



# **IMPRES<sup>™</sup> Battery Fleet Management Troubleshooting Guide and External Software and Component Configuration Guide**

**FEBRUARY 2022**

© 2022 Motorola Solutions, Inc. All rights reserved



**MN007501A01-AB**

# Intellectual Property and Regulatory Notices

## Copyrights

The Motorola Solutions products described in this document may include copyrighted Motorola Solutions computer programs. Laws in the United States and other countries preserve for Motorola Solutions certain exclusive rights for copyrighted computer programs. Accordingly, any copyrighted Motorola Solutions computer programs contained in the Motorola Solutions products described in this document may not be copied or reproduced in any manner without the express written permission of Motorola Solutions.

No part of this document may be reproduced, transmitted, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without the prior written permission of Motorola Solutions, Inc.

## Trademarks

MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.

## License Rights

The purchase of Motorola Solutions products shall not be deemed to grant either directly or by implication, estoppel or otherwise, any license under the copyrights, patents or patent applications of Motorola Solutions, except for the normal non-exclusive, royalty-free license to use that arises by operation of law in the sale of a product.

## Open Source Content

This product may contain Open Source software used under license. Refer to the product installation media for full Open Source Legal Notices and Attribution content.

## European Union (EU) and United Kingdom (UK) Waste of Electrical and Electronic Equipment (WEEE) Directive



— The European Union's WEEE directive and the UK's WEEE regulation require that products sold into EU countries and the UK must have the crossed-out wheeled bin label on the product (or the package in some cases). As defined by the WEEE directive, this crossed-out wheeled bin label means that customers and end-users in EU and UK countries should not dispose of electronic and electrical equipment or accessories in household waste.

Customers or end-users in EU and UK countries should contact their local equipment supplier representative or service centre for information about the waste collection system in their country.

## Disclaimer

Please note that certain features, facilities, and capabilities described in this document may not be applicable to or licensed for use on a specific system, or may be dependent upon the characteristics of a specific mobile subscriber unit or configuration of certain parameters. Please refer to your Motorola Solutions contact for further information.

© 2022 Motorola Solutions, Inc. All Rights Reserved

# Read Me First

This manual contains information about ASTRO Over-the-Air IMPRES™ Battery Fleet Management and how to use the system.

# Notations Used in This Manual

Throughout the text in this publication, you will notice the use of warning, caution, and notice notations. These notations are used to emphasize that safety hazards exist, and due care must be taken and observed.



**WARNING:** WARNING indicates a potentially hazardous situation which, if not avoided, could result in death or injury.



**CAUTION:** CAUTION indicates a potentially hazardous situation which, if not avoided, might result in equipment damage.



**NOTE:** NOTICE indicates an operational procedure, practice, or condition that is essential to emphasize.

# Contents

<b>Intellectual Property and Regulatory Notices.....</b>	<b>2</b>
<b>Read Me First.....</b>	<b>3</b>
<b>Notations Used in This Manual.....</b>	<b>4</b>
<b>Related Publications.....</b>	<b>7</b>
<b>Chapter 1: General Troubleshooting.....</b>	<b>8</b>
1.1 Common Solutions.....	8
1.2 Client PC is Unable to Connect to the Server PC.....	8
1.3 Unable to Activate Software.....	9
1.4 Database Error Messages.....	10
1.4.1 Fixing Retrieving Data Failure.....	11
1.4.2 Fixing Analysis Service Connection.....	12
1.5 ASTRO OTABM Network or Application Configuration Problem.....	13
1.6 ASTRO OTABM Application Configuration Problem.....	13
1.6.1 Troubleshooting Procedures.....	14
1.7 Contacting Service Team.....	14
<b>Chapter 2: Firewall Configuration.....</b>	<b>15</b>
2.1 Configuring Firewall.....	15
2.2 Enabling Windows Firewall to Accept Messages From UDP Ports (MOTOTRBO OTA).....	17
<b>Chapter 3: IMPRES Gen 2 Charger Drivers Manual Installation.....</b>	<b>24</b>
3.1 Installing IMPRES Gen 2 Charger Drivers Manually (Method 1).....	24
3.2 Installing IMPRES Gen 2 Charger Drivers Manually (Method 2).....	25
<b>Chapter 4: Generate License for Offline Activation.....</b>	<b>30</b>
4.1 Creating an Account.....	30
4.2 Creating the License .BIN from the HOST ID File.....	31
4.2.1 Generating License Successfully.....	34
<b>Chapter 5: Database Backup.....</b>	<b>36</b>
5.1 Backing Up the Database.....	36
<b>Chapter 6: Restrictions on Windows Domains for BFM Client-Server Connections.....</b>	<b>39</b>
<b>Chapter 7: Enable ASTRO Over-The-Air Battery Management (OTABM) Feature.....</b>	<b>40</b>
7.1 Intelligent Middleware (IMW) Overview.....	40
7.2 Configuration Process for ASTRO OTA.....	41
7.3 Configuring CPS for Subscriber/Radios.....	41
7.4 IMW Provisioning.....	42

7.5 Creating a Sensor Profile.....	43
7.6 IMW Device Configuration.....	46
7.6.1 For IMW versions 5.2.2 and older.....	46
7.6.2 For IMW versions 5.2.3 onwards.....	47
7.7 IMW Representational State Transfer.....	50
7.7.1 IMW REST Setup for IMW 5.2.2 and Older.....	51
7.7.2 User Creation for IMW 5.2.2 and Older.....	52
7.7.3 IMW REST Setup for IMW 5.2.3 Onwards.....	54
7.7.4 User Creation for IMW 5.2.3 Onwards.....	54
7.7.5 IMW Associated Application.....	55
7.8 API Endpoint.....	57
7.8.1 Configuring API Endpoint.....	57
7.9 IMW Static Group.....	59
7.9.1 Configuring IMW Static Group.....	59
<b>Chapter 8: IMW SIP Domain.....</b>	<b>63</b>
<b>Chapter 9: Checking the IMW Synchronization Status.....</b>	<b>64</b>

## Related Publications

The following list contains part numbers and titles of related publications.

- MN007471A01, *IMPRES™ Battery Fleet Management Ordering Guide*
- MN007473A01, *IMPRES™ Battery Fleet Management Installation Manual*
- MN007495A01, *IMPRES™ Battery Fleet Management User Guide*
- MN007501A01, *IMPRES™ Battery Fleet Management Troubleshooting Guide and External Software and Component Configuration Guide*
- MN008435A01, *IMPRES™ Battery Fleet Management WEB Interface User Guide for Release 4.0*
- 6880309T12, *MOTOTRBO System Planner*
- MN008144A01, *Intelligent Middleware Installation and Configuration Manual 5.2.4*
- MN005566A01, *Intelligent Middleware Installation and Configuration 5.2 and 5.2.2*
- MN008145A01, *Intelligent Middleware Feature Manual 5.2.4*

## Chapter 1

# General Troubleshooting

If you encounter any issues with your IMPRES™ Battery Fleet Management software, try the following solutions:

- Ensure the Operating System (OS) used on your PC is supported. Refer to *IMPRES Battery Fleet Management Installation Manual, MN007473A01* for list of supported OS.
- Ensure the IMPRES Battery Fleet Management software is the latest version. If not, update to the latest version and verify if the same issue still exists.

### 1.1

## Common Solutions

Ensure that the three default services for the IMPRES™ Battery Fleet Management software are running.

- Select **Start→Run**
- Type `""services.msc""` and press **Enter**.
- In the Service window, ensure that the status for these services is Started.
  - Motorola IMPRES Fleet Management Analysis Service
  - Motorola IMPRES Fleet Management Device Service
  - Motorola IMPRES Fleet Management Service Proxy



**NOTE:** If user selects Web Service installation in Install Wizard dialog box, the following service runs:

- Motorola IMPRES Fleet Management Radio Network Service
  - Motorola IMPRES Fleet Management Unified Network Service
- Restart any of these default services when abnormal behavior is encountered, and restart the IMPRES Battery Fleet Management software.

### 1.2

## Client PC is Unable to Connect to the Server PC

When Client PC is unable to connect to the Server PC, try the following solutions.

### Procedure:

- 1 Change the Server Address/Port. Ensure that the IMPRES Battery Fleet Management software is running as administrator so that the changes take effect.
- 2 Ensure that all Server and Client PC is installed with the latest version of IMPRES Battery Fleet Management software to avoid any incompatibility issue (example: different database structure).
- 3 If IMPRES™ Battery Fleet Management services used for Server or Client setup are blocked by the PC windows Firewall, refer to the *Setting up Server/Client Environment* section in the *IMPRES Battery Fleet Management Installation Guide* document to allow IMPRES Battery Fleet Management through windows Firewall.



### 1.3

## Unable to Activate Software

**Prerequisites:** When encountering activation issues, try the following solutions.

- 1 Ensure that the latest version of IMPRES Battery Fleet Management software is installed.
- 2 Activate the IMPRES Battery Fleet Management software using Offline Activation if Online Activation failed.
- 3 If Online or Offline activation fails, or activation successful but fails during the next IMPRES Battery Fleet Management software startup, perform the following steps:

**Procedure:**

- 1 Close the IMPRES Battery Fleet Management software.
- 2 Set **Folder Options** setting to **show hidden files**.
- 3 Go to `C:\ProgramData\IsolatedStorage` and delete everything in the folder.
- 4 Relaunch IMPRES Battery Fleet Management software.
- 5 Redo the activation.



**NOTE:** Do not delete this folder if there are no issues pertaining to activation.



**NOTE:** Running the IMPRES Battery Fleet Management application on a Virtual Machine with a dynamic physical MAC address can cause the application to lose activation. Configure the Virtual Machine with a static or a manual physical MAC address to run the IMPRES Battery Fleet Management application on a Virtual Machine.



**NOTE:** Running the IMPRES Battery Fleet Management application on a PC that has Wi-Fi as its primary NIC could cause loss of activation if the Wi-Fi is set to **RANDOMIZE** the MAC Address. To run the IMPRES Battery Fleet Management application on a PC that has Wi-Fi as its main NIC, ensure that **RANDOM MAC Address** is turned off in the Wi-Fi Settings.

**Postrequisites:** If activation issues persist, provide the following information to the service team:

- PC Operating System (example: Windows™ 10 Pro-64-bit)
- IMPRES™ Battery Fleet Management software version and region (example: FM V3.5)
- Customer Entitlement ID
- Machine HostID (Available on the Offline Activation Interface)
- Activation Log. Perform the following steps to get activation log:
  - 1 Go to `C:\Program Files (x86)\Motorola\IMPRES Fleet Management`.
  - 2 Open “log4cxxconfig.xml” with any text editor.
  - 3 Scroll to the end of the file, at the setting priority value=“ERROR”, modify it to priority value=“ALL”.
  - 4 Redo the activation.
  - 5 Select **Back to go back to** `C:\Program Files (x86)\Motorola\IMPRES Fleet Management`.
  - 6 Get the Activation log file from **LOGS** folder and attach it to the engineering team.


## 1.4

# Database Error Messages

This section describes the error messages when installing and running the Battery Fleet Management application.

## Errors During Installation

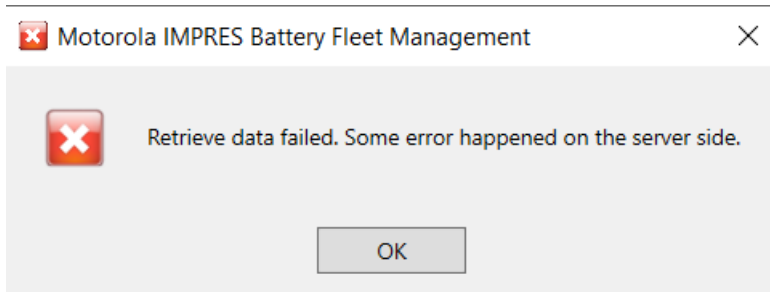
Table 1: Error Messages

Errors	Actions
Database will not install with error trying to access SQLNCLI	<p>Perform the following steps when your setup does not allow running applications from the download location of the administrator account and an error message <b>Can't find SQLNCLI</b> appears.</p> <ol style="list-style-type: none"><li>1 Go to Microsoft site.</li><li>2 Choose <b>Download SQLNCLI</b></li><li>3 Perform manual install.</li><li>4 Reinstall the SQL Express package.</li></ol>
Database is not installed properly	<p>Perform the following steps when you receive a database error message such as <b>Database is not installed properly...</b></p> <ol style="list-style-type: none"><li>1 Navigate to C:\Program Files (x86)\Motorola\IMPRES Fleet Management.</li><li>2 Run FleetDatabaseUpgrade.exe as administrator.</li></ol> <p>The script rebuilds all the tables and stored procedures used in Fleet Management (FM) database to the latest version.</p> <p> <b>NOTE:</b> Ensure that the script is running without error. dbupgrade.txt log file is generated in the same folder.</p>
When Running the Fleet Management Application	<p>Perform the following steps when you receive a database error message such as <b>Retrieve data failed...</b> or any other error message.</p> <ol style="list-style-type: none"><li>1 Select <b>Start→Run→Event Viewer</b>.</li><li>2 Expand <b>Applications and Services Logs</b>.</li><li>3 Right-click on the <b>FleetManagement</b> and select <b>Save All Events As....</b></li><li>4 Select English for <b>Display Information</b>.</li><li>5 Send the Fleet Management (FM) event logs to the engineering team for investigation.</li></ol>

## Retrieve Data Failed

This error message is an indication that the SQL database is not accessible. The following lists the possible causes:

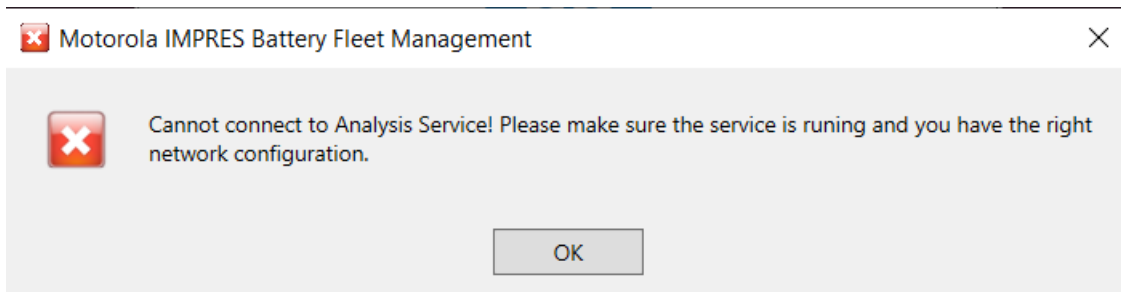
- SQL Express Service is not installed.
- SQL Express Service is not running.
- SQL Service was uninstalled and reinstalled, deactivating the Battery Fleet Management database.



 **NOTE:** See [Fixing Retrieving Data Failure](#) on page 11.

## Cannot Connect to Analysis Service

This error message is an indication that the analysis service is not running or cannot be contacted. The second case is where a client machine is unable to connect to the server.



 **NOTE:** See [Fixing Analysis Service Connection](#) on page 12.

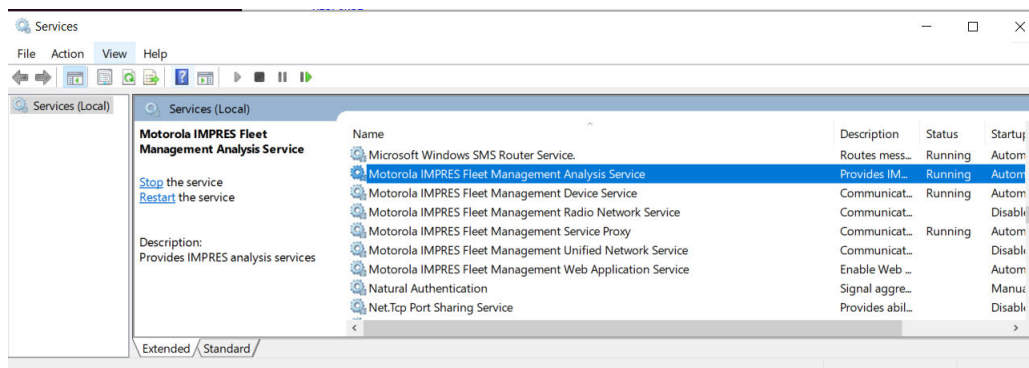
### 1.4.1

## Fixing Retrieving Data Failure

Perform the following steps when you receive a **Retrieve Data Failed** error.

### Procedure:

- 1 Select **Start→Run**.
- 2 Type `"services.msc"`.
- 3 Press **Enter**.
- 4 In the **Service** window, ensure that the status for **SQL Server (SQLEXPRESS)** is **Running**.



- 5 Perform one of the following options:

If...	Then...
the Service is not running	right-click on the service and select <b>Start</b> .
the SQL Server service fails to start	check if the Fleet Management database files are in the correct filepath: C:\Program Files (x86)\Microsoft SQL Server\MSSQL11.SQLEXPRESS\MSSQL\DATA
If the Fleet Management Database files do not exist	reinstall the IMPRES Battery Fleet Management package.

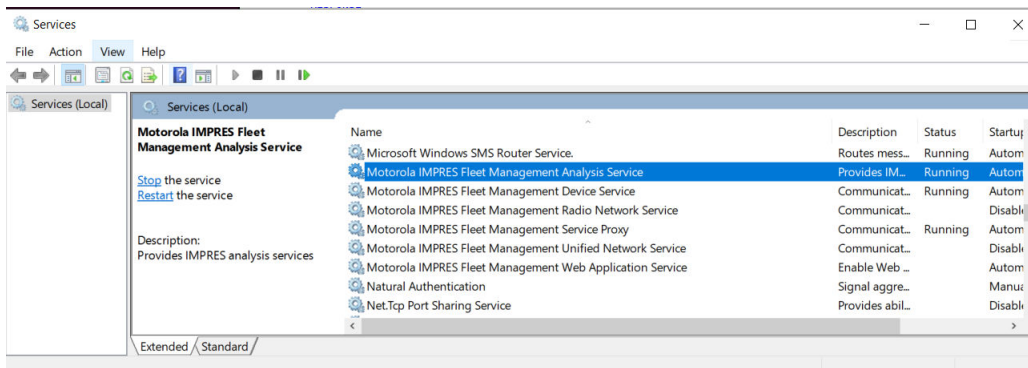
#### 1.4.2

### Fixing Analysis Service Connection

Perform the following steps when you receive a **Cannot Connect to Analysis Service** error.

#### Procedure:

- 1 Select **Start**→**Run**.
- 2 Type `""services.msc""`.
- 3 Press **Enter**.
- 4 In the **Service** window, ensure that the status for **Motorola IMPRES Fleet Management Analysis Service** is **Running**.



- 5 Perform one of the following options:

If...	Then...
the Service is not running	right-click on the service and select <b>Start</b> .
the error is because of a client machine is unable to connect to the server	<ol style="list-style-type: none"> <li>a Ensure that you run the IMPRES Battery Fleet Management as an Administrator.</li> <li>b Reconfigure the server address and server port.</li> <li>c Click <b>OK</b>.</li> </ol>

## 1.5

### ASTRO OTABM Network or Application Configuration Problem

This section describes the troubleshooting procedures for ASTRO Over-the-Air Battery Management (OTABM) network or application configuration problems.

Table 2: Network or Application Configuration Problem

Ensure IP connectivity is established.

