

# Kestrel Series Radars

Remote Access Manual



*This page has been left intentionally blank*

<b>Introduction</b>	<b>1</b>
<b>Operating Principles</b>	<b>1</b>
<i>Communication Methods</i>	<i>1</i>
<i>Connections</i>	<i>4</i>
<b>Remote Access Server</b>	<b>6</b>
<i>Modems</i>	<i>6</i>
<i>Servers</i>	<i>7</i>
<i>Active Connections</i>	<i>8</i>
<i>Devices</i>	<i>9</i>
<i>Messages</i>	<i>10</i>
<b>TrafficApp</b>	<b>11</b>
<i>General Configuration</i>	<i>11</i>
<i>Servers</i>	<i>12</i>
<i>Providers</i>	<i>13</i>
<i>Device Configuration</i>	<i>14</i>
<i>Radar Configuration</i>	<i>16</i>
<i>Device Provisioning</i>	<i>17</i>
<i>Device Communication</i>	<i>18</i>
<b>Checklist</b>	<b>19</b>

*This page has been left intentionally blank*

## Introduction

In many situations it may be convenient to access your radar devices remotely, this has a number of advantages over a direct physical connection:

- No physical connection required to “talk” to the device.
- Instant access to the device.
- Remote re-configuration and downloading of data.
- Cheaper on-going costs (no need to make site visits, fuel, time/wages)

We have endeavoured to create a system which is easy to configure and operate, this manual serves as a guide to configuring the server software and the radar modules for remote operation.

## Operating Principles

In almost all situations it is recommended that radar units are fitted with “pay and go” SIM cards, the radar devices are (normally) situated in public locations there is a potential that they may be subject to vandalism or theft and by using a “pay and go” SIM card you can limit the problems that this may cause.

### Communication Methods

The internet uses a system known as TCP/IP for communication between computers and devices, each device on the internet has an IP address which uniquely identifies it. If you know this IP address then it is possible to directly communicate with the computer or device.

If a computer has a GSM modem connected to it, then technically it should be possible for that computer to directly communicate with the radar module, if this radar module always uses the same IP address then this would be known as **Static IP** addressing.

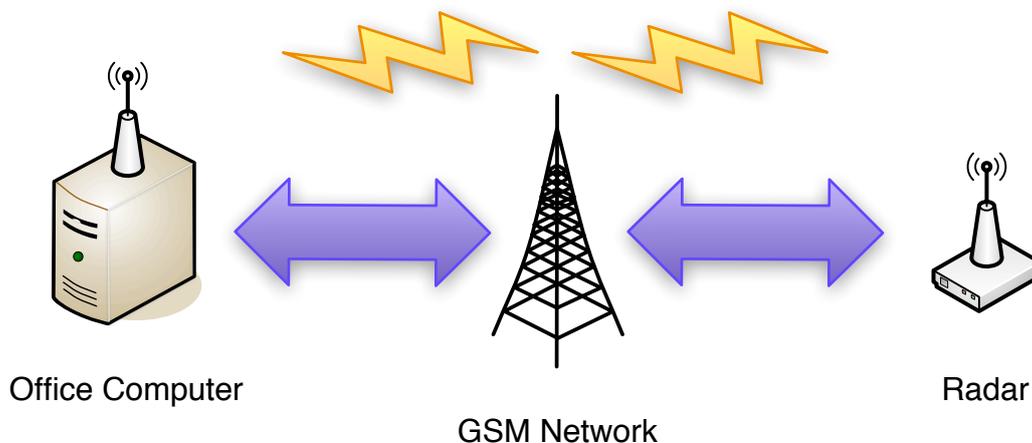


Figure 1.

Unfortunately with mobile phone networks this is not the normal mode of operation. There are a very limited set of IP addresses available and it is normal practice for mobile phone networks give out a new random address (from their pool) when a device wishes to use the internet. This has the effect that from one data session to another, different IP addresses will be allocated.

This complicates how connections to radars can be made.

There is also the problem of providing access to the mobile phone network for the client PC. The solution provided by Kestrel Radars is to use a an intermediary server to handle the mobile phone portions of the connection. This server does requires a static IP (because the radars will need to connect back to it) but because the server is using a normal internet connection (rather than a mobile phone) obtaining a static IP from your ISP should be easy.

The new architecture for connecting to remote devices is shown in figure 2.

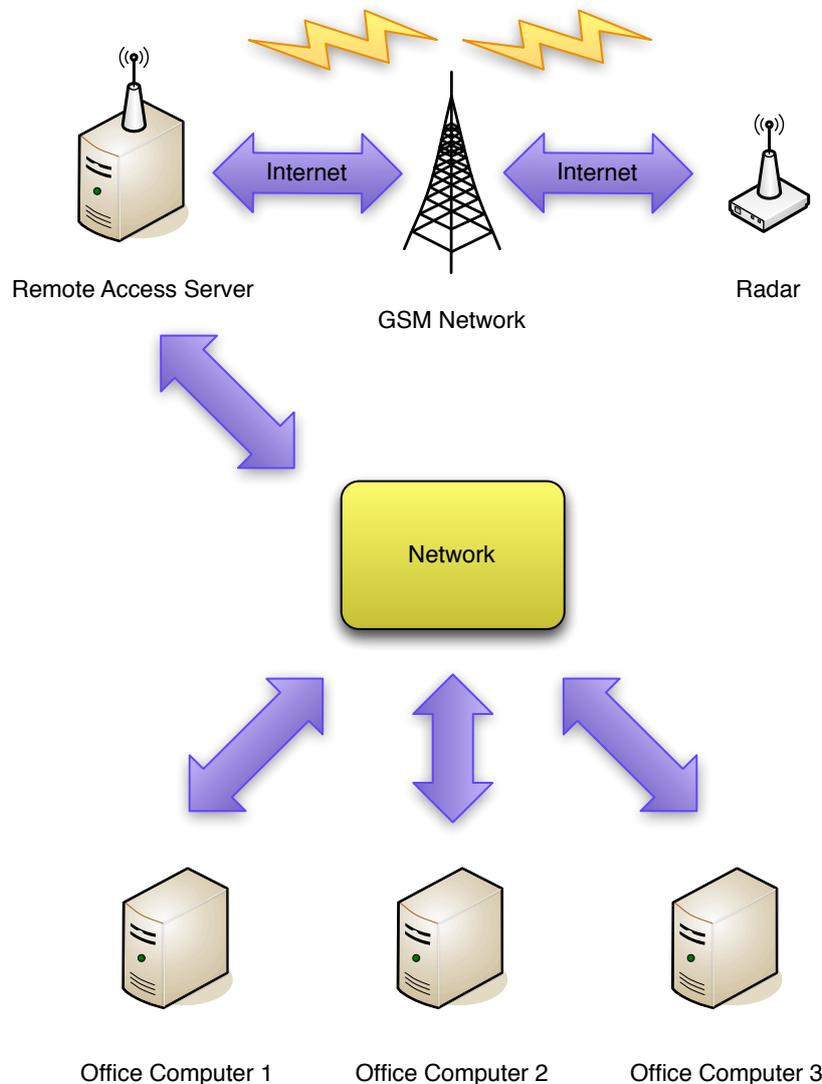


Figure 2.

