who has a Sipgate number connected and this can also be a PC Softphone, Mobile phone apps such as Zoiper,, SIP to analogue devices (e.g. Cisco Linksys 2 port adapter) and SIP trunks etc.

This is very handy for customers who want a UK presence to appear on their phone system that has SIP trunks and features enabled.

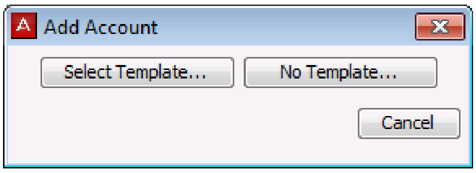
In the example below, I've explained (via screen shots) how I added an account on a BCM 50 at 6.0 and also that I gave it a two digit access code (73) that was set up in the routing table to allow me to dial out to other Sipgate users. If you are outside of the UK, you can still have this on your BCM system and configure it in the same way as I did. The first thing to do is to get an account registered!.

SIP Trunking (Public) and Accounts

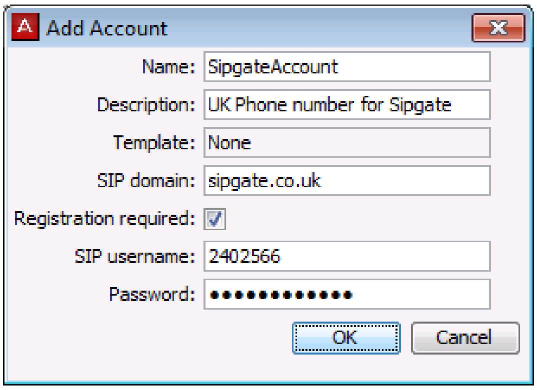
Log in with Element Manager and navigate to "Configuration", "Resources", "IP Trunks", "SIP Trunking", "Public" and "Accounts". Click on the tab option to "Add".



Select the “No Template…” box on the right.

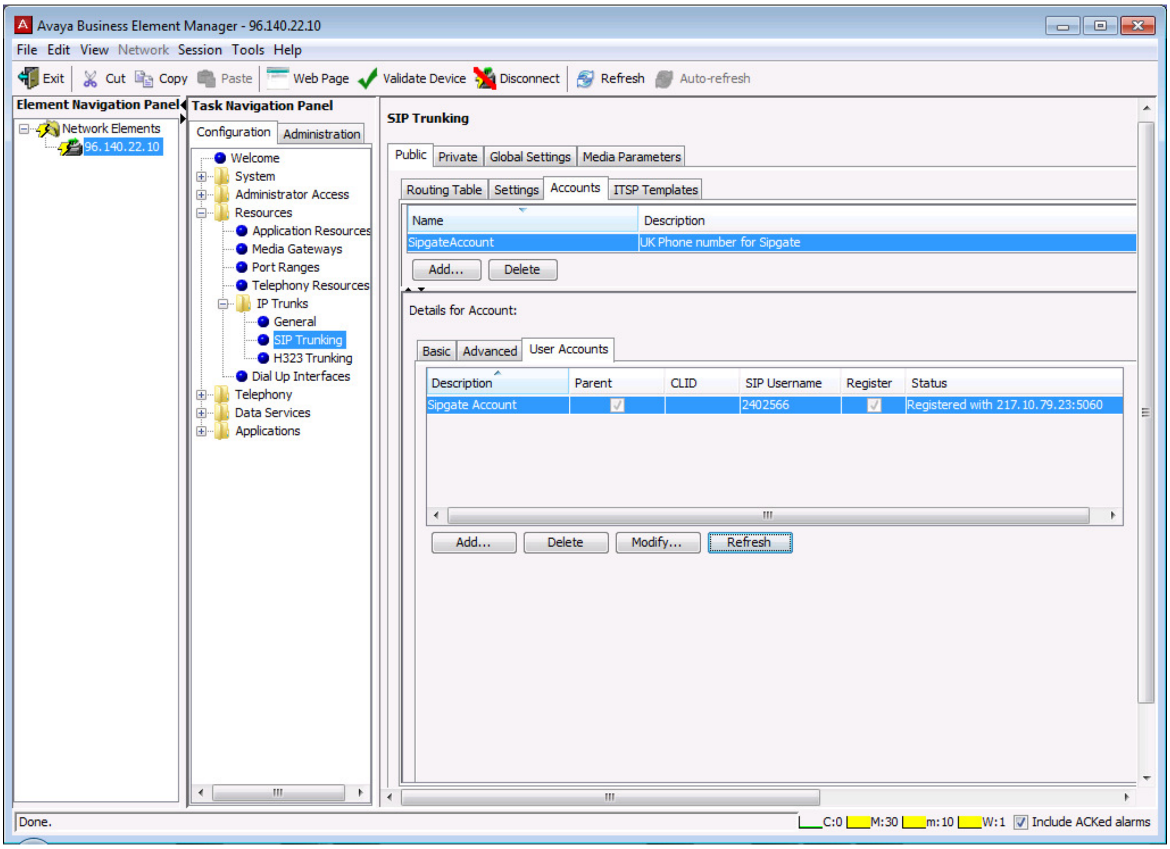


Fill in the details given to you via Sipgate as shown in the example below. The Name: and Description: entries can be whatever you want to use. Click OK, once completed.



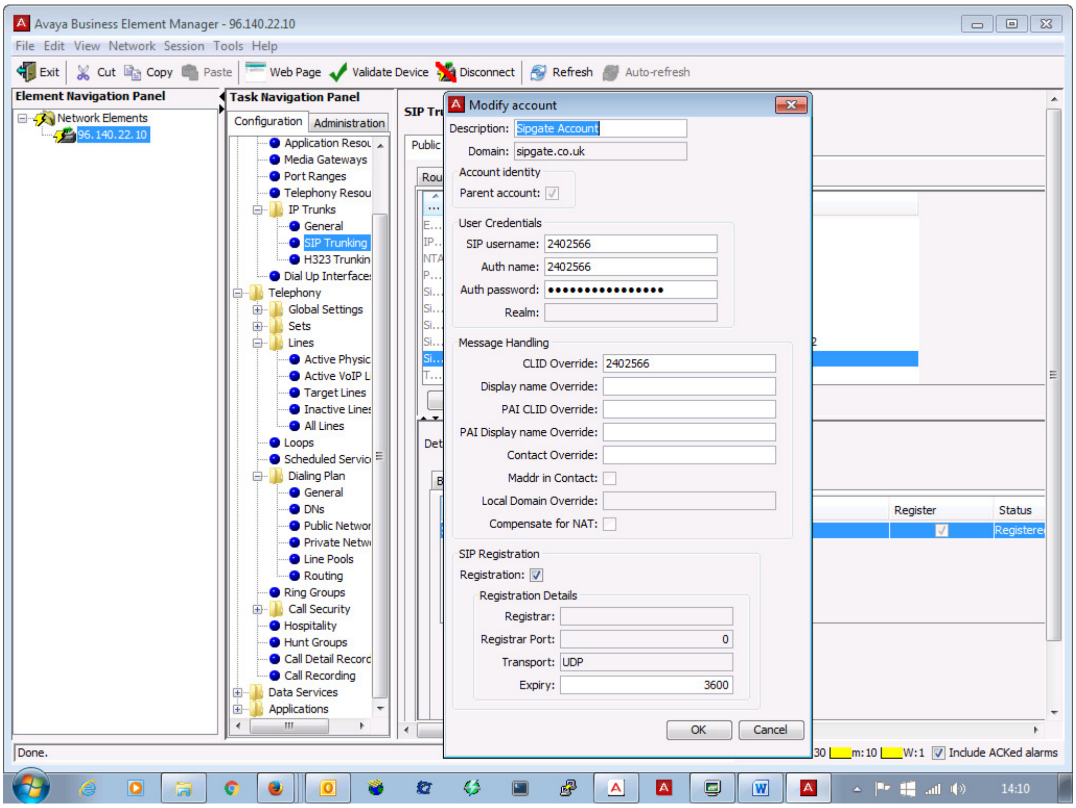
Making changes to the SIP account.

