Contents

1. Connect to the Opengear Device

1.1. Open a browser

1.2. https://10.17.249.76/ (replace the IP address with this Opengear Device IP address)

1.3. Use the IP Address that you obtained for the Opengear via DHCP

1.4. Default username and password are:

1.4.1. Username: root

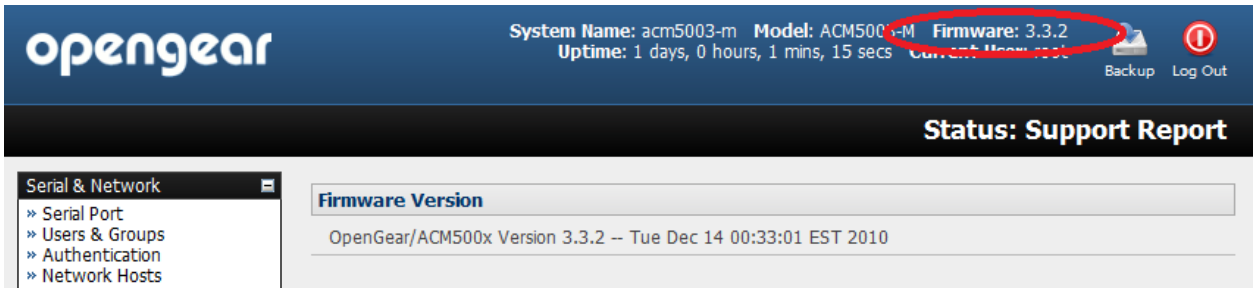
1.4.2. Password: default

2. Verify Firmware

2.1. Verify the OpenGear has the latest firmware installed by comparing the installed version (as found in the picture below) with the latest version offered at the following site.

2.2. Release Notes: http://ftp.opengear.com/download/release/

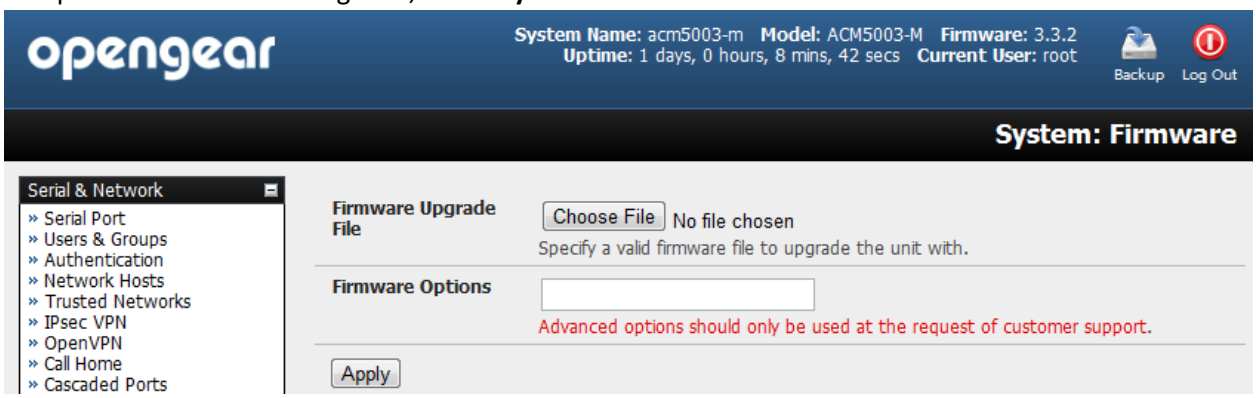
2.3. Firmware: http://ftp.opengear.com/download/release/current/



3. (Optional) Upgrade the firmware

3.1. Save the correct firmware image file on to the system you are configuring the Opengear device from.

3.2. To upload the firmware image file, select **System: Firmware**



3.3. Browse the correct directory and locate the downloaded file

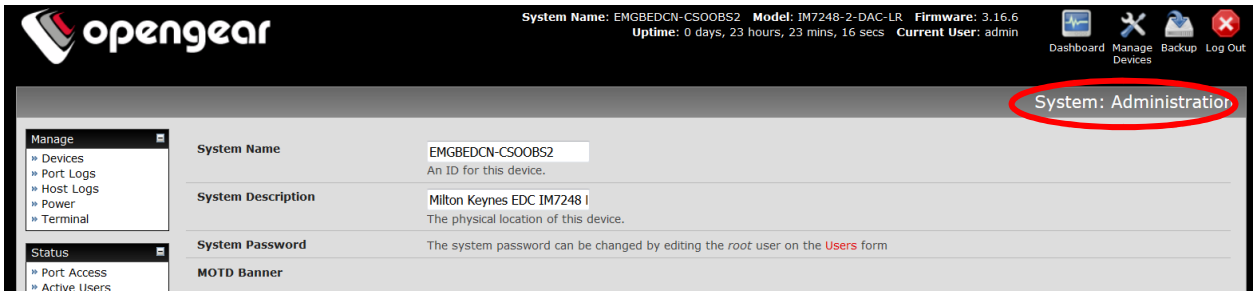
3.4. Click Apply and the Opengear device will undertake a soft reboot and commence upgrading the firmware. This process will take several minutes

3.5. After the firmware upgrade has completed, click here to return to the Management Console. Your Opengear device will have retained all its pre-upgrade configuration information

4. Complete the General Configuration

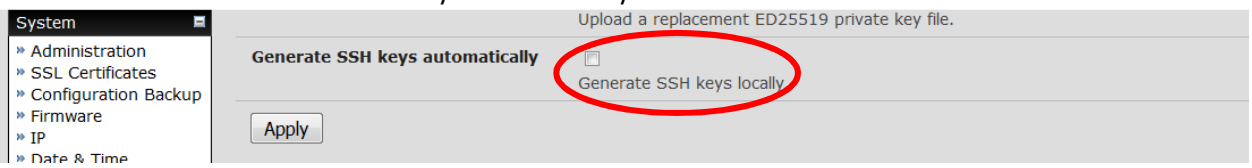
4.1. Select **System: Administration** to complete the Hostname according to naming standards (eg EMGBEDCN-CSOOBS2)

4.2. Complete the Description in the format (Ex. Milton Keynes EDC IM7248 Row B - 10.17.249.76)



4.3. Apply the Banner. Because of the formatting that is done in Opengear Banner section it may be easier just to go to another Opengear and copy/paste. A good example is 10.90.63.18.

4.4. Check the box for “Generate SSH keys automatically”



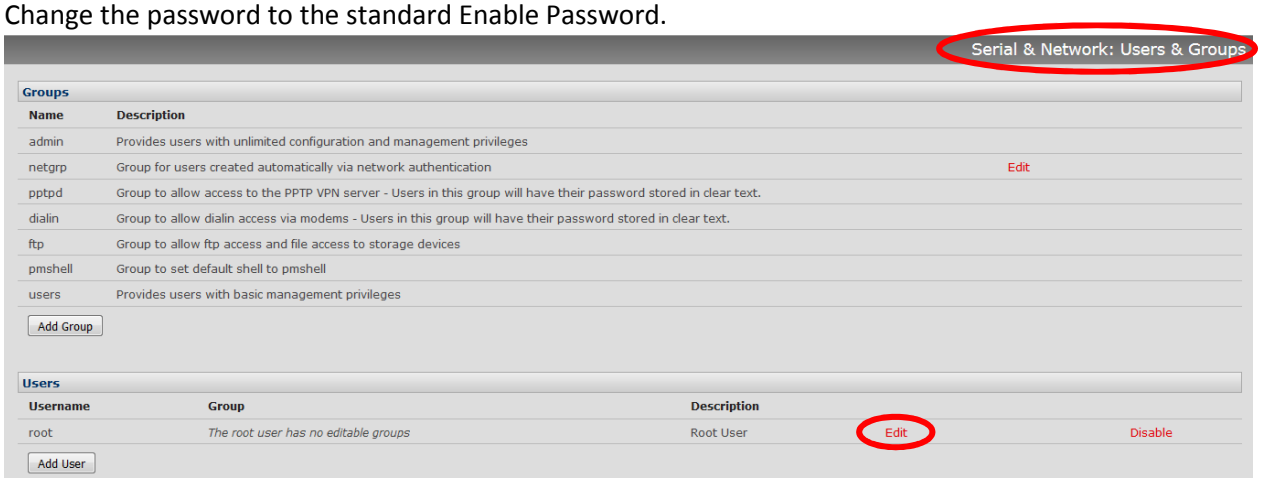
4.5. Select Apply

5. Change the root user password

5.1. Select **Serial & Network: Users & Groups**

5.2. Select ‘Edit’ for account root

5.3. Change the password to the standard Enable Password.



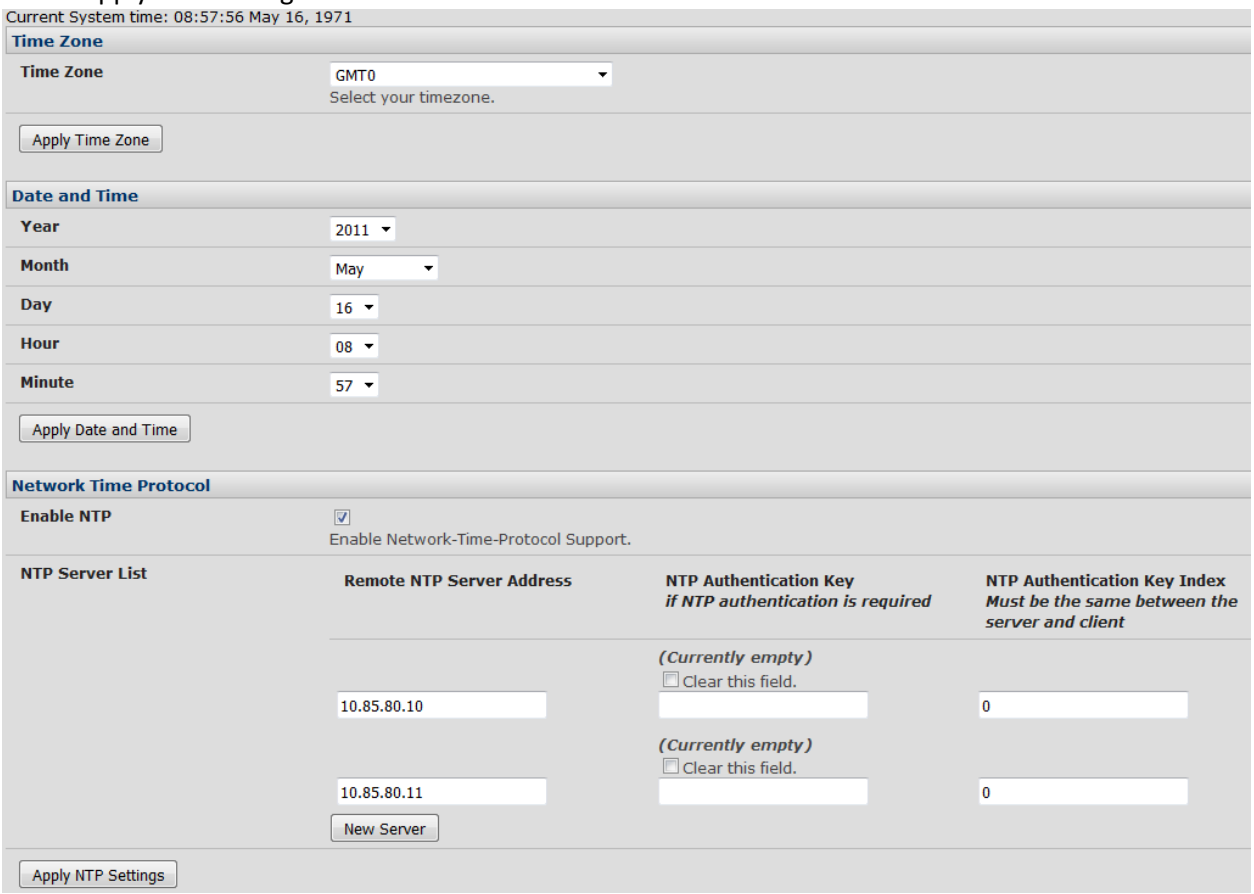
6. Configure NTP Settings

6.1. Select **System: Date & Time**

6.2. Check the box for Enable NTP

6.3. Configure the NTP Server List per Network Engineering standards

6.4. Select Apply NTP Settings



7. Configure the Serial Ports

7.1. Select Serial & Network: Select Serial Port

7.2. Select 'Edit' on the desired Serial Port

7.3. Configure the following:

7.3.1. **Label:** (Hostname)

