



# **How to setup a HALO OnSite Controller**

## Contents

1. Introduction to the HALO OnSite Controller.....	4
2. Connecting a HALO OnSite Controller to a network .....	6
2.1 Step 1: .....	6
2.2 Step 2: .....	6
2.3 Step 3: .....	7
2.4 Step 4: .....	7
2.5 Step 5: .....	8
3. Connecting Radios to the system .....	13
3.1 HyteraIP.JSON configuration file for PNC370 and PNC380S .....	13
3.2 VM780, PNC550 and PDC760.....	13
4. How to change the IP address of your Controller .....	14
4.1 Getting started.....	14
4.2 Changing the HALO OnSite Controller IP Address.....	16
4.3 Changing OMCH IP – this is the management platform IP .....	20
4.4 Log into the network management (UNMS).....	22
4.5 Updating the Monitoring System IP Addresses in the UNMS.....	23
4.5.1 Step 1: Modifying the equipment Communications IP .....	23
4.5.2 Step 2: Navigate to the Network Element Management Section .....	24
4.5.3 Step 3: TCF Service .....	25
4.5.4 Step 4: TMF Service .....	26
4.5.5 Step 5: DBS Service .....	27
4.5.6 Step 6: FRS Service.....	28
4.5.7 Step 7: PRES Service .....	29
4.5.8 Step 8: PHSS Service .....	30
5. Configuring your firewall for remote device access .....	31
5.1 Configuring the Controller for remote network access.....	31
5.1.1 How to query the Controller for the [TmfRemoteMediaAddrMap] parameter .....	31
5.2.2 How to modify/add/delete the table entries .....	33
5.2.3 Restarting the service after modifying the settings .....	33

## List of Figures

Figure 1. HALO OnSite Controller .....	4
Figure 2. HALO OnSite Controller Front Panel.....	4
Figure 3. HALO OnSite Rear Panel .....	5
Figure 4. Run Command.....	7
Figure 5. Ping Command good connectivity .....	8
Figure 6. UNMS Login Screen .....	9
Figure 7. Enter the Default UNMS login credentials .....	9
Figure 8. UNMS Topology Monitor Screen .....	10
Figure 9. Subscriber Management Menu.....	10
Figure 10. Subscriber Landing page.....	11
Figure 11. Organization Menu .....	11
Figure 12. Customer Subscriber List .....	12
Figure 13. WebLMT 2.0 .....	14
Figure 14. WebLMT Landing Page .....	15
Figure 15. Changing the language to English .....	15
Figure 16. WebLMT System IP Configuration Menu selection .....	16
Figure 17. WebLMT SystemIPConfig landing page.....	16
Figure 18. WebLMT SystemIPConfig .....	17
Figure 19. WebLMT SytemIPConfig updated IP settings .....	17
Figure 20. Putty terminal setup screen .....	18
Figure 21. Terminal Login screen in Putty .....	19
Figure 22. OMCHLink IP Settings.....	20
Figure 23. OMCHLink ID.....	21
Figure 24. UNMS Not completely loaded - no Captcha visible.....	22
Figure 25. UNMS ready for login - Captcha loaded.....	22
Figure 26. Equipment Management Menu Selection.....	23
Figure 27. Modify Equipment Menu .....	23
Figure 28. Network Element Management Menu .....	24
Figure 29. Network Element List.....	24
Figure 30. TCF Service Settings in the UNMS .....	25
Figure 31. TMF Service Settings in the UNMS .....	26
Figure 32. DBS Service Settings in the UNMS .....	27
Figure 33. FRS Service Settings in the UNMS .....	28
Figure 34. PRES Service Settings in the UNMS.....	29
Figure 35. PHSS Service Settings in the UNMS.....	30
Figure 36. TmfRemoteMediaAddrMap page.....	32
Figure 37. TmfRemoteMediaAddrMap Query menu.....	32
Figure 38. TmfRemoteMediaAddrMap Example Query result.....	33
Figure 39. Device Menu .....	33
Figure 40. ETC Menu .....	34
Figure 41. TMF Restart Selection .....	34

## 1. Introduction to the HALO OnSite Controller

The HALO OnSite Controller comes in a small form factor case with fans on the front pushing air through the case, exhausting it at the rear.



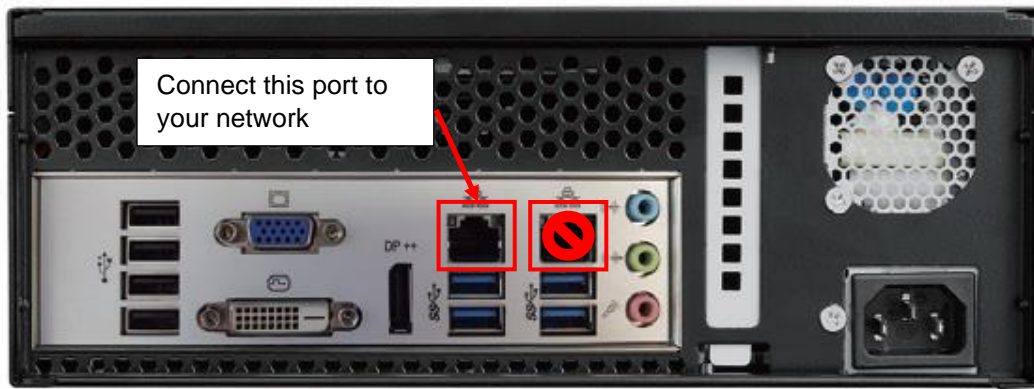
Figure 1. HALO OnSite Controller

There is a toggle power button on the front of the case, just below the LED indicators for Power and Hard Drive activity. There is also an orange reset button available. See Figure 2. HALO OnSite Controller Front Panel.



Figure 2. HALO OnSite Controller Front Panel

On the back of the Controller we have USB, Ethernet, Video, Audio and Power ports. The Ethernet and Power connections are the only ones that will be used in the device during normal setup and running conditions. The left Ethernet port is the one that is configured for external access and the default IP Address for it is: 172.168.43.47 with a mask of 255.255.255.0 and Gateway 172.168.43.1.



*Figure 3. HALO OnSite Rear Panel*

There is no need to connect a monitor or keyboard to the Controller, as you cannot manage the system via the operating system login.

## 2. Connecting a HALO OnSite Controller to a network

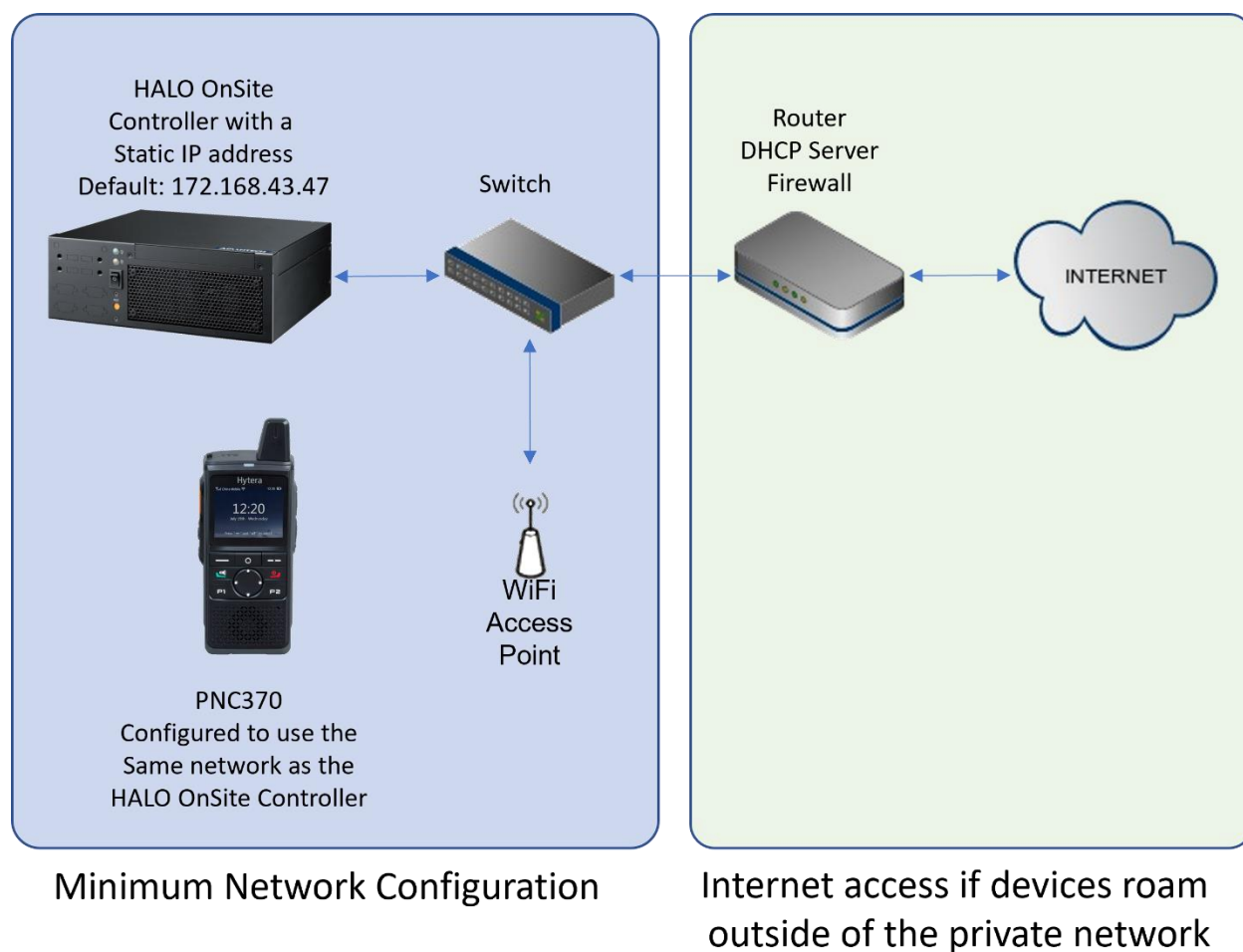
### 2.1 Step 1:

Plug in the power cable to the power connector on the back of the Controller and a regular AC power outlet able to supply 120VAC at maximum consumption of 300W.

There is no need to connect a keyboard or monitor to the HALO OnSite controller. All system and device management will be done via a browser.

### 2.2 Step 2:

Connect an ethernet cable to the left ethernet port of your HALO OnSite Controller and a LAN port on your WiFi router. This WiFi network needs to be the same network that you will be using for your management computer and the PNC devices.



## 2.3 Step 3:

Press the power button on the front of the HALO OnSite controller once, to turn it on. You will hear the fans spin up and you should see the drive activity light flashing orange as the system is starting up. Please allow a few mins for it to complete the startup process.