Now select the new SIP account entry by highlighting the line and click the sub tab “User Accounts”.

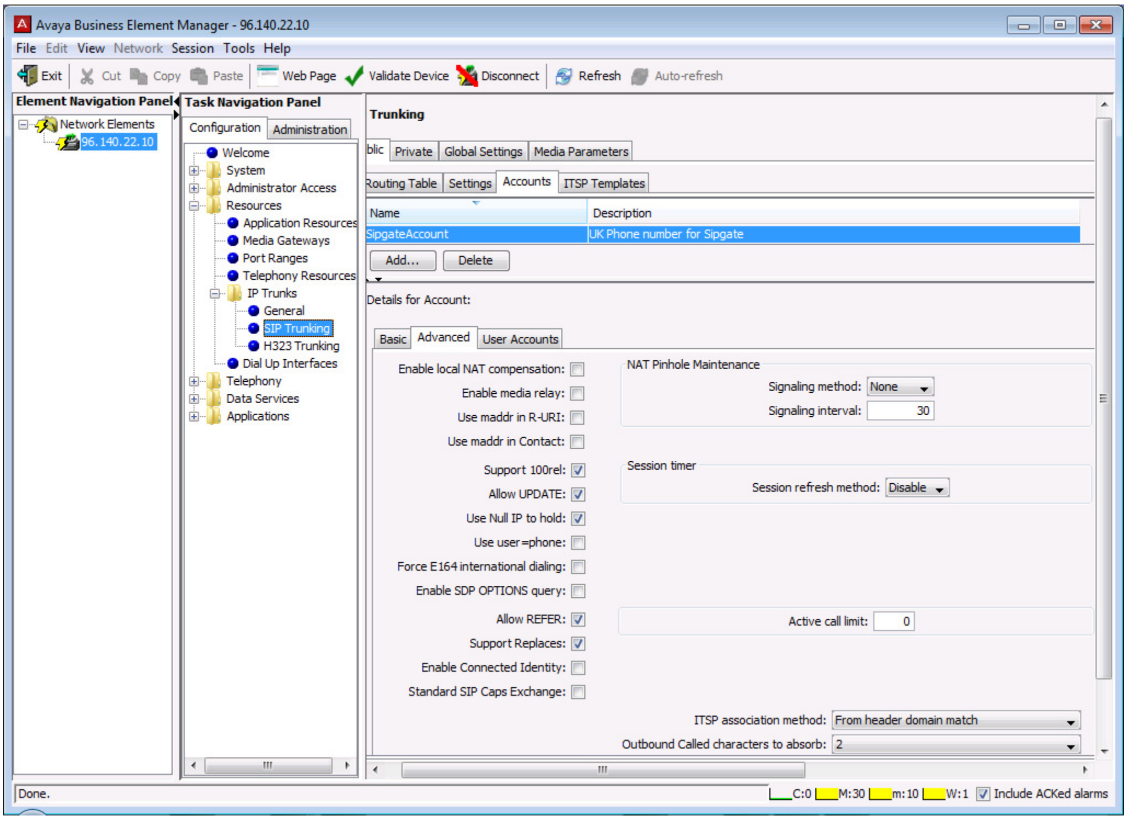


If the details were entered correctly, then you will see that it is now registered with Sipgate.

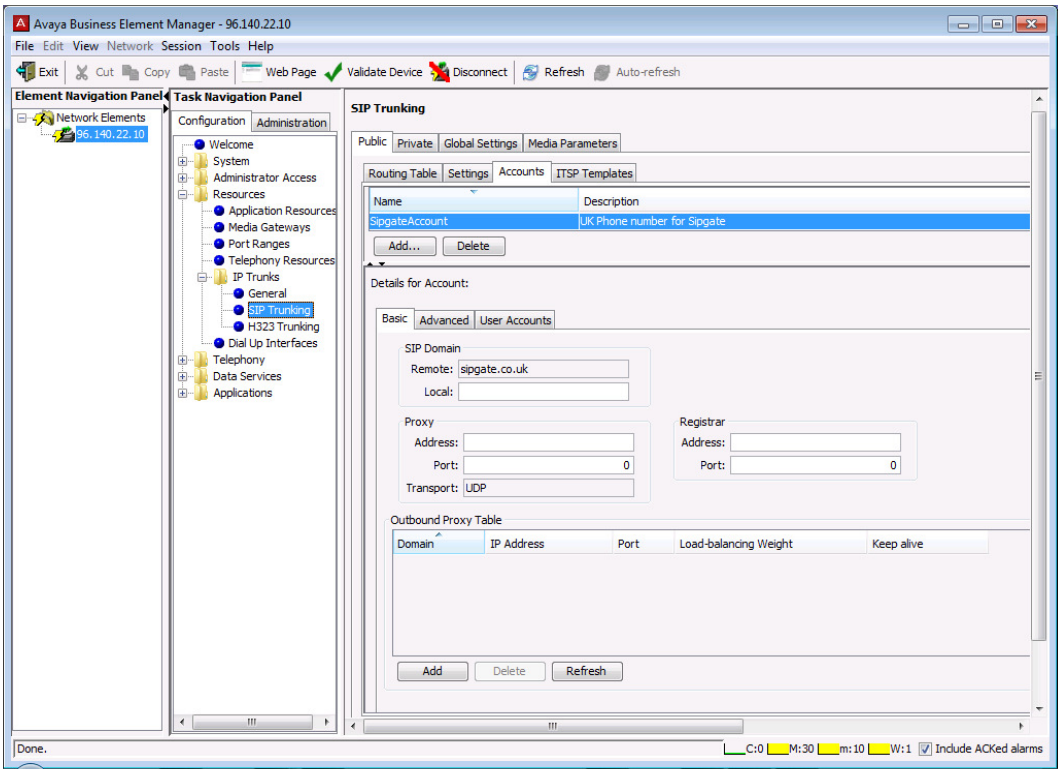
Whilst in this area, click on the “Modify…” tab. The SIP account number is the username, Auth name and CLID Overide which is also used in the target line, but only the first 7 digits are needed.
You don’t use the last two letters / digits that were supplied by Sipgate such as xxxxxxxe0 etc..