Scenario	Action
The APX radios and IMW	Log on to Intelligent Middleware (IMW), access the windows command line by pressing <b>WIN-DOWS KEY + R</b> and press Enter. You can successfully ping through IP address or by fully qualified domain name of one or more APX portable radios. The radio IP address can be found on the IP menu (if this menu is configured on the radio). Scroll down and select the required IP menu.
The battery management server and IDM	Log on to the battery management server, access the command line and ping the IP address or fully qualified domain name that is configured for the Internet Download Manager (IDM) in the battery management configuration menu.
The battery management server and IMW	Log on to the battery management server, access the windows command line by pressing <b>WINDOWS KEY + R</b> and press Enter. Ping the IP address or fully qualified domain name that is configured for the IMW in the battery management configuration menu.
The battery management server and the battery management clients	Log on to the battery management client, access the windows command line by pressing <b>WINDOWS KEY + R</b> and press Enter. Ping the IP address or fully qualified domain name that is configured for the battery management server in the battery management configuration menu.

If the IP connectivity is not found when testing between each of the network end-points, continue troubleshooting by checking connectivity to any intermediate network switches or routers between the end-points. If connectivity is not confirmed using the IMW, IDM or battery management host by fully qualified domain name, change to pinging by IP address to rule out a domain name service resolution issue. Domain Name System (DNS) resolution may be provided by the Windows host file or by an external DNS server.

## 1.6

### ASTRO OTABM Application Configuration Problem

This section contains troubleshooting procedures for ASTRO Over-the-Air Battery Management (OTABM) application configuration problems.

If the ASTRO Radio System Intelligent Middleware (IMW) and the Unified Network Service (UNS) of the Battery Fleet Management application are communicating, **UNS Connected** is displayed in green text at the bottom of the **Radios and Batteries** window.

Additionally, once the UNS and the IMW are initially communicating, if there are any connection issues, errors are reflected in the `UNS.log` file which can be found in the battery management server application root directory if the value of Debug key in

**Motorola.FleetManagement.UnifiedNetworkService.WS.exe.config** is set to `Y`.

After verifying IP connectivity between each of the required end points, check that the applications are configured correctly.

### 1.6.1

## Troubleshooting Procedures

The sections contains the troubleshooting procedures for battery management server.

### Procedure:

- 1 Confirm that the Identity manager (IDM) and IMW fully qualified domain names or IP addresses are correctly entered on the battery management server configuration screen. Check that the UNS and IMW client is enabled and that the user name and password match those configured in IDM.
- 2 Navigate to **Start** and type `services.msc`.  
Ensure Motorola IMPRES Fleet Management Unified Network Service is running.

### 1.7

## Contacting Service Team

If your issue still persist, contact your service team and provide the following information:

- PC Operating System (example: Windows 10 Pro-64-bit)
- IMPRES Battery Fleet Management software version and region (example: FM V3.5)
- Issue encountered
- Detailed steps to reproduce the issue

## Chapter 2

# Firewall Configuration

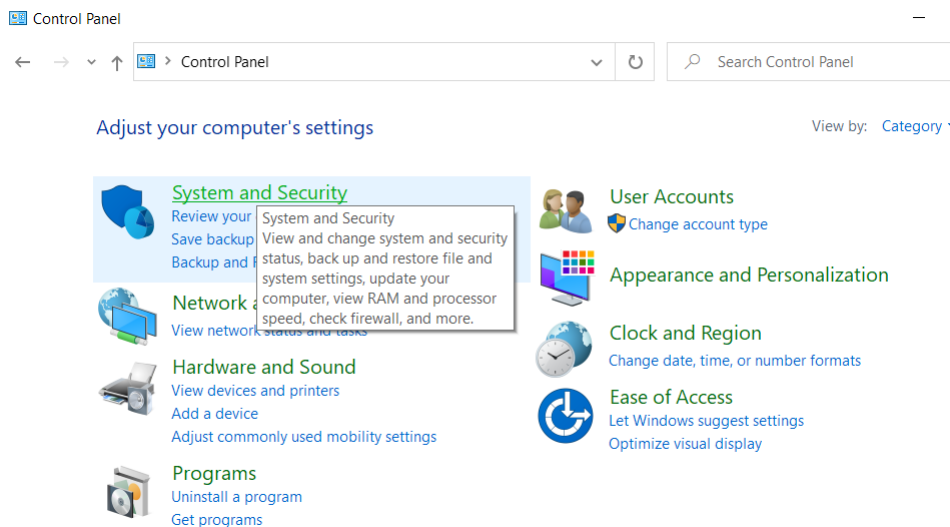
This chapter provides guidelines for troubleshooting the installation. For non-installation troubleshooting, refer to *MN007501A01 IMPRES Battery Fleet Management Troubleshooting Guide*.

## 2.1

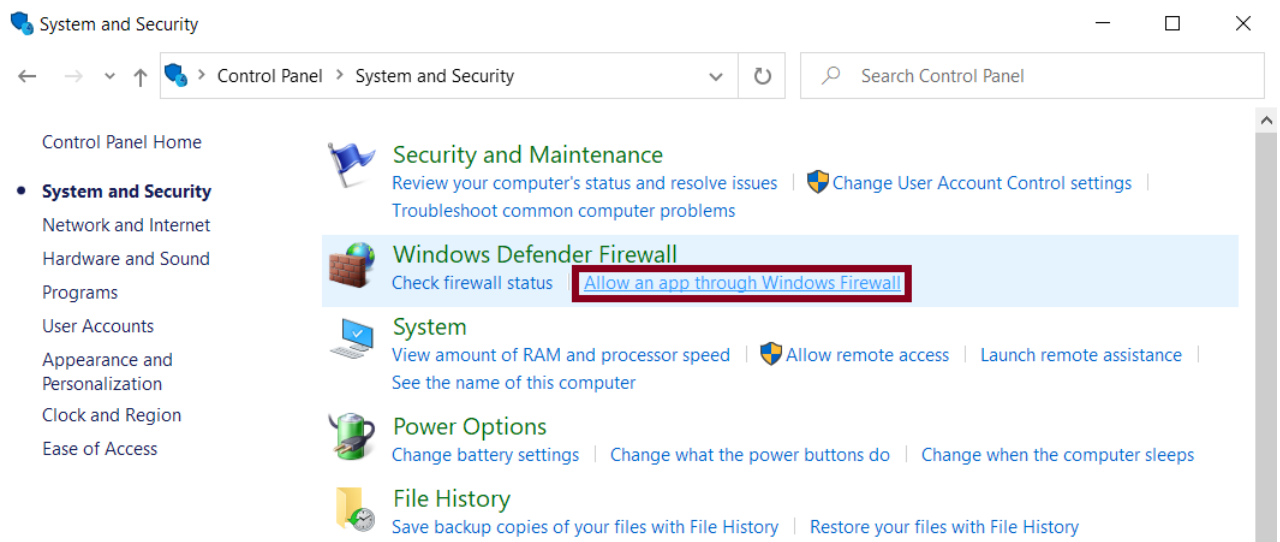
### Configuring Firewall

In some instances, the computer Windows Firewall blocks any communication services from other computers. The Windows services block the IMPRES Battery Fleet Management Server or Client setup. Perform the following steps to allow the IMPRES Battery Fleet Management application to communicate through Windows firewall.

#### 1 Select **Start**→**Control Panel**→**System and Security**.



#### 2 Select **Allow an app through Windows Firewall**.



#### 3 Click **Change Settings**→**Allow another app to communicate through Windows Firewall**.



## Allow apps to communicate through Windows Defender Firewall

To add, change, or remove allowed apps and ports, click Change settings.

What are the risks of allowing an app to communicate?

Change settings

Allowed apps and features:

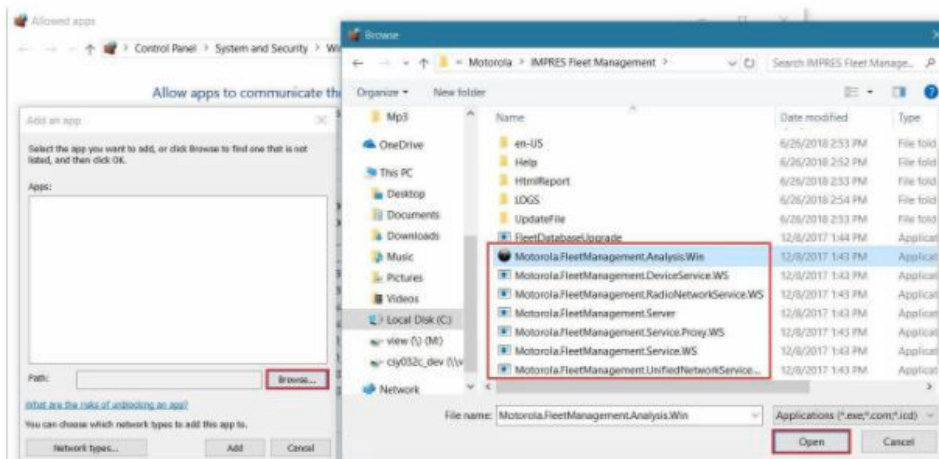
Name	Domain	Private	Public
<input checked="" type="checkbox"/> @{\Microsoft.DesktopAppInstaller_1.0.22011.0_x64_8wekyb3d8bb...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> @{\Microsoft.DesktopAppInstaller_1.0.30311.0_x64_8wekyb3d8bb...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> @{\Microsoft.Messaging_3.43.27001.0_x64_8wekyb3d8bbwe?ms-r...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> @{\Microsoft.Messaging_4.1901.10241.0_x64_8wekyb3d8bbwe?ms...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> @{\Microsoft.MicrosoftEdge_44.17763.1.0_neutral_8wekyb3d8bbw...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> @{\Microsoft.MicrosoftEdge_44.17763.1.0_neutral_8wekyb3d8bbw...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> @{\Microsoft.MicrosoftOfficeHub_17.8918.5926.0_x64_8wekyb3d8...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> @{\Microsoft.OneConnect_5.1807.1991.0_x64_8wekyb3d8bbwe?m...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> @{\Microsoft.OneConnect_5.1902.361.0_x64_8wekyb3d8bbwe?ms...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> @{\Microsoft.PPIProjection_10.0.17763.1_neutral_neutral_cw5n1h2t...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> @{\Microsoft.PPIProjection_10.0.17763.1_neutral_neutral_cw5n1h2t...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> @{\Microsoft.Windows.Cortana_1.11.5.17763_neutral_neutral_cw5n...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Details...

Remove

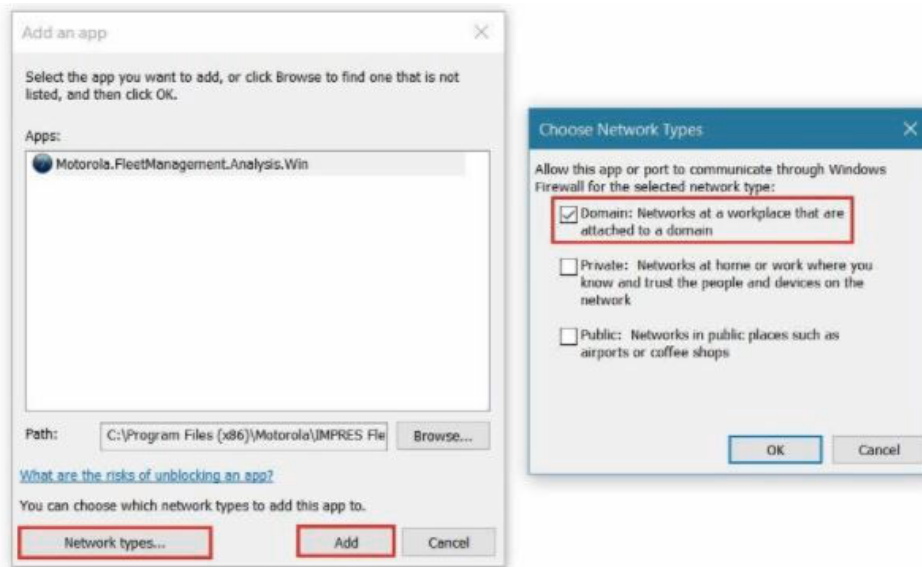
Allow another app...

- From the **Add and App** window, click **Browse** to locate the IMPRES Battery Fleet Management Service Application (.exe).

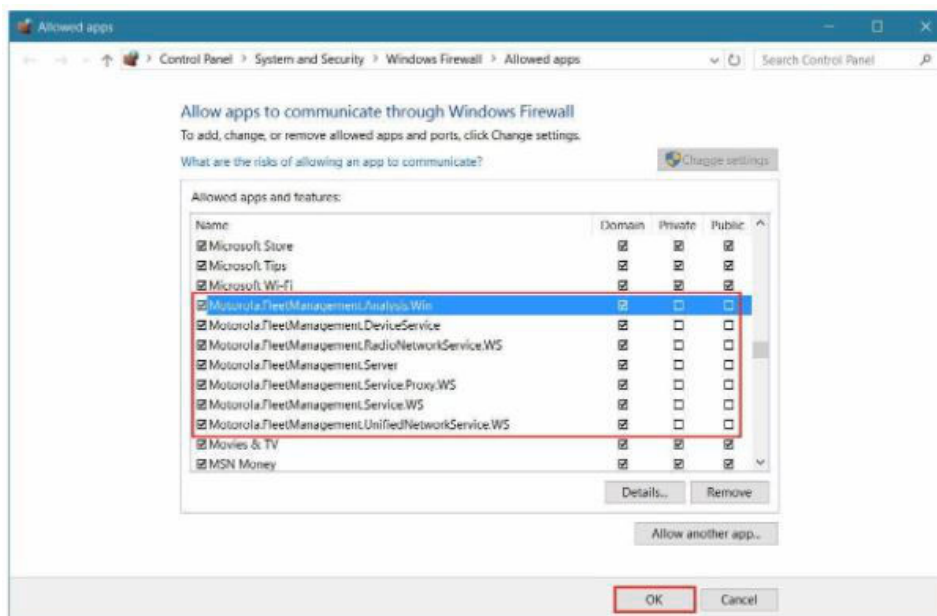


- Click **Open**.
- Ensure that the **Network Type** is selected by default to allow firewall for Domain only.
- Click **Add** to select application file into list.





- 8 Repeat steps 6 on page 16 and 7 on page 16 to add other service application files.
- 9 Click **OK** to close the window.



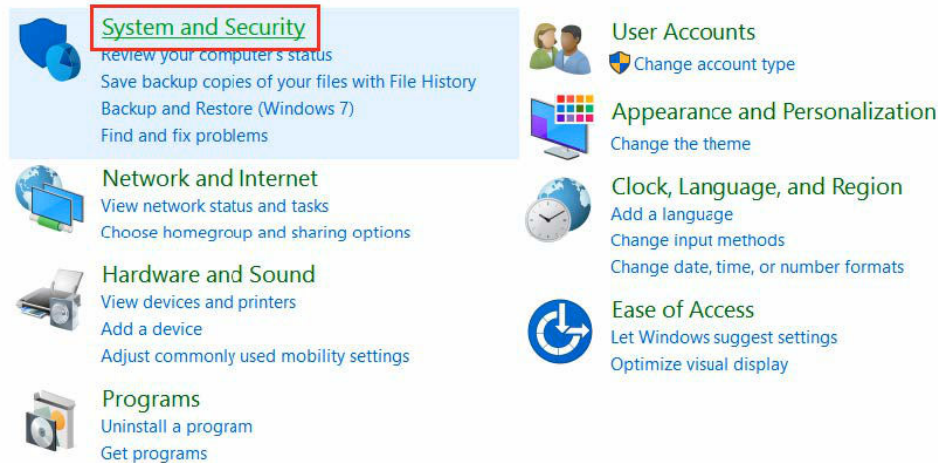
## 2.2

### Enabling Windows Firewall to Accept Messages From UDP Ports (MOTOTRBO OTA)

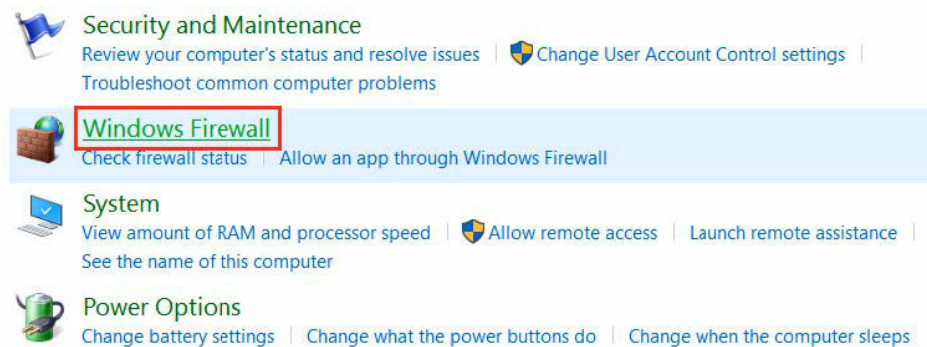
In some instances, the computer firewall blocks any messages from TCP or UDP ports. The UDP port blocks battery messages exchange over the radio RF links. You are not able to see any radio registration and battery data exchanges information in IMPRES Battery Fleet Management. The following are the procedures to enable the TCP/UDP inbound/outbound ports.

#### Procedure:

- 1 Navigate to the **Control Panel** and select **System and Security**.



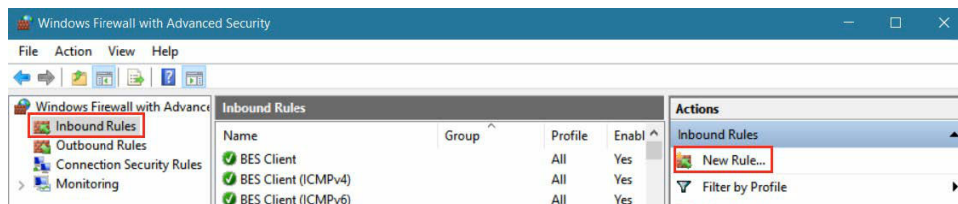
2 Select **Windows Firewall**.



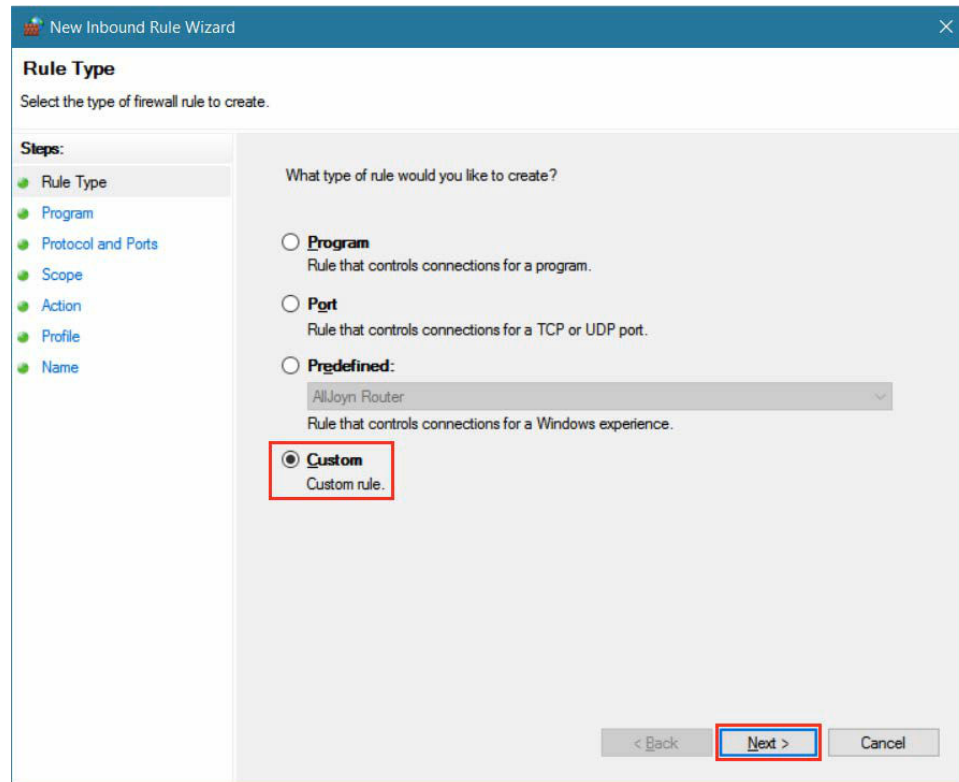
3 Select **Advanced settings** in the windows firewall window.