While you are waiting for this process to complete, please configure your PC to the same subnet as the IP address of your OnSite Controller, using the information below:

- a. IP Address of 172.168.43.50
- b. Use Mask of 255.255.255.0
- c. Use Gateway of 172.168.43.1
- d. No need for any DNS info.

## 2.4 Step 4:

Verify that you now have connectivity over the network to your HALO OnSite Controller. You can do the “ping” command in Windows. Use it as follows:

- a. Open the command prompt in Windows by pressing the “Windows Key + R” and typing in “cmd” in the box that appears. Then click “OK”.

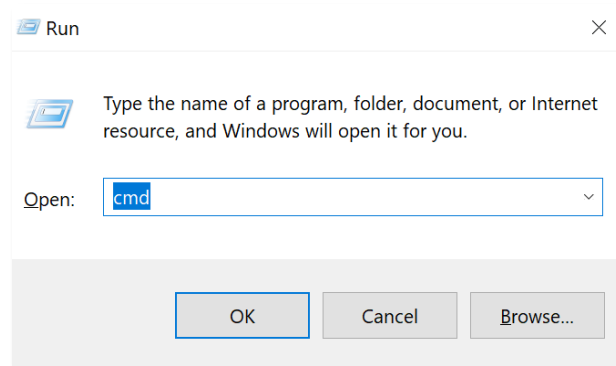
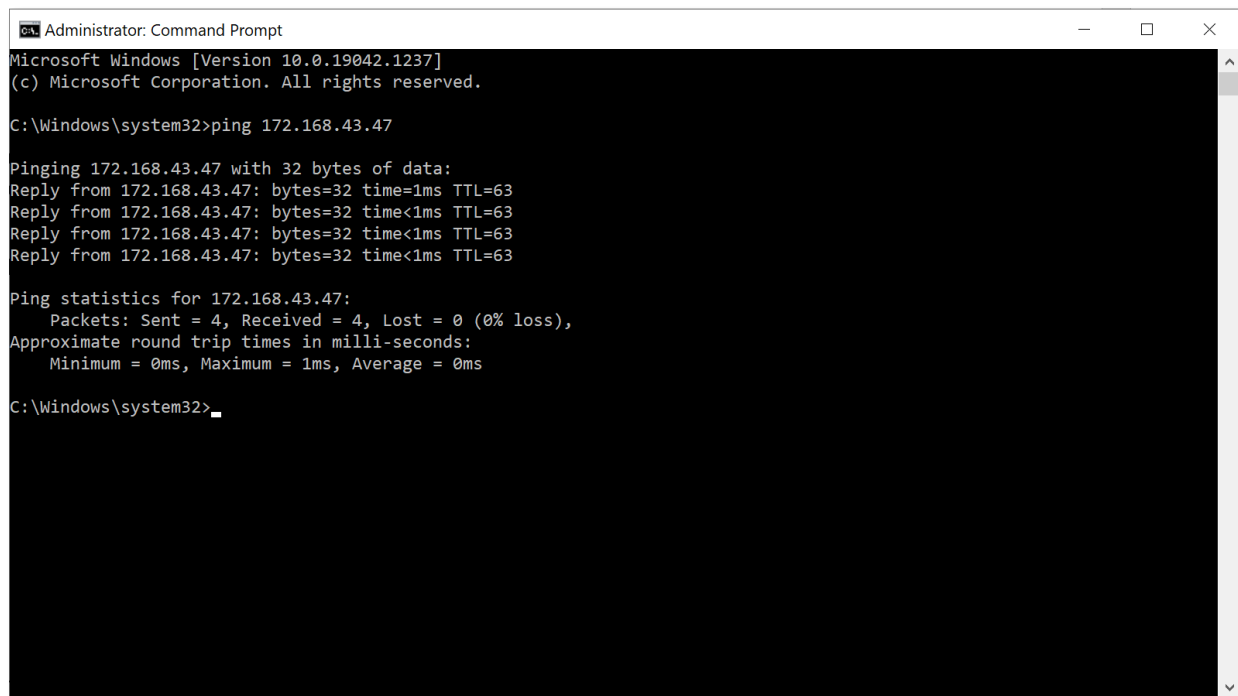


Figure 4. Run Command

- b. At the prompt type in “ping 172.168.43.47” followed by <enter>



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19042.1237]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>ping 172.168.43.47

Pinging 172.168.43.47 with 32 bytes of data:
Reply from 172.168.43.47: bytes=32 time=1ms TTL=63
Reply from 172.168.43.47: bytes=32 time<1ms TTL=63
Reply from 172.168.43.47: bytes=32 time<1ms TTL=63
Reply from 172.168.43.47: bytes=32 time<1ms TTL=63