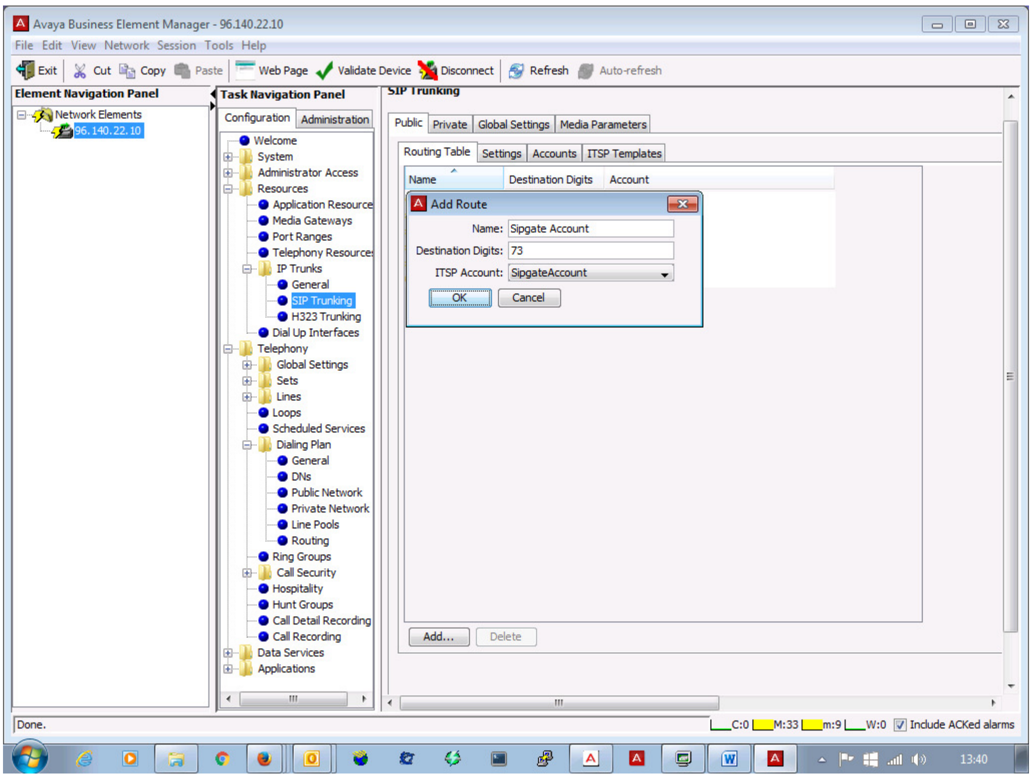
Now click left, on the “Advanced” tab to look at the settings where some areas might need changing.

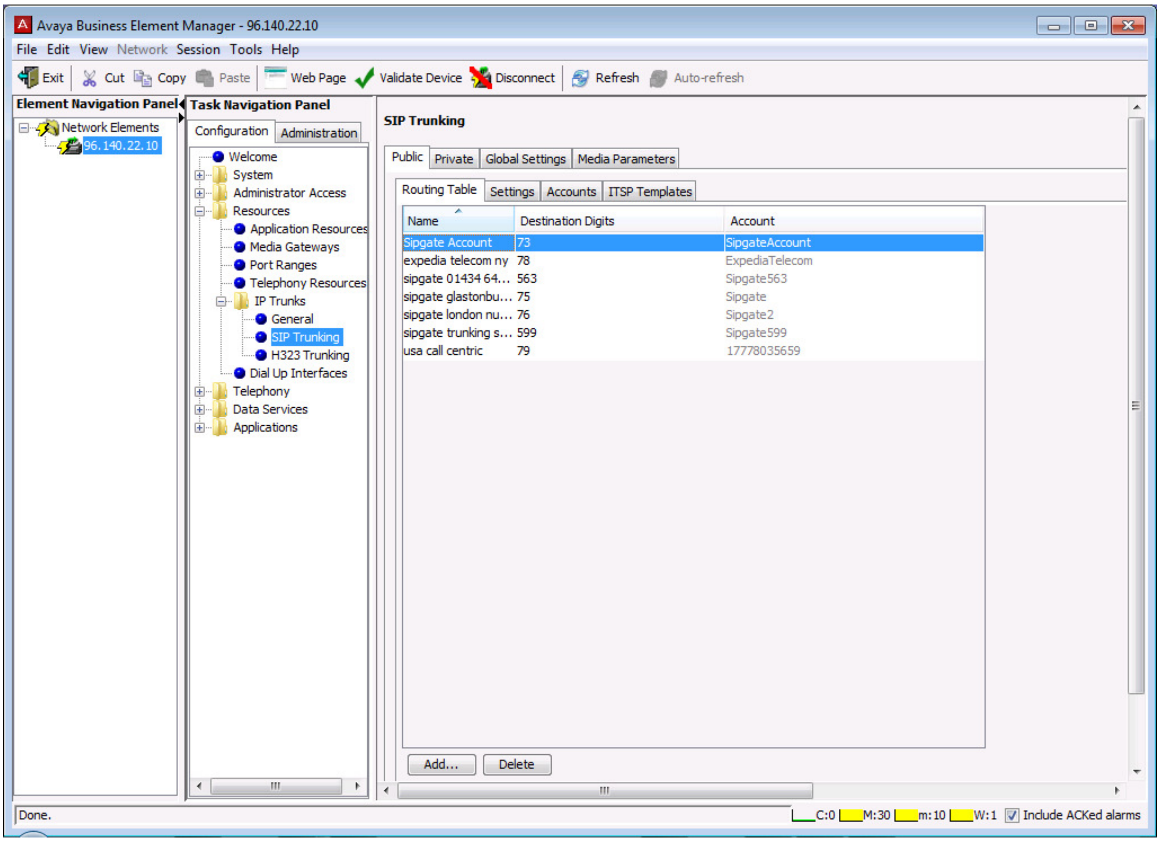


Note above that you need to set the “Outbound Called characters to absorb” (2) = 2 digts. What this means is that we will be using a 2 digit access code that is not sending out these digits to line.
Click left, for the “Basic” tab to look at the settings where some changes might need making.