We now have the remote access server acting as a gateway between the mobile phone network and remote radars and also between any computers that wish to communicate with them.



This also has the effect that only one modem is required to provide remote access from multiple PC's to any number of devices.

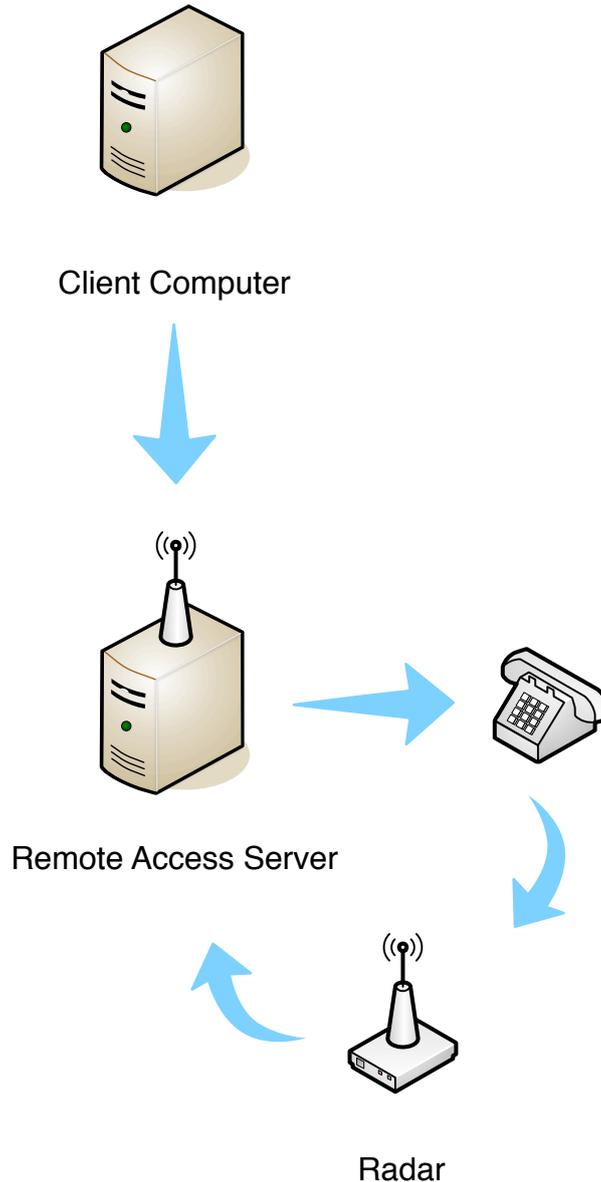
With very little extra configuration, it is also possible to make this server accessible over the internet, this allows you to run a remote access server on behalf of your customers and reduces the amount of configuration that end users will have to do.



## Connections

There is still one more problem that needs to be overcome, the remote radar devices still have dynamic IP addresses and therefore cannot be directly accessed over the internet. So how does the server connect to the remote device without knowing its IP address?

This is actually a simple process. The modem in the radar is actually a complete mobile phone and therefore has a telephone number which does not change. We make use of this to open a connection to a remote device, this process is shown in the following diagram:



*Figure 3.*

The connection flow now operates as follows:

1. The client computer requests a connection to the remote device by specifying the telephone number of device.
2. The remote access server uses its modem to “ring” (drop-call) the device.



3. The remote device detects the ring and connects to the server over TCP/IP.
4. The remote access server creates a “pipe” between the client and the remote device so that they can communicate directly.

This simple mechanism allows ad-hoc connections to remote devices without the need for special (and expensive!) data SIM cards with static IP addresses.