Ping statistics for 172.168.43.47:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Windows\system32>
```

Figure 5. Ping Command good connectivity

If you receive any other response such as “Destination host unreachable” or “Request timed out” then you do not have connectivity to your HALO OnSite controller. Check that all your cables are connected and the power is connected. If you still do not have connectivity, please contact support.

## 2.5 Step 5:

This step assumes that connectivity has been successfully verified in the previous steps. This step will not work if connectivity failed in the previous step.

Using Google Chrome enter the following details in the address bar “https://172.168.43.47” (IP address of your controller).



You will be greeted by the UNMS login screen as seen in Figure 6. UNMS Login Screen. Make sure the Captcha is visible. Under normal running conditions the captcha will show up when the page is loaded, however if the Controller is still in the startup phase, the captcha will not be visible, even if the page loaded successfully. You will not be able to login until the captcha is visible!



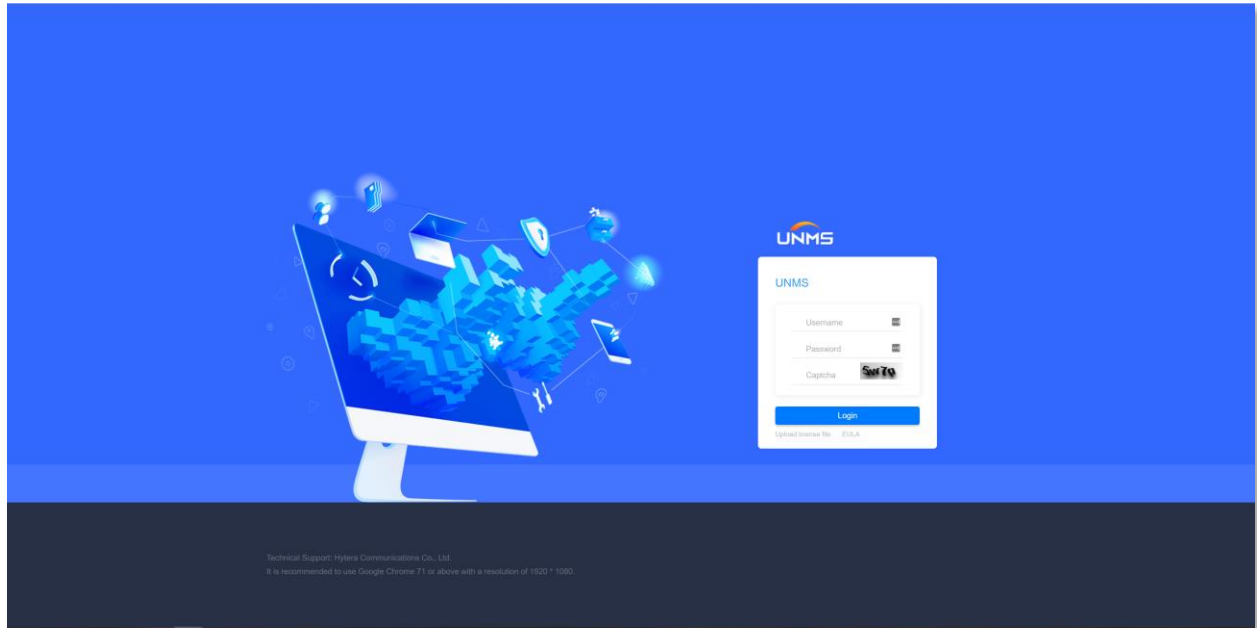


Figure 6. UNMS Login Screen

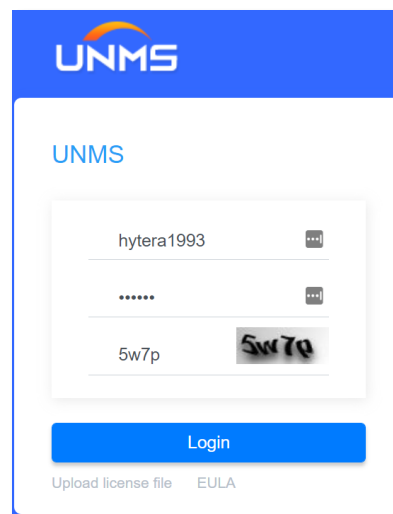


Figure 7. Enter the Default UNMS login credentials

The Captcha rotates on a regular basis, so it is good practice to click on the image to rotate it to the next one, before entering the matching characters in the field to the left of it.

**Note:** When you first login you will be greeted with a “change password” screen. At this point you can change your password, or you can retype your existing password to continue to use it. You can change the password from the user interface, without being prompted at first login.

The default credentials are:

**Username:** “hytera1993” **Password:** “123456”

This is the primary username for managing the subscribers and groups in the radio system. Once you have successfully logged in, you will be greeted with a window like Figure 8. UNMS Topology Monitor Screen.

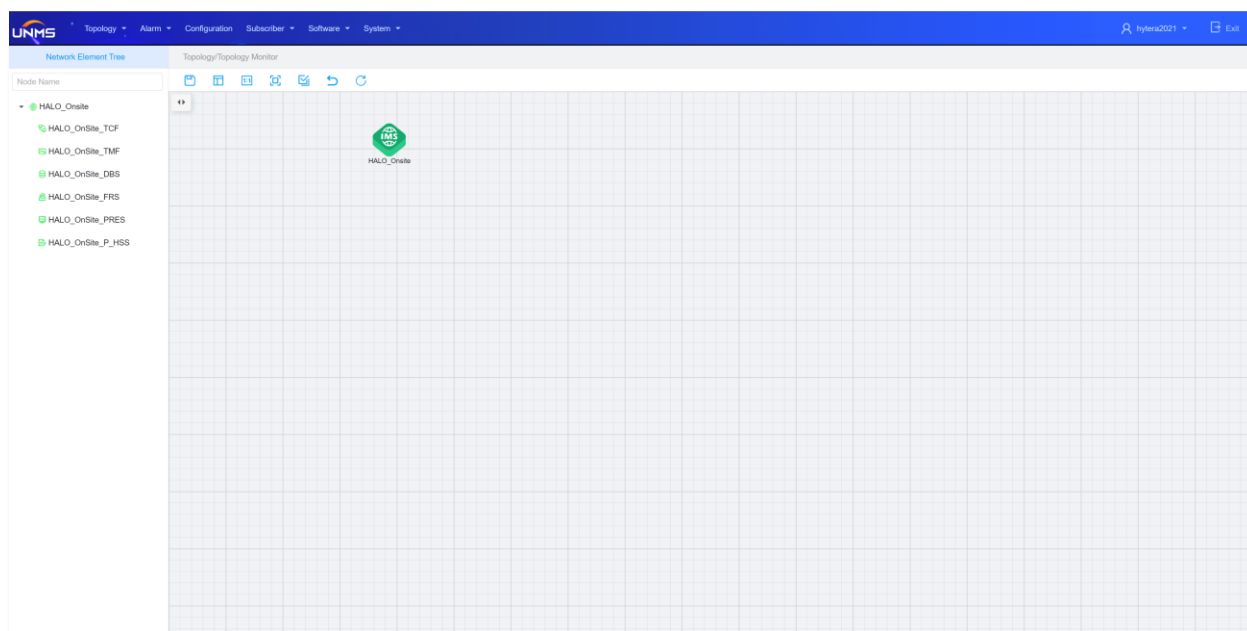


Figure 8. UNMS Topology Monitor Screen

You need to click on “Subscriber/IMS management” followed by “Subscriber management” to configure radios on the system. See Figure 9. Subscriber Management Menu.

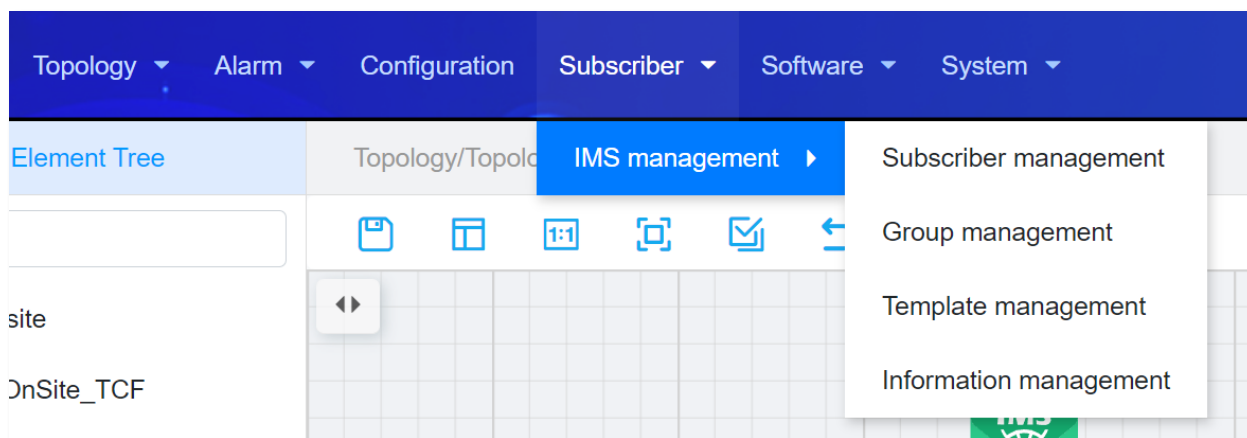


Figure 9. Subscriber Management Menu

After selecting “Subscriber management”, you will be greeted with a screen that seems to show that you have no subscribers, such as seen in Figure 10. Subscriber Landing page.

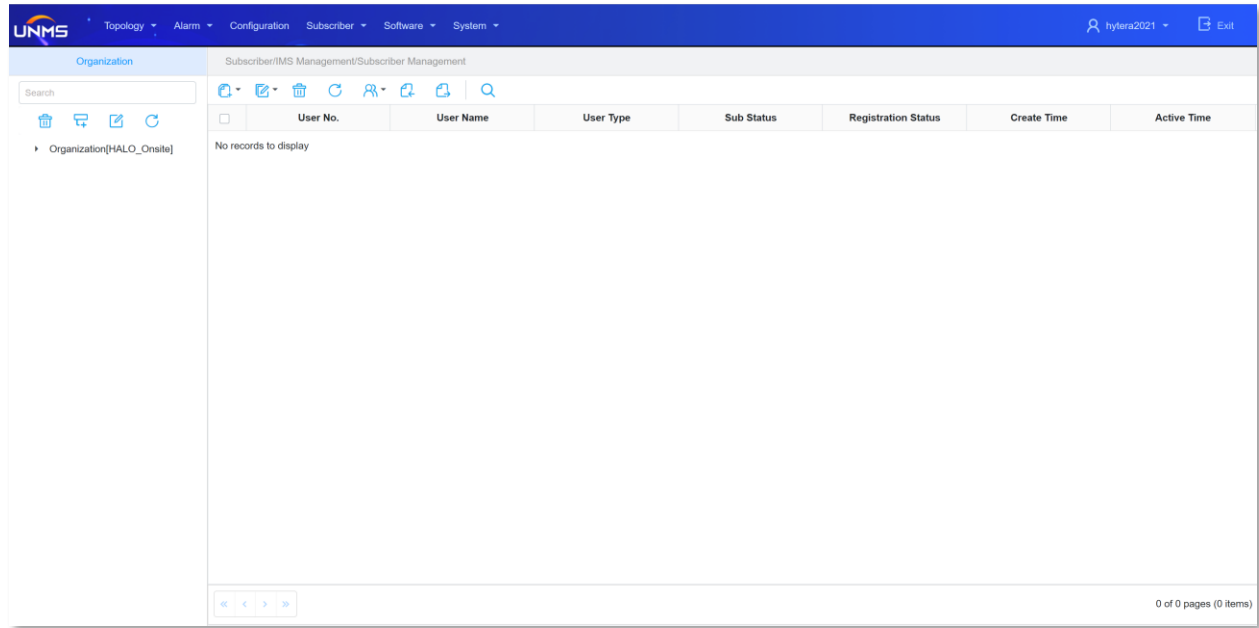


Figure 10. Subscriber Landing page

Simply click on the menu on the left “Organization” as seen in Figure 11. Organization Menu.

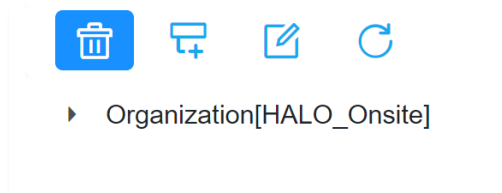


Figure 11. Organization Menu

Once you click on that, you will see another menu called “Customer”, keep in mind that this can be named anything, but for this instance it is named “Customer”. Select it, and you will see a list of all the devices configured for use on this system (Figure 12. Customer Subscriber List).

	User No.	User Name	User Type	Enable Switch	Create Time	Active Time
<input type="checkbox"/>	80020200	PNC370_1a	PNAS Terminal	Enable	2021-09-21 17:25:59	2021-01-31 17:45:58
<input type="checkbox"/>	80020201	550ABCD	PNAS Terminal	Enable	2021-09-07 12:35:29	2021-01-31 17:57:45
<input type="checkbox"/>	80020202	VM780	PNAS Terminal	Enable	2021-06-03 17:46:57	2021-03-23 07:33:49
<input type="checkbox"/>	80020203	80020203	PNAS Terminal	Enable	2021-04-26 11:22:38	
<input type="checkbox"/>	80020210	Test	PNAS Terminal	Enable	2021-07-19 06:42:37	
<input type="checkbox"/>	80020211	Test1	PNAS Terminal	Enable	2021-07-19 06:42:37	
<input type="checkbox"/>	80020212	Test2	PNAS Terminal	Enable	2021-07-19 06:42:38	
<input type="checkbox"/>	80020213	Test3	PNAS Terminal	Enable	2021-07-19 06:42:38	

Figure 12. Customer Subscriber List

You are now ready to start adding radios to the system. There is a complete manual available on how to manage subscribers and groups.

### 3. Connecting Radios to the system

The radios that will use the system must now be programmed with the following information to allow them to connect:

- Radio ID
- Password for the matching radio ID
- IP address of the server (default is 172.168.43.47)
- Port used to connect to the server (default is 5067)

#### 3.1 HyteraIP.JSON configuration file for PNC370 and PNC380S

The PNC370 and 380S units reads their configuration from the HyteraIP.JSON file. It is a text file with a specific structure, as shown below:

```
{
  "data" : [
    {
      "context" : "",
      "dns" : "8.8.8.8"
    }
  ],
  "id" : "1020101"
  "ip" : "172.168.43.47"
  "password" : "Hytera2021"
  "port" : "5067"
}
```

Each of the fields in the file have a specific value. The most important fields are:

- "id" – that is the radio identity configured for this radio in the UNMS
- "ip" – this is the IP Address of the controller, or if the radio is connecting via a firewall, it would be public IP Address of the firewall.
- "password" – this is the password that is associated with the radio identity configured in the UNMS
- "port" – this is the virtual port that the radio will use to send a connection request to the controller.

Hytera has a basic Excel VBA script file that can be used to generate the configuration files for each of the devices. Please contact Hytera to get access to this script.

#### 3.2 VM780, PNC550 and PDC760

These devices will use the username and password fields offered up by the application when you first run the application on the device. Be sure to enter the IP address of the server and the correct port number, before entering the username/password credentials.

## 4. How to change the IP address of your Controller

### 4.1 Getting started

This manual is based on changing the factory default IP of “172.168.43.47” to any address, this example uses “50.0.0.55”. The WebLMT management screen will be used to adjust the IP Address of the controller and uses port 15900.

Logging into WebLMT address “http://IP Address of your controller:15900”. The default controller will be set to: <http://172.168.43.47:15900>



Figure 13. WebLMT 2.0

In the username field (the topmost field), type “root” followed by “root” in the password field, followed by clicking on the blue button. Don’t worry if the characters are in Chinese, we’ll change that next.

We only need to update 1 of the fields in this configuration window. If your window is full of Chinese characters, then follow the next steps to change this configuration window to English. This language setting does not affect any of the other management screens. Select the “root” menu on the top right of the screen, then click on the first menu item, as seen in Figure 14. WebLMT Landing Page.

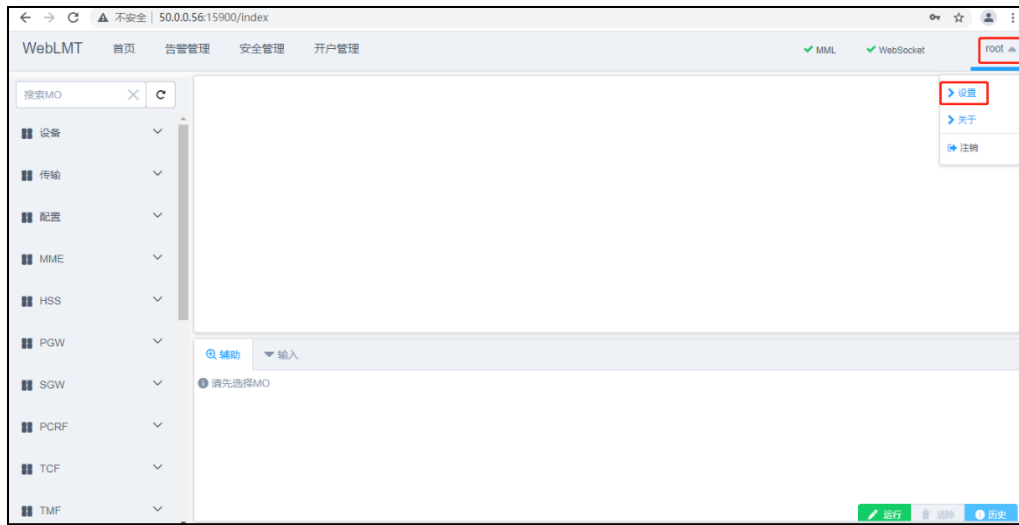


Figure 14. WebLMT Landing Page

Select “英文” under the “语言” menu. Click the blue button to accept the language change.

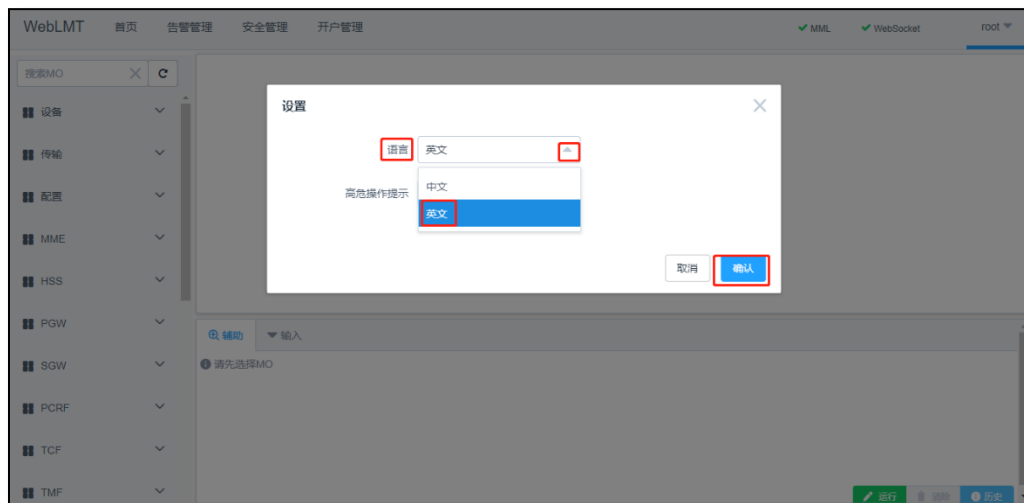


Figure 15. Changing the language to English

We are now ready to change the controller's IP address.

## 4.2 Changing the HALO OnSite Controller IP Address

Click on “equipment”, then select “System IP configuration”:

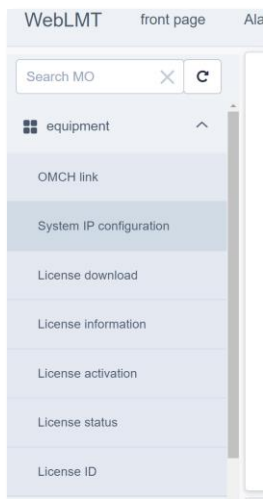


Figure 16. WebLMT System IP Configuration Menu selection

You will now be greeted with this window (notice the IP information is incomplete):

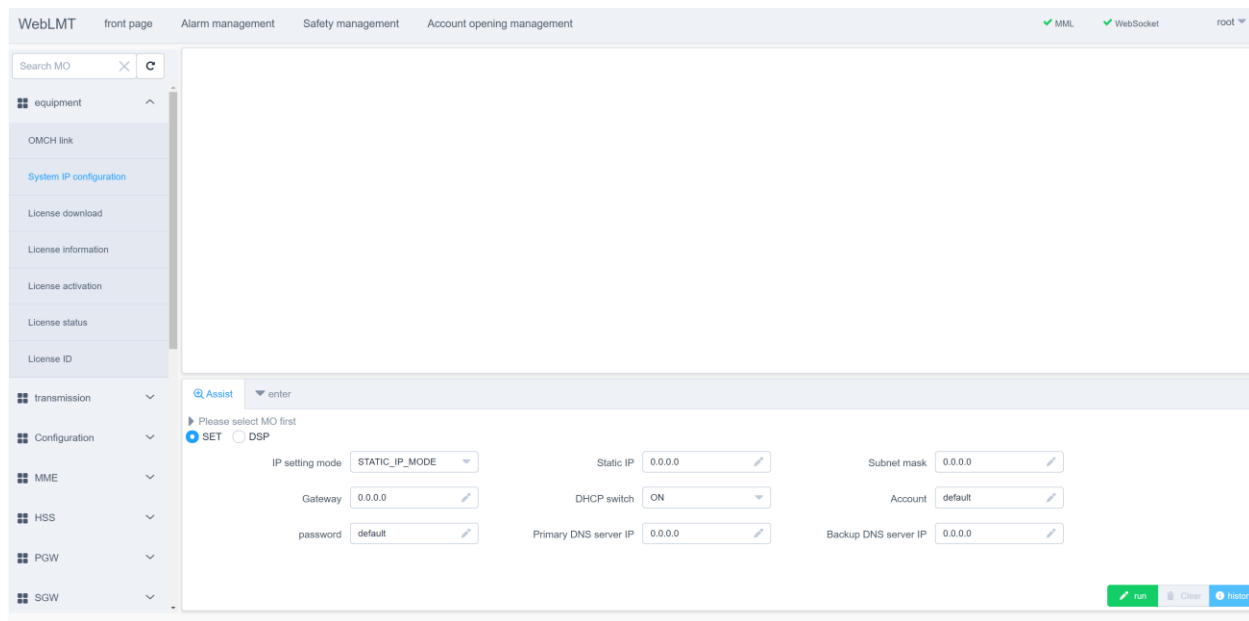


Figure 17. WebLMT SystemIPConfig landing page

To retrieve the current information, you need to select “DSP” and click “run”. It will show the results in the top part of the screen, highlighted in green.

Let’s now change the IP address of the controller, by clicking “SET”, followed by entering the “Static IP”, the “Static Netmask” and the “Static Gateway”, followed by “Execute” to implement the changes. The changes will take a few minutes to complete, just be patient. The “Execute” button will be grayed out while the IP Address is being applied to the system.



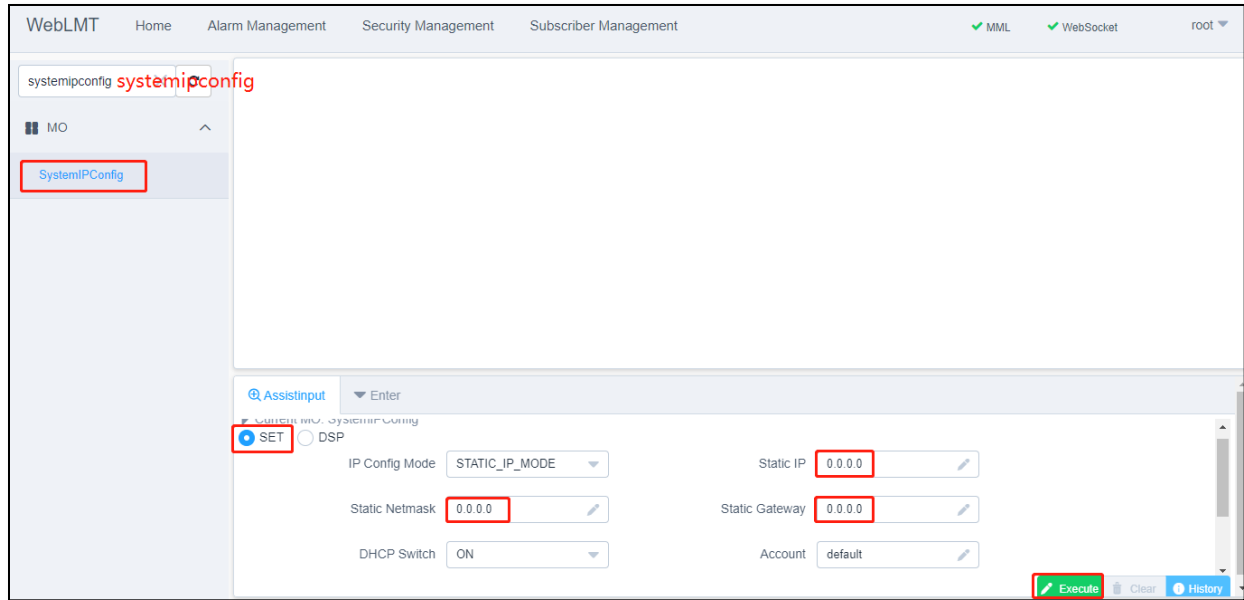


Figure 18. WebLMT SystemIPConfig

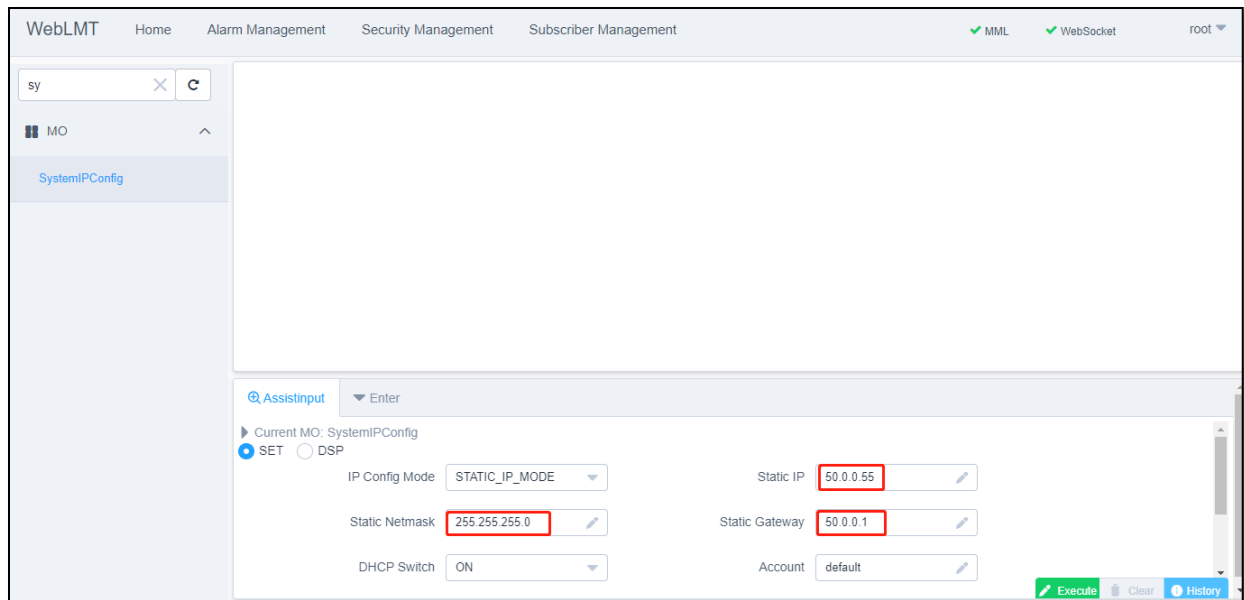


Figure 19. WebLMT SytemIPConfig updated IP settings

After changing the IP address, please restart the server and wait for 5 min for all the services to restart and attach to the new address. You need to use a terminal window to restart the server, something like MobaXterm or Putty works great. The IP address change instruction does not automatically reboot the controller.

Open Putty and select “SSH” as your session type.

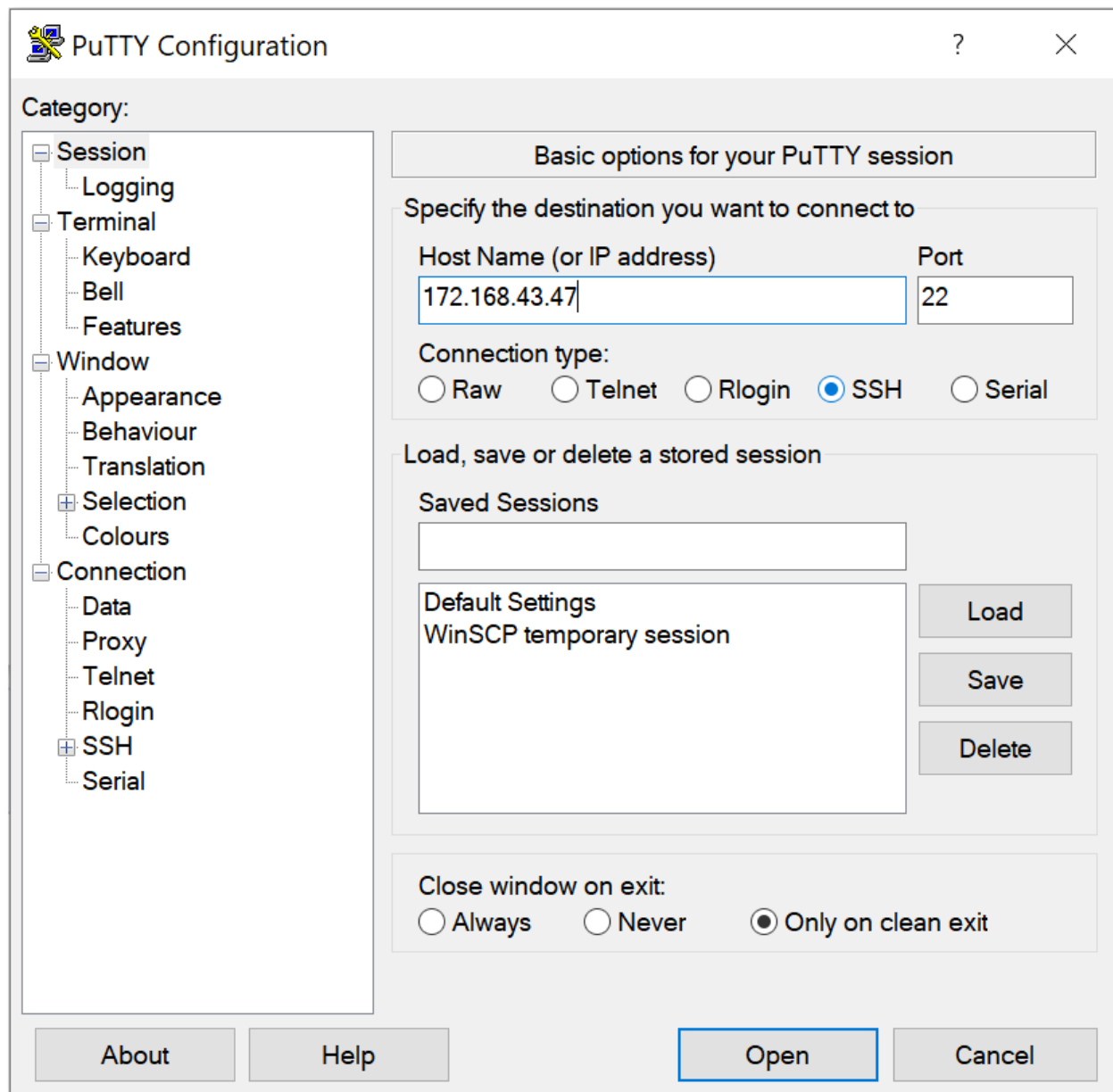


Figure 20. Putty terminal setup screen

Click “Open” after entering the data for your Controller. If you’ve just changed the IP address, in most cases you will still be able to use the old IP address, until the server has restarted. If the old address does not connect, please use the new IP address in this step. The IP address in the sample image is the default IP address for the controller.

Connecting remotely to the Controller is only allowed using the Guest account, so use the following credentials to sign on for the SSH session:

**User:** “guest”    **Password:** “WASD@1234”

Usernames and passwords are case sensitive. Once logged in, you will see this:

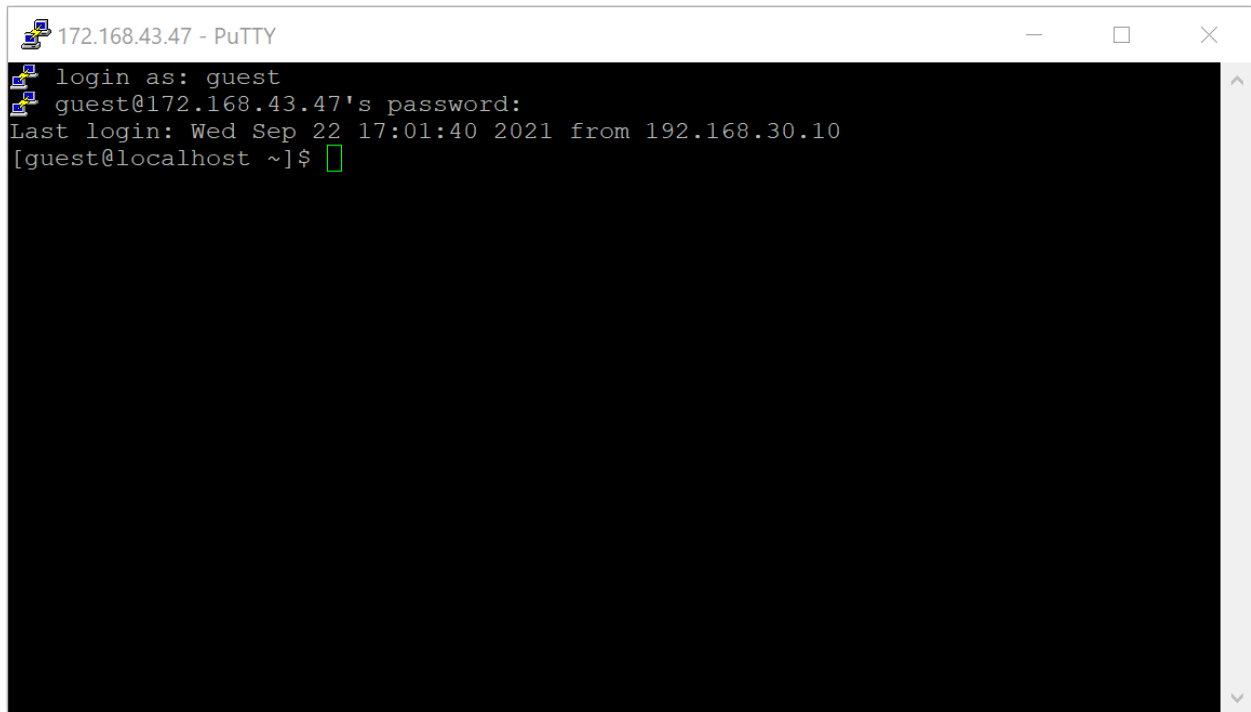


Figure 21. Terminal Login screen in Putty

You are now ready to reboot the Controller. At the green square above, type in the following command, followed by the enter key:

*"shutdown -r now"*

That will instruct the controller to reboot immediately. In the event you need to perform a clean shutdown of the controller, you can also use a variation of this command:

*"shutdown -h now"*

You will most likely be asked for a username password to execute that command:

User: "root"      password: "Bingo@1993"

## 4.3 Changing OMCH IP – this is the management platform IP

The final step in changing the IP Address is to adjust the OMCH IP to allow the network management services to connect to the new controller information.

Using the new IP address in your browser, type in “http://50.0.0.55:15900” followed by <enter>. The WebLMT should load just like before. After logging in using the “root/root” credentials, lets proceed to change the IP of the OMCH.

Click on “equipment”, then select “OMCHLINK”, then select the “MOD” option at the bottom of the screen. There will be a pop-up window that indicates the primary key ID to be “1”. Just click “OK”. Now proceed to enter the new IP information in the fields as indicated: “OMCH IP Address”, “Destination IP Address” to the new IP address, together with “Mask”, “Subnet Mask” and press “Execute”.

The screenshot displays the WebLMT interface for configuring OMCHLink IP settings. The browser's address bar is set to `http://50.0.0.55:15900`. In the left-hand navigation menu, the 'OMCH' section is expanded, and 'OMCHLink' is selected. The main content area shows the 'MOD' (Modify) configuration page for OMCHLink. The 'Current MO: OMCHLink' section has 'MOD' selected over 'GRY'. The configuration fields are as follows:

- ID:** 1
- DHCP Switch:** 1
- Ethernet Port:** (empty)
- OMCH IP Address:** 50.0.0.55
- Mask:** 255.255.255.0
- Destination IP Address:** 50.0.0.55
- Subnet Mask:** 255.255.255.0
- Route Type:** NET
- Next Hop IP Address:** 0.0.0.0
- Priority:** 10
- Description:** description

An 'Execute' button is located at the bottom right of the configuration area.

Figure 22. OMCHLink IP Settings

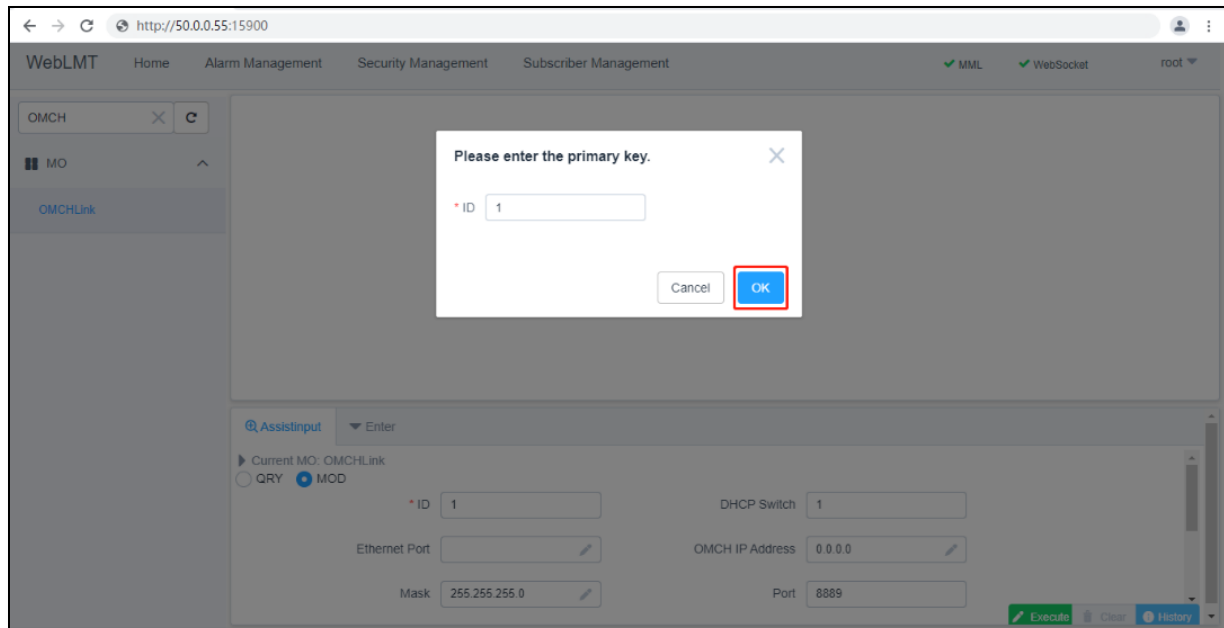


Figure 23. OMCHLink ID

We are almost done. Next we have to login to the UNMS and change the monitoring software to look at the correct address as well.

## 4.4 Log into the network management (UNMS)

Open the network management page. E.x. <https://50.0.0.55> and start using the system. This is the UNMS, not the WebLMT, so no need to include the 15900 port number with the address.

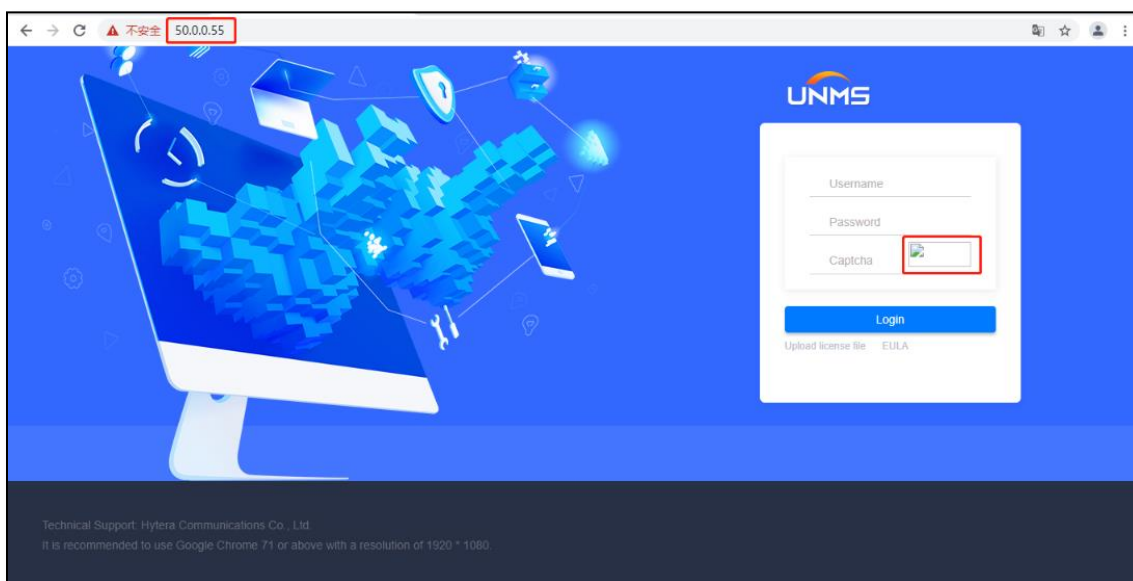


Figure 24. UNMS Not completely loaded - no Captcha visible

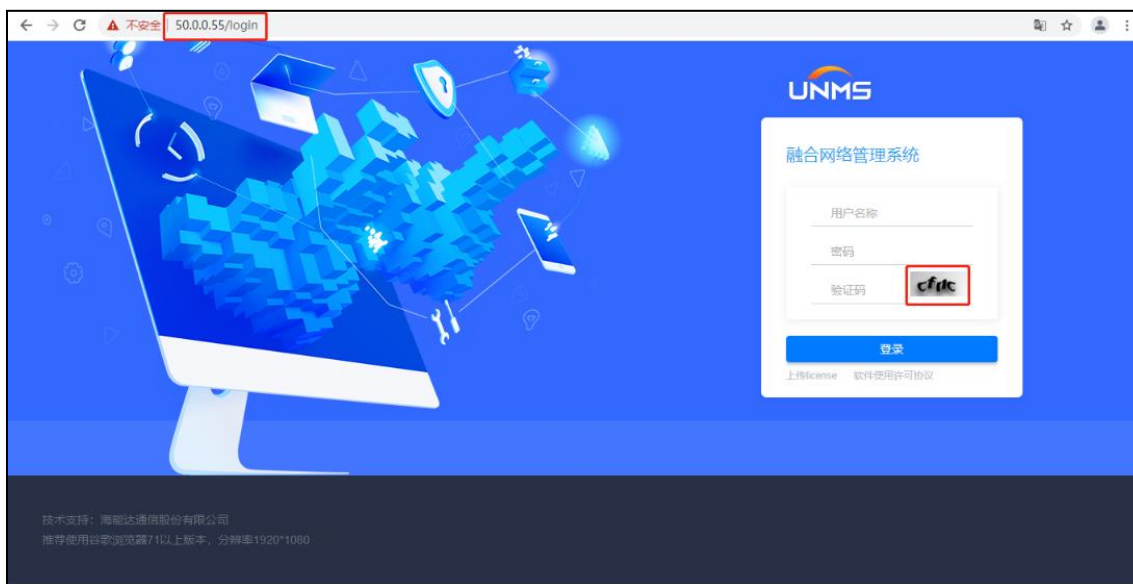


Figure 25. UNMS ready for login - Captcha loaded

## 4.5 Updating the Monitoring System IP Addresses in the UNMS

### 4.5.1 Step 1: Modifying the equipment Communications IP

After successfully logging into the UNMS, select Topology/Resource Management/Equipment Management to continue the IP address adjustments for the UNMS components.

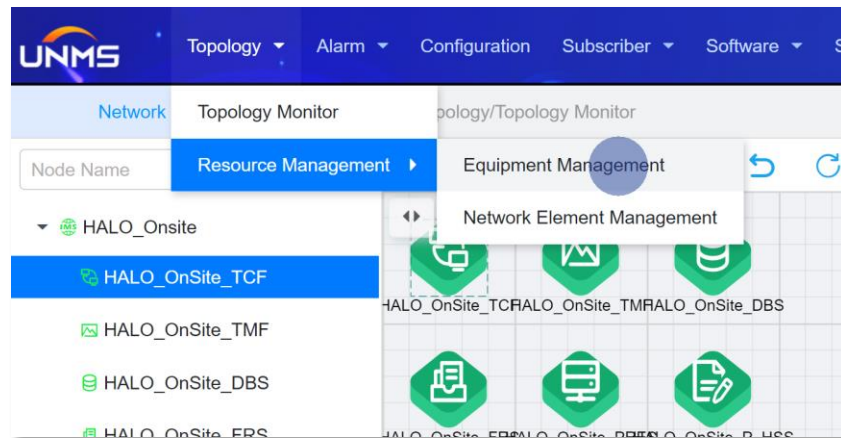


Figure 26. Equipment Management Menu Selection

You will be seeing a single item on the list that is the controller's name. Select it, followed by clicking on the Edit (pencil) button on the left of the screen. The "Modify Equipment" menu will appear as seen in Figure 27. Modify Equipment Menu. This image still shows the default IP address of the controller.

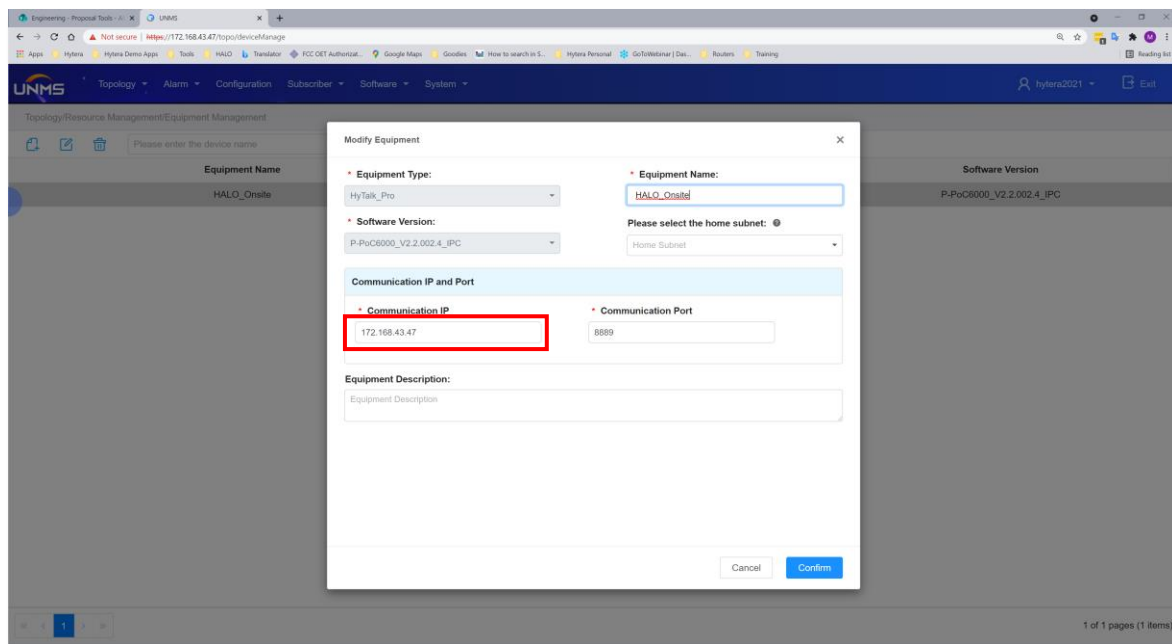


Figure 27. Modify Equipment Menu

Make sure the "Communication IP" is the same as the newly assigned IP Address of the controller.

## 4.5.2 Step 2: Navigate to the Network Element Management Section

Select “Topology/Resource Management/Network Element Management” as shown in Figure 28. Network Element Management Menu.

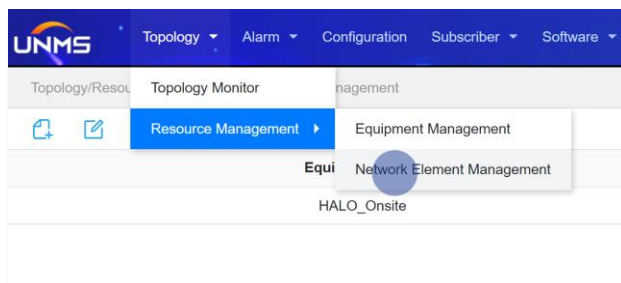


Figure 28. Network Element Management Menu

In Figure 29. Network Element List you can see a complete list of all the primary network elements installed on the Controller.

UNMS Topology Alarm Configuration Subscriber Software System						
Topology/Resource Management/Network Element Management						
Please enter the no name						
Network Element Name	Network Element Type	Home Equipment	Communication IP	Communication Port	Physical IP	Physical Port
HALO_OnSite_TCF	TCF	HALO_Onsite	172.168.43.47	8889	127.0.0.1	11001
HALO_OnSite_TMF	TMF	HALO_Onsite	172.168.43.47	8889	127.0.0.1	11002
HALO_OnSite_DBS	DBS	HALO_Onsite	172.168.43.47	8889	127.0.0.1	11004
HALO_OnSite_FRS	FRS	HALO_Onsite	172.168.43.47	8889	127.0.0.1	11006
HALO_OnSite_PRES	PRES	HALO_Onsite	172.168.43.47	8889	127.0.0.1	11005
HALO_OnSite_P_HSS	P_HSS	HALO_Onsite	172.168.43.47	8889	127.0.0.1	11007

Figure 29. Network Element List

We will now be modifying each of these services to match the updated IP address. If you do not update these addresses, various things will not be accessible, from alarms to not being able to add or remove radios or groups from the system.



### 4.5.3 Step 3: TCF Service

Ensure that the settings for “Physical IP” is “127.0.0.1” and that “Communication IP and Port” match your new IP address settings. Do not modify any of the other settings.

Modify Ne

×

\* Home Equipment:

HALO\_Onsite

\* Network Element Type:

TCF

Network Element Name:

HALO\_OnSite\_TCF

\* Communication IP and Port:

172.168.43.47:8889

\* Physical IP:

127.0.0.1

\* Physical Port:

11001

Network Element Description:

Network Element Description

Cancel

Confirm

Figure 30. TCF Service Settings in the UNMS

## 4.5.4 Step 4: TMF Service

Ensure that the settings for “Physical IP” is “127.0.0.1” and that “Communication IP and Port” match your new IP address settings. Do not modify any of the other settings.

Modify Ne

×

\* Home Equipment:

HALO\_Onsite

\* Network Element Type:

TMF

Network Element Name:

HALO\_OnSite\_TMF

\* Communication IP and Port:

172.168.43.47:8889

\* Physical IP:

127.0.0.1

\* Physical Port:

11002

Network Element Description:

Network Element Description

Cancel

Confirm

Figure 31. TMF Service Settings in the UNMS

#### 4.5.5 Step 5: DBS Service

Ensure that the settings for “Physical IP” is “127.0.0.1” and that “Communication IP and Port” match your new IP address settings. Do not modify any of the other settings.

Modify Ne

×

\* Home Equipment:

HALO\_Onsite

\* Network Element Type:

DBS

Network Element Name:

HALO\_OnSite\_DBS

\* Communication IP and Port:

172.168.43.47:8889

\* Physical IP:

127.0.0.1

\* Physical Port:

11004

Network Element Description:

Network Element Description

Cancel

Confirm

Figure 32. DBS Service Settings in the UNMS

## 4.5.6 Step 6: FRS Service

Ensure that the settings for “Physical IP” is “127.0.0.1” and that “Communication IP and Port” match your new IP address settings. Do not modify any of the other settings.

Modify Ne

×

\* Home Equipment:

HALO\_Onsite

\* Network Element Type:

FRS

Network Element Name:

HALO\_OnSite\_FRS

\* Communication IP and Port:

172.168.43.47:8889

\* Physical IP:

127.0.0.1

\* Physical Port:

11006

Network Element Description:

Network Element Description

Cancel

Confirm

Figure 33. FRS Service Settings in the UNMS

#### 4.5.7 Step 7: PRES Service

Ensure that the settings for “Physical IP” is “127.0.0.1” and that “Communication IP and Port” match your new IP address settings. Do not modify any of the other settings.

Modify Ne

×

\* Home Equipment:

HALO\_Onsite

\* Network Element Type:

PRES

Network Element Name:

HALO\_OnSite PRES

\* Communication IP and Port:

172.168.43.47:8889

\* Physical IP:

127.0.0.1

\* Physical Port:

11005

Network Element Description:

Network Element Description

Cancel

Confirm

Figure 34. PRES Service Settings in the UNMS

## 4.5.8 Step 8: PHSS Service

Ensure that the settings for “Physical IP” is “127.0.0.1” and that “Communication IP and Port” match your new IP address settings. Do not modify any of the other settings.

Modify Ne

×

\* Home Equipment:

HALO\_Onsite

\* Network Element Type:

P\_HSS

Network Element Name:

HALO\_OnSite\_P\_HSS

\* Communication IP and Port:

172.168.43.47:8889

\* Physical IP:

127.0.0.1

\* Physical Port:

11007

Network Element Description:

Network Element Description

Cancel

Confirm

Figure 35. PHSS Service Settings in the UNMS

## 5. Configuring your firewall for remote device access

The POC radios need 1 specific IP address to connect to the controller. If the devices are only being used on the private network, with no access from the public internet via either LTE or WiFi, then the IP is simply the IP address of the controller. This assumes that the IP address of the Controller is directly routable from anywhere on the customer's private network.

If, however, the devices will roam between private and public connections, the best practice is to configure all the devices the same and provide them the public IP of the firewall. Again, it is an IP address that is reachable by the radio from wherever it will be, roaming the internet or the private network. It does mean that the firewall will have to be configured to allow IP traffic from the private side of the network to contact the public IP of the firewall and be routed back to a private connection. IT specialists will be able to easily configure this use case.

The firewall will need the following ports forwarded to the controller for the devices to function correctly:

5067	TCP	PNAS Login Port	Sign on and initial call setup
8050	TCP	FRS Port	
8040	TCP	PRES Port	Managing Device Groups
9010	TCP	MDS Port	
20000-30000	UDP	TMF Media Port	Call audio and PTT signaling after the call is setup

### 5.1 Configuring the Controller for remote network access

The [TmfRemoteMediaAddrMap] parameter is used to tell the remote radio what IP address to connect to after a request for call. The Controller knows what the IP address of the origination radio is, so it can therefor identify the correct [InMediaProxyIp] IP Address to provide the remote radio.

This information is stored in a table in the controller and can be modified via the Configuration pages in the UNMS. The table works on a priority scheme, where the lowest index value will be processed first. Essentially when a call setup request reaches the controller, it will take a look at the table, starting at the entry with the lowest index value, followed by the next lowest value, comparing the IP address of the originating radio to the [RemoteNetIp]/[RemoteNetMask] values to identify the appropriate [InMediaProxyIp] to provide to the radio for the call.