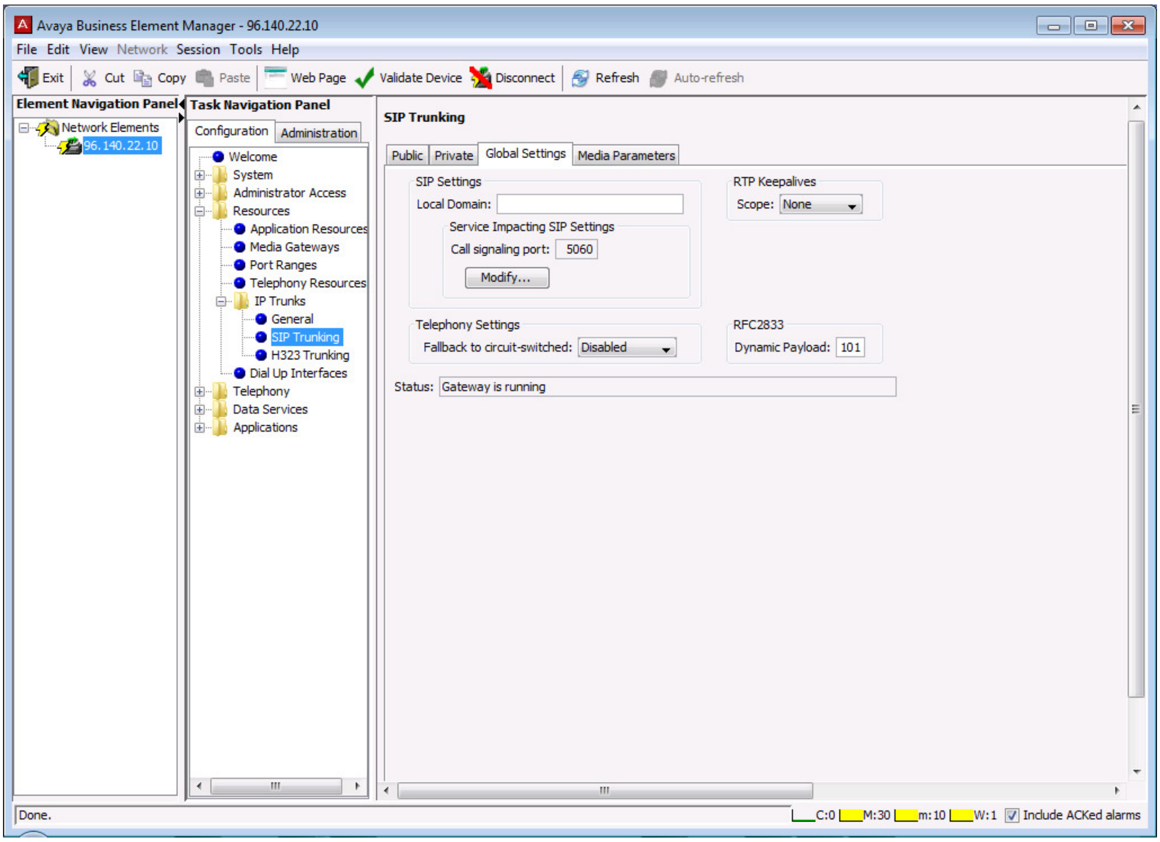


Navigate to “Configuration”, “Resources”, “IP Trunks”, “SIP Trunking”, “Public” and “Routing Table”. Click on the tab option to “Add”. This is where you add in a route to dial for the SIP trunk.