4 Select **Inbound Rules** at the left panel and click on **New Rule...** at the right panel.



5 Select **Custom** and click on **Next** button.



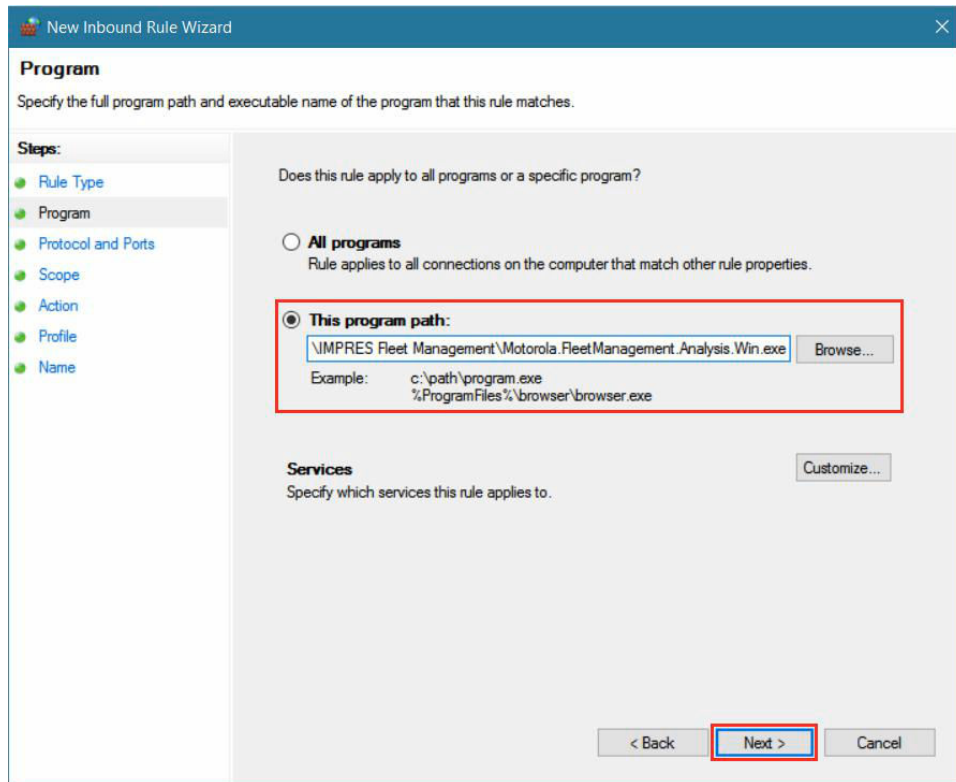
6 Select **This program path** → **Browse** → **Next**.



**NOTE:**

Browse and locate the IMPRES Battery Fleet Management application (.exe) file.

The default full path for the application file is located at C:\Program Files (x86)\Motorola\IMPRES Fleet Management\Motorola.FleetManagement.Analysis.Win.exe.



The screenshot shows the 'Program' step of the 'New Inbound Rule Wizard'. The left sidebar lists the steps: Rule Type, Program, Protocol and Ports, Scope, Action, Profile, and Name. The main area asks 'Does this rule apply to all programs or a specific program?'. The 'All programs' option is unselected. The 'This program path:' option is selected and highlighted with a red box. Below it, a text box contains the path '\\IMPRES Fleet Management\\Motorola.FleetManagement.Analysis.Win.exe' and a 'Browse...' button. Below the text box, an example shows 'c:\\path\\program.exe' and '%ProgramFiles%\\browser\\browser.exe'. At the bottom, there is a 'Services' section with a 'Customize...' button. At the very bottom, there are three buttons: '< Back', 'Next >' (highlighted with a red box), and 'Cancel'.

**Program**  
Specify the full program path and executable name of the program that this rule matches.

**Steps:**

- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

Does this rule apply to all programs or a specific program?

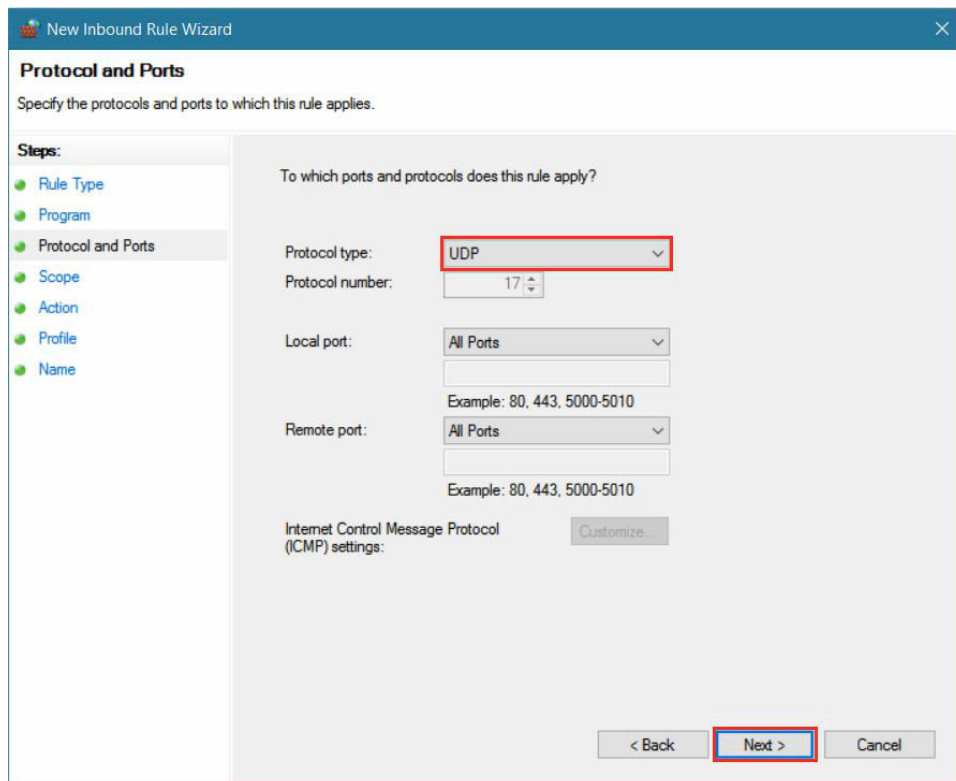
☐ All programs  
Rule applies to all connections on the computer that match other rule properties.

☒ This program path:  
\\IMPRES Fleet Management\\Motorola.FleetManagement.Analysis.Win.exe Browse...  
Example: c:\\path\\program.exe  
%ProgramFiles%\\browser\\browser.exe

**Services**  
Specify which services this rule applies to. Customize...

< Back Next > Cancel

7 Select UDP→Next.



The screenshot shows the 'Protocol and Ports' step of the 'New Inbound Rule Wizard'. The left sidebar lists the steps: Rule Type, Program, Protocol and Ports, Scope, Action, Profile, and Name. The main area asks 'To which ports and protocols does this rule apply?'. The 'Protocol type:' dropdown is set to 'UDP' and is highlighted with a red box. The 'Protocol number:' is set to '17'. The 'Local port:' dropdown is set to 'All Ports'. The 'Remote port:' dropdown is set to 'All Ports'. Below these, there are example ranges: 'Example: 80, 443, 5000-5010'. At the bottom, there is an 'Internet Control Message Protocol (ICMP) settings:' section with a 'Customize...' button. At the very bottom, there are three buttons: '< Back', 'Next >' (highlighted with a red box), and 'Cancel'.

**Protocol and Ports**  
Specify the protocols and ports to which this rule applies.

**Steps:**

- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

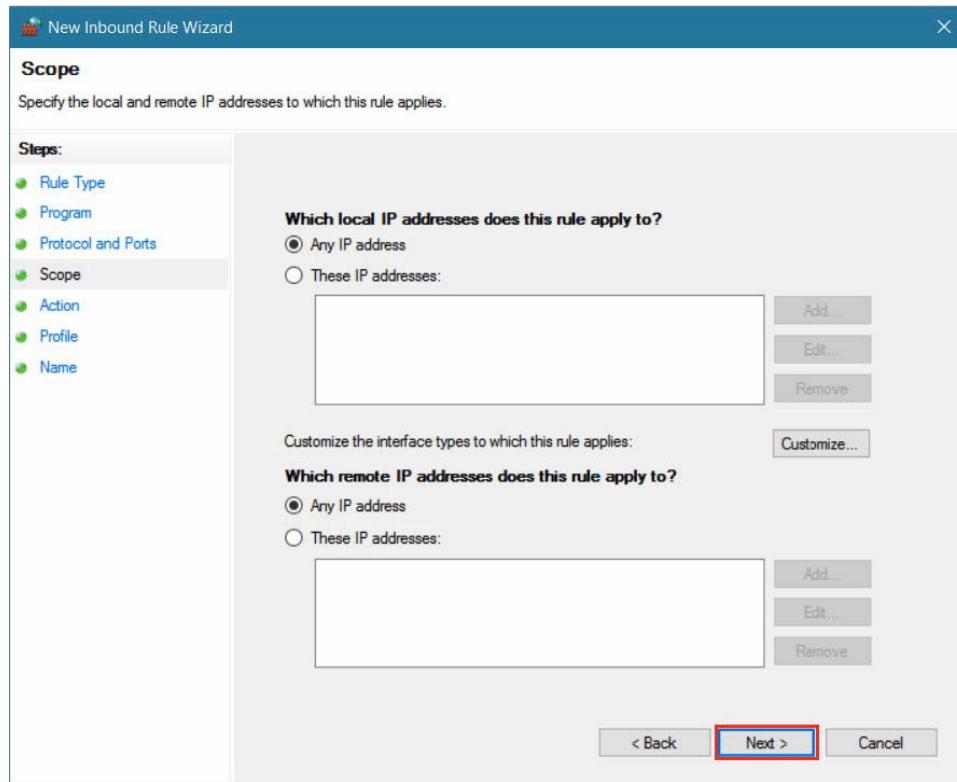
To which ports and protocols does this rule apply?

Protocol type: UDP  
Protocol number: 17  
Local port: All Ports  
Remote port: All Ports  
Example: 80, 443, 5000-5010  
Example: 80, 443, 5000-5010

Internet Control Message Protocol (ICMP) settings: Customize...

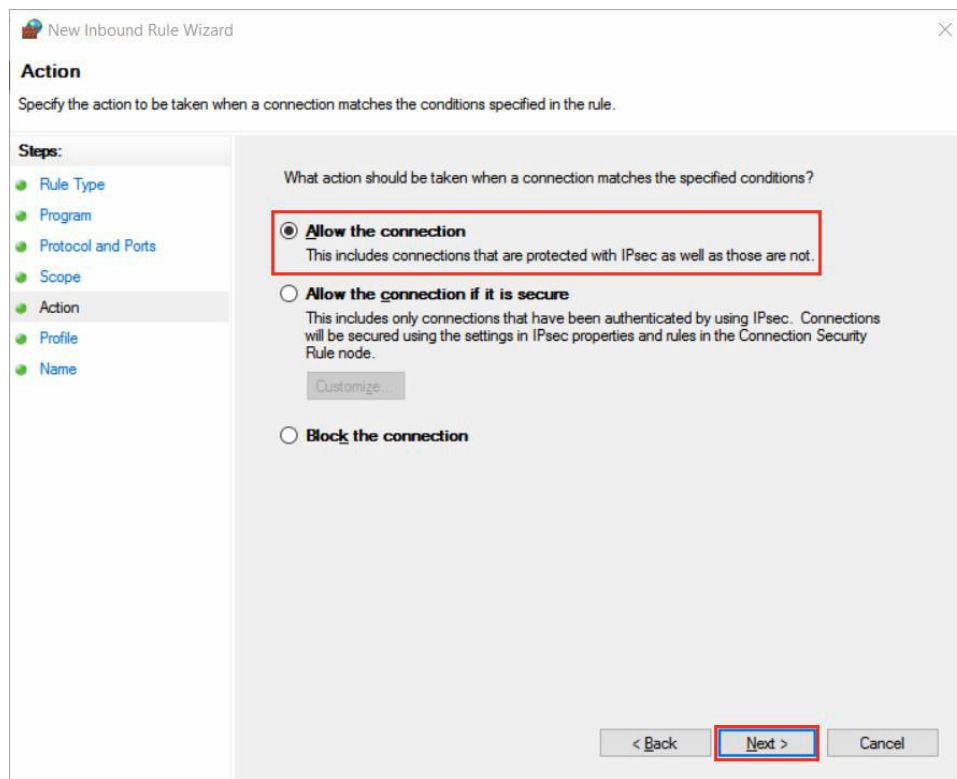
< Back Next > Cancel

8 Click Next.



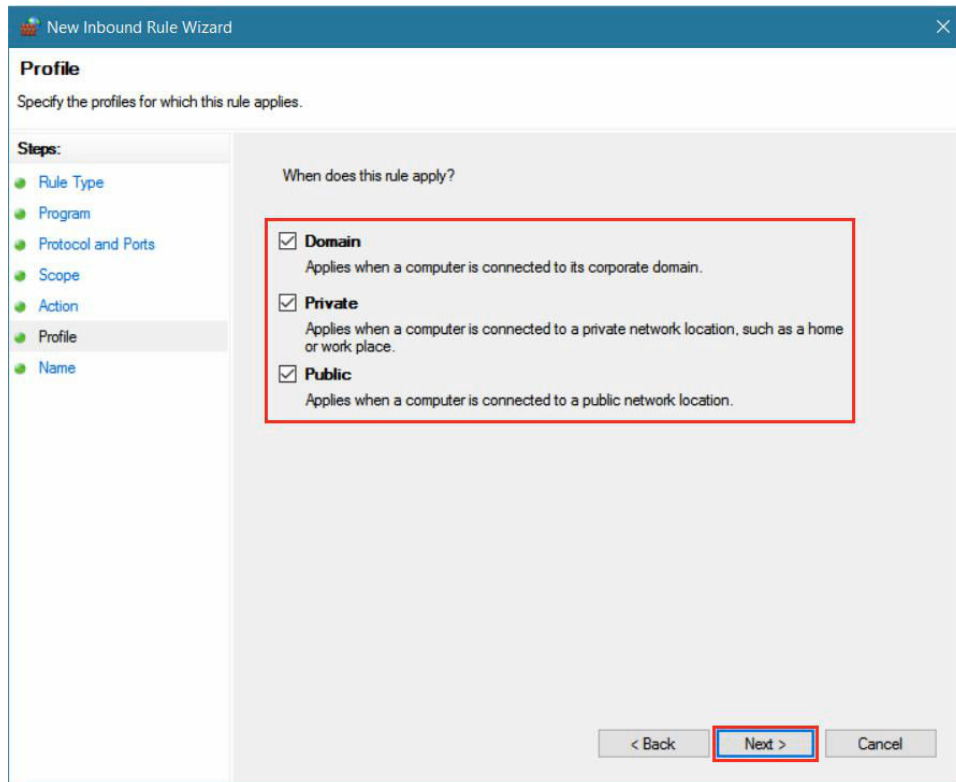
The image shows the 'New Inbound Rule Wizard' window, specifically the 'Scope' step. The left sidebar lists the steps: Rule Type, Program, Protocol and Ports, Scope (selected), Action, Profile, and Name. The main area is titled 'Specify the local and remote IP addresses to which this rule applies.' It contains two sections: 'Which local IP addresses does this rule apply to?' and 'Which remote IP addresses does this rule apply to?'. Both sections have radio buttons for 'Any IP address' (selected) and 'These IP addresses:'. Below each 'These IP addresses:' option is a text box and three buttons: 'Add...', 'Edit...', and 'Remove...'. There is also a 'Customize...' button. At the bottom, there are three buttons: '< Back', 'Next >' (highlighted with a red box), and 'Cancel'.

9 Select **Allow the connection**→**Next**.

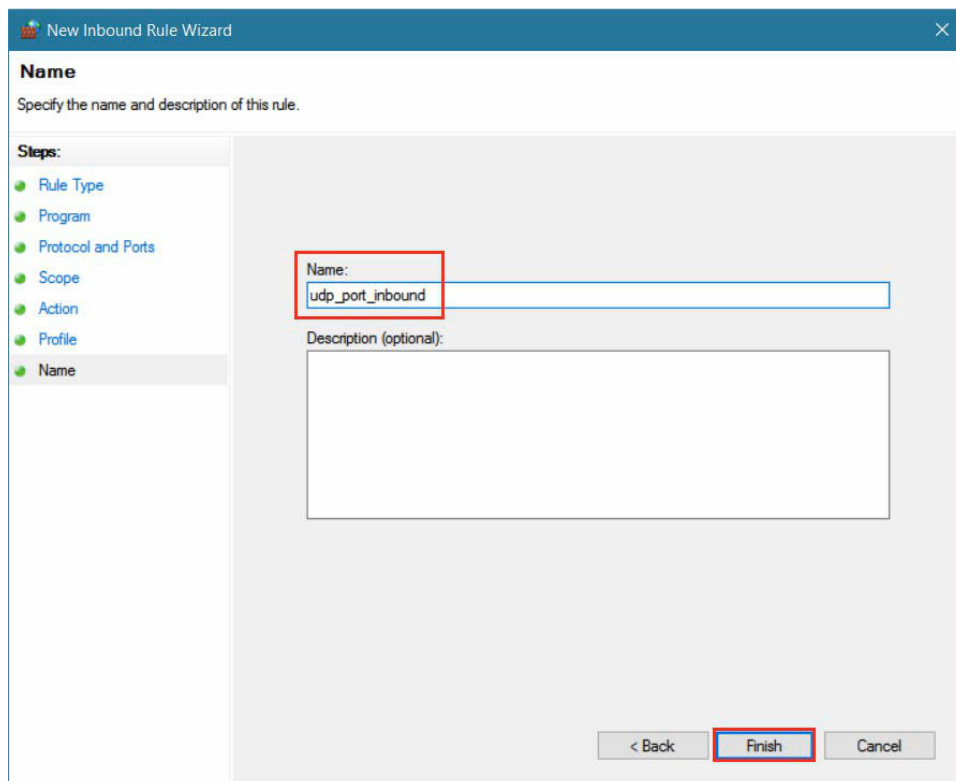


The image shows the 'New Inbound Rule Wizard' window, specifically the 'Action' step. The left sidebar lists the steps: Rule Type, Program, Protocol and Ports, Scope, Action (selected), Profile, and Name. The main area is titled 'Specify the action to be taken when a connection matches the conditions specified in the rule.' It contains a section titled 'What action should be taken when a connection matches the specified conditions?'. There are three radio button options: 'Allow the connection' (selected and highlighted with a red box), 'Allow the connection if it is secure', and 'Block the connection'. The 'Allow the connection' option has a description: 'This includes connections that are protected with IPsec as well as those are not.' The 'Allow the connection if it is secure' option has a description: 'This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.' and a 'Customize...' button. At the bottom, there are three buttons: '< Back', 'Next >' (highlighted with a red box), and 'Cancel'.