The most basic value would be to have all radios connect to the same IP address, using a single entry with 0.0.0.0/0.0.0.0 (all IP addresses) and providing the IP address of the server as the [InMediaProxyIp]. This works fine if the server IP is reachable from all parts of the network where the PoC radios will be roaming, however it becomes a bit trickier when radios are on different networks, where there are firewalls or NAT devices in the IP path.

#### 5.1.1 How to query the Controller for the [TmfRemoteMediaAddrMap] parameter

From the top menu, select "Configuration". Now select "HALO\_OnSite\_TMF". It is important to note that your naming convention might be slightly different, but the important thing to remember is that we are looking for the "TMF" service. Next click on the [TmfRemoteMediaAddrMap] item and you should see something like the screen below.

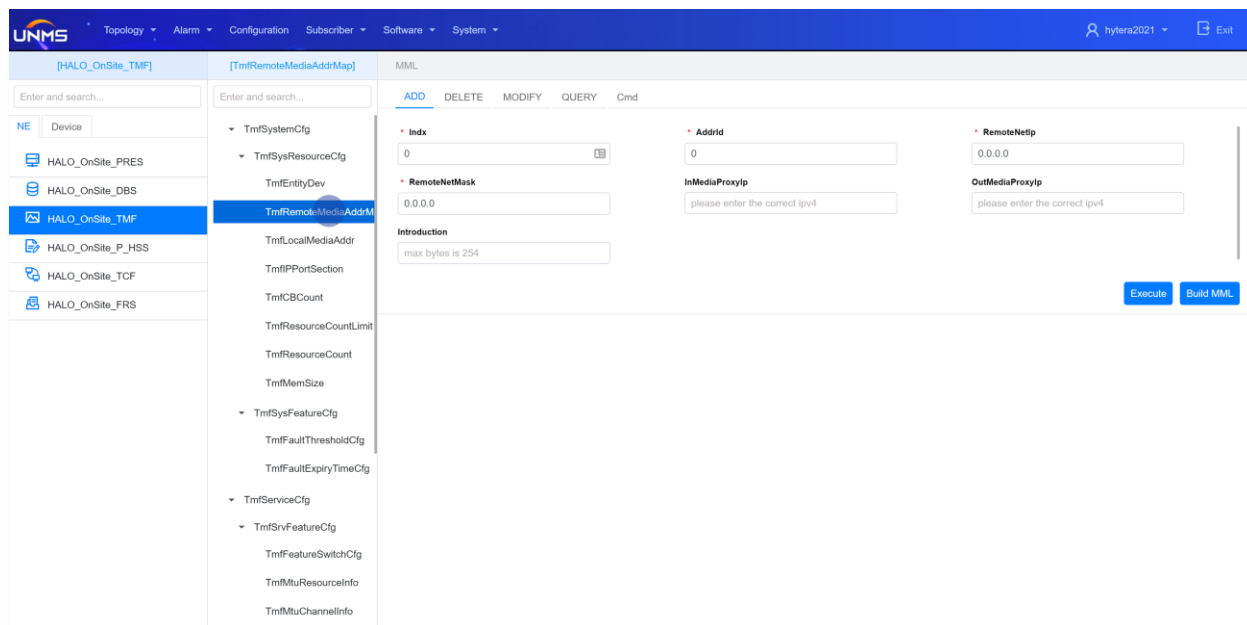


Figure 36. TmfRemoteMediaAddrMap page

This gets you to the correct menu options, so now you need to click on “Query”, leaving the “Indx” field blank, and click “Execute”.

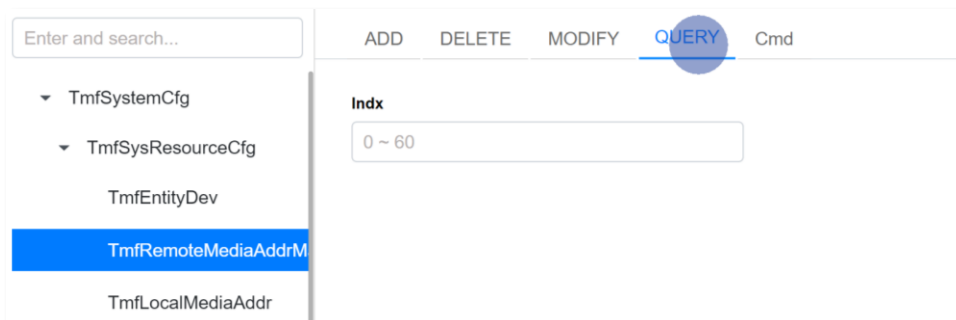


Figure 37. TmfRemoteMediaAddrMap Query menu

Depending on the controller’s current configuration, the list could look something like Figure 38. TmfRemoteMediaAddrMap Example Query result.



The screenshot shows the Hytera configuration interface. On the left is a sidebar with a search bar and a tree view of configuration categories. The 'TmfRemoteMediaAddrMap' category is selected. The main area has tabs for ADD, DELETE, MODIFY, and QUERY (which is active). Below the tabs is a table with columns: Indx, AddrId, RemoteNetIp, RemoteNetMask, InMediaProxyIp, OutMediaProxyIp, and Introduction. The table contains two rows of data. Above the table, there is a green box displaying query details: Begin Time (2021-09-24 13:42:44), End Time (2021-09-24 13:42:44), MML Command (QRY TmfRemoteMediaAddrMap : ne= 2004 ;), and MML Response (a table with 7 columns and 2 rows). Buttons for 'Execute' and 'Build MML' are visible on the right.

Indx	AddrId	RemoteNetIp	RemoteNetMask	InMediaProxyIp	OutMediaProxyIp	Introduction
0	0	192.168.30.0	255.255.255.0	172.168.43.47		Remote Network Access
2	0	0.0.0.0	0.0.0.0	192.168.40.1		

Figure 38. TmfRemoteMediaAddrMap Example Query result

## 5.2.2 How to modify/add/delete the table entries

Each of the entries in the table can be modified or deleted, and if you need more entries, simply pick the “add” menu. It is important to note that when you add a new item to use an unused “Indx” number. If you don’t have any unused spaces, and a specific row needs to be ahead of another, you might have to delete an entry and enter some new ones. Please check with Hytera Technical Support for assistance if you are unsure or your options.

## 5.2.3 Restarting the service after modifying the settings

Click on the “Configuration” menu on the top of the screen. The select “Device” from the menu on the left, as can be seen in Figure 39. Device Menu.

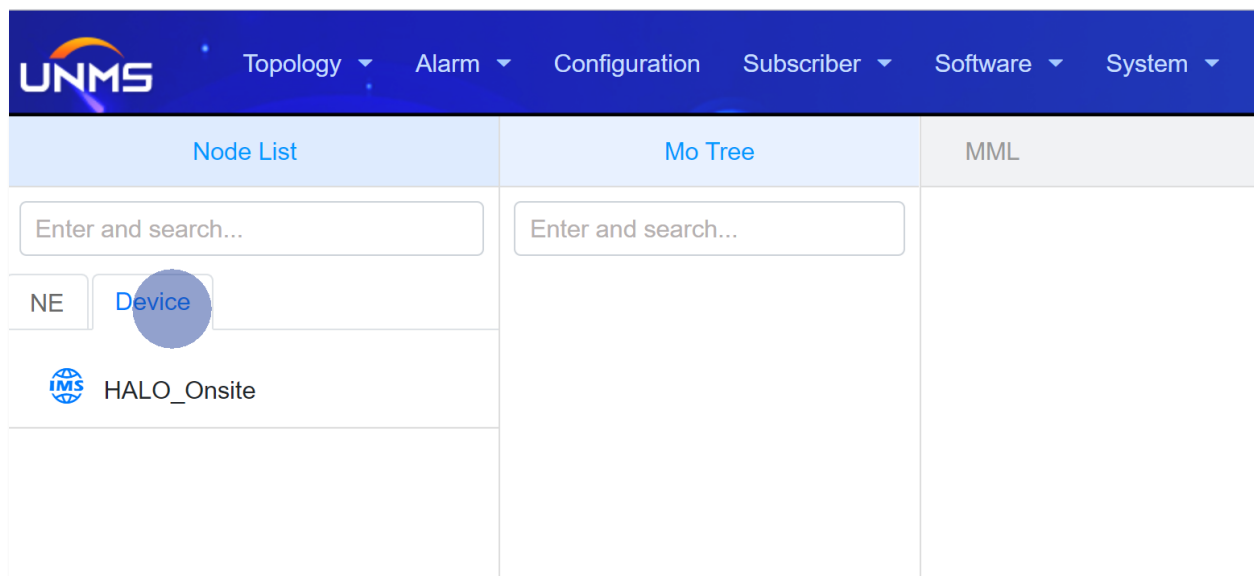


Figure 39. Device Menu

Next select “HALO\_OnSite” or whatever name your Controller is called from the left menu. Then scroll and select “ETC” from the second column, and you should see a screen as shown in Figure 40. ETC Menu.

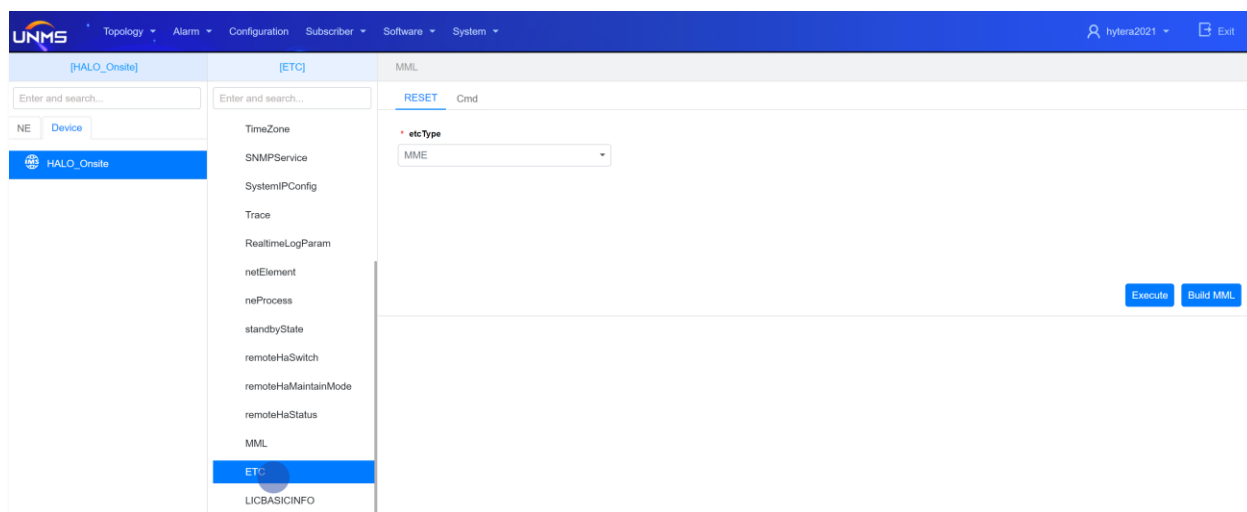


Figure 40. ETC Menu

In the right hand box, you have the option to now select the service you would like to restart. Click on the down arrow to the right of the selection box, and scroll until you see “TMF” and select it. Click on “Execute” to restart the service. See Figure 41. TMF Restart Selection. Give it a minute or so to completely restart. No need to worry about trying to make calls during this time, as it will not affect the service, but the call setup requests will fail to complete, until the service has restarted completely.

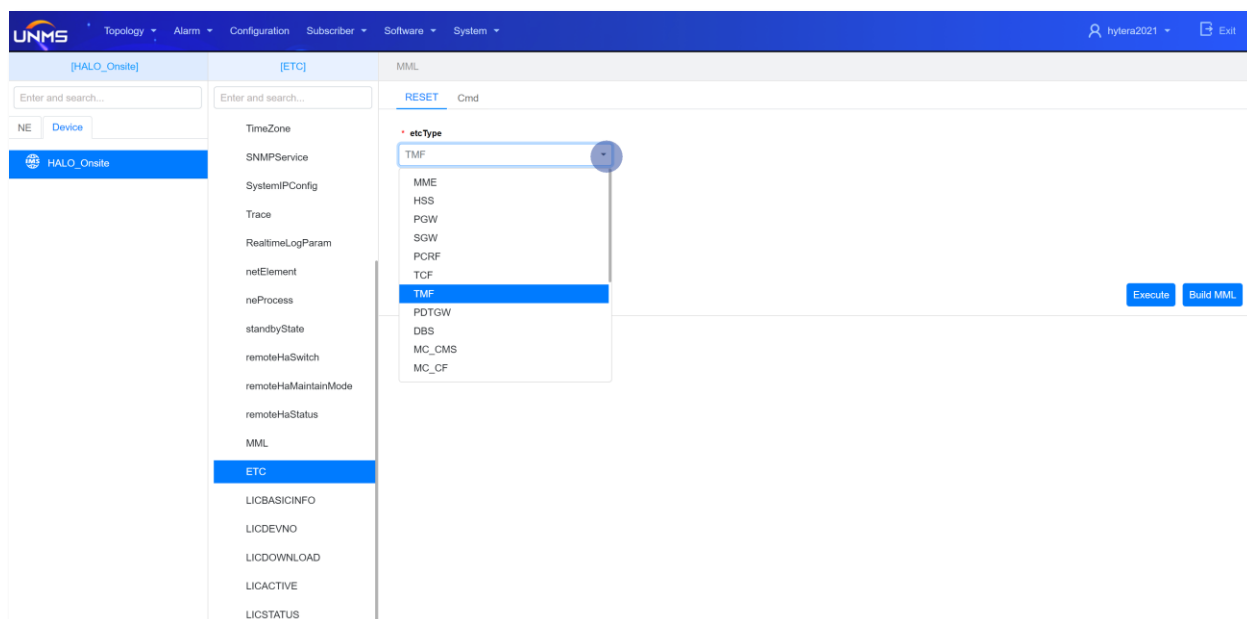


Figure 41. TMF Restart Selection