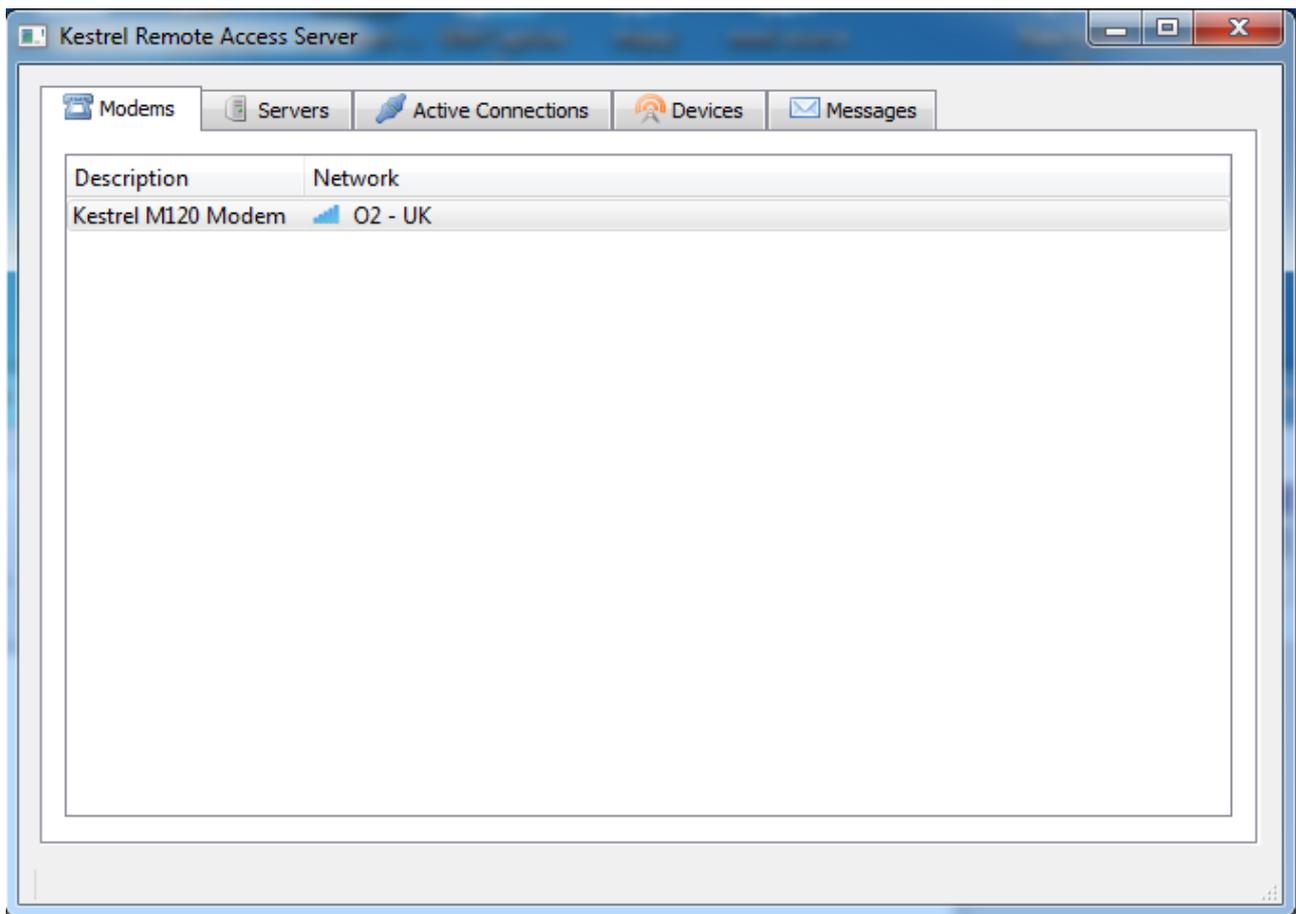


## Remote Access Server Configuration

The remote access server software is simple and requires very little configuration for operation, once installed the software will run in the background.

The software appears as an icon in the notification area of the task bar (near the clock) and the main window is opened by double clicking on the icon. (Closing the main window will not quit the software, it is still running and can be re-opened by double clicking the icon in the notification area)

### Modems

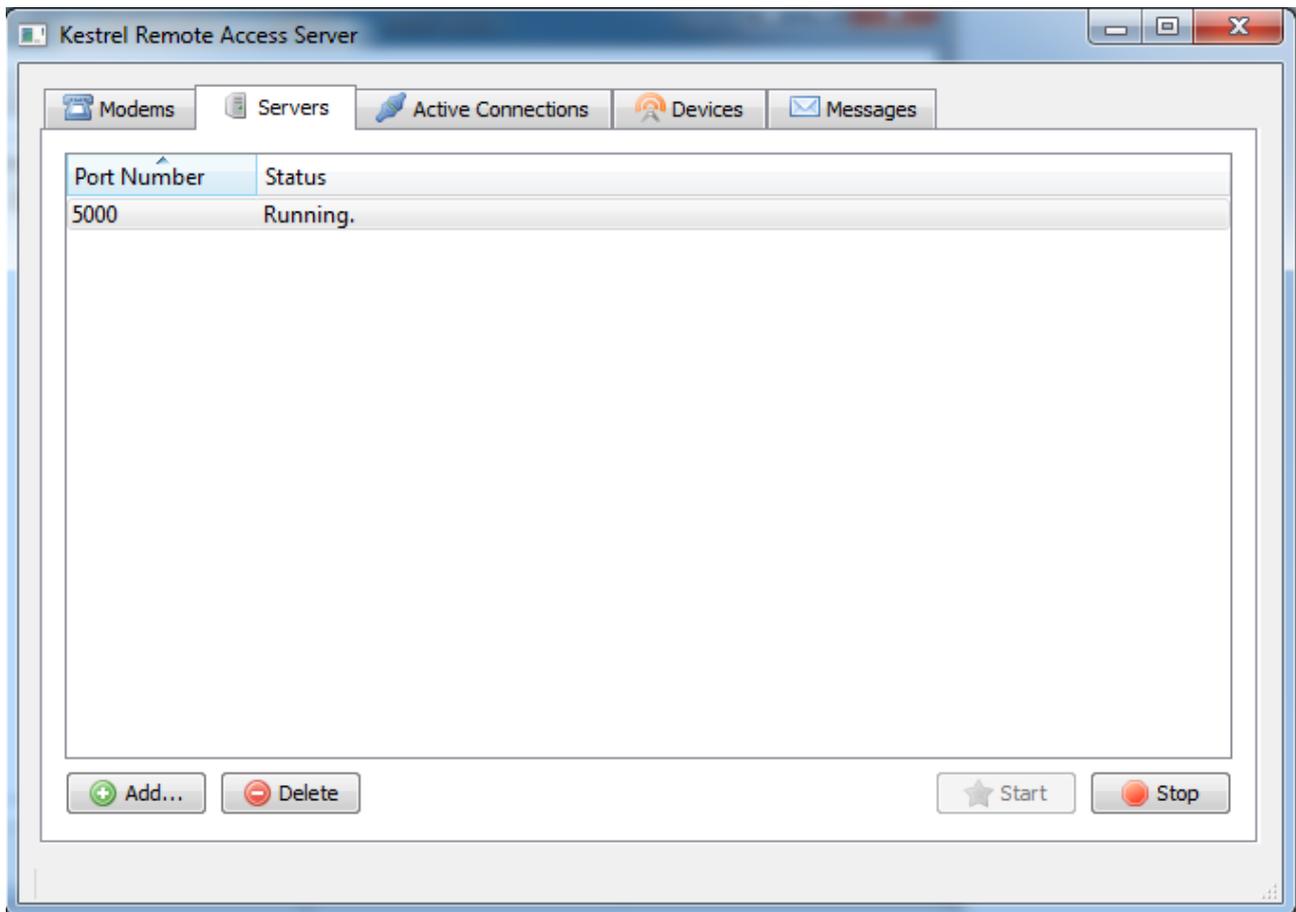


This shows that a modem has been found and that it is connected to the “O2 - UK” mobile phone network, the signal strength is also displayed.



## Servers

The servers tab shows the list of port numbers that server will respond to.