10 Select **Domain, Private, Public** and click **Next**.

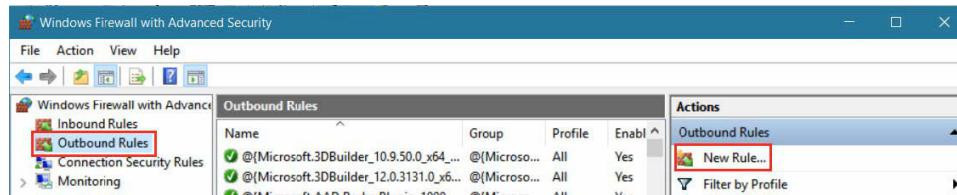


11 Type `udp_port_inbound` in the **Name** field and click **Finish**.



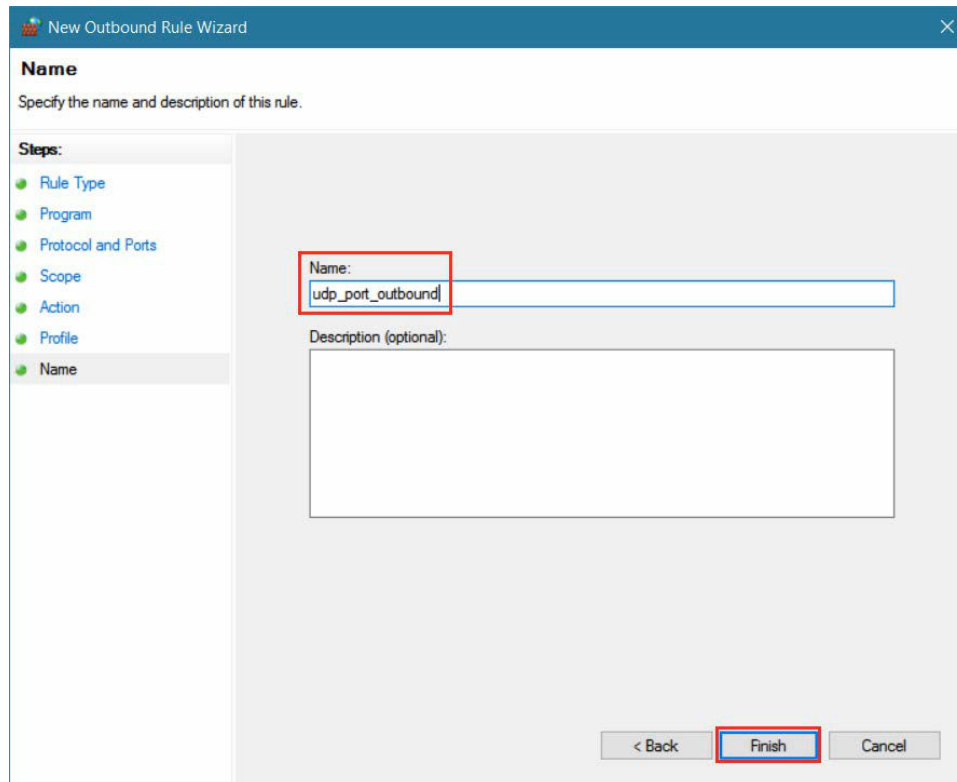
New inbound rule is created, and the inbound UDP port is allowed for IMPRES Battery Fleet Management application.

**12** To add a new outbound rule, select **Outbound Rules** in the left panel and click **New Rule...** in the right panel.



**13** To add a new outbound rule, repeat [step 5](#) to [step 11](#).

**14** Name the new rule, such as `udp_port_outbound` and click **Finish**.





## Chapter 3

# IMPRES Gen 2 Charger Drivers Manual Installation

### 3.1

## Installing IMPRES Gen 2 Charger Drivers Manually (Method 1)

You can perform a manual install of the IMPRES Gen 2 driver if your IMPRES Gen 2 charger drivers are not properly installed or the IMPRES Battery Fleet Management application is unable to detect IMPRES Gen 2 charger after the charger is connected to PC.

**Prerequisites:** To perform a manual installation on IMPRES Gen 2 drivers, exit all the IMPRES programs running on your computer. Connect the USB cable to the USB port on your computer.

### Procedure:

- 1 Run Command Prompt as Administrator.
- 2 Perform one of the following options:

If...	Then...
using 64-bit computer	<ol style="list-style-type: none"> <li>a Change the directory to the IMPRES Battery Fleet Management installation package unzipped folder to C:\Battery_Fleet_Management_V4.0\ISSetupPrerequisites\{BB7A14A1-192B-4C7F-80E5-C5AF52C8F002}.</li> <li>b Enter the 'reinstall64' to reinstall IMPRES Gen 2 Charger Drivers.</li> </ol>
using 32-bit computer	<ol style="list-style-type: none"> <li>a Change the directory to the IMPRES Battery Fleet Management installation package unzipped folder to C:\Battery_Fleet_Management_V4.0\ISSetupPrerequisites\{AA0EF3E7-03EA-468D-A207-21887C64EFA4}.</li> <li>b Enter the 'reinstall32' to reinstall IMPRES Gen 2 Charger Drivers.</li> </ol>

- 3 Wait until all the drivers are successfully installed.

```

Administrator: Command Prompt
Microsoft Windows [Version 10.0.19042.1348]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cd C:\Battery_Fleet_Management_V4.0\ISSetupPrerequisites\{BB7A14A1-192B-4C7F-80E5-C5AF52C8F002}

C:\Battery_Fleet_Management_V4.0\ISSetupPrerequisites\{BB7A14A1-192B-4C7F-80E5-C5AF52C8F002}>reinstall64
Installing Gen2Drivers...
1 file(s) copied.
Done!

C:\Battery_Fleet_Management_V4.0\ISSetupPrerequisites\{E6C1A7A5-A218-4010-A5A8-7EB680FE533E}>

```



## 3.2

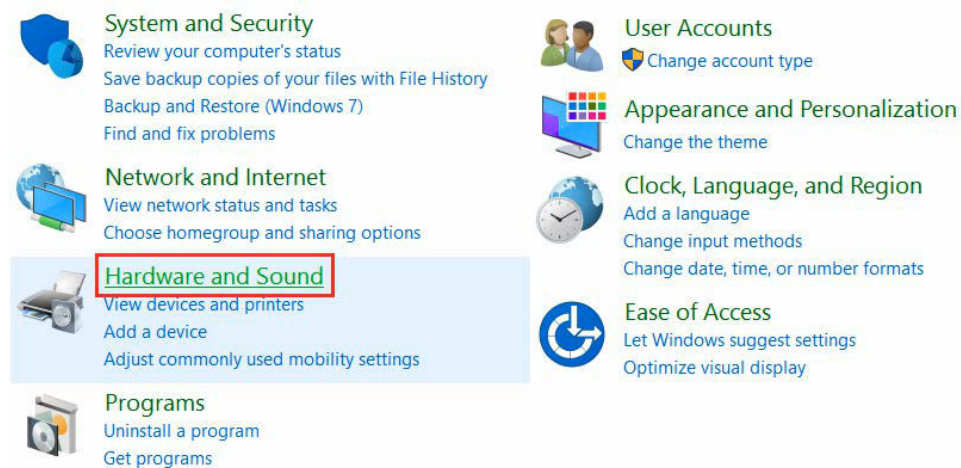
## Installing IMPRES Gen 2 Charger Drivers Manually (Method 2)

You can perform a manual install of the IMPRES Gen 2 driver if your IMPRES Gen 2 charger drivers are not properly installed or the IMPRES Battery Fleet Management application is unable to detect IMPRES Gen 2 charger after the charger is connected to PC.

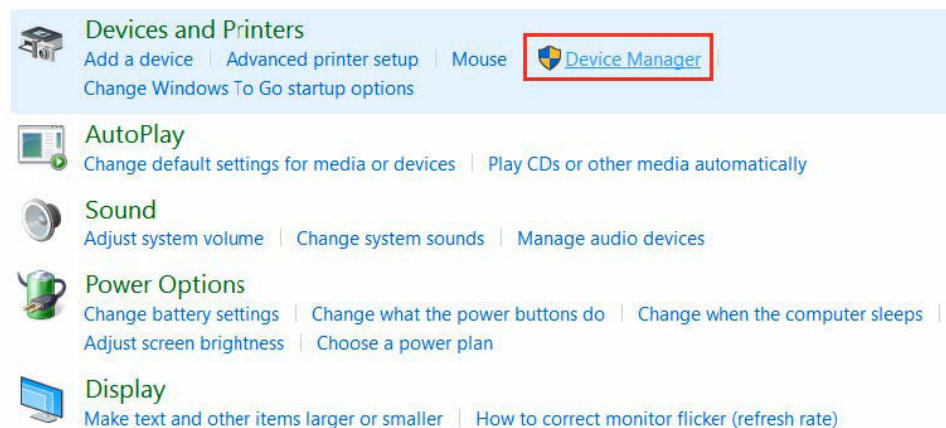
**Prerequisites:** To perform a manual installation on IMPRES Gen 2 drivers, exit all the IMPRES programs running on your computer. Connect the USB cable to the USB port on your computer.

### Procedure:

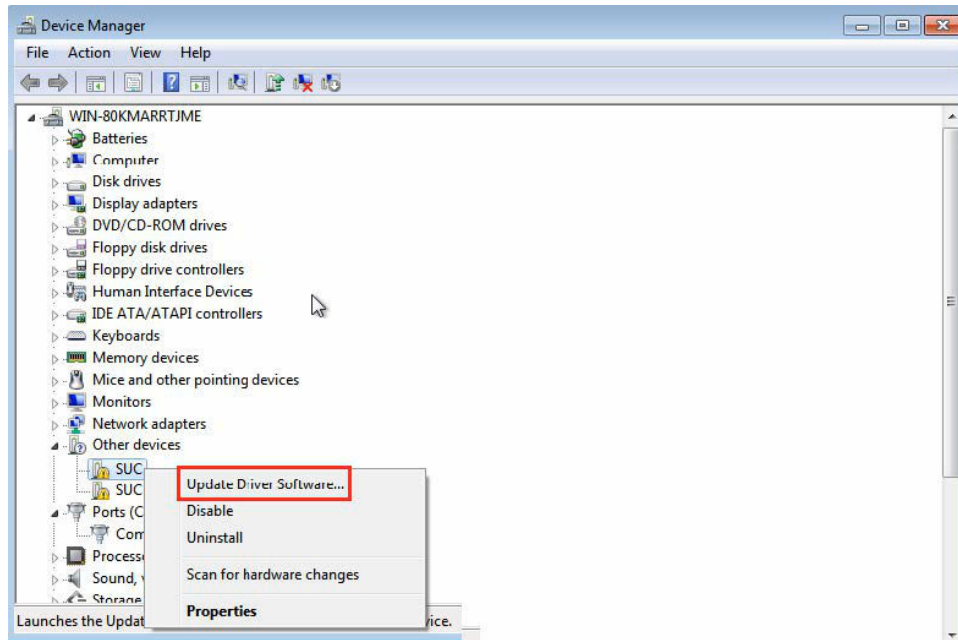
- 1 Navigate to the **Control Panel** and select **Hardware and Sound**.



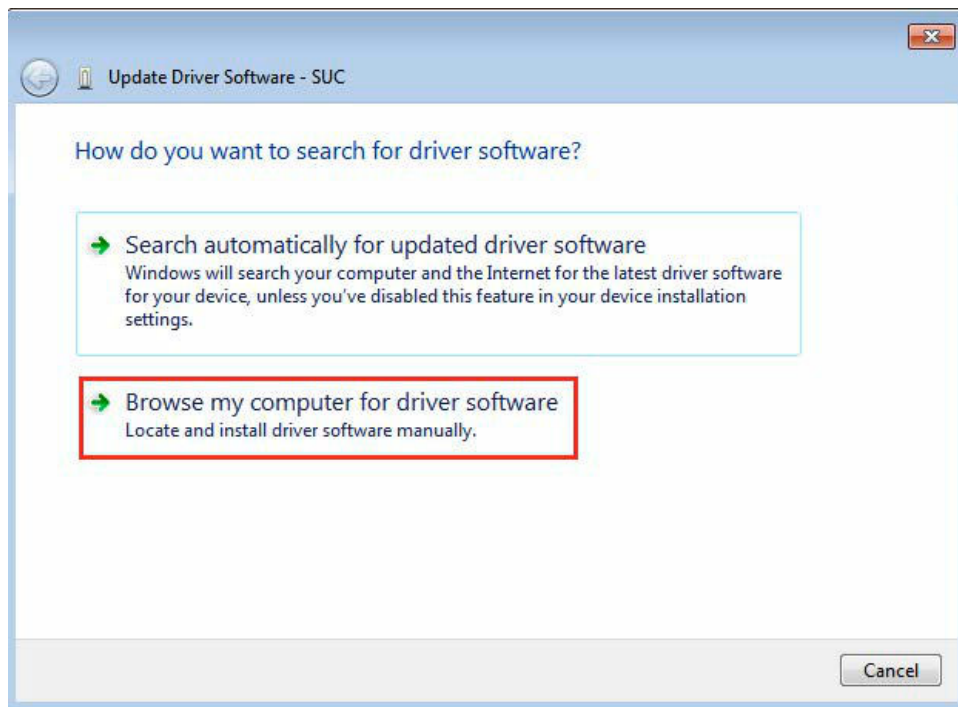
- 2 Select **Device Manager**.



- 3 In the Device Manager, navigate to **Other devices** and right click on the first SUC (or MUC) and select **Update Driver Software**.



- 4 Select **Browse my computer for driver software**.



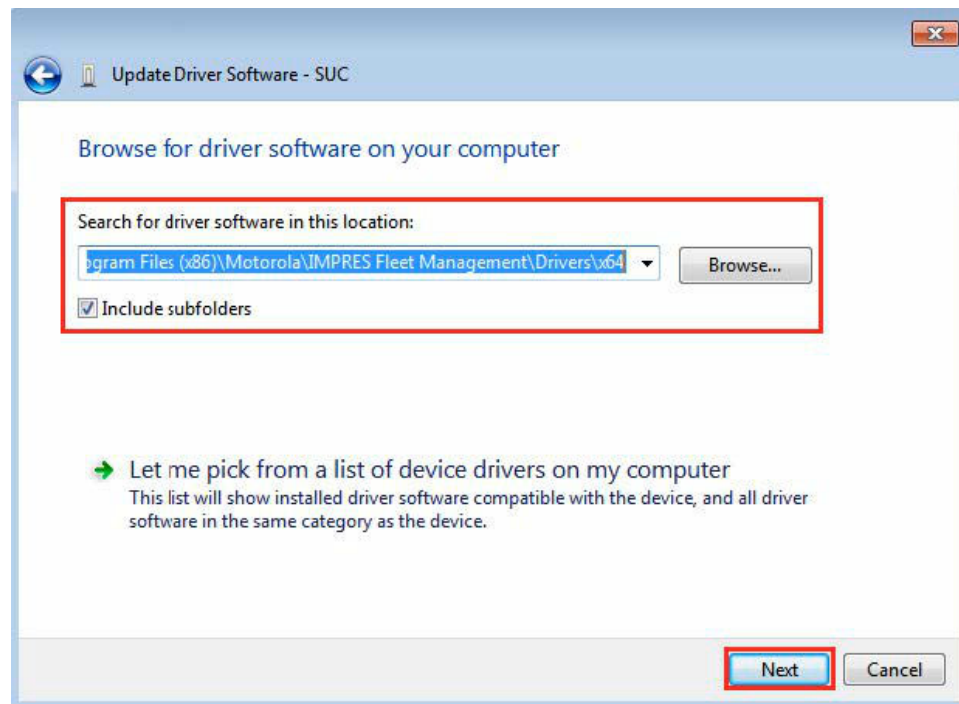
- 5 To manually locate the driver, click **Browse**.



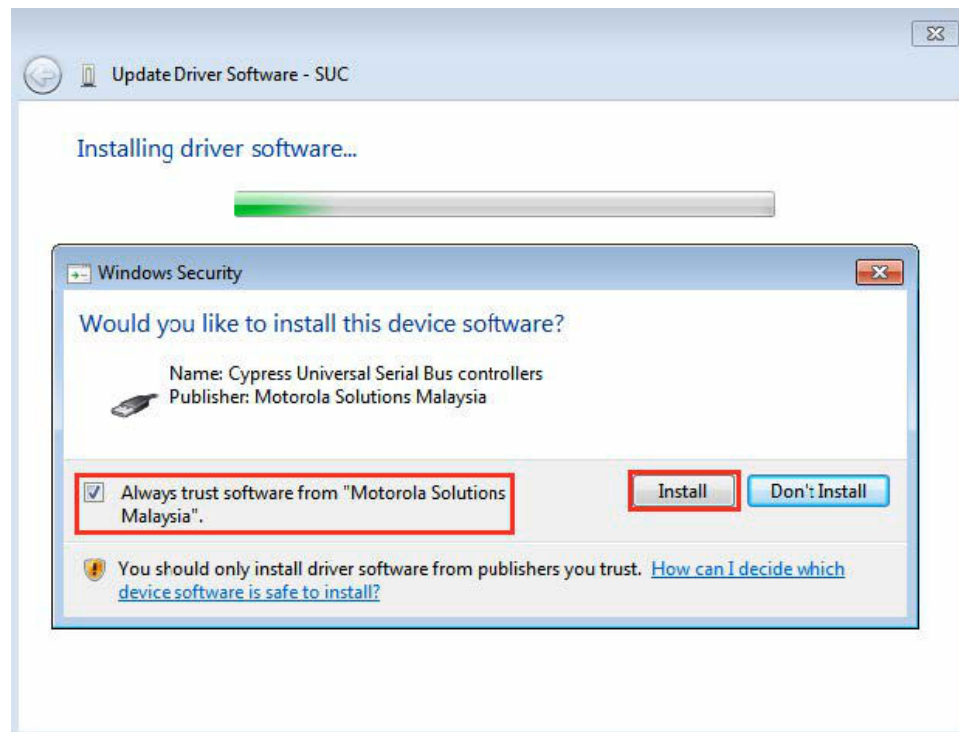
**NOTE:**

The driver files are located at the sub-folder of the IMPRES Battery Fleet Management installation folder. The default full path for the device drivers are located at C:\Program Files (x86)\Motorola\IMPRES Fleet Management\Drivers\x86 or x64, depending on whether your computer is a 32 bit computer (use the x86 folder) or a 64 bit computer (use the x64 folder).