7.3.2. **Baud Rate:** 9600,

7.3.3. **Data Bits:** 8

7.3.4. **Stop Bits:** 1

7.3.5. **Flow Control:** None

7.3.6. **DTR Mode:** Always On

7.3.7. **Signaling Mode:** RS232

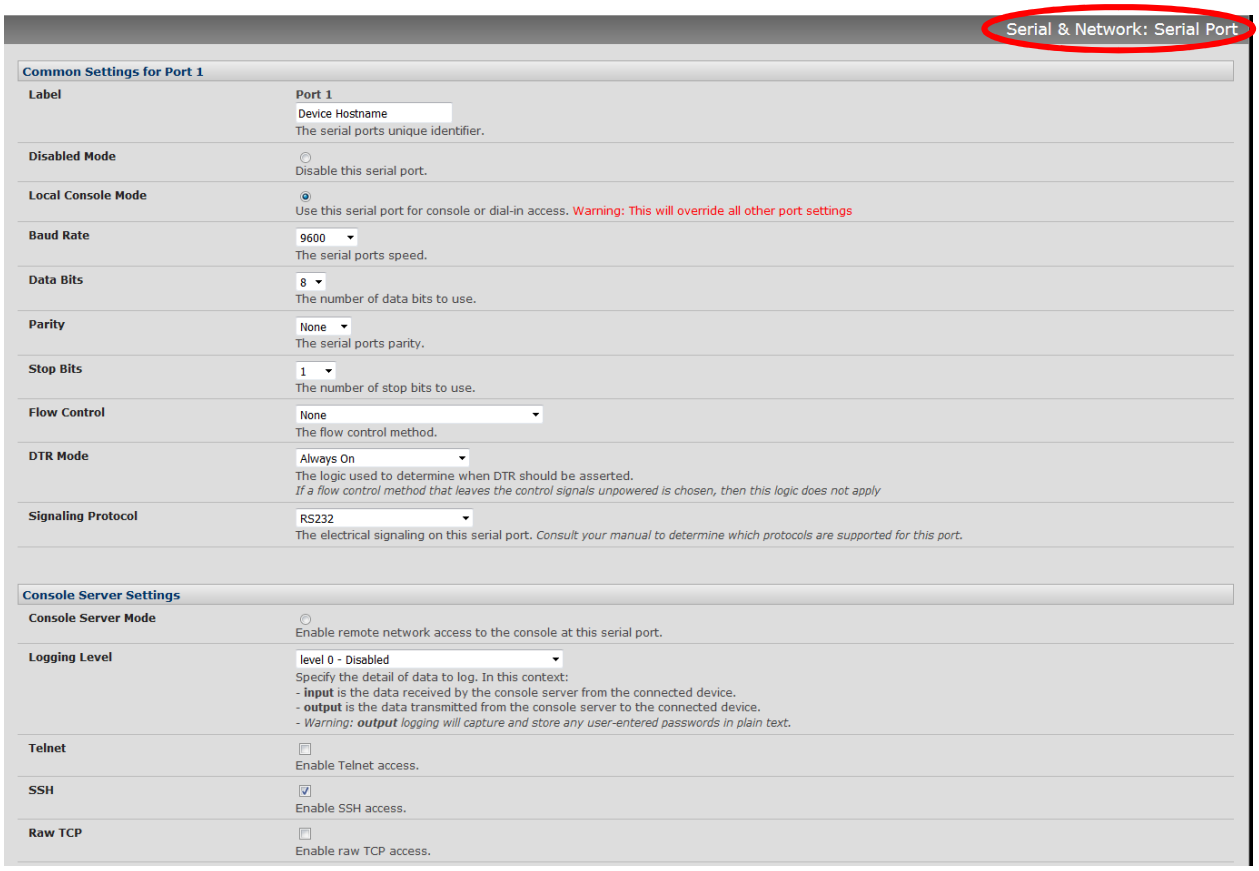
7.3.8. Select the button for **Console Server Mode** so that it will be available remotely.

7.3.9.Check the box for **SSH Enable**

7.3.10. Check the box for **Web Terminal**

7.3.11. Clear the Management LAN IP Alias

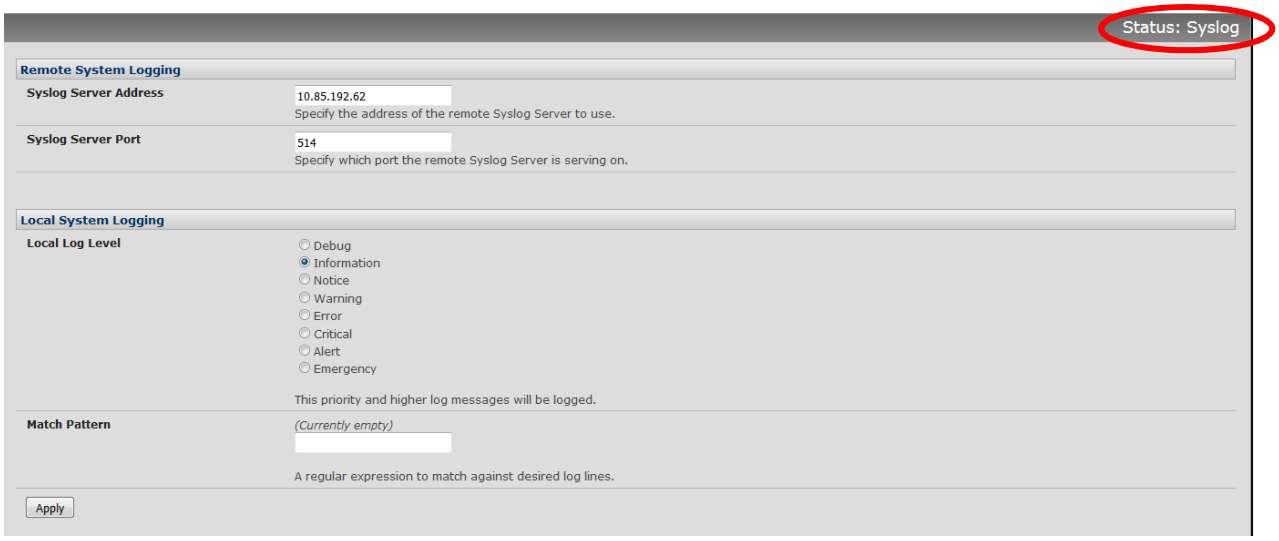
7.3.12. Clear the Authentication Password



8. Configure the Syslog Settings

8.1. Select **Status: Syslog**

8.2. Configure Syslog Settings with the appropriate Syslog Server Address. The example below is the IP address of the Syslog server to be used with all Americas' OpenGear devices. Europe and Asia/PAC would use the 10.2.3.62 Syslog server in Milton Keynes.



9. Configure the Network Interface

9.1. Select **System: Select IP**

9.2. Select the **Network Interface** tab and configure the following:

9.2.1. Select **Static** button

9.2.2. **IP Address** (Should be in the Management VLAN, usually 940)

9.2.3. **Mask** and **Gateway**

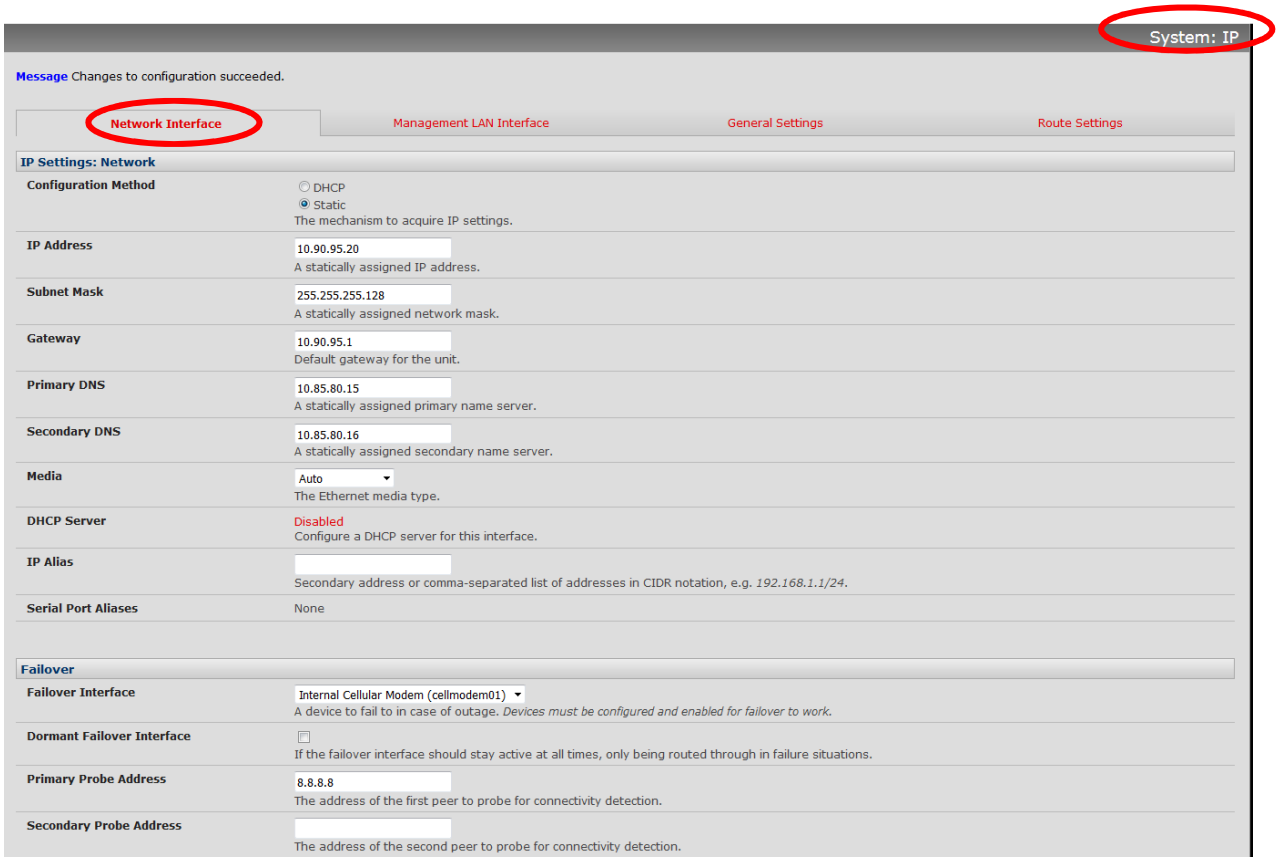
9.2.4. **DNS**, for Americas use 10.85.80.15 and 10.85.80.16