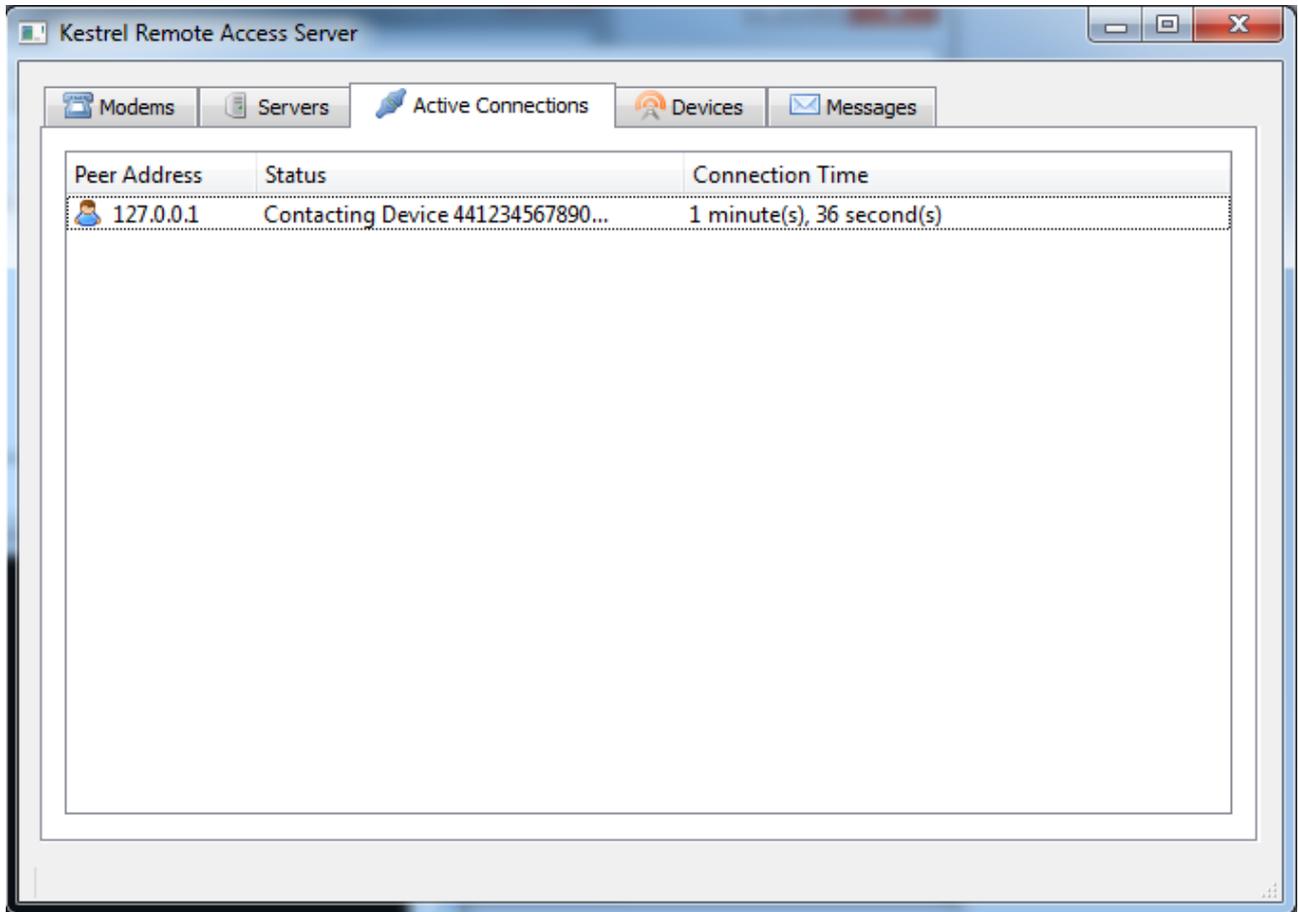


These ports should be accessible from the internet and you can have multiple ports accepting connections at the same time if required, this may be useful if you are providing a remote access server for third parties.

To add a new port, simply click the “**Add...**” button and select a port number.

## Active Connections

This tab shows the list of all devices/computers that are currently connected to the server, in addition it also shows the current state of the connection (logged in, dialing, connected etc).