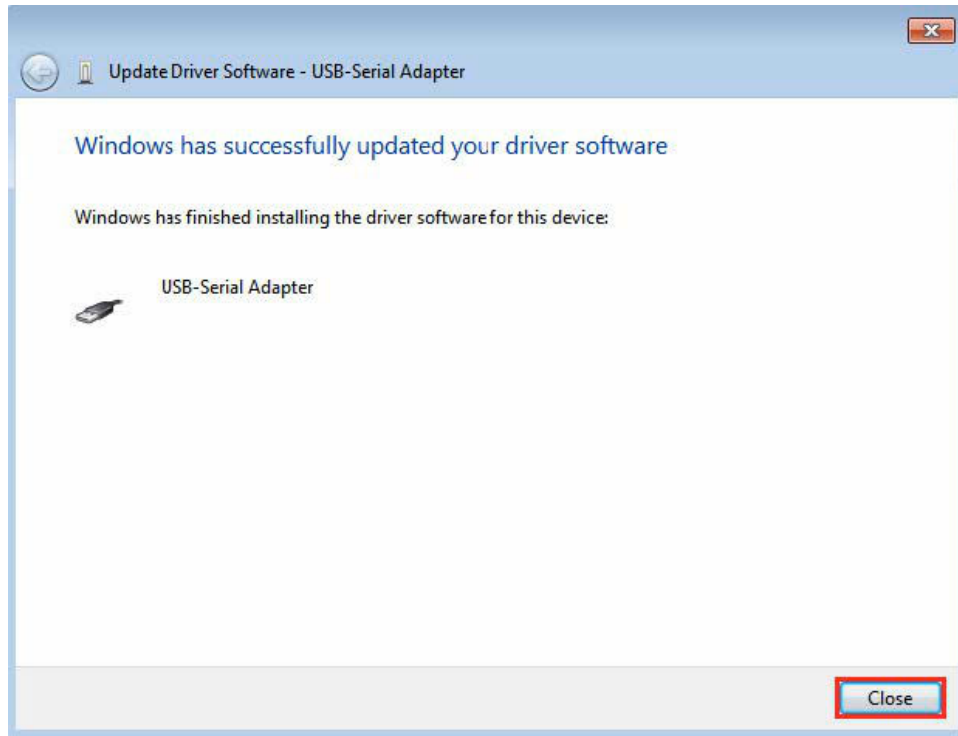
- 6 Once you have located the driver, click **Next**.



- 7 To proceed with the installation, check **Always trust software from “Motorola Solutions Malaysia”** and click **Install**.

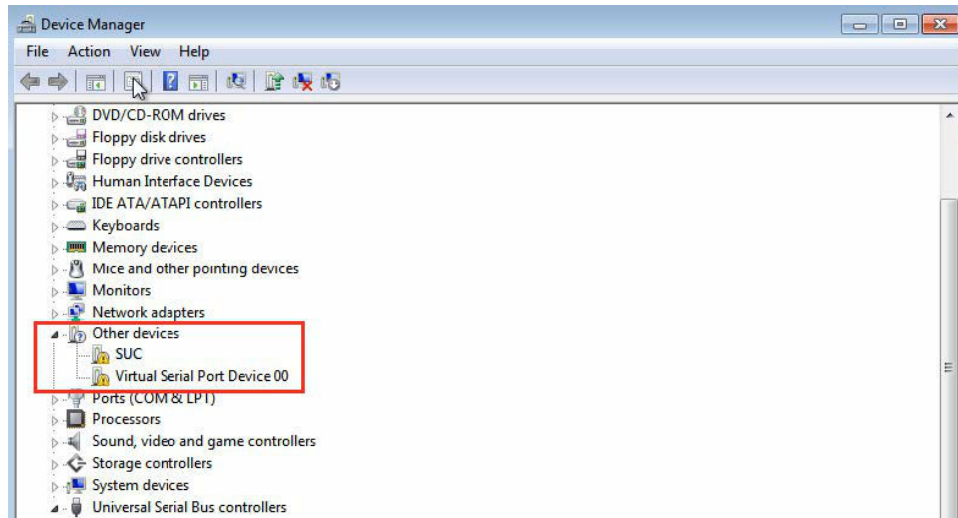


- 8 Click **Close** to complete the driver installation.



Once the driver is installed, another new hardware is displayed under **Other devices** which is the **Virtual Serial Port Device**.

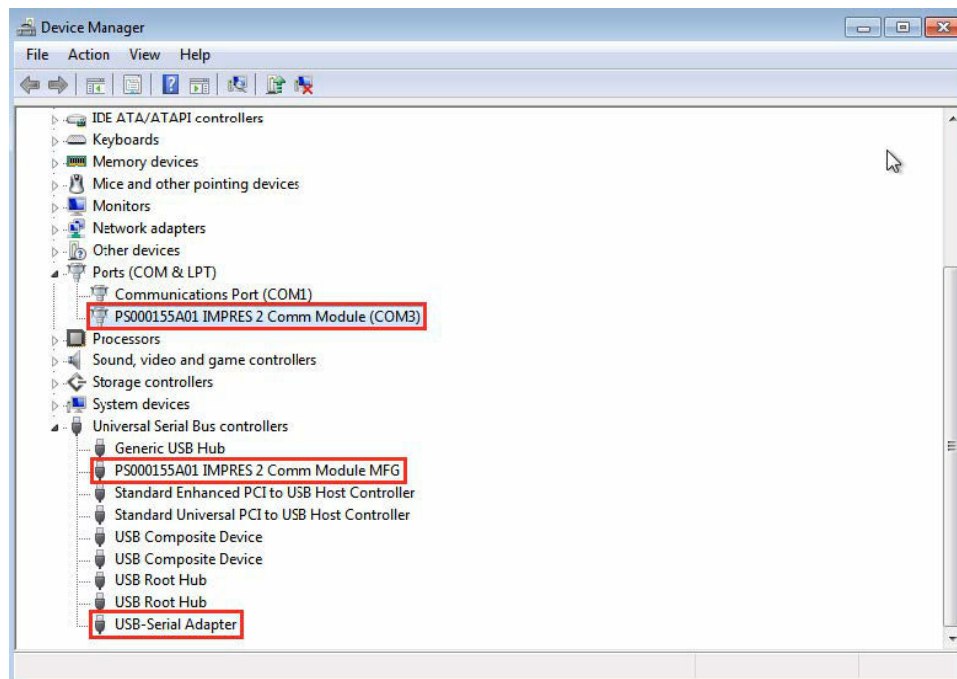
- 9 To install the remaining two devices, repeat [step 3](#) to [step 8](#).



**NOTE:**

When the drivers are installed, there are three known devices found under **Ports** and **Universal Serial Bus controllers**.

Different names are used for different MUC chargers.



## Chapter 4

# Generate License for Offline Activation

Follow this section to generate a license from a HOST ID for the following situations:

- If the machine is not connected to the internet, or
- the customer would like to manually generate and store the individual license files to perform offline activations

To generate the license file from the HOST ID the following are required:

- HOST ID: See the section in the installation guide named OFFLINE ACTIVATION and follow the steps to save the HOST ID
- An entitlement ID (EID): EID was provided to you at the time of purchase of your 20 licenses.
- An account on Motorola Solutions FLEXNET license web site: <https://licensing.motorolasolutions.com/flexnet/operationsportal/logon.do>

### 4.1

## Creating an Account

**Prerequisites:** Ensure that you have your EID to complete the process.

**Procedure:**

- 1 Go to the following link <https://licensing.motorolasolutions.com/flexnet/operationsportal/showSelfRegisterUserPage.do>
- 2 Fill up the **Self Service Registration** page.

The screenshot shows the 'Self Service Registration' page of the Motorola Solutions portal. The page has a header with the Motorola Solutions logo. The main content area is titled 'Self Service Registration' and contains a section 'Register for Account'. This section includes several input fields for user information: Entitlement ID, User Name, First Name, Last Name, Email Address, Phone, Fax, Street, City, State/Province, Zip/Postal Code, Country (a dropdown menu currently showing 'United States'), Locale (a dropdown menu currently showing 'English (United States)'), and Time Zone (a dropdown menu currently showing '(GMT -8.0) Pacific Time'). There is also a checkbox for 'Opt in to receive email' with radio buttons for 'Yes' and 'No' (the 'No' option is selected). At the bottom right of the form are three buttons: 'Back', 'Reset', and 'Complete'.

**3 Click Complete.**

Your EID would look similar to the following example:

**Example:** 2FBXXXXX-4XXX-1XXX-AXXX-E7EXXXXXXXXXX

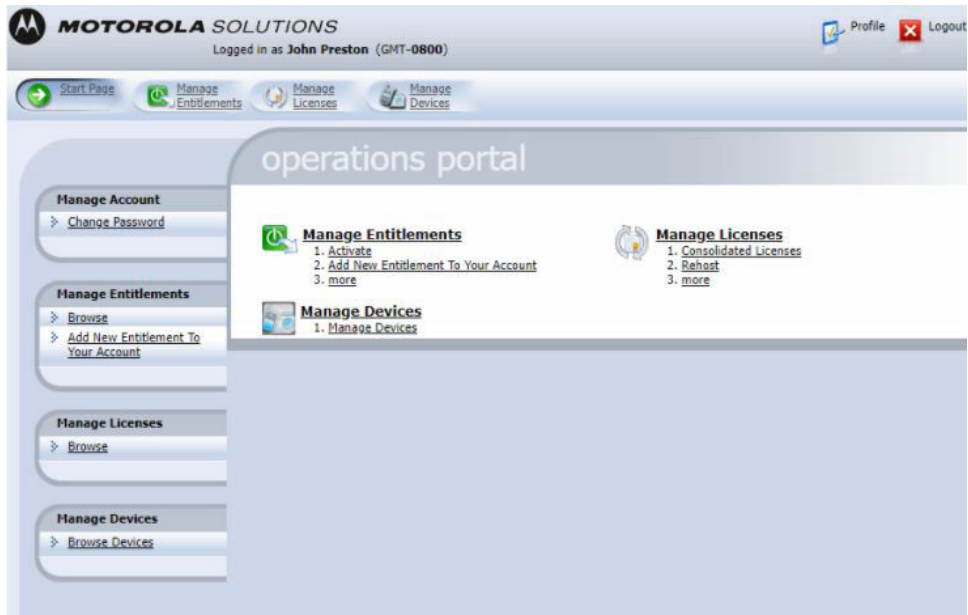
**4.2**

## Creating the License .BIN from the HOST ID File

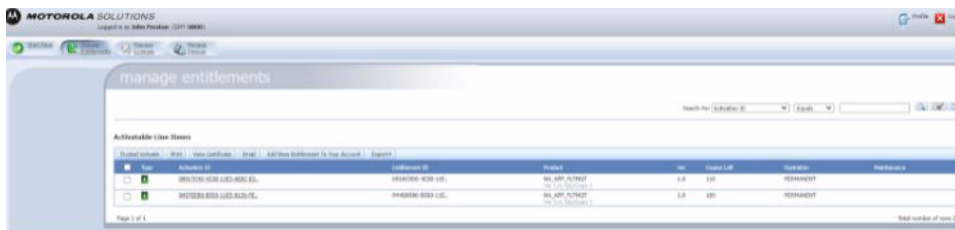
**Prerequisites:** Ensure that you have your `HOSTFILE.txt` (example: XXXXXXXXXXXX-10E7CXXXXXX) after you have completed the installation.

**Procedure:**

- 1 Login to the Motorola Solutions flex license server from the following link <https://licensing.motorolasolutions.com/flexnet/operationsportal/logon.do>



2 Click **Manage Entitlements** to add your EID.



3 In the **Manage Entitlement** page, select **Add New Entitlement**.



4 In the **Add New Entitlement to Your Account**, click the **MAP ID** button.

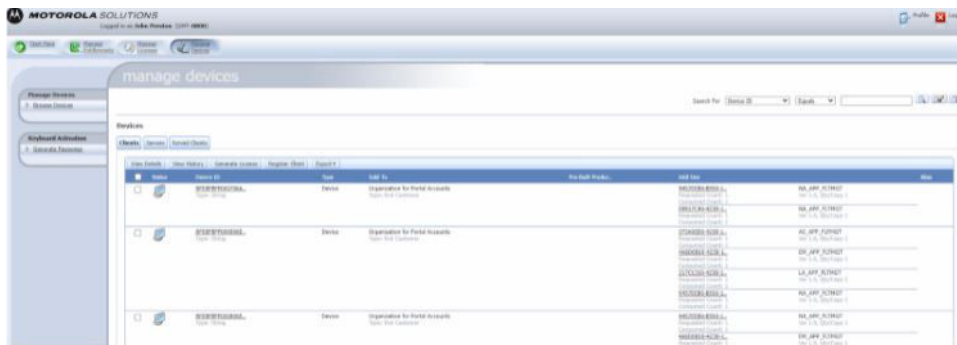


The ID is successfully mapped. The ID now appears in the entitlement lists.



5 In the **Manage Entitlements** page, select **Manage Devices**.

Wait for the page to load. The loading time depends on the number of devices.

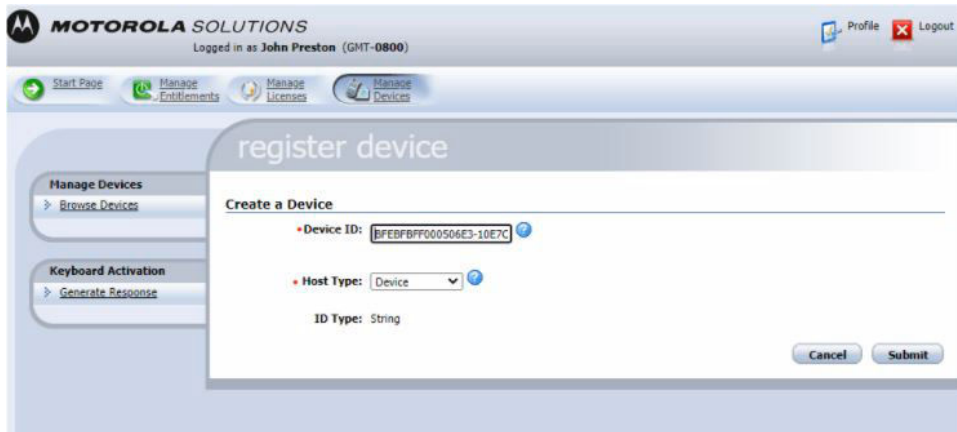


6 Select **Register Client** to generate a license.

7 Paste the content of the `HOSTID.txt` file into the **DeviceID** field.

8 Choose Device for the **Host Type** dropdown list.

9 Click **Submit**.



10 Fill up the required information.

11 Choose Add Ons for **Entitlement ID**.

12 Select the Entitlement ID.

13 Click **Save**.



Entitlement ID is displayed.

14 Click **Save**.



**NOTE:** If the license state shows **License not generated**, see [Generating License Successfully on page 34](#).

## Generating License Successfully

### Procedure:

- MOTOROLA** SOLUTIONS

Logged in as John Preston (347-6806)
 

Profile
 Logout

[Start Page](#)
[System Licenses](#)
[Device Licenses](#)
[Device Profiles](#)

## manage devices

### Edit Device

Device ID: 8P6BEPFF11056KD-10E70CEBFA0

Alias:

Type:

ID Type:

Publisher Identity:

Status:

Description:

#### End Customer and Channel Partners

Name	Contact	Email
End Customer		Organization For Public Accounts

#### Pre-Built License

Product	Product Version	License Model	Expiration	Date Filled
Pre-built license not yet generated.				

#### Add-Ons

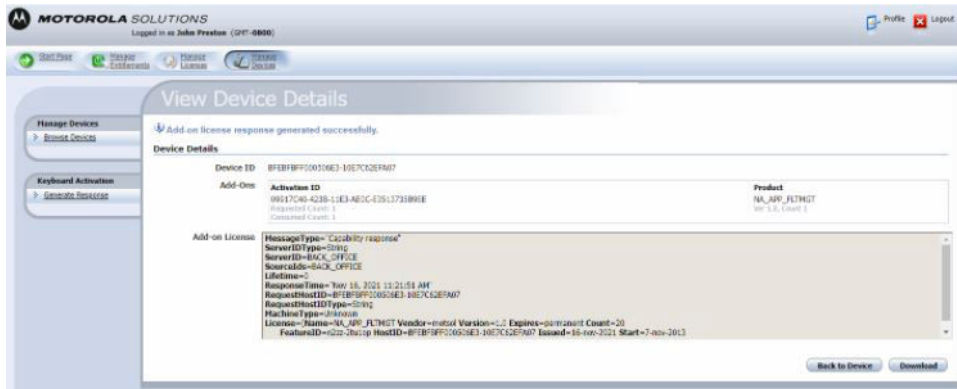
[Add Supplement Line Item](#)
[Remove Supplement Line Item](#)
[Generate License](#)

<input checked="" type="checkbox"/>	Supplement Line Item	Product	Expected Copies	Consumed Copies	Copies Left	Expiration	License State
<input type="checkbox"/>	8P6BEPFF-11056KD-10E70CEBFA0	NA_APP_UCHT 100 x 1.5, 120 x 1.5	<input type="text" value="1"/>	0	110	PERMANENT	License not generated

- 2 Select **Generate License**.
- 3 Select **No**.
- 4 Click **Generate**.



The license is now generated.



5 Click **Download**.

6 Save this BIN file to be used to complete the activation process.

**Postrequisites:** Use this BIN file to complete the offline activation process. See *MN007473A01 IMPRES™ Battery Fleet Management Installation Manual*

## Chapter 5

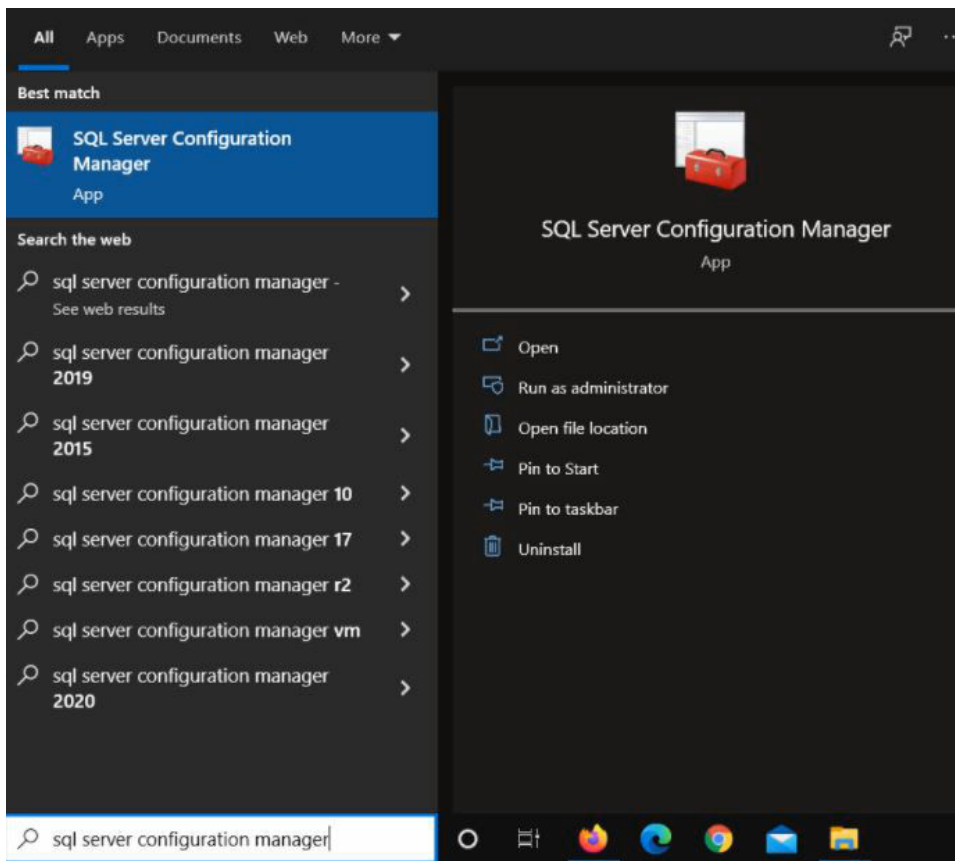
# Database Backup

### 5.1

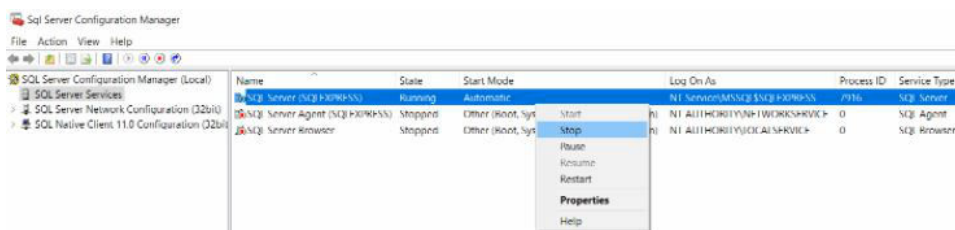
## Backing Up the Database

### Procedure:

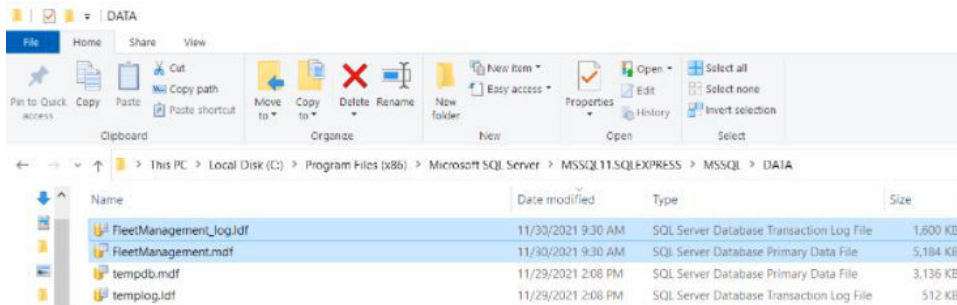
- 1 Open **SQL Server Configuration Manager**.