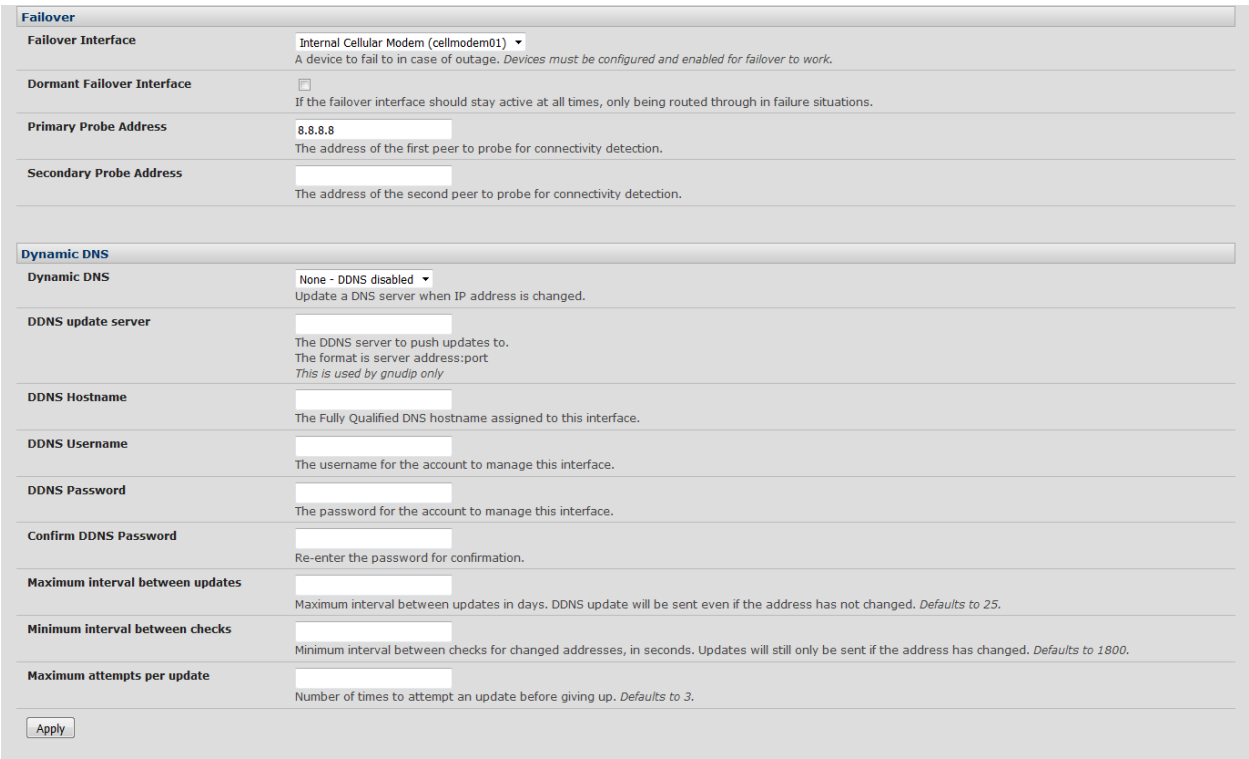
9.2.5. In the **Failover** Section set the **Failover Interface** to **'Internal Cellular Modem'**

9.2.6. **Primary Probe Address**, at this point we will use 8.8.8.8

9.2.7. Clear the DDNS Username

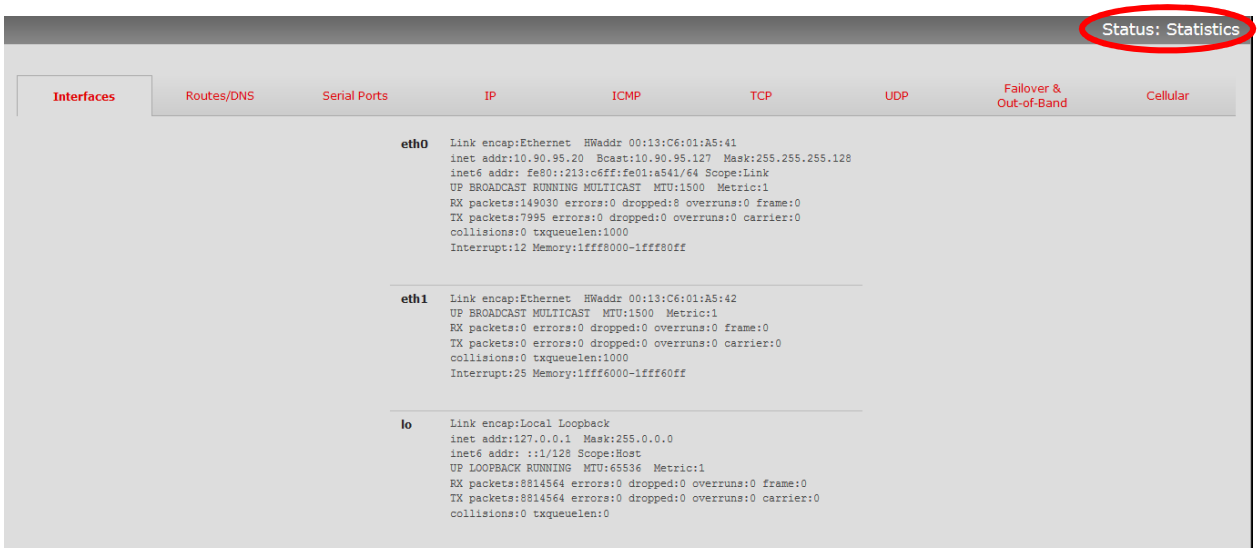
9.2.8. Clear the DDNS Password





10. Verify the Cellular SIM is Operational (If applicable)

10.1. Select **Status: Statistics** to verify that the Opengear **eth0** interface level is in normal state and not failed over to Cellular.

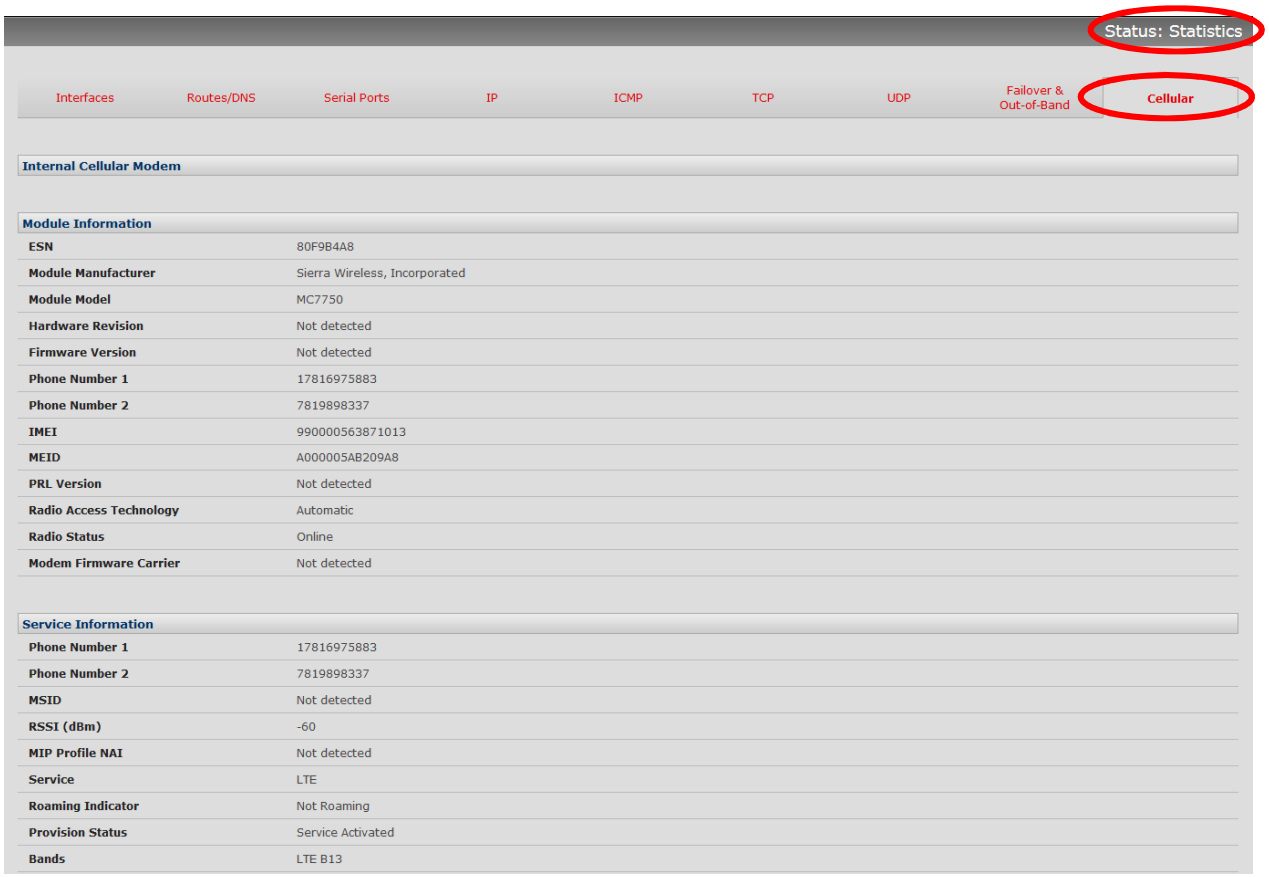


10.2. Select the **Failover & Out-of-Band** tab to verify that your Opengear is configured for failover and that the **Active Connection** is **Main** (LAN1) interface. If you see the following

message "*Warning: Failover Interface* ***Internal Cellular Modem (cellmodem)*** *is disabled.*" This can be enabled later in this document.

10.3. Select the **Cellular** tab and verify that the Opengear recognizes the SIM. The following fields should have content: **Phone Numbers**, **EMEI**, **MEID** etc.

10.4. The **RSSI (dBm)** represents the cellular signal strength and is preferred to be -50 to -60. Signal strength as low as -96 may work, but if it is this bad it is suggested to check the Antenna's to make sure they are connected correctly.



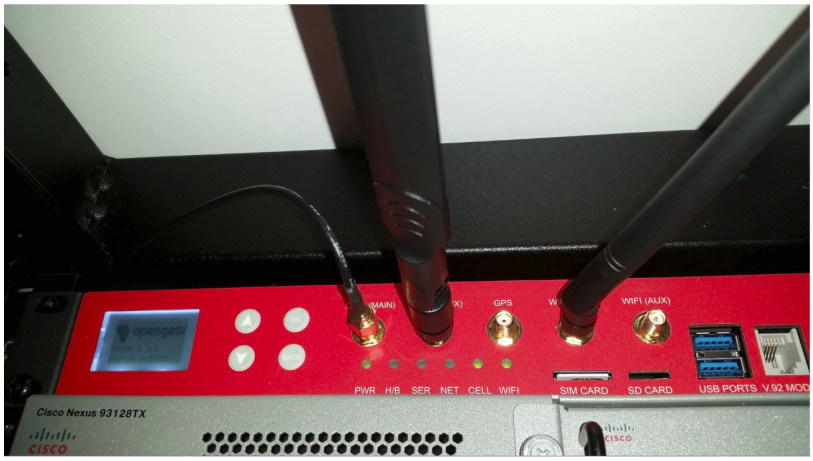
10.5. The **SIM Information** section should also show the **SIM State** as **'SIM Initialized'** and **SIM Lock** as **'SIM_READY.'**

SIM Information	
SIM State	SIM Initialized
SIM Lock	SIM_READY
PIN 1 Status	PIN is blocked
PIN 1 Retries Left	3
PIN 1 Unblocks Left	10
PIN 2 Status	PIN is enabled, verified
PIN 2 Retries Left	3
PIN 2 Unblocks Left	10
MCC	311
MNC	480
Country	United States
SIM Carrier	Verizon Wireless
ICCID	89148000002636738400
IMSI	311480264300473
MDN	17816975882
MSID	7819898328

10.6. The Antenna's should be connected as follows for the 5508 Series Opengear device.

10.7. The Antenna's should be connected as seen in the picture below for the IM72XX Series Opengear device. This Opengear in the photo has the optional External Antenna as well. Notice that the Flat antenna is connected to the Cell (Aux) port. The External Antenna is connected to the **Cell (Main).** The Antenna on the right is connected to the **WIFI (Main)** Port (this Antenna

does not impact the Cellular Signal Strength at all). It is shown here because this Opengear has the built-in WIFI functionality. Another thing worth mentioning is that, if possible, the short antennae's should be pointed straight up, not as they are here (straight out).