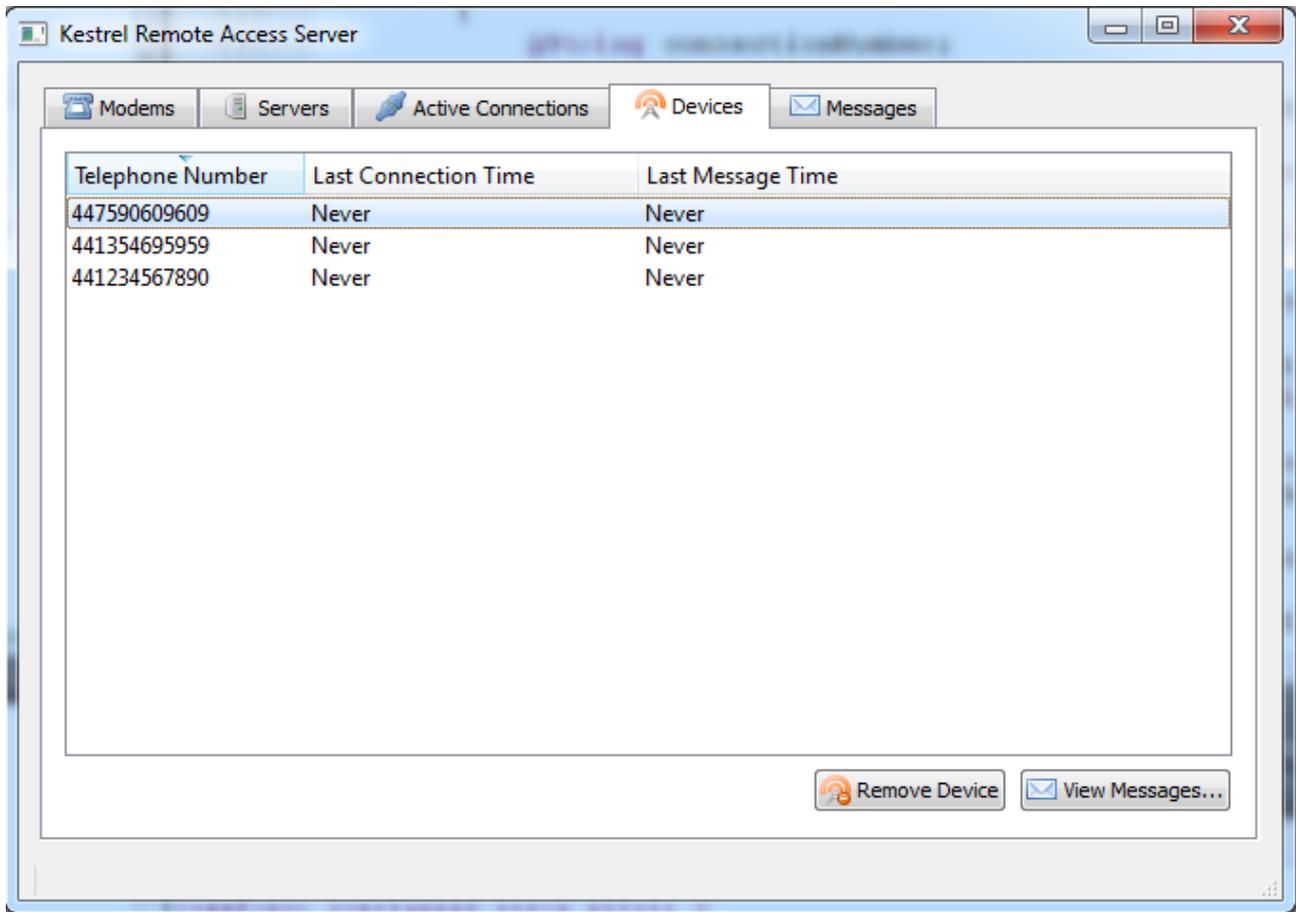


A connection can be closed by right clicking on the device and selecting “**Disconnect Client**” from the menu, please note that if a client is connected to a remote device then both connections will be closed.



## Devices

The devices tab shows a list of devices that are known to the server. (Either by connecting to the server or a client requesting access to that device)



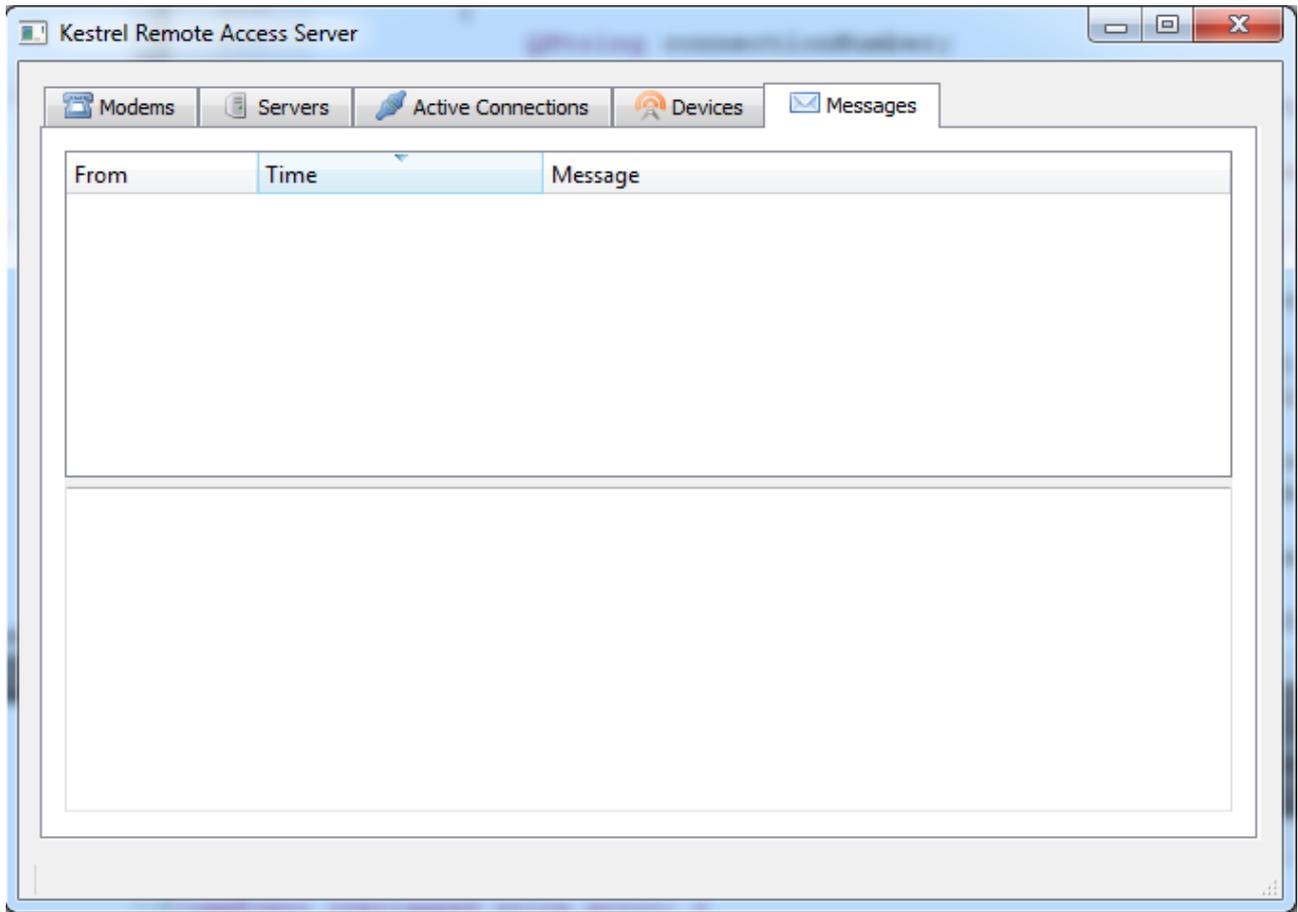
The last time that the device connected to the server and the last time that a message (SMS) was received from the device is shown. Devices can be removed from the list by highlighting the device and then clicking “**Remove Device**”.

In addition, SMS messages that have been received from a device can be shown by clicking “**View Messages...**”.

To aid in debugging, it may be useful to set a “friendly name” for a device so that rather than appearing as a phone number in the Remote Access Server it appears as something more logical. To do this, select a device and then right click and select “**Set Friendly Name...**” from the menu.

## Messages

The final tab shows a list of all messages that the server has received.



To view a message with correct formatting you should double click on the message to open it in a new window.