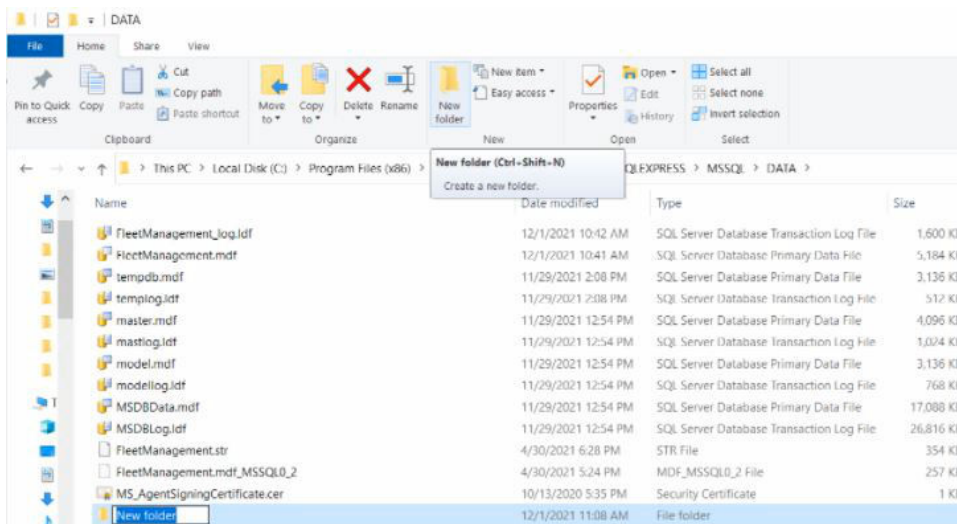
- 2 Select **SQL Server Configuration Manager**.
- 3 In the **SQL Server Configuration**, right-click on the main panel and select **Stop**.



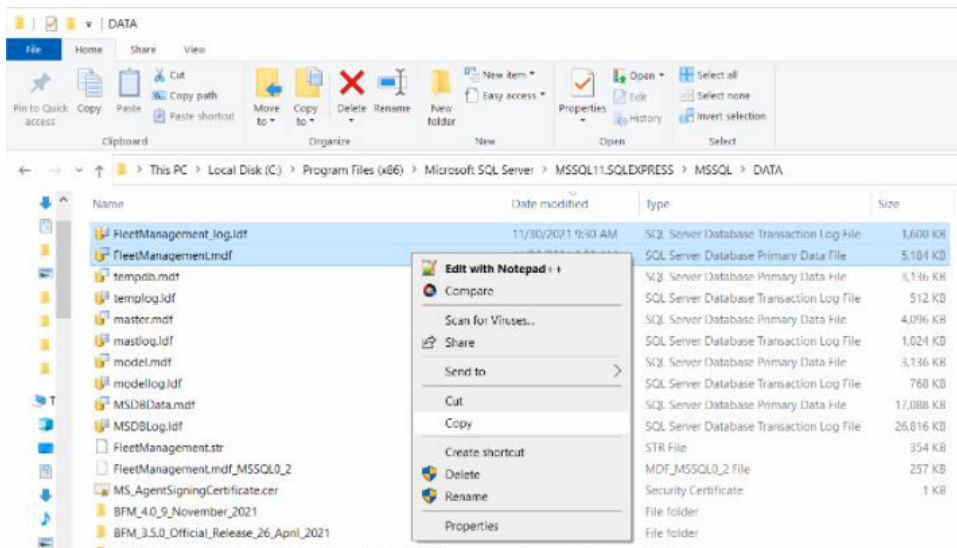
- 4 Navigate to C:\Program Files (x86)\Microsoft SQL Server\MSSQL11.SQLEXPRESS\MSSQL\DATAhighlight FleetManagement\_log.ldf and FleetManagement.mdf



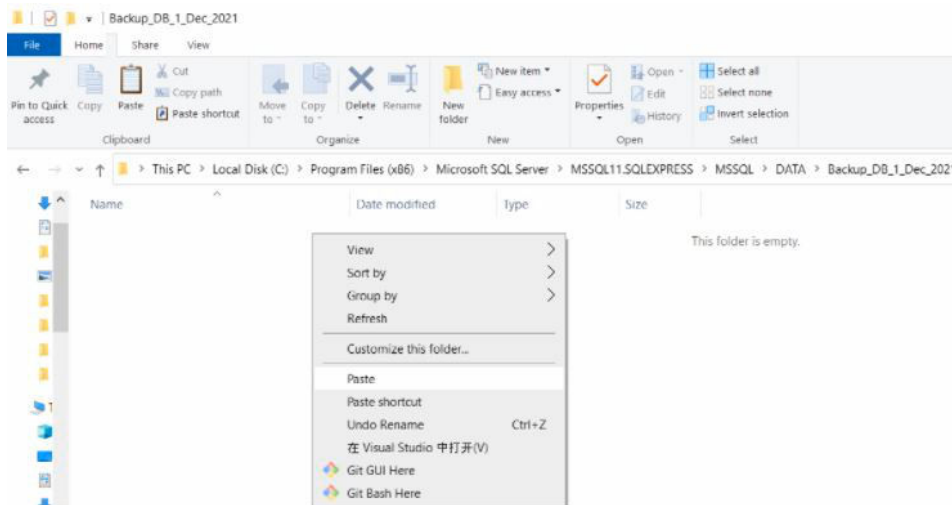
- 5 In C:\Program Files (x86)\Microsoft SQL Server\MSSQL11.SQLEXPRESS\MSSQL\DATA, right-click and select **New Folder**.



- 6 In C:\Program Files (x86)\Microsoft SQL Server\MSSQL11.SQLEXPRESS\MSSQL\DATA, right-click on the FleetManagement\_log.ldf and FleetManagement.mdf and select **Copy**.



- 7 In the newly created folder from [step 5](#) , right-click on a blank space and select **Paste**.



- 8 In the **SQL Server Configuration Manager**, right-click on the **SQL Server**.
- 9 Click **Start**.

## Chapter 6

# Restrictions on Windows Domains for BFM Client-Server Connections

The current BFM client-server connection uses a Windows NET socket configuration to communicate with each other. However, this connection requires that the client be in the same domain as the server. The following table indicates the relationships.

	<b>Cleint in Domain ABC</b>	<b>Client in Domain CDE</b>	<b>Client not in a Do- main</b>
Server in Domain ABC	Yes	No	Yes
Server not in Domain	No	No	No

## Chapter 7

# Enable ASTRO Over-The-Air Battery Management (OTABM) Feature

This feature is to aid the public safety customers to manage the long term health of the batteries. It is not meant to acquire the current real-time energy levels of all radios within the system.

This application is tightly integrated with functionality developed in the ASTRO subscriber radio as well as the ASTRO 25 Integrated voice and data trunked radio systems.

IMPRES Battery Management collects battery data from an Intelligent Middleware (IMW) server, which aggregates and manages sensor data from portable radios. This solution only supports Motorola Solutions IMPRES batteries on APX portable radios that are configured for the battery management feature. This solution does not work with 3rd party batteries or non-Motorola Solutions radios.

### 7.1

## Intelligent Middleware (IMW) Overview

Intelligent Middleware (IMW) is a suite of network services that enables interoperability between other applications and radio access networks such as PremierOne CAD and ASTRO 25 systems.

### IMW Presence Service Overview

IMW allows users and applications to receive a device or user presence status, which are present, absent, and unknown. IMW also uses Classic data service (IV&D) and allows an application to learn IP addresses and presence status of subscriber units.

A Username may be associated with different subscriber radios at different times, but the Device ID is always associated with the same radio. IMW provides the association between a Device ID and Username as well as the subscriber radio IP address and presence status information.

Licenses must be ordered to cover the number of radios that will use the IMW presence service. IMW presence service is required by each radio that will use the fleet management feature.

Table 3: Presence Service Licensing

Description	Nomenclature
Add: 0–100 Resources for Presence	UA00058AA
Add: 101–200 Resources for Presence	UA00059AA
Add: 201–400 Resources for Presence	UA00054AA
Add: 401–500 Resources for Presence	UA00055AA
Add: 501–1000 Resources for Presence	UA00056AA
Add: 1001–5000 Resources for Presence	UA00057AA

### Context (Sensor) Service Overview

Devices capable of linking with sensors and reporting sensor information can be associated with compatible sensors profiles in the Configuration Manager.



A license must be purchased per device that will report sensor or telemetry data.

Table 4: Context (Sensor) Service Licensing

Description	Nomenclature
UNS Resource Expansions	T8108
Add: Resources for Telemetry Service	UA00473AA

## 7.2

## Configuration Process for ASTRO OTA

The followings are the four configuration sections for ASTRO Over-the-Air (OTA):

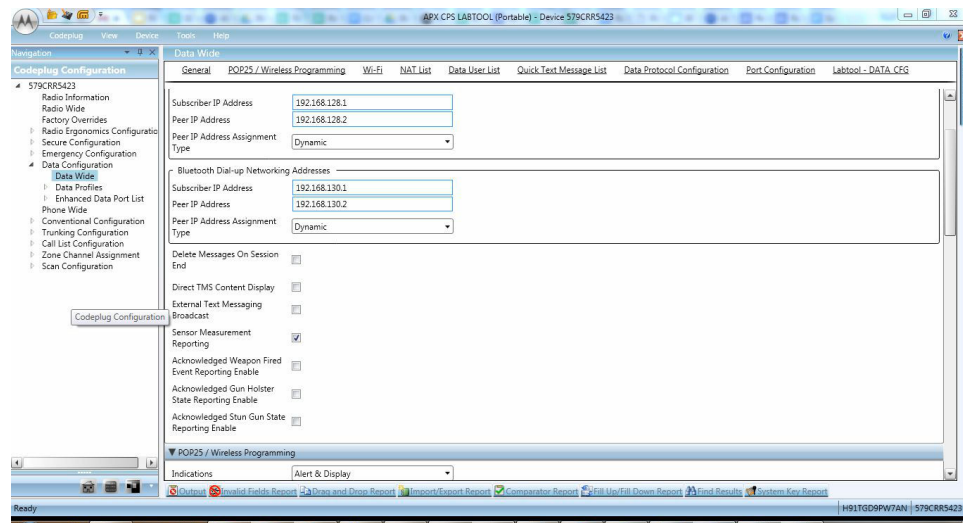
- Customer Programming Software (CPS) for subscriber
- Intelligent Middleware (IMW) Provisioning
- Identity Manager (IDM) Provisioning
- IMPRES Battery Fleet Management application

## 7.3

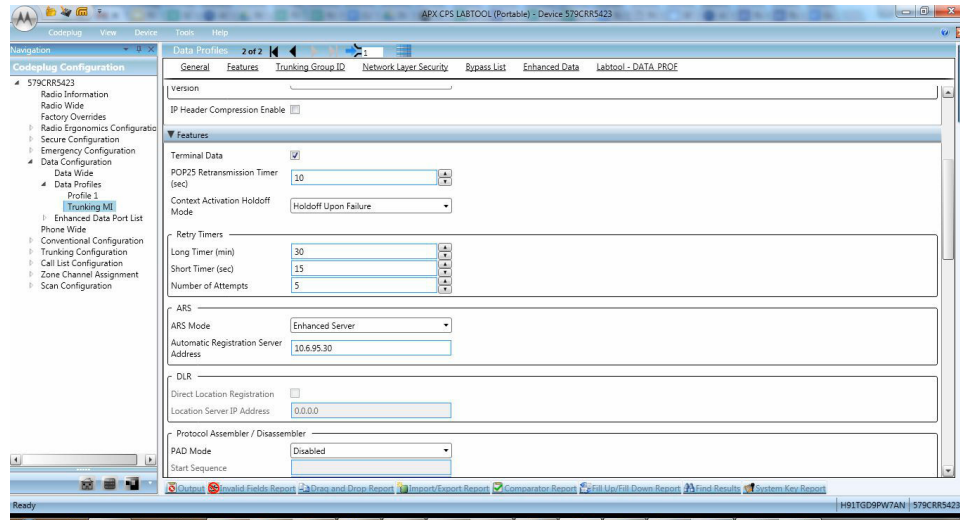
## Configuring CPS for Subscriber/Radios

Procedure:

- 1 To enable or provision the sensor capability on the radio, in Customer Programming Software (CPS), navigate to **Data Configuration→Data Wide→General→Sensor Measurement Reporting**.

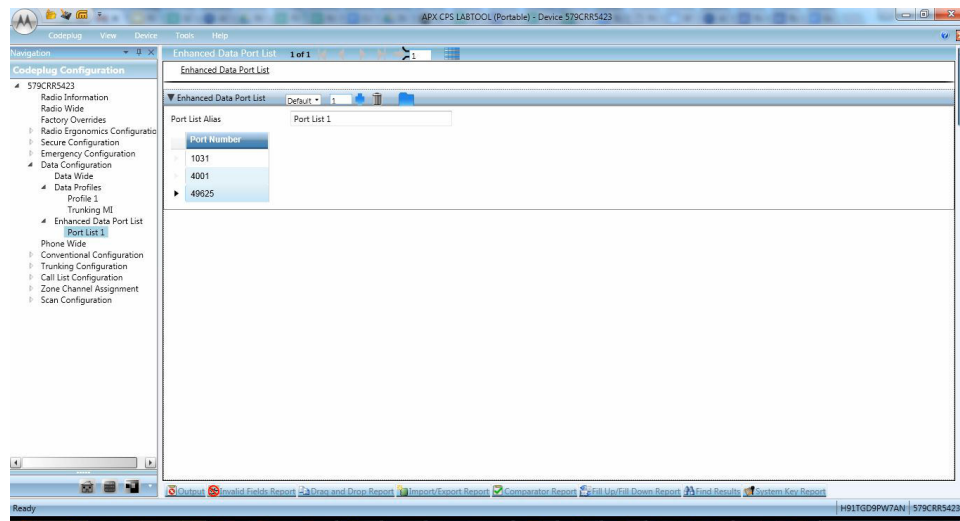


- 2 The following procedures are to enable or provision the ARS server mode on the radio:
  - 1 CPS - navigate to **Data Configuration→Data Profiles** and select the required profile.
  - 2 ARS - select **Enhanced Server** for ARS mode and enter the IP address of the IMW in the Automatic Registration Server Address field.



3 The following procedures are to enable or provision the Enhanced Data Ports:

- 1 CPS - navigate to **Data Configuration**→**Enhanced Data Port List**.
- 2 Port List Alias - Add **4001** (Location) and **49625** (Sensors).



## 7.4

### IMW Provisioning

The Intelligent Middleware (IMW) must be provisioned for the Battery Management feature.

Table 5: IMW Provisioning

Configurations	Description
Sensor configuration	Must be provisioned to inform the IMW that the battery management feature is in use
Application identity configuration	To provide authorization for the battery management server to access the IMW
Identity Manager	Configured a client ID, Name, and password to provide authorization for the battery management server to access the IMW

Configurations	Description
Device Identity	Records are used for each radio that uses the battery management feature and must be created or existing device identity records must be updated. These records identify each device, its group membership, and the configuration of which services each of each device is using.
Static group configuration	Battery management server can subscribe to a group of radios that are using the battery management feature. This allows the battery management server to be notified when any of the radios in this group turn on and registers with the IMW

For configuration, refer to [Creating a Sensor Profile](#).