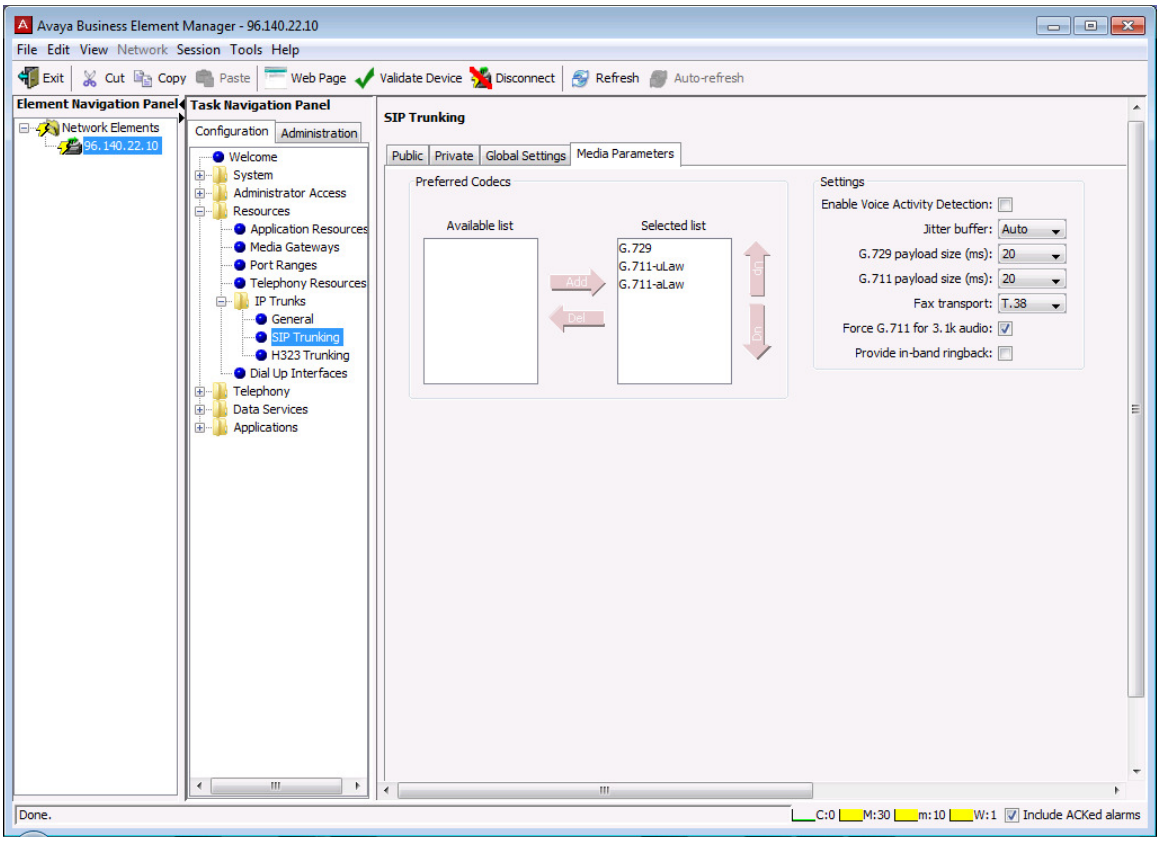




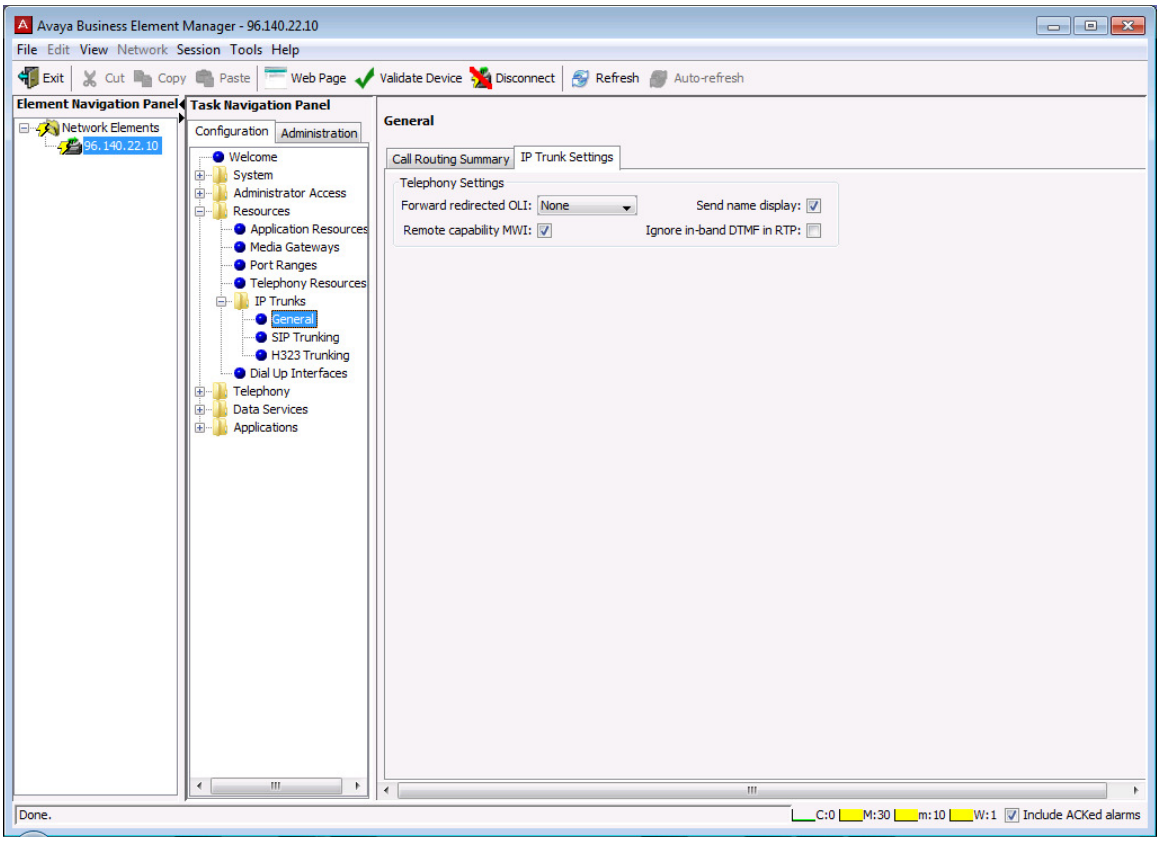
Global Settings



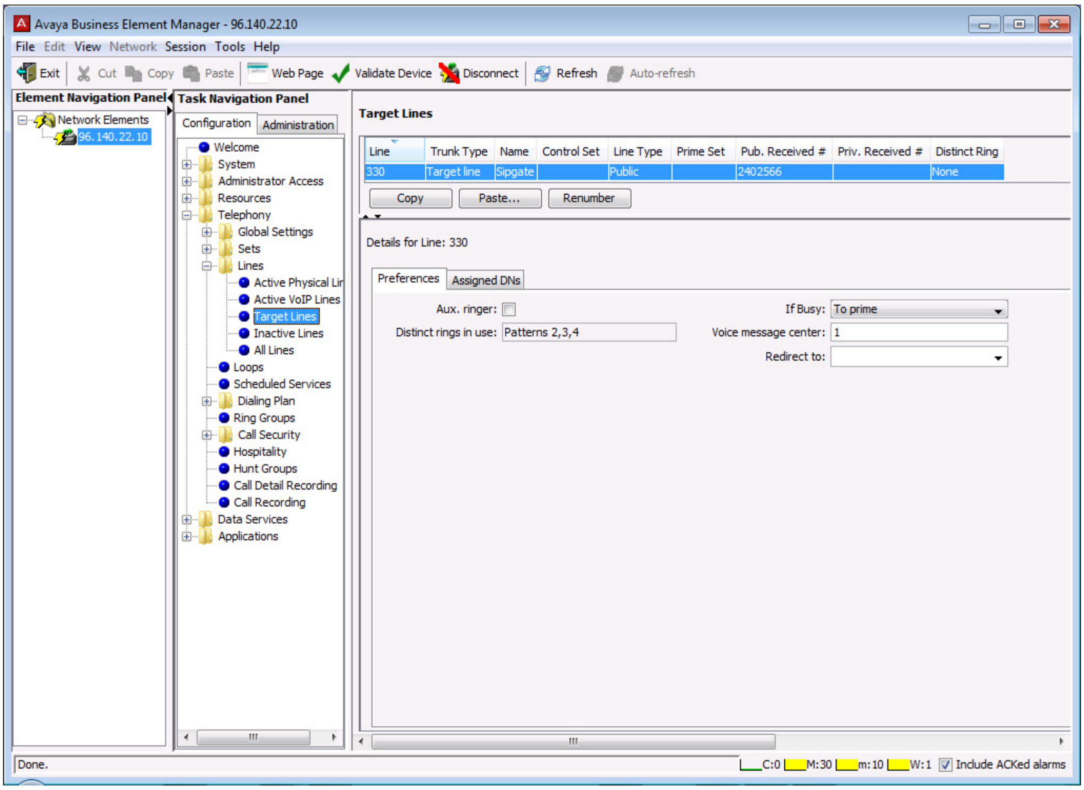
Media Parameters Some of these might need to be amended below.