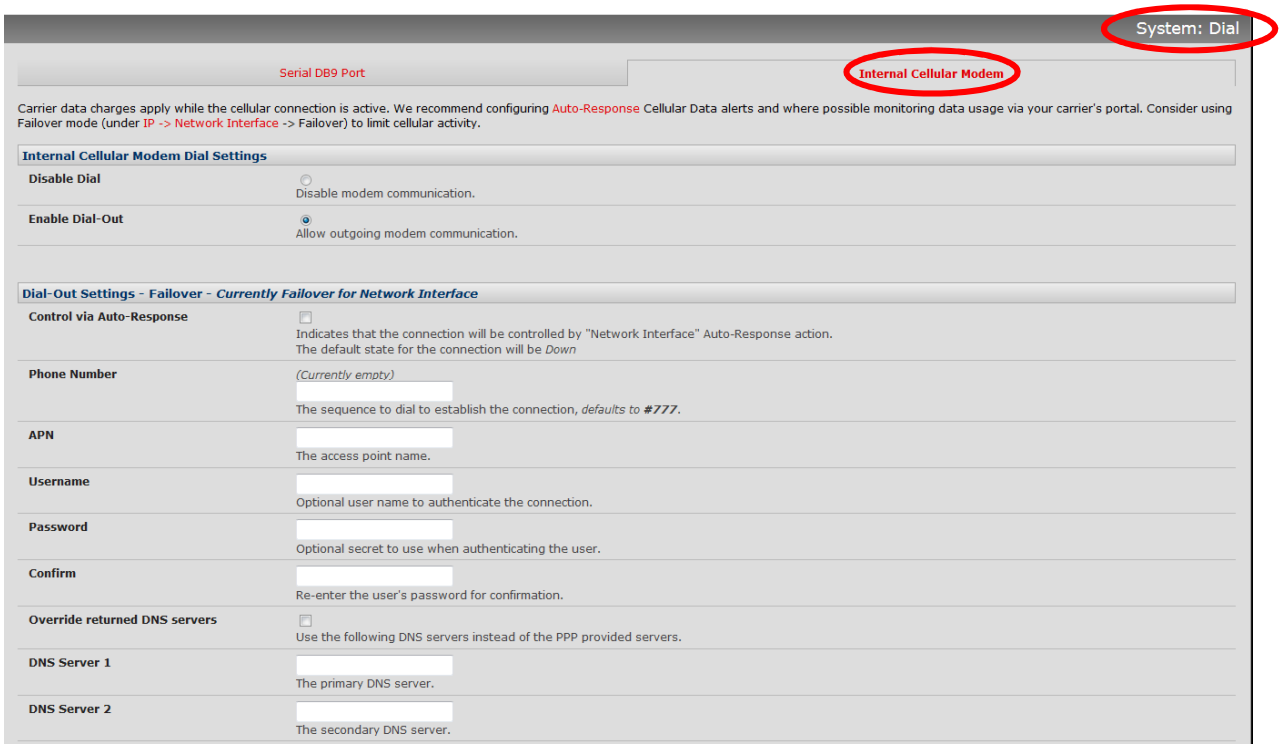


11. Preparing for the Call-Home Cellular Backup (if applicable)

11.1. Select **System: Select Dial**

11.2. Select the **Internal Cellular Modem** tab

11.3. Make sure the **'Enable Dial-Out'** button is selected



11.4. All other settings can be left blank for all except for **Dynamic DNS** (None – DDNS disabled) and **Radio Access Technology** (00: Automatic).

11.5. Additional Notes:

11.5.1. Note that APN is blank, in Europe we had to static configure this to a value provided by the carrier. More detail on this can be provided later as we learn more about the Opengear. To Try a different APN (Note Verizon you do not need an APN, leave it blank), Europe will require an APN.

11.5.2. To change or to add an APN, Disable Dial Modem communication and Apply. Type in the new APN name. Enable Dial Modem communications and Apply.

11.5.3. Whenever testing the Opengear failover function, and for that matter from time to time it is good to select Disable Dial Modem communication, Apply Modem Dial Settings. Then go back in again and select Enable Dial-Out Modem communications and select Apply as well. This has been described to me as waking up the modem in preparation for testing. Basically you are taking it out of sleep mode for the testing.

11.5.4. Under System:IP The Failover Interface is setup so that if there is a network problem, it kicks on the routing to cellular. If the **Dormant** box is not check, it keeps the cellular administratively down until a failover happens, when the network interface can no longer ping the Primary or Secondary Probe Address. We are currently using internet IP's 8.8.8.8 and 8.8.4.4 but will probably change that to Internal addresses.

11.5.5. When the **Dormant** box is selected, the cellular is always up and running but the routing will only change to cellular when an Ethernet failure happens.

11.5.6. When the **Dormant** box is unchecked, Cellular will never come up unless the Ethernet interface cannot ping the probe IP's. As a safety precaution we should do this option which means Cellular is down until we need it. If the Cellular gets a public IP address, we definitely don't want to have the Cellular up all the time because it can be attacked. If the Cellular gets a private IP address, the interface is only up when there is a failure and nobody can get to the IP anyway.

12. Configuring the Call-Home Cellular Backup (if applicable)

12.1. Notes: Two methods to add an Opengear device to Lighthouse (LH)

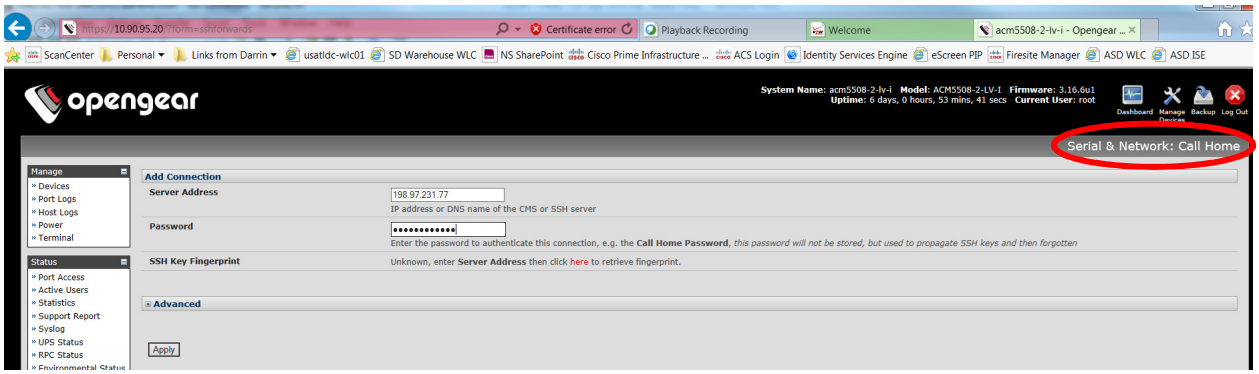
12.1.1. Regular (Manual) addition. Add this unit to the Lighthouse and it will be a routable IP address (internal) that is accessed. The LH would always use this fixed IP address to manage the Opengear device. This is used if the Opengear doesn't have or can't accept a SIM card.

12.1.2. Call Home Option – instead of the LH going to the Opengear via the Internal routable IP address, the Opengear calls the LH. Benefit of this option is that if there are two or three IP addresses on the same Opengear, It will initiate the Add Device to the LH, which has a

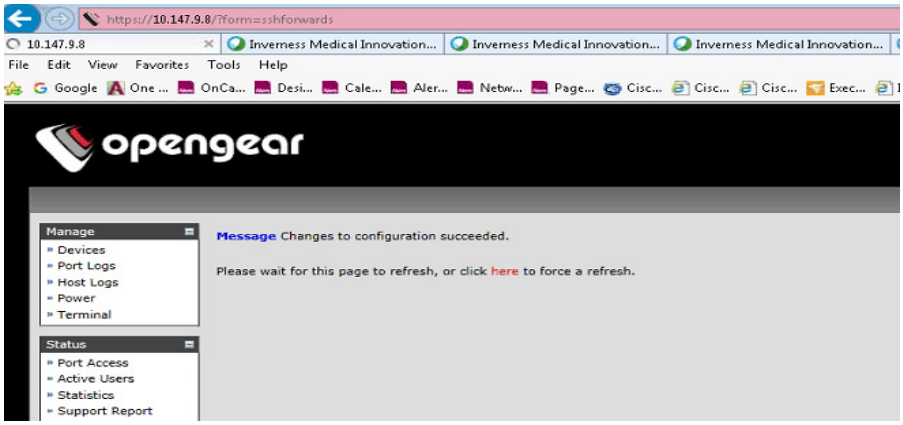
single Public IP address. If the Opengear is connected to the LH via Ethernet and that connection goes down, the Opengear uses the Cellular IP Address and will call the LH Public IP. The drawback on this option is that the LH must have a public or NAT'd public IP address (198.97.231.77:22). Ours does have this so we are good.

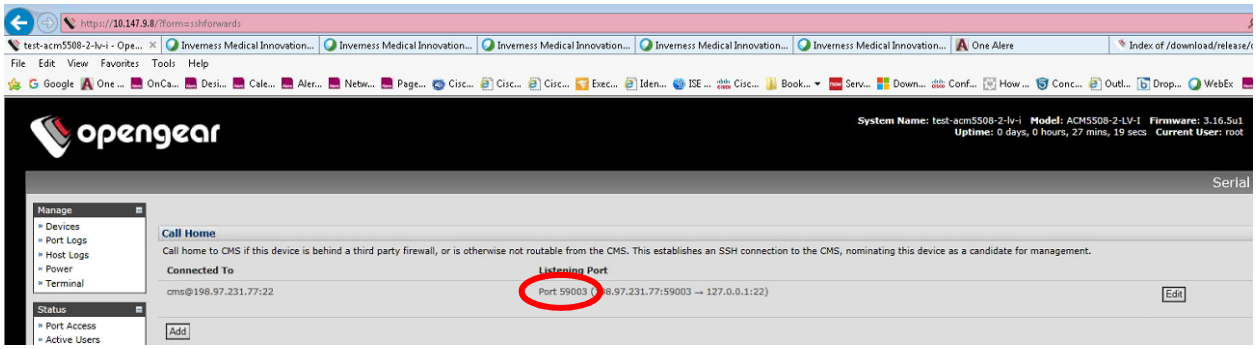
12.2. Select Serial & Network: Call Home

12.3. Enter the IP address of the LH Server (198.97.231.77) for the **Server Address** field, and the Enable Password. Select Apply.



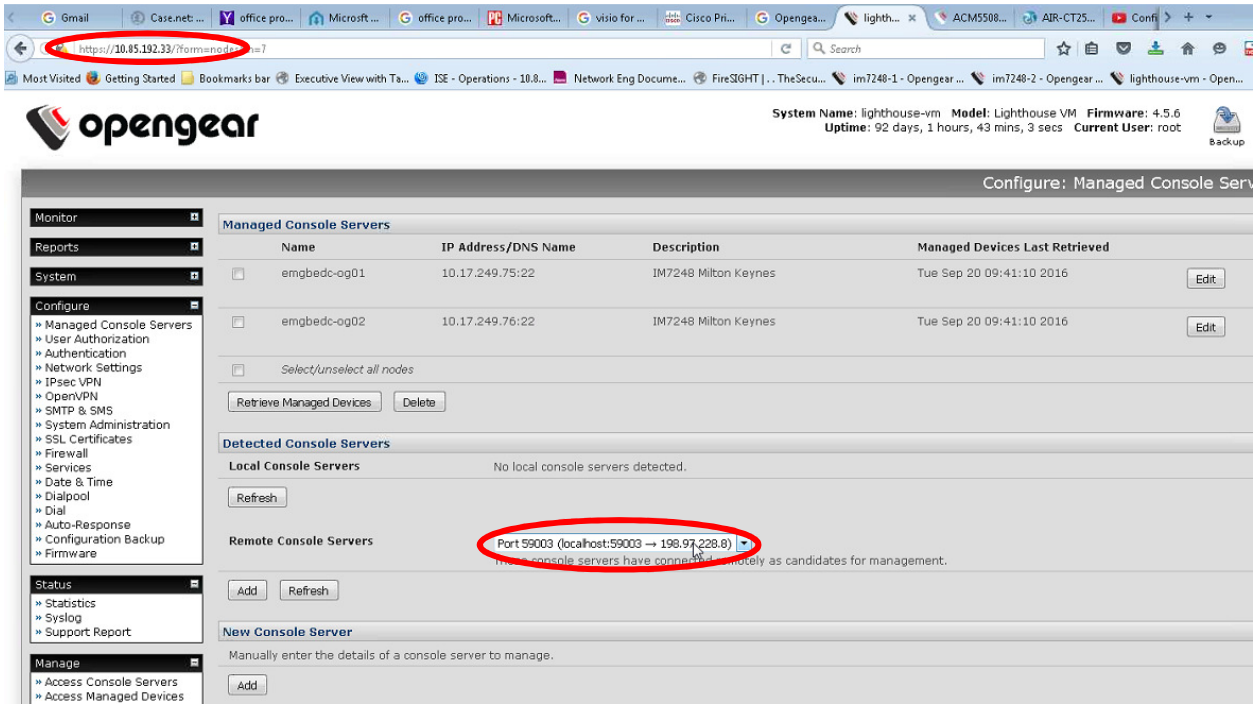
12.4. You should see the following, indicating the configuration succeeded. If you the message "Error Failed to authorize public key for cms@198.97.231.77, check Password" likely an access issue on the local firewall or a routing issue. SSH Port 22 inside (from internal) must be allowed for the session to be built from the Opengear to the Lighthouse server in ATL. An example of a Firewall Access issue follows:





12.5. Note that Port 59003 indicates this box and from the LH we would look for this Port to see that the LH is being called from this 59003 Opengear. For every Opengear added a different port will be auto-generated.