## 7.5

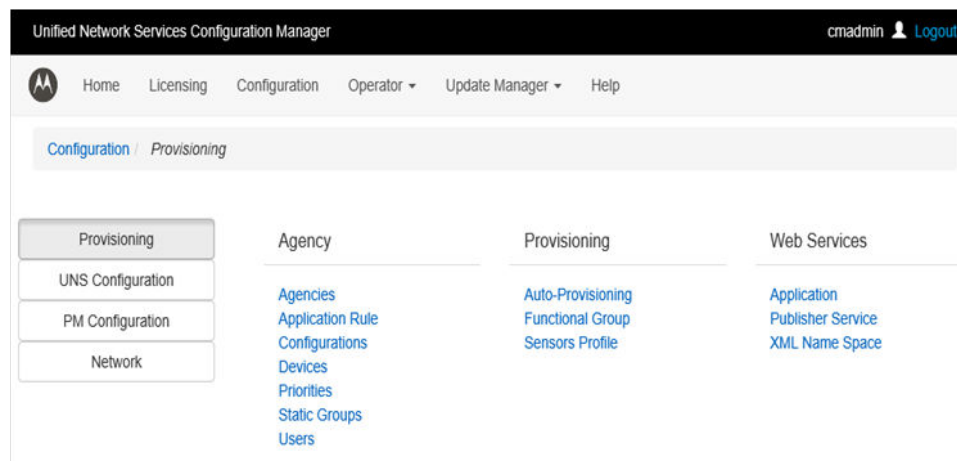
### Creating a Sensor Profile

#### IMW Configuration

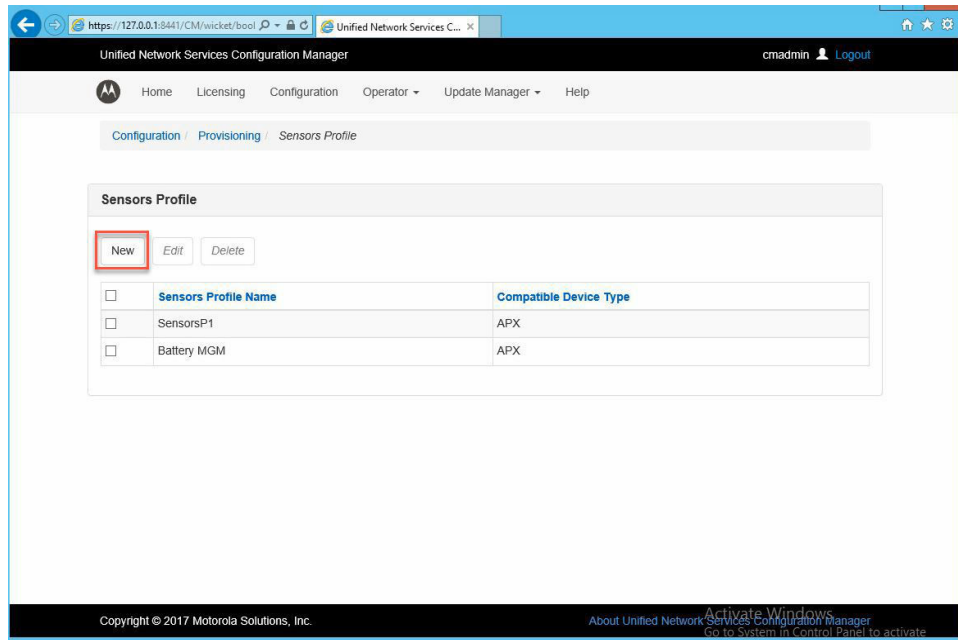
- Sensor Profile
- Application/User Creation
- Device Addition
  - Licenses
- Setup REST
  - IMW 5.2.2 and older
  - IMW 5.2.3
- API Endpoint
- Static Group

#### Procedure:

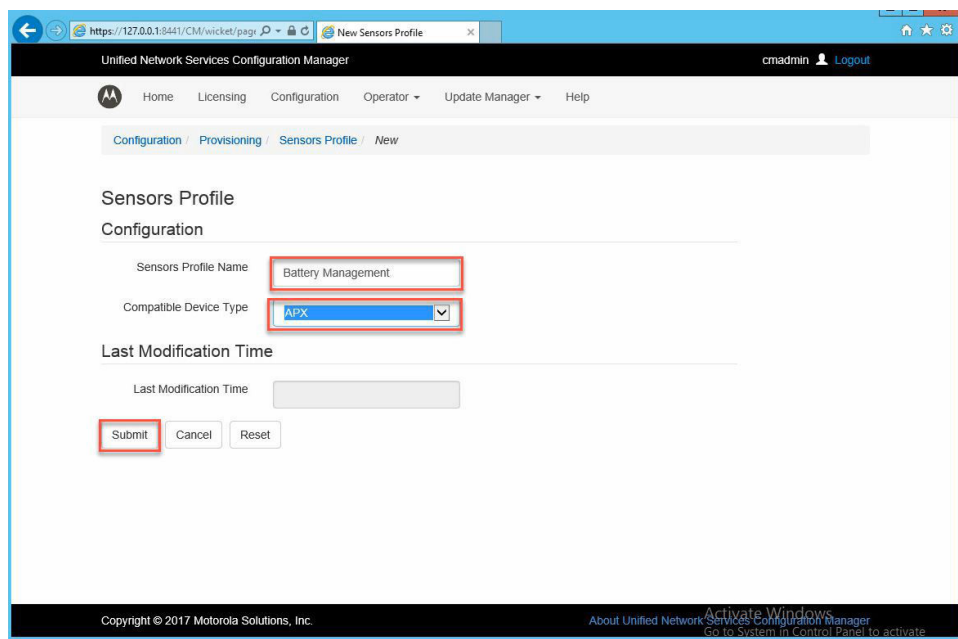
- 1 Log into the Intelligent Middleware (IMW) configuration manager and navigate to **Configuration/Provisioning/Sensors Profile**.



- 2 Add a new sensor profile for battery management.



- 3 Enter the profile name such as **Battery Management**.
- 4 Select **APX** for the compatible device type and click **Submit**.



- 5 Open up the newly created sensor profile and click **Associate** to select the Sensor Kit.

Sensor Kits

Associate

Delete

<input type="checkbox"/>	Sensor Kit Name
<input type="checkbox"/>	Battery

You do not need to edit the sensor configuration. The following is the sensor configuration.

Unified Network Services Configuration Manager

cmadmin Logout

Home Licensing Configuration Operator Update Manager Help

Sections

Configuration

Sensor Kits

Sensor Configurations

Sensor Kits

Associate

Delete

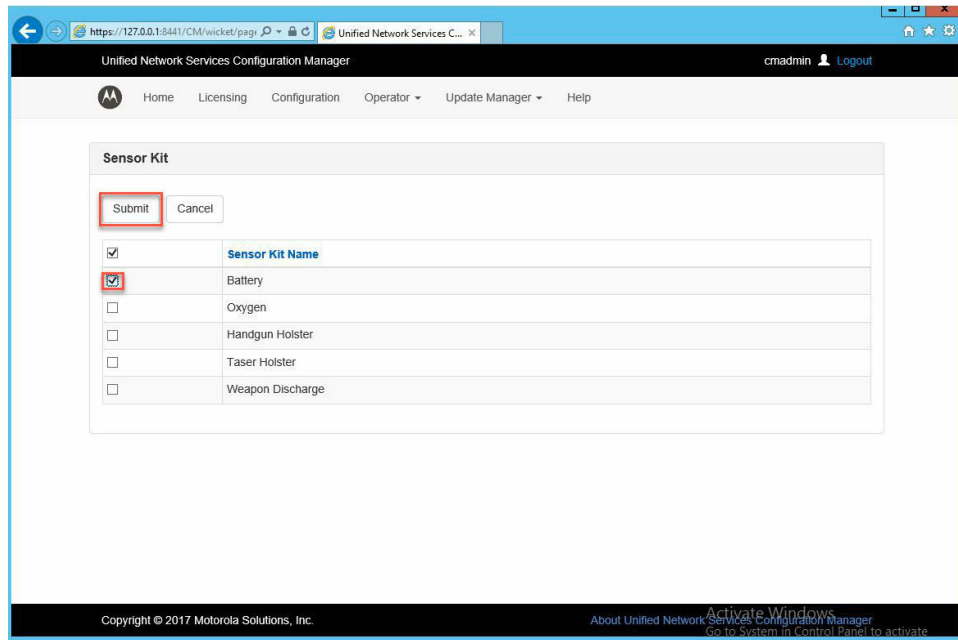
<input type="checkbox"/>	Sensor Kit Name
<input type="checkbox"/>	Battery

Sensor Configurations

Edit

<input type="checkbox"/>	Sensor Alias	Sensor Direction	Sensor Raise Description	Sensor Fall Description	Trigger Relationship	Trigger Value	Trigger Value Upper Range	Periodic Trigger Interval [seconds]
<input type="checkbox"/>	Battery Sensor	In			None			

6 Select the Battery Sensor kit name and click **Submit**.



## 7.6

### IMW Device Configuration

Every device in the system must be enabled for Presence and Context (Sensor Reporting). Existing devices might also have additional options depending on other uses in the system.

#### 7.6.1

#### For IMW versions 5.2.2 and older

##### Procedure:

- 1 In **Unified Network Services Configuration Manager** window, navigate to **Configuration/ Provisioning/Devices** and select each radio record that is used with the battery management feature.
- 2 Enable the following services:
  - Presence Service
  - Context Service

The screenshot shows the 'Unified Network Services Configuration Manager' web interface. The breadcrumb trail is 'Configuration / Provisioning / Devices / suid-bee00-039-00000c'. The 'Device Identity' section contains three text input fields: 'Device Name' (suid-bee00-039-00000c), 'Friendly Name' (suid-bee00-039-00000c), and 'Service ID' (504501390385117). The 'Configuration' section includes a 'Radio System' dropdown set to 'ASC'. Below this are four service configuration options, each with a radio button: 'Presence Service' (Allowed), 'Location Service' (Allowed), 'QoS Service' (Disallowed), and 'Context Service' (Allowed). The 'Allowed' radio buttons for 'Presence Service' and 'Context Service' are highlighted with red rectangles. At the bottom right, there is a 'Activate Windows' watermark.

### 7.6.2

## For IMW versions 5.2.3 onwards

### Procedure:

- 1 In Unified Network Services Configuration Manager window, navigate to **Configuration→Provisioning→Devices**.
- 2 Select the device to review or select **New** and verify the following information.
  - Device Name must be unique.
  - Friendly Name is use to help identify the device.
  - Service ID is an IMW internal tracking ID and can not be changed.
  - Network Device Identifier - Device ID on the ASTRO radio system.
  - Agency - Deployment dependant name. Used to structure the devices based typically based on a user's organizational structure

New

Edit

Delete

Edit all

<input checked="" type="checkbox"/>	Agency	Security Group	Device Name	Friendly Name
<input type="checkbox"/>	AIB	AIB	Radio03	APOUnit03
<input type="checkbox"/>	AIB	AIB	Radio02	APOUnit02
<input type="checkbox"/>	AIB	AIB	Radio04	APOUnit04
<input type="checkbox"/>	AIB	AIB	Radio05	APOUnit05
<input type="checkbox"/>	AIB	AIB	Radio06	APOUnit06
<input type="checkbox"/>	AIB	AIB	Radio07	APOUnit07
<input checked="" type="checkbox"/>	AIB	AIB	Radio20	APOUnit20

3 In Configuration, update the devices and verify the following information.

- Presence Service must be **Allowed**.
- Context Service must be **Allowed**.
- Security Group must match.
- Select the profile created in Sensor Profile.
- Network Device Identify is the ASTRO device ID.



## Configuration

Radio System	<input type="text" value="APO_AIB"/>	<input data-bbox="1242 294 1323 367" type="button" value="..."/>
Presence Service	<input checked="" type="radio"/> Allowed <input type="radio"/> Disallowed	
Location Service	<input checked="" type="radio"/> Allowed <input type="radio"/> Disallowed	
QoS Service	<input type="radio"/> Allowed <input checked="" type="radio"/> Disallowed	
Context Service	<input checked="" type="radio"/> Allowed <input type="radio"/> Disallowed	

Security Group	<input type="text" value="AIB"/>	<input data-bbox="1218 1050 1299 1123" type="button" value="..."/>
Functional Group	<input type="text" value="Default Functional Group"/>	<input data-bbox="1218 1155 1299 1228" type="button" value="..."/>
Location Network Profile	<input type="text" value="Location1"/>	<input data-bbox="1218 1260 1299 1333" type="button" value="..."/>
GPS Protocol	<input type="text" value="APX Trunked"/>	<input data-bbox="1218 1365 1299 1438" type="button" value="..."/>
	<input data-bbox="812 1438 852 1491" type="button" value="?"/>	
Associated Device	<input type="text"/>	<input data-bbox="1218 1522 1299 1596" type="button" value="..."/>
Sensors Profile	<input type="text" value="pa1_sensor"/>	<input data-bbox="1218 1627 1299 1701" type="button" value="..."/>

Network Device Identifier	<input type="text" value="20"/>
HPD Device IP Address	<input type="text"/>
<hr/>	
Last Modification Time	
Last Modification Time	<input type="text" value="2020-11-04 13:45:19"/>
<input type="button" value="Submit"/>	<input type="button" value="Cancel"/> <input type="button" value="Reset"/>

#### 4 Click **Submit**.

**Postrequisites:** Once all devices have been updated, perform a Delta Download in IMW.

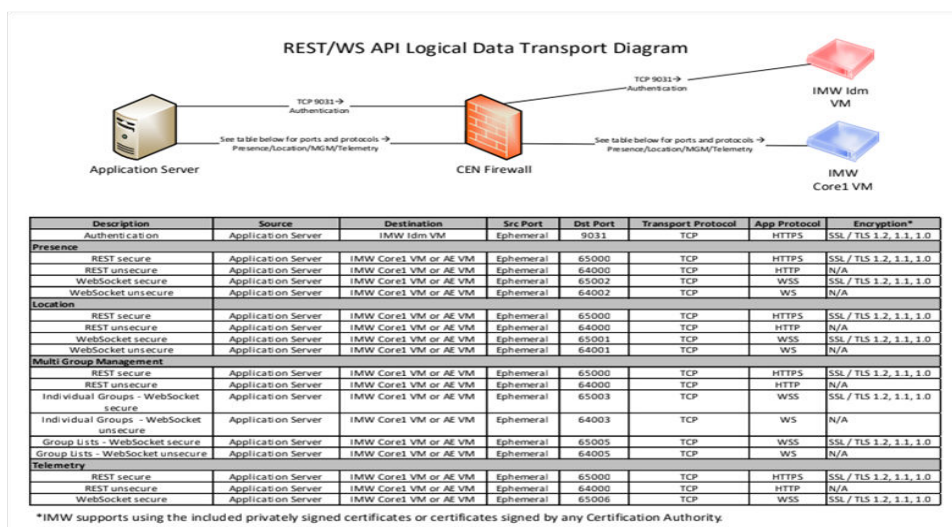
### 7.7

## IMW Representational State Transfer

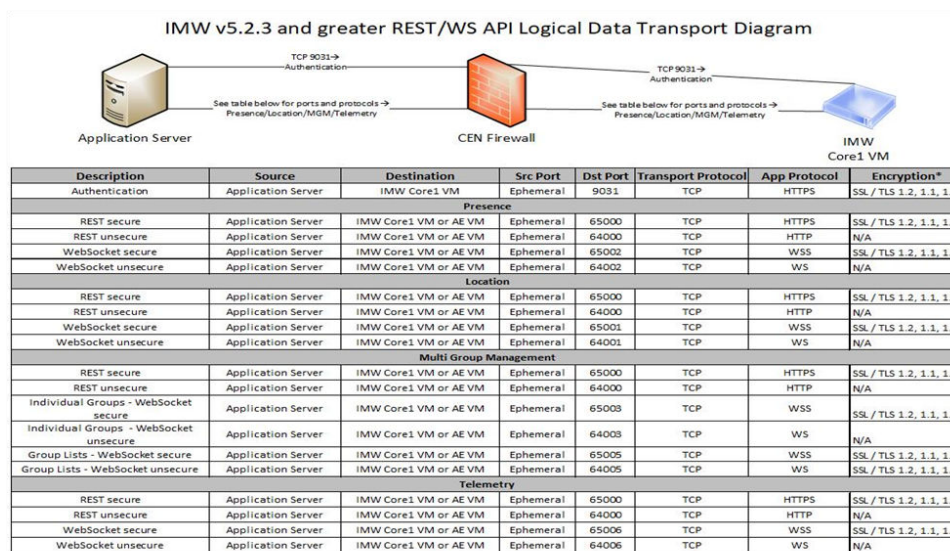
The IMW Representational State Transfer (REST) standard provides APIs similar to those defined by the 3GPP Parlay X standard but uses generally accepted REST API specifications.

The IMW interfaces are based on these standards, but also provide proprietary extensions to these interfaces. IMW REST and Web socket APIs provide query access to presence and location data, and messaging over HTTP or HTTPS. Subscription access to presence data, location data, group data, and context data are provided over Web sockets or Secure Web sockets. Requests and responses are encoded using the JavaScript Object Notation (JSON) format.

The following figure is applicable for IMW 5.2.1/5.2.2 only.



The following figure is applicable for IMW 5.2.3 only.



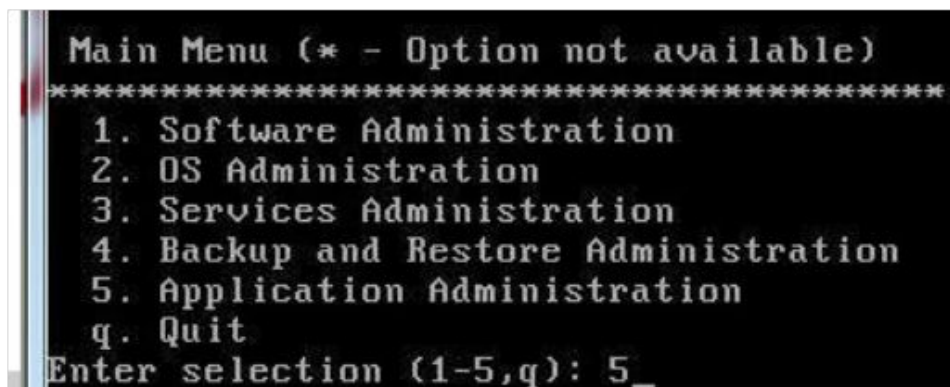
### 7.7.1

## IMW REST Setup for IMW 5.2.2 and Older

IMW versions 5.2.2 and older uses IDM.

### Procedure:

- 1 Connect into IDM Virtual Machine through the VSphere Console.
- 2 For Main Menu, select **5. Application Administration**.



- 3 For Application Administration, select **1. Identity Service Configuration**.
- 4 For Identity Service Configuration, select **2. Manage Credential Validator and Clients**.

```

Application Administration (* - Option not available)
*****
1. Identity Service Configuration
b. Back to Previous Menu
q. Quit
Enter selection (1,b,q): 1

Identity Service Configuration (* - Option not available)
*****
1. Configure Identity Service
2. Manage Credential Validator and Clients
3. Manage Database Passwords
4. Manage Certificates
5. Generate License Usage Reports
6. TLS configuration
b. Back to Previous Menu
q. Quit
Enter selection (1-6,b,q): 2_

```

- 5 Manage Credential Validator and Clients, select **6. Add Application Client**.
- 6 In Add Application Client, enter Client Id, Client Type, Client Password, Client Name, and Client Description.

```

Manage Credential Validator and Clients (* - Option not available)
*****
1. List Active Directories
2. Add Active Directory and SSOCClient
3. Remove Active Directory
4. Update Active Directory password
5. List Application Clients
6. Add Application Client
7. Delete Application Client
b. Back to Previous Menu
q. Quit
Enter selection (1-7,b,q): 6

Enter Client Id: BFM02
Enter Client Type [clientCredentials]:
Enter Client Password:
Enter Client Name [BFM02 ]: BFM02
Enter Client Description: Battery management server_

```



**NOTE:** This will be the Login and Password used in Battery Management

### 7.7.2

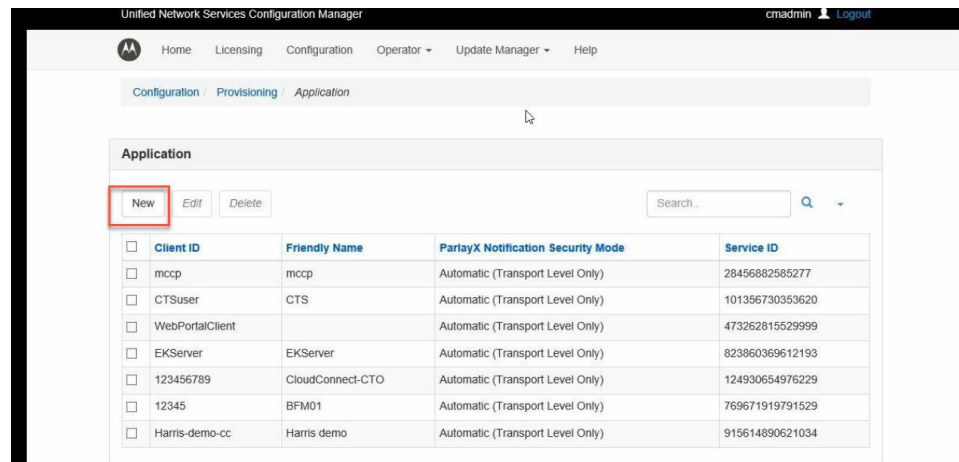
## User Creation for IMW 5.2.2 and Older

The client ID and password are the credentials used for the battery management application to connect to the IMW.