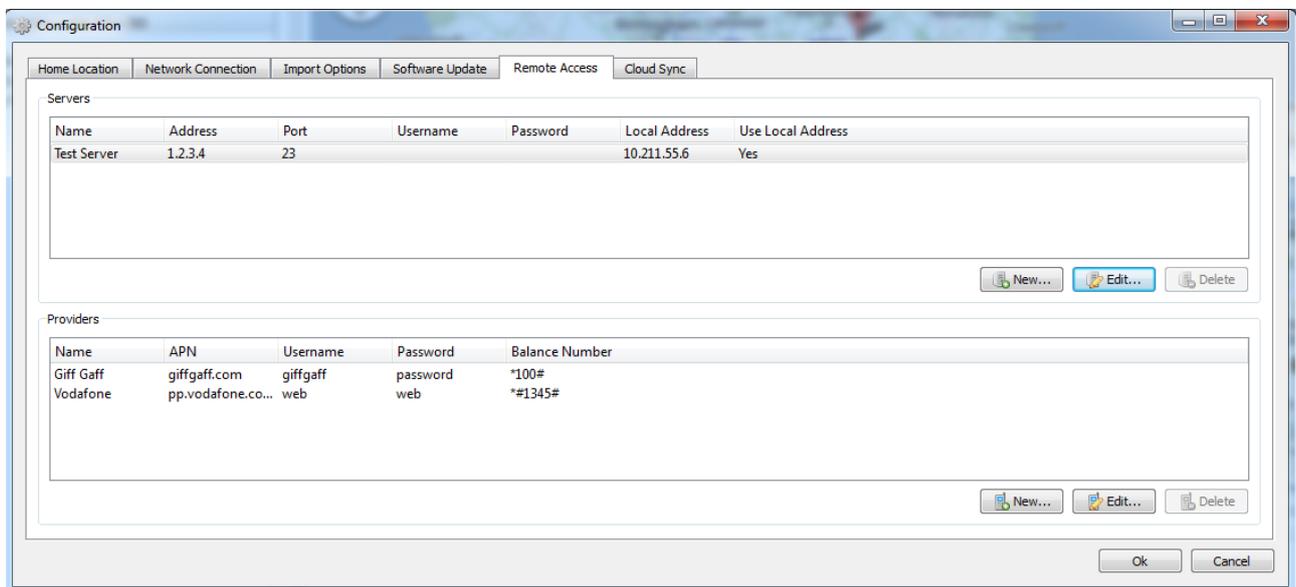
# TrafficApp Configuration

The client software for communication with remote devices is the Kestrel TrafficApp software. This software is used to configure locally connected or remote devices and for radars that have data collection options it is also used to remotely download and then process and analyse the collected data to produce comprehensive and easy to understand reports.

*This manual does not cover the complete operation of the TrafficApp software, instead this manual covers the steps required to configure a radar for remote access and to configure the TrafficApp software for connecting to a remote device.*

## General Configuration

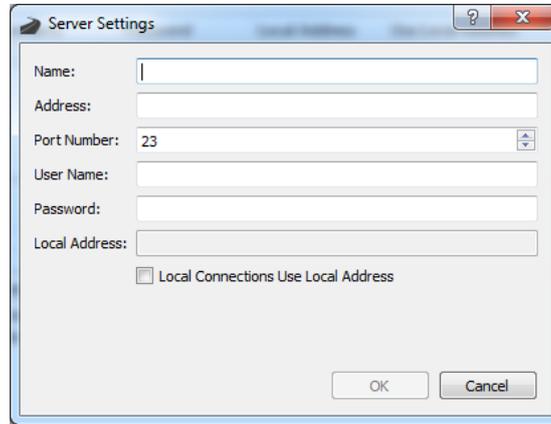
The first step in configuring TrafficApp for remote access is to configure the general remote access settings, select **"Tools/Options/Remote Access"**.



## **Servers**

This is the list of remote access servers that can be used to contact remote devices, in most cases there will be only one listed, you will need to create an entry which matches your server installation.

To create a new server entry, select the **"New..."** button under servers.



The following fields will need to be supplied:

- **Name** - *The name of the server, this is the name that will be used in the software to identify this server.*
- **Address** - *The IP address of the server (domain name may also be used) that the server can be contacted on. It is important that this field is filled in correctly as this is the address that will be stored in the configuration of the radar device during the "Provisioning" phase. This is the public address of the Kestrel Remote Access Server that you should have already configured.*
- **Port Number** - *The port number that the server can be contacted on (This should match an entry in the Kestrel Remote Access Server)*
- **User Name** - *Not used at present*
- **Password** - *Not used at present*
- **Local Address** - *Because the "address field" is sent to the device during provisioning, the value of that must be set to the public IP address of the server. This may cause problems when trying to connect to a public IP address that exists inside of your network, to address this problem the internal IP address of the server should be entered here.*

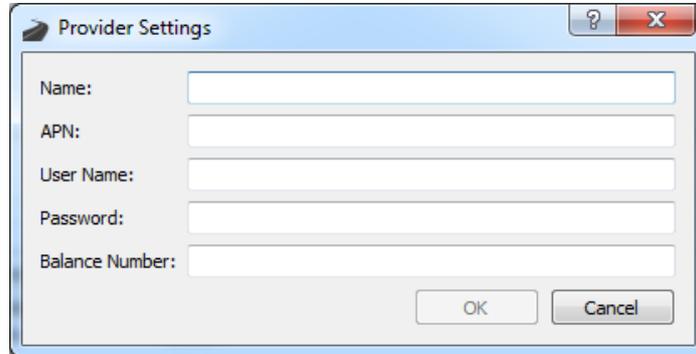
*When the "Local Connections Use Local Address" option is ticked, this local address will be used to connect to the server from TrafficApp rather than the public IP address.*



## Providers

This is a list of SIM card providers that are used by devices, this information is used when provisioning devices so that they know details such as APN names & login credentials.

To create a new provider entry, select the "New..." button under providers.



The screenshot shows a 'Provider Settings' dialog box with the following fields:

- Name:
- APN:
- User Name:
- Password:
- Balance Number:

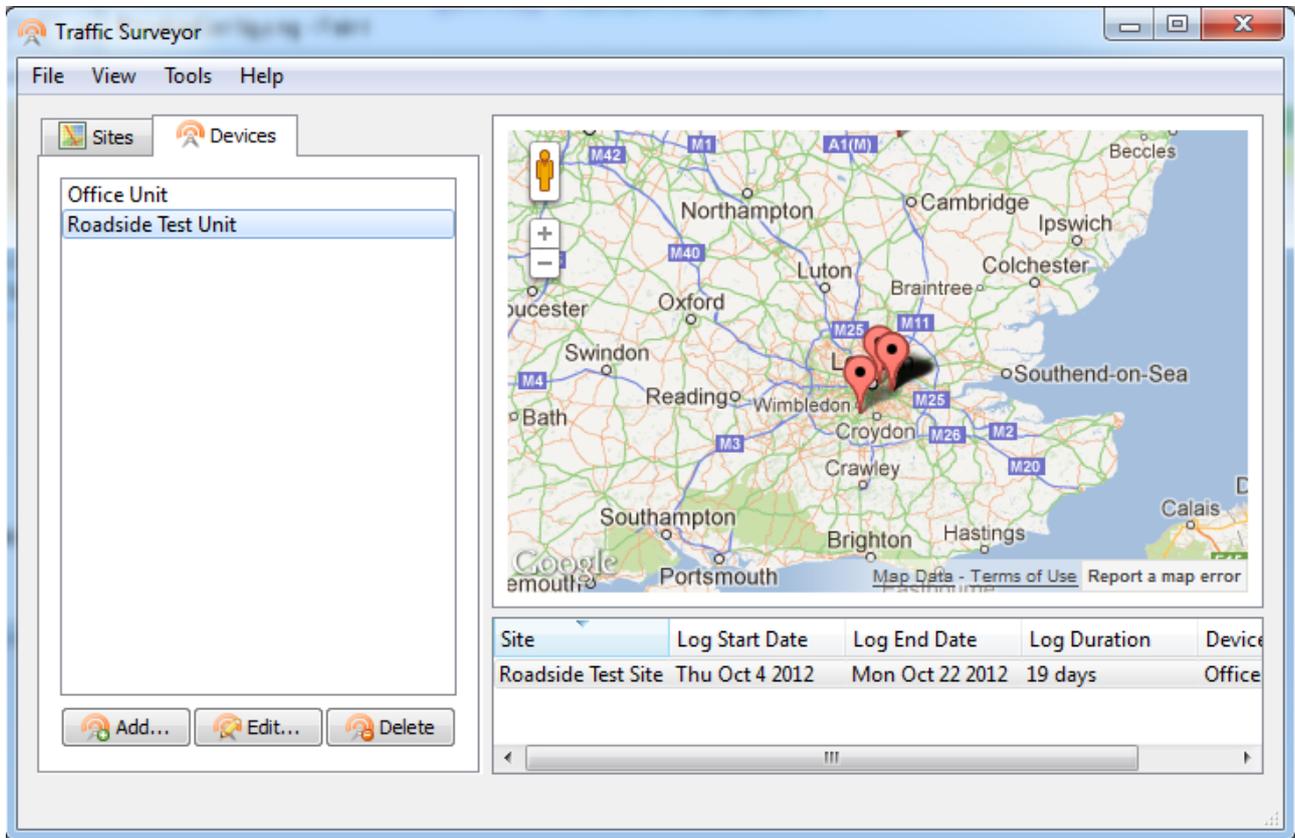
Buttons: OK, Cancel

The following fields will need to be supplied:

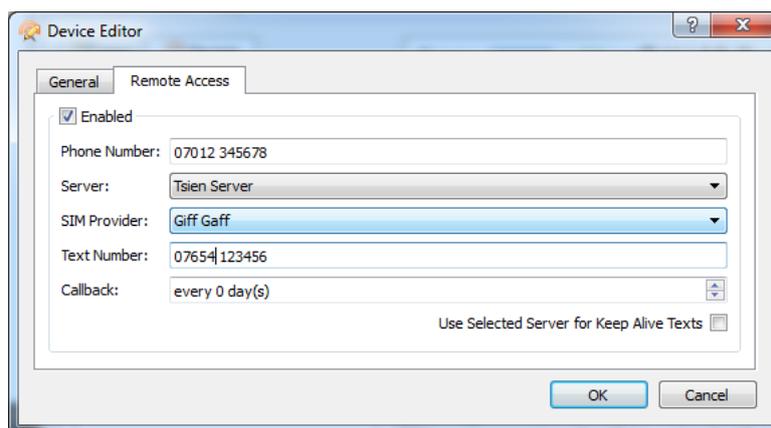
- **Name** - *The name of the SIM provider, this is the name that will be used in the software to identify this provider.*
- **APN** - *The APN name for this SIM provider, this will have been supplied by your mobile phone network.*
- **User Name** - *The user name that is used to log into the APN, this will have been supplied by your mobile phone network.*
- **Password** - *The password that is used to log into the APN, this will have been supplied by your mobile phone network.*
- **Balance Number** - *The short code sequence that is used to retrieve balance information, this is optional but if your mobile phone network supports this it can be used to retrieve balance information via an SMS message.*

## Device Configuration

The left hand side of the main TrafficApp window contains 2 tabbed views, the second tab is the devices tab and contains a list of devices that are know to the installation of TrafficApp.



To add a new device click “**Add...**” and to edit an existing device click “**Edit...**”, both options will open the same window to allow the site information to be entered.



The following information is required:

- **Enabled** - this needs to be ticked to tell the TrafficApp software to show options to allow remote access to the device.



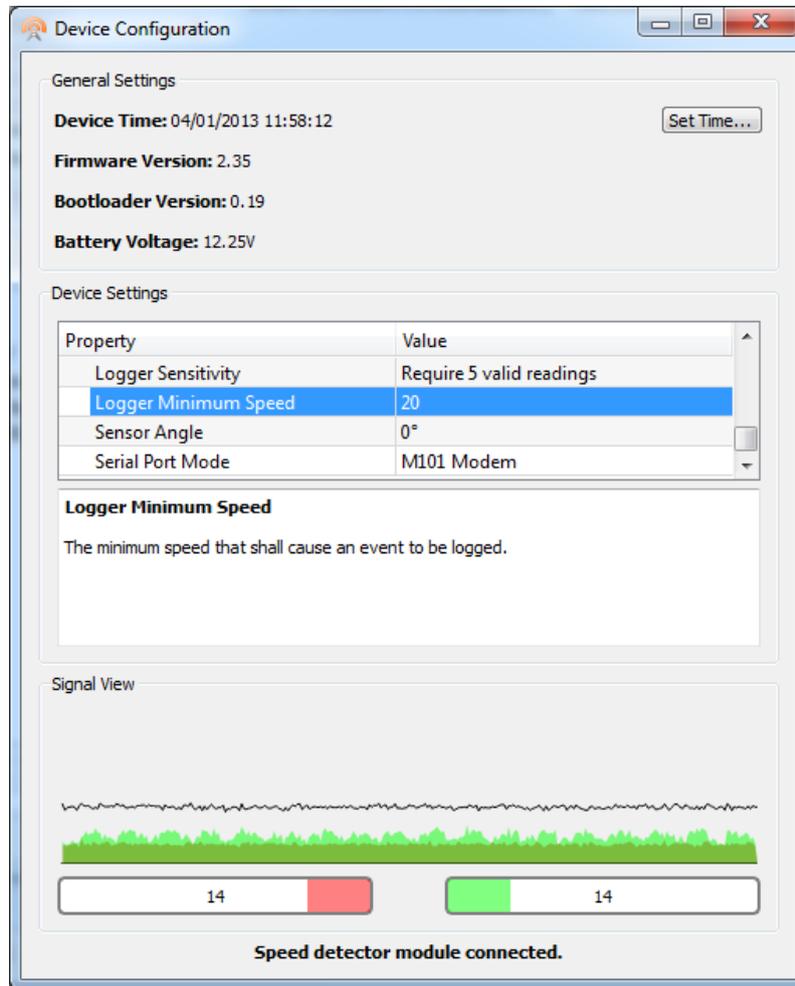
- **Phone Number** - this is used by the server to initiate a connection to a device, this must match the telephone number of the device. For users outside the UK please use the full international format for the telephone number, i.e 447123567890. This information will be transferred to the device during provisioning.
- **Server** - the server that should be used to contact the device, this information will be transferred to the device during provisioning.
- **SIM Provider** - the selected provider should match that of the SIM card that is inserted into the device. The APN name, username and password (which can be modified in main options for TrafficApp) will be transferred to the device during provisioning.
- **Use Selected Server For Keep Alive Texts** - this should be left un-ticked, this will allow the text number to be set.
- **Text Number** - this is the telephone number of the device that will receive status messages from the device, in most circumstances this number should be set to the telephone number of the server.
- **Callback** - the device will send a text message every “n” days to the server, this serves 2 purposes. Firstly you can check in the server logs to see if the device has contacted home and secondly some pay and go sims will deactivate if no usage is made on them within a certain time period, this option allows you to automatically keep the sim alive in these circumstances.