12.6. From the LH GUI, select **Managed Console Servers**, and locate the 59003 in the **Detected Console Servers** section, **Remote Console Servers**.



12.7. under **Remote Console Servers,** select the 59003 in the drop down box and select **Add**

12.8. Complete the information in the next screen.

12.8.1. **Name:** (e.g. AMUSMCIN-CSOOBS1)

12.8.2. **Description**:

12.8.3. Leave **IP address** and **SSH port** as it is configured.

12.8.4. **Remote Password** is used once (to exchange SSH Keys), configure it as the enable password.

12.8.5. Leave the **SSH Key Fingerprint** as it is configured.

12.8.6. Monitoring Section:

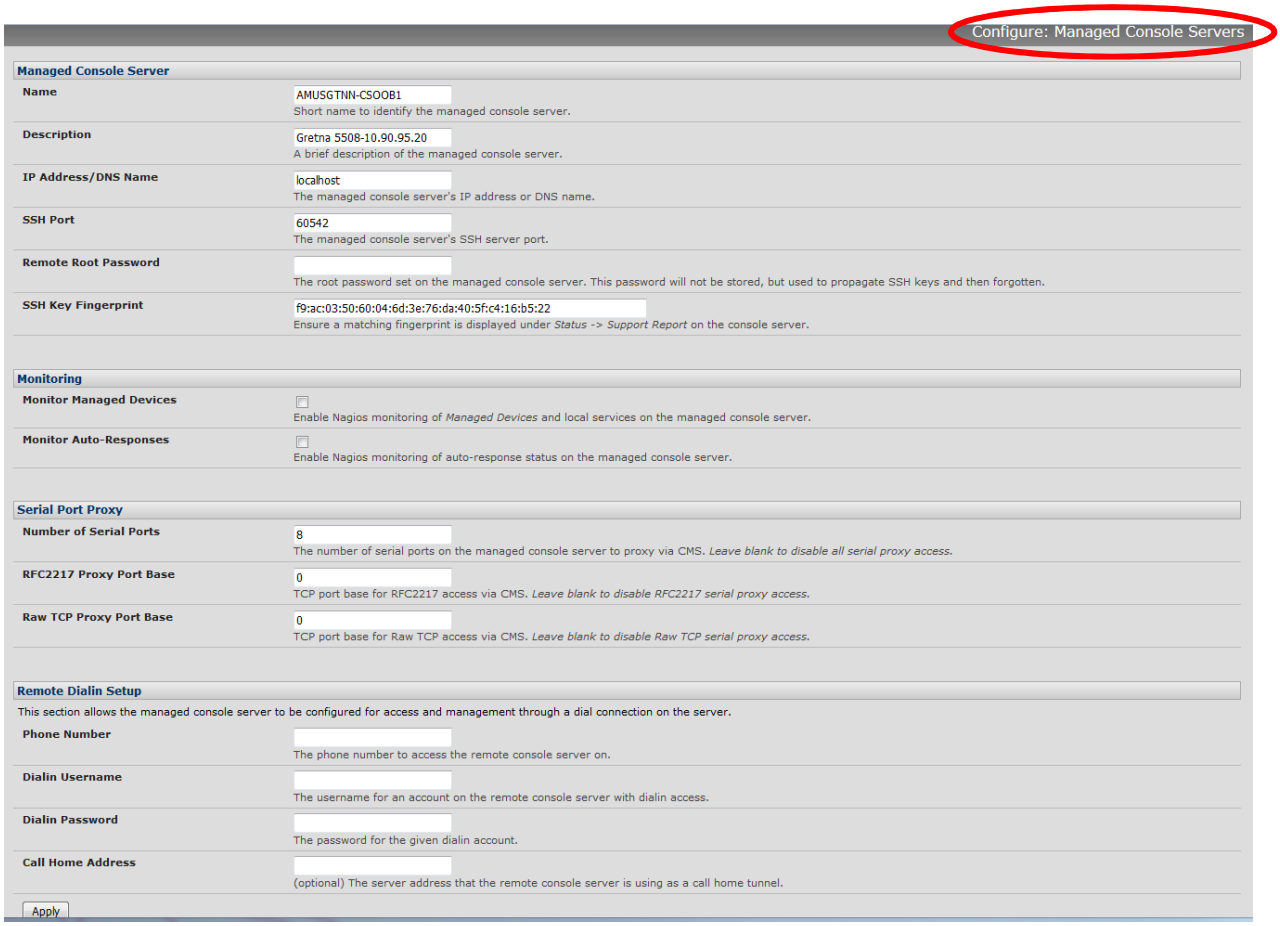
12.8.7. Leave Monitor Managed Devices unchecked because it is very chatty and would not be good if we for some reason switch to Cellular.

12.8.8. Leave **Monitor Auto-Responses** unchecked.

12.8.9. **Number of Serial Ports**: Enter 8 for the 5508 OG Device, 48 if an IM7248 etc.

12.8.10. Remove the **RFS2217** and **RAW TCP Proxy** configuration so that it is blank.

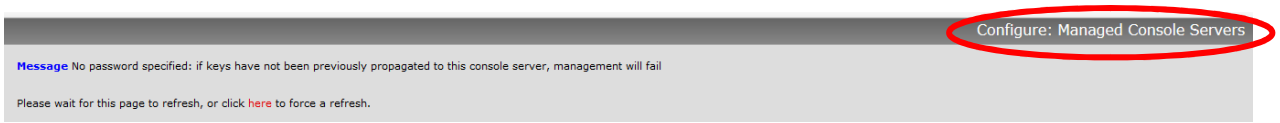
12.8.11. Select **Apply**



12.9. **Notes:**

12.9.1. The image above has a port of 60542 which does not match the aforementioned 59003. This is because the image was taken against another Opengear. Your Ports should match.

12.9.2. After you select Apply, it will take a little while to come back. Don't rush it or try to force a refresh. You will lose the settings. You may see a message like the following, just wait a few minutes, maybe spend this time to update your Goals or Time Allocations.



12.9.3. During this time, the LH is doing a reverse SSH thru the local host IP of the LH to the remote Opengear. This is to allow it to connect to different IP's whether it is Network (LAN) or Cellular over the same TCP port giving the functionality of failover.

12.10. Once the LH screen returns, select the check box next to the new console server that was just added and click on the **Retrieve Managed Devices** button.

12.10.1. Now you should see the LH come back with a screen of Managed Console Servers, which indicates that the remote Opengear was added. In this example AMUSGTNN-CSOOB1 was added.

12.11. At this point, the LH is still connecting to the Opengear via the internal network, not via the cellular. To access the Opengear from LH, select **Browse** on the AMUSGTNN-CSOOB1. To do this:

12.11.1. Select **Manage**: **Access Console Servers**

12.11.2. You should see a 'Window' of the Opengear Device in Light House. You will know that it is a window because you will see "This system is being accessed via Lighthouse – Click here to return to Lighthouse".

12.11.3. See below for an example of the San Diego Opengear device.

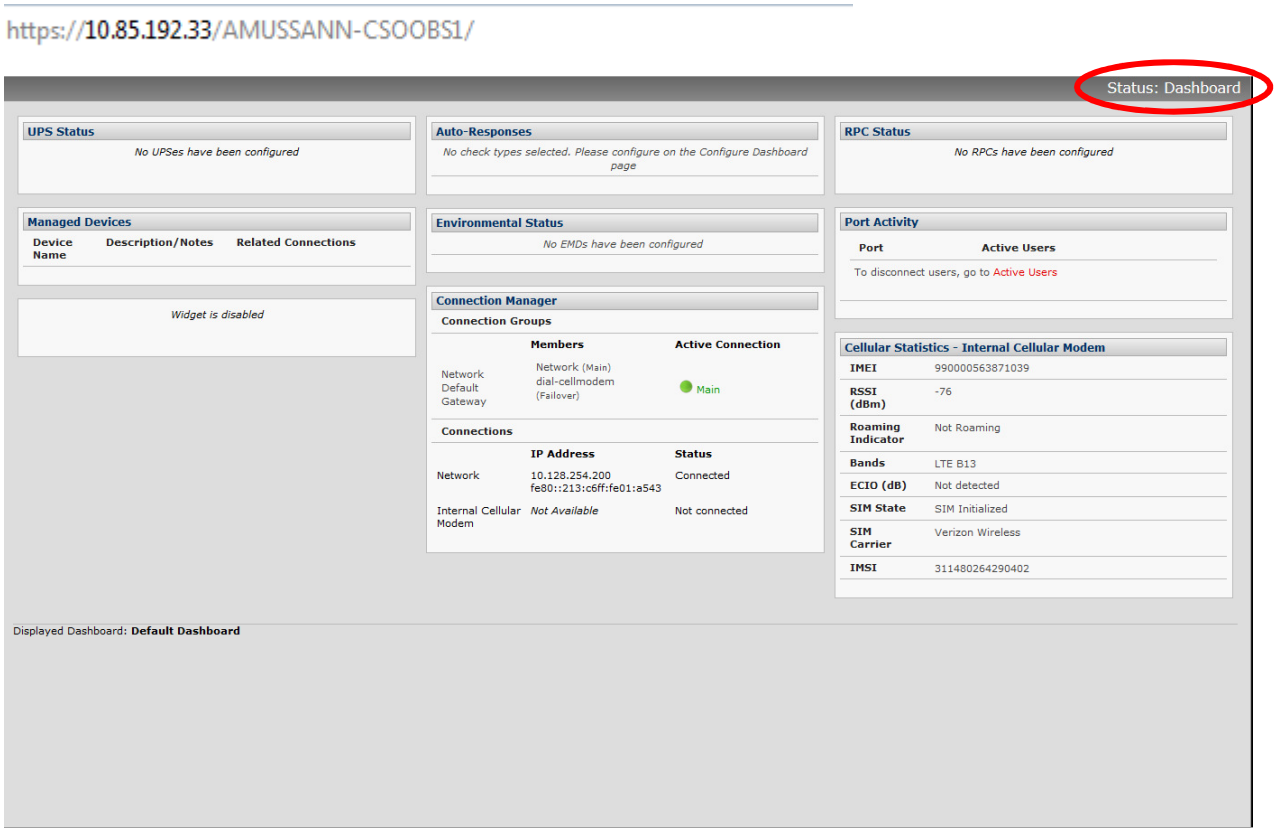
12.11.4. Note that the Network (LAN) is considered 'Main' and the Dial-Cellmodem is considered 'Failover'. The Active connection is Main since we are not actually using the Cellular Failover yet.

12.11.5. You are now connected to the remote Opengear so you may connect to Serial Ports, etc.

12.11.6. **Note:** Normally you will connect directly to the Opengear (in a Non-Failover State) to connect to various Serial Ports, or better yet, simply use SecureCRT to access (SSH) to each specific Serial Port on the remote Opengear device. This example was just intended to demonstrate that during a normal state the LH could be used as a transport 'Window' to a remote Opengear. During an actual outage on the OG LAN side which would make it unreachable via the LAN, the Cellular connection would come up and the Window via the Lighthouse would be your only option for connecting to Serial Ports.

12.11.7. Select '**Click here to return to Lighthouse**'

This system is being accessed via Lighthouse - click here to return to Lighthouse



This system is being accessed via Lighthouse - click here to return to Lighthouse

13. Testing the Call-Home Cellular Backup (if applicable)

13.1. **Note:** When you make configuration changes on the OpenGear devices, you need to go to the LH and retrieve the device configuration so that the LH knows the configuration change on the Opengear has occurred.