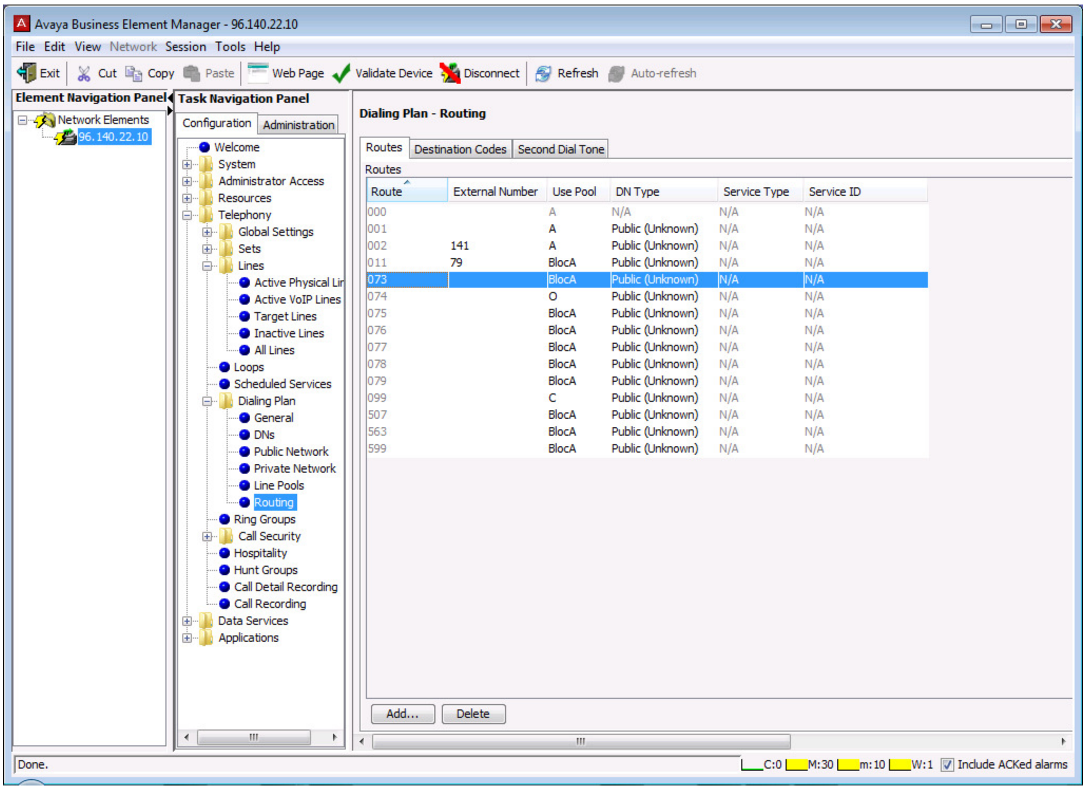
IP Trunks and General settings

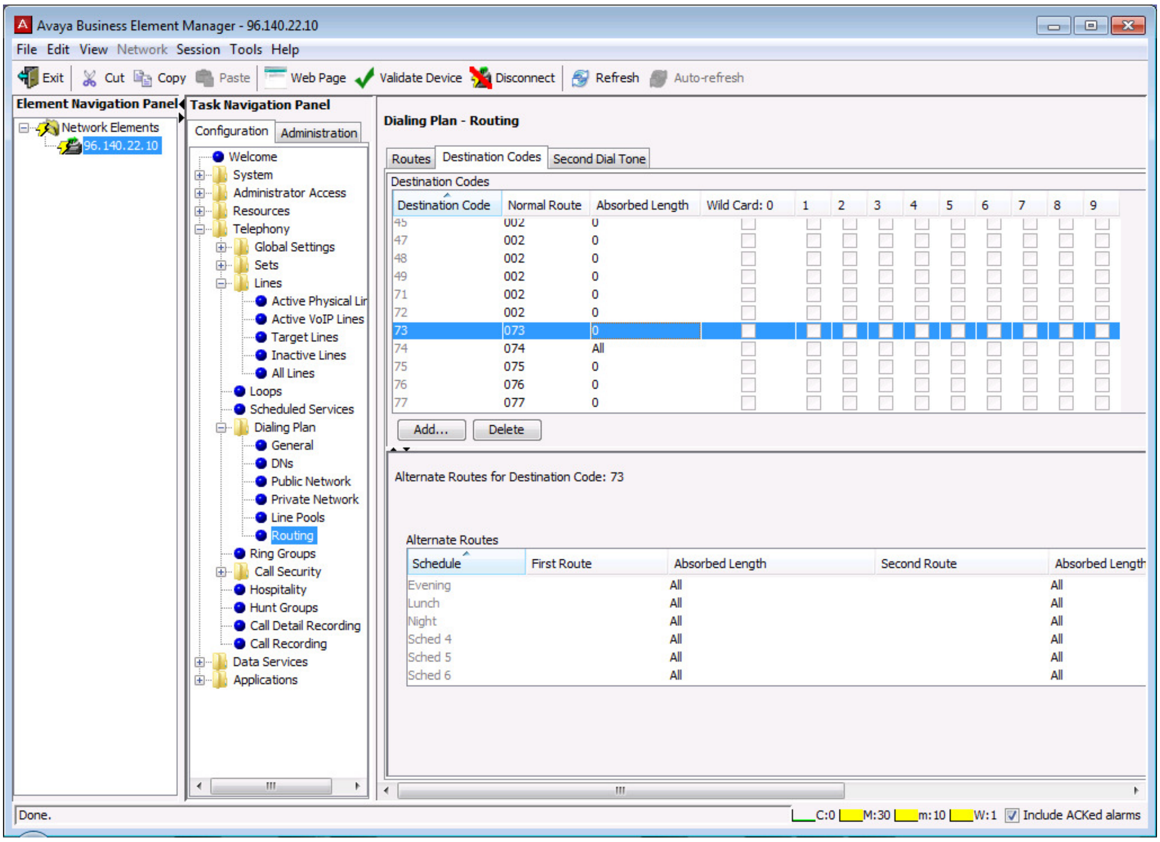


Finally, you need to set up the target line and routing tables. In my case, I used target line 330 to add in my Sipgate account in the Public Received # column as shown below.

