

# MOTOTRBO Radio Management Setup Guide

MOTOTRBO Radio Management Setup Guide © 2023 Wayne Holmes DJ0WH

MOTOTRBO™ is a trademark of Motorola Solutions Inc. All other names are the trademarks of their respective owners.

If you wish to translate this document into another language, it would be nice if you could share the link so I can add it here.

This document is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License. You may distribute and adapt this document on condition it is done free of charge; under a CC BY SA 4.0 licence and you attribute the author (me) as shown above. For more details about this, click [here](#).

This Google Docs document can be downloaded via the File menu (above, left). Various formats are available, but the best would be .pdf or .docx or .odt. As the document is regularly updated, you might need to download a new version as time goes by.

This document was last revised on 05.11.2023

## Why Radio Management

Before there was MOTOTRBO Radio Management, there was CPS (and before that RSS) - and codeplugs. In those days, to make a configuration change on 50 radios at a customer facility, you would have to travel to site; gather the radios; read; edit then write each one.

Travelling to and from the site is non-productive time, so too is sitting and waiting for users to bring you their radio or hunting down radios to be programmed. From my own experience, reprogramming 50 radios on site was a whole day's exercise! At best!

MOTOTRBO Radio Management will spare you all this hassle:

- Radios with the same model and profile can share a single configuration. Adding or editing anything only needs to be done once and that change is replicated on those radios.
- Changes made in Radio Management can be pushed out to radios over the air, using the RF channel or Wi-Fi\* with no need to watch over anything.
- Repeaters can be remotely reconfigured using an IP connection. No more travelling up to site.
- Carrying out firmware updates and adding new feature licences is now much easier.
- The configuration of low tier radios, which do not support over the air reconfiguration, can also be managed in Radio Management and any changes can be sent to them via a remote computer

and programming cable. Plugging and unplugging a cable can be done by a junior member of staff or the customer themselves.

- Isolated radios which are out of RF coverage with no internet connectivity can be configured using a programming cable and an offline version of the configuration change. This task can also be carried out by a junior member of staff or the customer themselves.

Your customers will also be amazed that they don't need to bring their radios in or have any interruption in their work as everything can be done remotely and on a schedule that suites them.

## **Introduction**

This document makes certain assumptions about the overall configuration. Your setup will probably be different so you will need to adapt some things to suit your customers requirements. I cannot cover every possible configuration here.

This material is not a replacement for knowledge and experience. If you are stuck, you need to contact someone to help - see below. I suggest reading everything if you are doing this for the first time.

Although I have done my best to make this as accurate as possible, there may be some mistakes. You are ultimately responsible for the overall system design and fixing any problems.

I am assuming that you know some stuff about computer networking as well as some stuff about MOTOTRBO. This means that I cannot go into detail about networking stuff nor can I explain how MOTOTRBO works.

This document will not show you how to configure the radio system - it is only there to help you manage your configuration using a very excellent tool called MOTOTRBO Radio Management.

## **If you need help**

Depending on where you work; if you need help with anything technical, here is who you need to contact:

1. If you work for an organisation that uses Motorola equipment, contact the company who supplied you this. In most cases, this will be a Motorola Solutions Reseller Partner. Check here to find a Reseller near you.

2. If you work for a government agency or organisation, who has a purchasing agreement with Motorola Solutions, you should contact your Account/Support Manager. Otherwise, contact the Motorola Solutions Customer Helpdesk in your region.
3. If you work for a Motorola Solutions Platinum or Distribution Partner, contact your Channel Account Manager; Customer Support Manager or the Motorola Solutions Customer Helpdesk in your region.
4. If you work for a Motorola Solutions Reseller (Gold; Silver or Registered), please contact the Distributor you work with; your Channel Account Manager or the Motorola Solutions Customer Helpdesk in your region.

## **Stuff to remember**

Do not use OTAP to read new (unknown to RM) radios. That's just crazy! Except if it's done on Wi-Fi.

This document only refers to conventional; IP Site Connect and Capacity Plus (single and multisite) systems. There is a section at the end that deals solely with Capacity Max.

New radios/repeaters of a certain model must be read to at least get the MVO data - otherwise the configuration cannot be written back.

For a CMSS use the HP serial number and not the Motorola 435\_\_\_\_\_ serial number. You can use the latter as an alias or put it in the comments but the HPE serial number is what's sent to the Device Programmer.

I suggest having a copy of the following manuals at hand in case you need them:

- Radio Management Setup Guide.
- Radio Management User Guide.
- MOTOTRBO System Planner (not for Capacity Max).
- Capacity Max System Planner (only for Capacity Max).
- Capacity Max Installation & Configuration Guide (only for Capacity Max).

## **A quick primer**

MOTOTRBO Radio Management allows you to manage the configuration of many radios from a central location. Rather than having multiple codeplugs with multiple versions, there is a configuration that is shared between multiple radios.

Having a single configuration for multiple radios reduces the risk of configuration mistakes and speeds up changes. Rather than changing one thing in thousands of codeplugs, you only need to make that change once and send the update to all affected radios.

OTAP (Over The Air Programming) goes hand-in-hand with Radio Management. Instead of connecting a radio to the PC, you can send configuration updates over the radio system; IP network or Wi-Fi.

The above is summed up quite well in [this video](#).

In its basic form, MOTOTRBO Radio Management consists of the following applications/services:

- Configuration Client.
- Device Programmer.
- Job Processor.
- Server.

These can be installed on the same computer or on multiple computers. There is normally only one instance of the Server. All of the above applications will connect to the server.

There can be multiple instances of the other applications but these need to be hosted on different computers (or virtual machines) and will need an IP connection to the Server or Job processor host.

## Operating System and Hardware Requirements

MOTOTRBO Radio Management runs in Windows 10 or Windows Server 2016 or later.

It is a good idea to install MOTOTRBO Radio Management on a separate computer or virtual machine with no other applications.

Fleet Site	Hardware
Small (<1000 radios)	Intel Xeon E5-2600 quad core 8 threads 16GB DDR4 RAM 1TB SSD or NVMe 1Gbps ethernet
Medium (1000;10000 radios)	Intel Xeon quad-core (8 threads) 16GB DDR4 RAM 1TB NVMe 2TB SSD 1Gbps ethernet

Large (10000, 50000 radios)	AMD EPYC 9124 16 core, 3.0 GHz, 64 MB L3 16GB DDR4 RAM 1TB NVMe 8TB RAID SSD 1Gbps ethernet
Huge (>50000 radios)	Dual Intel Xeon Gold 5218 SRF8T 16 core 256GB Registered ECC DDR4 SDRAM 1TB NVMe 32TB SSD RAID 1Gbps ethernet

## Installation

Make sure Windows has been updated and that you have admin rights on the local machine. Download Radio Management from MyView. Once downloaded, unzip and run setup.exe as Administrator (right-button click).

Select the program features to install.

☐ Radio Management Client (Version 2.138.176)

☒ Radio Management Server (Version 2.138.176)

☐ AutoUpdate Enable

☐ Radio Management Device Programmer (Version 2.138.176)

☐ Radio Management Job Processor (Version 2.138.176)

[Documentation](#) [Additional Applications](#)

Feature Description

This feature installs the Radio Management Client, which is used as a client of Radio Management and works in configuration mode.

NOTE: Please make sure no RMC instance is open before proceeding with the install.

InstallShield Next > Cancel

Radio Management Client is only needed if you will be managing radio configurations from this PC. My recommendation is to also install this on the server in case you need to check something while in the server room.

Radio Management Server only needs to be installed on the server. There can only be one instance of Radio Management Server per customer or system.

AutoUpdate Enable allows older Radio Management Client installations to be updated when connecting to the server.

Radio Management Device Programmer is only needed on computers which will attach to radios, either via Wi-Fi; via a Control Station or MNIS. Radio Management Device Programmer is also only needed on computers which will be used to program repeaters via IP.

Another possibility is to use Radio Management Device Programmer in offline mode where the write jobs are stored on a USB stick or portable drive and taken with a laptop and programming cable to locations where there is no radio coverage (for OTAP) or network (for IP/Wi-Fi). In this case, the radio get written via a cable but without a network connection to the server and without needing CPS or any access to the configurations.

Radio Management Job processor usually goes on the same machine as Radio Management Server. However, it is possible to have multiple Job Processors on different servers to handle large volume jobs on large systems.

## Auto Add Radio feature settings.

- ☐ Automatically read new radios and create a configuration
- ☒ Do not automatically add new radio to the RM database

### [Documentation](#)

### [Additional Applications](#)

#### Feature Description

This selection will prevent RM from automatically adding new radios detected thru USB and WiFi to the RM database. To add new radios into RM database, you need to enter the radios' serial number manually.

The default settings and advanced options can be changed in RM Server Utility.

InstallShield®

< Back

Next >

Cancel

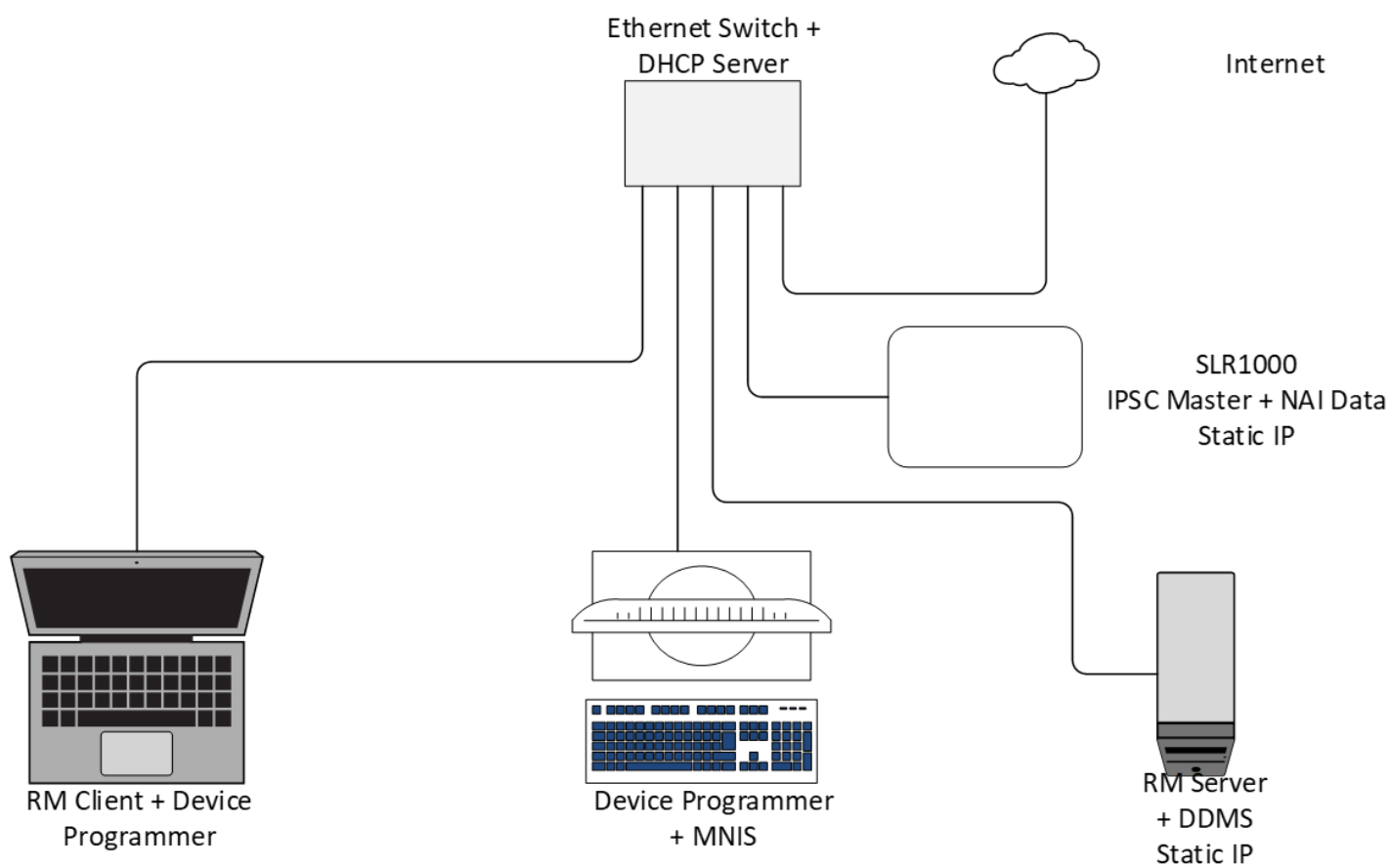
I strongly recommend selecting *Do not automatically add new radios to the RM database*. You can turn this on later if you need it.

One reboot is needed. Everything else is just accepted and okay - the usual installation wizard stuff.

If you see the powershell script running then there should be no installation errors. If the installation bombs out, more than likely you do not have admin rights or you did not update (and reboot) Windows.

## My setup





My setup (shown above) consists of:

- My work laptop with Radio Management Configuration Client on it.
- A desktop PC with Device Programmer; DDMS and MNIS on it.
- A tower PC with Radio Management Server and Job Processor installed on it.
- A SLR1000 with a dummy load on the and a piggy-tail on RX. The repeater is set up as an IPSC Master; has a static IP address as well as the NAI Data feature enabled.
- All of these devices are connected to a [Mikrotik hEX Lite](#), which works as an ethernet switch; DHCP server and allows me to connect to the internet via my home network.

You would only need an internet connection if you wanted to activate a feature licence in a radio or repeater or download something ([like this document](#)).

## Install MNIS if needed

When and where do you install MNIS? If you will use OTAP no matter what system topology. You would install MNIS on the PC which has an IP connection to the repeaters (and CMSS if present/used).

Installation is nothing special, just Accept and Next. It might make sense to also run this installer as an Administrator. Setup will also Install Visual C++.

The MNIS installer does require a reboot.

MNIS normally runs as a service

## Install DDMS if needed

When and where do you install DDMS? You would need at least one instance of DDMS if the radio system is not Capacity Max and you will either use RM to program radios via OTAP or a Control Station or MNIS. It would go on the machine that connects to the radio network via IP or on the machine that the Control Station is connected to.

To install is nothing special, just Accept and Next. It might make sense to run this installer as an Administrator.

## Install the MOTOTRBO Driver if needed

When and where do you install this driver? If the system is not Capacity Max and you will be doing OTAP via a Control Station. In this case, the driver gets installed on the PC attached to the Control Station.

The driver installer is located in folder X:\Y\{E1E1C138-4E4A-4468-95C9-D118A6EA8A27}. Where X and Y are the drive and folder where the Radio Management installation files are located. It is installed together with Device Programmer and to install it separately, you can copy the above file onto a USB stick or network share to deploy on other machines.

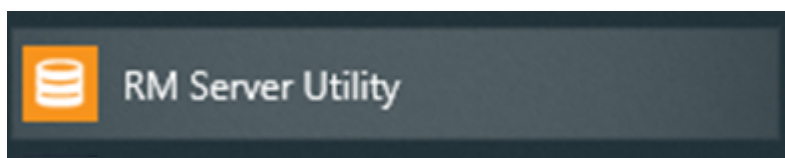
## Summary of when to use DDMS, MNIS and the MOTOTRBO driver

Optional application	Install if	DO NOT install if
DDMS	The radio system is not Capacity Max. You will use RM to program radios via OTAP. You will use a Control Station or MNIS.	The radio system is Capacity Max. You will only use RM to program repeaters. Radios will be programmed using Wi-Fi only.

MNIS	You will use RM to program radios via OTAP and a Control Station is not used. The radios are on a Capacity Max system.	You will use RM to program radios via <u>Wi-Fi only</u> . You will use RM to program radios via OTAP and a Control Station is used.
MOTOTRBO Driver	You will use a Control Station.	You will use MNIS.

Note that on non-Capacity Max systems, MNIS requires the NAI Data feature licence on repeaters that will be handling OTAP. The NAI Data feature licence is not needed to remotely program radios via a Control Station or to remotely program repeaters.

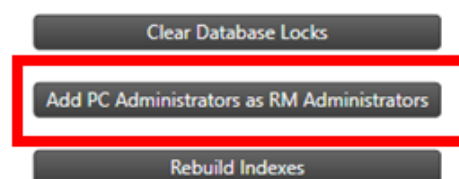
## Post installation tasks



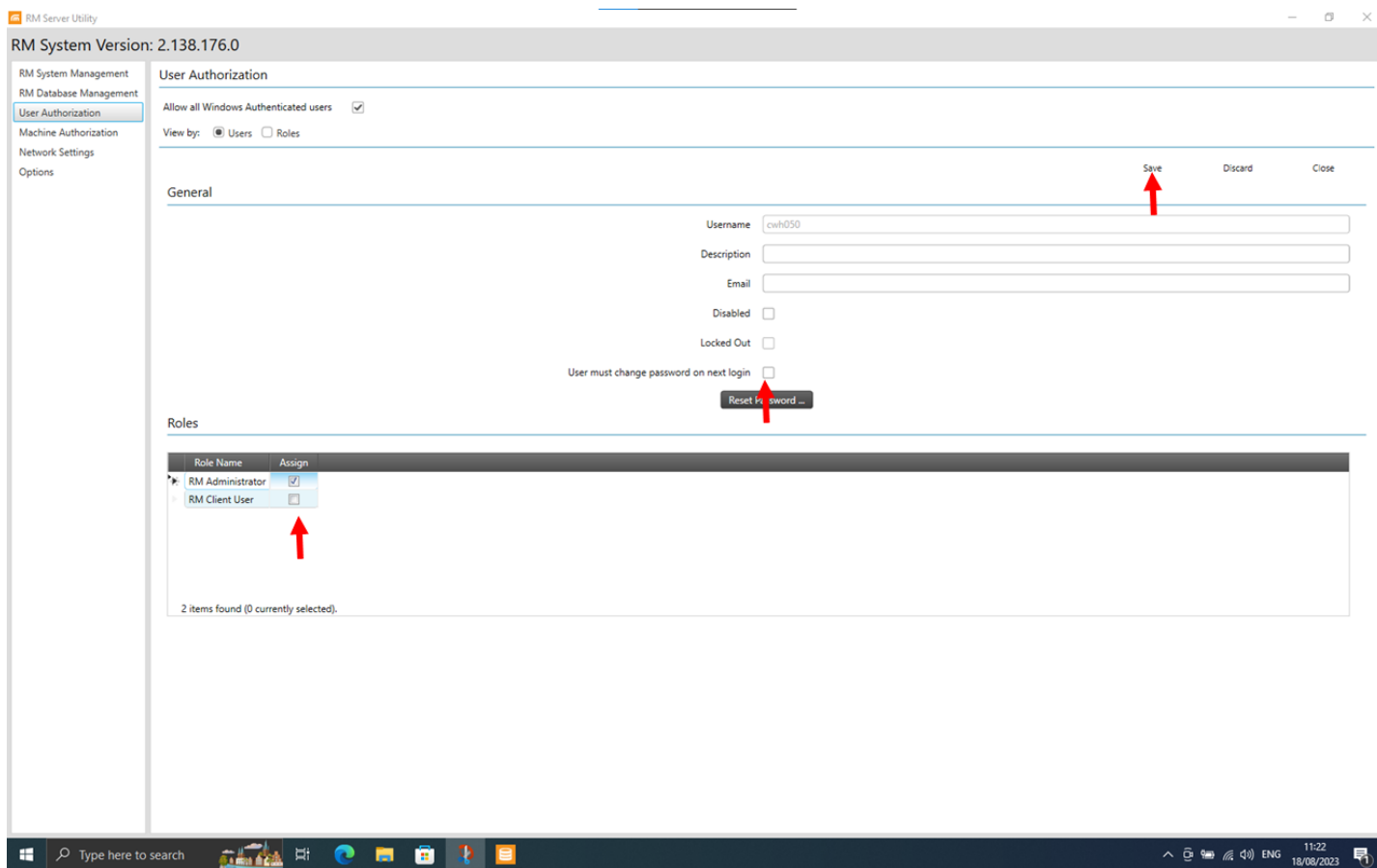
Start the RM Server Utility and go to RM Database Management. Under Database Backup click Browse and choose a location for the backup. Click Backup and wait for the backup to complete (a few seconds).