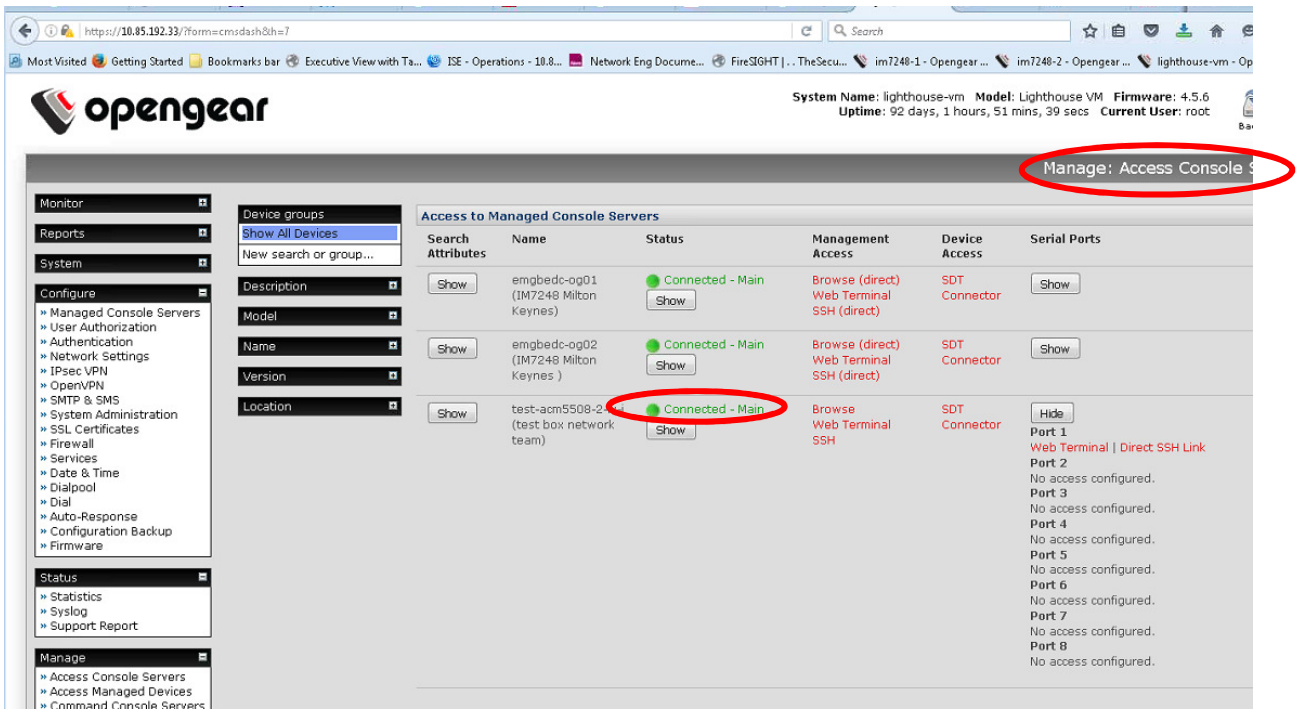
13.1.1. From the LH, simply check the Opengear that has had configuration changes and click on '**Retrieve Managed Devices**'

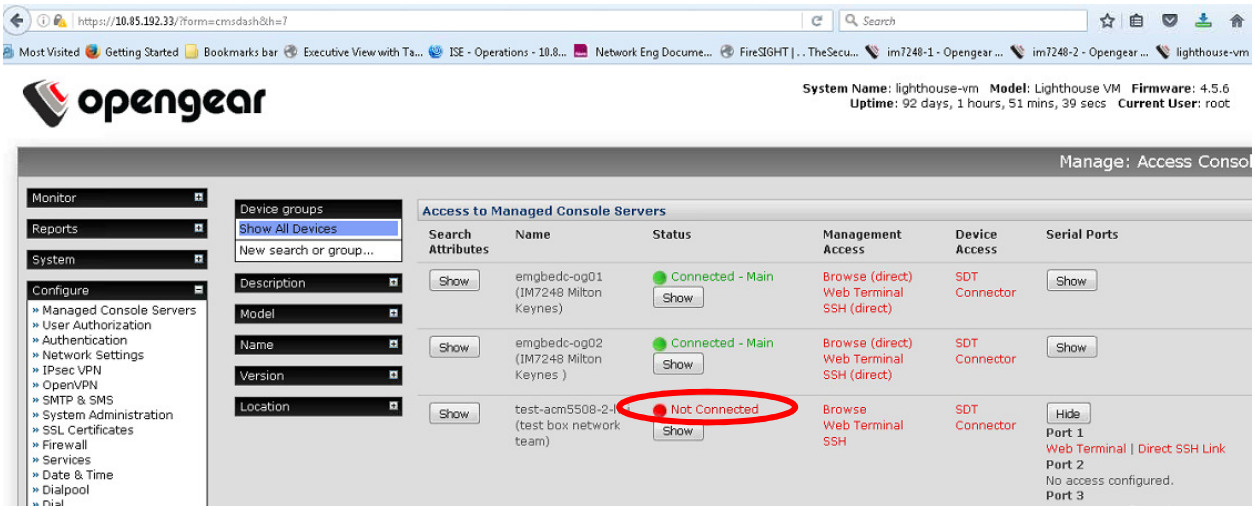
13.2. To test the cellular failover, simply disconnect the LAN port of the Opengear.

13.2.1. You have to wait awhile for Cellular to come up. The following page will take a little time to update because the monitoring is done with Nagios and it has a delay between updates. If the failure is a physical link down at the Opengear LAN interface, it will notice the failover quickly, but if the outage was several hops away, there is a delay due to the 30 sec ping/hold-down timer.

13.2.2. Also (optionally if you want to see it) on the LH CLI – you could do the command: ***# tail –F /var/log/messages.*** This will allow you to follow the progress of the failover.

13.2.3. Watch the Opengear device you're interested in, it should go from **'Connected Main'** to **'Not Connected'**. This may require you to refresh the screen.

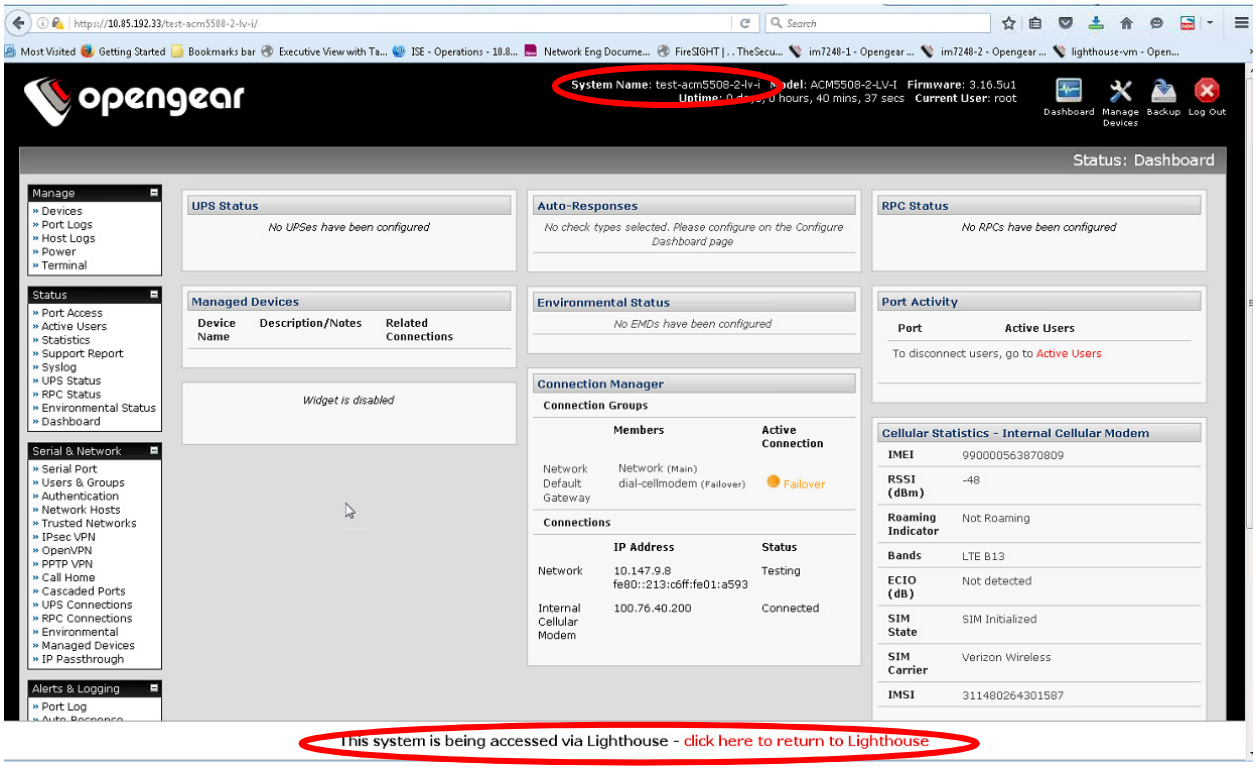




13.2.4. On the LH this is the common messages you will see:

```
Connect to remote > ^C
# tail -F /var/log/messages
<14>Sep 20 09:57:13 cgi[17376]: INFO     /home/httpd/cgi-bin/index.cgi - conman: writing out 14 entries to config file
<14>Sep 20 09:57:13 conman[1589]: INFO     conman - SIGHUP - Reloading Config
<14>Sep 20 09:57:13 conman[1589]: INFO     conman - Finished Reloading Config
<12>Sep 20 09:57:13 cgi[17376]: Command not successful: killall -HUP ard &>/dev/null: Operation not permitted
<12>Sep 20 09:57:13 cgi[17376]: Command not successful: killall -TERM ar_checkd &>/dev/null: Operation not permitted
<12>Sep 20 09:57:13 cgi[17376]: WARN     /home/httpd/cgi-bin/index.cgi - Failed to terminate snmp service
<38>Sep 20 09:59:26 sshd[16400]: Timeout, client not responding.
<86>Sep 20 09:59:26 sshd[16398]: pam_unix(sshd:session): session closed for user cms
<38>Sep 20 09:59:37 sshd[17454]: Timeout, client not responding.
<86>Sep 20 09:59:37 sshd[17386]: pam_unix(sshd:session): session closed for user cms
<38>Sep 20 10:01:22 sshd[18133]: WARNING: /etc/config/moduli does not exist, using fixed modulus
<38>Sep 20 10:01:24 sshd[18133]: Accepted publickey for cms from 70.195.12.76 port 10055 ssh2
<86>Sep 20 10:01:24 sshd[18133]: pam_unix(sshd:session): session opened for user cms by (uid=0)
<35>Sep 20 10:01:24 sshd[18135]: error: bind: Address already in use
<35>Sep 20 10:01:24 sshd[18135]: error: bind: Address already in use
```

13.3. **Note**: Nothing wrong here, remember the Opengear establishes a connection (via cellular) to the same IP that it was communicated with before the outage (via the LAN port). Sometimes Nagios doesn't update the 'Not Connected' to 'Connected" for whatever reason. To manually test the cellular failover to verify it switched, you can select **'Browse'** which is to the right of the 'Not Connected' message. If you do this, wait a few seconds for the screen to update and you should see something like the following:



13.3.1. Now you are connected to the remote Opengear via the Cellular connection. The connection is going thru the Lighthouse to a private IP address on the cellular modem (this case 100.76.40.200). You can now click on the "**Click here to return to Lighthouse**".

13.4. Now we are able to connect to a remote Opengear via the LH and connect to a serial port. Open up a CLI to the LH server (10.85.192.33) login as root and our standard Root/Admin/aaa.admin User Password.