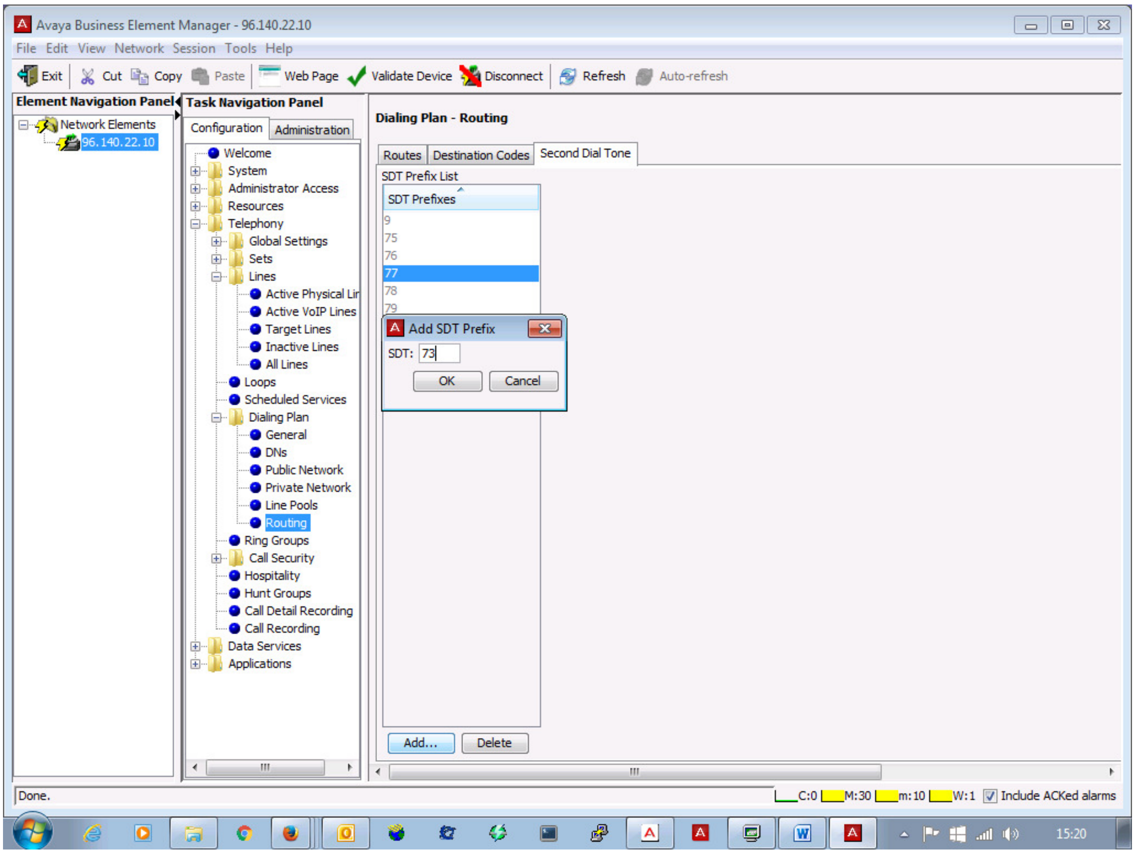


Because I used the “2” within the SIP programming to absorb two access code digits when wanting to make an outgoing call, I needed to go into the BCM routing table to configure access code 73 for my Sipgate account. I used routes 73 with BlocA and Public (UnKnown).

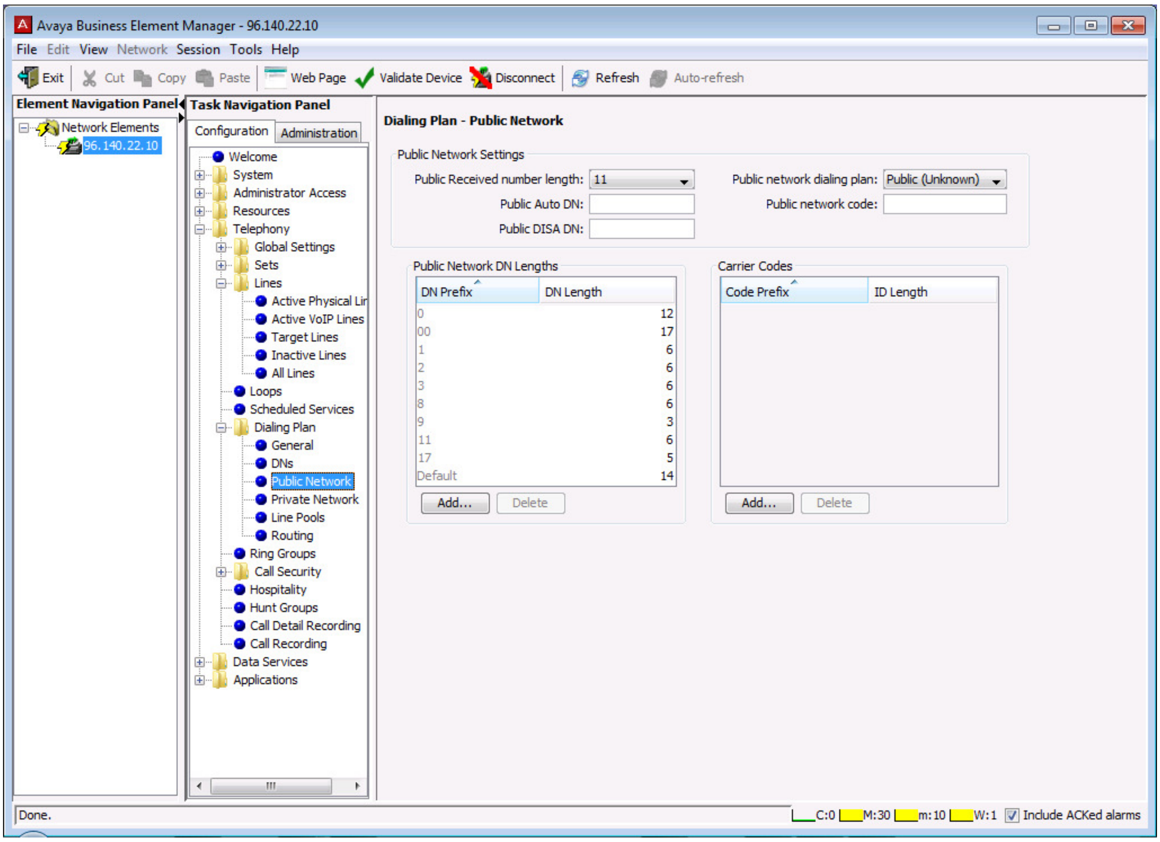




There is an option tab on the right to use a “Second Dial Tone” which is useful when using SIP trunks as you get dial tone after the access code has been entered. Just add in the access code as shown below. Click OK once it has been done.



Finally, the Dialing Public Network plan was changed when I had problems dialling out by increasing the default digits to 13 or 14. Also the Public Received number length was increased to 11.



The information listed in this guide should provide the basic information need to configure public SIP trunk accounts.

Trouble shooting and additional non-essential information

When setting up the BCM for SIP trunking, there are other areas that need to be checked. Some of these aren't in the Avaya documentation.

Router configuration

Initially, I had UDP port 5060 configured to port forward onto the BCM system. This has been removed and only the following are used.

BCM Unistim Signalling	ALL	UDP	7000 - 7001
UFTP Server	ALL	UDP	7002
BCM IP Phone Signalling	ALL	UDP	20000 - 20249

Even these ports are really required for SIP trunks, but will be needed if you plan to connect up IP phones across the internet using the BCM NAT Traversal license.

Application DN's

There is in my opinion a major flaw in security as my BCM system was recently hacked by dial through fraud a few months after installing a couple of SIP trunks onto it. I carried out an extensive search to try and find out when it started and how it was done. Although I had incoming trunks go to voicemail with a menu option, I didn't think that was the cause which is usually the case!.