## Radar Configuration

Before a device is ready to be used, the modem should be enabled. This must be done by connecting the radar module via USB to the computer and then using the TrafficApp to configure the connected device.

With the device connected via USB, select **“Tools/Configure Connected Device...”**



Right click inside the device settings property grid and ensure that “Show Advanced Settings” is ticked, once this is enabled the “Serial Port Mode” option will appear and should be set to “M101 Modem”.

Close the device configuration window and then cycle the power to the radar, after approximately a minute the radar should be ready for GSM communications (you can check this by ensuring that the the LED on the modem board is no longer lit, this will go on and off several times during startup, but after 60 seconds it should have gone out).

The radar is now ready for provisioning.



## Device Provisioning

Before the device can communicate with a server, the configuration must be sent to the device, this is called provisioning. During provisioning, the following core information is sent to the device:

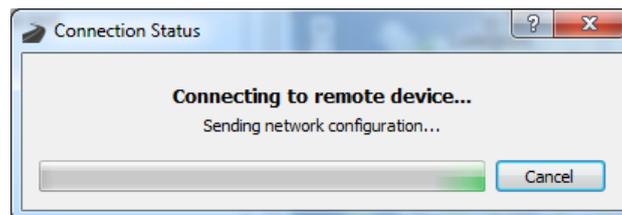
- The device's own phone number (this information is not available from the SIM card)
- The server IP address and port
- The network APN settings

Without this information being successfully sent to the device, it will not be able to communicate.

To provision a device, first ensure that both the device AND the server have credit and will be able to send and receive both text messages, calls and internet data.

Then from the Traffic App devices tab, right click on the device and select "**Provision Remote Device...**".

A progress window will appear.



This window shows the various stages of provisioning, from connecting to the server, sending the provisioning messages and waiting for the responses.

At the end of the process another window will appear which indicates whether or not the device was successfully provisioned.

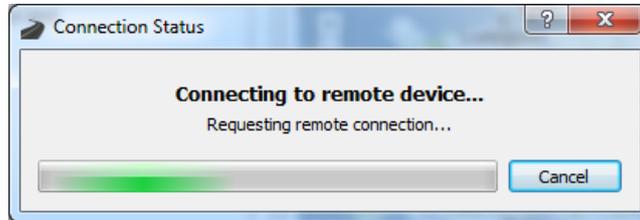
If there is a problem provisioning the device, we recommend that you check the following:

- The server is running and that the modem is listed and is connected to a mobile phone network.
- The SIM card in the server modem is able to send text messages and make phone calls.
- When provisioning the device, the server shows the connection from TrafficApp.
- The SIM card in the radar modem is active and is able to send & receive text messages and connect and use the internet.
- The radar modem is connected to a mobile phone network (you can see this if the light is not illuminated on the modem after around 1 minute after power up - the light will go on and off and eventually stay off)

## Device Communication

Once a device has successfully been provisioned, it will then (providing it was supplied with correct details) be possible to connect remotely to the device.

To connect to a device, in the devices tab in TrafficApp right click on a device and select “**Configure Remote Device...**”, a progress window will appear.



The TrafficApp software will then connect to the server which will then initiate a connection to the remote device, the device will then connect back to the server which will then be connected back to the TrafficApp software, once this is successful the normal device configuration window will appear.

Please note that when you are connected remotely to a device you cannot change the setting for the serial port, this is to prevent the remote device being accidentally changed to a state where it cannot be contacted.

For devices that support data collection, data can also be imported by right clicking on the device and selecting “**Import From Remote Device...**”, once connected TrafficApp will let the user select what data they wish to import.



## Checklist

The following checklist serves as a reminder of all configuration stages that need to be completed to allow remote access to radar devices.

1. Kestrel Remote Access Server (RAS) Software Installed
2. RAS server running on a machine with static IP to the internet.
3. Ports opened and accessible from the internet.
4. TrafficApp server configuration matches the RAS settings.
5. TrafficApp provider configuration matches the SIM card used in the radar device.
6. Device has been provisioned

If you are having trouble connecting at any particular stage, sometimes it is useful to put the device sim card in a mobile phone and check that the server rings it and that it also receives the provisioning text messages (provisioning will obviously fail as the SIM would not be in a radar).

If you are sure that the server can correctly communicate with the device (i.e sends SMS, is able to make phone calls) then you need to double check that the SIM card in the device is active, has credit and is able to send text messages and access the internet. (Again, sending text messages and internet access can easily be tested in a mobile phone).

If the SIM card is working correctly, then provisioning should complete successfully.

If provisioning is working but the device does not contact the server when requested, then double check that the APN settings are correct, if these are incorrect the device will not be able to access the internet.

Double check that the server IP and port are set to the static IP and that the server is accessible from the internet. (if you connect to the server from the internet using telnet, you will be able to type characters and the connection will automatically close when you press return).

If the server is running on a static IP but is simply port forwarded to an internal machine, then make sure that the "Local Connections Use Local Address" option is ticked in the TrafficApp server and that the correct internal IP address is listed.