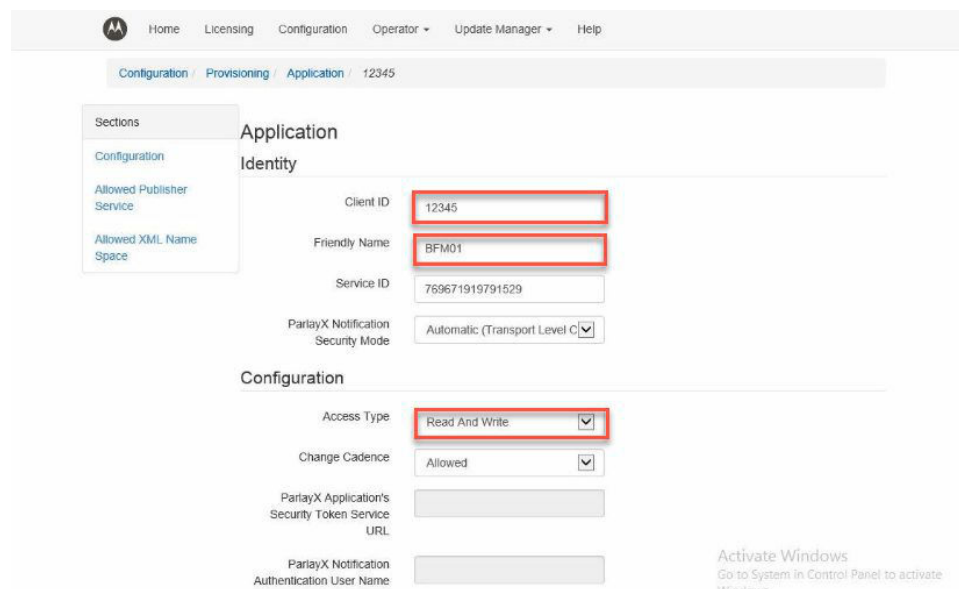
**Prerequisites:** The Client ID uses the same Username and Password as in section [Setting Up Client PC](#).

### Procedure:


- 1 To create a new application identity, navigate to **Configuration/Provisioning/Application→New**.



- 2 Provide the following information:
  - Client ID - Any decimal number
  - Friendly Name - Any name
- 3 Change the access type to **Read And Write**.



- 4 Create the application password.
 

 **NOTE:** The passwords have to be the same for all fields.
  - 5 Click **Submit**
- The Update Manager needs a **Full Configuration** download.

Home Licensing Configuration Operator Update Manager Help

URL

ParlayX Notification Authentication User Name

ParlayX Notification Authentication Password

Re-Enter ParlayX Notification Authentication Password

ParlayX API Access Password

Re-Enter ParlayX API Access Password

ParlayX API Access Locked

Last Modification Time

Last Modification Time 2018-05-03 12:50:54

Submit Cancel Reset

## 7.7.3

**IMW REST Setup for IMW 5.2.3 Onwards**

IMW version 5.2.3 and newer does not have IDM virtual Machine or Configuration. Functionality was migrated into the Core1 Virtual Machine. IMW 5.2.3 uses Application Configuration information.

## 7.7.4

**User Creation for IMW 5.2.3 Onwards****Procedure:**

- 1 To create a new application identity, navigate to **ConfigurationProvisioning/ Application→New**.

Home Licensing Configuration Operator Update Manager Help

Configuration / Provisioning / Application

Application

New Edit Delete

Search...

Client ID	Friendly Name	ParlayX Notification Security Mode	Service ID
mccp	mccp	Automatic (Transport Level Only)	28456882585277
CTSuser	CTS	Automatic (Transport Level Only)	101356730353620
WebPortalClient		Automatic (Transport Level Only)	473262815529999
EKServer	EKServer	Automatic (Transport Level Only)	823860369612193
123456789	CloudConnect-CTO	Automatic (Transport Level Only)	124930654976229
12345	BFM01	Automatic (Transport Level Only)	769671919791529

- 2 In **Application→Identity**, perform the following procedures:
  - a Enter the **Client ID**. Any decimal number can be used for this.
  - b Enter the **Friendly Name**. Any name can be used for this.
  - c Select the Interface Type as **ParlayREST**.

## Application

### Identity

Client ID	<input type="text" value="12345"/>
Friendly Name	<input type="text" value="BFM01"/>
Service ID	<input type="text" value="972139118258721"/>
Interface Type	<input type="text" value="ParlayREST"/> ▼
ParlayX Notification Security Mode	<input type="text" value="Automatic (Transport Level Only)"/> ▼

**3** In **Configuration**, perform the following procedures:

- a** Access Type should be set as **Read and Write**.
- b** API Access Password must follow complexity rules.



**NOTE:** This will be the Login and Password used in Battery Management.

- c** Select **No** for API Access Locked.
- d** Select **Yes** for Presence Access.
- e** Select **Yes** for Sensor Access.
- f** Others can be left at default.

**4** Click **Submit**.

**Postrequisites:** The update will require a Delta Update. Delta download can be done now or at the final configuration.

#### 7.7.5

### IMW Associated Application



**NOTE:** Applicable for all IMW releases.

**When and where to use:** Each application must be associated with an agency.

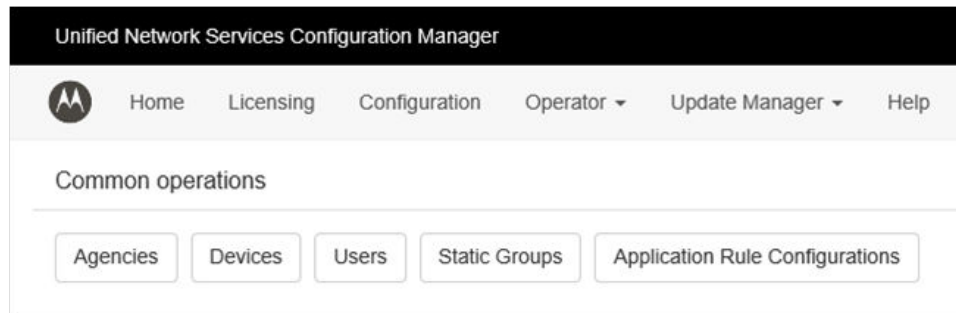
#### Procedure:

- 1** From the Home Screen, select **Agencies**.

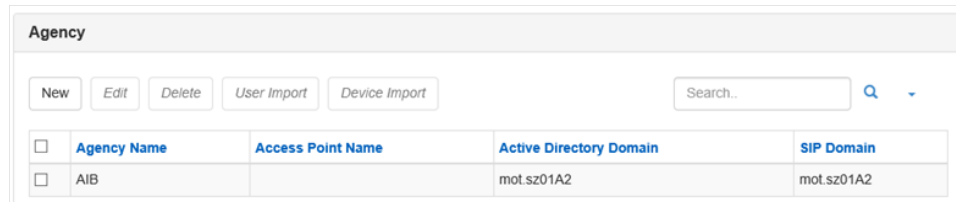


**NOTE:** An IMW might have multiple Agencies or a single.

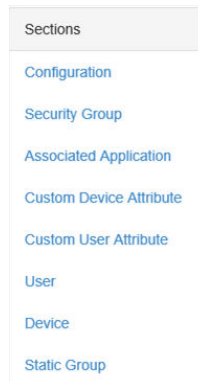




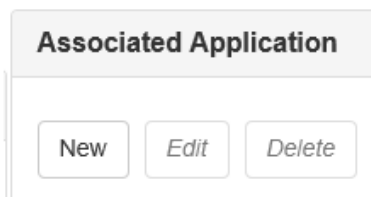
- 2 Select and edit the Agency that contains the devices being monitored.



- 3 Select **Associated Application**.



- 4 Select **New**. Insert two entries, one for the **Security Group** and one for the **Security Group\_apps**.



Final Screen shows the application name selected with Security Group and Security Group\_apps.



**Associated Application**

New
Edit
Delete

	Application	Security Group
<input type="checkbox"/>	12345	AIB
<input type="checkbox"/>	12345	AIB_apps

**Postrequisites:** A Delta Download is needed after this change.

## 7.8

### API Endpoint

API Endpoints are special-purpose virtual machines designed to meet the need for handling many subscriptions from dispatcher applications for query or subscribe over REST/WS for presence, location, telemetry, and mgm data.

Having multiple AE virtual machines enables Intelligent Middleware (IMW) to upscale the overall load of distributing notifications and handling queries (for presence or location) from several thousands of watchers. The IMW with AEs can be installed in the following configurations:

#### High Tier Software Installation

IMW core virtual machine and three separate AE virtual machines.

#### Low Tier Software Installation

AE services are installed on the IMW virtual machine with the other services.

Table 6: Low Tier versus High Tier Software Installation

Low Tier Software Installation	High Tier Software Installation
Non-Geo/Redundant	Geo/Redundant (Optional)
Low or High Tier Hardware	High Tier Hardware
-	Higher Capacity
-	Multiple (10 or more) ParlayX/REST Connection

## 7.8.1

### Configuring API Endpoint

#### Procedure:

- 1 To create a new API Endpoints, navigate to **Configuration/UNS Configuration/API Endpoints**.



**NOTE:** For the REST API to work, the Intelligent Middleware (IMW) needs a configured API Endpoint.

Unified Network Services Configuration Manager

Home Licensing Configuration Operator Update Manager Help

Configuration UNS Configuration API Endpoints

### API Endpoints Configuration

Transport Security Mode: Required (HTTPS and WSS only) ☒

Web Socket Lifetime: 8 hours ☒

Last Modification Time: 2016-07-19 17:40:15

Submit Cancel Reset

#### API Endpoint Instances

New Edit Delete

UNS 1 API Endpoint IP Address	UNS 2 API Endpoint IP Address
10.51.1.132	10.51.1.142

Provide the following information:

- Transport Security Mode - set to **Required (HTTPS and WSS only)**
- UNS 1 API Endpoint IP Address - Enter the Core1 (UNS) IP address from the IMW
- Web Socket Lifetime - 8 hours (Default)

If your system has 2 UNS that enter the other UNS IP address.



**NOTE:** If there are multiplier API Endpoints in the system, each API Endpoint must be filled in.

## 2 Configure the following settings:

Table 7: Low Tier and High Tier Configuration

Low Tier	High Tier
Create only AE1 (Another number can be used)	Create AE1, AE2, and AE3 (Numbers should match deployed Virtual machines)
Assign the IP address of Core1 VM	Assign IP addresses assigned to each Virtual Machine

## 3 Download the Delta configuration.

## 4 Perform the following actions:

Tier	Actions
Low Tier	<ul style="list-style-type: none"> <li>• On Core1 UNS Administrative Client. <ul style="list-style-type: none"> <li>• Stop all Services.</li> <li>• Restart all Services.</li> </ul> </li> </ul>
High Tier	<ul style="list-style-type: none"> <li>• On all 3 AEs UNS Administrative Client <ul style="list-style-type: none"> <li>• Stop all Services.</li> <li>• Restart all Services.</li> </ul> </li> <li>• On Core1 UNS Administrative Client</li> </ul>

Tier	Actions
	<ul style="list-style-type: none"> <li>• Stop all Services.</li> <li>• Restart all Services.</li> </ul>



**NOTE:** Screens will appear slightly differently on AE than on core 1.

- 5 Click **Submit**.
- 6 Navigate to **Update Manager/Delta Download** and select Agency and perform a **Delta Download**.

## 7.9

### IMW Static Group

A Static Group is a subset of devices associated together inside IMW during Runtime.

These devices must be part of the same Agency and should be part of a standard group. The Static Group is used as part of the REST/Websocket Presence and Location Subscriptions. IMPRES Fleet Management provides the updates for all members of a Static Group.

Some system will not have all devices monitored by IMPRES Fleet Management. In the case where only a subset of devices will be monitored, a custom static group can be created and the devices to be monitored can be assigned to this static group.

#### 7.9.1

### Configuring IMW Static Group

#### Procedure:

- 1 To create a new Static Group, navigate to **Configuration/Provisioning/Static Groups** and click **New**.



**NOTE:** It is also possible to use **sysgrp:all\_devices@SipDomain**. This is a predefined group of all devices. If all devices on this IMW use battery management, **sysgrp:all\_devices@SipDomain** can be used. SipDomain needs to be modified to the specific sip domain in use by the customer. If **all devices** selection is used, this step of creating a new static group can be skipped and **sysgrp:all\_devices@SipDomain** is entered in the battery management application configuration presentity field.

	Agency	Security Group	Static Group Name	Friendly Name
<input type="checkbox"/>	AIB	AIB	pa1-static	PA1 Static Group

- 2 Assign the Static Group to a single agency.

## Select agency for new static group

Select Agency

▼

OK

Cancel

- 3 Insert a Static Group Name and Friendly Name.



**NOTE:** The Static Group Name will be used in Battery Fleet Management as part of the Presentity.

## Static Group

### Identity

Static Group Name

BFM-Static

Friendly Name

Battery Fleet Mgt Static Group

### Configuration

Security Group

AIB

...

### Last Modification Time

Last Modification Time

Submit

Cancel

Reset

- 4 To change the Static Group into Multiple Static Groups, select the created Static Group and click **Edit**.

**Static Group**

New Edit Delete

Search..

	Agency	Security Group	Static Group Name	Friendly Name
<input type="checkbox"/>	AIB	AIB	pa1-static	PA1 Static Group
<input checked="" type="checkbox"/>	AIB	AIB	BFM-Static	Battery Fleet Mgt Static ...

- 5 To select devices to be associated with the Static Group, click **Associate Device**.



**NOTE:** Devices must be associated with the Static group or they will not report as part of the subscription.

**Static Group**

**Identity**

Static Group Name: BFM-Static

Friendly Name: Battery Fleet Mgt Static Group

**Configuration**

Security Group: AIB

**Last Modification Time**

Last Modification Time: 2021-01-25 11:46:18

Submit Cancel Reset

**Associated User, Device**

Associate User Associate Device Remove

Search..

	Name	Security Group	Type
No Records Found			

- 6 In the list of all the devices of the Agency, select each device to be added. Multiple selections is available, limited by the drop-down filter. Increase the drop-down filter if there are multiple pages to be added.

Device

Submit

Cancel

Search...

10

<input type="checkbox"/>	Device Name	Friendly Name	Security Group	Radio System	Presence Service	Location Service	QoS Service	Context Service	Group Management Service	Interoperability Capable	Network Device Identifier	HPD Device IP Address	Service ID
<input type="checkbox"/>	Radio03	APOUnit03	AIB	APO_AIB	Allowed	Allowed	Disallowed	Allowed	Disallowed	Disallowed	3		201408386993819
<input type="checkbox"/>	Radio02	APOUnit02	AIB	APO_AIB	Allowed	Allowed	Disallowed	Allowed	Disallowed	Disallowed	2		301594560259188
<input type="checkbox"/>	Radio04	APOUnit04	AIB	APO_AIB	Allowed	Allowed	Disallowed	Allowed	Disallowed	Disallowed	4		376543013819382
<input type="checkbox"/>	Radio05	APOUnit05	AIB	APO_AIB	Allowed	Allowed	Disallowed	Allowed	Disallowed	Disallowed	5		855297931585149
<input type="checkbox"/>	Radio06	APOUnit06	AIB	APO_AIB	Allowed	Allowed	Disallowed	Allowed	Disallowed	Disallowed	6		992448997422984
<input type="checkbox"/>	Radio07	APOUnit07	AIB	APO_AIB	Allowed	Allowed	Disallowed	Allowed	Disallowed	Disallowed	7		737931105922367
<input type="checkbox"/>	Radio20	APOUnit20	AIB	APO_AIB	Allowed	Allowed	Disallowed	Allowed	Disallowed	Disallowed	20		85942862079023
<input type="checkbox"/>	Radio08	APOUnit08	AIB	APO_AIB	Allowed	Allowed	Disallowed	Allowed	Disallowed	Disallowed	8		662417190240353
<input type="checkbox"/>	Radio09	APOUnit09	AIB	APO_AIB	Allowed	Allowed	Disallowed	Allowed	Disallowed	Disallowed	9		680244227035849
<input type="checkbox"/>	Radio10	APOUnit10	AIB	APO_AIB	Allowed	Allowed	Disallowed	Allowed	Disallowed	Disallowed	10		303204428354615

Showing 1 to 10 of 14

10

2

30

7 Click **Submit** for each selection.

## Chapter 8

# IMW SIP Domain

The IMW SIP Domain is used as part of the Presentity in Battery Fleet Management.

To find the SIP Domain, select Agency from the UNS Configuration Manager SIP Domain will be listed per Agency in the IMW.

Agency				
<div> <span>New</span> <span>Edit</span> <span>Delete</span> <span>User Import</span> <span>Device Import</span> </div> <div> <input type="text" value="Search.."/> <span>Q</span> <span>▼</span> </div>				
<input type="checkbox"/>	Agency Name	Access Point Name	Active Directory Domain	SIP Domain
<input type="checkbox"/>	AIB		mot.sz01A2	mot.sz01A2

## Chapter 9

# Checking the IMW Synchronization Status

Depending on the changes, the IMW requires either a Delta Download or a Full Download to push changes into the running database.

### Procedure:

- 1 To check for Synchronization Status, navigate to the **Update Manager**→**UNS Configuration Manager**.

The screenshot shows the 'Update Manager' interface. At the top, there is a navigation bar with links: Home, Licensing, Configuration, Operator, Update Manager, and Help. Below the navigation bar, there are two buttons: 'Download' and 'Refresh Synchronization Status'. To the right of these buttons, the 'System Synchronization Status' is displayed as 'Synchronized' in a green box, and the 'Last Synchronization Time' is '2021-01-26 19:50:00'. Below this, there is a dropdown menu with 'AIB' selected. The main section is titled 'Synchronization of Agency Objects' and contains a table with two columns: 'Data Category Name' and 'Synchronization Status'. The table has one row with 'Agency Provisioning Data' and 'Synchronized'.

Data Category Name	Synchronization Status
Agency Provisioning Data	Synchronized

- 2 Select **Delta Download**→**Agency**→**Refresh Synchronization Status**.

Your screen indicates one of the following results:

- Synchronized
- Delta Download Required
- Full Download Required

- 3 Perform one of the following actions:

Option	Actions
<b>Delta Download Required</b>	<ol style="list-style-type: none"> <li>Select <b>Agency</b>.</li> <li>Verify that there is no active downloads in the <b>Current Jobs</b> section.</li> <li>Select <b>Download</b>.</li> <li>Watch for job completion.</li> </ol>
<b>Full Download Required</b>	<ol style="list-style-type: none"> <li>Navigate to <b>Update Manager</b>→<b>Full Download</b>.</li> <li>Select <b>Application</b>.</li> <li>Verify that there is no active downloads.</li> <li>Select <b>Full Configuration Download</b>. Acknowledge the warning popup about now current downloads.</li> </ol>



Option	Actions
	<ul style="list-style-type: none"><li><b>e</b> Select <b>Yes</b>.</li><li><b>f</b> Verify Download Completion</li></ul>