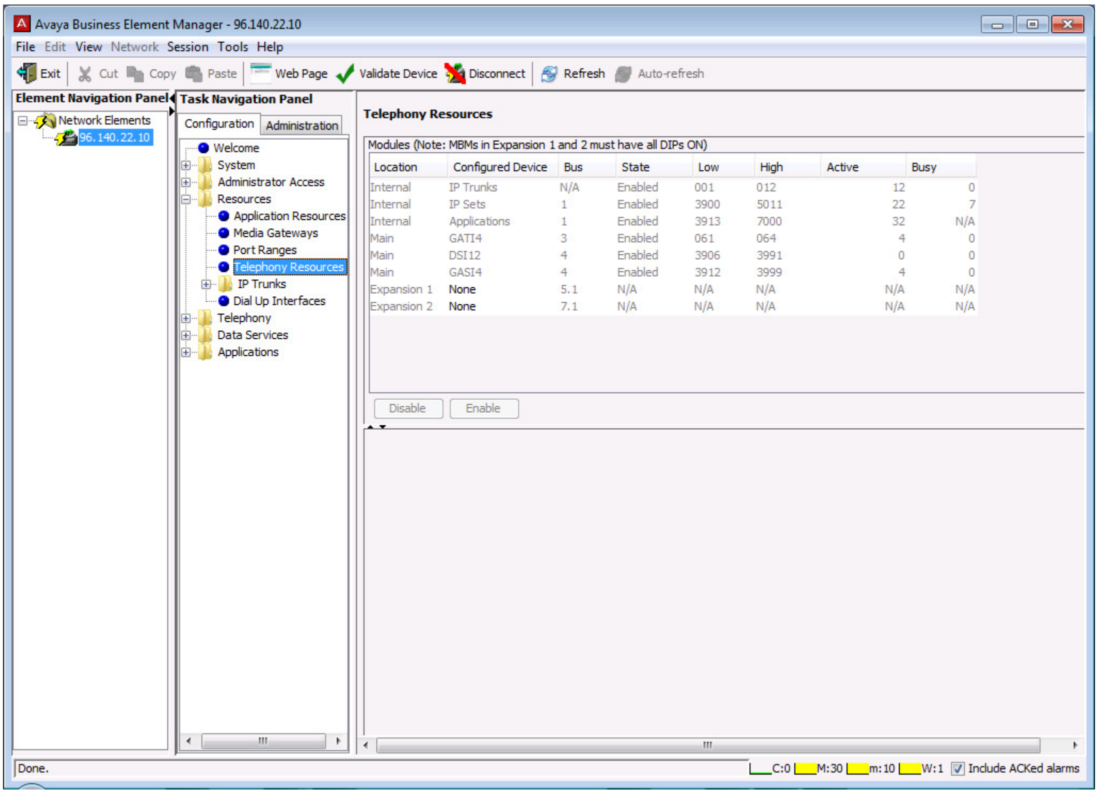
What I discovered was that I had **UDP ports 5060** and **443** set to my BCM, which I think gave the SIP hackers the ability to probe my system for any weaknesses and I had spotted some odd behaviour some time before it happened. It was quite trivial on the BCM Monitor tool that I saw incoming calls but none of my phones rang and no indication of who was calling me. This kept repeating around every 15 to 20 minutes.

I had one analogue trunk that was assigned in programming to **Pool A**. On just about all BCM systems, it looks as if Pool A was assigned to all Application DN's along with a **separate target line**.

The hackers broke out via the analogue line. The weird thing was that the CDR records didn't show any incoming traffic but only outgoing traffic via an Application DN, hence the reason for investigating this area.

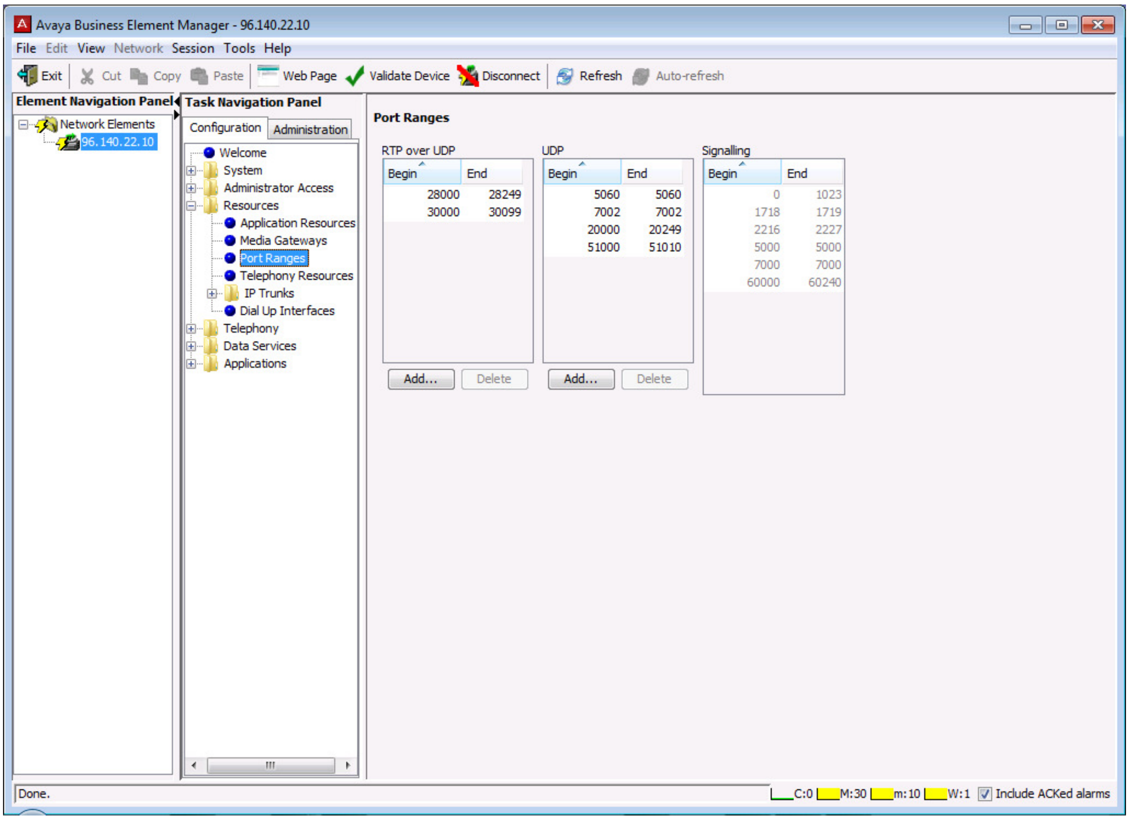
Since the outbreak of calls, I've tightened up everything which includes removal of any line pool and target lines from the Application DN's and made international calls restricted and changed their access to public or a different line pool. As stated above, the **UDP port 5060** and **443** was removed from my router and only the minimum ports remained.
My BCM monitor tool now only shows active or previous calls which indicates that my problem has now been blocked to the hackers.

Telephony Resources



BCM Port Ranges

Here is a screen shot showing the ranges used on my BCM system.



Application Resources