A backup of the blank (empty) database will be useful if you ever screw something up and need to start from scratch.

### Advanced Operations



You will see that User Authorisation and Machine Authorisation are both greyed out. To correct this, under Advanced Operations, click on *Add PC Administrators and RM Administrators* (button, middle, bottom). When prompted, click Yes. User Authorisation and Machine Authorisation will now be un-greyed. You need to do this in order to add RM Client user accounts.

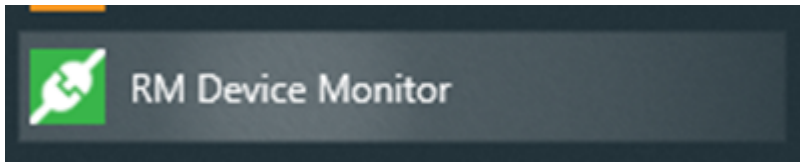


Still in the RM Server Utility, click on User Authorisation (left panel):

1. Click on the ⊕ (circle-plus) button and choose *Add Non Domain User*. (If you are using a Domain Controller you can choose *Add Domain User* and select an account from your Active Directory. In this case, the password step can be skipped since this will be managed by the domain etc.).
2. Enter a username and first-use password as well as any other (optional) relevant details.
3. Click OK.
4. Select the newly added user from the list and click the ✎ (edit-pen) button.
5. Under General, make sure that *User must change password on next login*.
6. Under Roles, make sure either *RM Administrator* or *RM Client User* are selected.
7. Click Save.
8. Repeat the above steps for any additional user you want to add.

Lastly, go to RM System Management and make sure that Discovers Server; Job Server and RM Server are all Available and Running. Close the RM Server Utility.

## Setting up Device programmer



On the PCs where you have installed Device Programmer, open RM Device Monitor and click on the Settings button and check/change the following:

## Motorola Device Programmer Settings

### RM Server

Address

Port

Authentication Method

Test Connection

### Device Communication Method

Communication Method ☒ USB ☒ Wireless (LAN) ☒ Over The Air  
☒ IP Program

### Device Discovery and Authentication

DNS-SD Listening Port

Device Discovery Server Name *cwh050-zb15g4*

Device Discovery Server IP *192.168.0.250*

### Radio Group

Assigned Radio Group  Updating Success

### IP Program Settings

#### Common

Minimum TCP Port

Maximum TCP Port

Local UDP Port

1. Under RM Server, enter the IP address of the RM Server. If it is on the same PC as the Device Programmer, leave it as localhost or 127.0.0.1.
2. Leave the Port and Authentication Method settings as they are.
3. Under Device Communication Method, choose the Device Communication Method(s) that will be used on this PC.
4. Leave the Device Discovery and Authentication Method settings as they are. This is used for Wi-Fi.
5. Under Radio Group, leave Assigned Radio Group as *All* for now. Otherwise read the section on [Multiple Device Programmers and Groups](#) now.

6. If you chose IP Program as a device communication method, IP Program Settings will be visible. IP Program is used by repeaters and the CMSS only. Leave these settings as they are.

**Link Establishment**  
Device Programmer ID

**Capacity Max**  
Device Programmer Device ID

**PN Server**  
Use PN Server ☐  
PN Server   
Port   
**Test Connection**

**Job Settings**  
Auto Process Jobs(USB and Wireless(LAN)) ☒  
Job Pacing    Minutes

**Language Settings**  
Select Language  ▼

**Offline Mode**  
**Work Offline**

7. Under PN Server, tick *Use PN Server* if your system is not a CapMax system and you are using DDMS. Enter the IP address where DDMS is installed. If this is the same PC, either localhost or 127.0.0.1. The port number to use is 3000.
8. Press the Test Connection button. Make sure the result is a pass.
9. You can leave the settings under Job Settings as is for now.
10. The Language Setting is up to you but remember to change this elsewhere.
11. Click OK to close. You might be prompted to restart Device Programmer – if so, select Yes.

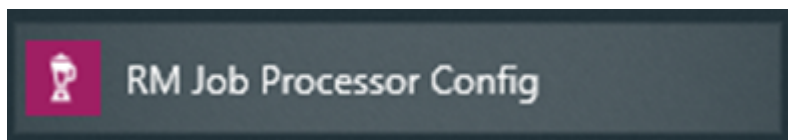
Offline Mode (and the Work Offline button) allows Radio Management to create a ZIP file containing write jobs. These jobs can be saved onto a USB stick and taken with a PC to site to program radios

or repeaters using a programming cable. This is useful when there is no connectivity between RM and the radios/repeaters in question.

Automatically Process Jobs USB & Wireless LAN should remain ticked. If Unticked, RM will wait for your input before doing a write job.

Job Pacing is useful when OTAP is used. If multiple write jobs are scheduled, it allows you to stagger the job starts to prevent a data storm or reduce processor load.

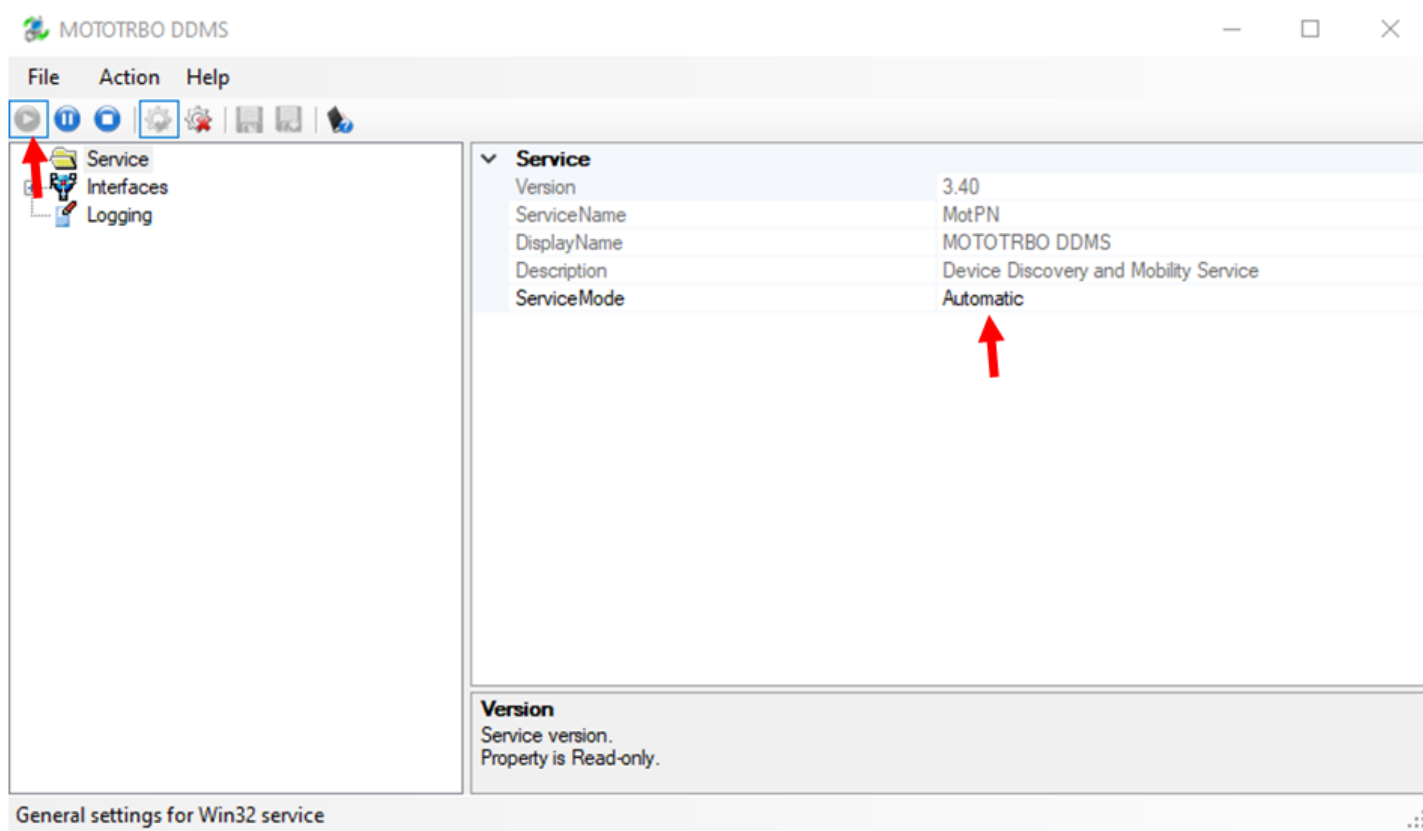
## Checking Job Processor



1. Start RM Job Processor Config.
2. Press the *Test Connection* button. If it was successful, you can close RM Job processor Config. If not, you need to make sure the RM server is running.
3. You can leave Concurrent Jobs at 1 but if you have multiple Device Programmers, you can increase this, provided the RM Job Processor has sufficient processor cores and threads to handle multiple simultaneous jobs.
4. The address can be changed if the RM Job Processor and RM Server are on different machines.
5. Close RM Job Processor Config.

## Setting up DDMS to work with your system





1. Open the MOTOTRBO DDMS Administrative Client.
2. Make sure ServiceMode is set to automatic and the Run ► button is greyed out. This means that the service is running. If it isn't greyed out, click it and make sure it goes grey.
3. Close the MOTOTRBO DDMS Administrative Client.

## Control Station Settings

If you plan to use a Control Station for OTAP, read this section. A Control Station cannot be used for Capacity Max systems.

You can configure the Control Station radio using CPS, or you can add it to Radio Management and configure it using the same tool you use for all the other radios.

In terms of RF parameters and so forth, you would configure the Control Station to work on the system like any other radio except that you would not add any talkgroups.

The Control Station will need a unique Radio ID and will be the ARS Radio ID for all radios on the system that will be provisioned via OTAP.

<b>General Settings</b>	
Note 1	If you manage the control station configuration from Radio Management, the Radio Name and ID are in Radio View.
Radio Name (see note 1)	Control Station X
Radio ID (see note 1)	See above
<b>Accessories</b>	
Cable Type	Motorola Solutions
<b>Security</b>	
Note 2	Configure as per your radio system.
<b>Network</b>	
CAI Network	12
Group CAI Network	225
Max TX PDU Size	750
Forward to PC	Via USB
Voice Only	Unticked
Data Modem System Type	Per your system
Data Modem Window Size	5, not required for OTAP
<b>Channel / Personality</b>	
Note 3	Except for the below, configure as per your radio system.
TX Power	First try low. If low doesn't work, change to high. Preferably you should leave this on low if you will do a lot of OTAP jobs. If you must run the control station at high power you should add some additional cooling (e.g. a fan blowing across the chassis).
TX Admit Criteria	Always or Colour Code Free.
In Call Criteria	Always
Data Call Confirmed	Ticked

At this point, you will need to use Windows Command Prompt in Administrator mode. To run Command prompt, search for cmd in the taskbar and when Command Prompt appears, choose to run as an administrator. Running Command Prompt as a normal user, even if you are an administrator on the computer, will not work.

Start by attaching the radio to the Device Programmer host PC.

Confirm that a MOTOTRBO network connection is visible in Windows Device Manager and in Networks. Confirm that you are able to ping the Control Station by going to the Command Prompt in Windows and typing:

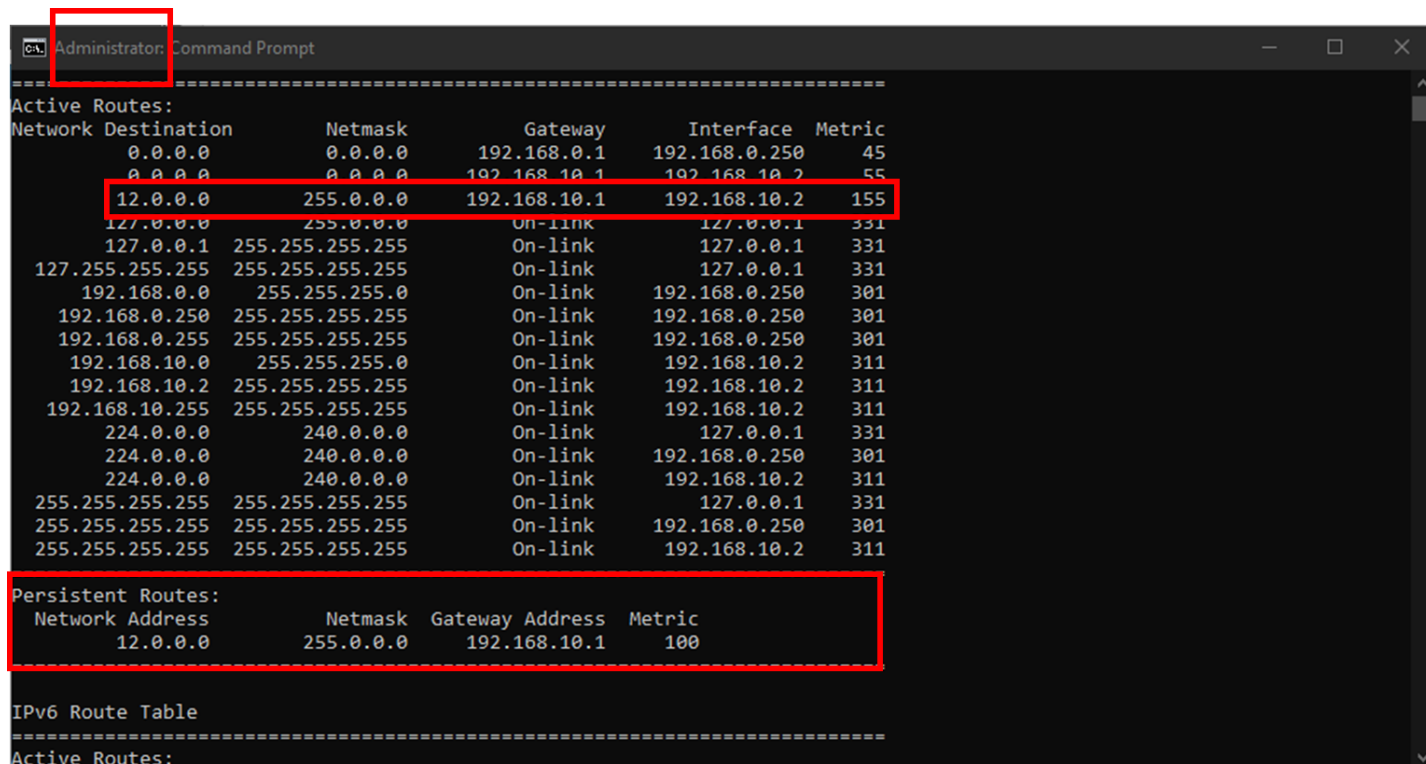
```
ping 192.168.10.1
```

In Windows Command Prompt, set the route for the 12.0.0.0/8 subnet to point to the control station:

```
route add -p 12.0.0.0 mask 255.0.0.0 192.168.10.1 metric 100
```

To check, use this command:

```
route print
```



```
Administrator: Command Prompt
=====
Active Routes:
Network Destination    Netmask          Gateway          Interface        Metric
0.0.0.0                0.0.0.0          192.168.0.1      192.168.0.250    45
0.0.0.0                0.0.0.0          192.168.10.1     192.168.10.2     55
12.0.0.0              255.0.0.0        192.168.10.1     192.168.10.2     155
127.0.0.0             255.0.0.0        On-link          127.0.0.1        331
127.0.0.1             255.255.255.255  On-link          127.0.0.1        331
127.255.255.255       255.255.255.255  On-link          127.0.0.1        331
192.168.0.0           255.255.255.0    On-link          192.168.0.250    301
192.168.0.250         255.255.255.255  On-link          192.168.0.250    301
192.168.0.255         255.255.255.255  On-link          192.168.0.250    301
192.168.10.0          255.255.255.0    On-link          192.168.10.2     311
192.168.10.2          255.255.255.255  On-link          192.168.10.2     311
192.168.10.255        255.255.255.255  On-link          192.168.10.2     311
224.0.0.0             240.0.0.0        On-link          127.0.0.1        331
224.0.0.0             240.0.0.0        On-link          192.168.0.250    301
224.0.0.0             240.0.0.0        On-link          192.168.10.2     311
255.255.255.255       255.255.255.255  On-link          127.0.0.1        331
255.255.255.255       255.255.255.255  On-link          192.168.0.250    301
255.255.255.255       255.255.255.255  On-link          192.168.10.2     311

Persistent Routes:
Network Address        Netmask    Gateway Address  Metric
12.0.0.0              255.0.0.0  192.168.10.1     100

IPv6 Route Table
=====
Active Routes:
```

Confirm that route print lists the entry for 12.0.0.0 is listed and is persistent.

Try to ping a radio by using:

```
ping 12.x.x.x -w:5000
```

The value of x is the Radio ID expressed as an IP address with 12 as the first octet (CAI).

To convert a Radio to an IPv4 address:

1. Convert the decimal Radio ID to hexadecimal.
2. Write the result down as a 24 byte number
3. Split this number into single 8-bit bytes separated by a dot.
4. Convert each byte back to a decimal number with 12 up front.

As an example, to convert Radio ID 1001 to an IP address:

1. Convert 1001 to hexadecimal.
2. Write the result down as a 24 byte number which is 0003E9
3. Split this number into single 8-bit bytes separated by a dot which is 00.03.E9
4. Convert each byte back to a decimal number. 00 becomes 0, 03 becomes 3 and E8 becomes 233. And with 12 up front it becomes 12.0.3.233

If you are able to ping both the Control Station and target radio, you are done with this task.

## Taking care of Windows Firewall

In the RM Server Utility, go to Network Settings. Do not change anything! Make a note of the port numbers and ranges.

By default these are:

- ☐ 443
- ☐ 49202
- ☐ 49205-49210
- ☐ 51020-51030
- ☐ 50003
- ☐ 65534

You will need to unblock these ports in Windows Firewall – which blocks all but 443 by default.

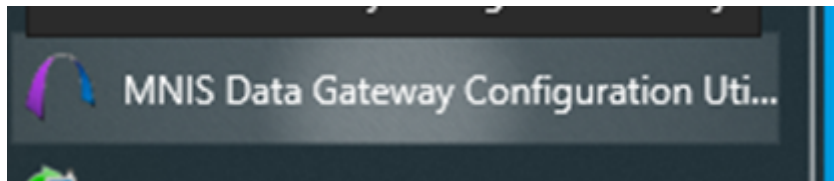
## Setting up MNIS

Skip this section if you will not be using MNIS. If you are using a Capacity max system you can skip this section too.

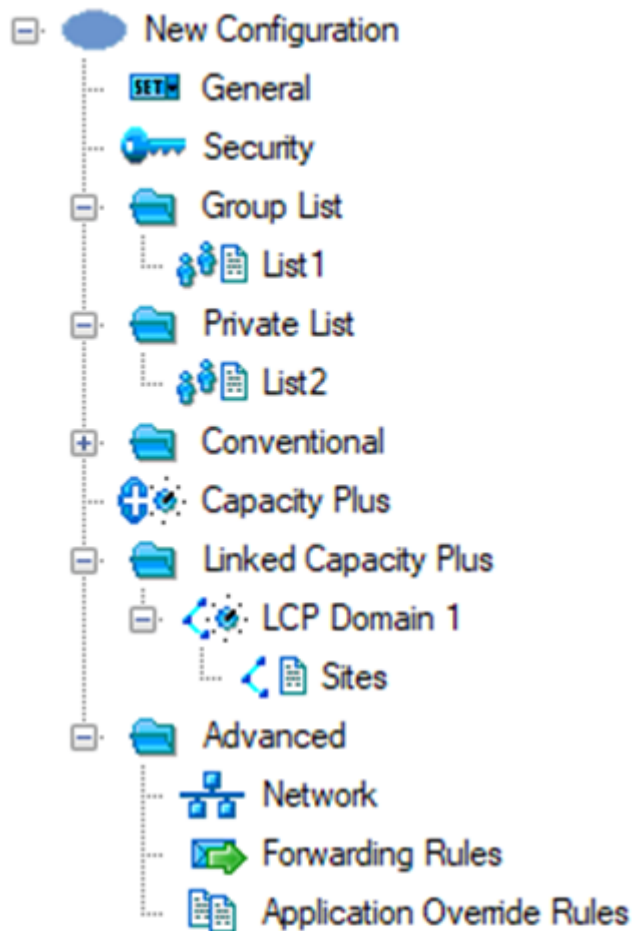
MNIS (MOTOTRBO Network Interface Service) is a Windows service application which supports data between PC-based applications and MOTOTRBO radios. It would be used in systems where a Control Station cannot be used or is not needed.

In Single Site; IP Site Connect and Capacity Plus systems, the repeaters on which data will pass, require a NAI Data Licence.

1. Make sure that:
  - a. The repeaters in the system, or those used for OTAP, have the NAI data licence.
  - b. There is an IP connection between the repeater(s) and the MNIS host.
  - c. There is an IP connection between MNIS, DDMS and the Device Programmer configured to use this MNIS instance.



2. Open the MNIS Data Gateway Configuration Utility. Click Configuration then New (menu, top left) then configure the following:



General Settings	
System Operation Mode	whatever system you have.
MNIS Application ID	See below
Enable Tunnel Interface	Ticked
MNIS IP Address	See below
Security	
Basic Privacy	If you are using Basic Privacy, specify the key here.
Enhanced Privacy Keys	If you are using Enhanced Privacy, add the keys to this table.
Symmetrical Keys	If you are using AES-256, add the keys to this table.
Group Lists	

Note 1	You can skip this
<b>Private Lists</b>	
Note 2	You can skip this
<b>Conventional Domain</b>	
Note 3	Only add an entry here if the System Operation Mode (above) is set to Conventional.
Master IP Address (see note 3 above)	The IP address of the Master Repeater
Master UDP Port (see note 3 above)	The UDP port of the Master repeater. By default this is 50000 but check the Master repeater configuration (or your system design) to make sure.
MNIS LE Port (see note 3 above)	Automatically Assigned
Authentication Key (see note 3 above)	Enter the IPSC Authentication Key if used. Note that this is not the RAS key nor any encryption key. This key is only used by the repeaters. You can find this
SFR Mode (see note 3 above)	Tick this if the repeater is using ERDM.
MOTOTRBO Link (see note 3 above)	Tick this if the system is using MOTOTRBO Link in any part of the network.
Private List	None (see note 2)
<b>Repeater Slot 1</b> (see note 3 above)	
Enable	Ticked, if timeslot 1 will be used for OTAP.
Revert Channel	Unticked (OTAP does not use data revert)
Security Setting	Depends on what you set in Security (above). If you are not using any encryption, you can leave this as None.
Security Alias	If Security Setting is set to anything other than None, you will need to choose which key to use. If you are not using any encryption, you can leave this blank.
<b>Repeater Slot 2</b> (see note 3 above)	

Enable	Ticked, if timeslot 2 will be used for OTAP.
Revert Channel	Unticked (OTAP does not use data revert)
Security Setting	Depends on what you set in Security (above). If you are not using any encryption, you can leave this as None.
Security Alias	If Security Setting is set to anything other than None, you will need to choose which key to use. If you are not using any encryption, you can leave this blank.
<b>Capacity Plus.</b>	
Note 4	Only edit the settings here if the system is a single site Capacity Plus system.
Master IP Address (see note 4 above)	The IP address of the Master Repeater
Master UDP Port (see note 4 above)	The UDP port of the Master repeater. By default this is 50000 but check the Master repeater configuration (or your system design) to make sure.
MNIS LE Port (see note 4 above)	Automatically Assigned
Authentication Key (see note 4 above)	Enter the IPSC Authentication Key if used. Note that this is not the RAS key nor any encryption key. This key is only used by the repeaters. You can find this
Security Setting (see note 4 above)	Depends on what you set in Security (above). If you are not using any encryption, you can leave this as None.
Security Alias (see note 4 above)	If Security Setting is set to anything other than None, you will need to choose which key to use. If you are not using any encryption, you can leave this blank.
Private List (see notes 1, 2 and 4 above)	None
Group List (see notes 1, 2 and 4 above)	None
Outbound Data Limit	Set this to the maximum number of timeslots you



	are prepared to use for OTAP. However, remember that voice will always take priority but if a data transfer is in progress, users may experience call rejections.
GPS Longitude	Not needed for OTAP
GPS Latitude	Not needed for OTAP
<b>Linked Capacity Plus Domain</b>	
Note 5	
Master IP Address (see note 5 above)	The IP address of the Master Repeater
Master UDP Port (see note 5 above)	The UDP port of the Master repeater. By default this is 50000 but check the Master repeater configuration (or your system design) to make sure.
MNIS LE Port (see note 5 above)	Automatically Assigned
Authentication Key (see note 5 above)	Enter the IPSC Authentication Key if used. Note that this is not the RAS key nor any encryption key. This key is only used by the repeaters. You can find this
Security Setting (see note 5 above)	Depends on what you set in Security (above). If you are not using any encryption, you can leave this as None.
Security Alias (see note 5 above)	If Security Setting is set to anything other than None, you will need to choose which key to use. If you are not using any encryption, you can leave this blank.
Private List (see notes 1, 2 and 5 above)	None
<b>Sites</b> (see note 5 above)	
Add	However many sites are in the MSCP system.
Site ID	The Site ID number per the Sites table in the Master Repeater configuration.
Group List (see notes 1, 2 and 5 above)	None

Outbound Data Limit	Set this to the maximum number of timeslots you are prepared to use for OTAP at each site. However, remember that voice will always take priority but if a data transfer is in progress, users may experience call rejections.
GPS Longitude	Not needed for OTAP
GPS Latitude	Not needed for OTAP
<b>Advanced</b>	
Data Call Confirmed	Ticked
Data Queue Limit	1000
Compressed UDP Header	None
Battery Saver Preamble	Ticked
Individual Data to Registered Site	Unticked (greyed out)
Selective Forwarding	See below
TX Preamble Duration	120ms
Conventional Channel Access	Normal
MNIS LE ID	Use MNIS ID
<b>Network &amp; Services</b>	
Note 6	Leave everything here as is. See below.
<b>Forwarding Rules</b>	
Note 7	Do not add anything here.
<b>Application Override Rules</b>	
Note 8	Do not add anything here.
The settings in Network and Services should look like below.	

## Network

CAI Network 12

CAI Group Network 225

## Services

ARS UDP Port 4005

TMS UDP Port 4007

Telemetry UDP Port 4008

Location Server UDP Port 4001

Station Information Protocol UDP Port 5017

Battery Management UDP Port 4012

Job Ticket UDP Port 4013

Sensor Request Response UDP Port 4015

User Defined UDP Port 1 Disabled

User Defined UDP Port 2 Disabled

User Defined UDP Port 3 Disabled

XCMP Enable ☐

XCMP Server UDP Port 4004

ARS Monitor ☐

ARS Monitor ID None

3. Once you are done, click the ☐ (save) button or click on the Configuration menu and select Save.
4. Once saved, click Configuration once more then Select Active Configuration, choose the file you've just saved and click on OK in the popup.
5. Lastly, click on the ▶ (play) button or click on the Service menu and select Start.
6. MNIS is now running as a service and you can now close the configuration tool.

Some things to remember from the above table:

- Selective forwarding is only needed if you will be using additional applications with MNIS, other than RM (OTAP). Examples of this would be IMPRES Battery Fleet Management or your favourite flavour of Dispatch Application. In which case, forwarding rules will need to be set
- The MNIS IP address must be in its own subnet. If you are using a control station on this PC, you should choose another 192.168.0.0/16 subnet not used by the connected radio.
- The MNIS Application ID is the Radio ID of MNIS. It is also the ARS Radio ID used by all radios on the system. This number must not be used by any radio and must be provisioned in all radios that will be OTAPed.

## Programming radios via Wi-Fi

Depending on the model, new radios which support Wi-Fi require a once-off activation via the internet. To do this, you can set up a special Access Point with the following details:

SSID: MOTOTRBO  
 Passkey: Radio Management (WPA2 Personal)

New radios have the above network in their codeplug by default. You must remove this once the radios have been programmed for the first time.

The Access Point with the above credentials must be locked down to prevent unauthorised access and use. The DHCP lease time must be set to short - most routers will go down to 30 minutes.

Radios which require a once-off activation, require access to the following addresses and ports:

Host	Port	Protocol	Direction
pool.ntp.org	123	UDP	Outbound
time.google.com	123	UDP	Outbound
devicecertmgmt-cmf21.motsolpki.com	49682-49684	TCP	Outbound

devicecertmgmt-cmf21.motsoipki.com	49682-49684	TCP	Outbound
locator.radiocentral.motorolasolutions.com	443	TCP	Outbound
api-us.radiocentral.motorolasolutions.com	443	TCP	Outbound
api-au.radiocentral.motorolasolutions.com	443	TCP	Outbound
usp9rmstorage.blob.core.windows.net	443	TCP	Outbound
aup9rmstorage.blob.core.windows.net	443	TCP	Outbound
global.azure-devices-provisioning.net	443	TCP	Outbound
iotcs-hub-us.azure-devices.net	8883	TCP	Both

In the radio configuration, under Wi-Fi Network, there is a Device Discovery Server Name field. If the Access Point and Device Programmer are on the same subnet, then you can leave this field empty. In this case, the radio will send the DNS-SD (MDNS) to a broadcast IP to notify the Device Programmer of its presence.

If the Access Point and Device Programmer are not on the same network, then you need to provide a fully qualified domain name (FQDN) or IP address for the Device Programmer host. In this case, the radio will send the DNS-SD to the Device programmer host only.

In either case, you need to ensure that the firewall on the Device Programmer host is properly configured to allow the required IP traffic to pass.

MOTOTRBO radios with Wi-Fi capabilities support the following security modes:

- WPA/WPA2 Personal is supported with both AES and TKIP encryption.
- WPA/WPA2 Enterprise is supported with both AES and TKIP encryption. In addition, in this mode, the radios also support EAP TLS; PEAP with Phase 2 authentication as TLS and MSCHAPV2 and EAP TTLS with Phase 2 authentication as PAP, CHAP, MSCHAP, and MSCHAPV2

If validation of the server certificate is required, the certificate of the subscriber and the certificate of the authentication server must be issued by the same Certificate Authority.

WPS is not supported due to security flaws discovered in the protocol.

WEP is supported but is for the most, obsolete and not recommended due to security flaws. The radios also support open Wi-Fi networks but this is very risky.

E-series radios; ION and the R7 are able to roam between Access Points on an Enterprise network without needing to perform full authentication - this is known as Opportunistic Key Caching. The radio performs full authentication only on the first connection. When this happens, the Pairwise Master Key

(PMK) is cached and used for all subsequent authentications as the radio roams between Access Points.

To enable this:

1. Click on Actions ⚙; Manage then Configurations.
2. Select the configuration of the radio you wish to enable this on and either click on the Edit button ✎ or right-button click the configuration and select Edit Configuration.
3. Navigate to the Wi-Fi Network set..
4. In the Network Profile Table, tick Opportunistic Key Caching.
5. Click Save.
6. Go to Radio View and schedule a write job for the affected radios.

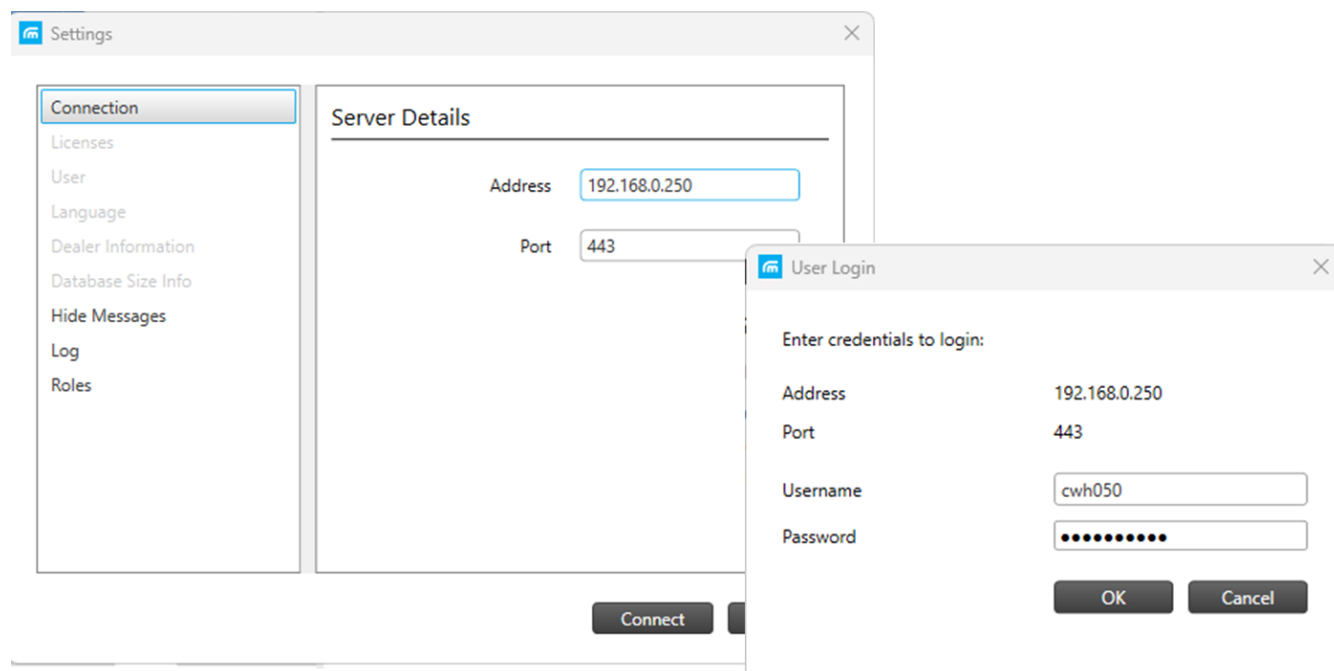
## Starting Radio Management Configuration Client for the first time

A reminder:

- Adding radios to Radio Management for the first time must be done using the USB programming cable or Wi-Fi. The same is true for repeaters. This means reading and then a once-off write.
- Any changes after that can be done via Wi-Fi, IP or OTAP.
- You only need to do the above once for each radio model. You can reuse the MVO and/or configuration on other radios of the same model and feature set.

To log in for the first time:

1. Start Radio Management Configuration Client.
2. Enter the IP address or FQDN of the RM Server and click Connect.
3. Log in using your assigned username and password - this you would have done when setting up the server.



You may be prompted to update your password once logged in - this depends on whether the user must change the password was ticked when you added the account.

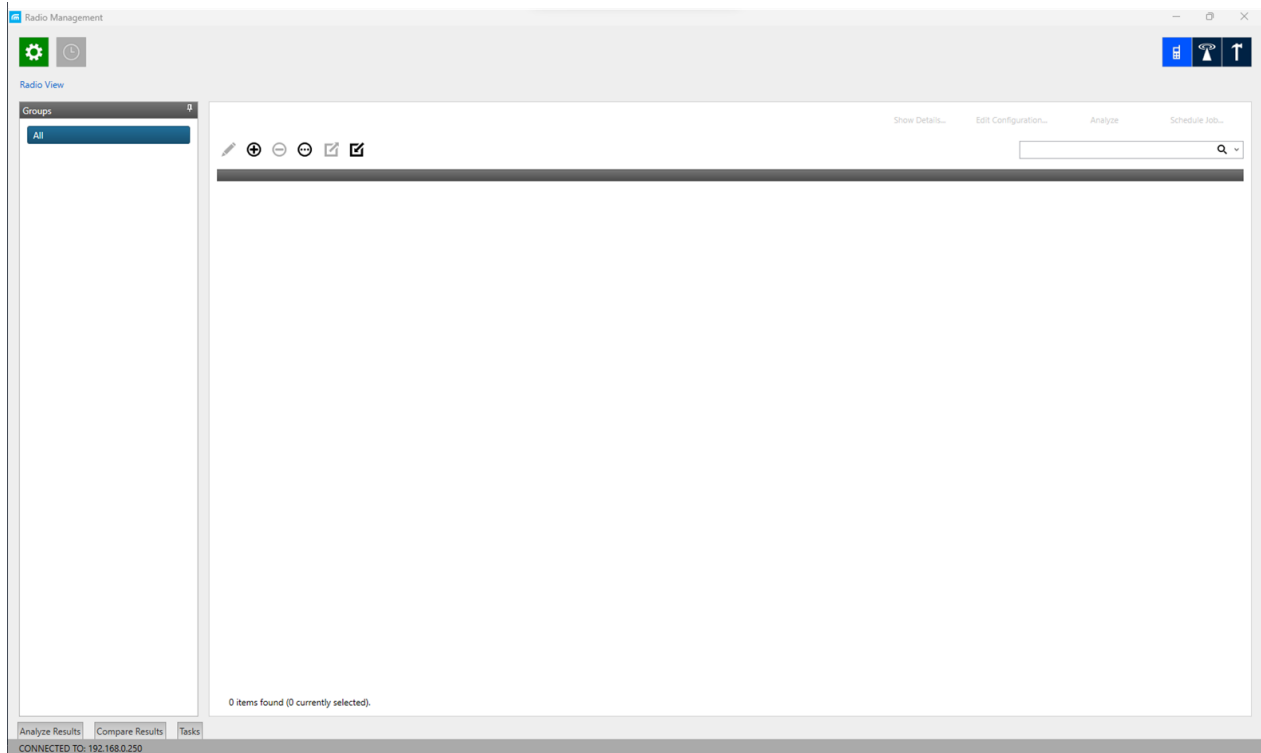
**Failed to connect to the RM server. The root cause may be:**

- 1) Wrong server name or IP address.**
  - 2) RM server service is not running.**
  - 3) Wrong UTC time settings.**
  - 4) Certificate file may be corrupt if the authentication method is "Certificate".**
  - 5) This PC is not in the same domain with RM server if authentication method is "Windows".**
- Refer to the help if you continue to get this message.**

If you see the above error check the following:

- ☐ Time on the server
- ☐ Time of the client PC
- ☐ Make sure no firewall is blocking TCP port 443.

4. If the login was successful, you should be presented with the below:



## What each button does in the RM client

What each button/element does in the above window.



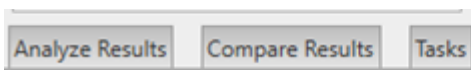
Actions menu.



Schedule.



Radio View, System View and Job View.



Analyse Results, Compare Results and Tasks. Click on them to see the information.



Groups list (nothing to do with Talkgroups). This allows you to organise radios and repeaters into groups and subgroups. Each group can represent a department or customer. This becomes useful if you have multiple Device Programmers.

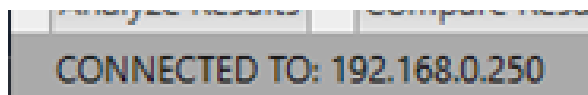




Edit, Add, Remove; More; Import and Export. Import and export allows you to import and export the displayed list.

Under more you can import and export a radio configuration. Importing allows you to import a ctb or ctb2 file that was created in CPS. Export allows you to export a radio as a xpsa file which can be read using CPS2.

Which server you are (were) connected to.



## What do the coloured blocks mean in the Modified column?

Colour	What has changed?
Grey	No changes (no need to write radio/repeater)
Purple	Codeplug modified
Green	Firmware modified
Teal	Language packs modified
Blue	Voice announcement files added
Orange	Text to speech files modified
Red	Bluetooth sensor files modified
Tan	Features ready for activation
Dark blue	Packages modified

## Adding Radios

There are three ways to add a radio to RM:

- Entering the serial number and scheduling a read job or applying an existing MVO and configuration. I will only show this method here.
- Importing codeplugs and applying an existing/matching MVO.
- Importing a spreadsheet and then either importing codeplugs plus MVO or scheduling a read job or applying an existing MVO and configuration.




The 'New Radio' dialog box is shown with the following fields and values:

Field	Value
Serial Number	871TSVV255
Radio ID	
CAI	
Radio Alias	
Radio IP	
Read/Write Password	


Buttons: OK, Cancel


To add a radio or repeater (or CMSS or MNIS if this is a Capacity Max system):

1. Make sure you are in Radio View .
2. Click on the ⊕ (add) button.
3. Enter the serial number of the radio or repeater to be added.
4. The other information is optional.
5. Click OK.

If the radio is attached locally via a programming cable or Wi-Fi, you can grab the serial number from the Device Programmer after a few seconds. If you've enabled Automatically Add Radios in the RM Server Configuration, you can skip the above as the radio will be added as soon as it's seen.

If you are adding a CMSS (Capacity Max only), use the HP serial number on the pull-out card. If you are adding a MNIS data gateway (Capacity Max only), enter a ten digit alphanumeric string. I use 000MNISDG1, 000MNISDG2 and so forth. For all other systems, MNIS is configured from within the tool and exported as a .gwcfg file.

6. Right-button click the newly added radio and select Schedule Job. You can also select the radio and press the schedule button .
7. In the Schedule Job window:
  - a. Select *Read*.
  - b. *Generate Configuration* must be ticked if this is the first radio of its type.
  - c. Generally, for a new setup, the *Connection Method* should be set to *USB + Wireless (LAN)*.
8. Click OK to start reading the radio or repeater. If this is a Capacity Max system, remember that you cannot read a CMSS or MNIS instance - only write or export.
9. Make sure the radio or repeater is connected and powered.


Schedule Job
×

Job Type

☐ Write
☐ No Switchover
☐ Switchover
☒ Read
☒ Generate configuration
☐ Apply to radio

Connection Method

☒ USB + Wireless (LAN)
☐ IP Program
☐ Over the Air
☐ Any

☐ Suppress ARS after Switchover

Switchover Timer (min):

0

Job Name:

Time Zone:

(UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

▼

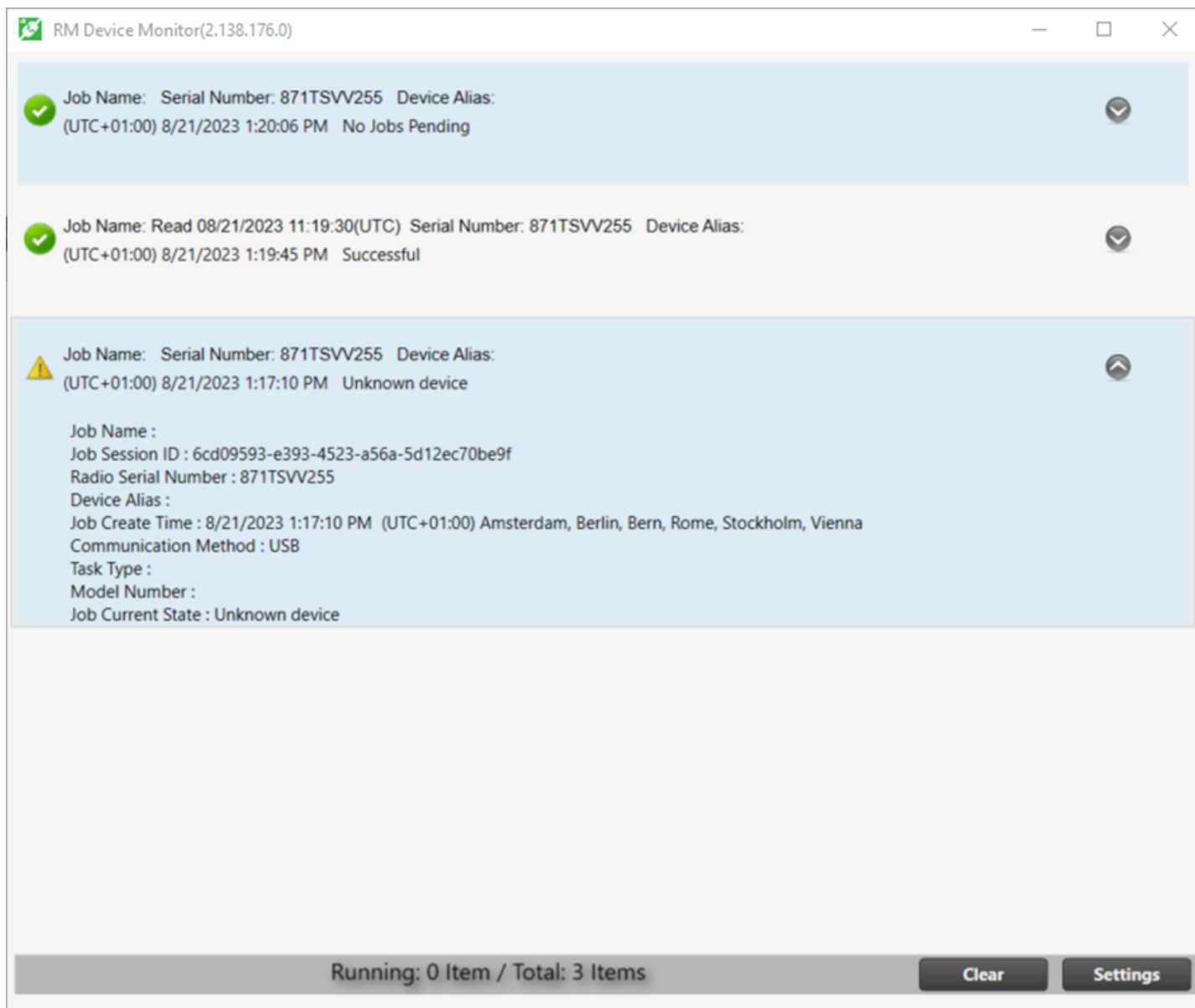
Start after

End before

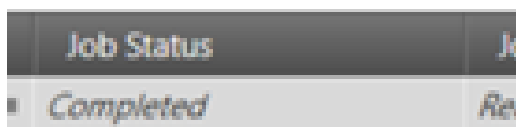
OK

Cancel

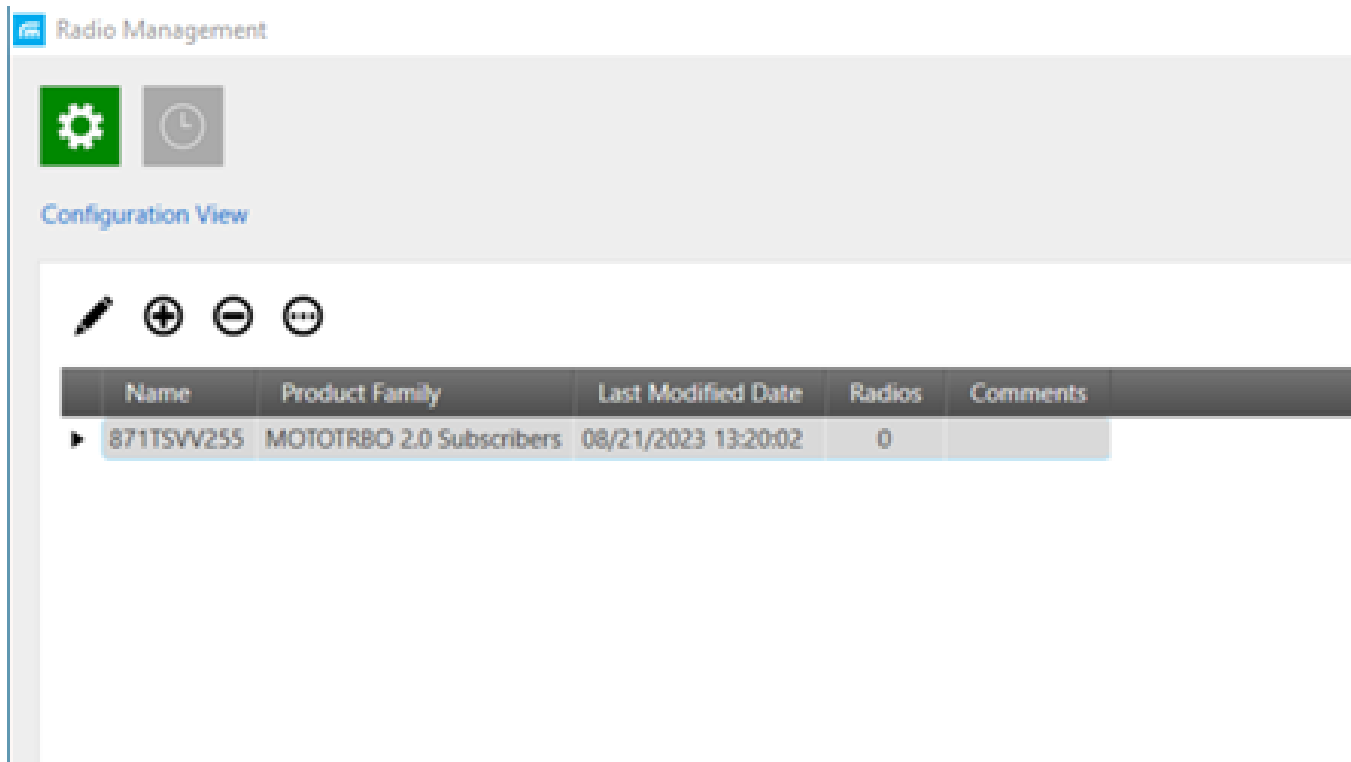
If you have the Device Programmer open, you might see the below. If you do, it means the read went through.



Back in the RM Client, the job will eventually have a status of Completed.



To edit the newly added radio's configuration, click on Actions ⚙ ; select Manage and then Configurations. The configuration of the radio you have just read is shown as it is below. Double click it to start editing or select it and click the edit ✎ button.



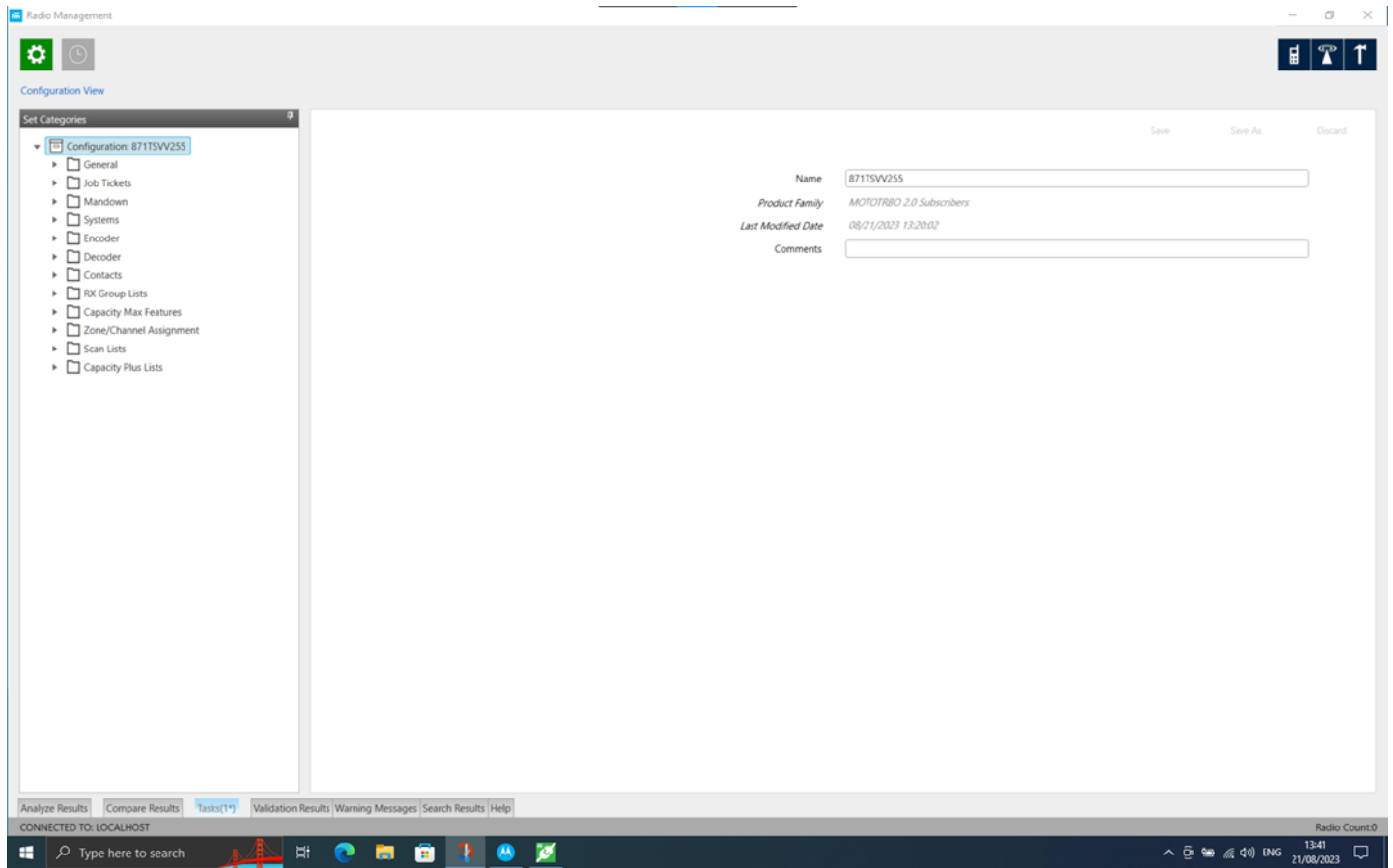
The configuration can now be edited just like in the CPS with some differences. The look and feel is exactly like CPS2.

For starters, you must give the configuration a logical name. When reading a new radio and generating the configuration, RM uses the device's serial number which is not good enough. I prefer to rename it to something like customer\_model\_config\_n (e.g. ACME\_DP4801e\_Config\_1)

Things like Radio ID and aliases are not in the configuration - these are all in the Radio View.

A configuration can be shared between multiple radios – as long as those radios are the same. A configuration is made up of multiple sets. You can copy one set to another configuration to save time.

After going out of each set, you have to save.



If you will be using OTAP, you must specify an ARS Radio ID (Network Set) and ARS must be enabled in all digital channels [i.e. not set to None].

You must specify an OTAP key. The OTAP key must be in all the radio for OTAP to work. You can manage the OTAP key values by going to Actions; Manage then OTAP Keys. You must also select which OTAP key will be used for the radios.



	Key ID	Key Alias	Key Value	In-Use Templates and Sets	In-Use Templates (Template Mode)	In-Use Sets(Configuration Mode)	Comments
▶	1	OTAP1	* ∅	1	0	1	
▶	2	AcmeEnt_1	123456789	0	0	0	

#### OTAP Authentication Key



	Authentication Key ID	Authentication Key Alias
▶	2	AcmeEnt_1

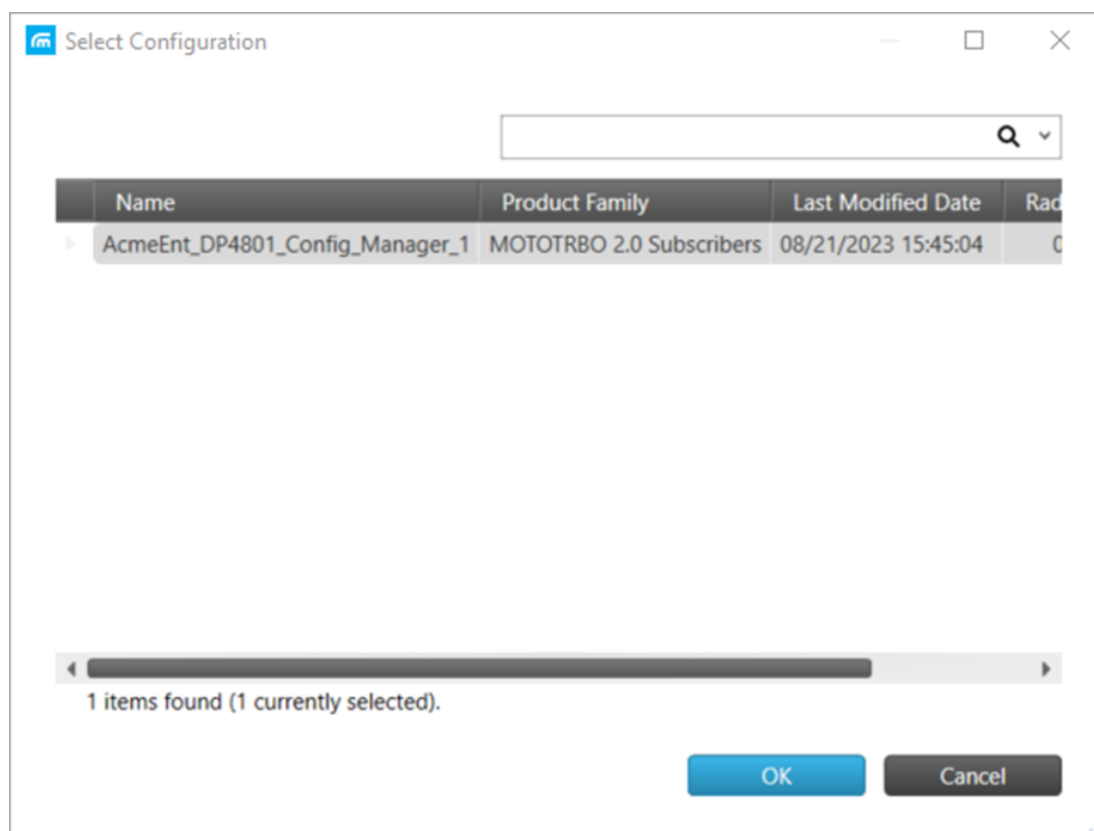
Once you are done with editing the radio configuration and are happy with it, close the configuration and go back to Radio View.

Select the radio you've just read/added; right-button click and choose Select Configuration. Select the configuration you've edited for this radio and click OK.





Serial Number	Radio Alias	Caller Alias	Conf
<div><div>CutCtrl+XCop Ctrl+CPasteCtrl+VShow Details...Ctrl+WDeleteDelSelect Group...Alt+Shift+GEdit Configuration...Ctrl+FSelect Configuration...Alt+Shift+FCompare</div></div>			



If Select Configuration is greyed out, you have probably added a serial number without reading the radio - no problem as long as there is an MVO for this device. If this happens, right-button click the radio or repeater once more and choose Select MVO. Then select the MVO that matches this device exactly. Once a MVO has been chosen, you can select a configuration as shown above.

Still, while in Radio View, you should now edit the following fields to suit your setup:

- Radio Alias is the text shown on the screen of the radio upon turn on or if the user goes into the menu. You can add something here even if it's a non-display model - this will help you later to find stuff.
- Caller Alias is the Talker Alias transmitted by the radio to other radios - even if the radio is not in their contact list. It requires some changes in the configuration to enable the feature.
- Group allows you to split radios into groups by customer or department. There is a section on this further down. This becomes important when you have more than one Device Programmer.
- Radio ID is the most important of all!

While still in Radio View, right-button click on the entry for the above radio(s) and select Analyse. Wait a few seconds while Radio Management parsers your configuration for any errors. Click on Analyze Results at the bottom left of the screen. If the result is green/pass, then you're ready to write the radio.

If you have errors, you have to correct them before writing the radio. Look at all the errors first. Fixing one error might clear the others. For example, in the below screen grab, fixing the contact error (7th on the list) will clear all of the others.

Analyze Results

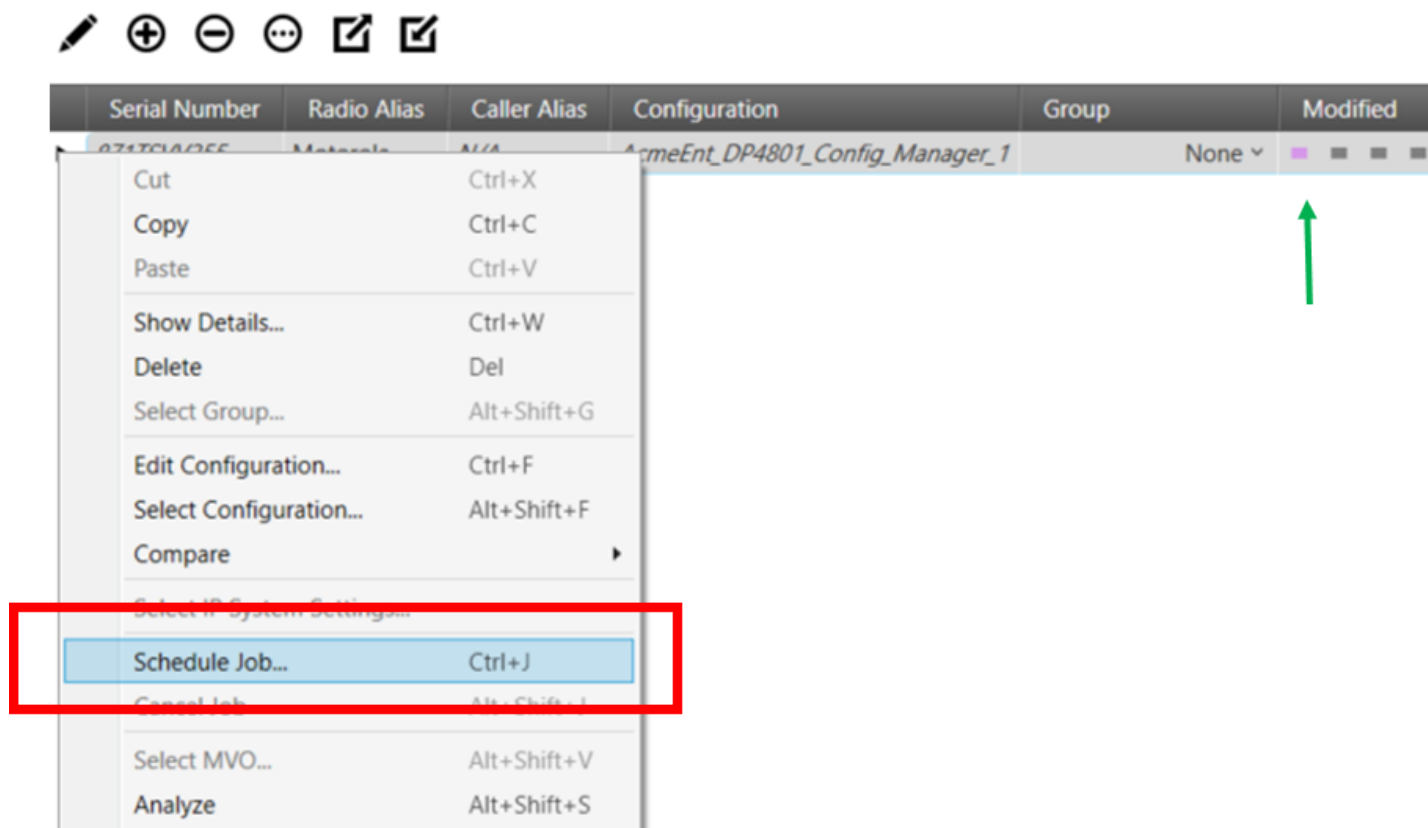
View by: ☒ All ☐ Errors ☐ Warnings

	Serial Number	Configuration	Item Path	Description
▶	871TSVV255	AcmeEnt_DP4801_Config_Manager_1	\Control Buttons:ControlButtons-601\One Touch Access:One Touch Access\Call	The expected call type
▶	871TSVV255	AcmeEnt_DP4801_Config_Manager_1	\Control Buttons:ControlButtons-601\One Touch Access:One Touch Access\Call	The expected call type
▶	871TSVV255	AcmeEnt_DP4801_Config_Manager_1	\Control Buttons:ControlButtons-601\One Touch Access:One Touch Access\Call	The expected call type
▶	871TSVV255	AcmeEnt_DP4801_Config_Manager_1	\Control Buttons:ControlButtons-601\One Touch Access:One Touch Access\Call	The expected call type
▶	871TSVV255	AcmeEnt_DP4801_Config_Manager_1	\Control Buttons:ControlButtons-601\One Touch Access:One Touch Access\Call	The expected call type
▶	871TSVV255	AcmeEnt_DP4801_Config_Manager_1	\Control Buttons:ControlButtons-601\One Touch Access:One Touch Access\Call	The expected call type
▶	871TSVV255	AcmeEnt_DP4801_Config_Manager_1	\Contacts	There should be at least 1 contact
▶	871TSVV255	AcmeEnt_DP4801_Config_Manager_1	\Digital RX Group List:List1\Members	There are no available members
▶	871TSVV255	AcmeEnt_DP4801_Config_Manager_1	\Capacity Plus RX Group List:List1\Members	There are no available members
▶	871TSVV255	AcmeEnt_DP4801_Config_Manager_1	\Flexible Capacity Plus RX Group List:FlexibleCapacityPlusRXGroupList-601\Members	Only Contacts contain members

10 items found (0 currently selected).

Error 10 Warning 0

Right-button click on the radio you've just run Analyze on, and select Schedule Job from the menu. Before doing that, notice that the purple block is now shown in the Modified column - this tells you that there are configuration changes pending for the radio.



From the Schedule Job window, select Write and USB. Enter a job name (optional but can be helpful). Click OK.

Remember that for the first time, you can only write a (new to RM) radio - often with the many changes - using USB. OTAP will be used later.



## Schedule Job



### Job Type

☒ Write

☒ No Switchover

☐ Switchover

☐ Read

☐ Generate configuration

☐ Apply to radio

### Connection Method

☒ USB + Wireless (LAN) ☐ IP Program ☐ Over the Air ☐ Any

☐ Suppress ARS after Switchover

Switchover Timer (min):

0

Job Name:

Time Zone:

(UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

Start after

End before

OK

Cancel

Modified	Job Status
✓ ■ ■ ■ ■ ■ ■ ■ ■	<i>Completed</i>


If all went well, the job status will change to Completed. When you see this, you can disconnect the radio from the PC. Like CPS2, when writing with RM via USB, the radio will reset.

## Adding more radios

You can add multiple radios that share the same configuration. There is no need to read all of them if they are:

- ☐ The same model.
- ☐ Are configured the same (except Radio ID and Aliases).
- ☐ Have the same firmware version.
- ☐ Have the same feature licences enabled.

To add many radios that meet the above criteria:

1. Add the serial numbers. You can also import them from a spreadsheet in .csv format. More about that in another section but also see below.
2. Select all the radios you've added.
3. Right-button click on the selected radios and choose Select MVO.
4. Choose the MVO which matches those radios. This will be the radio you've read in the previous steps.
5. Click OK.
6. Right-button click on the selected radios once more and choose Select Configuration.
7. Select the configuration you just created.
8. Click OK.
9. Go to Actions; Manage then Language Packs.
10. Click on the  button at the top and choose Import.
11. Select the required languages from the list.
12. Click Import.
13. Go back to Radio View and select all the radios you've added – if not selected already.
14. Right-button click on the selection and choose Upgrade Language Pack.
15. Right-button click on the selection and choose Analyze.

16. If the Analyze Results are all green, you can then schedule a write job. Don't worry about the empty Modified column, that'll get filled once the write job is done.



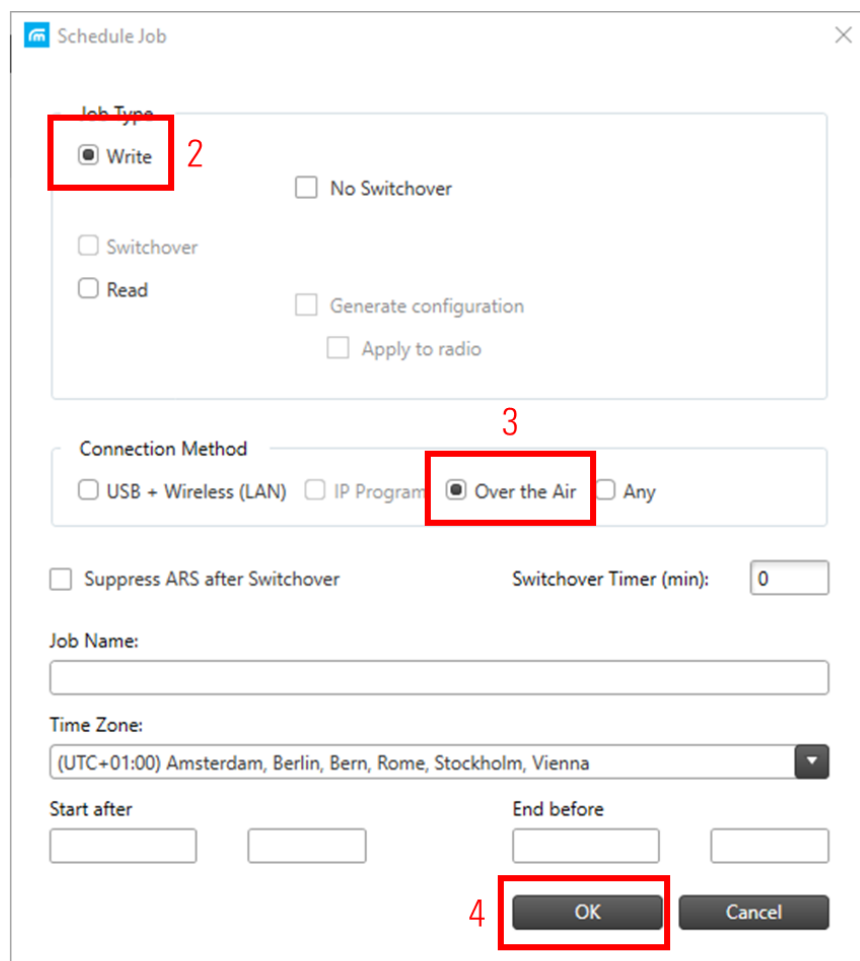
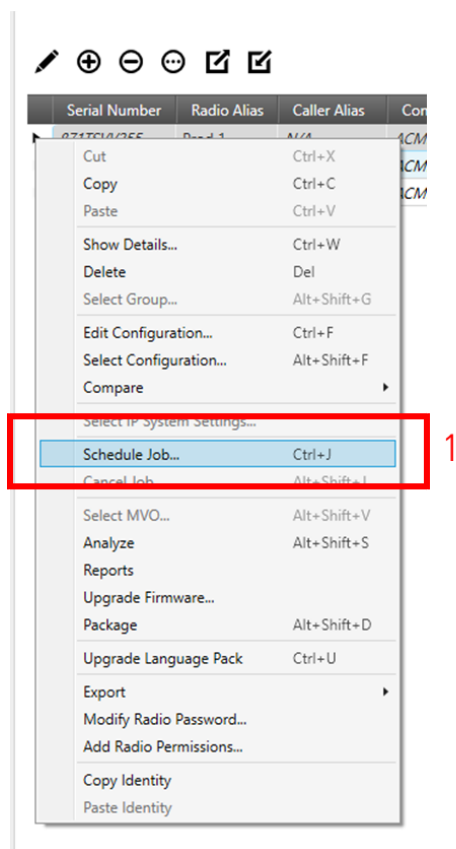
- Use the add button to add one radio at a time by manually entering the serial number.
- Use the import menu to import CTB, CTB2 or XPBA codeplug files.
- Use the import button to import a CSV file containing serial numbers.

## Some things to keep in mind

- You cannot OTAP a radio that wasn't added to RM.
- You cannot OTAP a radio that does not have any changes.
- The radio doesn't have to be on when you schedule a job (this is also true for jobs written v9ia USB). RM will keep trying to contact an offline radio.
- You cannot OTAP a firmware upgrade – but you can upgrade over Wi-Fi.
- OTAP will only send what was changed since last time – this reduces system load.
- You can schedule a write job to run during an off-peak period.
- If you made a mistake and need to cancel the write job, you can do so as long as the radio isn't being written at that point in time.

## Writing the radio(s) using OTAP

Right-button click on the newly added radio(s) and select Schedule Job from the context menu. In the popup, select *Write* and *Over the Air*.



You can schedule the OTAP write job for off-peak periods by entering dates and times under Start After and End Before. If any radios did not get OTAPed in that timeframe, they will eventually show as failed in Radio View.


## Adding Repeaters

Repeaters do not support OTAP. They do however support IP Remote Programming and in order to support this, you have to add an IP System.



To add and configure an IP System:

1. Click on the ⚙ Actions menu, then on Manage and IP System Settings.
2. Click on the ⊕ Add button.
3. Enter the following information:
  - a. System Type: Link Establishment Repeater
  - b. System Alias: Choose a name (e.g. Customer\_SystemType)

- c. Master Hostname/Address: IP address or FQDN of the Master Repeater
  - d. Port: Port number used by the Master.
  - e. Authentication Key: Authentication Key used by the system. If there is none, leave this blank
4. Click OK and click on Radio View to return to where you were before.


For the initial setup, repeaters do need to be connected to the Device Programming via a programming cable. If you have already configured the repeaters using CPS2 and have their codeplugs saved, you can import these using the  button in Radio View.

To add and read a repeater is exactly the same as adding a radio:

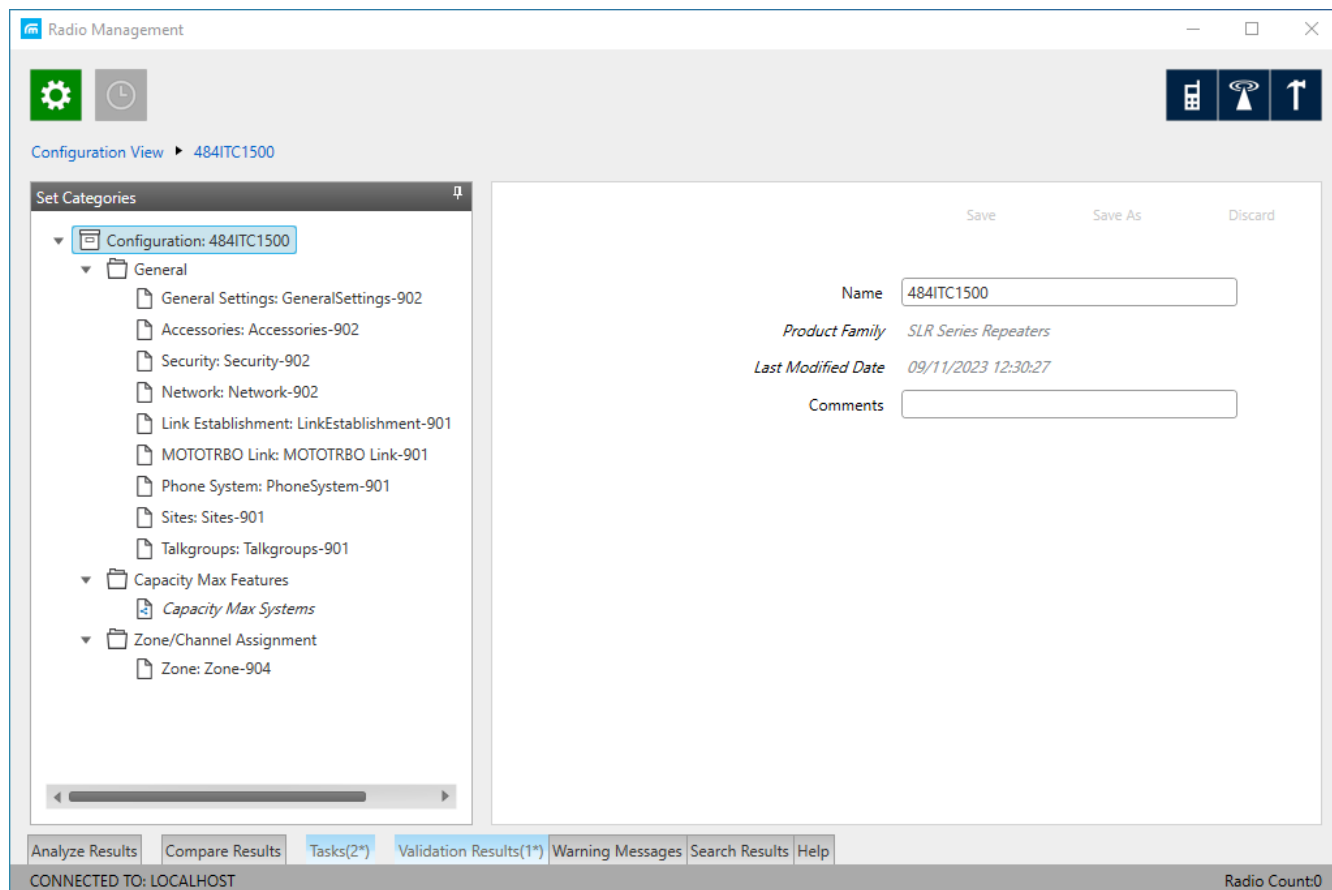
1. In Radio View, click  Add.
2. Enter the serial number of the repeater. The other information is optional and can be added later if needed.
3. Click OK.
4. Right-button click the newly added repeater and choose Schedule Job. Alternately, you can click on the  button - next to the Actions button.
5. In the Schedule Job window, select *Read*; tick *Generate Configuration* but do not tick *Apply to the radio*. In Connection Method make sure USB + Wireless(LAN) is selected.
6. You can optionally enter a Job Name.
7. There is no need to specify a date and time range for this task.
8. Click OK to start the job.

For reading via USB to work, there needs to be an IP connection between the RM server and DP host connected to the repeater. In DP, USB + Wireless (LAN) must be ticked. The repeater must be connected and powered up.

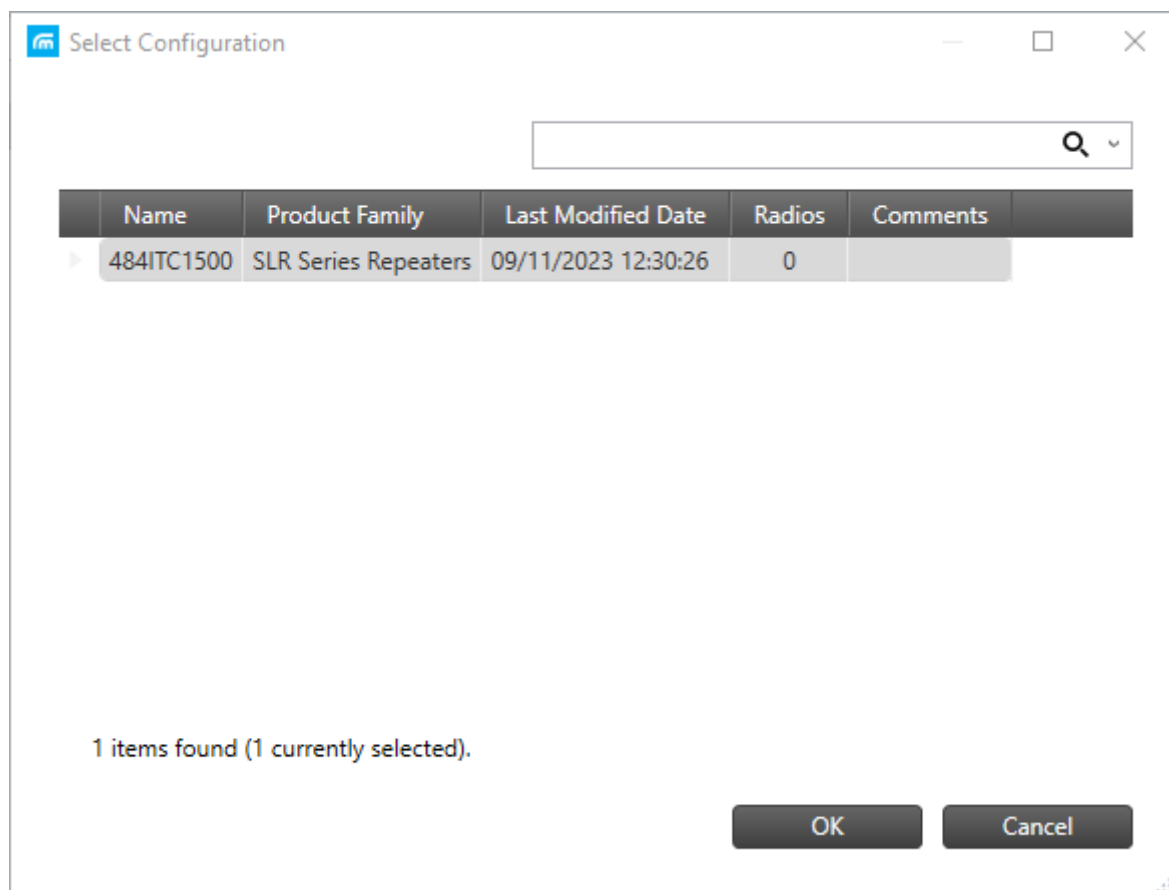
Once the repeater is read, the Job Status column entry for that device will show as *Completed*. Once completed, you can go about editing the configuration- this is the same as that for radios:

1. Click on Actions, Manage and Configurations.
2. Select the configuration you have just generated by reading the repeater and click the  Edit button. You can also right-button click on the configuration and select Edit from the content menu.
3. The configuration is exactly the same as that for radios or as configuring the repeater using CPS (see below image).






4. Once you are satisfied with the configuration, you can click on Radio View. Remember to save as you go through each set.
5. Change the Radio ID and Radio Alias to match your fleetmap. Yes, this is a repeater but it also has a Radio ID that must also be unique.
6. Right-button click on the repeater you've just edited the configuration for, and choose Select Configuration from the context menu.
7. Choose the configuration you've just edited and select OK to apply it.



8. While still in Radio View, right-button click on the newly added repeater once more and this time choose *Select IP System Settings*. Select the IP System Setting you created earlier and click OK to apply this.
9. Right-button click on the newly added repeater again and select *Analyze*. RM will parse your configuration and alert you to any errors. If there are none - like below - then you are good to go.

## Analyze Results

View by: ☒ All ☐ Errors ☐ Warnings

	Serial Number	Configuration	Item Path	Description	Actions
>	 478ITC1500	ACME_SLR_IPSCMaster			


1 items found (1 currently selected).

Error 0 Warning 0

Analyze Results

Compare Results

Tasks(4\*)

10. Right-button click the newly added repeater and choose Schedule Job. Alternately, you can click on the  button - next to the Actions button.
11. In the Schedule Job window, select Write and in Connection Method, make sure *USB + Wireless(LAN)* is selected this time.
12. You can enter a Job Name. I usually use something like "initial" or "Day0".
13. There is no need to specify a date and time range now but do remember writing a repeater will cause it to reset. So if the interruption is too risky, you might want to schedule the job for an off-peak period. For this the PC will need to remain connected to the repeater.
14. Click OK to start the write job and wait for it to complete.

## Some things to remember with regards to repeaters in RM

If the repeater was already configured and working prior to reading into RM, you do not need to change anything in the configuration except renaming the configuration and possibly renaming the sets. Please check the Radio ID and Radio Alias in Radio View though.

Each repeater must have its own configuration. Although this may go against the concept of sharing a configuration, in most systems, there are comparatively few repeaters and the amount of configuration work is also relatively small. You can copy sets between configurations - this will save you lots of time.

Multiple repeaters can share the same IP System Settings. This tells Radio Management at which IP address (or domain name) the Master Repeater can be found.

## Making updates to repeater codeplugs via IP

To write configuration changes to repeaters that have already been added and written:

1. Edit each repeater's configuration remembering to click save when moving between sets.
2. In Radio View you will notice that those repeaters will now have a purple block (and possibly other coloured block) in their modified column.
3. Select those repeaters, right-button click and choose Schedule Job.
4. In the Schedule Job window, select Write and in the Connection Method, make sure *IP* is instead selected.
5. You can enter a Job Name. I usually use something like "initial" or "Day0".
6. If needed, specify a date and time range you want the job to go through. The best is to do this sort of work during off-peak periods when the impact of an interruption will be less.
7. Click OK to start the job.

IP can be selected this time since the repeaters have been added and Radio management knows how to connect to them to do IP Remote Programming.

## Importing and exporting codeplugs to/from CPS and other RM instances

1. In Radio View, click on the ... button.
2. From the menu, select either import or export.
3. If you select import, you will be prompted to select a file. Select a valid codeplug. Files in ctb; ctb2 and .xpba format are supported. If you're exporting, skip 4 and 5.
4. As soon as you've selected a file and clicked OK, the following popup window will appear. If the file is invalid, RM will display an error message.

**Import Radios**

☐ Create radios

☐ Create configurations

☐ Apply configurations to radios

**Override Options**

☐ Always override

☐ Never override

Password:

**Import** **Cancel**

5. Ticking:

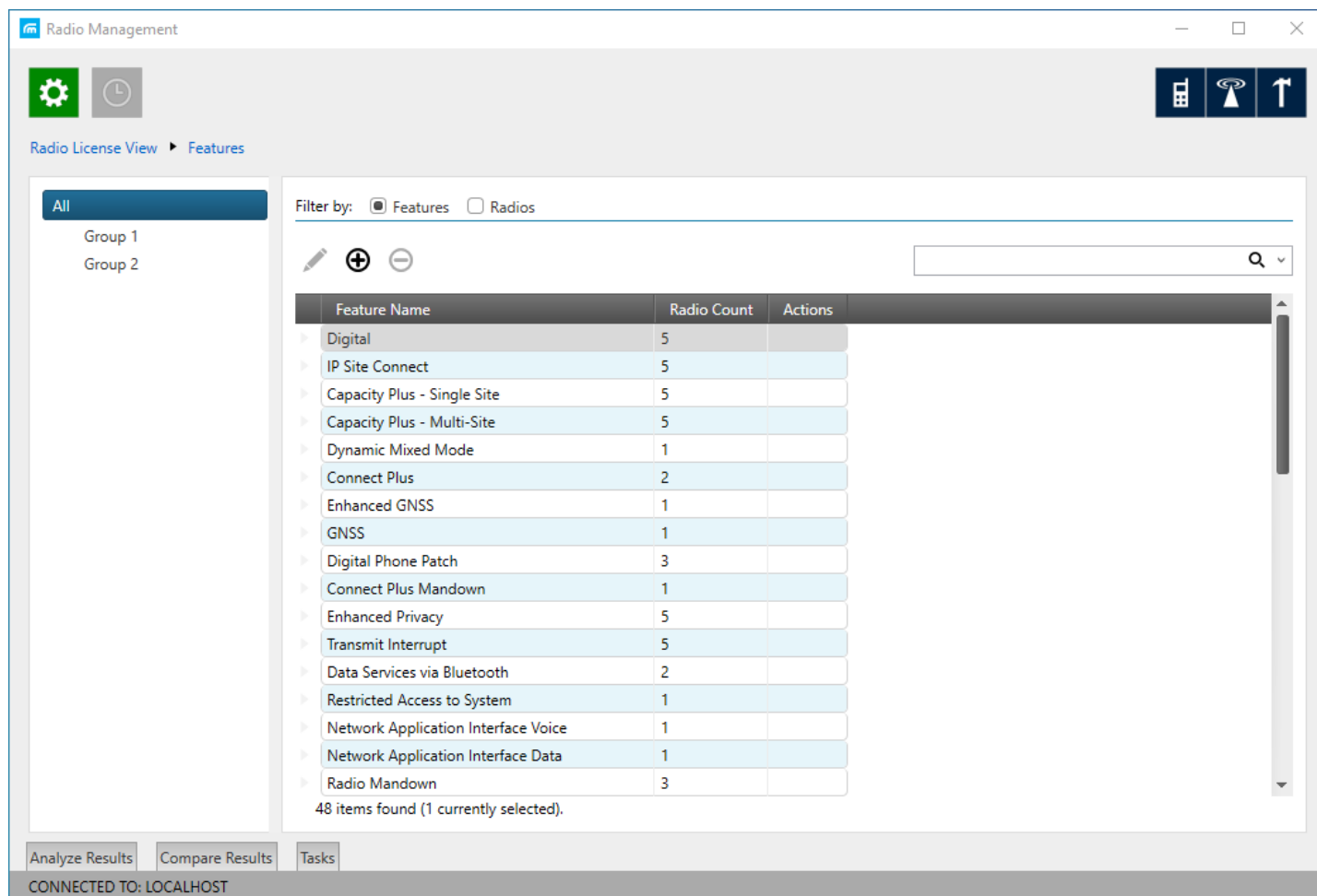
- a. Create radios will add the serial number to the Radio View list.
- b. Create configurations will generate a configuration from that codeplug.
- c. Apply configuration to radio will associate the to-be-created configuration with the to-be-added radio.
- d. Always override will overwrite the previous configuration for that radio if its serial number is already in the RM Server database.
- e. Never override does the opposite to always override.

If a password is used, enter it here. Also see the section titled [Cybersecurity](#). Regarding codeplug passwords.

6. If you choose to export.
7. You can only export one radio/repeater at a time. To export a radio, you first need to select it from the list in Radio View.
8. If you select export, you will be prompted to choose a location for the file. RM will only export the data as an .xpba file - this can be edited in CPS2 or imported into another RM instance.
9. Enter a filename and click OK.

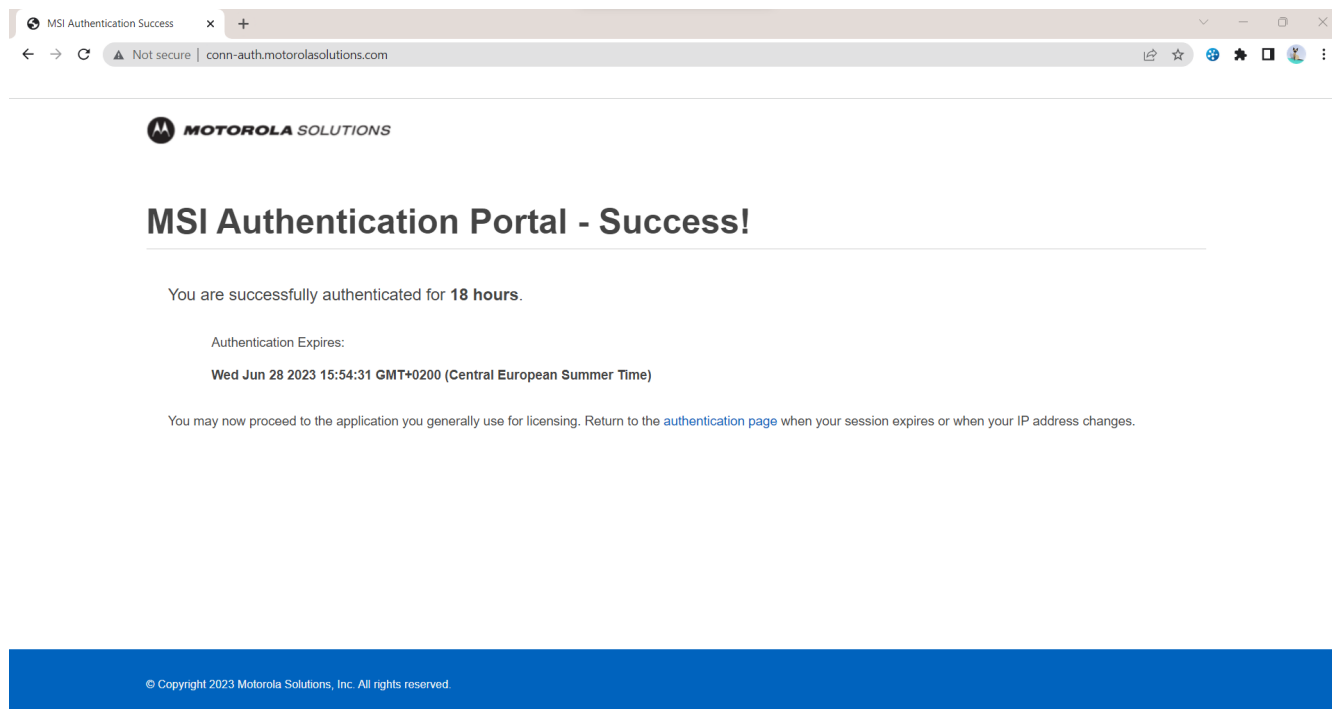
Making changes to a radio in CPS2 and writing this will require you to read the radio once more to synchronise the status.

## Adding or Restoring Licences

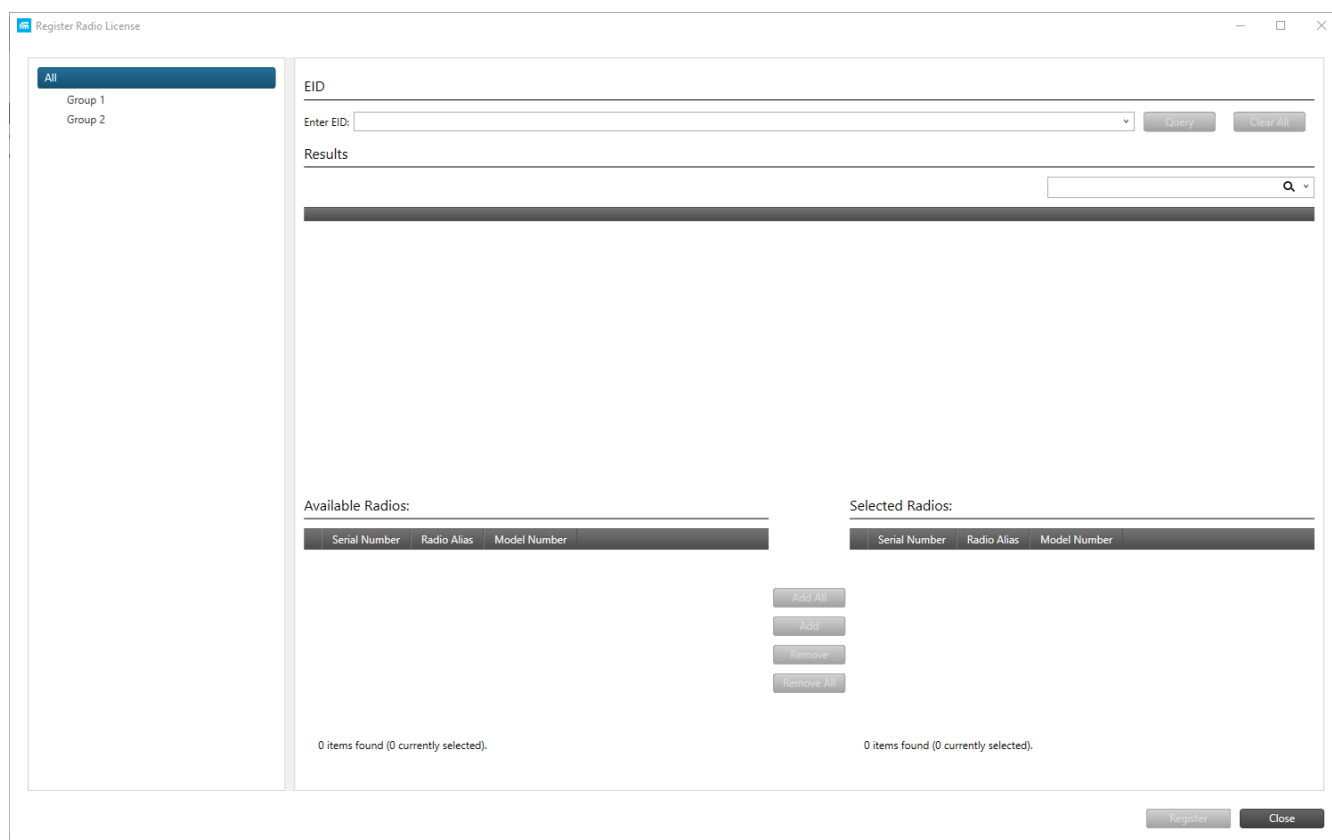


To add a feature licence to a radio or repeater:

1. Click Actions ⚙; Manage; Licences; Radio Licences. This brings you to a table which lists all the available licences and how many devices have them - as shown above. If you select Radios, the view switches to a list of radios and how many features are in each.
2. To register a feature licence, the PC on which Radio Management Client is running on, needs internet access. You will also need to have a browser window open.
3. In the web browser, go to <https://connect.motorolasolutions.com> and log in using your username and password. The username is the same you would use to access PartnerHub, LXP etc. If you work for a company who is not a Motorola Solutions channel partner, you need to contact your reseller to help you with this - see [If you need help](#).
4. Once logged in you should see the below page.



5. Go back to Radio Management Client and click on the ⊕ Add button at the top of the Radio Licence View window. This will bring up the below window.



6. Enter the supplied Entitlement ID (EID) in the EID field at the top of the window. To avoid mistakes, it is better to copy-paste this from the email. Once you've entered the EID, click on the Query button - which will be ungreyed.
7. The licences which are available on the supplied EID will be shown in the results table. Click on the licence you wish to register and enter the required quantity of licences you'd like to register.
8. Below that, the Available Radios table will become populated. Only radios which can support that feature will be listed.
9. Select the radios which you'd like to associate with that feature licence and click Add. You can Add All if you want to register all of them.
10. Once you are happy click on Register.
11. If the registration was successful, you can now go back to Radio View. Here you will notice that the Tan (Beige) block in the Modified column is shown next to the radio(s) which you activated that feature for.
12. You now need to schedule a write job for that (those) radio(s). This is a standard write job process as described in [Writing the radio\(s\) using OTAP](#) and [Making updates to repeater codeplugs via IP](#).

In some cases, when you've done a device recovery in CPS, the feature licences can disappear. This can also happen on a repeater if you've swapped out the modem board. If this ever happens, do the following:

1. If you haven't already, in your web browser, go to <https://connect.motorolasolutions.com> and log in using your username and password. The username is the same you would use to access PartnerHub, LXP etc. If you work for a company who is not a Motorola Solutions channel partner, you need to contact your reseller to help you with this - see [If you need help](#).
2. Once logged in you should see the successfully authenticated page as shown above (step 4).
3. In Radio Management Client, go to Actions ⚙, Settings and click on Licences. Then click on the Recover button next to Radio Licences (this applied to repeaters too).
4. If the recovery was successful, you can now go back to Radio View. Here you will notice that the Tan (Beige) block in the Modified column is shown next to the radio(s) on which you recovered those licences.
5. You now need to schedule a write job for that (those) radio(s).

If you have a firewall that blocks all internet access, you will need to ask your IT department to unblock TCP port 443 for sites [connect.motorolasolutions.com](https://connect.motorolasolutions.com) and [licensing.motorolasolutions.com](https://licensing.motorolasolutions.com).

## Upgrading Firmware

Upgrading radio or repeater firmware in Radio Management is a little different to CPS:



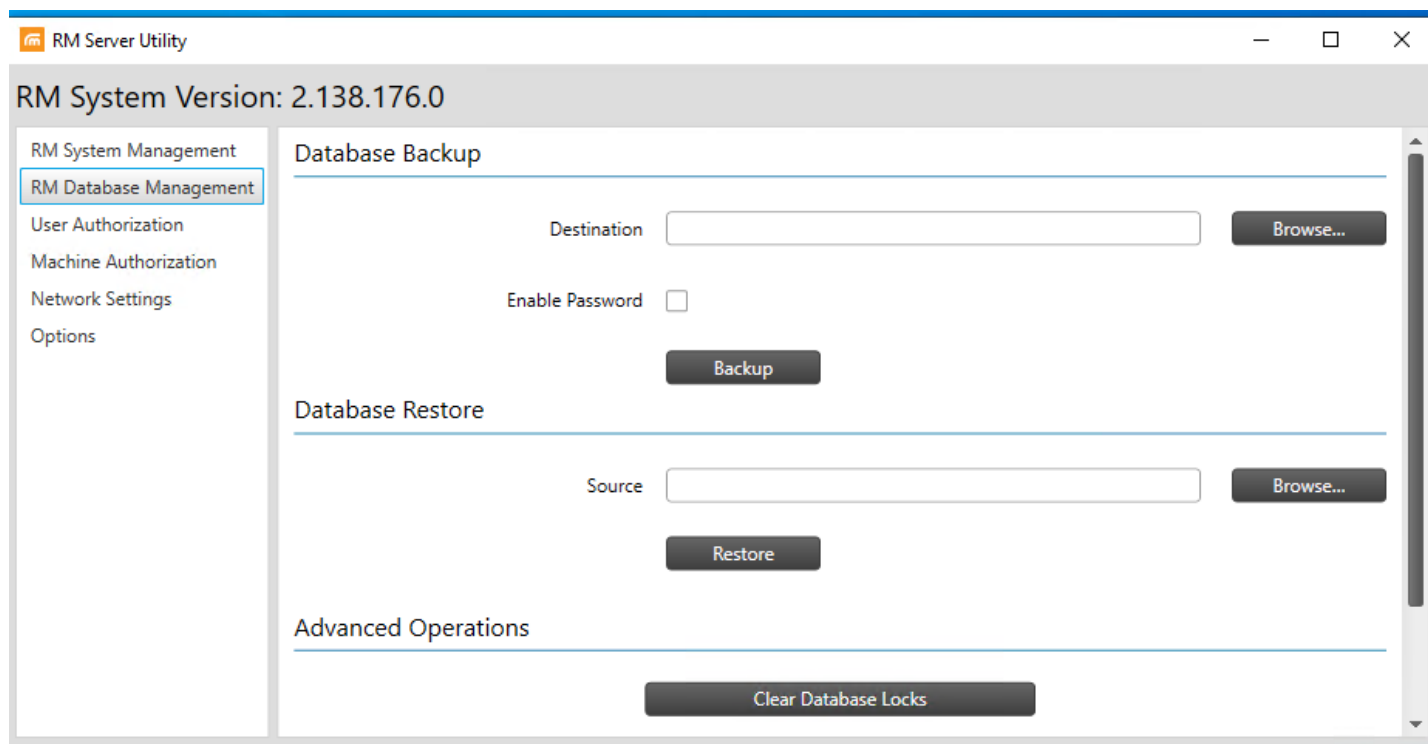
1. You need to download and install the firmware packs.
2. These must be imported into Radio Management. My suggestion is to install the firmware on the server and use the RM client to install them on the server using remote desktop. Importing firmware from a remote client means that the firmware files are copied across the network to the server - for the DP4000e series that can be as big as 1GB!
3. In Radio View you would first Upgrade the firmware - right-button click then select the firmware package you'd upgrade the radio or repeater to.
4. The green block in the Modified column will now be visible.
5. You then need to schedule a write job, either via USB or WiFi (or IP if it's a repeater).

It is not possible to upgrade firmware via OTAP. You can upgrade radios via Wi-Fi but I've never tried it. Repeaters can be upgraded via IP. Be careful with firmware upgrades - there is a small chance you could brick the radio if power is lost.

## Other important stuff

### Making Backups

It is important that you make regular backups of the database. This cannot be done using any of the scheduling tools in Windows. If running Windows and RM in a VM, you can schedule a snapshot. I also recommend keeping a copy of the installer somewhere just in case.



The screenshot shows the 'RM Server Utility' window. The title bar indicates 'RM System Version: 2.138.176.0'. On the left is a sidebar menu with the following items: 'RM System Management', 'RM Database Management' (which is highlighted with a blue border), 'User Authorization', 'Machine Authorization', 'Network Settings', and 'Options'. The main content area is divided into three sections: 1. 'Database Backup' which contains a 'Destination' text box with a 'Browse...' button to its right, an 'Enable Password' checkbox, and a 'Backup' button. 2. 'Database Restore' which contains a 'Source' text box with a 'Browse...' button to its right, and a 'Restore' button. 3. 'Advanced Operations' which contains a single 'Clear Database Locks' button.

To make a backup in RM, go to RM database management in the Server Utility. Click browse to find the place where you want to store the backup files and click backup. Optionally, you can add a password but if you do, be sure to keep that somewhere safe.

## **Access Control**

Access Control (a.k.a. Role Based Access) in Radio Management has nothing to do with the term [RBAC](#) used in computer systems - though the end result bears some similarity. What Access Control in Radio Management attempts to do, is to restrict access to certain parameters on a per-user basis.

Access Control does not support multi-factor authentication (2FA) but does support some level of Active Directory integration.

Access Control cannot restrict access to down to fields within a set.

Historically, access to Radio Management was by means of a username and password. With these credentials, a user was able to access all information in the database.

Access Control supports four levels of access:

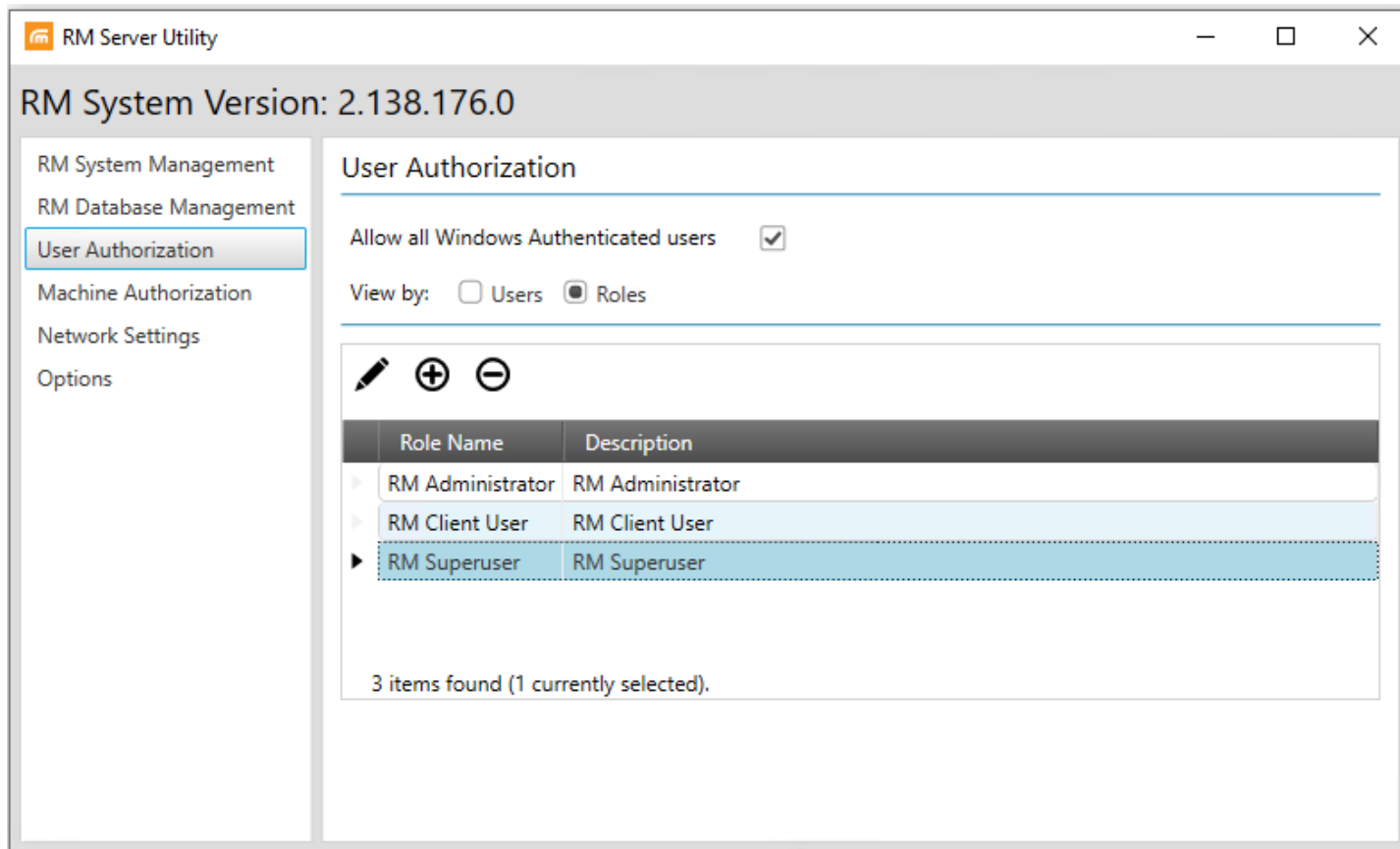
Level 0 authenticates users and roles. This is managed in the RM Server. To manage the other levels one needs to be logged in as an administrator.

Level 1 controls view or modify access to Radio Management-wide parameters such as keys at a table level.

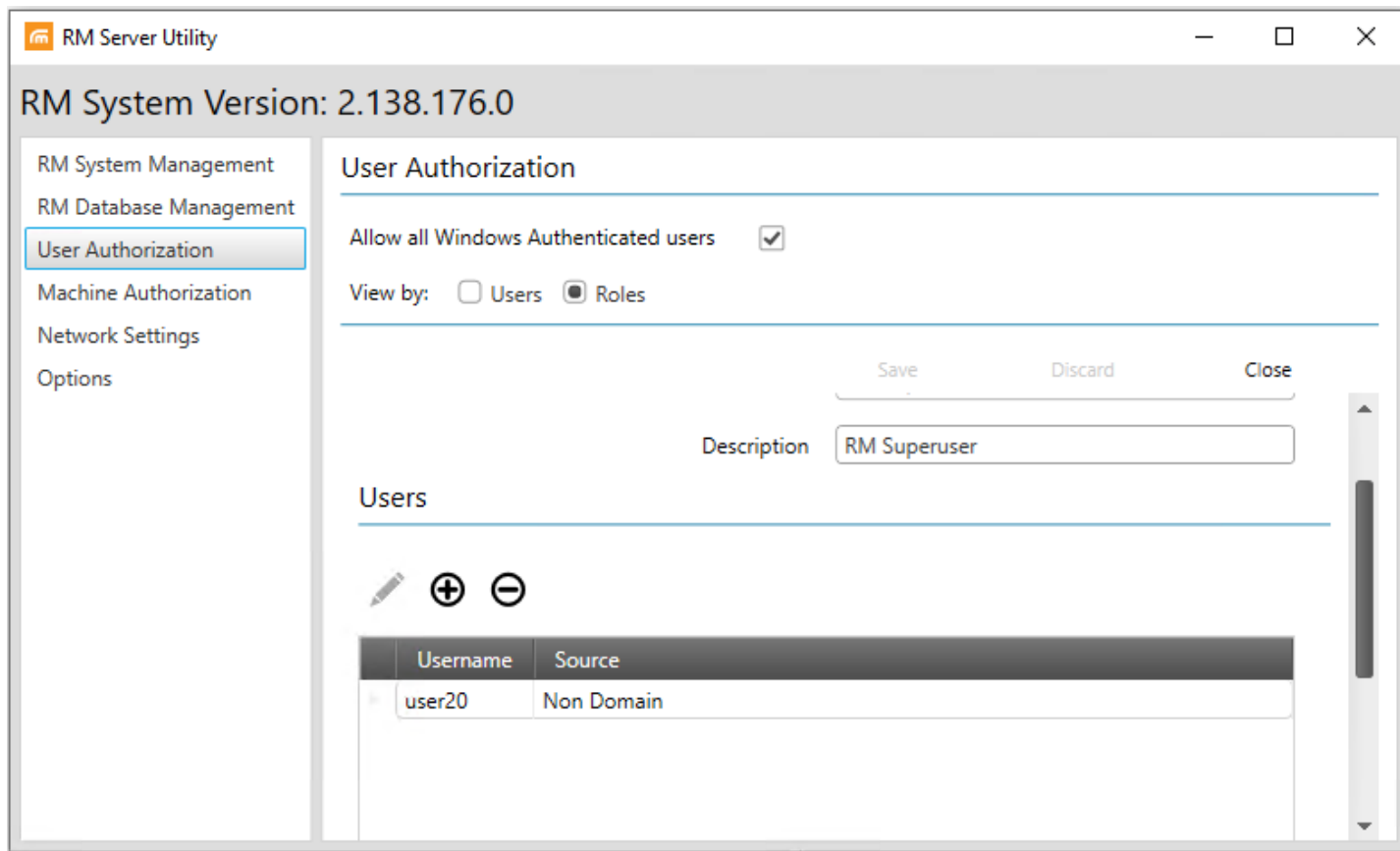
Level 2 allows users to view and modify radios and devices they have permissions for.

Level 3 allows view or modify access to configurations and sets.

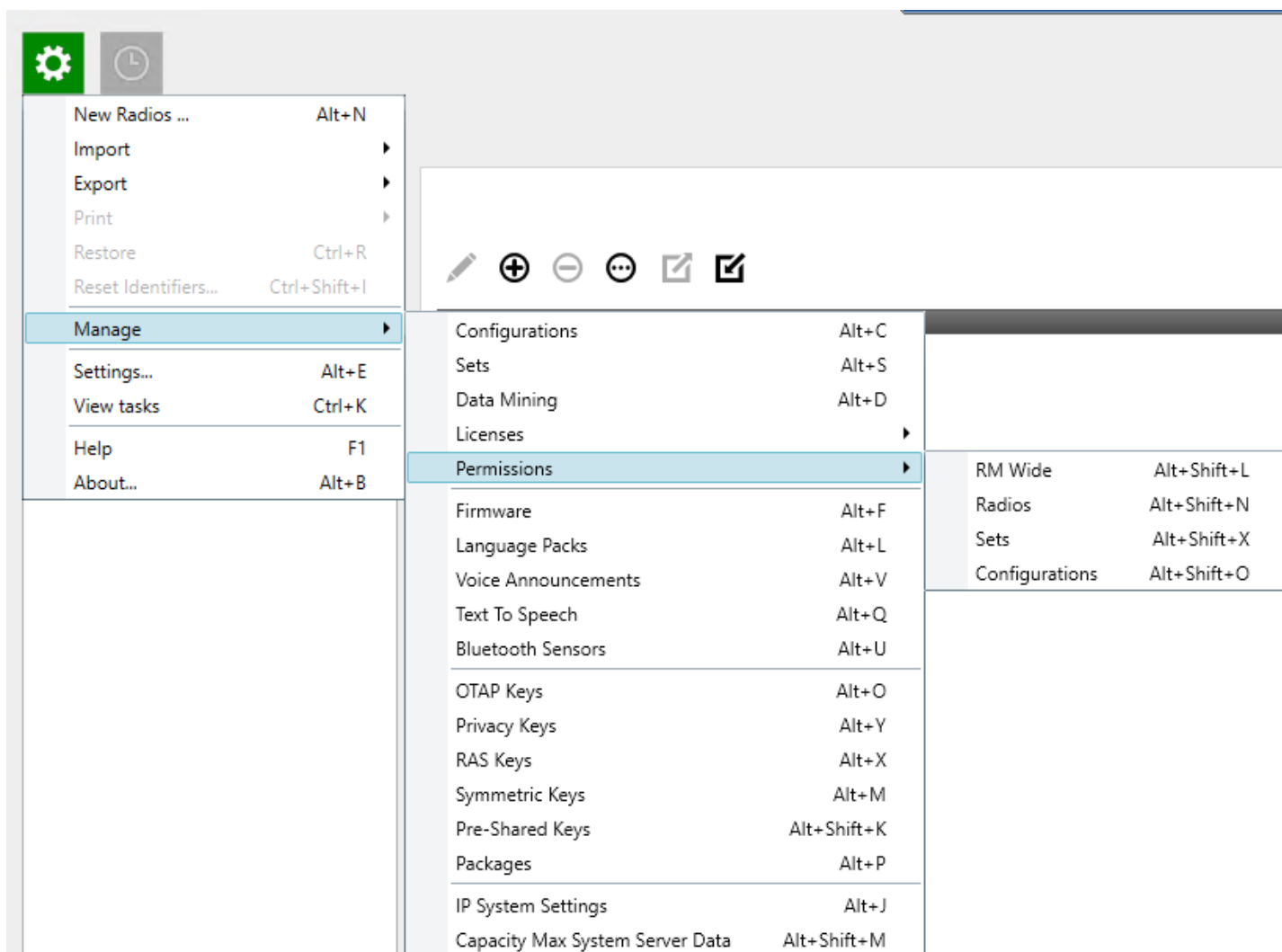
To configure role based access:



Begin by creating additional roles for each user type in the RM Server Utility. RM Client User and RM Administrator are both built-in roles. I have added RM Superuser. To get to this view make sure Roles is selected.



Then edit (✎) that role and add the required users to it by means of the (+) add button. Make sure that the user only has one role otherwise the role with the higher level of permissions may apply.



Then in Radio Management Client, access the Permissions menu by clicking on the Actions button: Manage and then Permissions. From here you are able to manage access to the following:

- RM Wide. Included here are all the keys. A role can be given view or modify access to these parameters.
- Radios. Included here is what one would see in Radio View and would include things like Radio IDs and aliases. A role can be given view or modify access to these parameters.
- Sets. This refers to
- Configurations

**Add Permissions** [X]

Role

Resource

- ☐ Symmetric Keys
- ☐ Privacy Keys
- ☐ RAS Keys
- ☐ OTAP Keys
- ☐ Pre-Shared Keys

Permission

- ☐ View
- ☐ Modify

OK Cancel

To link a role to specific permissions, click the Add (+) button. In some cases, you will need to do this from the Radio or Configuration View.

## What if Access Control is of no interest to you?

1. Open the RM Server Configuration utility.
2. Click on User Authorization.
3. Make sure that Roles is selected (radio button at the top)
4. Delete all roles except RM Administrator and RM Client User.
5. Now select Users (radio button at the top).
6. Make sure that each user has RM Administrator and RM Client User roles assigned to them.

## Cybersecurity.

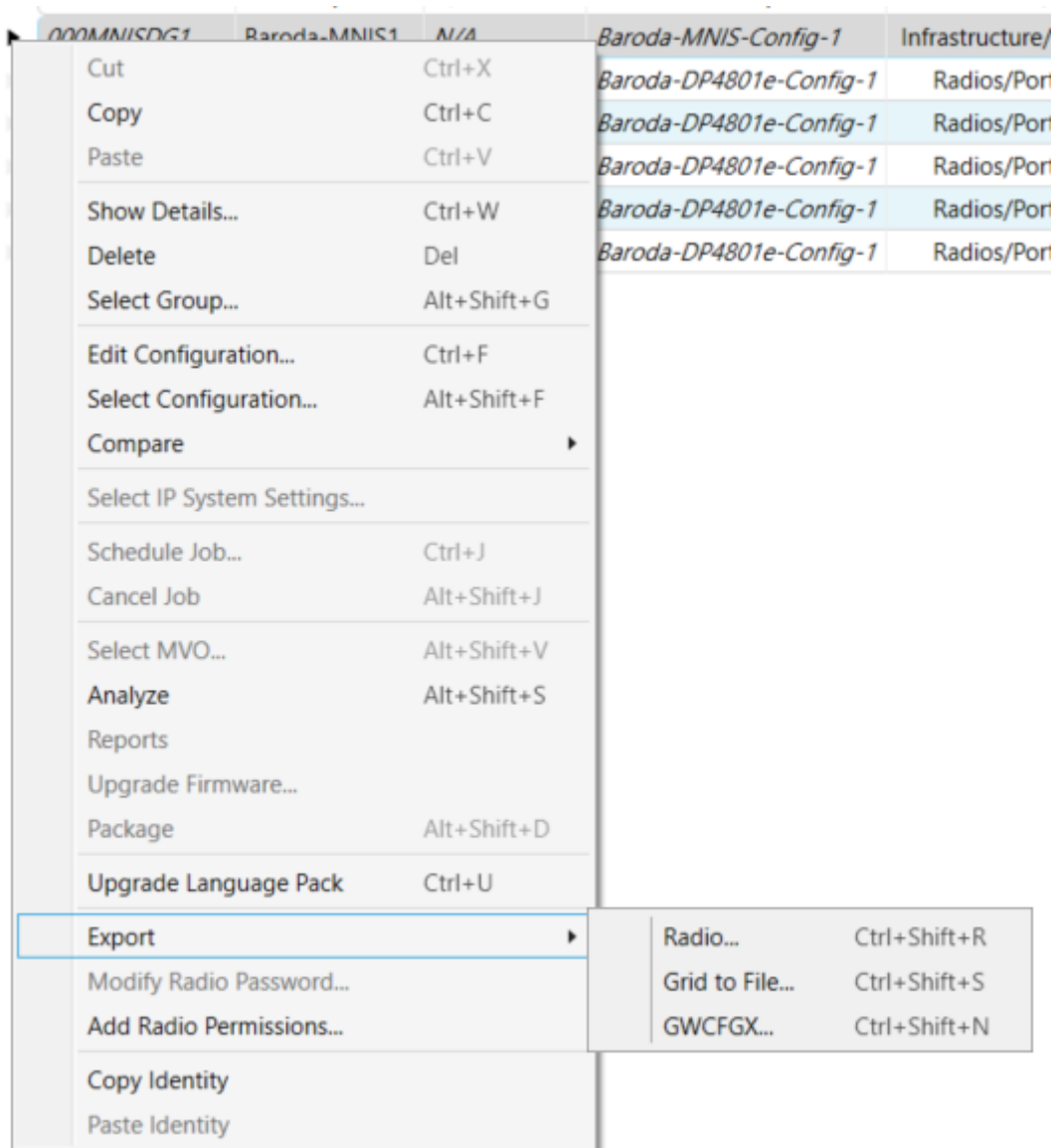
I am not a cybersecurity expert. This document only deals with cybersecurity as far as MOTOTRBO Radio Management goes - not the whole radio system.

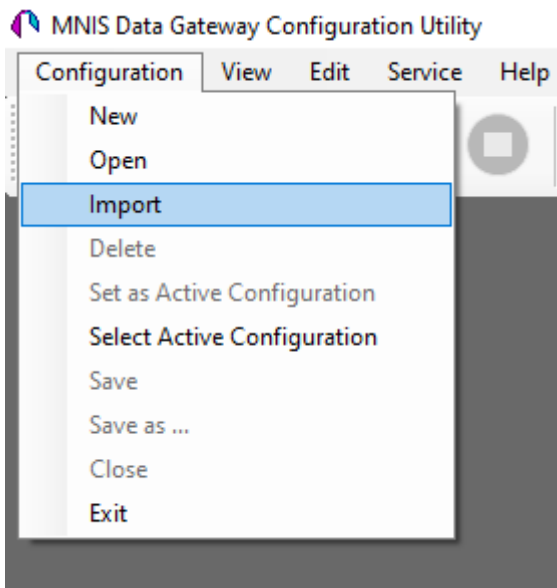
If this is a grey area for you, I suggest getting a Managed Service provider to provide you with some guidance on cybersecurity. The trouble with MSPs, is that they have no idea of radio - this is not their fault - but you should still listen to what they say. You can refer them to this document if it helps.

## Stuff to take note of for Capacity Max

You can only OTAP radios via the MNIS Data Gateway.

The MNIS Data Gateway is created and edited in Radio Management then exported as an .GWCFGX file and imported into MNIS (shown below).

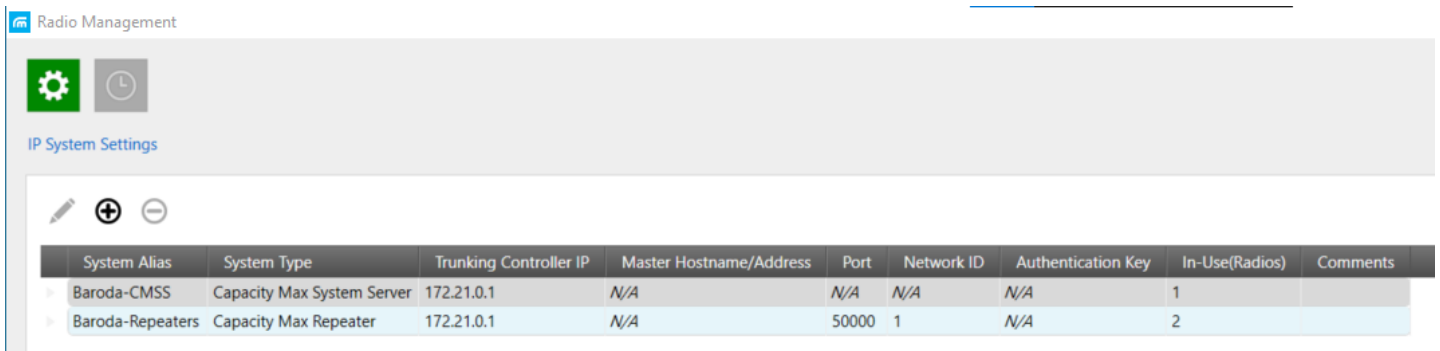




It is not possible to read the configuration data from a CMSS. You can read it but you will only get the MVO data. The CMSS is created and edited in Radio Management and written via IP.

When adding a CMSS to RM, use the HP serial number and not the Motorola 435\_\_\_\_\_ serial number. You can use the latter as an alias or put it in the comments but the HPE serial number is what the CMSS will send to the Device Programmer using DNS-SD.

In order to read or write the CMSS, you must add one Capacity Max System Server IP System Setting entry per CMSS.



All configuration of the CMSS is done with Radio Management. The only exception is adding user accounts to System Advisor using the web interface and JRE.

A Capacity Max system can support one primary and up to 4 alternate CMSSes per system. Each CMSS hosts three services (trunking controller; Voice and Radio Control Gateway and System Advisor), each of which can be configured to run as a primary or alternate on each of the CMSSes.



In order to IP Remote Program repeaters, you need to add one Capacity Max Repeater IP System Setting per system (network ID). If this Radio Management instance will only be managing one MOTOTRBO Capacity Max system, then you only need one for all repeaters.

### Some (maybe) useful information

Auto Add and Configure Devices in RM

Device Type	Allow Auto Add Radios	Template Mode	Configuration Mode	Auto Read Radios	Generate Configuration	Apply To Radio
Android	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
APX	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
MOTOTRBO	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Apply

In the RM Server Utility, under Options is a checkbox matrix that allows you to have Radio Management automatically add radios as soon as they are seen by any one of the Device Programmers. Optionally, you can have Radio Management read that radio and generate a configuration. This is really useful if you have to add many radios and don't have their serial numbers.



Serial Number	Radio Alias	Caller A
MY0547056R	Baroda-CMSS	N/A

Radio Management client also allows you to import serial numbers from a spreadsheet by pressing the import button (right). To get an idea of how the spreadsheet should be formatted, you can export whatever is in Radio View. The file format is CSV (comma delimited).

### Using Radio Management for multiple systems and customers

One of the misconceptions about MOTOTRBO Radio Management is that you need one instance per customer. While this might be true for customers who want to have everything on-premise, it does not apply to every system you deploy.

Another misconception is that you can/should only use Radio Management in conjunction with OTAP and/or high titer models. While OTAP does solve many headaches of going to site with a laptop and cable, you can use Radio Management for older and current radios which didn't/don't support OTAP.

The above diagram shows a Radio Management setup that allows you to manage the configuration of several customers from a single Radio Management server. Three customers are shown here. A; B and C. There is a Device Programmer host at each site. This does not have to be a high-power PC - something like a NUC will work fine.

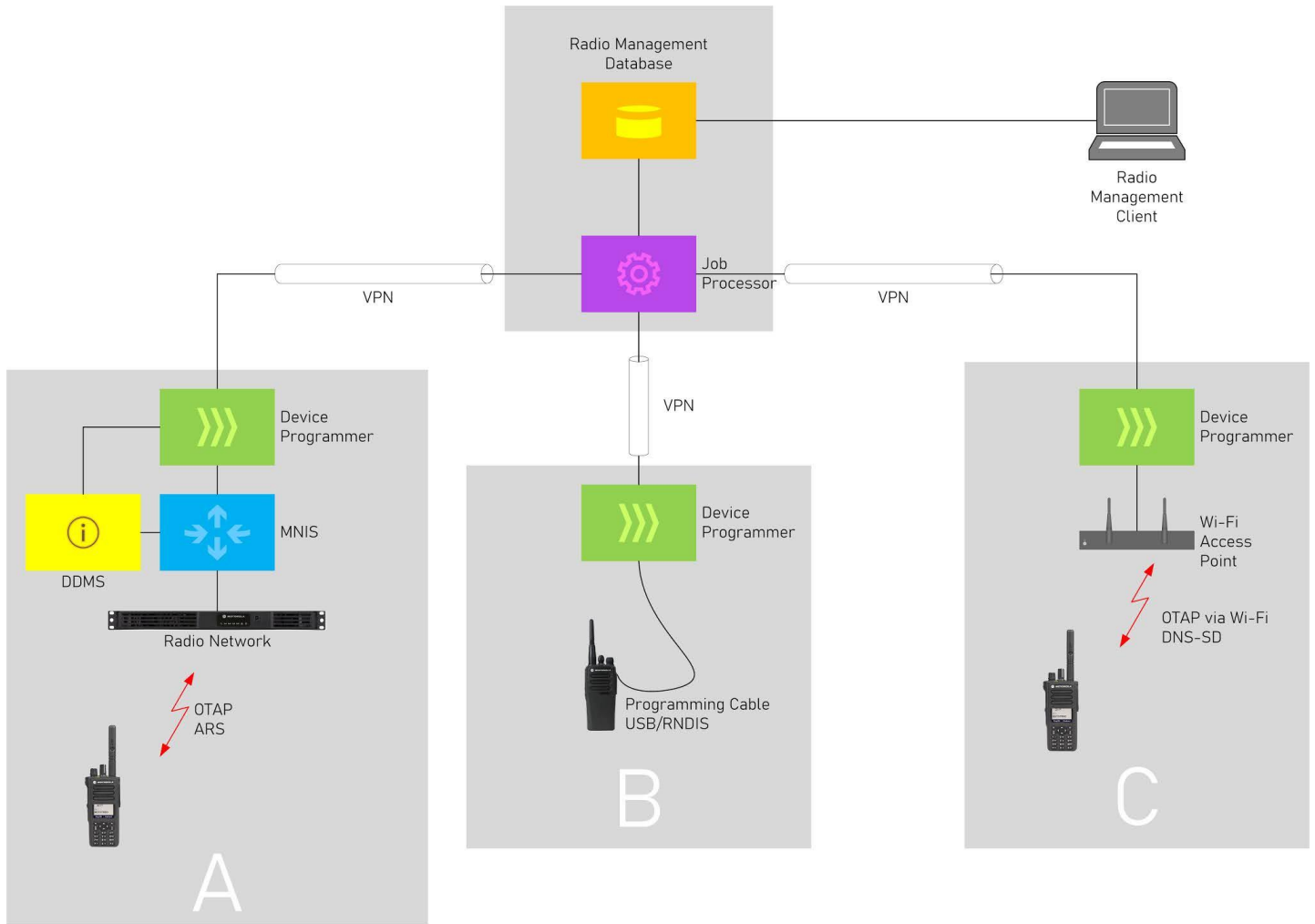
The setup at customer A uses MNIS and NAI. Because of this, DDMS is needed to inform Device programmer about the status of each radio. DDMS and MNIS could be installed on the same PC as Device Programmer. Programming is achieved here via OTAP using the radio channel(s).

The setup at customer B allows radios which do not support OTAP to be programmed. This customer would only need a PC onto which Device programmer is installed. The customer could also be shown how to connect the radios to the PC to download the configuration (potentially saving you a trip to site).

The setup at customer C uses Wi-Fi. This setup might be useful for getting new radios onto the system if the Access Point is set up with the default SSID and passcode in new radios.

The Device Programmer at each site will need some configuration and you will need to organise the information in your Radio Management Database.

Radio Management allows you to define folders and subfolders into which you can arrange different radios. In the below screenshot, we can see customer A; B and C. The radios (and repeaters) at customer B are then arranged by department and group - or whatever you choose!



## Multiple Device Programmers and Groups

**Groups**

- All
- Group 1
  - Team A
  - Team B
- Group 2
  - Team C
  - Team D
- Group 3
  - Team E
  - Team F

Serial Number	Radio Alias	Caller Alias	Configuration	Group
871TSVV255	Prod 1	N/A	ACME_DP4801e_Config_1	Group 1/Team A
865TYB6023	Prod 2	Wayne DJ0WH	ACME_R7FKP_Config_1	Group 1/Team B
038THC2312	CS 100	N/A	ACME_DM3601_CS	Group 2/Team C
478ITC1500	Motorola	N/A	ACME_SLR_IPSCMaster	Group 2/Team D
734TWX0298	Wayne 2	N/A	ACME_IONConfig_1	Group 3/Team E

MOTOTRBO Radio Management allows radios to be grouped together. To add groups, right-button click in the Groups column on the right-hand side of Radio View (see above). You can even create nested groups (e.g. Team A and B in Group 1). Each group can be given a name and you can add a radio to any of these groups.

For example, radios Prod 1 and Prod 2 (radio Alias column) are part of Group 1 but prod 1 is part of Team A - which is also part of Group 1. Clicking on Group 1 will display only these two radios since the others are members of other groups. Clicking on Team A will only display Prod 1.

These groups also serve another purpose! If you have multiple Device Programmers, you can configure each to only handle radios from a specific group.

Settings

### Motorola Device Programmer Settings

#### RM Server

Address

Port

Authentication Method

**Test Connection**

#### Device Communication Method

Communication Method ☒ USB ☐ Wireless (LAN) ☒ Over The Air  
☐ IP Program

#### Device Discovery and Authentication

DNS-SD Listening Port

Device Discovery Server Name *cwh050-hpzb15g4*

Device Discovery Server IP *192.168.0.250*

#### Radio Group

Assigned Radio Group  **Updating Success**

#### PN Server

Use PN Server ☒

PN Server

Port

**Test Connection**

#### Job Settings

**OK** **Cancel**

In the above example, this Device programmer will only process jobs for radios in Group 1.

**Motorola Device Programmer Settings**

**RM Server**

Address: localhost

Port: 443

Authentication Method: Certificate

Test Connection

**Device Communication Method**

Communication Method: ☒ USB ☐ Wireless (LAN) ☐ Over The Air

☒ IP Program

**Device Discovery and Authentication**

DNS-SD Listening Port: 5353

Device Discovery Server Name: cwh050-hpzb15g4

Device Discovery Server IP: 192.168.0.250

**Radio Group**

Assigned Radio Group: Group 2/Team D Updating Success

**IP Program Settings**

**Common**

Minimum TCP Port: 50000

Maximum TCP Port: 50100

Local UDP Port: 20000

**Link Establishment**

OK Cancel

In the above example, this Device Programmer will only process jobs for repeaters in Group 2 Team D. Note that since this is a repeater, only USB and IP program are selected as the Device Communication Methods.

If you have multiple Device Programmers you can have concurrent jobs running: you just need to increase the Concurrent Jobs setting in the Job Processor Settings.

## Upgrading Radio Management

It is important to make sure no radios are being written before starting the update.

To upgrade Radio Management, do the following:

1. Back up the existing database (as a safety precaution). Make a note of the old version and make sure you still have the installer for that.
2. Install the new version of Radio Management. Do not uninstall. Radio Management will update the database as part of the update.

During the upgrade, Radio Management will become unavailable and any ongoing read or write jobs will fail. It is therefore important to make sure no radios are being written before starting the update.

## Upgrading from Radio Management 1.x to 2.x

When Radio Management was introduced in 2012(?), the CPS was used as the client. The server also made use of so-called templates that were based on codeplugs - that is one or more radios shared a common template. This was known as *template mode* or *Radio Management R1.x*.

The probability that there are deployments out there, still using Radio Management 1.x, is probably very small - but not zero. The important point is that Radio Management 1.x is no longer supported and, if you have a deployment like this, you need to upgrade.

When running the installer, you will get prompted to check whether the existing database contains any template-mode data, if there is, you will have the opportunity to convert these into configuration-mode entries.

There is a certain way to upgrade from Radio Management R1.x to Radio Management R2.x. Backing up the database; uninstalling the old version of Radio Management then installing the new version won't work because the backed up database was not upgraded. When trying to restore, you'll get an error message or one of the SQL services will keep on stopping.

While the data in the Radio Management system is being upgraded, RM will not be available for configuring radios and depending on how many radios and templates there are, RM may be unavailable for a significant amount of time while the upgrade takes place.

In order to upgrade the data elements to RM 2.x, there must be sufficient free disk space - in addition to that used by RM. Also make sure that there are no pending or incomplete jobs - if any are pending wait until they are complete or cancel if you can.

But before upgrading, it makes good sense to perform a backup just in case.

If all the RM 1.x components are installed on the same machine, run the RM 2.x setup as normal. When you start Radio Management from within the CPS, you will be prompted to begin the upgrade process.

If RM 1.x Server is installed on a separate machine (separate from the other RM components) then only install RM Server and Auto Update on the RM Server machine.

Then install the CPS on the computers on which access the RM Server. The user will be prompted to perform the upgrade process when they access RM through CPS on any of these computers. Once the upgrade is complete, only one RM Client (CPS) should connect to the RM Server

On machines where the Device Programmer is installed, simply install the updated Device Programmer without any further actions.

## **Troubleshooting**

### **Client won't connect to the Server**

If you cannot connect to the Radio Management Server from the Radio Management Client, check the following:

- ☐ Do you get prompted to enter your username and password? If no, then you have a connectivity problem. Try pinging the server.
- ☐ Are you able to ping the server? If ping fails then you need to check your connection to the server. Work from your PC towards the server.
- ☐ Is the clock and timezone correct on both computers? Radio Management uses SSL to establish a secure connection. This is reliant on having an accurate time reference so check the time on the server and on your PC, the minute and second value must be the same.
- ☐ Is TCP port 443 unblocked on inbound and outbound in Windows Defender Firewall? To verify, try disabling Windows Defender Firewall temporarily. If you can connect when the firewall is down, you need to check the above setting.

### **Device Programmer won't connect to the Server**

If you cannot connect to the Radio Management Server from the Device Programmer, check the following:



- ☐ Are you able to ping the server? If ping fails then you need to check your connection to the server. Work from your PC towards the server.
- ☐ Is the clock and timezone correct on both computers? Radio Management uses SSL to establish a secure connection between the server and DP. This is reliant on having an accurate time reference so check the time on the server and on the DP host, the minute and second value must be the same.
- ☐ Is TCP port 443 unblocked on inbound and outbound in Windows Defender Firewall? To verify, try disabling Windows Defender Firewall temporarily. If you can connect when the firewall is down, you need to check the above setting.