#pmshell <cr>

```
# pmshell

 1: emgbedc-og01                                    2: emgbedc-og02
    IM7248 Milton Keynes                                IM7248 Milton Keynes
 3: test-acm5508-2-lv-i
    test box network team

Connect to remote > 3

 1: Port 1

Connect to port >
```

13.4.1. Enter your Port # of the device you want to connect to and <cr>

```
 1: Port 1

Connect to port > 1

AdamsCubeTemp>
AdamsCubeTemp>
AdamsCubeTemp>
AdamsCubeTemp>
AdamsCubeTemp>exit
```

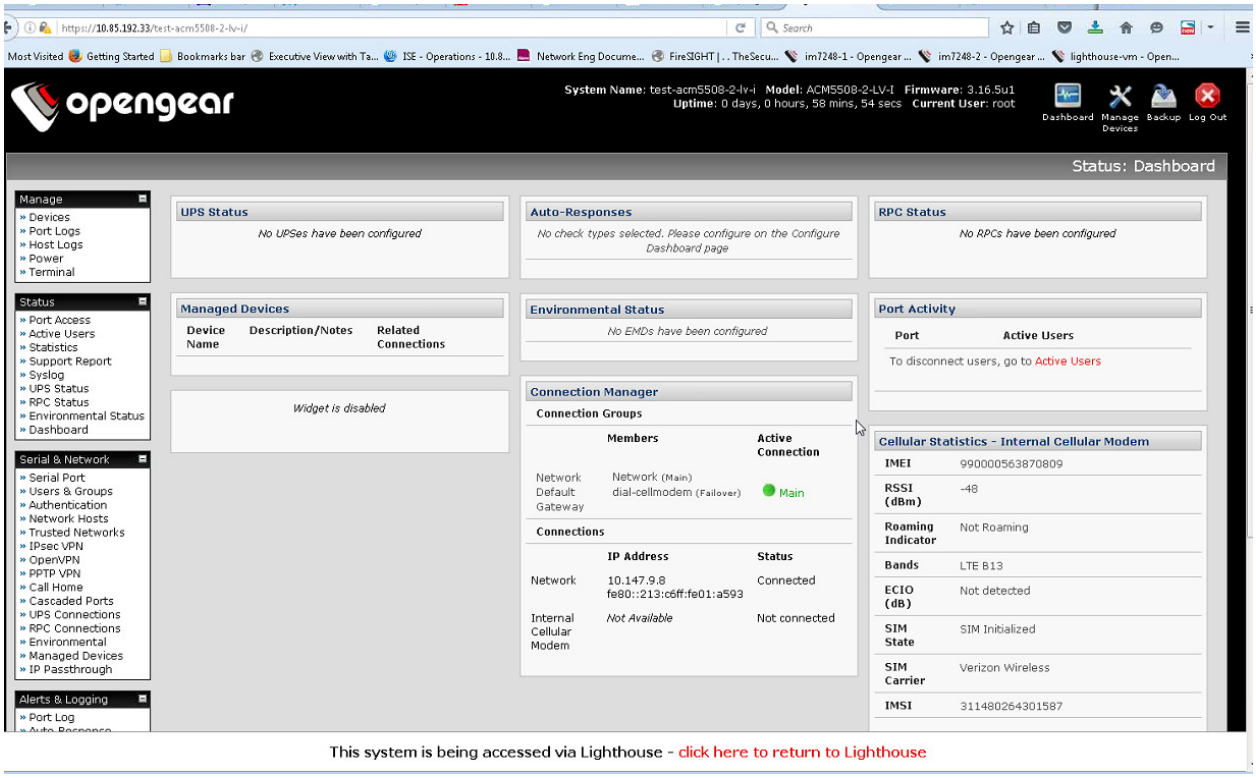
13.4.2. To get back to the “prompt #”, hit **enter** and ‘**~**.’

13.4.2.1. So in other words, <cr>, tilde, Period (no spaces)

13.4.3. To get back to the menu to select another console port, hit **enter** and ‘**~m**’

13.4.3.1. So in other words, <cr>, tilde, m (no spaces)

13.5. To go back to the Primary LAN connection following the failover test, reconnect the LAN interface on the Opengear, for example and wait for the tunnel to drop and come back up. You should see a screen like the following that shows the LAN connection came back up.



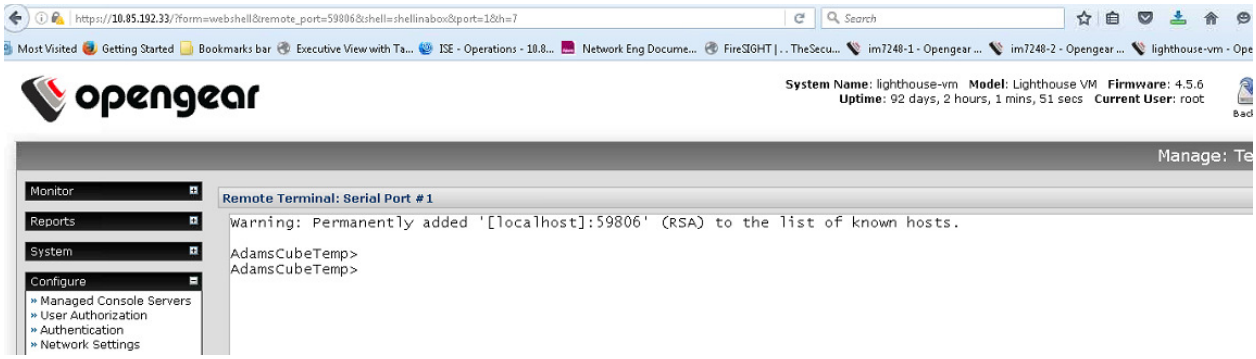
14. Alternative way to connect to the Opengear via the Lighthouse.

14.1. Use this feature as an alternative way to connect to a console port (LH CLI with pmshell menu was the other way).

14.1.1. On the Lighthouse, you can select the ‘Show’ button on the right side of the screen.

14.1.2. The Show button converts to a Hide button

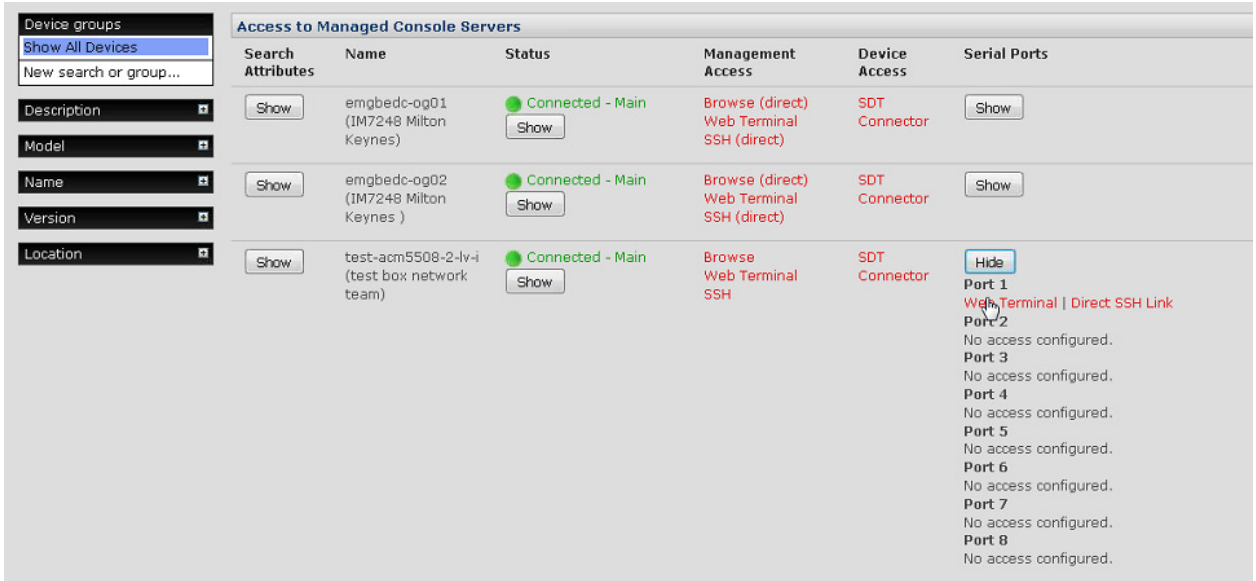
14.1.3. Select Web Terminal and you will see the following screen:



14.2. To get back:

14.2.1.1. Select Manage

14.2.1.2. Select Access Console Servers



14.3. There is a prerequisite for the Web Terminal method of accessing a Remote Opengear Serial Port.

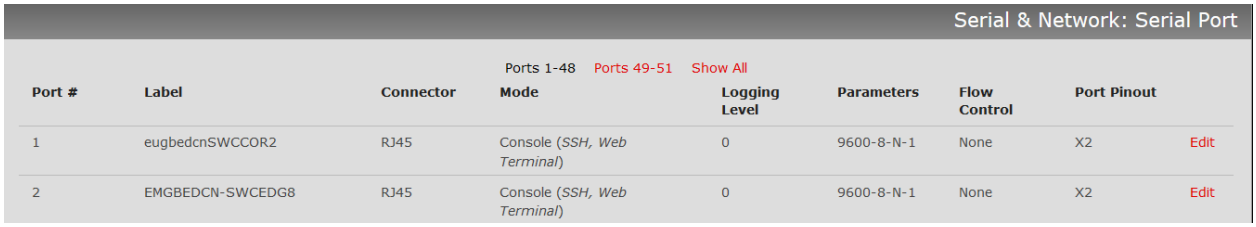
14.4. On the Opengear

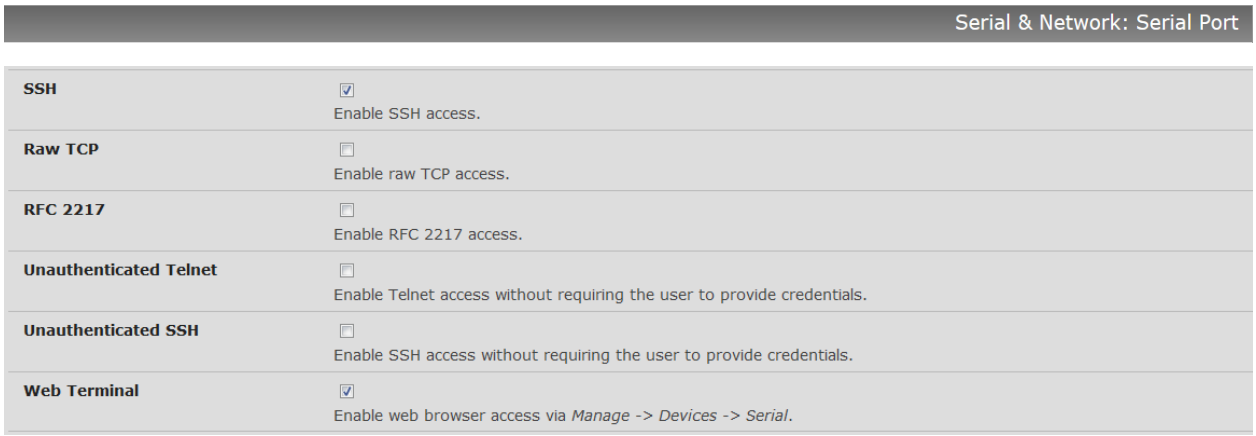
14.4.1. Select Serial & Network

14.4.2. Select Serial Port

14.4.3. Select 'Edit' on the desired Serial Port and don't forget to Apply

14.4.4. Select SSH and Web Terminal Setup on a specific console Port:





15. Configuring TACACS+

15.1. On the Opengear select **Serial & Network: Authentication** and configure the following sections:

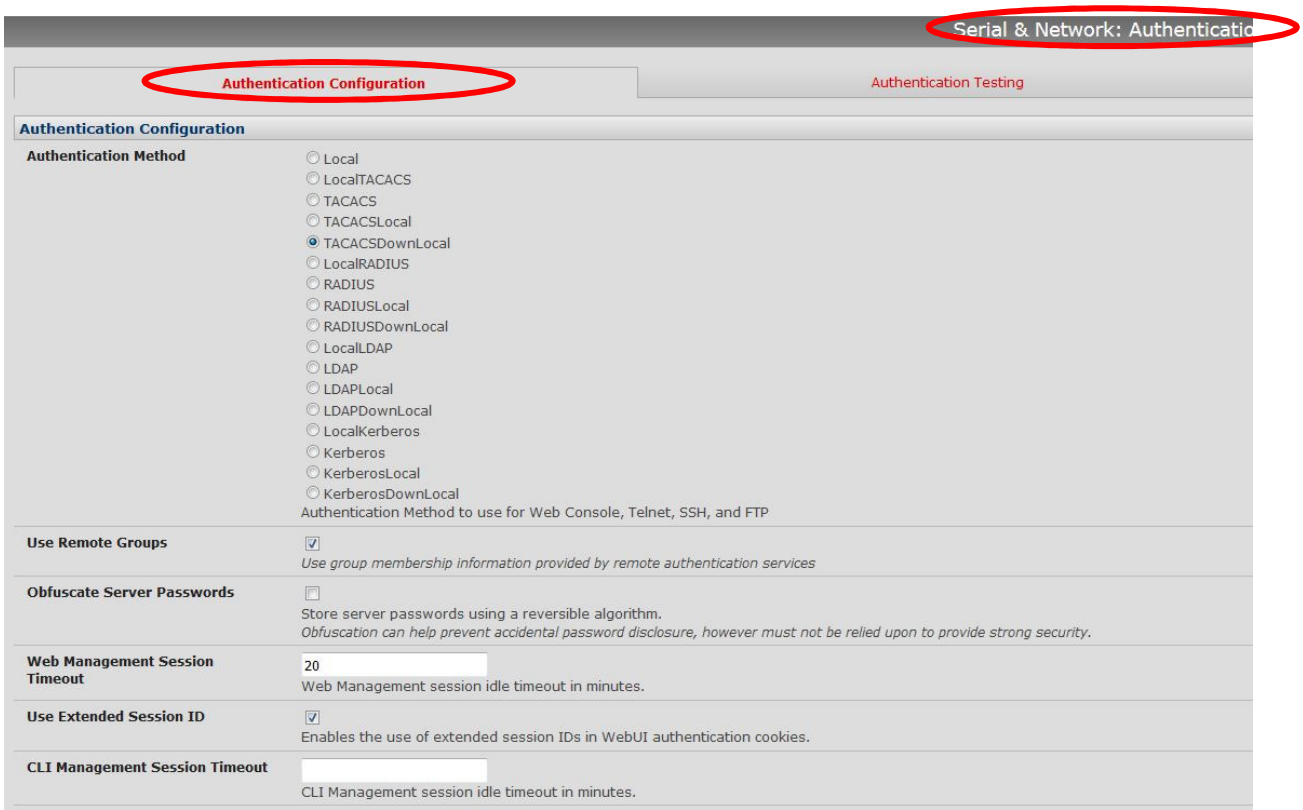
15.1.1. Authentication Configuration:

15.1.1.1. **Authentication Method**: TACACSDownLocal

15.1.1.2. **Use Remote Groups**: select box

15.1.1.3. **Web Management Session Timeout**: 20

15.1.1.4. **Use Extended Session ID**: select box



15.1.2. TACACS+:

15.1.2.1. **Authentication and Authorization Server Address**: 10.85.193.13, 10.85.193.14

15.1.2.2. **Disable Accounting**: leave alone:

15.1.2.3. **Accounting Server Address**: 10.85.193.13, 10.85.193.14

15.1.2.4. **Server Password**: (TACACS shared secret)

15.1.2.5. **Confirm Password**: (TACACS shared secret)

15.1.2.6. **TACACS Login Method**: (Leave Blank)

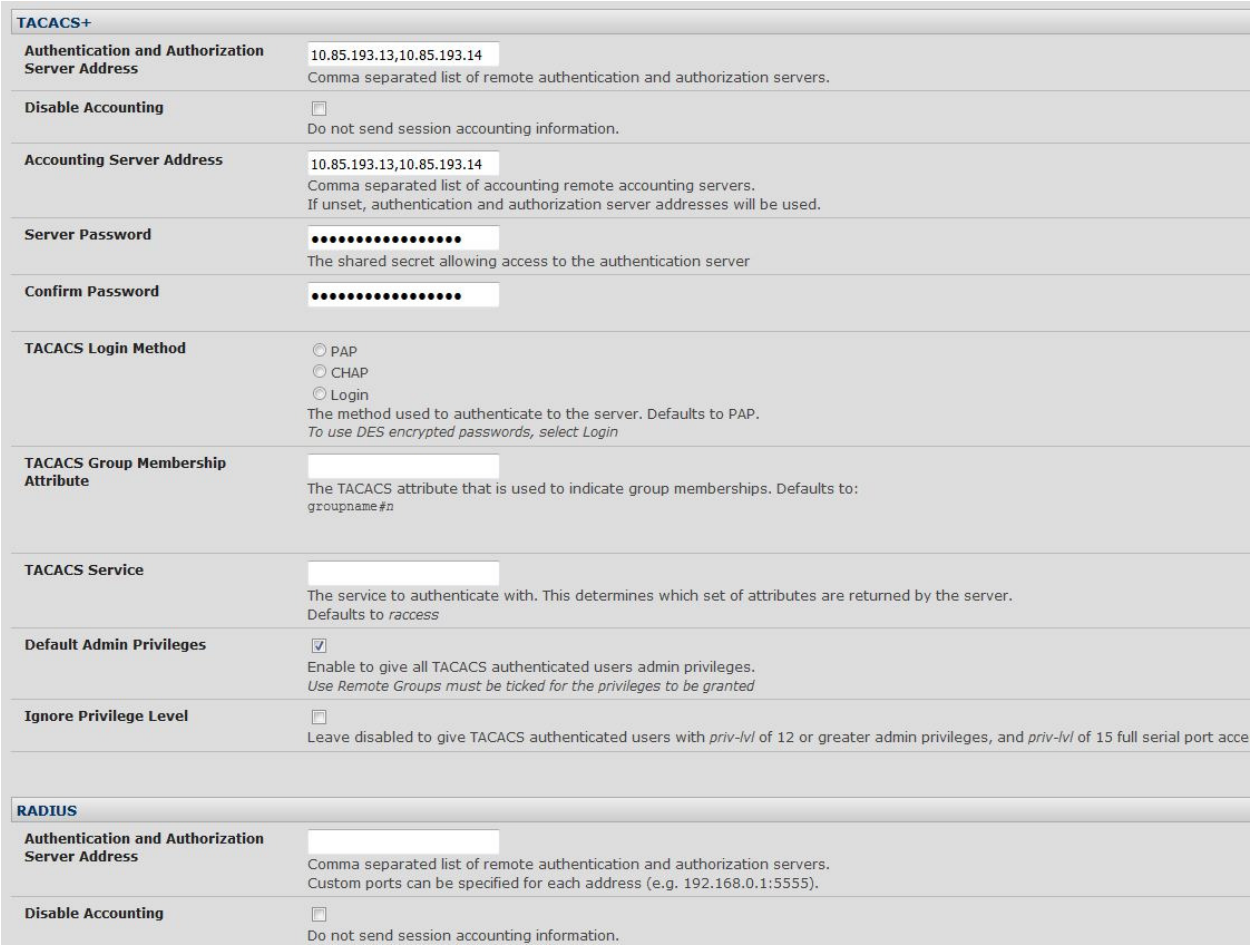
15.1.2.7. **TACACS Group Membership Attribute**: (Leave Blank)

15.1.2.8. **TACACS Service**: (Leave Blank)

15.1.2.9. **Default Admin Privileges**: Check Box

15.1.2.10. **Ignore Privilege Level**: (Leave Blank)

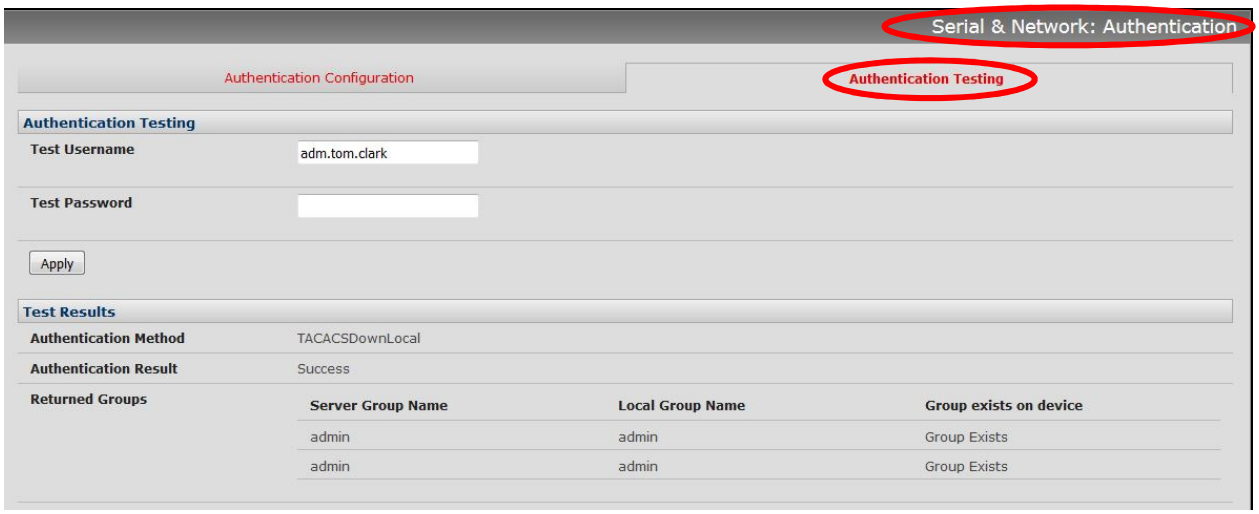
15.1.3. Leave all other sections blank.



15.2. Authentication Testing

15.2.1. Select **Serial & Network: Authentication** and then the **Authentication Testing Tab**

15.2.1.1. Type in the Test Username and Test Password and hit 'Apply'



16. Noteworthy Items to Consider

Sometimes you might encounter the need for a Host Route to be added to the local network in order to allow an Opengear device to communicate to the Internet (Towards the Public IP of the Lighthouse 198.97.231.77).

If a site receiving the Opengear device uses Atlanta DC for Internet this would be a problem. The Opengear would try to establish a connection to the LH and exit the ATL Internet and try to come back in towards the LH. Because Hair-Pinning isn't allowed at the Firewall the connection to the LH would fail.

If the site receiving the Opengear device has its own Internet connection this would not be a problem provided the Local Internet is utilized for direct client browsing to the Internet as opposed to having the local internet strictly used, for example, incoming internet traffic destined for locally hosted servers.

Because of this issue, this may be a case to build a second Lighthouse server in EDC. Locations that use Atlanta for Internet would have their Opengear Devices pointed to the EDC LH. Locations that use EDC for Internet would have their Opengear Devices pointed to the ATL LH.

Example: Gretna has its own Internet connection but it is only allowed for incoming traffic to Gretna Hosted Internet Servers. Regular browsing traffic outbound towards the Internet will route via Atlanta DC and would fail because of the hair-pinning issue (The LH is in Atlanta). The solution here is to put a Static Host Route in the local Core router and point traffic destined for the LH 198.97.231.77 via the Local Internet connection.

Description: Gretna OpenGear/LightHouse host route.

Example Script: AMUSGTNN-SWCCOR1

ip route 198.97.231.77 255.255.255.255 10.90.95.6

Also make sure you configure SSH Port 22 access on the Firewall Ingress-Inside if necessary.

Example:

AMUSGTNN-FWINET1#
object-group service PUBLIC_ACCESS tcp-udp
port-object eq 22

17. CLI commands on the Opengear Device.

- SSh to the Opengear 5508 Device via the Static IP address you assigned to it.
- To become root: sudo –I
    - $ prompt is admin
    - # prompt is root
- To view latest log messages: tail –F /var/log/messages
    - To stop the tail, enter CTRL-C
- Select the Disable Dial-Out communication (Under the Internal Cellular Modem tab)
- Select the Enable Dial-Out communication (Under the Internal Cellular Modem tab)
    - Delete anything in the Username and Password fields
- Select Apply Modem Dial Settings, this will allow us to monitor for any errors that may be occurring
- Other Commands:
    - Interface List: ifconfig
    - Cellular Modem Information: cellctl –lis
    - # config -g config.cellmodem
    - config.cellmodem.ddns.provider none
    - config.cellmodem.ppp.dialer.enabled on
    - Configure: tail –F /var/log/messages

- # config -g config.cms.address
- config.cms.address 198.97.231.77

- To change the Public IP of the LH (Already completed, so do not do)

- #config –s config.cms.address=198.97.231.77

- #config –a
- This retrieves the configuration from all remote OG devices into the Lighthouse.

- # pmshell <cr>

```
# pmshell
 1: emgbedc-og01                                          2: emgbedc-og02
    IM7248 Milton Keynes                                     IM7248 Milton Keynes
Connect to remote >
```

- To get out (to get back to the prompt #), hit enter and '~.'
    - So in other words, <cr>, tilde, Period (no spaces)
- To get out (back to menu to select another console port), hit enter and '~m'
    - So in other words, <cr>, tilde, m (no spaces)
- # cat etc/version

Open Issues Needing Resolution: